



Switch Ethernet (Switch gestionado en la nube)

Manual de usuario



Prefacio

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

Instrucciones de seguridad

Las siguientes palabras clave podrían aparecer en el manual.

Palabras de señalización	Significado
 DANGER	Indica un peligro potencial elevado que, de no evitarse, provocará la muerte o lesiones graves.
 WARNING	Indica un riesgo potencial medio o bajo que, de no evitarse, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, de no evitarse, podría ocasionar daños materiales, pérdida de datos, disminución del rendimiento o resultados impredecibles.
 ESD	Dispositivos sensibles a la electricidad estática. Indica un dispositivo sensible a las descargas electrostáticas.
 ELECTRIC SHOCK	Indica alto voltaje peligroso. Tenga cuidado de no entrar en contacto con la electricidad.
 LASER RADIATION	Indica riesgo de radiación láser. Tenga cuidado de evitar la exposición a un rayo láser.
 TIPS	Proporciona métodos para ayudarte 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
V1.0.0	Primer lanzamiento.	Agosto de 2024

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, usted podría recopilar datos personales de terceros, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para salvaguardar 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 sobre la existencia del área de vigilancia y facilitar la información de contacto requerida.

Acerca del manual

- El manual es solo para consulta. Pueden existir pequeñas diferencias entre el manual y el producto.
- No nos hacemos responsables de las pérdidas ocasionadas por el uso del producto de forma que no se ajuste al manual.
- El manual se actualizará de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones correspondientes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo de referencia. Pueden existir pequeñas diferencias entre la versión electrónica y la impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden generar algunas diferencias entre el producto real y el manual. Para obtener la versión más reciente del programa y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Es posible que existan errores de impresión o discrepancias en la descripción de las funciones, el funcionamiento y los datos técnicos. En caso de duda o controversia, nos reservamos el derecho a la interpretación final.
- Si no puede abrir el manual (en formato PDF), actualice el software de lectura o pruebe con otro software de lectura convencional.
- Todas las marcas comerciales, marcas registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si surge algún problema al utilizar el dispositivo.
- En caso de incertidumbre o controversia, nos reservamos el derecho a dar la explicación final.

Tabla de contenido

Prólogo.....	I 1
Gestión de la nube.....	1
1.1 Gestionado por la aplicación DoLynk Care.....	1
1.2 Gestionado por la plataforma DoLynk Care.....	5
2 Inicialización e inicio de sesión.....	8
2.1 Inicialización del dispositivo.....	8
2.2 Iniciar sesión en el dispositivo.....	8
2.3 Página de inicio.....	9
3 Configuración del conmutador.....	11
3.1 Configuración de la información del puerto.....	11
3.2 Configuración de VLAN.....	12
3.3 Gestión de PoE.....	14
3.3.1 Configuración global.....	14
3.3.2 Configuración de puertos.....	15
4 Seguridad.....	17
4.1 Configuración del aislamiento de puertos.....	17
4.2 Configuración del control de tormentas.....	17
4.3 Configuración del límite de velocidad del puerto.....	17
5 Configuración de red.....	19
5.1 Configurar las tablas MAC.....	19
5.2 Configuración de la protección contra bucles.....	20
5.3 Configuración de STP.....	20
5.3.1 STP.....	20
5.3.2 Instancia de puerto.....	21
5.4 Configuración de la agregación de enlaces.....	21
6 Monitoreo inteligente.....	23
6.1 Visualización de estadísticas del puerto.....	23
6.2 Visualización de la lista de dispositivos.....	23
7 Mantenimiento.....	24
7.1 Configuración de la duplicación de puertos.....	24
7.2 Configuración del firmware.....	24
7.2.1 Restaurar la configuración predeterminada de fábrica.....	24
7.2.2 Actualización de software.....	25
7.2.3 Reiniciar el dispositivo.....	25
7.3 Cambio de contraseña.....	25
7.4 Configuración de la red.....	25
7.5 Visualización de información del dispositivo.....	26

7.6 Visualización de la información del registro.....	26
7.7 Visualización de la información legal.....	26
Apéndice 1 Recomendación de seguridad.....	27

1. Gestión en la nube

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

1.1 Gestionado por la aplicación DoLynk Care

Procedimiento

Paso 1 Busca DoLynk Care en la App Store y descarga la aplicación.



Los usuarios de Android pueden descargar DoLynk Care desde Google Play.

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

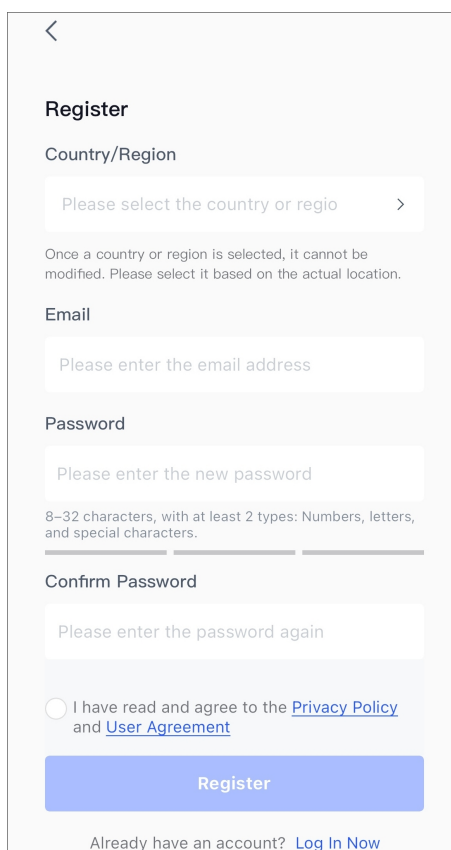
1. En el **Acceso** pantalla, toque **Crear una cuenta**.

2. En el **Registro** En la pantalla, complete la información en los campos obligatorios.



Algunos países o regiones permiten registrar una cuenta mediante el número de teléfono. Para más detalles, consulte la interfaz correspondiente.

