Switch administrado

Manual de operación web



V1.0.0

Prefacio

General

Este manual presenta las operaciones en la interfaz web del conmutador RTL (en adelante denominado "el conmutador"). Puede visitar el interruptor en el navegador web, configurar y administrar el interruptor.

Instrucciones de seguridad

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

Palabras de advertencia	Significado
DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
NOTE	Proporciona información adicional como énfasis y complemento del texto.

Funciones utilizadas con frecuencia

Icono/Parámetro	Descripción
	Editar un elemento.
o**Borrar**	Elimine elementos uno por uno o en lotes.
o	Habilite o deshabilite elementos uno por uno o en lotes.
Actualizaro**Autorefrescar**	Actualizar o actualizar automáticamente el contenido.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	enero 2024

Aviso de protección de privacidad

Como usuario del Dispositivo o controlador de datos, usted puede recopilar datos personales de otras personas, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar información clara y visible.

identificación para informar a las personas de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Tabla de contenido

Prefacio..... I

1 Iniciar sesión..... 1

1.1 Inicializando el interruptor..... 1

1.2 Iniciar sesión..... 2

2 Configuración rápida..... 4

2.1 Configuración de información general..... 4

2.2 Información del puerto..... 5

2.3 ONVIF..... 6

2.4 Visualización de IPC y NVR..... 7

3 Mantenimiento..... 8

3.1 Configuración de la hora del sistema..... 8

3.2 Ver información legal..... 8

3.3 Cambio de contraseña..... 9

3.4 Configuración del firmware..... 9

3.5 Gestión de archivos..... 10

3.6 Ver información del dispositivo..... 10

3.7 Visualización de información de registro..... 11

3.8 Monitoreo de estado..... 12

3.9 Visualización del diagnóstico..... 12

3.10 Configurar la duplicación..... 13

4 Configuración de red..... 15

4.1 configurar puertos..... 15

4.2 Configuración de EEE..... dieciséis

4.3 Configuración de VLAN..... 17

4.3.1 Definición de VLAN..... 17

4.3.2 Función VLAN..... 17

4.3.3 VLAN basada en puerto..... 17

4.3.4 Agregar VLAN..... 18

4.3.5 Configuración del puerto VLAN..... 19

4.4 Configuración de VLANIF..... 20

4.5 Configuración de IP y enrutamiento..... 21

4.6 Configuración de ERPS..... 22

4.6.1 Configuración de ERPS..... 22

4.6.2 Configuración MEP..... 23

4.7 Configurar la vigilancia IGMP..... 24

4.8 Configuración de STP..... 25

4.8.1 PTS..... 25
4.8.2 Instancia de puerto..... 26
4.9 Configurar la agregación de enlaces..... 27
4.10 Configuración del protocolo SNMP..... 28
4.10.1 Configuración de SNMP V1 y V2..... 28
4.10.2 Configuración de SNMP V3..... 29
4.11 Configuración de la tabla MAC..... 31
4.11.1 Agregar tabla MAC..... 31
4.11.2 Puerto de filtrado MAC..... 32
4.12 Configuración de LLDP..... 33
5 Gestión de PoE..... 34
5.1 Configuración de los ajustes de PoE..... 34
5.2 Configurar PoE perpetuo..... 35
5.3 Configuración de PoE de larga distancia..... 35
5.4 Visualización de estadísticas de eventos PoE..... 36
5.5 Configuración de PoE verde..... 36
5.6 Configuración de Forzar PoE..... 37
5.7 Configuración del perro guardián PoE..... 37
6 Seguridad..... 39
6.1 Servicios Básicos..... 39
6.1.1 Configuración de servicios básicos..... 39
6.1.2 Configurar HTTPS..... 39
6.2 Configuración del certificado CA..... 40
6.2.1 Instalación del certificado del dispositivo..... 40
6.2.2 Instalación de certificados de CA de confianza..... 41
6.3 Configurar la defensa contra ataques..... 42
6.3.1 Configurar el cortafuegos..... 42
6.3.2 Configuración del ataque Anti-DoS..... 44
6.4 Configuración del aislamiento de puertos..... 44
7 Política de Control..... 45
7.1 Configuración de la prioridad del puerto..... 45
7.2 Configuración de la tabla de asignación de prioridades..... 45
7.3 Configuración de la programación de colas..... 46
7.4 Configuración del límite de velocidad del puerto..... 47
7.5 Configurar el control de tormentas..... 47
8 Autenticación..... 49
8.1 Configuración de 802.1x..... 49
8.2 Configuración del radio..... 50
Apéndice 1 Recomendaciones de ciberseguridad..... 51

1.1 Inicializando el interruptor

Requisitos previos

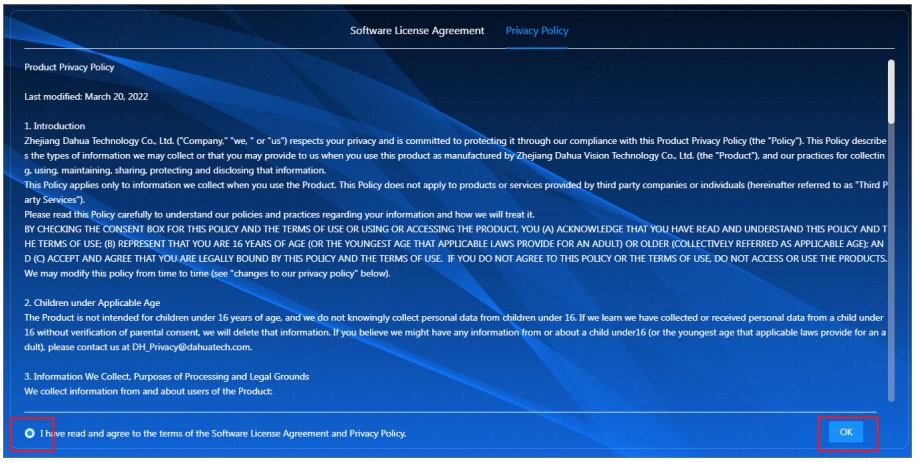
Antes de iniciar sesión, asegúrese de que el conmutador y el dispositivo de configuración estén conectados y encendidos.

Procedimiento

Paso 1 Abra el navegador IE, ingrese la dirección IP (192.168.1.110 de forma predeterminada) del conmutador en la barra de direcciones del navegador web y luego presione la tecla Enter.

Paso 2 Leer**acuerdo de licencia de software**y**política de privacidad**, haga clic**He leído y acepto los términos del Acuerdo de licencia de software y la Política de privacidad**y luego haga clic en**DE ACUERDO**.

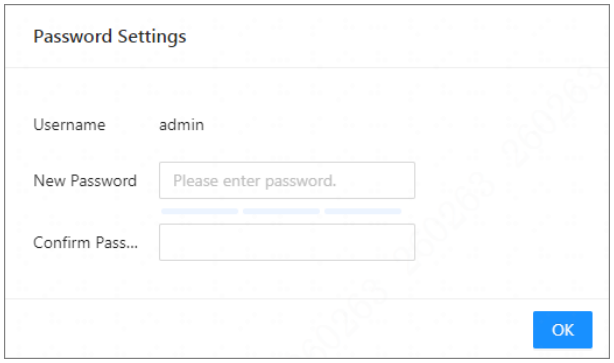
Figura 1-1 Política de lectura



Paso 3 Establezca la contraseña del usuario administrador.

El nombre de usuario es admin y la contraseña es personalizada.

Figura 1-2 Establecer contraseña



Etapa 4 Hacer clic**DE ACUERDO**.

1.2 Iniciar sesión

Requisitos previos

Antes de iniciar sesión, asegúrese de:

- Ya ha configurado la dirección IP del conmutador. La dirección IP de la VLAN 1 es 192.168.1.110 de forma predeterminada.
- La computadora está conectada a la red y puede hacer ping al conmutador.

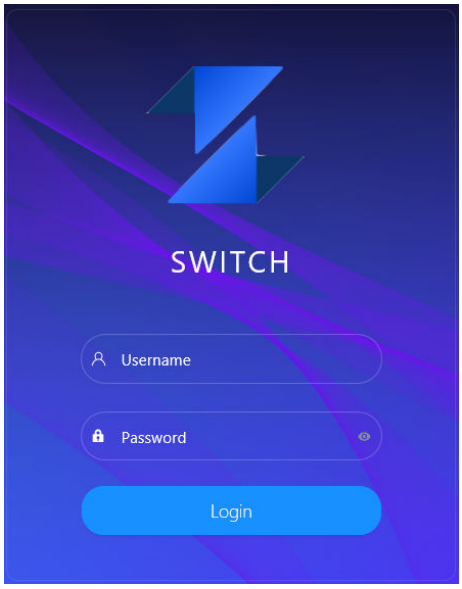
Procedimiento

Paso 1 Ingrese la dirección IP (192.168.1.110 de forma predeterminada) del conmutador en la barra de direcciones del navegador web y luego presione la tecla Intro.

Paso 2 Ingrese el nombre de usuario y la contraseña.

Paso 3 Hacer clic**Acceso**.

Figura 1-3 Iniciar sesión



- Cambie la contraseña después del primer inicio de sesión. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).
- Para obtener detalles sobre cómo cambiar la contraseña, consulte "3.3 Cambio de contraseña".

Figura 1-4 Página de inicio

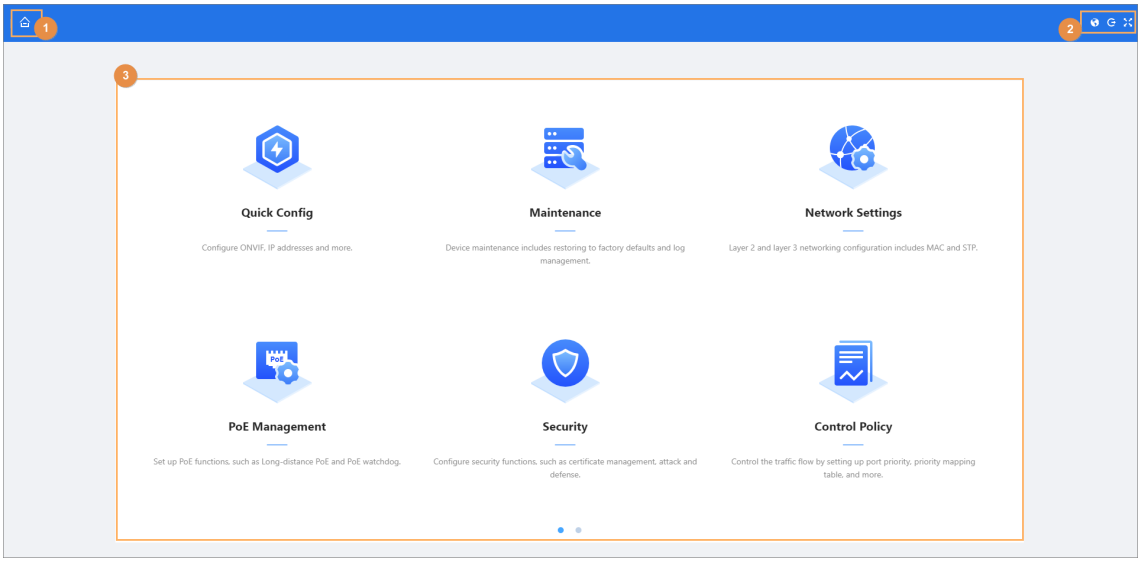


Tabla 1-1 Descripción de la página de inicio

No.	Nombre	Descripción
1		Vuelve a la página de inicio.
2		Cambie los idiomas del sistema. Soporta múltiples idiomas.
		Cierre la sesión del usuario y luego regrese a la página de inicio de sesión.
		La pantalla completa muestra la página web.
3	Indicación de estado	Vea en vivo el estado actual del interruptor.
	Configuración rápida	Configure ajustes rápidos, incluidos ONVIF, dirección IP y más.
	Mantenimiento	Configure los ajustes de mantenimiento, incluida la restauración a los valores predeterminados de fábrica y la gestión de registros.
	Configuración de la red	Configure los ajustes de red, incluidos los ajustes MAC y STP.
	Gestión de PoE	Configure los ajustes de PoE, incluidos PoE de larga distancia y vigilancia de PoE.
	Seguridad	Configure los ajustes de seguridad, incluida la gestión de certificados, ataques y defensa.
	Política de control	Configure los ajustes del flujo de tráfico, incluida la configuración de la prioridad del puerto, la tabla de asignación de prioridades y más.
	Autenticación	Configure la gestión de autenticación, incluidos 802.1x y RADIUS.

2 Configuración rápida

Puede ver la información del sistema y configurar los parámetros del conmutador, incluidos ONVIF, dirección IP y más. Las páginas del manual son solo de referencia y pueden diferir de las páginas reales.

2.1 Configuración de información general

Puede ver y configurar la información general, incluido el nombre, la dirección IP, la máscara de subred y la puerta de enlace predeterminada.

Procedimiento

Paso 1 Seleccionar**Configuración rápida**>**General**.

Paso 2 Puede ver y configurar la información general del conmutador.

Paso 3 (Opcional) Haga clic para habilitar la función DHCP.

Tenga en cuenta esta función. Una vez que DHCP esté habilitado, el enrutador o el servidor DHCP conectado con el conmutador asignará automáticamente una dirección IP al conmutador. La dirección IP original no podrá acceder a la página web.

Figura 2-1 Información general

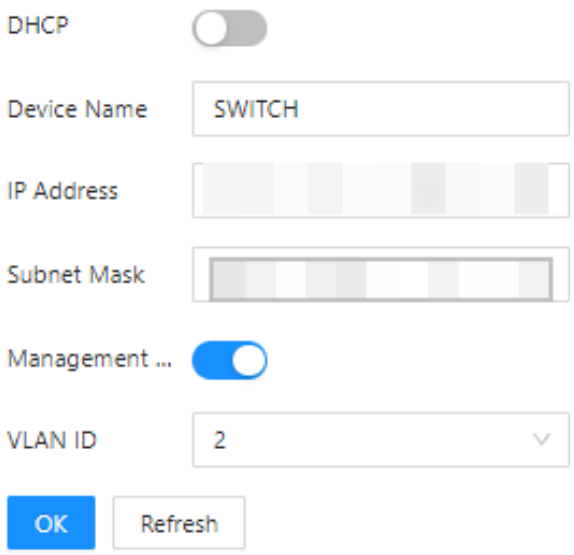


Tabla 2-1 Descripción de información general

Parámetro	Descripción
DHCP	Admite la habilitación de DHCP. Después de habilitar DHCP, se adquirirá y asignará automáticamente una nueva IP. Antes de asignar una nueva IP, se adopta la IP predeterminada 192.168.1.110.
Nombre del dispositivo	Muestra el nombre del dispositivo actual. Soporte para cambiar el nombre.
Dirección IP	Muestra la dirección IP actual. Admite configuración manual.
Máscara de subred	Admite ingresar la máscara de subred.

Parámetro	Descripción
VLAN administrada	Después**VLAN administrada**está habilitado, solo puede acceder a la página web a través de la IP de la VLAN administrada.
ID de VLAN	Muestra la ID de VLAN administrada actual.

2.2 Información del puerto

Puede ver información que incluye puerto, tipo, estado del enlace, velocidad/dúplex, VLAN, uso de RX, uso de TX y tipo de medio del conmutador.

Procedimiento

Paso 1 Seleccionar**Configuración rápida**>**Información del puerto**.

Paso 2 Vea la información del puerto del conmutador.

