Switch de escritorio no administrado de 100/1000 Mbps

Guía de inicio rápido

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Prefacio

General

Este manual presenta la estructura y la instalación del conmutador de escritorio no administrado de 100/1000 Mbps.

Modelos

DH-PFS3005-5ET-L

DH-PFS3008-8ET-L

DH-PFS3005-5GT-L

DH-PFS3008-8GT-L

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
 **PELIGRO**	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
 **ADVERTENCIA**	Indica un riesgo potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 **PRECAUCIÓN**	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 **CONSEJOS**	Indica alto voltaje peligroso. Tenga cuidado de no entrar en contacto con la electricidad.
 **NOTA**	Indica un peligro de radiación láser. Tenga cuidado de evitar la exposición a un rayo láser.

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Noviembre de 2019

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 actualizaría de acuerdo con las últimas leyes y regulaciones de los

regiones. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay 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 actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos
- técnicos, la descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra 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, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

El manual le ayuda a utilizar el producto correctamente. Para evitar peligros y daños a la propiedad, lea atentamente el manual antes de utilizar el producto y consérvelo 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 las 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 desarme el dispositivo sin instrucción profesional.
- Transporte, use y almacene el dispositivo en rangos permitidos de humedad y temperatura.

Requisitos de suministro de energía

- 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 deberá 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. Adopte la protección GND para dispositivos de tipo I.
-
- El acoplador es el aparato de desconexión. Manténgalo en ángulo para facilitar la operación.

Tabla de contenido

1 Estructura del dispositivo

Este manual es para varios modelos del conmutador. Aquí, tomemos el modelo DH-PFS3005-5ET-L como ejemplo. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.

1.1 Panel frontal y panel izquierdo

Hay series de indicadores en el panel frontal y 1 puerto de alimentación de CC en el panel izquierdo. Vea la Figura 1-1.

Figura 1-1 Panel frontal

Tabla 1-1 Descripción del panel frontal

Indicador	Color	Estado	Descripción
Poder	Verde	En	El interruptor está encendido. El
		Apagado	interruptor está apagado.
1–5 / 8	Verde 10/100/1000 Mbps	Brilla verde	Un dispositivo está conectado a un puerto del conmutador.
		Apagado	Un dispositivo está desconectado de un puerto del conmutador.
		Parpadea en verde	Enviar o recibir datos.

Puerto de alimentación de CC: la alimentación se suministra mediante un adaptador de alimentación de CC externo. Para obtener información sobre el voltaje de entrada de la alimentación de CC, consulte la sección de especificaciones.

1.2 Panel trasero

Hay puertos RJ-45 de 10/100/1000 Mbps en el panel posterior. Vea la Figura 1-2.

Figura 1-2 Panel trasero

Puerto RJ-45 de 10/100/1000 Mbps: admite la conexión del dispositivo con un ancho de banda de 10/100/1000 Mbps, cada puerto corresponde a un indicador de Enlace / Act / Velocidad.

2 Instalación y conexión

Este capítulo describe cómo instalar y conectar un conmutador Ethernet de 10 Gigabit.

2.1 Instalación

Paso 1 Coloque el interruptor sobre una mesa plana.

Paso 2 Asegúrese de que el adaptador de corriente esté conectado a la fuente de alimentación.

Paso 3 Asegúrese de que haya suficiente ventilación alrededor del interruptor para disipar el calor y el aire.

- Evite colocar objetos pesados sobre el interruptor.
- Para garantizar una conexión de cable estable, coloque el interruptor horizontalmente en el escritorio.

2.2 Conexión al conmutador

Los interruptores se pueden conectar a computadoras u otros dispositivos a través de UTP o pares trenzados de CAT3, CAT4 y CAT5. Se requiere UTP de CAT5 o CAT5e para una operación de 100 Mbps. Se requiere par trenzado de CAT5e o CAT6 para una operación de 1000 Mbps. Puede conectarse a puertos RJ-45 con 10/100/1000 Mbps en una computadora u otros dispositivos desde cualquier puerto del conmutador.

