Conmutador Fast Ethernet de 10 puertos con PoE de 8 puertos

Manual de usuario

ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO., LTD. V1.0.1

Prefacio

General

Este manual presenta las características y la estructura del conmutador Fast Ethernet de 10 puertos con PoE de 8 puertos (en adelante, "el Dispositivo").

Modelos

DH-PFS3010-8ET-65

Instrucciones de seguridad

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

Palabras de advertencia	Significado
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 provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Dirección de la empresa modificada.	agosto 2023
V1.0.0	Primer lanzamiento.	marzo 2020

Acerca del Manual

- El manual es sólo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por operaciones 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 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, el

Prevalecerá la versión electrónica.

- Todos los diseños y 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. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Aún así puede haber desviaciones en los datos técnicos, funciones y descripción de operaciones, o errores de impresión. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema al usar el dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

El manual le ayuda a utilizar nuestro producto correctamente. Para evitar peligros y daños a la propiedad, lea atentamente el manual antes de utilizar el producto y le recomendamos encarecidamente que lo conserve para consultarlo en el futuro.

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 instalación horizontal e instálelo en una superficie sólida y plana para evitar que se caiga.
- Evite salpicaduras de líquido sobre 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 con voltaje 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 fuente de alimentación

- Utilice la batería correctamente para evitar incendios, explosiones y otros peligros.
- Reemplace la batería con una batería 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 una fuente de alimentación que cumpla con la fuente de alimentación limitada, según IEC60950-1. Consulte la etiqueta del dispositivo.
- Adopte protección GND para dispositivos 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 10 puertos con PoE de 8 puertos es un tipo de conmutador comercial de capa 2 que admite fuente de alimentación Ethernet. Proporciona ocho puertos Ethernet de 10/100 Mbps y dos puertos de enlace ascendente de 100 Mbps.

1.2 Características

- Switch comercial de capa 2.
- Soporta 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 autoadaptación de 10/100 Mbps y admite los estándares de fuente de alimentación IEEE802.3af e IEEE802.3at.
- Adopta carcasa metálica. Admite fuente de
- alimentación de CA de 100 V-240 V.

1.3 Aplicación tipica

Figure 1-1 Escena típica de networking

2 Estructura del dispositivo

2.1 Panel frontal

Figure 2-1 Panel frontal

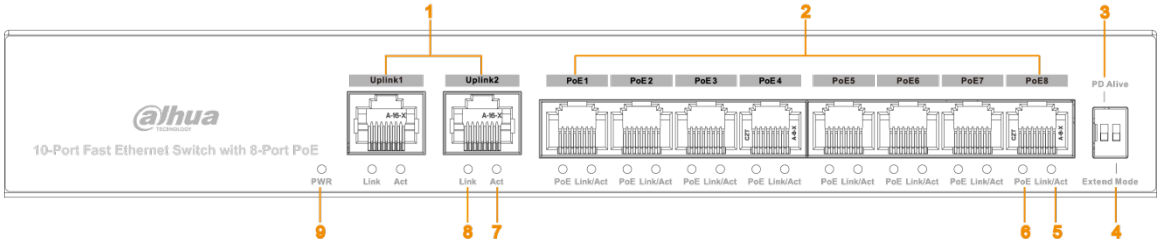

Tabla 2-1 Descripción del panel frontal

SN	Nombre	Descripción
1	Enlace ascendente1–Enlace ascendente2	10/100 Base-T, dos puertos de enlace ascendente autoadaptativos de 10/100 Mbps.
2	PoE1–PoE8	10/100 Base-T, ocho puertos de fuente de alimentación PoE autoadaptativos de 10/100 Mbps.
3	PD vivo	Cuando PD Alive está activado, IPC se puede mantener vivo.
4	Modo extendido	En modo extendido, los datos se pueden transmitir hasta 250 m en cable CAT6 con un ancho de banda de 10 M.
5	Enlace/Actuar	Indicador de estado de enlace de un solo puerto.
6	PoE	Indicador de estado PoE de un solo puerto.
7	Acto	Indicador de estado de transmisión de datos del puerto de enlace ascendente.
8	Enlace	Indicador de estado del enlace del puerto de enlace ascendente.
9	PWR	Indicador de encendido.

2.2 Panel trasero

Figure 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.
⏚	Tierra.
	El interruptor de bloqueo.

2.3 Fuente de alimentación PoE

Ocho puertos RJ45 de 100M admiten fuente de alimentación estándar IEEE802.3af e IEEE802.3at.

Appendix 1 Recomendaciones de ciberseguridad

1 La ciberseguridad es más que una simple palabra de moda: es algo que pertenece a todos los dispositivos que se utilizan. conectado 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 presentan algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

2 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 incluya 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 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 “verificación automática 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.

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

1. Protección física

Le sugerimos que realice protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales, e implemente permisos de control de acceso y administración de claves bien hechos para evitar que personal no autorizado lleve a cabo contactos físicos, como daños en el hardware, conexión no autorizada de un dispositivo extraíble (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 que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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 preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie 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. Habilite HTTPS

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

7. Vinculación de direcciones 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. Asigne cuentas y privilegios de manera 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 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 cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión cifrada de audio y vídeo

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada 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 la transmisión.

11. Auditoría segura

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique 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 habilitar la función de registro de red para garantizar 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:

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según 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.

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

Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para obtener anuncios de seguridad y las últimas recomendaciones de seguridad.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188