Figura 1-1 Registro



<

Register

Country/Region

Please select the country or regio >

Once a country or region is selected, it cannot be modified. Please select it based on the actual location.

Email

Please enter the email address

Password

Please enter the new password

8-32 characters, with at least 2 types: Numbers, letters, and special characters.

Confirm Password

Please enter the password again

☐ I have read and agree to the [Privacy Policy](#) and [User Agreement](#)

Register

Already have an account? [Log In Now](#)

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

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



- Algunos países o regiones permiten iniciar sesión mediante el número de teléfono. Para más detalles, consulte la interfaz correspondiente.
- Puedes iniciar sesión con la cuenta que registraste en Partner App o DoLynk.
Panel de control. Toca para ver las instrucciones.
- Si inicia sesión con su cuenta personal desde la aplicación Partner y no seleccionó el país o la región al registrar la cuenta, deberá seleccionar un país la primera vez que inicie sesión.
- Si inicia sesión con la cuenta de la empresa desde la aplicación Partner, deberá seleccionar un rol (administrador o empleado) para acceder por primera vez. Si selecciona el rol de empleado, deberá contactar primero con el administrador para crear una cuenta de empleado.

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

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

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



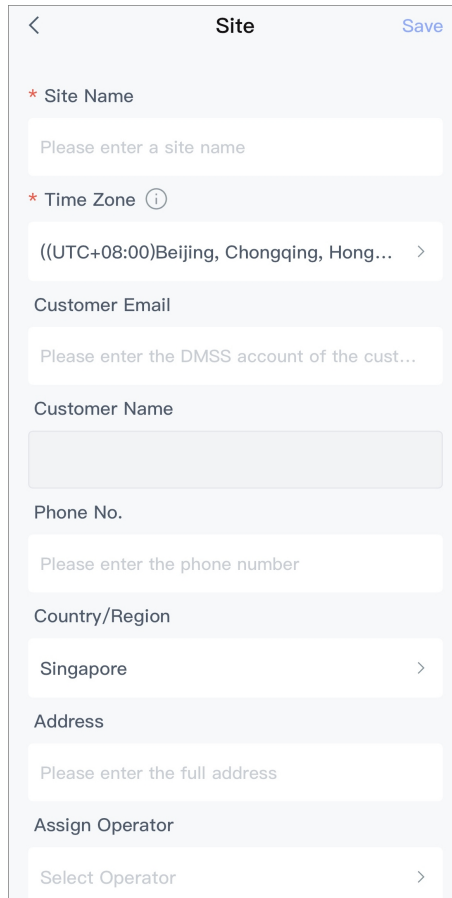
Ingrese la dirección de correo electrónico de la cuenta que su cliente registró en la aplicación DMSS. DoLynk Care la verificará.

- **País/Región:** El país o área se mantiene por defecto igual que el país o región de la cuenta.
- **Asignar operador** Seleccione un operador al que desee 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 detalles, consulte *Manual de usuario de DoLynk Care*.

Figura 1-2 Agregar un sitio



< Site Save

* Site Name

Please enter a site name

* Time Zone ⓘ

((UTC+08:00)Beijing, Chongqing, Hong... >

Customer Email

Please enter the DMSS account of the cust...

Customer Name

Phone No.

Please enter the phone number

Country/Region

Singapore >

Address

Please enter the full address

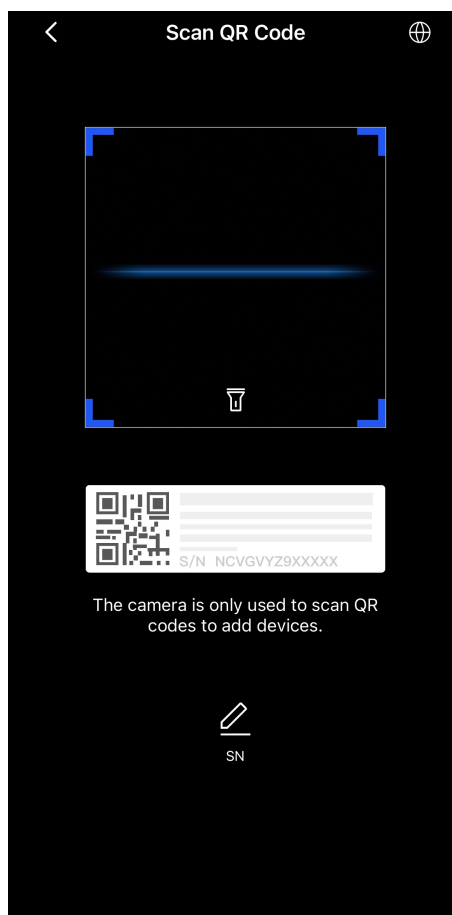
Assign Operator

Select Operator >

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,  **QR**.

Figura 1-3 Agregar un dispositivo

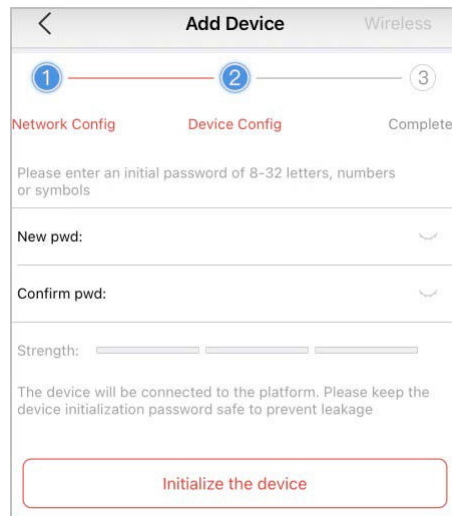


2. Escanee el código QR del dispositivo o toque para ingresar manualmente el número de serie del dispositivo.

Al agregar un dispositivo mediante el número de serie (SN), deberá ingresar el SN 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** En la 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 **DE ACUERDO**.

