

Conmutador PoE (conmutador de escritorio administrado de 16/24 puertos)

Guía de inicio rápido








Prefacio

General

Este manual presenta principalmente los pasos de hardware, instalación y cableado del conmutador de escritorio administrado de 16/24 puertos (en lo sucesivo, "el Dispositivo").

Instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	agosto 2021

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el 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 se produce algún problema durante el uso del dispositivo.

- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del Dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo, cumpla con las pautas cuando lo use y guarde el manual en un lugar seguro para futuras consultas.

Requisitos operativos



- Asegúrese de que la fuente de alimentación del dispositivo funcione correctamente antes de su uso.
- No extraiga el cable de alimentación del dispositivo mientras esté encendido.
- Utilice el dispositivo únicamente dentro del rango de potencia nominal.
- Transporte, use y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos llenos de líquido encima del dispositivo para evitar que fluyan líquidos hacia él.
- No desmonte el dispositivo.
- Rango de temperatura de funcionamiento: $-10\text{ }^{\circ}\text{C}$ ($14\text{ }^{\circ}\text{F}$) a $+55\text{ }^{\circ}\text{C}$ ($131\text{ }^{\circ}\text{F}$).
- Este es un producto de clase A. En un entorno doméstico, esto podría causar interferencias de radio, en cuyo caso se le puede pedir al usuario que tome las medidas adecuadas.

requerimientos de instalación



WARNING

- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente con las normas locales de seguridad eléctrica y asegúrese de que el voltaje en el área sea constante y cumpla con los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación. De lo contrario, el dispositivo podría dañarse.



- Observe todos los procedimientos de seguridad y use el equipo de protección requerido proporcionado para su uso mientras trabaja en alturas.
- No exponga el dispositivo a la luz solar directa ni a fuentes de calor.
- No instale el dispositivo en lugares húmedos, polvorientos o con humo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee el ventilador del dispositivo.
- Asegúrese de que el dispositivo esté en una instalación horizontal e instálelo en una superficie sólida y plana para evitar que se caiga.
- Utilice el adaptador de corriente o la fuente de alimentación de la carcasa proporcionada por el fabricante del dispositivo.
- El estabilizador de voltaje y el dispositivo de protección contra rayos son opcionales según la fuente de alimentación y el entorno circundante.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- Asegúrese de conectar a tierra el dispositivo (sección transversal del cable de cobre: $> 2,5\text{ mm}^2$; resistencia a tierra: $\leq 4\ \Omega$).
- Para garantizar la disipación del calor, el espacio entre el dispositivo y el área circundante no debe ser inferior a 10 cm en los lados y 10 cm en la parte superior del dispositivo.

- Conecte los aparatos eléctricos de clase I a una toma de corriente con puesta a tierra de protección.
- No bloquee el ventilador del dispositivo con objetos, como periódicos, manteles o cortinas.
- No coloque llamas abiertas, como una vela encendida, sobre el dispositivo.
- Al instalar el dispositivo, asegúrese de que el enchufe de alimentación y el acoplador del dispositivo sean fáciles de alcanzar para cortar la alimentación.

Requisitos de mantenimiento



- Apague el dispositivo antes del mantenimiento.
- Marque los componentes clave en el diagrama del circuito de mantenimiento con señales de advertencia.
- Cuando reemplace la batería, asegúrese de usar el mismo tipo. El uso inadecuado de la batería puede provocar una explosión.