Figura 2-2 Información del puerto

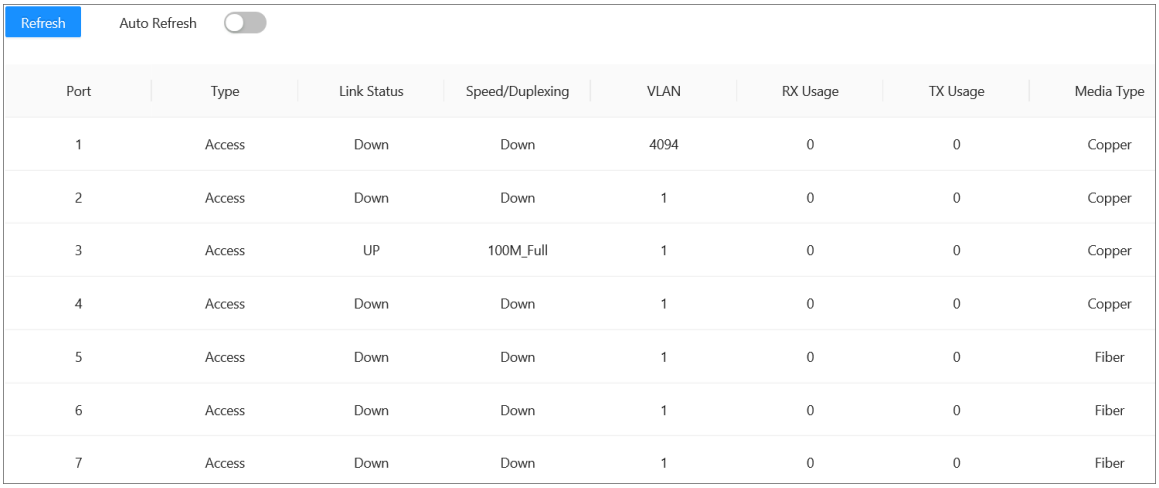


Tabla 2-2 Descripción de la información del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Descripción	Establezca la descripción del puerto. Admite la introducción de números, letras y caracteres especiales, independientemente de mayúsculas y minúsculas. Se pueden utilizar hasta 16 caracteres que no estén en blanco. No hay descripción por defecto.
Tipo	Incluye tres tipos:**Acceso**,**Híbrido**, y**Trompa**.
Estado del enlace	Incluye dos estados:**Arriba**y**Abajo**. ● Arriba: El puerto está conectado. ● Abajo: El puerto no está conectado o la conexión falla.
Velocidad/Dúplex	● En línea: muestra la velocidad del puerto y el modo dúplex. ● Sin conexión: pantallas**Abajo**.
VLAN	Puerto VLAN. VLAN 1 de forma predeterminada.
Uso de RX	Muestra el uso de recepción.

Parámetro	Descripción
uso de transmisión	Muestra el uso de envío.
Tipo de medio	Incluye dos tipos:**Cobre**y**Fibra**. ● Cobre: puerto RJ-45. ● Fibra: Puerto de fibra.

Operaciones relacionadas

- Hacer clic**Actualizar**para actualizar manualmente la información del puerto.
- Haga clic al lado de**Autorefrescar**para habilitar la actualización automática.

2.3 ONVIF

Seleccionar**Configuración rápida**>**Información del puerto**, puede ver la información del puerto del conmutador.

Hacer clic para habilitar la función de visualización ONVIF. Después de habilitar, la página muestra todos los puertos y el estado de conexión del interruptor.

- Puerto verde: indica una conexión exitosa.
- Puerto azul claro: Indica que no hay conexión o hay un error en la conexión.

Los diferentes modelos están equipados con diferente número de puertos. La siguiente figura es sólo como referencia. Consulte el producto real.

Figura 2-3 Información ONVIF



Tabla 2-3 Descripciones de puertos

Nombre	Descripción
Puerto	Muestra el número de puerto.
Descripción	Muestra la descripción del puerto.
Tipo de puerto	Incluye tres tipos:**Acceso**,**Híbrido**, y**Trompa**.
Estado del enlace	Incluye dos estados:**Arriba**y**Abajo**. ● Arriba: El puerto está conectado. ● Abajo: El puerto no está conectado o la conexión falla.
Estado de control de flujo	Verifique el estado de la función de control de flujo.

Nombre	Descripción
Velocidad/Dúplex	• En línea: muestra la velocidad del puerto y el modo dúplex. • Sin conexión: pantallas**Abajo**.
VLAN	Puerto VLAN. VLAN 1 de forma predeterminada.
PoE	Muestra el consumo de energía PoE. • Los conmutadores que no son PoE no admiten esta función. • Los diferentes modelos están equipados con diferentes números de puertos PoE. Consulte el producto real.
Uso de RX	La tarifa de recepción actual dividida por la tarifa real negociada durante un período de tiempo (normalmente 5 minutos).
Uso de transmisión	La tarifa de envío actual dividida por la tarifa real negociada durante un período de tiempo (normalmente 5 minutos).
Tipo de medio	Incluye dos tipos:**Cobre**y**Fibra**. • Cobre: puerto RJ-45. • Fibra: Puerto de fibra.

2.4 Visualización de IPC y NVR

Seleccionar**Configuración rápida**>**IPC y NVR**, puede ver la información del IPC, NVR y otros dispositivos conectados al conmutador.

3 Mantenimiento

3.1 Configuración de la hora del sistema

Puede ver y configurar la hora del sistema del conmutador.

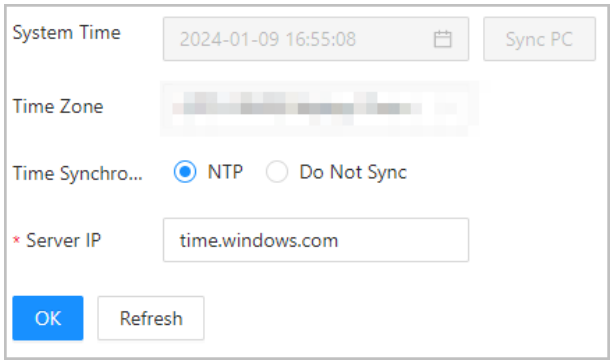
Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Hora del sistema**.

Paso 2 Configure la hora del sistema. Hay 3 métodos:

- Configurar manualmente el**Hora del sistema**y**Zona horaria**y luego haga clic en**DE ACUERDO**.
- Hacer clic**Sincronizar PC**para sincronizar la hora del interruptor con la hora de la computadora.
- Hacer clic para sincronizar la hora del cambio con la hora del servidor y luego haga clic en**DE ACUERDO**.

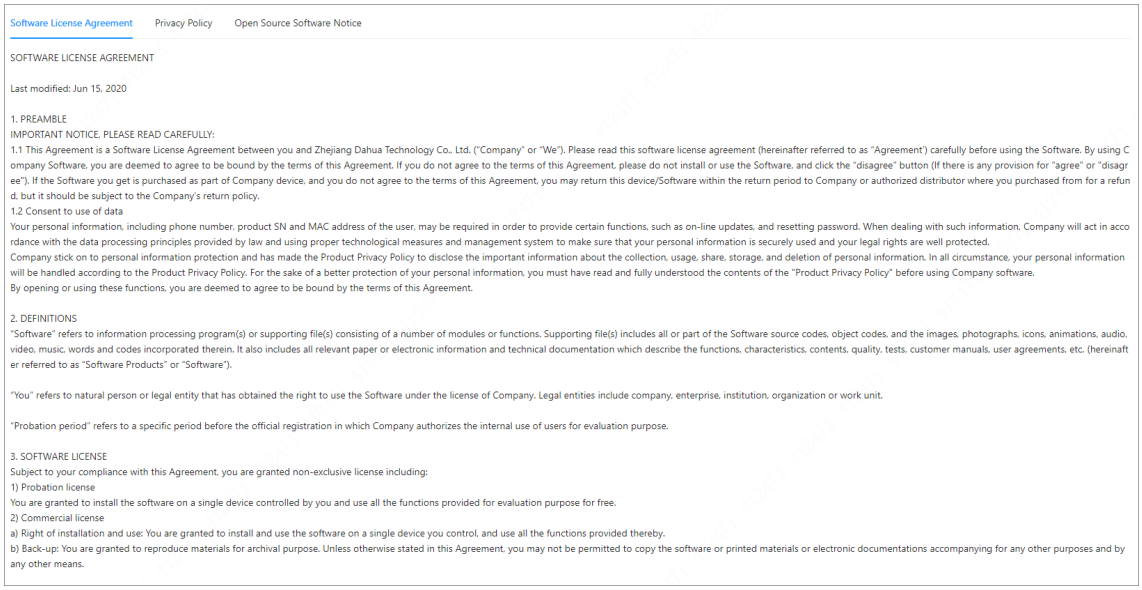
Figura 3-1 Configurar la hora



3.2 Ver información legal

Seleccionar**Mantenimiento**>**Información legal**, puedes ver**Aviso sobre software de código abierto**.

Figura 3-2 Información legal



3.3 Cambiar contraseña

Información de contexto

- Para utilizar la función iLinksView, el nombre de usuario y la contraseña de la plataforma iLinksView y el conmutador deben ser los mismos.
- El nombre de usuario es admin de forma predeterminada y no se puede cambiar.

Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Cambiar la contraseña**.

Paso 2 Ingresar**Contraseña anterior**,**Nueva contraseña**y**confirmar Contraseña**.

La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).

Paso 3 Seleccione la hora en que caduca la contraseña en la lista de**La contraseña caduca en**.

Puedes elegir**La contraseña caduca en**desde nunca, 30 días, 60 días, 90 días y 180 días. Hacer clic**DE**

Etapa 4 **ACUERDO**.

3.4 Configuración del firmware

Seleccionar**Mantenimiento**>**Configuración de firmware**, puede restaurar el dispositivo, actualizar el sistema y reiniciar el interruptor.

Restaurar los valores predeterminados de fábrica

Hacer clic**Restaurar los valores predeterminados de fábrica**para restaurar todos los parámetros del dispositivo a los valores predeterminados de fábrica.

Todos los parámetros se restauran a la configuración predeterminada excepto la dirección IP de la VLAN1.

Restaurar los valores predeterminados de fábrica

Hacer clic**Restaurar ahora**para restaurar todos los parámetros del dispositivo a los valores predeterminados de fábrica.

Todos los parámetros se restauran a la configuración predeterminada excepto la dirección IP de la VLAN1.

Actualiza el software

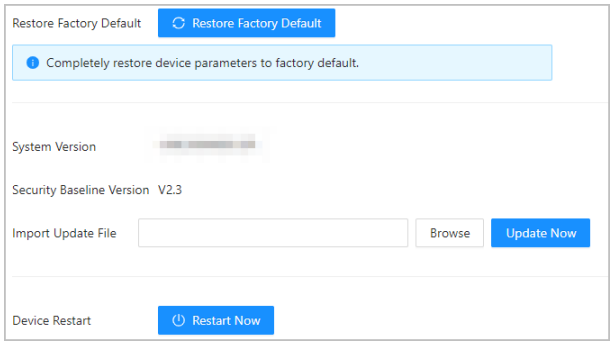
Hacer clic**Navegar**para importar el archivo de actualización y luego haga clic en**Actualizar ahora**.

La actualización del software puede tardar 3 minutos. Después de la actualización, el sistema se reiniciará automáticamente.

Reiniciar el dipositivo

Hacer clic**Reiniciar ahora**para reiniciar el dispositivo.

Figura 3-3 Configuración del firmware



3.5 Gestión de archivos

Puede configurar el archivo de copia de seguridad y restaurar el archivo.

Configuración de copia de seguridad

Recomendamos hacer una copia de seguridad de los registros para referencia futura.

Seleccionar**Mantenimiento**>**Gestión de archivos**>**Configuración de copia de seguridad**, haga clic**Exportar archivo de configuración**para exportar el archivo.

Configuración de restauración

Recomendamos hacer una copia de seguridad de los registros para referencia futura.

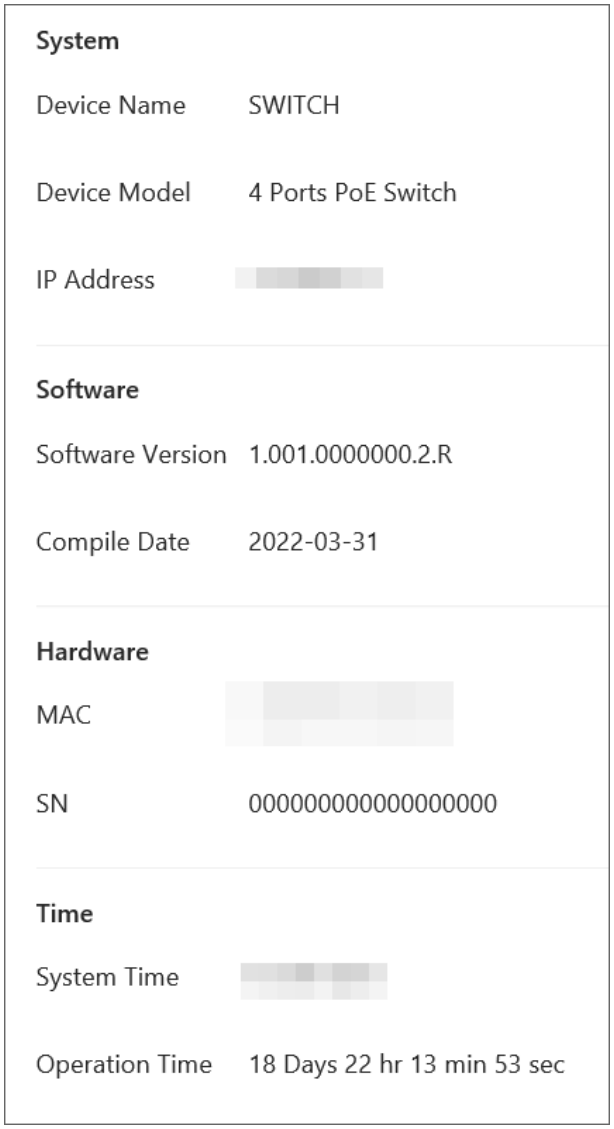
Seleccionar**Mantenimiento**>**Gestión de archivos**>**Restaurar configuración**, haga clic**Navegar**para seleccionar el archivo y luego haga clic en**Importar archivos de configuración**para importar el archivo.

La configuración importada sobrescribirá la configuración anterior.

3.6 Ver información del dispositivo

Seleccionar**Mantenimiento**>**Información del dispositivo**, puedes ver la información en**Sistema**,**Software**, **Hardware**y**Tiempo**.

Figura 3-4 Información del dispositivo



3.7 Ver información de registro

Puede ver la información de registro sobre las operaciones de cambio.

Información de contexto

Recomendamos habilitar la función de registro para garantizar que los registros de claves se puedan sincronizar con el servidor para referencia futura.

Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Registro**.

Paso 2 Configurar**Tiempo**y**Tipo**y luego haga clic en**Buscar**.

Paso 3 Puede ver la información del registro.

El tipo de registro incluye**Error**,**Advertencia**y**Mensaje**.

