POE-GSH802M

Switch de 8 puertos Gigabit PoE+

2-Gigabit SFP

POE-GSH1602M

Switch de 16 puertos Gigabits PoE+

2-Gigabits SFP + 2-Gigabits RJ-45

Manual técnico-
Español

Ver. SP-1.0

Historial de revisiones

Fecha	Versión	Descripción
22 de Octubre de 2022	SP-V 1.0	La primera edición

Contenido

POE-GSH802M 1

Switch de 8 puertos Gigabit PoE+ 1

2-Gigabit SFP 1

POE-GSH1602M 1

Switch de 16 puertos Gigabits PoE+ 1

2-Gigabits SFP + 2-Gigabits RJ-45 1

Manual técnico- Español 1

Ver. SP-1.0 1

1 Prefacio 5

2 Acceso vía interfaz web 6

3 Estado 15

4 Parámetros de Red 18

4.2 DNS 19

5 Puerto 22

5.4 Eee 32

6 Configuración POE 40

7 VLAN 43

7.1 VLAN 45

7.4 VLAN de Mac 62

7.6 GVRP 69

8 Tabla de Direcciones MAC 73

9 Árbol de Expansión 78

10 Descubrimiento 91

10.1 LLDP 92

11 DHCP 101

12 Multidifusión 108

12.4 MVR 119

13 Enrutamiento 123

14 Seguridad 131

14.1 RADIO 131

14.2 TACACS+ 133

14.3 AAA 134

15 ACL 167

15.1 ACL MAC 168

16 QoS 180

17 Diagnósticos 191

17.6 UDLD 196

18 Administración..... 199

18.4 SNMP..... 202

18.5 RMON..... 211

1 Prefacio

1.1 ¿A quién va dirigido?

Este manual ha sido preparado para instaladores, administradores de sistemas y usuarios responsables de la instalación, configuración y mantenimiento de redes. El mismo supone que el usuario entiende todos los protocolos de comunicación y gestión, así como los términos técnicos, principios teóricos, destrezas prácticas y experticia sobre los protocolos e interfaces relacionadas con las redes. Requiere experiencia de trabajo en la interfaz gráfica de usuario (GUI), Interfaz de línea de comando (CLI), Protocolo de Gerencia Simple de Red (SNMP) y el programa de navegación web.

**Nota: Este manual fue realizado con las imágenes de la interfaz WEB UI del POE-GSH802M.

1.2 Nomenclatura del Manual

Deben prevalecer los siguientes enfoques.

Convención GUI	Descripción
Interpretación	Describe operaciones y agrega información necesaria
 Precaución	Alerta al usuario de Precauciones debido a que la mala operación puede resultar en pérdida de datos o daño al equipo.

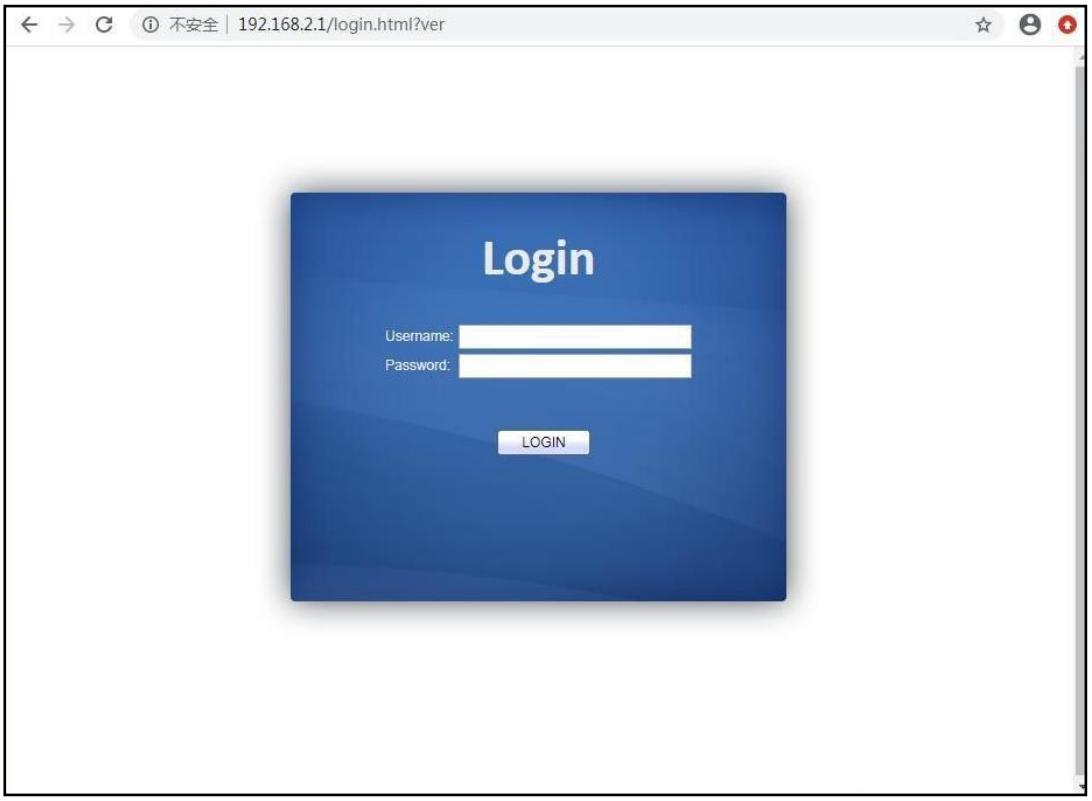
2 Acceso vía interfaz web

2.1 Acceso mediante Cliente de Gerencia de red

Escribe en la barra de comando del navegador, la dirección IP por defecto del switch: **http://192.168.2.1** y presione “Intro”. Descripción:

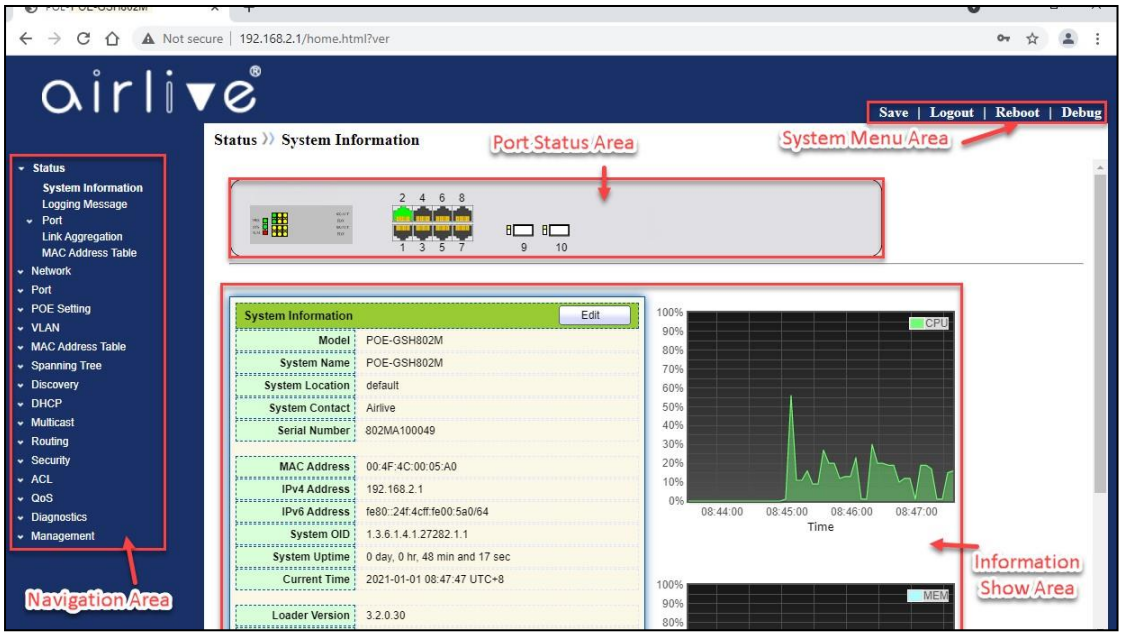
Los navegadores superiores a IE 9.0, Chrome 23.0 y Firefox 20.0 mantienen la IP del segmento de red del PC consistente con la del switch pero diferencia la dirección IP cuando accedes. Configura la dirección IP del PC como 192.168.2.x y la más cara de subred como 255.255.255.0 para el primer ingreso (1< x ≤254).

Una ventana aparecerá como se muestra a continuación. Escribe el nombre por defecto “**admin**” y la clave “**admin**”. Haga Click sobre el botón LOGIN para entrar al sistema del switch.



2.2 Conformación de la interfaz Cliente del Switch

La típica interfaz de operación de gestión web se muestra a continuación.



2.3 Barra de Navegación de la Interfaz Web

Hay opciones en el menú del sistema tales como “State, Network, Port, PoE Setting, VLAN, tabla de direcciones MAC, árbol de expansión, descubrimiento, DHCP, multidifusión, enrutamiento,
Seguridad, ACL, QoS, Diagnóstico y Gestión". Cada opción contiene submenús, como se muestra a continuación:

Opciones del menú	Submenús	Submenús secundarios	Descripción
Status	System Information		Muestra el estado del Puerto e información del producto
	Mensaje de Logging		Muestra el equipo en uso y el registro de operación
	Port	Statistics	Muestra estadística detallada del puerto
		Error Disabled	Muestra las fallas que ocurren al puerto
		Bandwidth Utilization	Muestra el ancho de banda por unidad de tiempo de los puertos

	Link Aggregation		Muestra el estado del Grupo de Agregación y sus miembros
	MAC Address Table		Muestra la tabla de direcciones MAC del dispositivo en uso
Network	IP Address		Configurar y ver la dirección IP de gestión
	DNS		Configurar y ver el DNS
	Hosts		Configurar y ver el Servidor DNS y la tabla dinámica de hosts
	System Time		Configurar y ver la actual hora del sistema
Port	Port Setting		Configurar y ver todos los puertos
	Error Disabled		Configurar y ver la protección de deshabilitar por error el puerto
Poe	Link Aggregation	Group	Configurar y ver los algoritmos de estrategia de balanceo de puertos contenida en el LAG
		Port Setting	Configurar y ver el LAG
		LACP	Verifica la prioridad LACP del sistema y configuración del puerto
	EEE		Configurar y ver el estado EEE e información
	Jumbo Frame		Configurar y ver la longitud del mensaje más largo transferido por el sistema
	Port Security		Configurar y ver la tasa límite de seguridad del Puerto, así como el estado del puerto
	Protected Port		Configurar y ver el aislamiento del puerto
	Storm Control		Configurar y ver la vigilancia de tormenta en el puerto
	Mirroring		Configurar y ver la duplicación de puerto
	PoE Port Setting		Configurar y ver el puerto PoE
	PoE Port Timer Setting		Configurar y ver el interruptor de sincronización del puerto PoE
	Configuración de reinicio del PoE Port		Configurar y ver el reinicio de la programación del puerto PoE

	Timer Reboot Setting		
VLAN	VLAN	Create VLAN	Configurar y ver la información VLAN del dispositivo
		VLAN Configuration	Configurar y ver la configuración VLAN de puertos
		Membership	Configurar y ver la información de VLANs
		Port Setting	Configurar y ver los atributos PVID y VLAN de los puertos
	Voice VLAN	Property	Configurar y ver la función Voice-VLAN y estado del puerto
		Voice OUI	Configurar y ver la información Voice-VLAN OUI
	Protocol VLAN	Protocol Group	Configurar y ver el protocolo de Grupo VLAN
		Group Binding	Configurar y ver el protocolo VLAN del puerto y el grupo de vinculación
	MAC VLA	MAC Group	Configurar y ver el Grupo de MAC VLAN
		Group Binding	Configurar y ver el puerto MAC VLAN y el grupo de vinculación
	Surveillance VLAN	Property	Configurar y ver la función Surveillance- VLAN y la información del estado
		Surveillance OUI	Configurar y ver la información Surveillance- VLAN OUI
	GVRP	Property	Configurar y ver el funcionamiento funcional global y el estado del puerto
		Membership	Configurar y ver las VLANs aprendidas y los puertos miembros
		Statistics	Configurar y ver la estadística de mensajes relacionados con los puertos
MAC Address Table	Dynamic Address		Configurar y ver las direcciones MAC dinámicas y el tiempo de envejecimiento del dispositivo
	Static Address		Configurar y ver las tablas de direcciones MAC del dispositivo

	Filtering Address		Configurar y ver las tablas de direcciones MAC a ser filtradas
	Port Security Address		Configurar y ver la tabla de direcciones MAC aprendidas por la seguridad del puerto
Árbol de expansión	Propiedad		Configurar y ver el estado STP y atributos
	Configuración del puerto		Configurar y ver los atributos del Puerto del STP
	Instancia de MST		Configurar y ver los atributos de instancia de STPs
	Configuración del puerto MST		Configurar y ver las instancias de STPs (incluyendo información del puerto
	Estadística		Configurar y ver la estadística del mensaje STP de cada puerto
Spanning Tree	Property Port Setting		Configurar y ver los atributos relacionados con LLDP
			Configurar y ver el estado de Transmisión & Recepción LLDP en cada puerto
	MST Instance		Configurar y ver el contenido de la tabla de estrategia de red MED
	MST Port Setting		Configurar y ver el estado MED de cada puerto
	Statistics		Configurar y ver los mensajes LLDP detallados de cada puerto
Discovery	LLDP	Property	Configurar y ver el estado LLDP y LLDP-MED
		Port Setting	Configurar y ver la información del LLDP vecino
		MED Network Policy	Configurar y ver el estado de Transmisión & Recepción del mensaje LLDP de cada puerto
		MED Port Setting	Configurar y ver los switches de servicio DHCP y los puertos del switch
DHCP	Propiedad	Packet View	Configurar y ver el conjunto de direcciones IP del Servidor DHCP
	Configuración del grupo de direcciones IP	Local Information	Configurar y ver VLAN IF y enlace de grupo de servidores DHCP
	Dirección IF de VLAN	Neighbor	Configuración de grupo DHCP
	Configuración de grupo		

	Client List		Ver la lista de clientes DHCP
	Client Static Binding Table		Configurar y ver la entrada de la tabla estática de clientes DHCP vinculadas
Multicast	General	Propiedad	Configurar y ver la configuración de esta función
		Dirección del grupo	Configurar y ver la información de multidifusión estática
		Puerto del router	Configurar y ver la información de multidifusión enrutada del puerto
		Reenvío de todo	Configurar y ver la información de multidifusión reenviada del puerto
		Regulación	Configurar y ver el límite de multidifusión de cada puerto
		Perfil de filtrado	Configurar y ver las direcciones de multidifusión filtradas
		Filtrado de enlaces	Configurar y ver la información vinculada asociada con la regla de filtrado y puertos
	IGMP Snooping	Propiedad	Configurar y ver el switch, la versión, etc.
		Consulta	Configurar y ver el estado del interrogador
		Estadística	Configurar y ver los mensajes de este protocolo
	MLD Snooping	Propiedad	Configurar y ver el protocolo, el switch, etc.
		Estadística	Configurar y ver los mensajes de este protocolo
	MVR	Propiedad	Configurar y ver la información de atributos como el switch
		Configuración del puerto	Configurar y ver el estado en cada Puerto
		Dirección del grupo	Configurar y ver la función, VLAN and dirección de grupo
Routing	IPv4 Management and Interfaces	Interfaz IPv4	Configurar y ver información de direcciones VLANIF IPv4
		Rutas IPv4	Configurar y ver rutas estáticas IPv4
		ARP	Configurar y ver la tabla ARP
	IPv6 Management and Interfaces	Interfaz IPv6	Configurar y ver información de la interfaz VLANIF IPv6
		Dirección IPv6	Configurar y ver la información de dirección VLANIF IPv6

		IPv6 Routes	Configurar y ver las rutas estáticas IPv6
		IPv6 Neighbors	Configurar y ver la tabla de vecinos IPv6
Security	RADIUS		Configurar y ver información del servidor RADIUS asociado
	TACACS+		Configurar y ver información del servidor TACACS+ asociado
	AAA	Method List	Configurar y ver el método de autenticación de acceso
		Login Authentication	Configurar y ver los métodos de autenticación de terminales
	Management Access	Management VLAN	Configurar y ver la gestión de VLAN
		Management Service	Configurar y ver el modo de servicio de gestión y atributos relevantes
		Management ACL	Configurar y ver la ACL dirigida a canales de gestión
		Management ACE	Configurar y ver configuración ACE de los canales de gestión
	Authentication Management	Property	Configurar y ver atributos de autenticación
		Port Setting	Configurar y ver información de autenticación de cada puerto
		MAC Local Account	Configurar y ver la lista de cuentas MAC local
		Web Local Account	Configurar y ver la lista de cuentas Web local
		Sessions	Configurar y ver información relacionada con la sesión de autenticación
	DoS	Property	Configurar y ver la opción de poder ver el switch
		Port Setting	Configurar y ver la opción de ver los puertos del switch
	Dynamic ARP inspection	Property	Configurar y ver la inspección dinámica ARP
		Statistics	Configurar y ver mensajes de estadística en el estado de inspección APR en cada puerto

	DHCP Snooping	Property	Configurar y ver el switch y su estado
		Statistics	Configurar y ver mensajes de estadística recibidos en cada puerto
		Option82 Property	Configurar y ver los atributos relacionados con la Opción 82
		Option82 Circuit ID	Configurar y ver el ID de Circuito de Opción 82
	IP Source Guard	Port Setting	Configurar y ver el estado de los puertos
		IMPV Binding	Configurar y ver la tabla IP, MAC, Port y VLAN vinculada
		Save Database	Configurar y ver el almacenamiento e información de entrada en la tabla vinculada
ACL	MAC ACL		Configurar y ver las reglas de ACL MAC
	MAC ACE		Configurar y ver la entrada de la tabla de MAC ACE
	IPv4 ACL		Configurar y ver las reglas de ACL IPv4
	IPv4 ACE		Configurar y ver la entrada de la tabla ACE IPv4
	IPv6 ACL		Configurar y ver las reglas de ACL IPv6
	IPv6 ACE		Configurar y ver la entrada de la tabla ACE IPv6
	ACL Binding		Configurar y ver las reglas de ACL y la aplicación al puerto vinculado
QoS	General	Property	Configurar y ver calidad de servicio QoS y estado del switch
		Queue Scheduling	Configurar y ver el algoritmo de la cola programada
		CoS Mapping	Configurar y ver la prioridad y la tabla de mapeo local CoS
		DSCP Mapping	Configurar y ver la prioridad y tabla de mapeo local DSCP
		IP Precedence Mapping	Configurar y ver la tabla de mapeo de precedencia IP
	Rate Limit	Ingress/Egress Port	Configurar y ver el límite de velocidad configurada del puerto

		Cola de salida	Configurar y ver velocidad límite configurada en cola de egreso
Diagnósticos	Registro	Propiedad	Configurar y ver el switch y su estado
		Servidor remoto	Configurar y ver la dirección de servidores remotos
	Señal		Ping de diagnóstico de red
	Traceroute		Diagnóstico de red por comando Traceroute
	Prueba de cobre		Diagnóstico del enlace de la interfaz eléctrica mediante VCT
	Módulo de fibra		Verificación del módulo SFP de las interfaces ópticas
	UDLD	Propiedad	Configurar y ver el switch y estado del enlace unidireccional
		Vecino	Configurar y ver el estado del enlace vecino
Administración	Cuenta de usuario		Configurar y ver usuario
	Firmware	Actualizar	Actualizar Software
	Configuración	Actualizar	Actualizar los archivos de configuración
		Guardar configuración	Guarda archivo de Configuración en funcionamiento
	SNMP	Vista	Configurar y ver la entrada de la tabla de función SNMP
		Grupo	Configurar y ver el grupo SMNP
		Comunidad	Configurar y ver el parámetro SNMP Community
		Usuario	Configurar y ver los atributos de usuario SNMP
		ID del motor	Configurar y ver los IDs SNMP y motor remoto
		Evento Trap	Configurar y ver las trampas SNMP y estado del switch
		Notificación	Configurar y ver el estado de la notificación SNMP del servidor
	RMON	Estadística	Configurar y ver el registro de estadística de todos los puertos
		Historia	Configurar y ver el histórico registrado del estado del switch
		Evento	Configurar y ver estado de eventos
		Alarm	Configurar y ver el estado de alarmas

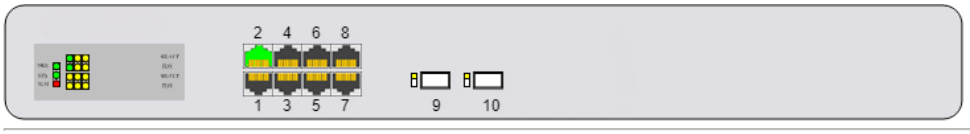
3 Estado

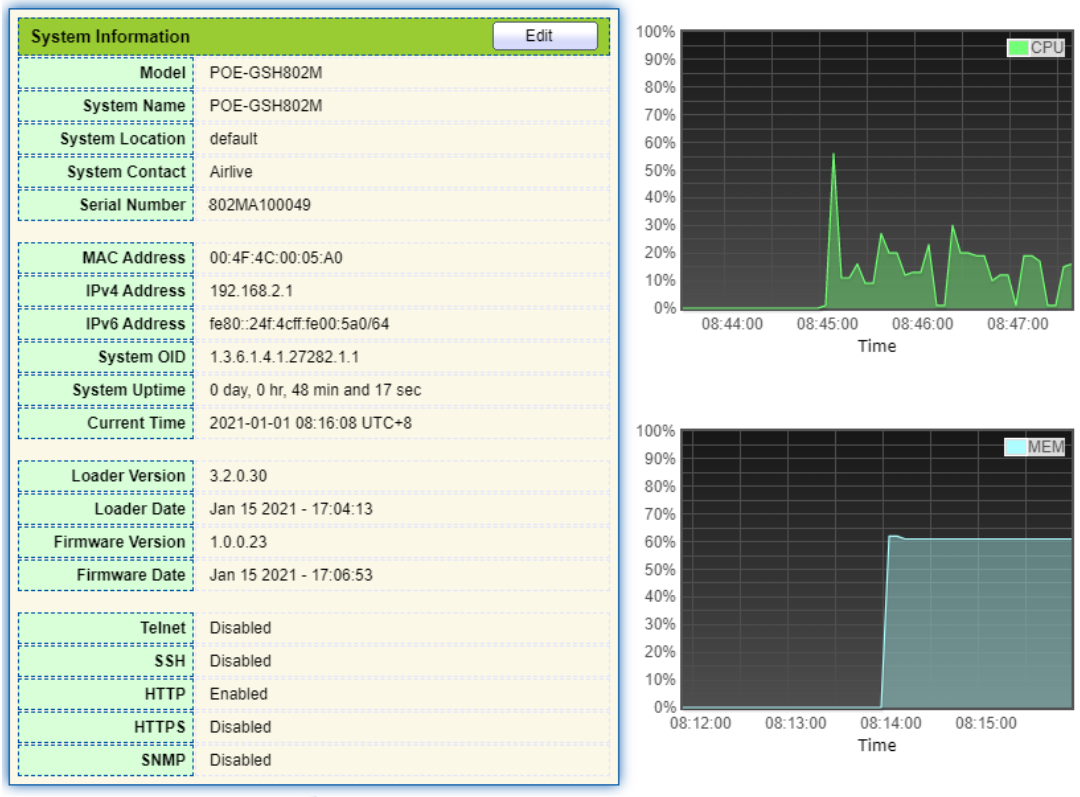
3.1 Información del Sistema

Para el switch que estás conectado, el panel de gestión de red despliega los puertos e información del producto, incluyendo, como, por ejemplo: número de puertos, Estado de los puertos, Información del producto, estados del dispositivo, funciones activas/ desactivas, etc.

Instrucciones:

1. Haga Click en “Status > System Information” en el menú de navegación, como se indica:





Descripción:

Coloca el apuntador del ratón sobre un Puerto para verificar el número, tipo, velocidad y estado de dicho puerto. Puedes editar el nombre “System Name”,

ubicación “Location” y contacto “Contact” en la información del producto. Presiona “Apply” y Finish, para guardar los cambios.

3.2 Estadística

Muestra el detallado flujo estadístico en un Puerto y la información que puede ser refrescado o borrado manualmente por el usuario.

1. Haga Click en “Status > Port > Statistics” en la barra de navegación. Como se indica:

Descripción:

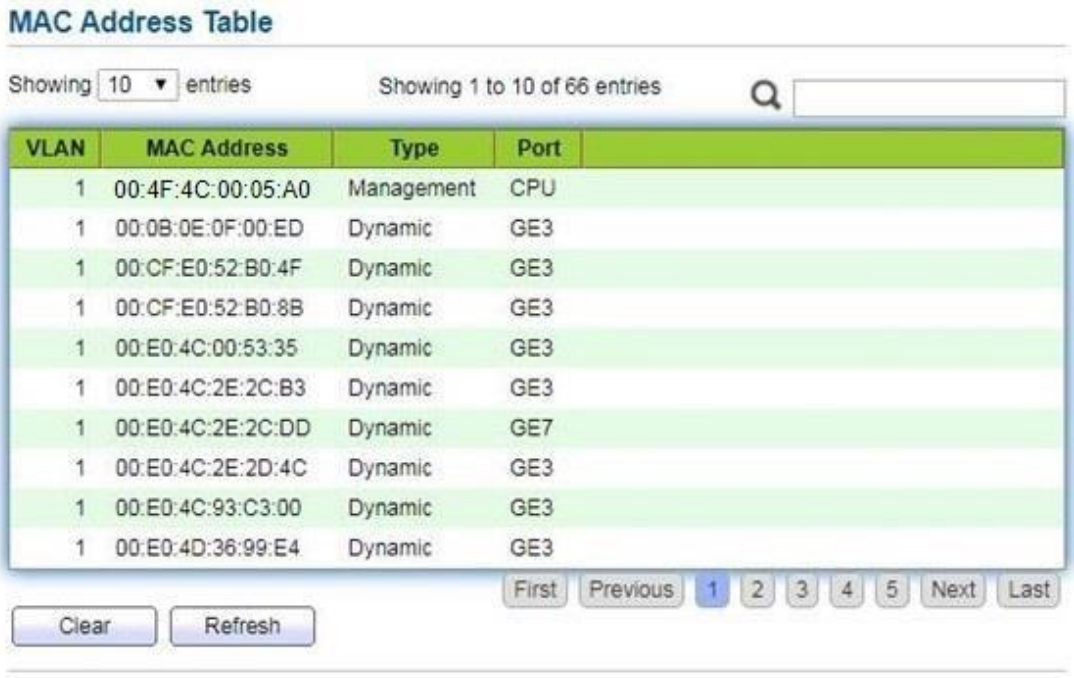
Haga click en “Clear” para borrar la estadística del Puerto actual y refrescarla página.

3.3 Tabla de direcciones MAC

Visualiza la tabla direcciones MAC.

Instrucciones:

1. Haga Click en “Status > MAC Address Table” del menú de navegación, como se indica:



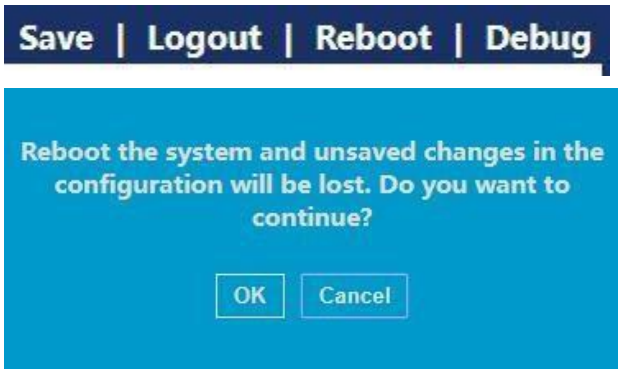
Los datos de la Interfaz se muestran a continuación.

Query Items	Descripción
MAC	Dirección MAC de destino
VLAN	El ID de VLAN al que pertenece la dirección MAC
Port	Mensaje de egreso correspondiente a la dirección MAC
Type	El campo **Dynamic** de la dirección MAC, refiere a la entrada que se desvanecerá de acuerdo con el parámetro de envejecimiento configurado. Los switches pueden agregar entradas basado en el mecanismo de aprendizaje de direcciones MAC o creación manual.
	El campo **Static** de dirección MAC, refiere a la tabla específica configurada manualmente y no envejecerá
	El campo **Management** de la dirección MAC, refiere a la dirección del puerto de gestión.

3.4 Volver a iniciar

1. Haga Click en “Reboot” en la opción superior derecha de la pantalla, como se indica.

   Configuraciones sin guardar se perderán. Presione OK, si desea continuar.



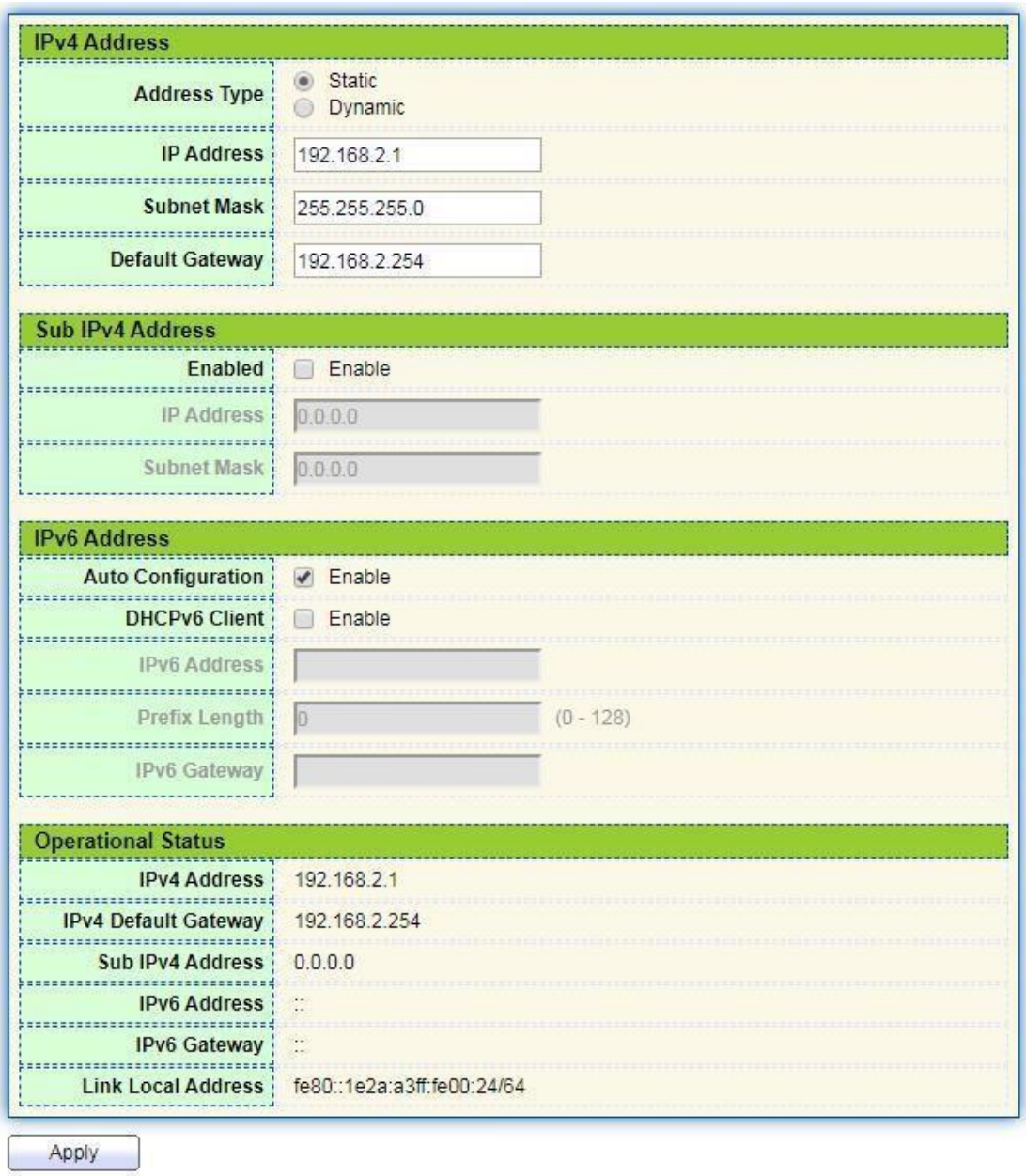
4 Parámetros de Red

4.1 Dirección IP

Cambia la dirección IP de administración en la interfaz web.

Instrucciones:

1. Haga click en “Network > IP Address” del menú de navegación para descubrir la dirección IPv4 192.168.2.1/24 por defecto, como se indica:
2. Repita este paso, selecciona tipo de dirección estática “Static”, introduzca la dirección IPv4 192.168.2.1, la máscara de subred 255.255.255.0, y la dirección de gestión de red 192.168.2.254. Presiona “Apply” para guardar los cambios y finalizar.

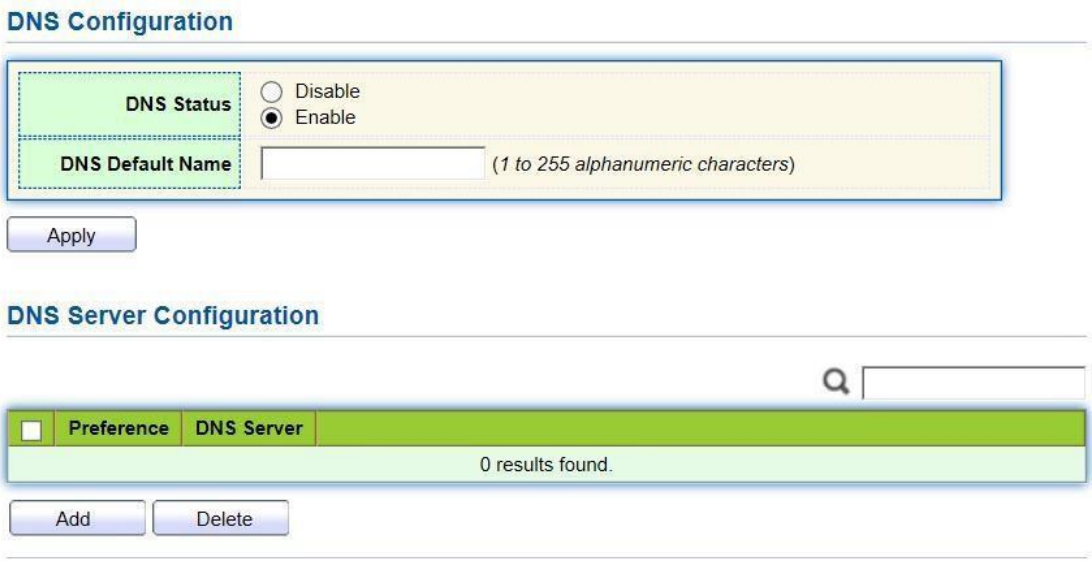


4.2 DNS

DNS son las siglas de Sistema de Dominio de Nombres (Domain Name System) para asignar nombres a los computadores y servicios de redes desde unidades hasta un dominio de jerarquías. Un dominio de nombre consiste en una cadena de nombres o abreviaciones separadas por puntos, correspondiendo con una dirección IP única. El DNS representa el servidor en Internet que resuelve los nombres de dominio. En Internet y otras redes TCP/IP, el nombre DNS recupera los nombres de computadores y servicios por medio de nombres fáciles de usar. Siendo uno de los servicios principales de internet, el DNS es una base de datos distribuida que vincula los nombres de dominio con sus correspondientes direcciones IP únicas.

Instrucciones:

1. Haga click en “Network > DNS” en el menú de navegación, como se indica.

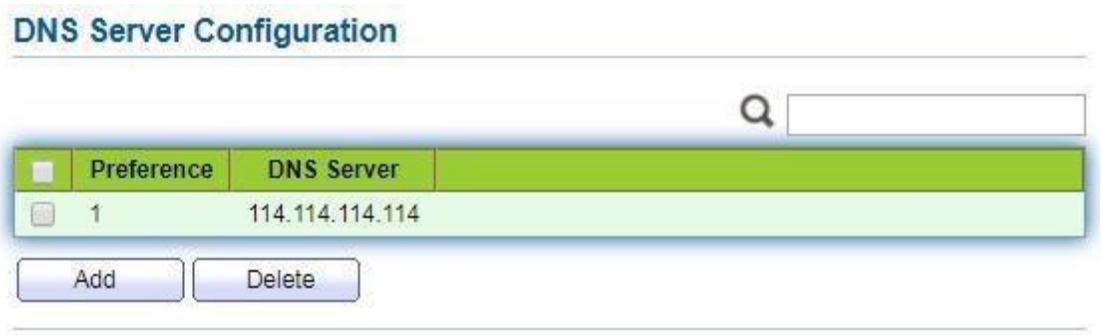


Los campos de la Interfaz son como se muestra a continuación.

Configuration Items	Descripción
DNS State	Cambiar DNS
DNS Default Name	Introduzca el nombre por defecto asignado

2. Presione “Add” para configurar el servidor DNS.

3. Presiona “Apply” para guardar los cambios y terminar, como se indica.



4.3 Hora y Fecha del Sistema

Se utiliza principalmente para configurar el día y hora del equipo, y se selecciona la fuente de la hora, el horario de verano (si aplica), etc.

Instrucciones

1. Haga click en “Network > System Time” del menú de navegación. Como se indica.

Los campos de la interfaz son como se muestran a continuación.

Configuration Items	Descripción
Time Source	Seleccione la fuente de la hora: SNTP, PC o manual
Time Zone	Configure la franja horaria
Address Type	Nombre de Host o dirección IPv4 (con SNTP como Fuente)
Server Address	Dirección de servidor (con SNTP como fuente)
Server Port No.	Número de Puerto del servidor (con SNTP como fuente)
Date	Introduzca la fecha Date: DD/MM/YYYY (con la fuente de hora en modo manual)
Time	Introduzca la hora: SS/MM/HH (con la Fuente de hora en modo manual)
Type	El horario de Verano puede ser: Ninguno (None), cíclico (cyclic), no cíclico (non-cyclic), Estados Unidos o Europa.
Reimbursed Time	Tiempo Reembolsado del horario de verano
Cyclic Mode	Configure el modo cíclico del horario de verano
Non-cyclic Mode	Configure el modo no cíclico del horario de verano

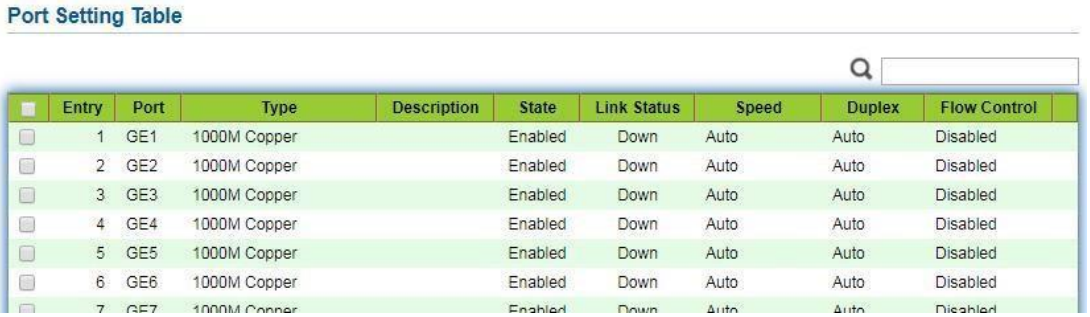
5 Puerto

5.1 Configuración de Puerto

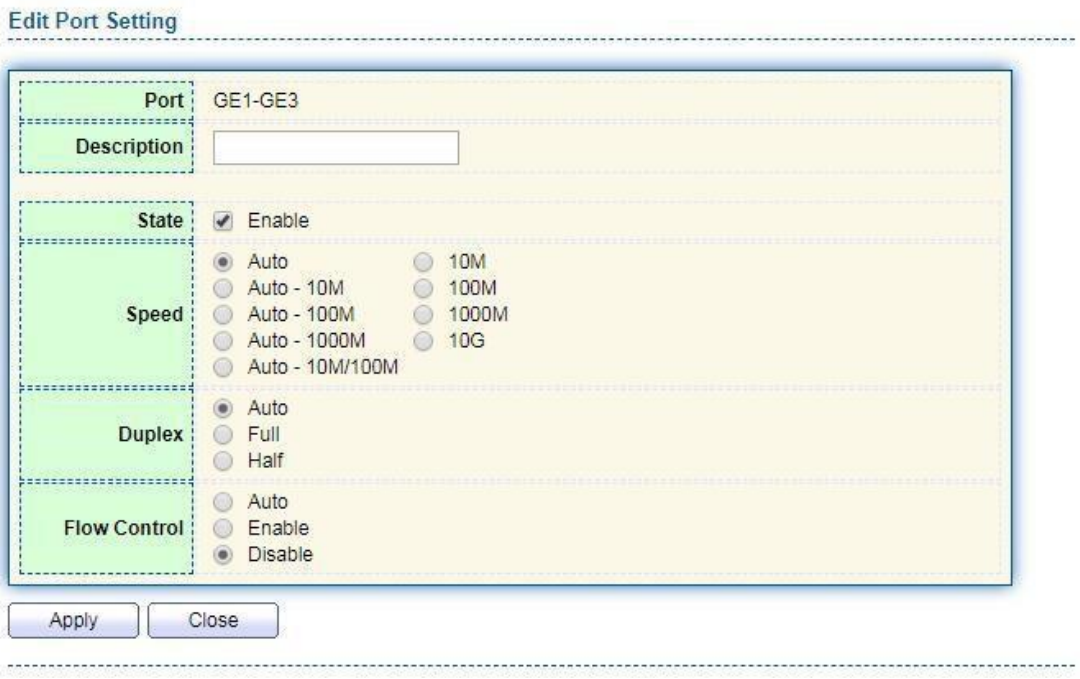
Las Interfaces deben ser identificadas de manera que los usuarios puedan inquirir y configurar las interfaces Ethernet cuando se desee.

Instrucciones:

1. Haga click en “Port > Port Setting” del menú de navegación:



2. Seleccione el Puerto a ser configurado, y presione “Edit”, como se indica:



Los campos de la Interfaz se muestran a continuación.

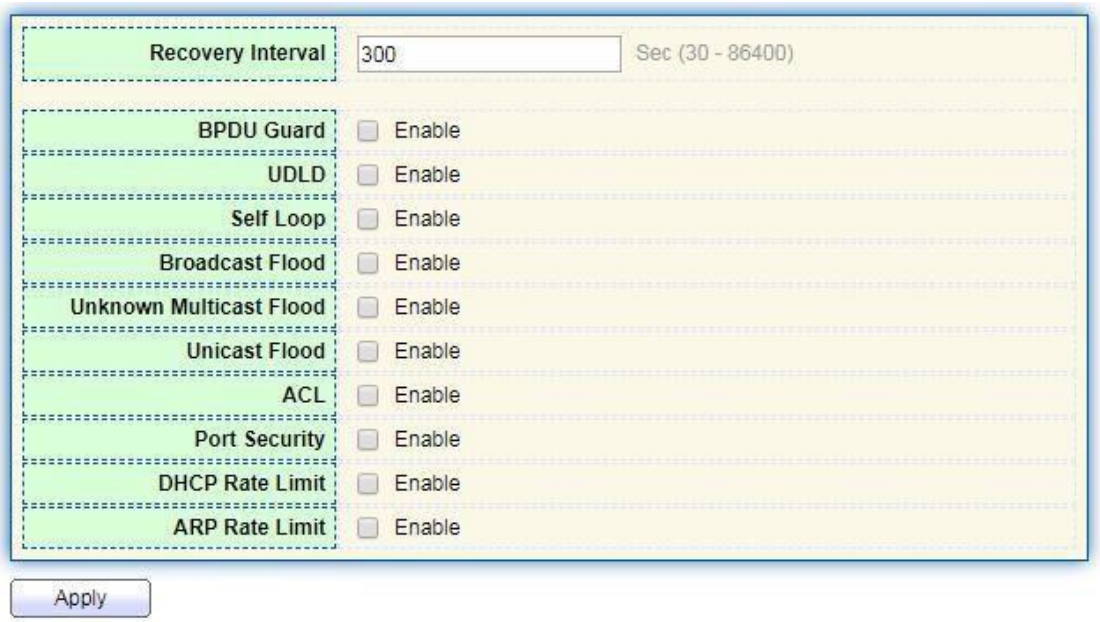
Configuration Items	Descripción
Port	Lista de Puertos
Description	Alias del Puerto
State	Habilitar o deshabilitar el puerto
Speed	Es configurable como auto negociación mandatoria para 10 Mb, 100 Mb and 1,000 Mb. Opciones de velocidades de 10Mbit/s, 100 Mbit/s y 1,000 Mbit/s están disponibles para las interfaces físicas Ethernet, según se requiera.
Duplex	Configurable auto negociación con opciones full o half dúplex.
Flow Control	Luego de ser habilitado tanto en los equipos de la red local como en la red opuesta remota, el local notificará al remoto para que pare la transmisión de mensajes cuando exista congestión de la red. El equipo remote ejecutará la instrucción de control de flujo de forma transitoria para asegurar que no exista pérdida de mensajes.
	Disable: Deshabilita la recepción/transmisión de la trama Pausa
	Enable: Habilita la recepción/transmisión de la trama de Pausa
	Auto negotiation: Negocia la trama de Pausa con la red remota automáticamente.

5.2 Error Deshabilitado

En general, si el software del switch detecta errores en el puerto, éste será detenido inmediatamente. En otras palabras, cuando el Sistema operativo del switch detecta algún evento de errores en el puerto del switch, éste automáticamente detiene ese puerto.

Instrucciones:

1. Haga click en “Port > Error Disabled” del menú de navegación para habilitar o deshabilitar la configuración como se indica a continuación:



5.3 Agregación de Enlace

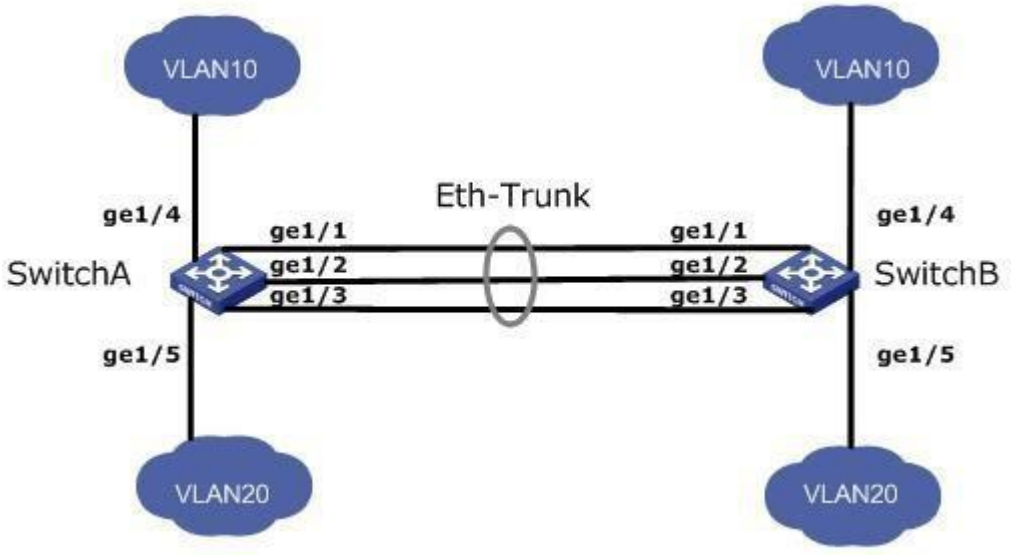
La agregación de enlace amplía el ancho de banda y la confiabilidad juntando un grupo de interfaces físicas en una única interfaz lógica.

El grupo de agregación “LAG” (Link Aggregation Group) es un enlace lógico compuesto por múltiples enlaces Ethernet llamado troncal ethernet (Eth-Trunk).

La incesante expansión de las redes aumenta la demanda de mayor ancho de banda y confiabilidad. Usualmente, se requiere una interfaz de red de alta velocidad y/o reemplazar el equipo equivalente para optimar el ancho de banda, lo cual puede ser costoso y complejo. Con agregación de enlaces puede seguir usando el mismo tipo.

La tecnología de Agregación de Enlaces junta múltiples interfaces físicas en una única interfaz lógica sin requerir actualización del hardware. Introduce un excelente mecanismo de respaldo de enlace que no solo mejora la confiabilidad, sino también comparte el flujo de carga sobre diferentes enlaces físicos.

Como se muestra a continuación, el Switch A está conectado con el Switch B por medio de tres enlaces Ethernet, los cuales son empaquetados como si fueran un solo enlace troncal (Eth-Trunk) lógico. Su ancho de banda es la sumatoria los tres enlaces, ampliando así el ancho de banda. Estos tres enlaces se respaldan mutuamente entre sí para ser más confiables.



La Agregación de Enlace presenta las siguientes justificaciones:

- Insuficiente ancho de banda de dos switches conectados entre sí.
- Insuficiente confiabilidad de dos switches conectados con un solo enlace.

La Agregación de Enlace puede ser de Modo Manual y Modo LACP, de acuerdo con el estado del protocolo de agregación de enlace (LINK Aggregation Control Protocol-LACP).

