Conmutador PoE administrado Gigabit de 16/24 puertos

Guía de inicio rápido

V1.0.2

Prefacio

General

Este manual presenta las funciones y operaciones del conmutador PoE administrado Gigabit de 16/24 puertos (en adelante, "el Dispositivo").

Instrucciones de seguridad

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

Palabras de advertencia	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, menor rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
NOTE	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.2	Funciones actualizadas.	agosto 2023
V1.0.1	Se actualizaron "1.1 Introducción del producto" y "1.2 Características del producto".	noviembre 2020
V1.0.0	Primer lanzamiento.	septiembre 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, 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.
- Desconecte primero la fuente de alimentación para evitar lesiones personales al retirar el cable.
- El estabilizador de voltaje y el pararrayos son opcionales según la fuente de alimentación del sitio y el entorno circundante.

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.
- Asegúrese de conectar a tierra el dispositivo (conéctelo con un cable de cobre cuya sección transversal no sea inferior a 2,5 mm^2 y la resistencia a tierra sea inferior o igual a 4Ω).

Precaución con la batería

- No ingiera la batería para evitar el riesgo de quemaduras químicas.
- Este producto contiene una batería de tipo botón. Si se ingiere la batería de tipo botón, puede provocar graves quemaduras internas en tan solo 2 horas y provocar la muerte.
- Mantenga las baterías nuevas y usadas fuera del alcance de los niños.
- Si el compartimento de la batería no cierra de forma segura, deje de usar el producto y manténgalo alejado de los niños.
- Si cree que las pilas pueden haber sido ingeridas o colocadas dentro de cualquier parte del cuerpo, busque atención médica inmediata.
- Riesgo de explosión si la batería se reemplaza por un tipo incorrecto.

- No tirar ni sumergir en agua, calentar a más de 100°C.(212°F），reparar o desmontar, dejar en un ambiente de presión de aire extremadamente baja o de temperatura extremadamente alta, aplastar, perforar, cortar o incinerar.
- Deseche la batería según lo exigen las ordenanzas o regulaciones locales.

Tabla de contenido

1.1 Introducción del producto

El conmutador PoE gestionado Gigabit de 16/24 puertos está diseñado y desarrollado para aplicaciones de transmisión de campo de vídeo de alta definición. El producto está equipado con un motor de conmutación de alto rendimiento y un buffer grande, que presenta un bajo retardo de transmisión y una alta confiabilidad.

Con un diseño de carcasa totalmente metálica sólida y sellada, el producto tiene un bajo consumo de energía. Con un ventilador en su interior que mejora la alta eficiencia de disipación de calor superficial, el producto puede funcionar en ambientes de -10 °C a 55 °C. Y la protección contra sobrecorriente, sobretensión y EMC del extremo de entrada de energía puede resistir eficazmente la interferencia de la electricidad estática, los rayos y los pulsos.

El producto posee una potente función de gestión de red. El sistema de administración de red admite iLinksView, CLI, web y software de administración de red basado en SNMP.

