Conmutador Ethernet (conmutador administrado en la nube)

Manual del usuario

Versión 1.0.0

Prefacio

Este manual presenta las funciones y operaciones del conmutador Ethernet (en adelante, el "dispositivo"). Léalo detenidamente antes de utilizar el producto. Tras leerlo, guarde el documento correctamente para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
DANGER	Indica un peligro potencial alto 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, reducciones en el rendimiento o resultados impredecibles.
ESD	Dispositivos sensibles a la electroestática. Indica un dispositivo que es sensible a la descarga electrostática.
ELECTRIC SHOCK	Indica alto voltaje peligroso. Tenga cuidado de no entrar en contacto con la electricidad.
LASER RADIATION	Indica un peligro de radiación láser. Tenga cuidado de evitar la exposición a un rayo láser.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Junio de 2024

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, podría recopilar datos personales de otras personas, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas 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 una identificación clara y visible para informar a las personas de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- 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 registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o 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 explicación final.

Tabla de contenido

1 Gestión de la nube

El dispositivo se puede administrar a través de la aplicación DoLynk Care y la plataforma DoLynk Care sin necesidad de inicialización después de encenderlo.

1.1 Administrado por la aplicación DoLynk Care

Procedimiento

Paso 1 Busque DoLynk Care en la tienda de aplicaciones y luego descargue la aplicación.

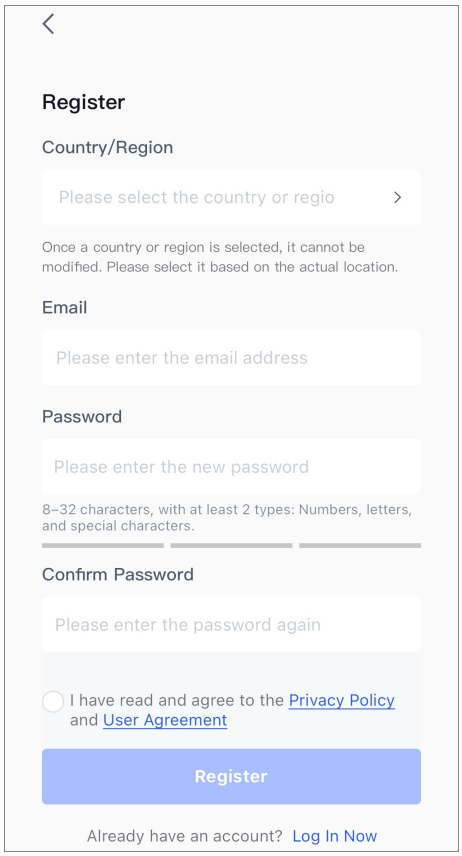
Para los usuarios de Android, pueden ir a Google Play para descargar DoLynk Care.

Paso 2 En tu teléfono, toca Para iniciar la aplicación, crea una cuenta.

1. En el**Acceso**pantalla, toque**Crear una cuenta**.
2. En el**Registro**Pantalla, complete la información de los campos obligatorios.

Algunos países o regiones permiten registrar una cuenta con el número de teléfono. Consulta la interfaz para obtener más información.

Figura 1-1 Registro



3. Lea el**política de privacidad**y**Acuerdo de usuario**, y luego seleccione el**He leído y acepto la Política de privacidad y el Acuerdo de usuario.**caja.
4. Toque**Registro**,y luego la aplicación vuelve a la**Acceso**pantalla.

Paso 3 Ingrese su dirección de correo electrónico y contraseña y luego toque**Acceso**.

- Algunos países o regiones admiten el uso del número de teléfono para iniciar sesión. Consulte la interfaz real para obtener más detalles.
- Puedes iniciar sesión con la cuenta que hayas registrado en Partner App o DoLynk Panel de control. Toque para ver las instrucciones.
- Si inicia sesión con su cuenta personal desde la aplicación para socios y no seleccionó el país o el área cuando registró la cuenta, deberá seleccionar un país cuando inicie sesión por primera vez.
- Si inicia sesión con la cuenta de empresa desde la App para Socios, deberá seleccionar un rol (administrador o empleado) para iniciar sesión por primera vez. Si el rol seleccionado es de empleado, primero deberá contactar al administrador para crear una cuenta de empleado.

Paso 4 Grifo  en la esquina superior izquierda de la página y luego toque el perfil de la cuenta.

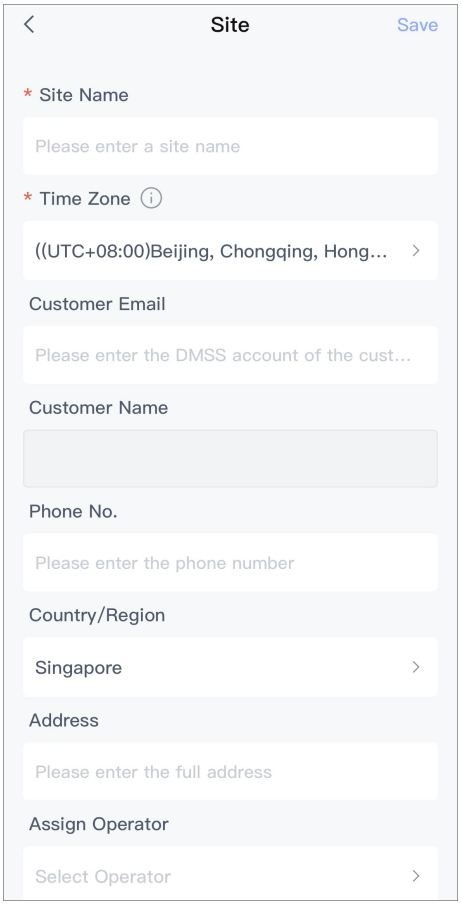
Paso 5 Grifo**Sitios**, y luego toque  para agregar un sitio.

- **Nombre del cliente**y**Correo electrónico del cliente**:Ingrese el nombre y el correo electrónico del usuario final.

  Ingrese la dirección de correo electrónico de la cuenta que su cliente registró en la aplicación DMSS. DoLynk Care la verificará.
- **País/Región**:El país o área se mantiene igual que el país o región de la cuenta de forma predeterminada.
- **Operador de asignación**:Seleccione un operador al que desea asignar este sitio.

  Antes de asignar un operador en la aplicación DoLynk Care, debe crear y administrar cuentas de operador en el portal de DoLynk Care. Para obtener más información, consulte*Manual del usuario de DoLynk Care*.

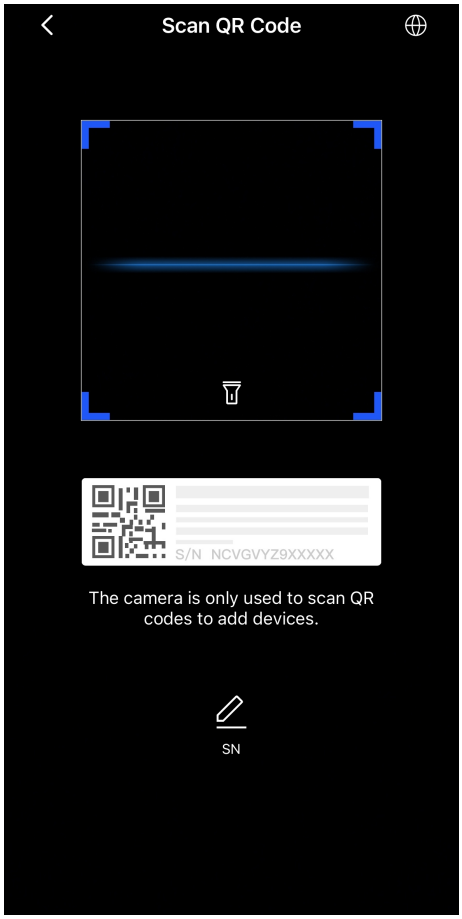
Figura 1-2 Agregar un sitio



Paso 6 Agregue dispositivos escaneando el código QR del dispositivo o ingresando manualmente el número de serie del dispositivo.

1. En la pantalla de inicio, pulsa . Pulsa **Código QR**.

Figura 1-3 Agregar un dispositivo



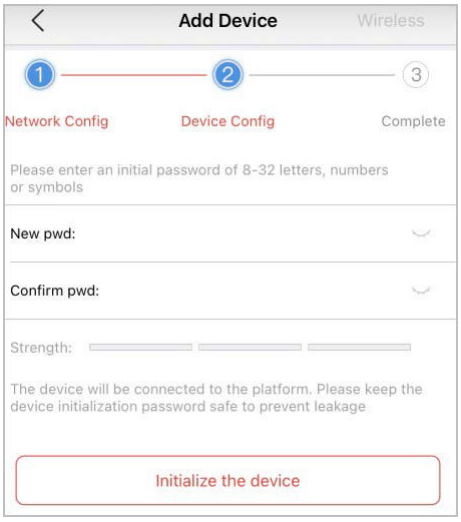
2. Escanee el código QR del dispositivo o toque para ingresar manualmente el número de serie del dispositivo.

