AXIS T8504-E Outdoor PoE Switch

Manual del usuario

Índice

Acerca de este manual 3
Objetivos 3
Destinatarios 3
Documentación relacionada 3
Abreviaturas 3
Información general 5
Características 5
Acceso de usuarios y seguridad 5
Primera configuración 8
Identificación de unidad a través de red IP 8
Interfaz web 10
Menú de interfaz web 10
Interfaz de serie SSH 16
Menú principal 16
Supervisión y configuración de SNMP 19
Habilitar SNMP 19
SNMP MIB 19
Mensaje de SysLog 21
Solución de problemas 23
Soporte 23
Más información 24

Acerca de este manual

Acerca de este manual

Objetivos

AXIS T8504–E es un Switch PoE exterior. Las principales ventajas de este producto son sus capacidades para exteriores y la capacidad de ampliar el alcance máximo de la red hasta 100 metros adicionales, hasta un total de 200 metros, entre el switch y los dispositivos alimentados, y proporcionar hasta 2x60 W y 2x30 W a sus dispositivos PoE alimentados por la red.

En este manual de usuario se proporciona información sobre cómo gestionar AXIS T8504–E a través de AXIS IPv4/IPv6, VLAN, RADIUS, TACACS+, interfaz web, SNMP y SHH.

Destinatarios

Este manual de usuario está diseñado para administradores de red, supervisores y técnicos de instalación con conocimientos sobre:

- Conceptos básicos y terminología de redes
- Topología de red con VLAN
- Protocolos de red
- Protocolos de autenticación de usuario, incluidos RADIUS y TACACS+

Documentación relacionada

Para obtener más información, consulte la siguiente documentación:

- Guía de instalación de producto
- RFC3621 SNMP MIB y MIB privado
- Crear certificado para servidor web protegido T8504–E

Abreviaturas

Abreviatura	Description (Descripción)
8021.Q	Igual que la VLAN
DES	Estándar de cifrado de datos
DGW	Puerta de enlace predeterminada
DHCPv4	Protocolo de configuración dinámica de host IPv4
DHCPv6	Protocolo de configuración dinámica de host IPv46
IPv4	Dirección IP larga de 32 bits
IPv6	Dirección IP larga de 128 bits
MD5	Algoritmo Digest de mensaje
MDI	Interfaz en función de los medios
MIB	Base de información de gestión
PoE	Alimentación a través de Ethernet
RADIUS	Servicio de usuario de acceso telefónico de autenticación remota
SFP	Interfaz de fibra, enchufe de pequeño tamaño

Acerca de este manual

SHA	Algoritmo Digest de mensaje
SNMP	Protocolo de administración de la red simple
SSH	Shell seguro
SSL	Capa de conexión segura
SysLog	Registro del sistema
TACACS+	Control de acceso al controlador de acceso del terminal
TFTP	Protocolo de transferencia de archivos insignificante
TLS	Seguridad de la capa de transporte
VLAN	Red de área local virtual

Información general

Información general

Características

A través de la gestión de la red del sistema se proporcionan diversas características.

- Sencilla actualización de software durante el tiempo de ejecución sin afectar a los puertos PoE activos
- Configuración y supervisión en tiempo real mediante la representación gráfica del dispositivo remoto
- Visualización de estado del sistema
- Informes de SysLog sobre eventos PoE, acceso de usuario remoto no válido, dirección DHCPv4/v6 inicial, etc.
- Traps SNMP que informan de varios eventos PoE, tales como dispositivo alimentado por PoE, de extracción o desmontaje

Capacidades de red del switch Ethernet

- Cuatro puertos Ethernet RJ45 herméticos con capacidad de 10 Mbit, 100 Mbit, semidúplex de 1000 Mbit y velocidad Ethernet full-duplex de 1000 Mbit
- Puerto Ethernet SFP hermético único
- Motor de comisión de direcciones MAC internas 8K
- VLAN: acceso, tronco y tronco filtrado
- Auto MDIX
- Imágenes Jumbo de 10KB

Capacidades de PoE

Están disponibles las siguientes opciones de PoE:

- **Dos puertos PoE 4Pair** que ofrecen hasta 60 W por puerto
- **Dos puertos PoE IEEE 802.3at** que ofrecen hasta 30 W por puerto
- **Habilitar/deshabilitar PoE** para habilitar o deshabilitar la salida de alimentación de los puertos PoE. Los datos de Ethernet siempre están habilitados.
- **Restablecimiento del dispositivo remoto** para restablecer el dispositivo alimentado conectado. El dispositivo se apaga temporalmente y, a continuación, se vuelve a encender.

Protocolos de red compatibles

Los siguientes protocolos de red son compatibles:

- **IPv4**: dirección IP larga de 32 bits (estática/DHCPv4)
- **IPv6**: dirección IP larga de 128 bits (estática/DHCPv6)
- **VLAN**: acceso, tronco y tronco filtrado

Acceso de usuarios y seguridad

Opciones de acceso

Puede acceder a la unidad a través de distintas interfaces:

Información general

- **Interfaz web a través de un navegador web**: para consultar el estado de PoE de la unidad, el estado de la red, la configuración de la unidad y la información de producción de la unidad

  HTTP es una interfaz de configuración sencilla basada en web.

  HTTPS-TLS es una interfaz de configuración sencilla y segura basada en web.

- **SNMP a través de una aplicación de administrador de SNMP**: para supervisar la unidad a través de la red (MIB-II RFC1213) y para supervisar o configurar las capacidades de PoE de la unidad (RFC3621)

  SNMPv2c para la gestión de SNMP no segura

  SNMPv3 para una gestión segura y cifrada

  RFC1213 MIB-II para estadísticas de red

  RFC3621 para PoE SNMP MIB

  Extensión de MIB privada para RFC3621 PoE MIB

  Varias infraestructuras y MIB de red tales como IP-MIB, TCP-MIB, UDP-MIB, etc.

- **SSH a través de un cliente SSH**: para consultar el informe de alimentación de PoE de la unidad, el estado de la red, la configuración de la unidad y la información de producción; para actualizar el software, habilitar o deshabilitar la funcionalidad PoE y para hacer ping a dispositivos de red remotos para pruebas de conectividad

Autenticación del usuario remoto

El acceso de los usuarios se puede administrar de las siguientes maneras:

- **Local**: el dispositivo administra el nombre de usuario y la contraseña de forma local
- **RADIUS**: el servidor RADIUS a través de la red autentica el nombre de usuario y la contraseña
- **TACACS+**: el servidor TACACS+ a través de la red autentica el nombre de usuario y la contraseña

Protocolos de seguridad

HTTP web y HTTPS, SNMPv2, SNMPv3 y SSH, utilizados para acceder a la unidad, ofrecen distintos niveles de seguridad. Además, RADIUS y TACACS+, usados para la autenticación de usuario remoto, ofrecen distintos niveles de seguridad.