En el primer modo, el establecimiento de la troncal (Eth-Trunk), los miembros de la interfaz deben ser agregados manualmente, sin LACP. También se le llama Modo de carga compartida (Load-sharing Mode) porque todos los enlaces hacen reenvío de datos y compartición de carga. En caso que algún enlace falle, el modo LAG promedia el tráfico con todas las remanentes. Este modo es preferido cuando los dos dispositivos conectados requieren un enlace de mayor ancho de banda, pero no soportan LACP.

5.3.1 Grupoo

Instrucciones para agregar un enlace de agregación estático:

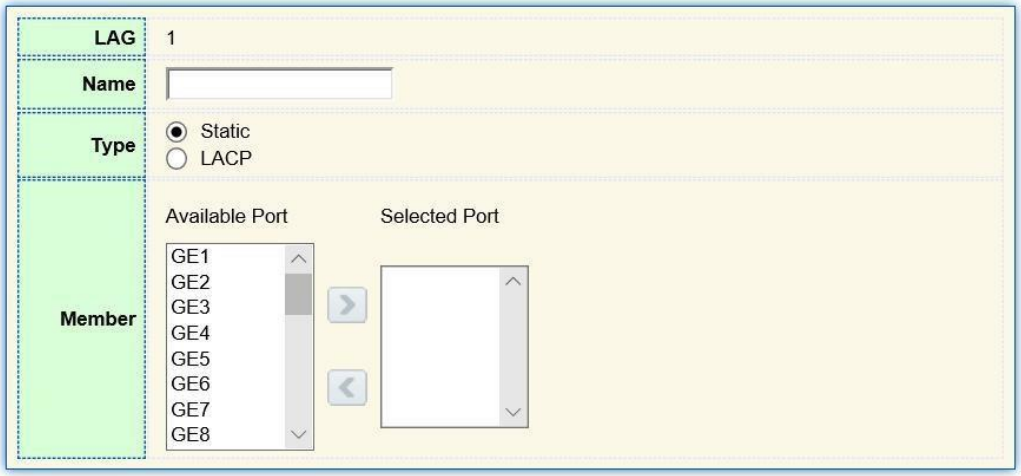
1. Haga click en “Port > Link Aggregation > Group”, seleccione una opción de algoritmo de balanceo. Presiona “Apply” para guardar los cambios y terminar, como se indica a continuación:

Link Aggregation Table

	LAG	Name	Type	Link Status	Active Member	Inactive Member
○	LAG 1		---	---		
○	LAG 2		---	---		
○	LAG 3		---	---		
○	LAG 4		---	---		
○	LAG 5		---	---		
○	LAG 6		---	---		
○	LAG 7		---	---		
○	LAG 8		---	---		

2. Selecciona uno de los ocho grupos LAG disponibles, presiona “Edit” para editar la configuración, como se muestra en la página a continuación:

Edit Link Aggregation Group



Los datos de la interfaz son como se muestra a continuación.

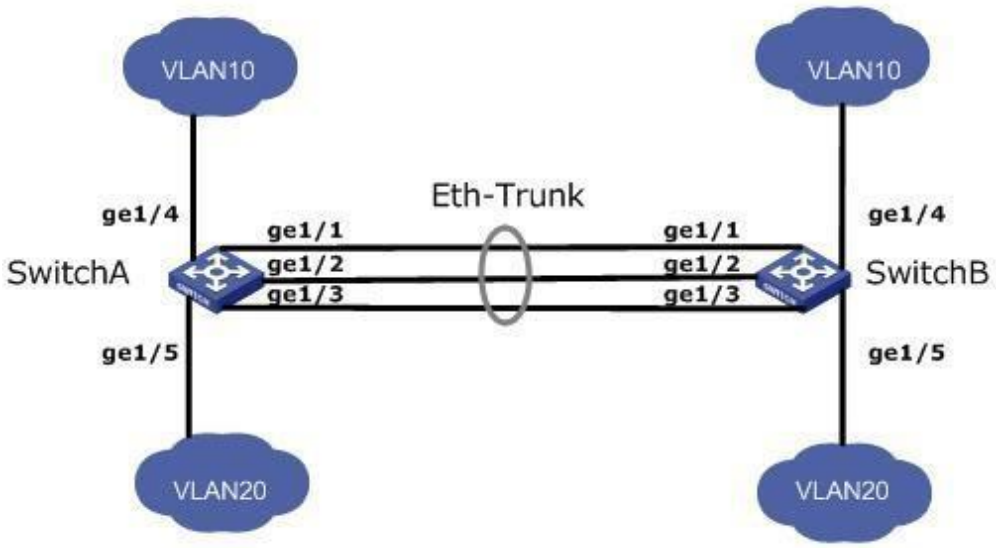
Campos de Configuración	Descripción
DNS State	Hay ocho grupos LAG numerados del 1 al 8.
DNS Default Name	Descripción del grupo LAG, modificable a conveniencia.
Campos de Configuración	Selecciona el modo manual o el modo LACP.
DNS State	Hasta ocho puertos miembros están disponibles en el grupo LAG.

Ilustración:

Como se muestra a continuación, el Switch A y Switch B conectan la VLAN 10 y 20 vía Ethernet respectivamente, con alto nivel de tráfico entre ellos.

Se espera que ambos switches A y B provean una calidad superior de ancho de banda para la comunicación de la VLAN. Entre tanto, se espera que exista una comunicación redundante para la transmisión confiable entre los enlaces.

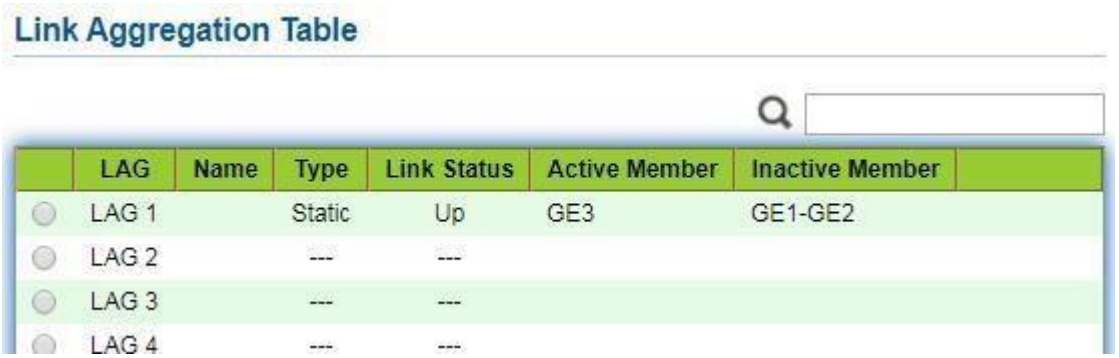
Diagrama de red con grupo LAG in modo manual:



Instrucciones:

1. Crea la interfaz troncal (ETH trunk) en el Switch A y agrega una interfaz como miembro para incrementar el ancho de banda. La configuración del Switch B es similar a la del Switch A.

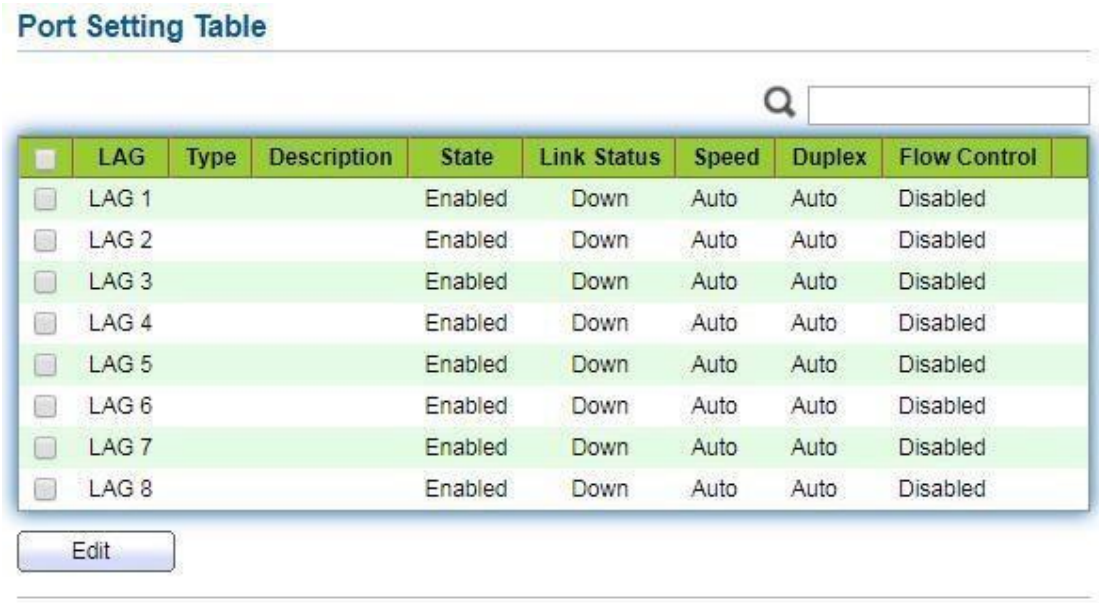
Haga click en “Port > Link Aggregation > Group”, selecciona “LAG 1” y puertos GE1, 2 y 3, y luego mueva los puertos seleccionados a la derecha. Presiona “Apply” y termina, como se muestra a continuación.



5.3.2 Configuración del puerto

Configuración de atributos del puerto miembro del grupo de agregación

1. Haga clic en “Port >Link Aggregation > Port Setting" para ingresar a la interfaz de configuración de atributos del puerto miembro del grupo de agregación de la siguiente manera:



5.3.3 LACP

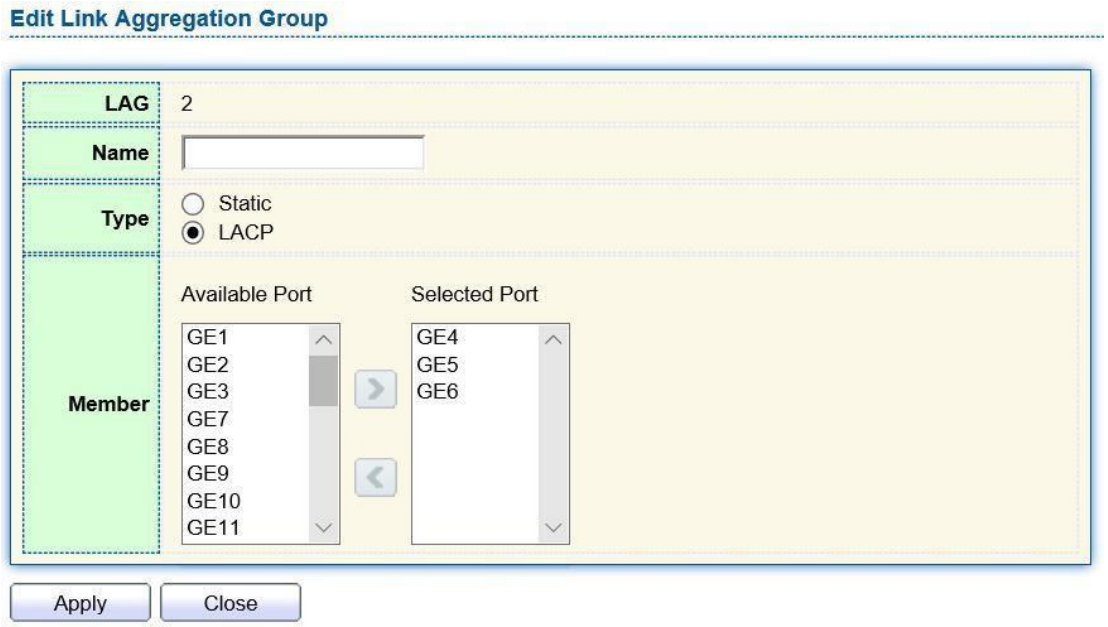
LACP (Link Aggregation Control Protocol), basado en el estándar IEEE 802.3ad, agrega y desagrega dinámicamente enlaces. Intercambia información con el dispositivo de la red del lado opuesto a través de la unidad de data LACPDU (Link Aggregation Control Protocol Data Unit).

Cuando un Puerto utiliza LACP, informa al dispositivo de la red remota la proridad del sistema, la MAC del sistema, la prioridad de puerto y su número, así como una llave de operación por medio de la unidad de data LACPDU. El dispositivo remoto compara esta información con la que está guardada para otros puertos luego de recibirla, llegando así a un acuerdo en cuanto a la participación de los puertos o rechazando una agregación dinámica.

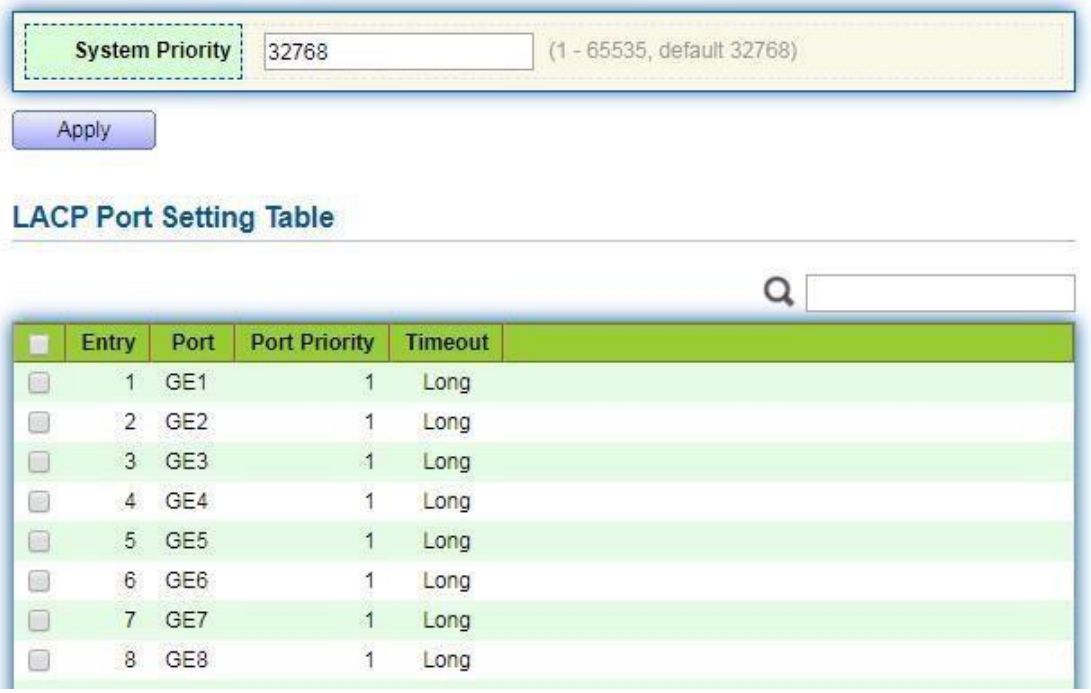
La agregación dinámica LACP es creada o borrada automáticamente por el sistema, es decir, los puertos internos pueden ser agregados o eliminados por sí solos. Solo los puertos conectados a un mismo dispositivo con la misma velocidad, dúplex, y configuración básica pueden ser agregados.

Instrucciones para adicionar una agregación de enlace dinámico:

1. Haga click en “Port > Link Aggregation > Group” en el menu de navegación, selecciona el ID LAG y el modo LACP. Luego edita con “Edit” como se indica a continuación:



2. Haga click en “Port >Link Aggregation > LACP” en el menú de navegación para configurar los atributos LACP tales como la prioridad del sistema, Prioridad del Puerto y el método de expiración, como se indica a continuación:



Los campos de la Interfaz se muestran a continuación:

Campos Configurables	Descripción
System Priority	El mecanismo LACP determina modo activo y pasivo entre dos dispositivos en base al estándar de prioridad.
Port	Lista de Puertos
Port Priority	El mecanismo LACP determina el modo dinámico de miembro LAG dependiendo de la prioridad del puerto en un esquema jerárquico
Timeout	Determina la frecuencia de transmisión de los mensajes LACP.

Descripción:

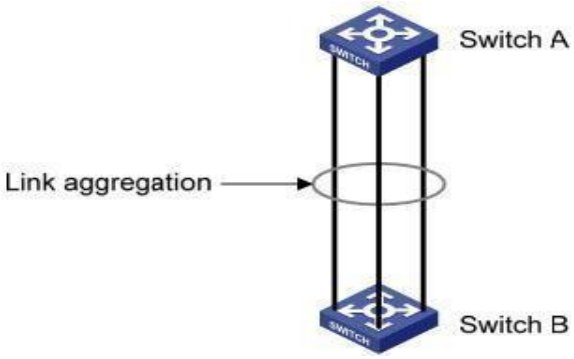
Asegúrese por favor que ningún miembro de la interfaz está accediendo a la troncal Eth-Trunk antes de cambiar el patrón de operación, de lo contario ocurre falla. El patron de trabajo de los dispositivos de una red local, debe ser consistente con el de los dispositivos de la red del lado opuesto.

Ilustración

En la figura siguiente el Switch Ethernet A agrega 3 puertos de desde GE1 a GE3 al Switch B, con el objeto de que cada puerto miembro comparta la carga.

Las siguientes configuraciones se ejemplifican mediante agregación dinámica

.



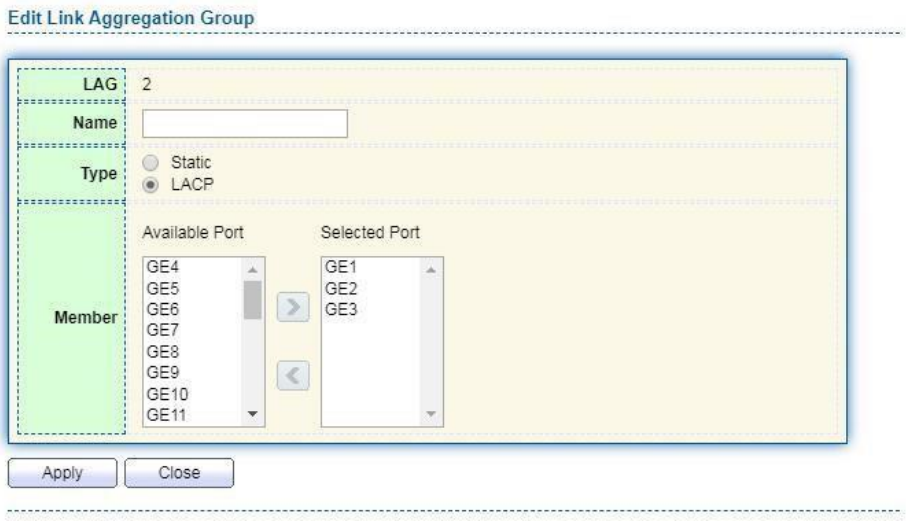
.

Descripción:

La siguiente es la configuración para el Switch A solamente, el cual debe permanecer igual respecto a la del Switch B para la agregación de puertos.

Instrucciones:

1. Haga click en “Port > Link Aggregation > Group” del menu de navegación, Presione “Edit” para editar LAG 2, luego seleccione GE1-GE3 en el modo LACP. Persona “Apply” y terminar como se indica:

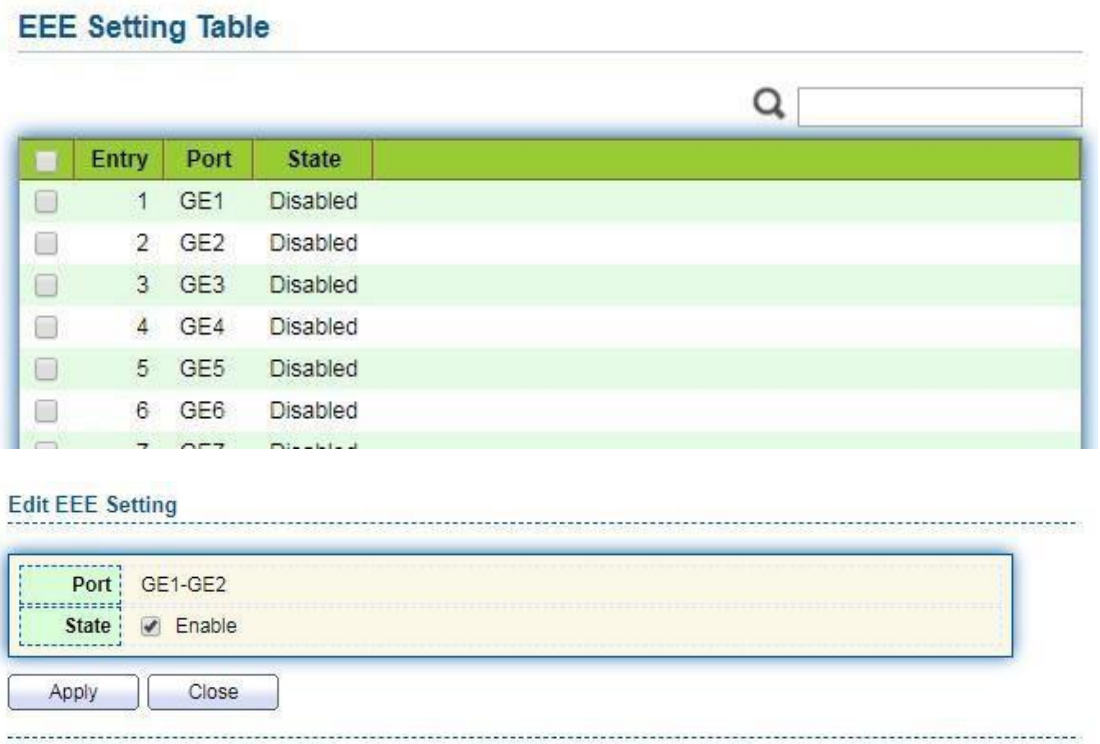


5.4 Eee

La energía del puerto se apagará en caso que no haya o haya

poco flujo:

1. Haga click en “Port > EEE” del menú de navegación, seleccione el puerto y presione “Edit” para cargar la configuración de la interfaz, como se indica:



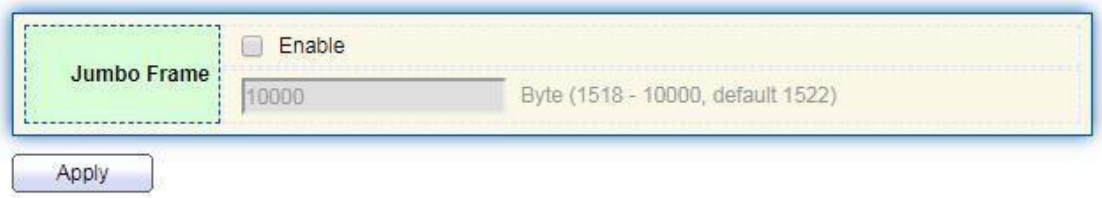
2. Fije el estado del Puerto como habilitado (enable) y presione “Apply” para completar la configuración, como se muestra a continuación:

5.5 Trama Jumbo

Fija la MTU (Unidad Máxima Transmisión) del puerto

Instrucciones:

1. Haga click en “Port > Jumbo Frame” en el menú de navegación, para configurar la trama Jumbo de la interfaz, como se indica a continuación:



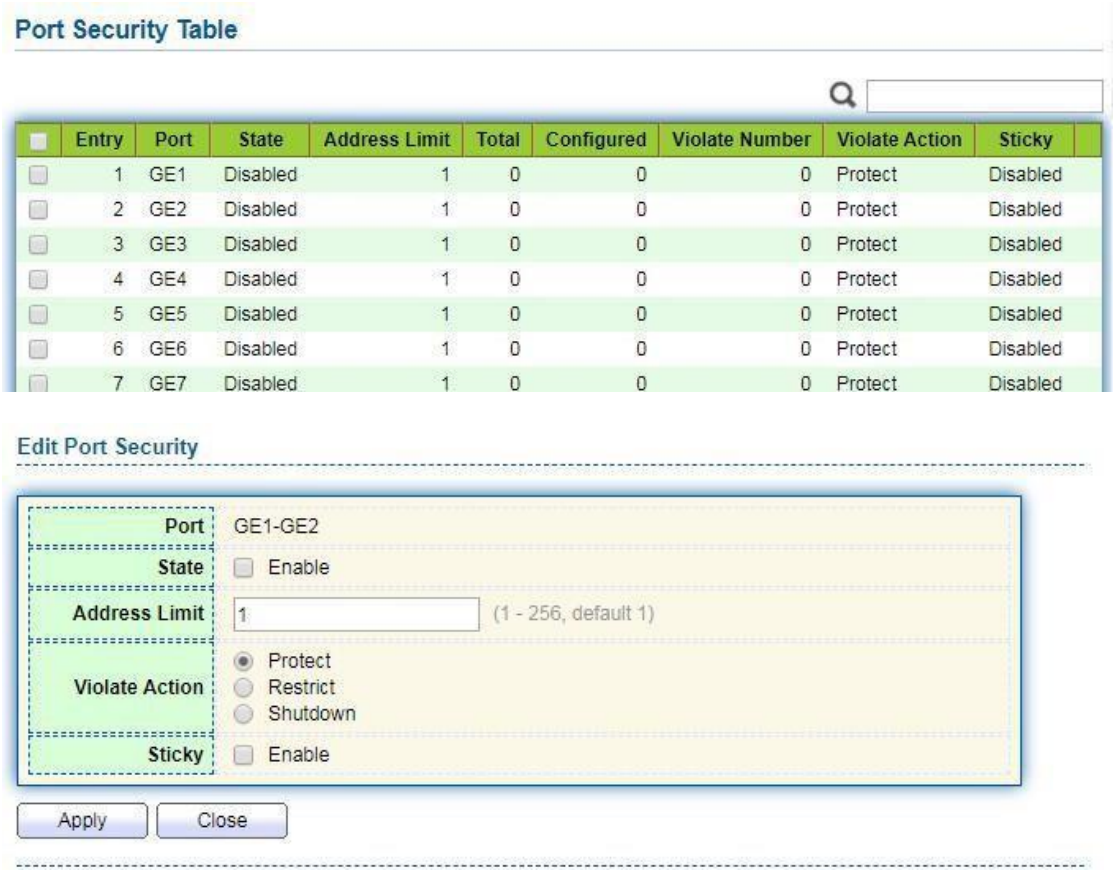
5.6 Seguridad del Port

La funcionalidad de seguridad del Puerto registra la dirección Ethernet MAC conectada al Puerto del switch por medio de la tabla de direcciones MAC, y solo una dirección MAC puede comunicarse a través de este puerto. Cuando los paquetes enviados por otras direcciones MAC pasan por este puerto, las funciones de seguridad del puerto lo impiden. El uso de funciones de seguridad de puertos puede evitar que dispositivos no autorizados accedan a la red y mejorar la seguridad. Además, las funciones de seguridad del puerto también se pueden usar para evitar que la tabla de direcciones MAC se llene debido a la inundación de direcciones MAC.

Instrucciones:

1. Haga click en “Port > Port Security” en el menú de navegación, introduzca la configuración de seguridad del puerto, como se muestra a continuación:

2. Haga click en “Port > Port Security” en el menú de navegación, seleccione el puerto y presione “Edit” para introducir el nivel de configuración de la interfaz del puerto, como se indica:

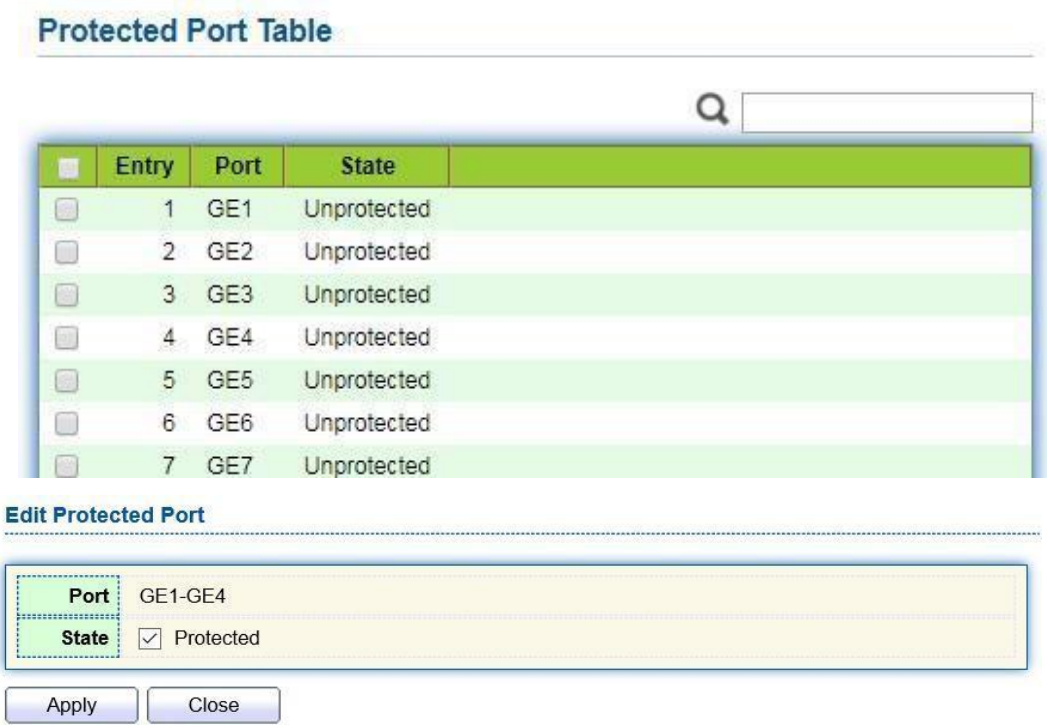


5.7 Puerto protegido

Los mensajes de difusión, multidifusión, etc. inundarán cada puerto, aunque el flujo a veces no necesita comunicación mutua. Bajo esta circunstancia, el aislamiento de puertos puede separar los mensajes entre dos puertos.

Instrucciones:

1. Haga click en “Port > Protected Port” en el menú de navegación, verifique el Puerto, o los puertos, a ser aislado, presione “Edit” para cambiar esta función, como se indica:



Instrucciones para acometer el aislamiento de puerto:

1. Haga click en “Port > Protected Port” en el menú de navegación, verifique y presione “Edit” para editar el puerto GE1, 2 and 3 a ser aislado. Presione “Apply” y Terminar, como se indica:

2. GE1, 2 y 3 fallan en comunicarse mutuamente porque son puertos no aislados.

5.8 Control de Tormentas

Las tormentas generadas a través de mensajes de difusión, multidifusión y unidifusión desconocidos se evitan de la siguiente manera. Estos mensajes se suprimirán según las tasas de paquetes, respectivamente. La tasa promedio de los mensajes recibidos por las interfaces de monitoreo se comparará con el umbral máximo configurado durante un intervalo de inspección. La supervisión de tormentas configurada se realizará en esta interfaz si la tasa promedio excede el umbral máximo.

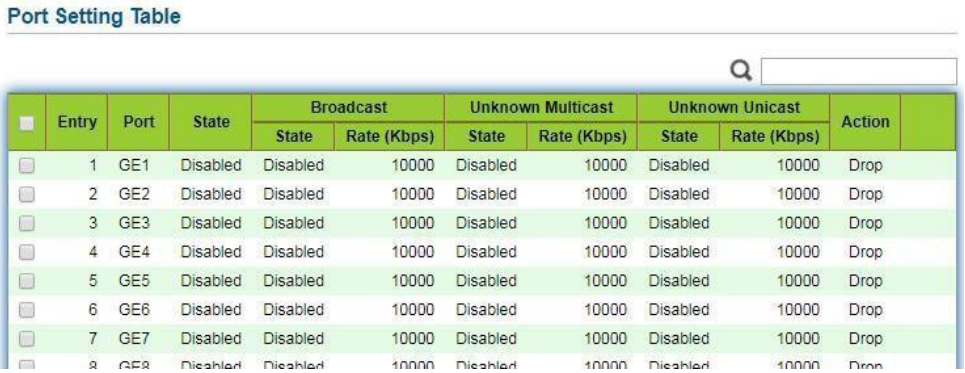
Cuando una interfaz Ethernet L2 recibe mensajes de difusión, multidifusión o unidifusión desconocidos, el dispositivo los reenviará a otras interfaces L2 en una misma VLAN (red de área local virtual) si la interfaz de salida no se puede reconocer de acuerdo con las direcciones MAC de destino. Como resultado, es posible que se produzca una tormenta de transmisión que degrade el rendimiento operativo del dispositivo.

Se pueden controlar tres tipos de flujo de mensajes mediante características de supervisión de tormentas para mantenerse alejado de las tormentas de difusión.

Instrucciones:

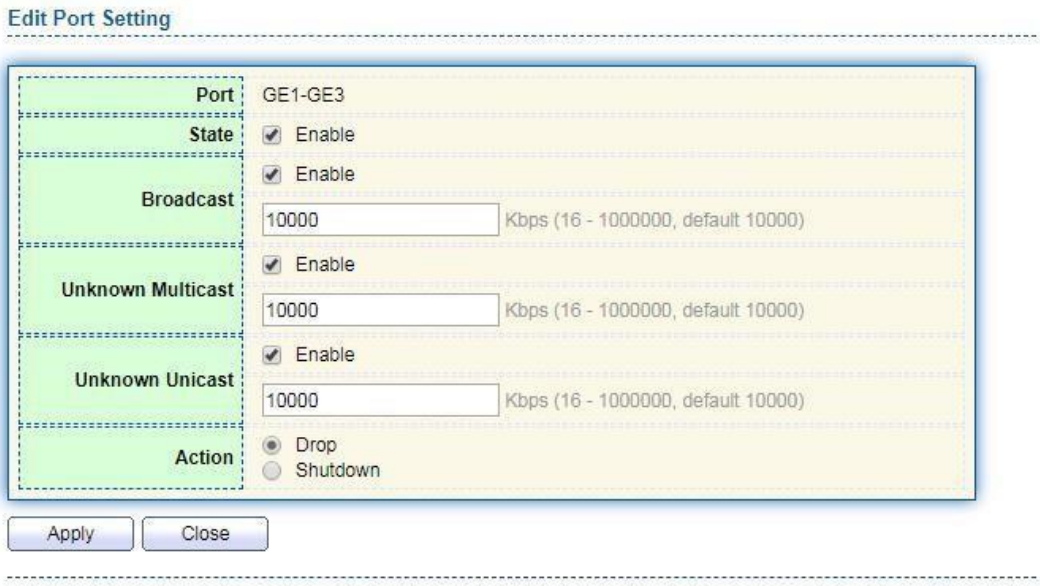
1. Haga click en “Port > Storm Control” en el menú de navegación para configurar los atributos relacionados con la política de tormentas tales como el modo, como se indica:

2. Seleccione el puerto adecuado y "edítelo" configurando las tasas de supervisión de tormentas de difusión, multidifusión desconocida y unidifusión en cada puerto.



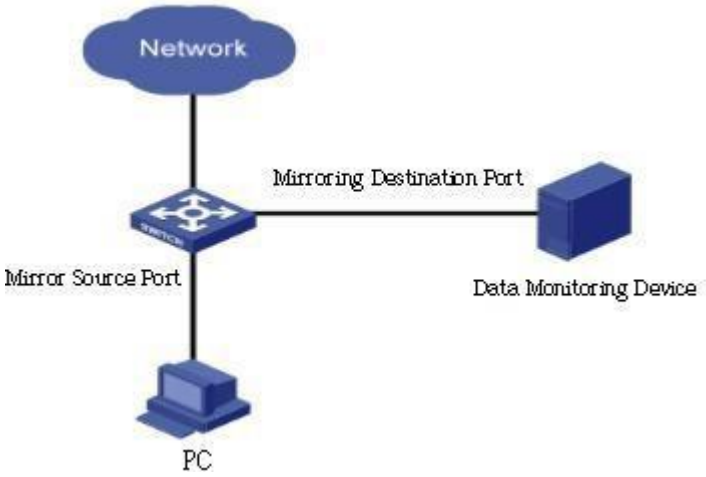
Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

3. Habilita parámetros como el estado del puerto, Difusión y Multidifusión:



5.9 Duplicación de Puertos

Port Mirroring permite copiar el mensaje de un puerto de switch específico al puerto de destino. El puerto copiado es el puerto de origen y el puerto de copia es el puerto de destino. El puerto de destino accede a los dispositivos de inspección de datos para que los usuarios puedan analizar los mensajes recibidos para monitorear la red y solucionar problemas de la siguiente manera:

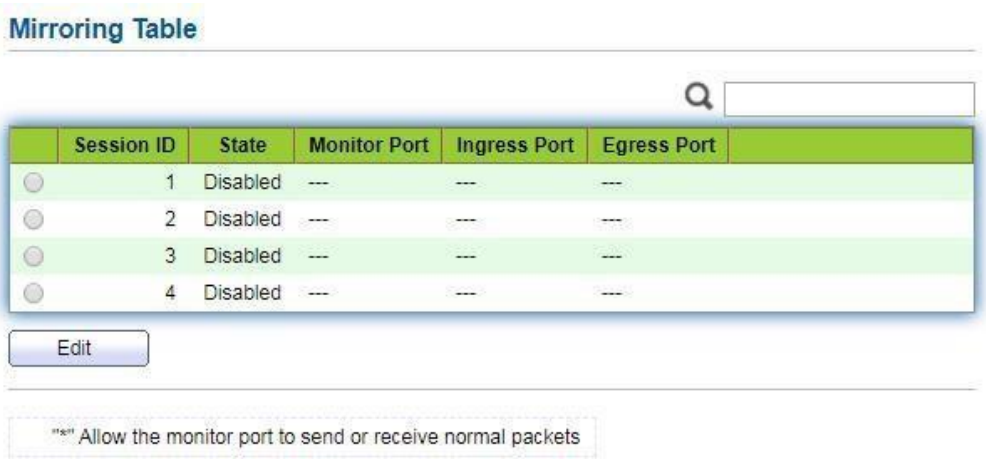


Instancia

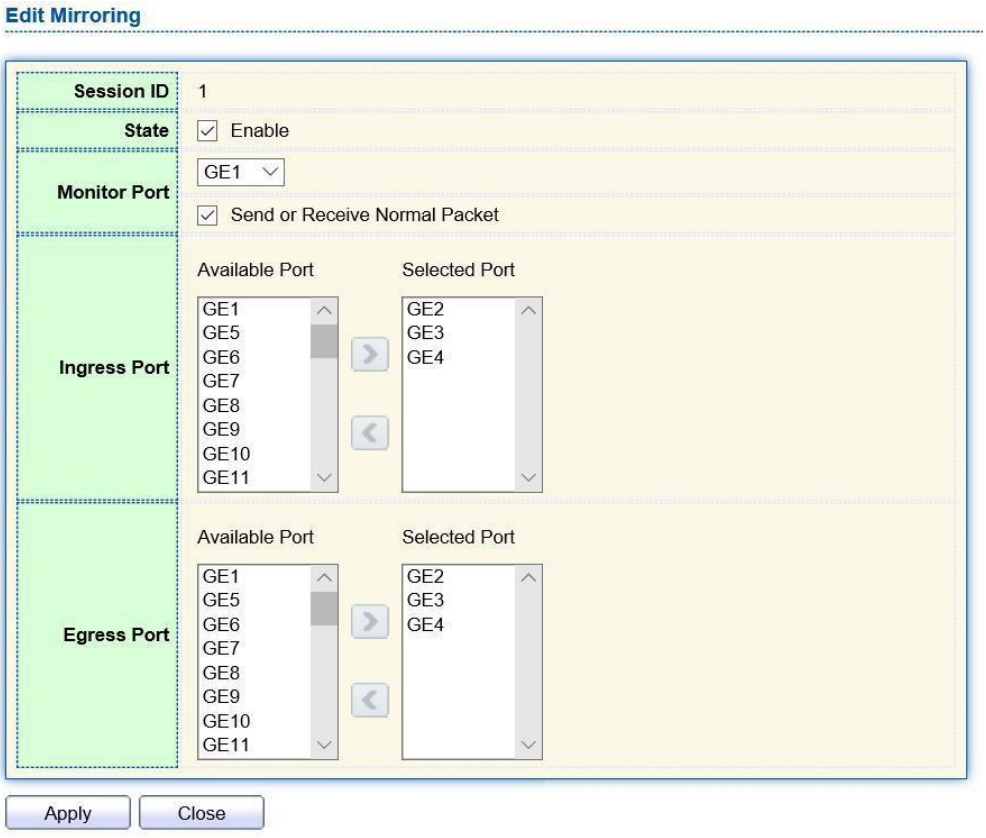
Switch de acceso PC1 y PC2 A a través de la interfaz GE1 y GE2 respectivamente. Los usuarios tienen la intención de monitorear los mensajes transmitidos de PC2 a PC1.

Instrucciones:

1. Haga click en “Port > Mirroring” en el menú de navegación. Cuatro juegos de reglas de duplicación pueden ser configuradas, como se indica:



2. Seleccione una sesión y "edítela" en la interfaz de configuración del grupo de duplicación:



Los campos de la Interfaz son como se muestran a continuación.

Elementos de configuración	Descripción
ID de sesión	El switch tiene 4 IDs de sesiones por defecto.
Estado	Habilita el Grupo de Duplicación.
Puerto de monitor	Solo se puede seleccionar un puerto físico ordinario, sin incluir el puerto de agregación de enlaces y el puerto de origen.
Puerto de entrada	Cualquier mensaje recibido se reflejará en el puerto de destino
Puerto de salida	Cualquier mensaje transmitido se reflejará en el puerto de destino

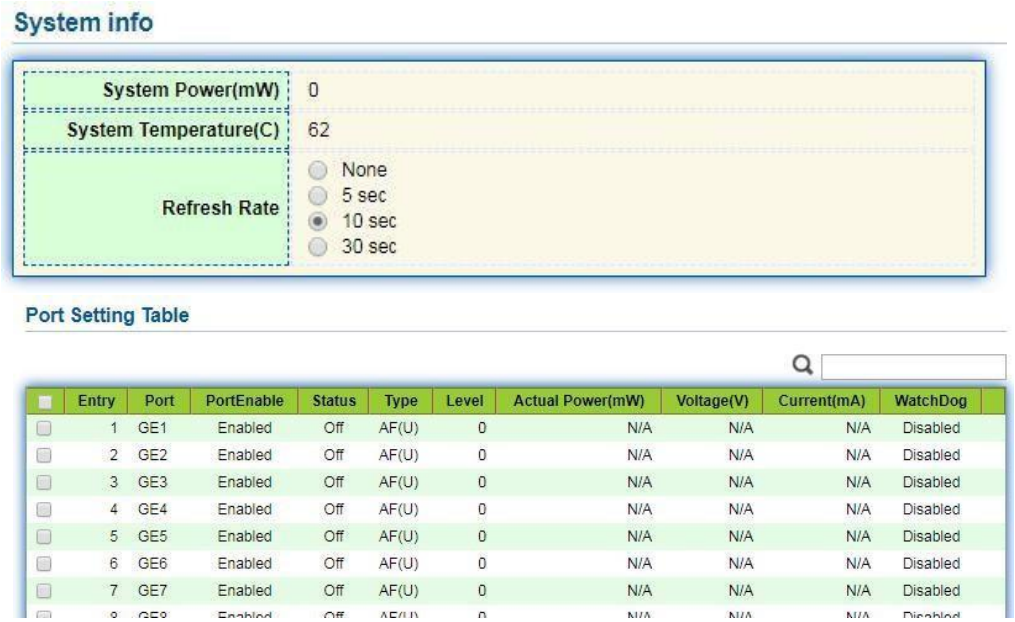
6 Configuración POE

PoE (Power over Ethernet) transmite la señal de datos para los terminales basados en IP (por ejemplo, teléfono IP, WAP y cámara IP) y suministra corriente continua a los dispositivos, sin cambiar el estado del cableado de la red Cat-5 existente. Garantiza un cableado estructurado seguro y un funcionamiento normal de la red para minimizar el costo.

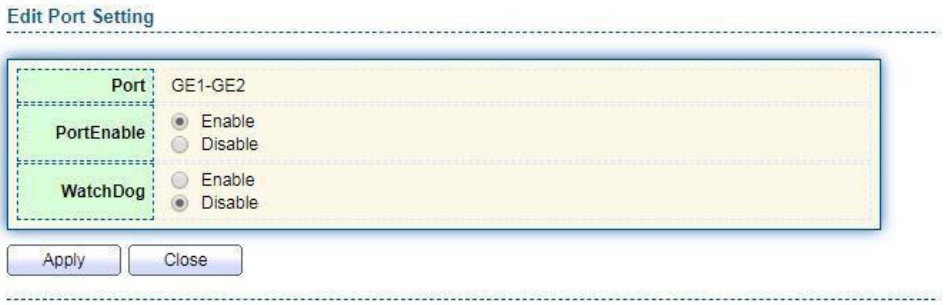
6.1 Configuración PoE del Puerto

Instrucciones:

1. Haga click en “POE Setting > POE Port Setting” en el menú de navegación:



2. Selecciona los puertos a ser configurados, y presiona “Edit” como se indica:



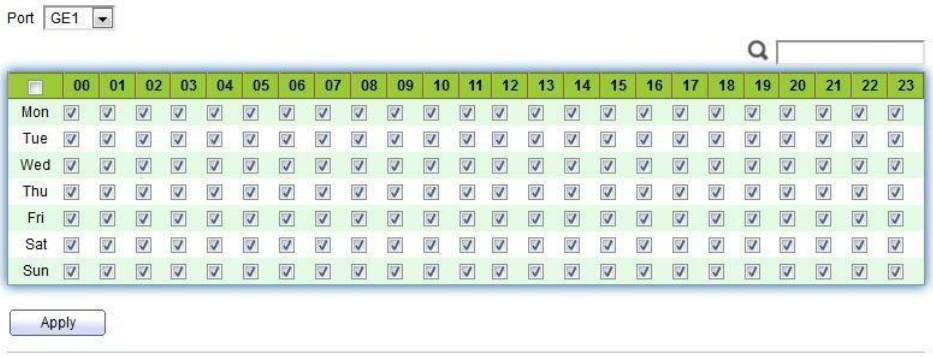
Los campos de la interfaz son como a continuación.

Campos Configurables	Descripción
PortEnable	Habilitar / Desabilitar la energía Poe del puerto
WatchDog	Habilitar/deshabilitar la función de vigilancia del puerto Poe; Después de habilitar la función de vigilancia, cuando el puerto POE se alimenta continuamente pero no hay tráfico, se activará la vigilancia POE. Después de 2 minutos de detección, la fuente de alimentación se detendrá y luego se encenderá. El ciclo de detección total es 5 veces.

6.2 Configuración del Temporizador del Puerto PoE

Instrucciones:

1.Haga click en “POE Setting > POE Port Timer Setting”, seleccione el tiempo de suministro de energía del programa Poe. “Aplicar” y Terminar, como a continuación:

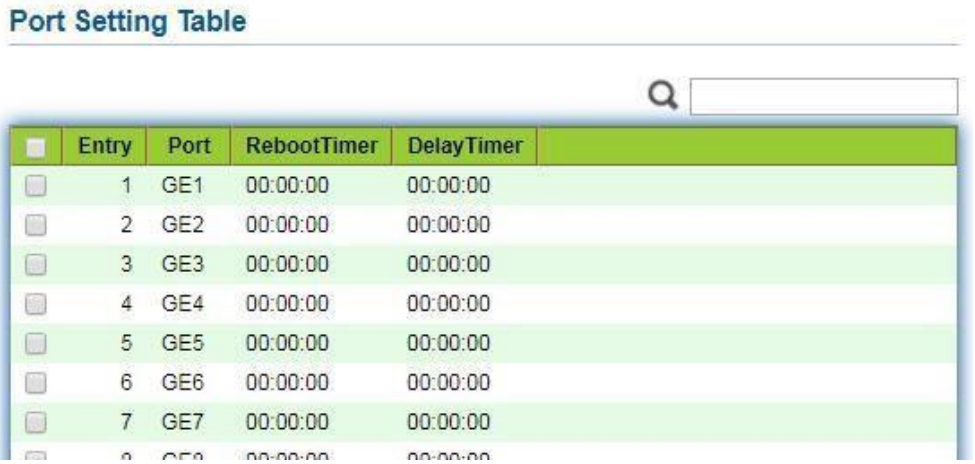


6.3 Configuración de reinicio del temporizador del puerto POE

Al configurar, la fuente de alimentación se puede reiniciar periódicamente según el puerto.

Instrucciones:

1. Haga click en “POE Setting > POE Port Timer Reboot Setting” en el menú de navegación, como se indica:



2. Seleccione el puerto y "Editar" para ingresar a la interfaz de configuración.

Los campos de la interfaz son como a continuación.