Figura 1-4 Inicializar el dispositivo



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

En la página de la consola, pulsa el perfil de la empresa para acceder a la página de gestión de la cuenta.

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

1.2 Gestionado por la plataforma DoLynk Care

Procedimiento

Paso 1 Crea una cuenta.

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

- Registro de cuenta personal

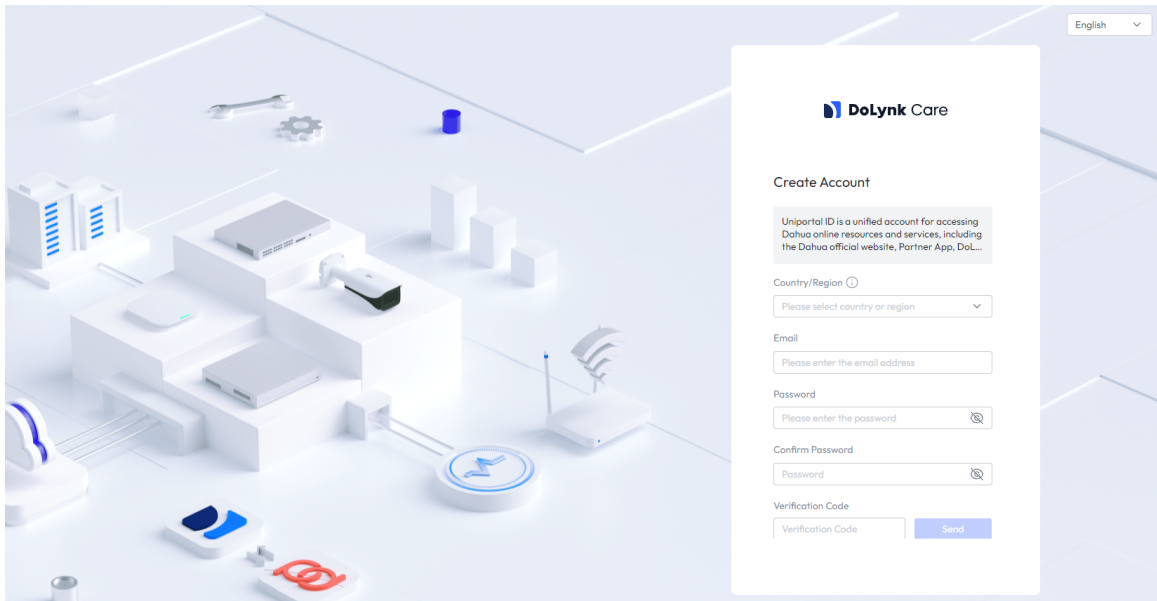
Puedes registrarte a través del portal de registro en la página de inicio de sesión de la plataforma. La cuenta registrada es personal. Si necesitas usar funciones como confiar dispositivos y comprar paquetes de servicios, deberás autenticar tu empresa después de iniciar sesión.

1. Introduce la dirección de la plataforma en el navegador y pulsa Intro. Selecciona 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. **Enviar** para obtener el código de verificación.
4. Introduzca el código de verificación que se envió al correo electrónico registrado y, a continuación, 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. Consulte la interfaz correspondiente para obtener más detalles.

Figura 1-5 Registro de cuenta personal



- Registro de invitación GSP: Para obtener más información, consulte el Manual del usuario de DoLink 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.**Acceso**.



- Algunos países o regiones permiten iniciar sesión mediante el número de teléfono. Para más detalles, consulte la interfaz correspondiente.
- Si inicia sesión con su cuenta personal desde la aplicación Partner y no seleccionó el país o la región al registrar la cuenta, deberá seleccionar un país la primera vez que inicie sesión.
- Si inicia sesión con la cuenta de la empresa desde la aplicación Partner, deberá seleccionar un rol (administrador o empleado) para acceder por primera vez. Si selecciona el rol de empleado, deberá contactar primero con el 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, a continuación, 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. Introduzca el nombre del dispositivo, el número de serie del dispositivo y la contraseña del dispositivo.

Debes seleccionar un sitio para el dispositivo. Puedes seleccionar un sitio existente de la lista o crear uno nuevo.



- Al agregar un dispositivo mediante el número de serie (SN), deberá ingresar el SN 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.
- No se puede agregar el dispositivo que ya está vinculado a un cliente.
- Si añades un interruptor, puedes cambiar la contraseña del dispositivo siguiendo las instrucciones que aparecen 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 gestionado ofrece acceso web. Puede iniciar sesión en la interfaz web para gestionar y configurar el dispositivo.

2.1 Inicialización del dispositivo

Requisitos previos

- Asegúrese de que el dispositivo esté conectado a la fuente de alimentación.
- Asegúrese de que el dispositivo esté conectado al ordenador y de que las direcciones IP del ordenador y del dispositivo estén en el mismo segmento.
- Por defecto, el DHCP está habilitado en el dispositivo. Al conectarse a una red, el dispositivo suele obtener una dirección IP de un servidor DHCP, y posteriormente se puede obtener la dirección IP del dispositivo de origen, como un enrutador. Si no hay un servidor DHCP disponible, la dirección IP del dispositivo es 192.168.1.110 por defecto.



Puedes usar la herramienta de configuración (Configtool) para obtener la dirección IP en determinados modelos de dispositivos.