1.2 Características del producto

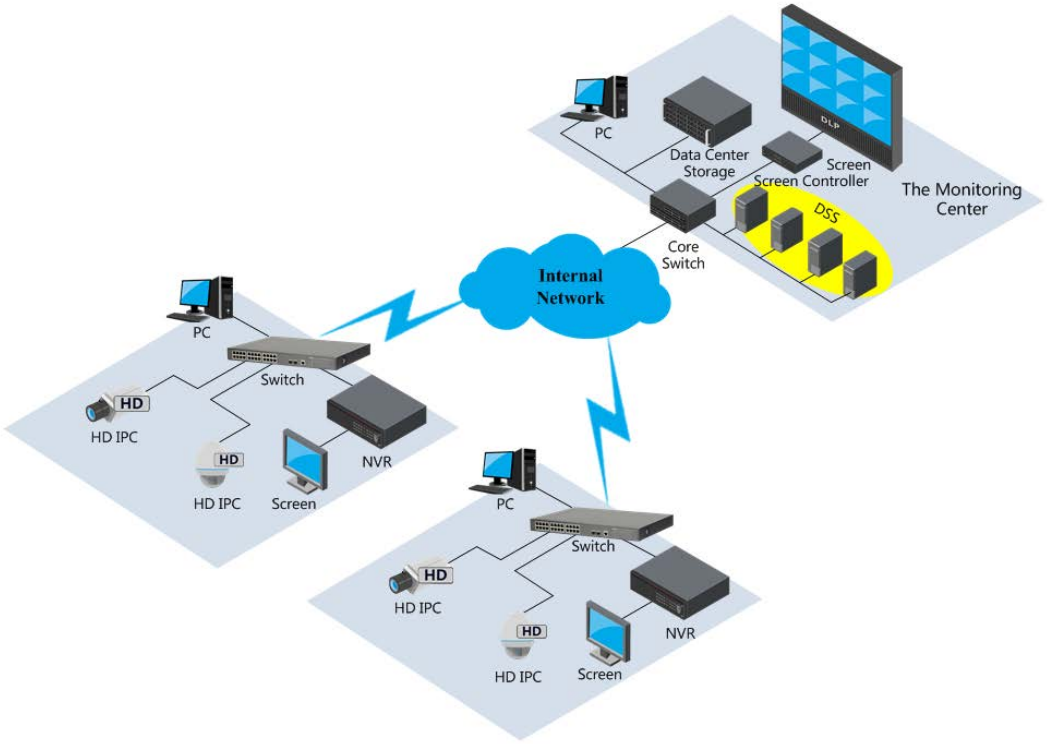
- Switch PoE de gestión de red de capa 2.
- Admite el estándar IEEE802.3af, IEEE802.3at.
- El puerto 1 y el puerto 2 admiten IEEE802.3bt y son compatibles con Hi-PoE.
- Redundancia de red: STP/RSTP/MSTP.
- Admite IPv4/IPv6 y DHCP.
- Gestión de red basada en SNMP.
- Configuración: consola web, Telnet, comando CLI.
- QoS (IEEE802.1p/1Q), CoS/ToS para aumentar el determinismo.
- Seguridad de red mejorada con IEEE802.1X, SNMP v1/v2c/v3, HTTPS y SSH.
- Gran búfer de datos de hasta 4 MB, transmisión en tiempo real.
- Estudio automático y envejecimiento de MAC, la capacidad de la lista de direcciones MAC es de 8K.
- Modo PD activo (vigilancia PoE).
- Modo de transmisión de larga distancia de 250 m.

  En modo extendido, la distancia de transmisión del puerto PoE es de hasta 250 m, pero la transmisión La velocidad cae a 10 Mbps. La distancia de transmisión real puede variar debido al consumo de energía de dispositivos conectados o el tipo y estado del cable.
- Diseño de alta protección EMC.

1.3 Aplicación típica

Tomamos el conmutador PoE administrado Gigabit de 24 puertos como ejemplo para presentar la escena de red típica.

Figura 1-1 Redes



2 Estructura del dispositivo

2.1 Panel frontal

Conmutador PoE administrado Gigabit de 16 puertos

Figura 2-1 Panel frontal

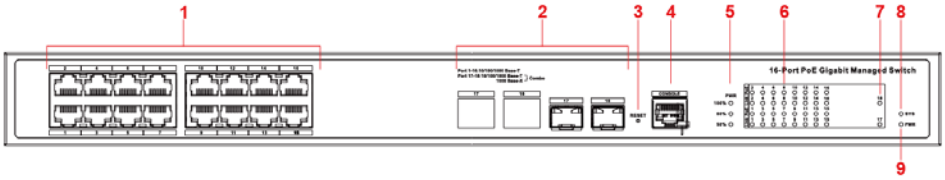


Tabla 2-1 Descripción del panel frontal

No.	Nombre	Descripción
1	Puerto RJ45	Puerto Ethernet, admite 10/100/1000 Mbps autoadaptativo.
2	Puerto combinado	2 puertos Ethernet, admiten autoadaptación de 10/100/1000 Mbps; 2 puertos ópticos, soporta 1000 Mbps autoadaptativos.
3	Botón de reinicio	Mantenga presionado el botón durante 5 s para restablecer el dispositivo y recuperar la configuración predeterminada.
4	Puerto serie de la consola	Puerto de depuración del dispositivo.
5	Uso de energía PoE indicador	Visualización del consumo de energía actual.
6	Indicador de enlace descendente	Estado actual del enlace del puerto y estado de PoE.
7	Indicador de puerto de enlace ascendente	Indicador de enlace/actuación.
8	Indicador del sistema	Estado del sistema: ● Cuando el dispositivo se inicia, la luz parpadea rápidamente. ● Cuando el dispositivo funciona correctamente, la luz parpadea lentamente.
9	Indicador de encendido	Estado de energía actual del dispositivo.