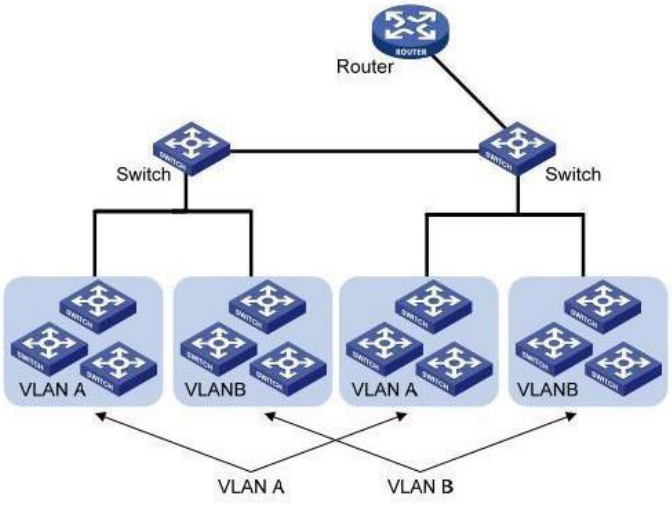
Configuration Items	Descripción
Port	Lista del Puerto
Reboot Timer	Configure el tiempo de sincronización de tiempo cuando el puerto PoE apaga la fuente de alimentación PoE. Solo admite la configuración de minutos.
DelayTimer	Después de que la fuente de alimentación PoE se apague en el tiempo de reinicio, el tiempo de retraso para reiniciar y encender la fuente de alimentación solo se puede configurar en minutos

Nota:

- Para usar esta función, debe configurar la sincronización de la hora del sistema.
- El tiempo mínimo de granularidad del reinicio del puerto Poe es de minutos.
- Cuando se configura el tiempo de reinicio, se debe configurar el tiempo de retraso.
- Cuando el tiempo de retraso es 00:00:00, significa que el puerto ya no está encendido.

7 VLAN

La VLAN no está restringida a ubicaciones físicas, lo que significa que los hosts en una misma VLAN se pueden colocar a voluntad. Como se muestra a continuación, cada VLAN, como dominio de difusión, divide una LAN física en LAN lógicas. Los anfitriones pueden intercambiar mensajes por medio de la comunicación tradicional. Para los hosts en diferentes VLAN, el dispositivo, como un enrutador o un conmutador L3, es imprescindible.



VLAN es superior al Ethernet convencional por lo siguiente:

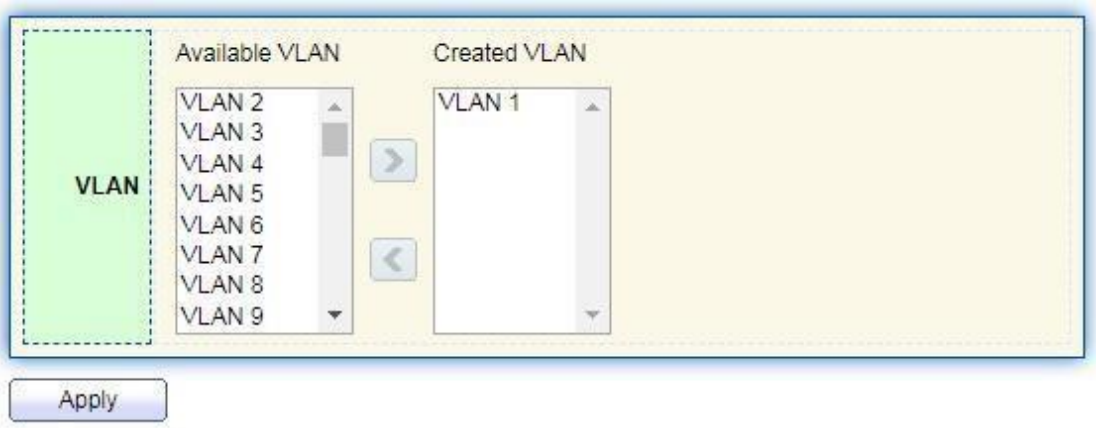
- Cobertura de dominio de difusión: el mensaje de difusión en una LAN está limitado en una VLAN para ahorrar ancho de banda y manejar los problemas relacionados con la red de manera más eficiente.

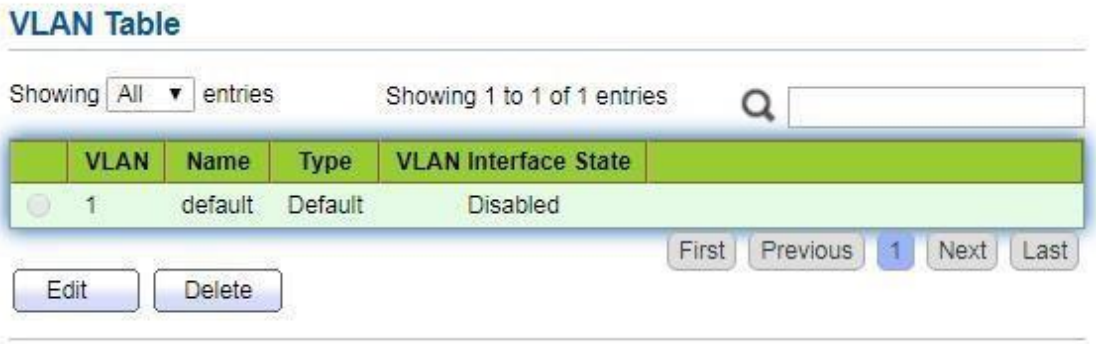
- Seguridad de LAN: los hosts de VLAN no se comunican entre sí porque los mensajes están separados por el dominio de transmisión en la capa de enlace de datos. Necesitan un enrutador o un conmutador de capa 3 para el reenvío de capa 3.
- Flexibilidad para crear un equipo de trabajo virtual: VLAN puede crear un equipo de trabajo virtual más allá del control de la red física. Los usuarios tienen acceso a la red sin cambiar la configuración si sus ubicaciones físicas se mueven dentro del alcance. Este conmutador de gestión es compatible con
- Tipos de VLAN basados en 802.1Q, protocolos, MAC y puertos. Para la configuración predeterminada, se debe adoptar el modo VLAN 802.1Q. La VLAN de puerto se divide según el número de interfaz de un conmutador. El administrador de red otorga a cada interfaz de conmutador un PVID diferente, es decir, una VLAN predeterminada de puerto. Si un marco de datos sin una etiqueta VLAN fluye hacia una interfaz de conmutador con un PVID, se marcará con el mismo PVID o se eliminará una etiqueta adicional, aunque la interfaz tenga un PVID.
- La solución a una trama de VLAN depende del tipo de interfaz, lo que facilita la definición de miembros pero reconfigura la VLAN en caso de movilidad de los miembros.

7.1 VLAN

7.1.1 Crear una VLAN

Instrucciones para crear una nueva VLAN:





1. Haga click en “VLAN > VLAN > Create VLAN” para seleccionar un nombre en el cuadro VLAN válido, muévalo al cuadro de creación de VLAN a la derecha (se pueden crear hasta 256 VLAN). “Aplicar” y terminar de la siguiente manera:

2. La VLAN creada se mostrará en la tabla de VLAN. Los usuarios pueden "Editar" la VLAN de la siguiente manera:

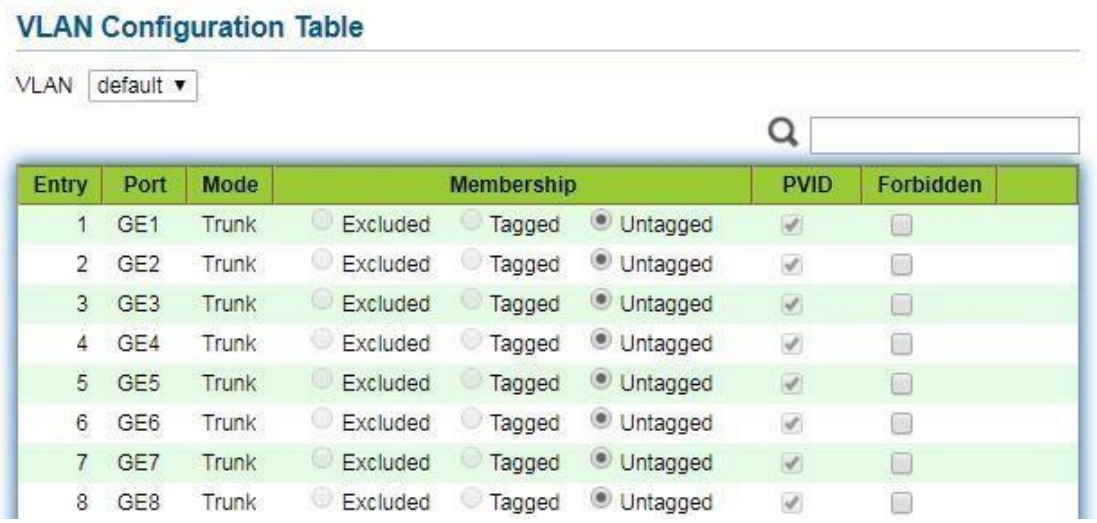
Los campos de la interfaz son como a continuación.

Campos Configurables	Descripción
VLAN ID	Se requiere seleccionar una identificación que oscile entre 1 y 4,094. Por ejemplo, 1-3,5,7 y 9. LAN 1 es el valor predeterminado, que no se repetirá en otra VLAN nueva.
Name	Es opcional modificar la descripción de VLAN según sea necesario.

7.1.2 Configuración de VLAN

Hay dos métodos. Uno es agregar múltiples puertos bajo una sola VLAN. El otro es agregar un puerto a varias VLAN. Se configuran según diferentes finalidades. Instrucciones para el primer método para agregar el puerto actual a una VLAN especificada

1. Haga clic en “VLAN > VLAN > Configuración de VLAN” en el menú de navegación, seleccione el ID de VLAN en la parte superior izquierda y luego haga clic en Información del puerto de la siguiente manera:



Los campos de la interfaz son como a continuación.

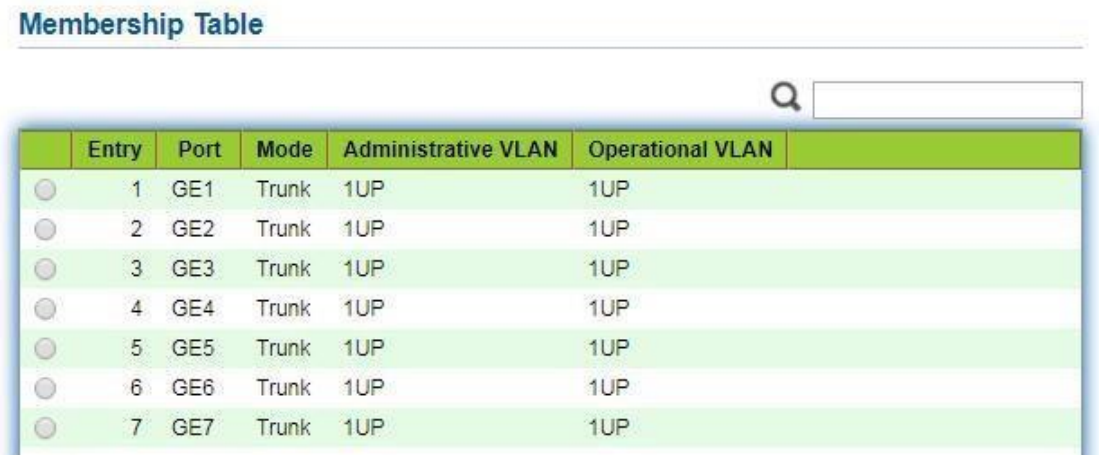
Campos Configurables	Descripción
VLAN	ID DE VLAN ID que se configurará
Port	Lista del Puerto
Mode	Modo de VLAN del puerto
Membership	Funciones de los miembros en el puerto VLAN: Excluido: el puerto está fuera de esta VLAN Etiquetado: el puerto es un miembro etiquetado de esta VLAN Sin etiquetar: el puerto es un miembro sin etiquetar de esta VLAN
PVID	Si esta VLAN es el puerto PVID
Forbidden	Si el mensaje de VLAN está prohibido para ser reenviado en este puerto

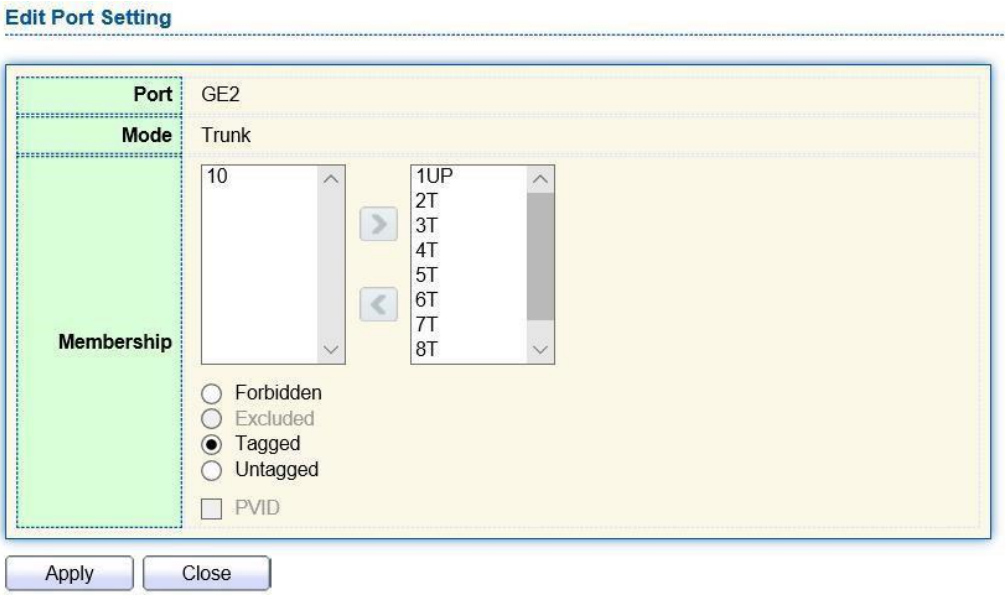
7.1.3 Membrecía

Instrucciones para el segundo método para agregar el puerto actual a una VLAN especificada

Instrucciones para el segundo método para agregar el puerto actual a una VLAN especificada

1. 1. Haga clic en “VLAN > VLAN > Membership” en el menú de navegación, seleccione el puerto a configurar y “Editar” para configurar sus atributos:



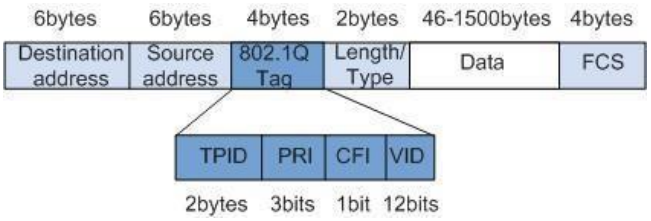


Los campos de la interfaz son como a continuación.

Campos Configurables	Descripción
Port	Lista de puertos
Mode	Modo VLAN del puerto
Membership	El puerto es el atributo de VLAN ID y VLAN:
	Prohibido: no reenviar el mensaje de VLAN Excluido: el puerto fuera de la VLAN Etiquetado: el miembro etiquetado de la VLAN Sin etiquetar: el miembro sin etiquetar de la VLAN PVID: si la VLAN es el puerto PVLAN

7.1.4 Configuración de Puerto

Configuración de troncales. Conectadas con otros conmutadores, las interfaces troncales conectan principalmente enlaces troncales para permitir que fluyan las tramas VLAN. IEEE 802.1q es el protocolo de encapsulación de enlace troncal y considera el estándar formal para redes de área local puenteadas virtuales. Cambia el formato de la trama de Ethernet al agregar una etiqueta 802.1q de 4 bits entre el campo de la dirección MAC de origen y el campo del protocolo.



Formato de fotograma 802.1q

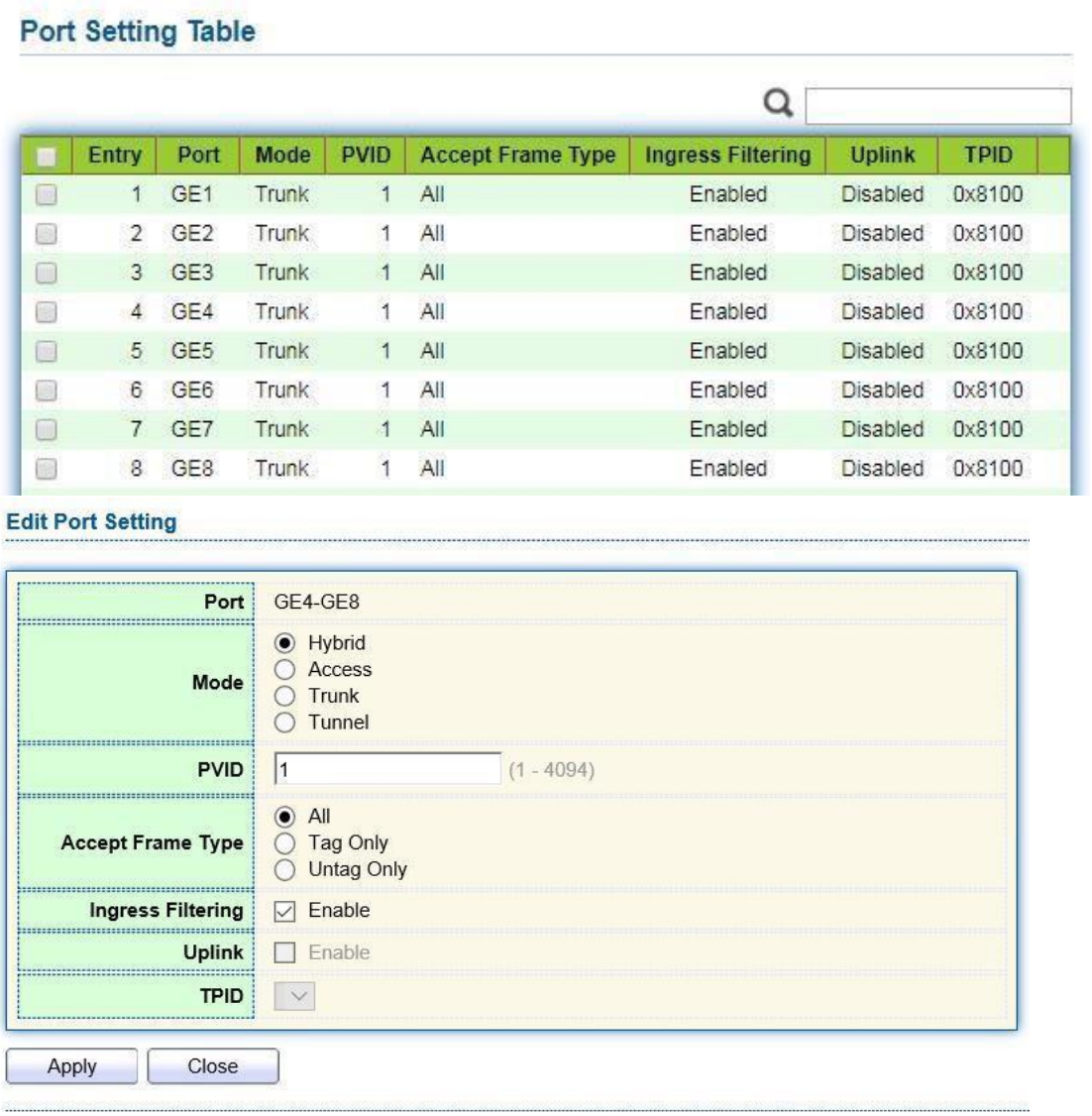
Significado de los campos de etiqueta 802.1q

Field	Length	Name	Analysis
TPID	2 bytes	Tag Protocol Identifier to describe the frame type	Hace referencia a la trama de etiqueta 802.1q cuando el valor es 0x8,100, que se descartará si el equipo pertinente no la recibe.
PRI	3 bits	Frame Priority	Va de 0 a 7, con la prioridad más alta representada por un número más grande. La trama de datos con mayor prioridad se enviará preferentemente en caso de congestión del conmutador.
CFI	1 bit	Canonical Format Indicator to reveal whether the MAC address is classical or not.	La dirección MAC es clásica cuando CFI es 0 y no clásica cuando CFI es 1. Promueve la compatibilidad entre Ethernet y Token Ring. CFI será 0 en Ethernet.
VID	12 bits	VLAN ID indicates the VLAN to which the frame belongs.	Va de 0 a 4095, siendo válido de 1 a 4094 ya que 0 y 4095 son los valores de retención del protocolo.

- Los paquetes enviados por cada conmutador compatible con el protocolo 802.1q contienen una ID de VLAN para indicar la VLAN a la que pertenece el conmutador. Por lo tanto, las tramas de Ethernet se dividen en dos tipos de la siguiente manera en una red de conmutación VLAN:
- Trama etiquetada: se refiere a la trama agregando una etiqueta 802.1q de 4 bits.
- Trama sin etiquetar: se refiere a la trama original sin una etiqueta 802.1q de 4 bits. Conectadas con otros conmutadores, las interfaces troncales conectan principalmente enlaces troncales para permitir que fluyan las tramas VLAN.

Instrucciones para la configuración de la troncal de la interfaz:

1. Haga clic en “VLAN > VLAN > Port Setting” en el menú de navegación, seleccione el puerto y “Editarlo” para configurar los atributos:



Los campos de la interfaz son como a continuación.

Campos Configurables	Descripción
Port	Número del Puerto a ser configurado
Mode	Modo VLAN de Puerto Híbrido: el puerto en este modo sirve como miembro de puertos etiquetados y no etiquetados de VLAN Acceso: el puerto en este modo sirve como el único miembro de VLAN Troncal: el puerto en este modo sirve como el único miembro no etiquetado de PVID y el miembro etiquetado de VLAN Túnel: puerto Q-in-Q VLAN
PVID	Puerto nativo de la VLAN
Accept Frame Type	Tipos de mensajes recibidos por los puertos Todo: todos los mensajes Solo etiquetar: solo se recibirán los mensajes etiquetados Solo sin etiquetar: solo se recibirán los mensajes sin etiquetar
Ingress Filtering	Un interruptor para decidir filtrar los mensajes de VLAN excluidos en el puerto
Uplink	Ya sea en modo de enlace ascendente o no
TPID	Número de identificación de la etiqueta VLAN

7.2 VLAN de voz

Tradicionalmente, se aplicará ACL (Lista de control de acceso) para distinguir los datos de voz y QoS (Calidad de servicio) para garantizar la calidad de la transmisión, mejorando así la prioridad. Para simplificar la configuración del usuario y facilitar la gestión del flujo de voz, surge Voice VLAN. La interfaz habilitada juzga si se trata de un flujo de datos de voz o no según el campo de dirección MAC de origen que accede al flujo de datos de la interfaz. El mensaje en la dirección MAC de origen es el flujo de datos de voz, que confirma el OUI (identificador único organizativo) de los dispositivos de voz configurados por el sistema. Las interfaces que reciben el flujo de datos de voz transmitirán automáticamente a la VLAN de voz, lo que simplifica la configuración del usuario y la gestión de datos de voz.

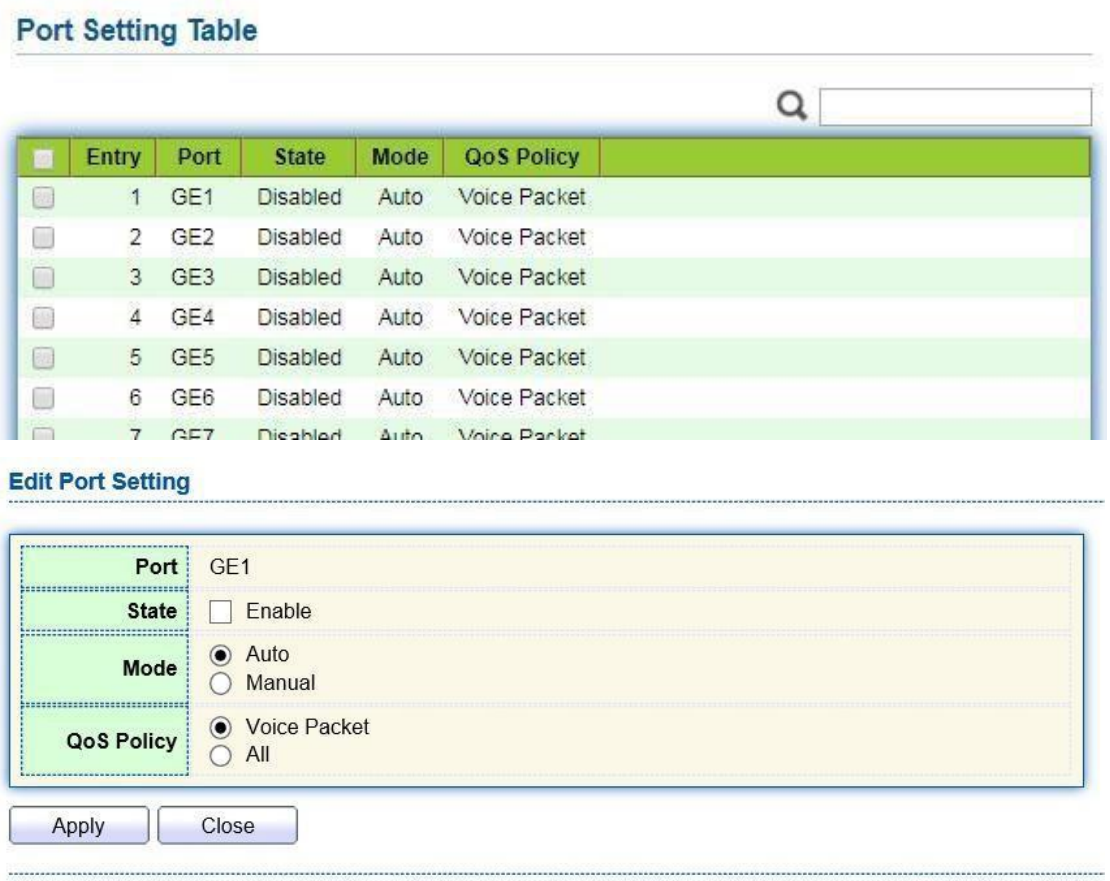
OUI de la VLAN de Voz

OUI representa un campo de dirección MAC. Su dirección se puede calcular en base a la dirección MAC de 48 bits y el bit de máscara correspondiente. La cantidad de bits de la dirección MAC de ingreso y el OUI coincidente está determinada por la longitud de todos los bits "1" en la máscara. Por ejemplo, si la dirección MAC es 1-1-1 y la máscara es FFFF-FF00–0000, el resultado de la ejecución y el cálculo de la dirección MAC y la máscara correspondiente, es decir, OUI, será 0001–0000–0000. Si los primeros 24 bits de la dirección MAC de ingreso coinciden con los de OUI, la interfaz VLAN de voz habilitada identifica el flujo de datos y el dispositivo de ingreso como el flujo de datos de voz y el dispositivo de voz, respectivamente. La VLAN de voz se divide para el flujo de datos de voz del usuario. Las VLAN de voz se crean para conectar las interfaces vinculadas con los dispositivos de voz para transmitir los datos de voz al interior de forma centralizada. Los datos de voz y los datos que no son de voz a menudo existen en la misma red. Los datos de voz necesitan una prioridad más alta que otros datos comerciales durante la transmisión para reducir la posible demora y la pérdida de paquetes.

1. Haga click en “VLAN > Voice VLAN > Property” en el menú de navegación:

Los campos de la interfaz son como a continuación.

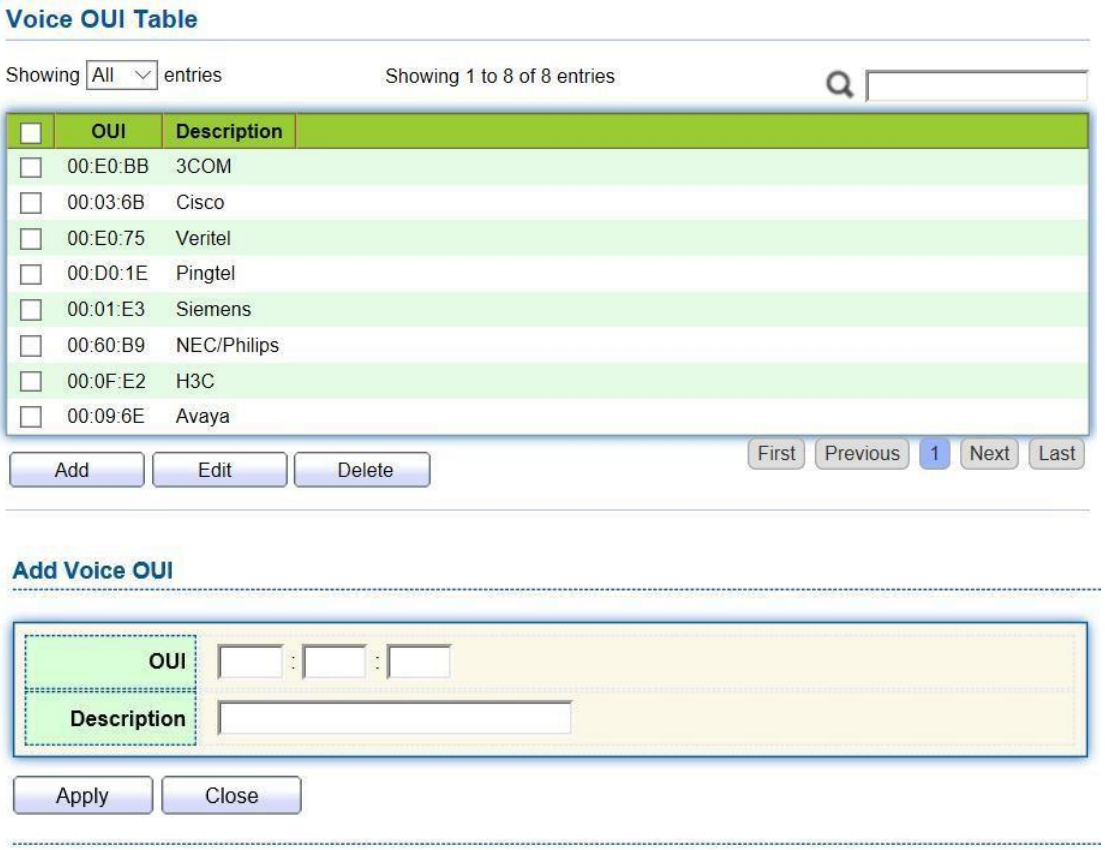
Elementos de configuración	Descripción
State	1
VLAN	Especifique la ID de VLAN agregada que va de 1 a 4094, p. 1- 3, 5, 7 y 9, con VLAN 1 por defecto. Se deben agregar otras VLAN sin etiquetar al puerto que necesita enlaces.
CoS / 802.1p Remarking	Ya sea para redefinir la prioridad del mensaje de VLAN de voz o no
Aging Time	Tabla del parámetro de envejecimiento



Los campos de la interfaz son como a continuación.

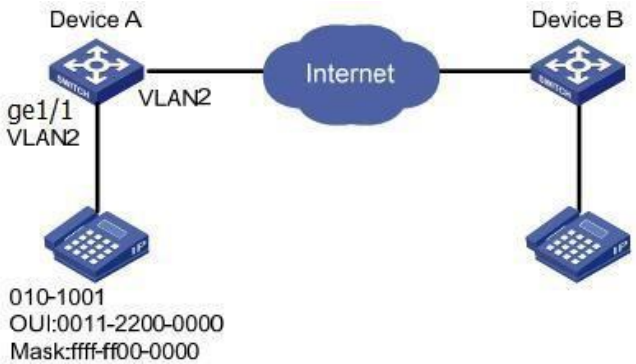
Elementos de configuración	Descripción
Port	Puerto de VLAN de voz habilitado
State	Seleccione para habilitar la VLAN de Voz
Mode	El puerto VLAN de voz se puede operar en modo automático y modo manual.

2. Haga click en “VLAN > Voice VLAN > Voice OUI” en el menú de navegación para configurar el segmento de dirección de OUI de Voice VLAN de la siguiente manera:

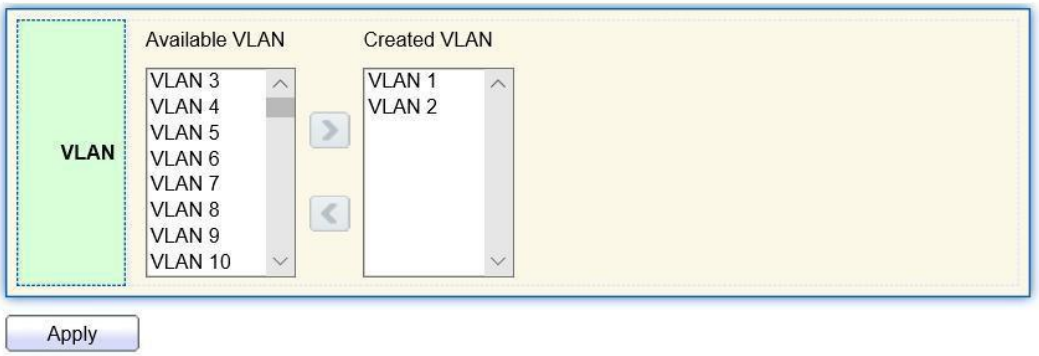


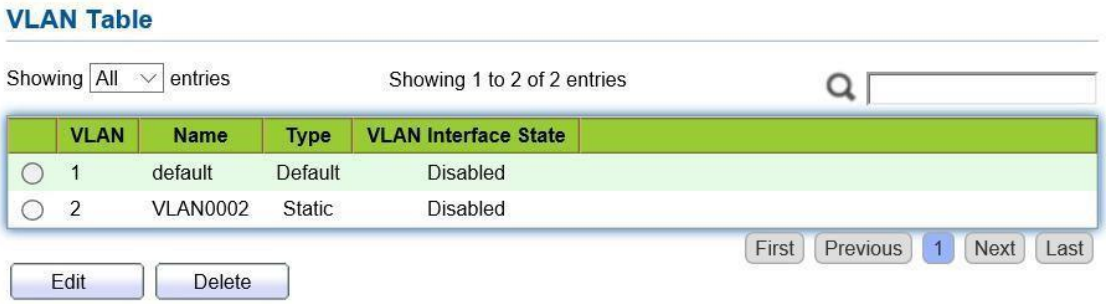
3. Completar los elementos de configuración correspondientes.
4. Presione “Apply” y Finish para terminar.

Por ejemplo, configure la VLAN de voz en modo manual para que los puertos que acceden a la telefonía IP puedan entrar/salir de la VLAN de voz y transmitir el flujo de voz dentro de ella. Cree VLAN2 para operar la VLAN de voz de forma segura, lo que permite que solo fluyan los datos de voz. La telefonía IP transmite el flujo de voz sin etiquetar a GE1, el puerto Trunk de ingreso. Los usuarios deben personalizar un OUI (0011-2231-05e1) y configurar el diagrama de red de VLAN de Voz en modo automático.



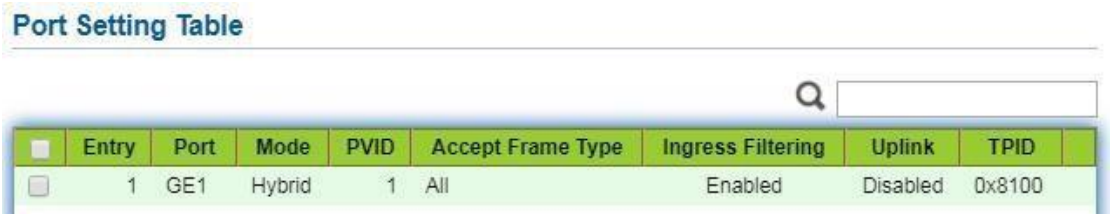
Instrucciones:



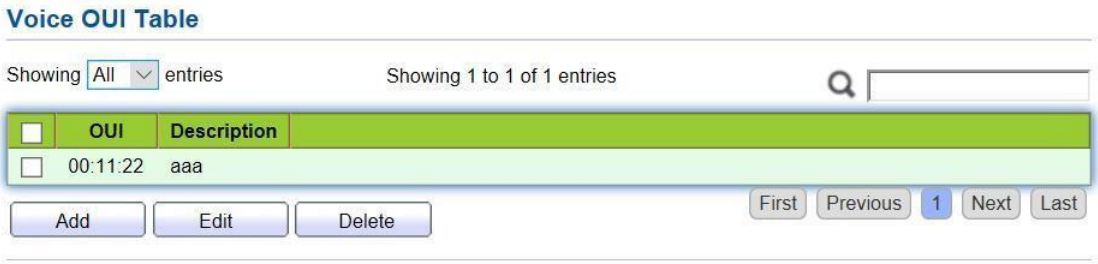


1. Create a VLAN to recognize the VLANs where employees belong. Haga click en "VLAN > VLAN > Create VLAN" en el menú de navegación para agregar VLAN 2 a la lista de VLAN a la derecha. "Aplicar" y terminar:

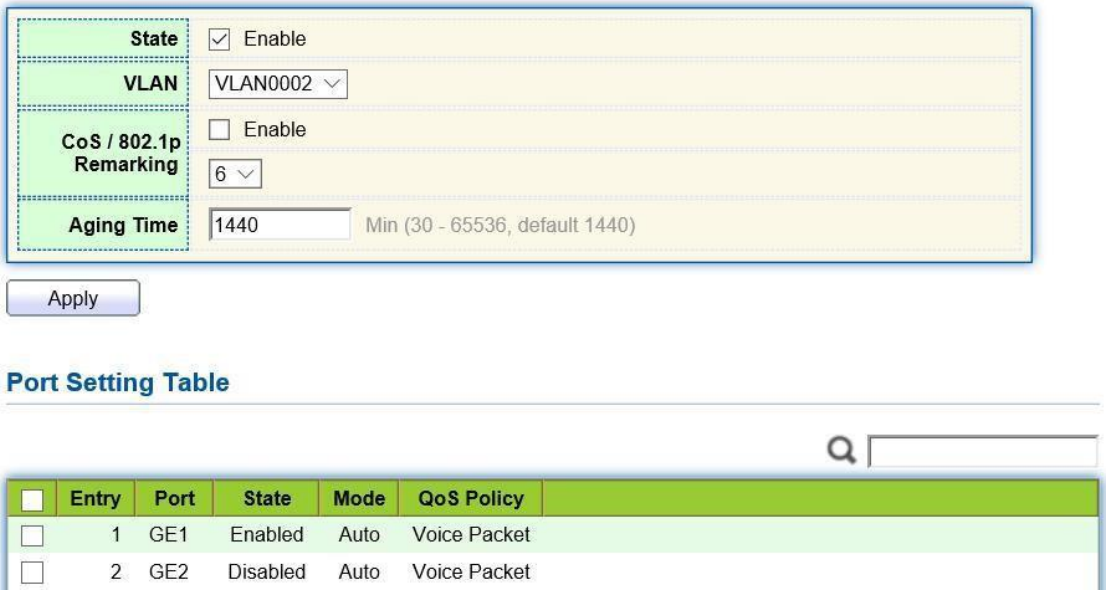
2. Configure la interfaz Ethernet GE1 del Switch A en modo Híbrido. Haga click en "VLAN > VLAN > Port Setting" en el menú de navegación, Presione "Edit" GE1 y selecciona Hybrid mode:



3. Haga click en "VLAN > Voice VLAN > Voice OUI" en el menú de navegación para configurar y agregar el rango de la dirección MAC de OUI e ingrese los primeros 24 bits de la dirección MAC del dispositivo de voz: 00:11:22. "Aplicar" y Terminar de la siguiente manera:



4. Habilite la VLAN de Voz del Puerto GE1. Haga click en “VLAN > Voice VLAN > Property” en el menú de navegación para habilitar la configuración global, seleccione VLAN2. Seleccione el puerto GE1 en la lista de configuración, "Editar" y habilite el modo automático. “Aplicar” y terminar de la siguiente manera:



Nota

Con el modo automático habilitado, los puertos reenviarán mensajes de VLAN de voz, aunque no haya ningún puerto en VLAN2.

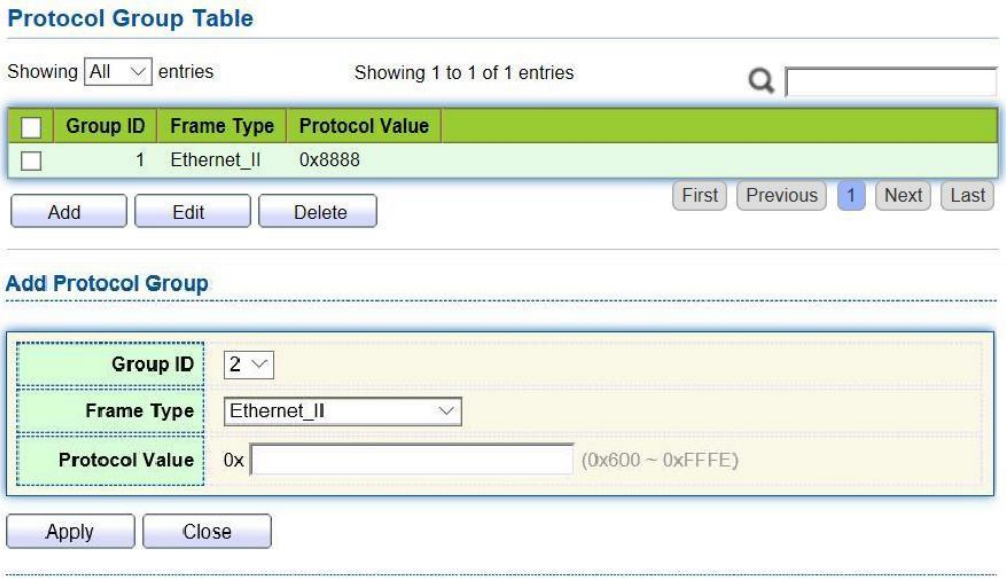
7.3 Protocolo VLAN

El protocolo VLAN distribuye diferentes ID de VLAN según el tipo de protocolo (familia) y el formato de encapsulación de los mensajes recibidos por las interfaces.

Los administradores deben preparar el esquema de mapeo entre el dominio de protocolo de la trama de Ethernet y la ID de VLAN que se agregará si se reciben tramas sin etiquetar. Fortaleza: dicho método de división mejorará la gestión y el mantenimiento al vincular los servicios de red y las VLAN. Deficiencias: Es necesaria la configuración inicial del esquema de relación de mapeo. Los formatos de dirección de los protocolos deben analizarse y convertirse, lo que conduce a una menor velocidad debido a la gran cantidad de recursos consumidos.

Instrucciones:

1. Haga click en “VLAN > Protocol VLAN > Protocol Group” en el menú de navegación:

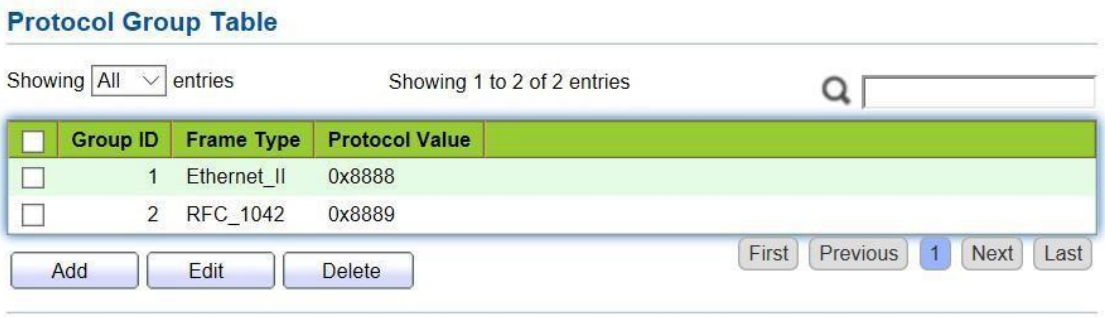


Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Group ID	Protocolo de grupo VLAN
Frame Type	Tipos de Trama: Ether2, LLC, RFC 1042
Protocol Value	Rangos desde 0x600 a 0xFFFE

2. Completa los elementos de configuración correspondientes.

3. "Aplicar" y finalizar.



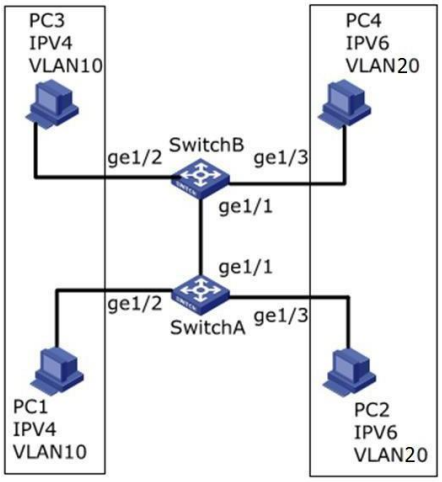
4. Haga click en "VLAN > Protocol VLAN > Group Binding" en el menú de navegación para enlazar el protocolo No., puerto No. y VLAN ID, para que la configuración surta efecto como sigue:

Descripción:

Configure los protocolos coincidentes IPv4 e IPv6, así como el protocolo ARP.

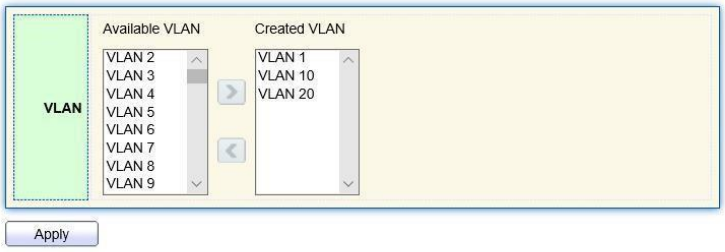
Por ejemplo, PC1 y 3 pueden acceder mutuamente, con el enlace del protocolo de comunicación IPv4 con VLAN10. PC2 y 4 pueden acceder mutuamente, con el protocolo de comunicación IPv6 enlazando con VLAN20.

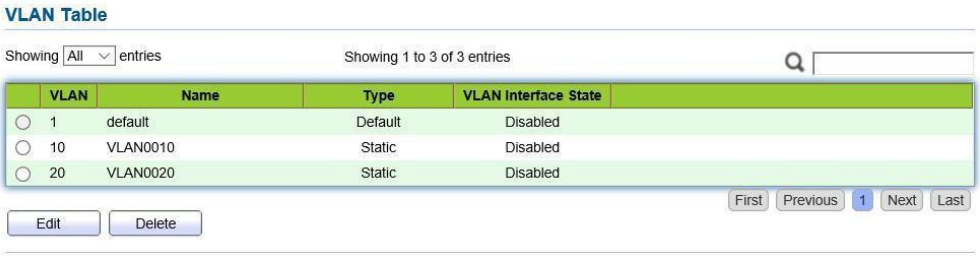
Diagrama de red de la división VLAN de protocolo



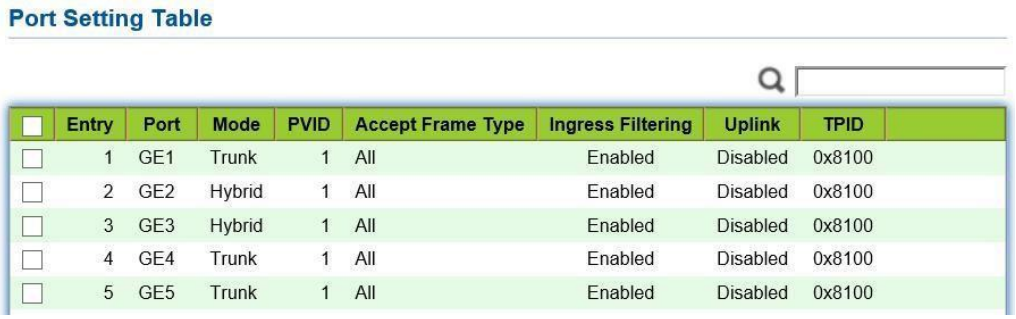
Instrucciones:

1. Cree una VLAN para reconocer las VLAN a las que pertenecen los empleados. Haga clic en "VLAN
   > VLAN > Crear VLAN", agregue VLAN10 y 20 a la Lista de
   creación de VLAN a la derecha, "Aplicar" y finalice:

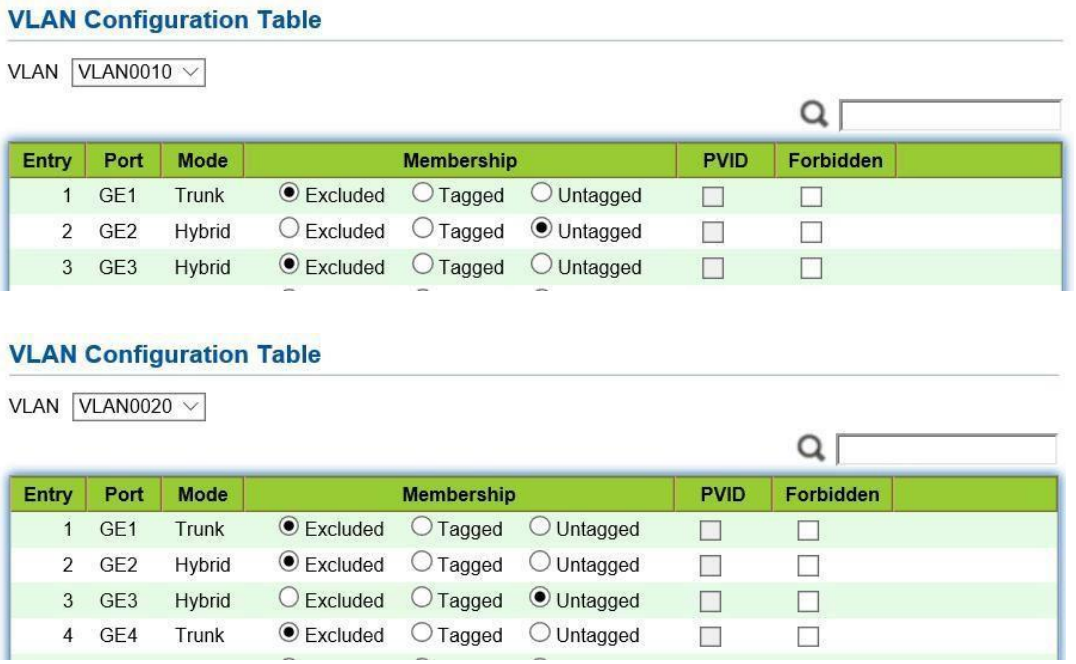




2. Configure las interfaces GE2 y GE3 del conmutador A en modo híbrido. Haga clic en "VLAN > VLAN > Port Setting", "Edit" las interfaces en modo híbrido:



3. Agregue GE2 y GE3 sin etiquetar a VLAN10 y VLAN20 respectivamente. Haga clic en "VLAN > VLAN > VLAN Configuration", desplegable en la lista para elegir VLAN10 y el puerto GE2 sin etiquetar. Siguiendo los mismos pasos, agregue el GE3 sin etiquetar a VLAN20 de la siguiente manera:

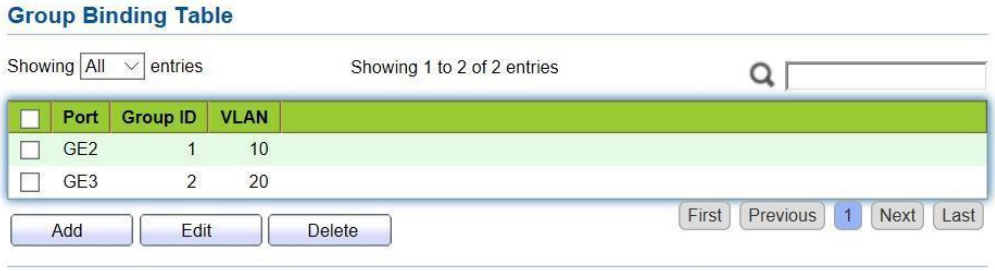


4. Agregue las interfaces GE2 y GE3 sin etiquetar del conmutador B a VLAN cuyos puertos necesitan enlaces. Los pasos son como los pasos 2 y 3.
5. Agregue la interfaz GE1 etiquetada del conmutador A a VLAN10 y 20. Haga clic en "VLAN > VLAN > VLAN Configuration", desplegable la lista para seleccionar VLAN10 y el miembro etiquetado de GE1. Configure VLAN20 de manera similar.