SNMPv1 y SNMPv2 utilizan cadena de comunidad para la autenticación Get/Set/Trap. SNMPv1 y SNMPv2 se consideran protocolo no seguro, ya que cualquier dispositivo de búsqueda de red puede interceptar la contraseña de la cadena de la comunidad.

SNMPv3 soluciona problemas de seguridad de SNMPv1/v2 agregando una capa de autenticación y cifrado en la parte superior de los paquetes de SNMP.

IP de la unidad, nombre de usuario y contraseña predeterminados

La unidad se suministra con los siguientes nombres de usuario y contraseñas predeterminados de fábrica:

IP de dirección IPv4 predeterminada de la unidad
= 192.168.0.254
máscara = 255.255.255.0

Nombre de usuario de HTTP/HTTPS web y SSH
= Contraseña root
= Buscar la contraseña predeterminada en la etiqueta del dispositivo

SNMPv2
GET community string = public
SET community string = write
Read community = public

Write community = write
Trap community = public

SNMPv3
Username = admin
Authentication password (MD5) = password
Privacy password (DES) = password
Authentication and encryption mode = MD5+DES

SNMPv3 notification
Username = trap
Authentication password = password
Privacy password = password
Authentication and encryption mode = None

Para obtener información sobre cómo recuperar el nombre de usuario y la contraseña, consulte *Recuperación de nombre de usuario y contraseña en la página 7*.

Recuperación de nombre de usuario y contraseña

Nota

El procedimiento de recuperación solo se puede realizar desde la red LAN local y no a través de Internet o desde otra red de IP. El usuario debe poder apagar la alimentación de la unidad cuando sea necesario. Todos los puertos PoE deben estar desconectados y la unidad solo debe tener un único enlace Ethernet activo.

Nota

Es posible que tenga que agregar un servicio de cliente Telnet a Windows 7 o Windows 8.

Nota

Todo el procedimiento de recuperación de la unidad que se ha encendido hasta que se aplique el nombre de usuario y la contraseña debe tardar menos de 120 segundos.

1. Desconecte todos los puertos PoE de la unidad excepto un cable Ethernet. Solo debe estar activo un único puerto Ethernet.
2. Desactive el cortafuegos o habilite el puerto UDP 514. A continuación, ejecute el servidor SysLog IPv4 compatible en el ordenador.
3. Apague la unidad. Espere 10 segundos y vuelva a encender la unidad.
4. Después de 15 segundos aproximadamente aparece un mensaje de SysLog. Identifique la dirección IPv6 de enlace local de la unidad. La dirección IPv6 de enlace local siempre empieza con FE80.
5. Abra una ventana de comandos en su ordenador.
   - En Windows 7, vaya a **Start (Inicio)** y escriba **cmd**.
   - Para Windows 8, pulse la tecla WINDOWS y la tecla R, a continuación, escriba **cmd**.
6. Escriba **ipconfig** para identificar el índice de la interfaz virtual de la dirección IPv6 de enlace local. El índice de la interfaz virtual se indica mediante un número después de %. Ejemplo: fe80::9c39:db8b:62de:7bv4%**17**
7. Prepare la conexión SSH escribiendo **Telnet** [unit Local-link IPv6 address][%virtual interface number] **2525**, pero no presione INTRO. Ejemplo: **Telnet fe80::9c39:db8b:62de:7bv4%17 2525**
8. Apague la unidad. Espere 10 segundos y vuelva a encender la unidad.
9. Espere 30 segundos y, a continuación, presione INTRO para iniciar la sesión Telnet en el puerto TCP 2525.
10. Escriba **axispasswordrecovery** como nombre de usuario y **axispasswordrecovery** como contraseña. Se muestra una opción de recuperación para restaurar toda la unidad a los valores predeterminados de fábrica, incluida la configuración de red de la unidad.

11. Presione Y para restaurar la unidad. La unidad se reinicia con la IPv4 192.168.0.254 predeterminada, escriba **root** como nombre de usuario y utilice la contraseña predeterminada impresa en la etiqueta del dispositivo.

Primera configuración

Al configurar la unidad por primera vez, siga estos pasos:

1. Configure la interfaz de red Ethernet para PC con los siguientes parámetros IPv4:

   Dirección IPv4 para PC: 192.168.0.40

   Máscara IPv4 para PC: 255.255.255.0

2. Conecte la interfaz de red Ethernet del PC a cualquiera de los puertos Ethernet de la unidad.
3. Abra un navegador web y escriba 192.168.0.254 en el campo de dirección.
4. Inicie sesión con el nombre de usuario y la contraseña predeterminados. Vea *IP de la unidad, nombre de usuario y contraseña predeterminados en la página 6*.
5. Configure la unidad. Se recomienda cambiar los nombres de usuario y las contraseñas por otros valores diferentes a los valores predeterminados.

Identificación de unidad a través de red IP

Para localizar la unidad a través de la red IP, la unidad envía un mensaje IPv4 SysLog n.º 0 en formato de retransmisión 255.255.255.255 encendido. Cualquier servidor SysLog conectado a través de LAN recibe este mensaje de SysLog. El mismo mensaje de SysLog se envía también a los servidores 1 y 2 de SysLog opcionales, si están configurados.

La unidad envía el mensaje dos veces. De este modo se garantiza que los servidores de SysLog reciben este mensaje de SysLog, independientemente de la configuración de red. El mensaje se envía primero antes de que se haga la configuración de VLAN y, posteriormente, de nuevo una vez que se haya realizado la configuración de VLAN.

El mensaje n.º 0 de SysLog contiene toda la información necesaria para poder acceder a la unidad a través de la red.