Conmutador PoE gestionado Gigabit de 24 puertos

Figura 2-2 Panel frontal

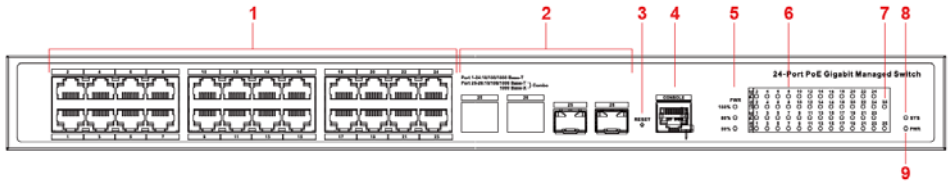


Tabla 2-2 Descripción del panel frontal

No.	Nombre	Descripción
1	Puerto RJ45	Puerto Ethernet, admite 10/100/1000 Mbps autoadaptativo.
2	Puerto combinado	2 puertos Ethernet, admiten autoadaptación de 10/100/1000 Mbps; 2 puertos ópticos, soporta 1000 Mbps autoadaptativos.

No.	Nombre	Descripción
3	Botón de reinicio	Mantenga presionado el botón durante 5 s para restablecer el dispositivo y recuperar la configuración predeterminada.
4	Puerto serie de la consola	Puerto de depuración del dispositivo.
5	Uso de energía PoE indicador	Visualización del consumo de energía actual.
6	Indicador de enlace descendente	Estado actual del enlace del puerto y estado de PoE.
7	Indicador de puerto de enlace ascendente	Indicador de enlace/actuación.
8	Indicador del sistema	Estado del sistema: ● Cuando el dispositivo se inicia, la luz parpadea rápidamente. ● Cuando el dispositivo funciona correctamente, la luz parpadea lentamente.
9	Indicador de encendido	Estado de energía actual del dispositivo.

2.2 Panel trasero

Figura 2-3 Panel trasero

Tabla 2-3 Descripción del panel trasero

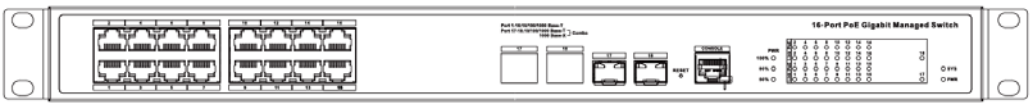
No.	Nombre	Descripción
1	Interruptor de alimentación	Encienda o apague el dispositivo.
2	Toma de corriente	Soporta 100-240 VCA.
3	Terminal de tierra	Tierra.

3 Instalación

3.1 Instalación del dispositivo

El dispositivo admite montaje en bastidor estándar. Instale el kit de montaje en bastidor en ambos lados del conmutador.