6. Protocolo relacionado y VLAN. Los ID de VLAN se asignan de acuerdo con el

tipo de protocolo (familia) y el formato de encapsulación de los mensajes recibidos por las interfaces. Haga clic en "VLAN > Protocol VLAN > Protocol Group" en el menú de navegación para agregar 2 reglas para grupos de protocolos:

7. Port, grupo de protocolos y enlace VLAN. Haga clic en "VLAN > Protocol Group > Group Binding", "Add" para enlazar GE2 y el grupo de enlace ID1 con VLAN10, y para enlazar GE3 y el grupo de enlace ID2 con VLAN20:



7.4 VLAN de Mac

Las VLAN basadas en MAC se dividen sujetas a las direcciones MAC de la tarjeta de red. Los administradores prepararán el esquema de asignación entre la dirección MAC y el ID de VLAN, que se agregará si el switch recibe tramas sin etiquetar.

Fuerza: No es necesario volver a configurar VLAN cuando cambia laubicación física de un usuario de terminal, lo que garantiza la seguridad del usuario y la flexibilidad de acceso. Deficiencia: Se aplica a la escena en la que la tarjeta de red y el entorno de red simple se reemplazan con poca frecuencia, con miembros definidos de antemano.

Instrucciones:

1. Haga clic en "VLAN > MAC VLAN > MAC Group" en el menú de navegación, y "Add" a new MAC group de la siguiente manera:

Los campos de la interfaz son como a continuación.

Campos Configurables	Descripción
Group ID	ID de grupo de VLAN MAC
MAC Address	La dirección MAC que se enlazará con VLAN
Mask	Indica el puerto de la dirección MAC. Ingrese 48 si es una coincidencia exacta. Otros deben ser coherentes con las máscaras de las direcciones IP.

Por ejemplo, una empresa con altos requisitos de seguridad de la información permite que sus PC solo accedan a la red interna. Como se muestra, el switch GE1 conecta los puertos de enlace ascendente del switch A, mientras que sus puertos descendentes conectan PC1, 2 y 3. Como resultado, PC1, 2 y 3 pueden acceder a la red interna a través de Switch A y S, mientras que otras PC no pueden.

Lógica de configuración: se utilizan los siguientes pasos para dividir la VLAN en función de la dirección MAC.

1. Cree una VLAN relevante.
2. Agregue interfaces Ethernet a la VLAN de una manera correcta.
3. Conecte la VLAN con las direcciones MAC de PC1, 2 y 3.

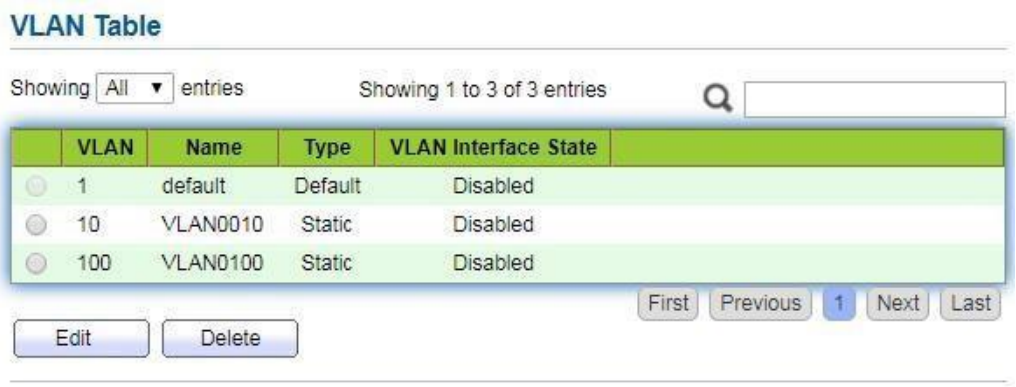
Preparación de datos: se deben preparar los siguientes datos para el momento de la configuración.

- Ajuste GE1 PVID de 100 en el switch.
- Configure GE1 para acceder a VLAN10 de la manera sin etiquetar en el switch.
- Configure GE2 para acceder a VLAN10 de la manera etiquetada en el switch.
- Configure la interfaz Switch A de forma predeterminada, es decir, todas las interfaces se agregarán a VLAN1 de forma Untagged.
- Conecte las direcciones MAC de PC1, 2 y 3 con VLAN10.

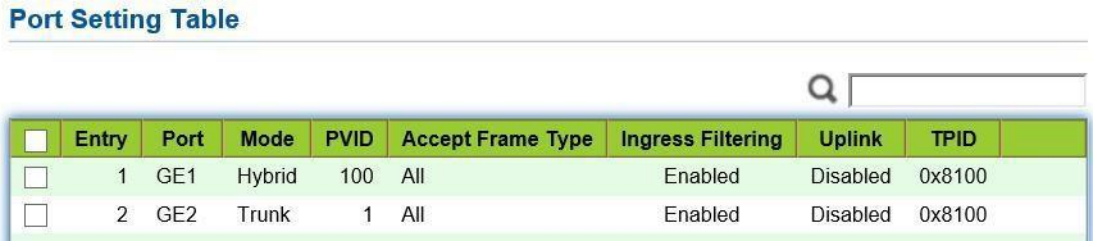
Dibuje un diagrama de red para la división VLAN basado en direcciones MAC:

Instrucciones:

1. Cree una VLAN para reconocer las VLAN a las que pertenecen los empleados. Haga clic en "VLAN > VLAN > Create VLAN" en el menú de navegación, agregue VLAN10 a la lista de creación de VLAN a la derecha, "Aplicar" y termine de la siguiente manera:



2. Configure el GE1 del switch en modo híbrido con PVID de 100 para que sirva como miembro Untagged de VLAN10. Configure GE2 en modo troncal para que actúe como miembro etiquetado de VLAN10.



Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
○	1	GE1	Hybrid	1U, 10U, 100P	1U, 10U, 100P
○	2	GE2	Trunk	1UP, 10T	1UP, 10T
○	3	GE3	Trunk	1UP	1UP

3. Configure las interfaces del conmutador A de forma predeterminada, es decir, todas las interfaces acceden a VLAN1 de forma no etiquetada. Conecte las direcciones MAC de PC1, 2 y 3 con VLAN10.

   Haga clic en "VLAN > MAC VLAN > MAC Group" en el menú de navegación, introduzca las direcciones MAC de PC1 (0022-0022-0022), PC2 (0033-0033-0033) y PC3 (0044-0044-0044), con la máscara de coincidencia exacta de 48 bits de la siguiente manera:

MAC Group Table

Showing All entries Showing 1 to 3 of 3 entries

	Group ID	MAC Address	Mask
☐	1	00:22:00:22:00:22	48
☐	2	00:33:00:33:00:33	48
☐	3	00:44:00:44:00:44	48

Add Edit Delete First Previous 1 Next Last

4. Haga click en “VLAN > MAC VLAN > Group Binding” en el menú de navegación, "Agregar" para seleccionar solo el puerto híbrido, el ID de grupo MAC que se enlazará y el ID de VLAN especificado. "Aplicar" y finalizar:

MAC Group Table

Showing All entries Showing 1 to 3 of 3 entries

	Group ID	MAC Address	Mask
☐	1	00:22:00:22:00:22	48
☐	2	00:33:00:33:00:33	48
☐	3	00:44:00:44:00:44	48

Add Edit Delete First Previous 1 Next Last

5. Verificación de la configuración

   Solo PC1, 2 y 3 tienen acceso a la red interna.

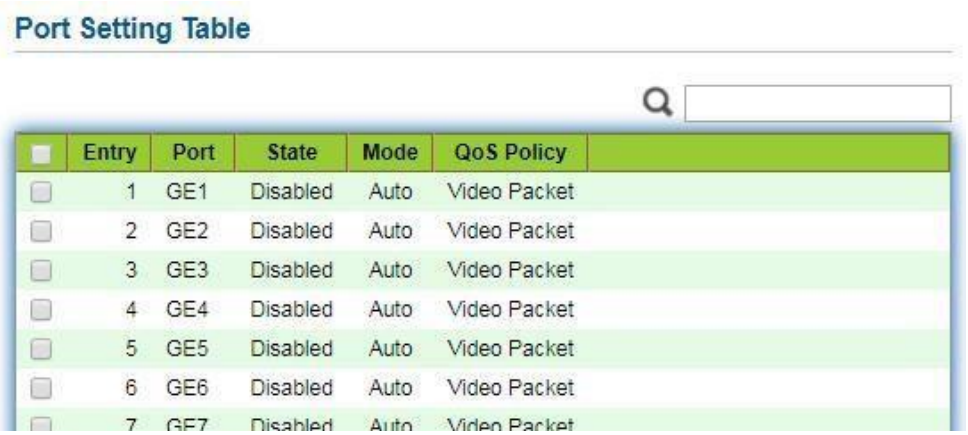
7.5 VLAN de vigilancia

La VLAN de vigilancia se utiliza principalmente para paquetes de flujo de video. Para garantizar la prioridad de dichos paquetes en el proceso de transmisión, es más alta que los paquetes ordinarios Instrucciones:

6. Haga click en “VLAN > Surveillance VLAN > Property” en el menú de navegación. Configura como se indica.

Los campos de la interfaz son como a continuación.

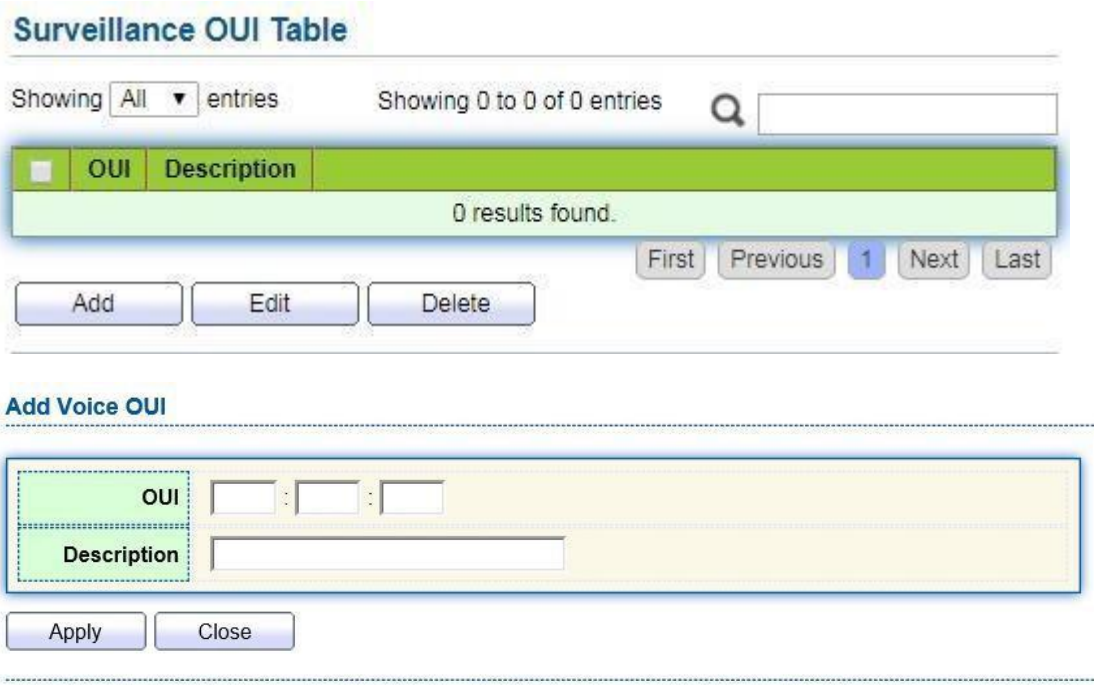
Elementos de configuración	Descripción
State	Compruebe y habilite la VLAN de vigilancia
VLAN	Especifique el ID de VLAN agregado que va de 1 a 4.094, por ejemplo, 1-3, 5, 7 y 9, con VLAN 1 de forma predeterminada. Otras VLAN deben agregarse de forma no etiquetada al puerto que necesita enlaces.
CoS / 802.1p Remarking	Si se debe redefinir la prioridad de los mensajes VLAN de voz o no
Aging Time	Tiempo de envejecimiento de la tabla



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	Puerto VLAN de voz habilitado
State	Compruebe y habilite la VLAN de vigilancia
Mode	El puerto VLAN de vigilancia se puede operar en modo automático y modo manual.
QoS Policy	Seleccione el mensaje que se verá afectado por QoS

1. Haga clic en "VLAN > Surveillance VLAN > Surveillance OUI" en el menú de navegación para configurar el segmento de direcciones de OUI de Surveillance VLAN de la siguiente manera:



2. Completa los elementos de configuración correspondientes.
3. Presione “Apply” y Finish como se indica:

7.6 GVRP

El protocolo de registro de VLAN GVRP es una aplicación del protocolo de registro de atributo general, que proporciona una función de eliminación de VLAN compatible con 802.1Q y un establecimiento dinámico de VLAN en el puerto troncal del puerto troncal 802.1Q.

Los conmutadores GVRP pueden intercambiar información de configuración de VLAN entre sí, cortar la transmisión innecesaria y el tráfico de unidifusión desconocido, y crear y administrar VLAN dinámicamente en conmutadores conectados a través del enlace troncal 802.1Q.

GID y GIP se utilizan en GVRP, que proporcionan el mecanismo de estado general Descripción y el mecanismo de difusión de información para aplicaciones basadas en GARP, respectivamente. GVRP solo se ejecuta en enlaces troncales 802.1Q. GVRP corta el enlace troncal para que solo se transmita la VLAN activa en la conexión troncal. Antes de que GVRP agregue una VLAN a la línea troncal, primero recibe la información de unión del conmutador. La información de actualización de GVRP y el temporizador se pueden cambiar. Los puertos GVRP tienen una variedad de modos operativos para controlar cómo adaptan las VLAN. GVRP puede agregar y administrar dinámicamente VLAN para VLAN

base de datos

GVRP admite la propagación de información de VLAN entre dispositivos. En GVRP, la información de VLAN de un conmutador se puede configurar manualmente y todos los demás conmutadores de la red pueden comprender dinámicamente las VLAN. El nodo terminal puede acceder a cualquier conmutador y conectarse a la VLAN requerida. Para utilizar GVRP, se debe instalar una tarjeta de interfaz de red (NIC) compatible con GVRP. La NIC compatible con GVRP se puede configurar para unirse a la VLAN requerida y luego acceder a un conmutador habilitado para GVRP. Se establece la conexión de comunicación entre la NIC y el conmutador, y se realiza la conectividad VLAN entre la NIC y el conmutador.

7.6.1 Propiedad

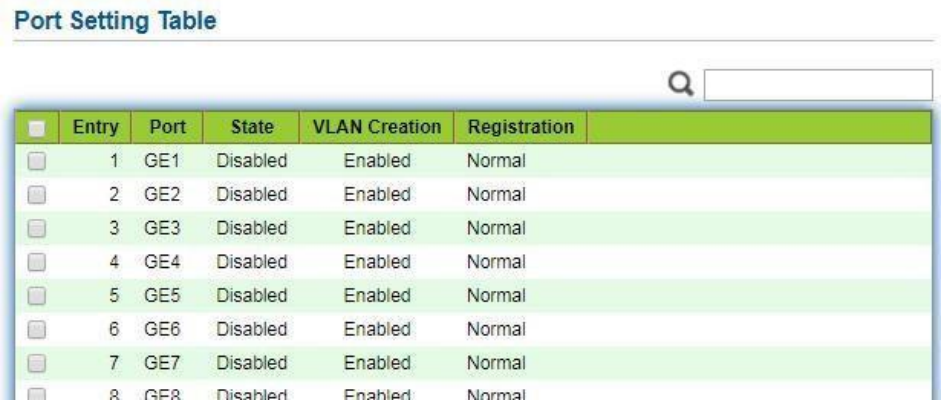
Configuración Global y por puerto.

Instrucciones:

1. Haga click en “VLAN > GVRP > Property” en el menú de navegación como se indica.

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
State	La función GVRP se habilita globalmente configurando
Join	Un valor en el rango de 1-20cs, es decir, en unidades de centésimas de segundo. El valor predeterminado es 20cs.
leave	Un valor en el rango de 60-300cs, es decir, en unidades de centésimas de segundo. El valor predeterminado es 60cs.
LeaveAll	Un valor en el rango de 1000-5000cs, es decir, en unidades de centésimas de segundo. El valor predeterminado es 1000cs.



2. Haga click en “VLAN > GVRP > Property” en el menú de navegación, seleccione el puerto y "Editar" para ingresar a la interfaz de configuración de la siguiente manera.

Los campos de la interfaz son como a continuación.

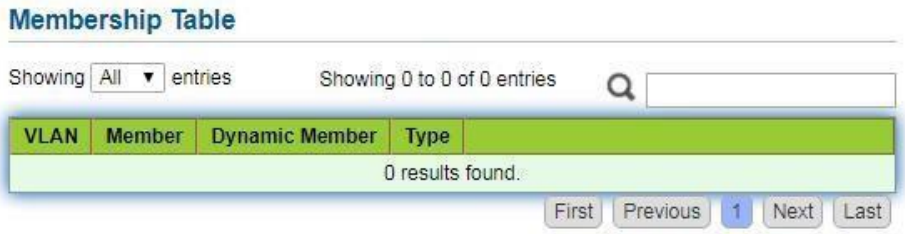
Elementos de configuración	Descripción
Port	Lista de Puertos
State	Habilitar o deshabilitar la función GVRP del puerto
VLAN Creation	Habilite o deshabilite para crear VLAN automáticamente
Registration	Tres modos de registro de GVRP Normal: permita que la VLAN dinámica se registre en el puerto y envíe mensajes de declaración de VLAN estática y VLAN dinámica al mismo tiempo Corregido: la VLAN dinámica no puede registrarse en el puerto, solo se envían mensajes de declaración de VLAN estática
	Prohibido: VLAN dinámica no puede registrarse en el puerto. Al mismo tiempo, todas las VLAN excepto vlan1 en el puerto se eliminan y solo se envía el mensaje de declaración de vlan1

7.6.2 Membrecía

Ver información de miembros dinámicos de GVRP.

Instrucciones:

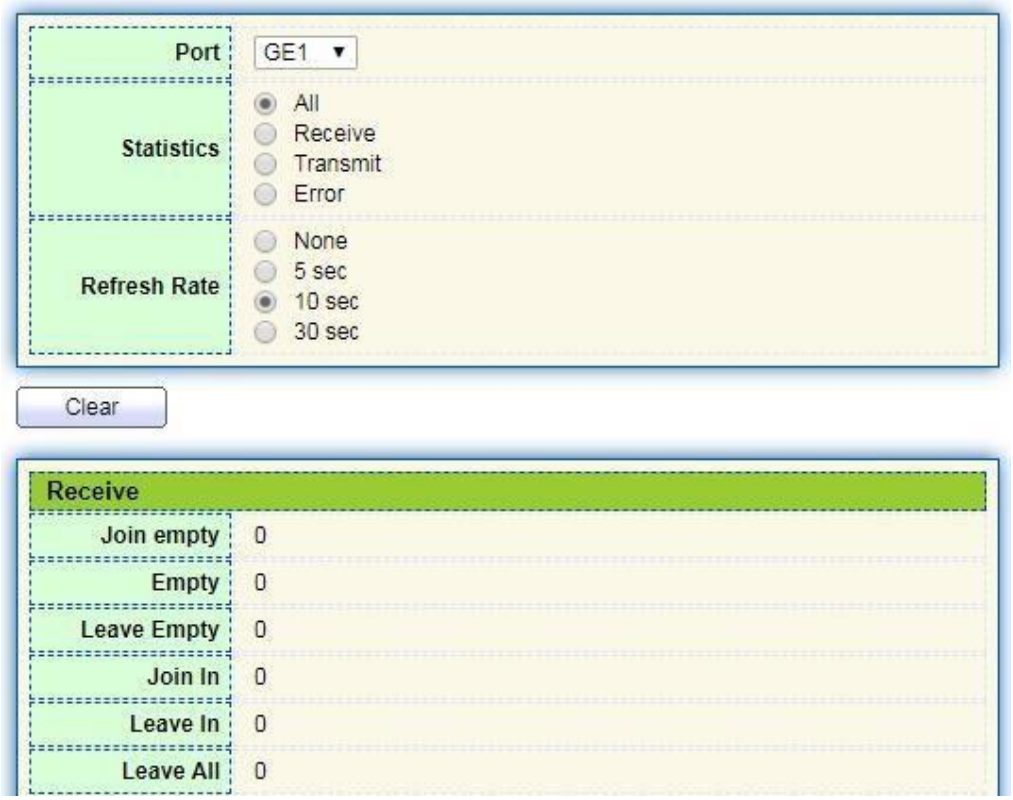
1. Haga click en “VLAN > GVRP > Membership” en el menú de navegación.



7.6.3 Estadística

Visualiza el mensaje GVRP del puerto
Instrucciones:

1. Haga click en “VLAN > GVRP > Statistics” en el menú de navegación:



8 Tabla de Direcciones MAC

- Los switches Ethernet se innovan principalmente para reenviar de acuerdo con los propósitos en la capa de enlace de datos. Es decir, la dirección MAC transmitirá los mensajes a los puertos correspondientes según los propósitos. La tabla de reenvío de direcciones MAC es una tabla L2 que ilustra las direcciones MAC y los puertos de reenvío, que es la base del reenvío rápido de mensajes L2. La tabla de reenvío de direcciones MAC contiene los siguientes datos:
- Dirección MAC de destino
- ID de VLAN perteneciente al puerto
- Número de entrada de reenvío de este dispositivo
- Hay dos tipos de reenvío de mensajes según la información de la tabla de direcciones MAC:
- Modo unicast: el conmutador transmite directamente los mensajes desde la salida de la tabla cuando la tabla de reenvío de direcciones MAC contiene entradas correspondientes con la dirección MAC de destino.
- Modo de difusión: Cuando el switch recibe los mensajes con la dirección de destino llena de F-bits, o no hay ninguna entrada correspondiente a la dirección de destino MACen la tabla de reenvío, el switch reenviará los mensajes a todos los puertos excluyendo el puerto receptor de esta manera.

8.1 Dirección Dinámica

El tiempo de vencimiento y la información de la tabla de las direcciones MAC se pueden configurar y verificar en esta página.

La tabla de direcciones MAC necesita actualizaciones constantes para adaptarse a los cambios de la red. Genera automáticamente entradas que están limitadas por su vida útil (es decir, el tiempo de envejecimiento). Las entradas que no se actualicen después del vencimiento se eliminarán. El tiempo de antigüedad de una entrada se volverá a calcular si su registro se actualiza antes de su vencimiento.

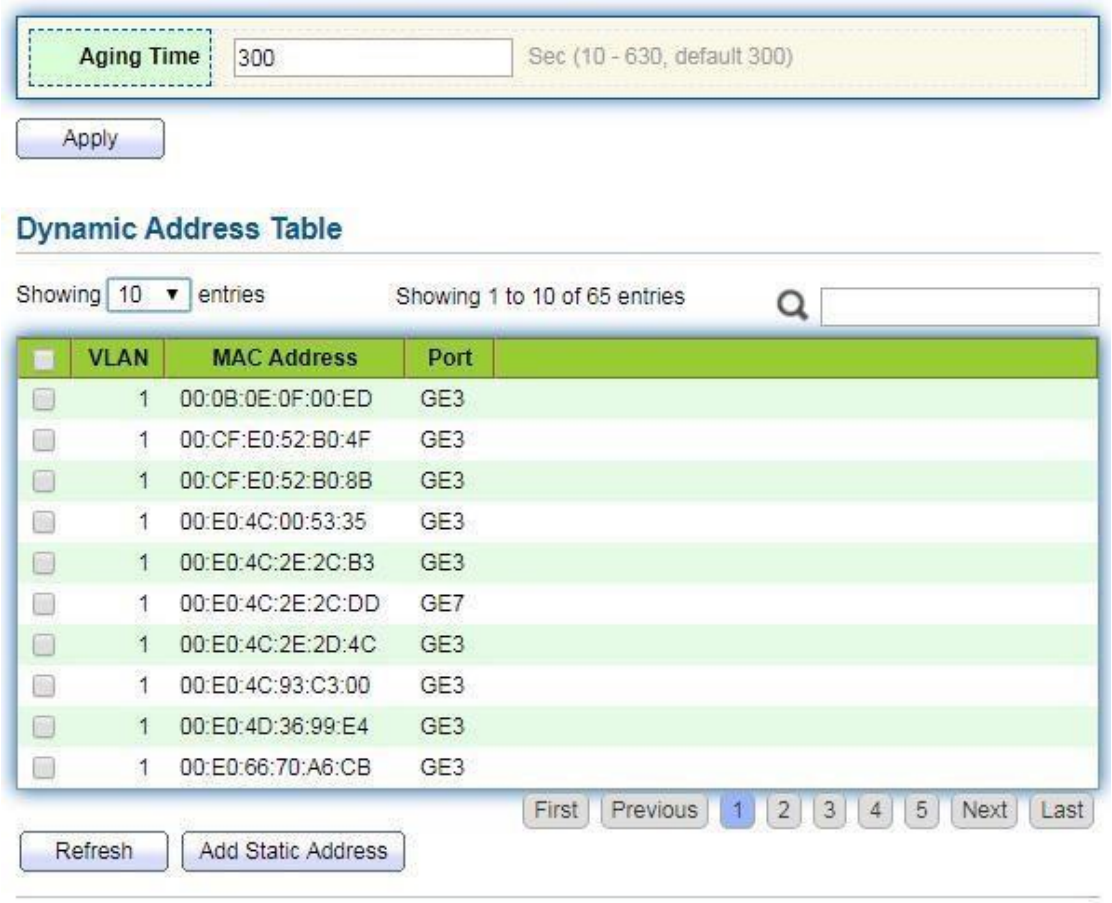
El tiempo de caducidad adecuado ayuda a alcanzar el objetivo de caducidad de la dirección MAC. La escasez de tiempo de envejecimiento puede hacer que muchos

conmutadores transmitan para descubrir los paquetes de las direcciones MAC de destino, lo que influye en el rendimiento del conmutador.

Envejecer demasiado puede hacer que el switch guarde las entradas de direcciones MAC obsoletas, agotando así los recursos de reenvío y no actualizando la tabla de reenvío en función de los cambios en la red.
El switch puede eliminar las entradas válidas de la tabla de direcciones MAC debido a un tiempo de caducidad demasiado corto, lo que reduce la eficiencia de reenvío. En general, el tiempo de envejecimiento recomendado es de 300 segundos por defecto.

Instrucciones para la configuración del Tiempo de Envejecimiento:

1. Haga click en “MAC Address Table > Dynamic Address” en el menú de navegación para configurar y ver la interfaz:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
MAC Aging Time	Introduzca el Tiempo de envejecimiento de la dirección MAC

2. Completa los elementos de configuración correspondientes.

3. Presiona “Apply” y Finish.

La tabla MAC almacena la dirección MAC, el número de VLAN, la información de entrada/salida, etc. que aprenden los switches. Al reenviar datos, localizará rápidamente la salida del dispositivo de acuerdo con la dirección MAC de destino y la tabla de consulta del número de VLAN de las tramas de Ethernet.
Para verificar la tabla de direcciones MAC, consulte la Sección 3.3 del Capítulo 3.

8.2 Direcciones Estáticas

Los usuarios configuran manualmente la tabla estática y la distribuyen a cada placa de interfaz, que no envejecerá.

Instrucciones:

1. Haga click en “MAC Address Table > Static Address” como a continuación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
MAC	Requerido. Introduzca la nueva dirección MAC. Ejemplo: HH:HH:HH:HH:HH:HH
VLAN	Requerido. Especifica el ID de la VLAN
MAC	Requerido. Seleccione el tipo de interfaz e ingrese el nombre de la interfaz Descripción: debe ser el puerto miembro de las VLAN configuradas.

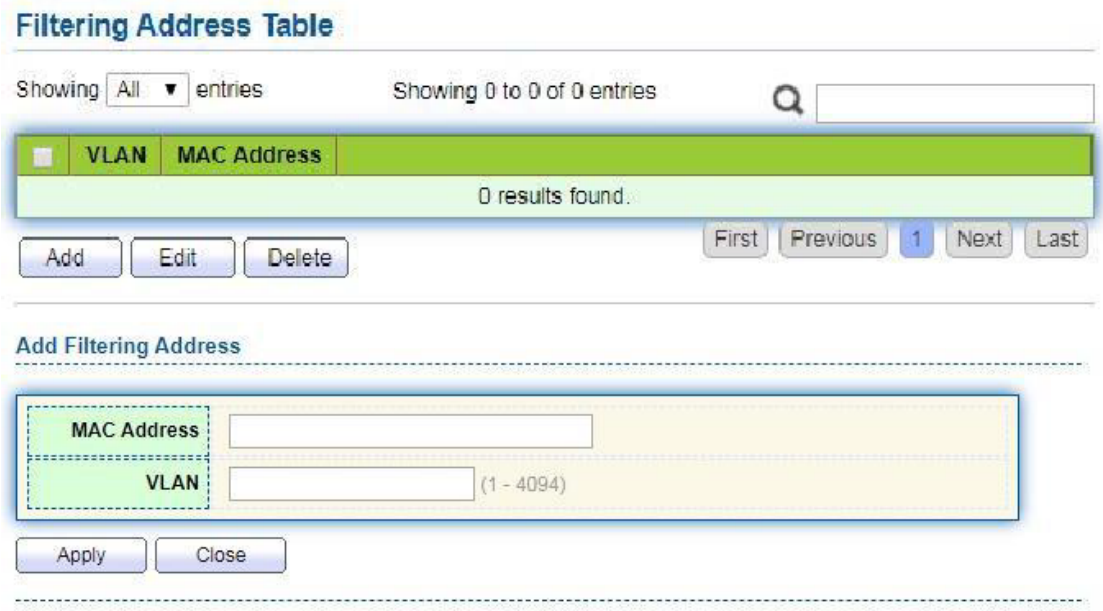
2. Completa los elementos de configuración correspondientes.
3. Presione “Apply” y Finish.

8.3 Filtrado de Direcciones

El switch descarta la trama de datos coincidente por configuración.

Instrucciones:

1. Haga clic en "MAC Address Table > Filtering Address", como se indica:



Los campos de la interfaz son como a continuación.

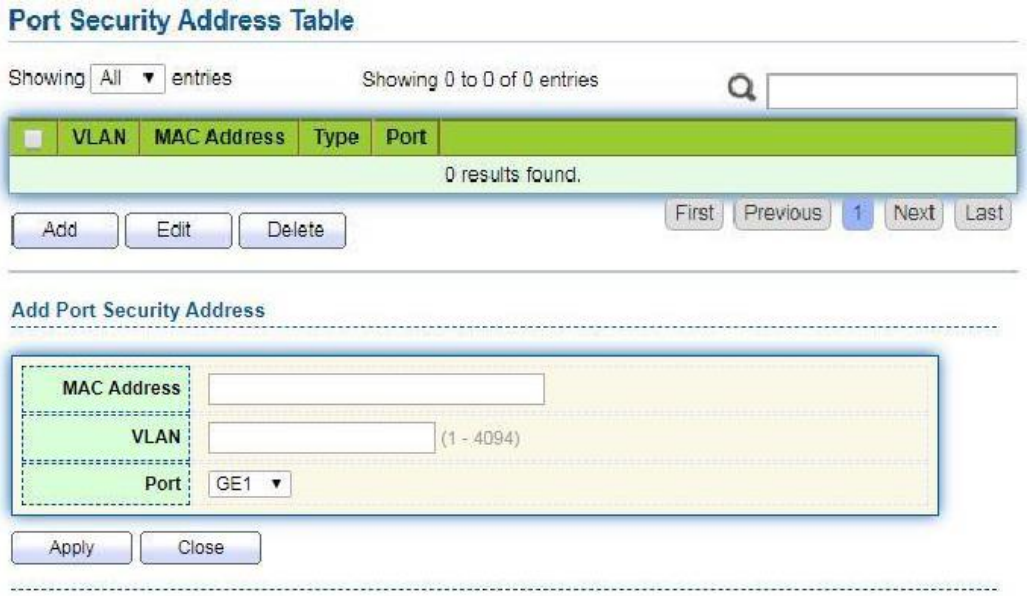
Elementos de configuración	Descripción
Dirección MAC	Dirección MAC a ser filtrada
VLAN	VLAN de la dirección MAC

8.4 Dirección de Seguridad del Puerto

Si la dirección MAC está configurada para proteger Mac, el puerto solo permite que las tramas de datos de la Mac segura pasen para siempre, y los demás se descartarán

Instrucciones:

1. Haga clic en "MAC Address Table > Port Security Address, como se indica:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
MAC Address	Dirección MAC de seguridad
VLAN	VLAN de la dirección MAC
Port	ID del Puerto que habilita la Seguridad del puerto

9 Árbol de Expansión

Los enlaces redundantes se utilizan a menudo para el respaldo de enlaces y la confiabilidad de la red en la red de conmutación Ethernet. Sin embargo, dichos enlaces generarán bucles en la red de conmutación, lo que provocará una tormenta de transmisión, una lista de direcciones MAC inestable y otras fallas, lo que empeorará la calidad de la comunicación de los usuarios o incluso interrumpirá la comunicación. Como resultado, aparece STP (Protocolo de árbol de expansión). Lo mismo ocurre con el desarrollo de otros protocolos, desde el STP original definido en IEEE 802.1D, hasta RSTP (Protocolo de árbol de expansión rápida) definido en IEEE 802.1W y MSTP (Protocolo de árbol de expansión múltiple) definido en IEEE 802.1S, STP continúa actualizándose.

MSTP es compatible con RSTP y STP, mientras que RSTP es compatible con STP. El contraste entre estos tres protocolos se muestra en la tabla siguiente:

Stp	Característica	Aplicar esto
STP	Un árbol libre de bucles como solución a tormentas de difusión y copias de seguridad redundantes. Converge lentamente.	Todas las VLAN se pueden compartir sin discriminación en el usuario o el flujo comercial.
RSTP	Un árbol libre de bucles como solución a tormentas de difusión y copias de seguridad redundantes. Converge rápidamente.	
MSTP	Un árbol libre de bucles como solución a tormentas de difusión y copias de seguridad redundantes. Converge rápidamente. Los árboles de expansión equilibran la carga entre las VLAN. Flujo de diferentes Las VLAN se reenviarán sujetas a las rutas.	Distingue el flujo de usuario y de negocio para compartir la carga. Diferentes VLAN reenvían el flujo a través de árboles de expansión separados.

- Después de implementar STP, se pueden lograr los siguientes objetivos mediante el cálculo de los bucles con topología:
- Eliminación de bucles: elimina posibles bucles de comunicación bloqueando enlaces redundantes.
- Copias de seguridad de enlaces: active enlaces redundantes para restaurar la conectividad de la red si falla la ruta activa.

9.1 Propiedad

Configure los parámetros globales de STP. En un entorno de red específico, los parámetros STP de algunos dispositivos deben ajustarse para lograr el mejor rendimiento.

Instrucciones:

1. Haga click en “Spanning Tree > Property” en el menú de navegación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
State	Está marcado de forma predeterminada para habilitar el árbol de expansión en nombre de los conmutadores.
Operation Mode	Hay 3 modos disponibles, a saber, STP, RSTP y MSTP.
Path Cost	En modo Largo y modo Corto
BPDU Handling	El método para manejar los mensajes BPDU recibidos por el dispositivo
Priority	Prioridad del Puerto
Hello Time	Intervalos entre mensajes “Hola”
Max Age	Tiempo máximo de envejecimiento
Forward Delay	Tiempo de retraso de reenvío
Tx Hold Count	Especifica el Tx-hold-count utilizado para limitar el número máximo de paquetes de transmisión por segundo
Region Name	Nombre de dominio MST. La placa maestra del conmutador establece la dirección MAC de forma predeterminada. Junto con la tabla de asignación de VLAN del dominio MST y el nivel de revisión de MSTP, el nombre de dominio del conmutador determinará conjuntamente el dominio al que pertenece.
Revision	El número de revisión MSTP
Max Hop	Especifica el número de saltos en una región MSTP antes de que se descarte la BPDU

2. Completa los elementos de configuración correspondientes.
3. Presiona “Apply” y Finish.

9.2 Configuración de Puerto

En un entorno de red específico, los parámetros STP de algunos dispositivos deben ajustarse para obtener el mejor rendimiento.

1. Haga clic en “Spanning Tree > Port Setting” en el menú de navegación, seleccione el puerto y “Editar” para configurar sus atributos:

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
3	GE3	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-3	200000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	200000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-7	200000

Edit Port Setting

Port	GE1
State	Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Edge Port	Enable
BPDU Filter	Enable
BPDU Guard	Enable
Point-to-Point	Auto / Enable / Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

Apply Close

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	El número de Puerto para configurar los atributos
State	Habilitar el STP o no.
Path Cost	Ingrese el valor del costo de la ruta de la interfaz Use el estándar IEEE 802.1t con un valor que va de 0 a 200,000,000
Priority	Seleccione la prioridad del puerto con un valor más pequeño que represente una prioridad más alta. La prioridad de la interfaz afecta la función de la interfaz en el MSTI especificado. En diferentes MSTI, los usuarios pueden configurar las prioridades para una misma interfaz. Como resultado, el flujo de diferentes VLAN se puede reenviar a lo largo de enlaces físicos para lograr compartir la carga de VLAN. Descripción: MSTP recalculará el rol de la interfaz y migrará su estado cuando cambie su prioridad.
Edge Port	En lugar de otro switch o segmento de red, el puerto perimetral debe conectarse directamente a los terminales de usuario. Puede pasar rápidamente al estado directo ya que los cambios de topología no crean bucles. Un puerto perimetral en configuración puede pasar rápidamente al estado de reenvío mediante STP. Para lograr esto, se recomienda que los puertos Ethernet conectados directamente a los terminales de usuario se configuren como puertos de borde.
BPDU Filter	Habilite el filtro BPDU en el cuadro
BPDU Guard	Habilitar la protección de BPDU o no. Desmarcado por defecto. Si BPDU Guard está habilitado, el dispositivo apagará las interfaces que reciben BPDU y notificará al NMS. Dichas interfaces solo pueden restaurarse manualmente por administradores de red
Point-to-Point	Selecciona los modos activado, apagado y automático. Modo automático: indica el estado de conexión entre la inspección automática predeterminada y los enlaces punto a punto. Modo habilitado: indica que el puerto específico está conectado a los enlaces punto a punto. Modo apagado: indica que el puerto específico no logra conectar los enlaces punto a punto.

2. Completa los elementos de configuración correspondientes.
3. Presiona “Apply” y Finish.

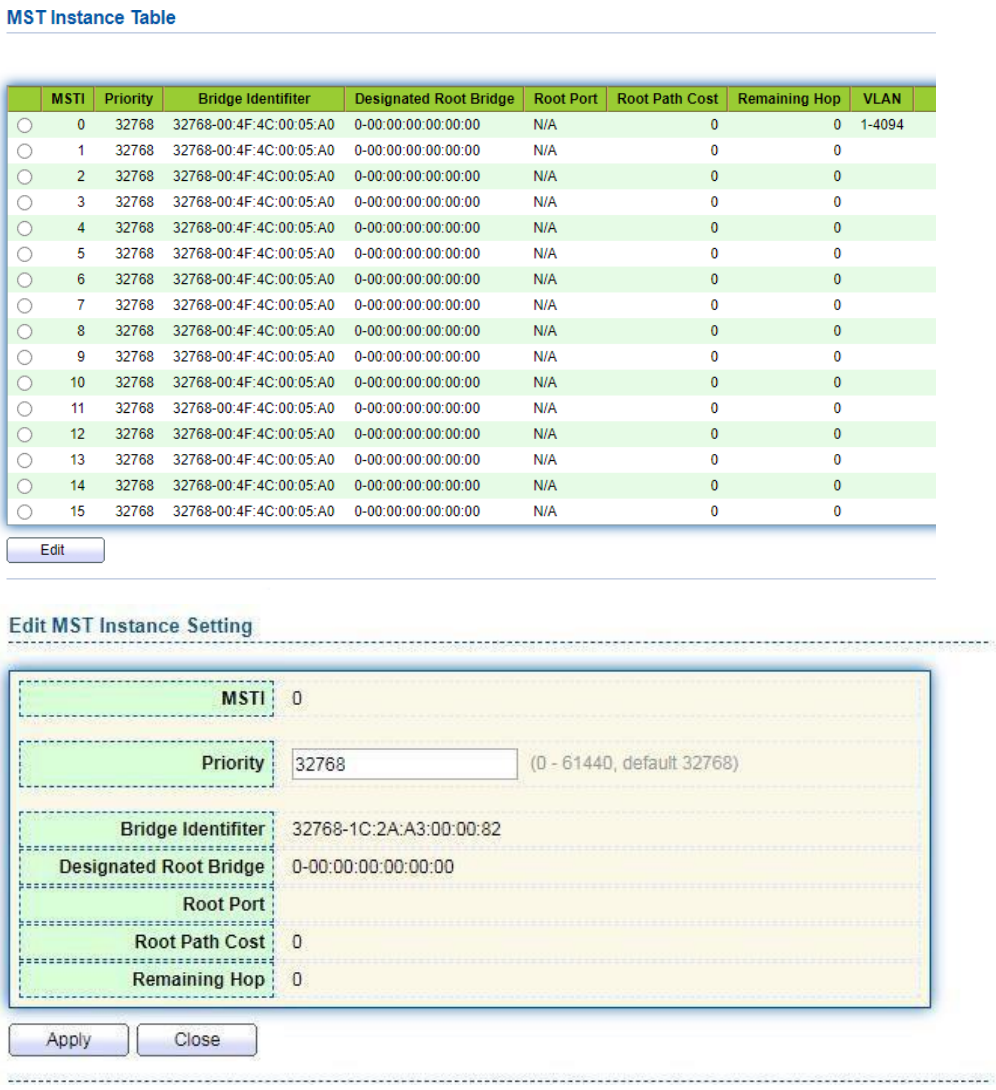
9.3 Instancias MST

MSTP divide una red de conmutación en múltiples dominios, con árboles de expansión independientes formados dentro de cada dominio. Cada árbol de expansión se denomina MSTI (instancia de árbol de expansión múltiple), y cada dominio se denomina Región MST: Región de árbol de expansión múltiple).

Descripción:
Una instancia es un grupo de VLAN que reduce el costo de comunicación y la tasa de utilización de recursos. Cada instancia, calculada de forma independiente con topología, puede equilibrar la carga. Las VLAN con la misma topología se pueden asignar a una misma instancia y se reenvían según el estado del puerto en las instancias de MSTP correspondientes.
En términos simples, asignados a la instancia de MST especificada, una o más VLAN se distribuyen a un árbol de expansión a la vez.

Instrucciones:

1. Haga clic en “Spanning Tree > MST Instance” en el menú de navegación, “Editar” las instancias de spanning tree seleccionadas para configurarlas de la siguiente manera: MSTP divide una red de conmutación en múltiples dominios, con árboles de expansión independientes formados dentro de cada dominio. Cada árbol de expansión se denomina MSTI (instancia de árbol de expansión múltiple), y cada dominio se denomina
2. Región MST: Región de árbol de expansión múltiple). Descripción:
3. Una instancia es un grupo de VLAN que reduce el costo de comunicación y la tasa de utilización de recursos. Cada instancia, calculada de forma independiente con topología, puede equilibrar la carga. Las VLAN con la misma topología se pueden asignar a una misma instancia y se reenvían según el estado del puerto en las instancias de MSTP correspondientes.
4. En términos simples, los asignados a la instancia de MST especificados, una o más VLAN se distribuyen a un árbol de expansión a la vez.
5. Instrucciones:
6. 6. 1. Haga clic en “Spanning Tree > MST Instance” en el menú de navegación, “Editar” las instancias de spanning tree seleccionadas para configurarlas de la siguiente manera:



Los campos de la interfaz son como a continuación.

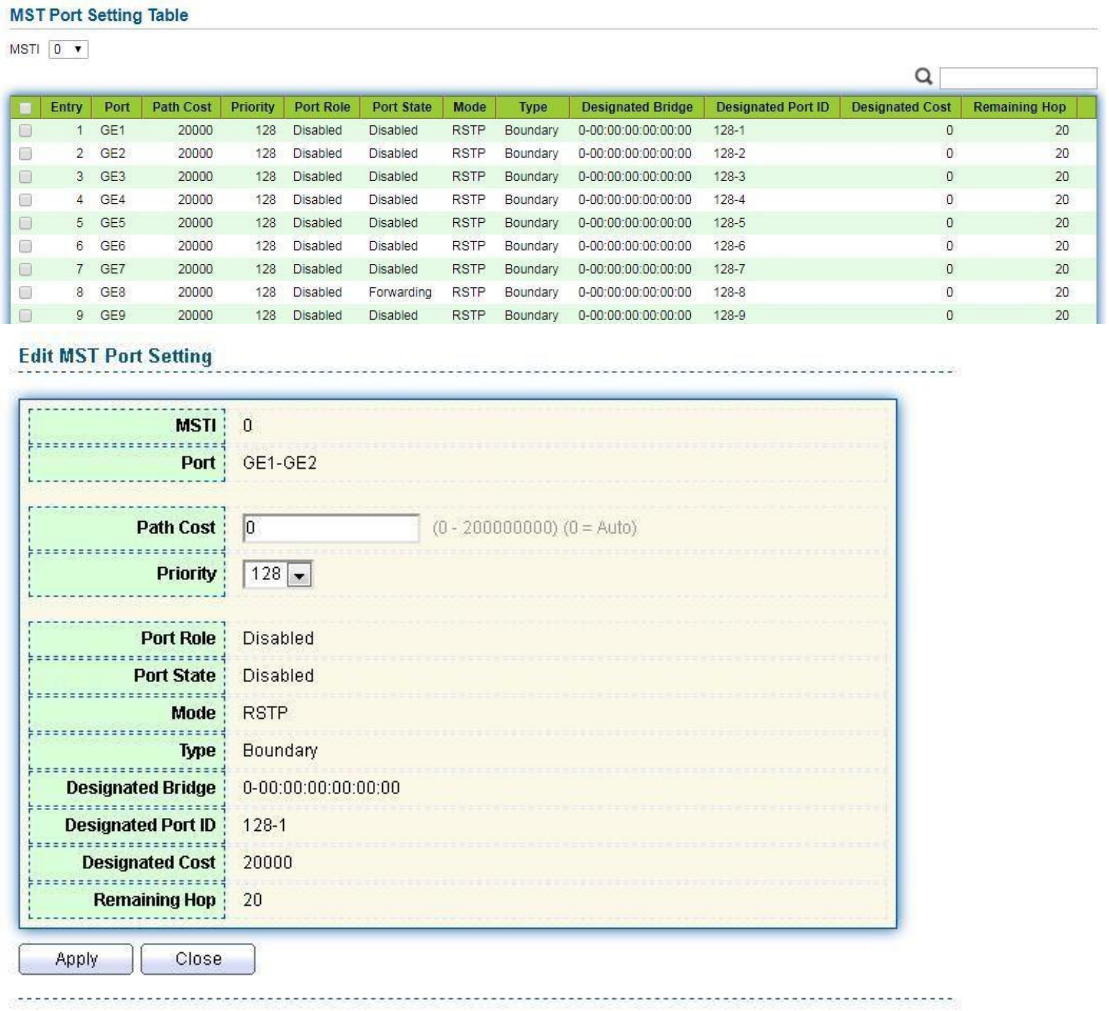
Elementos de configuración	Descripción
MSTI	El número de instancias de árboles de expansión oscila entre 0 y 15
VLAN	Número de VLAN asignado desde instancias
Priority	Establezca la prioridad de un múltiplo de 4096 para la instancia especificada, que va de 0 a 65 535 con 32 768 como valor predeterminado.