Tabla de contenido

Prefacio	yo
Medidas de seguridad y advertencias importantes	III
1. Información general	1
1.1 Introducción	1
1.2 Características	1
2 Puerto e Indicador	2
2.1 Panel frontal	2
2.2 Panel trasero	3
3 Instalación	4
4 Cableado	5
4.1 Conexión a tierra	5
4.2 Conexión del cable de alimentación	5
4.3 Conexión del puerto Ethernet	5
4.4 Conexión del puerto Ethernet SFP	6
4.5 Conexión del puerto Ethernet PoE	7
5 Operación rápida	8
5.1 Iniciar sesión a través de la Web	8
5.2 Restauración a la configuración de fábrica	8
Apéndice 1 Recomendaciones sobre ciberseguridad	9

1. Información general

1.1 Introducción

El dispositivo es un conmutador comercial de capa 2. Proporciona un motor de conmutación de alto rendimiento y una gran memoria de búfer para garantizar una transmisión fluida del flujo de video. Con un diseño totalmente metálico, el dispositivo tiene una gran capacidad de disipación de calor en la superficie de su carcasa y puede funcionar en entornos que van desde -10 °C (14 °F) hasta +55 °C (131 °F). Con su diseño DIP, proporciona una variedad de modos de trabajo que se adaptan a diferentes escenarios. El Dispositivo también es compatible con la gestión del consumo de energía, lo que le permite adaptarse a las fluctuaciones en el consumo de energía de los dispositivos terminales. Esto asegura un funcionamiento estable. Con administración web, SNMP y otras funciones, el dispositivo se puede administrar de forma remota. Puede conectarse directamente a iLinksView.

El Dispositivo es aplicable para su uso en diferentes escenarios, incluidos hogares, oficinas, pequeños centros comerciales y granjas de servidores.

1.2 Características

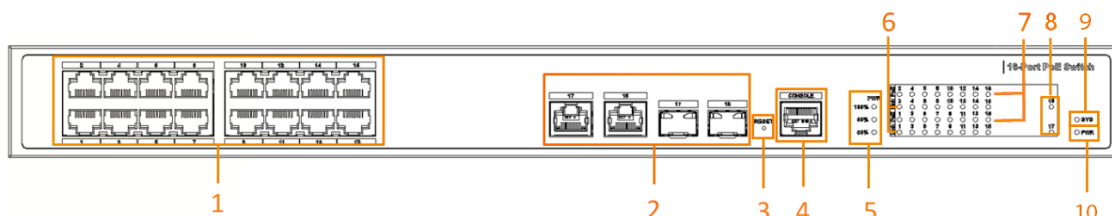
- Puertos Ethernet PoE de 16/24 × 100 Mbps, los puertos de enlace ascendente admiten puertos ópticos gigabit o puertos Ethernet.
- Todos los puertos cumplen con los requisitos de los estándares IEEE802.3af e IEEE802.3at. Los puertos rojos también cumplen con los estándares Hi-PoE e IEEE802.3bt, y los puertos naranjas cumplen con el estándar Hi-PoE.
- Transmisiones PoE de larga distancia de 250 m, que se pueden configurar en la web.
- Watchdog PoE para la detección en tiempo real del estado del dispositivo terminal, que se puede configurar en la web.
- Admite STP, RSTP y MSTP.
- Configuración de VLAN basada en IEEE802.1Q.
- Agregación manual de enlaces y LACP estático.
- Montaje en escritorio y montaje en rack.

2 Puerto e Indicador

2.1 Panel frontal

La siguiente figura es solo de referencia y puede diferir del dispositivo real.

Figura 2-1 Panel frontal



A continuación se muestran todos los puertos e indicadores del panel frontal del conmutador de escritorio administrado de 16/24 puertos. Es posible que su dispositivo real solo tenga algunos de ellos.