Ejemplo: `MsgID#000: Sistema UP. APP:v3.51.06 BOOT:v3.16 RST:Power-On BOOT:0=[APP OK] Host:axis-00055A034B49 MAC:00:05:5a:03:4b:49 VLAN:YES VLAN_MNGR:5 VLAN_UPLINK_PORT:3 VLAN_UPLINK_MODE:TRUNK DHCPv4:No IP1v4:192.168.0.254/24 DHCPv6:No IP1v6:2345::205:5AFF:FE03:4B49/64 IP2v6:FE80::205:5AFF:FE03:4B49/64`

Campo	Valor	Description (Descripción)
`MsgID#000: Sistema UP`		Numeración de mensajes de SysLog
`APP:`	`v3.51.06`	Versión del software de aplicación de la unidad
`ARRANQUE:`	`v3.16`	Versión de arranque de la unidad, utilizada para la actualización del software
`RST:`	`Encendido`	Razón para restablecer
`ARRANQUE:`	`0=[APP OK]`	
`Host:`	`axis-00055A034B49`	Axis seguido por la dirección MAC de la unidad
`MAC:`	`00:05:5a:03:4b:49`	Dirección MAC de la unidad
`VLAN:`	`SÍ`	Estado de VLAN habilitado o deshabilitado
`VLAN_UPLINK_PORT:`	`3`	Número de puerto Ethernet utilizado para la gestión de unidades

Información general

VLAN_UPLINK_MODE:	TRONCAL	El puerto de gestión se configura como acceso o tronco
DHCPv4:	No	DHCPv4 Sí o No
IP1v4:	192.168.0.254/24	Dirección IPv4 de la unidad
DHCPv6:	No	DHCPv6 Sí o No
IP1v6:	2345::205:5AFF:FE03:4B49/64	Dirección IPv6 de la unidad
IP2v6:	FE80::205:5AFF:FE03:4B49/64	Dirección IPv6 de enlace de unidad local

Interfaz web

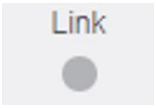
Menú de interfaz web

Status (Estado)

Vaya a **Status (Estado)** para ver el estado de la unidad. La página se actualiza automáticamente cada pocos segundos.

Nota

El enlace de red Ethernet siempre está habilitado, independientemente de la configuración de PoE (habilitada o deshabilitada).

Parámetro	Description (Descripción)
	Símbolo azul: se proporciona alimentación PoE Símbolo gris: sin alimentación PoE
	Símbolo azul: el puerto PoE está habilitado Símbolo gris: el puerto PoE está deshabilitado
	Símbolo azul: el enlace Ethernet está activado Símbolo gris: sin enlace Ethernet
	Símbolo azul: el módulo SFP se inserta en el puerto de uplink Símbolo gris: el puerto de uplink no tiene ningún módulo SFP insertado
Red	Informa de la velocidad de enlace Ethernet (10/100/1000 MB) y si la conexión de red está arriba o abajo
Status (Estado)	Indica el estado del puerto PoE si está habilitado, deshabilitado, con suministro eléctrico, etc.
Energía necesaria	Indica el consumo de energía real y la potencia máxima que puede proporcionar
Restablecimiento de PoE	Haga clic en **Reset (Restablecer)** para apagar la alimentación del puerto PoE y restablecer la alimentación de PoE. Nota Un puerto PoE deshabilitado por SSH o SNMP se habilitará después de un restablecimiento de PoE.
Consumo total de energía	Indica el consumo de energía agregado de todos los puertos PoE y el porcentaje de potencia consumida en relación con las capacidades de alimentación de la fuente de alimentación interna.

Básico

Vaya a **Basic (Básico)** para consultar la información básica sobre el producto.

Dirección IP en uso – Vaya a **IP address in use (dirección IP en uso)** para ver información sobre direcciones IPv4 e IPv6, máscaras, puertas de enlace predeterminadas y servidores de nombres de dominio (DNS).

Información de producto – Vaya a **Product information (Información del producto)** para ver la información general del producto como el nombre del producto, el número de serie, la versión del software y la versión del firmware de PoE, así como la información del módulo SFP, como el tipo de SFP, el proveedor, el número de pieza y el número de serie.

Configuración de red – Vaya a **Network configuration (Configuración de red)** para habilitar o deshabilitar DHCP, configurar IPv4, IPv6 y nombre de host de red. IPv4 e IPv6 utilizan el nombre de host para registrar el nombre de la unidad en el servidor DHCPv4/v6. Tenga en cuenta que IPv6 utiliza la terminología de FQDN como nombre de host.

IPv4/IPv6 de servicios de red – Vaya a **Network services IPv4/IPv6 (IPv4/IPv6 de servicios de red)** para configurar DNS y servidores de SysLog.

Configuración de PoE – Vaya a **PoE configuration (Configuración de PoE)** para configurar la alimentación del puerto PoE. Cuatro esquemas de alimentación de PoE ofrecen distintas distribución de potencia entre los cuatro puertos PoE. Las cuatro opciones cumplen con las capacidades máximas de alimentación de la unidad.

- 60 W: Proporcione alimentación a través de cuatro pares dentro del cable Ethernet. Cada par ofrece hasta 30 W.
- 30 W: Proporcionar alimentación a través de dos de los cuatro pares dentro del cable Ethernet
- 15.4 W: Proporcionar alimentación a través de dos de los cuatro pares dentro del cable Ethernet
- – –: Sin alimentación PoE. El puerto Ethernet está habilitado y funciona, pero PoE está deshabilitado.

Seguridad

Configuración de seguridad

Vaya a **Security configuration (Configuración de seguridad)** para configurar el nombre de usuario y la contraseña de la unidad para el acceso web o SSH remotos.

Nota

Solo se pueden utilizar caracteres ASCII 33–90 y 94–122 para los campos de nombre de usuario y contraseña.

HTTPS

Vaya a **HTTPS** para configurar si se debe utilizar HTTP o HTTPS (web protegida). Cuando HTTPS está activado, se utiliza TLSv1.2 para cifrar el tráfico de red web.

Nota

Para eliminar la advertencia del navegador web siempre que se acceda a la unidad a través de HTTPS, añada una regla de excepción al navegador web para que el navegador web sea "válido" o cargue un certificado firmado por la autoridad de certificación/firmado por el propio dispositivo.

RADIUS/TACACS+

RADIUS/TACACS+ habilita la autenticación de usuario remoto cuando el usuario accede a la unidad a través de web o SSH. El nombre de usuario y la contraseña se autentican a continuación mediante el servidor RADIUS/TACACS+.

Una de las ventajas de RADIUS/TACACS+ es que el nombre de usuario y la contraseña son fáciles de actualizar, especialmente si se van a administrar muchos dispositivos de red.

El inconveniente de RADIUS/TACACS+ es que no es posible acceder a la unidad si ambos servidores RADIUS/TACACS+ están fuera de servicio. Es posible activar el **Local login fallback (Sistema de reserva de inicio de sesión local)**, lo que permite que la unidad utilice su nombre de usuario y contraseña locales siempre que no haya respuesta de los servidores RADIUS/TACACS+.