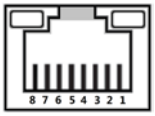
Figura 3-1 Montaje en bastidor



3.2 Cableado

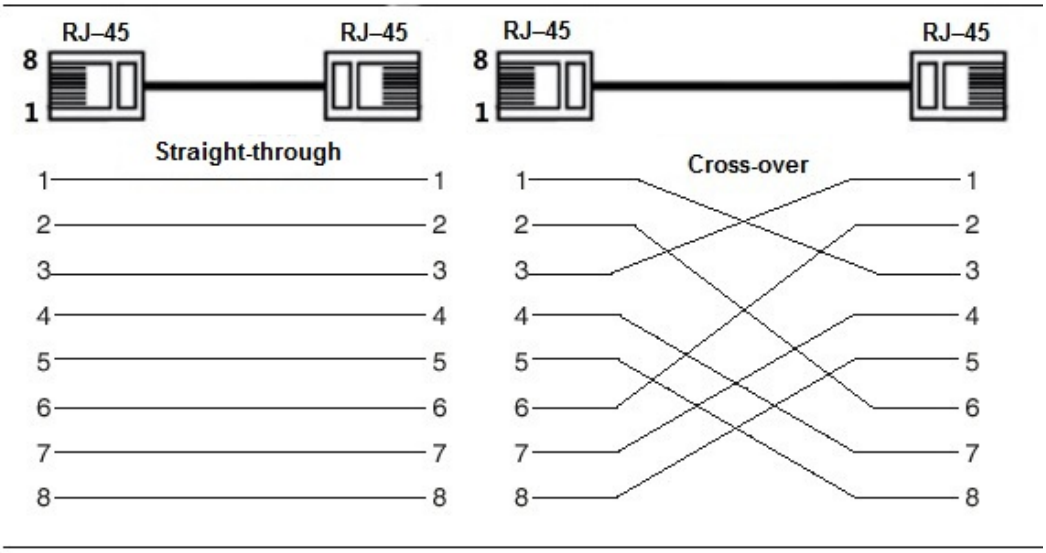
3.2.1 Puerto Ethernet

Figura 3-2 Número de pin del puerto Ethernet



El puerto Ethernet Base-T de 10/100/1000 Mbps adopta el puerto RJ45 estándar. Equipado con función de autoadaptación, se puede configurar automáticamente en modo de operación full duplex/half-duplex y admite la función de autorreconocimiento MDI/MDI-X del cable, lo que significa que el interruptor puede usar cable cruzado o recto. -a través de cable para conectar el dispositivo terminal al dispositivo de red.

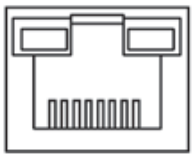
Figura 3-3 Descripción de pines



La conexión del cable del conector RJ45 se ajusta al estándar 568B (1 naranja blanco, 2 naranja, 3 verde blanco, 4 azul, 5 azul blanco, 6 verde, 7 marrón blanco, 8 marrón).

3.2.2 Puerto de consola

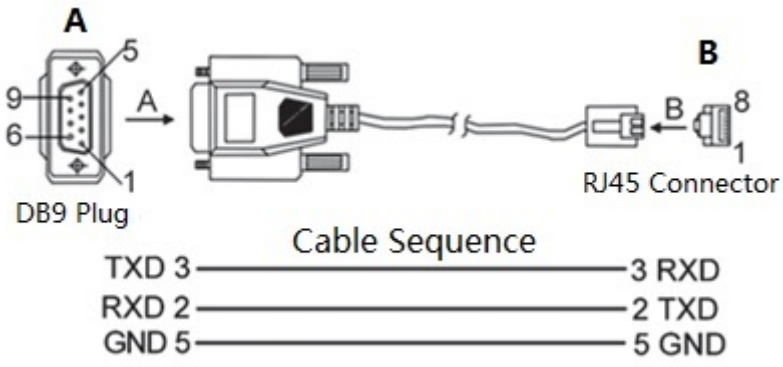
Figura 3-4 Puerto de consola



Consulte la Figura 3-4 para ver el puerto de la consola. El puerto de la consola del conmutador y el puerto serie de 9 pines que controla la computadora están conectados con un cable RJ-45-DB9. Puede llamar al software de la consola del dispositivo operando el software de superterminal del sistema Windows para la configuración, el mantenimiento y la administración del dispositivo.

Consulte la Figura 3-5 para ver la secuencia de cables de RJ-45-DB9.

Figura 3-5 Secuencia de cables de RJ45 DB9



Un extremo del cable RJ45 DB9 es un conector RJ45, que debe insertarse en el puerto de consola del dispositivo. Y el otro extremo es el conector DB9, que debe insertarse en la computadora que controla el puerto serie de 9 pines.

Tabla 3-1 Descripción de pines

clavija DB9	clavija RJ45	Señal	Descripción
2	3	RXD	Recibiendo información
3	2	TXD	Enviando datos
5	5	Tierra	Tierra

3.2.3 Puerto SFP

La señal se transmite a través de láser mediante cable de fibra óptica. El láser cumple con los requisitos. de productos láser de nivel 1. Para evitar lesiones en los ojos, no mire directamente al puerto óptico 1000 Base-X. cuando el dispositivo está encendido.