Figura 3-5 Información de registro

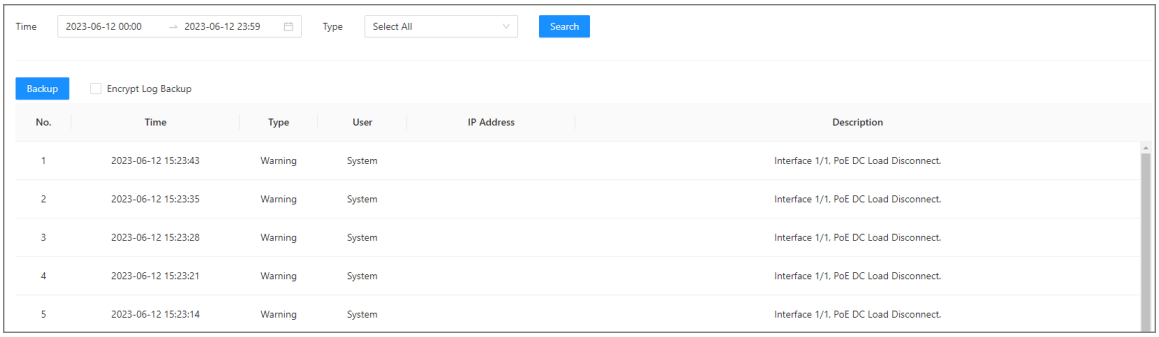


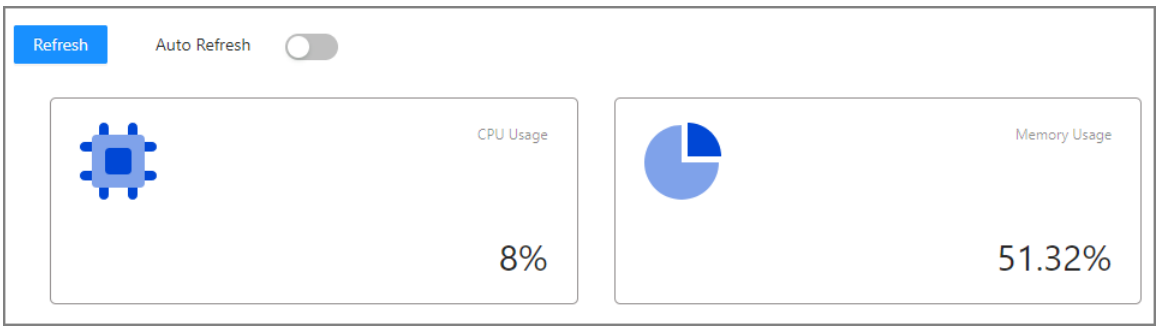
Tabla 3-1 Descripción del parámetro

Parámetro	Descripción
Respaldo	Toque para hacer una copia de seguridad de los registros buscados.
Cifrar copia de seguridad de registros	Haga clic en la casilla de verificación para cifrar los registros de respaldo.

3.8 Monitoreo de estado

Seleccionar**Mantenimiento**>**Monitoreo de estado**y luego podrá ver el uso de la CPU y el uso de la memoria.

Figura 3-6 Monitoreo de estado



3.9 Visualización del diagnóstico

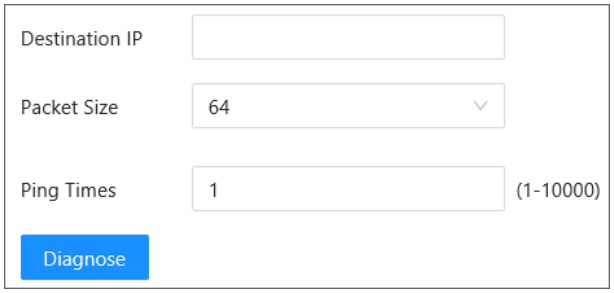
Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Diagnóstico**.

Paso 2 Introducir el**IP de destino**,y luego seleccione**Tamaño del paquete**y**Tiempos de ping**. Hacer

Paso 3 clic**Diagnosticar**.

Figura 3-7 Diagnóstico



3.10 Configurar la duplicación

Información de contexto

La duplicación copia el tráfico recibido o enviado, o ambos, en un origen específico a un puerto de destino para su análisis. La fuente especificada se denomina fuente reflejada, el puerto de destino se denomina puerto de observación y el tráfico copiado se denomina tráfico reflejado. La duplicación envía una copia del tráfico a través de un puerto de observación en el conmutador a un dispositivo de monitoreo para el análisis del servicio.

Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Espejo**. Hacer

Paso 2 clic**Agregar**.

Paso 3 En**Agregar grupo de duplicación**página, seleccione**Grupo de duplicación No.**,**Puerto de destino de duplicación**y luego seleccione entre**Sólo TX**,**Sólo recepción**, y**Ambos**según la situación real.

Etapa 4 Hacer clic**DE ACUERDO**.

Figura 3-8 Agregar grupo de duplicación

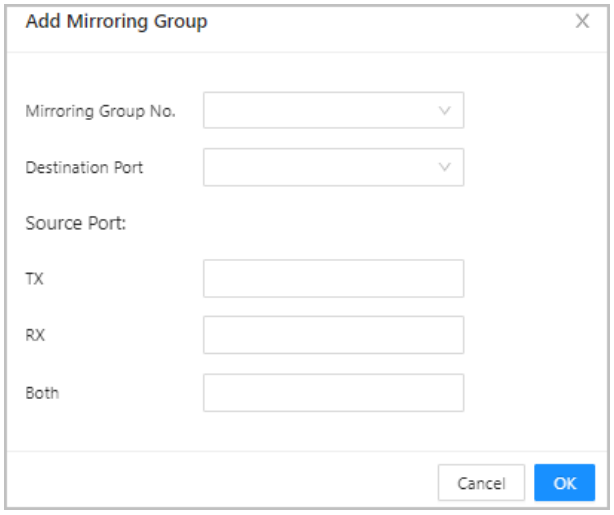


Tabla 3-2 Descripción del puerto de origen

Nombre	Descripción
Sólo TX	Solo admite el envío de tráfico.
Sólo recepción	Solo admite recibir tráfico.
Ambos	Admite tanto envío como recepción.

Operaciones relacionadas

- Hacer clic  para editar la información del grupo de duplicación.
- Hacer clic  o**Borrar**para eliminar el grupo de duplicación.

4 configuraciones de red

4.1 configurar puertos

Información de contexto

Puede configurar los parámetros del puerto, incluida la velocidad/dúplex, el control de flujo y otros parámetros. Los parámetros del puerto afectarán directamente el modo de funcionamiento del puerto. Realizar configuraciones según los requisitos prácticos.

La página web puede diferir según los diferentes dispositivos. Consulte las páginas reales.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Puerto**.

Paso 2 Puede ver y configurar los parámetros.

Figura 4-1 Configuración del puerto

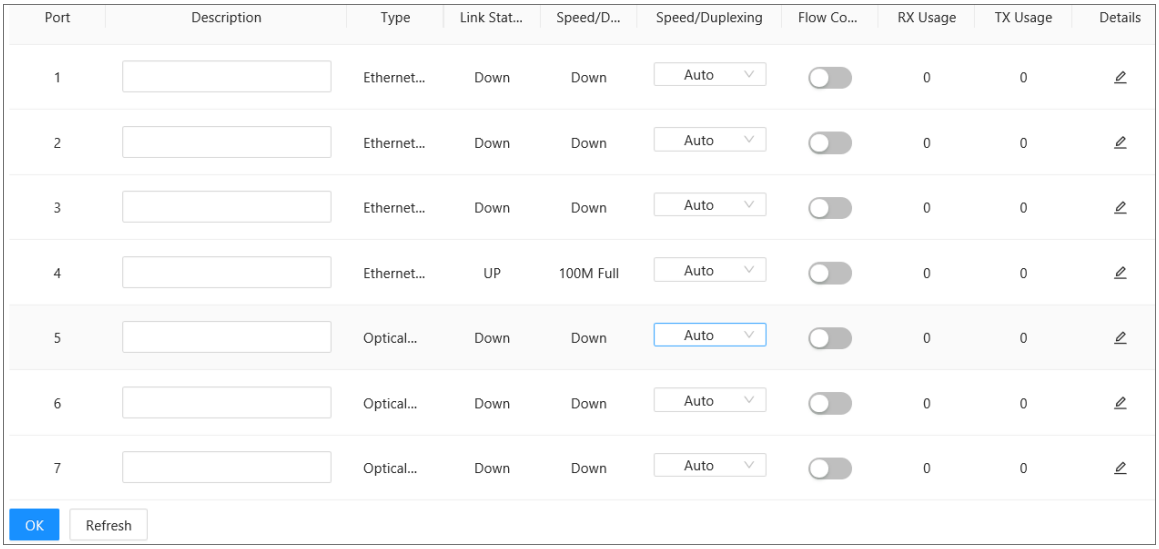


Tabla 4-1 Descripción de los parámetros del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Descripción	Introduzca la descripción del puerto. La descripción no puede exceder los 16 caracteres. Sólo se permiten números, letras y los siguientes caracteres especiales: . _-. El primer carácter debe ser una letra y el último carácter no debe ser un carácter especial.
Tipo de medio	Muestra dos tipos de medios, incluye dos tipos:**Cobre** y **Fibra**. ● Cobre: Puerto Ethernet. ● Fibra: Puerto óptico.

Parámetro	Descripción
Estado del enlace	Incluye dos estilos:**Arriba**y**Abajo**. ● Arriba: El puerto está conectado. ● Abajo: El puerto no está conectado o la conexión falla.
Estado de velocidad/dúplex	● En línea: muestra la velocidad del puerto y el modo dúplex. ● Sin conexión: pantallas**Abajo**.
Velocidad/Dúplex	Configure la velocidad y el modo dúplex desde**Abajo**,**Auto**,**10M la mitad**, **10M completo**,**100M la mitad**,**100M completos**, y**1000M lleno**.  La velocidad/dúplex se establece como**Auto**para puerto combinado.
Control de flujo	Hacer clic  para habilitar o deshabilitar la función.
Uso de RX	Muestra el uso de recepción.
uso de transmisión	Muestra el uso de envío.
Detalles	● Vea el RX total y el TX total de cada puerto. Puede actualizar o borrar la información detallada de cada puerto. ● Ver el número de bytes de error.

Paso 3 Hacer clic**DE ACUERDO**.

4.2 Configuración de EEE

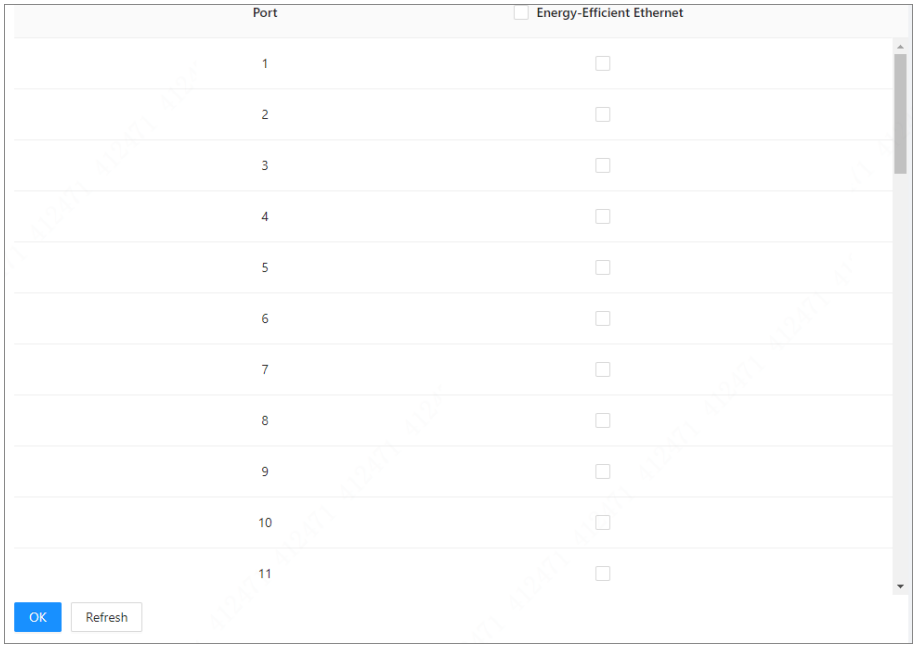
Habilite la función EEE (Ethernet de eficiencia energética).

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**EEE**.

Paso 2 Seleccione la casilla de verificación del puerto para habilitar el**Ethernet energéticamente eficiente**función y luego haga clic en**DE ACUERDO**para guardar la configuración.

Figura 4-2 Función EEE



4.3 Configuración de VLAN

4.3.1 Definición de VLAN

Lógicamente, una LAN (red de área local) se puede dividir en muchos subconjuntos. Cada subconjunto tiene su propia área de transmisión: LAN virtual (VLAN). Una VLAN se divide de una LAN de forma lógica en lugar de física, para lograr el área de transmisión aislada en la VLAN.

4.3.2 Función VLAN

- Mejorar el rendimiento de la red. Los paquetes de transmisión están en la VLAN, lo que puede controlar eficazmente la tormenta de transmisión de la red, reducir el ancho de banda de la red y mejorar la capacidad de procesamiento de la red.
- Mejorar la seguridad de la red. Los conmutadores en diferentes VLAN no pueden acceder entre sí y los hosts en diferentes VLAN no pueden comunicarse entre sí. Necesitan un enrutador o un conmutador de tres capas para reenviar el mensaje.
- Simplifique la gestión de la red. El anfitrión de un mismo grupo de trabajo virtual no está limitado a un área física, lo que puede simplificar la gestión de la red y facilitar el establecimiento de grupos de trabajo para usuarios en diferentes áreas.

4.3.3 VLAN basada en puerto

Los tipos de puerto incluyen**Acceso**,**Trompa**y**Híbrido**.

- Acceso: el puerto pertenece a una VLAN y se utiliza para conectarse al puerto de la computadora.
- Trunk: El puerto permite el paso de múltiples VLAN, recibir y enviar mensajes de múltiples VLAN, y se utiliza para conectarse entre los conmutadores.
- Híbrido: El puerto permite el paso de múltiples VLAN, recibir y enviar mensajes de múltiples VLAN, y se utiliza para conectarse entre los conmutadores y conectar la computadora.

4.3.4 Agregar VLAN

Información de contexto

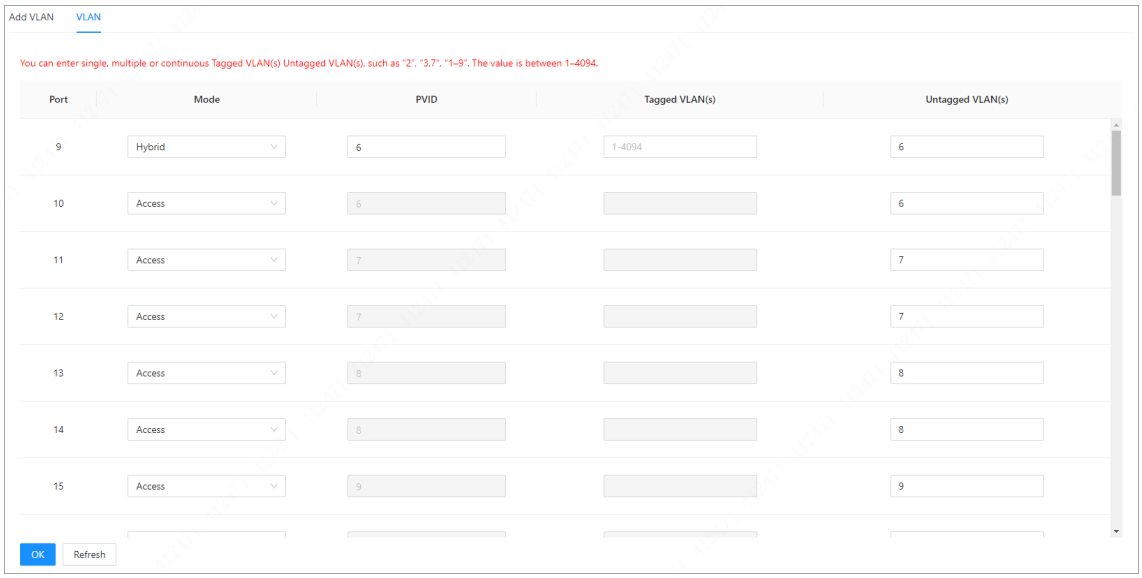
Puede agregar el puerto a la VLAN. La VLAN es VLAN1 de forma predeterminada.

El aislamiento de puertos y la VLAN no se pueden habilitar al mismo tiempo. Si uno de ellos está habilitado, el otro se desactivará automáticamente. Por favor tenga en cuenta.

