Conmutador Ethernet (conmutador administrado en la nube)

Manual del usuario

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 inicializarlo 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 requeridos.

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

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. Consulta 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 la empresa desde la aplicación Partner, debe seleccionar un rol, administrador o empleado para iniciar sesión por primera vez. Si el rol seleccionado es un empleado, primero debe comunicarse con el 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.

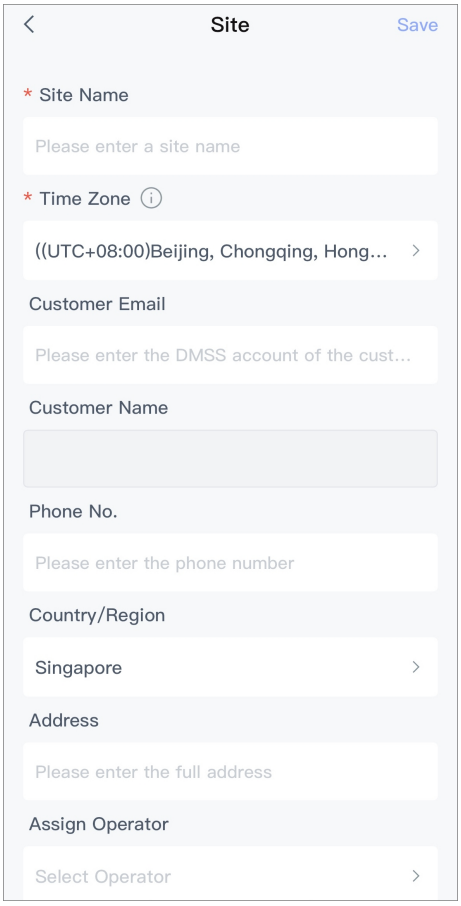
Paso 5 Grifo**Sitios**y luego toque  para agregar un sitio.

- **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 DoLynk Care. Para obtener más información, consulte*Manual del usuario de DoLynk Care*.

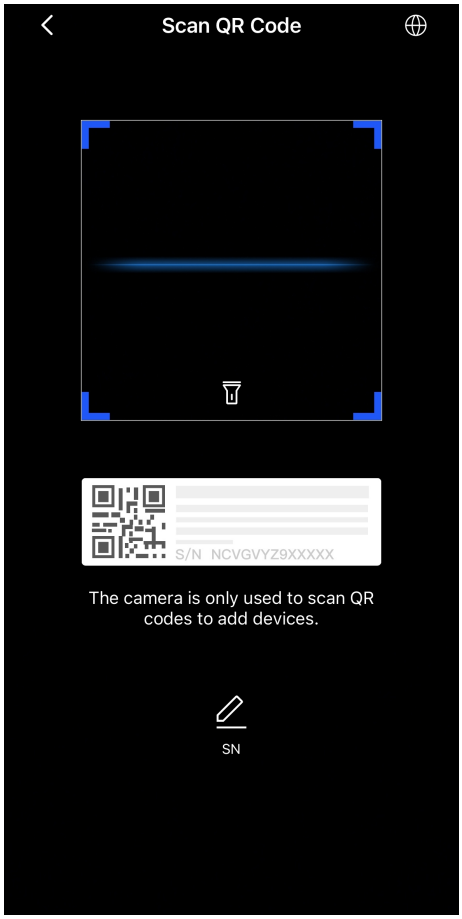
Figura 1-2 Agregar un sitio



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



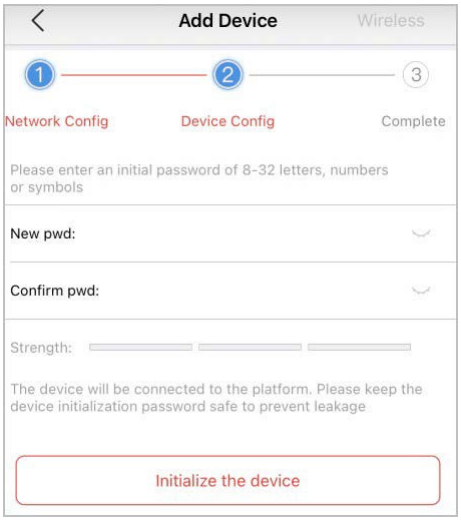
2. Escanee el código QR del dispositivo o toque para ingresar manualmente el número de serie del dispositivo.

   Al agregar un dispositivo a través del número de serie, debe ingresar el número de serie y la contraseña. La contraseña predeterminada antes de la inicialización del 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 usuario Manual, preguntas frecuentes y más.

