Switch de escritorio PoE no administrado Gigabit de 16 puertos

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta las características y la estructura del conmutador de escritorio PoE no administrado gigabit de 16 puertos (en adelante, "el dispositivo").

Las instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Septiembre de 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual.
- El manual se actualizará de acuerdo con las leyes y regulaciones más recientes de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si existe inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar 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.
- Aún puede haber desviaciones en los datos técnicos, la descripción de funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final.
- Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- 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.
- Si hay alguna duda o controversia, nos reservamos el derecho a una explicación final.

Advertencias y medidas de seguridad importantes

El manual le ayuda a utilizar nuestro producto correctamente. Para evitar peligros y daños a la propiedad, lea atentamente el manual antes de usar el producto y le recomendamos que lo guarde en un lugar seguro para futuras consultas.

Requisitos operativos

- No exponga el dispositivo directamente a la luz solar y manténgalo alejado del calor.
- No instale el dispositivo en un ambiente húmedo y evite el polvo y el hollín.
- Asegúrese de que el dispositivo esté en una instalación horizontal e instálelo sobre una superficie sólida y plana para evitar que se caiga.
- Evite salpicaduras de líquido en el dispositivo. No coloque objetos llenos de líquido sobre el dispositivo para evitar que el líquido fluya hacia el dispositivo.
- Instale el dispositivo en un ambiente bien ventilado. No bloquee la salida de aire del dispositivo.
- Utilice el dispositivo a la tensión nominal de entrada y salida.
- No desmonte el dispositivo sin instrucción profesional.
- Transporte, utilice y almacene el dispositivo en los rangos permitidos de humedad y temperatura.
- Al retirar el cable, primero apague el dispositivo para evitar lesiones personales.
- El estabilizador de voltaje y el dispositivo de protección contra rayos son opcionales según la fuente de alimentación y el entorno circundante.

Requisitos de la fuente de alimentación

- Utilice la batería correctamente para evitar incendios, explosiones y otros peligros.
- Reemplace la batería por una del mismo tipo.
- Utilice el cable de alimentación recomendado localmente dentro del límite de las especificaciones nominales.
- Utilice el adaptador de corriente estándar. No asumiremos ninguna responsabilidad por cualquier problema causado por un adaptador de corriente no estándar.
- La fuente de alimentación debe cumplir con el requisito SELV. Utilice la fuente de alimentación que cumpla con la fuente de alimentación limitada, de acuerdo con IEC60950-1. Consulte la etiqueta del dispositivo.
- Asegúrese de que el dispositivo esté conectado a tierra (el área de sección del cable GND debe ser superior a 2,5 mm^2 y la resistencia GND debe ser inferior a 5 Ω).
- El acoplador es el aparato de desconexión. Manténgalo en ángulo para facilitar su operación.

Tabla de contenido

1 Descripción general del producto

1.1 Introducción

El conmutador de escritorio PoE no administrado gigabit de 16 puertos es un tipo de conmutador comercial de capa dos. Proporciona dieciséis puertos Ethernet de 10/100/1000 Mbps y ninguno de enlace ascendente.

1.2 Características

- El puerto 1 y el puerto 2 admiten una fuente de alimentación Hi-PoE de 60 W.
- Conmutador comercial de capa dos.
- Admite los estándares IEEE802.3, IEEE802.3u, IEEE802.3X, EEE802.3az e IEEE802.3ab.
- Aprendizaje automático de MAC, envejecimiento, capacidad de dirección MAC 4K.
- Admite la autoadaptación MDI / MDIX.
- El puerto RJ45 admite la autoadaptación de 16 × 10/100/1000 Mbps, admite los estándares de fuente de alimentación IEEE802.3af e IEEE803.3at.
- Método de control de flujo: el dúplex completo adopta el estándar IEEE802.3x, el dúplex medio adopta el estándar de contrapresión.
- Adopta carcasa de metal.
- Admite fuente de alimentación DC 48V – 57V.
- Admite la instalación de montaje en pared.
- Soporta el orificio de bloqueo antirrobo.

1.3 Aplicación típica

Figura 1-1 Escena típica de redes

2 Estructura del dispositivo

2.1 Panel frontal

Figura 2-1 Panel frontal

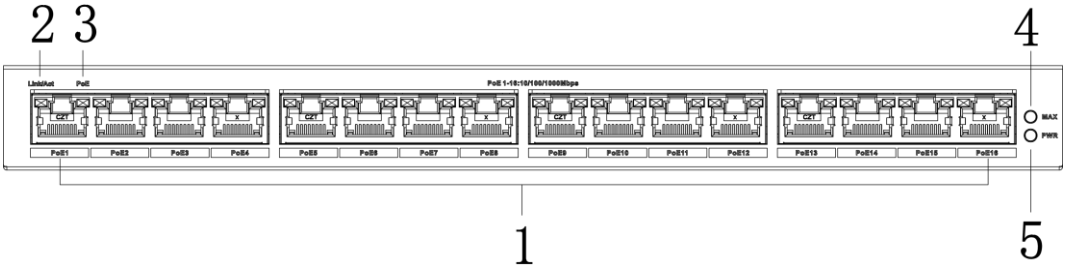

Tabla 2-1 La descripción del panel frontal

No.	Nombre	Descripción
1	10/100/1000 Base-T	Puertos de fuente de alimentación PoE autoadaptables de 16 × 10/100/1000 Mbps.
2	Enlace / acto	Luz indicadora de estado de enlace de puerto único. ● Apagado: el puerto no está vinculado. ● Encendido: el puerto está vinculado. ● Intermitente: se están transmitiendo datos.
3	PoE	Luz indicadora de estado PoE de un solo puerto. ● Apagado: no se utiliza la fuente de alimentación PoE. ● Encendido: se utiliza la fuente de alimentación PoE.
4	MAX	Luz indicadora de energía PoE, se enciende cuando el consumo de energía PoE del dispositivo es superior al 80% del valor nominal (152 W para este modelo).
5	PWR	Luz indicadora de encendido, mientras tanto, es la luz indicadora de estado de la fuente de alimentación PoE.