Conecte el interruptor y encienda, el interruptor se inicializa automáticamente y el indicador LED está encendido.

Si el indicador LED está apagado, verifique la fuente de alimentación y su conexión.

Apéndice 1 Especificaciones técnicas

Apéndice tabla 1-1 Especificaciones

Hardware					
Modelo		DH-PFS3005-5E DH-PFS3008-8E TL	TL	DH-PFS3005-5G DH-PFS3008-8G TL	TL
Estándares Conformidad		IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE802.3az		IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3x	
Medio de red		• 10Base-T: UTP de CAT3, CAT4 o CAT5 (máximo 100 M) 100Base-TX: UTP de CAT5 • o CAT5e (máximo 100 M)		• 10Base-T: UTP de CAT3, CAT4 o CAT5 (máximo 100 M) 100Base-TX: UTP de CAT5 • o CAT5e (máximo 100 M) • 1000Base-TX: UTP de CAT5e o CAT6 (máximo 100 M)	
Puerto		5 puertos RJ-45 adaptativos adaptativos con puertos 10/100 Mbps	8 puertos RJ-45 con 10/100 Mbps	5 puertos RJ-45 adaptables con puertos 10/100/1000 Mbps	8 puertos RJ-45 adaptables con 10/100/1000 Mbps
LED Indicar o	Enlace / acto	Verde, puerto RJ-45 de 10/100 Mbps		Verde, puerto RJ-45 de 10/100/1000 Mbps	
	Potestades YS	Verde		Verde	
Transmisión Modo		Almacenamiento y reenvio			
Capacidad de conmutación Paquete de 1 Gbps			1,6 Gbps	10 Gbps	16 Gbps
Memoria	Buffer	448 KB	448 KB	1,5 MB	1,5 MB
Dimensiones (L × W × H)		77 mm × 46 mm × 21 mm (3,03 ”× 1,81 "× 0,83")	132 mm × 70 mm × 26 mm (5,20 "× 2,76" × 1.02 ”)	77 mm × 46 mm 125 mm × 22 mm (4,92” × 1,81 "× 0,83")	65 mm × 21 mm (3,03 2,56 "× 0,87")
Solicitud medio ambiente		• Temperatura de funcionamiento: 0 ℃ hasta 40 ℃ (32 ℉ hasta 104 ℉) • Temperatura de almacenamiento: -40 ℃ hasta 70 ℃ (- 40 ℉ hasta 158 ℉) • Humedad de funcionamiento: 10% - 90% Humedad de • almacenamiento: 5% - 90% Entrada:			
Fuente de alimentación y Consumo		• 5 V / 500 mA corriente continua • Poder consumo n: 1,3 W	• Entrada: 5 V / 500 mA corriente continua • Poder consumo n: 1,5 W	• Entrada: 5 V / 1 A CC • Poder consumo n: 1,6 W	• Entrada: 5 V / 1 A CC • Poder consumo n: 4W

Apéndice 2 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 deben tomarse 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 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 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 "búsqueda 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 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 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 equipos 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 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 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 externas 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. **Habilitar lista blanca**

   Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. **Enlace de dirección MAC**

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

9. **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.

10. **Deshabilite los servicios innecesarios y elija 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 autenticación y de cifrado 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.

11. **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 encriptada provocará cierta pérdida en la eficiencia de transmisión.

12. **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.
    - Verifique el registro del equipo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

13. **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 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.

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

    Para garantizar mejor la seguridad de los equipos 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.

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

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Dirección: No.1199, Bin'an Road, Binjiang District, Hangzhou, PR China Código postal: 310053

Tel: + 86-571-87688883

Envíe por fax: + 86-571-87688815

Correo electrónico: overseas@dahuatech.com

Sitio web: www.dahuasecurity.com