1.2 Gestionado 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 de una invitación de GSP.

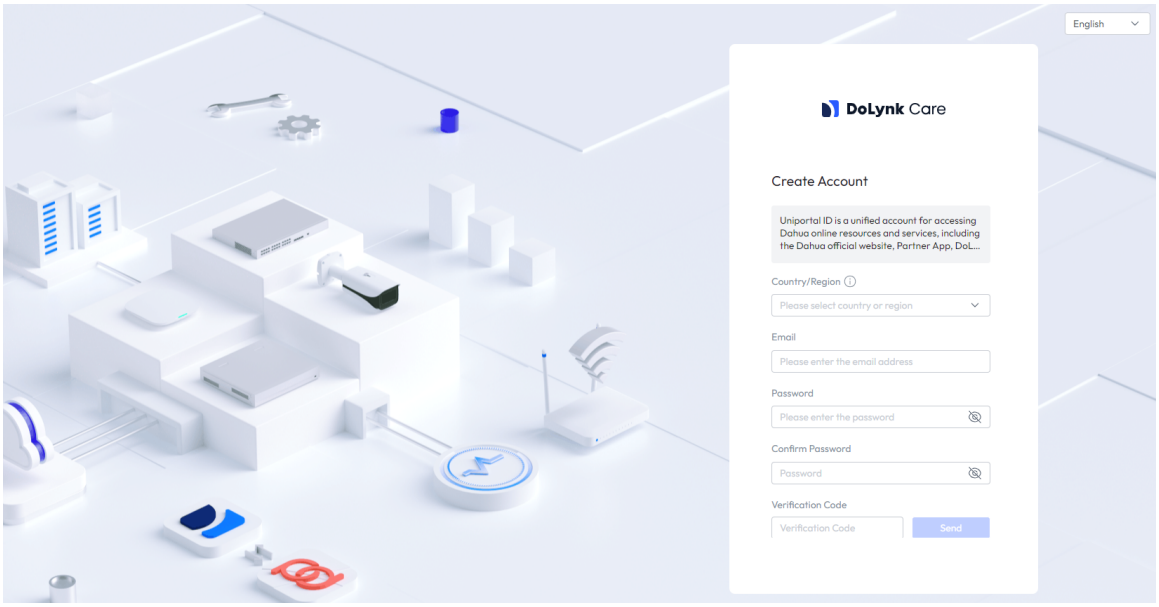
[a] Registro de cuenta personal

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

1. Ingrese la dirección de la plataforma en el navegador y luego 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, luego lea y seleccione**He leído y acepto la Política de privacidad y los Términos y condiciones**.Hacer clic **Inscribirse**.

Algunos países o regiones admiten el registro de una cuenta con el número de teléfono para obtener el código de verificación. Consulta la interfaz real para obtener más detalles.

Figura 1-5 Registro de cuenta personal



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

Paso 2 Abra el navegador, ingrese la dirección web y luego presione la tecla Enter. Ingrese el correo electrónico y la contraseña y luego haga clic en**Acceso**.

a Algunos países o regiones admiten el uso del número de teléfono para iniciar sesión. Consulta la interfaz real para obtener más detalles.

a 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.

a Si inicia sesión con la cuenta de la empresa desde la aplicación Partner, debe seleccionar un rol, administrador o empleado para iniciar sesión por primera vez. Si el rol seleccionado es un empleado, primero debe comunicarse con el administrador para crear una cuenta de empleado.

Paso 3 Añadir 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 un sitio existente de la lista o crear uno nuevo.

a Al agregar un dispositivo a través del número de serie, debe ingresar el número de serie y la contraseña. La contraseña predeterminada antes de la inicialización del dispositivo es el código SC, que se puede obtener de la etiqueta del dispositivo.

a No es posible agregar el dispositivo que se ha vinculado a un cliente.

a 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 la funcionalidad de 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 el dispositivo estén en el mismo segmento.
- De forma predeterminada, el DHCP está habilitado en el dispositivo. Cuando se conecta a una red, el dispositivo normalmente obtiene una dirección IP de un servidor DHCP y, a continuación, puede obtener la dirección IP del dispositivo desde el dispositivo ascendente, como un enrutador. Si no hay un servidor DHCP disponible, la dirección IP del dispositivo es 192.168.1.110 de forma predeterminada.

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

Procedimiento

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

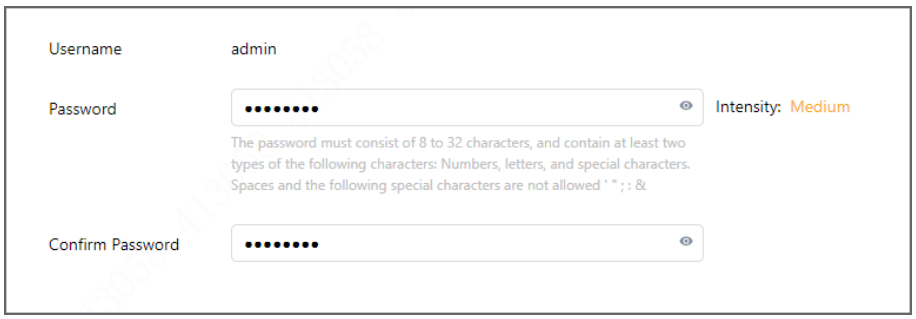
Paso 2 Seleccione el idioma y luego haga clic**Próximo**.

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 las indicaciones sobre la seguridad de la contraseña. La contraseña debe tener entre 8 y 32 caracteres y contener al menos dos tipos de 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 el dispositivo estén en el mismo segmento de red.

Procedimiento

Paso 1 Ingrese 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**.