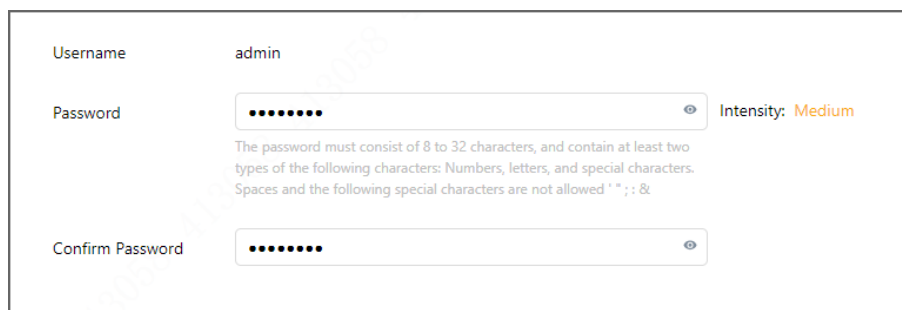
Procedimiento

- Paso 1** Introduzca la dirección IP del dispositivo en la barra de direcciones del navegador web y, a continuación, pulse la tecla Intro.
- 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** Configura la contraseña.



- El nombre de usuario predeterminado es admin.
- Configure una contraseña de alta seguridad según las indicaciones sobre la fortaleza de la contraseña. La contraseña debe tener entre 8 y 32 caracteres y contener al menos dos tipos entre números, letras y caracteres comunes (cualquier carácter visible que no sea ' ; : &).

Figura 2-1 Configurar contraseña



- Paso 5** Hacer clic **Completo**.

2.2 Iniciar sesión en el dispositivo

Requisitos previos

- El dispositivo ha sido inicializado.

- Asegúrese de que el dispositivo esté conectado al ordenador y de que las direcciones IP del ordenador y del dispositivo se encuentren en el mismo segmento de red.

Procedimiento

- Paso 1** Introduzca la dirección IP del dispositivo en la barra de direcciones del navegador web y, a continuación, pulse la tecla Intro.
- Paso 2** Introduce la contraseña.
- Paso 3** Hacer clic **Acceso**.

2.3 Página de inicio

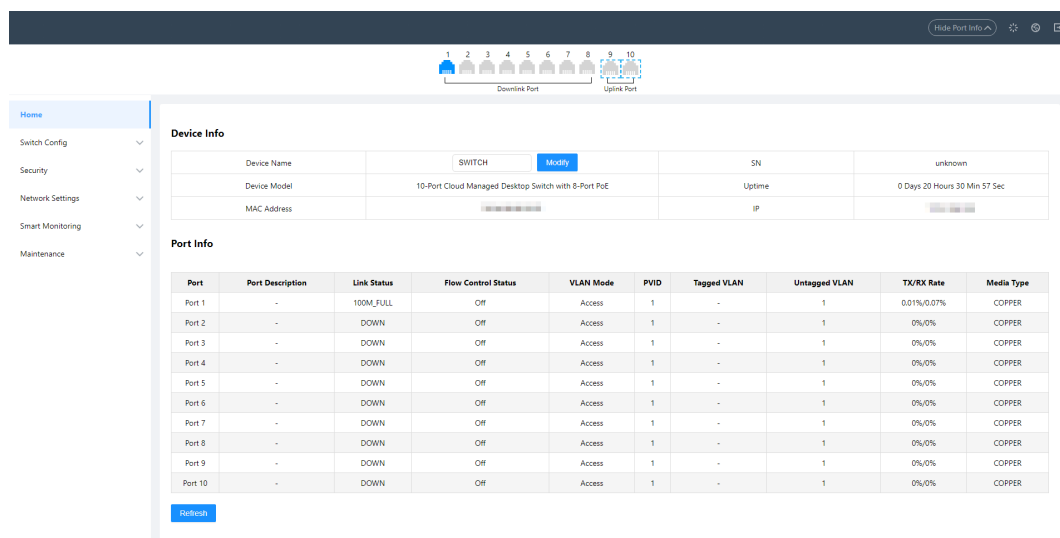
Después de iniciar sesión, el sistema será dirigido a la **Hogar** página.

La parte izquierda de la página consta de una barra de menú. En la parte superior, se muestra gráficamente el estado del puerto. En la esquina superior derecha, se puede 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.



Las páginas web son solo de referencia y pueden diferir de su dispositivo.

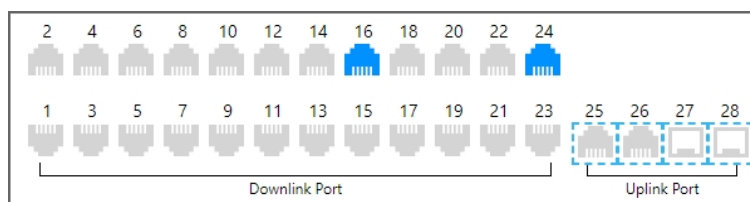
Figura 2-2 Página de inicio



Información del puerto

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

Figura 2-3 Información del puerto



Página principal

Hogar Esta página admite las siguientes funciones.

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



- ◇ Tras habilitar la VLAN de administración, solo podrá acceder a la página web del dispositivo a través de una dirección IP de la 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	Configure la descripción del puerto, también puede ir a Configuración del interruptor>Puerto para configurar.	
Estado del enlace	● Muestra la velocidad del puerto y el modo dúplex: El puerto está conectado. ● CAÍDO: El puerto no está conectado o la conexión falla.	
Estado del control de flujo	Vea el estado de la función de control de flujo, incluyendo EnyApagado Puedes ir a Configuración del interruptor>Puerto para configurar.	
Modo VLAN	Incluye AccesoyTrompa .	
PVID	La VLAN del puerto.	Ir a Configuración del interruptor>VLAN para configurar.
VLAN etiquetada	El ID de VLAN para el puerto que se permite etiquetar al enviar paquetes.	
VLAN sin etiquetar	El ID de VLAN para el puerto que puede enviarse sin etiquetar.	
Tasa TX/RX	La tasa de recepción o de envío actual dividida por la tasa real negociada durante un período de tiempo (normalmente 5 minutos).	
Tipo de medio	Incluye dos tipos: COBREyFIBRA . ● COBRE: Puerto RJ-45. ● FIBRA: Puerto de fibra óptica.	