Procedimiento

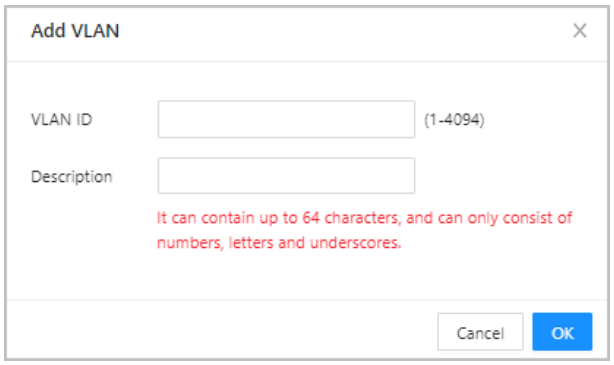
Paso 1 Seleccionar**Configuración de la red**>**VLAN**.

Figura 4-3 Configuración de VLAN



Paso 2 Sobre el**Agregar VLAN**página, haga clic**Agregar**, introducir el**ID de VLAN**y**Descripción**.

Figura 4-4 Agregar VLAN



Paso 3 Hacer clic**DE ACUERDO**.

La VLAN1 no se puede eliminar.

Operaciones relacionadas

- Hacer clic para editar VLAN.
- Hacer clic para eliminar VLAN.

4.3.5 Configuración del puerto VLAN

Puede configurar los parámetros de VLAN del puerto.

Figura 4-5 Configurar VLAN

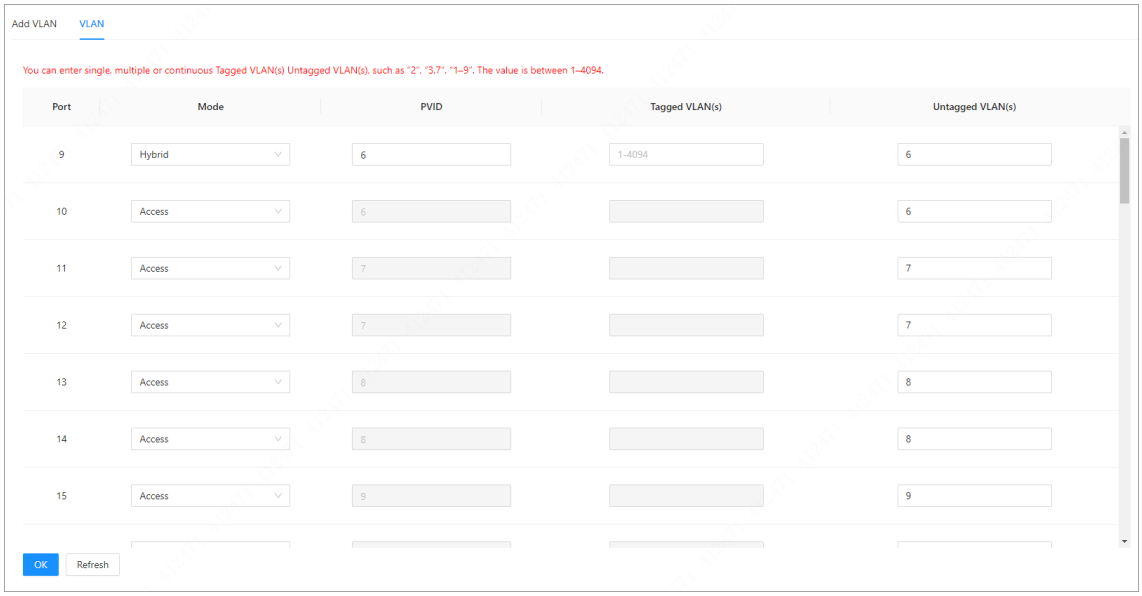


Tabla 4-2 Parámetro de configuración de VLAN del puerto

Parámetro	Descripción
Puerto	Muestra todos los puertos del conmutador.
Modo	Incluye tres modos:**Acceso**,**Híbrido**, y**Trompa**. ● Acceso: Pertenece a una VLAN. Comúnmente utilizado para conectar puertos de computadora. ● Trunk: permite el paso de múltiples VLAN. Recibe y envía múltiples paquetes VLAN. Normalmente se utiliza para la conexión entre interruptores. ● Híbrido: permite el paso de varias VLAN. Recibe y envía múltiples paquetes VLAN. Se utiliza para la conexión entre conmutadores o conmutador y computadora.
VLAN etiquetadas	Configure el ID de VLAN para el puerto que se puede etiquetar al enviar paquetes.
VLAN sin etiquetar	Configure el ID de VLAN para el puerto que puede desetiquetarse al enviar paquetes.

Tabla 4-3 Comparación del procesamiento de cuadros

Tipo de puerto	Marco sin etiquetar Procesando	Procesamiento de cuadros etiquetados	Transmisión de cuadros
Acceso	Recibe un sin etiquetar marco y agrega una etiqueta con el ID de VLAN predeterminado al marco.	• Acepta la trama etiquetada si la ID de VLAN de la trama coincide con la ID de VLAN predeterminada. • Descarta la trama etiquetada si el ID de VLAN de la trama difiere del ID de VLAN predeterminada.	Una vez eliminada la etiqueta PVID, se transmite la trama.
Trompa	• Agrega una etiqueta con el ID de VLAN predeterminado a una trama sin etiquetar y Acepta el marco si la interfaz lo permite. el ID de VLAN predeterminado. • Agrega una etiqueta con el ID de VLAN predeterminado a una trama sin etiquetar y descarta el marco si la interfaz lo niega el ID de VLAN predeterminado.	• Acepta una trama etiquetada si la interfaz permite el ID de VLAN contenido en la trama. • Descarta una trama etiquetada si la interfaz niega el ID de VLAN contenido en la trama.	• Si el ID de VLAN de la trama coincide con el predeterminado ID de VLAN y el ID de VLAN está permitido por la interfaz, el dispositivo elimina la etiqueta y transmite la trama. • Si la ID de VLAN de la trama difiere de la ID de VLAN predeterminada, pero la interfaz aún permite la ID de VLAN, el dispositivo transmitirá directamente la trama.
Híbrido			Si la interfaz permite el ID de VLAN de la trama, la trama se transmite. La interfaz puede ser configurado si transmitir fotogramas con etiquetas.

4.4 Configuración de VLANIF

Información de contexto

Una interfaz VLANIF es una interfaz lógica de Capa 3 que se usa más comúnmente para implementar la comunicación de Capa 3 entre hosts en diferentes VLAN en diferentes segmentos de red.

Cada interfaz VLANIF corresponde a una VLAN. Después de configurar una dirección IP para una interfaz VLANIF, la interfaz VLANIF se convierte en la puerta de enlace de los hosts de usuario dentro de esa VLAN y reenvía paquetes a través de segmentos de red en la Capa 3.

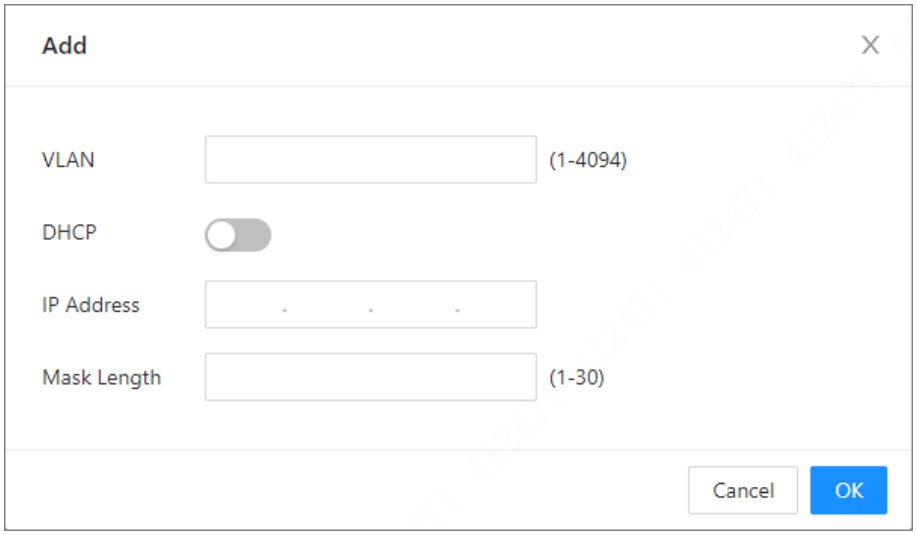
Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**VLANIF**.

Paso 2 Hacer clic**Agregar**,aporte**VLAN**número y luego habilite**DHCP**para el puerto con**Modo**como **Dinámica**.

Cuando**DHCP**deshabilitado, debes ingresar**Dirección IP**y**Longitud de la máscara**.

Figura 4-6 Agregar VLANIF



Operaciones relacionadas

- Eliminar la VLANIF: seleccione la VLAN y luego haga clic en**Borrar**o .
- Actualizar el parámetro: haga clic en**Actualizar**para actualizar los parámetros de VLAN.

4.5 Configuración de IP y enrutamiento

Presenta la configuración de IP y la configuración de enrutamiento del conmutador.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**IP y enrutamiento**.

Paso 2 Sobre el**Configuración de enrutamiento**pestaña, haga clic**Agregar**y luego configure los parámetros.

Algunos modelos solo admiten enrutamiento predeterminado. Consulte el producto real.

Figura 4-7 Configuración de enrutamiento



Tabla 4-4 Descripción de los parámetros de enrutamiento

Parámetro	Descripción
Red	Ingrese la dirección de destino o la red de destino para identificar el paquete IP.
Longitud de la máscara	Configure el segmento para identificar el conmutador o enrutador de destino con la dirección de destino.
Siguiente salto	Establezca la dirección del siguiente salto del enrutador.

Operaciones relacionadas

- Eliminar el enrutamiento: seleccione la VLAN y el enrutamiento y luego haga clic en**Borrar**o .
- Actualizar el parámetro: haga clic en**Actualizar**para actualizar los parámetros de la ruta.

4.6 Configuración de ERPS

ERPS es un protocolo definido por la Unión Internacional de Telecomunicaciones - Sector de Normalización de las Telecomunicaciones (UIT-T) para eliminar bucles en la Capa 2. Generalmente, los enlaces redundantes se utilizan en una red de conmutación Ethernet, como una red en anillo, para proporcionar respaldo de enlace y mejorar la confiabilidad de la red. . Sin embargo, el uso de enlaces redundantes puede producir bucles, lo que provoca tormentas de transmisión y hace que la tabla de direcciones MAC sea inestable. Como resultado, la calidad de la comunicación se deteriora e incluso los servicios de comunicación pueden verse interrumpidos. ERPS previene tormentas de transmisión e implementa una conmutación rápida de tráfico en una red donde hay bucles, proporciona una convergencia rápida y confiabilidad de clase operadora y permite que todos los dispositivos compatibles con ERPS en una red en anillo se comuniquen.

Es posible que algunos modelos no admitan la función ERPS. Consulte los productos reales.

4.6.1 Configuración de ERPS

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**ERPS**. Sobre el**ERPS**

Paso 2 pestaña, haga clic**Agregar**para agregar ERPS. Configure los

Paso 3 parámetros y luego haga clic en**DE ACUERDO**.

Figura 4-8 Agregar ERPS

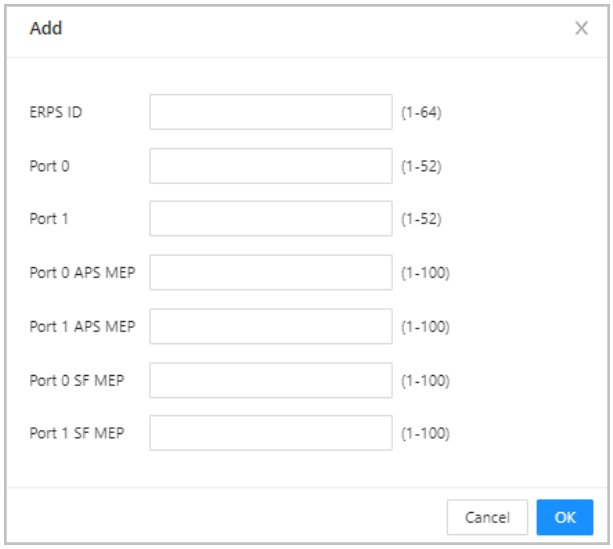


Tabla 4-5 Descripción de parámetros

Parámetro	Descripción
ID de ERPS	El número de identificación del ERPS.
Puerto 0	Dos puertos del switch para agregar al ERPS.
Puerto 1	
Puerto 0 APS eurodiputado	• BPDU MEP del puerto ERPS. • Monitoreo de enlace MEP del puerto ERPS. El puerto 0 APS MEP se mantiene igual que el puerto 0 SF MEP. El puerto 1 APS MEP se mantiene igual que el puerto 1 SF MEP.
Puerto 1 APS eurodiputado	
Puerto 0 SF MEP	
Puerto 1 SF eurodiputado	

4.6.2 Configuración del Parlamento Europeo

Información de contexto

MEP (punto final del grupo de entidades de mantenimiento) es parte del anillo ERPS. Un nodo se refiere a un dispositivo de conmutación de Capa 2 agregado a un anillo ERPS. Se puede agregar un máximo de dos puertos en cada nodo al mismo anillo ERPS.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**ERPS**. Sobre el**eurodiputado**

Paso 2 pestaña, haga clic**Agregar**para añadir eurodiputado. Configure

Paso 3 los parámetros del MEP.

Etapa 4 Hacer clic**OK**.

Figura 4-9 Agregar MEP

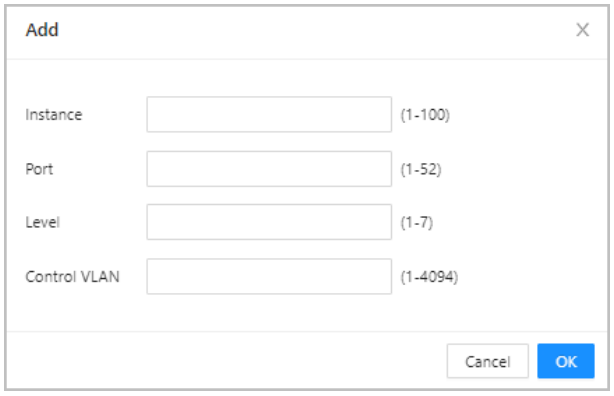


Tabla 4-6 Descripción del parámetro MEP

Parámetro	Descripción
Instancia	El número de la instancia del MEP.
Puerto	El número de puerto de MEP.
Nivel	Nivel de mantenimiento. Recomendamos establecerlo en 0.
Controlar VLAN	El ID de la VLAN de control en un segmento SEP.

4.7 Configurar la vigilancia IGMP

Información de contexto

IGMP Snooping (Internet Group Management Protocol Snooping) es el mecanismo de restricción de multidifusión que se ejecuta en el dispositivo de capa 2, para gestionar y controlar la multidifusión. Al analizar el paquete IGMP recibido, el dispositivo de capa 2, que ejecuta IGMP Snooping, crea el mapeo entre el puerto y la dirección de multidifusión MAC y reenvía los datos de multidifusión de acuerdo con el mapeo.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Espionaje IGMP**.

Paso 2 Hacer clic junto a**Espionaje IGMP**para habilitar la función.

Paso 3 Hacer clic junto a**IGMP Dejar mensajes grupales**para habilitar la función.

- Habilitar la función: Una vez habilitada la función, si el switch recibe mensajes grupales que no están registrados, abandona los mensajes. Se guardará el ancho de banda y luego se aumentará la velocidad de reenvío.
- Desactivar la función: Si los mensajes del grupo no están registrados, los mensajes se transmitirán en la VLAN. Se ocupará el ancho de banda y luego se reducirá la velocidad de reenvío.

Tenga en cuenta al habilitar**IGMP Dejar mensajes grupales**; de lo contrario, la multidifusión podría fallar.

Etapa 4 Hacer clic**DE ACUERDO**.

4.8 Configuración de STP

El Spanning Tree Protocol (STP) crea una topología lógica sin bucles para las LAN. Bloquea enlaces redundantes entre dos dispositivos de red y deja un único enlace activo entre ellos para eliminar bucles.

