Switch Fast Ethernet de 6 puertos con PoE de 4 puertos

Manual de usuario

TECNOLOGÍA CO., LTD DE LA VISIÓN DE ZHEJIANG DAHUA V1.0.0

Prefacio

General

Este manual presenta las características y la estructura del conmutador Fast Ethernet de 6 puertos con PoE de 4 puertos (en adelante, "el dispositivo").

Modelos

DH-PFS3006-4ET-36

Las instrucciones de seguridad

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

Significado de las palabras de señalización	
PELIGRO	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un peligro 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 resultar en daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Marzo 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 ocasionada por las operaciones que no cumplan con el
- manual. El manual se actualizaría 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 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 reciente y la documentación complementaria.
- Todavía puede haber desviaciones en los datos técnicos, las funciones y la descripción de las 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 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 en 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.

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. Adopte la protección
- GND para dispositivos de tipo I.
- 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

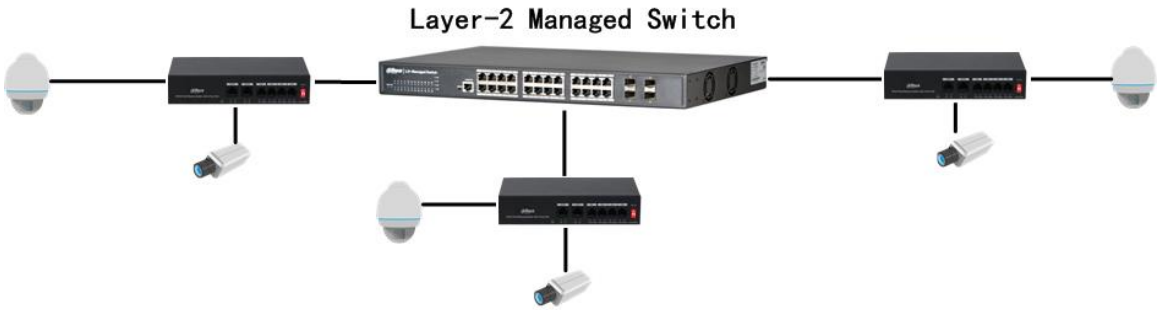
El conmutador Fast Ethernet de 6 puertos con PoE de 4 puertos es un tipo de conmutador comercial de capa 2 que admite la fuente de alimentación Ethernet. Proporciona cuatro puertos Ethernet de 10/100 Mbps y dos puertos de enlace ascendente de 100 Mbps.

1.2 Características

- Conmutador comercial de capa 2.
- Admite los estándares IEEE802.3, IEEE802.3u e IEEE802.3x. Estudio
- automático de MAC y envejecimiento, la capacidad de la dirección MAC es
- de 2K. Admite la autoadaptación MDI / MDIX.
- El puerto RJ45 admite la autoadaptación de 10/100 Mbps y admite los estándares de fuente de alimentación IEEE802.3af e IEEE802.3at.
- Adopta carcasa de metal.
- Admite fuente de alimentación de CA de 100 V-240 V.

1.3 Aplicación típica

Figura 1-1 Escena típica de redes



2 Estructura del dispositivo

2.1 Panel frontal

Figura 2-1 Panel frontal

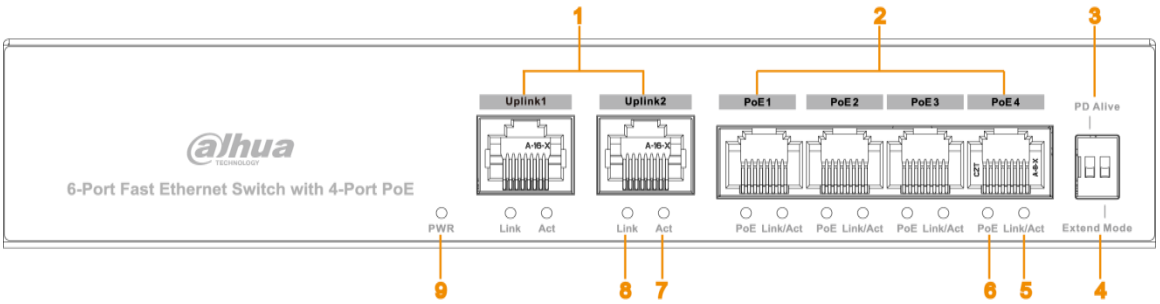


Tabla 2-1 Descripción del panel frontal

SN	Nombre	Descripción
1	Uplink1 – Uplink2	10/100 Base-T, dos puertos de enlace ascendente autoadaptables de 10/100 Mbps.
2	PoE1 – PoE4	10/100 Base-T, cuatro puertos de fuente de alimentación PoE autoadaptables de 10/100 Mbps.
3	PD Alive	Cuando PD Alive está activado, IPC se puede mantener vivo.
4	Modo extendido	En el modo extendido, los datos se pueden transmitir hasta 250 m en un cable CAT6 con un ancho de banda de 10 M.
5	Enlace / acto	Indicador de estado de enlace de puerto único.
6	PoE	Indicador de estado PoE de puerto único.
7	actuar	Indicador de estado de transmisión de datos del puerto de enlace ascendente. Indicador
8	Enlace	de estado de enlace del puerto de enlace ascendente.
9	PWR	Indicador de encendido.

2.2 Panel trasero

Figura 2-2 Panel trasero

Tabla 2-2 Descripción del panel trasero

Nombre	Descripción
PWR	Puerto de alimentación. Admite entrada de alimentación de CA de 100 V-240 V.
⏚	GND.
	El interruptor de bloqueo.

2.3 Fuente de alimentación PoE

Cuatro puertos RJ45 de 100 M admiten la fuente de alimentación estándar IEEE802.3af e 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 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 incluya 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 y gabinete especiales, 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 la información de restablecimiento de contraseñas oportunamente

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. Habilite el 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. Habilite HTTPS

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

7. Habilite la 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. Desactive 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.

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 cifrada provocará una pérdida en la eficiencia de la 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 usar 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.
- Se recomienda que habilite el firewall de su dispositivo o la función de lista negra y lista blanca para reducir el riesgo de que su dispositivo sea atacado.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

Zhejiang Dahua Vision Technology Co., Ltd | Address: No.1199 Bin an Road, Binjiang District, Hangzhou, PRC. | Tel: +86-571-87688883
Website: www.dahuasecurity.com | Fax: +86-571-87688815 | Email: overseas@dahuatech.com | Postcode: 310053