Parámetros comunes de RADIUS/TACACS+

Parámetro	Description (Descripción)
Habilitar autenticación	Configure si RADIUS/TACACS+ se debe activar o desactivar. Cuando se deshabilita RADIUS/TACACS+, se utilizan el nombre de usuario y la contraseña locales.

Habilitar reserva de inicio de sesión local	Cuando se habilita la opción de reserva de inicio de sesión local, se utilizan el nombre de usuario y la contraseña locales siempre que no hay respuesta de los servidores RADIUS/TACACS+. Esto puede suceder si los servidores están fuera de servicio o si se produce un problema de red.
Protocolo de autenticación	Seleccione el protocolo de autenticación de RADIUS o TACACS+.
Secreto compartido	Se debe configurar la misma cadena de clave privada configurada en la unidad y en el servidor RADIUS/TACACS+.
Dirección IP del servidor principal	Configure IPv4, IPv6 o nombre de host principales que se utilizarán para acceder al servidor RADIUS/TACACS+ principal.
Dirección IP del servidor secundario	Configure IPv4, IPv6 o nombre de host secundarios que se utilizarán para acceder al servidor RADIUS/TACACS+ principal.
Tiempo de espera (s)	Configure la hora para el tiempo de espera de la respuesta.

Parámetros adicionales de RADIUS

Parámetro	**Description (Descripción)**
Puerto UDP de autenticación	Configure el puerto UDP que utiliza el servidor RADIUS.

Parámetros adicionales de TACACS+

Parámetro	**Description (Descripción)**
Puerto TCP de autenticación	Configure el puerto TCP que utiliza el servidor TACACS+.

Nota

La versión de software 3.51.06 solo admite acceso a servidores RADIUS/TACACS+ a través de IPv4, ya sea con una dirección IPv4 o con un nombre de host que el servidor DNS resolverá.

Probar RADIUS/TACACS+

Vaya a **Test RADIUS/TACACS+ (Probar RADIUS/TACACS+)** para verificar la configuración de RADIUS/TACACS+ antes de activarla.

Nota

Durante las pruebas, la opción **Enable authentication (Habilitar autenticación)** debe estar deshabilitada.

1. Configure todos los parámetros de RADIUS/TACACS+, dejando la opción **Enable authentication (Habilitar autenticación)** deshabilitada.
2. Guarde la configuración. Si no, los parámetros se restaurarán a los valores guardados después de cada prueba, borrando cualquier valor no guardado.
3. Escriba el nombre de usuario y la contraseña.
4. Haga clic en **Test configuration (Probar configuración)**. Aparecerá un mensaje en espera y, a continuación, **OK** o **FAIL (FALLO)**.
5. Si es necesario, cambie y guarde la configuración y vuelva a probar.
6. Cuando el resultado de la prueba sea correcto, establezca **Enable authentication (Habilitar autenticación)** en habilitado. Guarde la configuración, que activa la configuración de RADIUS/TACACS+.

Configuración de VLAN

La comprobación del estado de la configuración VLAN se realiza al encender la unidad y cuando se solicita un cambio de configuración de VLAN a través de la web. La comprobación del estado es para asegurarse de que la unidad siga siendo manejable a través de la red después de aplicar la configuración de VLAN. En caso de que la nueva configuración de VLAN pueda provocar que la unidad

no funciones, aparecerá un mensaje de error en la página web para solicitudes a través de Internet. Si se detecta un problema al encender la unidad, se restaurará la configuración de la unidad a los valores predeterminados de fábrica.

Habilitar VLAN y puerto de administración

Parámetro	Description (Descripción)
Habilitar VLAN	Habilite o deshabilite la funcionalidad de VLAN.
Puerto de uplink de administración	Este parámetro no tiene ningún efecto en el tráfico de VLAN real. El puerto de uplink de administración ayuda a la unidad a evaluar si la nueva configuración de VLAN podría bloquear la administración de la unidad a través de VLAN de este puerto. Si se detecta un posible conflicto, aparece un mensaje de error y se rechazará la nueva configuración de VLAN.
ID de VLAN de administración	Configure qué ID de VLAN se va a utilizar al gestionar la unidad siempre que esté activada la VLAN.

Configuración de los puertos de VLAN

Parámetro	Description (Descripción)
Modo VLAN	Configure el modo VLAN de acceso o tronco para cada uno de los puertos Ethernet. Acceso: la VLAN solo se utiliza dentro de la unidad para dividir o limitar el acceso de paquetes solo a puertos específicos. Se descartan los paquetes etiquetados para VLAN entrantes que reciba el puerto de acceso VLAN. El etiquetado de VLAN se añade al paquete de la unidad para los paquetes entrantes de acceso VLAN. El etiquetado interno de VLAN de la unidad se descarta para los paquetes salientes de acceso VLAN. Tronco: todos los paquetes de Ethernet están etiquetados como VLAN. Se descartan los paquetes de VLAN sin etiqueta que reciba el puerto del tronco de VLAN.
ID de VLAN del modo de acceso	Configure el ID de VLAN que se utilizará siempre que el puerto se configure como Acceso. El puerto de administración interna de la unidad actúa como solo acceso. Solo se puede alcanzar desde un único ID de VLAN de administración.
TRONCO: filtrar VLAN desconocida	Configure el puerto del tronco de VLAN como filtrado o no filtrado. Habilitado: solo el flujo de datos de algunos ID de VLAN, especificados en la lista de VLAN del tronco, pasa a través del puerto del tronco de VLAN. El resto del tráfico etiquetado de VLAN se descarta. Deshabilitado: el flujo de datos de todos los ID de VLAN pasa a través del puerto del tronco de VLAN.
VLAN DE TRONCO	Muestre los ID de VLAN que pueden pasar por el puerto del tronco de VLAN siempre **TRONCO: filtrar VLAN desconocida** está habilitado.

Configuración de SNMP

Vaya a **SNMP configuration (Configuración de SNMP)** para configurar los parámetros aplicables a SNMPv2c y SNMPv3.

SNMPv2c

Parámetro	Description (Descripción)
Habilitar SNMPv2c	Habilite o deshabilite la compatibilidad con SNMPv2c.
Comunidad de lectura	Configure la cadena de comunidad SNMPv2c GET. Ejemplo: público.
Comunidad de escritura	Configure la cadena de comunidad SNMPv2c SET. Ejemplo: privada.
Comunidad de trampa	Configure la cadena de comunidad de trampa de SNMPv2c. Ejemplo: público.

