



AW-GEV-104B-130

AW-GEV-184B-250

AW-GEV-264B-370

Conmutador PoE administrado VivoCam Web Smart

Manual de usuario

Rev. 2.0

Para la versión de firmware 0003

Acerca de este manual

Derechos de autor

Copyright © 2017 VIVOTEK Inc. Todos los derechos reservados.

Los productos y programas descritos en esta Guía del usuario son productos con licencia de VIVOTEK Inc. Esta Guía del usuario contiene información de propiedad protegida por derechos de autor, y esta Guía del usuario y todo el hardware, software y documentación que la acompaña tienen derechos de autor. Ninguna parte de esta Guía del usuario puede ser copiada, fotocopiada, reproducida, traducida o reducida a ningún medio electrónico o legible por máquina por cualquier medio electrónico o mecánico. Incluyendo fotocopias, grabaciones o sistemas de almacenamiento y recuperación de información, para cualquier propósito que no sea el uso personal del comprador, y sin el previo permiso expreso por escrito de VIVOTEK Inc.

Objetivo

Esta guía del usuario de la GUI brinda información específica sobre cómo operar y usar las funciones de administración del conmutador de la serie AW-GEV a través del navegador web HTTP / HTTPS.

Audiencia

El manual está diseñado para que lo utilicen administradores de red que son responsables del funcionamiento y mantenimiento de los equipos de red; en consecuencia, asume un conocimiento básico de trabajo de las funciones generales del conmutador, el Protocolo de Internet (IP) y el Protocolo de transferencia de hipertexto (HTTP).

Convenciones

Las siguientes convenciones se utilizan en este manual para mostrar información.

GARANTÍA

Consulte el folleto de garantía / asistencia al cliente que se incluye con el producto. Puede obtener una copia de los términos de garantía específicos aplicables a sus productos y piezas de repuesto VIVOTEK en su distribuidor autorizado de la Oficina de ventas y servicio de VIVOTEK.

Descargo de responsabilidad

VIVOTEK no garantiza que el hardware funcionará correctamente en todos los entornos y aplicaciones, y no ofrece garantía ni representación, ya sea implícita o expresa, con respecto a la calidad, rendimiento, comerciabilidad o idoneidad para un propósito particular. VIVOTEK se exime de responsabilidad por cualquier inexactitud u omisión que pueda haber ocurrido. La información contenida en esta Guía del usuario está sujeta a cambios sin previo aviso y no representa un compromiso por parte de VIVOTEK. VIVOTEK no asume ninguna responsabilidad por cualquier inexactitud que pueda estar contenida en esta Guía del usuario. VIVOTEK no se compromete a actualizar o mantener actualizada la información de esta Guía del usuario y se reserva el derecho a realizar mejoras en esta Guía del usuario y / o en los productos descritos en esta Guía del usuario, en cualquier momento y sin previo aviso.



NOTA:

Para los usuarios que utilizan este conmutador en una aplicación de vigilancia, puede ir directamente al Capítulo 13 para obtener información directamente relacionada con las implementaciones de vigilancia.

Tabla de contenido

ACERCA DE ESTE MANUAL	II
<i>Revisión histórica</i>	<i>vii</i>
INTRODUCCIÓN	1
CAPÍTULO 1 FUNCIONAMIENTO DE LA GESTIÓN BASADA EN WEB	3
CAPÍTULO 2 SISTEMA	7
2-1 SISTEMA INFORMACIÓN	7
2-2 IP AVANCE	9
2-2.1 Configuración de IP	9
2-2.2 Estado de IP	13
2-3 SISTEMA T Y O ME	15
2-4 ltros OG	19
2-4.1 Configuración de Syslog	19
2-4.2 Ver registro	21
2-5 LLDP	23
2-5.1 Configuración LLDP	23
2-5.2 Configuración LLDP-MED	26
2-5.3 Vecino LLDP	33
2-5.4 Vecino LLDP-MED	35
2-5.5 Estadísticas LLDP	39
2-6 ARRIBA norte PAG	41
CAPÍTULO 3 GESTIÓN PORTUARIA	43
3-1 PORT C ONFIGURACIÓN	43
3-2 PORT S ESTADÍSTICAS	46
3-3 SFP PORT I NFO	50
3-4 ENERGY m i FICIENTE m i THERNET	52
3-5 ltros TINTA A GREGACIÓN	53
3-5.1 Puerto	53
3-5.2 Vista de agregador	55
3-5.3 Modo hash de agregación	57
3-5.4 Prioridad del sistema LACP	59
3-6 ltros OOP PAG ROTECCIÓN	60
3-6.1 Configuración	60
3-6.2 Estado	62
CAPÍTULO 4 GESTIÓN DE POE	64
4-1 P O CE ONFIGURACIÓN	64
4-2 P O ES TATUS	66
CAPÍTULO 5 GESTIÓN DE VLAN	68
5-1 VLAN C ONFIGURACIÓN	68
5-2 VLANM EMPRESA	72
5-3 VLAN P ORT S TATUS	74
CAPÍTULO 6 CALIDAD DE SERVICIO	76
6-1 G LOBAL S AJUSTES	76
6-2 P ORT S AJUSTES	78
6-3 P ORT PAG OLICING	80
6-4 P ORT S MÁS FELIZ	81
6-5 S TORM C ONTROL	83
6-6 P ORT S CHEDULER	85

6-7 C O S / 802.1 PAG METRO APLICACIÓN	86
6-8 C O S / 802.1 PAG R EMARKING	87
6-9 IP P RECEDENCIA METRO APLICACIÓN	88
6-10 IP P RECEDENCIA R EMARKING	89
6-11 DSCP M APLICACIÓN	90
6-12 DSCP R EMARKING	91
CAPÍTULO 7 ÁRBOL EXTENSIBLE	92
7-1 S TATE	92
7-2 R EGION C ENCENDIDO	94
7-3 yo NSTANCIA V IEW	95
CAPÍTULO 8 TABLAS DE DIRECCIONES MAC	102
8-1C ONFIGURACIÓN	102
8-2 yo NFORMACIÓN	105
CAPÍTULO 9 MULTICAST	107
9-1 IGMP S NOOPING	107
9-1.1 <i>Configuración básica</i>	107
9-1.2 <i>Configuración de VLAN</i>	110
9-1.3 <i>Estado</i>	112
9-1.4 <i>Información de grupo</i>	114
9-1.5 <i>Información de IGMP SFM</i>	116
CAPÍTULO 10 SEGURIDAD.....	118
10-1 M GESTIÓN	118
10-2 IEEE 802.1X	122
10-2.1 <i>Configuración</i>	122
10-2.2 <i>Estado</i>	125
10-3 P ORT S SEGURIDAD	127
10-3.1 <i>Configuración</i>	127
10-3.2 <i>Estado</i>	130
10-4 RADIO	132
10-4.1 <i>Configuración</i>	132
10-4.2 <i>Estado</i>	135
CAPÍTULO 11 DIAGNÓSTICO	140
11-1 P EN G.....	140
11-2 C APAZ D IAGNÓSTICOS	142
11-3 T RACEROUTE	143
11-4 M IRROR	144
CAPITULO 12 MANTENIMIENTO.....	146
12-1 C ONFIGURACIÓN	146
12-1.1 <i>Guardar configuración de inicio</i>	146
12-1.2 <i>Configuración de copia de seguridad</i>	148
12-1.3 <i>Restaurar configuración</i>	149
12-1.4 <i>Activar config</i>	150
12-1.5 <i>Eliminar configuración</i>	151
12-2 R ESTART D EVICE	152
12-3 F ACTORIA D EFAULTS	153
12-4 F IRMWARE	154
12-4.1 <i>Actualización de firmware</i>	154
CAPITULO 13 VIGILANCIA - SEGUIMIENTO GRÁFICO	155
13-1 O VERVISTA	155

SEGUIMIENTO GRÁFICO	157
T OPOLOGÍA V IEW	157
F LOOR V IEW	165
METRO AP V IEW	167
ADMINISTRACIÓN	168
D EVICE L IST	168 CÁMARA Y CODIFICADOR VVTK
.....	169 CONFIGURAR LA CÁMARA
.....	170
MANTENIMIENTO	171

Revisión histórica

Liberación	Fecha	Revisión
Versión inicial	2016/08/25	1.0
Lanzamiento FW0003	2017/09/05	2.0

Botón de reinicio de hardware / modo

El botón de reinicio se utiliza para reiniciar el interruptor PoE o para restaurar la configuración predeterminada de fábrica. A veces, el reinicio del sistema puede devolver el interruptor PoE al funcionamiento normal. Si los problemas del sistema persisten después del restablecimiento, restaure la configuración de fábrica y vuelva a intentarlo.

Reiniciar : Prensa 3 ~ 10 segundos y suelte el botón de reinicio empotrado. Espere a que se reinicie el conmutador PoE.

Restablecer los valores predeterminados de fábrica: presione durante más tiempo del 10 segundos y suelte el botón de reinicio empotrado. Espere a que el conmutador PoE se restablezca a los valores predeterminados de fábrica y reinicie.

El botón de modo se utiliza para cambiar el modo del indicador LED.

Enlace / ACT / Velocidad: presione más corto que 3 segundos y suelte el botón de modo empotrado. Se encenderá el LED Link / ACT / Speed.

Verde cuando se muestra el estado de Enlace / ACT / Velocidad de los puertos Ethernet.

PoE : Presione más corto que 3 segundos y suelte el botón de modo empotrado. El LED de PoE se encenderá. Verde cuando se muestra el estado del enlace PoE con dispositivos alimentados.

Visión general

En esta Guía del usuario, no solo le indicará cómo instalar y conectar su sistema de red, sino también cómo configurar y monitorear el AW-GEV-104B-130, AW-GEV-184B-250 o AW-GEV-264B-370 a través del interfaz serie web por (RJ-45) y puertos Ethernet paso a paso. Se muestran muchas explicaciones detalladas de las funciones de hardware y software, así como los ejemplos del funcionamiento de la interfaz basada en web.

Los conmutadores de la serie AW-GEV son el conmutador gestionado inteligente + web de próxima generación de VIVOTEK, es una cartera de conmutadores gestionados asequibles que proporciona una infraestructura fiable para la red de su empresa. Estos conmutadores brindan las funciones más inteligentes que necesita para mejorar la disponibilidad de sus aplicaciones comerciales críticas, proteger su información confidencial y optimizar el ancho de banda de su red para entregar información y aplicaciones de manera más efectiva. Proporciona la combinación ideal de asequibilidad y capacidades para redes de nivel de entrada que incluyen aplicaciones para pequeñas empresas o empresas y lo ayuda a crear una fuerza laboral más eficiente y mejor conectada.

Los conmutadores administrados Web Smart + de la serie AW-GEV proporcionan puertos 10/18/26 en un solo dispositivo; la especificación se resalta de la siguiente manera.

- Servidor DHCP y cliente y retransmisión y espionaje
- Colas de hardware de QoS, clasificación, limitación de velocidad, programación de cola de prioridad VLAN basada en etiquetas, VLAN basada en puerto, VLAN basada en protocolo, VLAN basada en subred IP, VLAN basada en MAC
- VLAN privada Edge (PVE), VLAN de voz, VLAN Q-in-Q, Registro de VLAN de multidifusión VLAN GVRP (MVR)
- 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP) y protección de bucle IEEE802.3ad LACP y agregación de enlaces estáticos
- IGMP Snooping v1 / v2 y Querier y Proxy
- SNMP v1 / v2c / v3 Modelo de seguridad basado en el usuario (USM)
- IEEE802.1x RADIUS y TACACS + Autenticación IP Source Guard
- Ethernet de bajo consumo IEEE802.3az

Descripción general de esta guía del usuario

- Capítulo 1 "Funcionamiento de la gestión basada en web" Capítulo 2 "Sistema"
- Capítulo 3 "Administración de puertos" Capítulo 4 "Administración de PoE" Capítulo 5 "Administración de VLAN" Capítulo 6 "Calidad de servicio" Capítulo 7 "Árbol de expansión"
- Capítulo 8 "Tablas de direcciones MAC"

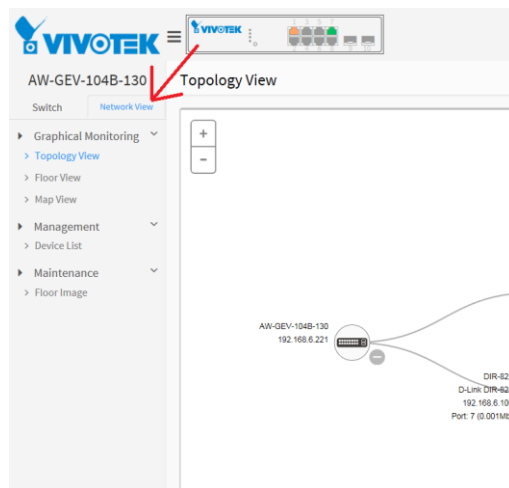
- Capítulo 9 "Multidifusión"
- Capítulo 10 "Seguridad"
- Capítulo 11 "Diagnóstico"
- Capítulo 12 "Mantenimiento"
- Capítulo 13 "Vigilancia"

Inicial
Configuración



IMPORTANTE:

1. Se recomienda utilizar **IE10** o **IE11** para abrir una consola web con el conmutador PoE.
2. Este conmutador PoE está diseñado específicamente para aplicaciones de vigilancia. Viene con una interfaz de vigilancia integrada para facilitar la configuración. Se accede a la interfaz a través de un menú con pestañas, y los cambios de configuración realizados en su ventana tienen una prioridad más alta que los de los menús de configuración del conmutador.

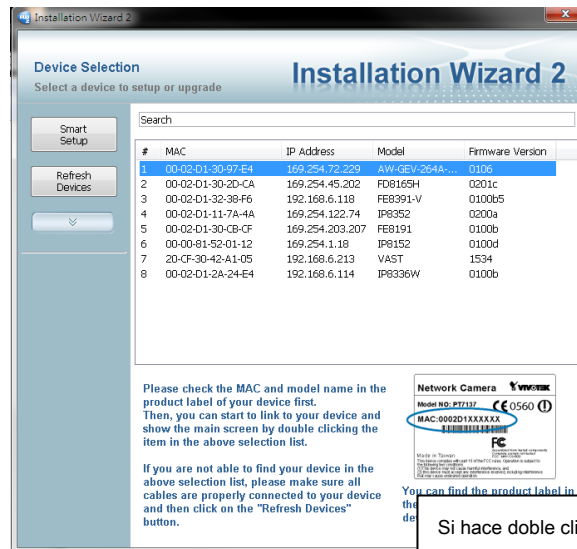


Este capítulo le indica cómo configurar y administrar el conmutador a través de la interfaz de usuario web. Con esta función, puede acceder fácilmente y monitorear a través de cualquier puerto del conmutador todo el estado del conmutador, incluido el estado de las MIB, cada actividad del puerto, estado del árbol de expansión, estado de agregación de puertos, tráfico de multidifusión, VLAN y estado de prioridad, incluso ilegal registro de acceso y así sucesivamente.

T Los valores predeterminados de los interruptores de la serie AW-GEV se enumeran en la tabla debajo:

Dirección IP	Cliente DHCP
Subred Máscara	255.255.255.0
Defecto Puerta	N / A
Nombre de usuario	administración
Contraseña	administración

Puede encontrar el conmutador PoE utilizando la utilidad IW2 de VIVOTEK. Si se producen conflictos de direcciones de red, utilice esta utilidad para localizar el conmutador PoE.



Si hace doble clic en la entrada que se encuentra en la utilidad IW2, se abrirá una consola IE. Si prefiere usar Firefox o Google Chrome, puede ingresar manualmente la dirección IP en el campo URL de su navegador.

Si habilitó el servidor DHCP integrado en el conmutador PoE, puede explorarlo. Por ejemplo, escriba <http://192.168.1.1> en la fila de direcciones en un navegador, mostrará la siguiente pantalla y le pedirá que ingrese un nombre de usuario y contraseña para iniciar sesión y acceder a la autenticación.

El nombre de usuario predeterminado es "administración" y la contraseña es administración. Por primera vez que lo use, ingrese el nombre de usuario y la contraseña predeterminados, y luego haga clic en el <Iniciar sesión> botón. El proceso de inicio de sesión ahora está completo. En este menú de inicio de sesión, debe ingresar el nombre de usuario y la contraseña completos respectivamente, el interruptor AW-GEV no le dará un acceso directo al nombre de usuario automáticamente. Esto parece inconveniente pero más seguro.

El conmutador AW-GEV permite que dos o más usuarios gestionen el conmutador utilizando la identidad del administrador. Los cambios de configuración realizados tendrán efecto dependiendo de quién realizó el último cambio de configuración.

Este capítulo le indica cómo configurar y administrar el conmutador AW-GEV a través de la interfaz de usuario web. Con esta función, puede acceder fácilmente y monitorear a través de cualquier puerto del conmutador todo el estado del conmutador, incluido el estado de las MIB, cada actividad del puerto, estado del árbol de expansión, estado de agregación de puertos, tráfico de multidifusión, VLAN y estado de prioridad, incluso ilegal registro de acceso y así sucesivamente.

Una vez que el conmutador AW-GEV haya finalizado la configuración de su interfaz, puede examinarlo. Por ejemplo, escriba <http://192.168.1.1> en la fila de direcciones en un navegador, mostrará la siguiente pantalla y le pedirá que ingrese el nombre de usuario y la contraseña para iniciar sesión y acceder a la autenticación.



AW-GEV-104B-130

PASSWORD IP ADDRESS DATE & TIME INFORMATION

Change default password

New password

Repeat new password

Next

Aparecerá una página del asistente de inicio la primera vez que acceda al conmutador. El primer paso es configurar una contraseña para la seguridad de acceso.

Si es necesario, configure una IP estática para el conmutador. Haga clic en Siguiente para continuar.



AW-GEV-104B-130

PASSWORD IP ADDRESS DATE & TIME INFORMATION

Set IP address

Obtain IP address via DHCP

Set IP address manually

Previous Next

Luego, puede configurar los datos y la configuración de tiempo para el conmutador asignando un servidor de tiempo de red o ingresando manualmente los valores usando el calendario.



Debe ingresar información adicional como el contacto del sistema y la ubicación del sistema. Cuando termine, haga clic en el botón Aplicar.



El nombre de usuario predeterminado es **"administración"** y la contraseña es **vacio** . Por primera vez que lo use, ingrese el nombre de usuario y la contraseña predeterminados, y luego haga clic en el **< Iniciar sesión>** botón. El proceso de inicio de sesión ahora está completo. En este menú de inicio de sesión, debe ingresar el nombre de usuario y la contraseña completos respectivamente, el interruptor AW-GEV no le dará un

acceso directo al nombre de usuario automáticamente. Esto parece inconveniente, pero más seguro.

El conmutador AW-GEV permite que dos o más usuarios utilicen la identidad del administrador para administrar este conmutador, cuyo administrador haga la última configuración, será una configuración disponible para afectar el sistema.



norte BENEFICIOS SEGÚN OBJETIVOS:

Quando inicie sesión en la página Cambiar WEB para administrar. Primero debe escribir el nombre de usuario del administrador. La contraseña estaba en blanco, así que cuando escriba después del nombre de usuario final, presione Intro. Página de administración para ingresar a la WEB.


Quando inicia sesión en la administración de la interfaz de usuario web del conmutador de la serie AW-GEV, puede usar el inicio de sesión ipv4 ipv6 para administrar

Para optimizar el efecto de visualización, le recomendamos que utilice Microsoft IE 6.0 arriba, Netscape V7.1 arriba o Firefox V1.00 arriba y tenga una resolución de 1024x768. El conmutador admitía una interfaz de navegador web neutral



norte BENEFICIOS SEGÚN OBJETIVOS:

Como conmutador AW-GEV, la función habilita dhcp, por lo que si no tiene un servidor DHCP para proporcionar direcciones IP al conmutador, el conmutador **ip predeterminada** **192.168.1.1**



The image shows a login form with a light gray border. It contains two input fields: the top one is empty, and the bottom one is labeled "Password". Below the input fields is a blue button with the text "Login" in white.

Figura 1: La página de inicio de sesión

Este capítulo describe todas las tareas básicas de configuración que incluyen la información del sistema y cualquier parámetro de administración del conmutador (por ejemplo, hora, cuenta, IP, Syslog y NTP).

2-1 Información del sistema

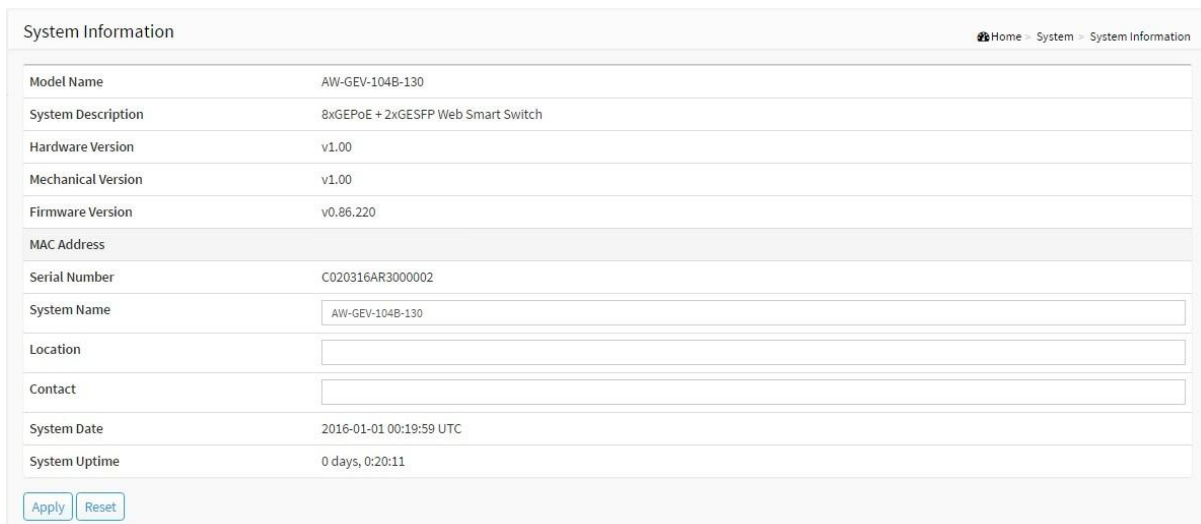
Puede identificar el sistema configurando el nombre del sistema, la ubicación y el contacto del conmutador.

Aquí se proporciona la información de contacto del sistema de interruptores.

interfaz web

Para configurar la información del sistema en la interfaz web:

1. Haga clic en Sistema y Información del sistema.
2. Escriba el nombre del sistema, la ubicación y la información de contacto en esta página.
3. Haga clic en Aplicar.



System Information	
Model Name	AW-GEV-104B-130
System Description	8xGEPoE + 2xGESFP Web Smart Switch
Hardware Version	v1.00
Mechanical Version	v1.00
Firmware Version	v0.86.220
MAC Address	
Serial Number	C020316AR3000002
System Name	<input type="text" value="AW-GEV-104B-130"/>
Location	<input type="text"/>
Contact	<input type="text"/>
System Date	2016-01-01 00:19:59 UTC
System Uptime	0 days, 0:20:11

Buttons:

Figura 2-1: Información del sistema acción

Descripción de parámetros:

- **Nombre del sistema :**

Un nombre asignado administrativamente para este nodo administrado. Por convención, este es el nombre de dominio completo del nodo. Un nombre de dominio es una cadena de texto extraída del alfabeto (AZ, az), dígitos (0-9), signo menos (-). No se permiten caracteres de espacio como parte de un nombre. El primer carácter debe ser un carácter alfabético. Y el primer o último carácter no debe ser un signo menos. La longitud de cadena permitida es de 0 a 128.

- **Localización :**

La ubicación física de este nodo (por ejemplo, armario telefónico, tercer piso). La longitud de cadena permitida es de 0 a 128 y el contenido permitido son los caracteres ASCII de 32 a 1.

- **Contacto :**

La identificación textual de la persona de contacto para este nodo gestionado, junto con información sobre cómo contactar a esta persona. La longitud de cadena permitida es de 0 a 128 y el contenido permitido son los caracteres ASCII de 32 a 126.

2-2 Dirección IP

2-2.1 Configuración de IP

Habilitación de DHCP IPv4:

Habilita la configuración del modo de cliente DHCP para escuchar un servidor DHCP en la red local.

Dirección IPv4:

La dirección IPv4 de la interfaz VLAN1.

Máscara de subred:

La máscara de red IPv4 de la interfaz VLAN1.

Servidor DNS:

Seleccione la fuente del servicio DNS.

1. Sin servidor DNS.
2. Configurado: definido por el usuario.
3. Desde cualquier interfaz DHCP: proporcionada por un enrutador que ofrece el servicio DHCP
4. Desde esta interfaz DHCP: si existe un enrutador en una configuración de VLAN específica, escuche el enrutador particular para el servicio DNS.

IPv4 DHCP Client Enable	<input type="checkbox"/>
IPv4 Address	<input type="text" value="192.168.50.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.50.254"/>
DNS Server	<input type="text" value="No DNS server"/> <input type="button" value="v"/>

Figura 2-2.1: Configuración de IP

2-2.2 Configuración avanzada de IP

La dirección IPv4 para el conmutador se puede obtener a través del servidor DHCP para VLAN 1. Para configurar manualmente una dirección, debe cambiar la configuración predeterminada del conmutador a valores que sean compatibles con su red. Es posible que también deba establecer una puerta de enlace predeterminada entre el conmutador y las estaciones de administración que existen en otro segmento de la red.

Configure la información de IP administrada por conmutador en esta página

Configure los parámetros básicos de IP, controle las interfaces IP y las rutas IP.

El número máximo de interfaces admitidas es 8 y el número máximo de rutas es 8.

Interfaz web

Para configurar una configuración de IP en la interfaz web:

1. Haga clic en Sistema, Avanzado de IP y Configuración de IP.
2. Haga clic en Agregar interfaz y podrá crear una nueva interfaz en el conmutador.
3. Haga clic en Agregar ruta y podrá crear una nueva ruta en el conmutador.
4. Haga clic en Aplicar

IP Configuration Home > System > IP Address > Configuration

DNS Server Configured 8.8.8.8

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.1.1	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
<input type="checkbox"/>	0.0.0.0	0	192.168.1.254	0

Figura 2-2.2: La configuración de IP

Descripción de parámetros:

Configuración IP

• **Servidor DNS :**

Esta configuración controla la resolución de nombres DNS realizada por el conmutador. Se admiten los siguientes modos:

- Sin servidor DNS
No se utilizará ningún servidor DNS.
- Configurado
Proporcione explícitamente la dirección IP del servidor DNS en notación decimal con puntos. Desde esta interfaz
- DHCP
Especifique desde qué interfaz habilitada para DHCP debe preferirse un servidor DNS proporcionado.
- Desde cualquier interfaz DHCP
Se utilizará el primer servidor DNS ofrecido desde una concesión DHCP a una interfaz habilitada para DHCP.

Interfaces IP

• **Borrar :**

Seleccione esta opción para eliminar una interfaz IP existente.

• **VLAN:**

La VLAN asociada con la interfaz IP. Solo los puertos de esta VLAN podrán acceder a la interfaz IP. Este campo solo está disponible para ingresar cuando se crea una nueva interfaz.

• **DHCP IPv4 habilitado:**

Habilite el cliente DHCP marcando esta casilla. Si esta opción está habilitada, el sistema configurará la dirección IPv4 y la máscara de la interfaz usando el protocolo DHCP. El cliente DHCP anunciará el nombre del sistema configurado como nombre de host para proporcionar búsqueda de DNS.

• **Tiempo de espera de reserva de IPv4 DHCP:**

La cantidad de segundos para intentar obtener una concesión DHCP. Una vez que expire este período, se utilizará una dirección IPv4 configurada como dirección de interfaz IPv4. Un valor de cero desactiva la

mecanismo de reserva, de modo que DHCP seguirá intentándolo hasta que se obtenga una concesión válida. Los valores legales son de 0 a 4294967295 segundos.

- **Arrendamiento actual de IPv4 DHCP:**

Para las interfaces DHCP con una concesión activa, esta columna muestra la dirección de la interfaz actual, proporcionada por el servidor DHCP.

- **Dirección IPv4:**

La dirección IPv4 de la interfaz en notación decimal con puntos.

Si DHCP está habilitado, este campo no se utiliza. El campo también puede dejarse en blanco si no se desea el funcionamiento de IPv4 en la interfaz.

- **Máscara IPv4:**

La máscara de red IPv4, en número de bits (longitud del prefijo). Los valores válidos están entre 0 y 30 bits para una dirección IPv4.

Si DHCP está habilitado, este campo no se utiliza. El campo también puede dejarse en blanco si no se desea el funcionamiento de IPv4 en la interfaz.

- **Dirección IPv6:**

La dirección IPv6 de la interfaz. Una dirección IPv6 está en registros de 128 bits representados como ocho campos de hasta cuatro dígitos hexadecimales con dos puntos que separan cada campo (:). Por ejemplo, fe80 :: 215: c5ff: fe03: 4dc7. El símbolo :: es una sintaxis especial que se puede utilizar como una forma abreviada de representar varios grupos de ceros contiguos de 16 bits; pero solo puede aparecer una vez. También puede representar una dirección IPv4 legalmente válida. Por ejemplo, :: 192.1.2.34. El campo puede dejarse en blanco si no se desea el funcionamiento de IPv6 en la interfaz.

- **Máscara IPv6:**

La máscara de red IPv6, en número de bits (longitud del prefijo). Los valores válidos están entre 1 y 128 bits para una dirección IPv6.

El campo puede dejarse en blanco si no se desea el funcionamiento de IPv6 en la interfaz.

Rutas IP

- **Borrar :**

Seleccione esta opción para eliminar una ruta IP existente.

- **La red :**

La red IP de destino o la dirección de host de esta ruta. El formato válido es la notación decimal con puntos o una notación IPv6 válida. Una ruta predeterminada puede usar el valor 0.0.0.0 o IPv6 :: notación.

- **Longitud de la máscara:**

La red IP de destino o la máscara de host, en número de bits (longitud del prefijo). Define la cantidad de una dirección de red que debe coincidir para calificar para esta ruta. Los valores válidos están entre 0 y 32 bits respectivamente 128 para rutas IPv6. Solo una ruta predeterminada tendrá una longitud de máscara de 0 (ya que coincidirá con cualquier cosa).

- **Puerta de enlace:**

La dirección IP de la puerta de enlace IP. El formato válido es la notación decimal con puntos o una notación IPv6 válida. La puerta de enlace y la red deben ser del mismo tipo.

- **Next Hop VLAN (solo para IPv6):**

El ID de VLAN (VID) de la interfaz IPv6 específica asociada con la puerta de enlace.

El VID dado varía de 1 a 4094 y será efectivo solo cuando la interfaz IPv6 correspondiente sea válida.

Si la dirección de la puerta de enlace IPv6 es de enlace local, debe especificar la VLAN del siguiente salto para la puerta de enlace. Si la dirección de la puerta de enlace IPv6 no es de enlace local, el sistema ignora la VLAN del siguiente salto para la puerta de enlace.

Botones

- **Agregar interfaz:**

Haga clic para agregar una nueva interfaz IP. Se admite un máximo de 8 interfaces.

- **Agregar ruta:**

Haga clic para agregar una nueva ruta IP. Se admite un máximo de 8 rutas.

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

NOTA: Si configura conmutadores y cámaras IP para que utilicen IP estáticas, asegúrese de configurar el mismo valor de puerta de enlace y la misma configuración de subred para cámaras IP en enrutadores IP para que todos los conmutadores funcionen correctamente en la vista de topología.

2-2.2 Estado de IP

Esta página muestra el estado de la capa de protocolo IP. El estado está definido por las interfaces IP, las rutas IP y el estado de la caché de vecinos (caché ARP).

Interfaz web

Para mostrar la configuración del registro en la interfaz web:

1. Haga clic en Sistema, Avance de IP y Estado de IP.
2. Mostrar la IP Configuración información.

IP Status Home > System > IP Advance > IP Status

Auto-refresh off Refresh

IP Interfaces

Interface	Type	Address	Status
OS:lo	Link	00-00-00-00-00-00	UP LOOPBACK RUNNING MTU:16436 Metric:1
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
VLAN1	Link		UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
VLAN1	IPv4	192.168.1.1/24	
VLAN1	IPv6	fe80::2e0:4cff:fe00:0/64	

IP Routes

Network	Gateway	Status	Interface
127.0.0.0/24	0.0.0.0	UP	OS:lo
192.168.1.0/24	0.0.0.0	UP	VLAN1
::1/128	::	UP	OS:lo
fe80::/64	::	UP	VLAN1
fe80::2e0:4cff:fe00:0/128	::	UP	OS:lo
ff00::/8	::	UP	VLAN1

Neighbour Cache

IP Address	Link Address
192.168.1.33	VLAN1:00-e0-4c-36-14-16

Figura 2-2.2: El estado de IP

Descripción de parámetros:

Interfaces IP

- **Interfaz :**
Muestra el nombre de la interfaz.
- **Escribe :**
Muestra el tipo de dirección de la entrada. Puede ser LINK o IPv4.
- **Dirección :**
Muestra la dirección actual de la interfaz (del tipo dado).
- **Estado :**
Muestra las banderas de estado de la interfaz (y / o dirección).

Rutas IP

- **La red :**
Muestre la red IP de destino o la dirección de host de esta ruta.
- **Puerta de enlace:**
Muestre la dirección de la puerta de enlace de esta ruta.
- **Estado :**
Muestra las banderas de estado de la ruta.
- **Interfaz:**
Muestra el nombre de la interfaz.

Caché vecino

- **Dirección IP :**
Muestra la dirección IP de la entrada.
- **Dirección de enlace:**
Muestre la dirección de enlace (MAC) para la que existe un enlace a la dirección IP proporcionada.

Botones

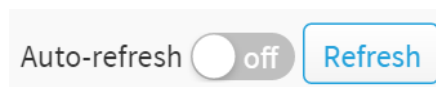


Figura 2-2.2: Los botones de estado de IP

- **Autorefreshar :**
Marque esta casilla para actualizar la página automáticamente. La actualización automática ocurre cada 3 segundos.
- **Actualizar :**
Haga clic para actualizar la página inmediatamente.

2-3 Hora del sistema

El conmutador proporciona formas manuales y automáticas de configurar la hora del sistema a través de NTP. La configuración manual es simple y simplemente ingresa "Año", "Mes", "Día", "Hora" y "Minuto" dentro del rango de valor válido indicado en cada elemento.

Interfaz web

Para configurar la hora en la interfaz web:

1. Haga clic en Sistema y hora del sistema.
2. Especifique el parámetro Hora.
3. Haga clic en Aplicar.

Time Configuration
Home > System > System Time

Time Configuration

Clock Source	Local Settings ▾	Configure NTP Server
System Date	2000-01-01 18:24:01	(yyyy-mm-dd hh:mm:ss)

Time Zone Configuration

Time Zone	None ▾
Acronym	<input type="text"/> (0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time	<input type="checkbox"/> off
Start Time settings	
Month	Jan ▾
Week	1 ▾
Day	Mon ▾
Hours	0 ▾
End Time settings	
Month	Jan ▾
Week	1 ▾
Day	Mon ▾
Hours	0 ▾
Offset settings	
Offset	60 (1 - 1440) Minutes

[Apply](#)
[Reset](#)

Figura 2-3: La configuración de la hora

Descripción de parámetros:

Configuración de tiempo

- **Fuente de reloj:**

Hay dos modos para configurar cómo funciona la fuente de reloj. Seleccione "Configuración local": Fuente de reloj de la hora local. Seleccione "Servidor NTP": fuente de reloj del servidor NTP.

- **Fecha del sistema :**

Muestra la hora actual del sistema. El año de la fecha del sistema limita entre 2001 y 2037.

Configuración de zona horaria

- **Zona horaria :**

Enumera varias zonas horarias en todo el mundo. Seleccione la zona horaria adecuada en el menú desplegable y haga clic en Aplicar para configurar.

- **Acrónimo:**

El usuario puede establecer el acrónimo de la zona horaria. Este es un acrónimo configurable por el usuario para identificar la zona horaria. (Rango: hasta 16 caracteres)

Configuración del horario de verano Horario de

- **verano:**

Esto se utiliza para adelantar o retrasar el reloj de acuerdo con las configuraciones establecidas a continuación para una duración definida del horario de verano. Seleccione 'Desactivar' para desactivar la configuración del horario de verano. Seleccione 'Recurrente' y configure la duración del horario de verano para repetir la configuración cada año. Seleccione 'No recurrente' y configure la duración del horario de verano para la configuración de hora única. (Predeterminado: deshabilitado).

Configuración recurrente

- **Configuración de la hora de inicio:**

Semana: seleccione el número de la semana de inicio.

Día: seleccione el día de inicio.

Mes: seleccione el mes de inicio.

Horas: seleccione la hora de inicio.

- **Configuración de la hora de finalización:**

Semana: seleccione el número de la semana final.

Día: seleccione el día de finalización.

Mes: seleccione el mes final.

Horas: seleccione la hora final.

- **Configuración de compensación:**

Compensación: ingrese la cantidad de minutos que se agregarán durante el horario de verano. (Rango: 1 a 1440)



norte BENEFICIOS SEGÚN OBJETIVOS: En "Configuración de la hora de inicio" y "Configuración de la hora de finalización" se muestra lo que estableció en la información de campo "Configuración de la hora de inicio" y "Configuración de la hora de finalización".

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

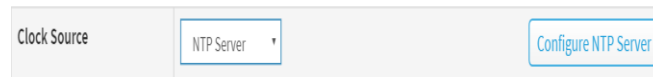


Figura 4-4: El botón Configurar servidor NTP

- **Configure el servidor NTP:**

Haga clic para configurar el servidor NTP, cuando la fuente del reloj seleccione en el servidor NTP.

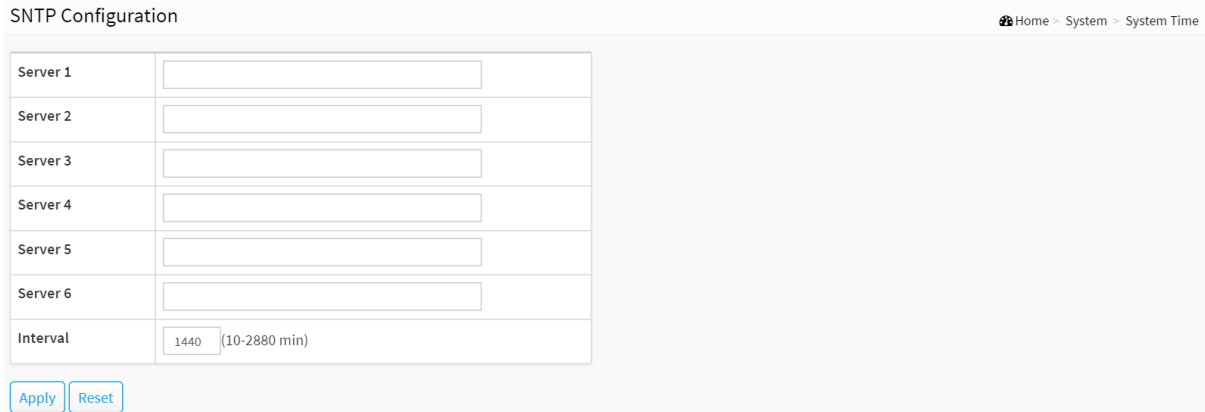


Figura 4-4: La configuración de SNTP

NTP es el protocolo de tiempo de red y se utiliza para sincronizar la hora de la red basada en la hora media de Greenwich (GMT). Si usa el modo NTP y selecciona un servidor de hora NTP incorporado o especifica manualmente un servidor NTP definido por el usuario, así como la zona horaria, el conmutador sincronizará la hora en un breve espacio de tiempo después de presionar el botón <Apply>. Aunque sincroniza la hora automáticamente, NTP no actualiza la hora periódicamente sin que el usuario lo procese.

La zona horaria es un horario de compensación fuera de GMT. Primero debe seleccionar la zona horaria y luego realizar la sincronización de la hora a través de NTP porque el conmutador combinará esta compensación de zona horaria y la hora NTP actualizada para que salga como la hora local; de lo contrario, no podrá obtener la hora correcta. El conmutador admite zona horaria configurable de -12 a +13 paso 1 hora.

Zona horaria predeterminada: +8 Hrs.

Descripción de parámetros :

- **Servidor 1 a 6:**

Proporcione la dirección NTP IPv4 o IPv6 de este conmutador. La dirección IPv6 está en registros de 128 bits representados como ocho campos de hasta cuatro dígitos hexadecimales con dos puntos que separan cada campo (:). Por ejemplo, 'fe80 :: 215: c5ff: fe03: 4dc7'. El símbolo '::' es una sintaxis especial que se puede utilizar como una forma abreviada de representar varios grupos de ceros contiguos de 16 bits; pero solo puede aparecer una vez. También puede representar una dirección IPv4 legalmente válida. Por ejemplo, ':: 192.1.2.34'.

- **Intervalo**

Puede especificar el intervalo de tiempo en segundos después del cual se debe realizar una verificación de tiempo y, en caso de desviación, una resincronización del reloj interno del dispositivo con el servidor de tiempo especificado a través del Protocolo de tiempo de red (NTP).

Botones

Estos botones se muestran en la página SNTP:

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

2-4 Registro

2-4.1 Configuración de Syslog

La configuración de Syslog es un estándar para registrar mensajes de programa. Permite la separación del software que genera mensajes desde el sistema que los almacena y el software que los reporta y analiza. Se puede utilizar también como mensajes informativos, de análisis y de depuración generalizados. Es compatible con una amplia variedad de dispositivos y receptores en múltiples plataformas.

Interfaz web

Para configurar Configuración de Syslog en la interfaz web:

1. Haga clic en Sistema, Registro y Configuración de Syslog.
2. Especifique que los parámetros de syslog incluyen la dirección IP del servidor Syslog y el número de puerto.
3. Evoque el Syslog para habilitarlo.
4. Haga clic en Aplicar.