3 Configuración del interruptor

3.1 Configuración de la información del puerto

Puede configurar los parámetros del puerto, incluyendo velocidad/dúplex, control de flujo y otros. Estos parámetros afectarán directamente al modo de funcionamiento del puerto. Realice las configuraciones según sus necesidades.

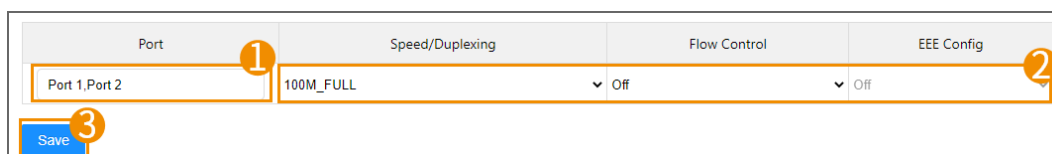
Procedimiento

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

Paso 2 Seleccione el número de puerto, configure los parámetros y luego haga clic **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 fiabilidad de los datos.
- **Configuración EEE:** Habilitar la función EEE (Ethernet de bajo consumo energético) puede reducir el consumo de energía cuando la red está inactiva y lograr un efecto de ahorro energético.

Figura 3-1 Configuración del puerto (1)



The screenshot shows a configuration form with four main sections: Port, Speed/Duplexing, Flow Control, and EEE Config. The Port field is set to 'Port 1, Port 2'. The Speed/Duplexing field is set to '100M_FULL'. The Flow Control field is set to 'Off'. The EEE Config field is set to 'Off'. A 'Save' button is located at the bottom left. Numbered callouts 1, 2, and 3 point to the Port field, the Speed/Duplexing field, and the Save button respectively.

Paso 3 En el **Descripción del puerto** En la casilla, introduzca la descripción del puerto.

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

Figura 3-2 Configuración del puerto (2)

Port	Port Description	Media Type	Speed/Duplexing Config	Speed/Duplexing Status	Flow Control	Flow Control Status	EEE Config
Port 1		COPPER	AUTO	DOWN	On	Off	On
Port 2		COPPER	AUTO	100M_FULL	On	Off	On
Port 3		COPPER	AUTO	DOWN	Off	Off	Off
Port 4		COPPER	AUTO	DOWN	Off	Off	Off
Port 5		COPPER	AUTO	DOWN	Off	Off	On
Port 6		COPPER	AUTO	DOWN	On	Off	On

Refresh

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 óptica.
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: Pantallas 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 EEE	Indica si la función EEE está habilitada.

3.2 Configuración de VLAN

Puedes añadir el puerto a la VLAN. La VLAN es VLAN1 por defecto.

Información general

Lógicamente, una LAN (Red de Área Local) se puede dividir en varios subconjuntos. Cada subconjunto tiene su propia área de difusión: una LAN virtual (VLAN). Una VLAN se separa de una LAN sobre una base lógica, no física, para lograr un área de difusión aislada dentro de la VLAN.

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

- **Acceso:** El puerto pertenece a una VLAN y se utiliza para conectarse al puerto del ordenador.
- **Trompa:** El puerto permite el paso de múltiples VLAN, la recepción y el envío de mensajes de múltiples VLAN, y se utiliza para conectar entre los conmutadores.

Procedimiento

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

Paso 2 Introduzca el ID y la descripción de la VLAN y, a continuación, haga clic en **Ahorrar**.



Seleccione la VLAN y luego haga clic **Borrar** Para eliminar la VLAN. La VLAN1 no se puede eliminar.

Figura 3-3 Agregar VLAN

Add VLAN
VLAN

VLAN ID	Description
2 (2-4094)	

Save

☐	VLAN ID	Description	Tagged Port List	Untagged Port List
☐	1	Default_VLAN		1-6
☐	2	VLAN2		
☐	3	VLAN3		
☐	6	VLAN6		
☐	7	VLAN7		
☐	8	VLAN8		
☐	1234	VLAN1234		

Delete

Paso 3 Haz clic en el **VLAN** pestaña para configurar los parámetros VLAN del puerto. 1.

Seleccione uno o más puertos.

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

Figura 3-4 VLAN

Add VLAN
VLAN

Port	Mode	PVID	Tagged VLAN(s)	Untagged VLAN(s)
Port1,Port2	Trunk	VLAN1	VLAN2,VLAN3	

Save

Port	Mode	PVID	Tagged VLAN	Untagged VLAN
Port1	Access	1	-	1
Port2	Access	1	-	1
Port3	Access	1	-	1
Port4	Access	1	-	1
Port5	Access	1	-	1
Port6	Access	1	-	1

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 enviarse sin etiquetar.
- Cuando el modo es Trunk, debe configurar el PVID y la VLAN etiquetada.

PVID indica que el puerto está agregado a una VLAN. Por defecto, el puerto pertenece a la VLAN 1. El ID de VLAN para el puerto que se permite etiquetar al enviar paquetes.

Tabla 3-2 Comparación del procesamiento de fotogramas

Tipo de puerto	Marco sin etiquetar tratamiento	Marco etiquetado tratamiento	Transmisión del bastidor
Acceso	Recibe un archivo sin etiquetar toma el marco y agrega una etiqueta con el ID de VLAN predeterminado al marco.	● Acepta la trama etiquetada si el ID de VLAN de la trama coincide con el ID de VLAN predeterminado. ● Descarta la trama etiquetada si el ID de VLAN de la trama difiere del ID de VLAN predeterminado.	Una vez eliminada la etiqueta PVID, se transmite la trama.