   Al agregar un dispositivo mediante el número de serie (SN), debe ingresar el SN y la contraseña. La contraseña predeterminada antes de inicializar el dispositivo es el código SC, que se puede obtener de la etiqueta del dispositivo.

3. Seleccione un sitio y luego toque**DE ACUERDO**.
4. En el**Agregar dispositivo**Pantalla, seleccione un tipo de dispositivo.
5. Si el dispositivo que está agregando no está inicializado, ingrese la contraseña y confírmela nuevamente, y luego toque**Inicializar el dispositivo**para completar la inicialización.

   Si el dispositivo que está agregando está inicializado, ingrese la contraseña y luego haga clic en**DE ACUERDO**.

Figura 1-4 Inicializar el dispositivo



6. Toque**Terminado**y luego podrá ver el dispositivo en la lista de dispositivos.

En la página de la consola, toque el perfil de la empresa para ir a la página de administración de la cuenta.

Grifo al lado de**Ayuda y comentarios**Para ver el documento en la aplicación, incluido el del usuario. Manual, preguntas frecuentes y más.

1.2 Administrado por la plataforma DoLynk Care

Procedimiento

Paso 1 Crear una cuenta.

Para iniciar sesión por primera vez en DoLynk Care, primero debe crear una cuenta. Los métodos de registro incluyen el registro de una cuenta personal y el registro por invitación de GSP.

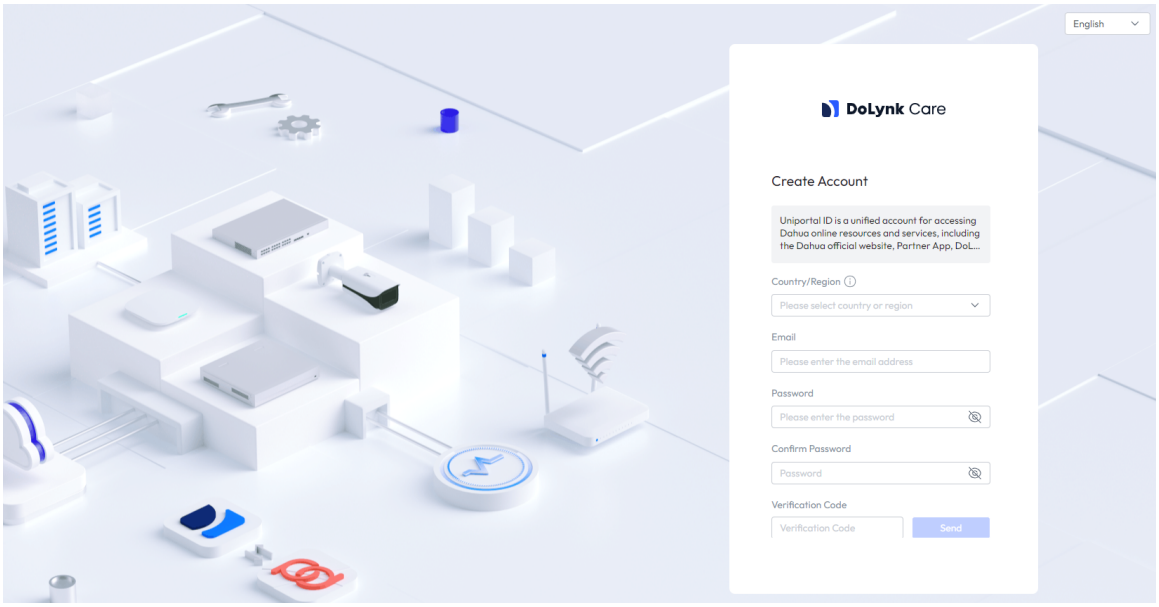
- Registro de cuenta personal

  Puede registrarse a través del portal de registro de la página de inicio de sesión de la plataforma. La cuenta registrada es personal. Si necesita usar funciones como confiar dispositivos y comprar paquetes de servicios, deberá autenticar su empresa después de iniciar sesión.

  1. Ingrese la dirección de la plataforma en el navegador y presione Enter. Seleccione el idioma en la esquina superior derecha de la página.
  2. Haga clic**Crear una cuenta**para crear una cuenta.
  3. Seleccione el país o la región, ingrese la dirección de correo electrónico y la contraseña y luego haga clic en **Enviar**para obtener el código de verificación.
  4. Ingrese el código de verificación que se envió al correo electrónico registrado y luego lea y seleccione**He leído y acepto la Política de Privacidad y los Términos y Condiciones.**.Hacer clic **Inscribirse**.

  Algunos países o regiones permiten registrar una cuenta con el número de teléfono para obtener el código de verificación. Consulta la interfaz para obtener más información.

Figura 1-5 Registro de cuenta personal



- Registro de invitación de GSP: para obtener más detalles, consulte el Manual del usuario de DoLynk Care.

Paso 2 Abra el navegador, introduzca la dirección web y pulse Intro. Introduzca el correo electrónico y la contraseña, y haga clic en**Acceso**.

- Algunos países o regiones admiten el uso del número de teléfono para iniciar sesión. Consulte la interfaz real para obtener más detalles.
- Si inicia sesión con su cuenta personal desde la aplicación Partner y no seleccionó el país o el área cuando registró la cuenta, deberá seleccionar un país cuando inicie sesión por primera vez.
- Si inicia sesión con la cuenta de empresa desde la app Partner, deberá seleccionar un rol (administrador o empleado) para iniciar sesión por primera vez. Si el rol seleccionado es de empleado, primero deberá contactar al administrador para crear una cuenta de empleado.

Paso 3 Agregar un sitio.

1. Haga clic**Sitios**en la página de la consola.
2. Haga clic**Agregar**en la página de administración del sitio y luego configure los parámetros.
3. Haga clic**DE ACUERDO**.

Paso 4 Agregar dispositivos.

1. Haga clic**Dispositivos**en la página de la consola.
2. Haga clic**Agregar**.
3. Ingrese el nombre del dispositivo, el número de serie del dispositivo y la contraseña del dispositivo.

   Debe seleccionar un sitio para el dispositivo. Puede seleccionar uno existente de la lista o crear uno nuevo.

   - Al agregar un dispositivo mediante el número de serie (SN), debe ingresar el SN y la contraseña. La contraseña predeterminada antes de inicializar el dispositivo es el código SC, que se puede obtener de la etiqueta del dispositivo.
   - No es posible agregar el dispositivo que está vinculado a un cliente.
   - Si agrega un interruptor, puede cambiar la contraseña del dispositivo siguiendo las instrucciones en pantalla.

4. Haga clic**DE ACUERDO**.

Hacer clic  en la esquina superior derecha para ir a**Ayuda**página, ver el documento en la plataforma, incluyendo manual de usuario, preguntas frecuentes y más.

2 Inicialización e inicio de sesión

El conmutador administrado en la nube ofrece acceso web. Puede iniciar sesión en la interfaz web para administrar y configurar el dispositivo.

2.1 Inicialización del dispositivo

Prerrequisitos

- Asegúrese de que el dispositivo esté conectado a la fuente de alimentación.
- Asegúrese de que el dispositivo esté conectado a la computadora y que las direcciones IP de la computadora y del dispositivo estén en el mismo segmento.
- El DHCP está habilitado por defecto en el dispositivo. Al conectarse a una red, el dispositivo suele obtener una dirección IP de un servidor DHCP, y luego se puede obtener la dirección IP del dispositivo ascendente, como un router. Si no hay un servidor DHCP disponible, la dirección IP predeterminada del dispositivo es 192.168.1.110.

  Puede utilizar Configtool para obtener la dirección IP en modelos seleccionados de dispositivos.

Procedimiento

Paso 1 Introduzca la dirección IP del dispositivo en la barra de direcciones del navegador web y luego presione la tecla Enter.

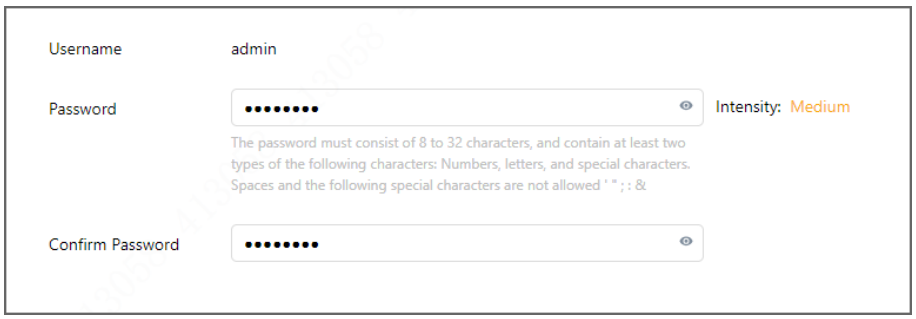
Paso 2 Seleccione el idioma y luego haga clic**Próximo**.