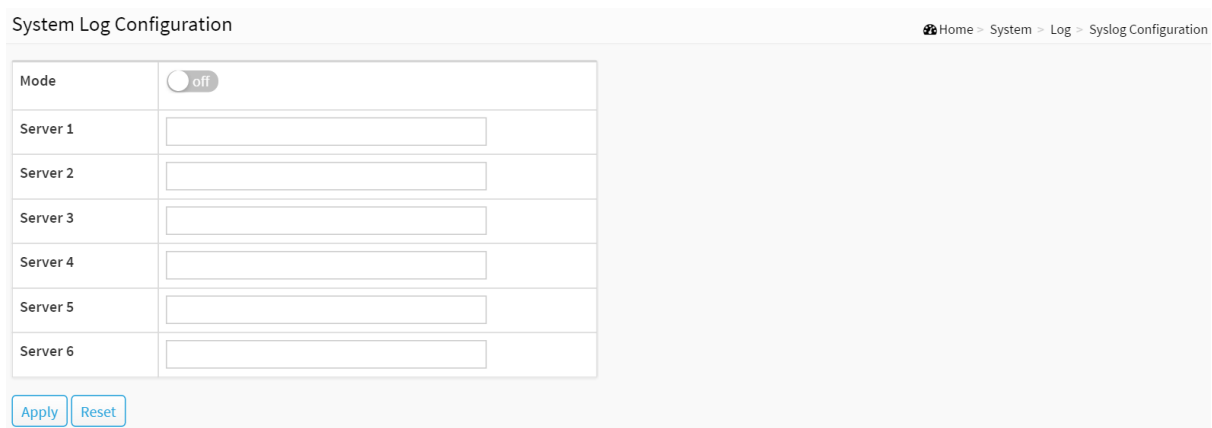


Figura 2-4.1: Configuración del registro del sistema

Descripción de parámetros:

- **Modo :**

Indique el funcionamiento del modo servidor. Cuando la operación de modo está habilitada, el mensaje de syslog se enviará al servidor de syslog. El protocolo syslog se basa en la comunicación UDP y se recibe en el puerto UDP 514 y el servidor syslog no enviará reconocimientos al remitente ya que UDP es un protocolo sin conexión y no proporciona reconocimientos. El paquete syslog siempre se enviará incluso si el servidor syslog no existe. Los modos posibles son:

Activado: habilita el funcionamiento en modo servidor.

Apagado: Desactiva el funcionamiento del modo servidor.

- **Servidor 1 a 6:**

Indica la dirección de hosts IPv4 del servidor syslog. Si el conmutador proporciona la función DNS, también puede ser un nombre de host.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

2-4.2 Ver registro

Esta sección describe que muestra la información de registro del sistema del conmutador

Interfaz web

Para mostrar la configuración del registro en la interfaz web:

1. Haga clic en Sistema, Registro y Ver registro.
2. Muestra la información del registro.



The screenshot shows the 'System Log Information' page. At the top right, there is a breadcrumb trail: Home > System > Log > View Log. Below the title, there are two buttons: 'Refresh' and 'Clear Logs'. A search bar is located on the right side. The main content is a table with the following data:

ID	Level	Time	Message
1	Warning	2001-01-02 01:59:59	Bad password attempt for user 'admin' and authenticated by Web
2	Warning	2001-01-02 02:00:03	Bad password attempt for user '' and authenticated by Web
3	Warning	2001-01-02 02:00:04	Bad password attempt for user '' and authenticated by Web
4	Info	2001-01-02 02:00:08	Login passed for user 'admin'

Below the table, it says 'Showing 1 to 4 of 4 entries'. At the bottom right, there are navigation buttons: 'Previous', '1', and 'Next'.

Figura 2-4.2: Información del registro del sistema

Descripción de parámetros:

- **IDENTIFICACIÓN :**
 - ID (> = 1) de la entrada del registro del sistema.
- **Nivel :**
 - nivel de la entrada del registro del sistema. Se admiten los siguientes tipos de niveles:
 - Depurar:** mensaje de nivel de depuración.
 - Info:** mensaje informativo.
 - Aviso :** condición normal, pero significativa.
 - Advertencia :** condición de advertencia.
 - Error :** condición de error.
 - Crit:** condiciones críticas.
 - Alerta :** se deben tomar medidas de inmediato.
 - Emerg:** el sistema no se puede utilizar.
- **Hora :**
 - Mostrará el registro de registro por hora del dispositivo. La hora de la entrada del registro del sistema.
- **Mensaje :**
 - Mostrará el mensaje de detalles del registro. El mensaje de la entrada del registro del sistema.
- **Buscar :**
 - Puede buscar la información que desea ver.
- **Mostrar entradas:**

Puedes elegir cuántos artículos quieres lucir.

Botones

- **Actualizar :**
Actualiza las entradas del registro del sistema, comenzando por el ID de entrada actual.
- **Registros claros:**
Borre todas las entradas del registro del sistema.
- **Próximo :**
Actualiza las entradas del registro del sistema, pase a la página siguiente.
- **Anterior :**
Actualiza las entradas del registro del sistema, pase a la página anterior.

2-5 LLDP

El conmutador admite LLDP. Para obtener información actualizada sobre su modelo de conmutador, el Protocolo de descubrimiento de capa de enlace (LLDP) proporciona un método basado en estándares para permitir que los conmutadores se anuncien a sí mismos en dispositivos adyacentes y conozcan los dispositivos LLDP adyacentes. El Protocolo de descubrimiento de capa de enlace (LLDP) es un protocolo de capa de enlace independiente del proveedor en el conjunto de protocolos de Internet utilizado por dispositivos de red para anunciar su identidad, capacidades y vecinos en una red de área local IEEE 802, principalmente Ethernet cableada. IEEE se refiere formalmente al protocolo como Descubrimiento de conectividad de control de acceso a medios y estaciones especificado en el documento de estándares IEEE 802.1AB.

2-5.1 Configuración LLDP

Puede por puerto para hacer la configuración LLDP y los parámetros detallados, la configuración entrará en vigencia inmediatamente. Esta página permite al usuario inspeccionar y configurar la configuración actual del puerto LLDP.

Interfaz web

Para configurar LLDP:

1. Haga clic en Configuración del sistema, LLDP y LLDP.
2. Modificar los parámetros de tiempo de LLDP
3. Configure el modo requerido para transmitir o recibir mensajes LLDP
4. Especifique la información para incluir en el campo TLV de los mensajes publicitados
5. Haga clic en Aplicar

LLDP Configuration Home > System > LLDP > LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

Port	Mode	CDP aware	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
1	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

8	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Reset

Figura 2-5.1: Configuración LLDP

Descripción de parámetros:

Parámetros LLDP

- Intervalo de Tx:**

El conmutador transmite periódicamente tramas LLDP a sus vecinos para que la información de descubrimiento de la red esté actualizada. El intervalo entre cada trama LLDP está determinado por el valor del intervalo Tx. Los valores válidos están restringidos a 5 - 32768 segundos.
- Tx Hold:**

Cada trama LLDP contiene información sobre cuánto tiempo se considerará válida la información en la trama LLDP. El período válido de información LLDP se establece en Tx Hold multiplicado por Tx Interval segundos. Los valores válidos están restringidos a 2 - 10 veces.
- Retraso de Tx:**

Si se cambia alguna configuración (por ejemplo, la dirección IP) se transmite una nueva trama LLDP, pero el tiempo entre las tramas LLDP siempre será al menos el valor de Tx Delay segundos. Tx Delay no puede ser mayor que 1/4 del valor del intervalo Tx. Los valores válidos están restringidos a 1 - 8192 segundos.
- Tx Reinit:**

Cuando se deshabilita un puerto, LLDP se deshabilita o se reinicia el conmutador, se transmite una trama de apagado de LLDP a las unidades vecinas, lo que indica que la información de LLDP ya no es válida. Tx Reinit controla la cantidad de segundos entre el cuadro de apagado y una nueva inicialización LLDP. Los valores válidos están restringidos a 1 - 10 segundos.

Configuración del puerto LLDP

La configuración del puerto LLDP se relaciona con el seleccionado actualmente, como se refleja en el encabezado de la página.

- Puerto :**

El número de puerto del conmutador del puerto LLDP lógico.
- Modo :**

Seleccione el modo LLDP.

Solo Rx El switch no enviará información LLDP, pero se analiza la información LLDP de las unidades vecinas.

Solo Tx El conmutador eliminará la información LLDP recibida de los vecinos, pero enviará información LLDP.

Deshabilitado El conmutador no enviará información LLDP y descartará la información LLDP recibida de los vecinos.

Si está habilitado, el conmutador enviará información LLDP y analizará la información LLDP recibida de los vecinos.
- Reconocimiento de CDP:**

Seleccione conciencia de CDP.

La operación CDP está restringida a decodificar tramas CDP entrantes (el conmutador no transmite tramas CDP). Las tramas CDP solo se decodifican si LLDP en el puerto está habilitado.

Solo se decodifican los TLV CDP que se pueden asignar a un campo correspondiente en la tabla de vecinos LLDP. Todos los demás TLV se descartan (los TLV CDP no reconocidos y las tramas CDP descartadas no se muestran en las estadísticas de LLDP). Los TLV de CDP se asignan a la tabla de vecinos LLDP como se muestra a continuación.

El "ID de dispositivo" de CDP TLV se asigna al campo "ID de chasis" de LLDP.

La "Dirección" de CDP TLV se asigna al campo "Dirección de administración" de LLDP. El TLV de dirección CDP puede contener varias direcciones, pero solo la primera dirección se muestra en la tabla de vecinos LLDP.

El "ID de puerto" de CDP TLV se asigna al campo "ID de puerto" de LLDP.

CDP TLV "Versión y plataforma" se asigna al campo LLDP "Descripción del sistema".

Tanto el CDP como el LLDP admiten "capacidades del sistema", pero las capacidades del CDP cubren capacidades que no forman parte del LLDP. Estas capacidades se muestran como "otras" en la tabla de vecinos LLDP.

Si todos los puertos tienen el reconocimiento de CDP desactivado, el conmutador reenvía las tramas CDP recibidas de los dispositivos vecinos. Si al menos un puerto tiene habilitado el reconocimiento de CDP, el conmutador termina todas las tramas de CDP.



norte BENEFICIOS SEGÚN OBJETIVOS: Cuando CDP la conciencia en un puerto está deshabilitada CDP la información no se elimina de inmediato, pero se obtiene cuando se excede el tiempo de espera.

- **Descripción del puerto:**

TLV opcional: cuando se marca, la "descripción del puerto" se incluye en la información LLDP transmitida.

- **Nombre del sistema:**

TLV opcional: cuando se marca, el "nombre del sistema" se incluye en la información LLDP transmitida.

- **Descripción del sistema:**

TLV opcional: cuando se marca, la "descripción del sistema" se incluye en la información LLDP transmitida.

- **Capa del sistema:**

TLV opcional: cuando se marca, la "capacidad del sistema" se incluye en la información LLDP transmitida.

- **Dirección de administración:**

TLV opcional: cuando se marca, la "dirección de gestión" se incluye en la información LLDP transmitida.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

2-5.2 Configuración LLDP-MED

Media Endpoint Discovery es una mejora de LLDP, conocida como LLDP-MED, que proporciona las siguientes funciones:

Detección automática de políticas de LAN (como VLAN, configuración de servicios diferenciados y de prioridad de capa 2 (Diffserv)) que permite conectar y usar la red.

Descubrimiento de la ubicación del dispositivo para permitir la creación de bases de datos de ubicación y, en el caso de Voice over Internet Protocol (VoIP), servicios 911 mejorados.

Administración de energía extendida y automatizada de los puntos finales de Power over Ethernet (PoE).

Gestión de inventario, que permite a los administradores de red rastrear sus dispositivos de red y determinar sus características (fabricante, versiones de software y hardware, y número de serie o activo).

Esta página le permite configurar LLDP-MED. Esta función se aplica a los dispositivos VoIP que admiten LLDP-MED.

Interfaz web

Para configurar LLDP-MED:

1. Haga clic en Configuración del sistema, LLDP y LLDP-MED
2. Modificar el parámetro de conteo de repetición de inicio rápido, el valor predeterminado es 4
3. Modificar los parámetros de ubicación de coordenadas
4. Rellenar parámetros de ubicación de dirección cívica
5. Agregar nueva política
6. Haga clic en Aplicar, se mostrará la siguiente configuración de puerto de política
7. Seleccione ID de política para cada puerto
8. Haga clic en Aplicar.

LLDP-MED Configuration Home > System > LLDP > LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count seconds

Coordinates Location

Latitude	<input style="width: 40px;" type="text" value="0"/> °	<input type="text" value="North"/>	Longitude	<input style="width: 40px;" type="text" value="0"/> °	<input type="text" value="East"/>
Altitude	<input style="width: 40px;" type="text" value="0"/>	<input type="text" value="Meters"/>	Map Datum	<input type="text" value="WGS84"/>	

Civic Address Location

Country code	<input type="text"/>	State/Province	<input type="text"/>	County	<input type="text"/>
City	<input type="text"/>	City district	<input type="text"/>	Block (Neighborhood)	<input type="text"/>
Street	<input type="text"/>	Leading street direction	<input type="text"/>	Trailing street suffix	<input type="text"/>
Street suffix	<input type="text"/>	House no.	<input type="text"/>	House no. suffix	<input type="text"/>
Landmark	<input type="text"/>	Additional location info	<input type="text"/>	Name	<input type="text"/>
Zip code	<input type="text"/>	Building	<input type="text"/>	Apartment	<input type="text"/>
Floor	<input type="text"/>	Room no.	<input type="text"/>	Place type	<input type="text"/>
Postal community name	<input type="text"/>	P.O. Box	<input type="text"/>	Additional code	<input type="text"/>

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
<input type="checkbox"/>	0	Voice	Tagged	1	0	0

[Add New Policy](#)

Policy Port Configuration

Port	Policy ID
	0
1	<input type="checkbox"/>
2	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>

[Apply](#) [Reset](#)

Figura 2-5.2: Configuración LLDP-MED

Descripción de parámetros :

Recuento de repeticiones de inicio rápido

Inicio rápido e identificación de la ubicación del servicio de llamadas de emergencia El descubrimiento de los puntos finales es un aspecto de importancia crítica de los sistemas VoIP en general. Además, es mejor anunciar solo aquellas piezas de información que son específicamente relevantes para tipos particulares de puntos finales (por ejemplo, solo anunciar la política de red de voz a dispositivos con capacidad de voz permitidos), tanto para conservar el espacio limitado de LLDPDU como para reducir problemas de seguridad e integridad del sistema

que puede venir con un conocimiento inadecuado de la política de la red.

Teniendo esto en cuenta, LLDP-MED define una interacción LLDP-MED Fast Start entre el protocolo y las capas de aplicación además del protocolo, para lograr estas propiedades relacionadas. Inicialmente, un dispositivo de conectividad de red solo transmitirá TLV LLDP en una LLDPDU. Solo después de que se detecte un dispositivo terminal LLDP-MED, un dispositivo de conectividad de red compatible con LLDP-MED comenzará a anunciar TLV LLDP-MED en LLDPDU salientes en el puerto asociado. La aplicación LLDP-MED acelerará temporalmente la transmisión de LLDPDU para que comience en un segundo, cuando se haya detectado un nuevo vecino LLDP-MED para compartir información LLDP-MED lo más rápido posible con nuevos vecinos.

Debido a que existe el riesgo de que se pierda una trama LLDP durante la transmisión entre vecinos, se recomienda repetir la transmisión de inicio rápido varias veces para aumentar la posibilidad de que los vecinos reciban la trama LLDP. Con el contador de repeticiones de inicio rápido es posible especificar el número de veces que se repetirá la transmisión de inicio rápido. El valor recomendado es 4 veces, dado que se transmitirán 4 tramas LLDP con un intervalo de 1 segundo, cuando se reciba una trama LLDP con nueva información.

Cabe señalar que LLDP-MED y el mecanismo de inicio rápido LLDP-MED solo están diseñados para ejecutarse en enlaces entre dispositivos de conectividad de red LLDP-MED y dispositivos de punto final y, como tal, no se aplica a enlaces entre elementos de infraestructura de LAN, incluida la conectividad de red. Dispositivos u otros tipos de enlaces.

Ubicación de coordenadas

- **Latitud:**

La latitud DEBE normalizarse dentro de 0-90 grados con un máximo de 4 dígitos.

Es posible especificar la dirección al norte del ecuador o al sur del ecuador.

- **Longitud:**

La longitud DEBE normalizarse dentro de 0-180 grados con un máximo de 4 dígitos.

Es posible especificar la dirección al este del primer meridiano o al oeste del primer meridiano.

- **Altitud:**

La altitud DEBE normalizarse entre -32767 y 32767 con un máximo de 4 dígitos.

Es posible seleccionar entre dos tipos de altitud (pisos o metros).

Metros: representa los metros de altitud definidos por el datum vertical especificado.

Pisos: representa la altitud en una forma más relevante en edificios que tienen diferentes dimensiones de piso a piso. Una altitud = 0.0 es significativa incluso fuera de un edificio y representa el nivel del suelo en la latitud y longitud dadas. Dentro de un edificio, 0.0 representa el nivel del piso asociado con el nivel del suelo en la entrada principal.

- **Datos del mapa:**

El Datum del mapa se utiliza para las coordenadas dadas en estas opciones:

WGS84: (3D geográfico) - Sistema geodésico mundial 1984, código CRS 4327 y nombre del primer meridiano: Greenwich.

NAD83 / NAVD88: Datum norteamericano 1983, código CRS 4269, nombre del primer meridiano: Greenwich; el datum vertical asociado es el Datum vertical norteamericano de 1988 (NAVD88). Este par de datos se utilizará al hacer referencia a ubicaciones en tierra, no cerca del agua de la marea (que usaría Datum = NAD83 / MLLW).

NAD83 / MLLW: Datum norteamericano 1983, código CRS 4269, nombre del primer meridiano: Greenwich; el datum vertical asociado es la media baja del agua (MLLW). Este par de datos se utilizará al hacer referencia a ubicaciones en el agua / mar / océano.

Ubicación de la dirección cívica

Información de configuración de ubicación basada en direcciones cívicas IETF Geopriv (dirección cívica LCI).

- **Código de país :**

El código de país ISO 3166 de dos letras en mayúsculas ASCII - Ejemplo: DK, DE o US.

- **Expresar :**

Subdivisiones nacionales (estado, cantón, región, provincia, prefectura).

- **Condado :**

Condado, parroquia, pistola (Japón), distrito.

- **Ciudad :**

Ciudad, municipio, shi (Japón) - Ejemplo: Copenhague.

- **Distrito de la ciudad :**

División de la ciudad, municipio, distrito de la ciudad, distrito, chou (Japón).

- **Bloque (barrio):**

Barrio, cuadra.

- **Calle :**

Calle - Ejemplo: Poppelvej.

- **Dirección de la calle principal:**

Dirección de la calle principal - Ejemplo: N.

- **Sufijo de calle final:**

Sufijo de calle final - Ejemplo: SW.

- **Sufijo de la calle:**

Sufijo de calle - Ejemplo: Ave, Platz.

- **Casa no. :**

Número de casa - Ejemplo: 21.

- **Casa no. sufijo :**

Sufijo de número de casa - Ejemplo: A, 1/2.

- **Punto de referencia :**

Dirección de referencia o de vanidad - Ejemplo: Universidad de Columbia.

- **Información adicional de ubicación:**

Información adicional sobre la ubicación - Ejemplo: ala sur.

- **Nombre :**

Nombre (ocupante de la residencia y la oficina) - Ejemplo: Flemming Jahn.

- **Código postal :**

Código postal / postal - Ejemplo: 2791.

- **Edificio :**

Edificio (estructura) - Ejemplo: Biblioteca baja.

- **Departamento :**

Unidad (Apartamento, suite) - Ejemplo: Apto 42.

- **Suelo :**

Piso - Ejemplo: 4.

- **Habitación no. :**

Número de habitación - Ejemplo: 450F.

- **Tipo de lugar:**

Tipo de lugar - Ejemplo: Oficina.

- **Nombre de la comunidad postal:**

Nombre de la comunidad postal - Ejemplo: Leonia.

- **Apartado de correos:**

Apartado de correos (PO BOX) - Ejemplo: 12345.

- **Código adicional:**

Código adicional - Ejemplo: 1320300003.

- **Servicio de llamada de emergencia:**

Servicio de llamadas de emergencia (por ejemplo, E911 y otros), tal como lo define TIA o NENA.

- **Servicio de llamada de emergencia:**

El formato de datos del identificador ELIN del servicio de llamadas de emergencia se define para llevar el identificador ELIN como se usa durante la configuración de la llamada de emergencia a un PSAP tradicional basado en troncales CAMA o ISDN. Este formato consta de una cadena de dígitos numéricos, correspondiente al ELIN que se utilizará para llamadas de emergencia.

Políticas

Network Policy Discovery permite el descubrimiento y diagnóstico eficientes de problemas de discrepancia con la configuración de VLAN, junto con los atributos de Capa 2 y Capa 3 asociados, que se aplican a un conjunto de aplicaciones de protocolo específicas en ese puerto. Las configuraciones de políticas de red inadecuadas son un problema muy importante en los entornos de VoIP que con frecuencia resultan en la degradación de la calidad de la voz o la pérdida del servicio.

Las políticas solo están diseñadas para su uso con aplicaciones que tienen requisitos específicos de política de red en "tiempo real", como servicios interactivos de voz y / o video.

Los atributos de la política de red anunciados son:

1. ID de VLAN de capa 2 (IEEE 802.1Q-2003)
2. Valor de prioridad de la capa 2 (IEEE 802.1D-2004)
3. Valor de punto de código Diffserv de capa 3 (DSCP) (IETF RFC 2474)

Esta política de red se anuncia potencialmente y se asocia con varios conjuntos de tipos de aplicaciones compatibles con un puerto determinado. Los tipos de aplicaciones que se abordan específicamente son:

1. Voz
2. Voz de invitado
3. Softphone Voice
4. Videoconferencia
5. Transmisión de video
6. Control / Señalización (admite condicionalmente una política de red separada para los tipos de medios anteriores)

Una red grande puede admitir múltiples políticas de VoIP en toda la organización y diferentes políticas por tipo de aplicación. LLDP-MED permite que se anuncien múltiples políticas por puerto, cada una correspondiente a un tipo de aplicación diferente. Diferentes puertos en la misma red

El dispositivo de conectividad puede anunciar diferentes conjuntos de políticas, según la identidad del usuario autenticado o la configuración del puerto.

Cabe señalar que LLDP-MED no está diseñado para ejecutarse en enlaces que no sean entre dispositivos de conectividad de red y puntos finales y, por lo tanto, no necesita anunciar la multitud de políticas de red que se ejecutan con frecuencia en un interior de enlace agregado a la LAN.

- **Borrar :**

Marque para eliminar la política. Se eliminará durante el próximo guardado.

- **ID de política:**

ID de la póliza. Esto se genera automáticamente y se utilizará al seleccionar las políticas que se asignarán a los puertos específicos.

- **Tipo de aplicación :**

Uso previsto de los tipos de aplicaciones:

1. Voz: para su uso por teléfonos dedicados de telefonía IP y otros dispositivos similares que admitan servicios de voz interactivos. Por lo general, estos dispositivos se implementan en una VLAN separada para facilitar la implementación y mejorar la seguridad mediante el aislamiento de las aplicaciones de datos.

2. Señalización de voz (condicional): para uso en topologías de red que requieren una política diferente para la señalización de voz que para los medios de voz. Este tipo de aplicación no debe anunciarse si se aplican las mismas políticas de red que las que se anuncian en la política de la aplicación de voz.

3. Guest Voice: admite un servicio de voz de 'conjunto limitado de funciones' separado para usuarios invitados y visitantes con sus propios teléfonos de telefonía IP y otros dispositivos similares que admiten servicios de voz interactivos.

4. Señalización de voz de invitado (condicional): para uso en topologías de red que requieren una política diferente para la señalización de voz de invitado que para los medios de voz de invitado. Este tipo de aplicación no debe publicitarse si se aplican las mismas políticas de red que las anunciadas en la política de la aplicación Guest Voice.

5. Softphone Voice: para que lo utilicen aplicaciones de softphone en dispositivos típicos centrados en datos, como PC o portátiles. Esta clase de puntos finales con frecuencia no admite múltiples VLAN, si es que lo hace, y generalmente se configuran para usar una VLAN 'sin etiquetar' o una única VLAN específica de datos 'etiquetados'. Cuando se define una política de red para su uso con una VLAN 'sin etiquetar' (consulte el indicador Etiquetado a continuación), el campo de prioridad L2 se ignora y solo el valor DSCP tiene relevancia.

6. Videoconferencia: para uso de equipos dedicados de videoconferencia y otros dispositivos similares que admitan servicios de video / audio interactivos en tiempo real.

7. Transmisión de video: para uso mediante transmisión o distribución de contenido de video basado en multidifusión y otras aplicaciones similares que admiten servicios de transmisión de video que requieren un tratamiento de política de red específico. Las aplicaciones de video que dependen de TCP con almacenamiento en búfer no serían un uso previsto de este tipo de aplicación.

8. Señalización de video (condicional): para uso en topologías de red que requieren una política separada para la señalización de video que para los medios de video. Este tipo de aplicación no debe publicitarse si se aplican las mismas políticas de red que las que se anuncian en la política de aplicaciones de videoconferencia.

- **Etiqueta :**

Etiqueta que indica si el tipo de aplicación especificado está utilizando una VLAN "etiquetada" o "no etiquetada".

Sin etiquetar indica que el dispositivo está utilizando un formato de trama sin etiquetar y, como tal, no incluye un encabezado de etiqueta según lo definido por IEEE 802.1Q-2003. En este caso, tanto el ID de VLAN como el

Los campos de prioridad de la capa 2 se ignoran y solo el valor DSCP tiene relevancia.

Etiquetado indica que el dispositivo está usando el formato de marco etiquetado IEEE 802.1Q, y que se están usando tanto el ID de VLAN como los valores de prioridad de Capa 2, así como el valor DSCP. El formato etiquetado incluye un campo adicional, conocido como encabezado de etiqueta. El formato de trama etiquetada también incluye tramas etiquetadas con prioridad según lo definido por IEEE 802.1Q-2003.

- **ID de VLAN:**

Identificador de VLAN (VID) para el puerto como se define en IEEE 802.1Q-2003.

- **Prioridad L2:**

Prioridad L2 es la prioridad de Capa 2 que se utilizará para el tipo de aplicación especificado. La prioridad L2 puede especificar uno de los ocho niveles de prioridad (0 a 7), según lo definido por IEEE 802.1D-2004. Un valor de 0 representa el uso de la prioridad predeterminada según se define en IEEE 802.1D-2004.

- **DSCP:**

Valor de DSCP que se utilizará para proporcionar el comportamiento del nodo Diffserv para el tipo de aplicación especificado según se define en IETF RFC 2474. DSCP puede contener uno de los 64 valores de puntos de código (0 a 63). Un valor de 0 representa el uso del valor DSCP predeterminado como se define en RFC 2475.

- **Configuración de políticas de puerto:**

Cada puerto puede anunciar un conjunto único de políticas de red o atributos diferentes para las mismas políticas de red, según la identidad del usuario autenticado o la configuración del puerto.

- **Puerto :**

El número de puerto al que se aplica la configuración.

- **Identificación de la política:**

El conjunto de políticas que se aplicarán a un puerto determinado. El conjunto de políticas se selecciona marcando las casillas de verificación correspondientes a las políticas.

Botones

- **Agregar una nueva política:**

Haga clic para agregar una nueva política. Especifique el tipo de aplicación, etiqueta, ID de VLAN, prioridad L2 y DSCP para la nueva política. Haga clic en "Aplicar".

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

2-5.3 Vecino LLDP

Esta página proporciona una descripción general del estado de todos los vecinos LLDP. La tabla mostrada contiene una fila para cada puerto en el que se detecta un vecino LLDP. Las columnas contienen la siguiente información:

Interfaz web

Para mostrar vecinos LLDP:

1. Haga clic en Sistema, LLDP y LLDP Vecino.
2. Haga clic en Actualizar para la pantalla web de actualización manual.
3. Haga clic en Actualizar automáticamente para actualizar automáticamente la pantalla web.

LLDP Neighbor Information							
Local Port	Chassis ID	Port ID	Port Description	System Name	System Capabilities	System Description	Management Address
Port 5	0.0.0.0	0017E0330C9C:P1	SW PORT	SEP0017E0330C9C	Bridge(+), Telephone(+)	Cisco IP Phone 7941G,V,	
Port 7	00-01-C1-00-00-00	4	Port #4	GS-2310P0330C9C	Bridge(+)	8-Port 10/100/1000Base-T + 2 TP/(100/1G) SFP Combo PoE+ L2 Plus Managed Switch	192.168.3.18 (IPv4)

Figura 2-5.3: Información del vecino LLDP



norte BENEFICIOS SEGÚN OBJETIVOS: Si su red sin ningún dispositivo admite LLDP, la tabla mostrará "No se encontró información de vecino LLDP".

Descripción de parámetros:

- **Puerto local:**

El puerto en el que se recibió la trama LLDP.

- **ID de chasis:**

El ID de chasis es la identificación de las tramas LLDP del vecino.

- **ID de puerto:**

El ID de puerto remoto es la identificación del puerto vecino.

- **Descripción del puerto:**

La descripción del puerto es la descripción del puerto anunciada por la unidad vecina.

- **Nombre del sistema :**

El nombre del sistema es el nombre anunciado por la unidad vecina.

- **Capacidades del sistema:**

Capacidades del sistema describe las capacidades de la unidad vecina. Las posibles capacidades son:

1. Otro
2. Repetidor
3. Puente

- 4. Punto de acceso WLAN
- 5. Enrutador
- 6. Teléfono
- 7. Dispositivo de cable DOCSIS
- 8. Estación solamente
- 9. Reservado

Cuando una capacidad está habilitada, la capacidad va seguida de (+). Si la capacidad está deshabilitada, la capacidad va seguida de (-).

- **Descripción del sistema**

Muestra la descripción del sistema.

- **Dirección de administración:**

La dirección de administración es la dirección de la unidad vecina que se utiliza para las entidades de capa superior para ayudar a la administración de la red al descubrimiento. Esto podría contener, por ejemplo, la dirección IP del vecino.

Botones

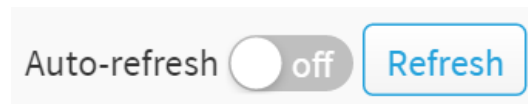


Figura 2-5.3: Los botones LLDP Vecino

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática ocurre cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

2-5.4 Vecino LLDP-MED

Esta página proporciona una descripción general del estado de todos los vecinos LLDP-MED. La tabla mostrada contiene una fila para cada puerto en el que se detecta un vecino LLDP. Esta función se aplica a los dispositivos VoIP que admiten LLDP-MED. Las columnas contienen la siguiente información:

Interfaz web

Para mostrar vecino LLDP-MED:

1. Haga clic en Sistema, LLDP y LLDP-MED Vecino.
2. Haga clic en Actualizar para la pantalla web de actualización manual.
3. Haga clic en Actualizar automáticamente para actualizar automáticamente la pantalla web.

LLDP-MED Neighbor Information Home > System > LLDP > LLDP-MED Neighbor

Auto-refresh off

Port 5						
Device Type	Capabilities					
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory					
Application Type	Policy	Tag	VLAN ID	Priority	DSCP	
Voice Signaling	Unknown	Untagged	-	-	-	
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities			MAU Type	
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode, Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links			100BaseTXFD - 2 pair category 5 UTP, full duplex mode	

Figura 2-5.4: Información del vecino LLDP-MED



norte BENEFICIOS SEGÚN OBJETIVOS: Si su red sin ningún dispositivo es compatible con LLDP-MED, la tabla mostrará "No se encontró información de vecino LLDP-MED".

Descripción de parámetros

- **Puerto :**

El puerto en el que se recibió la trama LLDP.

- **Tipo de dispositivo :**

Los dispositivos LLDP-MED se componen de dos tipos de dispositivos principales: dispositivos de conectividad de red y dispositivos de punto final.

- **Definición de dispositivo de conectividad de red LLDP-MED**

Los dispositivos de conectividad de red LLDP-MED, como se define en TIA-1057, brindan acceso a la infraestructura LAN basada en IEEE 802 para dispositivos de punto final LLDP-MED. Un dispositivo de conectividad de red LLDP-MED es un dispositivo de acceso LAN basado en cualquiera de las siguientes tecnologías:

1. Enrutador / conmutador LAN

2. Puente IEEE 802.1

3. Repetidor IEEE 802.3 (incluido por razones históricas)

4. Punto de acceso inalámbrico IEEE 802.11

5. Cualquier dispositivo que admita las extensiones IEEE 802.1AB y MED definidas por TIA-1057 y pueda retransmitir tramas IEEE 802 mediante cualquier método.

- **Definición de dispositivo de punto final LLDP-MED:**

Los dispositivos de punto final LLDP-MED, como se define en TIA-1057, están ubicados en el borde de la red LAN IEEE 802 y participan en el servicio de comunicación IP utilizando el marco LLDP-MED.

Dentro de la categoría de dispositivo de punto final LLDP-MED, el esquema LLDP-MED se divide en más clases de dispositivo de punto final, como se define a continuación.

Cada clase de dispositivo de punto final LLDP-MED se define para aprovechar las capacidades definidas para la clase de dispositivo de punto final anterior. Por ejemplo, cualquier dispositivo de punto final LLDP-MED que declare cumplimiento como un punto final de medios (clase II) también admitirá todos los aspectos de TIA-1057 aplicables a puntos finales genéricos (clase I) y cualquier dispositivo de punto final LLDP-MED que declare cumplimiento como dispositivo de comunicación. (Clase III) también admitirá todos los aspectos de TIA-1057 aplicables tanto a los puntos finales de medios (clase II) como a los puntos finales genéricos (clase I).

- **Criterio de valoración genérico LLDP-MED (Clase I):**

La definición de punto final genérico LLDP-MED (Clase I) es aplicable a todos los productos de punto final que requieren los servicios de descubrimiento LLDP básicos definidos en TIA-1057, sin embargo, no admiten medios IP ni actúan como un dispositivo de comunicación del usuario final. Dichos dispositivos pueden incluir (pero no se limitan a) controladores de comunicación IP, otros servidores relacionados con la comunicación o cualquier dispositivo que requiera servicios básicos como se define en TIA-1057.

Los servicios de descubrimiento definidos en esta clase incluyen la configuración de LAN, la ubicación del dispositivo, la política de red, la administración de energía y la administración de inventario.

- **Punto final de medios LLDP-MED (Clase II):**

La definición de punto final de medios LLDP-MED (Clase II) es aplicable a todos los productos de punto final que tienen capacidades de medios IP, sin embargo, pueden o no estar asociados con un usuario final en particular. Las capacidades incluyen todas las capacidades definidas para la Clase de punto final genérico anterior (Clase I), y se amplían para incluir aspectos relacionados con la transmisión de medios. Las categorías de productos de ejemplo que se espera que se adhieran a esta clase incluyen (pero no se limitan a) pasarelas de voz / medios, puentes de conferencias, servidores de medios y similares.

Los servicios de descubrimiento definidos en esta clase incluyen el descubrimiento de políticas de capa de red específicas del tipo de medio.

- **Punto final de comunicación LLDP-MED (Clase III):**

La definición de punto final de comunicación LLDP-MED (Clase III) es aplicable a todos los productos de punto final que actúan como dispositivos de comunicación del usuario final que admiten medios IP. Las capacidades incluyen todas las capacidades definidas para las clases anteriores de Punto final genérico (Clase I) y Punto final de medios (Clase II), y se amplían para incluir aspectos relacionados con los dispositivos del usuario final. Las categorías de productos de ejemplo que se espera que se adhieran a esta clase incluyen (pero no se limitan a) dispositivos de comunicación del usuario final, como teléfonos IP, softphones basados en PC u otros dispositivos de comunicación que apoyan directamente al usuario final.

Los servicios de descubrimiento definidos en esta clase incluyen la provisión de un identificador de ubicación (incluida la información ECS / E911), compatibilidad con conmutadores L2 integrados y gestión de inventario.

- **Capacidades LLDP-MED:**

Capacidades LLDP-MED describe las capacidades LLDP-MED de la unidad de vecindario. Las posibles capacidades son:

1. Capacidades LLDP-MED

2. Política de red
3. Identificación de la ubicación
4. Energía extendida a través de MDI - PSE
5. Energía extendida a través de MDI - PD
6. Inventario
7. Reservado

- **Tipo de aplicación :**

Tipo de aplicación que indica la función principal de las aplicaciones definidas para esta política de red, anunciada por un dispositivo de conectividad de red o de punto final. Los posibles tipos de aplicaciones se muestran a continuación.

1. Voz: para su uso por teléfonos dedicados de telefonía IP y otros dispositivos similares que admitan servicios de voz interactivos. Por lo general, estos dispositivos se implementan en una VLAN separada para facilitar la implementación y mejorar la seguridad mediante el aislamiento de las aplicaciones de datos.
2. Señalización de voz: para uso en topologías de red que requieren una política diferente para la señalización de voz que para los medios de voz.
3. Guest Voice: para admitir un servicio de voz de conjunto de funciones limitado separado para usuarios invitados y visitantes con sus propios teléfonos de telefonía IP y otros dispositivos similares que admitan servicios de voz interactivos.
4. Señalización de voz de invitado: para usar en topologías de red que requieren una política diferente para la señalización de voz de invitado que para los medios de voz de invitado.
5. Softphone Voice: para que lo utilicen aplicaciones de softphone en dispositivos típicos centrados en datos, como PC o portátiles.
6. Videoconferencia: para uso de equipos dedicados de videoconferencia y otros dispositivos similares que admitan servicios de video / audio interactivos en tiempo real.
7. Transmisión de video: para uso mediante transmisión o distribución de contenido de video basado en multidifusión y otras aplicaciones similares que admiten servicios de transmisión de video que requieren un tratamiento de política de red específico. Las aplicaciones de video que dependen de TCP con almacenamiento en búfer no serían un uso previsto de este tipo de aplicación.
8. Señalización de video: para uso en topologías de red que requieren una política separada para la señalización de video que para los medios de video.

- **Política :**

La política indica que un dispositivo de punto final desea anunciar explícitamente que el dispositivo requiere la política. Puede ser definido o desconocido

Desconocido: la política de red para el tipo de aplicación especificado se desconoce actualmente.

Definido: la política de red está definida.

- **ETIQUETA :**

TAG indica si el tipo de aplicación especificado está utilizando una VLAN etiquetada o no etiquetada. Puede ser etiquetado o no etiquetado.

Sin etiquetar: el dispositivo utiliza un formato de trama sin etiquetar y, como tal, no incluye un encabezado de etiqueta según lo definido por IEEE 802.1Q-2003.

Etiquetado: el dispositivo utiliza el formato de marco etiquetado IEEE 802.1Q.

- **ID de VLAN:**

VLAN ID es el identificador de VLAN (VID) para el puerto según se define en IEEE 802.1Q-2003. Se utiliza un valor de 1 a 4094 para definir una ID de VLAN válida. Se utiliza un valor de 0 (Prioridad etiquetada) si el

El dispositivo utiliza tramas etiquetadas con prioridad según lo definido por IEEE 802.1Q-2003, lo que significa que solo el nivel de prioridad IEEE 802.1D es significativo y en su lugar se utiliza el PVID predeterminado del puerto de entrada.

- **Prioridad:**

Prioridad es la prioridad de Capa 2 que se utilizará para el tipo de aplicación especificado. Uno de los ocho niveles de prioridad (0 a 7).

- **DSCP:**

DSCP es el valor de DSCP que se utilizará para proporcionar el comportamiento del nodo Diffserv para el tipo de aplicación especificado como se define en IETF RFC 2474. Contiene uno de los 64 valores de puntos de código (0 a 63).

- **Autonegociación**

Autonegociación identifica si el socio de enlace admite la negociación automática MAC / PHY.

- **Estado de negociación automática**

Estado de negociación automática identifica si la negociación automática está habilitada actualmente en el socio de enlace. Si **Autonegociación** es compatible y **Estado de negociación automática** está deshabilitado, el

El modo operativo 802.3 PMD se determinará por el valor del campo de tipo MAU operativo en lugar de por negociación automática.

- **Capacidades de negociación automática**

Capacidades de negociación automática muestra las capacidades MAC / PHY de los socios de enlace.

Botones

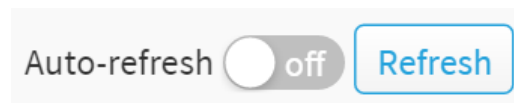


Figura 2-5.4: Los botones LLDP Vecino

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática ocurre cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

2-5.5 Estadísticas LLDP

Se muestran dos tipos de contadores. Los contadores globales son contadores que se refieren a todo el conmutador, mientras que los contadores locales se refieren a contadores por puerto para el conmutador seleccionado actualmente.

Interfaz web

Para mostrar estadísticas LLDP:

1. Haga clic en Estadísticas del sistema, LLDP y LLDP.
2. Haga clic en Actualizar para la pantalla web de actualización manual.
3. Haga clic en Actualizar automáticamente para la pantalla web de actualización automática.
4. Haga clic en Borrar para borrar todos los contadores.

LLDP Counter								
Home > System > LLDP > LLDP Statistics								
Auto-refresh <input type="checkbox"/> off <input type="button" value="Refresh"/> <input type="button" value="Clear"/>								
LLDP Global Counters								
Neighbor entries were last changed			367 days, 5:26:04 (31728364 sec. ago)					
Total Neighbors Entries Added			0					
Total Neighbors Entries Deleted			0					
Total Neighbors Entries Dropped			0					
Total Neighbors Entries Aged Out			0					
LLDP Statistics Local Counters								
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Figura 2-5.5: Información de estadísticas LLDP

Descripción de parámetros:

Contadores globales

- **Las entradas vecinas se cambiaron por última vez en:**
También muestra la hora en que se eliminó o agregó la última entrada por última vez. También muestra el tiempo transcurrido desde que se detectó el último cambio.
- **Total de entradas de vecinos añadidas:**
Muestra el número de nuevas entradas agregadas desde el reinicio del switch.
- **Total de entradas de vecinos eliminadas:**
Muestra el número de nuevas entradas eliminadas desde el reinicio del switch.
- **Total de entradas de vecinos eliminadas:**
Muestra el número de tramas LLDP descartadas debido a que la tabla de entrada está llena.
- **Total de entradas de vecinos vencidas:**

Muestra el número de entradas eliminadas debido a la expiración del período de vida.