2.2 Panel trasero

Figura 2-2 Panel trasero

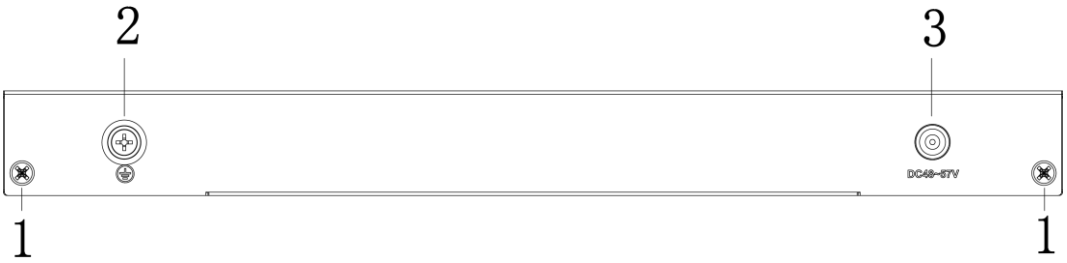

Tabla 2-2 La descripción del panel posterior

No.	Nombre	Descripción
1	Agujero de bloqueo	Bloquea el interruptor.
2	Terminal de tierra	GND.

No.	Nombre	Descripción
3	Puerto de alimentación	Soporta DC 48V – 57V.

2.3 Panel lateral

Figura 2-3 Panel lateral

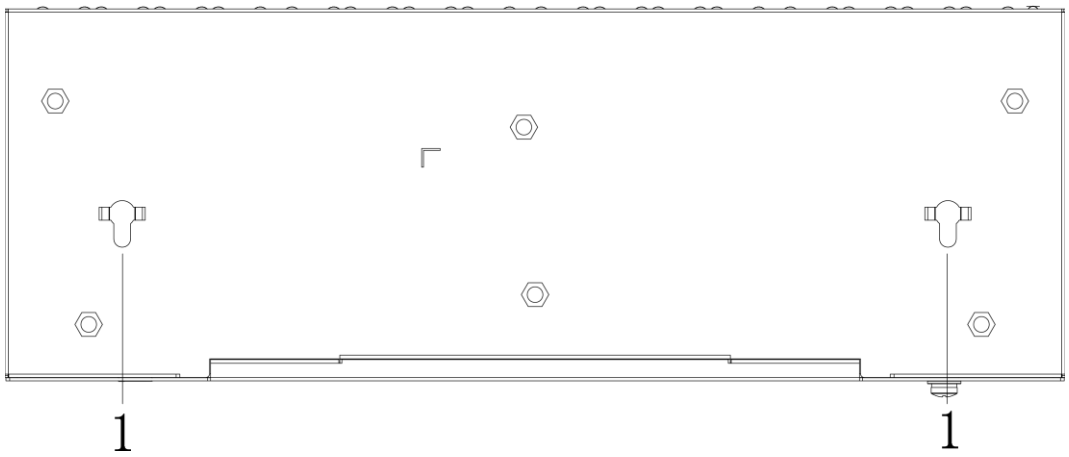

Tabla 2-3 La descripción del panel lateral

No.	Nombre	Descripción
1	Agujero de montaje en pared	Admite la instalación de montaje en pared.

2.4 Fuente de alimentación PoE

- Dos puertos RJ-45 de 1000M admiten los estándares IEEE802.3af, IEEE802.3at y la fuente de alimentación Hi-PoE de 60W.
- Catorce puertos RJ-45 de 1000M admiten la fuente de alimentación estándar IEEE802.3af, IEEE802.3at.

Apéndice 1 Recomendaciones de 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 muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

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

1. **Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No 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 cliente a tiempo**

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

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

1. **Proteccion fisica**

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

2. **Cambie las contraseñas con regularidad**

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. **Establecer y actualizar contraseñas Restablecer información a tiempo**

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan 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 con la contraseña incorrecta varias veces, 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 en cualquier conjunto de números entre 1024 ~ 65535, reduciendo 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 que vincule la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de ARP.

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

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

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

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

● FTP：Elija SFTP y configure contraseñas seguras.

● Punto de acceso AP：Elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10.**Transmisión encriptada de audio y video**

Si su contenido de datos de audio y video es muy importante o sensible, 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 cifrada provocará una pérdida en la eficiencia de la transmisión.

11.**Auditoría segura**

● Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.

● Verificar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12.**Registro de red**

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

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

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

● Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la 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 utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.

● Establecer el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.

● Habilite la función de filtrado de direcciones IP / MAC para limitar el rango de hosts permitidos para acceder al dispositivo.