Información del sistema (MIB-II, v2c/v3)

Parámetro	Description (Descripción)
Contacto del sistema	Configure la cadena OiD de contacto del sistema SNMP MIB-II. Ejemplo: John.
Nombre del sistema	Configure el nombre del sistema SNMP MIB-II. Ejemplo: Mi unidad.
Ubicación del sistema	Configure la ubicación del sistema SNMP MIB-II. Ejemplo: Universidad.

PoE MIB (RFC3621, v2c/v3)

Parámetro	Description (Descripción)
Habilitar notificaciones	Habilite o deshabilite los siguientes informes de trampa de PoE: • Se proporciona/elimina la alimentación PoE del dispositivo alimentado • El consumo total de energía de la unidad supera el xy % de potencia máxima de la unidad • El consumo total de energía de la unidad se restableció a menos del xy % de la potencia máxima de la unidad
Notificar el uso de energía superado (1–99 %).	Si esta opción está habilitada, se notifica al usuario siempre que el consumo total de energía de la unidad (xy %) de potencia máxima de la unidad supere o esté por debajo del valor especificado.

SNMPv3

Parámetro	Description (Descripción)
Habilitar SNMPv3	Habilite o deshabilite la compatibilidad con SNMPv3.
Nombre de usuario	Configurar la cadena de nombre de usuario de SNMPv3.
Contraseña de autenticación	Configurar la contraseña SNMPv3 que va a utilizar MD5/SHA.
Contraseña de privacidad	Configurar la contraseña SNMPv3 que va a utilizar DES/AES.
Modo de autenticación y cifrado	Configure el modo de autenticación y cifrado SNMPv3. Ninguno: sin autenticación ni cifrado, lo que significa que no hay seguridad. MD5: autenticación MD5 sin cifrado. El paquete se puede cambiar y se puede analizar fácilmente mediante análisis de redes. SHA: autenticación SHA sin cifrado. MD5+DES: autenticación MD5 y cifrado DES SHA+DES: autenticación SHA y cifrado DES MD5+AES: autenticación MD5 y cifrado AES SHA+AES: autenticación SHA y cifrado AES

Notificación SNMPv3 (trampa)

Parámetro	Description (Descripción)
Nombre de usuario	Configurar la cadena de nombre de usuario de notificación SNMPv3.
Contraseña de autenticación	Configure la contraseña de notificación de SNMPv3 que va a utilizar MD5/SHA.

Contraseña de privacidad	Configure la contraseña de notificación de SNMPv3 que va a utilizar DES/AES.
Modo de autenticación y cifrado	Configure el modo de autenticación y cifrado de notificación de SNMPv3. Ninguno: sin autenticación ni cifrado, lo que significa que no hay seguridad. MD5: autenticación MD5 sin cifrado. El paquete se puede cambiar y se puede analizar fácilmente mediante análisis de redes. SHA: autenticación SHA sin cifrado. MD5+DES: autenticación MD5 y cifrado DES SHA+DES: autenticación SHA y cifrado DES MD5+AES: autenticación MD5 y cifrado AES SHA+AES: autenticación SHA y cifrado AES

Administradores de trampa de SNMP IPv4/IPv6 remotos (v2c/v3)

Parámetro	Description (Descripción)
Administrador de trampas n.º 1	Configure el primer nombre IPv4/IPv6/DNS de los informes de trampas de la unidad de recepción de servidor de administrador de SNMP remoto como Cold-Start, etc.
Administrador de trampas n.º 2	Configure el segundo nombre IPv4/IPv6/DNS de los informes de trampas de la unidad de recepción de servidor de administrador de SNMP remoto como Cold-Start, etc.

Mantenimiento

Reset (Reiniciar) – Existen cuatro opciones de restablecimiento diferentes:

- **Para realizar un reinicio seguro sin perder alimentación de PoE**, se restablecen el administrador de red interno y el switch Ethernet interno (la red estará fuera de servicio durante unos segundos), dejando la alimentación de PoE sin modificar. Los dispositivos alimentados continúan funcionando con normalidad como si no se realizara ningún reinicio.
- **Un reinicio seguro** restablece el administrador de red interno, el controlador PoE interno y el switch Ethernet interno.
- **La restauración de los valores de fábrica pero el mantenimiento de los ajustes de IP**, restablece la configuración de la unidad a la configuración predeterminada de fábrica, de manera que la configuración de red IPv4/IPv6 no se modifica. VLAN y RADIUS/TACACS+ están deshabilitados. Se mantiene la opción de acceder a la unidad a través de la red como hasta ahora.
- **La restauración de todos los valores de fábrica** restaura la unidad a la configuración predeterminada de fábrica completa. La unidad IP está establecida en 192.168.0.254 y la VLAN está deshabilitada.

Actualización de firmware – Una actualización de firmware solo actualiza el administrador de red interno. El firmware de PoE no se modifica. La actualización puede tardar hasta 10 minutos. Durante este tiempo, la funcionalidad de conmutación de red sigue siendo ininterrumpida, pero la unidad no es manejable. La funcionalidad de PoE sigue activa, pero el tráfico de red se puede interrumpir durante varios segundos.

Configuración de productos – Vaya a **Product configuration (Configuración de producto)** para descargar o cargar un archivo de configuración de productos. Esta funcionalidad se puede utilizar para realizar una copia de seguridad de la configuración de la unidad, modificar la configuración de la unidad sin conexión o para crear un archivo de configuración principal que configure fácilmente varias unidades.

Interfaz de serie SSH

Interfaz de serie SSH

La interfaz SSH está diseñada para varias tareas de mantenimiento, como la actualización del firmware de PoE, etc. Se ha diseñado para ofrecer una interfaz fácil y cómoda para los administradores de TI que estén familiarizados con SSH. Para simplificar el uso de SSH, la interfaz de SSH se utiliza mediante menús.

SSH está protegido por contraseña y comparte el mismo nombre de usuario y contraseña que para el acceso web.

SSH admite autenticación mediante nombre de usuario y contraseña de RADIUS y TACACS+.

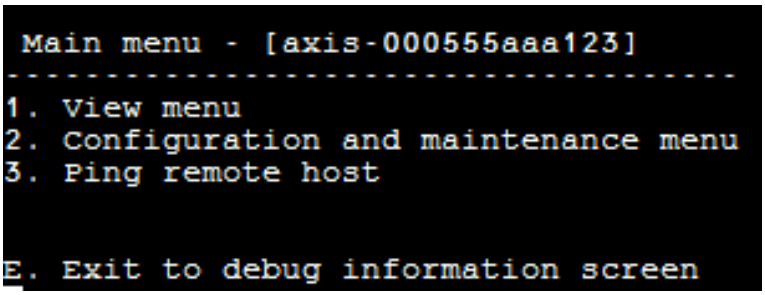
Nota

Solo un usuario remoto a la vez puede acceder a la unidad a través de SSH. En el caso de que un segundo usuario de SSH remoto intente acceder a la unidad mientras el primer usuario de SSH esté todavía activo, se mostrará un mensaje al segundo usuario de SSH, en el que se le solicita que intente volver a conectarse a través de SSH más tarde.