Contadores locales

La tabla mostrada contiene una fila para cada puerto. Las columnas contienen la siguiente información:

- **Puerto local:**
El puerto en el que se reciben o transmiten las tramas LLDP.
- **Marcos Tx:**
El número de tramas LLDP transmitidas en el puerto.
- **Marcos Rx:**
El número de tramas LLDP recibidas en el puerto.
- **Errores de Rx:**
El número de tramas LLDP recibidas que contienen algún tipo de error.
- **Marcos descartados:**
Si se recibe una trama LLDP en un puerto y la tabla interna del conmutador se ha llenado por completo, la trama LLDP se cuenta y se descarta. Esta situación se conoce como "Demasiados vecinos" en el estándar LLDP. Las tramas LLDP requieren una nueva entrada en la tabla cuando el ID de chasis o el ID de puerto remoto no están incluidos en la tabla. Las entradas se eliminan de la tabla cuando el enlace de un puerto determinado está inactivo, se recibe una trama de apagado LLDP o cuando la entrada caduca.
- **TLV descartados:**
Cada trama LLDP puede contener múltiples piezas de información, conocidas como TLV (TLV es la abreviatura de "Valor de longitud de tipo"). Si un TLV tiene un formato incorrecto, se cuenta y se descarta.
- **TLV no reconocidos:**
El número de TLV bien formados, pero con un valor de tipo desconocido.
- **Org. Descartado:**
La cantidad de TLV recibidos organizacionalmente.
- **Age-Outs:**
Cada trama LLDP contiene información sobre cuánto tiempo es válida la información LLDP (tiempo de vencimiento). Si no se recibe una nueva trama LLDP dentro del tiempo de vencimiento, se elimina la información de LLDP y se incrementa el contador de Vencimiento.

Botones



Figura 2-5.5: Los botones de información de estadísticas LLDP

- **Autorefrescar :**
Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.
- **Actualizar :**
Haga clic para actualizar la página.
- **Claro :**
Borra los contadores del puerto seleccionado.

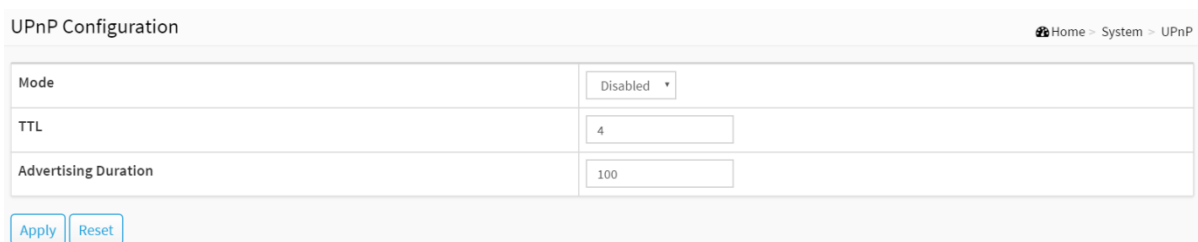
2-6 UPnP

UPnP es un acrónimo de Universal Plug and Play. Los objetivos de UPnP son permitir que los dispositivos se conecten sin problemas y simplificar la implementación de redes en el hogar (intercambio de datos, comunicaciones y entretenimiento) y en entornos corporativos para una instalación simplificada de componentes de computadora.

Interfaz web

Para configurar la configuración UPnP en la interfaz web:

1. Haga clic en Sistema y UPnP.
2. Desplácese para seleccionar el modo para habilitar o deshabilitar.
3. Especifique los parámetros en cada campo en blanco.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer.
6. Volverá a los valores guardados anteriormente.



UPnP Configuration	
Mode	Disabled
TTL	4
Advertising Duration	100

Apply Reset

Figura 2-6: Configuración UPnP

Descripción de parámetros:

Estos parámetros se muestran en la página de configuración de UPnP:

- **Modo :**

Indica el modo de operación UPnP. Los modos posibles son:

Activado: Habilite el funcionamiento del modo UPnP.

Discapacitado: Desactiva el funcionamiento del modo UPnP.

Cuando el modo está habilitado, dos ACE se agregan automáticamente para atrapar paquetes relacionados con UPnP en la CPU. Los ACE se eliminan automáticamente cuando el modo está desactivado.

- **TTL:**

UPnP utiliza el valor TTL para enviar mensajes publicitarios SSDP. Los valores válidos están en el rango de 1 a 255.

- **Duración de la publicidad:**

La duración, transportada en paquetes SSDP, se utiliza para informar a un punto de control o puntos de control con qué frecuencia deben recibir un mensaje de publicidad SSDP desde este conmutador. Si un punto de control no recibe ningún mensaje dentro de la duración, pensará que el interruptor ya no existe. Debido a la naturaleza poco confiable de UDP, en el estándar se recomienda que dicha actualización de los anuncios se realice en menos de la mitad de la duración de la publicidad. En la implementación, el conmutador envía mensajes SSDP periódicamente en el intervalo de la mitad de la duración de la publicidad menos 30 segundos. Los valores válidos están en el rango de 100 a

86400.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

La sección describe cómo configurar los parámetros de detalles del puerto del conmutador. Otros, puede usar la configuración del puerto para habilitar o deshabilitar el puerto del conmutador. Supervise el contenido o el estado de los puertos en la función.

3-1 Configuración de puerto

Esta página muestra las configuraciones de puerto actuales. Los puertos también se pueden configurar aquí.

Interfaz web

Para configurar una configuración de puerto actual en la interfaz web:

1. Haga clic en Administración de puertos y configuración de puertos.
2. Especifique la velocidad configurada, control de flujo.
3. Especifique el alias del puerto detallado o la descripción, una cadena alfanumérica que describa el nombre completo y la identificación de la versión para el tipo de hardware del sistema, la versión de software y la aplicación de red.
4. Haga clic en Aplicar.

Port Configuration Home > Port Management > Port Configuration

[Refresh](#)

Port	Link	Speed		Flow Control			Description
		Status	Mode	Rx Status	Tx Status	Mode	
1	●	100Mfdx	Auto	On	On	<input type="checkbox"/>	
2	●	down	Auto	Off	Off	<input type="checkbox"/>	
3	●	down	Auto	Off	Off	<input type="checkbox"/>	
8	●	down	Auto	Off	Off	<input type="checkbox"/>	
9	●	down	Auto	Off	Off	<input type="checkbox"/>	
10	●	down	Auto	Off	Off	<input type="checkbox"/>	

[Apply](#) [Reset](#)

Figura 3-1: Configuración del puerto

Descripción de parámetros:

- Puerto :

Este es el número de puerto lógico para esta fila.

- **Enlace :**

El estado actual del enlace se muestra gráficamente. El verde indica que el enlace está activo y el rojo que está inactivo.

- **Velocidad de enlace actual:**

Proporciona la velocidad de enlace actual del puerto.

- **Velocidad de enlace configurada:**

Selecciona cualquier velocidad de enlace disponible para el puerto de conmutador dado. Solo se muestran las velocidades admitidas por el puerto específico.

Las posibles velocidades son:

Deshabilitado: deshabilita la operación del puerto del conmutador.

Auto: velocidad de negociación automática del puerto con el socio de enlace y selecciona la velocidad más alta que sea compatible con el socio de enlace.

HDX de 10 Mbps: fuerza el puerto cu en modo semidúplex de 10 Mbps.

FDX de 10 Mbps: fuerza el puerto cu en modo dúplex completo de 10 Mbps.

HDX de 100 Mbps: fuerza el puerto cu en modo semidúplex de 100 Mbps.

FDX de 100 Mbps: fuerza el puerto cu en modo dúplex completo de 100 Mbps.

FDX de 1 Gbps: fuerza el puerto en dúplex completo de 1 Gbps.

FDX de 2,5 Gbps: fuerza el puerto Serdes en modo dúplex completo de 2,5 Gbps.

SFP_Auto_AMS: determina automáticamente la velocidad del SFP. Nota: No hay una forma estandarizada de realizar la detección automática de SFP, por lo que aquí se hace leyendo la rom de SFP. Debido a la falta de una forma estandarizada de realizar la detección automática de SFP, es posible que algunos SFP no sean detectables. El puerto está configurado en modo AMS. El puerto Cu está configurado en modo automático.

100-FX: puerto SFP en velocidad 100-FX. Puerto Cu deshabilitado.

100-FX_AMS: puerto en modo AMS. Puerto SFP en velocidad 100-FX. Puerto Cu en modo automático.

1000-X: puerto SFP en velocidad 1000-X. Puerto Cu deshabilitado.

1000-X_AMS: puerto en modo AMS. Puerto SFP en velocidad 1000-X. Puerto Cu en modo automático. Los puertos en modo AMS con velocidad 1000-X tienen el puerto Cu preferido. Los puertos en modo AMS con velocidad 100-FX tienen el puerto de fibra preferido.

- **Control de flujo :**

Cuando se selecciona Velocidad automática en un puerto, esta sección indica la capacidad de control de flujo que se anuncia al socio de enlace. Cuando se selecciona un ajuste de velocidad fija, eso es lo que se utiliza. La columna Current Rx indica si se obedecen las tramas de pausa en el puerto y la columna Current Tx indica si se transmiten las tramas de pausa en el puerto. Los ajustes de Rx y Tx están determinados por el resultado de la última negociación automática.

Verifique la columna configurada para usar el control de flujo. Esta configuración está relacionada con la configuración de Velocidad de enlace configurada.

- **Descripción:**

Ingrese hasta 47 caracteres como nombre descriptivo para identificar este puerto.

Botones

- **Actualizar :**

Puede hacer clic en ellos para actualizar el estado del enlace del puerto manualmente.

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

3-2 Estadísticas de puertos

La sección describe la información de las estadísticas del puerto y proporciona una descripción general de las estadísticas de tráfico generales para todos los puertos del conmutador.

Interfaz web

Para mostrar la descripción general de las estadísticas del puerto en la interfaz web:

1. Haga clic en Administración de puertos y estadísticas de puertos.
2. Si desea actualizar automáticamente, debe activar la opción "Actualizar automáticamente".
3. Haga clic en "Actualizar" para actualizar las estadísticas del puerto o borrar toda la información cuando haga clic en "Borrar".
4. Si desea ver la estadística detallada del puerto, debe hacer clic en ese puerto.

Port Statistics Overview Home > Port Management > Port Statistics

Auto-refresh off

Port	Packets		Bytes		Errors		Drops	
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted
1	6858	2790	1794496	1148081	0	0	2756	0
2	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0

Figura 3-2: Descripción general de las estadísticas del puerto

Descripción de parámetros:

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila.
- **Paquetes:**
El número de paquetes recibidos y transmitidos por puerto.
- **Bytes:**
El número de bytes recibidos y transmitidos por puerto.
- **Errores:**
El número de tramas recibidas con error y el número de transmisiones incompletas por puerto.
- **Gotas:**
El número de tramas descartadas debido a la congestión de entrada o salida.

Botones



Figura 3-2: Botones de descripción general de estadísticas del puerto

- **Autofrescar :**
Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

- **Claro :**

Borra los contadores de todos los puertos.

Si desea ver la estadística detallada del puerto, debe hacer clic en ese puerto. Los contadores mostrados son los totales para recibir y transmitir, los contadores de tamaño para recibir y transmitir, y los contadores de errores para recibir y transmitir.

Detailed Port 1 Statistics Home > Port Management > Port Statistics

Auto-refresh off Port 1 ▾

Receive Total		Transmit Total	
Rx Packets	7882	Tx Packets	3417
Rx Octets	2113151	Tx Octets	1395217
Rx Unicast	4909	Tx Unicast	3403
Rx Multicast	2337	Tx Multicast	12
Rx Broadcast	636	Tx Broadcast	2
Rx Pause	0	Tx Pause	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	2619	Tx 64 Bytes	875
Rx 65-127 Bytes	1831	Tx 65-127 Bytes	234
Rx 128-255 Bytes	697	Tx 128-255 Bytes	18
Rx 256-511 Bytes	3	Tx 256-511 Bytes	627
Rx 512-1023 Bytes	2548	Tx 512-1023 Bytes	1608
Rx 1024-1518 Bytes	184	Tx 1024-1518 Bytes	55
Rx 1519-2047 Bytes	0	Tx 1519-2047 Bytes	0
Rx 2048-4095 Bytes	0	Tx 2048-4095 Bytes	0
Rx 4096-9216 Bytes	0	Tx 4096-9216 Bytes	0
Rx 9217-16383 Bytes	0	Tx 9217-16383 Bytes	0

Receive Error Counters		Transmit Error Counters	
Rx Drops	2856	Tx Drops	0
Rx CRC/Alignment	0	Tx Late Collision	0
Rx Undersize	0	Tx Excessive Collision	0
Rx Oversize	0	Tx Oversize	0
Rx Fragments	0		
Rx Jabber	0		

Figura 3-2: Estadísticas detalladas del puerto

Descripción de parámetros:

- **Barra de desplazamiento superior izquierda:**

Para desplazarse qué puerto mostrar las estadísticas del puerto con "Port-1", "Port-2", ...

Reciba el total y transmita el total

- **Paquetes Rx y Tx:**

El número de paquetes recibidos y transmitidos (buenos y malos).

- **Octetos Rx y Tx:**

El número de bytes recibidos y transmitidos (buenos y malos). Incluye FCS, pero excluye los bits de trama.

- **Unicast Rx y Tx:**

El número de paquetes de unidifusión recibidos y transmitidos (buenos y malos).

- **Multidifusión Rx y Tx:**

El número de paquetes de multidifusión recibidos y transmitidos (buenos y malos).

- **Transmisión de Rx y Tx:**

El número de paquetes de difusión recibidos y transmitidos (buenos y malos).

- **Pausa de Rx y Tx:**

Un recuento de las tramas de control MAC recibidas o transmitidas en este puerto que tienen un código de operación que indica una operación de PAUSA.

Contadores de tamaño de recepción y transmisión

El número de paquetes recibidos y transmitidos (buenos y malos) se divide en categorías según sus respectivos tamaños de trama.

Recibir contadores de errores

- **Gotas Rx:**

El número de tramas caídas debido a la falta de búferes de recepción o congestión de salida.

- **Rx CRC / Alineación:**

El número de tramas recibidas con CRC o errores de alineación.

- **Rx de tamaño insuficiente:**

El número de tramas 1 cortas recibidas con CRC válido.

- **Rx de gran tamaño:**

El número de 2 tramas largas recibidas con CRC válido.

- **Fragmentos de Rx:**

El número de tramas 1 cortas recibidas con CRC no válido.

- **Rx Jabber:**

El número de 2 tramas largas recibidas con CRC no válido.

- **Rx filtrado:**

El número de tramas recibidas filtradas por el proceso de reenvío.

Las tramas cortas son tramas que tienen un tamaño inferior a 64 bytes.

Las tramas largas son tramas que son más largas que la longitud de trama máxima configurada para este puerto.

Transmitir contadores de errores

- **Gotas de Tx:**

El número de tramas descartadas debido a la congestión del búfer de salida.

- **Tx Late / Exc. Coll. :**

El número de fotogramas caídos debido a colisiones excesivas o tardías.

Botones



Figura 3-2: Los botones de Estadísticas detalladas del puerto

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

- **Claro :**

Borra los contadores del puerto seleccionado.

3-3 Información del puerto SFP

La sección describe que el conmutador podría mostrar la información detallada del módulo SFP que se conecta al conmutador. La información incluye: tipo de conector, tipo de fibra, longitud de onda, velocidad de bits y OUI del proveedor, etc.

Interfaz web

Para mostrar la información de SFP en la interfaz web:

1. Haga clic en Administración de puertos e Información del puerto SFP.
2. Para mostrar la información de SFP.

SFP Port Information Home > Port Management > SFP Port Info

Auto-refresh off Port 9 ▾

Port	9
Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Figura 3-3: Información del puerto SFP

Descripción de parámetros:

- **Barra de desplazamiento superior izquierda:**
Para desplazarse qué puerto mostrar las estadísticas del puerto con "Port-9", "Port-10".
- **Tipo de conector:**
Muestra el tipo de conector, por ejemplo, UTP, SC, ST, LC, etc.
- **Tipo de fibra:**
Muestra el modo de fibra, por ejemplo, multimodo, monomodo.
- **Longitud de onda central de Tx:**
Muestra la longitud de onda central de transmisión de fibra óptica, por ejemplo, 850 nm, 1310 nm, 1550 nm, etc.
- **Tasa de bits:**
Muestra la tasa de bits nominal del transceptor.
- **Proveedor OUI:**

Muestra el código OUI asignado por IEEE.

- **Nombre del vendedor:**

Muestra el nombre de la empresa del fabricante del módulo.

- **Proveedor P / N:**

Muestra el nombre del producto de la denominación por fabricante del módulo.

- **Vendor Rev (revisión):**

Muestra la revisión del módulo.

- **Proveedor SN (número de serie):**

Muestra el número de serie asignado por el fabricante.

- **Código de fecha:**

Muestre la fecha en que se hizo este módulo SFP.

- **La temperatura:**

Muestra la temperatura actual del módulo SFP.

- **Vcc:**

Muestre el voltaje de CC de trabajo del módulo SFP.

- **Mon1 (sesgo) mA:**

Muestre la corriente de polarización del módulo SFP.

- **Mon2 (TX PWR):**

Muestre la potencia de transmisión del módulo SFP.

- **Mon3 (RX PWR):**

Muestre la potencia del receptor del módulo SFP.

Botones



Figura 3-3: Botones de información del puerto SFP

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

3-4 Ethernet de bajo consumo energético

EEE es una abreviatura de Energy Efficient Ethernet definida en IEEE 802.3az.

Esta página permite al usuario inspeccionar y configurar la configuración actual del puerto EEE.

EEE es una opción de ahorro de energía que reduce el uso de energía cuando hay muy poca utilización de tráfico (o no hay tráfico).

EEE funciona apagando los circuitos cuando no hay tráfico. Cuando un puerto recibe datos para transmitir, todos los circuitos se encienden. El tiempo que se tarda en encender los circuitos se denomina tiempo de activación. El tiempo de activación predeterminado es 17 us para enlaces de 1 Gbit y 30 us para otras velocidades de enlace. Los dispositivos EEE deben acordar el valor del tiempo de activación para asegurarse de que tanto el dispositivo receptor como el transmisor tengan todos los circuitos encendidos cuando se transmite tráfico. Los dispositivos pueden intercambiar información sobre la hora de activación de los dispositivos mediante el protocolo LLDP.

Interfaz web

Para configurar una Ethernet de eficiencia energética en la interfaz web:

1. Haga clic en Administración de puertos y Ethernet energéticamente eficiente.
2. El puerto para seleccionar habilitar o deshabilitar Ethernet de eficiencia energética
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Energy Efficient Ethernet Configuration Home > Port Management > Energy Efficient Ethernet

Port Energy Efficient Ethernet Configuration

Port	Configure
1	Disabled ▾
2	Disabled ▾
9	Disabled ▾
10	Disabled ▾

Figura 3-4: Configuración de Ethernet energéticamente eficiente

Descripción de parámetros:

- **Puerto :**
El número de puerto del conmutador del puerto EEE lógico.
- **Configurar:**
Controla si EEE está habilitado para este puerto de conmutador.
- **Botones**
- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

3-5 Agregación de enlaces

3-5.1 Puerto

Esta sección describe que la configuración / estado del puerto se utiliza para configurar la propiedad troncal de todos y cada uno de los puertos del sistema de conmutadores.

Interfaz web

Para configurar la propiedad troncal de todos y cada uno de los puertos en la interfaz web:

1. Haga clic en Administración de puertos, Agregación de enlaces y puerto. Especifique el método, el
2. grupo, el rol de LACP y el tiempo de espera de LACP. Haga clic en Aplicar para guardar la
3. configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Trunk Port Setting/Status Home > Port Management > Link Aggregation > Port

Trunk Port Setting					Trunk Port Status	
Port	Method	Group	LACP Role	LACP Timeout	Aggtr	Status
1	None	0	Active	Fast	1	Ready
2	LACP	1	Active	Fast	2	---
8	None	0	Active	Fast	8	---
9	None	0	Active	Fast	9	---
10	None	0	Active	Fast	10	---

Apply Reset

Figura 3-5.1: Configuración / estado del puerto troncal

Descripción de parámetros :

- **Puerto :**

El puerto lógico para la configuración contenida en la misma fila.
- **Método:**

Esto determina el método que utiliza un puerto para agregarse con otros puertos.

 - **Ninguno :**

Un puerto que no desea agregarse con ningún otro puerto debe elegir esta configuración predeterminada.
 - **LACP:**

Un puerto usa LACP como su método troncal para agregarse con otros puertos que también usan LACP.
 - **Estático:**

Un puerto usa Static Trunk como su método de troncal para agregarse con otros puertos que también usan Static Trunk.
- **Grupo :**

A los puertos que elijan el mismo método de enlace que no sea "Ninguno" se les debe asignar un número de grupo único (es decir, ID de grupo, el valor válido es de 1 a 5) para declarar que desean agregarse entre sí.

- **Rol de LACP:**

Solo se hace referencia a este campo cuando el método de enlace troncal de un puerto es LACP.

- **Activo:**

Un puerto LACP activo comienza a enviar LACPDU a su socio de enlace justo después de que la entidad del protocolo LACP comenzara a tomar el control de este puerto.

- **Pasiva:**

Un puerto LACP pasivo no enviará activamente LACPDU antes de recibir una LACPDU de su socio de enlace.

- **Tiempo de espera de LACP:**

El tiempo de espera controla el período entre las transmisiones de BPDU.

- **Rápido :**

Transmitirá paquetes LACP cada segundo,

- **Lento :**

Esperará 30 segundos antes de enviar un paquete LACP.

- **Aggr:**

Aggr es una abreviatura de "agregador". Cada puerto es también un agregador, y su propio ID de agregador es el mismo que su propio número de puerto. Podemos considerar un agregador como un representante de un grupo de enlaces. Los puertos con el mismo ID de grupo y que utilizan el mismo método de enlace tendrán la oportunidad de agregarse a un puerto de agregador en particular. Este puerto del agregador suele ser el puerto con el número de puerto más pequeño dentro del grupo de enlaces.

- **Estado :**

Este campo representa el estado de enlace de un puerto que utiliza un método de enlace distinto de "Ninguno". También representa el estado del enlace de administración de un puerto que utiliza el método de enlace "Ninguno". "---" significa "no listo"

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

3-5.2 Vista de agregador

Para mostrar la información de enlace de puertos actual desde el punto de vista del agregador.

Interfaz web

Para ver el detalle de LACP en la interfaz web:

1. Haga clic en Administración de puertos, Agregación de enlaces y Vista de agregador. Haga clic en el detalle de
2. LACP.

Aggregator View Home > Port Management > Link Aggregation > Aggregator View

Aggregator	Method	Member Ports	Ready Ports	Lacp Detail
1	None	1	1	<input type="radio"/>
2	LACP	2		<input type="radio"/>
8	None	8		<input type="radio"/>
9	None	9		<input type="radio"/>
10	None	10		<input type="radio"/>

[Lacp Detail](#)

Figura 3-5.2: Vista de agregador

Descripción de parámetros:

- **Agregador:**
Muestra el ID del agregador de cada puerto. De hecho, cada puerto es también un agregador, y su propio ID de agregador es el mismo que su propio número de puerto.
- **Método:**
Muestre el método que usa un puerto para agregar con otros puertos.
- **Puertos miembros:**
Muestre todos los puertos miembros de un agregador (puerto).
- **Puertos listos:**
Muestre solo los puertos miembros listos dentro de un agregador (puerto).
- **Detalle de lacp:**
Puede seleccionar el puerto en el que desea ver el detalle de LACP.

Botones

- **Detalle de lacp:**
Haga clic en este botón y verá la información del agregador. Los detalles se describen a continuación.

Aggregator 2 Information

Aggregator Information				
Actor			Partner	
System Priority	Mac Address		System Priority	Mac Address
32768	00-E0-4C-00-00-00		32768	00-00-00-00-00-00
Actor Port	Actor Key	Trunk Status	Partner Port	Partner Key
2	257	---	2	0

[Back](#)

Figura 3-5.2: El detalle de LACP

Descripción de parámetros:

Actor

- Prioridad del sistema:**
 Muestra la parte de Prioridad del sistema del Actor de agregación. (1-65535)
- Dirección MAC :**
 El ID del sistema del actor de agregación.
- Puerto del actor:**
 El número de puerto del actor conectado a este puerto.
- Actor clave:**
 La clave que el actor ha asignado a este ID de agregación.

Pareja

- Prioridad del sistema:**
 Muestra la parte de Prioridad del sistema del socio de agregación. (1-65535).
- Dirección MAC :**
 El ID del sistema del socio de agregación.
- Puerto asociado:**
 El número de puerto del socio conectado a este puerto.
- Clave de socio:**
 La clave que el socio ha asignado a este ID de agregación.
- Estado del maletero:**
 Este campo representa el estado de enlace de un puerto que utiliza un método de enlace distinto de "Ninguno". También representa el estado del enlace de administración de un puerto que utiliza el método de enlace "Ninguno". "—" significa "no listo".

Botón

- Atrás :**
 Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.

3-5.3 Modo hash de agregación

Interfaz web

Para configurar el modo hash de agregación en la interfaz web:

1. Haga clic en Port Management, Link Aggregation y Aggregator Hash Mode. Haga clic en Colaboradores de
2. código hash para seleccionar el modo.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

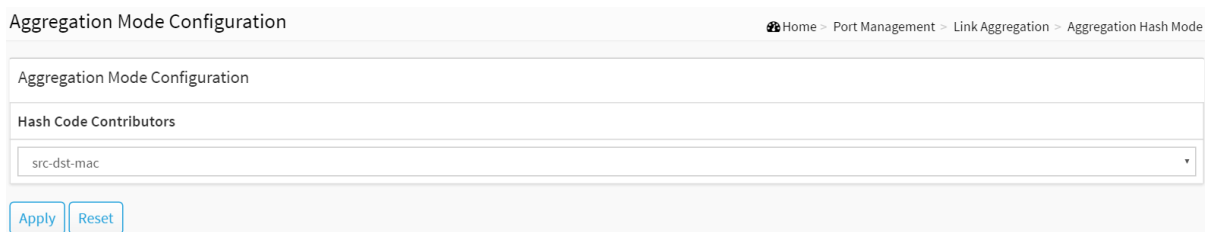


Figura 3-5.3: Modo hash de agregación

Descripción de parámetros:

Colaboradores del código hash

- **src-mac:**
Dirección MAC de origen

La dirección MAC de origen se puede utilizar para calcular el puerto de destino de la trama. Marque para habilitar el uso de la dirección MAC de origen, o desmarque para deshabilitar. De forma predeterminada, la dirección MAC de origen está habilitada.
- **dst-mac:**
Dirección MAC de destino

La dirección MAC de destino se puede utilizar para calcular el puerto de destino de la trama. Marque para habilitar el uso de la dirección MAC de destino, o desmarque para deshabilitar. De forma predeterminada, la dirección MAC de destino está desactivada.
- **ip:**
Dirección IP

La dirección IP se puede utilizar para calcular el puerto de destino de la trama. Marque para habilitar el uso de la dirección IP, o desmarque para deshabilitar. De forma predeterminada, la dirección IP está habilitada.
- **src-dst-mac:**
Dirección MAC de origen + Dirección MAC de destino.
- **src-ip:**
Dirección MAC de origen + Dirección IP.
- **dst-ip:**
Dirección MAC de destino + Dirección IP.
- **src-dst-ip:**
Dirección MAC de origen + Dirección MAC de destino + Dirección IP.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

3-5.4 Prioridad del sistema LACP

Se utiliza para establecer la parte de prioridad del ID del sistema LACP. LACP solo agregará los puertos cuyos socios de enlace de pares estén todos en un solo sistema. A cada sistema que admita LACP se le asignará un identificador de sistema único a nivel mundial para este propósito. Un ID de sistema es un campo de 64 bits que comprende una dirección MAC de 48 bits y un valor de prioridad de 16 bits. El usuario puede establecer la prioridad del sistema. Su rango es de 1 a 65535. Predeterminado: 32768.

Interfaz web

Para configurar la prioridad del sistema LACP en la interfaz web:

1. Haga clic en Administración de puertos, Agregación de enlaces y Prioridad del sistema LACP. Especifique la
2. prioridad del sistema LACP.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

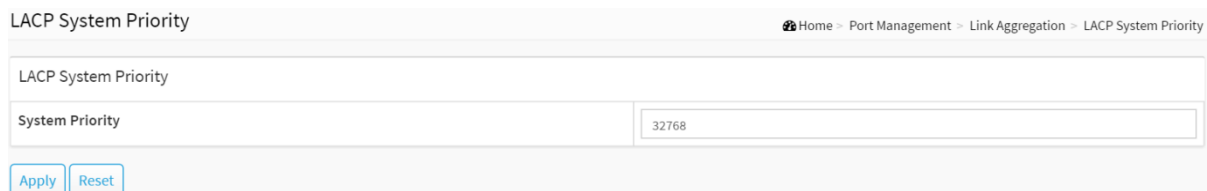


Figura 3-5.4: La prioridad del sistema LACP

Descripción de parámetros:

- **Prioridad del sistema:**

1-65535.

Muestra la parte de Prioridad del sistema de un ID de sistema.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

3-6 Protección de bucle

3-6.1 Configuración

La protección de bucle se utiliza para detectar la presencia de tráfico. Cuando el conmutador recibe la dirección MAC del paquete (trama de detección de bucle) de la misma manera que uno mismo desde el puerto, se muestra la protección de bucle. El puerto se bloqueará cuando reciba las tramas de protección en bucle. Si desea reanudar el puerto bloqueado, busque la ruta de bucle y elimine la ruta de bucle, luego seleccione reanudar el puerto bloqueado y haga clic en "Reanudar" para activar los puertos bloqueados.

Interfaz web

Para configurar los parámetros de protección de bucle en la interfaz web:

1. Haga clic en Administración de puertos, Protección y configuración de bucle.
2. Evoque para seleccionar habilitar o deshabilitar la protección de bucle de puerto.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Loop Protection Configuration Home > Port Management > Loop Protection > Configuration

Global Configuration

Enable Loop Protection	<input type="radio"/> off
Transmission Time	<input type="text" value="5"/> seconds
Shutdown Time	<input type="text" value="180"/> seconds

Port Configuration

Port	Enable	Action	Tx Mode
1	<input checked="" type="checkbox"/>	Shutdown Port	Enable
2	<input checked="" type="checkbox"/>	Shutdown Port	Enable
8	<input checked="" type="checkbox"/>	Shutdown Port	Enable
9	<input checked="" type="checkbox"/>	Shutdown Port	Enable
10	<input checked="" type="checkbox"/>	Shutdown Port	Enable

Figura 3-6.1: Configuración de protección de bucle

Descripción de parámetros :

configuración global

- **Habilitar protección de bucle:**

Controla si las protecciones de bucle están habilitadas (en su conjunto).

- **Tiempo de transmisión :**

El intervalo entre cada PDU de protección de bucle enviada en cada puerto. Los valores válidos son de 1 a 10 segundos.

- **Hora de apagado:**

El período (en segundos) durante el cual un puerto se mantendrá deshabilitado en caso de que se detecte un bucle (y la acción del puerto apaga el puerto). Los valores válidos son de 0 a 604800 segundos (7 días). Un valor de cero mantendrá un puerto deshabilitado (hasta el próximo reinicio del dispositivo).

Configuración del puerto

- **Puerto :**
El número de puerto del conmutador del puerto.
- **Habilitar :**
Controla si la protección de bucle está habilitada en este puerto de conmutador
- **Acción:**
Configura la acción realizada cuando se detecta un bucle en un puerto. Los valores válidos son Shutdown Port, Shutdown Port y Log o Log Only.
- **Modo Tx:**
Controla si el puerto está generando activamente PDU de protección de bucle o si solo está buscando de forma pasiva PDU en bucle.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

3-6.2 Estado

Esta sección muestra el estado del puerto de protección de bucle de los puertos del conmutador seleccionado actualmente.

Interfaz web

Para mostrar el estado de la protección de bucle en la interfaz web:

1. Haga clic en Administración de puertos, Protección de bucle y estado.
2. Si desea actualizar automáticamente la información, debe activar la "Actualización automática".
3. Haga clic en "Actualizar" para actualizar el estado de protección de bucle.

Loop Protection Status Home > Port Management > Loop Protection > Status

Auto-refresh off [Refresh](#)

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Up	-	-
10	Shutdown	Enabled	0	Down	-	-

Figura 3-6.2: Estado de protección de bucle

Descripción de parámetros:

- **Puerto**
El número de puerto del conmutador del puerto lógico.
- **Acción**
La acción del puerto configurada actualmente.
- **Transmitir**
El modo de transmisión del puerto configurado actualmente.
- **Bucles**
La cantidad de bucles detectados en este puerto.
- **Estado**
El estado de protección de bucle actual del puerto.
- **Lazo**
Si actualmente se detecta un bucle en el puerto.
- **Hora del último bucle**
La hora del último evento de bucle detectado.

Botones



Figura 3-6.2: Botones de estado de protección de bucle

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

PoE es un acrónimo de Power over Ethernet. La alimentación a través de Ethernet se utiliza para transmitir energía eléctrica a dispositivos remotos a través de un cable Ethernet estándar. Por ejemplo, podría usarse para alimentar teléfonos IP, puntos de acceso de LAN inalámbrica y otros equipos, donde sería difícil o costoso conectar el equipo a la fuente de alimentación principal.

4-1 Configuración de PoE

Esta página permite al usuario inspeccionar y configurar los ajustes actuales del puerto PoE y mostrar todos los PoE Supply W.

Interfaz web

Para configurar Power over Ethernet en la interfaz web:

1. Haga clic en Administración de PoE y Configuración de PoE.
2. Especifique el modo PoE o PoE +, la prioridad y la potencia máxima (W).
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Power Over Ethernet Configuration Home - PoE Management - PoE Configuration

PoE Power Supply Configuration

Primary Power Supply [W]	0
Capacitor Detection	<input type="checkbox"/>

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
1	<input checked="" type="checkbox"/>	Low ▾	30
2	<input checked="" type="checkbox"/>	Low ▾	30
3	<input checked="" type="checkbox"/>	Low ▾	30
7	<input checked="" type="checkbox"/>	Low ▾	30
8	<input checked="" type="checkbox"/>	Low ▾	30

Figura 4-1: Configuración de PoE

Descripción de parámetros:

Configuración de la fuente de alimentación PoE

- **Fuente de alimentación primaria [W]:**
Para mostrar los vatios de la fuente de alimentación principal.
- **Detección de condensadores:**
Haga clic para habilitar o deshabilitar la configuración del condensador.

Configuración del puerto PoE

- **Puerto :**

Este es el número de puerto lógico para esta fila.

- **Modo PoE:**

El modo PoE representa el modo operativo PoE para el puerto. Habilite o deshabilite PoE.

- **Prioridad:**

La prioridad representa la prioridad de los puertos. Hay tres niveles de prioridad de energía denominados Baja, Alta y Crítica.

La prioridad se utiliza en el caso de que los dispositivos remotos requieran más energía de la que puede entregar la fuente de alimentación. En este caso, el puerto con la prioridad más baja se apagará comenzando por el puerto con el número de puerto más alto.

- **Potencia máxima [W]:**

El valor de Potencia máxima contiene un valor numérico que indica la potencia máxima en vatios que se puede entregar a un dispositivo remoto.

El valor máximo permitido es 30 W.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

4-2 Estado de PoE

Esta página permite al usuario inspeccionar el estado actual de todos los puertos PoE.

Interfaz web

Para mostrar el estado de PoE en la interfaz web:

1. Haga clic en Gestión de PoE y Estado de PoE
2. Desplácese "Actualización automática" para activar / desactivar.
3. Haga clic en "Actualizar" para actualizar las estadísticas detalladas del puerto.

Power Over Ethernet Status Home > PoE Management > PoE Status

Auto-refresh off

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	154[W]	0[W]	0[W]	0[mA]	Low	No PD detected
2	0	154[W]	0[W]	0[W]	0[mA]	Low	No PD detected
3	0	154[W]	0[W]	0[W]	0[mA]	Low	No PD detected
6	0	154[W]	0[W]	0[W]	0[mA]	Low	No PD detected
7	0	154[W]	0[W]	0[W]	0[mA]	Low	No PD detected
8	0	154[W]	0[W]	0[W]	0[mA]	Low	No PD detected

Figura 4-2: Estado de PoE

Descripción de parámetros:

- **Puerto local:**

Este es el número de puerto lógico para esta fila.

- **Clase PD:**

Cada PD se clasifica según una clase que define la potencia máxima que utilizará el PD. La clase PD muestra la clase PD.

Se definen cinco clases:

Clase 0: Máx. potencia 15,4 W

Clase 1: Max. potencia 4.0 W

Clase 2: Max. potencia 7.0 W

Clase 3: Max. potencia 15,4 W

Clase 4: Max. potencia 30.0 W

- **Poder solicitado:**

La potencia solicitada muestra la cantidad de potencia solicitada que el PD desea reservar.

- **Poder asignado:**

La energía asignada muestra la cantidad de energía que el switch ha asignado para el PD.

- **Energía usada:**

La energía usada muestra cuánta energía está usando actualmente el PD.

- **Usado actual:**

La energía usada muestra cuánta corriente está usando actualmente el PD.

- **Prioridad:**

La Prioridad muestra la prioridad del puerto configurada por el usuario.

- **Estado del puerto:**

El estado del puerto muestra el estado del puerto. El estado puede ser uno de los siguientes valores:

PoE no disponible - No se encontró ningún chip PoE - PoE no es compatible con el puerto.

PoE desactivado - PoE desactivado: PoE está desactivado por el usuario.

PoE apagado - Se excedió el presupuesto de energía - La energía total solicitada o utilizada por los PD excede la energía máxima que la fuente de energía puede entregar, y los puertos con la prioridad más baja están apagados.

No se detectó PD: no se detectó PD para el puerto.

PoE apagado - Sobrecarga de PD - El PD ha solicitado o usado más energía de la que el puerto puede entregar y está apagado.

PoE apagado - PD está apagado.

PD no válido: se detectó PD, pero no funciona correctamente.

Botones



Figura 4-2: Los botones de estado de PoE

- **Autorefreshar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

5-1 Configuración de VLAN

Para asignar una VLAN específica para fines de administración. La VLAN de administración se utiliza para establecer una conexión IP al conmutador desde una estación de trabajo conectada a un puerto en la VLAN. Esta conexión admite una sesión VSM y SNMP. De forma predeterminada, la VLAN de administración activa es la VLAN 1, pero puede designar cualquier VLAN como la VLAN de administración mediante la ventana VLAN de administración. Solo una VLAN de administración puede estar activa a la vez.

Cuando especifica una nueva VLAN de administración, se pierde su conexión HTTP a la VLAN de administración anterior. Por esta razón, debe tener una conexión entre su estación de administración y un puerto en la nueva VLAN de administración o conectarse a la nueva VLAN de administración a través de una ruta de varias VLAN.

Interfaz web

Para configurar la configuración de membresía de VLAN en la interfaz web:

1. Haga clic en Administración de VLAN y configuración de VLAN.
2. Especifique VLAN existentes, tipo de Ether para puertos S personalizados.
3. Haga clic en Aplicar.

VLAN Configuration Home > VLAN Management > VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88a8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1
2	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1

Apply Reset

Figura 5-1: Configuración de VLAN

Descripción de parámetros:

Configuración de VLAN global

- **VLAN de acceso permitido:**

Este campo muestra las VLAN que se crean en el conmutador.

De forma predeterminada, solo existe la VLAN 1. Se pueden crear más VLAN utilizando una sintaxis de lista donde el

los elementos individuales están separados por comas. Los rangos se especifican con un guión que separa el límite superior e inferior.

El siguiente ejemplo creará las VLAN 1, 10, 11, 12, 13, 200 y 300: 1,10-13,200,300. Se permiten espacios entre los delimitadores.

- **Ethertype para puertos S personalizados:**

Este campo especifica el ethertype / TPID (especificado en hexadecimal) utilizado para los puertos S personalizados. La configuración está en vigor para todos los puertos cuyo Tipo de puerto se establece en S-Custom-Port.

Configuración de puerto VLAN

- **Puerto :**

Este es el número de puerto lógico de esta fila.

- **Modo :**

El modo de puerto (el predeterminado es Acceso) determina el comportamiento fundamental del puerto en cuestión. Un puerto puede estar en uno de los tres modos que se describen a continuación.

Siempre que se seleccione un modo en particular, los campos restantes de esa fila aparecerán atenuados o se podrán modificar según el modo en cuestión.

Los campos en gris muestran el valor que obtendrá el puerto cuando se aplique el modo.

Acceso:

Los puertos de acceso se utilizan normalmente para conectarse a las estaciones finales. Las funciones dinámicas como Voice VLAN pueden agregar el puerto a más VLAN en segundo plano. Los puertos de acceso tienen las siguientes características:

- Miembro de exactamente una VLAN, la VLAN de puerto (también conocida como VLAN de acceso), que por defecto es 1,
- acepta marcos sin etiquetar y marcos con etiqueta C,
- descarta todas las tramas que no están clasificadas en la VLAN de acceso,
- en la salida, todas las tramas se transmiten sin etiquetar.

Maletero:

Los puertos troncales pueden transportar tráfico en varias VLAN simultáneamente y normalmente se utilizan para conectarse a otros conmutadores. Los puertos troncales tienen las siguientes características:

- De forma predeterminada, un puerto troncal es miembro de todas las VLAN existentes. Esto puede estar limitado por el uso de VLAN permitidas,
- a menos que VLAN Trunking esté habilitado en el puerto, las tramas clasificadas en una VLAN de la que el puerto no es miembro se descartarán,
- De forma predeterminada, todas las tramas, excepto las clasificadas en la VLAN de puerto (también conocida como VLAN nativa) se etiquetan en la salida. Las tramas clasificadas en la VLAN del puerto no se etiquetan con C en la salida,
- El etiquetado de salida se puede cambiar para etiquetar todos los marcos, en cuyo caso solo se aceptan los marcos etiquetados al ingresar,
- Es posible que esté habilitado el enlace troncal VLAN.

Híbrido:

Los puertos híbridos se asemejan a los puertos troncales en muchos aspectos, pero agregan características de configuración de puertos adicionales. Además de las características descritas para los puertos troncales, los puertos híbridos tienen estas capacidades:

- Se puede configurar para que no reconozca la etiqueta VLAN, la etiqueta C, la etiqueta S o la etiqueta personalizada S,
- se puede controlar el filtrado de entrada,
- La aceptación de entrada de tramas y la configuración del etiquetado de salida se pueden configurar de forma independiente.

- **Puerto VLAN:**

Determina el ID de VLAN del puerto (también conocido como PVID). Las VLAN permitidas están en el rango de 1 a 4095, el valor predeterminado es 1.

Al ingresar, las tramas se clasifican en la VLAN del puerto si el puerto está configurado como VLAN inconsciente, la trama no está etiquetada o el reconocimiento de VLAN está habilitado en el puerto, pero la trama tiene una etiqueta de prioridad (ID de VLAN = 0).