Tabla 2-1 Descripción del panel frontal

No.	Descripción
1	Puertos Ethernet PoE autoadaptativos de 10/100 Mbps.
2	Puerto de enlace ascendente, incluidos puertos Ethernet autoadaptativos de 10/100/1000 Mbps y puerto óptico de 1000 Mbps.
3	Botón de reinicio. Manténgalo presionado durante más de 5 segundos y suéltelo después de que todos los indicadores de estado del panel se enciendan para restaurar el dispositivo a su configuración predeterminada.
4	Puerto de consola.
5	Indicadores de potencia de salida PoE. <ul style="list-style-type: none"> ● Verde fijo: Potencia total $\leq 50\%$. ● Verde y amarillo fijos: $50\% < \text{potencia total} \leq 80\%$. ● Verde, amarillo y rojo fijos: $80\% < \text{potencia total}$.
6	Indicadores de estado de conexión de un solo puerto (Link). <ul style="list-style-type: none"> ● Encendido: Conectado al dispositivo. ● Apagado: no conectado al dispositivo.
7	Indicadores de estado del puerto PoE. <ul style="list-style-type: none"> ● Encendido: alimentado por PoE. ● Apagado: No alimentado por PoE.
8	Indicadores de estado de conexión del puerto Uplink (Link). <ul style="list-style-type: none"> ● Encendido: Conectado al dispositivo. ● Apagado: no conectado al dispositivo.
9	Indicador de estado del sistema (SYS). <ul style="list-style-type: none"> ● Intermitente: El funcionamiento es normal. ● Apagado: la operación no es normal.
10	Indicador de encendido. <ul style="list-style-type: none"> ● Encendido: encendido. ● Apagado: Apagado.

2.2 Panel trasero

La siguiente figura es solo de referencia y puede diferir del dispositivo real.

Figura 2-2 Panel trasero



Tabla 2-2 Descripción del panel trasero

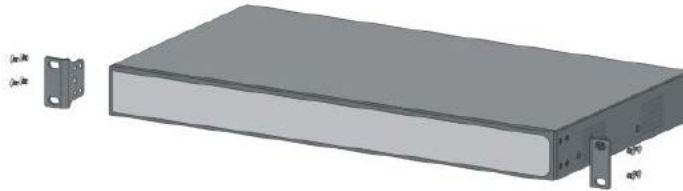
No.	Descripción
1	Interruptor de alimentación.
2	Puerto de alimentación, admite 100-240 VCA.
3	Terminal de tierra.

3 Instalación

El dispositivo admite montaje en bastidor.

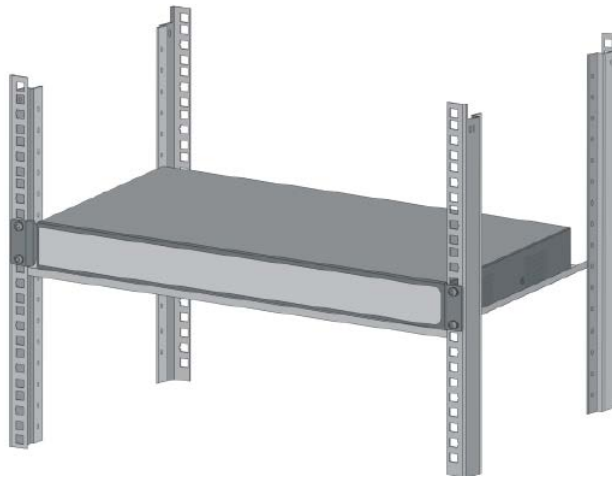
Paso 1 Fije el soporte de montaje al panel lateral del dispositivo (uno en cada lado) y asegúrelo con los tornillos provistos con el bastidor.

Figura 3-1 Instale el soporte



Paso 2 Fije el dispositivo al bastidor con tornillos.

Figura 3-2 Instalar dispositivo



4 Cableado

4.1 Conexión a tierra

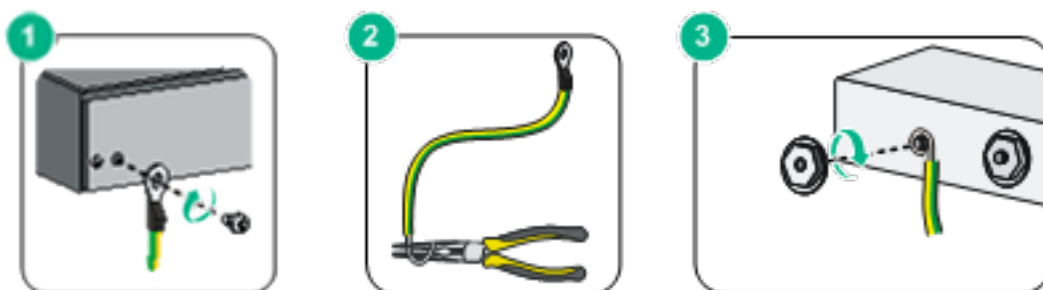
Conectar a tierra el dispositivo puede protegerlo contra rayos e interferencias.