Nota

Las sesiones SSH no activas (el usuario remoto no pulsa ninguna tecla) finalizan automáticamente transcurridos tres minutos.

Menú principal



Para identificar fácilmente la unidad a la que se accede, la cadena de nombre de host de la unidad se muestra a la derecha del título del menú principal. Esto resulta especialmente útil cuando el usuario tiene varias unidades.

Ver menú

View menu (Ver menú) proporciona información sobre el estado de los puertos PoE, los parámetros de red y la información de la unidad.

Menu item (Elemento del menú)	Description (Descripción)
1. Consultar estado de los puertos PoE	Vaya a este elemento del menú para obtener la siguiente información: • Red: información sobre la velocidad de enlace Ethernet (10/100/1000) y el tipo de conexión HD/FD • PoE: información sobre el consumo de energía de cada dispositivo conectado • Potencia total: información sobre el consumo de energía total de todos los dispositivos alimentados conectados a todos los puertos PoE activos. También muestra la potencia máxima disponible. • Fuente de alimentación: información sobre la tensión interna de la fuente de alimentación de la unidad

2. Consultar parámetros de red	Vaya a este elemento del menú para obtener la siguiente información: • Parámetros de red IPv4 en uso: muestra si DHCPv4 está habilitado o deshabilitado. También muestra la dirección IPv4, la máscara IPv4 y la puerta de enlace predeterminada IPv4 en uso. • Parámetros de red IPv6 en uso: muestra si DHCPv6 está habilitado o deshabilitado. También muestra la dirección IPv6 en uso, el prefijo IPv6 y la puerta de enlace predeterminada IPv6. IPv6 puede informar de varias direcciones IPv6 que se han obtenido automáticamente, además de una dirección IPv6 estática/DHCPv6. • Parámetros de red DNS en uso: información sobre direcciones IP de servidor de nombres de dominio IPv4/IPv6 en uso, configuradas estáticamente u obtenidas por DHCPv4/DHCPv6. • Más parámetros de red : información sobre la dirección MAC de la unidad
3. Consultar información de la unidad	Vaya a este elemento del menú para obtener un resumen de los parámetros de producción de la unidad: • Número de pieza: información sobre el número de pieza de marketing de la unidad (T8504–E) • S/N: información sobre el número de serie de seis dígitos de la unidad • Número de producto: información sobre el número de producción de la unidad (solo para uso interno) • Versión aplicación: información sobre la versión de software del administrador de red • Versión de arranque: información sobre la versión de arranque de administrador de red • Firmware: versión de firmware de PoE • Tiempo de encendido del sistema: información acerca del tiempo transcurrido desde el restablecimiento o la alimentación de la unidad • Hora GMT del sistema: información acerca de la hora GMT de la unidad tal y como se ha obtenido de un servidor NTP. Siempre que la unidad no pueda obtener la hora NTP de un servidor NTP, se muestra el mensaje "incorrecto". • Hora local del sistema: información sobre la hora local de la unidad (GMT más cambio de zona horaria). Siempre que la unidad no pueda obtener la hora NTP de un servidor NTP, se muestra el mensaje "incorrecto".

Menú de configuración y mantenimiento

Vaya al **Menú de configuración y mantenimiento** para configurar o restablecer la unidad o para actualizar el software.

Menu item (Elemento del menú)	Description (Descripción)
1. Habilitar/deshabilitar puerto PoE	Habilite o deshabilite un puerto PoE. El enlace de Ethernet permanece habilitado incluso cuando no se proporciona alimentación.
2. Descargar el certificado WEB SSL del servidor TFTP (restablecer solo servidor web)	Descargue certificados firmados por el propio usuario o firmados por la autoridad de certificación desde un servidor TFTP, para permitir una navegación web segura en la unidad mediante confirmación de seguridad por parte del navegador web (bloqueo verde en el área URL del navegador web)
3. Actualizar el firmware de PoE de la unidad (restablecer la unidad)	Actualizar firmware de PoE. Los archivos de actualización se descargan desde un servidor TFTP. La funcionalidad PoE no está disponible durante la actualización del firmware (aproximadamente 5-10 minutos).
4. Restaurar la unidad a la configuración predeterminada de semifábrica (excepto la configuración de IP)	Restablezca la configuración de la unidad a la configuración predeterminada de fábrica, pero no modifica la configuración de red de IPv4/IPv6. De esta forma, se mantiene la opción de acceder a la unidad a través de la red como hasta ahora.
5. Restaurar la unidad a la configuración predeterminada de fábrica completa	Restablezca toda la unidad a la configuración predeterminada de fábrica completa.

6. Restablecer solo el administrador de red	Restablezca solo el administrador de red interno, responsable de las interfaces de gestión de red de las unidades, tales como web, SSH, SNMP, etc. También se restablece el switch Ethernet interno; la red estará fuera de servicio durante unos segundos. Solo la alimentación PoE no se modifica. Los dispositivos alimentados continúan funcionando con normalidad como si no se realizara ningún restablecimiento.
7. Restablecer unidad	Restablezca toda la unidad, incluido el administrador de red interno, el controlador PoE y el switch Ethernet interno.
8. Habilitar/deshabilitar la puerta de enlace predeterminada de ping automática para garantizar la conectividad de red	Habilite o deshabilite el ping automático para la puerta de enlace predeterminada. Si la opción está activada, la unidad verifica la conectividad de red correcta mediante un ping a la puerta de enlace predeterminada cada 12 segundos (IPv4 DGW o IPv6 DGW). Después de 10 fallos de ping consecutivos, el módulo de gestión de red se restablece sin que afecte a los puertos PoE.

Ping a host remoto

Vaya a **Ping remote host (Ping a host remoto)** para probar problemas de conectividad de red.

Supervisión y configuración de SNMP

Se pueden supervisar y gestionar varias unidades utilizando herramientas de gestión de red estándar de terceros, tales como HP Openview, IBM Tivoli, SNMPc, etc.

Habilitar SNMP

La interfaz de administrador de red es compatible con SNMPv1, SNMPv2 y SNMPv3. La unidad acepta y responde a paquetes de SNMPv1, pero como SNMPv1 está obsoleto, se envían traps de SNMP y notificaciones en SNMPv2, SNMPv3 o ambos.