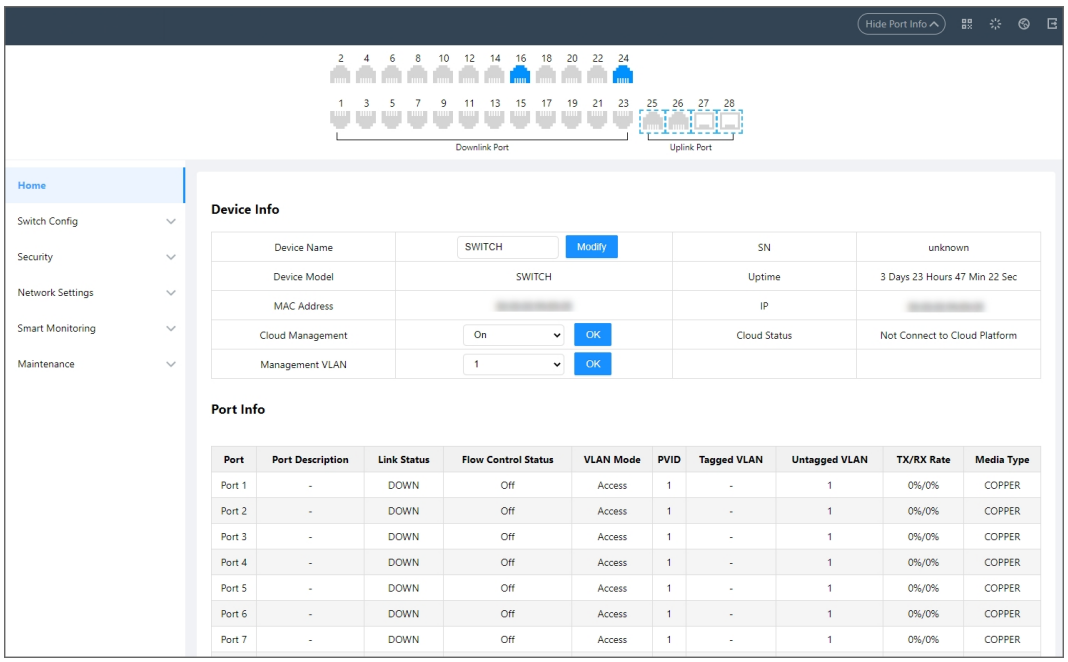
2.3 Página de inicio

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, hay una pantalla gráfica del estado del puerto. En la esquina superior derecha, se puede ocultar o mostrar la información del puerto, cerrar sesión, reiniciar el dispositivo, cambiar los idiomas del sistema y escanear códigos QR para acceder a la información.

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

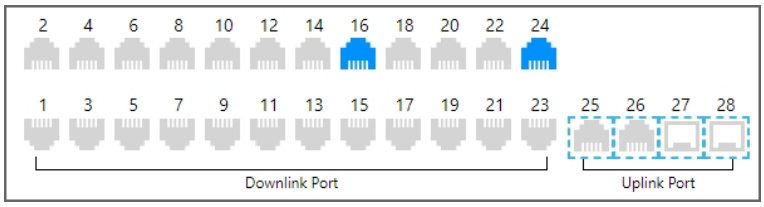
Figura 2-2 Página de inicio



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 de forma predeterminada. Si deshabilita esta función, el dispositivo no se podrá gestionar a través de la aplicación DoLynk Care. Para obtener más información sobre cómo utilizar 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**Cambiar configuración**>**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 falla la conexión.	
Estado del control de flujo	Ver el estado de la función de control de flujo, incluyendo**En**y**Apagado**Puedes ir a **Cambiar configuración**>**Puerto**Para configurar.	
Modo VLAN	Incluye**Acceso**y**Trompa**.	
PVID	La VLAN del puerto.	Ir a**Cambiar configuración**> **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.	
Tasa 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, incluidos la velocidad/dúplex, el control de flujo y otros parámetros. Los parámetros del puerto afectarán directamente el modo de funcionamiento del puerto. Realice las configuraciones de acuerdo con los requisitos prácticos.

Procedimiento

Paso 1 Seleccionar**Cambiar configuración**>**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 superar los 16 caracteres. Solo números, letras y el carácter especial (_).

Figura 3-2 Configuración del puerto (2)

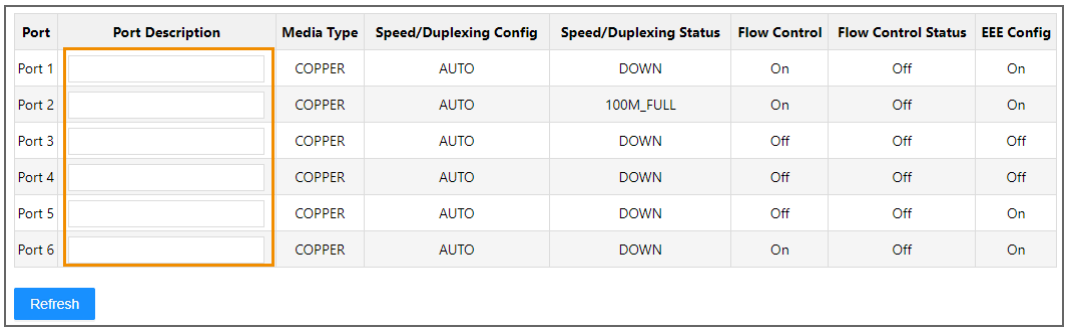


Tabla 3-1 Descripción de los parámetros del puerto

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	a En línea: muestra la velocidad del puerto y el modo dúplex. a 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

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

Información de contexto

Lógicamente, una LAN (red de área local) se puede dividir en muchos subconjuntos. Cada subconjunto tiene su propia área de difusión: LAN virtual (VLAN). Una VLAN se divide de una LAN sobre una base lógica en lugar de sobre una base 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.

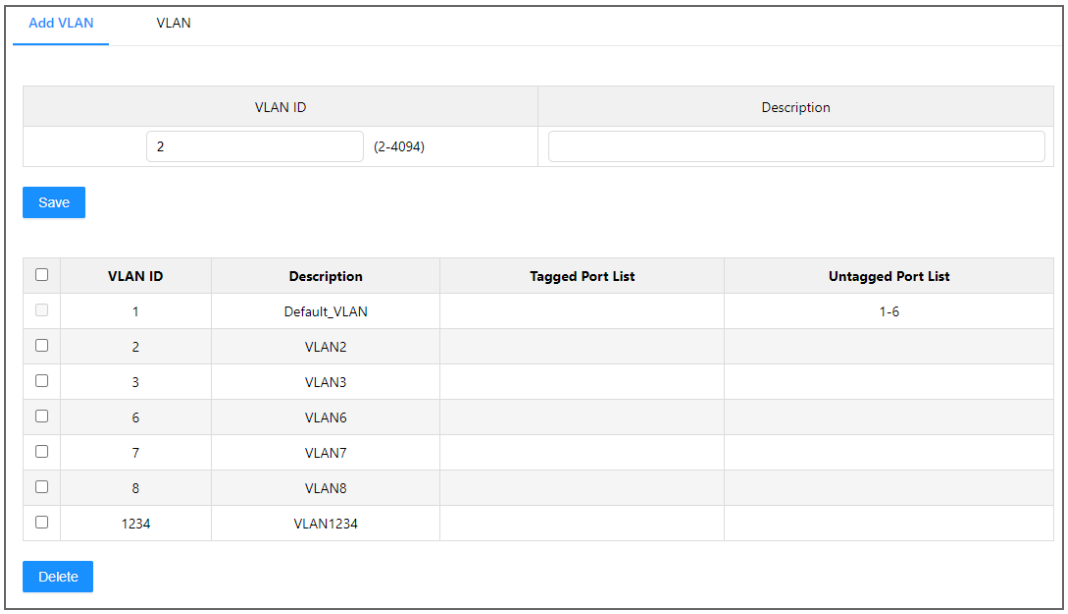
Procedimiento

Paso 1 Seleccionar**Cambiar configuración**>**VLAN**>**Agregar VLAN**.