Tipo de puerto	Marco sin etiquetar tratamiento	Marco etiquetado tratamiento	Transmisión del bastidor
Trompa	● Agrega una etiqueta con el ID de VLAN predeterminado a una trama sin etiquetar. y acepta el marco si el La interfaz permite la VLAN predeterminada IDENTIFICACIÓN. ● Agrega una etiqueta con el ID de VLAN predeterminado a una trama sin etiquetar. y descarta el marco si el La interfaz niega la VLAN predeterminada IDENTIFICACIÓN.	● Acepta una trama etiquetada si la interfaz permite el ID de VLAN que contiene. ● Descarta una trama etiquetada si el ID de VLAN que contiene la trama es denegado por el interfaz.	● Si el ID de VLAN de la trama coincide con el predeterminado ID de VLAN y el ID de VLAN está permitido por la interfaz, el dispositivo Elimina la etiqueta y transmite la trama. ● Si el ID de VLAN de la trama difiere del ID de VLAN predeterminado, pero la interfaz aún permite dicho ID de VLAN, el dispositivo transmitirá la trama 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 dispositivo alimentado (PD) y suministrarle energía de forma remota a través de puertos Ethernet. La función PoE permite un suministro de energía centralizado y una copia de seguridad práctica. Los terminales de red no necesitan alimentación externa, solo un cable de red.



Los switches que no son PoE no son compatibles con esta función.

3.3.1 Configuración global

Puede configurar la alimentación PoE continua, la alimentación disponible y la alimentación de alerta.

Procedimiento

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

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

Habilite la alimentación PoE continua, que permite que los dispositivos alimentados sigan recibiendo energía incluso después de que se reinicien.

Paso 3 Configure 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 la alimentación PoE continua se muestran en la parte inferior de la página. La potencia reservada es igual a la potencia total menos la potencia de alerta.



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

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

Figura 3-5 Configuración global

Global Config

Port Config

Perpetual PoE

☒

Save

Available Power	Alert Power
54 (1~60)W	60 (1~60)W

Save

Total Power(W)	Available Power(W)	Alert Power(W)	Power Consumption(W)	Reserved Power(W)	Remaining Power(W)	Perpetual PoE
60	54	60	0	0	60	Off

Refresh

Paso 4 Hacer clic **Ahorrar**.

3.3.2 Configuración de puertos

Configure la función PoE del puerto.

Procedimiento

Paso 1 Seleccionar **Configuración del interruptor > 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 el PD y suministrarle energía de forma remota a través de puertos eléctricos Ethernet.
- **PoE de larga distancia:**Tras habilitar la alimentación PoE de largo alcance, 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.

- **PoE Watchdog:**Con la función de supervisión PoE activada, puede monitorizar el PD y mantenerlo en línea, además de comprobar el estado de los dispositivos PD 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 en 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 no sea un dispositivo estándar, utilice esta función para forzar el suministro de energía PoE.



Una vez habilitada la función PoE forzado, el puerto suministrará energía al dispositivo conectado, independientemente de si cumple o no con los requisitos. Tenga esto en cuenta.



Fuerza PoE y Vigilante de PoE pueden estar habilitados al mismo tiempo.

Figura 3-6 Configuración del puerto

Global Config
Port Config

Port	PoE	Long Distance PoE	PoE Watchdog	Force PoE
Port 1, Port 2	On	Off	Off	Off

Save

Port	Level	Power Consumption(W)	PoE Enable	Long Distance PoE	PoE Watchdog	Force PoE
Port 1	-	0	On	Off	Off	Off
Port 2	-	0	On	Off	Off	Off
Port 3	-	0	On	Off	Off	Off
Port 4	-	0	On	Off	Off	Off

Refresh

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 oscila entre 0 y 8, y el nivel estándar de alimentación Hi-PoE se muestra como 5+.
Consumo de energía (W)	Muestra la potencia PoE actual consumida por el puerto individual correspondiente.
Habilitar PoE	Indica si la alimentación a través de Ethernet (PoE) está habilitada para el puerto.
PoE de larga distancia	
PoE Watchdog	
Fuerza PoE	

4 Seguridad

4.1 Configuración del aislamiento de puertos

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

Procedimiento

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

Paso 2 Habilitar la separación de puertos.



Una vez habilitado el aislamiento de puertos, los puertos de enlace descendente estarán aislados y los de enlace ascendente no. (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 se reenvían continuamente en la red, lo que afecta a las comunicaciones y reduce considerablemente el rendimiento de la red. El control de tormentas permite limitar el flujo de difusión del puerto y descartar las tramas una vez que 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, active el control de tormentas y, a continuación, introduzca la velocidad.

Figura 4-1 Control de tormentas

For the port being configured, the suppression rate must be the same for its multicast, broadcast, and unknown unicast.

Type	Port	Enable	Speed Limit (Mbit/sec)
Broadcast ▼		On ▼	100 (1~100)M

Save

Port	Port Type	Broadcast	Multicast	Unknown Unicast	Speed Limit (Mbit/sec)
Port 1	Physical Port	On	Off	Off	100
Port 2	Physical Port	On	Off	Off	100

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 la velocidad deseada.

Procedimiento

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

Paso 2 Seleccione el puerto y la dirección, active el límite de velocidad del puerto y, a continuación, introduzca la velocidad.

La dirección incluye tanto hacia afuera como hacia adentro.

Figura 4-2 Límite de velocidad del puerto

Port	Direction	Enable	Speed Limit (Mbit/sec)
Port 1,Port 2	In	On	100 (1~1000)M

Port	Port Type	Input Port Speed (Mbit/sec)	Output Port Speed (Mbit/sec)
------	-----------	-----------------------------	------------------------------

Paso 3Hacer clic **Ahorrar**.

5. Configuración de red

5.1 Configurar las tablas MAC

La tabla MAC (Control de Acceso al Medio) registra la relación entre la dirección MAC y el puerto, así como la información que incluye la VLAN a la que pertenece dicho puerto. Cuando el dispositivo reenvía un paquete, consulta la tabla MAC para obtener la dirección MAC de destino. Si la dirección MAC de destino se encuentra en la tabla, el paquete se reenvía directamente a través del puerto registrado. Si no se encuentra en la tabla, el dispositivo utiliza la difusión para reenviar el paquete 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 **Agregar**.