Figura 3-6 Estructura del módulo SFP

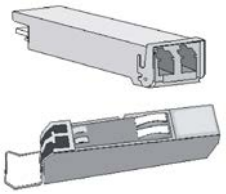
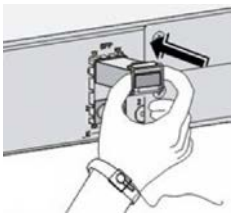


Figura 3-7 Instalación del módulo SFP



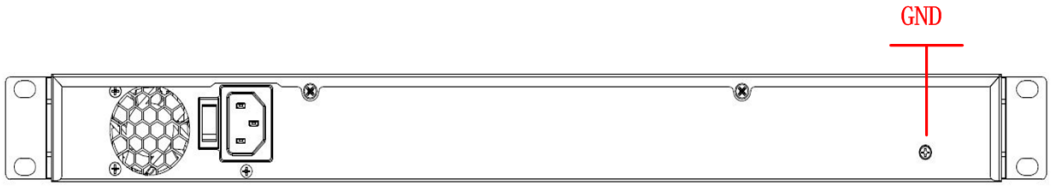
Instalación del puerto SFP

Antes de instalar el módulo SFP, use guantes antiestáticos y luego use una muñequera antiestática. Asegúrese de que los guantes antiestáticos y la muñequera antiestática estén en buen contacto.

1. Levante la manija del módulo SFP verticalmente y péguela al gancho superior.
2. Sostenga el módulo SFP por ambos lados y empújelo suavemente dentro de la ranura SFP hasta que esté firmemente conectado a la ranura (tanto la tira de resorte superior como la inferior del módulo SFP están firmemente pegadas a la ranura SFP).

3.2.4 TIERRA

Figura 3-8 Terminal GND



La GND normal del dispositivo es una garantía importante para la protección contra rayos y antiinterferencias del dispositivo. Debe conectar el cable GND antes de encender el dispositivo y apagar el dispositivo antes de desconectar el cable GND.

Hay un tornillo GND en la placa de cubierta del dispositivo para el cable GND, que se llama gabinete GND. Conecte un extremo del cable GND con el terminal prensado en frío y fíjelo en el gabinete GND con el tornillo GND. El otro extremo del cable GND debe estar conectado de manera confiable a tierra.

El área de sección del cable GND debe ser superior a 2,5 mm^2 y la resistencia GND debe ser menor. que 4Ω.

4 operaciones rápidas

Presentaremos brevemente la configuración de VLAN en esta sección. Consulte el manual de línea de comando correspondiente para obtener una configuración detallada.

4.1 Primer inicio de sesión por puerto de consola

Es la forma más básica de iniciar sesión en la interfaz local a través del puerto de la consola y también es el método para configurar otras formas de iniciar sesión en el dispositivo.

Paso 1 Apague la computadora.

Paso 2 Utilice el cable del puerto de consola predeterminado para conectar la PC y el dispositivo.

Primero inserte el conector DB (orificio) del cable del puerto de consola en el puerto serie de 9 pines de la PC y luego inserte el conector RJ45 en el puerto de consola del dispositivo.

- Confirme el signo en el puerto durante la conexión, en caso de que pueda conectarse al puerto incorrecto puerto.
- Desconecte RJ45 y luego DB-9 cuando desmonte el cable del puerto de la consola.

Figura 4-1 Iniciar sesión a través del puerto de la consola

Paso 3 Encienda la computadora.

Etapa 4 Ejecute el programa de simulación de terminal en la PC y luego seleccione el puerto serie que conectará el dispositivo y configure los parámetros de comunicación del terminal.

Los siguientes valores de parámetros deben estar de acuerdo con los valores del dispositivo; los valores predeterminados se muestran a continuación.

- Velocidad de transmisión: 115200
- Bits de datos: 8
- Bit de parada: 1
- Paridad: ninguna
- Control de flujo: ninguno

- Si la PC utiliza el sistema operativo Windows Server 2003, agregue super terminal programa en el componente de Windows y luego inicie sesión y administre el dispositivo de acuerdo a la forma presentada en este manual.
- Si la PC usa Windows Server 2008, Windows Vista, Windows 7 u otro sistema operativo sistemas, prepare un software de control de terminal de terceros, consulte el software guía de operación o ayuda en línea para el método de operación.