STP, RSTP y MSTP proporcionan las siguientes capacidades:

- STP: un protocolo de gestión en la capa de enlace de datos se utiliza para detectar y evitar bucles en una red de Capa 2. Sin embargo, la topología de la red converge lentamente.
- RSTP: una mejora de STP que permite una rápida convergencia de la topología de la red. Sin embargo, tanto RSTP como STP tienen el defecto de que todas las VLAN en la misma LAN comparten el mismo árbol de expansión.
- MSTP: una tabla de mapeo de VLAN virtual en la que los ID de VLAN están asociados con instancias de árbol de expansión. No solo esto, MSTP divide una red de conmutación en múltiples regiones, cada una de las cuales tiene múltiples instancias de árbol de expansión que son mutuamente independientes. A diferencia de STP y RSTP, MSTP proporciona múltiples rutas redundantes para el reenvío de datos. Además, implementa equilibrio de carga entre VLAN.

4.8.1 PTS

Información de contexto

Cuando el árbol de expansión está habilitado, no se puede utilizar iLinkView.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**STP**.

Paso 2 Haga clic al lado de**STP**para habilitar la función STP.

Paso 3 Seleccione Modo de trabajo.

Etapa 4 Hacer clic**Avanzado**y luego configure los parámetros avanzados.

Figura 4-10 Configurar STP

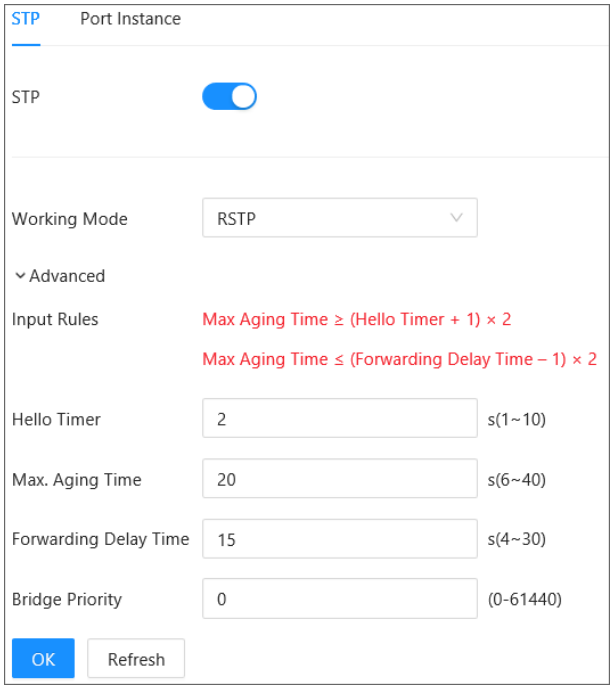


Tabla 4-7 Descripción de los parámetros avanzados

Parámetro	Descripción
STP	El protocolo básico del árbol de expansión.
RSTP	Una mejora de STP permite una rápida convergencia de la topología de la red.
Hola temporizador	El período del puente raíz que envía BPDU. El tiempo oscila entre 1 segundo y 10 segundos.
Máx. tiempo de envejecimiento	El tiempo de envejecimiento de la BPDU actual. El tiempo oscila entre 6 segundos y 40 segundos.
Retraso de reenvío tiempo	Después de establecer el cambio topológico, el puente mantiene el tiempo de espionaje y estado de estudio. El tiempo oscila entre 4 segundos y 30 segundos.
Prioridad del puente	El valor oscila entre 0 y 61440.

4.8.2 Instancia de puerto

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**STP**>**Instancia de puerto**.

Paso 2 Ingresar**Prioridad**y**Costo de la ruta raíz**de cada puerto.

- El valor de**Prioridad**varía de 0 a 240 y debe ser un múltiplo entero de 16.
- El valor de**Prioridad**es 128 por defecto.

Figura 4-11 Instancia de puerto

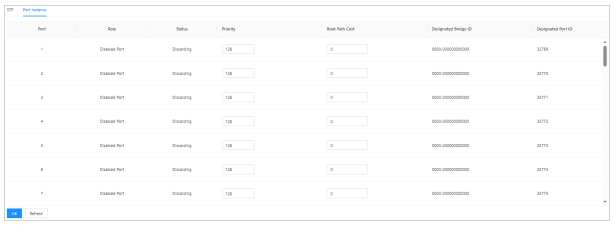


Tabla 4-8 Descripción de parámetros de la instancia del puerto

Parámetro	Descripción
Role	El STP básico.
Estado	Una mejora de STP permite una rápida convergencia de la topología de la red.
Prioridad	La prioridad del puerto.
Costo de la ruta raíz	El costo de la ruta raíz del puerto.
ID de puente designado	El ID de puente designado del puerto.
ID de puerto designado	El ID del puerto designado del puerto.

4.9 Configurar la agregación de enlaces

Información de contexto

La agregación de enlaces consiste en formar varios puertos físicos del conmutador en un puerto lógico. Los múltiples enlaces en el mismo grupo pueden considerarse como un enlace lógico con un ancho de banda mayor.

Mediante la agregación, los puertos del mismo grupo pueden compartir el flujo de comunicación para generar un mayor ancho de banda. Además, los puertos del mismo grupo pueden realizar copias de seguridad recíprocas y dinámicas para mejorar la confiabilidad del enlace.

- La agregación de enlaces es mutuamente excluyente con el modo STP, IGMP Snooping y el modo 802.1x. Cuando el modo STP está habilitado, no se puede configurar la agregación de enlaces. Debe desactivar el modo STP antes de configurar la agregación de enlaces.
- No recomendamos implementar configuración y funciones avanzadas para los puertos que se utilizan para la agregación de enlaces.
- La agregación de enlaces se puede dividir en agregación estática y LACP. Generalmente, los dispositivos pares con agregación de enlaces de conmutador son el conmutador y el adaptador de red.
- Solo los puertos con la misma velocidad, dúplex, larga distancia y configuración de VLAN pueden estar en un grupo de agregación.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Agregar un link**. Hacer

Paso 2 clic**Agregar**.

Paso 3 Selecciona el**Grupo de agregación No.**.

Etapa 4 Selecciona el**Modo de grupo de agregación**,y luego haga clic**DE ACUERDO**. El modo de grupo de agregación incluye estático, LACP activo y LACP pasivo.

- Estático: El modo estático también se conoce como modo manual. La interfaz Eth-Trunk debe crearse manualmente y las interfaces de los miembros deben agregarse manualmente. El protocolo LACP está deshabilitado.
- LACP activo: la interfaz Eth-Trunk debe crearse manualmente y las interfaces de los miembros deben agregarse manualmente. En comparación con la estática, la selección de la interfaz se configura mediante el protocolo LACP. Este modo coloca una interfaz en un estado de negociación activa. En este modo, la interfaz inicia negociaciones con otras interfaces enviando LACPDU.
- LACP pasivo: las interfaces Eth-Trunk se crean y las interfaces de miembros se agregan mediante el protocolo LACP. Este modo coloca una interfaz en un estado de negociación pasiva. En este modo, la interfaz responde a las LACPDU que recibe pero no inicia la negociación de LACPDU.

Paso 5 Seleccione los puertos que desea agregar y luego haga clic en**DE**

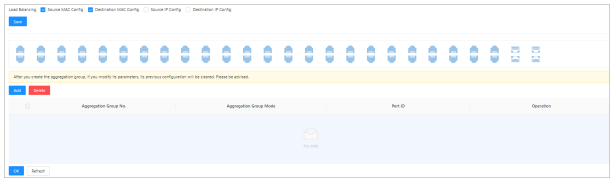
Paso 6 **ACUERDO**. Selecciona el**Clave operativa**.

- Sólo puede configurar la agregación de enlaces cuando el**Modo de grupo de agregación**está configurado como LACP.
- El valor oscila entre 1 y 65535.

Paso 7 Selecciona el**Se acabó el tiempo**de**Tiempo de espera prolongado**o**Tiempo de espera corto**. Hacer clic**DE**

Paso 8 **ACUERDO**.

Figura 4-12 Agregación de enlaces



4.10 Configuración del protocolo SNMP

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

- Admite la gestión inteligente de dispositivos de red. Al utilizar la plataforma de administración de red basada en SNMP, el administrador de la red puede consultar el estado de ejecución y los parámetros del dispositivo de red, y puede configurar el parámetro, encontrar el error, realizar un diagnóstico de fallas y luego planificar la capacidad y crear el informe.
- SNMP admite la gestión de dispositivos de diferentes características físicas. SNMP proporciona sólo la biblioteca de funciones más básica. Independiente la tarea de gestión y la característica física y la tecnología de red del dispositivo gestionado, para gestionar los dispositivos de diferentes fabricantes.

La red SNMP proporciona 2 elementos, NMS y Agente.

- NMS (Sistema de gestión de red) es el administrador de la red SNMP y proporciona una interfaz amigable hombre-máquina para ayudar al administrador de la red a finalizar la mayor parte del trabajo de administración de la red.
- El agente es la función administrada en la red SNMP y recibe y maneja el paquete de solicitud del NMS. En algunas circunstancias de emergencia, por ejemplo, si el estado del puerto cambia, el Agente puede enviar un paquete de alarma al NMS de forma proactiva.

4.10.1 Configuración de SNMP V1 y V2

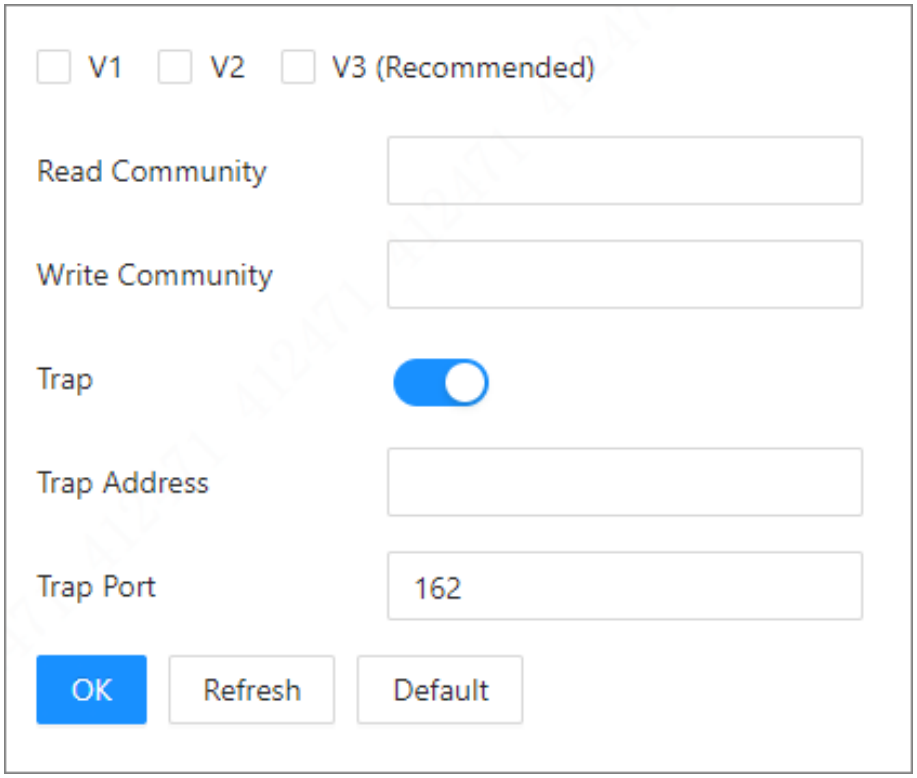
Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**SNMP**

Paso 2 . Seleccionar**V1**o**V2**versión.

Paso 3 Configurar parámetros, incluyendo**Leer comunidad**,**Escribir comunidad**,**Dirección trampa**, y**Puerto trampa**.

Figura 4-13 SNMP



Etapa 4 Hacer clic**DE ACUERDO**.

4.10.2 Configuración de SNMP V3

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**SNMP**.

Paso 2 Seleccionar**V3**.

Paso 3 Configurar parámetros.

Figura 4-14 SNMP V3

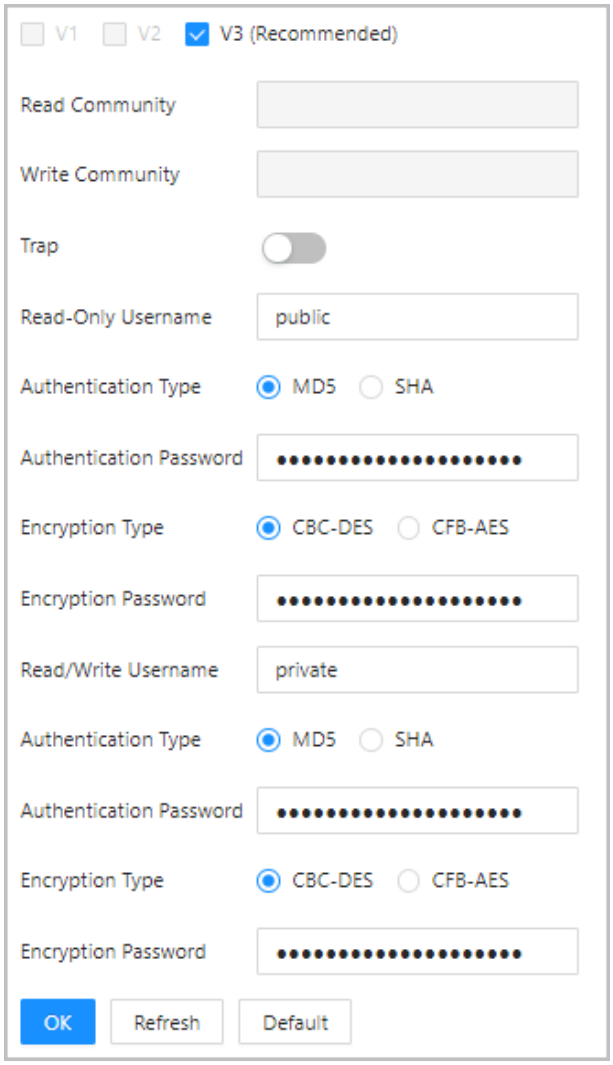


Tabla 4-9 Descripción de los parámetros SNMP

Parámetro	Descripción
Leer comunidad	Comunidad de lectura respaldada por los programas de agentes.
escribir comunidad	Comunidad de escritura respaldada por los programas de agentes.
dirección trampa	La dirección de destino de la información de captura enviada por el programa agente.
Puerto trampa	El puerto de destino de la información de captura enviada por el programa agente.
Nombre de usuario de solo lectura	Establezca el nombre de usuario de solo lectura. Es sólo para V3.
Tipo de autenticación	Configure el modo de autenticación cuando el nivel de seguridad sea**Autenticación sin cifrado**o **Autenticación y cifrado**. El modo de autenticación incluye**MD5**y**sha**.
Contraseña de autenticación	Establecer contraseña de autenticación.

Parámetro	Descripción
Tipo de cifrado	Configure el modo de cifrado cuando el modo de autenticación esté**Autenticación y cifrado**.
Contraseña de cifrado	Establezca la contraseña de cifrado cuando el modo de autenticación esté activado.**Autenticación y cifrado**.
Leer/escribir nombre de usuario	Establecer usuario de lectura y escritura.

Etapa 4 Hacer clic**DE ACUERDO**.

4.11 Configuración de la tabla MAC

La tabla MAC (Control de acceso a medios) registra la relación entre la dirección MAC y el puerto, y la información, incluida la VLAN a la que pertenece el puerto. Cuando el dispositivo reenvía el paquete, consulta en la tabla de direcciones MAC la dirección MAC de destino del paquete. Si la dirección MAC de destino del paquete está contenida en la tabla de direcciones MAC, el paquete se reenvía directamente a través del puerto de la tabla. Y si la dirección MAC de destino del paquete no está contenida en la tabla de direcciones MAC, el dispositivo adopta la transmisión para reenviar el paquete a todos los puertos excepto al puerto de recepción en la VLAN.