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

Figura 5-1 MAC estática

You can only configure up to 16 static MACs.

MAC Address	VLAN ID	Port
00:00:00:00:00:00	(1~4094)	Port 1

Add

No.	MAC Address	VLAN ID	Port
1	00:00:00:00:00:02	2	1

Delete

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

Figura 5-2 Búsqueda MAC

MAC Address	Port
00:00:00:00:00:02	Unlimited

Search

MAC Address	MAC Type	VLAN ID	Port
00:00:00:00:00:02	Static	2	Port 1

Paso 4 Haz clic en el **Lista MAC** pestaña y luego ver 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 aclarar la información.

5.2 Configuración de la protección contra bucles

Seleccionar **Configuración de red > Protección de bucle**. Habilite la protección contra bucles y, a continuación, haga clic. **Ahorrar**

Una vez habilitada la protección contra bucles, si se detecta un bucle, el puerto que lo causó se deshabilitará y luego se restablecerá automáticamente una vez que se elimine el bucle.

5.3 Configuración de STP

El Protocolo de Árbol de Expansión (STP) crea una topología lógica sin bucles para las redes LAN. Bloquea los enlaces redundantes entre dos dispositivos de red cualesquiera 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, utilizado 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 presentan el inconveniente de que todas las VLAN de la misma LAN comparten el mismo árbol de expansión.
- MSTP: Una tabla de asignación de VLAN virtuales 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 varias instancias de árbol de expansión independientes entre sí. A diferencia de STP y RSTP, MSTP proporciona múltiples rutas redundantes para el reenvío de datos. Asimismo, implementa el balanceo de carga entre VLAN.



El STP solo está disponible en determinados modelos.

5.3.1 STP

Procedimiento

- Paso 1** Seleccionar **Configuración de red > STP**
- Paso 2** **STP** Habilitar STP.
- Paso 3** Seleccione el modo de funcionamiento, incluyendo STP y
- Paso 4** RSTP. Configure los parámetros.

Figura 5-3 Configuración STP

Enable		☒		
$\text{Max Aging Time} \geq (\text{Hello Timer} + 1) \times 2$ $\text{Max Aging Time} \leq (\text{Forwarding Delay Time} - 1) \times 2$				
Working Mode	Hello Timer	Max. Aging Time	Forwarding Delay Time	Bridge Priority
STP	2 (1~10)s	20 (6~40)s	15 (4~30)s	32768 (0~61440)s
Save				
Working Mode	Hello Timer	Max. Aging Time	Forwarding Delay Time	Bridge Priority
STP	0	0	0	0

Tabla 5-1 Descripción de los parámetros STP

Parámetro	Descripción
Hola temporizador	Periodo durante el cual el puente raíz envía BPDU. El tiempo oscila entre 1 y 10 segundos.
Tiempo máximo de envejecimiento	El tiempo de envejecimiento de la BPDU actual. El tiempo oscila entre 6 y 40 segundos.
Retraso en el reenvío Tiempo	Tras establecer el cambio topológico, el puente mantiene el tiempo de espionaje y el estado de estudio. El tiempo oscila entre 4 y 30 segundos.
Prioridad de puente	El valor oscila entre 0 y 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 **Ahorrar**.



- El valor de **Prioridad** Su rango va 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

Port	Priority	Root Path Cost
Port 1, Port 2	128 (0~240)	0 (0~200000000)

Save

Port	Role	Status	Priority	Root Path Cost	Designated Bridge ID	Designated Port ID
Port 1	Disabled Port	Discard	128	0	-	-
Port 2	Disabled Port	Discard	128	0	-	-
Port 3	Disabled Port	Discard	128	0	-	-
Port 4	Disabled Port	Discard	128	0	-	-
Port 5	Disabled Port	Discard	128	0	-	-
Port 6	Disabled Port	Discard	128	0	-	-
Port 7	Disabled Port	Discard	128	0	-	-
Port 8	Disabled Port	Discard	128	0	-	-

5.4 Configuración de la agregación de enlaces

La agregación de enlaces consiste en agrupar varios puertos físicos de un conmutador en un único puerto lógico. Los múltiples enlaces de un mismo grupo pueden considerarse como un enlace lógico con mayor ancho de banda. Mediante la agregación, los puertos de un mismo grupo pueden compartir el flujo de comunicación, lo que permite un mayor ancho de banda. Además, los puertos de un mismo grupo pueden respaldarse de forma recíproca y dinámica para mejorar la fiabilidad del enlace.

Información general

Para establecer correctamente una agregación de enlaces, la configuración de agregación de enlaces en el dispositivo remoto debe ser la misma que la configuración en este dispositivo.



La agregación de enlaces solo está disponible en determinados modelos.

Procedimiento

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

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

El tipo incluye **Configuración MAC de origen**, **Configuración 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

Load Balancing

☒ Source MAC Config
 ☒ Destination MAC Config

☒ Source IP Config
 ☒ Destination IP Config

☒ TCP/UDP Source Port
 ☒ TCP/UDP Destination Port

Save

Aggregation Group No.	Port	Aggregation Group Mode
AGG 2	Port 3, Port 1, Port 2	Static

Add

☐	Aggregation Group No.	Port	Aggregation Group Mode
☐	1	25,26	Static
☐	3	11,12	Static
☐	4	17,18	Static

Delete

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 habilitados no se pueden agregar a grupos de agregación.

Paso 4 Hacer clic **Agregar**.

Seleccione el grupo de agregación y luego haga clic **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 Vea 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 para el descubrimiento de enlaces. Permite definir sus capacidades principales, dirección de administración, número de dispositivo y número de puerto como TLV (Type Length Value), encapsularlos en LLDPDU (Link Layer Discovery Protocol Data Unit) y enviarlos a su vecino. El vecino almacena la información recibida en una MIB (Management Information Base) estándar, lo que permite a la administración de la red consultar y evaluar el estado de la comunicación del enlace.