Paso 3 Lea la declaración legal, seleccione**He leído y acepto los términos del Acuerdo de licencia de software y la Política de privacidad.**,y luego haga clic**Próximo**.

Paso 4 Configurar la contraseña.

- El nombre de usuario predeterminado es admin.
- Configure una contraseña de alta seguridad según la solicitud de seguridad. La contraseña debe tener entre 8 y 32 caracteres, incluyendo al menos dos tipos: números, letras y caracteres comunes (cualquier carácter visible excepto "; : &).

Figura 2-1 Configurar contraseña



Paso 5 Hacer clic**Completo**.

2.2 Iniciar sesión en el dispositivo

Prerrequisitos

- El dispositivo ha sido inicializado.

- Asegúrese de que el dispositivo esté conectado a la computadora y que las direcciones IP de la computadora y del dispositivo estén en el mismo segmento de red.

Procedimiento

Paso 1 Introduzca la dirección IP del dispositivo en la barra de direcciones del navegador web y luego presione la tecla Enter.

Paso 2 Introduzca la contraseña.

Paso 3 Hacer clic**Acceso**.

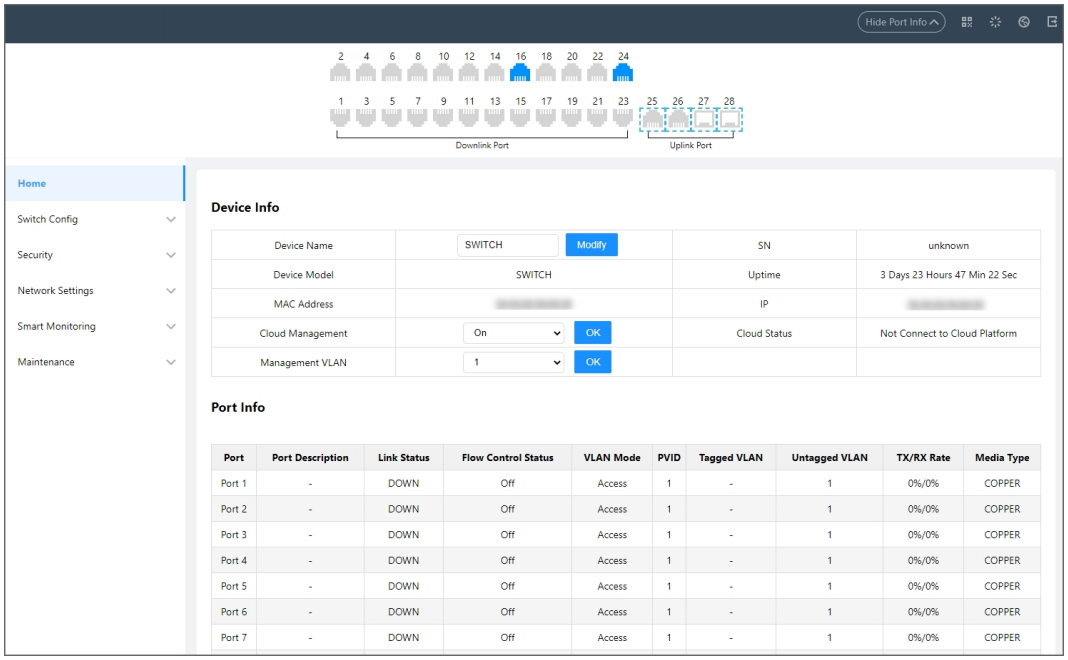
2.3 Página de inicio

Después de iniciar sesión, el sistema será dirigido a la**Hogar**página.

El lado izquierdo de la página consta de una barra de menú. En la parte superior, se muestra una visualización gráfica del estado del puerto. En la esquina superior derecha, se pueden ocultar o mostrar la información del puerto, cerrar sesión, reiniciar el dispositivo, cambiar el idioma del sistema y escanear códigos QR para acceder a la información.

La página web es sólo para referencia y puede diferir según su dispositivo.

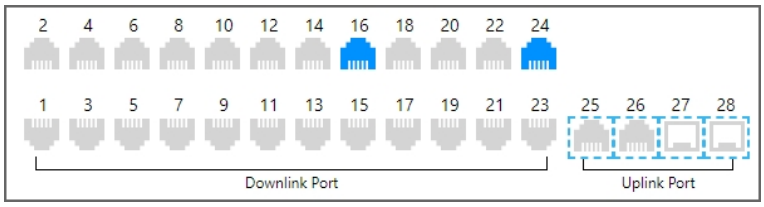
Figura 2-2 Página de inicio



Información del puerto

- Puerto azul: El puerto conectado al dispositivo.
- Puerto gris: El puerto no está conectado al dispositivo.
- Coloque el cursor sobre un puerto para ver su información de conexión, incluido el estado del puerto, el estado del enlace y el consumo de energía.
- Haga clic en un puerto y luego vaya a**Puerto**página.

Figura 2-3 Información del puerto



Página de inicio

HogarLa página admite las siguientes funciones.

- **Información del dispositivo**:Configure el nombre del dispositivo, la VLAN de administración y la administración de la nube.

  ⚠

  ◇ La gestión de la nube está habilitada por defecto. Si la desactiva, el dispositivo no podrá gestionarse a través de la aplicación DoLynk Care. Para obtener más información sobre el uso de la gestión de la nube, consulte "1 Gestión de la nube".

  ◇ Después de habilitar la VLAN de administración, solo podrá acceder a la página web del dispositivo a través de una dirección IP de VLAN de administración.
- **Información del puerto**:Muestra el estado del enlace, el estado del control de flujo y el modo VLAN de cada puerto.

Tabla 2-1 Descripción de la información del puerto

Parámetro	Descripción	
Puerto	Muestra todos los puertos del dispositivo.	
Descripción del puerto	Configura la descripción del puerto, también puedes ir a**Configuración del conmutador**>**Puerto**Para configurar.	
Estado del enlace	● Muestra la velocidad del puerto y el modo dúplex: el puerto está conectado. ● ABAJO: El puerto no está conectado o la conexión falla.	
Estado del control de flujo	Ver el estado de la función de control de flujo, incluyendo**En**y**Apagado**. Puedes ir a **Configuración del conmutador**>**Puerto**Para configurar.	
Modo VLAN	Incluye**Acceso**y**Trompa**.	
PVID	La VLAN del puerto.	Ir a**Configuración del conmutador** > **VLAN**Para configurar.
VLAN etiquetada	El ID de VLAN para el puerto que puede etiquetarse al enviar paquetes.	
VLAN sin etiquetar	El ID de VLAN para el puerto que puede no tener etiquetas al enviar paquetes.	
Tarifa TX/RX	La tasa de recepción actual o la tasa de envío dividida por la tasa negociada real 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.	

Configuración de 3 conmutadores

3.1 Configuración de la información del puerto

Puede configurar los parámetros del puerto, como la velocidad/dúplex, el control de flujo y otros. Estos parámetros afectarán directamente su modo de funcionamiento. Configure según sus necesidades.

Procedimiento

Paso 1 Seleccionar**Configuración del conmutador**>**Puerto**.

Paso 2 Seleccione el número de puerto, configure los parámetros y luego haga clic en**Ahorrar**.

- **Velocidad/Dúplex**:Configure la velocidad y el modo dúplex. La velocidad/dúplex se configura como**Auto**para puerto combinado.
- **Control de flujo**:Habilitar la función de control de flujo puede aliviar eficazmente la congestión de la red, reducir la pérdida de datos y mejorar la estabilidad de la red y la confiabilidad de los datos.
- **Configuración de EEE**:Habilitar la función EEE (Ethernet de eficiencia energética) puede reducir el consumo de energía cuando la red está inactiva y lograr un efecto de ahorro de energía.

Figura 3-1 Configuración del puerto (1)

Paso 3 En el**Descripción del puerto**En el cuadro, ingrese la descripción del puerto.

La descripción no puede exceder los 16 caracteres. Solo números, letras y el carácter especial (_).