7. Completa los elementos de configuración correspondientes.
8. Presiona “Apply” y Finish, como se indica.

9.4 Configuración del puerto MST

Instrucciones:

1. Haga clic en "Spanning Tree > MST Port Setting” en el menú de navegación, verifique el puerto a modificar de la lista de todos los puertos del dispositivo, "Editar" para ingresar a la interfaz de configuración detallada de la siguiente manera:



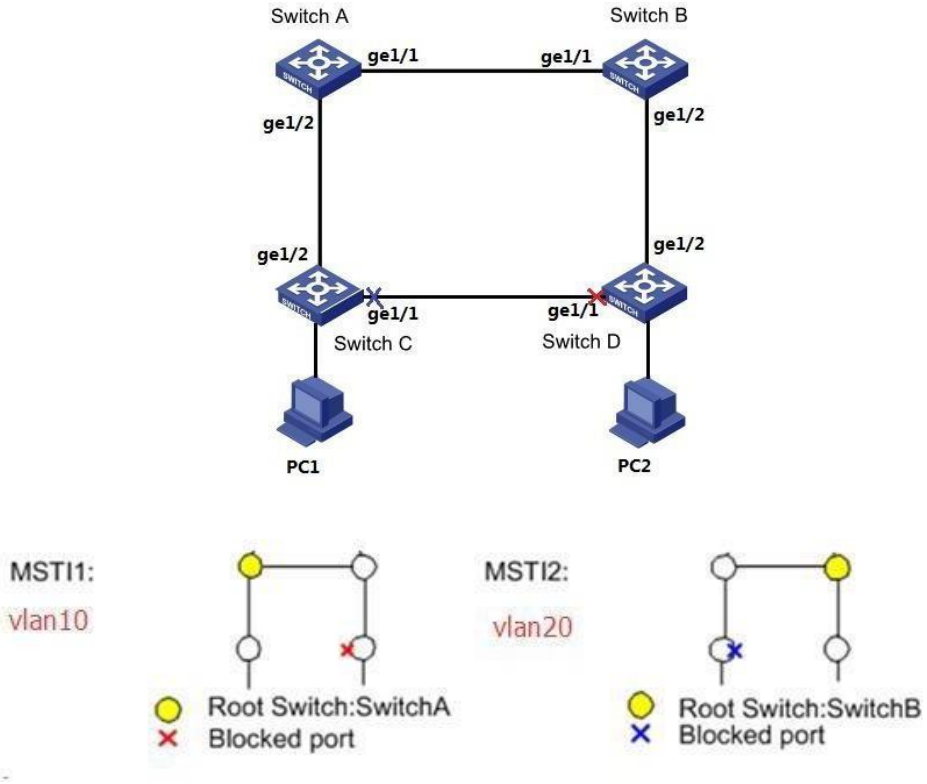
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
MSTI	Seleccione la instancia para la configuración a través del cuadro desplegable en la parte superior izquierda.
Port	Seleccione el puerto que configurarán los usuarios
Path Cost	Introduzca el valor de costo de ruta de acceso de la interfaz Utilice el estándar IEEE 802.1t con un valor comprendido entre 0 y 200.000.000
Priority	Seleccione la prioridad del puerto con un valor menor que represente una prioridad más alta. La prioridad de la interfaz afecta a la función de la interfaz en el MSTI especificado. En diferentes MSTI, los usuarios pueden configurar las prioridades para una misma interfaz. Como resultado, el flujo de diferentes VLAN se puede reenviar a lo largo de enlaces físicos para lograr el uso compartido de la carga de VLAN. Descripción: MSTP volverá a calcular el rol de interfaz y migrará su estado cuando cambie su prioridad.
Port Role	3 tipos de puertos raíz, a saber, puerto especificado, puerto de respaldo y puerto deshabilitado.
Port State	Incluyendo 3 estados, a saber, Descarte, Reenvío y Desactivado
Mode	Modo STP actual
Type	Los tipos de puerto de la instancia contienen puertos internos y de límite

2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y finalizar.

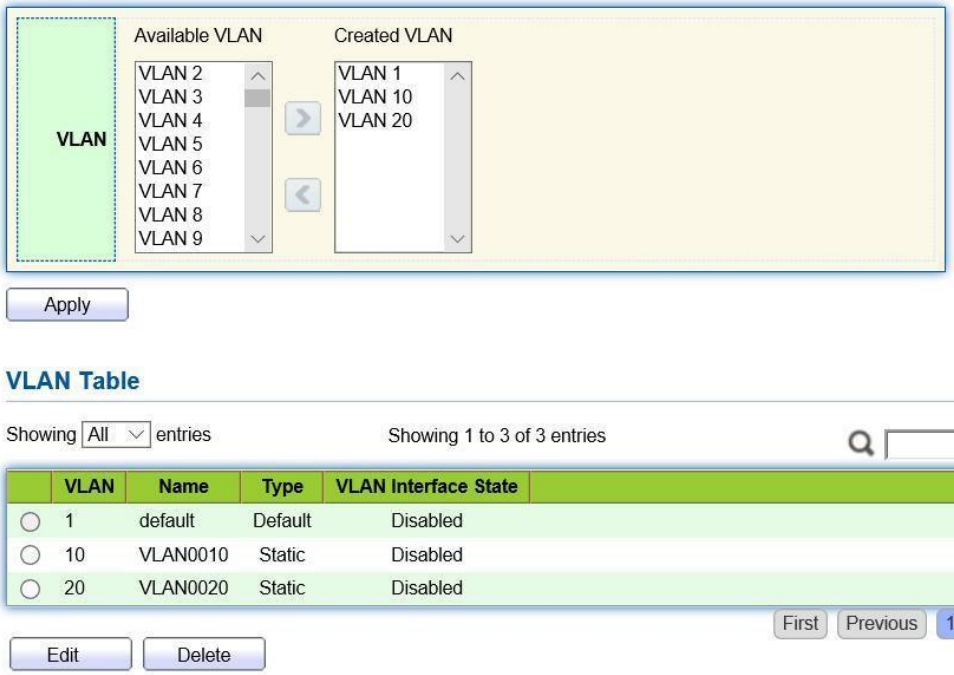
Ejemplo de configuración de la función MSTP:

Los conmutadores A, B, C y D ejecutan MSTP, que introduce instancias para compartir la carga de VLAN10 y 20. MSTP puede configurar la tabla de asignación de VLAN para asociar VLAN con instancias de árbol de expansión y para asignar VLAN10 desde la instancia 1 y VLAN20 desde la instancia 2.

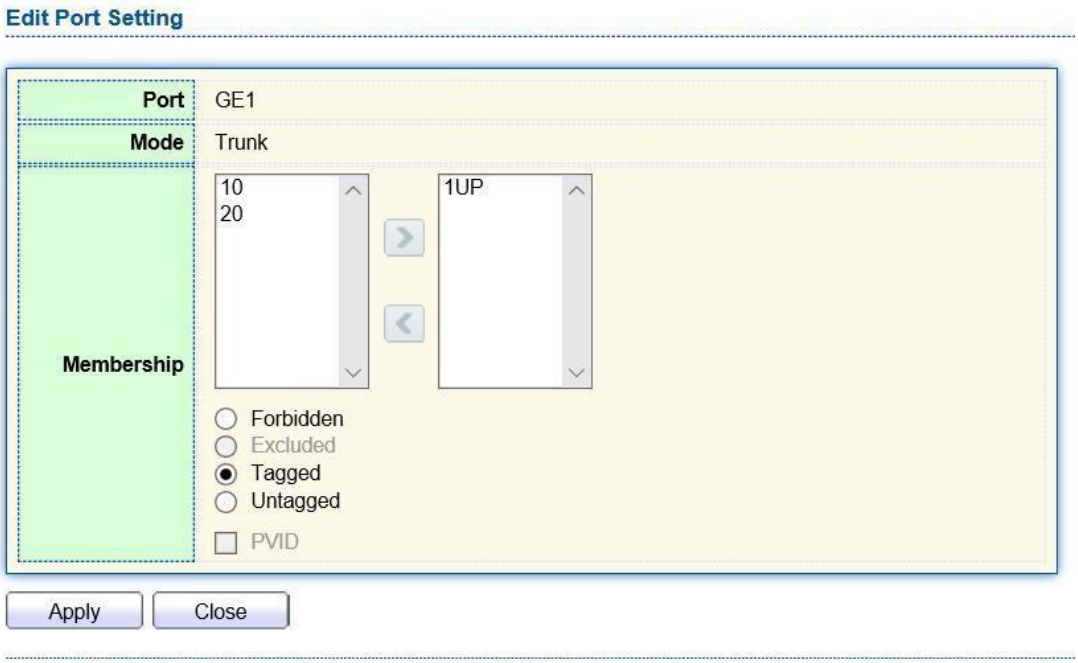


Instrucciones:

1. Los conmutadores A, B, C y D crean VLAN10 y 20 para configurar la función de reenvío L2 de los dispositivos en el anillo. Haga clic en "VLAN > VLAN > Create VLAN" en el menú de navegación, rellene las configuraciones correspondientes. "Aplicar" y terminar de la siguiente manera.



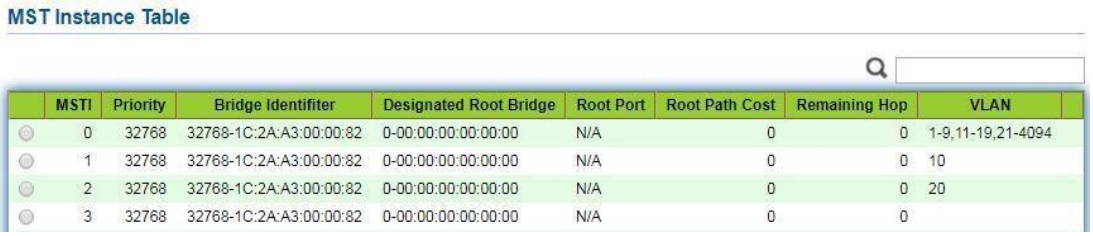
2. Las VLAN se agregan a los bucles de entrada de los puertos del switch. Haga clic en "VLAN > VLAN > Membership" en el menú de navegación, seleccione el puerto de anillo a configurar, mueva VLAN10 y 20 a la casilla derecha y márquelos con "Etiquetado". "Aplicar" y finalizar:



3. Haga clic en "Spanning Tree > Property" en el menú de navegación, y elija el modo MSTP de la siguiente manera:

4. Configure la asignación de VLAN entre las instancias MSTI1 y MSTI2. Haga clic en "Spanning Tree > MST Instance" para rellenar los parámetros correspondientes y "Add"

   de la siguiente manera:



Nota:

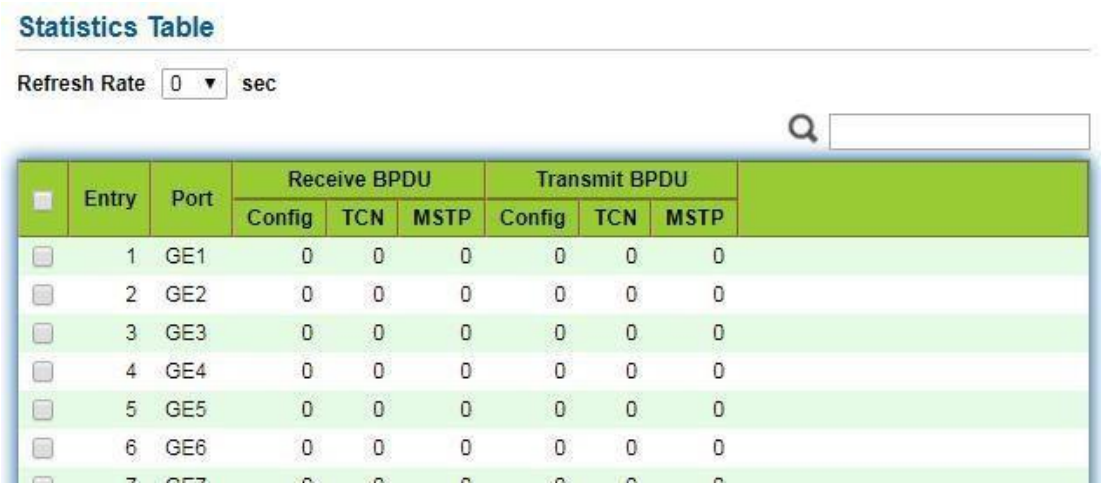
- Establezca la prioridad de MSTI1 en 0 y MSTI2 en 4.096 antes de configurar el conmutador A.
- Establezca la prioridad de MSTI1 en 4.096 y MSTI2 en 0 antes de configurar el conmutador B.
- La prioridad debe ser un múltiplo de 4.096.

5. El conmutador B sirve como puente raíz de MSTI2 y puente raíz de copia de seguridad de MSTI1 en el dominio. Consulte 5 para obtener instrucciones.
6. La red en forma de árbol eliminará los bucles.

9.5 Estadística

Instrucciones:

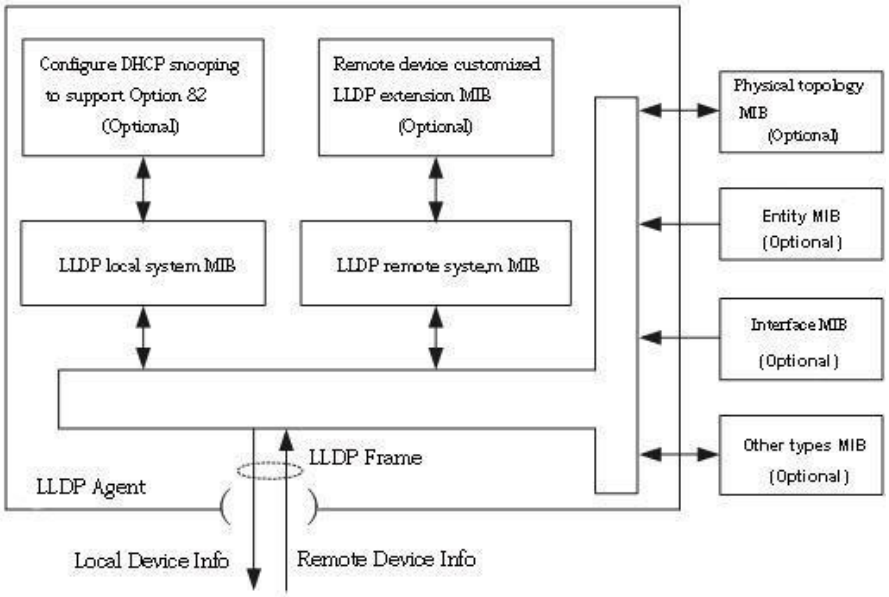
1. Haga clic en "Spanning Tree > Statistics" en el menú de navegación, estadísticas del puerto de entrada de la siguiente manera:



10 Descubrimiento

LLDP (Link Layer Discovery Protocol) se define en IEEE 802.1ab. Es un método de descubrimiento L2 estándar que integra la información como direcciones de administración, identificaciones de dispositivos e interfaces de dispositivos de red local y transmite a los dispositivos vecinos. Después de recibir la información, la guardarán en forma de MIB estándar (Base de información de gestión) para la consulta NMS y el juicio de comunicación de enlaces.

También puede integrar la información y transmitir a sus propios dispositivos remotos. La información recibida por el dispositivo de red local se mantendrá en forma de MIB. A continuación se muestra cómo funciona. Diagrama de bloques de los principios LLDP



LLDP se realiza en base a:

- El módulo LLDP actualiza su sistema local MIB, así como la extensión personalizada MIB, a través de la interacción entre el agente LLDP y MIBs de topología física, entidad, interfaz y otros tipos.
- Encapsule la información del dispositivo de red local en tramas LLDP y transmita al dispositivo remoto.
- Reciba la trama LLDP enviada por el dispositivo remoto para actualizar la MIB del sistema remoto LLDP y la MIB de extensión personalizada.
- Domine la información del dispositivo remoto, como la interfaz de conexión y la dirección MAC, a través de la función de transmisión y recepción del agente LLDP.

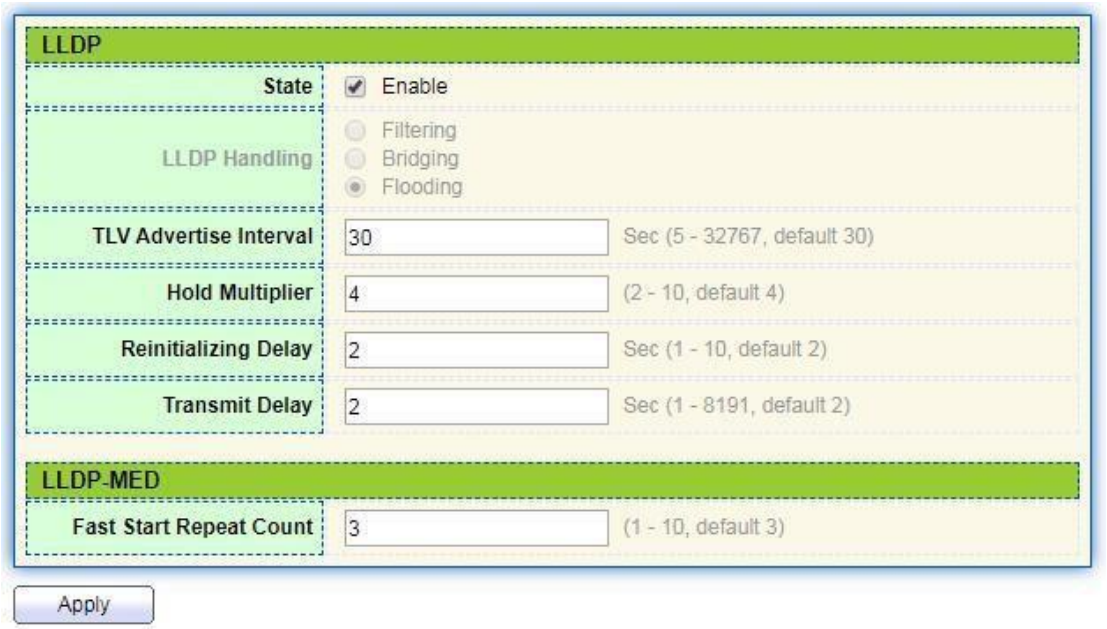
- La MIB del sistema local almacena información del dispositivo local, incluidos los ID de dispositivo e interfaz, el nombre y la descripción del sistema, la descripción de la interfaz, la dirección de administración de la red, etc.
- La MIB del sistema remoto almacena información del dispositivo local, incluidos los ID de dispositivo e interfaz, el nombre y la descripción del sistema, la descripción de la interfaz, la dirección de administración de red, etc.

Basado en **LLDP**, **LLDP-MED** permite que otras unidades se expandan. La información verificada por los dispositivos de red facilita el análisis de fallas y profundiza la comprensión precisa de la topología de red por parte del sistema de gestión.

10.1 LLDP

Instrucciones:

1. Haga click en “Discovery > LLDP > Property” en el menú de navegación.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
State	Habilitar o deshabilitar el LLDP
LLDP Handling	Los mensajes LLDP se procesarán mediante "Filtrado", "Puente" e "Inundación" al deshabilitar el LLDP.
TLV Advertise Interval	30s por defecto van de 5 a 32.768s.
Hold Multiplier	El período de transmisión del producto con 4 por defecto varía de 2 a 10. Período de transmisión * el producto no debe ser superior a 65.535.
Reinitializing Delay	2s por defecto van de:1 a 10s.
Transmit Delay	2s por defecto van de:1 a 8.191s.
Fast Start Repeat Count	3s por defecto del puerto LLDP-MED que van de 1 a 10s.

Los mensajes Ethernet encapsulados con LLDPDU (unidad de datos LLDP) se reconocen como mensaje LLDP. Cada TLV es una unidad de LLDPDU transportada con información especificada.

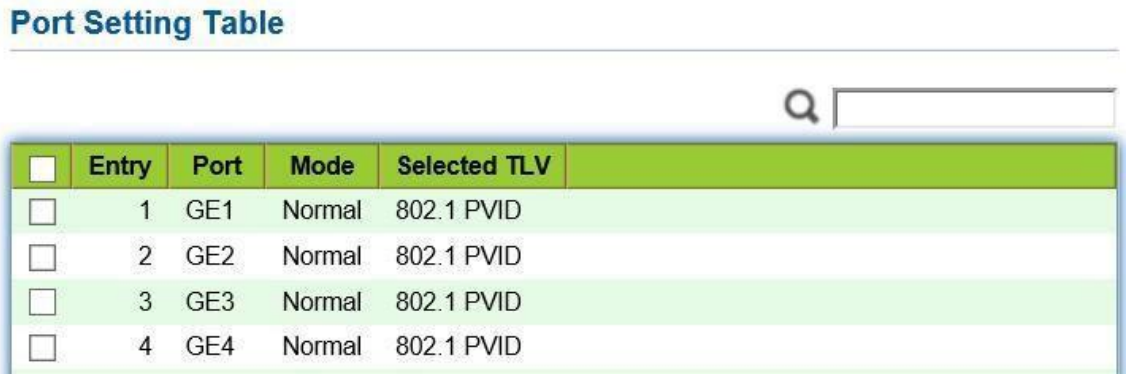
2. Completa los elementos de configuración correspondientes.

3. "Aplicar" y terminar.

10.2 Configuración del puerto

Instrucciones

1. Haga click en “Discovery > LLDP > Port Setting” en el menú de navegación as follows.

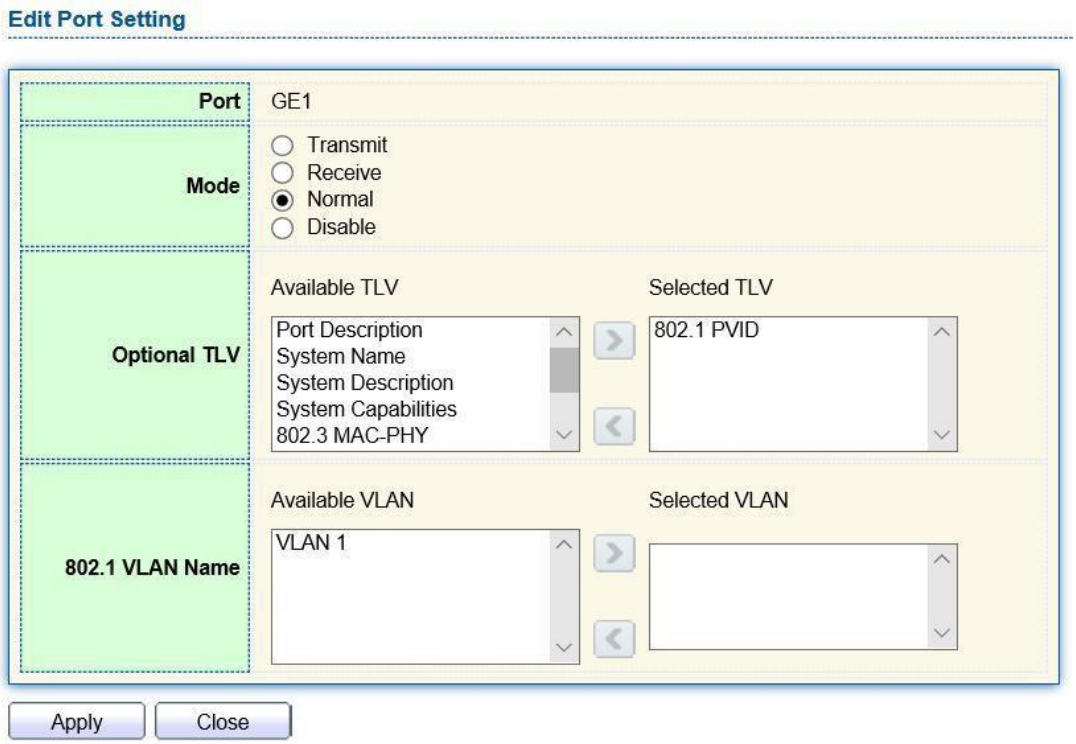


Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	Lista de puertos
Mode	El modo LLDP incluye: Transmitir, Recibir, Normal, Deshabilitar, el valor predeterminado es Normal Transmitir: transmitir mensajes LLDP solamente; Recibir: recibir mensajes LLDP solamente; Normal: transmitir y recibir mensajes LLDP; Desactivar: no transmitir ni recibir mensajes LLDP.
Selected TLV	Información de TLV y VLAN seleccionadas

LLDP puede funcionar en 4 patrones: Transmitir: transmitir mensajes LLDP solamente; Recibir: recibir mensajes LLDP solamente; Normal: transmitir y recibir mensajes LLDP; Desactivar: no transmitir ni recibir mensajes LLDP.

2. Compruebe el puerto correspondiente y "Editar" la configuración del puerto. "Aplicar" y terminar de la siguiente manera.



Los campos de la interfaz son como a continuación.

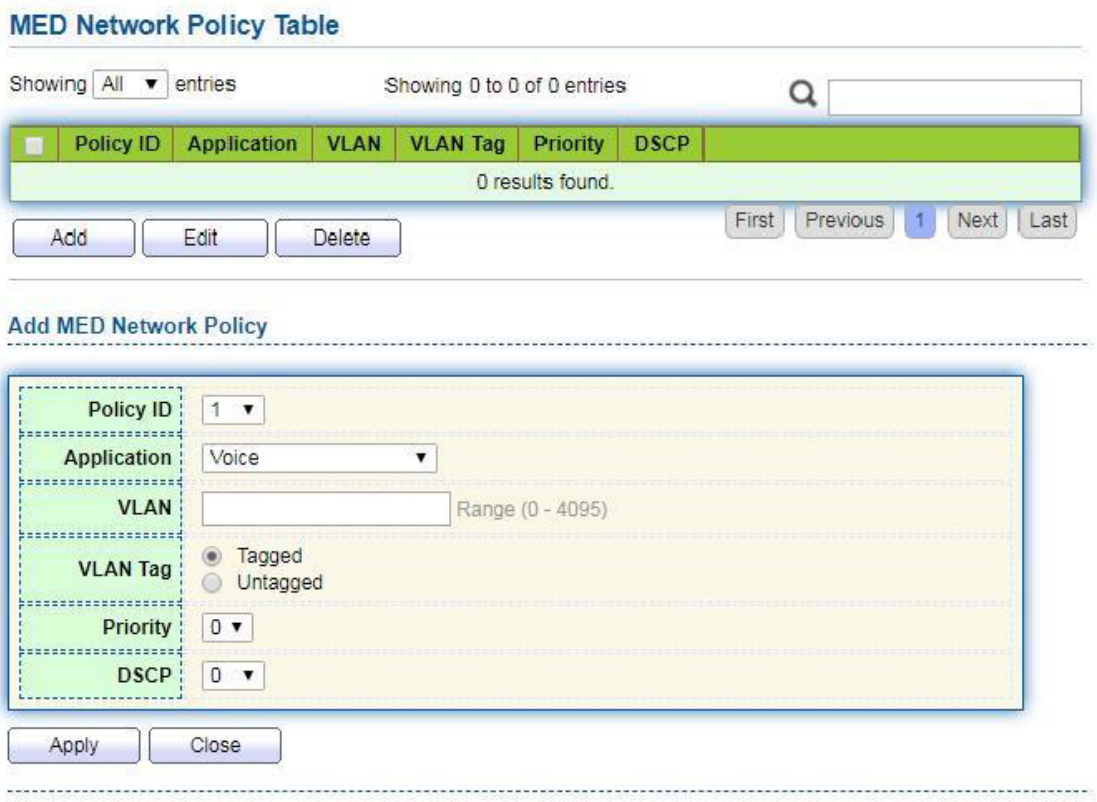
Elementos de configuración	Descripción
Port	Lista de puertos
Mode	El modo LLDP incluye: Transmitir, Recibir, Normal, Deshabilitar, el valor predeterminado es Normal Transmitir: transmitir mensajes LLDP solamente; Recibir: recibir mensajes LLDP solamente; Normal: transmitir y recibir mensajes LLDP; Desactivar: no transmitir ni recibir mensajes LLDP.
Optional TLV	Seleccione la información de TLV y VLAN
802.1 VLAN Name	Seleccione el nombre de VLAN

10.3 Política de red MED

MED se basa en IEEE 802.1ab. LLDP es el protocolo de descubrimiento de vecinos de IEEE, que puede ser extendido por otras organizaciones. La información identificada a partir de dispositivos de red, como conmutadores y puntos de acceso inalámbricos, puede ayudar con el análisis de fallas y permitir que los sistemas de administración comprendan con precisión la topología de la red.

Instrucciones

1. Haga click en “Discovery > LLDP > MED Network Policy” en el menú de navegación.



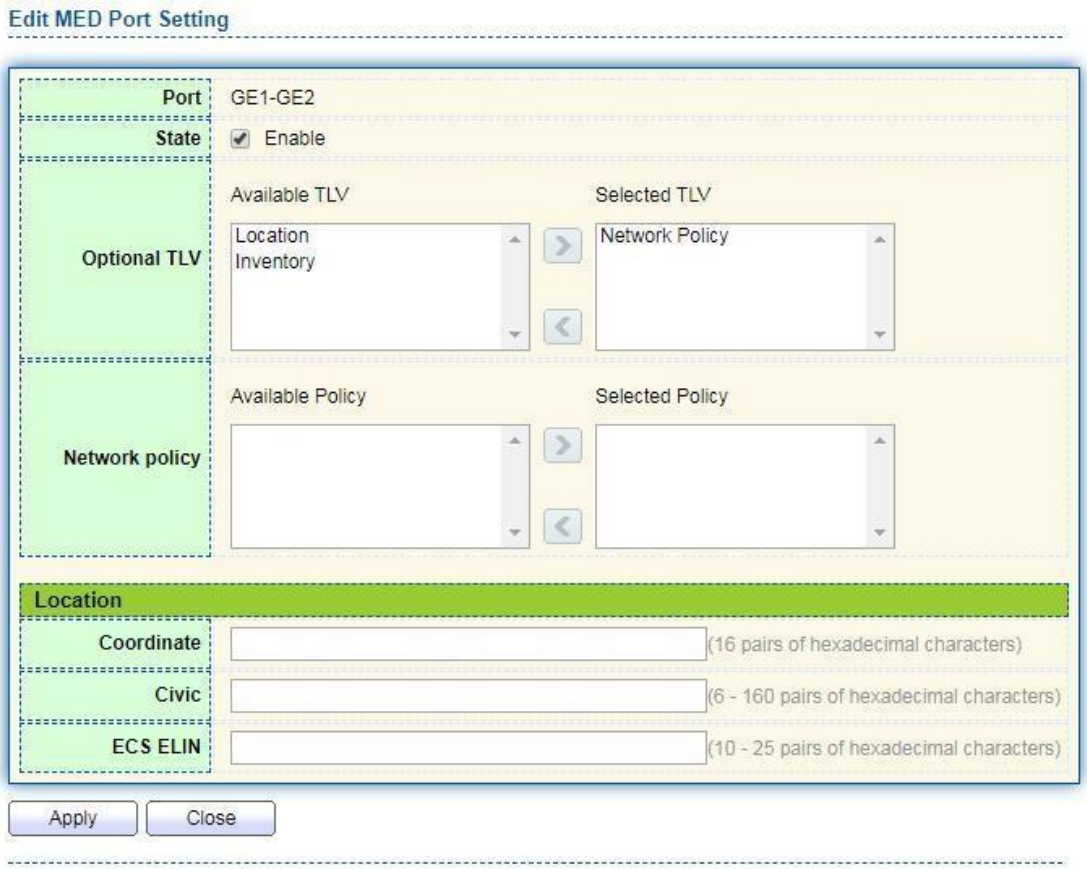
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Policy ID	Número de identificación de póliza
Application	Configurar y publicar TLV de directiva de red
VLAN	Número de VLAN
VLAN Tag	Modo VLAN, opcional etiquetado o sin etiquetar
Priority	CoS para servicios
DSCP	DSCP para servicios

10.4 Configuración del puerto MED

Instrucciones

1. Haga click en “Discovery > LLDP > MED Port Setting” en el menú de navegación.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Entry	Nº de serie de la configuración del puerto MED
Port	Lista de puertos
State	Estado de habilitación de puerto
Network Policy	Configurar y publicar TLV de directiva de red
Location	Configurar y publicar TLV de ubicación
Inventory	Configurar y publicar TLV de inventario

10.5 Vista de paquetes

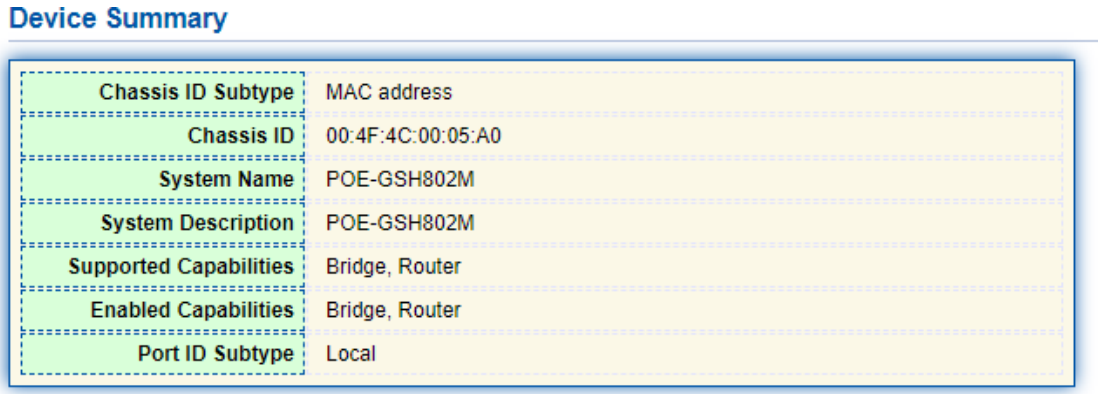
Instrucciones

1. Haga click en “Discovery > LLDP > Packet View” en el menú de navegación.

10.6 Información local

Instrucciones para el resumen del dispositivo:

1. Haga click en “Discovery > LLDP > Local Information” en el menú de navegación.



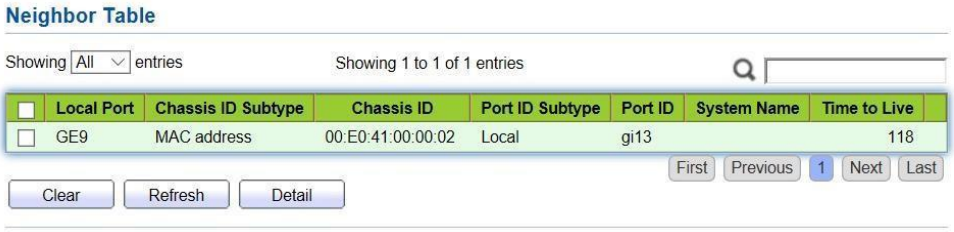
Instrucciones para la tabla de estado del puerto:

2. Haga click en “Discovery > LLDP > Local Information” en el menú de navegación.

10.7 Vecino

Instrucciones para la visualización de vecinos LLDP.

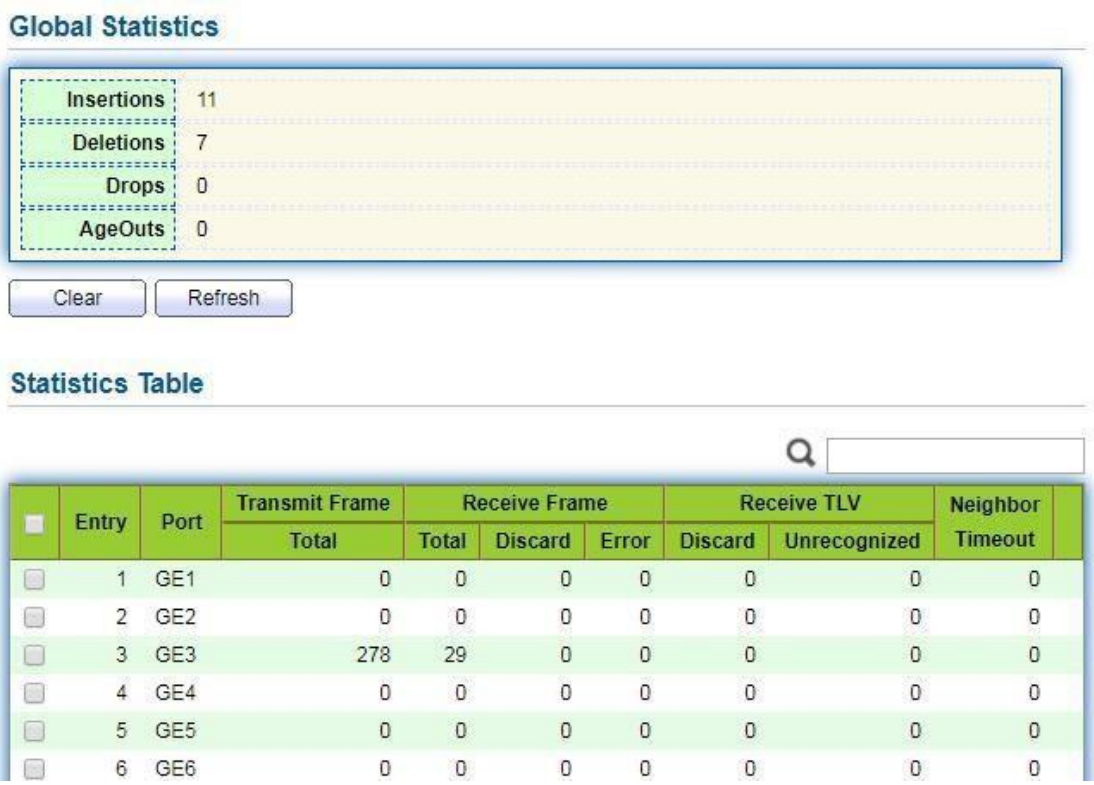
1. Haga click en “Discovery > LLDP > Neighbor” en el menú de navegación as.



10.8 Estadística

Instrucciones:

1. Haga click en “Discovery > LLDP > Statistics” en el menú de navegación.



11 DHCP

Breve introducción al servidor DHCP

Con la expansión de la escala de red y la mejora de la complejidad de la red, la configuración de la red se está volviendo cada vez más compleja. La ubicación de la computadora cambia (como una computadora portátil o una red inalámbrica) y el número de computadoras excede la dirección IP que se puede asignar. El Protocolo de configuración dinámica de host (DHCP) se desarrolla para cumplir estos requisitos. El protocolo DHCP funciona en el modo cliente/servidor. El cliente DHCP solicita la información de configuración del servidor DHCP dinámicamente y el servidor DHCP devuelve la información de configuración correspondiente según la directiva.

En una aplicación típica de DHCP, generalmente incluye un servidor DHCP y varios clientes (como PC y portátil), como se muestra en la Figura 1-1.

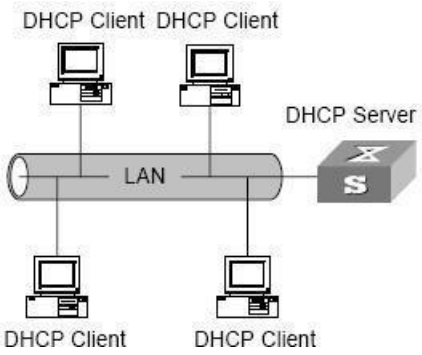


Figura 1-1. En una aplicación típica de DHCP

Asignación de direcciones IP de DHCP

Estrategia de asignación de direcciones IP

De acuerdo con las diferentes necesidades de los clientes, DHCP proporciona tres estrategias de asignación de direcciones IP.

- Asignación manual de direcciones: el administrador vincula la dirección IP fija para algunos clientes específicos (como el servidor WWW). Envíe la dirección IP fija configurada al cliente a través de DHCP.
- Asignación automática de direcciones: DHCP asigna direcciones IP con plazo de concesión ilimitado a los clientes.
- Asignación dinámica de direcciones: DHCP asigna una dirección IP con un período válido al cliente, y el cliente debe volver a solicitar la dirección después de la expiración de la vida útil. La mayoría de los clientes obtienen esta alineación dinámica de direcciones.

10.2.2 Proceso de adquisición de direcciones IP dinámicas

El proceso de interacción de mensajes entre el cliente DHCP y el servidor DHCP se muestra en la figura 2-1.

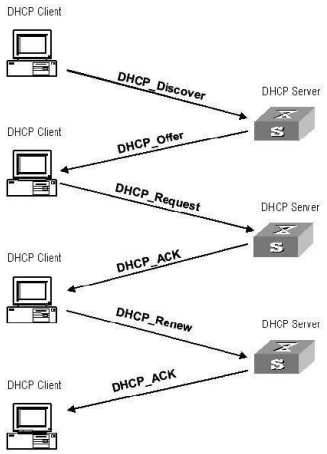


Figura 2-1. Proceso de interacción

Para obtener la dirección IP dinámica legal, el cliente DHCP interactúa con información diferente con el servidor en diferentes etapas. Generalmente, hay tres modos de la siguiente manera:

(1) El cliente DHCP inicia sesión en la red por primera vez

Cuando el cliente DHCP inicia sesión en la red por primera vez, establece contacto principalmente con el servidor DHCP a través de cuatro etapas.

- La fase de descubrimiento: la etapa en la que el cliente DHCP busca el servidor DHCP. El cliente envía el mensaje DHCP discover en modo de difusión, y sólo el servidor DHCP responderá.
- La etapa de proporcionar la dirección IP: es decir, la etapa en la que el servidor DHCP proporciona la dirección IP. Después de recibir el mensaje de detección DHCP del cliente, el servidor DHCP selecciona una dirección IP no asignada del grupo de direcciones IP y la asigna al cliente, y envía el mensaje de oferta DHCP que contiene la dirección IP arrendada y otras configuraciones al cliente.
- La etapa de selección: la etapa en la que el cliente DHCP selecciona la dirección IP. Si más de un servidor DHCP envía un mensaje de oferta DHCP al cliente, el cliente sólo acepta el primer mensaje de oferta DHCP recibido y, a continuación, responde al mensaje de solicitud DHCP difundiendo a cada servidor DHCP. La información contiene el contenido de la dirección IP de solicitud del servidor DHCP seleccionado.
- La etapa de confirmación: la etapa en la que el servidor DHCP confirma la

dirección IP proporcionada. Cuando el servidor DHCP recibe el mensaje de solicitud DHCP respondido por el cliente DHCP, enviará el mensaje de confirmación dhcp-ack que contiene la dirección IP y otras configuraciones proporcionadas por el cliente; de lo contrario, devolverá el dhcp-nak , que indica que la dirección no se puede asignar al cliente. Después de recibir el mensaje de confirmación dhcp-ack devuelto por el servidor, el cliente enviará ARP (la dirección de destino es la dirección a la que está asignado) en modo de difusión para la detección de direcciones. Si no se recibe respuesta dentro del tiempo especificado, el cliente utilizará esta dirección.

(2) El cliente DHCP vuelve a iniciar sesión en la red

Cuando el cliente DHCP vuelve a iniciar sesión en la red, establece contacto principalmente con el servidor DHCP a través de los siguientes pasos.

- Después de que el cliente DHCP inicie sesión correctamente en la red por primera vez y, a continuación, vuelva a iniciar sesión en la red, sólo necesita difundir el mensaje de solicitud DHCP que contiene la dirección IP asignada la última vez, y no es necesario para enviar de nuevo el mensaje de detección DHCP.
- Después de recibir el mensaje de solicitud DHCP, si la dirección solicitada por el cliente no está asignada, se devolverá el mensaje de confirmación dhcp-ack para notificar al cliente DHCP que continúe usando la dirección IP original.
- Si la dirección IP no se puede asignar al cliente DHCP (por ejemplo, seha asignado a otros clientes), el servidor DHCP devolverá un mensaje dhcp-nak. Después de recibir el mensaje, el cliente envía el mensaje de descubrimiento DHCP nuevamente para solicitar una nueva dirección IP.

(3) El cliente DHCP extiende la validez de la concesión de la dirección IP

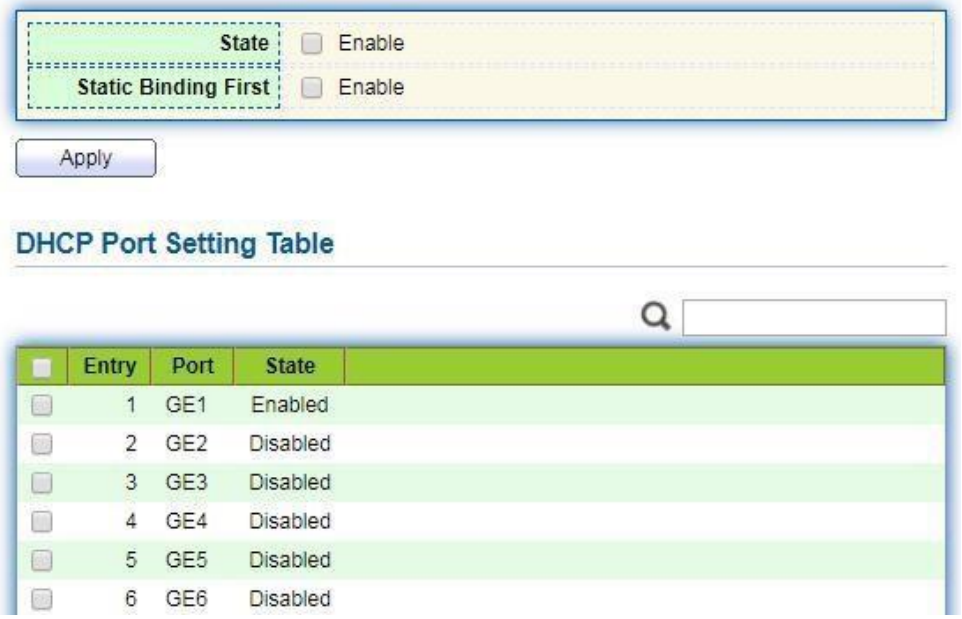
La dirección IP dinámica asignada por el servidor DHCP al cliente suele tener un plazo de concesión determinado. Después de la expiración, el servidor recuperará la dirección IP. Si el cliente DHCP desea seguir utilizando la dirección, es necesario actualizar la concesión de IP.

En la práctica, el cliente DHCP envía un mensaje de solicitud DHCP al servidor DHCP de forma predeterminada cuando el plazo de concesión de la dirección IP llega a la mitad para completar la actualización de la concesión IP. Si la dirección IP es válida, el servidor DHCP responderá al mensaje dhcp-ack para informar al cliente DHCP de que se ha obtenido una nueva concesión.

11.1 Propiedad

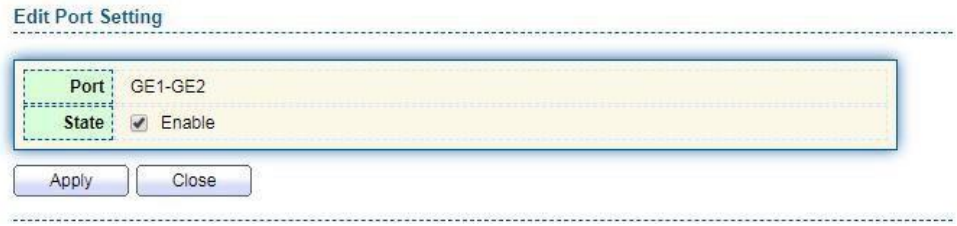
Instrucciones de configuración de enlace global y estático DHCP:

1. Haga click en “DHCP > Property” en el menú de navegación as.



Instrucciones para la configuración del puerto DHCP:

2. Haga clic en "DHCP > Property" y seleccione el puerto y haga clic en "Editar" de la siguiente



manera.