Procedimiento

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

Paso 2 Habilite LLDP y luego haga clic **Ahorrar**. Consulta 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				
Port 2				
Port 2				

7 Mantenimiento

7.1 Configuración de la duplicación de puertos

La función de duplicación copia el tráfico recibido o enviado, o ambos, desde 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 del conmutador 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:** Solo admite la recepción de tráfico.
- **Ambos:** Admite tanto el envío como la recepción.

Figura 7-1 Duplicación de puertos

Input and output messages from the source port will be mirrored to the destination port. (The destination port can only capture packets. It cannot transmit data to the switch.)

Source Port	Direction	Destination Port
Port 2, Port 3	Both ▼	Port 5 ▼

Save

Source Port	Direction	Destination Port

Paso 3 Hacer clic **Ahorrar**.

7.2 Configuración del firmware

7.2.1 Restaurar la configuración predeterminada de fábrica

Procedimiento

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

Paso 2 Hacer clic **Por defecto**, Introduzca la contraseña y, a continuación, haga clic **DE ACUERDO**.



- Todos los parámetros se restablecen a la configuración predeterminada, excepto la dirección IP, la máscara de subred, la puerta de enlace y el DNS.
- No puede restablecer 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 **Actualizar** Haga clic en **.DE**
- Paso 3** **ACUERDO**.
- La actualización del software puede tardar hasta 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 usar la esquina superior derecha  para reiniciar el dispositivo.

7.3 Cambio de contraseña

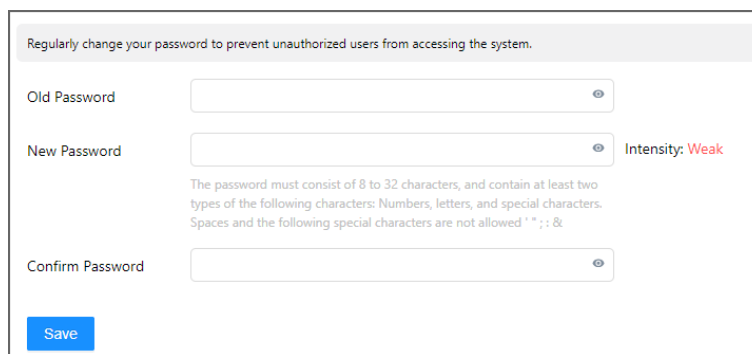
Procedimiento

- Paso 1** Seleccionar **Mantenimiento>Cambiar la contraseña**.
- Paso 2** Introduzca la contraseña anterior, la nueva contraseña y confirme la contraseña.



La contraseña debe constar de entre 8 y 32 caracteres no en blanco y contener al menos dos tipos de caracteres entre 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 dirección IP.
- **Deshabilitar DHCP:** Introduzca 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 de la red.
- **Desactivar la obtención automática de DNS:** Introduzca las direcciones IP de DNS1 y DNS2.

Figura 7-3 Red

DHCP	IP Address	Subnet Mask	Gateway	Auto Obtain DNS	DNS1	DNS2
Off ▼		255.255.252.0		Off ▼	8.8.8.8	8.8.4.4

[Save](#)

Paso 3 Hacer clic **Ahorrar**.

7.5 Visualización de la información del dispositivo

Seleccionar **Mantenimiento** > **Información del dispositivo** Puedes ver información como el nombre del dispositivo, la versión del software, la dirección MAC y el tiempo de funcionamiento.

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** > **Declaración legal** Haga clic en la pestaña correspondiente para ver el acuerdo de licencia del software, la política de privacidad y el aviso sobre 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 incluya el nombre de la cuenta ni el nombre de la cuenta en orden inverso;
- No utilice caracteres consecutivos, 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 pirateada.

3. Asigne las cuentas y los permisos adecuadamente.

Agregue usuarios según corresponda, en función de los requisitos de servicio y administración, y asígneles los permisos mínimos necesarios.

4. Habilitar la función de bloqueo de cuenta

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

5. Establezca y actualice la información de restablecimiento de contraseña de manera oportuna.

El dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que ciberdelincuentes utilicen esta función, modifique su información de inmediato si hay algún cambio. 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 los servicios web a través de canales seguros.

2. Transmisión cifrada de audio y vídeo

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

3. Desactive los servicios no esenciales y utilice el modo seguro.

Si no son necesarios, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, punto de acceso AP, etc., para reducir las superficies de ataque.

Si es necesario, se recomienda encarecidamente elegir modos seguros, que incluyen, 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 correo.
- FTP: Elija SFTP y configure contraseñas complejas.
- Punto de acceso: Seleccione 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 que los ciberdelincuentes lo adivinen.

Configuración de red

1. Habilitar lista de permitidos

Se recomienda activar la función de lista de permitidos y permitir el acceso al dispositivo únicamente a las direcciones IP incluidas en dicha lista. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la del dispositivo compatible a la lista de permitidos.

2. Enlace de dirección MAC

Se recomienda vincular la dirección IP de la puerta de enlace con la dirección MAC del dispositivo para reducir el riesgo de suplantación de identidad 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:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa;
- Según 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 dividir la red y lograr el aislamiento de la red;
- Implementar un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal de terminales a la red privada.

Auditoría de seguridad

1. Comprobar usuarios en línea

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

2. Consultar el registro del dispositivo

Al consultar los registros, podrá obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave realizadas por los usuarios que han iniciado sesión.

3. Configurar el registro de red

Debido a la limitada capacidad de almacenamiento 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 su posterior seguimiento.

Seguridad del software

1. Actualiza el firmware a tiempo.

Según las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que cuenten con las funciones y la seguridad más recientes. Si el dispositivo está conectado a una 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 la última versión del software cliente.

Protección física

Se recomienda implementar medidas de protección física para los dispositivos (especialmente los de almacenamiento), como colocar el dispositivo en una sala de máquinas y un armario dedicados, y contar con control de acceso.

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

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188