Figura 3-2 Configuración del puerto (2)

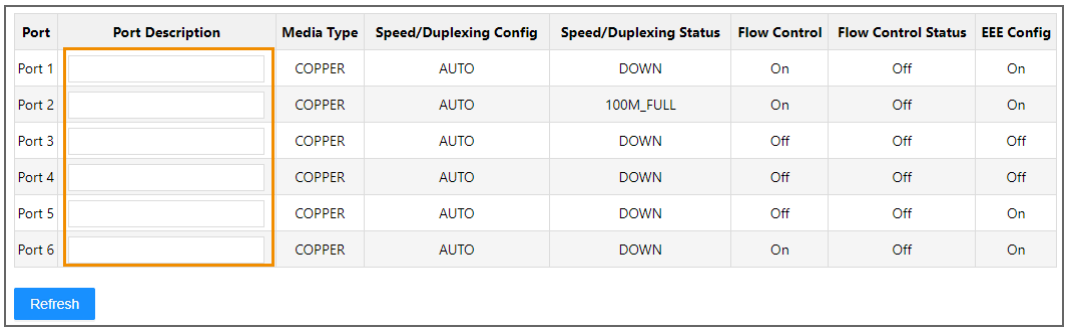


Tabla 3-1 Descripción de los parámetros del puerto

Parámetro	Descripción
Tipo de medio	Incluye dos tipos:**COBRE**y**FIBRA**. ● **COBRE**:Puerto RJ-45. ● **FIBRA**:Puerto de fibra.
Velocidad/Dúplex Configuración	Se muestran los parámetros configurados para este puerto.

Parámetro	Descripción
Velocidad/Dúplex Estado	• En línea: muestra la velocidad del puerto y el modo dúplex. • Sin conexión: Muestra**ABAJO**.
Control de flujo	Muestra si la función de control de flujo está habilitada y el estado actual del control de flujo.
Estado del control de flujo	
Configuración de EEE	Muestra si la función EEE está habilitada.

3.2 Configuración de VLAN

Puedes agregar el puerto a la VLAN. La VLAN predeterminada es VLAN1.

Información de fondo

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

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

- **Acceso**:El puerto pertenece a una VLAN y se utiliza para conectarse al puerto de la computadora.
- **Trompa**:El puerto permite que pasen múltiples VLAN, para recibir y enviar mensajes de múltiples VLAN, y se utiliza para conectar entre los conmutadores.

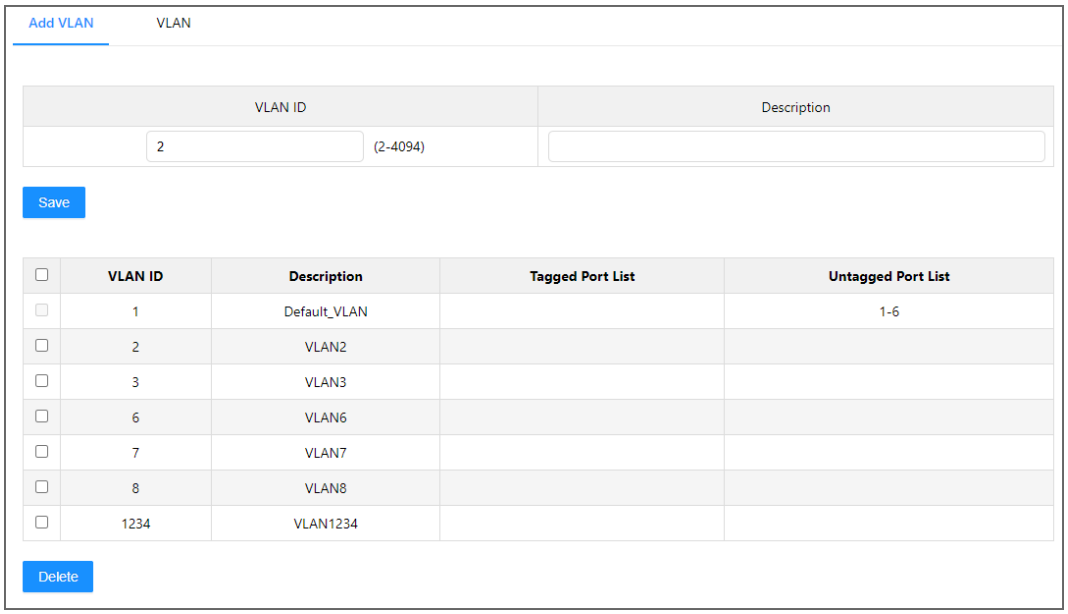
Procedimiento

Paso 1 Seleccionar**Configuración del conmutador**>**VLAN**>**Agregar VLAN**.

Paso 2 Ingrese el ID de VLAN y la descripción y luego haga clic en**Ahorrar**.

Seleccione la VLAN y luego haga clic en**Borrar**para eliminar la VLAN. VLAN1 no se puede eliminar.

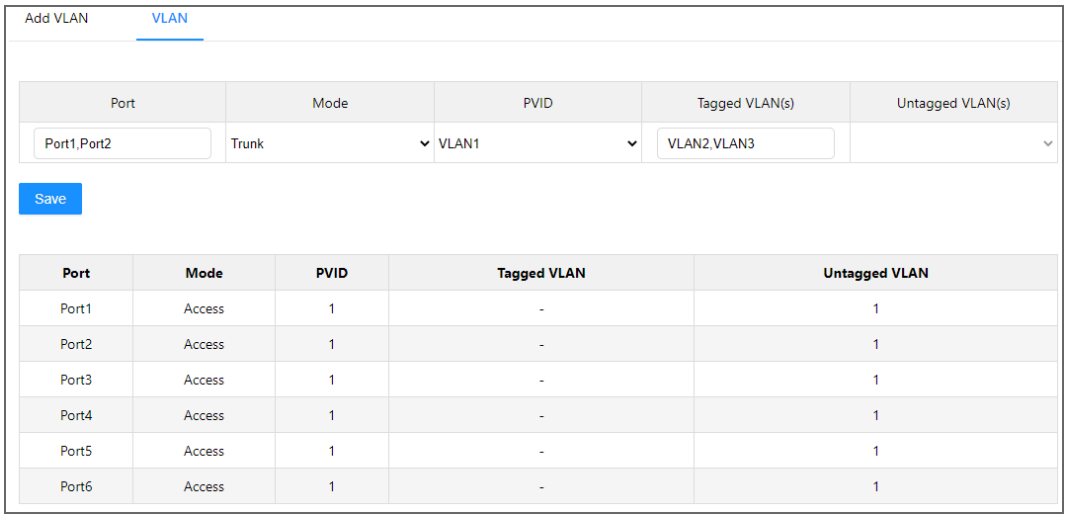
Figura 3-3 Agregar VLAN



Paso 3 Haga clic en el**VLAN**Pestaña para configurar los parámetros de VLAN del puerto. 1. Seleccione uno o más puertos.

2. Seleccione el modo VLAN, incluido**Acceso**y**Trompa**.

Figura 3-4 VLAN



3. Configure PVID, VLAN etiquetada y VLAN sin etiquetar.

- Cuando el modo es Acceso, debe configurar la VLAN sin etiquetar. Esta VLAN indica el ID de VLAN del puerto que puede estar sin etiquetar al enviar paquetes.
- Cuando el modo es Troncal, debe configurar PVID y VLAN etiquetada.

  PVID indica que el puerto está agregado a una VLAN. De forma predeterminada, el puerto pertenece a la VLAN 1. El ID de VLAN del puerto que se puede etiquetar al enviar paquetes.

Tabla 3-2 Comparación del procesamiento de cuadros

Tipo de puerto	Marco sin etiquetar tratamiento	Marco etiquetado tratamiento	Transmisión de tramas
Acceso	Recibe un sin etiquetar marco y agrega una etiqueta con la ID de VLAN predeterminada al marco.	• Acepta el marco etiquetado si la ID de VLAN del marco coincide con la ID de VLAN predeterminada. • Descarta el marco etiquetado si la ID de VLAN del marco difiere de la ID de VLAN predeterminada.	Una vez eliminada la etiqueta PVID, se transmite el marco.

Tipo de puerto	Marco sin etiquetar tratamiento	Marco etiquetado tratamiento	Transmisión de tramas
Trompa	• Agrega una etiqueta con la ID de VLAN predeterminada a un marco sin etiquetar y acepta el marco si el permisos de interfaz la VLAN predeterminada IDENTIFICACIÓN. • Agrega una etiqueta con la ID de VLAN predeterminada a un marco sin etiquetar y descarta el marco si el la interfaz niega la VLAN predeterminada IDENTIFICACIÓN.	• Acepta un marco etiquetado si la interfaz permite la ID de VLAN transportada en el marco. • Descarta un marco etiquetado si el ID de VLAN transportado en el marco es denegado por el interfaz.	• Si el ID de VLAN del marco coincide con el valor predeterminado El ID de VLAN y el ID de VLAN están permitidos por la interfaz, el dispositivo elimina la etiqueta y transmite el marco. • Si la ID de VLAN del marco difiere de la ID de VLAN predeterminada, pero la interfaz aún permite la ID de VLAN, el dispositivo transmitirá el marco directamente.