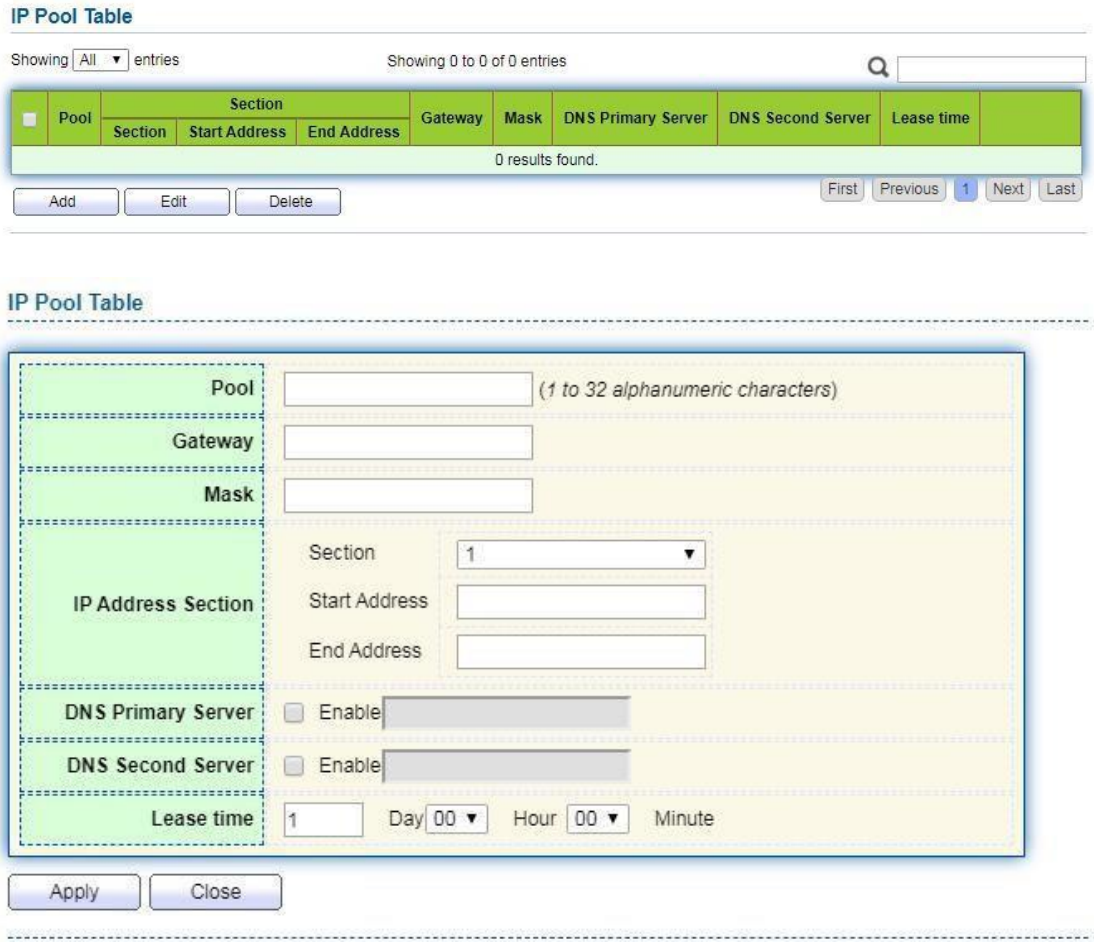
Nota:

Habilite el servidor DHCP o el modo de retransmisión DHCP, el puerto debe habilitar esta función

11.2 Configuración del grupo de direcciones IP

Instrucciones de configuración del grupo de IP DHCP:

1. Haga clic en "DHCP > IP Pool Setting", Haga clic en "Add" para agregar IP pool de la siguiente manera.



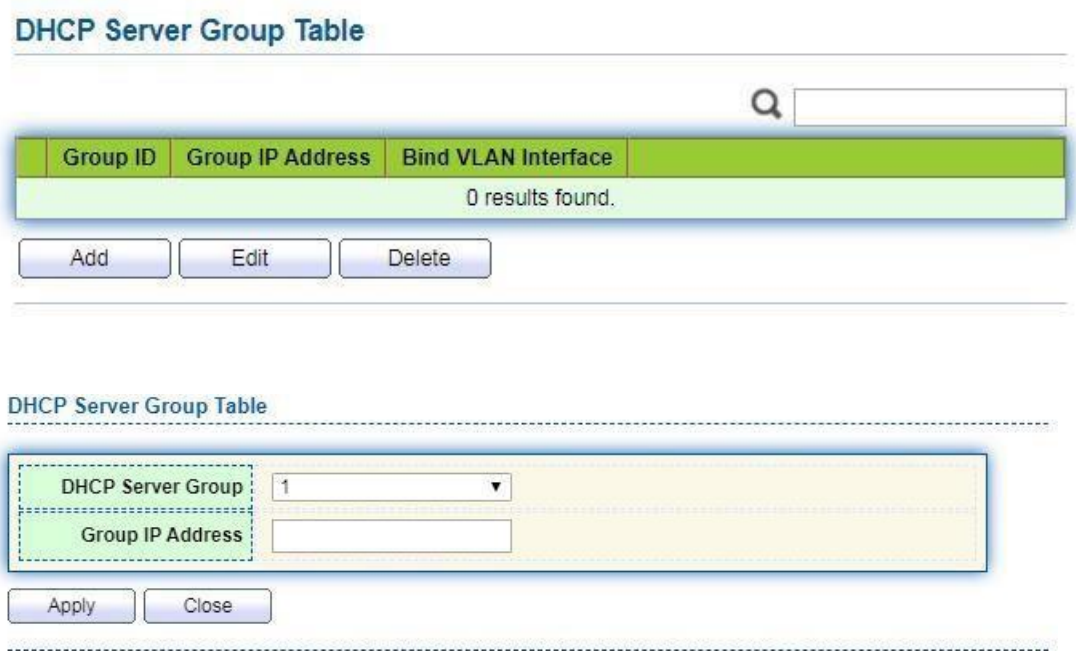
Nota:

La dirección de inicio y la dirección final no se pueden configurar ni contienen una dirección de puerta de enlace.

11.3 Configuración del grupo de direcciones IF de VLAN

Instrucciones de configuración del grupo de servidores:

1. Haga clic en "DHCP > VLAN IF Address Group Setting", ingrese a la tabla de grupos de servidores DHCP y haga clic en "Add" para configurar el grupo de servidores de la siguiente manera.



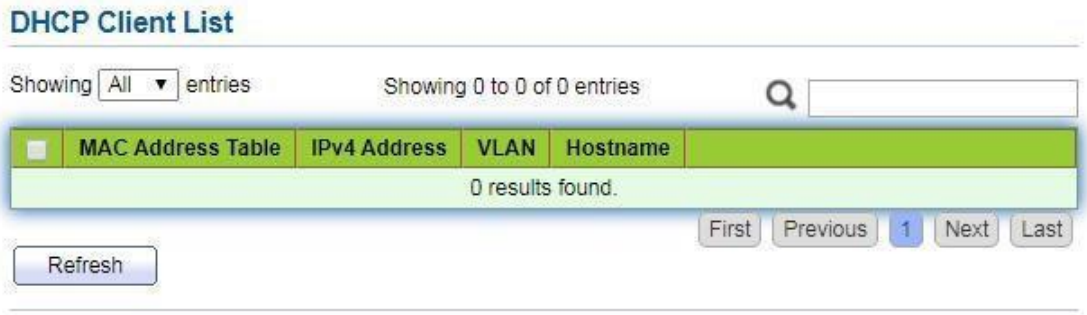
Instrucciones de configuración de enlace de grupo de servidores e interfaz VLAN:

1. Haga clic en "DHCP > VLAN IF Address Group Setting", ingrese a la tabla VLAN Interface Address Pool, seleccione la interfaz y el grupo de servidores, y luego haga clic en "Apply" de la siguiente manera.

11.4 Lista de clientes

Información de la lista de clientes Instrucciones:

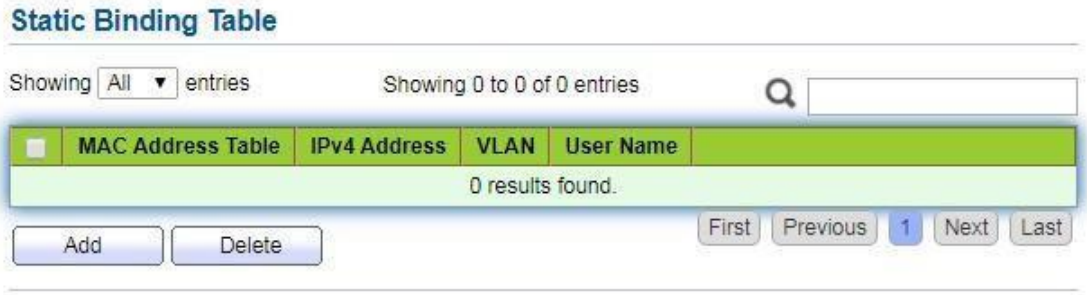
1. Haga clic en "DHCP > Client List", ingrese la lista de clientes DHCP de la siguiente manera.



11.5 Tabla de enlace estático de cliente

Instrucciones de configuración de asignación de direcciones IP estáticas:

1. Haga clic en "DHCP > Client Static Binding Table", ingrese Static Binding Table y haga clic en "Add" de la siguiente manera.



Nota:

La configuración IP del enlace estático debe estar dentro del ámbito de la asignación de direcciones IP.

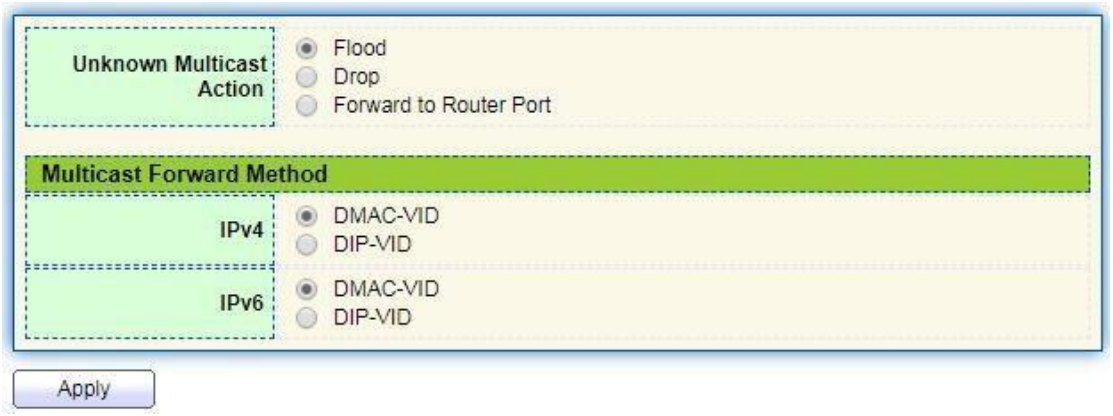
12 Multidifusión

12.1 General

12.1.1 Propiedad

Instrucciones:

1. Haga click en “Multicast > General > Property” en el menú de navegación.

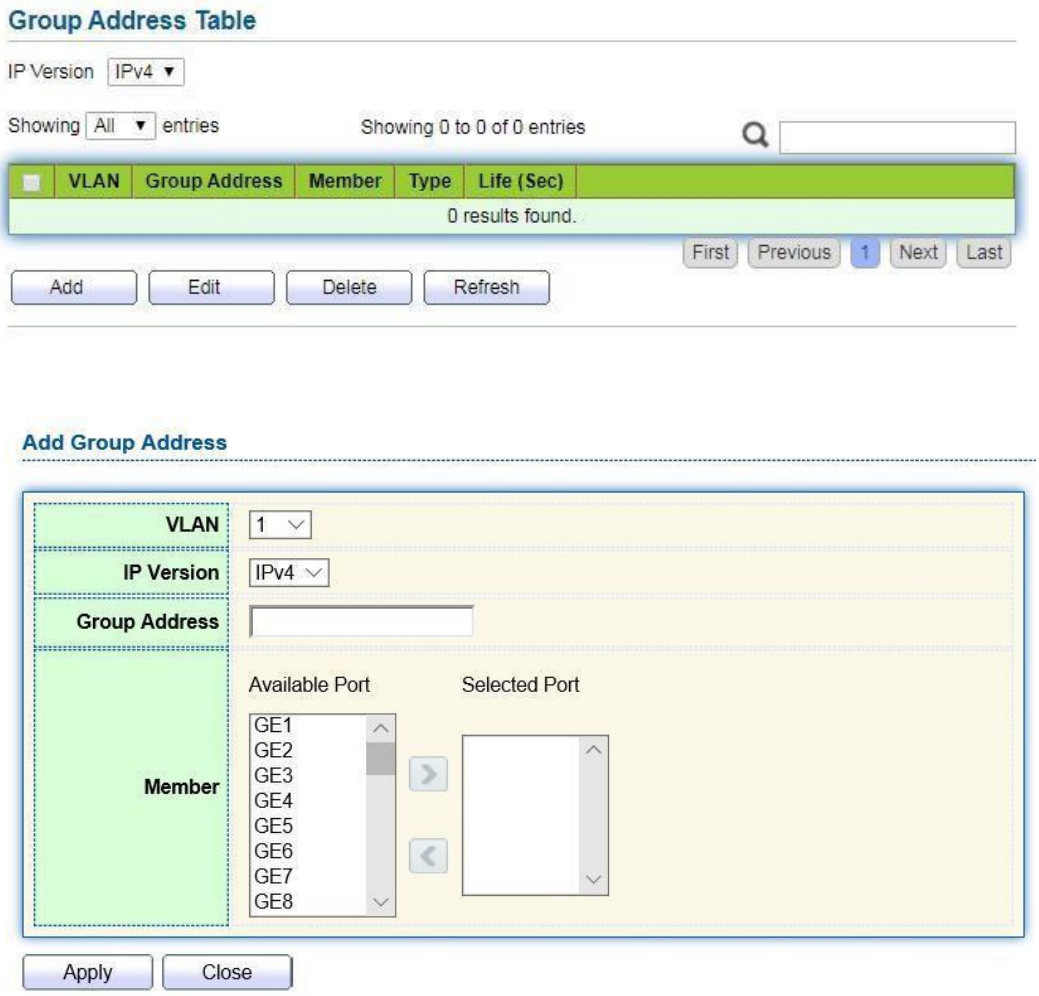


12.1.2 Dirección del grupo

De acuerdo con el modo de solicitud anterior de multidifusión, el enrutador de multidifusión copiará y reenviará datos a cada VLAN que contenga receptores cuando los usuarios de diferentes VLAN soliciten el mismo grupo de multidifusión, lo que desperdicia mucho de ancho de banda. IGMP Snooping configura VLAN de multidifusión conectando los diferentes usuarios de los puertos del switch a una misma VLAN de multidifusión para recibir datos de multidifusión. De esta manera, el flujo de multidifusión solo se puede transmitir dentro de una VLAN de multidifusión, ahorrando así ancho de banda. Además, la seguridad y el ancho de banda están garantizados porque las VLAN de multidifusión están completamente aisladas de las VLAN de usuario.

Instrucciones

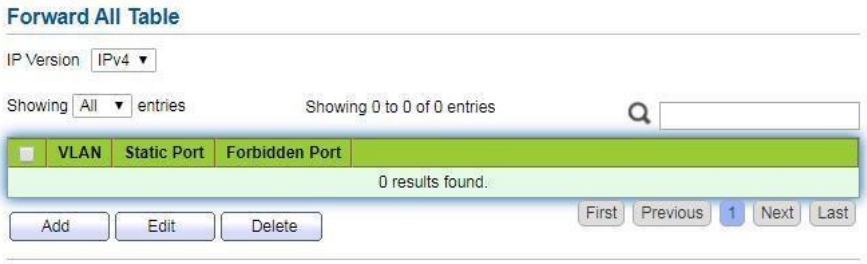
1. Haga clic en "Multicast > Group Address", "Add" a new static multicast item, y "Edit" los existentes de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	ID de VLAN al que pertenece el grupo de multidifusión. Desplácese para seleccionar una VLAN existente.
IP Version	Si v4 o v6 es la versión de la dirección IP de multidifusión
Multicast Address	Introduzca la dirección de multidifusión
Member	Agregar miembro(s) de multidifusión

2. Completa los elementos de configuración correspondientes.



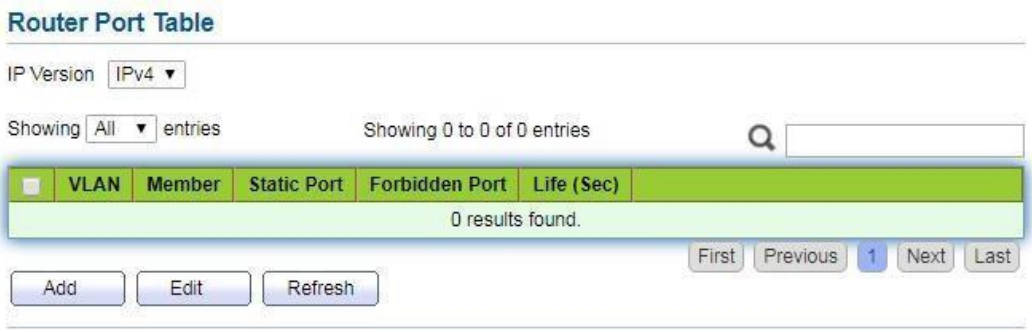
3. "Aplicar" y Finalizar de la siguiente manera.

12.1.3 Puerto del router

Configure y vea el puerto del enrutador de multidifusión.

Instrucciones:

1. Haga click en “Multicast > General > Router Port” en el menú de navegación.



12.1.4 Reenviar todo

Configurar y ver el puerto de reenvío de multidifusión.

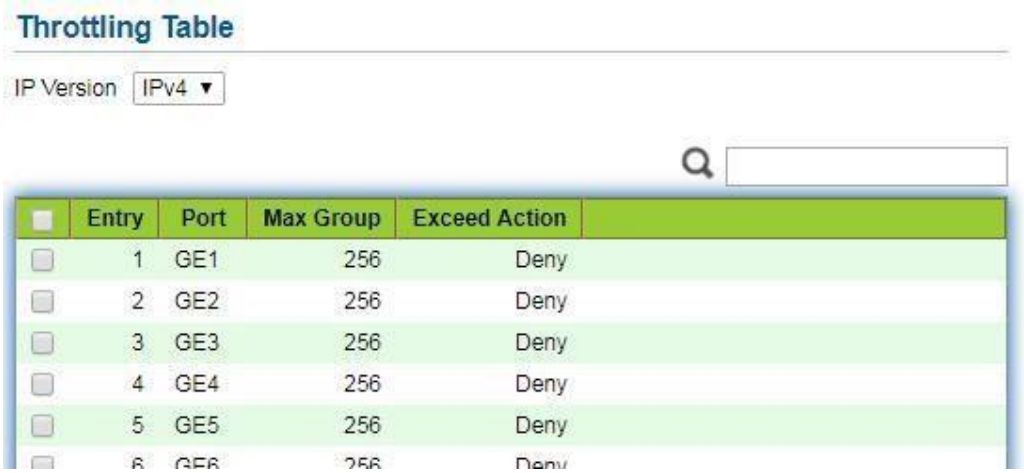
Instrucciones:

1. Haga click en “Multicast > General > Forward All” en el menú de navegación.

12.1.5 Regulación

Configurar y ver las restricciones de grupo de multidifusión de puertos. Instrucciones:

1. Haga click en “Multicast > General > Throttling” en el menú de navegación.



12.1.6 Perfil de filtrado

Configurar y ver el perfil de filtrado de multidifusión del puerto.

Instrucciones:

Haga click en “Multicast > General > Filtering Profile” en el menú de navegación.

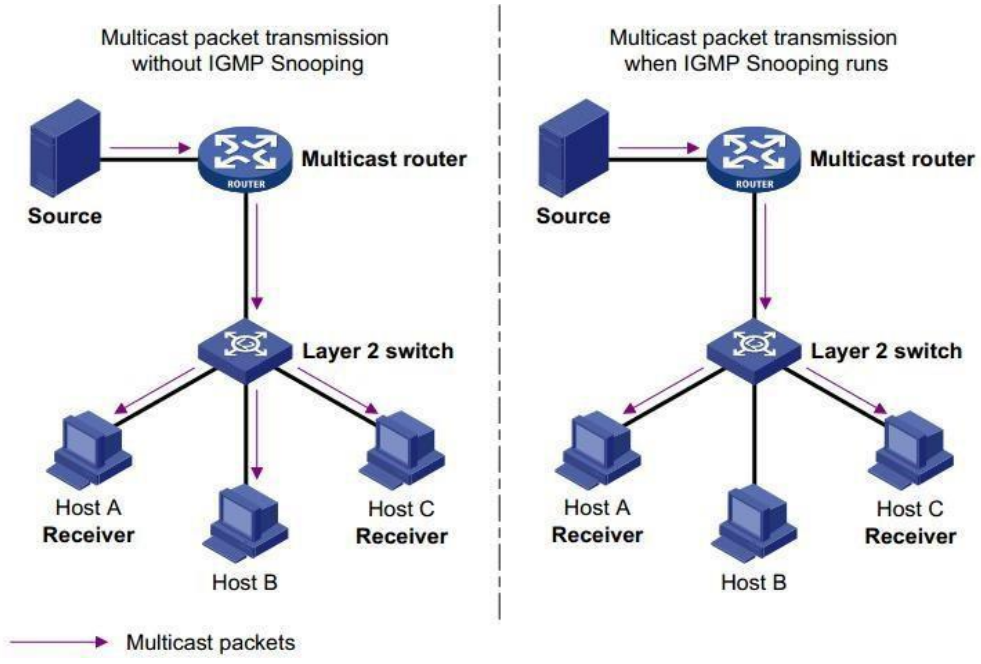
Configurar y ver el perfil de filtrado de multidifusión y la relación de enlace de puerto.

1. Haga click en “Multicast > General > Filtering Binding” en el menú de navegación.

12.2 IGMP Fisgoneo

IGMP Snooping (Internet Group Management Protocol Snooping) es un mecanismo de restricción en dispositivos L2 para administrar y controlar grupos de multidifusión. Al analizar los mensajes IGMP recibidos, los dispositivos L2 establecen un mapeo entre los puertos y las direcciones de multidifusión MAC y reenvían los datos de multidifusión en consecuencia.

Como se muestra a continuación, los datos de multidifusión se transmiten en L2 sin IGMP snooping. Cuando se ejecuta el espionaje IGMP, los datos de grupos de multidifusión conocidos se transmiten a receptores especificados, mientras que los datos de multidifusión desconocidos todavía están en la capa 2.

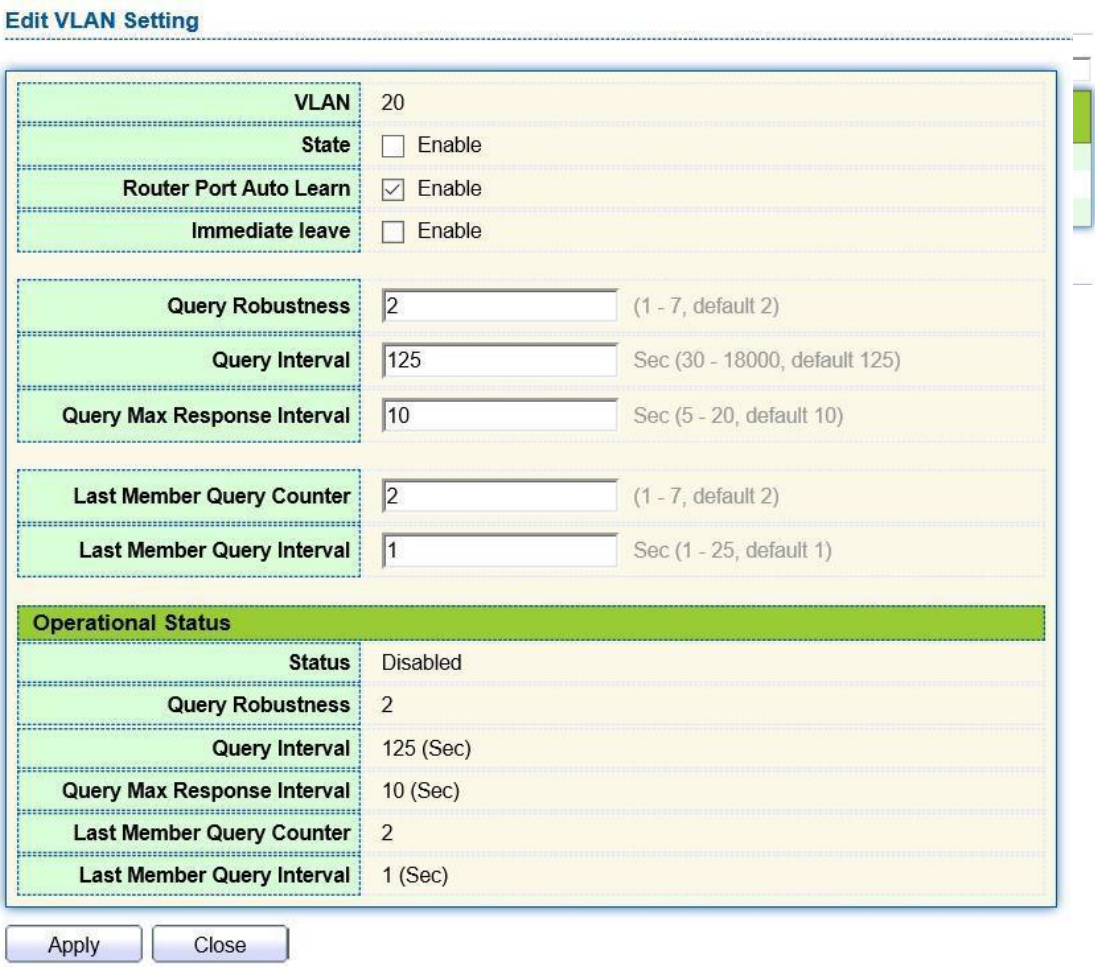


12.2.1 Propiedad

IGMP Snooping está en el switch L2 entre los routers multicast y los hosts de usuario, aplicable para desplegar redes IPv4. Está configurado en una VLAN para espiar los mensajes IGMP/MLD transmitidos entre routers y hosts, y para establecer una tabla de reenvío L2 para datos multicast, con el fin de gestionar y controlar el reenvío de datos multicast en la red L2.

La función Global IGMP Snooping debe estar habilitada ya que está deshabilitada de forma predeterminada. Instrucciones:

1. Haga clic en "Multicast > IGMP Snooping > Property", seleccione la VLAN que se configurará a partir de la información de VLAN creada y "Edite" los detalles de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
State	Habilitar o deshabilitar el IGMP Snooping en esta VLAN
Router Port Auto Learn	Habilitar o deshabilitar el aprendizaje automático del puerto de ruta
Immediate leave	Los miembros de multidifusión se van rápidamente
Query Robustness	La variable de robustez permite ajustar la pérdida de paquetes esperada en una red
Query Interval	El intervalo entre consultas de mensajes
Query Max Response Interval	Tiempo de espera (sobre el tiempo máximo de respuesta) de un mensaje de consulta
Last Member Query Counter	Número máximo de consultas para un grupo especificado
Last Member Query Interval	El intervalo entre consultas de mensajes para un grupo especificado

2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y finalizar.

12.2.2 Consulta

Configurar y ver IGMP snooping Querier.

Instrucciones:

1. Haga click en “Multicast > IGMP Snooping > Querier” en el menú de navegación.

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	VLAN de multidifusión
State	Habilitar o deshabilitar IGMP snooping querier
Operational Status	Estado de ejecución de IGMP snooping querier
Version	Versión para querier
Querier Address	Dirección de multidifusión para consulta

12.2.3 Estadística

Configure y vea las estadísticas de espionaje

IGMP. Instrucciones:

1. Haga click en “Multicast > IGMP Snooping > statistics” en el menú de navegación.

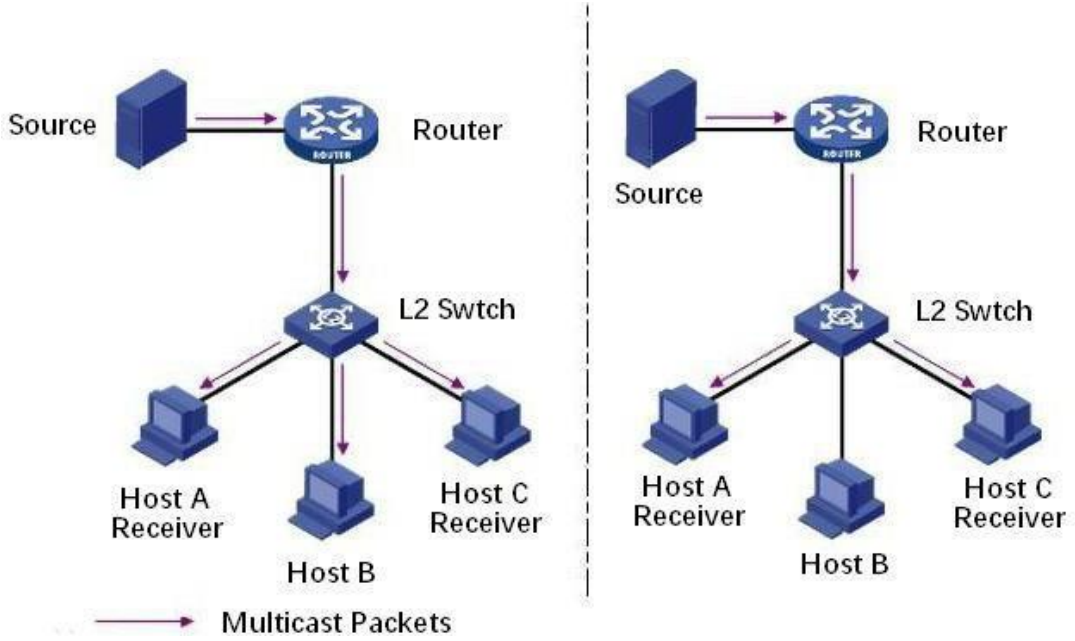
12.3 MLD Fisgoneo

MLD snooping es la abreviatura de multicast Listener Discovery snooping.

Es un mecanismo de restricción de multidifusión IPv6 que se ejecuta en dispositivos de capa 2, que se utiliza para administrar y controlar grupos de multidifusión IPv6.

El dispositivo de segunda capa que ejecuta MLD snooping establece una relación de mapeo entre el puerto y la dirección de multidifusión MAC mediante el análisis del mensaje MLD recibido y reenvía los datos de multidifusión IPv6 de acuerdo con la relación de mapeo.

Como se muestra en la siguiente figura, cuando el dispositivo de capa 2 no ejecuta MLD snooping, los paquetes de datos de multidifusión IPv6 se transmiten en la capa 2; cuando el dispositivo de capa 2 ejecuta MLD snooping, los paquetes de datos de multidifusión de grupos de multidifusión IPv6 conocidos no se transmitirán en la capa 2, sino que se multidifundirán a los receptores designados en la capa 2.



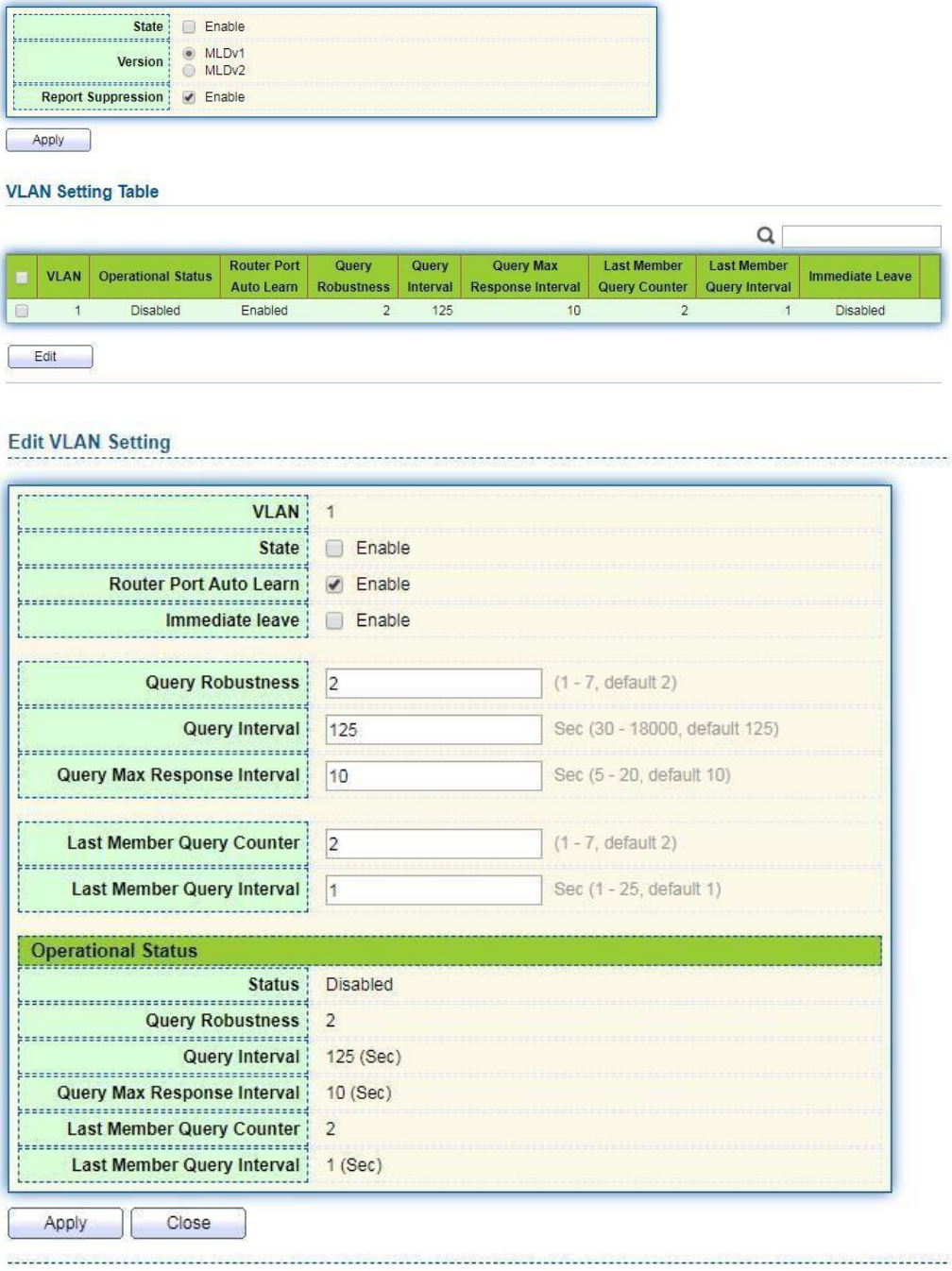
MLD snooping solo puede enviar información a los receptores que lo necesitan a través de la multidifusión de capa 2, lo que puede traer los siguientes beneficios:

- Reducir los paquetes de difusión en la red de capa 2 y ahorrar el ancho de banda de la red;
- Mejore la seguridad de la información de multidifusión IPv6.
- Es conveniente cargar cada host por separado.

12.3.1 Propiedad

La función Global MLD Snooping debe estar habilitada ya que está deshabilitada de forma predeterminada. Instrucciones:

1. Haga clic en "Multicast > MLD Snooping > Property", seleccione la VLAN que se configurará a partir de la información de VLAN creada y "Edite" los detalles de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
State	Habilitar o deshabilitar el IGMP Snooping en esta VLAN
Router Port Auto Learn	Habilitar o deshabilitar el aprendizaje automático del puerto de ruta
Immediate leave	Los miembros de multidifusión se van rápidamente
Query Robustness	La variable de robustez permite ajustar la pérdida de paquetes esperada en una red
Query Interval	El intervalo entre consultas de mensajes
Query Max Response Interval	Tiempo de espera (sobre el tiempo máximo de respuesta) de un mensaje de consulta
Last Member Query Counter	Número máximo de consultas para un grupo especificado
Last Member Query Interval	El intervalo entre consultas de mensajes para un grupo especificado

2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y finalizar.

12.3.2 Estadística

Configure y vea las estadísticas de espionaje MLD.

Instrucciones:

1. Haga click en “Multicast > MLD Snooping > statistics” en el menú de navegación.

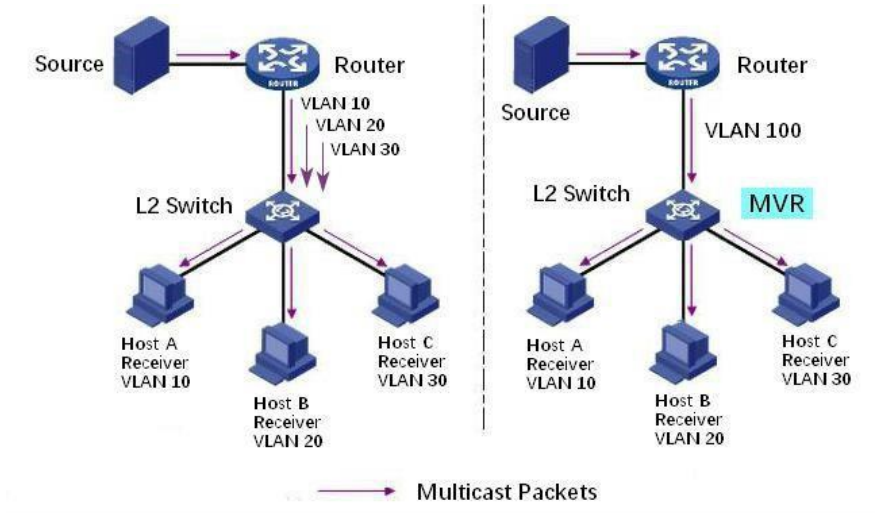
12.4 MVR

Para resolver el problema de la difusión de tráfico multicast basado en VLAN en red de capa 2, utilizamos el protocolo IGMP snooping para controlar el receptor, es decir, solo el receptor puede recibir el tráfico multicast normalmente.

Sin embargo, IGMP snooping solo puede controlar eficazmente el tráfico de la misma VLAN multidifusión, pero no el tráfico VLAN cruzado. Como resultado, la eficiencia de múltiples replicaciones de la misma multidifusión en diferentes VLAN todavía existe.

Para resolver el problema de inundación de VLAN cruzada, adoptamos la multidifusión dedicada.

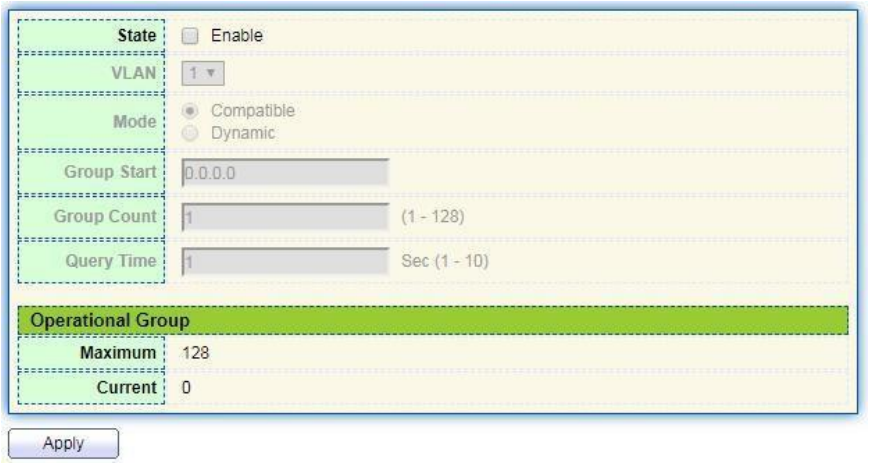
VLAN del tráfico de origen de multidifusión, como se muestra en la siguiente figura.



12.4.1 Propiedad

La función MVR global debe estar habilitada ya que está deshabilitada de forma predeterminada. Instrucciones:

1. Haga clic en la propiedad "Multicast> MVR >", ingrese a la interfaz de configuración global de MVR de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
State	Habilitar o deshabilitar MVR
VLAN	ID de VLAN que se va a configurar
Mode	Compatible: La CPU del switch MVR normalmente reenvía el mensaje de consulta del router y el mensaje de unión del cliente para formar la tabla de reenvío multicast del aprendizaje dinámico. Sin embargo, la CPU no reenviará el mensaje de unión al puerto del enrutador, por lo que el enrutador superior no recibirá el siguiente mensaje de unión, lo que hace que los datos del enrutador no se puedan reenviar al conmutador normalmente. En este modo, es necesario configurar el router manualmente La tabla de reenvío de multidifusión reenvía los datos al conmutador
	Dinámico: La única diferencia entre el modo dinámico y el modo compatible es que la CPU puede reenviar el mensaje de unión al puerto del router en el modo dinámico, por lo que el router de capa superior puede aprender la tabla de reenvío de multidifusión dinámicamente, y no hay necesidad de Configurar manualmente la tabla de reenvío de multidifusión del router para reenviar los datos al conmutador
Group Start	La dirección de aparición del grupo de multidifusión
Group Count	Número de direcciones de grupo de multidifusión
Query Time	Tiempo de consulta de grupo de multidifusión

2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y finalizar.

12.4.2 Configuración del puerto

Instrucciones:

1. Haga clic en "Multicast > MVR > Port Setting", ingrese a la interfaz de configuración del puerto MVR de la siguiente manera:

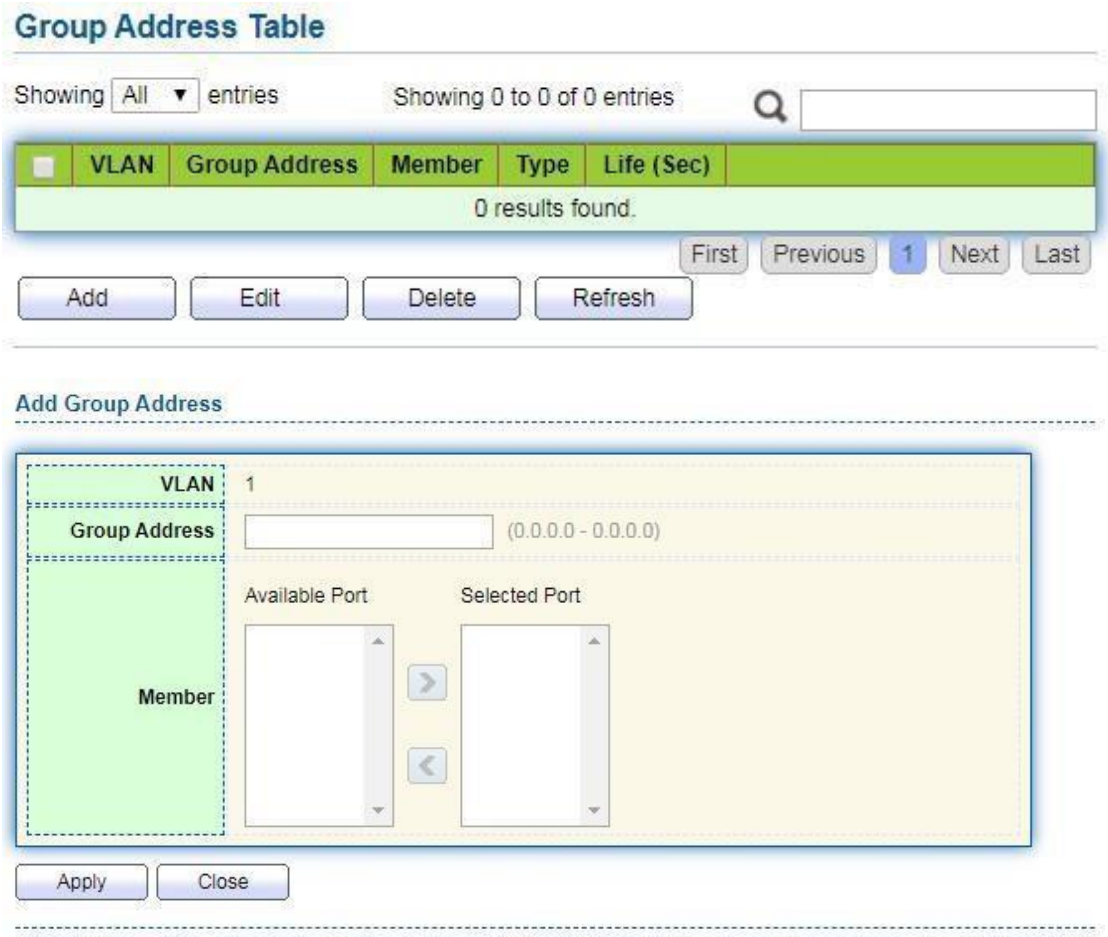
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	Lista de puertos
Role	Modo de puerto Receptor: Representa el puerto del conmutador al que está conectado el host de multidifusión, que se utiliza para recibir el flujo de multidifusión. Origen: el puerto de origen hace referencia al puerto de origen del flujo de multidifusión del puerto de acceso de origen de multidifusión de capa superior
Immediate Leave	Los miembros de multidifusión se van rápidamente

12.4.3 Dirección del grupo

Instrucciones:

1. Haga clic en "Multicast > MVR > Group Address", vea la información del grupo de multicast de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	ID de VLAN para multidifusión
Group Address	Introduzca la dirección de multidifusión
Member	Agregar miembro(s) de multidifusión

13 Enrutamiento

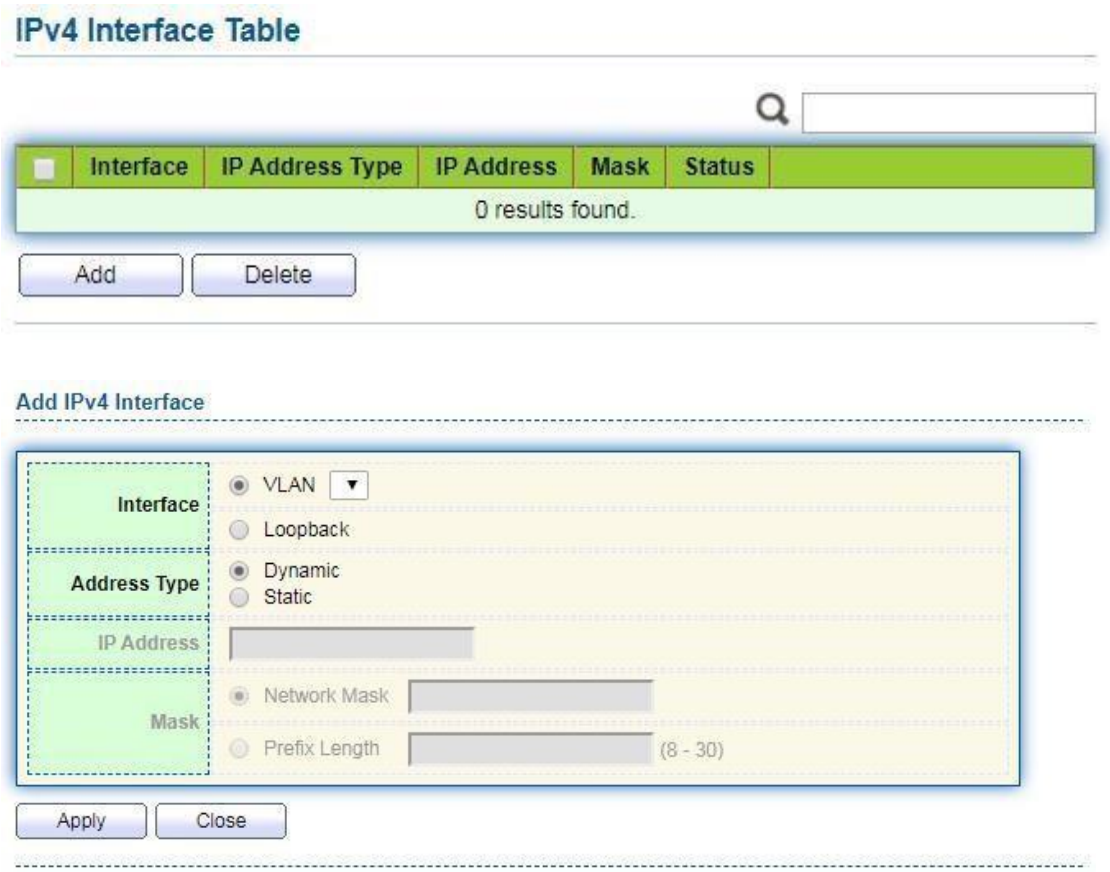
El switch proporciona tres capas de interfaz VLAN, que se utiliza para comunicarse con dispositivos de capa de red. La interfaz VLANIF es una interfaz de capa de red, que se puede configurar con la dirección IP. Antes de crear la interfaz VANIF, primero se debe crear la VLAN correspondiente. Con la ayuda de la interfaz VANIF, los switches pueden comunicarse con otros dispositivos de capa de red.