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

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

Figura 3-3 Agregar VLAN

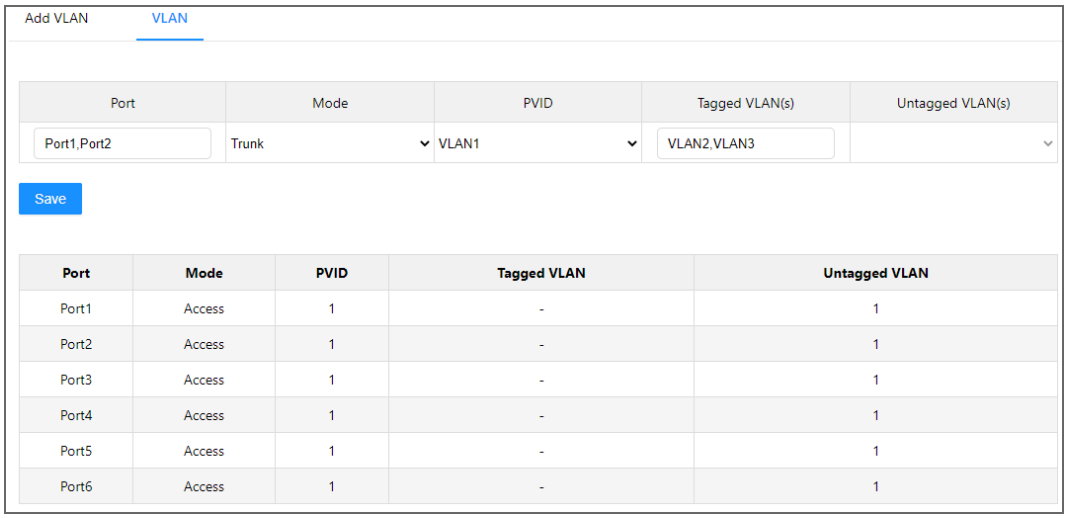


Paso 3 Haga clic en el**VLAN**Pestaña para configurar los parámetros VLAN del puerto.

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. La VLAN sin etiquetar indica el ID de VLAN para el 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 se agregó a una VLAN. De manera predeterminada, el puerto pertenece a la VLAN 1. El ID de VLAN para el 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 cuadros
Acceso	Recibe un mensaje 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.	Después de eliminar la etiqueta PVID, se transmite el marco.

Tipo de puerto	Marco sin etiquetar tratamiento	Marco etiquetado tratamiento	Transmisión de cuadros
Trompa	a Agrega una etiqueta con la ID de VLAN predeterminada a un marco sin etiqueta y acepta la marco si el permisos de interfaz la VLAN predeterminada IDENTIFICACIÓN. a Agrega una etiqueta con la ID de VLAN predeterminada a un marco sin etiqueta y descarta el marco si el La interfaz niega la VLAN predeterminada IDENTIFICACIÓN.	a Acepta un marco etiquetado si la interfaz permite la ID de VLAN incluida en el marco. a Descarta un marco etiquetado si la ID de VLAN transportada en el marco es denegada por el interfaz.	a Si el ID de VLAN del marco coincide con el valor predeterminado El ID de VLAN y el ID de VLAN está permitido por la interfaz, el dispositivo elimina la etiqueta y transmite el marco. a 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 el PD (dispositivo alimentado) para el suministro de energía remoto a través de puertos eléctricos Ethernet. La función PoE permite el suministro de energía centralizado y una copia de seguridad conveniente. Los terminales de red no necesitan una fuente de alimentación externa, sino 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**Cambiar configuración**>**PoE**>**Configuración global**.

Paso 2 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.

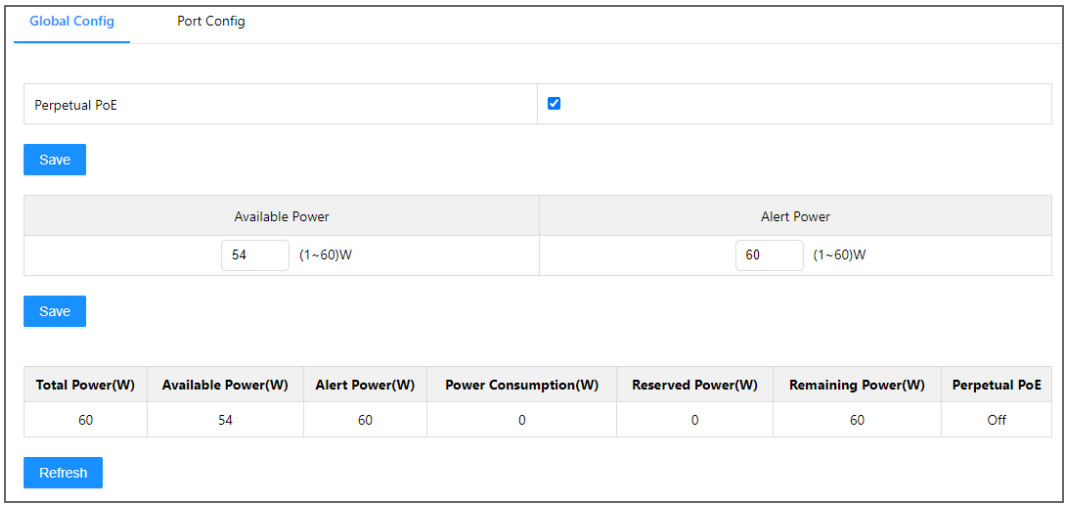
La potencia total, la potencia disponible, la potencia de alerta, el consumo de energía, la potencia reservada, la potencia restante y el PoE perpetuo se muestran en la parte inferior de la página. La potencia reservada = Potencia total – Potencia de alerta.

a La potencia de alerta debe ser mayor que la potencia disponible.

a La potencia disponible se refiere a la potencia máxima que se puede suministrar a los dispositivos alimentados. Cuando el consumo de energía es menor que la potencia disponible, se permite encender nuevos dispositivos alimentados.