Paso 1 Retire el tornillo de conexión a tierra del dispositivo y páselo a través del orificio redondo del terminal OT del cable de conexión a tierra. Gire el tornillo de conexión a tierra en el sentido de las agujas del reloj con un destornillador de cruz para sujetar el terminal OT del cable de conexión a tierra.

Paso 2 Enrolle el otro extremo del cable de tierra en un círculo con los alicates de punta fina. Conecte el otro

Paso 3 extremo del cable de tierra a la barra de tierra, luego gire la tuerca hexagonal en el sentido de las agujas del reloj con una llave para sujetar el otro extremo del cable de tierra al terminal de tierra.

Figura 4-1 Conexión a tierra



4.2 Conexión del cable de alimentación

Antes de conectar el cable de alimentación, asegúrese de que el dispositivo esté conectado a tierra de forma segura.

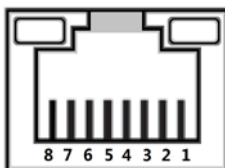
Paso 1 Conecte un extremo del cable de alimentación al conector de alimentación del dispositivo.

Paso 2 Conecte el otro extremo del cable de alimentación a la toma de corriente externa.

4.3 Conexión del puerto Ethernet

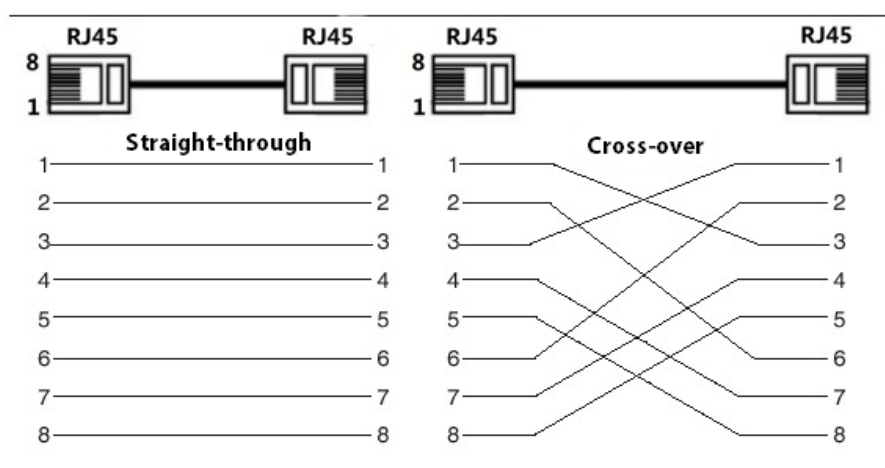
El puerto Ethernet es un puerto RJ-45 estándar. Con su función de autoadaptación, se puede configurar automáticamente en modo de funcionamiento dúplex completo/semidúplex. Es compatible con el reconocimiento automático MDI/MDI-X del cable, lo que le permite utilizar un cable cruzado o un cable directo para conectar el dispositivo terminal al dispositivo de red.

Figura 4-2 Número de pin del puerto Ethernet



La conexión del cable del conector RJ-45 cumple con el estándar 568B (1 naranja blanco, 2 naranja, 3 verde blanco, 4 azul, 5 azul blanco, 6 verde, 7 marrón blanco, 8 marrón) .