13.1 Gestión e interfaces IPv4

13.1.1 Interfaz IPv4

Instrucciones:

1. Haga clic en "Routing > IPv4 Management and Interfaces > IPv4 Interface", ingrese la configuración de la interfaz IPv4 capa 3 de la siguiente manera:



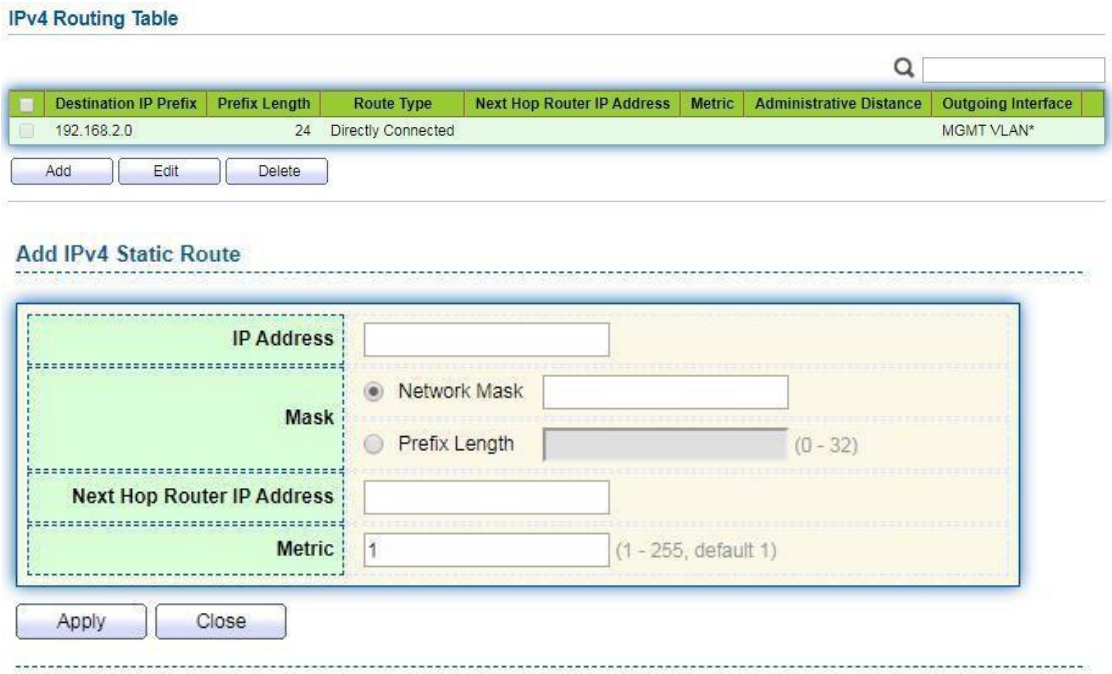
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
Loopback	Interfaz de bucle invertido
Address Type	Dinámico: DHCP obtiene la dirección IP de la interfaz Estático: La dirección IP de la interfaz se configura manualmente
IP Address	La dirección IP de la interfaz
Mask	La máscara de dirección IP de la interfaz

13.1.2 Rutas IPv4

Instrucciones:

1. Haga clic en "Routing > IPv4 Management and Interfaces > IPv4 Routes", ingrese la configuración de la interfaz de ruta estática IPv4 de la siguiente manera:



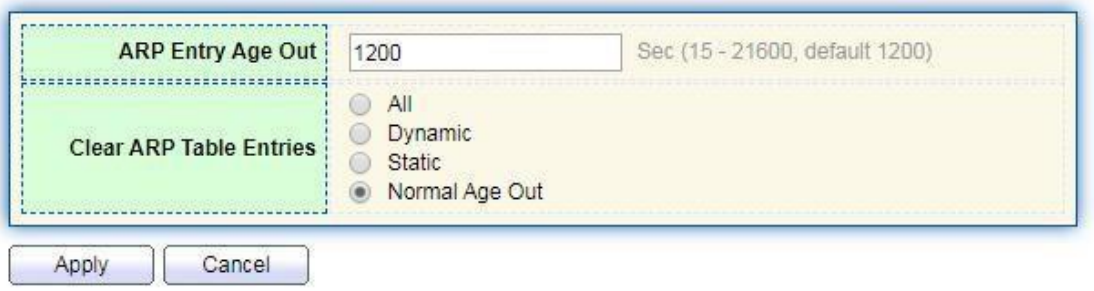
Los campos de la interfaz son como a continuación.

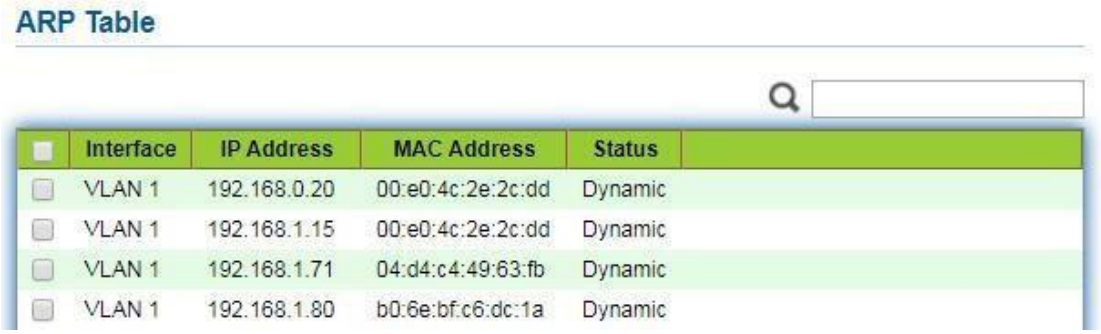
IP Address	Descripción
Mask	Segmento de dirección IP de destino
Next Hop Router IP Address	Máscara de dirección IP de destino
Metric	La dirección IP del próximo salto debe estar en el mismo segmento de red que la puerta de enlace de interfaz
IP Address	Saltos de red

13.1.3 ARP

Instrucciones:

1. Haga clic en "Routing > IPv4 Management and Interfaces >ARP", configure y vea las entradas de la tabla ARP de la siguiente manera:





Los campos de la interfaz son como a continuación.

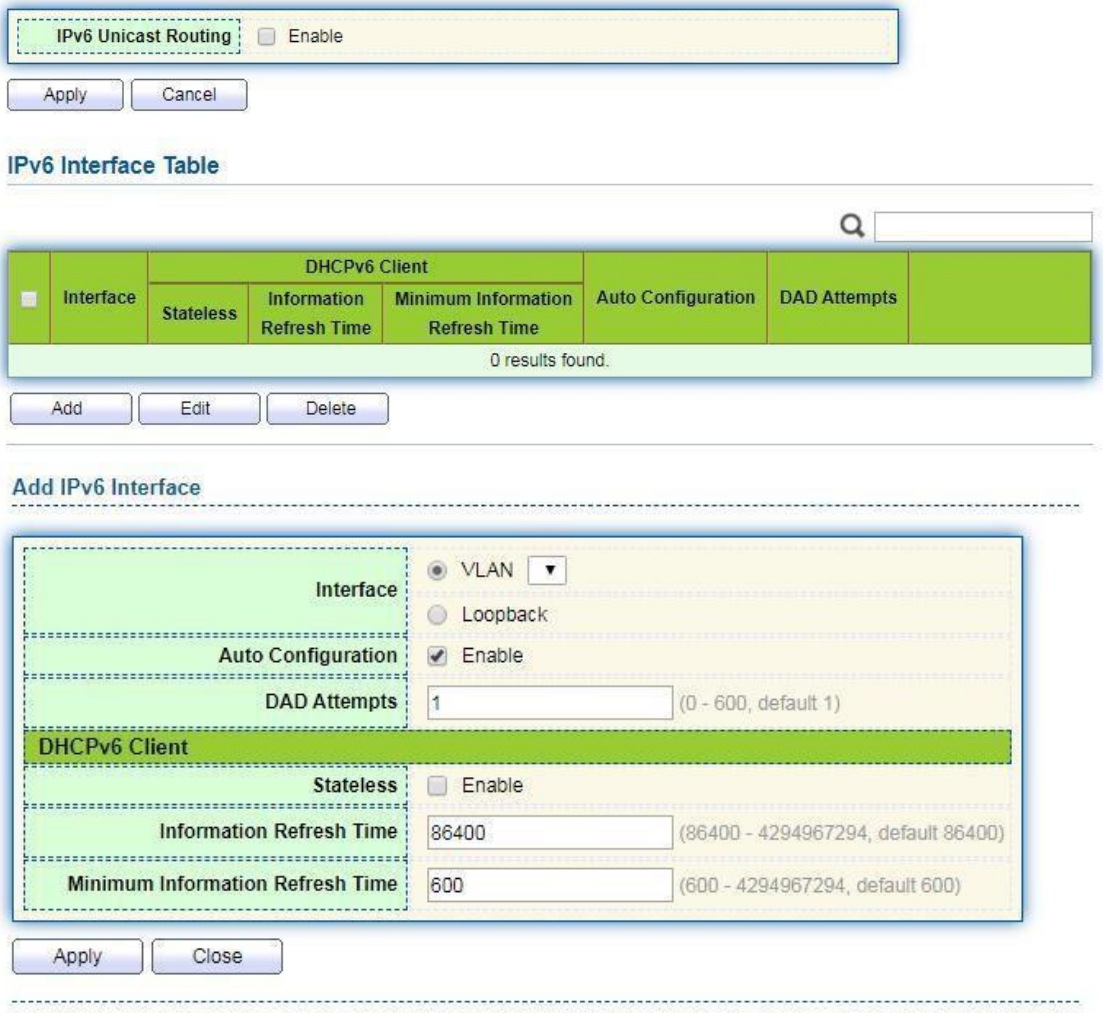
Elementos de configuración	Descripción
Interface	Interfaz VLANIF
IP Address	Dirección IP del mismo segmento de red que la puerta de enlace de interfaz
MAC Address	Dirección MAC correspondiente a la dirección IP

13.2 Administración e interfaces IPv6

13.2.1 Interfaz IPv6

Instrucciones:

1. Haga clic en "Routing > IPv6 Management and Interfaces > IPv6 Interface", ingrese la configuración de la interfaz IPv6 capa 3 de la siguiente manera:



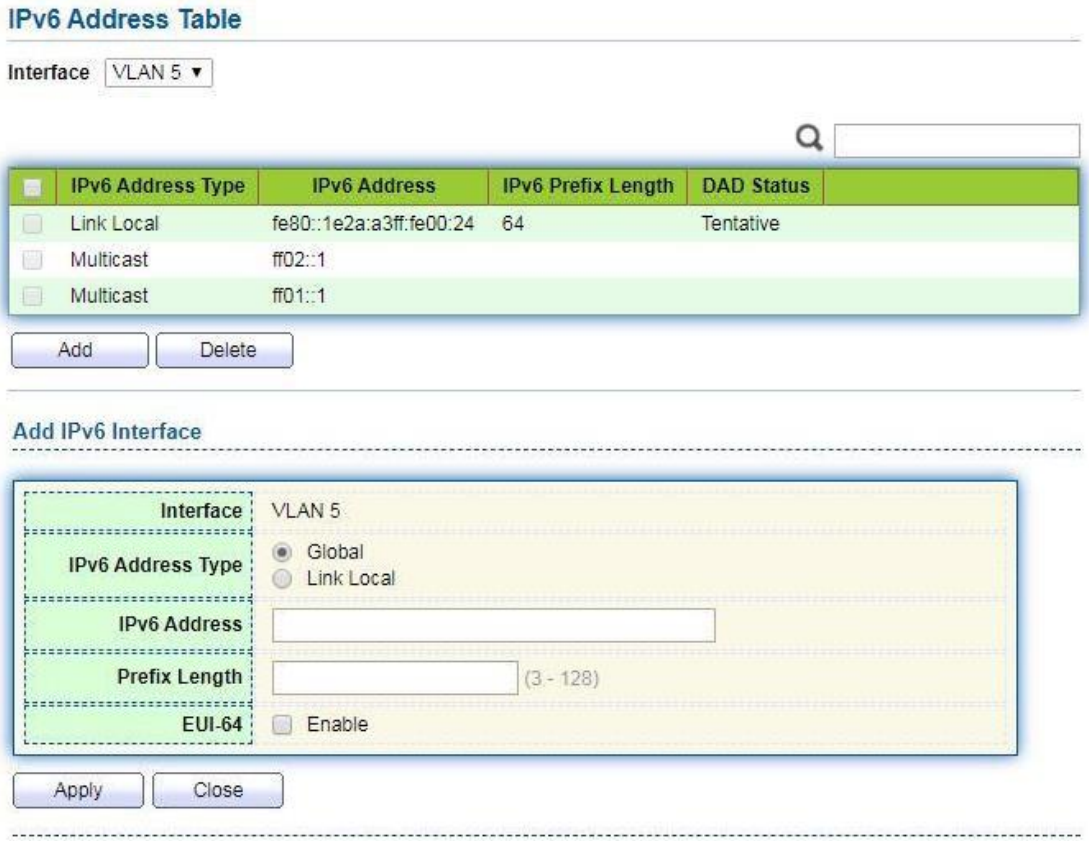
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
Loopback	Interfaz de bucle invertido
Auto Configuration	Conmutador de configuración automática
DAD Attempts	Configurar el número de veces que se envían mensajes de solicitud de vecino para la detección de direcciones duplicadas
Stateless	Configuración automática sin estado
Information Refresh Time	Tiempo de actualización de la configuración automática
Minimum Information Refresh Time	Tiempo de actualización mínimo para la configuración automática

13.2.2 Dirección IPv6

Instrucciones:

1. Haga clic en "Routing > IPv6 Management and Interfaces > IPv6 Address", ingrese a la interfaz de configuración de direcciones IPv6 de la siguiente manera:



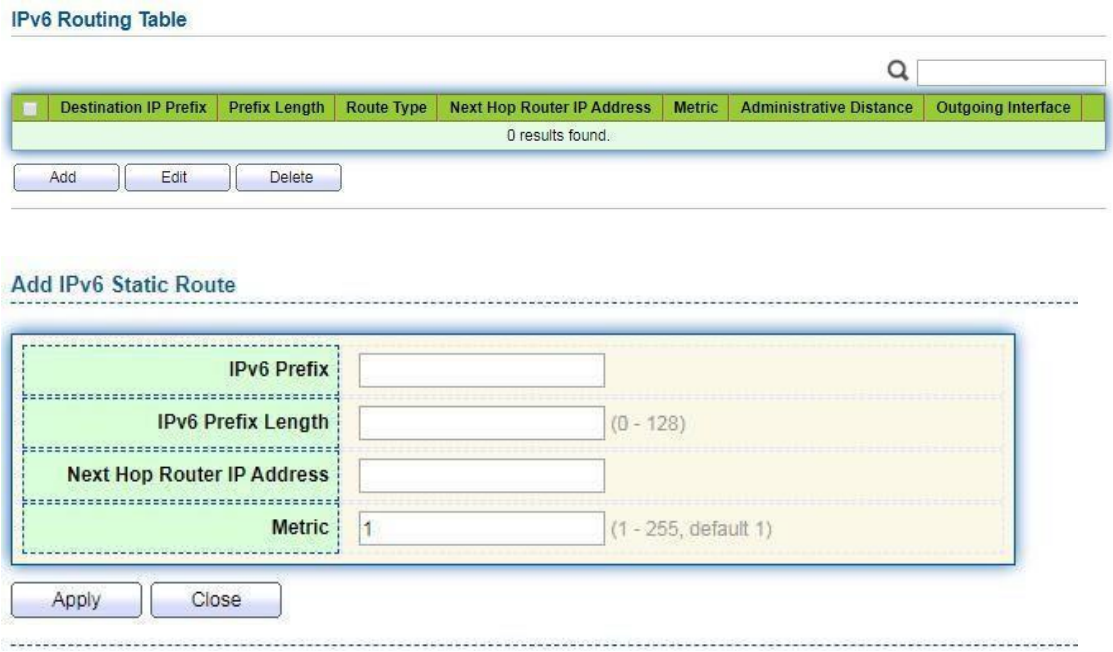
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Interface	Interfaz VLANIF
IPv6 Address Type	Global: dirección IPv6 global Enlace local: dirección IPv6 local
IPv6 Address	Dirección IPv6
Prefix Length	Prefijo de la dirección IPv6
EUI-64	Habilitar o deshabilitar la dirección derivada de la dirección IEEE802

13.2.3 Rutas IPv6

Instrucciones:

1. Haga clic en "Routing > IPv6 Management and Interfaces > IPv6 Routes", ingrese la configuración de la interfaz de ruta estática IPv6 de la siguiente manera:



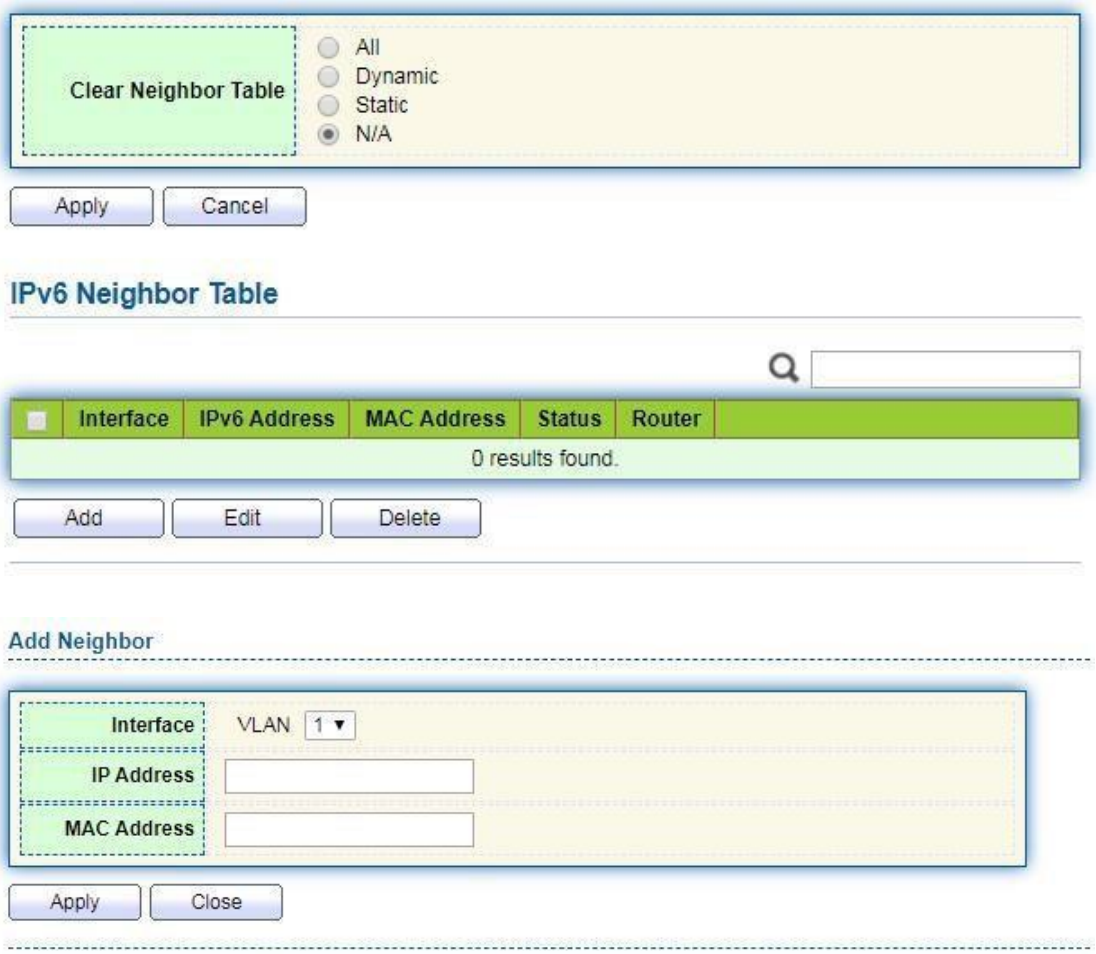
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
IPv6 Prefix	Segmento de direcciones IPv6 de destino
IPv6 Prefix Length	Prefijo de dirección IPv6 de destino
Next Hop Router IP Address	La dirección IPv6 del próximo salto debe estar en el mismo segmento de red que la puerta de enlace de interfaz
Metric	Saltos de red

13.2.4 Vecinos

Instrucciones:

1. Haga clic en "Routing > IPv6 Management and Interfaces > Neighbors", configure y vea las entradas de la tabla de vecinos IPv6 de la siguiente manera:



Los campos de la interfaz son como a continuación.

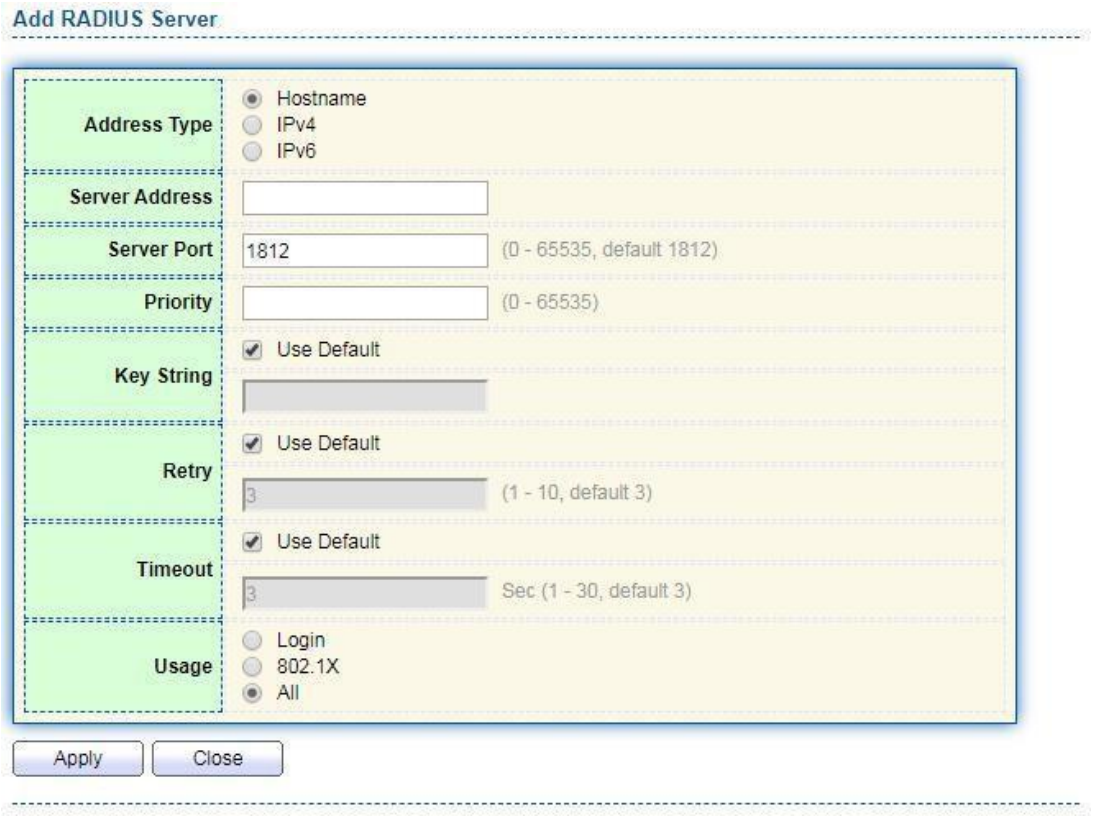
Elementos de configuración	Descripción
Interface	Interfaz VLANIF
IP Address	Dirección IPv6 del mismo segmento de red que la puerta de enlace de interfaz
MAC Address	Dirección MAC correspondiente a la dirección IPv6

14 Seguridad

14.1 RADIO

Instrucciones:

1. Haga clic en "Seguridad > RADIUS", ingrese a la interfaz RADIUS de la siguiente manera:



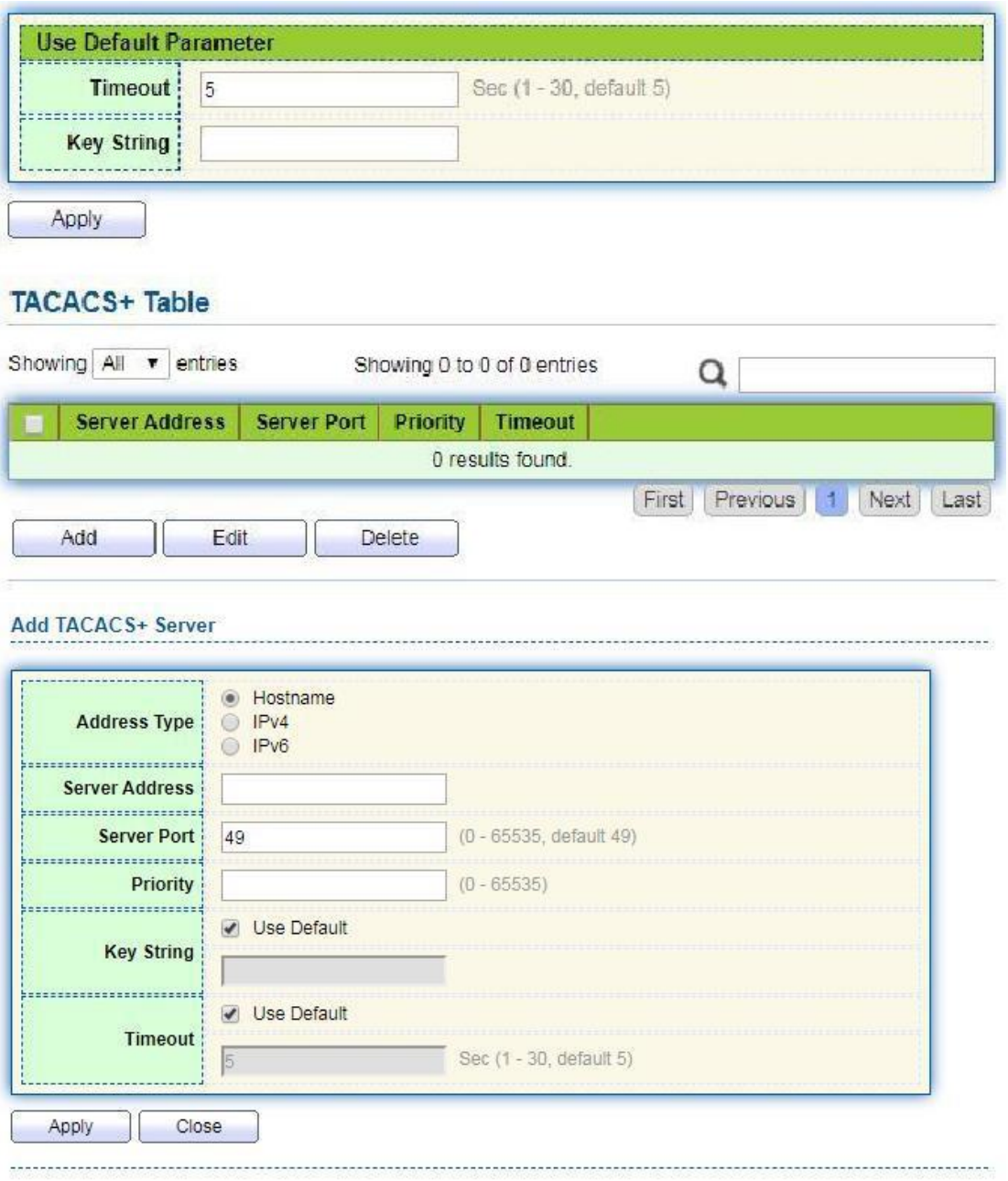
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Address Type	Dependiendo del tipo, puede elegir Nombre de host, IPv4, IPv6
Server Address	Dirección IP del servidor
Server Port	Puerto de servicio
Priority	Prioridad del servicio
Key String	La clave secreta, compartida entre el servidor RADIUS y el conmutador
Retry	Retransmitir es el número de veces
Timeout	para esperar una respuesta de un servidor RADIUS antes de retransmitir la solicitud
Usage	Escenarios de uso

14.2 TACACS+

Instrucciones:

1. Haga clic en "Seguridad > TACACS+", ingrese a la interfaz TACACS+ de la siguiente manera:



Los campos de la interfaz son como a continuación.

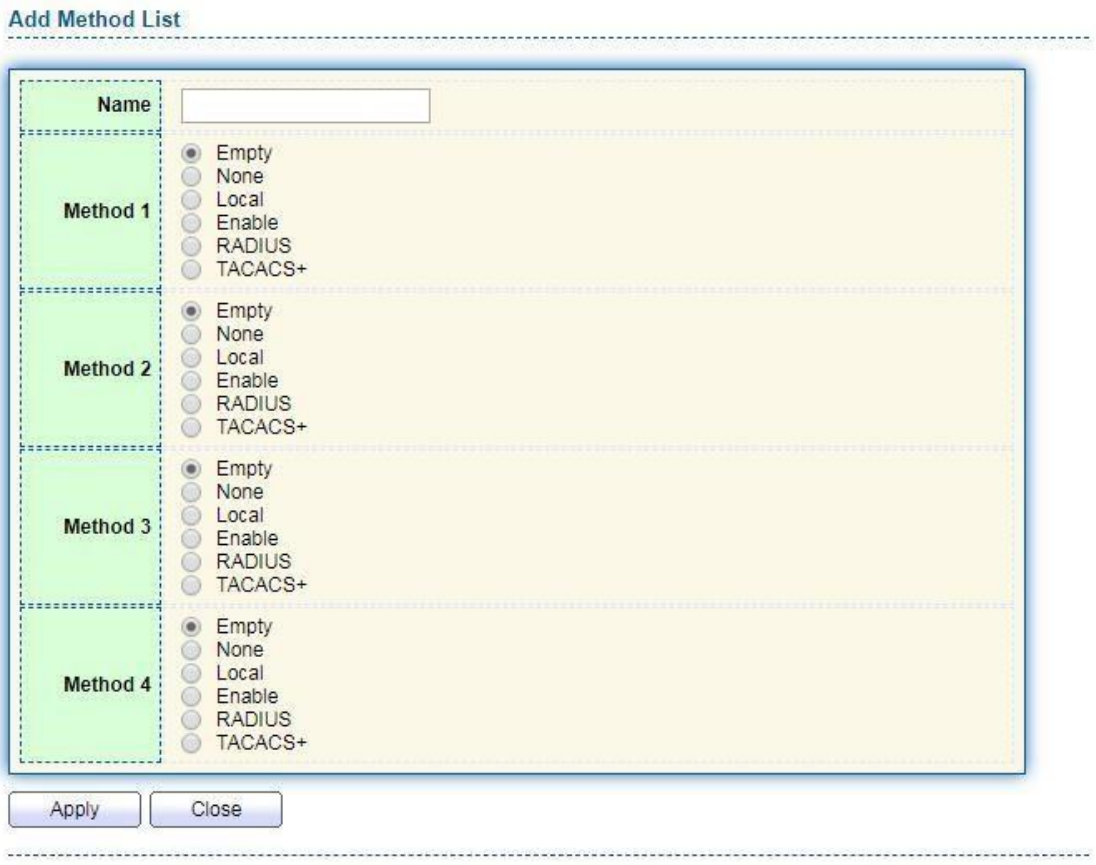
Elementos de configuración	Descripción
Address Type	Dependiendo del tipo, puede elegir Nombre de host, IPv4, IPv6
Server Address	Dirección IP del servidor
Server Port	Puerto de servicio
Priority	Prioridad del servicio
Key String	La clave secreta, compartida entre el servidor RADIUS y el conmutador
Retry	Retransmitir es el número de veces
Timeout	para esperar una respuesta de un servidor RADIUS antes de retransmitir la solicitud

14.3 AAA

14.3.1 Lista de métodos

Instrucciones:

1. Haga clic en "Security > AAA > Method List", ingrese a la interfaz de la lista de métodos de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Name	Nombre del método
Method 1-4	Vacío: el método está deshabilitado Ninguno: No hacer nada y simplemente hacer que el usuario se autentique Local: usar la base de datos de cuentas de usuario local para autenticarse Habilitar: usar la base de datos de contraseñas de habilitación local para autenticarse RADIUS: Usar el servidor Radius remoto para autenticarse TACACS+: Usar el servidor remoto TACACS+ para autenticarse

14.3.2 Autenticación de inicio de sesión

Instrucciones:

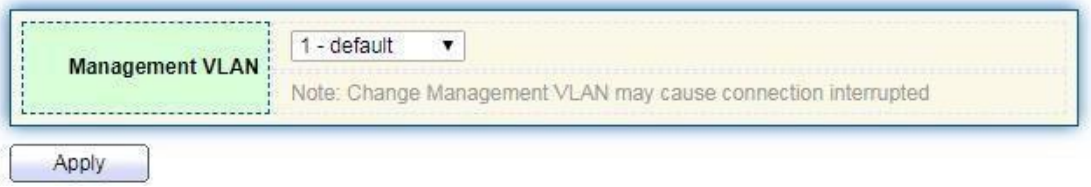
1. Haga clic en "Seguridad>AAA >Autenticación de inicio de sesión ", ingrese a la interfaz de autenticación de inicio de sesión de la siguiente manera:

14.4 Acceso de administración

14.4.1 VLAN de administración

Instrucciones:

1. Haga clic en "Security > Management Access > Management VLAN", ingrese a la interfaz VLAN de administración de la siguiente manera:



14.4.2 Servicio de Gestión

Instrucciones para Telnet:

1. Haga clic en "Security > Management Access > Management Service", ingrese a la interfaz del servicio de administración de la siguiente manera:

Instrucciones para SSH:

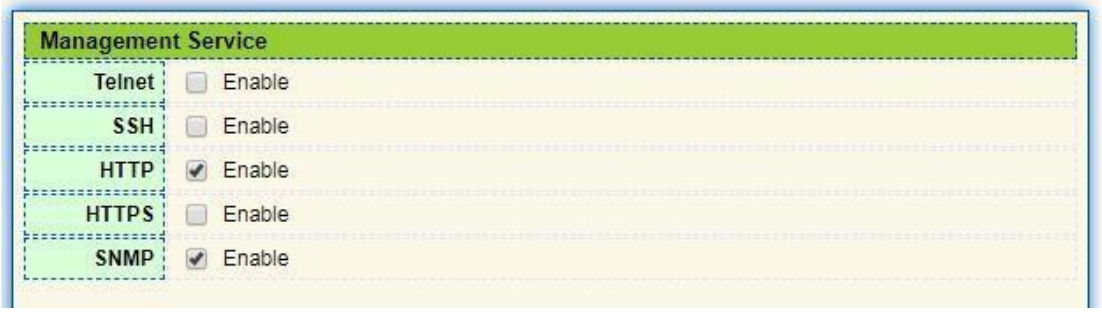
2. Haga clic en "Security > Management Access > Management Service", ingrese a la interfaz del servicio de administración de la siguiente manera:

Instrucciones para HTTPS:

3. Haga clic en "Security > Management Access > Management Service", ingrese a la interfaz del servicio de administración de la siguiente manera:

Instrucciones para SNMP:

4. Haga clic en "Security > Management Access > Management Service", ingrese a la interfaz del servicio de administración de la siguiente manera:



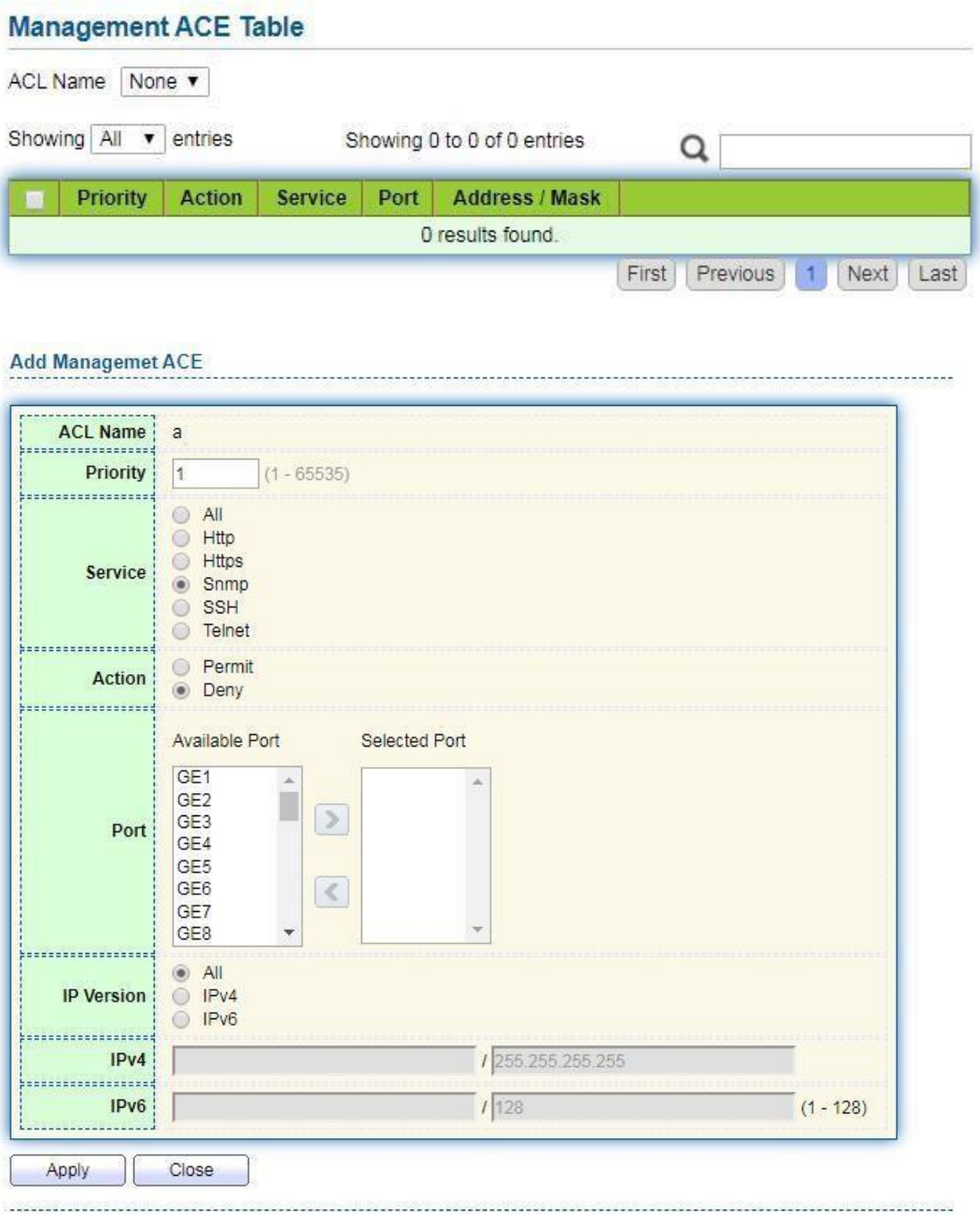
14.4.3 ACL de administración

ACLS aplicado a la gestión.

Instrucciones:

1. Haga clic en "Security > Management Access > Management ACL", ingrese a la interfaz ALC de administración de la siguiente manera:

2. Haga clic en "Security > Management Access > Management ACE", ingrese a la interfaz ACE de administración de la siguiente manera:



Los campos de la interfaz son como a continuación.

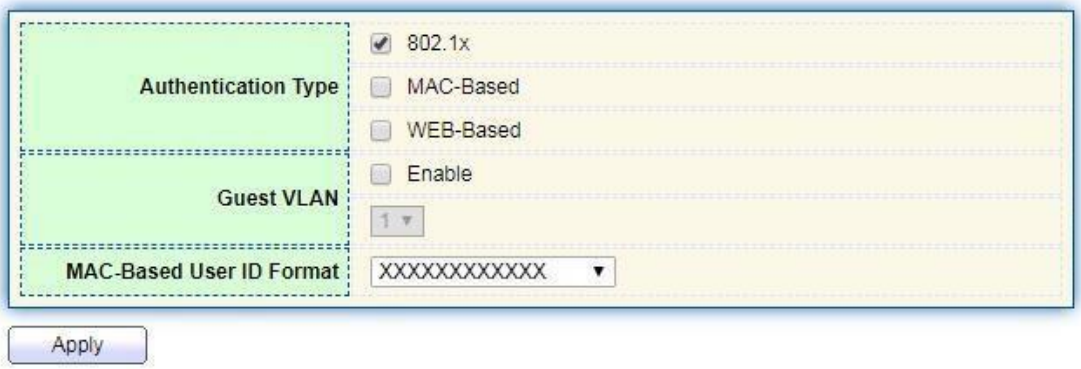
Elementos de configuración	Descripción
ACL Name	Nombre de ACL
Priority	Prioridad de ACL
Service	Tipo de servicio utilizado
Action	Acción del partido
Port	El puerto en el que se aplica esta ACL
IP Version	Administrar la versión de la dirección IP
IPv4	Dirección IPv4
IPv6	Dirección IPv6

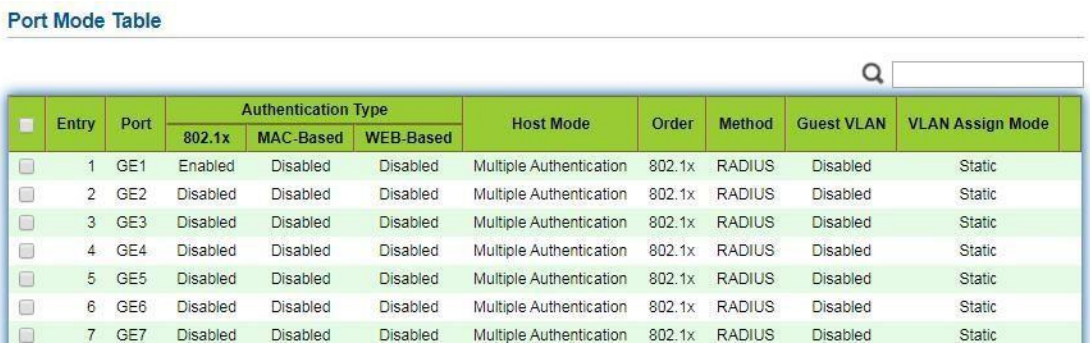
14.5 Administrador de autenticación

14.5.1 Propiedad

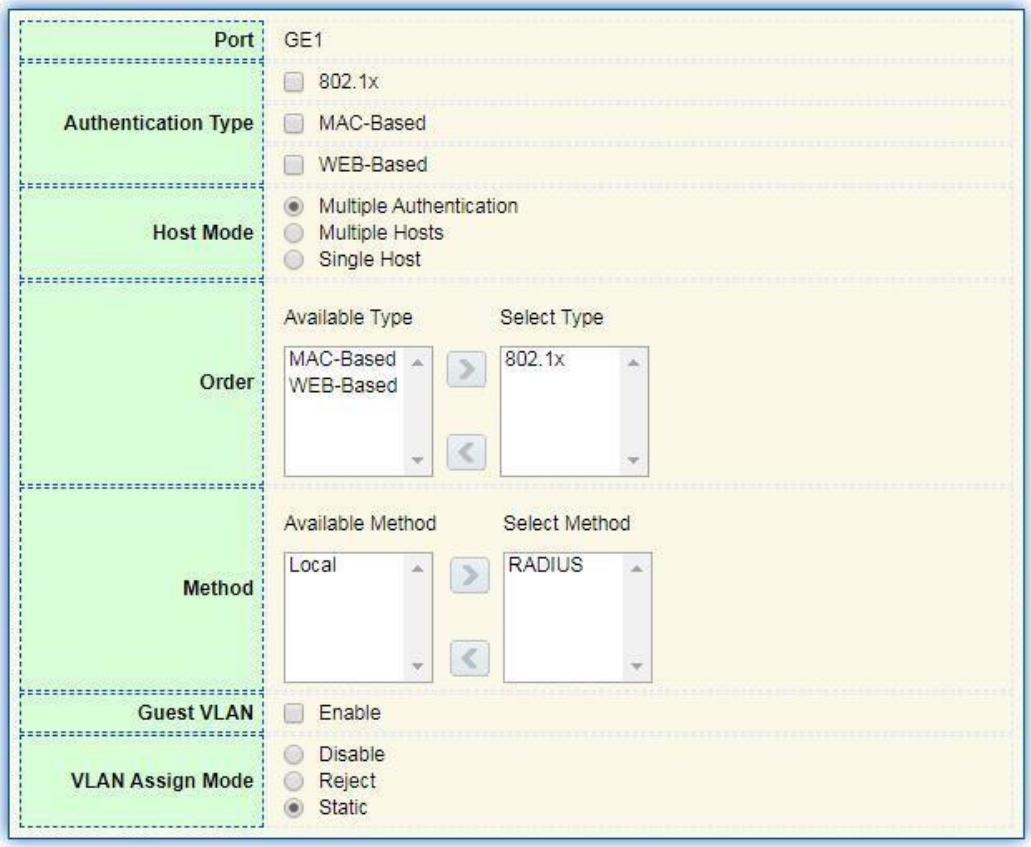
Habilite la configuración global del control de acceso a la red de autenticación 802.1x/MAC/WEB Instrucciones:

1. Haga clic en "Security > Management Manager > Property", ingrese a la interfaz global de la siguiente manera:





Edit Port Mode



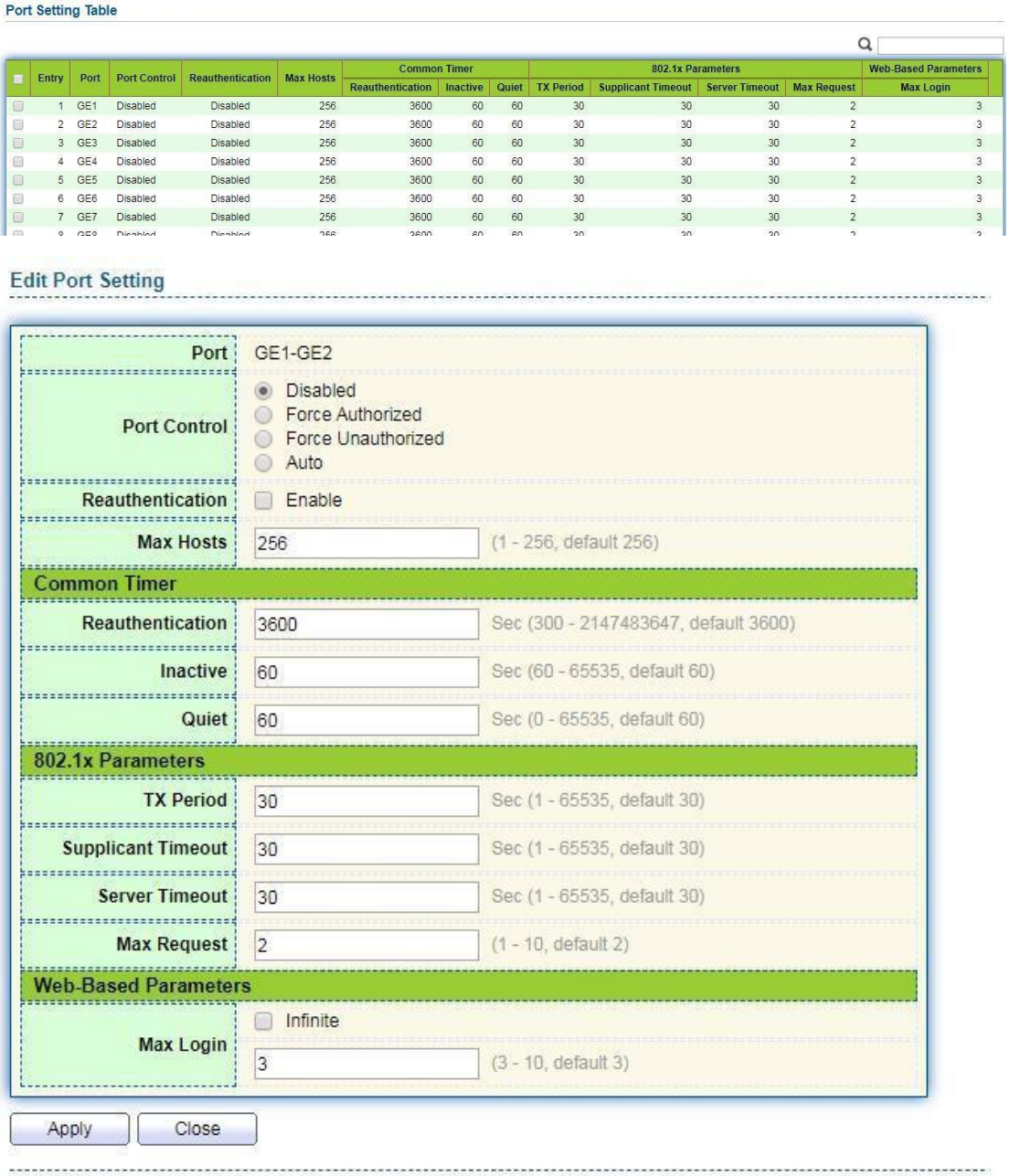
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	Lista de puertos
Authentication Type	Tipo de autenticación de puerto
Host Mode	Autenticación múltiple: En este modo, cada cliente debe pasar el procedimiento de autenticación individualmente. Múltiples hosts: En este modo, solo es necesario autenticar un cliente y otros clientes obtendrán la misma accesibilidad de acceso. Host único: En este modo, solo se puede autenticar un host. Es lo mismo que el modo de autenticación múltiple con un número máximo de hosts configurado para ser 1
Order	Acción del partido
Method	Orden del método de autenticación de puertos
Guest VLAN	VLAN de invitados
VLAN Assign Mode	Modo de asignación de VLAN RADIUS de puerto Rechazar: Si obtiene información autorizada por VLAN, simplemente úsela. Sin embargo, si no hay información autorizada por VLAN, rechace el host y hágalo no autorizado Estático: Si obtiene información autorizada por VLAN, simplemente úsela. Si no hay información autorizada por VLAN, mantenga la VLAN original del host.