Nota

Por motivos de seguridad, la unidad se envía con SNMPv2 y SNMPv3 deshabilitados. Antes de habilitar SNMP, se recomienda encarecidamente modificar cadenas de comunidad de SNMP.

Para habilitar SNMP:

- Vaya **Security > SNMMP configuration (Seguridad > Configuración de SNMMP)** y habilite SNMPv2 o SNMPv3.
- Asegúrese de que las cadenas de la comunidad SNMPv2 coincidan con la configuración de manager de SNMP.
- Asegúrese de que el nombre de usuario de SNMPv3, la contraseña de autenticación, la contraseña de privacidad y los métodos de cifrado coinciden con la configuración de administrador de SNMP.

Para habilitar traps:

- Vaya a **Remote IPv4/IPv6 SNMP trap managers (Administradores de trap de SNMP IPv4/IPv6 remotos)** y configure la dirección IP de administrador remoto.
- Asegúrese de que el nombre de usuario de notificación de SNMPv3, la contraseña de autenticación, la contraseña de privacidad y los métodos de cifrado coinciden con la configuración de administrador de trap de SNMP.
- Vaya a PoE MIB y habilite las notificaciones de PoE para obtener notificaciones sobre cambios en el estado del puerto PoE, si el consumo de energía de la unidad supera o desciende por debajo de un nivel determinado, etc.

SNMP MIB

El administrador de SNMP admite varios MIB.

MIB de red – Se pueden utilizar varios MIB de red, como RFC1213 MIB-II para proporcionar estadísticas de red. Tenga en cuenta que estas MIB no están diseñados para utilizarse en la configuración de red a través de SNMP.

RFC3621 – Alimentación a través de Ethernet (PoE) MIB que proporciona varias capacidades de PoE. Vea *RFC3621 PoE MIB en la página 19*.

MIB privada – Mejora la funcionalidad de PoE más allá de RFC3621 PoE MIB. Vea *MIB privada en la página 20*.

RFC3621 PoE MIB

RFC3621 PoE MIB se encuentra en el árbol de SNMP MIB 1.3.6.1.2.1.105. La MIB se divide en tres secciones.

Parámetros de puerto – La primera sección gestiona los puertos PoE y proporciona funciones como habilitar y deshabilitar puertos, leer el estado del puerto, clase, etc. Se accede a cada OiD como tabla de matriz de dos dimensiones.

Parámetros de PSE principales – La segunda sección gestiona la fuente de alimentación que proporciona alimentación a un grupo de puertos PoE. Permite leer el consumo de energía total, el estado de la fuente de alimentación, etc.

Traps de PoE – La tercera sección permite y deshabilita el envío de traps de PoE a los administradores de SNMP remotos.

Supervisión y configuración de SNMP

MIB privada

La MIB privada SNMP admite los siguientes OiD de SNMP:

Nombre de OiD	Tipo (R/W)	Description (Descripción)
poePortConsumptionPower	R	Consumo de alimentación del puerto PoE [vatios]
poePortMaxPower	R	Potencia máxima disponible del puerto PoE [vatios]
poePortType	R	Tipo de puerto PoE: dos pares, 30 [vatios], cuatro pares, 60 [vatios]
mainVoltage	R	Tensión de fuente de alimentación de la unidad [voltio]

Mensaje de SysLog

La unidad envía varios informes de eventos a un host IPv4/IPv6 externo en el que se ejecuta una aplicación daemon de SysLog. El host IPv4/IPv6 registra los eventos para usarlos en un futuro. Configure la dirección IP del servidor de SysLog al visitar la página web de configuración de la unidad si se envían los eventos de SysLog.

Existen tres categorías de eventos de registro:

Retransmisión de eventos de SysLog de IPv4 – Cualquier servidor de Syslog en la red LAN debe interceptar estos eventos de registro **independientemente de la configuración de SysLog de la unidad**. Esto facilita la localización de la unidad IP en la red y la presentación de informes de eventos importantes, como la recuperación de unidades por un fallo eléctrico, etc.

Traps de RFC3621 PoE – Las traps de RFC3621 PoE también se envían como mensajes de SysLog, lo que simplifica la lectura de tales eventos para el usuario remoto.

Eventos de SysLog patentados – Estos eventos de registro incluyen posibles fallos o posibles vulneraciones de seguridad, como cuando un usuario remoto intenta acceder con un nombre de usuario incorrecto a través de web/SSH, etc.

Tipos de mensajes de SysLog

ID de mensaje	Description (Descripción)	Información proporcionada	Comments (Comentarios)
0	**sistema UP** se envía cuando se proporciona alimentación a la unidad o el administrador de red interno se restablece.	• Versión de la aplicación • Versión de arranque • Causa del restablecimiento • Estado de arranque • Nombre de host de la unidad • Dirección MAC de la unidad • VLAN (Sí/No) Si es así, también se proporciona el ID de VLAN. El ID de VLAN se utiliza para gestionar la unidad. Qué puerto y si el puerto se configura como acceso o tronco. • Dirección IPv4 (estática/HDCPv4) • Todas las direcciones IPv6 (estática/DHCPv6)	El mensaje se envía en formato de retransmisión 255.255.255.255 a cualquier servidor de SysLog conectado a través de la red LAN y a Los servidores 1 y 2 de SysLog.
1	**El estado del puerto PoE cambiado** se envía cuando se cambia el estado del puerto PoE, por ejemplo, cuando se inserta o se elimina un dispositivo.	Nuevo estado de PoE definido en RFC3621 (búsqueda, suministro de alimentación, fallo, etc.)	RFC3621 SNMP PoE MIB, informe de SysLog equivalente en trap
2	**El uso de alimentación PoE supera el xy % de potencia máxima de la fuente de alimentación** se envía cuando el uso de la potencia de PoE supera el valor establecido.	Consumo de energía en porcentaje de salida de la fuente de alimentación máxima	RFC3621 SNMP PoE MIB, informe de SysLog equivalente en trap