En la salida, las tramas clasificadas en la VLAN del puerto no se etiquetan si la configuración de Etiquetado de salida está configurada para desmarcar la VLAN del puerto.

La VLAN de puerto se denomina "VLAN de acceso" para los puertos en modo de acceso y VLAN nativa para los puertos en modo troncal o híbrido.

- **Tipo de puerto:**

Los puertos en modo híbrido permiten cambiar el tipo de puerto, es decir, si la etiqueta VLAN de una trama se usa para clasificar la trama al ingresar a una VLAN en particular y, de ser así, a qué TPID reacciona. Asimismo, en la salida, el tipo de puerto determina el TPID de la etiqueta, si se requiere una etiqueta.

Inconsciente:

Al ingresar, todas las tramas, ya sea que lleven una etiqueta VLAN o no, se clasifican en la VLAN del puerto y las posibles etiquetas no se eliminan al salir.

Puerto C:

Al ingresar, las tramas con una etiqueta VLAN con TPID = 0x8100 se clasifican en la ID de VLAN incrustada en la etiqueta. Si una trama no está etiquetada o tiene una etiqueta de prioridad, la trama se clasifica en el puerto VLAN. Si los marcos deben etiquetarse en la salida, se etiquetarán con una etiqueta C.

Deporte:

Al ingresar, las tramas con una etiqueta VLAN con TPID = 0x8100 o 0x88A8 se clasifican en la ID de VLAN incrustada en la etiqueta. Si una trama no está etiquetada o tiene una etiqueta de prioridad, la trama se clasifica en el puerto VLAN. Si los marcos deben etiquetarse en la salida, se etiquetarán con una etiqueta S.

Puerto S-personalizado:

Al ingresar, las tramas con una etiqueta VLAN con un TPID = 0x8100 o igual al Ethertype configurado para puertos Custom-S se clasifican según la ID de VLAN incrustada en la etiqueta. Si una trama no está etiquetada o tiene una etiqueta de prioridad, la trama se clasifica en el puerto VLAN. Si los marcos deben etiquetarse en la salida, se etiquetarán con la etiqueta S personalizada.

- **Filtrado de entrada:**

Los puertos híbridos permiten cambiar el filtrado de entrada. Los puertos de acceso y troncales siempre tienen habilitado el filtrado de entrada.

Si el filtrado de entrada está habilitado (la casilla de verificación está marcada), las tramas clasificadas en una VLAN de la que el puerto no es miembro se descartan.

Si el filtrado de entrada está deshabilitado, las tramas clasificadas en una VLAN de la que el puerto no es miembro se aceptan y se envían al motor de conmutación. Sin embargo, el puerto nunca transmitirá tramas clasificadas a VLAN de las que no sea miembro.

- **Troncalización de VLAN:**

Los puertos híbridos y troncales permiten habilitar el enlace troncal VLAN.

Cuando el enlace troncal de VLAN está habilitado, las tramas clasificadas en VLAN desconocidas se aceptan en el puerto tanto si el filtrado de entrada está habilitado como si no.

Esto es útil en escenarios donde una nube de conmutadores intermediarios debe puentear VLAN que no se han creado. Al configurar los puertos que conectan la nube de conmutadores como puertos troncales, pueden transportar sin problemas esas VLAN de un extremo al otro.

- **Aceptación de ingreso:**

Los puertos híbridos permiten cambiar el tipo de tramas que se aceptan al ingresar.

Etiquetado y sin etiquetar

Se aceptan marcos etiquetados y sin etiquetar.

Solo etiquetado

Solo se aceptan tramas etiquetadas al ingresar. Los fotogramas sin etiquetar se descartan.

Solo sin etiquetar

Solo se aceptan tramas sin etiquetar al ingresar. Los fotogramas etiquetados se descartan.

- **Etiquetado de salida:**

Los puertos en modo Troncal e Híbrido pueden controlar el etiquetado de tramas en la salida.

Desmarcar VLAN del puerto

Las tramas clasificadas en el puerto VLAN se transmiten sin etiquetar. Otras tramas se transmiten con la etiqueta correspondiente.

Etiquetar todo

Todas las tramas, ya sean clasificadas en el puerto VLAN o no, se transmiten con una etiqueta.

Desmarcar todo

Todas las tramas, ya sean clasificadas en el puerto VLAN o no, se transmiten sin etiqueta. Esta opción solo está disponible para puertos en modo híbrido.

- **VLAN permitidas:**

Los puertos en modo Trunk e Hybrid pueden controlar de qué VLAN se les permite convertirse en miembros. Los puertos de acceso solo pueden ser miembros de una VLAN, la VLAN de acceso.

La sintaxis del campo es idéntica a la sintaxis utilizada en el campo VLAN existentes. De forma predeterminada, un puerto puede convertirse en miembro de todas las VLAN posibles y, por lo tanto, se establece en 1-4095.

El campo puede dejarse vacío, lo que significa que el puerto no será miembro de ninguno de los

VLAN, pero si está configurado para VLAN Trunking **será S** hasta poder transportar todas las VLAN desconocidas.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

5-2 Membresía de VLAN

Esta página proporciona una descripción general del estado de membresía de los usuarios de VLAN.

Los puertos pertenecen a la unidad de pila actualmente seleccionada, como se refleja en el encabezado de la página.

Interfaz web

Para configurar la configuración de membresía de VLAN en la interfaz web:

1. Haga clic en Administración de VLAN y membresía de VLAN.
2. Desplácese por la barra para elegir qué VLAN le gustaría que aparezcan.
3. Haga clic en Actualizar para actualizar el estado.

VLAN Membership Status Home > VLAN Management > VLAN Membership

Auto-refresh Refresh Clear

Show entries Search:

VLAN ID	Port Members										Untagged Port Members									
	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Previous 1 Next

Figura 7-2: Membresía de VLAN

Descripción de parámetros:

- **USUARIO DE VLAN:**

El módulo de usuario de VLAN utiliza servicios de la funcionalidad de administración de VLAN para configurar membresías de VLAN y configuraciones de puertos de VLAN como PVID y UVID. Actualmente admitimos los siguientes tipos de usuarios de VLAN:

CLI / Web / SNMP: Estos se conocen como estáticos.

NAS: NAS proporciona autenticación basada en puertos, que implica comunicaciones entre un solicitante, un autenticador y un servidor de autenticación.

MVRP: El Protocolo de registro de VLAN múltiple (MVRP) permite el registro dinámico y la cancelación del registro de VLAN en los puertos de una red con puente de VLAN.

VLAN de voz: La VLAN de voz es una VLAN configurada especialmente para el tráfico de voz que generalmente se origina en teléfonos IP.


MVR: MVR se utiliza para eliminar la necesidad de duplicar el tráfico de multidifusión para los suscriptores en cada VLAN. El tráfico de multidifusión para todos los canales se envía solo en una única VLAN (multidifusión).


MSTP: El protocolo de árbol de expansión múltiple 802.1s (MSTP) utiliza VLAN para crear múltiples árboles de expansión en una red, lo que mejora significativamente la utilización de los recursos de la red mientras mantiene un entorno sin bucles.


- **ID de VLAN:**

ID de VLAN para la que se muestran los miembros del puerto.

- **Miembros del puerto (configuración de VLAN 功能不同 要做修改)**

Se muestra una fila de casillas de verificación para cada puerto para cada ID de VLAN. Si se incluye un puerto en una VLAN, una imagen  será mostrado.

Si un puerto está incluido en una lista de puertos prohibidos, una imagen  será mostrado.

Si un puerto está incluido en una lista de puertos prohibidos y el usuario de VLAN dinámica registra una VLAN en el mismo puerto prohibido, el puerto de conflicto se mostrará como .

- **Miembros del puerto no etiquetados:**

La interfaz es un miembro sin etiquetar de la VLAN. Las tramas de la VLAN se envían sin etiquetar a la interfaz VLAN.

- **Membresía de VLAN:**

La página de estado de membresía de VLAN mostrará los miembros del puerto de VLAN actuales para todas las VLAN configuradas por un usuario de VLAN seleccionado (la selección se permitirá mediante un cuadro combinado). Cuando se seleccionan TODOS los usuarios de VLAN, se mostrará esta información para todos los usuarios de VLAN, y esto es por defecto. La membresía de VLAN permite que las tramas clasificadas según el ID de VLAN se reenvíen a los respectivos puertos miembros de VLAN.

- **Mostrar entradas:**

Puedes elegir cuántos artículos quieres lucir.

- **Buscar :**

Puede buscar la información que desea ver.

Botones



Figura 5-2: Los botones de pertenencia a VLAN

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

- **Claro :**

Haga clic para borrar la página.

- **Próximo :**

Actualiza las entradas del registro del sistema, pase a la página siguiente.

- **Anterior :**

Actualiza las entradas del registro del sistema, pase a la página anterior.

5-3 Estado del puerto VLAN

La función Estado del puerto recopila la información de todos los estados de las VLAN y la informa por orden de Static NAS MVRP MVP Voice VLAN MSTP GVRP Combined.

Interfaz web

Para mostrar el estado del puerto VLAN en la interfaz web:

1. Haga clic en Administración de VLAN y estado del puerto de VLAN.
2. Especifique la VLAN de voz estática NAS MVRP MVP MSTP GVRP combinada.
3. Visualice la información del estado del puerto.

VLAN Port Status Home > VLAN Management > VLAN Port Status

Auto-refresh

Port	Port Type	Ingress Filter	Frame Type	Port VLAN ID	Tx Tag
1	C-Port	true	All	1	None
2	C-Port	false	Tagged	1	All
3	C-Port	false	Untagged	1	All except-native
8	C-Port	true	All	1	None
9	C-Port	true	All	1	None
10	C-Port	true	All	1	None

Figura 5-3: Estado del puerto VLAN

Descripción de parámetros:

USUARIO DE VLAN

El módulo de usuario de VLAN utiliza los servicios de la funcionalidad de administración de VLAN para configurar las membresías de VLAN y la configuración del puerto de VLAN, como PVID, UVID. Actualmente admitimos los siguientes tipos de usuarios de VLAN:

CLI / Web / SNMP: Estos se conocen como estáticos.

NAS: NAS proporciona autenticación basada en puertos, que implica comunicaciones entre un solicitante, un autenticador y un servidor de autenticación.

VLAN de voz: La VLAN de voz es una VLAN configurada especialmente para el tráfico de voz que generalmente se origina en teléfonos IP.

MVR: MVR se utiliza para eliminar la necesidad de duplicar el tráfico de multidifusión para los suscriptores en cada VLAN. El tráfico de multidifusión para todos los canales se envía solo en una única VLAN (multidifusión).

MSTP: El protocolo de árbol de expansión múltiple 802.1s (MSTP) utiliza VLAN para crear múltiples árboles de expansión en una red, lo que mejora significativamente la utilización de los recursos de la red mientras mantiene un entorno sin bucles.

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila.
- **Tipo de puerto:**

Muestra el tipo de puerto. El tipo de puerto puede ser desconocido, puerto C, puerto S, puerto S personalizado.

Si el tipo de puerto no es consciente, todas las tramas se clasifican según el ID de la VLAN del puerto y las etiquetas no se eliminan. El puerto C es el puerto del cliente. El puerto S es el puerto de servicio. El puerto S personalizado es un puerto S con TPID personalizado.

- **Filtrado de entrada:**

Muestra el filtrado de entrada en un puerto. Este parámetro afecta el procesamiento de entrada de VLAN. Si el filtrado de entrada está habilitado y el puerto de entrada no es miembro de la VLAN clasificada, la trama se descarta.

- **Tipo de marco :**

Muestra si el puerto acepta todos los marcos o solo los marcos etiquetados. Este parámetro afecta el procesamiento de entrada de VLAN. Si el puerto solo acepta tramas etiquetadas, las tramas no etiquetadas recibidas en ese puerto se descartan.

- **ID de VLAN del puerto:**

Muestra el ID de VLAN del puerto (PVID) que un usuario determinado desea que tenga el puerto.

El campo está vacío si no lo reemplaza el usuario seleccionado.

- **Etiqueta Tx:**

Muestra el estado del marco de filtrado de salida, ya sea etiquetado o sin etiquetar.

Botones



Figura 5-3: Botones de estado del puerto VLAN

- **Autofrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

- **Claro :**

Haga clic para borrar la página.

6-1 Configuración global

Utilice la página Configuración global para establecer el comportamiento de confianza para el modo básico de QoS. Esta configuración está activa cuando el switch está en el modo básico de QoS. Los paquetes que ingresan a un dominio de QoS se clasifican en el borde del dominio de QoS.

Interfaz web

Para configurar los ajustes globales en la interfaz web:

1. Haga clic en Calidad de servicio y configuración global.
2. Seleccione el modo de confianza cuando el conmutador esté en el modo básico de QoS. Si un nivel de CoS de paquete y una etiqueta DSCP se asignan a colas separadas, el modo de confianza determina la cola a la que se asigna el paquete.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

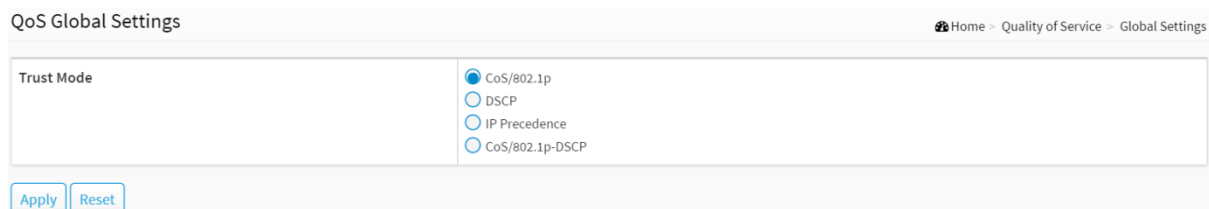


Figura 6-1: Configuración global de QoS

Descripción de parámetros:

Modo de confianza

- **CoS / 802.1p:**

El tráfico se asigna a las colas según el campo VPT en la etiqueta VLAN, o según el valor CoS / 802.1p predeterminado por puerto (si no hay una etiqueta VLAN en el paquete entrante), la asignación real del VPT a la cola puede configurarse en la página CoS / 802.1p to Queue.

- **DSCP:**

Todo el tráfico IP se asigna a las colas según el campo DSCP en el encabezado IP. La asignación real del DSCP a la cola se puede configurar en la página DSCP to Queue. Si el tráfico no es tráfico IP, se asigna a la cola de mejor esfuerzo.

- **Prioridad de IP:**

El tráfico se asigna a las colas según la precedencia de IP. La asignación real de la precedencia de IP a la cola se puede configurar en la página Precedencia de IP a la cola.

- **CoS / 802.1p-DSCP:**

Utiliza el modo Trust CoS para tráfico que no es IP y el modo Trust DSCP para tráfico IP.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-2 Configuración de puerto

Interfaz web

Para configurar la configuración del puerto de QoS en la interfaz web:

1. Haga clic en Calidad de servicio y configuración del puerto.
2. Seleccione Modo, CoS predeterminado, CoS de origen, CoS de observación para cada puerto.
3. Haga clic en qué puerto necesita para habilitar Observación Cos, Observación DSCP, Observación Precedencia IP
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Port Settings Home > Quality of Service > Port Settings

Port	Mode	Default CoS	Source CoS	Remark CoS	Remark DSCP	Remark IP Precedence
1	untrust	0	C-TAG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	untrust	0	C-TAG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	untrust	0	C-TAG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	untrust	0	C-TAG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Reset

Figura 6-2: Configuración del puerto de QoS

Descripción de parámetros:

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila.
- **Modo :**
 - **Desconfianza:**
Todo el tráfico de entrada en el puerto se asigna a la cola de mejor esfuerzo y no se realiza ninguna clasificación / priorización.
 - **Confianza :**
El tráfico de entrada de priorización de puertos se basa en el modo confiable configurado en todo el sistema, que es el modo confiable CoS / 802.1p, el modo confiable de precedencia IP o el modo confiable DSCP.
- **CoS predeterminado:**
Seleccione el valor CoS predeterminado que se asignará a los paquetes entrantes sin etiquetar. El rango es de 0 a 7.
- **Fuente CoS:**
El valor de CoS se determina en función de C-Tag o S-Tag para los paquetes etiquetados entrantes.
- **Observación CoS:**
Haga clic en la casilla de verificación para señalar la prioridad CoS / 802.1p para el tráfico de salida en este puerto.
- **Observación DSCP:**
Haga clic en la casilla de verificación para comentar el valor DSCP para el tráfico de salida en este puerto.
- **Observación de la precedencia de IP**

Haga clic en la casilla de verificación para comentar la precedencia de IP para el tráfico de salida en este puerto.

Nota: La prioridad de CoS / 802.1p y la prioridad de IP, o la prioridad de CoS / 802.1p y el valor de DSCP se pueden remarcar simultáneamente para el tráfico de salida en un puerto, pero el valor de DSCP y la prioridad de IP no se pueden remarcar simultáneamente.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-3 Vigilancia portuaria

Esta sección proporciona una descripción general de las políticas de puerto de entrada de QoS para todos los puertos del conmutador. La vigilancia de puertos es útil para restringir los flujos de tráfico y marcar tramas por encima de tasas específicas. La vigilancia es principalmente útil para los flujos de datos y los flujos de voz o video porque la voz y el video generalmente mantienen una tasa de tráfico constante.

Interfaz web

Para configurar las políticas de puerto de QoS en la interfaz web:

1. Haga clic en Calidad de servicio y vigilancia portuaria.
2. Haga clic en qué puerto necesita para habilitar las políticas de puerto de entrada de QoS y configure la condición de límite de velocidad.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Ingress Port Policers Home > Quality of Service > Port Policing

Port	Enable	Rate (kbps)
1	<input type="checkbox"/>	<input type="text" value="1000000"/>
2	<input type="checkbox"/>	<input type="text" value="1000000"/>
9	<input type="checkbox"/>	<input type="text" value="1000000"/>
10	<input type="checkbox"/>	<input type="text" value="1000000"/>

Figura 6-3: Configuración de las políticas de puerto de entrada de QoS

Descripción de parámetros:

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila. Haga clic en el número de puerto para configurar los programadores.
- **Activado :**
Para evocar qué puerto debe habilitar la función de políticas de puerto de entrada de QoS.
- **Velocidad :**
Para establecer el valor de límite de velocidad para este puerto, el valor predeterminado es 1000000.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

Formador de puertos 6-4

Esta sección proporciona una descripción general de los modeladores de puertos de salida de QoS para todos los puertos del conmutador. Otros, el usuario podría obtener toda la información detallada de los puertos que pertenecen a la unidad de pila seleccionada actualmente, como se refleja en el encabezado de la página.

Interfaz web

Para configurar QoS Port Shapers en la interfaz web:

1. Haga clic en Quality of Service y Port Shaper.
2. Seleccione qué puerto necesita para configurar QoS Egress Port Shaper.
3. Haga clic en qué puerto necesita habilitar y configure la condición de límite de velocidad.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Egress Port Shaper for Port 1 Home > Quality of Service > Port Shaper

Port

Queue Shaper

Queue	Enable	Rate (kbps)
0	<input type="checkbox"/>	<input type="text" value="1000000"/>
1	<input type="checkbox"/>	<input type="text" value="1000000"/>
2	<input type="checkbox"/>	<input type="text" value="1000000"/>
6	<input type="checkbox"/>	<input type="text" value="1000000"/>
7	<input type="checkbox"/>	<input type="text" value="1000000"/>

Port Shaper

Enable	Rate (kbps)
<input type="checkbox"/>	<input type="text" value="1000000"/>

Figura 6-4: El modelador de puertos de salida de QoS

Descripción de parámetros:

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila. Haga clic en el número de puerto para configurar los modeladores.

Formador de cola

- **Cola :**
El número de cola del modelador de cola en este puerto de conmutador.
- **Habilitar :**
Controla si el modelador de cola está habilitado para esta cola en este puerto de conmutador.
- **Tasa (kbps):**
Controla la velocidad del modelador de cola. El valor predeterminado es 1000000.

Formador de puertos

- **Habilitar :**

Controla si el modelador de puertos está habilitado para este puerto de conmutador.

- **Tasa (kbps):**

Controla la velocidad del modelador de puertos. El valor predeterminado es 1000000.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-5 Control de tormentas

La sección permite al usuario configurar el control Storm para el conmutador. Hay un control de velocidad de tormentas de fallas de búsqueda de destino, control de velocidad de tormentas de multidifusión y un control de velocidad de tormentas de difusión. Estos solo afectan a las tramas inundadas, es decir, tramas con un par (ID de VLAN, DMAC) que no está presente en la tabla de direcciones MAC. La configuración indica la velocidad de paquetes permitida para tráfico de unidifusión, multidifusión o difusión a través del conmutador.

Interfaz web

Para configurar los parámetros de configuración de Storm Control en la interfaz web:

1. Haga clic en Calidad de servicio y control de tormentas.
2. Haga clic en el puerto que debe habilitarse y configure la condición de límite de velocidad.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Storm Configuration Home > Quality of Service > Storm Control

Port	Broadcast		Multicast		DLF	
	Enable	Rate (pps)	Enable	Rate (pps)	Enable	Rate (pps)
1	<input type="checkbox"/>	500	<input type="checkbox"/>	500	<input type="checkbox"/>	500
2	<input type="checkbox"/>	500	<input type="checkbox"/>	500	<input type="checkbox"/>	500
9	<input type="checkbox"/>	500	<input type="checkbox"/>	500	<input type="checkbox"/>	500
10	<input type="checkbox"/>	500	<input type="checkbox"/>	500	<input type="checkbox"/>	500

Figura 6-5: Configuración de Storm Control

Descripción de parámetros:

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila. Haga clic en el número de puerto para configurar el control de tormentas.
- **Tipo de marco :**
La configuración de una fila en particular se aplica al tipo de trama que se enumera aquí: Difusión, multidifusión o DLF (error de búsqueda de destino).
- **Habilitar :**
Habilite o deshabilite el estado del control de tormentas para el tipo de trama dado.
- **Velocidad :**
La unidad de velocidad son paquetes por segundo (pps). Los valores válidos son: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K o 1024K. , 1024K, 2048K, 4096K, 8192K, 16384K o 32768K. , 1024K, 2048K, 4096K, 8192K, 16384K o 32768K.
El 1 kpps es en realidad 1002,1 pps.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-6 Programador de puertos

Esta sección proporciona una descripción general del Programador de puertos de salida de QoS para todos los puertos del conmutador, y los puertos pertenecen a la unidad de pila actualmente seleccionada, como se refleja en el encabezado de la página.

Interfaz web

Para configurar los programadores de puertos de QoS en la interfaz web:

1. Haga clic en Quality of Service y Port Scheduler.
2. Seleccione el modo de programador para cada puerto.
3. Si selecciona WRR o WFQ, puede configurar el peso.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Egress Port Scheduler Home > Quality of Service > Port Scheduler

Port	Scheduler Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	0	0	0	0	0	0	0	0
2	Strict Priority	0	0	0	0	0	0	0	0
9	Strict Priority	0	0	0	0	0	0	0	0
10	Strict Priority	0	0	0	0	0	0	0	0

Apply Reset

Figura 6-6: Horarios del puerto de salida de QoS

Descripción de parámetros:

- **Puerto :**
El puerto lógico para la configuración contenida en la misma fila.
- **Modo de programador:**
Controla si el modo de programador es "Prioridad estricta", "WRR" o "WFQ" en este puerto de conmutador.
- **Peso :**
Controla el peso de esta cola. El valor predeterminado es "0". Este valor está restringido a 1-100. Este parámetro solo se muestra si el "Modo de programador" está configurado como "Ponderado".

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-7 Asignación de CoS / 802.1p

Utilice la página CoS / 802.1p to Queue para asignar las prioridades de 802.1p a las colas de salida. La tabla CoS / 802.1p to Queue determina las colas de salida de los paquetes entrantes según la prioridad 802.1p en sus etiquetas VLAN. Para los paquetes entrantes sin etiquetar, la prioridad 802.1p será la prioridad predeterminada CoS / 802.1p asignada a los puertos de entrada.

Interfaz web

Para configurar el mapeo Cos / 802.1p en la interfaz web:

1. Haga clic en Quality of Service y Cos / 802.1p Mapping.
2. Seleccione ID de cola.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Ingress CoS/802.1p to Queue Mapping Home > Quality of Service > CoS/802.1p Mapping

CoS/802.1p	Queue ID
0	1 ▼
1	0 ▼
2	2 ▼
6	6 ▼
7	7 ▼

Apply Reset

Figura 6-7: Asignación de CoS / 802.1p de entrada de QoS a cola

Descripción de parámetros:

- **CoS / 802.1p:**
Muestra los valores de etiqueta de prioridad 802.1p que se asignarán a una cola de salida, donde 0 es la prioridad más baja y 7 es la prioridad más alta.
- **ID de cola:**
Seleccione la cola de salida a la que se asigna la prioridad 802.1p. Se admiten ocho colas de salida, donde la cola 8 es la cola de salida de mayor prioridad y la cola 1 es la cola de salida de menor prioridad.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-8 Observación de CoS / 802.1p

Utilice la página Colas a CoS / 802.1p para indicar la prioridad de CoS / 802.1p para el tráfico de salida de cada cola.

Interfaz web

Para configurar Cos / 802.1p Remarking en la interfaz web:

1. Haga clic en Quality of Service y Cos / 802.1p Remarking.
2. Seleccione CoS / 802.1p.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Egress Queue to CoS/802.1p Remarking Home > Quality of Service > CoS/802.1p Remarking

Queue ID	CoS/802.1p
0	0 ▼
1	1 ▼
2	2 ▼
6	6 ▼
7	7 ▼

Apply Reset

Figura 6-8: Cola de salida de QoS para remarcación de CoS / 802.1p

Descripción de parámetros:

- **ID de cola:**
Muestra el ID de la cola, donde la cola 8 es la cola de salida de mayor prioridad y la cola 1 es la cola de salida de menor prioridad.
- **CoS / 802.1p:**
Para cada cola de salida, seleccione la prioridad CoS / 802.1p a la que se comenta el tráfico de salida de la cola.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-9 Asignación de precedencia de IP

Para asignar la precedencia de IP a la cola de salida.

Interfaz web

Para configurar la asignación de precedencia de IP en la interfaz web:

1. Haga clic en Quality of Service and IP Precedence Mapping.
2. Seleccione ID de cola.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Ingress IP Precedence to Queue Mapping Home > Quality of Service > IP Precedence Mapping

IP Precedence	Queue ID
0	0 ▼
1	1 ▼
2	2 ▼
6	6 ▼
7	7 ▼

Apply Reset

Figura 6-9: Precedencia de IP de entrada de QoS al mapeo de cola

Descripción de parámetros:

- **Prioridad de IP:**

Muestra los valores de etiqueta de prioridad de precedencia de IP que se asignarán a una cola de salida, donde 0 es la prioridad más baja y 7 es la prioridad más alta.

- **ID de cola:**

Seleccione la cola de salida a la que se asigna la prioridad de precedencia de IP. Se admiten ocho colas de salida, donde la cola 8 es la cola de salida de mayor prioridad y la cola 1 es la cola de salida de menor prioridad.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-10 Observación de precedencia de IP

Para asignar la cola de salida a la precedencia de IP.

Interfaz web

Para configurar el remarcado de precedencia de IP en la interfaz web:

1. Haga clic en Quality of Service and IP Precedence Remarking.
2. Seleccione Precedencia de IP.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Egress Queue to IP Precedence Remarking Home > Quality of Service > IP Precedence Remarking

Queue ID	IP Precedence
0	0 ▼
1	1 ▼
2	2 ▼
6	6 ▼
7	7 ▼

Apply Reset

Figura 6-10: La cola de salida de QoS para el remarcado de precedencia de IP

Descripción de parámetros:

- **ID de cola:**
Muestra el ID de la cola, donde la cola 8 es la cola de salida de mayor prioridad y la cola 1 es la cola de salida de menor prioridad.
- **Prioridad de IP:**
Para cada cola de salida, seleccione la prioridad de precedencia de IP a la que se comenta el tráfico de salida de la cola.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-11 Mapeo DSCP

Utilice la página DSCP to Queue para asignar IP DSCP a las colas de salida. La tabla DSCP to Queue determina las colas de salida de los paquetes IP entrantes en función de sus valores DSCP. La etiqueta de prioridad de VLAN (VPT) original del paquete no se modifica.

Es posible lograr la QoS deseada en una red simplemente cambiando el DSCP a la asignación de cola, el método de programación de la cola y la asignación de ancho de banda.

Interfaz web

Para configurar el mapeo DSCP en la interfaz web:

1. Haga clic en Quality of Service and DSCP Mapping.
2. Seleccione ID de cola.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Ingress DSCP to Queue Mapping Home - Quality of Service - DSCP Mapping

DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID	DSCP	Queue ID
0 (BE)	0	16 (CS2)	16	32 (CS4)	32	48 (CS6)	48
1	1	17	17	33	33	49	49
2	2	18 (AF21)	18	34 (AF41)	34	50	50
3	3	19	19	35	35	51	51
4	4	20 (AF22)	20	36 (AF42)	36	52	52
5	5	21	21	37	37	53	53
6	6	22 (AF23)	22	38 (AF43)	38	54	54
7	7	23	23	39	39	55	55
8 (CS1)	8	24 (CS3)	24	40 (CS5)	40	56 (CS7)	56
9	9	25	25	41	41	57	57
10 (AF11)	10	26 (AF31)	26	42	42	58	58
11	11	27	27	43	43	59	59
12 (AF12)	12	28 (AF32)	28	44	44	60	60
13	13	29	29	45	45	61	61
14 (AF13)	14	30 (AF33)	30	46 (EF)	46	62	62
15	15	31	31	47	47	63	63

Apply Reset

Figura 6-11: Asignación de DSCP a cola de entrada de QoS

Descripción de parámetros:

- **DSCP:**
Muestra el valor DSCP en el paquete entrante y su clase asociada.
- **ID de cola:**
Seleccione la cola de reenvío de tráfico del menú desplegable Cola de salida al que se asigna el valor DSCP.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

6-12 Observación DSCP

Utilice la página Colas a DSCP para comentar el valor de DSCP para el tráfico de salida de cada cola.

Interfaz web

Para configurar el DSCP Remarking en la interfaz web:

1. Haga clic en Quality of Service y DSCP Remarking.
2. Seleccione DSCP.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

QoS Egress Queue to DSCP Remarking Home > Quality of Service > DSCP Remarking

Queue ID	DSCP
0	0 (BE) *
1	8 (CS1) *
2	16 (CS2) *
6	48 (CS6) *
7	56 (CS7) *

Apply Reset

Figura 6-12: Cola de salida de QoS al remarcado DSCP

Descripción de parámetros:

- **ID de cola:**
Muestra el ID de la cola, donde la cola 8 es la cola de salida de mayor prioridad y la cola 1 es la cola de salida de menor prioridad.
- **DSCP:**
Para cada cola de salida, seleccione la prioridad DSCP a la que se comenta el tráfico de salida de la cola.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

El Protocolo de árbol de expansión (STP) se puede utilizar para detectar y deshabilitar bucles de red y para proporcionar enlaces de respaldo entre conmutadores, puentes o enrutadores. Esto permite que el conmutador interactúe con otros dispositivos de puente (es decir, un conmutador, puente o enrutador compatible con STP) en su red para garantizar que solo exista una ruta entre dos estaciones en la red, y proporcionar enlaces de respaldo que toman el control automáticamente cuando un enlace principal deja de funcionar.

STP - STP utiliza un algoritmo distribuido para seleccionar un dispositivo de puente (conmutador, puente o enrutador compatible con STP) que sirve como raíz de la red de árbol de expansión. Selecciona un puerto raíz en cada dispositivo de puente (excepto el dispositivo raíz) que incurre en el costo de ruta más bajo al reenviar un paquete desde ese dispositivo al dispositivo raíz. Luego selecciona un dispositivo de puente designado de cada LAN que incurre en el costo de ruta más bajo al reenviar un paquete desde esa LAN al dispositivo raíz. Todos los puertos conectados a los dispositivos de puente designados se asignan como puertos designados. Después de determinar el árbol de expansión de menor costo, habilita todos los puertos raíz y los puertos designados, y deshabilita todos los demás puertos. Por lo tanto, los paquetes de red solo se reenvían entre los puertos raíz y los puertos designados, lo que elimina cualquier posible bucle de red.

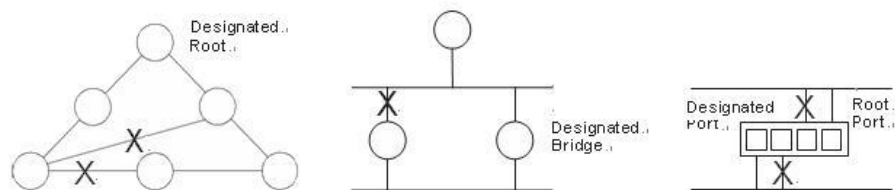


Figura 9: Protocolo de árbol de expansión

Una vez que se ha establecido una topología de red estable, todos los puentes escuchan Hello BPDU (unidades de datos de protocolo de puente) transmitidas desde el puente raíz. Si un puente no recibe un saludo BPDU después de un intervalo predefinido (edad máxima), el puente asume que el enlace al puente raíz está caído. Este puente iniciará negociaciones con otros puentes para reconfigurar la red y restablecer una topología de red válida.

7-1 Estado

La sección describe que puede seleccionar habilitar o no el protocolo de árbol de expansión, y puede seleccionar qué versión de protocolo desea.

Interfaz web

Para configurar la versión del Protocolo de árbol de expansión en la interfaz web:

1. Haga clic en Árbol de expansión y estado.
2. Evocar para habilitar o deshabilitar el protocolo de árbol de expansión. Seleccione la
3. versión del Protocolo de árbol de expansión.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

MSTP State Home > Spanning Tree > State

Multiple Spanning Tree Protocol	<input type="checkbox"/> off
Force Version	MSTP ▾

Figura 7-1: El estado del árbol de expansión

Descripción de parámetros:

- **Protocolo de árbol de expansión múltiple:**

Puede seleccionar habilitar el protocolo de árbol de expansión o no.

- **Forzar versión:**

La configuración de la versión del protocolo STP. Los valores válidos son STP, RSTP y MSTP.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

7-2 Configuración de región

La sección describe cómo configurar la identificación básica de un puente MSTP. Los puentes que participan en una región MST común deben tener el mismo nombre de región y nivel de revisión.

Interfaz web

Para configurar Region Config en la interfaz web:

5. Haga clic en Spanning Tree and Region Config. Especifique el nombre de
6. la región y el nivel de revisión. Haga clic en Aplicar para guardar la
7. configuración.
8. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

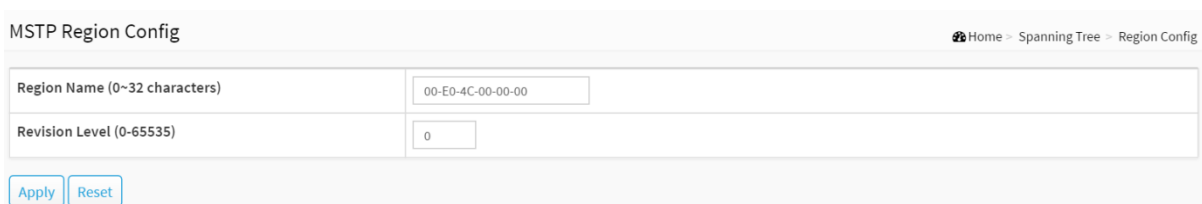


Figura 7-2: Configuración de la región

Descripción de parámetros:

- **Nombre de configuración:**
El nombre que identifica la asignación de VLAN a MSTI. Los puentes deben compartir el nombre y la revisión (ver más abajo), así como la configuración de mapeo de VLAN a MSTI para compartir árboles de expansión para MSTI (intrarregión). El nombre tiene un máximo de 32 caracteres.
- **Revisión de configuración:**
La revisión de la configuración de MSTI mencionada anteriormente. Debe ser un número entero entre 0 y 65535.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

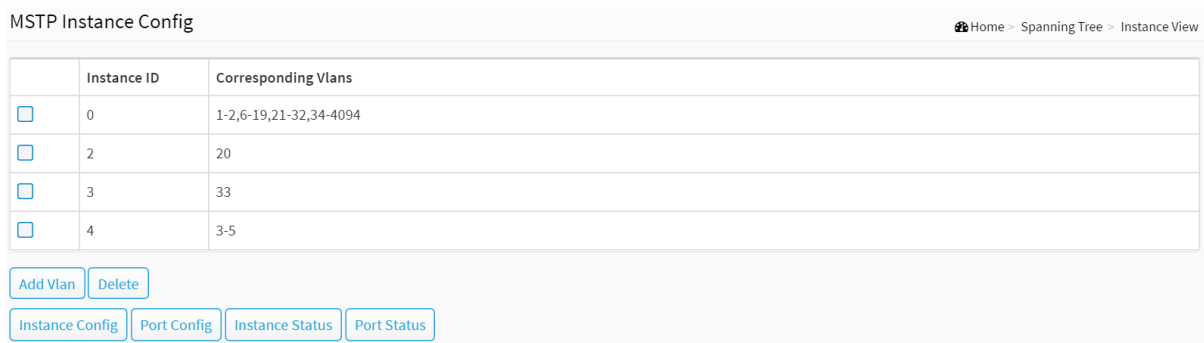
7-3 Vista de instancia

La sección que proporciona una tabla de instancias de MST que incluye información (membresía vlan de un MSTI) de todas las instancias de expansión aprovisionadas en la región de MST particular a la que pertenece el puente. A través de esta tabla, se pueden aplicar datos de configuración de MSTP adicionales y se puede recuperar el estado de MSTP.

Interfaz web

Para configurar la instancia MSTP en la interfaz web:

1. Haga clic en Árbol de expansión e instancia. Haga clic para
2. agregar vlan.
3. Especifique la instancia y el puerto.
4. Haga clic en Estado de la instancia y Estado del puerto para ver los detalles.
5. Si desea cancelar la configuración, debe hacer clic en Eliminar.



	Instance ID	Corresponding Vlans
<input type="checkbox"/>	0	1-2,6-19,21-32,34-4094
<input type="checkbox"/>	2	20
<input type="checkbox"/>	3	33
<input type="checkbox"/>	4	3-5

[Add Vlan](#) [Delete](#)
[Instance Config](#) [Port Config](#) [Instance Status](#) [Port Status](#)

Figura 7-3: Configuración de instancia MSTP

Descripción de parámetros:

- **ID de instancia:**
Cada instancia de árbol de expansión debe tener un ID de instancia único dentro de 0 ~ 4095. La instancia 0 (CIST) siempre existe y no se puede eliminar. Se pueden agregar o eliminar instancias de expansión adicionales (MSTI). Se debe proporcionar al menos un vlan para que un MSTI declare la necesidad de que exista el MSTI.

- **Vlans correspondientes:**

0-4095.

Varias VLAN pueden pertenecer a un MSTI. Todos los vlans que no se aprovisionan a través de esto se asignarán automáticamente a la Instancia 0 (CIST).

Botones

- **Agregar Vlan:**
Para agregar un MSTI y proporcionar sus miembros de vlan o modificar miembros de vlan para un MSTI específico, puede agregar hasta 63 para que un total de 64.
- **Borrar :**
Para eliminar un MSTI.

- **Configuración de instancia:**
Para aprovisionar parámetros de rendimiento del árbol de expansión por instancia.
- **Configuración de puerto:**
Para aprovisionar parámetros de rendimiento de árbol de expansión por instancia por puerto.
- **Estado de la instancia:**
Para mostrar el informe de estado de una instancia de árbol de expansión en particular.
- **Estado del puerto:**
Para mostrar el informe de estado de todos los puertos con respecto a una instancia de árbol de expansión específica.

Consulte la siguiente introducción:

- **Agregar Vlan:**

MSTP Create MSTI/Add Vlan Mapping

Instance ID	<input type="text"/>
Vlan Mapping	<input type="text"/>

Figura 7-3: Agregar Vlan

Descripción de parámetros:

- **ID de instancia:**
El rango es 1-4094
- **Mapeo de Vlan:**
La lista de VLAN asignadas al MSTI. Las VLAN se pueden proporcionar como una sola (xx, xx está entre 1 y 4094) VLAN, o un rango (xx-yy), cada una de las cuales debe estar separada por una coma y / o un espacio. Una VLAN solo se puede asignar a un MSTI. Un MSTI no utilizado debe dejarse vacío. (Es decir, no tener ninguna VLAN asignada). Ejemplo: 2,5,20-40.

Botones

- **Aplicar :**
Haga clic para guardar los cambios.
- **Reiniciar :**
Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.
- **Cancelar :**
Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.

- **Configuración de instancia a instancia 0:**

Instance Configuration (ID=0) Home > Spanning Tree > Instance View

Priority	32768
Max. Age	20 seconds
Forward Delay	15 seconds
Max. Hops	20 seconds

Figura 7-3: Configuración de instancia a instancia 0

Descripción de parámetros:

- **Prioridad:**

El parámetro de prioridad utilizado en la conexión CIST (Common and Internal Spanning Tree).

0/4096/8192/12288/16384/20480/24576/28672/32768/36864/40960/45056/49152/53248/57344/61440

- **MAX. Edad :**

6-40 seg. La misma definición que en el protocolo RSTP.

- **Retraso de reenvío:**

4-30 seg. La misma definición que en el protocolo RSTP.

- **MAX. Lúpulo:**

6-40 seg. Es un nuevo parámetro para el protocolo de árbol de expansión múltiple. Se utiliza en las instancias internas del árbol de expansión. Los "saltos restantes de CIST" o "saltos restantes de MSTI" en el mensaje del protocolo del árbol de expansión se reducirían en uno cuando el mensaje se propague al puente vecino. Si los saltos restantes en un mensaje son cero, el mensaje (BPDU) se considerará no válido. Max Hops se utiliza para especificar el valor inicial de los saltos restantes para el puente raíz regional (ya sea la raíz regional CIST o la raíz regional MSTI).

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

- **Atrás :**

Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.

