Conmutador Ethernet (conmutador no administrado de 5 y 8 puertos con carcasa de plástico)

Guía de inicio rápido

Versión 1.0.1

Prefacio

Este manual presenta las funciones y operaciones del conmutador no administrado de 5 y 8 puertos con carcasa de plástico (en adelante, "el conmutador"). Lea atentamente antes de utilizar el conmutador y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
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 provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.1	Se actualizó la descripción del panel posterior.	Agosto de 2022
Versión 1.0.0	Primer lanzamiento.	Julio de 2022

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, es posible que recopile datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Actualizaciones de productos

Es posible 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 de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de explicación final.
- Actualice el software de lectura o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

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 y cumpla con las pautas al usarlo.

Requisitos de transporte

Transporte el dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de almacenamiento

Conservar el dispositivo en condiciones de humedad y temperatura permitidas.

Requisitos de instalación

 WARNING

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con los códigos y normas de seguridad eléctrica locales. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.

- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Coloque el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de armario proporcionada por el fabricante.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma 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.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañar el dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con toma de tierra.
- El dispositivo debe estar conectado a tierra mediante un cable de cobre con una sección transversal de 2,5 mm_2y una resistencia de tierra no mayor a 4 Ω.
- El estabilizador de voltaje y el protector contra sobretensiones eléctricas son opcionales dependiendo del suministro de energía real en el sitio y del entorno ambiental.
- 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.
- Al instalar el dispositivo, asegúrese de que el enchufe de alimentación y el acoplador del aparato sean de fácil acceso para cortar la energía.

Requisitos de funcionamiento

 WARNING

- No desmonte el dispositivo sin instrucción profesional.
- Utilice el dispositivo dentro del rango nominal de entrada y salida de energía.
- Asegúrese de que la fuente de alimentación sea correcta antes de usar.
- Asegúrese de que el dispositivo esté apagado antes de desmontar los cables para evitar lesiones personales.
- No desconecte el cable de alimentación del costado del dispositivo mientras el adaptador esté encendido.

- Utilice el dispositivo en las condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo que evite que el líquido fluya hacia él.
- Temperatura de funcionamiento: 0 °C (32 °F) a +45 °C (113 °F).
- No bloquee el ventilador del dispositivo con objetos, como un periódico, un mantel o una cortina.
- No coloque una llama abierta sobre el dispositivo, como una vela encendida.

Requisitos de mantenimiento

 WARNING

- Apague el dispositivo antes de realizar el mantenimiento.
- Marque los componentes clave en el diagrama del circuito de mantenimiento con señales de advertencia.

Tabla de contenido

1 Estructura

1.1 Panel superior

Figura 1-1 Panel superior (5 puertos)

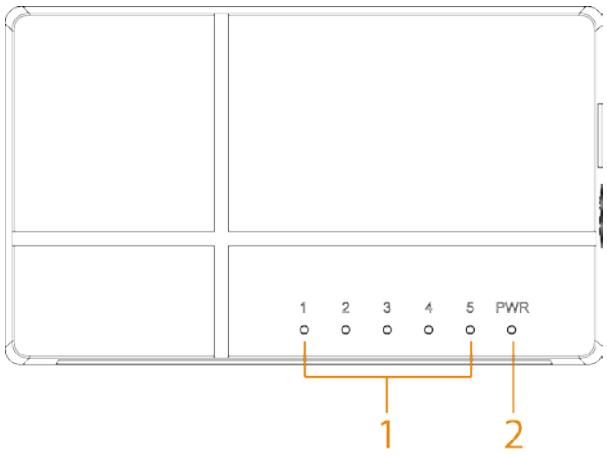

Figura 1-2 Panel superior (8 puertos)

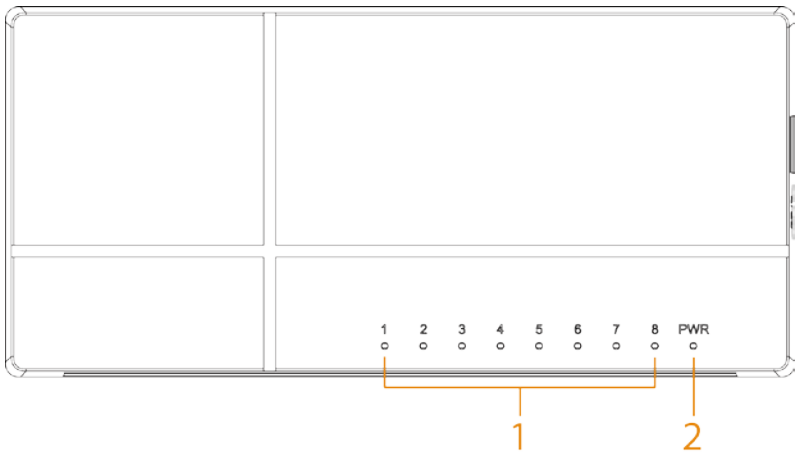

Tabla 1-1 Panel superior

No.	Descripción
1	Indicador de estado de conexión/transmisión del puerto (Link/Act). ● Fijo encendido: conectado. ● Apagado: Desconectado. ● Destellos: Transmitiendo datos.
2	Indicador de encendido. ● Fijo encendido: encendido. ● Apagado: Apagado.