- Durante el funcionamiento, el consumo de energía real puede fluctuar. Cuando el consumo de energía excede la energía de alerta, los puertos se alimentarán de bajo a alto según la prioridad (cuanto mayor sea el número de puerto, menor será la prioridad), hasta que el consumo de energía sea menor que la energía de alerta.

Figura 3-5 Configuración global



Paso 4 Hacer clic**Ahorrar**.

3.3.2 Configuración del puerto

Configure la función PoE del puerto.

Procedimiento

Paso 1 Seleccionar**Cambiar configuración**>**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 externamente PD 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 control PoE habilitado, puede monitorear el dispositivo de almacenamiento en línea y mantenerlo en línea, y verificar el estado de los dispositivos de almacenamiento en línea según los intervalos de tiempo. Si no hay transmisión de datos, el puerto PoE se apagará y reiniciará automáticamente.

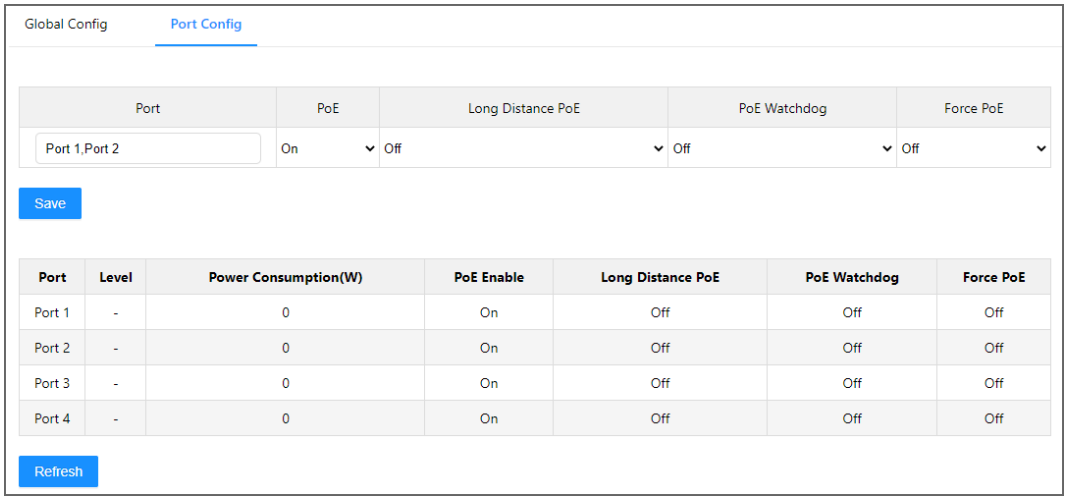
  Los intervalos de tiempo para las comprobaciones del estado de los dispositivos PD aumentan progresivamente, comenzando desde 1 minuto y duplicándose cada vez (1, 2, 4, 8, 16 y más). El intervalo de tiempo máximo es de 1024 minutos.

- **Fuerza PoE**:Cuando el dispositivo alimentado conectado al puerto es un dispositivo no estándar, utilice esta función para forzar el suministro de energía PoE.

Una vez que se habilite la alimentación PoE forzada, el puerto forzará el suministro de energía al dispositivo alimentado, independientemente de que el dispositivo conectado al puerto cumpla o no con 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 suministro de energía de los dispositivos terminales. El nivel de suministro de energía varía de 0 a 8, y el nivel estándar de suministro de energía 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 tiene como objetivo lograr un aislamiento de capa 2 entre mensajes. La función de aislamiento de puertos ofrece a los usuarios una solución de red más segura y flexible.

Procedimiento

Paso 1 Seleccionar**Seguridad**>**Aislamiento de puerto**

Paso 2 Habilitar separación de puertos.

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

Paso 3 Hacer clic**Ahorrar**.

4.2 Configuración del control de tormentas

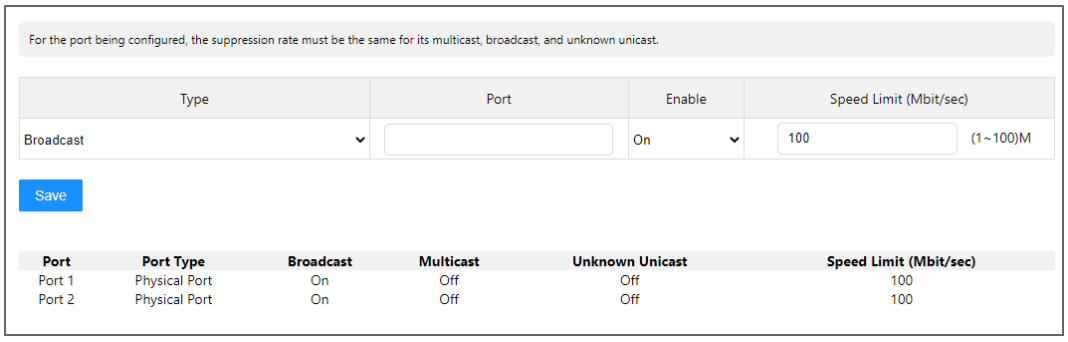
Las tramas de difusión en la red se reenvían continuamente, lo que afecta las comunicaciones adecuadas y reduce en gran medida el rendimiento de la red. El control de tormentas puede limitar los flujos de difusión del puerto y descartar las tramas de difusión una vez que el flujo supera el umbral especificado,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