4. Haga clic**Ahorrar**.

3.3 Gestión de PoE

PoE se refiere a que el dispositivo utiliza cables de red para conectar externamente un dispositivo alimentado (PD) y obtener alimentación remota a través de puertos Ethernet. La función PoE permite una alimentación centralizada y un respaldo práctico. Los terminales de red no necesitan alimentación externa, solo un cable de red.

Los conmutadores que no son PoE no admiten esta función.

3.3.1 Configuración global

Puede configurar PoE perpetuo, energía disponible y energía de alerta.

Procedimiento

Paso 1 Seleccionar**Configuración del conmutador**>**PoE**>**Configuración**

Paso 2 **global**. Seleccionar**PoE perpetuo**,y luego haga clic**Ahorrar**.

Habilite PoE perpetuo, que permite que los dispositivos alimentados continúen recibiendo energía incluso después de que se reinicie el dispositivo.

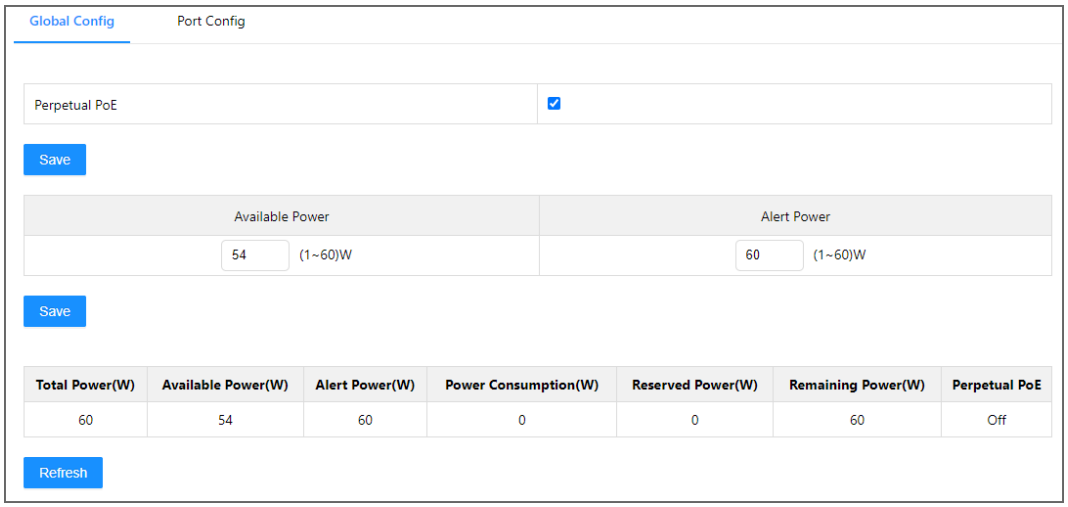
Paso 3 Configurar la potencia disponible y la potencia de alerta.

La potencia total, la potencia disponible, la potencia de alerta, el consumo de energía, la potencia reservada, la potencia restante y el PoE permanente se muestran en la parte inferior de la página. La potencia reservada = Potencia total – Potencia de alerta.

- La potencia de alerta debe ser mayor que la potencia disponible.
- La potencia disponible se refiere a la potencia máxima que se puede suministrar a los dispositivos alimentados. Cuando el consumo de energía es inferior a la potencia disponible, se permite el encendido de nuevos dispositivos alimentados.

- Durante el funcionamiento, el consumo real de energía puede fluctuar. Cuando el consumo de energía supera la potencia de alerta, los puertos se alimentarán de menor a mayor según la prioridad (a mayor número de puerto, menor prioridad), hasta que el consumo de energía sea inferior a la potencia de alerta.

Figura 3-5 Configuración global



Paso 4 Hacer clic**Ahorrar**.

3.3.2 Configuración del puerto

Configurar la función PoE del puerto.

Procedimiento

Paso 1 Seleccionar**Configuración del conmutador**>**PoE**>**Configuración del puerto**.

Paso 2 Seleccione el número de puerto, habilite PoE, PoE de larga distancia, PoE watchdog y fuerce PoE según sea necesario.

- **PoE**:El dispositivo utiliza cables de red para conectar PD externamente para el suministro de energía remoto a través de puertos eléctricos Ethernet.
- **PoE de larga distancia**:Después de habilitar PoE de larga distancia, la distancia máxima de transmisión cambiará de 100 m a 250 m y la velocidad de transmisión se reducirá a 10 Mbps.

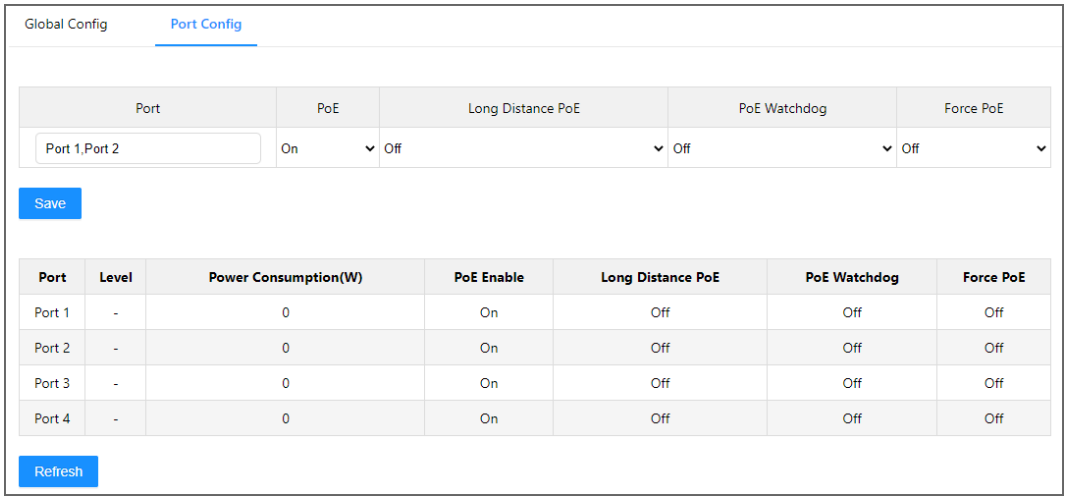
  La distancia de transmisión real puede variar debido al consumo de energía de los dispositivos conectados o al tipo y estado del cable.
- **Vigilancia de PoE**:Con el PoE Watchdog habilitado, puede supervisar los dispositivos PD y mantenerlos en línea, además de verificar su estado según intervalos de tiempo. Si no hay transmisión de datos, el puerto PoE se apagará y reiniciará automáticamente.

  Los intervalos de tiempo para las comprobaciones del estado de los dispositivos PD aumentan progresivamente, comenzando desde 1 minuto y duplicándose cada vez (1, 2, 4, 8, 16 y más). El intervalo máximo es de 1024 minutos.
- **Fuerza PoE**:Cuando el dispositivo alimentado conectado al puerto es un dispositivo no estándar, utilice esta función para forzar la fuente de alimentación PoE.

Tras habilitar la alimentación forzada PoE, el puerto forzará el suministro de energía al dispositivo alimentado, independientemente de si el dispositivo conectado cumple los requisitos. Tenga en cuenta lo siguiente.

Fuerza PoEy**Vigilancia de PoE**No se pueden habilitar al mismo tiempo.

Figura 3-6 Configuración del puerto



Paso 3 Hacer clic**Ahorrar**.

Tabla 3-3 Descripción de los parámetros PoE

Parámetro	Descripción
Nivel	Muestra el nivel de alimentación de los dispositivos terminales. El nivel de alimentación varía de 0 a 8, y el nivel estándar de alimentación Hi-PoE se muestra como 5+.
Consumo de energía (W)	Muestra la energía PoE actual consumida por el puerto individual correspondiente.
Habilitar PoE	Muestra si PoE está habilitado para el puerto.
PoE de larga distancia	
Vigilancia de PoE	
Fuerza PoE	

4 Seguridad

4.1 Configuración del aislamiento del puerto

El aislamiento de puertos permite lograr el aislamiento de capa 2 entre mensajes. Esta función proporciona a los usuarios una solución de red más segura y flexible.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Aislamiento del puerto**.

Paso 2 Habilitar separación de puertos.

Una vez habilitado el aislamiento de puertos, los puertos de enlace descendente se aislarán, pero los de enlace ascendente no. (Los datos solo se pueden transferir entre los puertos de enlace ascendente y descendente).

Paso 3 Hacer clic**Ahorrar**.