1.2 Panel lateral

Figura 1-3 Panel lateral (5 puertos)

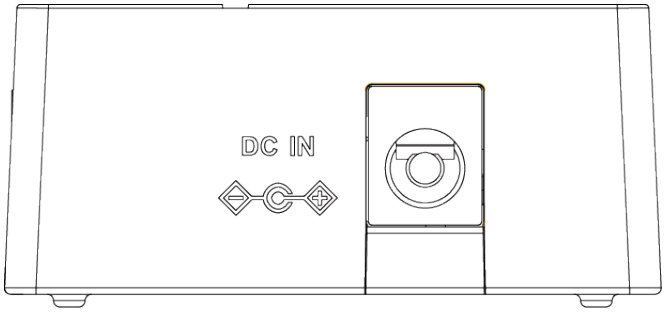

Figura 1-4 Panel lateral (8 puertos)

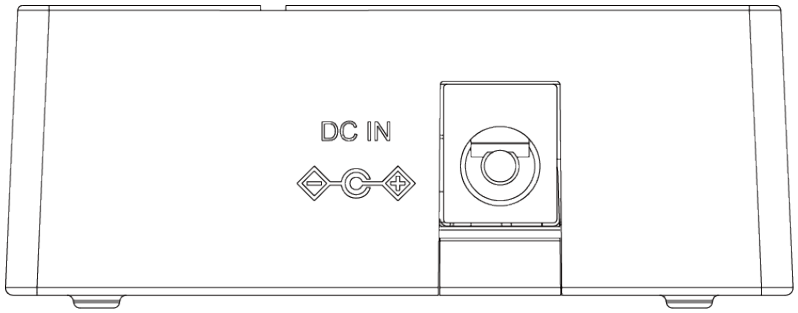

Tabla 1-2 Panel lateral

Nombre	Descripción
Puerto de entrada de alimentación de CC	Enciende el Switch con un adaptador de alimentación de CC externo.

1.3 Panel posterior

Figura 1-5 Panel posterior (5 puertos)

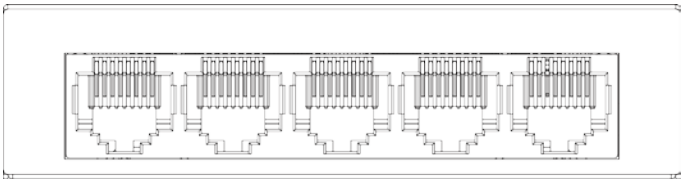

Figura 1-6 Panel posterior (5 puertos)

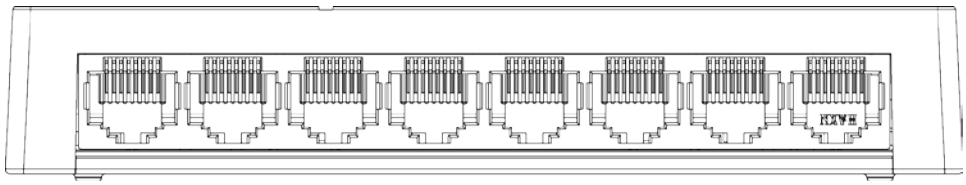

Tabla 1-3 Panel posterior

Nombre	Descripción
Puerto Ethernet	Puerto autoadaptativo de 10 Mbps/100 Mbps o 10 Mbps/100 Mbps/1000 Mbps.

2 Instalación y conexión

2.1 Instalación del conmutador

Paso 1 Coloque el Switch sobre un escritorio plano.

Paso 2 Verifique el adaptador de alimentación de CC y luego conéctelo al puerto de entrada de alimentación de CC en el panel lateral.

- Asegúrese de dejar suficiente espacio para la disipación del calor.
- No coloque nada pesado sobre el Switch.

2.2 Conexión

Conecte el adaptador de corriente al puerto de entrada de alimentación de CC en el panel lateral y luego conéctelo a la toma de corriente. Verifique el estado del indicador de alimentación. Si el indicador está encendido, el conmutador está encendido y comenzará la inicialización automáticamente.

- El conmutador se puede conectar a un puerto RJ–45 de 10/100 Mbps o de 10 Mbps/100 Mbps/1000 Mbps en computadoras u otros dispositivos con cable UTP de categoría 3, categoría 4, categoría 5 de conexión directa o par trenzado cruzado.
- Al conectar el Switch a un puerto de 100 Mbps de computadoras u otros dispositivos, utilice la Categoría 5 o par trenzado UTP categoría 5e.

Apéndice 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que concierne a todos los dispositivos 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 conectados los hará menos susceptibles a los ataques. A continuación, se ofrecen algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a 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 caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta ni el nombre de la cuenta en orden inverso;
- No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres 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 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 esté conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

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

1.**Protección física**

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

2.**Cambie las contraseñas periódicamente**

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

El dispositivo admite la función de restablecimiento de contraseña. Configure a tiempo la información relacionada con el restablecimiento de contraseña, incluido el buzón de correo del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección de contraseña, se recomienda no utilizar aquellas que se puedan adivinar fácilmente.

4.**Habilitar bloqueo de cuenta**

La función de bloqueo de cuenta está activada 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, se bloqueará la cuenta correspondiente y la dirección IP de origen.

5.**Cambiar el puerto 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 externas puedan adivinar qué puertos está utilizando.

6.**Habilitar HTTPS**

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

7.**Vinculación de dirección MAC**

Le recomendamos vincular 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 manera razonable**

Según los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9.**Desactivar servicios innecesarios y elegir modos seguros**

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir 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 autenticación seguras.
- SMTP: elija TLS para acceder al servidor de buzón.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10.**Transmisión de audio y vídeo encriptados**

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 que los datos de audio y video sean robados durante la transmisión.

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de transmisión.

11.**Auditoría segura**

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Comprobar 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 un período prolongado, se recomienda que habilite la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el seguimiento.

13.Construir un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo 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 la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red 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 a los que se les permite acceder al dispositivo.