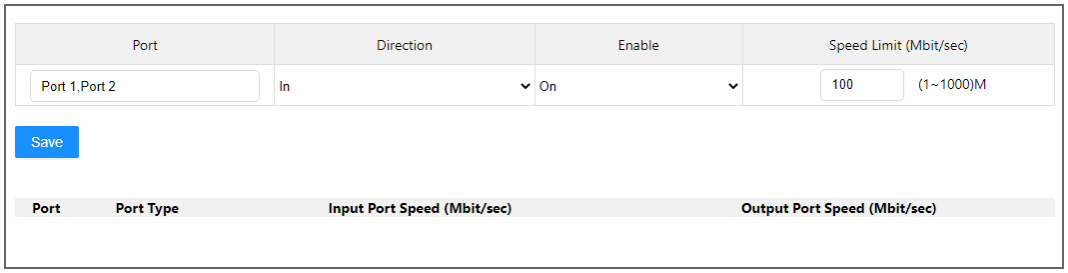
Procedimiento

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 (Media Access Control) registra la relación entre la dirección MAC y el puerto, y la información que incluye 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.

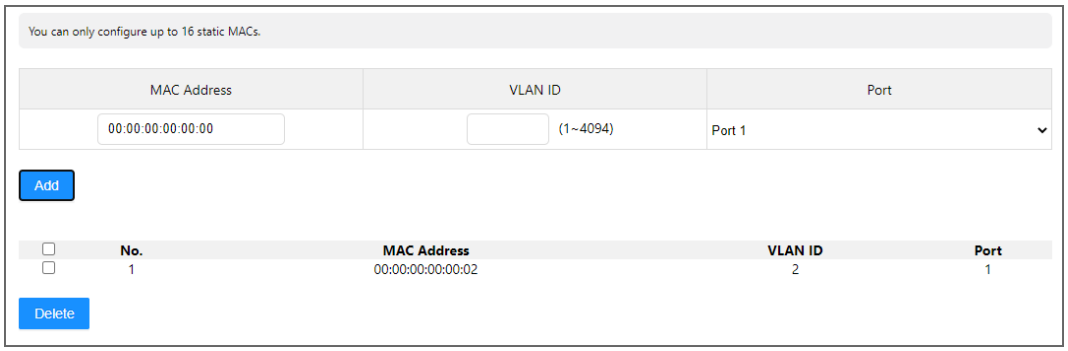
Procedimiento

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

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

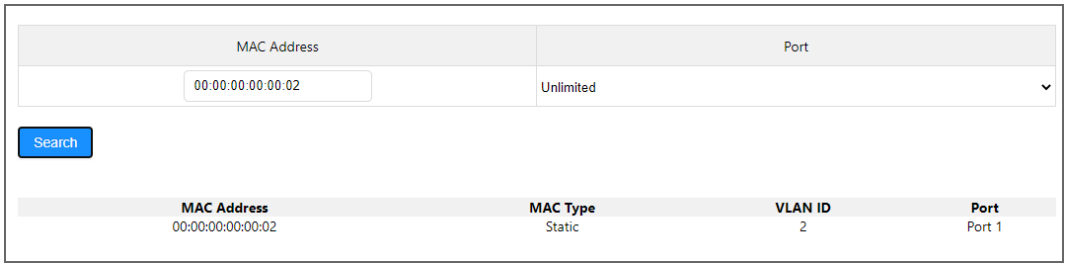
- Solo puedes configurar hasta 16 MAC estáticas.
- Seleccione una MAC y luego haga clic en**Borrar**, puedes eliminar la MAC estática.

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 elementos. Para buscar más información, acceda 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 Spanning Tree Protocol (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: Protocolo de gestión en la capa de enlace de datos que se utiliza para detectar y prevenir 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 red. Sin embargo, tanto RSTP como STP tienen un defecto: todas las VLAN de la misma LAN comparten el mismo árbol de expansión.
- MSTP: una tabla de mapeo de VLAN virtual en la que los identificadores 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 el equilibrio de carga entre las VLAN.

El STP solo está disponible en modelos seleccionados.

5.3.1 Procedimiento de prueba estándar

Procedimiento

Paso 1 Seleccionar**Configuración de red**>**PTP-S**>**PTP-S**

Paso 2 Habilitar el STP.

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

Paso 4 Configure los parámetros.

Figura 5-3 Configuración de STP

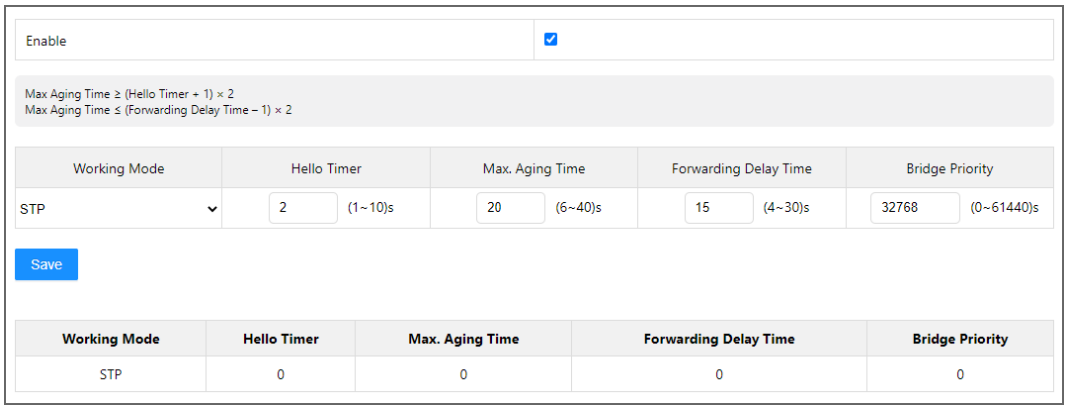


Tabla 5-1 Descripción de los parámetros del STP

Parámetro	Descripción
Hola temporizador	El período durante el cual el puente raíz envía BPDU. El tiempo varía entre 1 segundo 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	Después de configurar el cambio topológico, el puente mantiene el tiempo de espionaje y el estado de estudio. El tiempo varía de 4 segundos a 30 segundos.
Prioridad del puente	El valor varía de 0 a 61440.