Mensaje de SysLog

3	**El consumo de alimentación de PoE es inferior al xy % de potencia máxima** que se envía cuando el consumo de alimentación de PoE es inferior al valor establecido.	Consumo de energía en porcentaje de salida de la fuente de alimentación máxima	RFC3621 SNMP PoE MIB, informe de SysLog equivalente en trap
6	**La configuración predeterminada** se envía cuando la unidad se restaura a la configuración predeterminada		La IP del servidor SysLog no se modifica cuando se restaura la unidad a la configuración predeterminada.
7	**La configuración de la unidad cambiada** se envía cuando se cambia la configuración de la unidad.		
9	**El restablecimiento del controlador PoE** se envía cuando se restablece el controlador PoE.		
10	**El controlador PoE sin firmware** se envía cuando el firmware del controlador PoE se borra o daña.		
11	**SSH no válido** se envía cuando un usuario remoto intenta acceder a la unidad mediante SSH con un nombre de usuario o contraseña incorrectos.	Dirección IPv4/IPv6 de usuario remoto	
12	**DHCPv4** solo se envía la primera vez que se obtiene la dirección de DHCPv4 ya sea cambiando de estática a DHCPv4 o en encendido.	• Nombre de host de la unidad • Dirección MAC de la unidad • Dirección de DHCPv4	El mensaje se envía en formato de retransmisión 255.255.255.255 a cualquier servidor de SysLog conectado a través de la red LAN y a Los servidores 1 y 2 de SysLog.
13	**DHCPv6** solo se envía la primera vez que se obtiene la dirección de DHCPv6 ya sea cambiando de estática a DHCPv6 o en encendido.	• Nombre de host de la unidad • Dirección MAC de la unidad • Dirección de DHCPv6	El mensaje se envía en formato de retransmisión 255.255.255.255 a cualquier servidor de SysLog conectado a través de la red LAN y a Los servidores 1 y 2 de SysLog.
14	**La configuración de VLAN no válida** se envía cuando la unidad al encenderse detecta que las configuraciones de VLAN actuales evitan que la unidad se pueda administrar a través de la red. Esto es posiblemente debido a un nuevo archivo de configuración defectuoso que se está cargando en la unidad. La unidad se restaura a los valores predeterminados de semifábrica, desactiva la VLAN y restaura la mayoría de los parámetros de configuración a predeterminados de fábrica, de manera que los parámetros de IP de red de la unidad no se modifican. A continuación, la unidad se reinicia.		El mensaje se envía en formato de retransmisión 255.255.255.255 a cualquier servidor de SysLog conectado a través de la red LAN y a Los servidores 1 y 2 de SysLog.

Solución de problemas

La siguiente tabla de solución de problemas le guiará a través de los problemas más habituales. Si no puede encontrar la información que busca, póngase en contacto con el distribuidor local para obtener más ayuda.

Problema	Pasos correctivos
Error al hacer ping en la dirección IP de la unidad.	1. Compruebe que el PC y la unidad comparten la misma red IP. 2. Lance el servidor de SysLog. 3. Apague la unidad y enciéndala de nuevo. Espere a que aparezca el mensaje SysLog n.º 0 para enviar un informe de la dirección IP de la unidad.
Se puede hacer ping en la unidad desde un host local, pero al intentar utilizar la utilidad ping de la unidad no hay respuesta.	1. Desactive el firewall del host. 2. Si el ping es correcto, vaya a las opciones de firewall avanzadas y habilite la opción ping, los puertos TFTP (puerto UDP 69) y los puertos de trap SNMP (puerto UDP 162).
El software no se puede actualizar a través de TFTP.	1. Utilice la utilidad ping de unidad para hacer ping al host en el que se ejecuta la aplicación del servidor TFTP. 2. Apague el firewall o habilite el puerto UDP 69. 3. Compruebe que se ha copiado el paquete de archivos de actualización adecuado en la carpeta raíz del servidor TFTP.
Iniciar sesión en la unidad mediante SSH funciona, pero la sesión de SSH finaliza transcurrido un tiempo.	La sesión de SSH finaliza transcurridos tres minutos si no se presiona ninguna tecla y no se produce actividad.
No se han recibido eventos trap de SNMP.	1. Consulte la configuración de la unidad mediante un navegador web. 2. Verifique que **SNMP** está seleccionado. 3. Verifique que la IP del administrador de SNMP remoto coincide. 4. Verifique que la cadena de comunidad trap coincida con la configuración de trap de administrador de SNMP remoto. 5. Desactive el firewall en la estación de administrador de SNMP o permita que el puerto UDP 162 pase a través de él.
La IP del servidor de SysLog está configurada correctamente, pero los mensajes de registro no se reciben.	Desactive el firewall de host o permita que el puerto UDP 514 pase a través de él.
El inicio de sesión en la unidad no funciona desde que se ha habilitado RADIUS/TACACS+.	1. Siga las instrucciones en *Recuperación de nombre de usuario y contraseña en la página 7*. 2. Configure todos los ajustes que incluyan los valores RADIUS/TACACS+, dejando la opción **Enable Authentication (Habilitar autenticación)** deshabilitada. 3. Utilice la característica "Probar nombre de usuario y contraseña" en la página web de RADIUS/TACACS+ para verificar que un usuario remoto pueda iniciar sesión en la unidad. 4. Establezca **Enable Authentication (Habilitar autenticación)** en habilitado.
No se envían trampas de SNMP de PoE.	1. Habilite la notificación de RFC3621 en la página web de configuración de SNMP. 2. Configure la IP de administrador de trampas de SNMP. 3. Habilite SNMPv2 o SNMPv3.

Soporte

Si precisa asistencia técnica, póngase en contacto con su distribuidor de Axis. Si sus preguntas no se pueden responder inmediatamente, su distribuidor reenviará sus consultas a través del canal apropiado para garantizar una respuesta rápida. Si dispone de conexión a Internet, puede realizar las siguientes acciones:

- Descargarse la documentación del usuario y las actualizaciones de software

- Buscar respuestas a problemas resueltos en la base de datos de preguntas frecuentes (busque por productos, categorías o frases)
- Informar de problemas al personal del servicio de asistencia técnica de Axis mediante el inicio de sesión en su zona privada de asistencia técnica
- Hablar mediante chat con el personal del servicio de asistencia técnica de Axis
- Visitar la página de asistencia técnica de Axis en *axis.com/support*

Si precisa asistencia técnica, póngase en contacto mediante los canales apropiados según su acuerdo de licencia AVHS para garantizar una respuesta rápida.

Si precisa asistencia técnica, póngase en contacto con el servicio de asistencia técnica de ADP para garantizar una respuesta rápida.

Más información

Visite el centro de aprendizaje de Axis, *axis.com/learning*, para consultar guías, tutoriales, seminarios web y cursos que pueden resultarle útiles.

Manual del usuario
AXIS T8504-E Outdoor PoE Switch
© Axis Communications AB, 2018 - 2024
Ver. M3.2
Fecha: Junio 2024
N.º de pieza T10126544