4.2 Configuración del control de tormentas

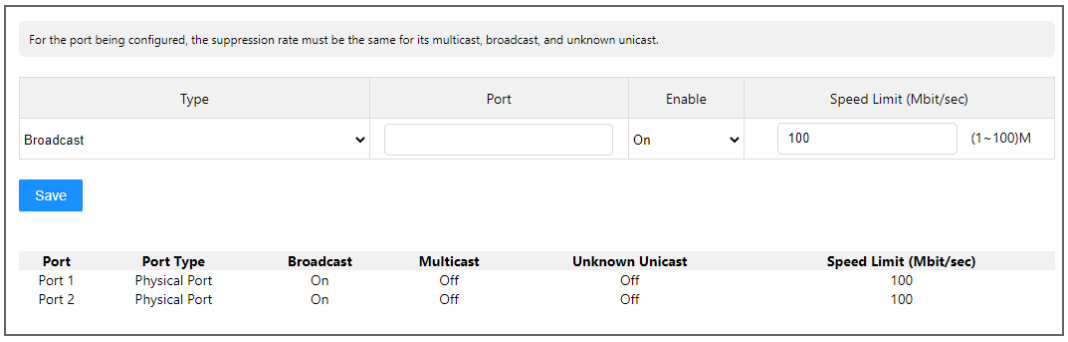
Las tramas de difusión en la red se reenvían continuamente, lo que afecta la correcta comunicación y reduce considerablemente el rendimiento de la red. El control de tormentas puede limitar los flujos de difusión del puerto y descartar las tramas de difusión cuando el flujo supera el umbral especificado, lo que reduce el riesgo de tormentas de difusión y garantiza el correcto funcionamiento de la red.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Control de tormentas**.

Paso 2 Seleccione el tipo y el puerto, habilite el control de tormentas y luego ingrese la velocidad.

Figura 4-1 Control de tormentas



Paso 3 Hacer clic**Ahorrar**.

4.3 Configuración del límite de velocidad del puerto

Configure la política de limitación de velocidad de los puertos para controlar el flujo de paquetes de datos que entran y salen del puerto a una velocidad deseada.

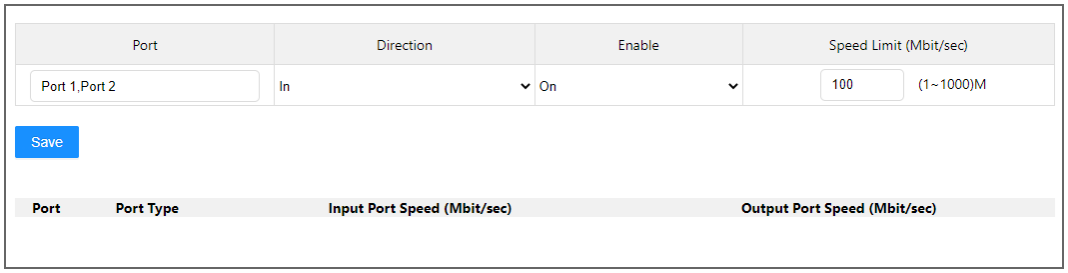
Procedimiento

Paso 1 Seleccionar**Seguridad**>**Límite de velocidad del puerto**.

Paso 2 Seleccione el puerto y la dirección, habilite el límite de velocidad del puerto y luego ingrese la velocidad.

La dirección incluye entrada y salida.

Figura 4-2 Límite de velocidad del puerto



Paso 3 Hacer clic**Ahorrar**.

5 Configuraciones de red

5.1 Configurar tablas MAC

La tabla MAC (Control de Acceso al Medio) registra la relación entre la dirección MAC y el puerto, incluyendo la VLAN a la que pertenece dicho puerto. Al reenviar un paquete, el dispositivo consulta la dirección MAC de destino en la tabla de direcciones MAC. Si la dirección MAC de destino figura en la tabla, el paquete se reenvía directamente a través del puerto de la tabla. Si no figura en la tabla, el dispositivo utiliza la difusión para reenviarlo a todos los puertos de la VLAN, excepto al puerto receptor.

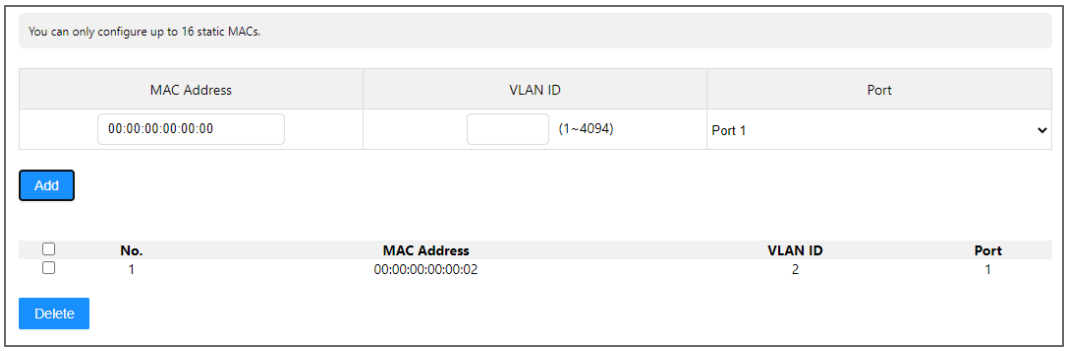
Procedimiento

Paso 1 Seleccionar**Configuración de red**>**Gestión de MAC**>**MAC estática**, ver la información de la tabla MAC.

Paso 2 Configure la dirección MAC, el ID de VLAN y el puerto y luego haga clic en**Agregar**.

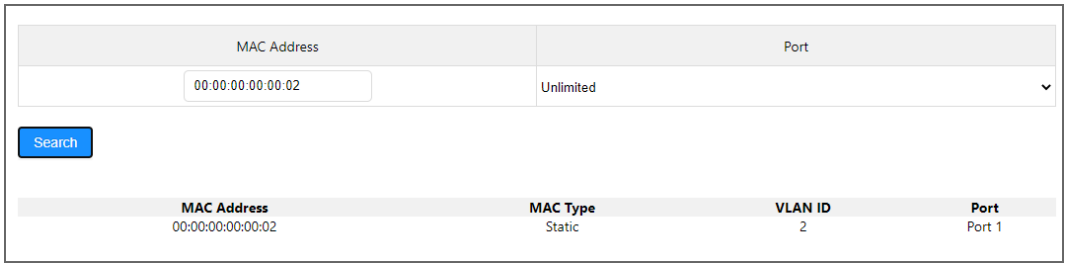
- Sólo puedes configurar hasta 16 MAC estáticas.
- Seleccione una MAC y luego haga clic en**Borrar**, puedes eliminar la MAC estática.

Figura 5-1 MAC estática



Paso 3 Haga clic en el**Búsqueda MAC**pestaña, ingrese la dirección MAC o seleccione el puerto y luego haga clic en **Buscar**para buscar rápidamente la dirección MAC.

Figura 5-2 Búsqueda de MAC



Paso 4 Haga clic en el**Lista de MAC**pestaña y luego ver las direcciones MAC.

Se pueden mostrar hasta 100 artículos. Para buscar más información, vaya a**Búsqueda MAC**.

Hacer clic**Claro**,y luego haga clic**DE ACUERDO**para borrar la información.

5.2 Configuración de la protección de bucle

Seleccionar**Configuración de red**>**Protección de bucle**, habilite la protección de bucle y luego haga clic en**Ahorrar**. Una vez habilitada la protección de bucle, si se detecta un bucle, el puerto que lo causó se deshabilitará y luego se restaurará automáticamente después de eliminar el bucle.

5.3 Configuración de STP

El Protocolo de Árbol de Expansión (STP) crea una topología lógica sin bucles para redes LAN. Bloquea los enlaces redundantes entre dos dispositivos de red y deja un único enlace activo entre ellos para eliminar los 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 prevenir bucles en una red de capa 2. Sin embargo, converge la topología de la red lentamente.
- RSTP: Una mejora de STP que permite una rápida convergencia de la topología de red. Sin embargo, tanto RSTP como STP presentan el defecto de que todas las VLAN de la misma LAN comparten el mismo árbol de expansión.
- MSTP: Una tabla de mapeo de VLAN virtual donde los ID de VLAN se asocian con instancias de árbol de expansión. Además, MSTP divide una red de conmutación en múltiples regiones, cada una con múltiples instancias de árbol de expansión independientes entre sí. A diferencia de STP y RSTP, MSTP proporciona múltiples rutas redundantes para el reenvío de datos. Además, implementa el balanceo de carga entre VLAN.

El STP sólo está disponible en modelos selectos.

5.3.1 STP

Procedimiento

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

Paso 2 Habilitar el STP.

Paso 3 Seleccione el modo de trabajo, incluyendo STP y RSTP.

Paso 4 Configure los parámetros.