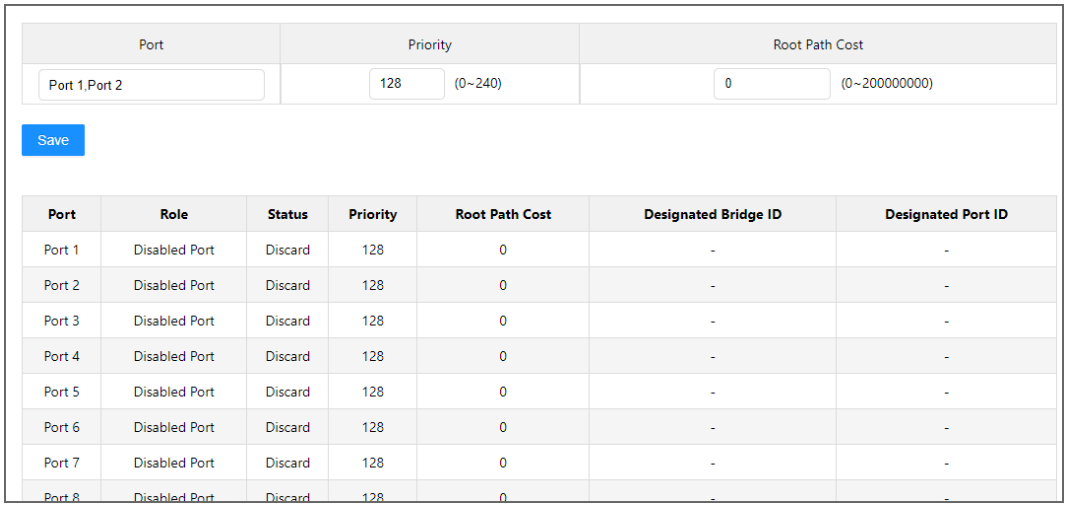
Paso 5 Hacer clic**Ahorrar**.

5.3.2 Instancia de puerto

Seleccionar**Configuración de red**>**PTP-S**>**Instancia de puerto**, seleccione el puerto, ingrese la prioridad y el costo de la ruta raíz y luego haga clic**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 formar múltiples puertos físicos del conmutador en un puerto lógico. Los múltiples enlaces del mismo grupo pueden considerarse como un enlace lógico con un mayor ancho de banda. A través de 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 de forma recíproca y dinámica para mejorar la confiabilidad del enlace.

Información de contexto

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.

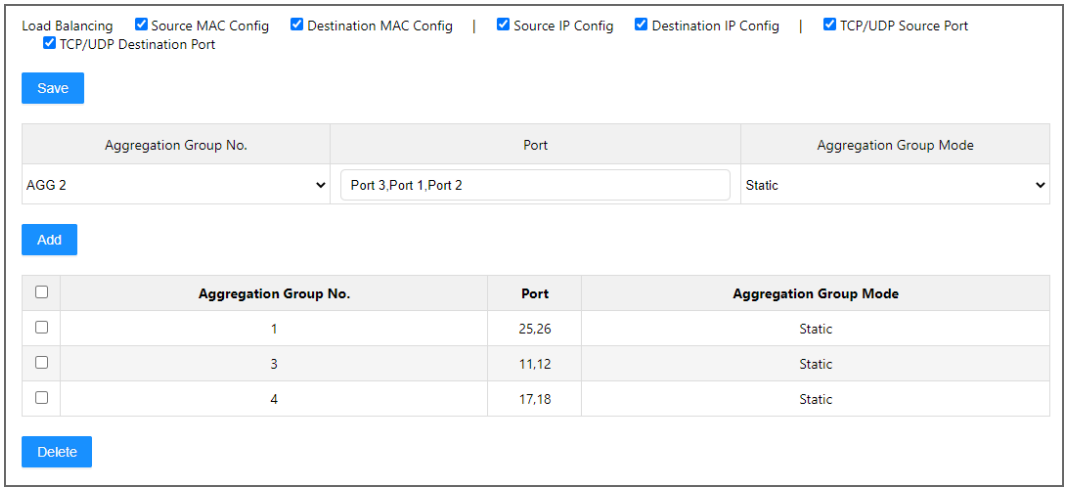
Procedimiento

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 n.º**y número de puerto. El

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

Los puertos con control de tormentas o límite de velocidad del 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

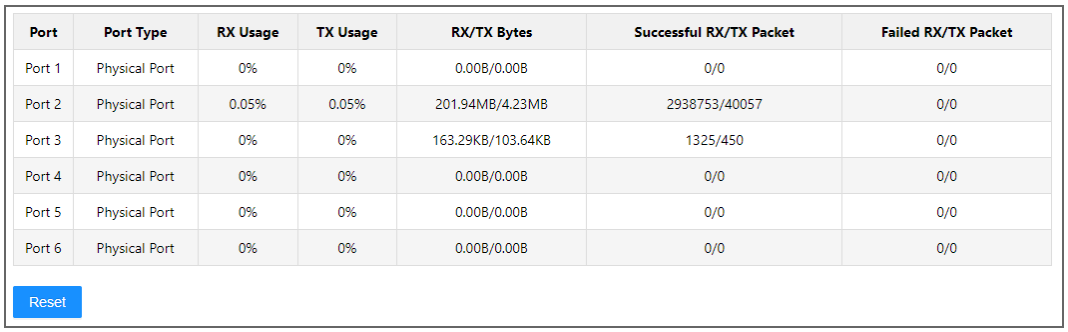
Procedimiento

Paso 1 Seleccionar**Monitoreo inteligente**>**Estadísticas del puerto**.