- **Configuración del puerto a la instancia 0:**

Port Config								Migration Check
Port	Path Cost	Priority	Admin Edge	Admin P2P	Restricted Role	Restricted TCN	Mcheck	
1	Auto	128	Yes	Auto	No	No	---	
2	Auto	128	Yes	Auto	No	No	---	
3	Auto	128	Yes	Auto	No	No	---	
8	Auto	128	Yes	Auto	No	No	---	
9	Auto	128	Yes	Auto	No	No	---	
10	Auto	128	Yes	Auto	No	No	---	

Apply Back

Figura 7-3: Configuración del puerto a la instancia 0

Descripción de parámetros:

- Puerto :**

El puerto lógico para la configuración contenida en la misma fila.
- Costo de ruta:**

1 - 200 000 000

La misma definición que en la especificación RSTP. Pero en MSTP, este parámetro se puede aplicar respectivamente a los puertos de CIST y a los puertos de cualquier MSTI.
- Prioridad:**

0/16/32/48/64/80/96/112/128/144/160/176/192/208/224/240

La misma definición que en la especificación RSTP. Pero en MSTP, este parámetro se puede aplicar respectivamente a los puertos de CIST y a los puertos de cualquier MSTI.
- Admin Edge:**

Sí No

La misma definición que en la especificación RSTP para los puertos CIST.
- Administrador P2P:**

Auto / Verdadero / Falso

La misma definición que en la especificación RSTP para los puertos CIST.
- Rol restringido:**

Sí No

Si "Sí" hace que el puerto no se seleccione como puerto raíz para el CIST o cualquier MSTI, incluso si tiene el mejor vector de prioridad de árbol de expansión. Dicho puerto se seleccionará como puerto alternativo después de que se haya seleccionado el puerto raíz. Este parámetro es "No" por defecto. Si se establece, puede provocar una falta de conectividad de árbol de expansión. Lo establece un administrador de red para evitar que los puentes externos a una región central de la red influyan en la topología activa del árbol de expansión, posiblemente porque esos puentes no están bajo el control total del administrador.
- TCN restringido:**

Sí No

Si "Sí" hace que el puerto no propague las notificaciones de cambio de topología recibidas y los cambios de topología a otros puertos. Este parámetro es "No" por defecto. Si se configura, puede causar

Pérdida temporal de conectividad después de cambios en la topología activa de árboles de expansión como resultado de información persistente de ubicación de la estación aprendida incorrectamente. Lo establece un administrador de red para evitar puentes externos a una región central de la red, lo que provoca la eliminación de direcciones en esa región, posiblemente porque esos puentes no están bajo el control total del administrador. O el estado de funcionamiento de MAC para las LAN conectadas cambia con frecuencia.

- **Mcheck:**

La misma definición que en la especificación RSTP para los puertos CIST.

Botones

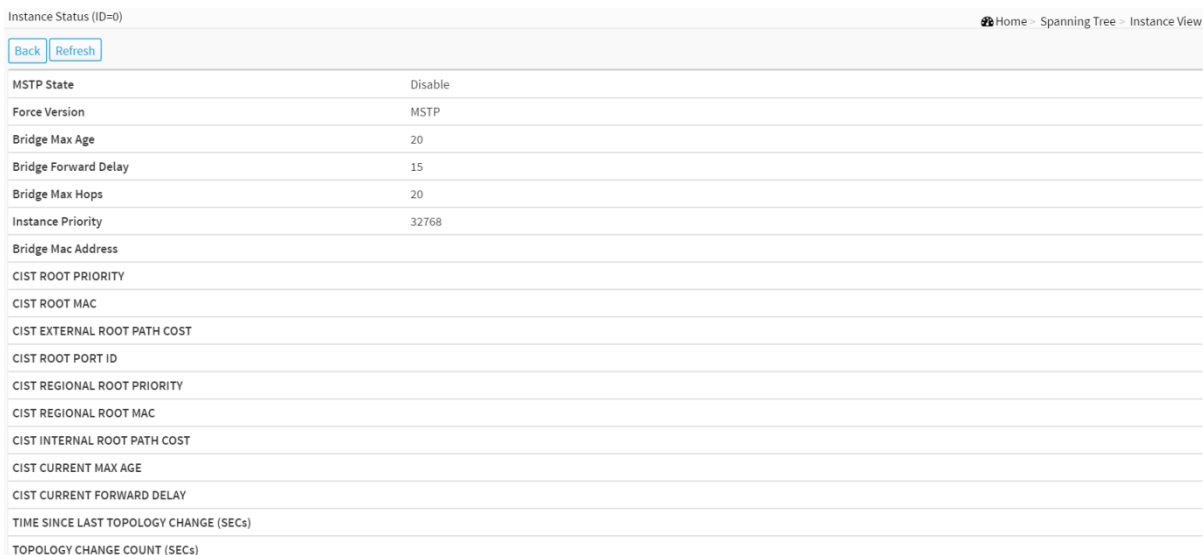
- **Aplicar :**

Haga clic para guardar los cambios.

- **Atrás :**

Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.

- **Estado de la instancia a la instancia 0:**



Instance Status (ID=0)	
MSTP State	Disable
Force Version	MSTP
Bridge Max Age	20
Bridge Forward Delay	15
Bridge Max Hops	20
Instance Priority	32768
Bridge Mac Address	
CIST ROOT PRIORITY	
CIST ROOT MAC	
CIST EXTERNAL ROOT PATH COST	
CIST ROOT PORT ID	
CIST REGIONAL ROOT PRIORITY	
CIST REGIONAL ROOT MAC	
CIST INTERNAL ROOT PATH COST	
CIST CURRENT MAX AGE	
CIST CURRENT FORWARD DELAY	
TIME SINCE LAST TOPOLOGY CHANGE (SECS)	
TOPOLOGY CHANGE COUNT (SECS)	

Figura 7-3: Estado de la instancia a la instancia 0

Descripción de parámetros:

- **Estado MSTP:**

El protocolo MSTP es Activado o Desactivado.

- **Forzar versión:**

Muestra la versión actual del protocolo de árbol de expansión configurada.

- **Edad máxima del puente:**

Muestra la configuración de Max Age del puente en sí.

- **Retardo de reenvío del puente:**

Muestra la configuración de Retraso de reenvío del puente en sí .

- **Bridge Max Hops:**

Muestra la configuración de Max Hops del puente en sí.

- **Prioridad de instancia:**

Valor de prioridad del árbol de expansión para una instancia de árbol específica (CIST o MSTI).

- **Dirección Mac del puente:**

La dirección Mac del propio puente.
- **PRIORIDAD DE LA RAÍZ DE LA CIST:**

Valor de prioridad del árbol de expansión del puente raíz CIST.
- **MAC DE RAÍZ DE CIST:**

Dirección Mac del puente raíz CIST.
- **COSTO DE LA RUTA DE LA RAÍZ EXTERNA DE CIST:**

Valor del costo de la ruta raíz desde el punto de vista de la región MST del puente.
- **ID DE PUERTO RAÍZ CIST:**

El ID de puerto del puerto raíz del puente. En MSTP, el puerto del mismo nivel de un puerto raíz puede residir en una región de MST diferente o en la misma región de MST. El primer caso indica que el propietario del puerto raíz es el puente raíz regional CIST.
- **PRIORIDAD DE RAÍZ REGIONAL DE LA CIST:**

Valor de prioridad del árbol de expansión del puente raíz regional CIST. Tenga en cuenta que el puente raíz regional CIST es diferente del puente raíz CIST. Una excepción es que cuando un puente que pertenece a una región MST resulta ser el puente raíz del CST (Common Spanning Tree). Una región MST en el CST se puede considerar como un puente RSTP común. El IST (Internal Spanning Tree) y los MSTI son transparentes para los puentes fuera de esta región.
- **MAC DE RAÍZ REGIONAL CIST:**

Dirección Mac del puente raíz regional CIST.
- **COSTO DE LA RUTA DE LA RAÍZ INTERNA DE LA CIST:**

Valor del costo de la ruta raíz desde el punto de vista de los puentes dentro del IST.
- **EDAD MÁXIMA ACTUAL CIST:**

Edad máxima del puente raíz CIST.
- **RETRASO DE AVANCE CORRIENTE CIST:**

Retraso de reenvío del puente raíz CIST.
- **TIEMPO DESDE EL ÚLTIMO CAMBIO DE TOPOLOGÍA (SEC):**

El tiempo transcurrido desde el último cambio de topología es el tiempo transcurrido en unidades de segundos para que se produzca un grupo de "cambios de topología y (o) recepción de notificaciones de cambio de topología". Cuando se repita una nueva serie de cambios de topología, este contador se restablecerá a 0.
- **RECUENTO DE CAMBIOS DE TOPOLOGÍA (SEC):**

El recuento de cambios de topología por instancia de árbol de expansión expresa el tiempo transcurrido en unidades de segundos desde el comienzo del cambio de topología del árbol de expansión hasta el final de la convergencia de STP. Una vez que no se produce ningún cambio de topología y no se reciben más notificaciones de cambio de topología, el recuento de cambios de topología se restablecerá a 0.

Botones

- **Atrás :**

Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.
- **Actualizar :**

Haga clic para actualizar la página.

- **Estado del puerto a la instancia 0:**

Port Status of Instance 0

Home - Spanning Tree - Instance View

Back Refresh

Port No	Status	Role	Path Cost	Priority	Hello	Oper. Edge	Oper. P2P	Restricted Role	Restricted Tcn
1	FORWARDING	DSGN	200000	128	2	V	V		
2	DISCARDING	disable	20000000	128	2	V			
3	DISCARDING	disable	20000000	128	2	V			
8	DISCARDING	disable	20000000	128	2	V			
9	DISCARDING	disable	20000000	128	2	V			
10	DISCARDING	disable	20000000	128	2	V			

Figura 7-3: Estado del puerto a la instancia 0

Descripción de parámetros:

- **Puerto No:**
El número de puerto al que se aplica la configuración.
 - **Estado:**
El estado de reenvío. Misma definición que la especificación RSTP. Los valores posibles son "FORWARDING", "LEARNING", "DISCARDING"
 - **Papel:**
El papel que desempeña un puerto en la topología del árbol de expansión. Los valores posibles son "deshabilitar" (deshabilitar puerto), "alternativo" (puerto alternativo), "respaldo" (puerto de respaldo), "ROOT" (puerto raíz), "DSGN" (puerto designado), "MSTR" (puerto maestro) . Los últimos 3 son roles de puerto posibles para que un puerto transite al estado de REENVÍO.
 - **Costo de ruta:**
Muestra el valor del costo de la ruta del puerto resuelto actualmente para cada puerto en una instancia de árbol de expansión en particular.
 - **Prioridad:**
Muestra el valor de prioridad de puerto para cada puerto en una instancia de árbol de expansión en particular.
 - **Hola:**
Visualización de Hello Time por puerto. Toma la siguiente forma:
Configuración actual de Hello Time / Hello Time.
 - **Oper. Borde:**
Si un puerto es un puerto Edge en realidad.
 - **Oper. P2P:**
Si un puerto es o no un puerto punto a punto en realidad.
 - **Rol restringido:**
Igual que se menciona en "Configuración de puerto".
 - **Tcn restringido:**
Igual que se menciona en "Configuración de puerto".
- Botones**
- **Atrás :**
Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.
 - **Actualizar :**
Haga clic para actualizar la página.

8-1 Configuración

La conmutación de tramas se basa en la dirección DMAC contenida en la trama. El conmutador crea una tabla que asigna las direcciones MAC a los puertos del conmutador para saber a qué puertos deben ir las tramas (según la dirección DMAC en la trama). Esta tabla contiene entradas tanto estáticas como dinámicas. El administrador de la red configura las entradas estáticas si el administrador desea realizar una asignación fija entre la dirección DMAC y los puertos del conmutador.

Las tramas también contienen una dirección MAC (dirección SMAC), que muestra la dirección MAC del equipo que envía la trama. El conmutador utiliza la dirección SMAC para actualizar automáticamente la tabla MAC con estas direcciones MAC dinámicas. Las entradas dinámicas se eliminan de la tabla MAC si no se ha visto ninguna trama con la dirección SMAC correspondiente después de un tiempo de antigüedad configurable

Interfaz web

Para configurar la tabla de direcciones MAC en la interfaz web:

1. Haga clic en Configuración y tablas de direcciones MAC.
2. Especifique Desactivar envejecimiento automático y Tiempo de envejecimiento.
3. Especifique los miembros del puerto (automático, desactivado, seguro).
4. Agregue una nueva entrada estática, especifique la dirección IP y Mac de la VLAN, los miembros del puerto, el bloque.
5. Haga clic en Aplicar.

MAC Table Configuration Home > MAC Address Table > Configuration

Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Aging Time	300 seconds

MAC Table Learning

	Port Member									
	1	2	3	4	5	6	7	8	9	10
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

Delete	VLAN ID	MAC Address	Block	Port Member
<input type="checkbox"/>	1	00-00-00-00-00-00	<input type="checkbox"/>	Port 1
<input type="checkbox"/>	2	00-00-00-00-00-00	<input type="checkbox"/>	Port 2
<input type="checkbox"/>	3	00-00-00-00-00-00	<input type="checkbox"/>	Port 3

Figura 8-1: Configuración de la tabla de direcciones MAC

Descripción de parámetros:

Configuración de envejecimiento:

De forma predeterminada, las entradas dinámicas se eliminan de la tabla MAC después de 300 segundos. Esta eliminación también se llama envejecimiento.

Configure el tiempo de envejecimiento ingresando aquí un valor en segundos; por ejemplo, Segundos de tiempo de edad.

El rango permitido es de 10 a 1000000 segundos.

Deshabilite el envejecimiento automático de las entradas dinámicas marcando



Desactive el envejecimiento automático.

Aprendizaje de tabla MAC

Si el modo de aprendizaje para un puerto determinado está atenuado, otro módulo tiene el control del modo, por lo que el usuario no puede cambiarlo. Un ejemplo de un módulo de este tipo es la autenticación basada en MAC según 802.1X. Cada puerto puede realizar el aprendizaje en función de las siguientes configuraciones:

- **Auto:**

El aprendizaje se realiza automáticamente tan pronto como se recibe un marco con SMAC desconocido.

- **Desactivar :**

No se aprende.

- **Seguro:**

Solo se aprenden las entradas de MAC estáticas, todas las demás tramas se descartan.



norte BENEFICIOS SEGÚN OBJETIVOS: Asegúrese de que el enlace utilizado para administrar el switch se agregue a la Static Mac Table antes de cambiar al modo de aprendizaje seguro; de lo contrario, el enlace de administración se perderá y solo podrá restaurarse mediante otro puerto no seguro o conectándose al switch a través del Interfaz de serie.

Configuración de la tabla MAC estática

Las entradas estáticas en la tabla MAC se muestran en esta tabla. La tabla MAC estática puede contener 64 entradas. El máximo de 64 entradas es para toda la pila, no por conmutador.

La tabla MAC se ordena primero por ID de VLAN y luego por dirección MAC.

- **Borrar :**

Marque para borrar la entrada. Se eliminará durante el próximo guardado.

- **ID de VLAN:**

El ID de VLAN de la entrada.

- **Dirección MAC :**

La dirección MAC de la entrada.

- **Cuadra :**

Haga clic en él si desea bloquear esta dirección mac.

- **Miembros del puerto:**

Las marcas de verificación indican qué puertos son miembros de la entrada. Marque o desmarque según sea necesario para modificar la entrada.

Botones

- **Agregar una nueva entrada estática:**

Haga clic para agregar una nueva entrada a la tabla MAC estática. Especifique el ID de VLAN, la dirección MAC y los miembros del puerto para la nueva entrada. Haga clic en "Aplicar".

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

8-2 Información

Las entradas en la tabla MAC se muestran en esta página. La tabla MAC contiene hasta 8192 entradas y se ordena primero por ID de VLAN y luego por dirección MAC.

Interfaz web

Para mostrar la tabla de direcciones MAC en la interfaz web:

1. Haga clic en Información y tabla de direcciones MAC.
2. Visualice la tabla de direcciones MAC.

Dynamic MAC Table Home -> MAC Address Table -> Information

Auto-refresh off Refresh Clear

Show entries Search:

Type	VLAN	MAC Address	Block	CPU	Port Members											
					1	2	3	4	5	6	7	8	9	10		
Static	1	00-00-00-00-00-00	No		✓											
Dynamic	1	00-E0-4C-36-14-16	No		✓											
Static	2	00-00-00-00-00-00	No			✓										
Static	3	00-00-00-00-00-00	No				✓									

Previous **1** Next

Figura 8-2: Información de la tabla de direcciones MAC

Descripción de parámetros:

Navegando por la tabla MAC

Cada página muestra hasta 999 entradas de la tabla MAC, el valor predeterminado es 20, seleccionado a través del campo de entrada "entradas por página". Cuando se visita por primera vez, la página web mostrará las primeras 20 entradas desde el principio de la tabla MAC. El primero que se muestra será el que tenga la ID de VLAN más baja y la dirección MAC más baja que se encuentra en la tabla MAC.

Los campos de entrada "Iniciar desde dirección MAC" y "VLAN" permiten al usuario seleccionar el punto de inicio en la Tabla MAC. Al hacer clic en el botón "Actualizar", se actualizará la tabla mostrada a partir de esa o la siguiente coincidencia de tabla MAC más cercana. Además, los dos campos de entrada, al hacer clic en el botón "Actualizar", asumirán el valor de la primera entrada mostrada, lo que permitirá una actualización continua con la misma dirección de inicio.

El >> utilizará la última entrada de los pares de direcciones VLAN / MAC mostrados actualmente como base para la próxima búsqueda. Cuando se llega al final, el texto "No más entradas" se muestra en la tabla mostrada. Utilice el botón << para empezar de nuevo.

- **Switch (solo pila)**

La unidad de pila donde se aprende la entrada.

- **Escribe :**

Indica si la entrada es estática o dinámica, 802.1x, DMS.

- **VLAN:**

El ID de VLAN de la entrada.

- **Dirección MAC :**

La dirección MAC de la entrada.

- **Cuadra :**

Si la dirección mac está bloqueada o no.

- **Miembros del puerto:**

Los puertos que son miembros de la entrada.

Botones



Figura 8-2: Botones de información de la tabla de direcciones MAC

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

- **Claro :**

Haga clic para borrar la página.

- **Próximo :**

Actualiza las entradas del registro del sistema, pase a la página siguiente.

- **Anterior :**

Actualiza las entradas del registro del sistema, pase a la página anterior.



norte BENEFICIOS SEGÚN OBJETIVOS:

00-40-C7-73-01-29: la dirección MAC de su conmutador (para IPv4) 33-33-00-00-00-01: MAC de destino (para anuncio de enrutador IPv6) (referencia IPv6 RA.JPG)

33-33-00-00-00-02: MAC de destino (para solicitud de enrutador IPv6) (referencia IPv6 RS.JPG)

33-33-FF-73-01-29: MAC de destino (para solicitud de vecino IPv6) (referencia IPv6 DAD.JPG)

33-33-FF-A8-01-01: la dirección MAC de su conmutador (para IP global IPv6)

FF-FF-FF-FF-FF-FF: para difusión.

9-1 Inspección IGMP

La función se utiliza para establecer los grupos de multidifusión para reenviar el paquete de multidifusión a los puertos miembros y, por naturaleza, evita desperdiciar el ancho de banda mientras los paquetes de multidifusión IP se ejecutan en la red. Esto se debe a que un conmutador que no admite IGMP o IGMP Snooping no puede distinguir el paquete de multidifusión del paquete de transmisión, por lo que solo puede tratarlos a todos como el paquete de transmisión. Sin IGMP Snooping, la función de reenvío de paquetes de multidifusión es sencilla y nada es diferente del paquete de difusión.

Un conmutador admitido IGMP Snooping con las funciones de consulta, informe y salida, un tipo de paquete intercambiado entre IP Multicast Router / Switch y IP Multicast Host, puede actualizar la información de la tabla Multicast cuando un miembro (puerto) se une o abandona una IP Dirección de destino de multidifusión. Con esta función, una vez que un conmutador recibe un paquete de multidifusión IP, reenviará el paquete a los miembros que se unieron a un grupo de multidifusión IP especificado anteriormente.

Los paquetes serán descartados por IGMP Snooping si el usuario transmite paquetes de multidifusión al grupo de multidifusión que no se habían creado de antemano. El modo IGMP permite que el conmutador emita la función IGMP que le permite activar el proxy IGMP o espiar el conmutador, que se conecta a un enrutador más cercano a la raíz del árbol. Esta interfaz es la interfaz ascendente. El enrutador de la interfaz ascendente debe ejecutar IGMP.

9-1.1 Configuración básica

La sección describe cómo configurar el espionaje IGMP básico en el conmutador, que se conecta a un enrutador más cercano a la raíz del árbol. Esta interfaz es la interfaz ascendente. El enrutador de la interfaz ascendente debe ejecutar IGMP.

Interfaz web

Para configurar los parámetros de IGMP Snooping en la interfaz web:

1. Haga clic en Multicast, IGMP Snooping y Basic Configuration.
2. Evocar para seleccionar habilitar o deshabilitar qué configuración global.
3. Evoque qué puerto quiere convertirse en un puerto de enrutador o habilite / deshabilite la función Fast Leave.
4. Desplácese para configurar la aceleración y el perfil.
5. Haga clic en Aplicar para guardar la configuración.
6. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Global Configuration				
Snooping Enabled	<input type="radio"/> off			
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>			
IGMP SSM Range	232.0.0.0 / 8			
Proxy Enabled	<input type="checkbox"/>			

Port Related Configuration				
Port	Router Port	Fast Leave	Throttling	Profile
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	-
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	-
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	-
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	-
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited	-

Figura 9-1.1: Configuración de indagación IGMP

Descripción de parámetros:
configuración global

- Espionaje habilitado:**

Habilite la inspección global de IGMP.

- Inundación IPMCv4 no registrada habilitada:**

Habilite la inundación de tráfico IPMCv4 no registrada.

- Rango IGMP SSM:**

El rango SSM (multidifusión específica de origen) permite que los hosts y enrutadores compatibles con SSM ejecuten el modelo de servicio SSM para los grupos en el rango de direcciones. Formato: (dirección IP / submáscara)

- Proxy habilitado:**

Habilite el proxy IGMP. Esta función se puede utilizar para evitar el reenvío innecesario de unirse y dejar mensajes al enrutador.

Configuración relacionada con el puerto

- Puerto :**

Muestra el índice de puerto físico del conmutador.

- Puerto del enrutador:**

Especifique qué puertos actúan como puertos de enrutador. Un puerto de enrutador es un puerto en el conmutador Ethernet que conduce al dispositivo de multidifusión de capa 3 o al interrogador IGMP.

Si se selecciona un puerto miembro de agregación como puerto de enrutador, toda la agregación actuará como puerto de enrutador.

- Licencia rápida:**

Habilite la salida rápida en el puerto.

- Estrangulamiento:**

Habilite para limitar la cantidad de grupos de multidifusión a los que puede pertenecer un puerto de conmutador.

- Perfil:**

Puede seleccionar el perfil cuando edita en Perfil de filtrado de multidifusión.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

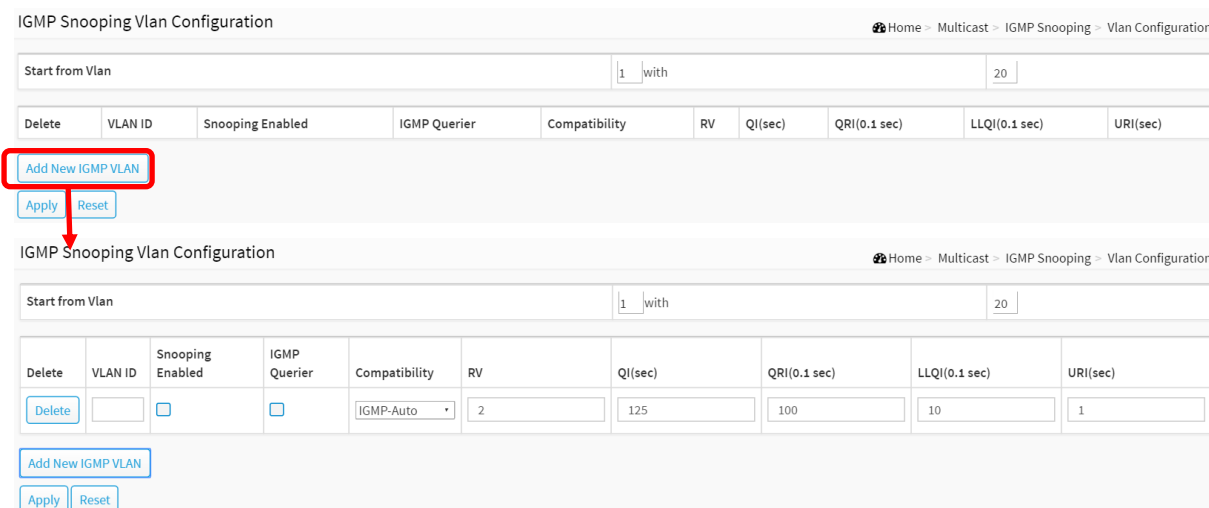
9-1.2 Configuración de VLAN

La sección describe el proceso de configuración de VLAN integrado con la función IGMP Snooping. Para Cada página de configuración muestra hasta 99 entradas de la tabla de VLAN, el valor predeterminado es 20, seleccionado a través del campo de entrada "entradas por página". Cuando se visita por primera vez, la página web mostrará las primeras 20 entradas desde el principio de la tabla VLAN. El primero que se muestra será el que tenga la ID de VLAN más baja que se encuentra en la tabla de VLAN. Los campos de entrada "VLAN" permiten al usuario seleccionar el punto de partida en la tabla VLAN. Al hacer clic en el botón, se actualizará la tabla mostrada a partir de esa o la siguiente coincidencia de tabla de VLAN más cercana.

Interfaz web

Para configurar IGMP Snooping VLAN Configuration en la interfaz web:

1. Haga clic en Multicast, IGMP Snooping and VLAN Configuration.
2. Haga clic para agregar una nueva VLAN IGMP.
3. Haga clic en Aplicar para guardar la configuración.
4. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.



IGMP Snooping Vlan Configuration Home - Multicast - IGMP Snooping - Vlan Configuration

Start from Vlan with

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)
Delete	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	IGMP-Auto	2	125	100	10	1

[Add New IGMP VLAN](#)

[Apply](#) [Reset](#)

IGMP Snooping Vlan Configuration Home - Multicast - IGMP Snooping - Vlan Configuration

Start from Vlan with

Delete	VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI(sec)	QRI(0.1 sec)	LLQI(0.1 sec)	URI(sec)
Delete	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	IGMP-Auto	2	125	100	10	1

[Add New IGMP VLAN](#)

[Apply](#) [Reset](#)

Figura 9-1.2: Configuración de VLAN de indagación IGMP

Descripción de parámetros:

- **Comience desde Vlan:**
Puede hacer clic en ellos. Actualiza la tabla mostrada a partir de los campos de entrada "VLAN".
- **Borrar :**
Marque para eliminar la entrada. La entrada designada se eliminará durante el próximo guardado.
- **ID de VLAN:**
Muestra el ID de VLAN de la entrada.
- **Espionaje habilitado:**
Habilite la indagación IGMP por VLAN. Solo se pueden seleccionar hasta 32 VLAN. .
- **Querier IGMP:**

Habilite para unirse a la elección de IGMP Querier en la VLAN. Desactivar para actuar como no interrogador IGMP.

- **Compatibilidad:**

La compatibilidad es mantenida por hosts y enrutadores que toman las acciones apropiadas según las versiones de IGMP que operan en hosts y enrutadores dentro de una red. La selección permitida es IGMP-Auto, IGMPv1 forzado, IGMPv2 forzado, IGMPv3 forzado, el valor de compatibilidad predeterminado es IGMP-Auto.

- **RV:**

Robustez Variable. La variable de robustez permite ajustar la pérdida de paquetes esperada en una red. El rango permitido es de 1 a 255; El valor predeterminado de la variable de robustez es 2.

- **QI (seg):**

Intervalo de consulta. El intervalo de consultas es el intervalo entre consultas generales enviadas por el interrogador. El rango permitido es de 1 a 31744 segundos; el intervalo de consulta predeterminado es de 125 segundos.

- **QRI (0,1 segundos):**

Intervalo de respuesta a la consulta. El tiempo de respuesta máximo utilizado para calcular el código de respuesta máxima insertado en las consultas generales periódicas. El rango permitido es de 0 a 31744 en décimas de segundo; El intervalo de respuesta de consulta predeterminado es 100 en décimas de segundo (10 segundos).

- **LLQI (0,1 segundos):**

Intervalo de consulta del último miembro. El tiempo de consulta del último miembro es el valor de tiempo representado por el intervalo de consulta del último miembro, multiplicado por el recuento de consultas del último miembro. El rango permitido es de 0 a 31744 en décimas de segundo; el intervalo predeterminado de consulta del último miembro es 10 en décimas de segundo (1 segundo).

- **URI (seg):**

Intervalo de informe no solicitado. El intervalo de informes no solicitados es el tiempo entre las repeticiones del informe inicial de membresía de un anfitrión en un grupo. El rango permitido es de 0 a 31744 segundos, el intervalo de informe no solicitado predeterminado es de 1 segundo. .

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

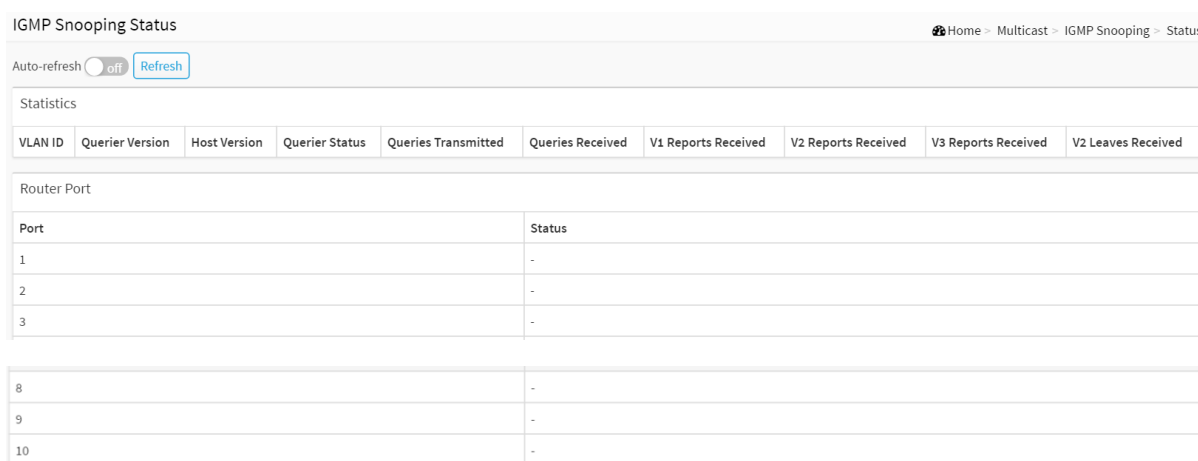
9-1.3 Estado

Después de completar la configuración de IGMP Snooping, puede dejar que el conmutador muestre el estado de IGMP Snooping. La sección le permite permitir que el interruptor muestre el estado de detalle de IGMP Snooping.

Interfaz web

Para mostrar el estado de IGMP Snooping en la interfaz web:

1. Haga clic en Multicast, IGMP Snooping and Status.
2. Si desea actualizar automáticamente la información, debe activar la "Actualización automática".
3. Haga clic en "Actualizar" para actualizar el estado de indagación IGMP.



VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
Router Port									
Port	Status								
1	-								
2	-								
3	-								
8	-								
9	-								
10	-								

Figura 9-1.3: Estado de indagación IGMP

Descripción de parámetros:

Estadística

- **ID de VLAN:**
El ID de VLAN de la entrada.
- **Versión de consulta:**
Versión de consulta de trabajo actualmente.
- **Versión de host:**
Versión de host de trabajo actualmente.
- **Estado del interrogador:**
Muestra que el estado del interrogador es "ACTIVO" o "INACTIVO".
"DESHABILITADO" indica que la interfaz específica está deshabilitada administrativamente.
- **Consultas transmitidas:**
El número de consultas transmitidas.
- **Consultas recibidas:**
El número de consultas recibidas.

- **Informes V1 recibidos:**

El número de informes V1 recibidos.

- **Informes V2 recibidos:**

El número de informes V2 recibidos.

- **Informes V3 recibidos:**

El número de informes V3 recibidos.

- **Hojas V2 recibidas:**

El número de hojas V2 recibidas.

Puerto del enrutador

Muestra qué puertos actúan como puertos de enrutador. Un puerto de enrutador es un puerto en el conmutador Ethernet que conduce al dispositivo de multidifusión de capa 3 o al interrogador IGMP. Estático denota que el puerto específico está configurado para ser un puerto de enrutador. Dinámico denota que se aprende que el puerto específico es un puerto de enrutador. Ambos indican que el puerto específico está configurado o se aprende a ser un puerto de enrutador.

- **Puerto**

Número de puerto del conmutador.

- **Estado**

Indique si el puerto específico es un puerto de enrutador o no.

Botones



Figura 9-1.3: Los botones de estado de inspección IGMP

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

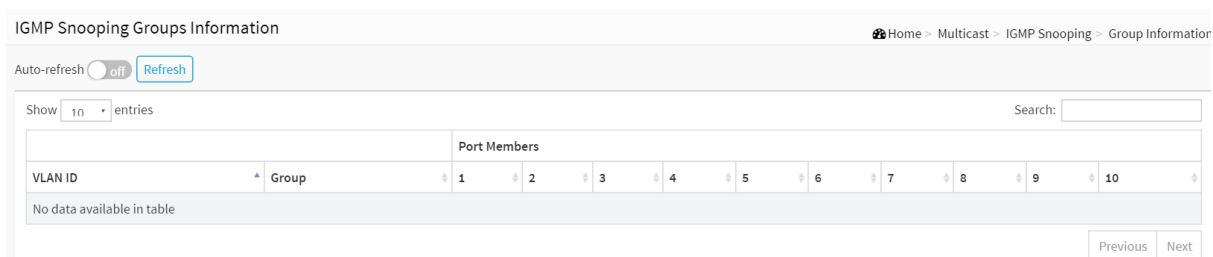
9-1.4 Información de grupo

Después de completar la configuración de la función IGMP Snooping, puede dejar que el conmutador muestre la información del grupo IGMP Snooping. Las entradas en la tabla de grupos IGMP se muestran en esta página. La tabla de grupos IGMP se ordena primero por ID de VLAN y luego por grupo. Utilizará la última entrada de la tabla mostrada actualmente como base para la siguiente búsqueda. Cuando se llega al final, el texto "No más entradas" se muestra en la tabla mostrada. Utilice el botón para empezar de nuevo.

Interfaz web

Para mostrar la información del grupo de indagación IGMP en la interfaz web:

1. Haga clic en Multidifusión, Inspección IGMP e Información de grupo.
2. Especifique cuántas entradas mostrar en una página.
3. Si desea actualizar automáticamente la información, debe activar la opción "Actualizar automáticamente".
4. Haga clic en "Actualizar" para actualizar una entrada de la información de los grupos de indagación IGMP.
5. Haga clic en Anterior / siguiente para cambiar de página.



IGMP Snooping Groups Information Home > Multicast > IGMP Snooping > Group Information

Auto-refresh off

Show entries Search:

VLAN ID	Group	Port Members									
		1	2	3	4	5	6	7	8	9	10
No data available in table											

Figura 9-1.4: Información de los grupos de indagación IGMP

Descripción de parámetros:

Navegación por la tabla de grupos IGMP

Cada página muestra hasta 99 entradas de la tabla del Grupo IGMP, el valor predeterminado es 20, seleccionado a través del campo de entrada "entradas por página". Cuando se visita por primera vez, la página web mostrará las primeras 20 entradas desde el principio de la tabla de grupos IGMP.

Los campos de entrada "Iniciar desde VLAN" y "grupo" permiten al usuario seleccionar el punto de partida en la tabla de grupos IGMP. Al hacer clic en el botón, se actualizará la tabla mostrada a partir de esa o la siguiente coincidencia de tabla de grupo IGMP más cercana. Además, los dos campos de entrada, al hacer clic en un botón, asumirán el valor de la primera entrada mostrada, lo que permitirá una actualización continua con la misma dirección de inicio.

Utilizará la última entrada de la tabla mostrada actualmente como base para la siguiente búsqueda. Cuando se llega al final, el texto "No más entradas" se muestra en la tabla mostrada. Utilice el botón para empezar de nuevo.

- **Buscar :**

Puede buscar la información que desea ver.

- **Mostrar entradas:**

Puedes elegir cuántos artículos quieres lucir.

- **ID de VLAN:**

ID de VLAN del grupo.

- **Grupos:**

Dirección de grupo del grupo mostrado.

- **Miembros del puerto:**

Puertos de este grupo.

Botones



Figura 9-1.4: Botones de información de grupos de indagación IGMP

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

- **Próximo :**

Actualiza las entradas del registro del sistema, pase a la página siguiente.

- **Anterior :**

Actualiza las entradas del registro del sistema, pase a la página anterior.

9-1.5 Información de IGMP SFM

Las entradas en la tabla de información IGMP SFM se muestran en esta página. La tabla de información IGMP SFM (multidifusión filtrada en origen) también contiene la información de SSM (multidifusión específica de origen). Esta tabla está ordenada primero por ID de VLAN, luego por grupo y luego por puerto. Las diferentes direcciones de origen que pertenecen al mismo grupo se tratan como una sola entrada.

Interfaz web

Para mostrar la información de IGMP SFM en la interfaz web:

1. Haga clic en Multicast, IGMP Snooping e IGMP SFM Information.
2. Si desea actualizar automáticamente la información, debe activar la "Actualización automática".
3. Haga clic en "Actualizar" para actualizar una entrada de la información de los grupos de indagación IGMP.
4. Haga clic en Anterior / siguiente para cambiar de página.

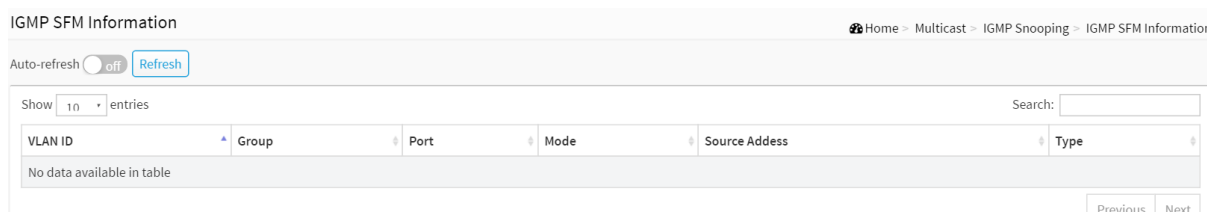


Figura 9-1.5: Información de IGMP SFM

Descripción de parámetros:

Navegación por la tabla de información de IGMP SFM

Cada página muestra hasta 99 entradas de la tabla de información IGMP SFM, el valor predeterminado es 20, seleccionado a través del campo de entrada "entradas por página". Cuando se visita por primera vez, la página web mostrará las primeras 20 entradas desde el principio de la Tabla de información de IGMP SFM.

Los campos de entrada "Start from VLAN" y "group" permiten al usuario seleccionar el punto de partida en la tabla de información IGMP SFM. Al hacer clic en el botón se actualizará la tabla mostrada a partir de esa o la siguiente coincidencia de la Tabla de información IGMP SFM más cercana. Además, los dos campos de entrada, al hacer clic en un botón, asumirán el valor de la primera entrada mostrada, lo que permitirá una actualización continua con la misma dirección de inicio.

Utilizará la última entrada de la tabla mostrada actualmente como base para la siguiente búsqueda. Cuando se llega al final, el texto "No más entradas" se muestra en la tabla mostrada. Utilice el botón para empezar de nuevo.

- **Buscar :**

Puede buscar la información que desea ver.

- **Mostrar entradas:**

Puedes elegir cuántos artículos quieres lucir.

- **ID de VLAN:**

ID de VLAN del grupo.

- **Grupo :**

Dirección de grupo del grupo mostrado.

- **Puerto :**
Número de puerto del conmutador.
- **Modo :**
Indica el modo de filtrado mantenido por (ID de VLAN, número de puerto, dirección de grupo). Puede ser Incluir o Excluir.
- **Dirección de la fuente :**
Dirección IP de la fuente. Actualmente, el sistema limita el número total de direcciones de origen IP para el filtrado a 128.
- **Escribe :**
Indica el tipo. Puede ser Permitir o Denegar.

Botones



Figura 9-1.5: Botones de información de grupos de indagación IGMP

- **Autorefrescar :**
Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.
- **Actualizar :**
Haga clic para actualizar la página inmediatamente.
- **Próximo :**
Actualiza las entradas del registro del sistema, pase a la página siguiente.
- **Anterior :**
Actualiza las entradas del registro del sistema, pase a la página anterior.

Esta sección le muestra cómo configurar los ajustes de seguridad del puerto del conmutador. Puede utilizar la función Port Security para restringir la entrada a una interfaz limitando e identificando direcciones MAC.

10-1 Gestión

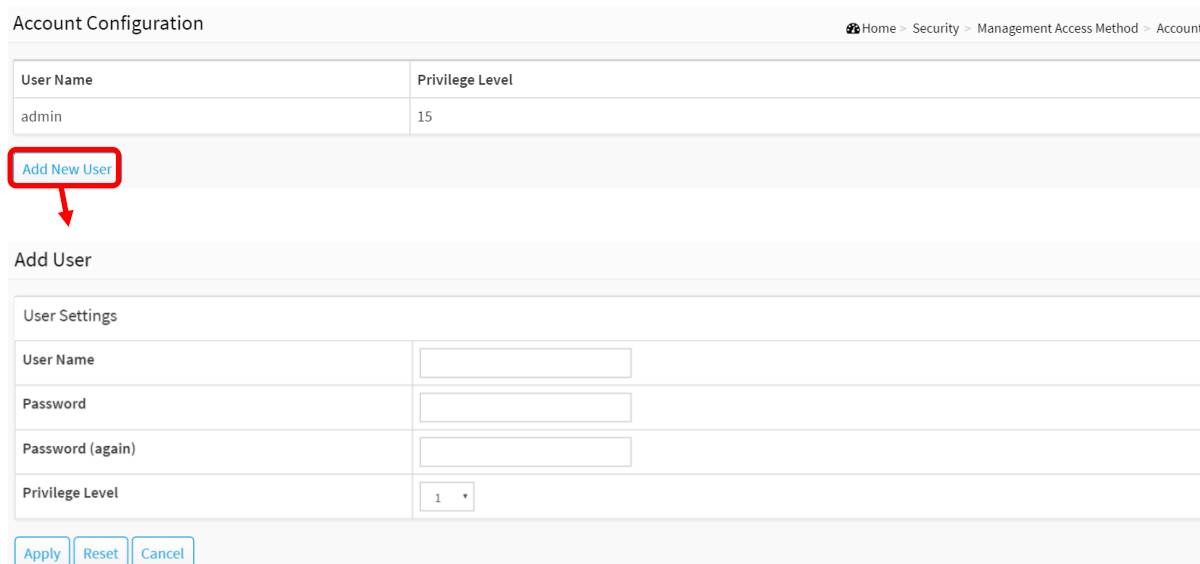
10-1.1 Cuenta

Esta página proporciona una descripción general de los usuarios actuales. Actualmente, la única forma de iniciar sesión como otro usuario en el servidor web es cerrar y volver a abrir el navegador.