Paso 5 Después de encender el dispositivo, muestra información de autoverificación del dispositivo en el terminal

software de control, y solicitará a los usuarios que presionen la tecla Intro después de la autoverificación, luego mostrará el mensaje de ingreso de nombre de usuario y contraseña.

Paso 6 Ingrese el nombre de usuario y la contraseña y luego presione Entrar.

El nombre de usuario predeterminado es admin y la contraseña predeterminada es admin.

La siguiente línea de comando (SWITCH#) se muestra después de presionar Enter, lo que significa que el inicio de sesión se ha realizado correctamente.

Ingrese el comando correspondiente y podrá configurar el dispositivo o verificar el estado operativo del dispositivo, y podrá ingresar? en cualquier momento si necesitas ayuda.

```
+ M25PXX: Dispositivo de inicio con JEDEC ID 0xC22018.
Placa Luton10 detectada (VSC7428 Rev. D).

Entorno de arranque y depuración de RedBoot(tm) [ROMRAM] Versión no
certificada, versión 1_31-4752 - compilada a las 17:29:35, 29 de julio de 2017

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot es software libre, amparado por la licencia eCos, derivada de la Licencia Pública
General GNU. Le invitamos a cambiarlo y/o distribuir copias del mismo bajo ciertas
condiciones. Según los términos de la licencia, el código fuente de RedBoot y los
términos completos de la licencia deben haber estado disponibles para usted. Redboot
viene SIN NINGUNA GARANTÍA.

Plataforma: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80028f20-0x87fdfffc disponible]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 bloques
== Ejecutando script de arranque en 3.000 segundos - ingrese Ĉ para cancelar
RedBoot> diag -p
RedBoot> fis load -x linux
Firma MD5 validada
Etapa 1: 0x80100000, longitud 4641272 bytes
Initrd: 0x80600000, longitud 188416 bytes
Línea de comando del kernel: init=/usr/bin/stage2-loader loglevel=4
RedBoot> exec
Ahora arrancando el kernel de Linux:
Dirección base 0x80080000 Entrada 0x80100000 Línea de
comando: init=/usr/bin/stage2-loader loglevel=4
 Fis activo: linux
[       0.374113] vcfw_uio vcfw_uio: carga del controlador UIO
[       0.378957] vcfw_uio vcfw_uio: recurso de memoria no válido
[       0.384141] iounmap: dirección incorrecta (nula)
00:00:00 Etapa 1 arrancada 00:00:00
Usando dispositivo: /dev/mtd7
00:00:01 Montado /dev/mtd7
00:00:01 Cargando etapa 2 desde el archivo NAND 'n6G5Xw'
```

```
00:00:05 Total: 4195 ms, ubifs = 748 ms, rootfs 3422 ms de los cuales xz = 0 ms de los cuales untar = 0 ms

Iniciando aplicación... wuxuwuxu Usando el
punto de montaje existente para /switch/
system time:2017-10-14 17:59:53
W icfg 18:00:22 71/icfg_commit_tftp_load_and_trigger#2695: Advertencia: TFTP obtiene Bringup-config: Se
agotó el tiempo de espera de la operación.

Presione ENTER para comenzar

Nombre de usuario: administrador
Contraseña:
CAMBIAR#
```

Ingrese el comando correspondiente para configurar el dispositivo o verificar el estado operativo del dispositivo. y puedes entrar? en cualquier momento si necesitas ayuda.

4.2 Configuración predeterminada de fábrica del dispositivo

Puede iniciar sesión en la página web del dispositivo a través de la siguiente dirección IP. Se pueden aplicar el nombre de usuario y la contraseña para iniciar sesión en la página web a través del puerto de la consola.

Tabla 4-1 Valores predeterminados de fábrica del dispositivo

Parámetro	Nota
dirección IP	192.168.1.110
Nombre de usuario	administración
Contraseña	

- iLinksView está habilitado de forma predeterminada y el nombre de usuario predeterminado es admin, la contraseña predeterminada es lt_91_il_02_nmp.
- Cuando utilice iLinksView para administrar el dispositivo, tenga en cuenta que el nombre de usuario y la contraseña deben ser el mismo que ha configurado en iLinksView; de lo contrario, iLinksView no puede descubrir el dispositivo.