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 (Link Layer Discovery Protocol) es un método estándar de descubrimiento de la capa de enlace. Puede formar sus principales capacidades, dirección de administración, número de dispositivo y número de puerto como TLV (Type Length Value), encapsularlo en LLDPDU (Link Layer Discovery Protocol Data Unit) y liberarlo a su vecino. El vecino mantendrá la información recibida en forma de MIB (Management Information Base) estándar, de modo que la administración de la red pueda consultar y juzgar el estado de comunicación del enlace.

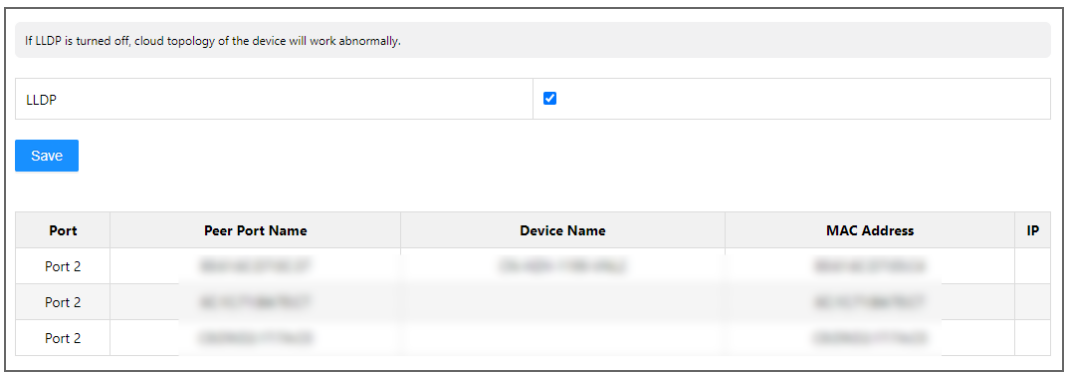
Procedimiento

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

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

Paso 3 información del dispositivo remoto LLDP.

Figura 6-2 Lista de dispositivos



7 Mantenimiento

7.1 Configuración de duplicación de puertos

La duplicación copia el tráfico recibido o enviado, o ambos, en una fuente específica a un puerto de destino para su análisis. La fuente específica se denomina fuente duplicada, el puerto de destino se denomina puerto de observación y el tráfico copiado se denomina tráfico duplicado. 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

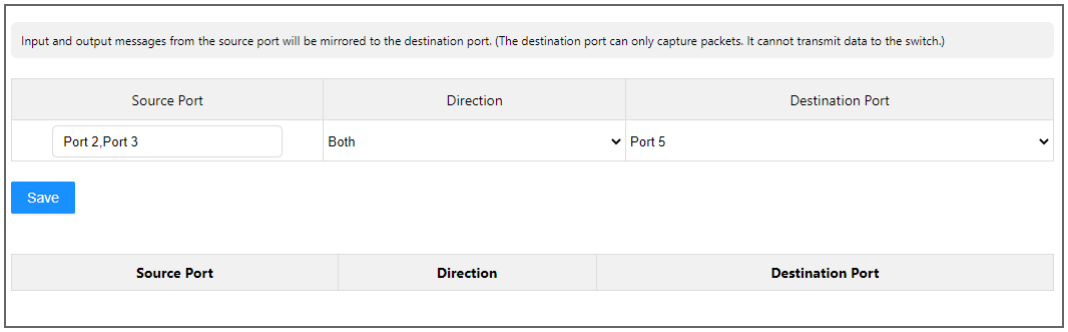
Paso 1 Seleccionar**Mantenimiento**>**Duplicación de puertos**.

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

Las instrucciones incluyen Solo tratamiento, Solo receta y Ambos.

- **Solo Tx**:Solo admite el envío de tráfico.
- **Solo con receta**:Solo 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 Actualización de 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 en**DE**

Paso 3 **ACUERDO**.

La actualización del software puede tardar 3 minutos. Después de 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

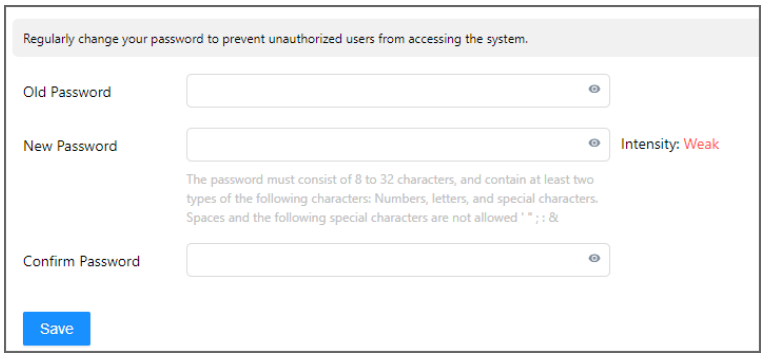
Procedimiento

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

Paso 2 Ingrese la contraseña anterior, la nueva contraseña 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

Configure la dirección IP y el servidor DNS.

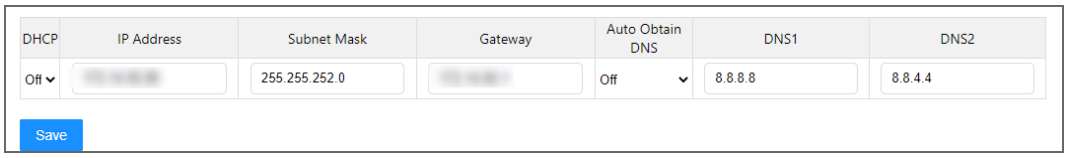
Procedimiento

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 la 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 administración de la nube a través de 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 Recomendaciones 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 de forma predeterminada. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Después de varios intentos fallidos de ingresar la contraseña, se bloquearán la cuenta correspondiente y la dirección IP de origen.

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 actores maliciosos, si hay algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

Configuración del servicio

1.**Habilitar HTTPS**

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

2.**Vinculación de dirección 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, particione 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 período 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 realizar el seguimiento.

Seguridad del software

1.**Actualizar el firmware a tiempo**

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. 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.**Actualice 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).