Interfaz web

Para configurar Usuario en la interfaz web:

1. Haga clic en Seguridad, administración y cuenta.
2. Haga clic en Agregar nuevo usuario.
3. Especifique el parámetro Nombre de usuario.
4. Haga clic en Aplicar.



Account Configuration Home - Security - Management Access Method - Account

User Name	Privilege Level
admin	15

Add New User

Add User

User Settings

User Name	<input type="text"/>
Password	<input type="password"/>
Password (again)	<input type="password"/>
Privilege Level	1 ▾

Apply Reset Cancel

Figura 10-1.1: Configuración de la cuenta

Descripción de parámetros:

- **Nombre de usuario :**

El nombre que identifica al usuario. Este también es un enlace para Agregar / Editar usuario.

- **Contraseña :**

Para escribir la contraseña. La longitud de cadena permitida es de 0 a 255 y el contenido permitido son los caracteres ASCII de 32 a 126.

- **Contraseña de nuevo) :**

Para volver a escribir la contraseña. Debe volver a escribir la misma contraseña en el campo.

- **Nivel de privilegio :**

El nivel de privilegio del usuario. El rango permitido es de 1 a 15. Si el valor del nivel de privilegio es 15, se puede acceder a todos los grupos, es decir, se le concede el control total del dispositivo. Pero otros valores deben referirse a cada nivel de privilegio de grupo. El privilegio del usuario debe ser igual o mayor que el nivel de privilegio del grupo para tener acceso a ese grupo. De forma predeterminada, la mayoría de los grupos con nivel de privilegio 5 tiene acceso de solo lectura y el nivel de privilegio 10 tiene acceso de lectura y escritura. Y el mantenimiento del sistema (carga de software, valores predeterminados de fábrica, etc.) necesita un nivel de privilegio de usuario 15. Generalmente, el nivel de privilegio 15 se puede usar para una cuenta de administrador, el nivel de privilegio 10 para una cuenta de usuario estándar y el nivel de privilegio 5 para una cuenta de invitado. .

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

- **Cancelar :**

Haga clic para deshacer los cambios realizados localmente y volver a los usuarios.

- **Borrar usuario :**

Elimina el usuario actual. Este botón no está disponible para nuevas configuraciones (Agregar nuevo usuario).

10-1.2 Gestión de acceso

Esta sección le muestra cómo configurar la tabla de administración de acceso del conmutador, incluidos HTTP / HTTPS, SNMP. Puede administrar el conmutador a través de una LAN Ethernet o de Internet.

Interfaz web

Para configurar una configuración de administración de acceso en la interfaz web:

1. Haga clic en Seguridad, administración y administración de acceso.
2. Seleccione "activado" en el modo de configuración de gestión de acceso.
3. Haga clic en "Agregar nueva entrada".
4. Especifique la dirección IP, la longitud de la máscara.
5. Método de gestión de acceso verificado (HTTP / HTTPS, SNMP) en la entrada.
6. Haga clic en Aplicar.

Access Management Configuration Home > Security > Management Access Method > Access Management

Mode on off

Delete	VLAN ID	IP Address	Mask Length	HTTP/HTTPS	SNMP	TELNET/SSH
<input type="button" value="Delete"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Delete"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figura 10-1.2: Configuración de administración de acceso

Descripción de parámetros:

- **Modo :**

Indica el funcionamiento del modo de gestión de acceso. Los modos posibles son:

En : Habilite la operación del modo de administración de acceso.

Apagado : Desactive el funcionamiento del modo de gestión de acceso.
- **ID de VLAN:**

Indica el ID de VLAN para la entrada de administración de acceso.
- **Borrar :**

Marque para borrar la entrada. Se eliminará durante el próximo guardado.
- **Dirección IP :**

Ingrese la dirección IP de origen.
- **Longitud de la máscara:**

Ingrese la longitud de la máscara.
- **HTTP / HTTPS:**

Indica que el host puede acceder al conmutador desde la interfaz HTTP / HTTPS si la dirección IP del host coincide con el rango de direcciones IP proporcionado en la entrada.
- **SNMP:**

Indica que el host puede acceder al conmutador desde la interfaz SNMP si la dirección IP del host coincide con el rango de direcciones IP proporcionado en la entrada.

Botones

- **Agregar nueva entrada:**

Haga clic para agregar una nueva entrada de administración de acceso.

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

10-2 IEEE 802.1X

10-2.1 Configuración

La sección describe cómo configurar los parámetros 802.1X del conmutador. El 802.1X se puede utilizar para conectar a los usuarios con una variedad de recursos, incluido el acceso a Internet, conferencias telefónicas, impresión de documentos en impresoras compartidas o simplemente iniciando sesión en Internet.

Interfaz web

Para configurar IEEE 802.1X en la interfaz web:

1. Haga clic en Seguridad, IEEE 802.1X y Configuración.
2. Seleccione "activado" en el modo de configuración IEEE 802.1X.
3. Reautenticación marcada habilitada.
4. Establecer el período de reautenticación (el valor predeterminado es 3600 segundos).
5. Seleccione Estado de administrador y muestra Estado del puerto.
6. Haga clic en Aplicar para guardar la configuración.
7. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

802.1X Configuration Home > Security > IEEE 802.1X > Configuration

System Configuration

Mode	<input type="radio"/> off
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	<input type="text" value="3600"/> seconds
EAPOL Timeout	<input type="text" value="30"/> seconds

Port Configuration

Port	Admin State	Port State
1	Force Authorized	Globally Disabled
2	Force Authorized	Globally Disabled
3	Force Authorized	Globally Disabled
8	Force Authorized	Globally Disabled
9	Force Authorized	Globally Disabled
10	Force Authorized	Globally Disabled

Figura 10-2.1: Configuración IEEE 802.1X

Descripción de parámetros:

Configuración del sistema

- **Modo :**

Encendido o apagado.

Indica si IEEE 802.1X está habilitado o deshabilitado globalmente en el conmutador. Si está deshabilitado globalmente, todos los puertos pueden reenviar tramas.

- **Reautenticación habilitada:**

Si se marca, los solicitantes / clientes autenticados con éxito se vuelven a autenticar después de la

intervalo especificado por el Período de reautenticación. La reautenticación para puertos habilitados para 802.1X se puede usar para detectar si un nuevo dispositivo está conectado a un puerto de conmutador o si un solicitante ya no está conectado.

Para los puertos basados en MAC, la reautenticación solo es útil si la configuración del servidor RADIUS ha cambiado. No implica la comunicación entre el conmutador y el cliente y, por lo tanto, no implica que un cliente todavía esté presente en un puerto (consulte el período de caducidad a continuación).

- **Período de reautenticación:**

Determina el período, en segundos, después del cual un cliente conectado debe volver a autenticarse. Esto solo está activo si la casilla de verificación Reautenticación habilitada está marcada. Los valores válidos están en el rango de 1 a 3600 segundos.

- **Tiempo de espera de EAPOL:**

Determina el tiempo de retransmisión de tramas EAPOL de identidad de solicitud.

Los valores válidos están en el rango de 1 a 255 segundos. Esto no tiene ningún efecto para los puertos basados en MAC.

Configuración del puerto

- **Puerto :**

El número de puerto para el que se aplica la siguiente configuración.

- **Estado de administración:**

Si 802.1X está habilitado globalmente, esta selección controla el modo de autenticación del puerto. los siguientes modos están disponibles:

- **Fuerza autorizada:**

En este modo, el conmutador enviará una trama EAPOL Success cuando se activa el enlace del puerto, y cualquier cliente en el puerto podrá acceder a la red sin autenticación.

- **Fuerza no autorizada:**

En este modo, el conmutador enviará una trama de falla EAPOL cuando se active el enlace del puerto y no se permitirá el acceso a la red a ningún cliente en el puerto.

- **802.1X basado en puerto:**

En el mundo 802.1X, el usuario se denomina suplicante, el conmutador es el autenticador y el servidor RADIUS es el servidor de autenticación. El autenticador actúa como intermediario, reenviando solicitudes y respuestas entre el solicitante y el servidor de autenticación. Las tramas enviadas entre el solicitante y el conmutador son especiales

Tramas 802.1X, conocidas como tramas EAPOL (EAP sobre LAN). Las tramas EAPOL encapsulan las PDU EAP (RFC3748). Las tramas enviadas entre el conmutador y el servidor RADIUS son paquetes RADIUS. Los paquetes RADIUS también encapsulan las PDU EAP junto con otros atributos como la dirección IP del conmutador, el nombre y el número de puerto del solicitante en el conmutador. EAP es muy flexible, ya que permite diferentes métodos de autenticación, como MD5-Challenge, PEAP y TLS. Lo importante es que el autenticador (el conmutador) no necesita saber qué método de autenticación están usando el solicitante y el servidor de autenticación, o cuántas tramas de intercambio de información se necesitan para un método en particular. El conmutador simplemente encapsula la parte EAP de la trama en el tipo relevante (EAPOL o RADIUS) y la reenvía.

Cuando se completa la autenticación, el servidor RADIUS envía un paquete especial que contiene una indicación de éxito o fracaso. Además de enviar esta decisión al solicitante, el conmutador la utiliza para abrir o bloquear el tráfico en el puerto del conmutador conectado al solicitante.



norte BENEFICIOS SEGÚN OBJETIVOS: Suponga que dos servidores backend están habilitados y que el tiempo de espera del servidor está configurado en X segundos (usando la página de configuración AAA), y suponga que el primer servidor de la lista está actualmente inactivo (pero no

considerado muerto).

Ahora, si el solicitante retransmite las tramas de EAPOL Start a una velocidad más rápida que X segundos, nunca se autenticará, porque el conmutador cancelará las solicitudes del servidor de autenticación de backend en curso cada vez que reciba una nueva trama de EAPOL Start del suplicante.

Y dado que el servidor aún no ha fallado (porque los X segundos no han expirado), el mismo servidor será contactado en la próxima solicitud de servidor de autenticación de backend desde el conmutador. Este escenario se repetirá para siempre. Por lo tanto, el tiempo de espera del servidor debe ser menor que la tasa de retransmisión de tramas de inicio de EAPOL del solicitante.

- **Estado del puerto:**

El estado actual del puerto. Puede asumir uno de los siguientes valores:

Desactivado globalmente: IEEE 802.1X está desactivado globalmente.

Enlace inactivo: IEEE 802.1X está habilitado globalmente, pero no hay ningún enlace en el puerto.

Autorizado: el puerto está en modo Autorizado en vigor o un solo solicitante y el solicitante está autorizado.

No autorizado: el puerto está en modo Forzado no autorizado o en modo de un solo suplicante y el servidor RADIUS no ha autorizado correctamente al suplicante.

X Auth / Y Unauth: el puerto está en modo de múltiples suplicantes. Actualmente, X clientes están autorizados y Y no están autorizados.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

10-2.2 Estado

La sección describe cómo mostrar la información de estado de cada puerto 802.1X del conmutador. El estado incluye el estado del administrador, el estado del puerto, la última fuente, la última identificación y la identificación de la VLAN del puerto.

Interfaz web

Para mostrar el estado de 802.1X en la interfaz web:

1. Haga clic en Seguridad, IEEE 802.1X y Estado.
2. Marcó "Actualización automática".
3. Haga clic en "Actualizar" para actualizar las estadísticas detalladas del puerto.
4. Puede seleccionar qué puerto desea que muestre las estadísticas 802.1X.

802.1X Status Home - Security - IEEE 802.1X - Status

Auto-refresh off

Port	Admin State	Port State	Last Source	Last ID	Port VLAN ID
1	Force Authorized	Globally Disabled			0
2	Force Authorized	Globally Disabled			0
3	Force Authorized	Globally Disabled			0
8	Force Authorized	Globally Disabled			0
9	Force Authorized	Globally Disabled			0
10	Force Authorized	Globally Disabled			0

Figura 10-2.2: Estado de IEEE 802.1X

Descripción de parámetros:

Estado 802.1X

- **Puerto :**

El número de puerto del conmutador. Haga clic para navegar a las estadísticas detalladas de 802.1X para este puerto.
- **Estado de administración:**

Estado administrativo actual del puerto. Consulte Estado de administración de 802.1X para obtener una descripción de los posibles valores.
- **Estado del puerto:**

El estado actual del puerto. Consulte Estado del puerto 802.1X para obtener una descripción de los estados individuales.
- **Última fuente:**

La dirección MAC de origen contenida en la trama EAPOL recibida más recientemente para la autenticación basada en EAPOL y la trama recibida más recientemente de un nuevo cliente para la autenticación basada en MAC.
- **Última identificación:**

El nombre de usuario (identidad del solicitante) que se incluye en la trama EAPOL de identidad de respuesta recibida más recientemente para la autenticación basada en EAPOL, y la dirección MAC de origen de la trama recibida más recientemente de un nuevo cliente para la autenticación basada en MAC.
- **ID de VLAN del puerto:**

El ID de VLAN en el que 802.1X ha puesto el puerto. El campo está en blanco, si el ID de VLAN del puerto no es

anulado por 802.1X.

Si el servidor RADIUS asigna el ID de VLAN, se agrega "(asignado por RADIUS)" al ID de VLAN. Lea más sobre las VLAN asignadas por RADIUS aquí.

Si el puerto se mueve a la VLAN invitada, se agrega "(Invitado)" al ID de la VLAN. Lea más sobre las VLAN invitadas aquí.

Botones



Figura 10-2.2: Botones de estado IEEE 802.1X

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

- **Si selecciona el puerto 1 para mostrar estadísticas 802.1X.**



Figura 10-2.2: Puerto de estadísticas 802.1X 1

Descripción de parámetros:

- **Puerto :**

Puede seleccionar qué puerto desea que muestre las estadísticas 802.1X.

- **Estado de administración:**

Estado administrativo actual del puerto. Consulte Estado de administración de 802.1X para obtener una descripción de los posibles valores.

- **Estado del puerto:**

El estado actual del puerto. Consulte Estado del puerto 802.1X para obtener una descripción de los estados individuales.

Botones

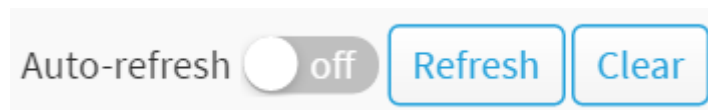


Figura 10-2.2: Botones del puerto de estadísticas IEEE 802.1X

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página.

- **Claro :**

Borra los contadores del puerto seleccionado.

10-3 Seguridad del puerto

10-3.1 Configuración

Esta sección le muestra cómo configurar los ajustes de seguridad del puerto del conmutador. Puede utilizar la función Port Security para restringir la entrada a una interfaz limitando e identificando direcciones MAC.

Interfaz web

Para configurar una configuración de seguridad de puerto en la interfaz web:

1. Haga clic en Seguridad, Seguridad de puertos y Configuración.
2. Seleccione "Activado" en el Modo de configuración del sistema.
3. Configure el modo (habilitado, deshabilitado), límite, acción (trampa, apagado, trampa y apagado) para cada puerto.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

Port Security Configuration Home > Security > Port Security > Configuration

System Configuration

Mode Disabled ▾

Port Configuration

Port	Mode	Limit	Action	State	Re-open
1	Disabled ▾	4	None ▾		Reopen
2	Disabled ▾	4	None ▾		Reopen
8	Disabled ▾	4	None ▾		Reopen
9	Disabled ▾	4	None ▾		Reopen
10	Disabled ▾	4	None ▾		Reopen

Apply Reset

Figura 10-3.1: Configuración de seguridad del puerto

Descripción de parámetros:

Configuración del sistema

- **Modo :**

Indica si el control de límite está habilitado o deshabilitado globalmente en el interruptor. Si está deshabilitado globalmente, otros módulos aún pueden usar la funcionalidad subyacente, pero las verificaciones de límites y las acciones correspondientes están deshabilitadas.

Configuración del puerto

La tabla tiene una fila para cada puerto en el conmutador seleccionado y varias columnas, que son:

- **Puerto :**

El número de puerto al que se aplica la siguiente configuración.

- **Modo :**

Controla si el Control de límite está habilitado en este puerto. Tanto este como el modo global deben

debe establecerse en Habilitado para que el Control de límite esté en efecto. Tenga en cuenta que otros módulos pueden seguir utilizando las funciones de seguridad del puerto subyacentes sin habilitar el control de límites en un puerto determinado.

- **Límite :**

La cantidad máxima de direcciones MAC que se pueden asegurar en este puerto. Este número no puede exceder 1024. Si se excede el límite, se toma la acción correspondiente.

El conmutador "nace" con un número total de direcciones MAC de las que se extraen todos los puertos cada vez que se ve una nueva dirección MAC en un puerto habilitado para Port Security. Dado que todos los puertos toman del mismo grupo, puede suceder que no se pueda otorgar un máximo configurado, si los puertos restantes ya han usado todas las direcciones MAC disponibles.

- **Acción:**

Si se alcanza el límite, el conmutador puede realizar una de las siguientes acciones:

Ninguno: No permita más direcciones MAC limitadas en el puerto, pero no realice ninguna otra acción.

Trampa: Si se ven direcciones MAC de límite + 1 en el puerto, envíe una trampa SNMP. Si el envejecimiento está deshabilitado, solo se enviará una captura SNMP, pero con el envejecimiento habilitado, se enviarán nuevas capturas SNMP cada vez que se exceda el límite.

Apagar: Si se ven direcciones MAC de límite + 1 en el puerto, apague el puerto. Esto implica que todas las direcciones MAC seguras se eliminarán del puerto y no se aprenderá ninguna dirección nueva. Incluso si el enlace se desconecta físicamente y se vuelve a conectar en el puerto (desconectando el cable), el puerto permanecerá cerrado. Hay tres formas de volver a abrir el puerto:

- 1) Inicie el interruptor,
- 2) Deshabilite y vuelva a habilitar el control de límite en el puerto o el interruptor,
- 3) Haga clic en el botón Reabrir.

Trampa y apagado: Si se ven direcciones MAC de límite + 1 en el puerto, se tomarán las acciones de "Trampa" y "Apagado" descritas anteriormente.

- **Expresar :**

Esta columna muestra el estado actual del puerto como se ve desde el punto de vista del Control de Límites. El estado toma uno de cuatro valores:

Discapacitado: El control de límites está deshabilitado o deshabilitado globalmente en el puerto.

Listo: Aún no se ha alcanzado el límite. Esto se puede mostrar para todas las acciones.

Límite alcanzado: Indica que se alcanzó el límite en este puerto. Este estado solo se puede mostrar si Acción se establece en ninguna o Trampa.

Shutdown: indica que el módulo de control de límite cierra el puerto. Este estado solo se puede mostrar si Acción está configurada para apagar o Trap & Shutdown.

- **Botón de reapertura:**

Si este módulo cierra un puerto, puede volver a abrirlo haciendo clic en este botón, que solo se habilitará si este es el caso. Para otros métodos, consulte apagar en la sección Acción.



norte **BENEFICIOS SEGÚN OBJETIVOS:** T que al hacer clic en el botón reabrir hace que la página se actualice, por lo que los cambios no confirmados se perderán

Botones

- **Aplicar**

Haga clic para guardar los cambios.

- **Reiniciar**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

10-3.2 Estado

Esta sección muestra el estado de la seguridad del puerto. Port Security es un módulo sin configuración directa. La configuración proviene indirectamente de otros módulos: los módulos de usuario. Cuando un módulo de usuario ha habilitado la seguridad del puerto en un puerto, el puerto se configura para el aprendizaje basado en software. En este modo, las tramas de direcciones MAC desconocidas se pasan al módulo de seguridad del puerto, que a su vez pregunta a todos los módulos de usuario si deben permitir que esta nueva dirección MAC la reenvíe o la bloquee. Para que una dirección MAC se establezca en el estado de reenvío, todos los módulos de usuario habilitados deben acordar unánimemente permitir que la dirección MAC reenvíe. Si solo uno elige bloquearlo, se bloqueará hasta que ese módulo de usuario decida lo contrario. La página de estado se divide en dos secciones: una con una leyenda de los módulos de usuario y otra con el estado real del puerto.

Interfaz web

Para mostrar un estado de seguridad del puerto en la interfaz web:

1. Haga clic en Seguridad, Seguridad del puerto y estado.
2. Marcó "Actualización automática".
3. Haga clic en "Actualizar" para actualizar las estadísticas detalladas del puerto.
4. Haga clic en el número de puerto para ver el estado de este puerto en particular.

Port Security Status Home > Security > Port Security > Status

Auto-refresh [Refresh](#)

Port Status

Port	State	Mac Count
1	Ready	1
2	Ready	0
3	Ready	0
4	Ready	0
5	Ready	0
8	Disabled	-
9	Disabled	-
10	Disabled	-

Figura 1 0-3.2: El estado de seguridad del puerto

Descripción de parámetros:

- **Puerto :**
El número de puerto para el que se aplica el estado.
- **Expresar :**
Muestra el estado actual del puerto. Puede tomar uno de cuatro valores:
 - Discapacitado:** Actualmente, ningún módulo de usuario utiliza el servicio de seguridad de puertos.
 - Listo:** El servicio Port Security está siendo utilizado por al menos un módulo de usuario y está esperando que lleguen tramas de direcciones MAC desconocidas.
 - Límite alcanzado:** El servicio de seguridad de puerto está habilitado por al menos el módulo de usuario de control de límites, y ese módulo ha indicado que se alcanzó el límite y no se deben aceptar más direcciones MAC.
 - Apagar:** El servicio Port Security está habilitado por al menos el módulo de usuario de Control de Límites, y ese módulo ha indicado que se excede el límite. No se pueden aprender direcciones MAC en el puerto hasta que se vuelva a abrir administrativamente en la configuración de Control de límites

Página web.

- **Conteo MAC (actual, límite):**

Las dos columnas indican la cantidad de direcciones MAC aprendidas actualmente (reenviando y bloqueadas) y la cantidad máxima de direcciones MAC que se pueden aprender en el puerto, respectivamente.

Si no hay módulos de usuario habilitados en el puerto, la columna Actual mostrará un guión (-).

Botones



Figura 10-3.2: Botones de estado de seguridad del puerto

- **Autorefrescar :**

Marque esta casilla para actualizar la página automáticamente. La actualización automática se produce cada 3 segundos.

- **Actualizar :**

Haga clic para actualizar la página inmediatamente.

10-4 RADIO

10-4.1 Configuración

Interfaz web

Para configurar un RADIUS en la interfaz web:

1. Haga clic en Seguridad, RADIUS y Configuración.
2. Establecer tiempo de espera, retransmisión, tiempo muerto, clave, dirección IP de NAS, dirección IPv6 de NAS, identificador de NAS.
3. Haga clic en "Agregar nueva entrada".
4. Configure el nombre de host, el puerto de autenticación, el puerto de cuenta, el tiempo de espera, la retransmisión, la clave. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer. Volverá a los valores guardados previamente.

RADIUS Server Configuration Home > Security > RADIUS > Configuration

Global Configuration

Timeout	<input type="text" value="5"/> seconds
Retransmit	<input type="text" value="3"/> times
Deadtime	<input type="text" value="0"/> minutes
Key	<input type="text"/>
NAS-IP-Address	<input type="text"/>
NAS-IPv6-Address	<input type="text"/>
NAS-identifier	<input type="text"/>

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Add New Entry						
Apply	Reset					

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Add New Entry						
Apply	Reset					

Figura 10-4.1: Configuración de RADIUS

Descripción de parámetros:

configuración global

Esta configuración es común para todos los servidores RADIUS.

- **Se acabó el tiempo :**

El tiempo de espera es el número de segundos, en el rango de 1 a 1000, para esperar una respuesta de un servidor RADIUS antes de retransmitir la solicitud.

- **Retransmitir:**

Retransmitir es el número de veces, en el rango de 1 a 1000, una solicitud RADIUS se retransmite a un servidor que no responde. Si el servidor no ha respondido después de la última retransmisión, se considera inactivo.

- **Tiempo muerto :**

El tiempo muerto, que se puede establecer en un número entre 0 y 1440 minutos, es el período durante el cual el conmutador no enviará nuevas solicitudes a un servidor que no haya respondido a una solicitud anterior. Esto evitará que el conmutador intente continuamente ponerse en contacto con un servidor que ya ha determinado como inactivo.

Establecer el tiempo muerto en un valor mayor que 0 (cero) habilitará esta función, pero solo si se ha configurado más de un servidor.

- **Llave :**
La clave secreta, de hasta 63 caracteres de longitud, compartida entre el servidor RADIUS y el conmutador.
- **Dirección IP del NAS:**
La dirección IPv4 que se utilizará como atributo 4 en los paquetes de solicitud de acceso RADIUS. Si este campo se deja en blanco, se utiliza la dirección IP de la interfaz saliente.
- **Dirección NAS-IPv6:**
La dirección IPv6 que se utilizará como atributo 95 en los paquetes de solicitud de acceso RADIUS. Si este campo se deja en blanco, se utiliza la dirección IP de la interfaz saliente.
- **Identificador NAS:**
El identificador, de hasta 255 caracteres, se utilizará como atributo 32 en los paquetes de solicitud de acceso RADIUS. Si este campo se deja en blanco, el NAS-Identifier no está incluido en el paquete.

Configuración del servidor

La tabla tiene una fila para cada servidor RADIUS y varias columnas, que son:

- **Borrar :**
Para eliminar una entrada del servidor RADIUS, marque esta casilla. La entrada se eliminará durante el siguiente guardado.
- **Nombre de host:**
La dirección IP o el nombre de host del servidor RADIUS.
- **Puerto de autenticación:**
El puerto UDP que se utilizará en el servidor RADIUS para la autenticación.
- **Puerto de cuenta:**
El puerto UDP que se utilizará en el servidor RADIUS para la contabilidad.
- **Se acabó el tiempo :**
Esta configuración opcional anula el valor de tiempo de espera global. Si lo deja en blanco, se utilizará el valor de tiempo de espera global.
- **Retransmitir:**
Esta configuración opcional anula el valor de retransmisión global. Si lo deja en blanco, se utilizará el valor de retransmisión global.
- **Llave :**
Esta configuración opcional anula la clave global. Si lo deja en blanco, se utilizará la clave global.

Botones

- **Adición de una nueva entrada de servidor:**
Haga clic para agregar un nuevo servidor RADIUS. Se agrega una fila vacía a la tabla y el servidor RADIUS se puede configurar según sea necesario. Se admiten hasta 5 servidores.
El botón se puede utilizar para deshacer la adición del nuevo servidor.

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

10-4.2 Estado

Esta sección le muestra una descripción general / detalle del estado de los servidores de autenticación y contabilidad RADIUS para garantizar que la función sea viable.

Interfaz web

Para mostrar un estado de RADIUS en la interfaz web:

1. Haga clic en Seguridad, RADIUS y estado.
2. Seleccione el servidor para mostrar las estadísticas detalladas de un RADIUS en particular.

RADIUS Server Status		
Home > Security > RADIUS > Status		
RADIUS Authentication Server Status		
#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled
RADIUS Accounting Server Status		
#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Figura 10-4.2: Descripción general del estado del servidor RADIUS

Descripción de parámetros:

Estado del servidor de autenticación RADIUS

- **#:**

El número de servidor RADIUS. Haga clic para navegar a las estadísticas detalladas de este servidor.
- **Dirección IP :**

La dirección IP y el número de puerto UDP (en <Dirección IP>: notación <Puerto UDP>) de este servidor.
- **Expresar :**

El estado actual del servidor. Este campo toma uno de los siguientes valores:

 - **Discapacitado :**

El servidor está deshabilitado.
 - **No está listo :**

El servidor está habilitado, pero la comunicación IP aún no está en funcionamiento.
 - **Listo :**

El servidor está habilitado, la comunicación IP está en funcionamiento y el módulo RADIUS está listo para aceptar intentos de acceso.
 - **Muerto (quedan X segundos):**

Se hicieron intentos de acceso a este servidor, pero no respondió dentro del tiempo de espera configurado. El servidor se ha desactivado temporalmente, pero se volverá a activar cuando expire el tiempo muerto. El número de segundos que quedan antes de que esto ocurra se muestra entre paréntesis. Este estado solo es accesible cuando más de un servidor está habilitado.

Estado del servidor de contabilidad RADIUS

- **#:**
El número de servidor RADIUS. Haga clic para navegar a las estadísticas detalladas de este servidor.
- **Dirección IP :**
La dirección IP y el número de puerto UDP (en <Dirección IP>: notación <Puerto UDP>) de este servidor.
- **Expresar :**
El estado actual del servidor. Este campo toma uno de los siguientes valores:
 - **Discapacitado:**
El servidor está deshabilitado.
 - **No está listo:**
El servidor está habilitado, pero la comunicación IP aún no está en funcionamiento.
 - **Listo:**
El servidor está habilitado, la comunicación IP está en funcionamiento y el módulo RADIUS está listo para aceptar intentos de contabilidad.
 - **Muerto (quedan X segundos):**
Se realizaron intentos de contabilidad en este servidor, pero no respondió dentro del tiempo de espera configurado. El servidor se ha desactivado temporalmente, pero se volverá a activar cuando expire el tiempo muerto. El número de segundos que quedan antes de que esto ocurra se muestra entre paréntesis. Este estado solo es accesible cuando más de un servidor está habilitado.
- **Si selecciona el servidor n. ° 1 para mostrar las estadísticas de RADIUS**

RADIUS Statistics Home > Security > RADIUS > Status

Auto-refresh off Refresh Clear server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:0		
State	Disabled		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1			
Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:0		
State	Disabled		
Round-Trip Time	0 ms		

Figura 10-4.2: El servidor de estadísticas RADIUS

Descripción de parámetros:

- **servidor:**

Puede seleccionar qué servidor desea que muestre RADIUS.

Estadísticas de autenticación RADIUS para el servidor n. ° 1

Las estadísticas se corresponden con las especificadas en RFC4668 - RADIUS Authentication Client MIB. Utilice el cuadro de selección de servidor para cambiar entre los servidores backend para mostrar detalles.

- **Acepta acceso:**

El número de paquetes RADIUS Access-Accept (válidos o no válidos) recibidos del servidor.

- **Rechazos de acceso:**

El número de paquetes RADIUS Access-Reject (válidos o no válidos) recibidos del servidor.

- **Desafíos de acceso:**

El número de paquetes de desafío de acceso RADIUS (válidos o no válidos) recibidos del servidor.

- **Respuestas de acceso con formato incorrecto:**

El número de paquetes RADIUS Access-Response con formato incorrecto recibidos del servidor. Los paquetes con formato incorrecto incluyen paquetes con una longitud no válida. Los autenticadores incorrectos, los atributos del autenticador de mensajes o los tipos desconocidos no se incluyen como respuestas de acceso con formato incorrecto.

- **Autenticadores incorrectos:**

La cantidad de paquetes RADIUS Access-Response que contienen autenticadores no válidos o atributos de Autenticador de mensajes recibidos del servidor.

- **Tipos desconocidos:**

La cantidad de paquetes RADIUS que se recibieron con tipos desconocidos del servidor en el puerto de autenticación y se descartaron.

- **Paquetes caídos:**

La cantidad de paquetes RADIUS que se recibieron del servidor en el puerto de autenticación y se eliminaron por algún otro motivo.

- **Solicitudes de acceso:**

El número de paquetes de solicitud de acceso RADIUS enviados al servidor. Esto no incluye retransmisiones.

- **Retransmisiones de acceso:**

El número de paquetes de solicitud de acceso RADIUS retransmitidos al servidor de autenticación RADIUS.

- **Solicitudes pendientes :**

El número de paquetes de solicitud de acceso RADIUS destinados al servidor que aún no

agotó el tiempo de espera o recibió una respuesta. Esta variable se incrementa cuando se envía una solicitud de acceso y se reduce debido a la recepción de una aceptación de acceso, rechazo de acceso, desafío de acceso, tiempo de espera o retransmisión.

- **Tiempos de espera:**

El número de tiempos de espera de autenticación en el servidor. Después de un tiempo de espera, el cliente puede volver a intentarlo en el mismo servidor, enviarlo a un servidor diferente o darse por vencido. Un reintento al mismo servidor se cuenta como retransmisión y como tiempo de espera. Un envío a un servidor diferente se cuenta como una Solicitud y como un tiempo de espera.

- **Dirección IP :**

Dirección IP y puerto UDP para el servidor de autenticación en cuestión.

- **Expresar :**

Muestra el estado del servidor. Toma uno de los siguientes valores:

- **Discapacitado :**

El servidor seleccionado está deshabilitado.

- **No está listo :**

El servidor está habilitado, pero la comunicación IP aún no está en funcionamiento.

- **Listo :**

El servidor está habilitado, la comunicación IP está en funcionamiento y el módulo RADIUS está listo para aceptar intentos de acceso.

- **Muerto (quedan X segundos):**

Se hicieron intentos de acceso a este servidor, pero no respondió dentro del tiempo de espera configurado. El servidor se ha desactivado temporalmente, pero se volverá a activar cuando expire el tiempo muerto. El número de segundos que quedan antes de que esto ocurra se muestra entre paréntesis. Este estado solo es accesible cuando más de un servidor está habilitado.

- **Tiempo de viaje :**

los hora intervalo (Medido en milisegundos) Entre la más reciente Access-Reply / Access-Challenge y la solicitud de acceso que coincidió con el del servidor de autenticación RADIUS. La granularidad de esta medida es de 100 ms. Un valor de 0 ms indica que aún no ha habido comunicación de ida y vuelta con el servidor.

Estadísticas de contabilidad RADIUS para el servidor n. ° 1

Las estadísticas se corresponden estrechamente con las especificadas en RFC4670 - RADIUS Accounting Client MIB. Utilice el cuadro de selección de servidor para cambiar entre los servidores backend para mostrar detalles.

- **Respuestas:**

La cantidad de paquetes RADIUS (válidos o no válidos) recibidos del servidor.

- **Respuestas con formato incorrecto:**

La cantidad de paquetes RADIUS con formato incorrecto recibidos del servidor. Los paquetes con formato incorrecto incluyen paquetes con una longitud no válida. Los autenticadores incorrectos o los tipos desconocidos no se incluyen como respuestas de acceso con formato incorrecto.

- **Autenticadores incorrectos:**

La cantidad de paquetes RADIUS que contienen autenticadores no válidos recibidos del servidor.

- **Tipos desconocidos:**

La cantidad de paquetes RADIUS de tipos desconocidos que se recibieron del servidor en el puerto de contabilidad.

- **Paquetes caídos:**

La cantidad de paquetes RADIUS que se recibieron del servidor en el puerto de contabilidad y se descartaron por algún otro motivo.

- **Peticiones :**

La cantidad de paquetes RADIUS enviados al servidor. Esto no incluye retransmisiones.

- **Retransmisiones:**

El número de paquetes RADIUS retransmitidos al servidor de contabilidad RADIUS.

- **Solicitudes pendientes :**

La cantidad de paquetes RADIUS destinados al servidor que aún no han agotado el tiempo de espera ni han recibido una respuesta. Esta variable se incrementa cuando se envía una solicitud y se reduce debido a la recepción de una respuesta, tiempo de espera o retransmisión.

- **Tiempos de espera:**

El número de tiempos de espera de contabilidad para el servidor. Después de un tiempo de espera, el cliente puede volver a intentarlo en el mismo servidor, enviarlo a un servidor diferente o darse por vencido. Un reintento al mismo servidor se cuenta como retransmisión y como tiempo de espera. Un envío a un servidor diferente se cuenta como una Solicitud y como un tiempo de espera.

- **Dirección IP :**

Dirección IP y puerto UDP del servidor de contabilidad en cuestión.

- **Expresar :**

Muestra el estado del servidor. Toma uno de los siguientes valores:

- **Discapacitado :**

El servidor seleccionado está deshabilitado.

- **No está listo :**

El servidor está habilitado, pero la comunicación IP aún no está en funcionamiento.

- **Listo :**

El servidor está habilitado, la comunicación IP está en funcionamiento y el módulo RADIUS está listo para aceptar intentos de contabilidad.

- **Muerto (quedan X segundos):**

Se realizaron intentos de contabilidad en este servidor, pero no respondió dentro del tiempo de espera configurado. El servidor se ha desactivado temporalmente, pero se volverá a activar cuando expire el tiempo muerto. El número de segundos que quedan antes de que esto ocurra se muestra entre paréntesis. Este estado solo es accesible cuando más de un servidor está habilitado.

- **Tiempo de viaje :**

El intervalo de tiempo (medido en milisegundos) entre la Respuesta más reciente y la Solicitud que coincide con ella desde el servidor de contabilidad RADIUS. La granularidad de esta medida es de 100 ms. Un valor de 0 ms indica que aún no ha habido comunicación de ida y vuelta con el servidor.

Este capítulo proporciona un conjunto de diagnósticos básicos del sistema. Les permite a los usuarios saber si el sistema está en buen estado o necesita ser reparado. La verificación básica del sistema incluye Ping, Traceroute y VeriPHY Cable Diagnostics.

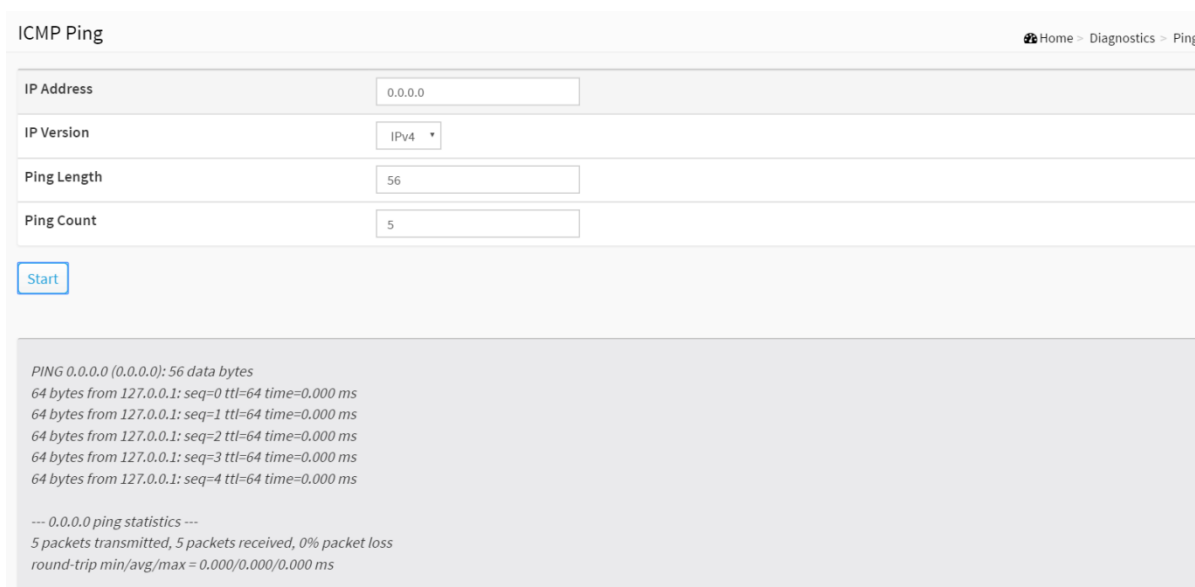
11-1 Ping

Esta sección le permite emitir paquetes ICMP PING para solucionar problemas de conectividad IPv6.

Interfaz web

Para configurar un PING en la interfaz web:

1. Haga clic en Diagnóstico y ping.
2. Especifique la dirección IP, la versión de IP y el tamaño de PING.
3. Haga clic en Iniciar.



The screenshot shows a web interface titled "ICMP Ping" with a breadcrumb "Home > Diagnostics > Ping". It contains four input fields: "IP Address" (0.0.0.0), "IP Version" (IPv4), "Ping Length" (56), and "Ping Count" (5). A "Start" button is located below the fields. The results area displays the following text:

```

PING 0.0.0.0 (0.0.0.0): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.000 ms

--- 0.0.0.0 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
    
```

Figura 11-1: El ping ICMP

Descripción de parámetros:

- **Dirección IP :**
Para configurar la dirección IP del dispositivo, desea hacer ping.
- **Versión de IP:**
Para configurar la versión de IP que desee.
- **Longitud de ping:**

El tamaño de la carga útil del paquete ICMP. Los valores oscilan entre 2 bytes y 1452 bytes.

- **Recuento de ping:**

El recuento del paquete ICMP. Los valores oscilan entre 1 vez y 60 veces.

- **Comienzo:**

Haga clic en el botón "Inicio" y luego el conmutador comenzará a hacer ping al dispositivo utilizando el tamaño de paquete ICMP establecido en el conmutador.

Después de presionar, se transmiten 5 paquetes ICMP y el número de secuencia y el tiempo de ida y vuelta se muestran al recibir una respuesta. La página se actualiza automáticamente hasta que se reciben las respuestas a todos los paquetes o hasta que se agota el tiempo de espera.

Servidor PING6 :: 10.10.132.20

64 bytes desde :: 10.10.132.20: icmp_seq = 0, tiempo = 0ms

64 bytes desde :: 10.10.132.20: icmp_seq = 1, tiempo = 0ms

64 bytes desde :: 10.10.132.20: icmp_seq = 2, tiempo = 0ms

64 bytes desde :: 10.10.132.20: icmp_seq = 3, tiempo = 0ms

64 bytes desde :: 10.10.132.20: icmp_seq = 4, tiempo = 0ms

Envió 5 paquetes, recibió 5 OK, 0 incorrecto

11-2 Diagnóstico de cables

Esta sección se utiliza para ejecutar VeriPHY Cable Diagnostics. Presione para ejecutar los diagnósticos. Esto tardará aproximadamente 5 segundos. Si se seleccionan todos los puertos, esto puede tardar aproximadamente 15 segundos. Cuando se completa, la página se actualiza automáticamente y puede ver los resultados del diagnóstico del cable en la tabla de estado del cable. Tenga en cuenta que VeriPHY solo es preciso para cables de 7 a 140 metros de longitud. Los puertos de 10 y 100 Mbps se conectarán mientras se ejecuta VeriPHY. Por lo tanto, ejecutar VeriPHY en un puerto de administración de 10 o 100 Mbps hará que el conmutador deje de responder hasta que se complete VeriPHY.

Interfaz web

Para configurar una configuración de diagnóstico de cables en la interfaz web:

1. Haga clic en Diagnóstico y diagnóstico de cables.
2. Especifique el puerto que desea verificar.
3. Haga clic en Iniciar.