Figura 5-3 Configuración de STP

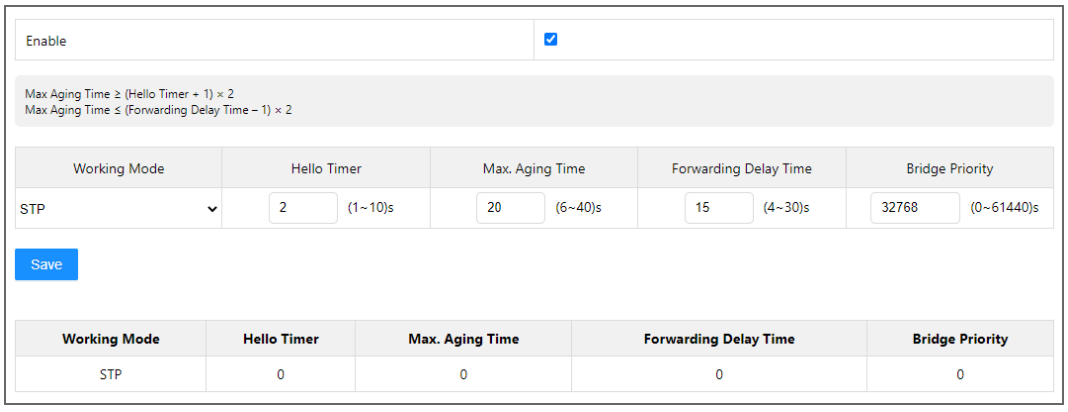


Tabla 5-1 Descripción de los parámetros STP

Parámetro	Descripción
Hola temporizador	El periodo de envío de BPDU por el puente raíz varía entre 1 y 10 segundos.
Tiempo máximo de envejecimiento	El tiempo de envejecimiento de la BPDU actual varía entre 6 y 40 segundos.
Retraso de reenvío Tiempo	Tras configurar el cambio topológico, el puente mantiene el tiempo de vigilancia y el estado de estudio. El tiempo varía entre 4 y 30 segundos.
Prioridad de puente	El valor varía de 0 a 61440.

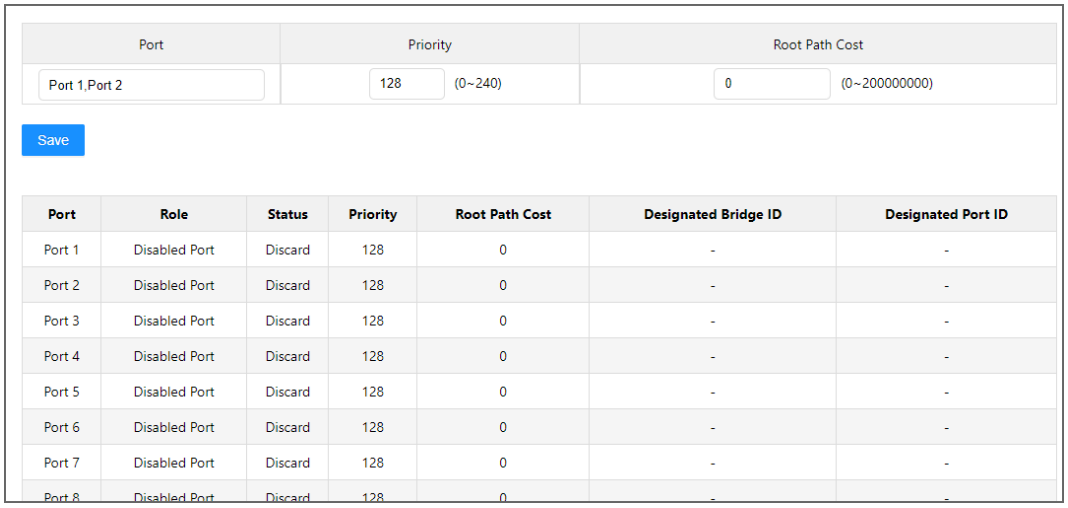
Paso 5 Hacer clic**Ahorrar**.

5.3.2 Instancia de puerto

Seleccionar**Configuración de red**>**STP**>**Instancia de puerto**, seleccione el puerto, ingrese la prioridad y el costo de la ruta raíz y luego haga clic en**Ahorrar**.

- 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 5-4 Instancia de puerto



5.4 Configuración de la agregación de enlaces

La agregación de enlaces consiste en integrar múltiples puertos físicos del switch en un puerto lógico. Los múltiples enlaces del mismo grupo se pueden considerar como un enlace lógico con mayor ancho de banda. Mediante la agregación, los puertos del mismo grupo pueden compartir el flujo de comunicación para lograr un mayor ancho de banda. Además, los puertos del mismo grupo pueden respaldarse recíprocamente y dinámicamente para mejorar la fiabilidad del enlace.

Información de fondo

Para establecer con éxito una agregación de enlaces, las configuraciones de agregación de enlaces en el dispositivo par deben ser las mismas que las configuraciones en este dispositivo.

La agregación de enlaces solo está disponible en modelos seleccionados.

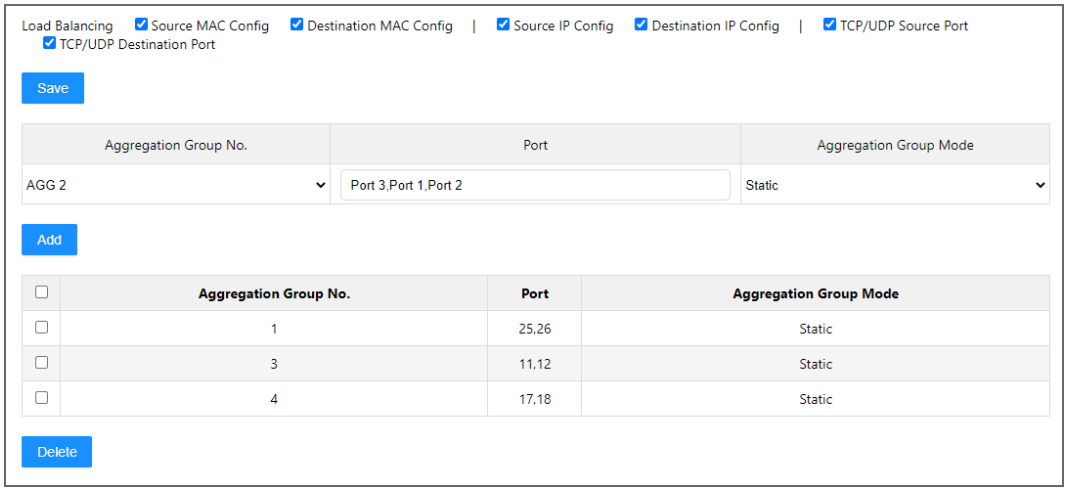
Procedimiento

Paso 1 Seleccionar**Configuración de red**>**Agregación de enlaces**.

Paso 2 En el**Equilibrio de carga**área, seleccione el tipo y luego haga clic**Ahorrar**.

El tipo incluye**Configuración MAC de origen**,**Configuración de MAC de destino**,**Configuración de IP de origen** , **Configuración de IP de destino**,**Puerto de origen TCP/UDP**y**Puerto de destino TCP/UDP**.

Figura 5-5 Agregación de enlaces



Paso 3 Seleccione el**Grupo de agregación No.**y número de puerto. El

modo de grupo de agregación es**Estático**por defecto.

Los puertos con control de tormentas o límite de velocidad de puerto habilitados no se pueden agregar a grupos de agregación.

Paso 4 Hacer clic**Agregar**.

Seleccione el grupo de agregación y luego haga clic en**Borrar**para eliminar el grupo de agregación.

6 Monitoreo inteligente

6.1 Visualización de estadísticas del puerto

Procedimiento

Paso 1 Seleccionar**Monitoreo inteligente**>**Estadísticas portuarias**.

Paso 2 Ver el tipo de puerto, el uso de recepción y el uso de envío.

Hacer clic**Reiniciar**para restablecer las estadísticas del puerto.

Figura 6-1 Estadísticas del puerto

Port	Port Type	RX Usage	TX Usage	RX/TX Bytes	Successful RX/TX Packet	Failed RX/TX Packet
Port 1	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 2	Physical Port	0.05%	0.05%	201.94MB/4.23MB	2938753/40057	0/0
Port 3	Physical Port	0%	0%	163.29KB/103.64KB	1325/450	0/0
Port 4	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 5	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
Port 6	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0

Reset

6.2 Visualización de la lista de dispositivos

LLDP (Protocolo de Descubrimiento de Capa de Enlace) es un método estándar de descubrimiento de capa de enlace. Puede configurar sus principales capacidades, dirección de administración, número de dispositivo y número de puerto como TLV (Valor de Longitud de Tipo), encapsularlos en LLDPDU (Unidad de Datos del Protocolo de Descubrimiento de Capa de Enlace) y compartirlos con su vecino. Este conservará la información recibida en forma de MIB (Base de Información de Administración) estándar, para que la administración de la red pueda consultar y evaluar el estado de la comunicación del enlace.