4.3 Configuración de VLAN

VLAN (red de área local virtual) se utiliza con frecuencia durante la aplicación real; Está dividido internamente en múltiples conceptos básicos de red. VLAN consiste en organizar varios dispositivos en una red de forma lógica, independientemente de la ubicación física de los dispositivos. Cada VLAN es una red lógica, que está equipada con todas las funciones y atributos de la red física tradicional. Cada VLAN es un dominio de difusión; El paquete de transmisión solo se puede reenviar dentro de una VLAN, no a través de la VLAN.

VLAN basada en el puerto

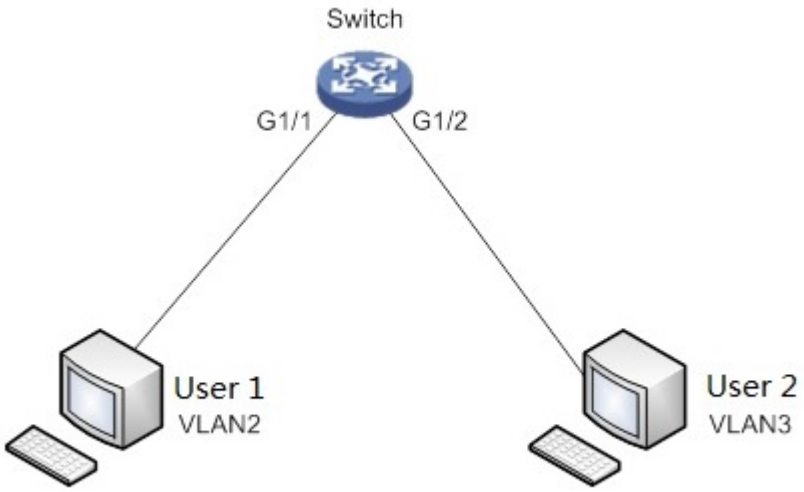
VLAN basada en puerto significa que un conmutador puede realizar la división de grupos de trabajo lógicos mediante el control de la interoperabilidad entre dos y entre varios puertos. Dividir la VLAN del puerto de manera razonable puede mejorar en gran medida la seguridad de la red y el índice de uso del ancho de banda, además de reducir la probabilidad de una tormenta de transmisión. El modelo admite 4094 VLAN; debe seleccionar una ID de VLAN al crear la VLAN, que oscila entre 2 y 4094. El conmutador crea la VLAN1 de forma predeterminada y la VLAN1 no se puede eliminar.

Ejemplo de aplicación

Requisito de red

Hay dos usuarios, el usuario 1 y el usuario 2. Estos dos usuarios deben estar en una VLAN diferente debido a las diferentes funciones y entornos de la red. El usuario 1 pertenece a VLAN2 y se conecta al puerto del switch G1/1 (Gigabit Ethernet 1/1); El usuario 2 pertenece a la VLAN 3 y se conecta al puerto del switch G1/2 (Gigabit Ethernet 1/2).

Figura 4-2 Redes VLAN



Pasos de configuración

La configuración del conmutador se muestra a continuación.

1. Inicie sesión en el dispositivo. Consulte "4.1 Primer inicio de sesión por puerto de consola".

2. Ejecute el siguiente comando para crear VLAN.

```
INTERRUPTOR #configurar terminal
INTERRUPTOR (config)#vlan 2
INTERRUPTOR (config-vlan)# salir
INTERRUPTOR (config)#vlan 3
CAMBIAR (config-vlan) # salir
```

3. Ejecute el siguiente comando para distribuir puertos en la VLAN.

```
SWITCH (config)# interfaz GigabitEthernet 1/1
SWITCH (config-if)# switchport acceso vlan 2
SWITCH (config-if)# salida
SWITCH (config)# interfaz GigabitEthernet 1/2
SWITCH (config-if)# switchport acceso vlan 3
SWITCH (config-if)# salida
```

Apéndice 1 Recomendaciones de ciberseguridad

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

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 contener 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 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 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.

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 oportunamente**

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.**Habilitar 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.**Cambiar 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.**Habilitar HTTPS**

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

7.**Enlace 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 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 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.