Cable Diagnostics Home > Diagnostics > Cable Diagnostics

Port 1

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--

Figura 11-2: El Diagnóstico de cables

Descripción de parámetros:

- **Puerto :**
El puerto en el que solicita los diagnósticos de cable.
- **Estado del cable**
- **Puerto :**
Número de puerto.
- **Par :**
El estado del par de cables.
- **Largo :**
La longitud (en metros) del par de cables.
- **Botón**
- **Comienzo :**
Comience a realizar diagnósticos por cable en el puerto que seleccionó.

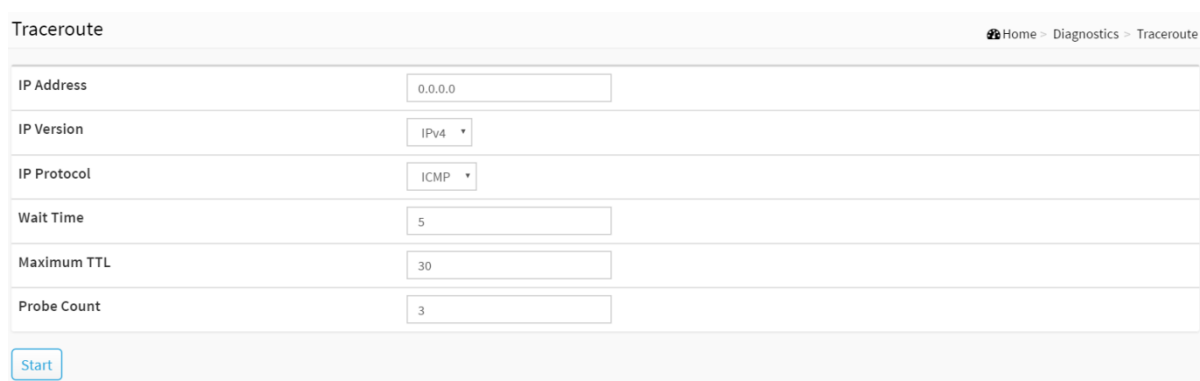
11-3 Traceroute

Esta página le permite emitir paquetes ICMP, TCP o UDP para diagnosticar problemas de conectividad de red.

Interfaz web

Para configurar un Traceroute en la interfaz web:

1. Haga clic en Diagnósticos y Traceroute.
2. Especifique la dirección IP, la versión IP, el protocolo IP y el tamaño de la ruta de seguimiento.
3. Haga clic en Iniciar.



The screenshot shows a web interface titled "Traceroute" with a breadcrumb "Home > Diagnostics > Traceroute". The interface contains several input fields and dropdown menus:

- IP Address:** A text input field containing "0.0.0.0".
- IP Version:** A dropdown menu currently set to "IPv4".
- IP Protocol:** A dropdown menu currently set to "ICMP".
- Wait Time:** A text input field containing "5".
- Maximum TTL:** A text input field containing "30".
- Probe Count:** A text input field containing "3".

At the bottom left of the form area, there is a blue "Start" button.

Figura 11-3: El Traceroute

Descripción de parámetros:

- **Dirección IP :**
La dirección IP de destino.
- **Versión de IP:**
Para configurar la versión de IP que desee.
- **Protocolo:**
Los paquetes de protocolo (ICMP, UDP, TCP) que se van a enviar.
- **Tiempo de espera :**
Configure el tiempo (en segundos) para esperar una respuesta a una sonda (por defecto, 5.0 segundos). Los valores oscilan entre 1 y 60. El tamaño de carga útil del paquete ICMP. Los valores oscilan entre 2 bytes y 1452 bytes.
- **TTL máximo:**
Especifica el número máximo de saltos (valor máximo de tiempo de vida) que sondeará traceroute. Los valores oscilan entre 1 y 255. El valor predeterminado es 30.
- **Recuento de sondas:**
Establece el número de paquetes de sondeo por salto. Los valores oscilan entre 1 y 10. El valor predeterminado es 3.

11-4 Espejo

Puede reflejar el tráfico desde cualquier puerto de origen a un puerto de destino para realizar un análisis en tiempo real. Luego, puede conectar un analizador lógico o una sonda RMON al puerto de destino y estudiar el tráfico que cruza el puerto de origen de una manera completamente discreta.

La configuración del espejo sirve para monitorear el tráfico de la red. Por ejemplo, asumimos que el puerto A y el puerto B son el puerto de monitoreo y el puerto monitoreado respectivamente, por lo tanto, el tráfico recibido por el puerto B se copiará al puerto A para su monitoreo.

Interfaz web

Para configurar el Mirror en la interfaz web:

1. Haga clic en Diagnóstico y creación de reflejo.
2. Desplácese para seleccionar Monitor Destination Port en qué puerto.
3. Desplácese a desactivado, activado, Solo TX y Solo RX para configurar el modo de espejo de puerto.
4. Haga clic en Aplicar para guardar la configuración.
5. Si desea cancelar la configuración, debe hacer clic en el botón Restablecer.
6. Volverá a los valores guardados anteriormente.

Mirror Configuration Home - Diagnostics - Mirroring

Mode	<input type="checkbox"/> off
Monitor Destination Port	Port 1 ▾
Monitor Source Port Configuration	
Port	Mode
1	Disabled ▾
2	Disabled ▾
8	Disabled ▾
9	Disabled ▾
10	Disabled ▾

Apply Reset

Figura 11-4: Configuración del espejo

Descripción de parámetros:

- **Modo :**

Indica el funcionamiento del modo espejo. Los modos posibles son:

en: Habilite el funcionamiento del modo espejo.

apagado: Desactive el funcionamiento del modo espejo.

- **Monitorear el puerto de destino:**

Puerto a espejo también conocido como puerto espejo. Las tramas de los puertos que tienen habilitada la duplicación de origen (rx) o destino (tx) se duplican en este puerto. Desactivado desactiva la duplicación.

Configuración del puerto de origen espejo

La siguiente tabla se utiliza para habilitar Rx y Tx.

- **Puerto :**

El puerto lógico para la configuración contenida en la misma fila.

- **Modo :**

Seleccione el modo espejo.

Sólo Rx Las tramas recibidas en este puerto se reflejan en el puerto espejo. Las tramas transmitidas no se reflejan.

Sólo Tx Las tramas transmitidas en este puerto se reflejan en el puerto espejo. Las tramas recibidas no se reflejan.

Deshabilitado, ni las tramas transmitidas ni las tramas recibidas se reflejan.

Habilitado Las tramas recibidas y las tramas transmitidas se reflejan en el puerto espejo.



norte BENEFICIOS SEGÚN OBJETIVOS: Para un puerto determinado, una trama solo se transmite una vez. Por lo tanto, no es posible reflejar los marcos Tx en el puerto de espejo. Debido a esto, el modo para el puerto espejo seleccionado está limitado a Deshabilitado o solo Rx.

Botones

- **Aplicar :**

Haga clic para guardar los cambios.

- **Reiniciar :**

Haga clic para deshacer los cambios realizados localmente y volver a los valores guardados anteriormente.

Este capítulo describe todas las tareas de configuración de mantenimiento del conmutador para mejorar el rendimiento de la red local, incluido Guardar / Hacer copia de seguridad / Restaurar / Activar / Eliminar dispositivo de reinicio, Valores predeterminados de fábrica, Actualización de firmware.

12-1 Configuración

El switch almacena su configuración en varios archivos de texto en formato CLI. Los archivos son virtual (basado en RAM) o almacenado en flash en el conmutador.

Hay tres archivos de sistema:

- **running-config:** un archivo virtual que representa la configuración actualmente activa en el conmutador. Este archivo es volátil.
- **startup-config:** la configuración de inicio para el conmutador, leída en el momento del inicio.
- **default-config:** un archivo de solo lectura con configuración específica del proveedor. Este archivo se lee cuando el sistema se restaura a la configuración predeterminada.

También es posible almacenar hasta otros dos archivos y aplicarlos a running-config, por lo tanto configuración de conmutación.

12-1.1 Guardar configuración de inicio

Esta copia running-config en startup-config, asegurando así que la configuración actualmente activa se utilizará en el próximo reinicio.

Interfaz web

Para guardar la configuración en ejecución en la interfaz web:

1. Haga clic en Mantenimiento, Configuración y Guardar configuración de inicio.
2. Haga clic en Guardar configuración.

Please note:

The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Configuration

Figura 12-1.1: Guardar configuración de inicio

Descripción de parámetros:

Botón

- **Guardar configuración:**

Haga clic para guardar la configuración, la configuración en ejecución se escribirá en la memoria flash para que el sistema arranque y cargue este archivo de configuración de inicio.

12-1.2 Configuración de copia de seguridad

Esta sección describe cómo exportar la configuración del conmutador para necesidades de mantenimiento. Todos los archivos de configuración actuales se exportarán como formato de texto.

Es posible descargar un archivo desde el navegador web a todos los archivos del switch, excepto default-config, que es de solo lectura.

Seleccione el archivo para descargar, seleccione el archivo de destino en el destino y haga clic en.

Si el destino es running-config, el archivo se aplicará a la configuración del conmutador. Esto se puede hacer de dos formas:

- **Modo de reemplazo:** la configuración actual se reemplaza por completo con la configuración en el archivo descargado.
- **Modo de fusión:** el archivo descargado se fusiona en running-config.

Si el sistema de archivos está lleno (es decir, contiene los tres archivos del sistema mencionados anteriormente más otros dos archivos), no es posible crear archivos nuevos, pero primero se debe sobrescribir un archivo existente o eliminar otro.

Interfaz web

Para descargar la configuración en la interfaz web:

1. Haga clic en Mantenimiento, configuración y configuración de copia de seguridad.
2. Haga clic en Copia de seguridad.

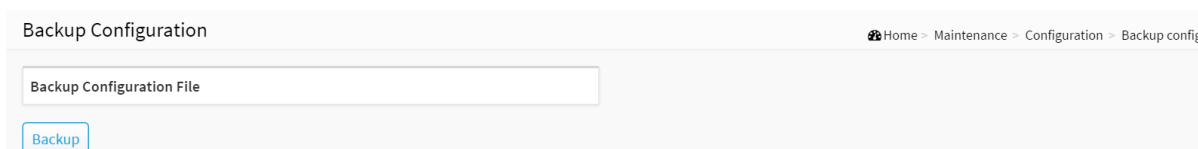


Figura 12-1.2: Configuración de copia de seguridad

Descripción de parámetros:

Botón

- **Respaldo :**

Haga clic en el botón "Copia de seguridad" y el conmutador comenzará a descargar la configuración de la memoria flash a la PC o al servidor.

12-1.3 Restaurar configuración

La función de carga de configuración se respaldará y guardará la configuración de la configuración del conmutador en la PC del navegador web en ejecución.

Es posible cargar cualquiera de los archivos del conmutador en el navegador web. Seleccione el archivo y haga clic en Upload of running-config puede tardar un poco en completarse, ya que el archivo debe estar preparado para la carga.

Interfaz web

Para restaurar la configuración en la interfaz web:

1. Haga clic en Mantenimiento, configuración y restauración de la configuración.
2. Haga clic en Cargar.

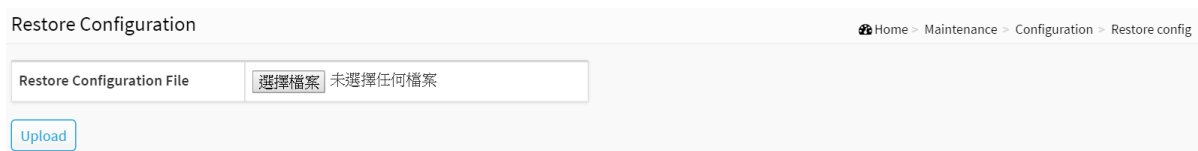


Figura 12-1.3: Restaurar configuración

Hay tres archivos de sistema:

1. running-config: un archivo virtual que representa la configuración actualmente activa en el conmutador. Este archivo es volátil.
2. startup-config: la configuración de inicio para el conmutador, leída en el momento del inicio.
3. default-config: un archivo de solo lectura con configuración específica del proveedor. Este archivo se lee cuando el sistema se restaura a la configuración predeterminada.

Descripción de parámetros:

Botón

- **選擇 檔案:**

Haga clic en el " 選擇 檔案." Botón para buscar el archivo de texto de configuración y el nombre del archivo

- **Subir :**

Haga clic en el botón "Cargar" y luego la PC de administración web en ejecución comenzará a cargar la configuración de la configuración de la PC de ubicación en el conmutador administrado.

12-1.4 Activar config

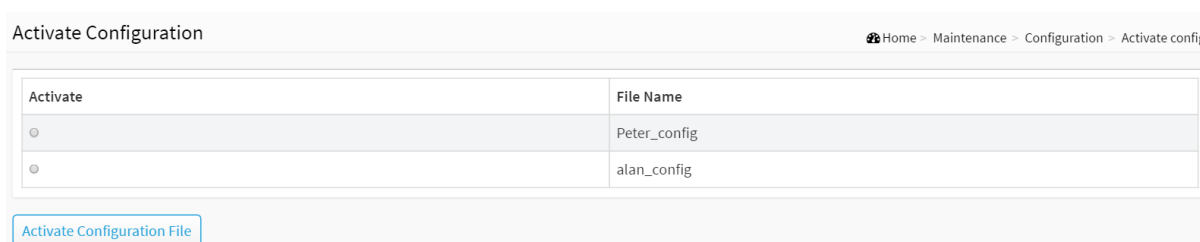
Es posible activar cualquiera de los archivos de configuración presentes en el switch, excepto running-config, que representa la configuración actualmente activa.

Seleccione el archivo para activar y haga clic. Esto iniciará el proceso de reemplazar completamente la configuración existente con la del archivo seleccionado.

Interfaz web

Para activar la configuración en la interfaz web:

1. Haga clic en Mantenimiento, Configuración y Activar configuración.
2. Haga clic en Activar Seleccionar.



Activate	File Name
<input type="radio"/>	Peter_config
<input type="radio"/>	alan_config

Activate Configuration File

Figura 12-1.4: Activación de la configuración

Hay dos archivos de sistema:

1. default-config: un archivo de solo lectura con configuración específica del proveedor. Este archivo se lee cuando el sistema se restaura a la configuración predeterminada.
2. startup-config: la configuración de inicio para el conmutador, leída en el momento del inicio.

Descripción de parámetros:

- **Activar**

Puede seleccionar el archivo que desea activar.

Botones

- **Activar archivo de configuración:**

Haga clic en el botón "Activar archivo de configuración", luego el archivo seleccionado se activará y será la configuración en ejecución de este conmutador.

12-1.5 Eliminar configuración

Es posible eliminar cualquiera de los archivos grabables almacenados en flash, incluido startup-config. Si se hace esto y el switch se reinicia sin una operación de guardado previa, esto efectivamente restablece el switch a la configuración predeterminada.

Interfaz web

Para eliminar la configuración en la interfaz web:

1. Haga clic en Mantenimiento, Configuración y Eliminar configuración.
2. Haga clic en Eliminar selección.

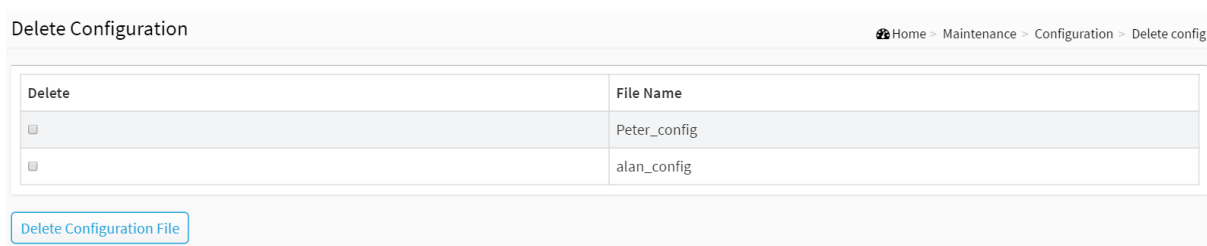


Figura 12-1.5: Eliminar configuración

Descripción de parámetros:

- **Borrar**

Puede seleccionar el archivo que desea eliminar.

Botones

- **Eliminar archivo de configuración:**

Haga clic en el botón "Eliminar archivo de configuración" y luego se eliminará el archivo seleccionado.

12-2 Reiniciar dispositivo

Esta sección describe cómo reiniciar el conmutador para cualquier necesidad de mantenimiento. Todos los archivos de configuración o secuencias de comandos que haya guardado en el conmutador aún deberían estar disponibles posteriormente.

Interfaz web

Para configurar una configuración de reinicio del dispositivo en la interfaz web:

1. Haga clic en Mantenimiento y reiniciar dispositivo.
2. Haga clic en Sí.

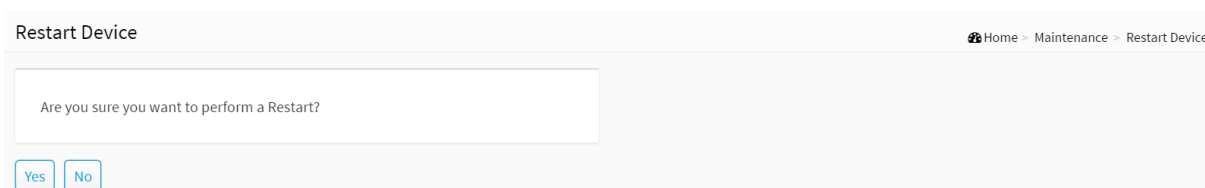


Figura 12-2: Reiniciar dispositivo

Descripción de parámetros:

Reiniciar el dispositivo :

Puede reiniciar el interruptor en esta página. Después de reiniciar, el conmutador se iniciará normalmente.

Botones

- **Sí :**
Haga clic en "Sí" y el dispositivo se reiniciará.
- **No :**
Haga clic para deshacer cualquier acción de reinicio.

12-3 Valores predeterminados de fábrica

Esta sección describe cómo restablecer la configuración del conmutador a los valores predeterminados de fábrica. Todos los archivos de configuración o secuencias de comandos se recuperarán a los valores predeterminados de fábrica.

Interfaz web

Para configurar una configuración predeterminada de fábrica en la interfaz web:

1. Haga clic en Mantenimiento y valores predeterminados de fábrica.
2. Puede elegir si desea mantener la configuración de ip o no.
3. Haga clic en Sí.

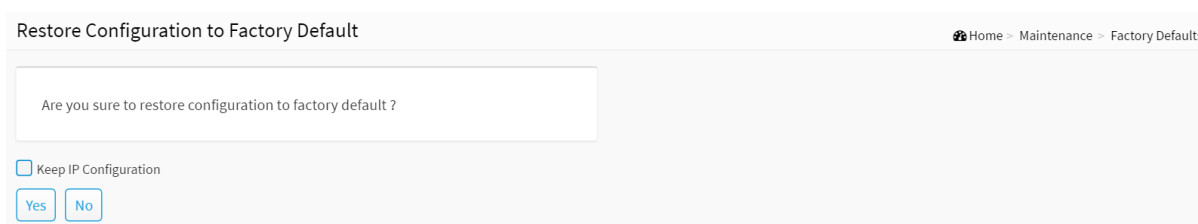


Figura 12-3: Valores predeterminados de fábrica

Descripción de parámetros:

Botones

- **Mantener la configuración de IP:**
Elija si desea mantener la configuración de ip o no.
- **Sí :**
Haga clic en el botón "Sí" para restablecer la configuración a los valores predeterminados de fábrica.
- **No :**
Haga clic en para volver a la página Estado del puerto sin restablecer la configuración.

12-4 Firmware

Esta sección describe cómo actualizar el firmware. El Switch se puede mejorar con más funciones de valor agregado instalando actualizaciones de firmware.

12-4.1 Actualización de firmware

Esta página facilita una actualización del firmware que controla el conmutador.

Interfaz web

Para configurar una configuración de actualización de firmware en la interfaz web:

1. Haga clic en Mantenimiento, firmware y actualización de firmware.
2. Haga clic en Cargar.

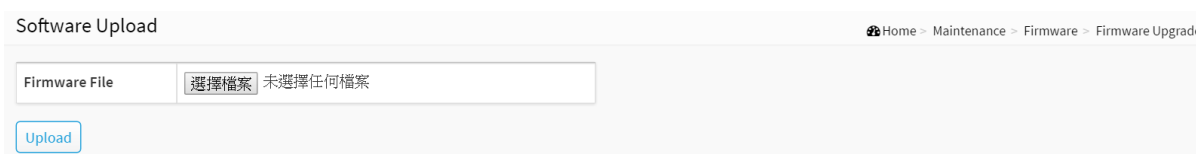


Figura 12-4.1 La actualización del firmware

Descripción de parámetros:

- **Seleccione Archivo :**

Haga clic en el botón "Seleccionar archivo" para buscar la URL del firmware y el nombre del archivo.



norte BENEFICIOS SEGÚN OBJETIVOS: Esta página facilita una actualización del firmware que controla el conmutador. La carga de software actualizará todos los conmutadores administrados a la ubicación de una imagen de software y hará clic en. Una vez que se carga la imagen del software, una página anuncia que se inició la actualización del firmware. Después de aproximadamente un minuto, el firmware se actualiza y todos los conmutadores administrados se reinician. el interruptor se reinicia.



W ADVERTENCIA: Mientras se actualiza el firmware, el acceso a la Web parece haber desaparecido. El LED frontal parpadea en verde / apagado con una frecuencia de 10 Hz mientras la actualización del firmware está en curso. No reinicie ni apague el dispositivo en este momento o el interruptor puede dejar de funcionar después.



IMPORTANTE:

1. Se recomienda utilizar **IE10** o **IE11** para abrir una consola web con el conmutador PoE.
2. Este conmutador PoE está diseñado específicamente para aplicaciones de vigilancia. Viene con una interfaz de vigilancia integrada para facilitar la configuración. Se accede a la interfaz de Vigilancia a través de un menú con pestañas, y los cambios de configuración realizados en su ventana tienen mayor prioridad que los de los menús de configuración del Switch.

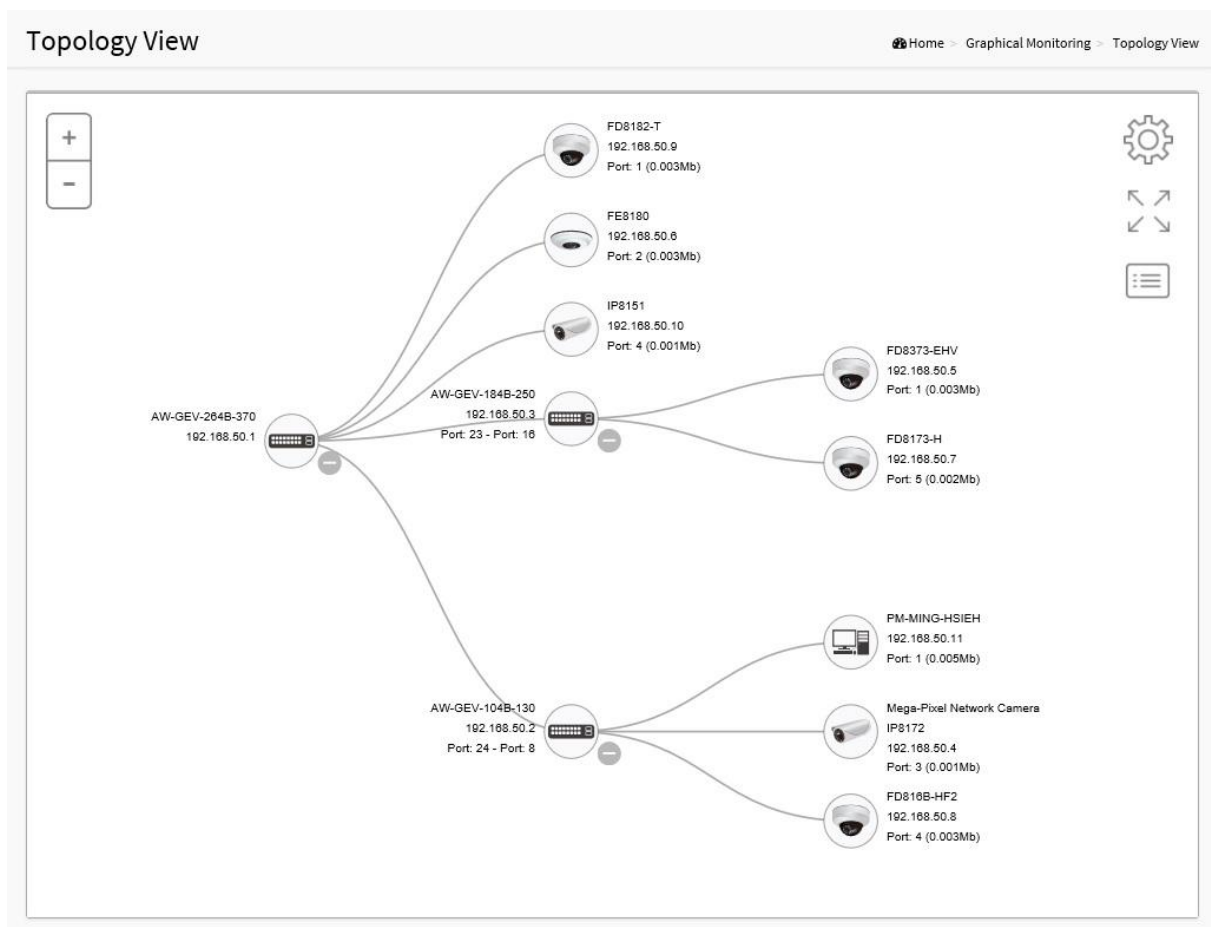


Figura 13-1: Vista de topología: lista de dispositivos

13-1. INTRODUCCIÓN (para las funciones de Vigilancia):

1. Todos los dispositivos conectados a los conmutadores se pueden descubrir y mostrar automáticamente utilizando protocolos de red estándar como LLDP, UPnP, ONVIF, Bonjour, etc.
2. Los usuarios pueden operar las siguientes funciones a través de una interfaz gráfica de usuario web intuitiva.
 - Apague, de forma remota, las cámaras IP, NVR o cualquier dispositivo PoE.

- Identifique dónde está exactamente el cable roto, de forma remota. Detecta
- problemas de tráfico anormales en cámaras IP / NVR.
- Supervise el estado de los dispositivos de forma intuitiva, por ejemplo, enlace, alimentación PoE, tráfico, etc.
- Configure VLAN / QoS de forma intuitiva para una mejor calidad / fiabilidad de la solución.

3. La interfaz admite hasta 256 dispositivos.

La interfaz está diseñada para ser extremadamente fácil de usar / administrar / instalar IP Phone, IP Cam o Wifi-AP para aplicaciones empresariales.

El usuario puede implementar el dispositivo IP a través de la vista de topología / piso / mapa hasta la ubicación de instalación y, a través de Diagnóstico y Monitor de tráfico, también puede verificar el estado del enlace y monitorear el rendimiento.

13-2. Modo de vigilancia

Information Home > Management > Information

Mode	Enabled ▾
Total Device	2
On-line Devices	2
Off-line Devices	0
Controller IP	192.168.1.1

13-2. El modo de vigilancia

- Modo de vigilancia: habilite / deshabilite la función de vigilancia o configure el modo con prioridad alta para el interruptor maestro.
- Dispositivo total: muestra cuántos dispositivos IP se detectan y se muestran en la vista de topología.
- Dispositivos en línea: muestra cuántos dispositivos IP en línea en la vista de topología.
- Dispositivo fuera de línea: muestra cuántos dispositivos IP están actualmente fuera de línea en la vista de topología.
- IP del controlador: muestra la IP del conmutador maestro (la IP del conmutador PoE que configura el modo de vigilancia como de alta prioridad).

13-3. Supervisión gráfica: vista de topología

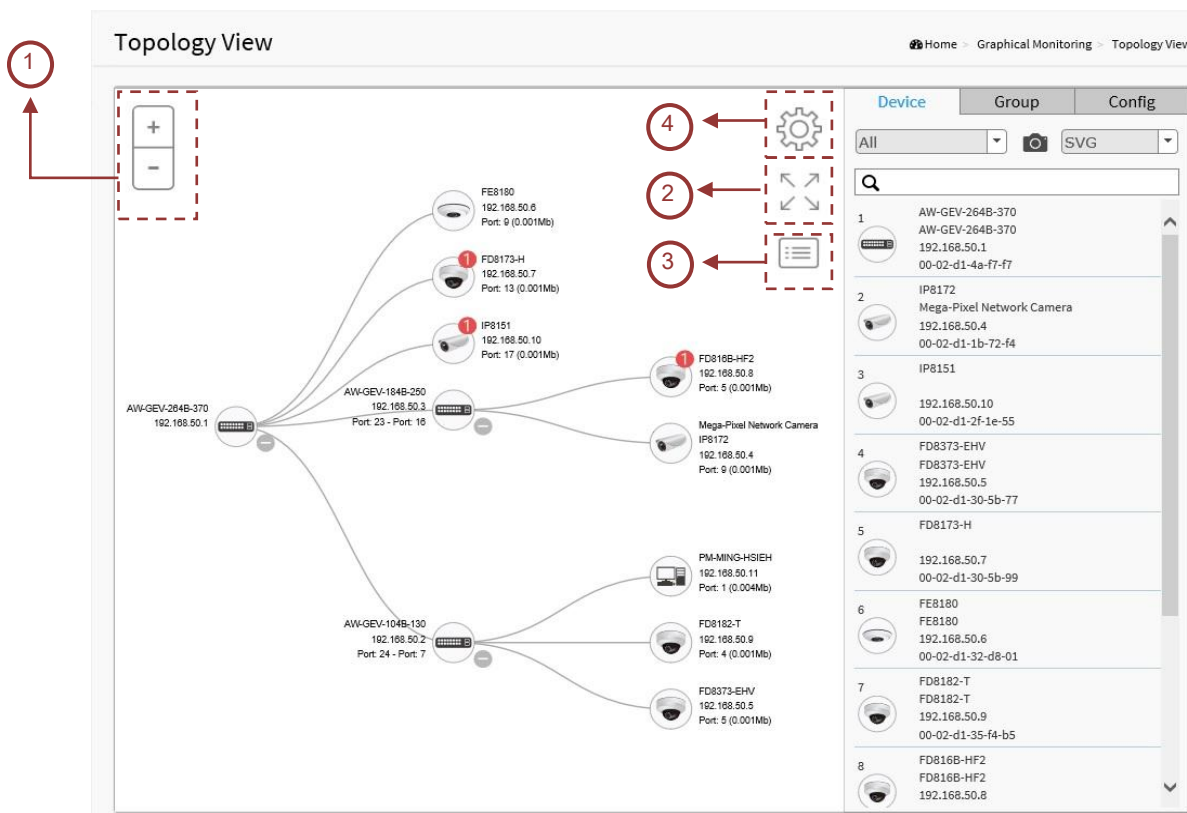





Figura 13-3: Vista de topología

Descripción funcional:

1.  Icono con botones más y menos: acercar y alejar la vista de topología, los usuarios pueden desplazar la rueda del mouse para lograr el mismo propósito.
2.  Icono con tipo de vista de pantalla: haga clic para cambiar a la vista de pantalla completa o haga clic nuevamente para volver a la vista normal.
3.  Icono con lista de información: los usuarios pueden seleccionar qué tipo de información se mostrará en la vista de topología de cada dispositivo. Se pueden seleccionar hasta 3 opciones a la vez.

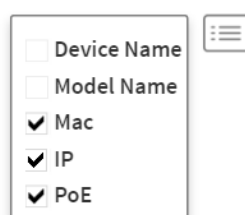


Figura 13-3: La lista de información

4. Iconos de dispositivo





- 
 Icono en negro: enlace del dispositivo. Los usuarios pueden seleccionar funciones y comprobar sus problemas.
- 
 Icono en rojo: enlace del dispositivo inactivo. Los usuarios pueden diagnosticar el estado del enlace.
- 
 Icono con números: significa que se han producido algunos eventos (por ejemplo, dispositivo fuera de línea, IP duplicado,... etc.) en el dispositivo IP, los usuarios pueden hacer clic en el icono del dispositivo para comprobar los eventos relacionados en la ventana de notificación.
- 
 Icono con un signo de interrogación: significa que se detectó el dispositivo IP, pero no se puede reconocer el tipo de dispositivo (clasificado como un tipo de dispositivo desconocido).
- Haga clic con el botón izquierdo en el icono de cualquier dispositivo para mostrar la consola del dispositivo y realizar más acciones:



Figura 13-3: Consola del dispositivo

- Consola del tablero: muestra información del dispositivo y acciones relacionadas para el dispositivo.
 - Diferentes tipos de dispositivos admiten diferentes funciones:
 - Si un dispositivo IP se reconoce como conmutador PoE, admitirá las funciones "Actualizar" y "Buscar conmutador".
 - Si un dispositivo IP se reconoce como dispositivo PoE, admitirá la función "Reiniciar" además de "Actualizar" y "Buscar interruptor".
 - Si un dispositivo IP se reconoce como cámara IP a través del protocolo ONVIF, admitirá la función "Streaming".
 - Tipo de dispositivo: el tipo de dispositivo se muestra automáticamente. Si se detecta un tipo desconocido, los usuarios aún pueden seleccionar el tipo de una lista predefinida.
 - Nombre del dispositivo: cree su propio nombre de dispositivo o alias para una fácil administración, como 1F_Lobby_Cam1.
 - Nombre del modelo, dirección MAC, dirección IP, máscara de subred, puerta de enlace, suministro de PoE y

Los PoE Usados se muestran automáticamente.

- Puerto HTTP: puede reasignar el número de puerto http al dispositivo para mayor seguridad.



Login

- Inicio de sesión: haga clic en el icono de acción de inicio de sesión para iniciar sesión en el dispositivo a través de una consola http para una mayor configuración o monitoreo de estado.



Diagnostics

- Diagnóstico: haga clic en el icono de acción de diagnóstico para realizar el diagnóstico del cable, examinar dónde está el cable roto y verificar si la conexión del dispositivo está activa o no haciendo ping.
 - Estado del cable:
 - Icono verde: el cable está conectado correctamente.
 - Icono rojo: el cable no está conectado correctamente. Los usuarios pueden verificar la información de distancia (XX metros) para identificar la ubicación de un enlace roto.
 - Conexión:
 - Icono verde: el dispositivo hizo ping correctamente.
 - Icono rojo: el dispositivo no se transmite / recibe datos correctamente, lo que significa que el ping no se realizó correctamente.

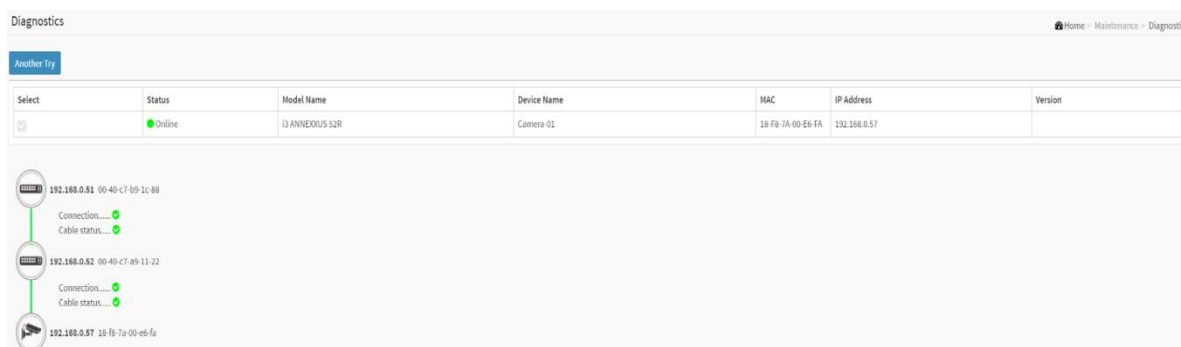


Figura 13-3: Los diagnósticos



Live Stream

- Transmisión en vivo: al conectar cámaras VIVOTEK, puede admitir la visualización de transmisión en vivo a través del navegador IE 11 con el reproductor Quicktime instalado.



Management


- Gestión: al conectar cámaras VIVOTEK, puede admitir la configuración de la configuración de red y la contraseña de la cámara.


Al habilitar el cliente DHCP, la cámara obtendrá la dirección IP del servidor DHCP que está en la red automáticamente.

Al deshabilitar el cliente DHCP, puede configurar una IP estática para la cámara.

FD8182-T (192.168.50.9)	
Device Name	FD8182-T
DHCP Client	Enable
IP Address	192.168.50.9
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.254
Primary DNS Server	8.8.8.8
Secondary DNS Server	
Root password	
Confirm Root password	
<input type="button" value="✓ Apply"/>	

Figura 13-3: Gestión

- 

Default Predeterminado: Restablece las cámaras VIVOTEK a la configuración predeterminada de fábrica.
- 

PoE Reboot Reinicio de PoE: haga clic en el icono de acción de reinicio para reiniciar el dispositivo de forma remota y así recuperar el dispositivo a su funcionamiento normal.









AW-GEV-264B-370	
Device Type	SWITCH
Device Name	AW-GEV-264B-370
Model Name	AW-GEV-264B-370
Mac Address	00-02-d1-4a-f7-f7
IP Address	192.168.50.1
Http port	80
PoE Supply	8.5 W
 Login  Find Switch  PoE Config  Diagnostics	
 Dashboard  Notification	

Figura 13-3: Panel de control del interruptor

- 

Login Inicio de sesión: haga clic en el icono de acción de inicio de sesión para iniciar sesión en el dispositivo a través de una consola http para una mayor configuración o monitoreo de estado.
- 

Find Switch Buscar interruptor: Todos los LED verdes en el interruptor parpadearán durante 15 segundos. Esto permite a un administrador ubicar el conmutador en una sala de equipos con muchos dispositivos.



- PoE Config** Configuración de PoE: Habilitar la función de verificación automática puede detectar la conexión entre el puerto PoE y el dispositivo alimentado. Si desactiva esta función, la detección se desactivará.



- Parent Node** Icono con nodo en blanco: cuando el conmutador PoE detecta más de dos dispositivos IP desde el mismo puerto, el conmutador no puede resolver el diseño de este dispositivo IP, en su lugar, mostrará un nodo en blanco para presentar esta situación. Los usuarios pueden utilizar la función "Nodo principal" para ajustar el diseño en el Tablero.

- Consola de notificaciones: muestra alarmas y registros de eventos. Las notificaciones pueden incluir: 1. Dispositivo reiniciado por el usuario (por ejemplo, PoE); 2. Dispositivo fuera de línea causado por la desconexión de la red; 3. IP duplicado; 4. Error de autenticación al iniciar sesión en una cámara IP.



Figura 13-3: Consola de notificaciones

- Monitor Console: muestra el tráfico con fines de verificación del estado del dispositivo.
 - Para cada dispositivo IP, excepto los conmutadores PoE, los usuarios pueden configurar un umbral de rendimiento y recibir notificaciones cuando el rendimiento actual sea inferior o superior a los valores configurados.
 - Si ambos valores son "0", significa que la función está deshabilitada.
 - El intervalo de sondeo predeterminado es de 1 segundo, cuando se cierra la página Vigilancia, el intervalo de sondeo cambiará a alrededor de 5 segundos.

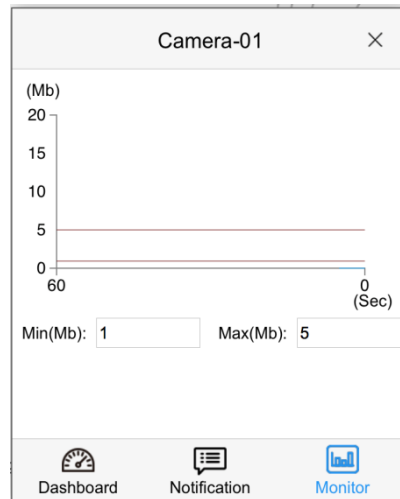

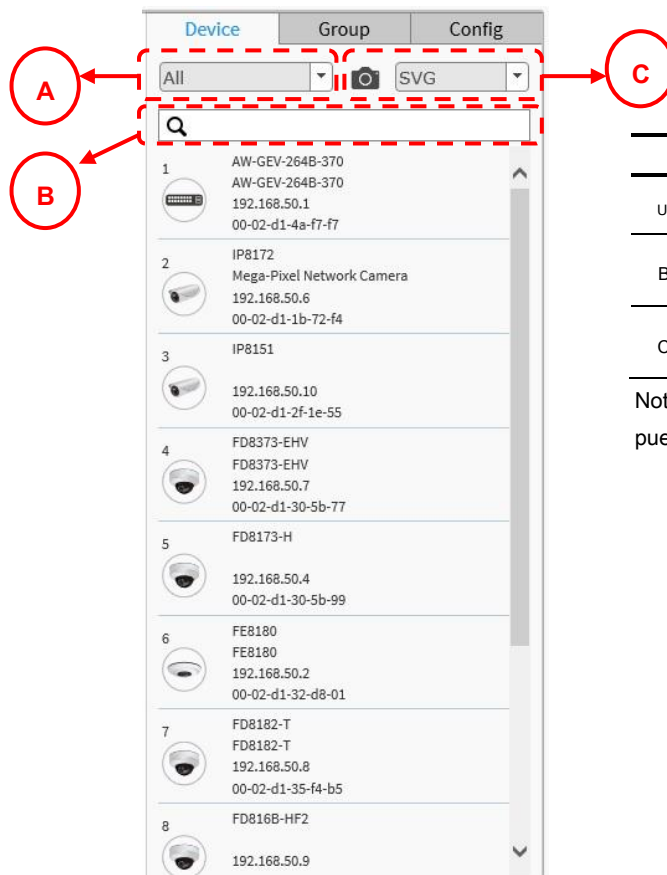


Figura 13-3: La consola del monitor

5.  En la esquina superior derecha, hay un "icono de configuración". La página Configuración proporciona acceso al dispositivo, grupo, configuración, vista de topología de exportación y funciones de búsqueda avanzada para la topología.

13-4. Consola de búsqueda de dispositivos

Todos los dispositivos y la información relacionada se mostrarán en la lista.