Procedimiento

Paso 1 Seleccionar**Monitoreo de red**>**Lista de dispositivos**

Paso 2 Habilite el LLDP y luego haga clic en**Ahorrar**. Ver la

Paso 3 información del dispositivo remoto LLDP.

Figura 6-2 Lista de dispositivos

If LLDP is turned off, cloud topology of the device will work abnormally.

LLDP

Save

Port	Peer Port Name	Device Name	MAC Address	IP
Port 2	[redacted]	[redacted]	[redacted]	
Port 2	[redacted]		[redacted]	
Port 2	[redacted]		[redacted]	

7 Mantenimiento

7.1 Configuración de la duplicación de puertos

La duplicación copia el tráfico recibido, enviado o ambos en un origen específico a un puerto de destino para su análisis. El origen especificado se denomina origen reflejado, 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 del switch a un dispositivo de monitorización para el análisis del servicio.

Procedimiento

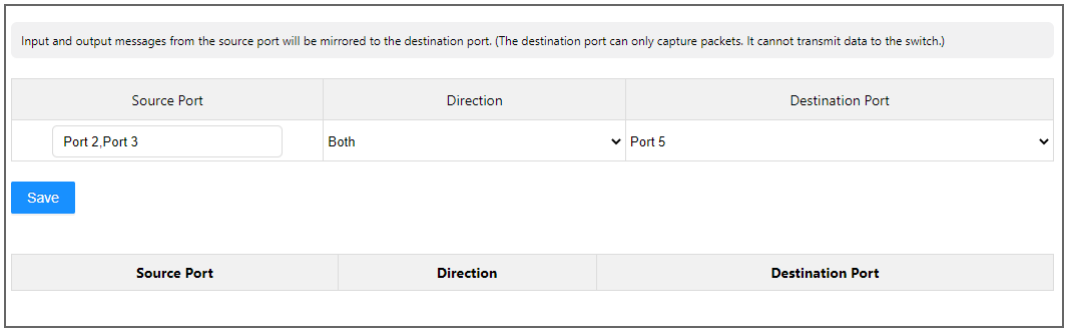
Paso 1 Seleccionar**Mantenimiento**>**Duplicación de puertos**.

Paso 2 Seleccione el puerto de origen, la dirección y el puerto de destino.

Las instrucciones incluyen Solo Tx, Solo Rx y Ambos.

- **Solo Tx**:Solo admite el envío de tráfico.
- **Solo con receta médica**:Sólo admite recepción de tráfico.
- **Ambos**:Admite tanto envío como recepción.

Figura 7-1 Duplicación de puertos



Paso 3 Hacer clic**Ahorrar**.

7.2 Configuración del firmware

7.2.1 Restaurar valores predeterminados de fábrica

Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Configuración del firmware**.

Paso 2 Hacer clic**Por defecto**,Ingrese la contraseña y luego haga clic**DE ACUERDO**.

- Todos los parámetros se restauran a la configuración predeterminada, excepto la dirección IP, la máscara de subred, la puerta de enlace y el DNS.
- Puedes restaurar todos los parámetros mediante el botón de reinicio.

7.2.2 Actualizar software

Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Configuración del firmware**.

Paso 2 Hacer clic**Navegar**para importar el archivo de actualización y luego haga clic en**Actualizar**. Haga clic**DE**

Paso 3 **ACUERDO**.

La actualización del software podría tardar 3 minutos. Tras la actualización, el sistema se reiniciará automáticamente.

7.2.3 Reiniciar el dispositivo

Seleccionar**Mantenimiento**>**Configuración del firmware**, haga clic**Reanudar**,y luego haga clic**DE ACUERDO**.

También puedes utilizar la esquina superior derecha para reiniciar el dispositivo.

7.3 Cambio de contraseña

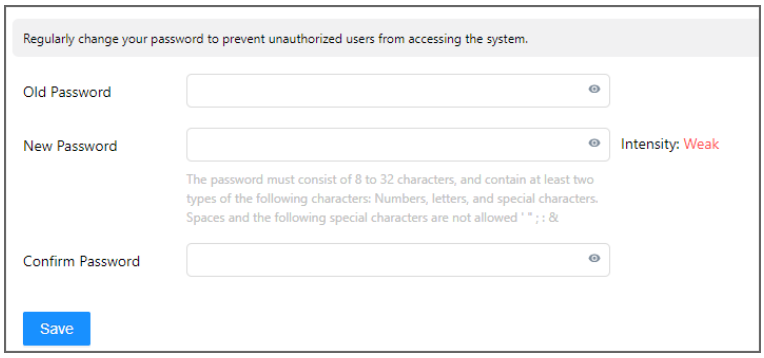
Procedimiento

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

Paso 2 Ingrese la contraseña anterior, la contraseña nueva y confirme la contraseña.

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

Figura 7-2 Cambiar contraseña



Paso 3 Hacer clic**Ahorrar**.

7.4 Configuración de la red

Configurar la dirección IP y el servidor DNS.

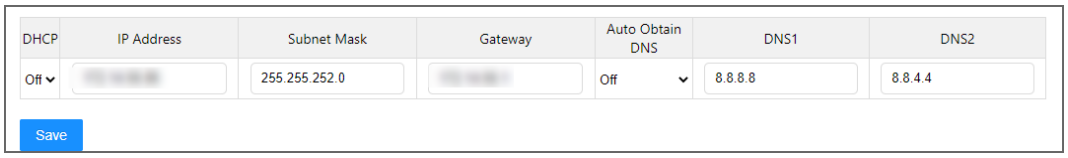
Procedimiento

Paso 1 Seleccionar**Mantenimiento**>**Red**.

Paso 2 Configure los parámetros.

- Habilitar DHCP: después de habilitar DHCP, se adquirirá y asignará automáticamente una nueva IP.
- Deshabilitar DHCP: ingrese la dirección IP, la máscara de subred y la puerta de enlace para configurar una dirección IP estática.
- Habilitar obtención automática de DNS: el dispositivo obtiene automáticamente la dirección IP del servidor DNS en la red.
- Deshabilitar la obtención automática de DNS: Ingrese las direcciones IP de DNS1 y DNS2.

Figura 7-3 Red



Paso 3 Hacer clic**Ahorrar**.

7.5 Visualización de la información del dispositivo

Seleccionar**Mantenimiento**>**Información del dispositivo**Puede ver información como el nombre del dispositivo, la versión del software, la dirección MAC y el tiempo de ejecución. También puede habilitar la gestión de la nube desde esta página.

7.6 Visualización de la información del registro

Seleccionar**Mantenimiento**>**Información de registro**, ver la información del registro.

7.7 Visualización de información legal

Seleccionar**Mantenimiento**>**Aviso legal**, haga clic en la pestaña correspondiente para ver el acuerdo de licencia de software, la política de privacidad y el aviso de software de código abierto.

Apéndice 1 Recomendación de seguridad

Gestión de cuentas

1.**Utilice contraseñas complejas**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos;
- No contenga 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 repetidos, como 111, aaa, etc.

2.**Cambie las contraseñas periódicamente**

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o descifrada.

3.**Asignar cuentas y permisos de forma adecuada**

Agregue usuarios de forma adecuada según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4.**Habilitar la función de bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada por defecto. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Tras varios intentos fallidos de contraseña, la cuenta y la dirección IP de origen correspondientes se bloquearán.

5.**Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna**

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por cibercriminales, si se produce algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no usar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

Se recomienda habilitar HTTPS para acceder a servicios web a través de canales seguros.

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

Si el contenido de sus datos de audio y video es muy importante o confidencial, se recomienda utilizar la función de transmisión encriptada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3.**Desactiva los servicios no esenciales y utiliza el modo seguro**

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, etc., para reducir las superficies de ataque.

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

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

4.**Cambiar HTTP y otros puertos de servicio predeterminados**

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de ser adivinado por actores de amenazas.

Configuración de red

1.**Habilitar lista de permitidos**

Se recomienda activar la lista de permitidos y permitir que solo las IP de dicha lista accedan al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la del dispositivo compatible a la lista de permitidos.

2.**Vinculación de direcciones MAC**

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

3.**Construir un entorno de red seguro**

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa;
- De acuerdo con las necesidades reales de la red, divida la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red para lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

Auditoría de seguridad

1.**Comprobar usuarios en línea**

Se recomienda revisar periódicamente a los usuarios en línea para identificar usuarios ilegales.

2.**Comprobar el registro del dispositivo**

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3.**Configurar el registro de red**

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

Seguridad del software

1.**Actualizar el firmware a tiempo**

Según las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión oportunamente para garantizar que cuenten con las funciones y la seguridad más recientes. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualizaciones en línea para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

2.**Actualizar el software del cliente a tiempo**

Se recomienda descargar y utilizar el software de cliente más reciente.

Protección física

Se recomienda que realice una protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados, y tener control de acceso.

y gestión de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serie).