4.11.1 Agregar tabla MAC

Puede vincular la dirección MAC al puerto en cierta VLAN.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Tabla MAC**.

Paso 2 Sobre el**Tabla MAC**pestaña, haga clic**Agregar**.

Paso 3 Configure la dirección MAC, VLAN y puerto.

Por ejemplo, vincule la dirección MAC 00:00:00:00:00:01 al puerto 3 en VLAN 2. Haga clic en**DE**

Etapa 4 **ACUERDO**.

Figura 4-15 Agregar tabla MAC



Operaciones relacionadas

Figura 4-16 operaciones relacionadas



- Eliminar dirección MAC estática: seleccione una MAC y luego haga clic en**Borrar**.
- Actualizar la lista de direcciones MAC: haga clic en**Actualizar**o habilitar**Autorefrescar**.
- Borrar dirección MAC dinámica: haga clic en**Borrar MAC dinámica**.

- Busque la dirección MAC y el puerto: ingrese la dirección MAC o el número de puerto en la esquina superior derecha y luego haga clic en**Buscar**.

4.11.2 Puerto de filtrado MAC

Información de contexto

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

- Dispositivos en la lista de permitidos MAC.
- Los dispositivos MAC estáticos cambian de los dispositivos MAC dinámicos.

Después de habilitar el filtrado MAC del puerto, el puerto no puede acceder a la dirección de administración ni iniciar sesión.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Tabla MAC**.

Paso 2 Sobre el**filtrado MAC**, seleccione el puerto y luego haga clic en para habilitar el filtrado función.

Paso 3 Configure el filtrado MAC del puerto.

- Cambio de dinámico a estático.

  1. Seleccione un registro y luego seleccione junto a**Reservado**.
  2. Haga clic**DE ACUERDO**.

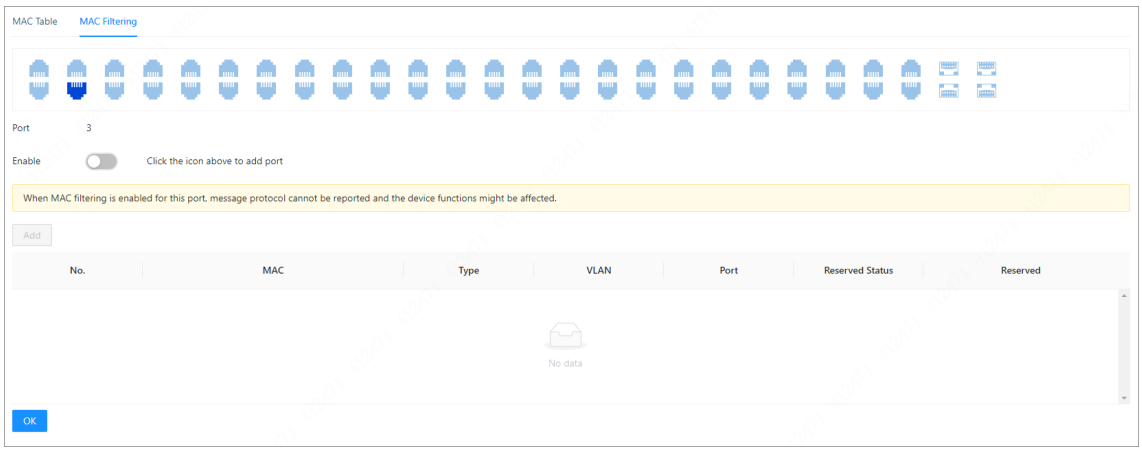
  El tipo cambia de**Dinámica**a**Estático**.

  Los dispositivos MAC estáticos pueden comunicarse con el puerto normalmente.

- Cree una lista de MAC permitidos.

  1. Haga clic**Agregar**.
  2. Configure la dirección MAC y VLAN.
  3. Haga clic**DE ACUERDO**.

Figura 4-17 Filtrado MAC



4.12 Configuración de LLDP

Información de contexto

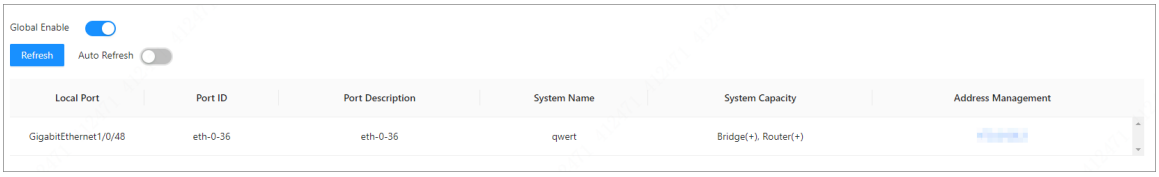
LLDP (Protocolo de descubrimiento de capa de enlace) es una forma estándar de descubrimiento de capa de enlace. Puede formar sus capacidades principales, dirección de administración, número de dispositivo y número de puerto como TLV (valor de longitud de tipo), encapsularlo en LLDPDU (Unidad de datos del protocolo de descubrimiento de capa de enlace) y liberarlo a su vecino. El vecino mantendrá la información recibida en forma de MIB (Base de información de gestión) estándar, para que la gestión de la red pueda consultar y juzgar el estado de comunicación del enlace.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**LLDP**.

Paso 2 Sobre el**Dispositivo remoto LLDP**pestaña, vea la información del dispositivo remoto LLDP.

Figura 4-18 Dispositivo remoto LLDP



5 Gestión de PoE

PoE se refiere a que el dispositivo utiliza cables de red para conectar externamente PD (Powered Device) para el suministro de energía remota a través de puertos eléctricos Ethernet. La función PoE permite un suministro de energía centralizado y una copia de seguridad conveniente. Los terminales de red no necesitan fuente de alimentación externa, solo un cable de red. Cumple con los estándares IEEE 802.3af, IEEE 802.3at e IEEE 802.3bt, el dispositivo utiliza un puerto de alimentación unificado globalmente. Se puede utilizar en teléfonos IP, AP (punto de acceso) inalámbrico, cargador de energía portátil, máquina de tarjetas de crédito, cámara de red y recopilación de datos.

- Los conmutadores que no son PoE no admiten esta función.
- Sólo algunos modelos de conmutadores PoE cumplen con el estándar IEEE 802.3at. El puerto BT único admite hasta 90 W. Consulte los productos reales.

5.1 Configuración de los ajustes de PoE

Seleccionar**Gestión de PoE**>**Configuración de PoE**. Puede configurar los ajustes de energía, el estado de energía, el estado del puerto y el control.

Procedimiento

Paso 1 En**Configuración de energía**, puede ver la potencia total de los 4 puertos y configurar la potencia reservada y la potencia de alerta.

Paso 2 En**Estado de energía**, puede ver la energía consumida, la energía restante y la energía reservada.

Paso 3 En**Estado y control del puerto**,seleccione de la lista debajo del**Gestión de PoE**para habilitar o deshabilitar PoE del puerto correspondiente.

Etapa 4 Hacer clic**DE ACUERDO**.

Figura 5-1 Configuración de PoE

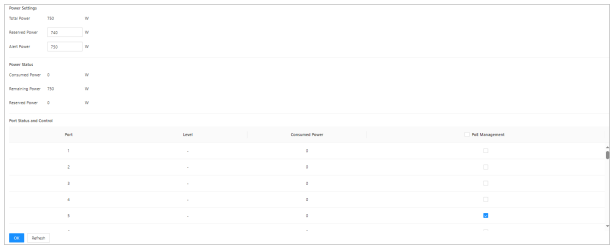


Tabla 5-1 Descripción de los parámetros PoE

Parámetro		**Descripción**
Configuración de energía	Poder total	Muestra la potencia PoE total.
	potencia reservada	Configure la alimentación PoE reservada.
	Poder de alerta	Configura la alimentación PoE de alerta.
Estado de energía	Energía consumida	Muestra la energía PoE actual consumida por todos los puertos.
	Poder restante	Muestra la potencia PoE restante actual.
	potencia reservada	Alimentación PoE inutilizable. Potencia reservada = potencia total – potencia de sobrecarga.
Estado del puerto y control	Nivel	Muestra el nivel de alimentación de los dispositivos terminales. El nivel de la fuente de alimentación varía de 0 a 8, y el nivel estándar de la fuente de alimentación Hi-PoE se muestra como 5+.

Parámetro		Descripción
	Energía consumida	Muestra la energía PoE actual consumida por el puerto único correspondiente.
	Gestión de PoE	Seleccionar de**Permitir**y**Desactivar**. ● Al seleccionar el**Desactivar**, el sistema no suministra energía al PD ni reserva energía para el PD. ● Al seleccionar el**Permitir**, el puerto PoE no provocará una sobrecarga de energía PoE. De lo contrario, no podrá habilitar PoE para el puerto PoE. ● De forma predeterminada, PoE está deshabilitado en un puerto PoE. ● Sobrecarga de energía del PSE: cuando la cantidad total del consumo de energía de todos los puertos excede la potencia máxima del PSE, el sistema considera que el PSE está sobrecargado.

5.2 Configuración de PoE perpetuo

Procedimiento

Paso 1 Seleccionar**Gestión de PoE**>**PoE perpetuo**. Haga clic para

Paso 2 habilitar**Habilitación global**. Hacer clic**DE ACUERDO**para

Paso 3 guardar la configuración.

5.3 Configuración de PoE de larga distancia

Información de contexto

Después de habilitar PoE de larga distancia, la distancia máxima de transmisión cambiará de 100 ma 250 m, y la velocidad de transmisión se reducirá de 100 Mbps a 10 Mbps.

En modo extendido, la distancia de transmisión del puerto PoE es de hasta 250 m pero la velocidad de transmisión cae a 10 Mbps. La distancia de transmisión real puede variar debido al consumo de energía de los dispositivos conectados o al tipo y estado del cable.

Procedimiento

Paso 1 Seleccionar**Gestión de PoE**>**PoE de larga distancia**.

Paso 2 Haga clic en el puerto correspondiente para habilitar PoE de larga distancia. Hacer clic**DE**

Paso 3 **ACUERDO**.

Figura 5-2 PoE de larga distancia



5.4 Ver estadísticas de eventos PoE

Seleccionar**Gestión de PoE**>**Estadísticas de eventos PoE**para ver las estadísticas de eventos PoE.

Tabla 5-2 Descripción de las estadísticas de eventos PoE

Parámetro	Descripción
Sobrecarga	El puerto único se inicia cuando la corriente de alimentación ha excedido el umbral actual.
Cortocircuitado	Cuando el chip de alimentación envía energía al puerto, se produce un cortocircuito.
Desconexión de CC	La alimentación de un solo puerto está apagada.
Cortocircuito durante puesta en marcha	La energía es un cortocircuito cuando el chip de alimentación envía energía.
Protección contra el sobrecalentamiento	Un solo puerto se inicia cuando la temperatura del chip de alimentación supera el umbral.

5.5 Configuración de PoE verde

Información de contexto

Green PoE puede reducir el consumo de energía manteniendo la total compatibilidad con los equipos existentes.

Procedimiento

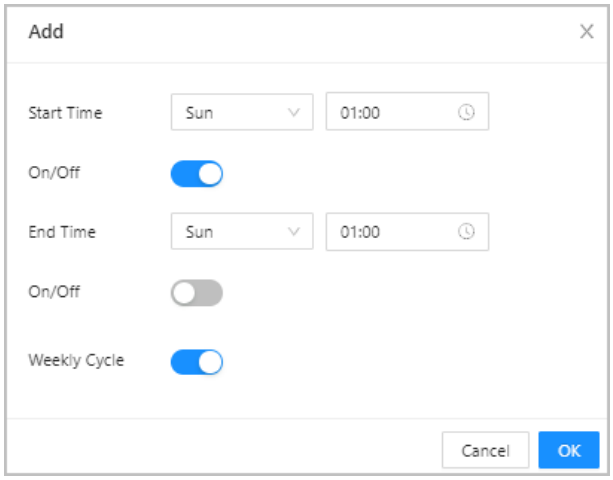
Paso 1 Seleccionar**Gestión de PoE**>**PoE verde**. Agregar

Paso 2 **Hora de inicio**y**Hora de finalización**.

Paso 3 Seleccione el puerto y luego haga clic en Hacer clic para habilitar el PoE verde.

Etapa 4 **DE ACUERDO**.

Figura 5-3 PoE verde



5.6 Configuración de Forzar PoE

Información de contexto

Después de habilitar Forzar PoE, el puerto forzará el suministro de energía al dispositivo alimentado, independientemente de que el dispositivo conectado al puerto cumpla o no con los requisitos. Por favor tenga en cuenta.

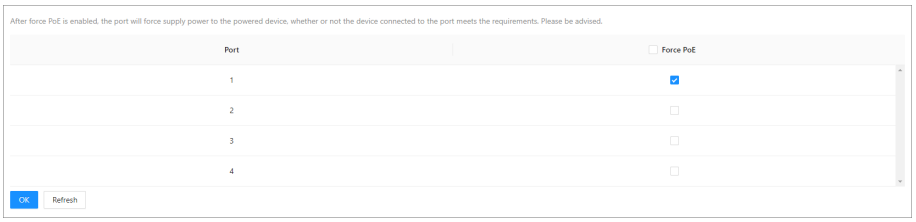
Procedimiento

Paso 1 Seleccionar**Gestión de PoE**>**Forzar PoE**.

Paso 2 Haga clic en el puerto correspondiente para habilitar forzar PoE. Hacer clic**DE**

Paso 3 **ACUERDO**.

Figura 5-4 Forzar PoE



5.7 Configuración del perro guardián PoE

Información de contexto

Con el perro guardián PoE habilitado, puede monitorear PD y mantenerlo en línea, y verificar el estado de los dispositivos PD cada 60 s. Si no hay transmisión de datos, el puerto PoE se apagará y reiniciará automáticamente.

Forzar PoEy**perro guardián de PoE**no se pueden habilitar al mismo tiempo.

Procedimiento

Paso 1 Seleccionar**Gestión de PoE**>**perro guardián de PoE**. Haga clic en el puerto

Paso 2 correspondiente para habilitar el mecanismo de vigilancia PoE.

Paso 3 Hacer clic**DE ACUERDO**.

Figura 5-5 Vigilancia PoE



6 seguridad

6.1 Servicios Básicos

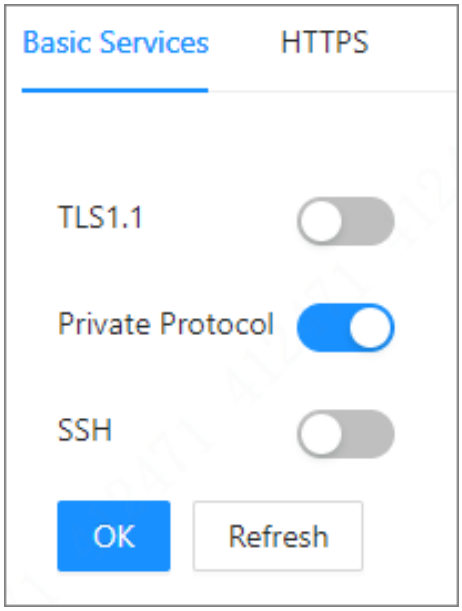
6.1.1 Configuración de servicios básicos

El protocolo de capa de transporte seguro (TLS) se utiliza para garantizar la confidencialidad y la integridad de los datos entre dos aplicaciones de comunicación. Este protocolo consta de dos capas: TLS Record y TLS Handshake. TLS1.1 utiliza un algoritmo de cifrado débil. Te recomendamos desactivarlo.

Un protocolo privado es un protocolo no publicado. Te recomendamos desactivarlo.

SSH y Secure Shell son protocolos de seguridad basados en la capa de aplicación. SSH es un protocolo confiable que brinda seguridad para sesiones de inicio de sesión remotas y otros servicios de red. El uso de SSH puede prevenir eficazmente la fuga de información durante la administración remota.