Device	Group	Config
All	SVG	
1	AW-GEV-264B-370 AW-GEV-264B-370 192.168.50.1 00-02-d1-4a-f7-f7	
2	IP8172 Mega-Pixel Network Camera 192.168.50.6 00-02-d1-1b-72-f4	
3	IP8151 192.168.50.10 00-02-d1-2f-1e-55	
4	FD8373-EHV FD8373-EHV 192.168.50.7 00-02-d1-30-5b-77	
5	FD8173-H 192.168.50.4 00-02-d1-30-5b-99	
6	FE8180 FE8180 192.168.50.2 00-02-d1-32-d8-01	
7	FD8182-T FD8182-T 192.168.50.8 00-02-d1-35-f4-b5	
8	FD816B-HF2 192.168.50.9	

Función	
UNA.	Filtrar dispositivos por tipo de dispositivo
B.	Busque dispositivos por palabras clave o usando la búsqueda de texto completo
C.	Guarde toda la vista de configuración en SVG, PNG o PDF

Nota: el navegador IE solo admite SVG, Chrome puede admitir SVG / PNG / PDF

Figura 13-4: Consola de búsqueda de dispositivos

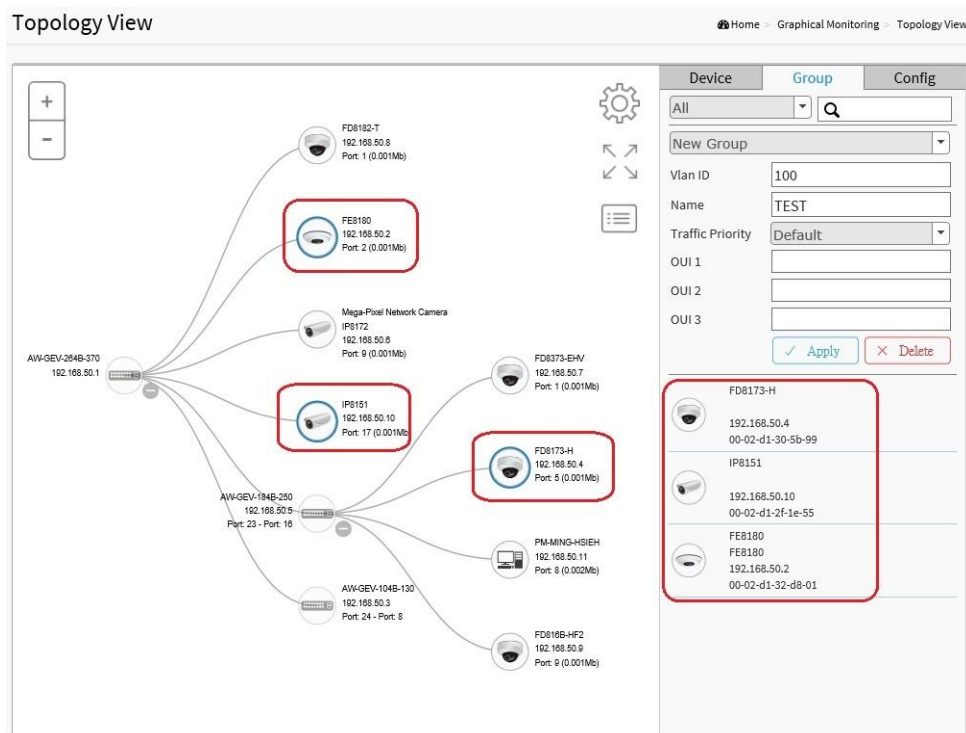
- **Consola de grupo**

También puede configurar la agrupación de VLAN en la Vista de topología. Para configurar la agrupación, proceda con lo siguiente:

1. Habilite el modo de agrupación seleccionando el menú "Grupo" del menú Lista de dispositivos. Seleccione Nuevo grupo en el menú desplegable. Cámaras o servidores IP con un solo clic para incluirlos en el grupo. Al configurar un grupo existente, seleccione un grupo existente.
2. Seleccione los miembros que prefiere de la topología.
3. Ingrese un nombre de grupo, una descripción y una ID de VLAN única. Consulte el capítulo anterior para obtener más detalles. VLAN ID es el identificador de VLAN (VID) para el puerto según se define en IEEE 802.1Q-2003. Se utiliza un valor de 1 a 4094 para definir una ID de VLAN válida. Se usa un valor de 0 (Prioridad etiquetada) si el dispositivo está usando tramas etiquetadas de prioridad según lo definido por IEEE 802.1Q-2003, lo que significa que solo el nivel de prioridad IEEE 802.1D es significativo y el PVID predeterminado del puerto de entrada se usa en su lugar.

Los identificadores organizativos únicos (OUI) son los primeros tres bytes de una dirección MAC, mientras que los últimos tres bytes contienen una ID de estación única. Puede agregar un fabricante con el OUI. Ingrese los primeros 3 octetos como el hexadecimal xx-xx-xx para especificar el rango del dispositivo.

Cuando termine, haga clic en el botón Aplicar para que la configuración surta efecto. Haga clic en el botón Guardar para guardar su configuración.



The screenshot shows the 'Topology View' of a network management console. On the left, a network diagram shows a central switch (AW-GEV-294B-370) connected to several other devices, including cameras and servers. On the right, there is a configuration panel for a group named 'TEST'. The panel includes fields for 'Vlan ID' (100), 'Name' (TEST), and 'Traffic Priority' (Default). Below the configuration panel, there is a list of devices that are part of the group, including FD8173-H, IP8151, FE8180, and others, with their respective IP addresses and MAC addresses.

Figura 13-4: Configuración de agrupamiento en la vista de topología

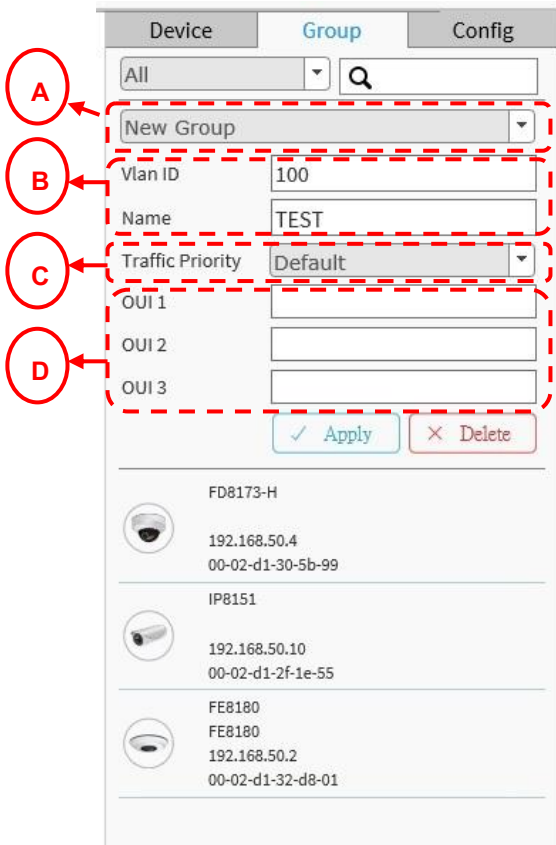
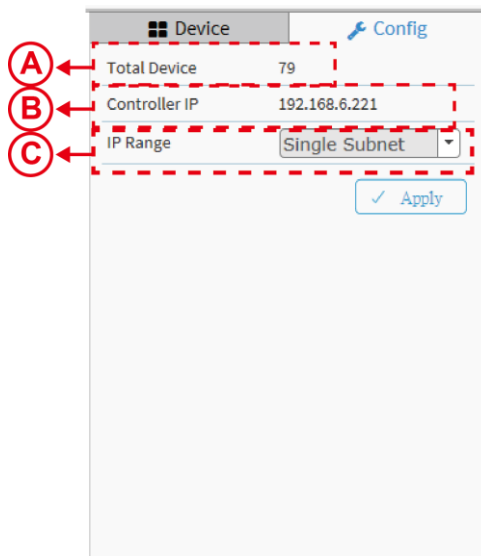


Figura 13-4: Consola de grupo

- Consola de configuración del sistema



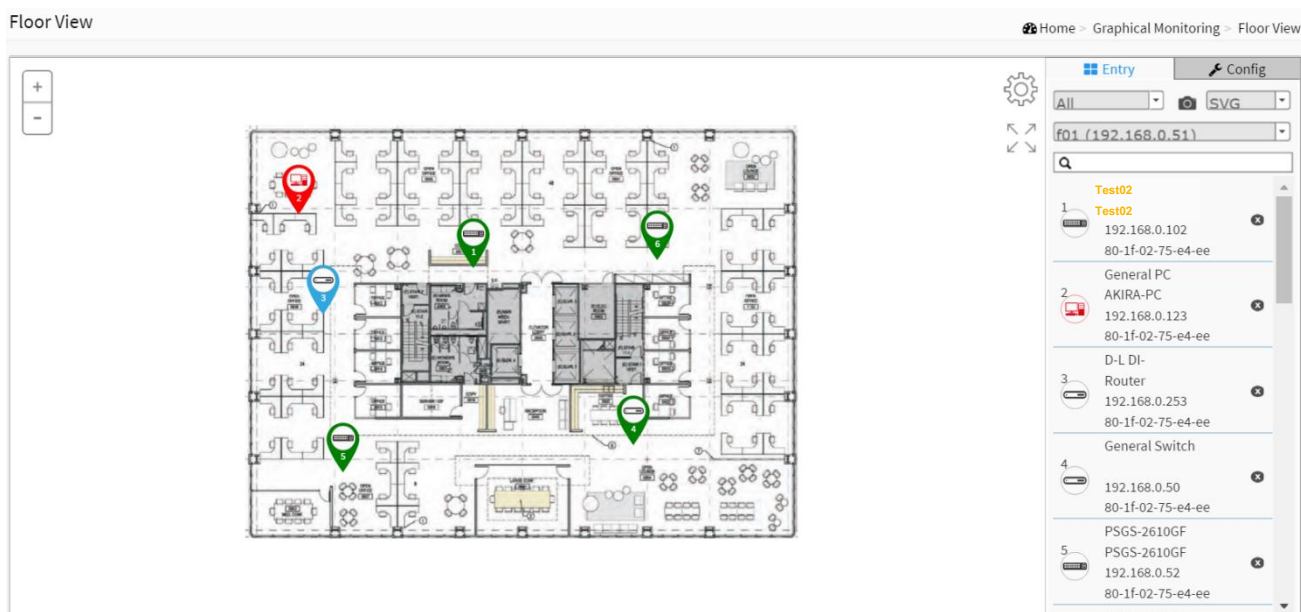
La consola de configuración del sistema


Función	
UNA.	Agrupe dispositivos filtrando, buscando, haciendo clic en los iconos del dispositivo o especificando OUI.
B.	Asigne el ID o el nombre de VLAN al grupo.
C.	Configure la prioridad del tráfico para la VLAN.
D.	Identificadores únicos organizacionales (OUI), ingrese los primeros 3 octetos como el hexadecimal xx-xx-xx para especificar el rango del dispositivo.

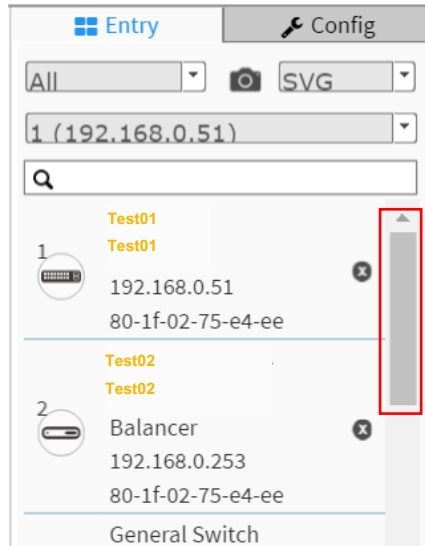
Función	
UNA.	Muestra el número de dispositivos IP detectados en la vista de topología.
B.	Muestra la IP del controlador.
C.	- Subred única: la interfaz escaneará la red local en busca de dispositivos donde reside el conmutador PoE. La máscara de subred es "255.255.255.0". - Subred múltiple: hasta 4 rangos de subred (Clase C subredes, por ejemplo, 192.168.1.1 ~ 192.168.4.254) puede ser asignado manualmente. (En el caso, sugerimos a los usuarios que ajusten la máscara de subred del conmutador a "255.255.0.0" para llegar a dispositivos IP en diferentes subredes).

Vista del piso

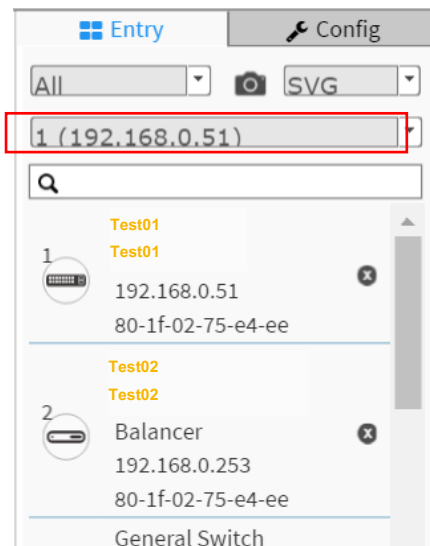
Los usuarios pueden planificar y representar fácilmente los dispositivos IP en los sitios de instalación utilizando las imágenes de piso personalizables.



- Seleccione los dispositivos del panel de entrada a la derecha. Cuando los dispositivos aparezcan en la imagen del piso, arrástrelos a una ubicación preferida.
- Encuentra la ubicación del dispositivo al instante
- Se pueden almacenar 10 mapas en cada conmutador
- Aplicaciones de vigilancia IP / VoIP / Wi-Fi
- Otras funciones son idénticas a las de la Vista de topología Para colocar y quitar un icono de dispositivo:
 - Para seleccionar un dispositivo, haga clic en su icono en el panel de Entrada.
 - El icono del dispositivo se mostrará en la ubicación predeterminada de la imagen del piso.
 - Haga clic y mantenga presionado el botón izquierdo del mouse y arrastre el icono a la ubicación preferida en la vista del piso.
- Haga clic en la imagen del  en el panel de entrada para eliminar un dispositivo de la vista del piso signo de la cruz.



- Si hay más de dos imágenes de piso, seleccione una imagen de piso de la lista desplegable.



Vista del mapa

En esta página, puede ver una representación realista de dispositivos a través del mapa de Google. Esta vista de mapa se aplica en implementaciones de áreas amplias al aire libre. Las condiciones previas para utilizar esta función son:

- La computadora cliente que tiene una sesión web con el conmutador PoE debe tener una **Internet** conexión.

Para configurar la Vista del mapa de vigilancia en la interfaz web: Haga clic en

Vigilancia> Vista gráfica> Mapa de Google.

1. En el mapa de Google, muévase a su ubicación y acérquese a una vista preferida. Para moverse en la pantalla, haga clic y mantenga presionado el botón izquierdo del mouse para moverse en la dirección preferida. También puede introducir la dirección que tiene en mente en el cuadro de búsqueda, por ejemplo, Sunset Boulevard, Los Ángeles, etc. También se admite la ubicación GPS de su posición actual.
2. Haga clic para seleccionar un dispositivo. El dispositivo aparecerá en el mapa. Haga clic y
3. arrastre el dispositivo a una ubicación preferida.
4. Repita el proceso anterior para completar la configuración del mapa y haga clic en Aplicar para finalizar la configuración.

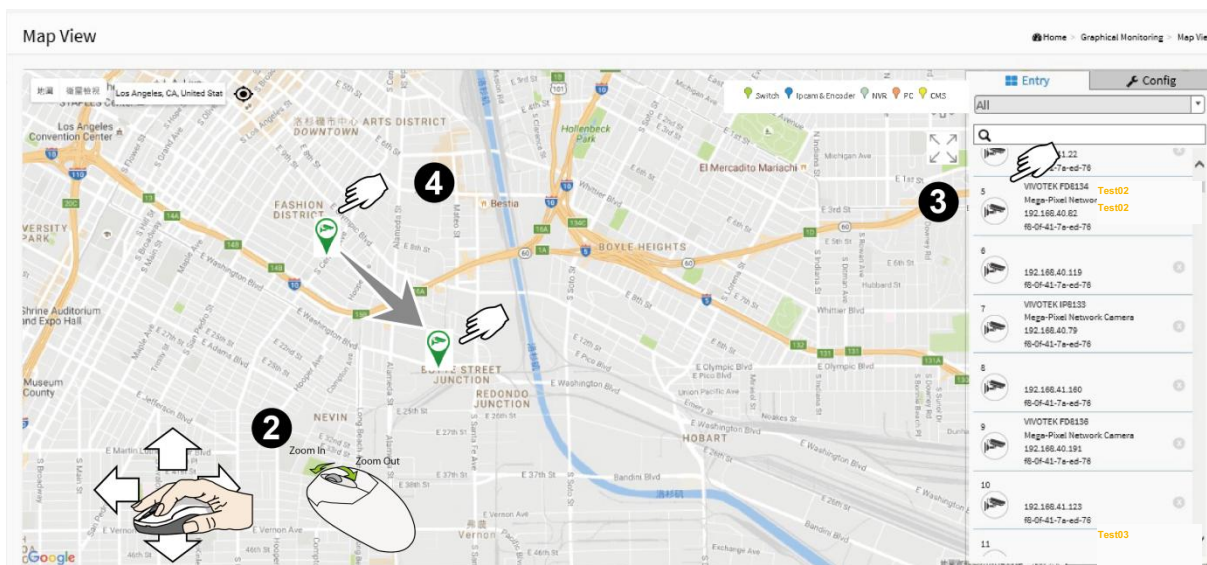


Figura 13-14: Vista de mapa

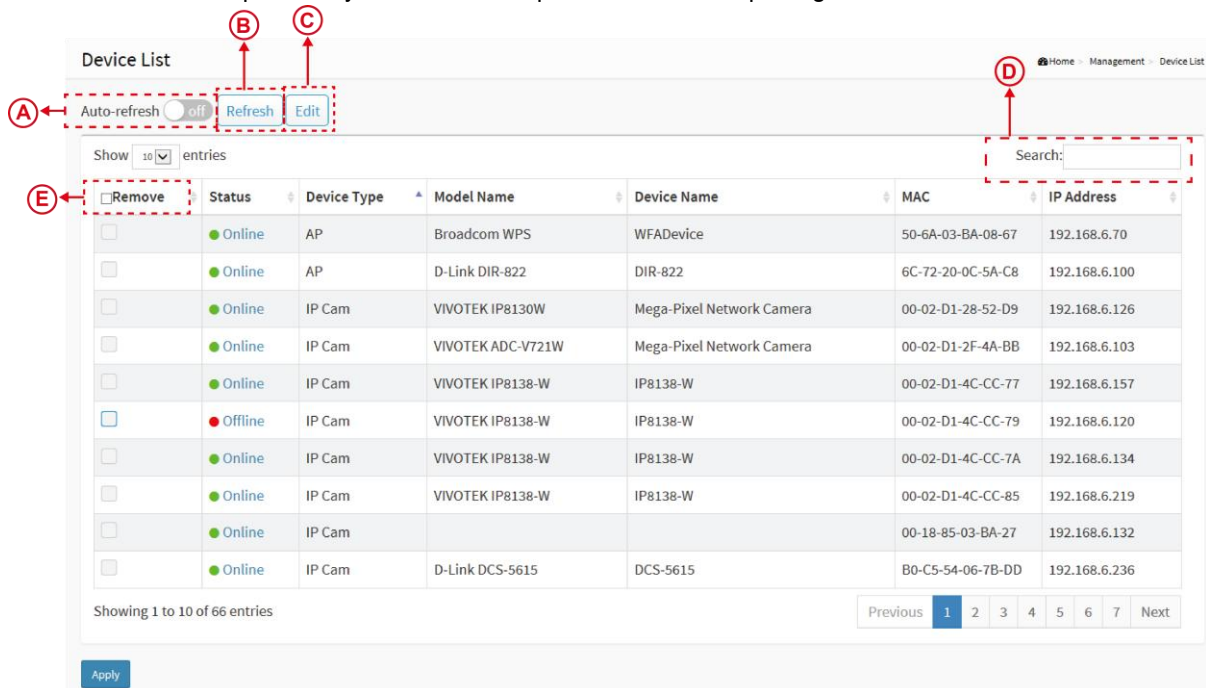
Para regresar a una ubicación que visitó anteriormente, simplemente haga clic en una cámara o dispositivo (en la Lista de dispositivos) que implantó en el mapa. La vista del mapa actual volverá a la ubicación que configuró anteriormente.

- Anclar dispositivos en Google Map. Encuentre
- dispositivos al instante desde el mapa. Búsqueda en
- línea de empresa / dirección.
- Aplicaciones de cámara IP / Wi-Fi para exteriores.
- Otras funciones son idénticas a las de la vista de topología.

administración

Lista de dispositivos

Mostrará todos los dispositivos y su información que son detectados por Vigilancia.



The screenshot shows the 'Device List' page. Annotations are as follows:

- A**: Points to the 'Auto-refresh' toggle switch, currently set to 'off'.
- B**: Points to the 'Refresh' button.
- C**: Points to the 'Edit' button.
- D**: Points to the search input field.
- E**: Points to the 'Remove' checkbox for a device.

Show	10	entries		Status	Device Type	Model Name	Device Name	MAC	IP Address
<input type="checkbox"/>	● Online	AP	Broadcom WPS	WFADevice	50-6A-03-BA-08-67	192.168.6.70			
<input type="checkbox"/>	● Online	AP	D-Link DIR-822	DIR-822	6C-72-20-0C-5A-C8	192.168.6.100			
<input type="checkbox"/>	● Online	IP Cam	VIVOTEK IP8130W	Mega-Pixel Network Camera	00-02-D1-28-52-D9	192.168.6.126			
<input type="checkbox"/>	● Online	IP Cam	VIVOTEK ADC-V721W	Mega-Pixel Network Camera	00-02-D1-2F-4A-BB	192.168.6.103			
<input type="checkbox"/>	● Online	IP Cam	VIVOTEK IP8138-W	IP8138-W	00-02-D1-4C-CC-77	192.168.6.157			
<input type="checkbox"/>	● Offline	IP Cam	VIVOTEK IP8138-W	IP8138-W	00-02-D1-4C-CC-79	192.168.6.120			
<input type="checkbox"/>	● Online	IP Cam	VIVOTEK IP8138-W	IP8138-W	00-02-D1-4C-CC-7A	192.168.6.134			
<input type="checkbox"/>	● Online	IP Cam	VIVOTEK IP8138-W	IP8138-W	00-02-D1-4C-CC-85	192.168.6.219			
<input type="checkbox"/>	● Online	IP Cam			00-18-85-03-BA-27	192.168.6.132			
<input type="checkbox"/>	● Online	IP Cam	D-Link DCS-5615	DCS-5615	B0-C5-54-06-7B-DD	192.168.6.236			

Showing 1 to 10 of 66 entries

Previous 1 2 3 4 5 6 7 Next

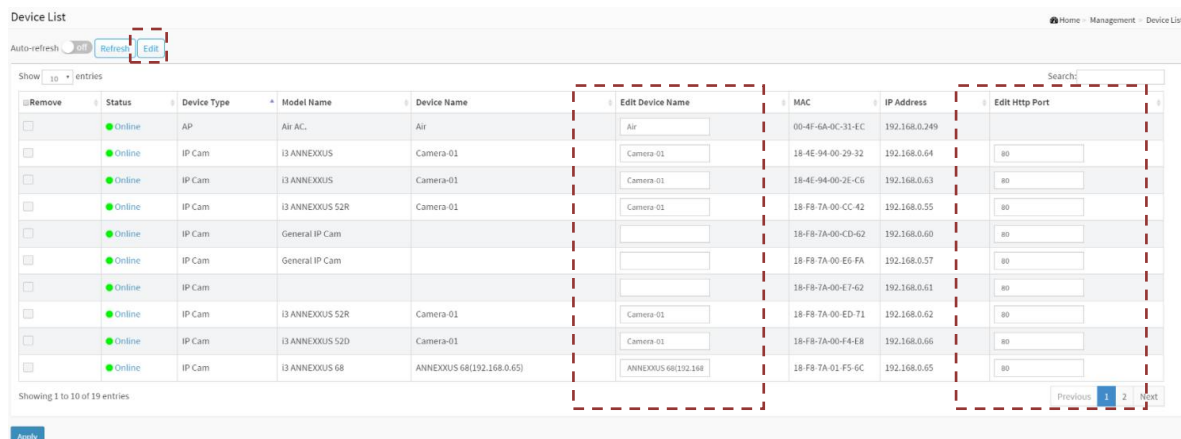
Apply

UNA. **Auto-refresh** off Si desea que el conmutador PoE actualice automáticamente la información, entonces necesita evocar la función "Actualización automática".

B. **Refresh** Haga clic en este botón para actualizar el estado de todos los dispositivos.

C. **Edit** Haga clic en este botón para editar el nombre del dispositivo y el puerto http.

- El usuario puede presionar el botón "Editar" para editar el nombre del dispositivo y el puerto HTTP para cada dispositivo IP. Esta función también se puede configurar en la vista Panel de control de topología.
- No hay una función de conexión HTTP para dispositivos de tipo PC y dispositivos desconocidos, por lo tanto, la interfaz de usuario no proporciona la función "Editar puerto HTTP" para ellos.



The screenshot shows the 'Device List' page with the 'Edit Device Name' and 'Edit Http Port' columns highlighted. The 'Edit Device Name' column contains input fields for each device's name, and the 'Edit Http Port' column contains input fields for each device's HTTP port.

Show	10	entries		Status	Device Type	Model Name	Device Name	MAC	IP Address	Edit Http Port
<input type="checkbox"/>	● Online	AP	Air AC	Air	00-4F-6A-0C-31-4C	192.168.0.249	Air			
<input type="checkbox"/>	● Online	IP Cam	3 ANNEXXUS	Camera-01	18-4E-94-00-29-32	192.168.0.64	Camera-01			80
<input type="checkbox"/>	● Online	IP Cam	3 ANNEXXUS	Camera-01	18-4E-94-00-2E-C6	192.168.0.63	Camera-01			80
<input type="checkbox"/>	● Online	IP Cam	3 ANNEXXUS S2R	Camera-01	18-F8-7A-00-CC-42	192.168.0.55	Camera-01			80
<input type="checkbox"/>	● Online	IP Cam	General IP Cam		18-F8-7A-00-CD-62	192.168.0.60				80
<input type="checkbox"/>	● Online	IP Cam	General IP Cam		18-F8-7A-00-E6-FA	192.168.0.57				80
<input type="checkbox"/>	● Online	IP Cam			18-F8-7A-00-E7-62	192.168.0.61				80
<input type="checkbox"/>	● Online	IP Cam	3 ANNEXXUS S2R	Camera-01	18-F8-7A-00-ED-T1	192.168.0.62	Camera-01			80
<input type="checkbox"/>	● Online	IP Cam	3 ANNEXXUS S2D	Camera-01	18-F8-7A-00-F4-E8	192.168.0.66	Camera-01			80
<input type="checkbox"/>	● Online	IP Cam	3 ANNEXXUS 68	ANNEXXUS 68(192.168.0.65)	18-F8-7A-01-F5-6C	192.168.0.65	ANNEXXUS 68(192.168.0.65)			80

Showing 1 to 10 of 19 entries

Previous 1 2 Next

Apply

D. Search: Busque dispositivos tecleando palabras con búsqueda de texto completo.

MI. Remove La función Eliminar solo se aplica a los dispositivos sin conexión.

Nota:

El nombre del dispositivo no se guardará hasta que haga clic en el botón Aplicar. No haga clic en los botones de actualización, actualización automática o edición antes de aplicar un nuevo nombre de dispositivo.

Codificador y cámara VVTK

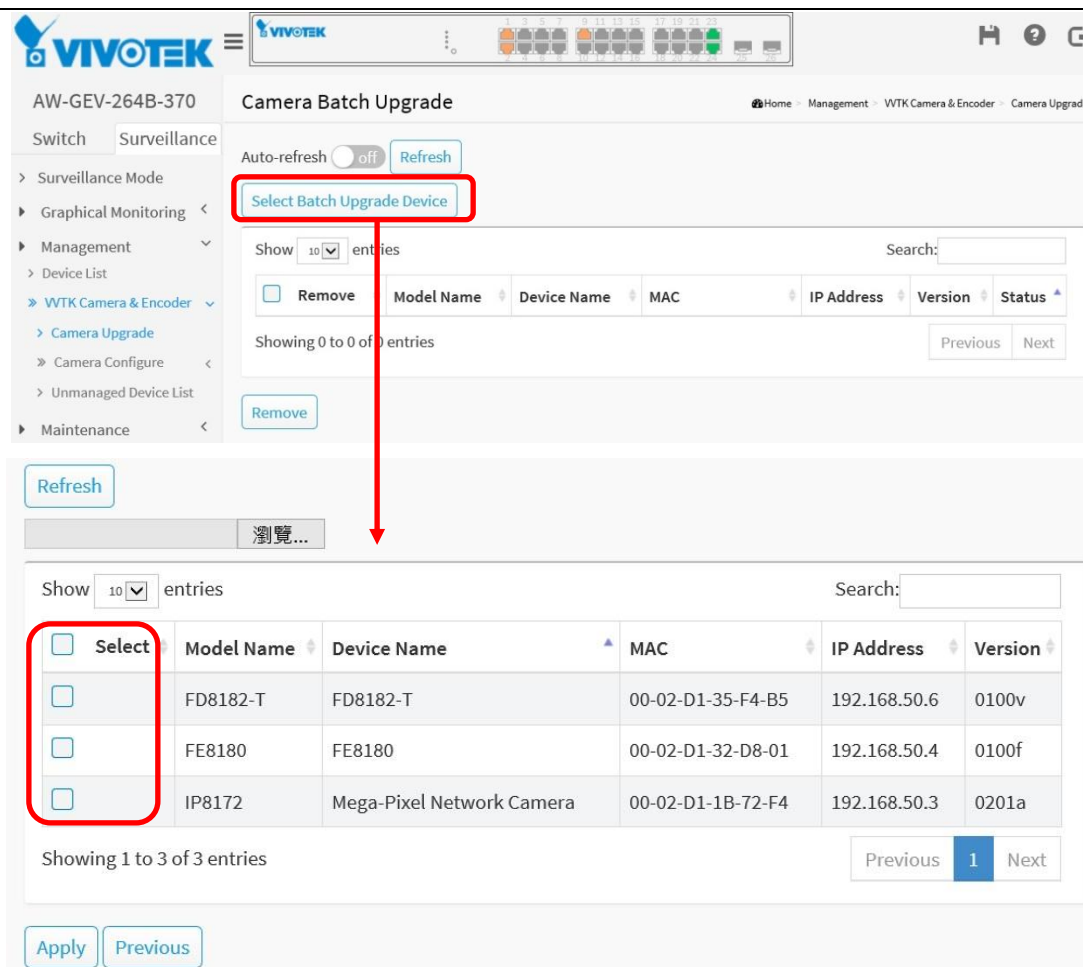
Actualización de la cámara

Esta sección describe cómo actualizar el firmware de la cámara. Las revisiones del firmware de la cámara pueden estar disponibles a lo largo del tiempo para mejorar la funcionalidad. Si tiene varias cámaras del mismo modelo, puede actualizar su firmware en un proceso.

interfaz web

Para configurar la actualización de la cámara de vigilancia en la interfaz web:

1. Haga clic en Vigilancia> Administración> Cámara y codificador> Actualización de cámara.
2. Haga clic en "Seleccionar dispositivo de actualización por lotes" para ingresar a la página seleccionada.
3. Haga clic en "Elegir archivo" para seleccionar el firmware de la computadora cliente.
4. Clics únicos o múltiples en sus casillas de verificación para seleccionar cámaras.
5. Haga clic en Aplicar para cargar el firmware en el búfer del conmutador.



AW-GEV-264B-370 **Camera Batch Upgrade** Home - Management - VTK Camera & Encoder - Camera Upgrade

Auto-refresh off Refresh

Select Batch Upgrade Device

Show 10 entries Search:

<input type="checkbox"/> Remove	Model Name	Device Name	MAC	IP Address	Version	Status
Showing 0 to 0 of 0 entries						
Previous Next						

Remove

Refresh

瀏覽...

Show 10 entries Search:

<input type="checkbox"/> Select	Model Name	Device Name	MAC	IP Address	Version
<input type="checkbox"/>	FD8182-T	FD8182-T	00-02-D1-35-F4-B5	192.168.50.6	0100v
<input type="checkbox"/>	FE8180	FE8180	00-02-D1-32-D8-01	192.168.50.4	0100f
<input type="checkbox"/>	IP8172	Mega-Pixel Network Camera	00-02-D1-1B-72-F4	192.168.50.3	0201a

Showing 1 to 3 of 3 entries Previous 1 Next

Apply Previous

Configurar cámara

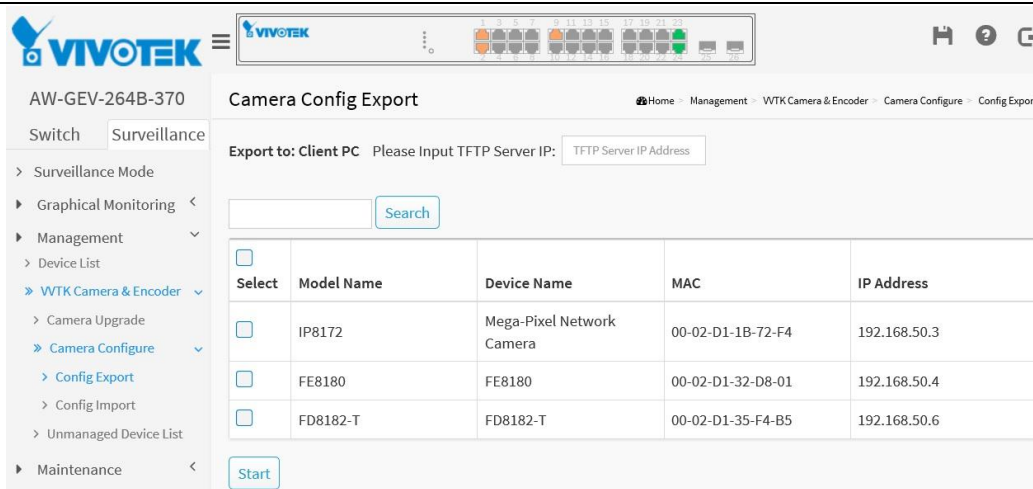
Exportación de configuración

interfaz web

Para configurar la información de vigilancia en la interfaz web:

1. Haga clic en Vigilancia> Administración> Cámara y codificador> Exportar configuración.
2. Seleccione la cámara desde la que exportar el archivo de configuración. Puede exportar la configuración a una computadora cliente, se requiere un servidor TFTP en su red. El perfil de configuración se transporta a través de un servidor TFTP.

El cuadro de búsqueda permite filtrar la búsqueda de dispositivos mediante el nombre del modelo, la dirección MAC o las direcciones IP.



AW-GEV-264B-370

Switch Surveillance

Surveillance Mode

- Graphical Monitoring
- Management
 - Device List
 - WTK Camera & Encoder
 - Camera Upgrade
 - Camera Configure
 - Config Export
 - Config Import
 - Unmanaged Device List
 - Maintenance

Camera Config Export

Export to: Client PC Please Input TFTP Server IP:

Search

Select	Model Name	Device Name	MAC	IP Address
<input type="checkbox"/>	IP8172	Mega-Pixel Network Camera	00-02-D1-1B-72-F4	192.168.50.3
<input type="checkbox"/>	FE8180	FE8180	00-02-D1-32-D8-01	192.168.50.4
<input type="checkbox"/>	FD8182-T	FD8182-T	00-02-D1-35-F4-B5	192.168.50.6

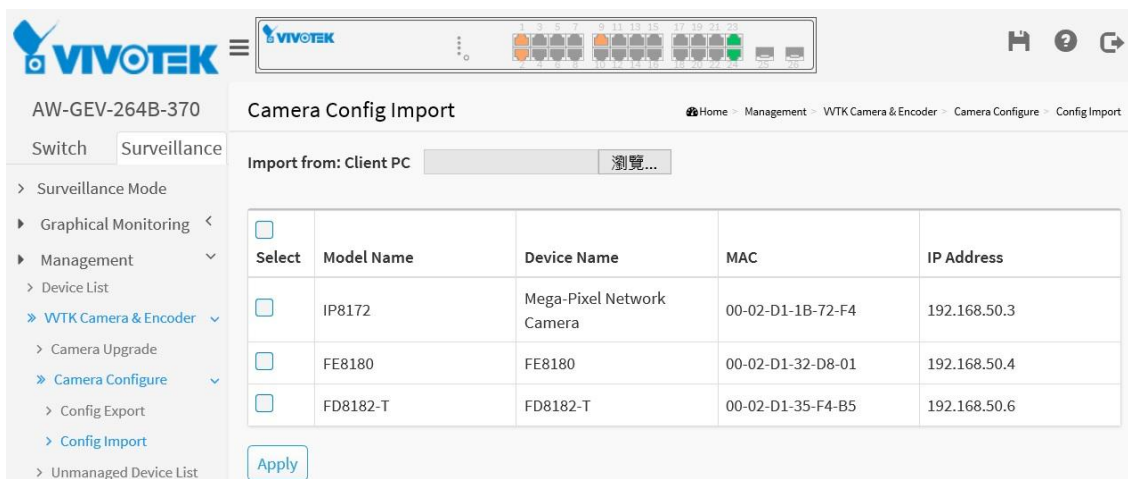
Start

Importación de configuración

interfaz web

Para configurar la configuración de la cámara, en la interfaz web:

1. Haga clic en Vigilancia> Administración> Cámara y codificador VVTK> Configurar cámara> Importar configuración.
2. Seleccione el dispositivo para importar el archivo de configuración desde la PC cliente.
3. Seleccione la cámara IP para cargar el archivo de configuración con un solo clic en su casilla de verificación. Haga clic en el botón Aplicar.
- 4.



AW-GEV-264B-370

Switch Surveillance

Surveillance Mode

- Graphical Monitoring
- Management
 - Device List
 - WTK Camera & Encoder
 - Camera Upgrade
 - Camera Configure
 - Config Export
 - Config Import
 - Unmanaged Device List
 - Maintenance

Camera Config Import

Import from: Client PC

Select	Model Name	Device Name	MAC	IP Address
<input type="checkbox"/>	IP8172	Mega-Pixel Network Camera	00-02-D1-1B-72-F4	192.168.50.3
<input type="checkbox"/>	FE8180	FE8180	00-02-D1-32-D8-01	192.168.50.4
<input type="checkbox"/>	FD8182-T	FD8182-T	00-02-D1-35-F4-B5	192.168.50.6

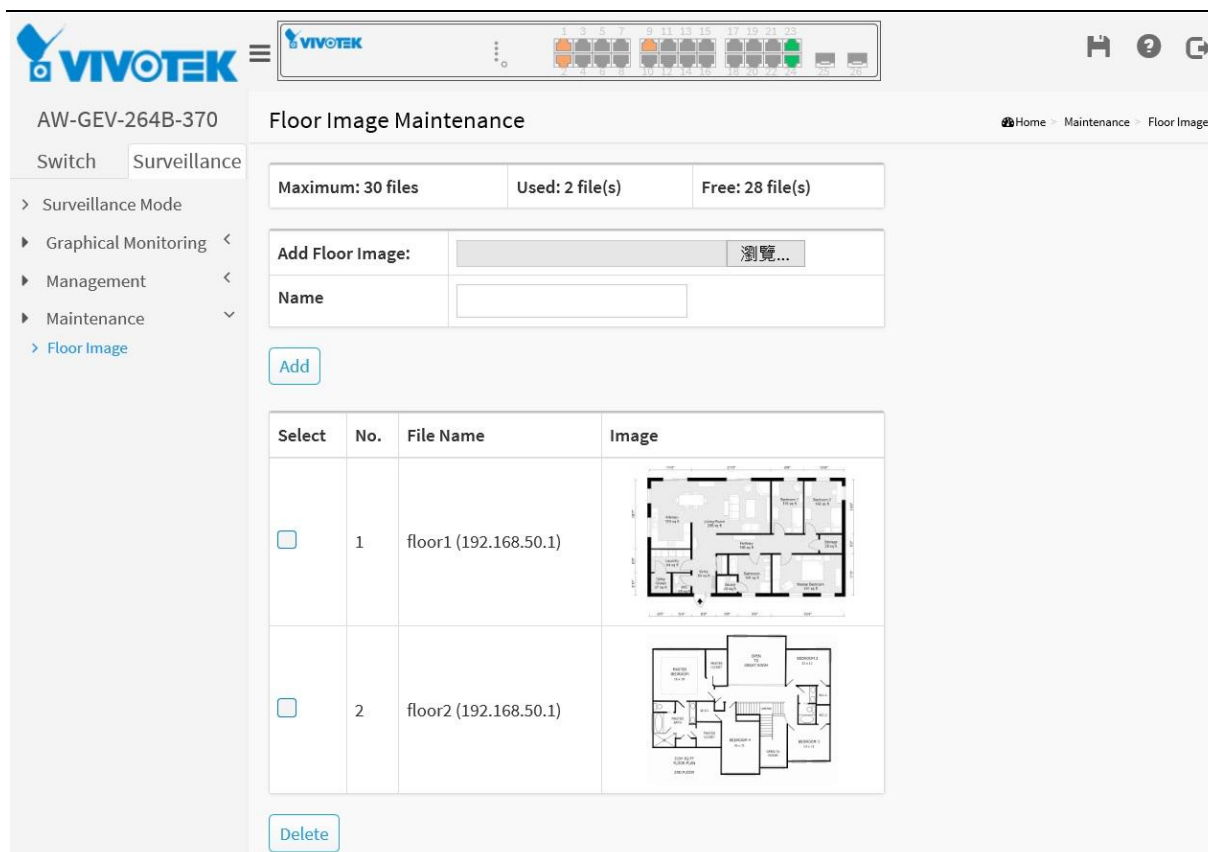
Apply

Mantenimiento

Imagen del piso

En esta página, los usuarios pueden agregar o eliminar imágenes del piso.

- Se pueden cargar hasta 30 archivos de imagen en el conmutador PoE. Solo admite formatos JPG y PNG.
- El máximo. El tamaño del archivo está limitado a 512 KB.
- Todas las imágenes del piso en la misma red se pueden compartir mediante múltiples conmutadores PoE.
- Por ejemplo:
Si Switch1 tiene 10 imágenes de piso, Switch2 tiene 5 imágenes, las 15 imágenes de piso en total se pueden compartir y seleccionar en diferentes switches PoE en la misma red.
- El nombre del archivo de imagen se mostrará con su dirección IP para que los usuarios sepan qué conmutador PoE contiene la imagen del piso.



AW-GEV-264B-370

Switch Surveillance

Surveillance Mode

Graphical Monitoring

Management

Maintenance

Floor Image

Floor Image Maintenance



Home Maintenance Floor Image

Maximum: 30 files Used: 2 file(s) Free: 28 file(s)

Add Floor Image: 瀏覽...

Name

Add

Select	No.	File Name	Image
<input type="checkbox"/>	1	floor1 (192.168.50.1)	
<input type="checkbox"/>	2	floor2 (192.168.50.1)	

Delete