Figura 4-3 Cable de conexión



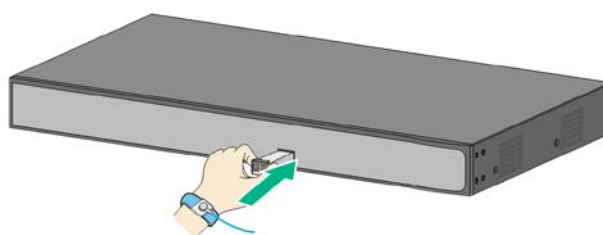
4.4 Conexión del puerto Ethernet SFP



- Al instalar el módulo óptico SFP, no toque el dedo dorado del módulo óptico SFP.
- No retire el tapón antipolvo del módulo óptico SFP antes de conectar la fibra óptica.
- No inserte directamente el módulo óptico SFP en la ranura mientras la fibra óptica esté insertada en ella.
Desconecte la fibra óptica antes de instalarla.

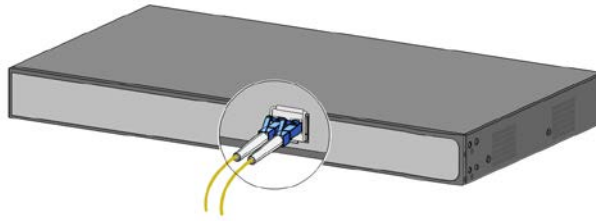
- Paso 1** Use la muñequera antiestática y confirme que la muñequera antiestática esté en buen contacto con su piel y que el dispositivo esté conectado a tierra de manera confiable.
- Paso 2** Suba el asa del módulo óptico SFP verticalmente y sostenga el módulo óptico por ambos lados con las manos.
- Paso 3** Empuje suavemente el módulo óptico en la ranura en dirección horizontal hasta que el módulo óptico SFP esté firmemente conectado a la ranura.

Figura 4-4 Instale el módulo SFP



- Paso 4** Retire la tapa antipolvo del conector LC de la fibra óptica y el tapón antipolvo del módulo óptico SFP.
- Paso 5** Conecte el conector LC de la fibra óptica al módulo óptico SFP.

Figura 4-5 Conexión de fibra óptica



4.5 Conexión del puerto Ethernet PoE

Si el dispositivo terminal tiene un puerto Ethernet PoE, puede conectar directamente este puerto al puerto Ethernet PoE del dispositivo a través del cable de red para lograr una conexión de red y fuente de alimentación sincronizadas. La distancia máxima entre el Dispositivo y el dispositivo terminal es de unos 100 m.



Cuando se conecta a un dispositivo que no es PoE, el dispositivo debe usarse con una fuente de alimentación aislada.

5 Operación rápida

5.1 Iniciar sesión a través de la Web

Puede iniciar sesión en el Dispositivo a través de la web para su administración y operación. Para obtener más información, consulte el manual de funcionamiento web.



Para el primer inicio de sesión, debe cambiar la contraseña de acuerdo con el indicador de la interfaz.

Tabla 5-1 Configuración predeterminada de fábrica

Parámetro	Descripción
dirección IP	192.168.1.110/255.255.255.0
Nombre de usuario	administración
Clave	<ul style="list-style-type: none">● Web: sin contraseña inicial, definida por el usuario durante la inicialización.● iLinkView: lt_91_il_02_nmp <p>Cuando utilice iLinkView para la administración de dispositivos, asegúrese de que el nombre de usuario y la contraseña del dispositivo coincidan con los de iLinkView; de lo contrario, iLinkView no podrá descubrir el dispositivo.</p>

5.2 Restauración a la configuración de fábrica

Hay dos formas de restaurar el dispositivo a la configuración de fábrica.

- Mantenga presionado el botón **Reiniciar** durante 5 segundos para restaurar el dispositivo a la configuración de fábrica.
- Inicie sesión en la web o utilice la línea de comandos. Para obtener más información, consulte el manual de operaciones web o el manual de referencia de la línea de comandos.

Apéndice 1 Recomendaciones sobre ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a realizar para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su equipo:

1. Protección Física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en un gabinete y una sala de computadoras especiales, e implemente una administración de claves y un permiso de control de acceso bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de equipos extraíbles (como un disco flash USB), puerto serie), etc.

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10 Transmisión encriptada de audio y video

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

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11 Auditoría segura

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

12 Registro de red

Debido a la limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13 Construir un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

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