Figura 6-1 Servicios básicos



6.1.2 Configurar HTTPS

Información de contexto

HTTPS (Protocolo de transferencia de hipertexto sobre capa de conexión segura) es una entrada de servicio basada en Seguridad de la capa de transporte (TLS). HTTPS proporciona servicio web, servicio de acceso ONVIF y servicio de acceso RTSP.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**HTTPS**.

Paso 2 (Opcional) En el**Servicios basicos**pestaña, haga clic en haga clic**DE** para habilitar TLS1.1 según sea necesario y luego **ACUERDO**.

De forma predeterminada, la página web solo admite TLS1.2. Si debe utilizar TLS1.1, debe habilitar TLS1.1 en la página web. Tenga en cuenta que TLS1.1 plantea riesgos de seguridad. Le recomendamos desactivar TLS1.1 para evitar riesgos inesperados.

Paso 3 Sobre el**HTTPS**, haga clic en Seleccionar para habilitar HTTPS.

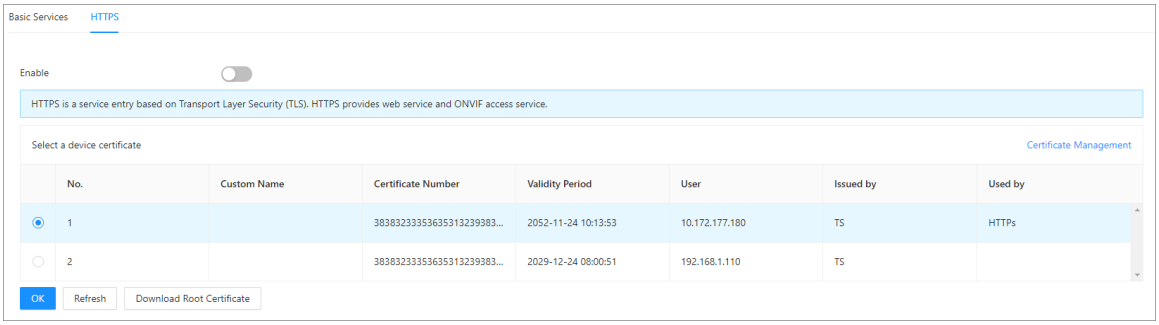
Etapa 4 un certificado de dispositivo.

Paso 5 Seleccionar**Gestión de certificados**y la página pasará a**Certificado de CA**página.

Para obtener más información, consulte "6.2 Configuración del certificado CA".

Paso 6 Hacer clic**DE ACUERDO**.

Figura 6-2 Configurar HTTPS



6.2 Configuración del certificado CA

6.2.1 Instalación del certificado del dispositivo

Información de contexto

Un certificado de dispositivo es una prueba del estado legal del dispositivo. Por ejemplo, cuando el navegador visita el dispositivo a través de HTTPS, se debe verificar el certificado del dispositivo.

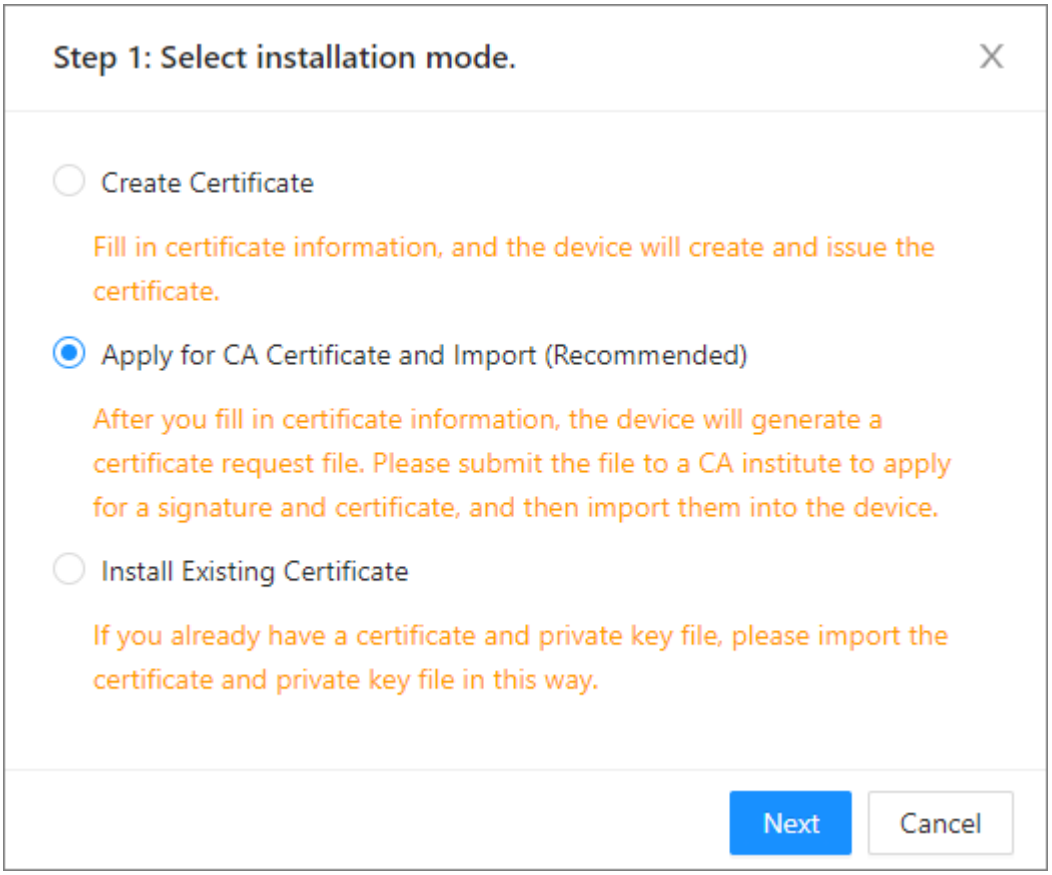
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**. Sobre el

Paso 2 **Certificado de dispositivo**pestaña, haga clic**Instalar certificado de dispositivo**.

Paso 3 Seleccione un modo de instalación según sea necesario.

Figura 6-3 Seleccionar el modo de instalación



Etapa 4 Complete la información del certificado y luego haga clic en**Crear e instalar certificado**,**Crear y descargar**, y**Importar e instalar**.

Paso 5 (Opcional) Haga clic**Ingrese al modo de edición**para editar el**Nombre personalizado**y luego haga clic en**Guardar configuración**.

Figura 6-4 Editar certificado



Operaciones relacionadas

- Descargue el certificado: Haga clic .
- Eliminar el certificado: haga clic en .

6.2.2 Instalación de certificados de CA confiables

Información de contexto

Se utiliza un certificado de CA confiable para verificar el estado legal de un host. Por ejemplo, se deberá instalar un certificado de CA de conmutador para la autenticación 802.1x.

Solo admite la instalación de certificados de CA subordinados.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Certificado de CA**.

Paso 2 En**Certificados de CA confiables**pestaña, haga clic**Instalar certificado de confianza**.

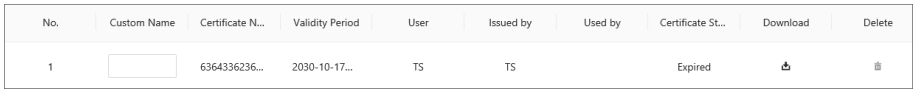
Paso 3 Hacer clic**Navegar**,y luego haga clic**DE ACUERDO**.

Figura 6-5 Instalar certificado de confianza



Etapa 4 (Opcional) Haga clic**Ingrese al modo de edición**para editar el**Nombre personalizado**y luego haga clic en**Guardar configuración**.

Figura 6-6 Editar certificado



Operaciones relacionadas

- Descargue el certificado: Haga clic .
- Eliminar el certificado: haga clic en .

6.3 Configurar la defensa contra ataques

6.3.1 Configuración del cortafuegos

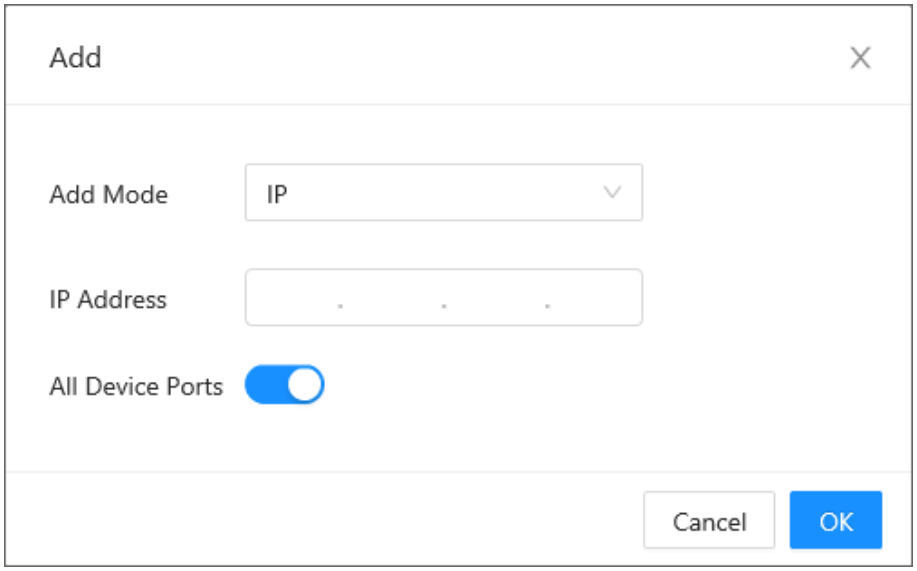
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Defensa de ataque**.

Paso 2 Sobre el**Cortafuegos**pestaña, haga clic**Todo**y todos los hosts de origen IP/MAC pueden acceder a todos los puertos del dispositivo.

Hacer clic**Lista de permitidos**,y solo los hosts de origen cuya IP/MAC esté en la siguiente lista pueden acceder a los puertos correspondientes del dispositivo y luego haga clic en**Agregar**para agregar hosts a la lista de permitidos.

Figura 6-7 Agregar a la lista de permitidos



Hacer clic**Lista de bloqueos**,y el host de origen correspondiente enumerado de direcciones IP/MAC tiene prohibido visitar los puertos correspondientes del dispositivo mediante conexión de red. Hacer clic**Agregar**para agregar hosts a la lista de bloqueo.

Figura 6-8 Agregar a la lista de bloqueo

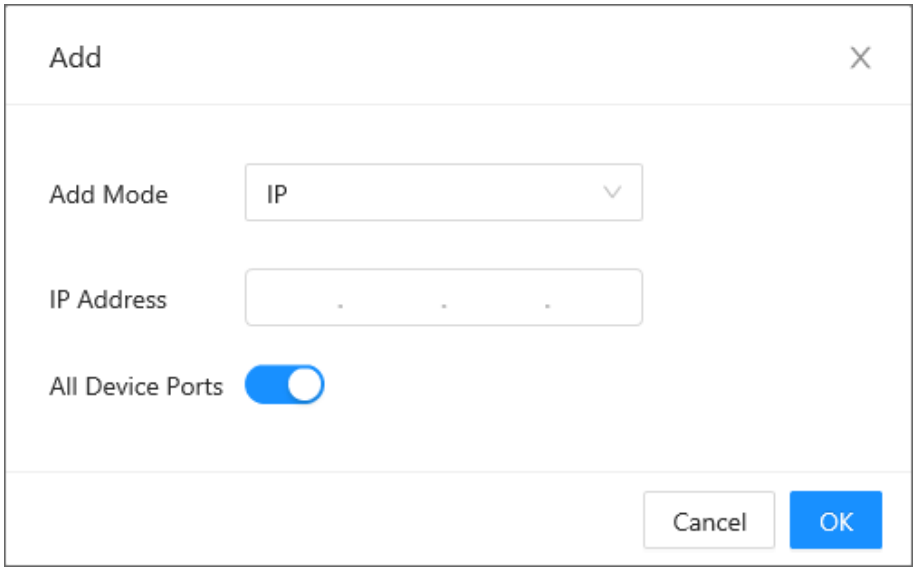


Tabla 6-1 Cortafuegos

Parámetro	Descripción
Todo	Todos los hosts de origen IP/MAC pueden acceder a todos los puertos del dispositivo.
Lista de permitidos	Solo los hosts de origen cuya IP/MAC esté en la siguiente lista pueden acceder a los puertos correspondientes del dispositivo.
Lista de bloqueos	El host de origen correspondiente de direcciones IP/MAC enumerado tiene prohibido visitar los puertos correspondientes del dispositivo.

Paso 3 Hacer clic**DE ACUERDO**.

6.3.2 Configuración del ataque Anti-DoS

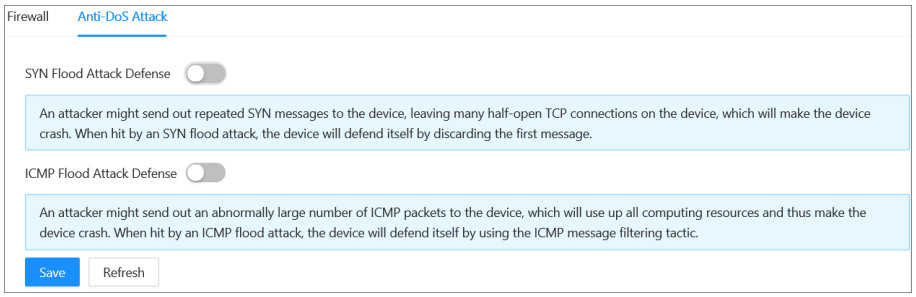
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Defensa de ataque**.

Paso 2 Sobre el**Ataque anti-DoS**pestaña, haga clic en Haga para permitir diferentes funciones de defensa según sea necesario.

Paso 3 clic**Ahorrar**.

Figura 6-9 Ataque Anti-DoS



6.4 Configuración del aislamiento de puertos

Información de contexto

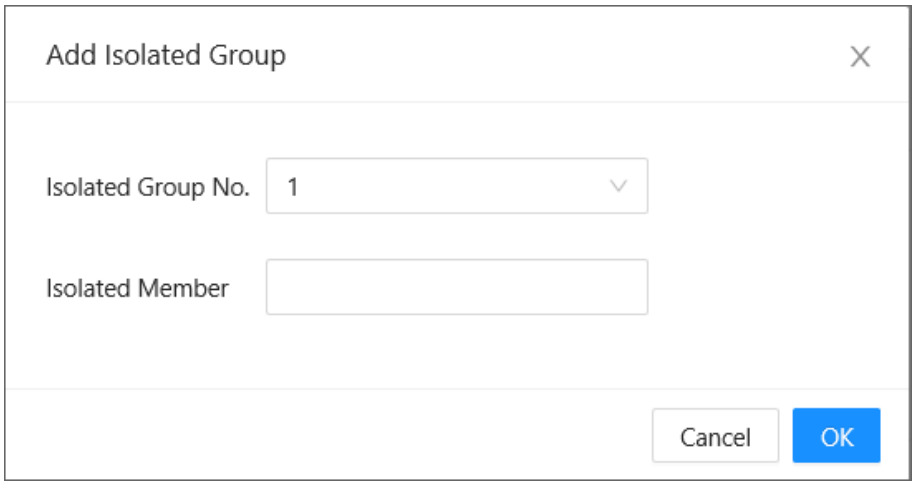
El aislamiento de puertos consiste en lograr el aislamiento de capa 2 entre mensajes. Solo necesita agregar el puerto al grupo de aislamiento para aislar los datos de capa 2 entre los puertos del grupo de aislamiento. La función de aislamiento de puertos proporciona a los usuarios una solución de red más segura y flexible.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Aislamiento de puertos**. Hacer

Paso 2 clic**Agregar**.

Figura 6-10 Agregar grupo aislado



Paso 3 Seleccionar**Grupo aislado No.**y**Miembro aislado**y luego haga clic en**DE ACUERDO**.

Operaciones relacionadas

- Editar grupo aislado: haga clic en .
- Borrar grupo aislado: haga clic en .

7 Política de control

7.1 Configuración de la prioridad del puerto

Información de contexto

De forma predeterminada, la prioridad 802.1p y la prioridad DSCP para una VLAN de voz son 6 y 46 respectivamente. Puede configurar dinámicamente la prioridad 802.1p y la prioridad DSCP para planificar prioridades para diferentes servicios de voz.

- La prioridad 802.1p se indica mediante el valor en el campo PRI de 3 bits en cada trama VLAN 802.1Q. Este campo determina la prioridad de transmisión de paquetes de datos cuando un dispositivo de conmutación está congestionado.
- El valor DSCP se indica mediante los 6 bits en el campo Tipo de servicio (ToS) en el encabezado del paquete IPv4. DSCP, como señalización para DiffServ, se utiliza para garantizar la QoS en redes IP. El controlador de tráfico en la puerta de enlace de la red toma acciones basándose simplemente en la información transportada por los 6 bits.

Procedimiento

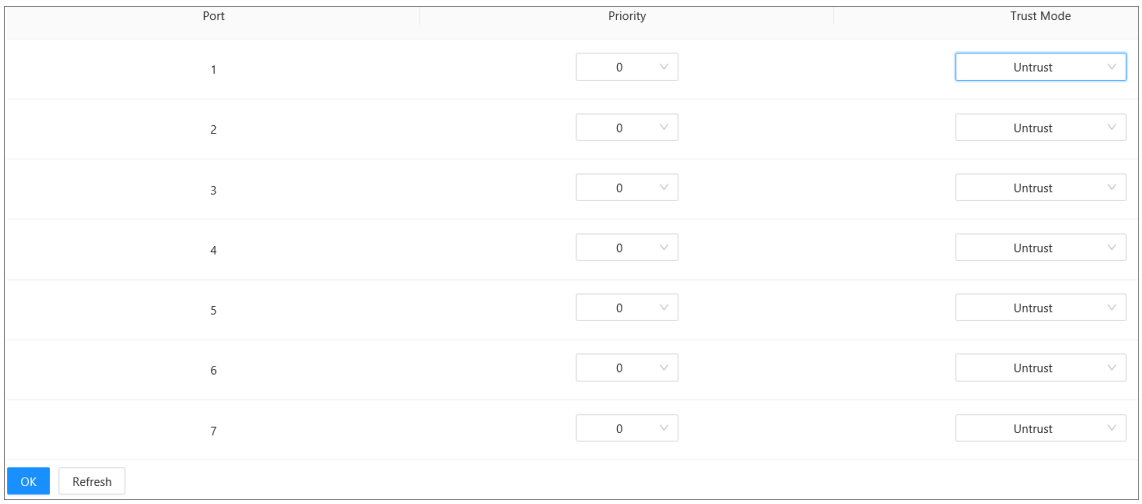
Paso 1 Seleccionar**Política de control**>**Prioridad de puerto**.

Paso 2 Seleccione del**Prioridad**y**Modo de confianza**.

El modo de confianza incluye 4 tipos de**Desconfiar**,**802.1P**,**DSCP**, y**DSCP y 802.1P**.

Paso 3 Hacer clic**DE ACUERDO**.

Figura 7-1 Configurar la prioridad del puerto



7.2 Configuración de la tabla de asignación de prioridades

Procedimiento

Paso 1 Seleccionar**Política de control**>**Tabla de mapeo de prioridades**.

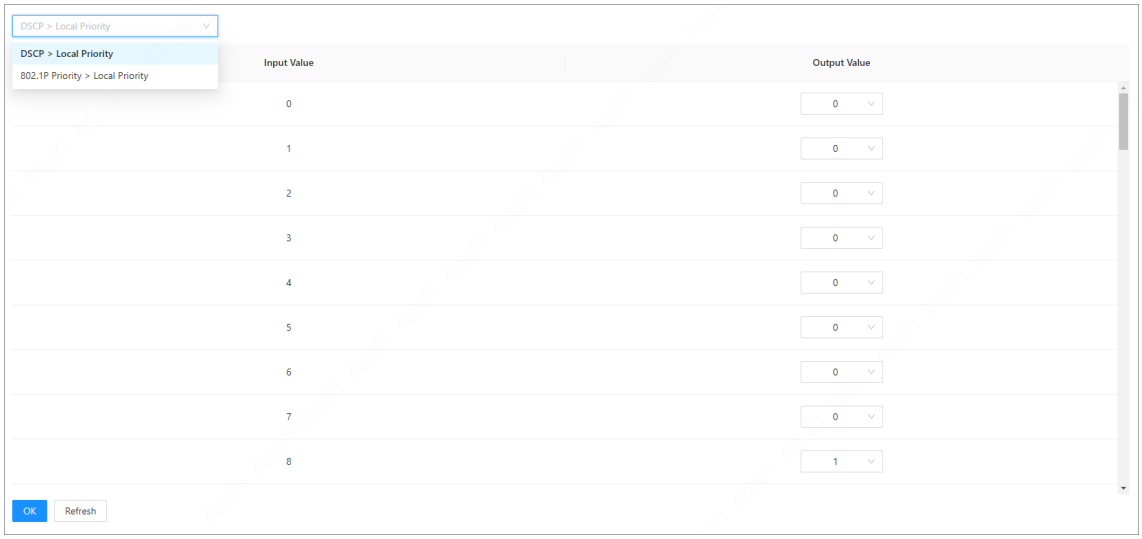
Paso 2 Seleccionar**DSCP > Prioridad local**o**802.1p > Prioridad local**.

Paso 3 Seleccionar**Valor de salida**.

El valor de entrada y el valor de salida varían según los diferentes modos.

Etapa 4 Hacer clicDE ACUERDO.

Figura 7-2 Mapeo de prioridades



7.3 Configurar la programación de colas

Información de contexto

- PQ: cola prioritaria. PQ programa paquetes en orden de prioridad descendente. Los paquetes en colas con una prioridad más baja se pueden programar solo después de que se hayan programado todos los paquetes en las colas con una prioridad más alta.
- WRR: Round Robin ponderado. En la programación WRR, el dispositivo programa paquetes en colas mediante sondeo según el peso de la cola. Después de una ronda de programación, los pesos de todas las colas se reducen en 1. La cola cuyo peso se reduce a 0 no se puede programar.

Procedimiento

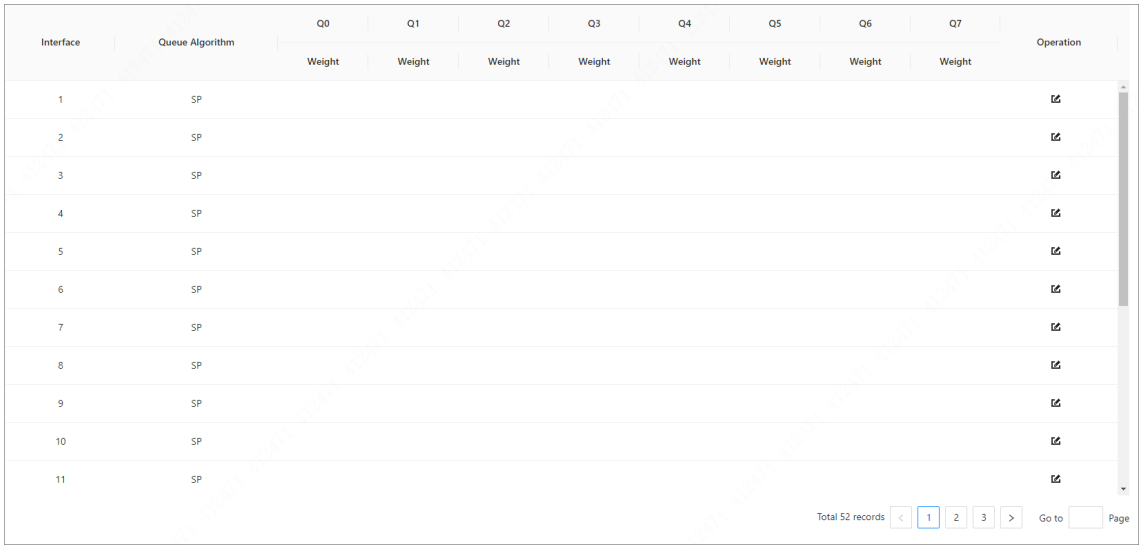
Paso 1 Seleccionar**Política de control**>**Programación de**

Paso 2 **colas**. Seleccione del**Algoritmo de cola**.

En el modo WRR, la relación de peso de la cola de prioridad es Cola0:Cola1:Cola2:Cola3=1:2:4:8.

Paso 3 Hacer clicDE ACUERDO.

Figura 7-3 Programación de colas



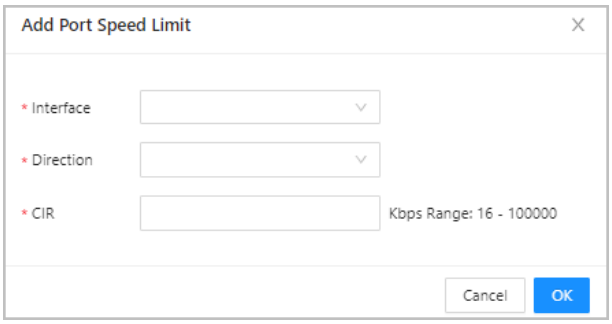
7.4 Configuración del límite de velocidad del puerto

Procedimiento

Paso 1 Seleccionar**Política de control**>**Límite de velocidad del puerto**. Hacer

Paso 2 clic**Agregar**.

Figura 7-4 Agregar límite de velocidad del puerto



Paso 3 Introducir el**Interfaz**,**Dirección**, y**CIR**.

- los valores de**Dirección**incluir**En**y**Afuera**.
- La regla de entrada para CIR: rango de 16 a 100000 y debe ser un múltiplo entero de 16.

Etapa 4 Hacer clic**DE ACUERDO**.

7.5 Configuración del control de tormentas

Información de contexto

Las tramas de difusión en la red se reenvían continuamente, lo que afecta las comunicaciones adecuadas y reduce en gran medida el rendimiento de la red. El control de tormentas puede limitar los flujos de transmisión del puerto y descartar las tramas de transmisión una vez que el flujo excede el especificado.

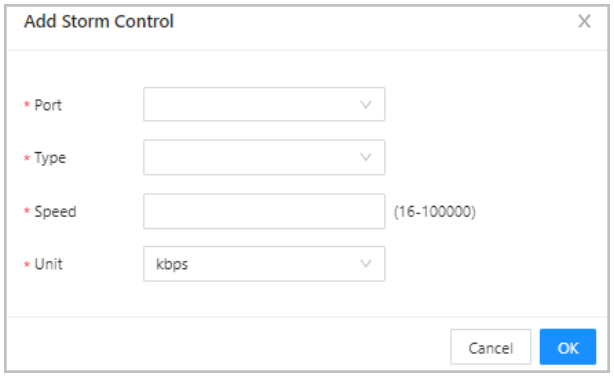
umbral, que puede reducir el riesgo de la tormenta de transmisión y garantizar el funcionamiento adecuado de la red.

Procedimiento

Paso 1 Seleccionar**Política de control**>**Control de tormentas**. Hacer

Paso 2 clic**Agregar**.

Figura 7-5 Agregar control de tormentas



Paso 3 Introducir el**Puerto**,**Tipo**, y**Velocidad**. Hacer clic**DE**

Etapa 4 **ACUERDO**.

8 Autenticación

8.1 Configuración de 802.1x

Información de contexto

802.1X es un protocolo de autenticación de red que abre puertos para el acceso a la red cuando una organización autentica la identidad de un usuario y le autoriza el acceso a la red.

Procedimiento

Paso 1 Hacer clic al lado de**Permitir**para habilitar NAS (almacenamiento conectado a la red).

Paso 2 Seleccionar de**Estado del puerto**.

El estado incluye**Auto**,**Fuerza no autorizada**, y**Fuerza autorizada**.

Figura 8-1 Configurar 802.1x

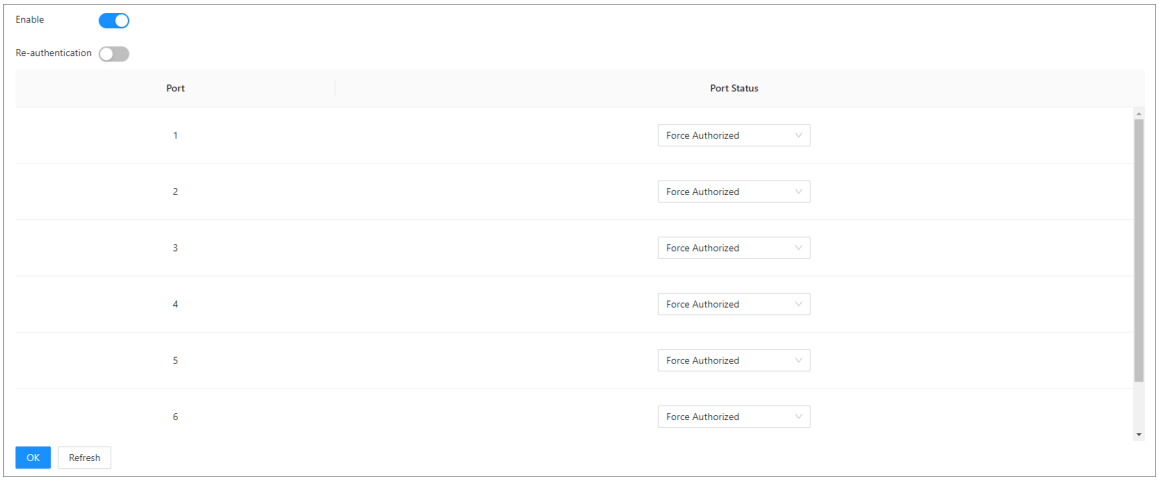


Tabla 8-1 Descripción de 802.1x

Parámetro	Descripción
Auto	El puerto configura automáticamente el estado según los resultados de la autenticación.
Fuerza no autorizada	● El puerto siempre está en estado no autorizado y los usuarios no pueden autenticarse. ● El dispositivo no proporciona servicios de autenticación para los usuarios que acceden a través de este puerto.
Fuerza autorizada	El puerto siempre está en estado autorizado y los usuarios pueden acceder a los recursos de la red sin autenticación.

Paso 3 Hacer clic**DE ACUERDO**.

8.2 Configuración del radio

Información de contexto

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

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

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

Procedimiento

Paso 1 Seleccionar**Autenticación**>**RADIO**.

Figura 8-2 RADIO



Paso 2 Hacer clic**Agregar**.

Figura 8-3 Agregar RADIO



Paso 3 Selecciona el**Dirección IP**,**puerto**, y**llave**. Hacer clic**DE**

Etapa 4 **ACUERDO**.

Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red de dispositivos:

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya el nombre de la cuenta ni el nombre de la cuenta en orden inverso.
- No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

2.**Actualice el firmware y el software del cliente a tiempo**

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "es bueno tener" para mejorar la seguridad de la red de su dispositivo:

1.Protección física

Le sugerimos que realice protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales, e implemente permisos de control de acceso y administración de claves bien hechos para evitar que personal no autorizado lleve a cabo contactos físicos, como daños en el hardware, conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2.**Cambie las contraseñas con regularidad**

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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

4.**Habilitar bloqueo de cuenta**

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

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

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

6.**Habilitar HTTPS**

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

7.**Enlace de dirección MAC**

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de ARP.

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

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

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

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. **Transmisión cifrada de audio y vídeo**

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada para reducir el riesgo de que los datos de audio y video sean robados durante la transmisión.

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

11. **Auditoría segura**

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

12. **Registro de red**

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

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

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.