14.5.2 Configuración del puerto

Instrucciones:

1. Haga clic en "Security > Management Manager > Port Setting", ingrese a la interfaz de configuración de puerto de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	Lista de puertos
Port Control	Forzar autorización: El puerto está autorizado por fuerza y todos los clientes tienen accesibilidad a la red. Forzar no autorizado: el puerto es forzado no autorizado y todos los clientes Automático: Necesita pasar el procedimiento de autenticación para obtener accesibilidad de red
Reauthentication	Habilitar la reautenticación de puertos
Max Hosts	El número máximo de hosts del puerto para el modo de autenticación múltiple
Reauthentication	El valor del período de reautenticación del puerto con una unidad de segundo si la base de datos local o el servidor de autenticación remota no asignan el tiempo de reautenticación
Inactive	El valor de tiempo de espera inactivo del puerto
Quiet	El valor del período de silencio del puerto
TX Period	El valor del período TX EAP del puerto 802.1x
Supplicant Timeout	El valor de tiempo de espera del suplicante de puerto
Server Timeout	El valor de tiempo de espera del servidor 802.1x del puerto
Max Request	El valor máximo de solicitud EAP del puerto 802.1x
Max Login	El número máximo de intentos de inicio de sesión de autenticación WEB del puerto

14.5.3 Cuenta local basada en MAC

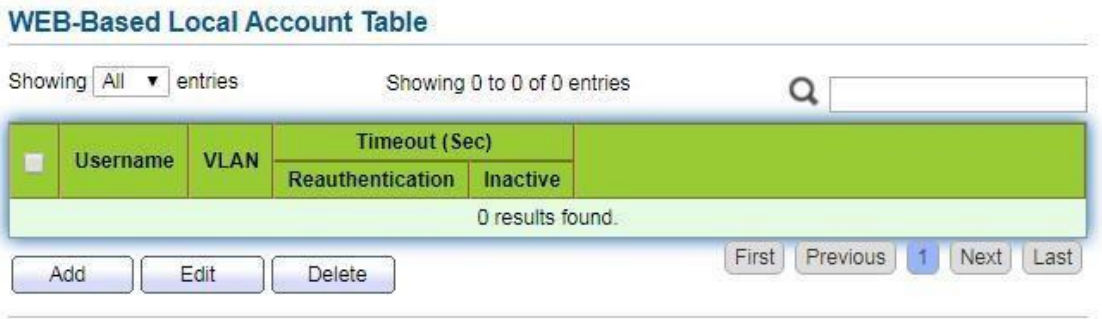
Instrucciones:

1. Haga clic en "Security > Management Manager > cuenta local basada en MAC", ingrese a la interfaz de configuración de la siguiente manera:

14.5.4 Cuenta local basada en web

Instrucciones:

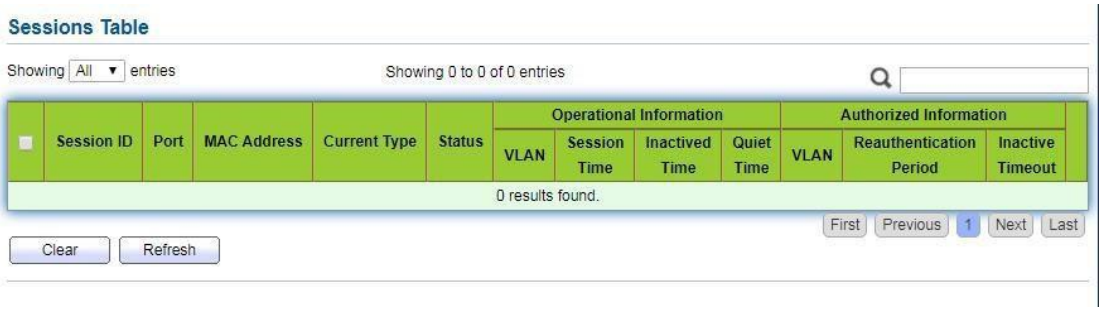
1. Haga clic en "Security > Management Manager > WEB-Based Local Account", ingrese a la interfaz de configuración de la siguiente manera:



14.5.5 Sesiones

Instrucciones:

1. Haga clic en "Security > Management Manager > Sessions", vea la interfaz de sesiones de la siguiente manera:

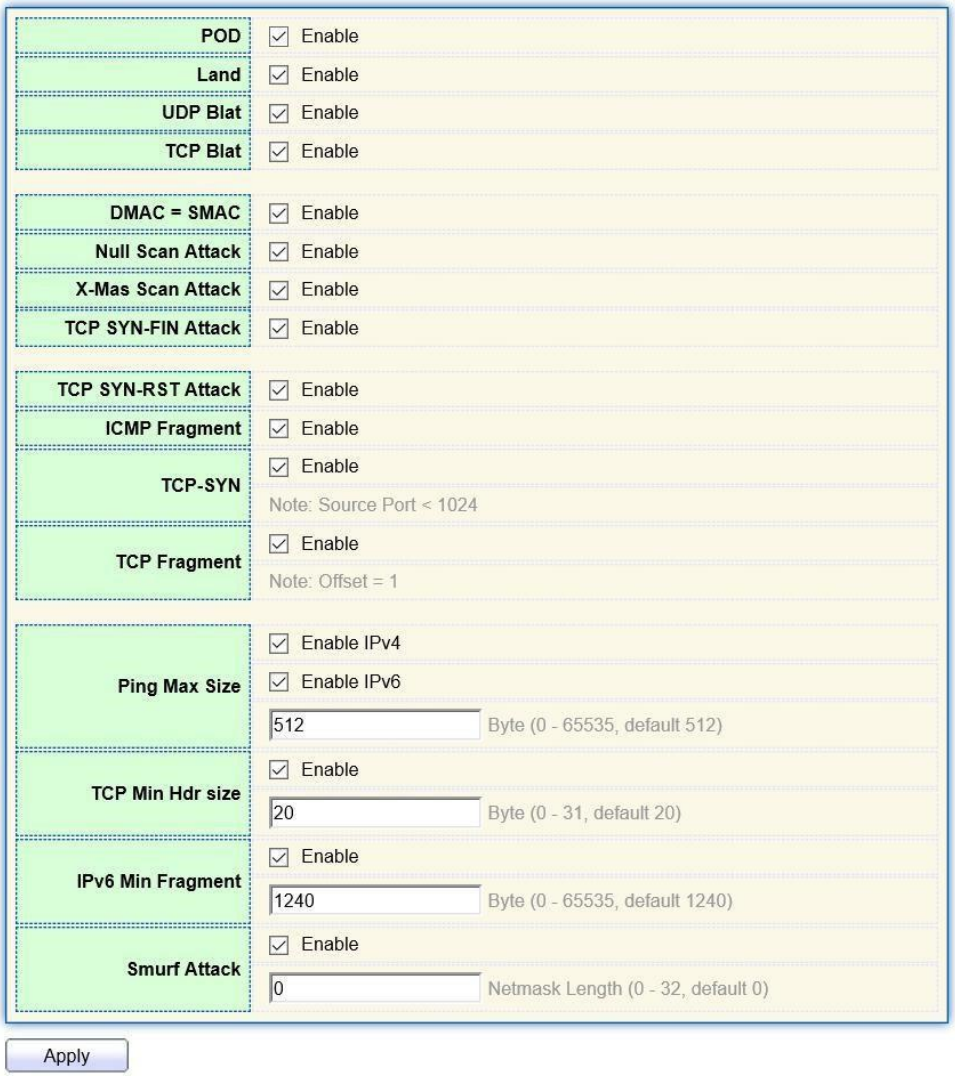


14.6 De

14.6.1 Propiedad

Habilite la opción Resistencia al ataque para que el conmutador sea más seguro. Instrucciones

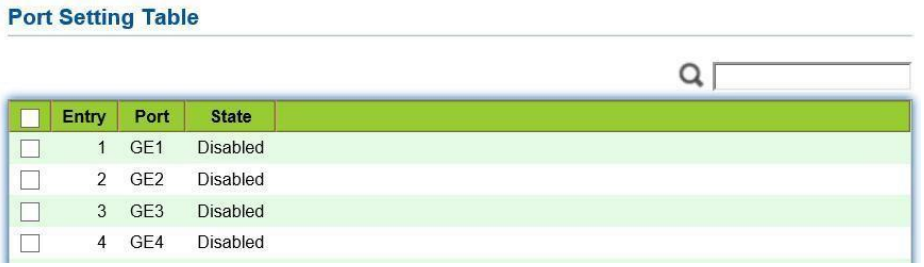
1. Haga clic en "Security > DoS > Property" en la interfaz "DoS Global Configuration" de la siguiente manera.



14.6.2 Configuración del puerto

La resistencia a ataques DoS está habilitada en función de los puertos. Instrucciones

1. Haga clic en "Security > DoS > Port Setting" de la siguiente manera:



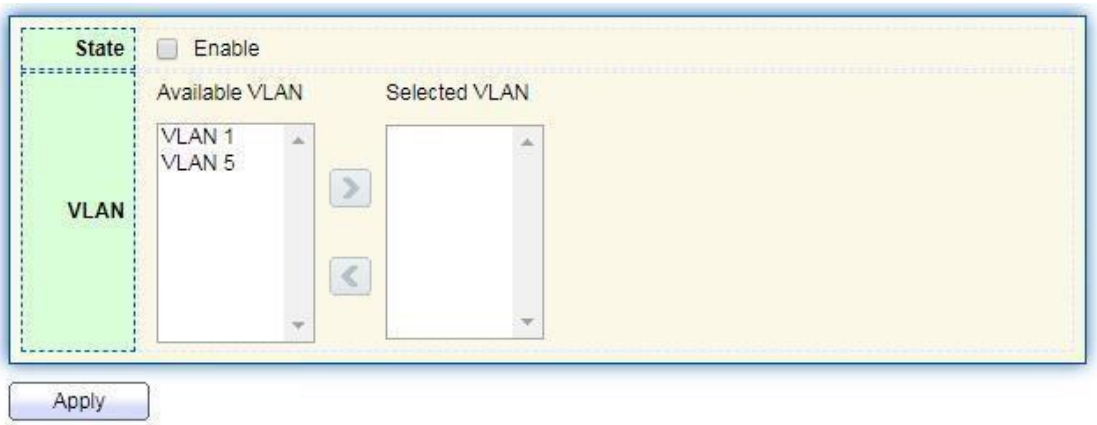
2. Seleccione y "Edite" el puerto para habilitar o deshabilitar la función de resistencia a ataques DoS de la siguiente manera.

14.7 Inspección ARP dinámica

14.7.1 Propiedad

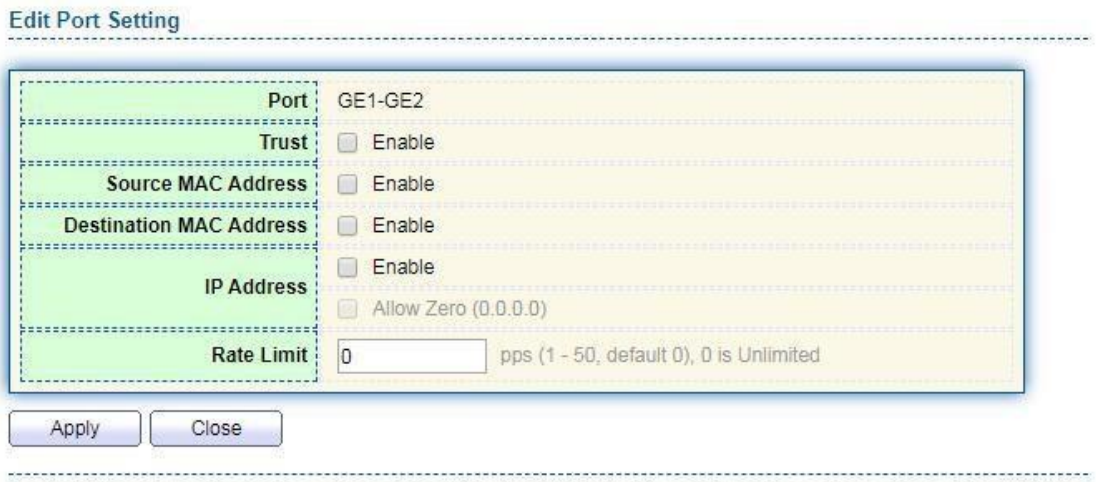
Instrucciones

1. Haga clic en "Security > Dynamic ARP Inspection > Property" ingrese a la interfaz de configuración global de la siguiente manera:



2. Seleccione el puerto y "Editar" para ingresar a la interfaz de configuración del puerto de la siguiente manera:

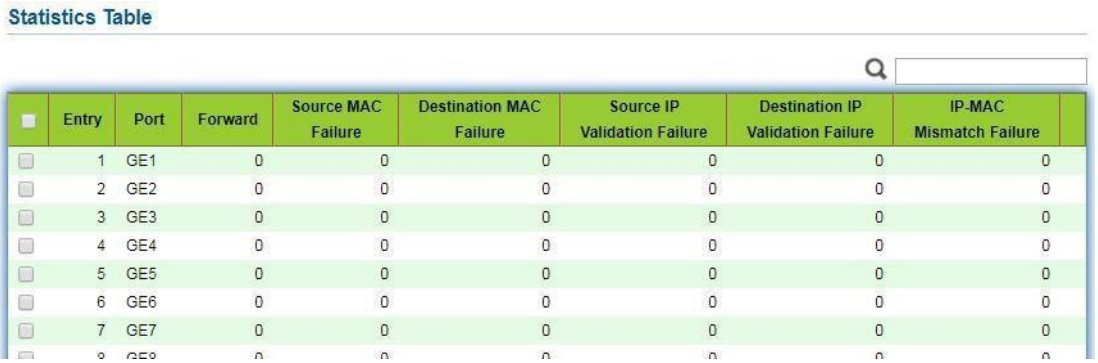
Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited
6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited



14.7.2 Estadística

Instrucciones

1. Haga clic en "Security > Dynamic ARP Inspection > Statistics" (Seguridad inspección estadísticas de ARP dinámicas) y vea las estadísticas de DAI de la siguiente manera:



Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0

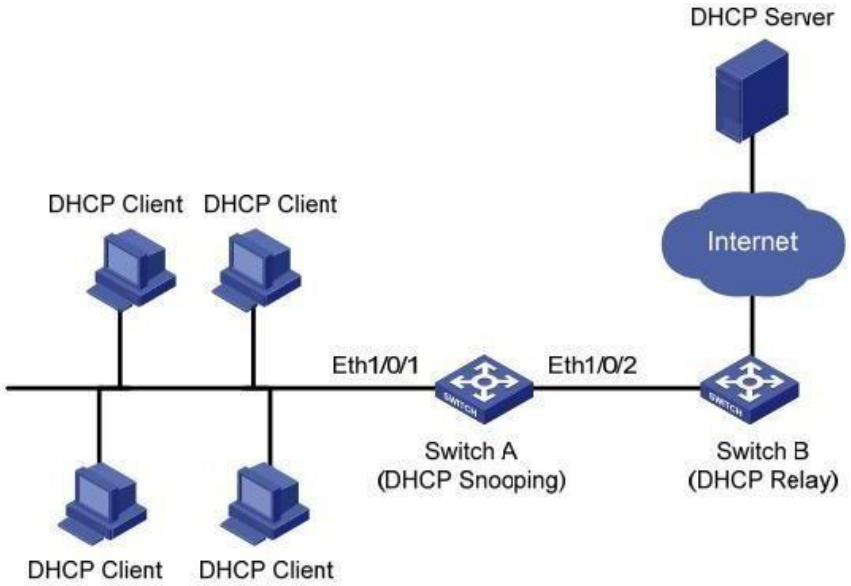
14.8 Espionaje DHCP

Por razones de seguridad, es posible que el administrador de red deba registrar la dirección IP de un usuario que navega por Internet y confirmar la correspondencia entre la dirección IP obtenida del servidor DHCP y la dirección MAC del host.

Switch puede registrar la dirección IP del usuario a través del relé DHCP seguro en la capa de red.

Switch puede monitorear los mensajes DHCP y registrar la dirección IP del usuario a través de DHCP Snooping en la capa de enlace de datos. Además, el servidor DHCP privado en la red puede provocar una dirección IP incorrecta para el usuario. Para garantizar que los usuarios obtengan direcciones IP a través del servidor DHCP legal, el mecanismo de seguridad DHCP Snooping dividelos puertos en Puerto de confianza y Puerto no confiable.

El puerto de confianza conecta directa o indirectamente el servidor DHCP legal. Reenvía el Mensajes DHCP recibidos para garantizar la dirección IP correcta para el cliente DHCP. El puerto que no confía conecta el servidor DHCP ilegal. Los mensajes DHCPACK y DHCPOFFER recibidos desde el servidor DHCP en el puerto que no confía se descartarán para evitar direcciones IP incorrectas.



Redes típicas de DHCP Snooping

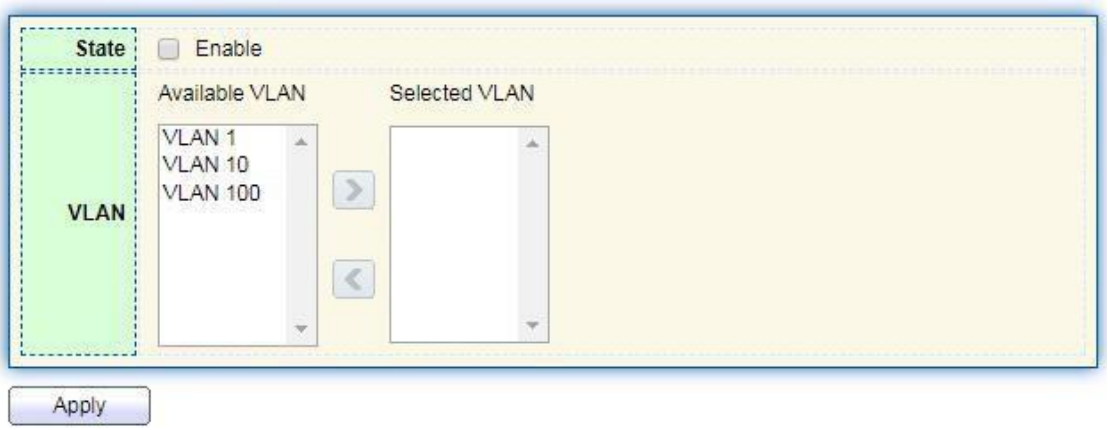
Los métodos siguientes se utilizan para obtener la dirección IP y la dirección MAC del usuario del servidor DHCP:

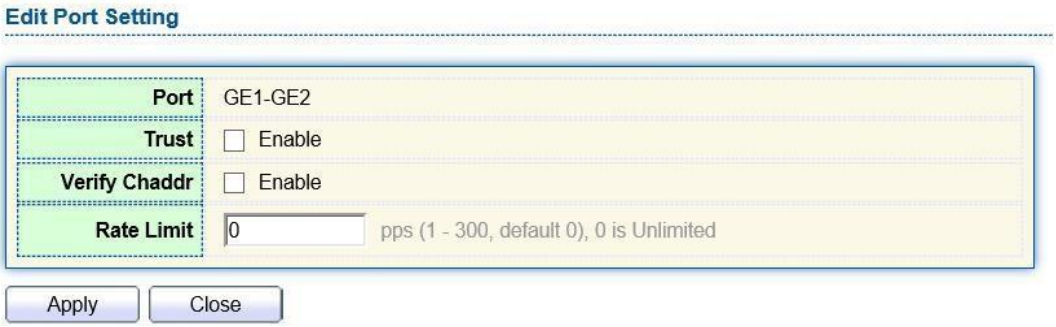
- Snooping el mensaje DHCPREQUEST
- Snooping el mensaje DHCPACK

14.8.1 Propiedad

Habilite las instrucciones de
espionaje DHCP:

1. Haga clic en "Security > DHCP Snooping > Property". Espionaje DHCP
   La interfaz se divide en configuración global y configuración de puerto . Seleccione el puerto a modificar en la configuración del puerto y "Editar" los detalles de la siguiente manera:

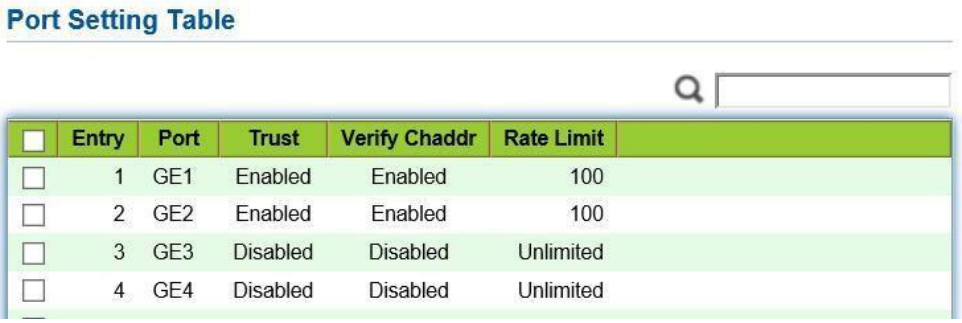




Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
State	Habilitar y deshabilitar el DHCP Snooping
VLAN	Nº de VLAN válido. de DHCP Snooping
Port	Configure el puerto No. de DHCP Snooping
Trust	Si el puerto es un puerto de confianza
Client Address Inspection	Si la inspección de coherencia para las direcciones de cliente está habilitada
Rate Limit	Si el puerto habilita el límite de velocidad y configura el valor

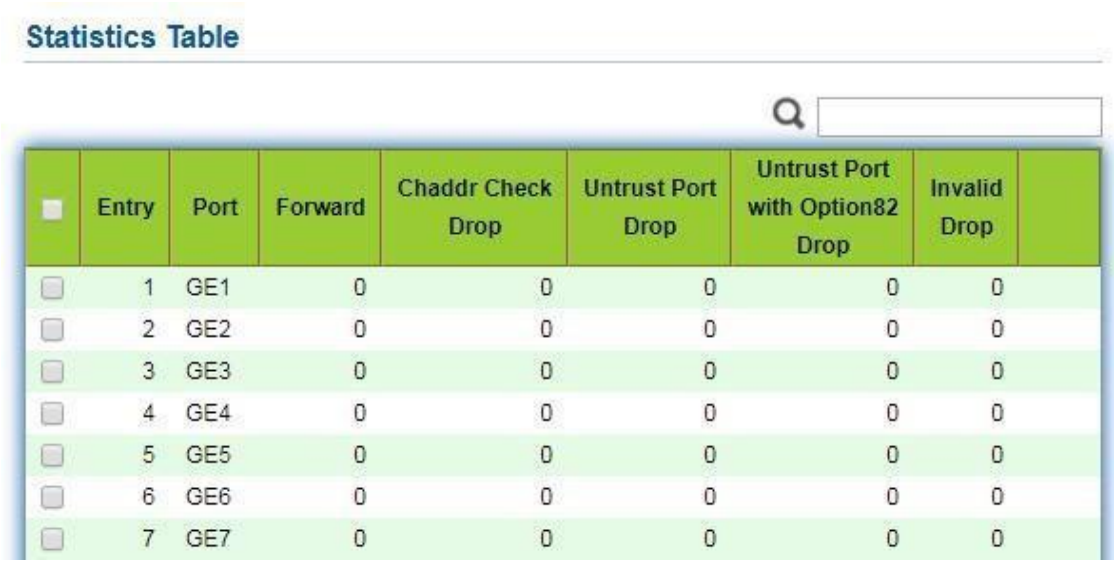
2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y terminar de la siguiente manera.



14.8.2 Estadística

Instrucciones

1. Haga clic en "Security > Dynamic ARP Inspection > Statistics" (Seguridad inspección ARP dinámica Estadísticas) ver las estadísticas de DHCP Snooping de la siguiente manera:



14.8.3 Option82 (propiedad)

Los servidores DHCP privados en la red pueden conducir a direcciones IP incorrectas obtenidas por los usuarios. El mecanismo de seguridad DHCP Snooping basado en el conmutador Ethernet PS7024 divide los puertos en puerto de confianza y puerto no confiable para proporcionar las direcciones IP a través de servidores DHCP legales.

- El puerto de confianza conecta directa o indirectamente el servidor DHCP legal. Garantiza la dirección IP correcta para el cliente DHCP mediante el reenvío de los mensajes DHCP recibidos.
- Untrust Port conecta servidores DHCP ilegales. Los mensajes DHCP ACK y DHCPOFFER respondidos por el servidor DHCP en puertos que no sean de confianza se descartarán para evitar direcciones IP incorrectas.

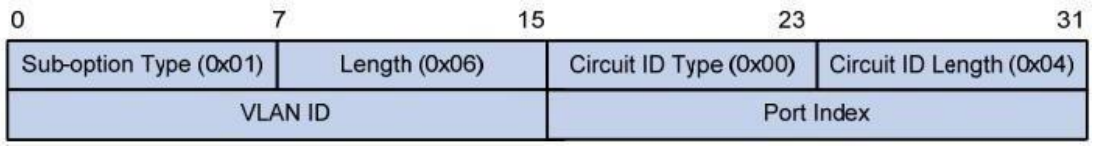
La opción 82 es la opción de información del agente de retransmisión en los mensajes DHCP, que indicala ubicación del cliente DHCP. Cuando el relé DHCP (o dispositivo DHCP Snooping) recibe la solicitud, mensaje enviado desde el cliente DHCP al servidor DHCP, los administradores pueden agregar la opción 82 para localizar el cliente DHCP y controlar la seguridad, el costo, etc. Los servidores que admiten la opción 82 crean enfoques más flexibles para la asignación de direcciones en línea con las direcciones IP y otras políticas de asignación de parámetros.

En la opción 82 figuran hasta 255 subopciones. Debe definirse al menos una subopción si se define la opción 82. El dispositivo actual admite 2 subopciones: Subopción de ID de circuito y Subopción de ID remoto

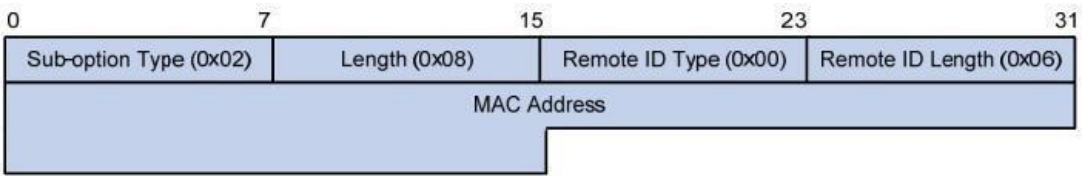
Los fabricantes generalmente llenan las opciones según sea necesario, ya que RFC 3046 no logra uniformar las opciones de la Opción 82. Como dispositivo de retransmisión DHCP, el conmutador Ethernet admite los formatos de relleno extendidos para las subopciones de la opción 82 y los valores predeterminados de relleno son los siguientes:

- Subopción 1: VLAN No. y el índice de puerto (número físico del puerto menos 1) del puerto que recibe el mensaje de solicitud enviado por el cliente DHCP.
- Suboptación2: dirección MAC del puente del dispositivo de retransmisión DHCP que recibe el mensaje de solicitud del cliente DHCP.

Subopción 1: VLAN No. y el índice de puerto (número físico del puerto menos 1) del puerto que recibe el mensaje de solicitud enviado por el cliente DHCP de la siguiente manera.



Subopción 2: dirección MAC puente del dispositivo de retransmisión DHCP que recibe el mensaje DHCPREQUEST del cliente DHCP.



Mecanismo de compatibilidad con la retransmisión DHCP de la opción 82

Los procesos de adquisición de la dirección IP del cliente DHCP del servidor DHCP a través del relé DHCP son básicamente los mismos que los directamente del servidor DHCP. Los pasos de descubrimiento, aprovisionamiento, selección y validación son esenciales. El mecanismo de soporte de la retransmisión DHCP se introduce de la siguiente manera:

(1) La retransmisión DHCP comprobará la opción 82 en el mensaje DHCPREQUEST recibido y la manejará en consecuencia.

- Para los mensajes existentes de la Opción 82, la retransmisión DHCP se procesará de acuerdo con las políticas de configuración (descartar, reemplazar con la opción 82 de la retransmisión o mantener la opción 82 original) y, a continuación, se reenviará a DHCP Server.
- Para los mensajes sin la opción 82, la retransmisión DHCP agregará y reenviará los nuevos mensajes al servidor DHCP.

(2) La retransmisión DHCP desactivará la opción 82 del mensaje de respuesta recibido del servidor DHCP y, a continuación, reenviará el mensaje con la información de configuración de DHCP al cliente DHCP.

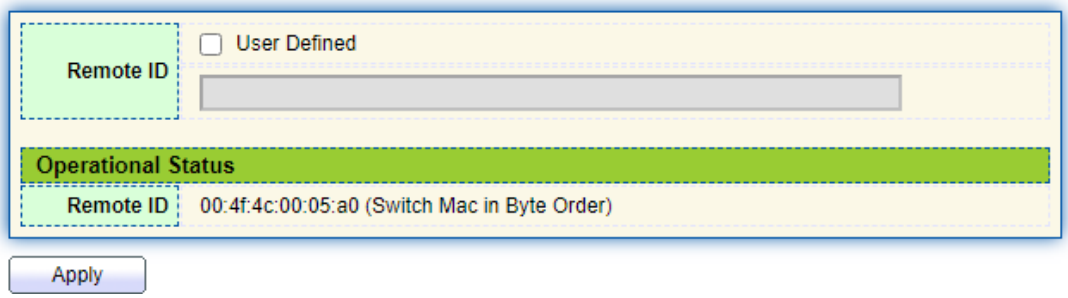
Descripción:

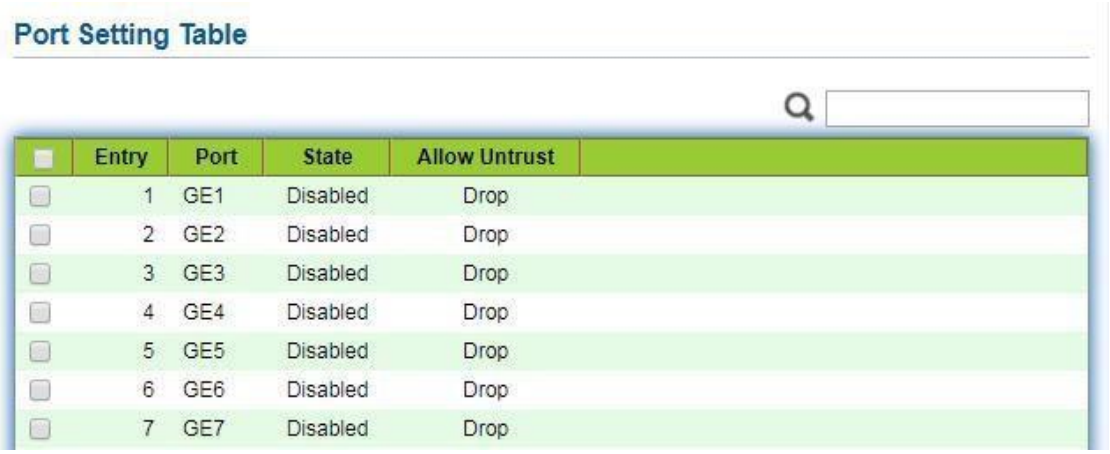
El cliente DHCP transmite un mensaje DHCPDISCOVERY y un mensaje DHCPREQUEST. DHCP relay agregará la opción 82 a ambos mensajes debido a los diferentes mecanismos de procesamiento de los servidores DHCP de los fabricantes para el mensaje de solicitud. Algunos dispositivos controlan la opción 82 en el mensaje DHCPDISCOVERY, mientras que otros la controlan en el mensaje DHCPREQUEST.

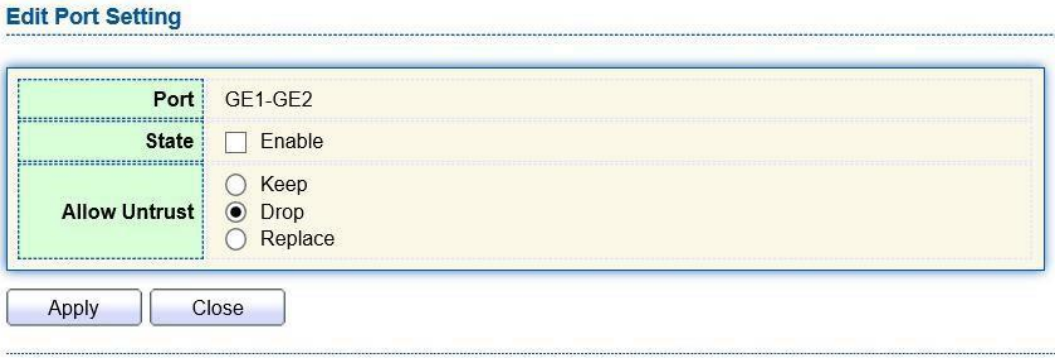
Un switch con funcionesDHCP Snooping y Option 82 recibe mensajes DHCPREQUEST con la opción 82 enviados por clientes DHCP. DHCP Snooping toma diferentes mecanismos de procesamiento de acuerdo con diferentes estrategias de procesamiento de configuración y contenidos de subopciones.

Instrucciones:

1. Haga clic en "Security > DHCP Snooping > Option82 Property". Las configuraciones globales y de puerto están contenidas. Seleccione el puerto a configurar y "Editar" los detalles de la siguiente manera:







Los campos de la interfaz son como a continuación.

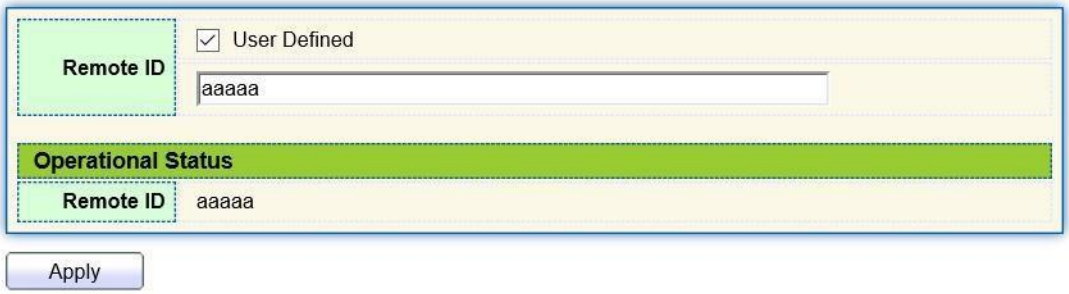
Elementos de configuración	Descripción
Remote ID	Rellene los campos ID remoto de la opción 82 (como XXXX definido por el usuario)
Port	Si el puerto No. de la opción 82 está habilitada
Untrust Port Access	Untrust Port procesa los mensajes con la opción 82 habilitada: Mantenimiento: deje la opción 82 en el mensaje sin cambios y reenvíela Descartar: descartar el mensaje Sustitución: sustituya y reenvíe el campo Opción 82 del mensaje según la configuración del ID del circuito

Descripción:

El campo Option82 configura de forma independiente las sub opciones Circuit ID o RemoteID. Se puede configurar individualmente o simultáneamente sin ningún orden específico. La opción DHCP 82 debe configurarse en la barra de usuario, de lo contrario, los mensajes DHCPenviados al servidor DHCP no llevarán la opción 82.

Al recibir el mensaje de respuesta DHCP del servidor DHCP, el mensaje que contiene la opción 82 se reenviará después de eliminar el campo o se reenviará directamente si el mensaje no contiene la opción 82.

2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y terminar de la siguiente manera.



Apply

Port Setting Table

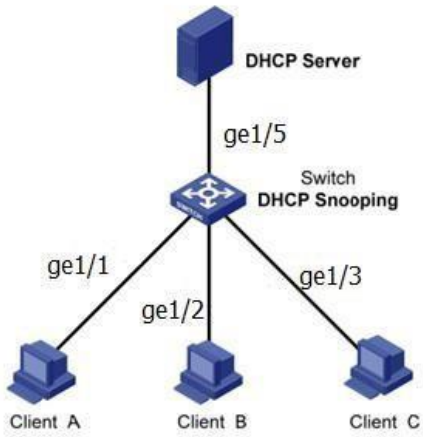
Entry	Port	State	Allow Untrust
1	GE1	Enabled	Replace
2	GE2	Enabled	Replace
3	GE3	Enabled	Replace
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop

Ilustración de la configuración típica de DHCP Snooping

Como se muestra a continuación, el puerto del conmutador GE1-5 está conectado al servidor DHCP y los puertos GE1-1, 2 y 3 están conectados al cliente DHCP A, B y C respectivamente.

- Habilite DHCP Snooping en el switch.
- Establezca el GE1-5 como el puerto de confianza de DHCP Snooping.
- Active la función de compatibilidad con la opción 82 en el conmutador. Para el mensaje GE1-3 que fluye a través del puerto, rellene la opción 82 de acuerdo con la configuración predeterminada de ID de circuito e ID remoto.

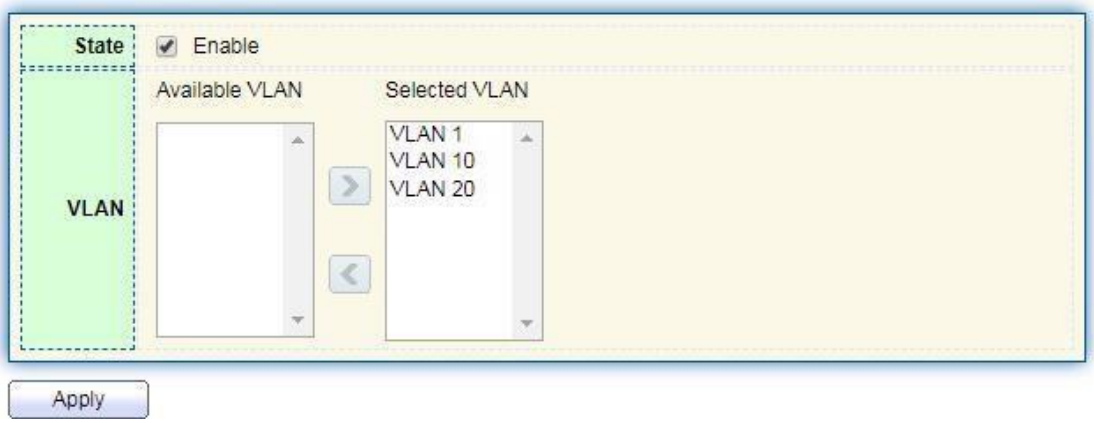
Network Diagram



Configure DHCP snooping to support Option 82

Instrucciones:

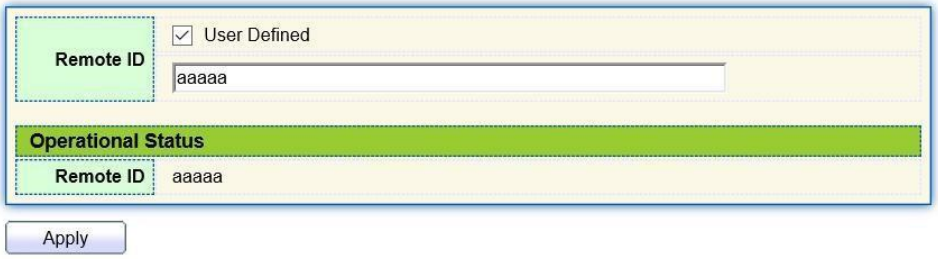
1. Habilite el snooping DHCP del conmutador. Haga clic en "Security > DHCP Snooping > Property" en el menú de navegación para habilitar la función de la siguiente manera:

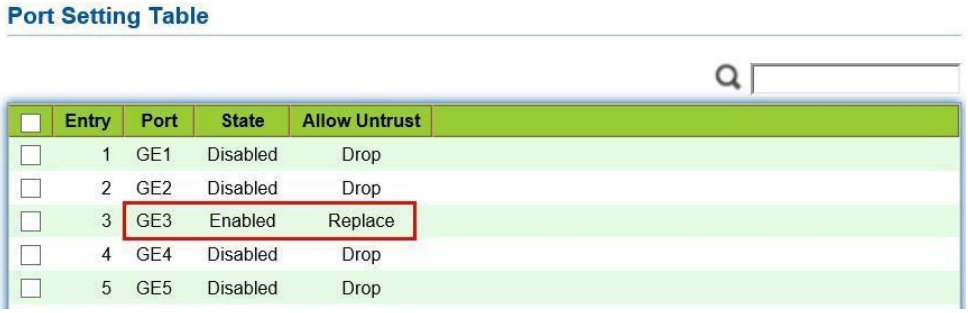


2. Establezca el GE1-5 como el puerto de confianza de DHCP Snooping, complete las configuraciones correspondientes y "Editar" de la siguiente manera:

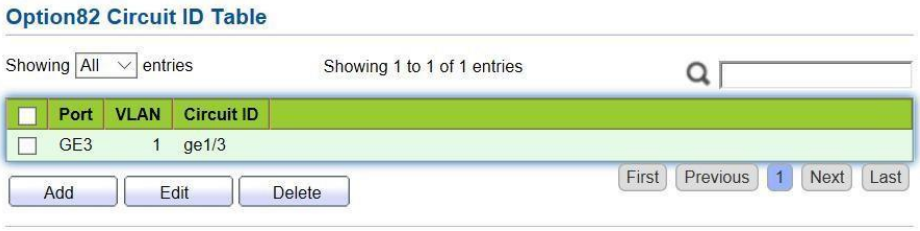
3. Configure en el puerto GE3 para que el ID remoto definido por el usuario se pueda establecer mediante la opción 82.

   Haga clic en "Security > DHCP Snooping > Option82 Property", verifique y configure el puerto. "Aplicar" y terminar de la siguiente manera:





4. Configure en el puerto GE3 para que el ID del circuito se pueda establecer mediante la opción 82. Haga clic en el botón
"Security > DHCP Snooping > Option82 Circuit ID" para configurar el puerto.
"Aplicar" y terminar de la siguiente manera:



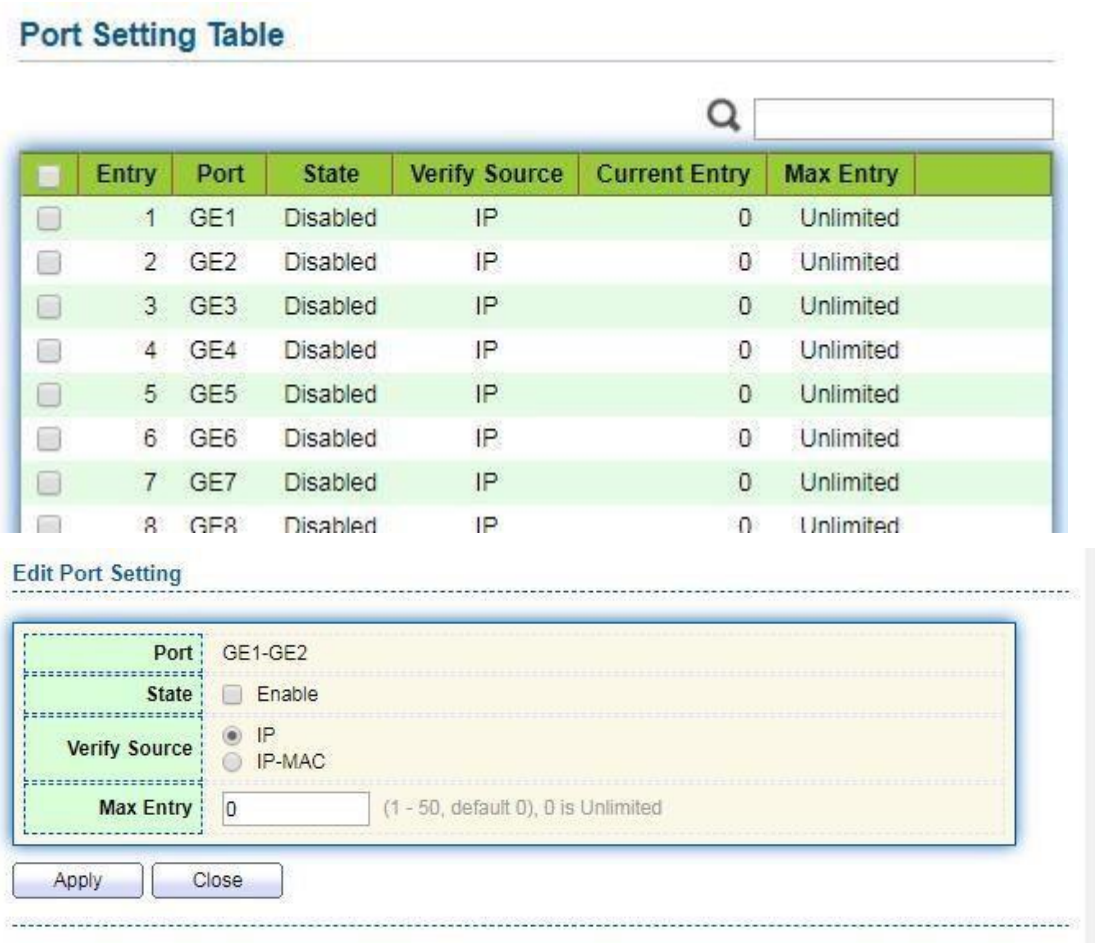
14.9 Protección de origen IP

IP source guard (IPSG) es una tecnología de filtrado de tráfico de puertos basada en IP / Mac, que puede evitar ataques de suplantación de direcciones IP en LAN. IPSG puede garantizar que la dirección IP del dispositivo terminal en la red de capa 2 no será secuestrada, y también puede garantizar que el dispositivo no autorizado no pueda acceder a la red o atacar la red a través de su propia dirección IP especificada, lo que resulta en un bloqueo y parálisis de la red.

14.9.1 Configuración del puerto

Instructions

1. Haga clic en "Security> IP Source Guard > PortSetting" ingrese a la interfaz de configuración del puerto de la siguiente manera:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	Lista de puertos
State	Habilitar o deshabilitar IPSG
Verify Source	Dirección IP de origen predeterminada del filtro Source Guard. El "IP-MAC" filtra no solo la dirección IP de origen, sino también la dirección MAC de origen
Max Entry	Número máximo de puertos permitidos

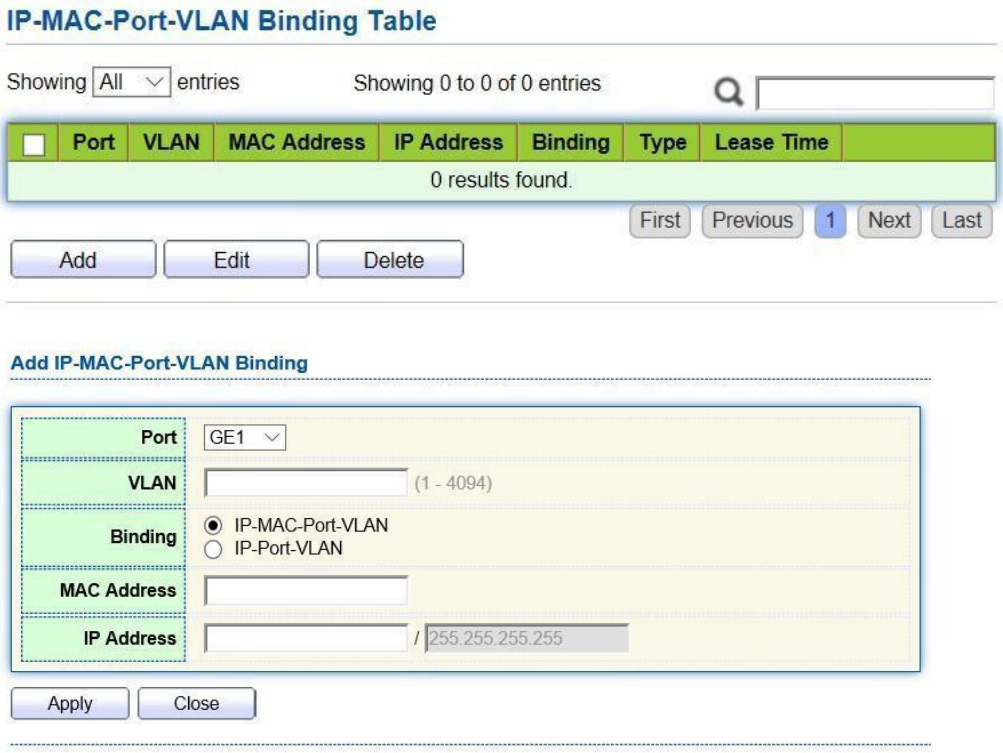
14.9.2 Enlace IMPV

En la red DHCP, los usuarios (usuarios no DHCP) que obtienen direcciones IP estáticamente pueden atacar la red imitando el servidor DHCP, construyendo un mensaje de solicitud DHCP, etc. Los usuarios legales de DHCP pueden sufrir riesgos de seguridad al usar la red normalmente.

Habilitar las entradas MAC estáticas basadas en la interfaz generada por la tabla de enlace DHCP Snooping puede evitar tales ataques. Luego, el dispositivo, basado en la tabla de enlace DHCP Snooping correspondiente a todos los usuarios DHCP, ejecuta automáticamente el comando para generar entradas MAC estáticas y deshabilitar la capacidad de aprendizaje de la interfaz. de entradas dinámicas. Solo los mensajes que coinciden con el MAC de origen y las entradas MAC estáticas pueden fluir a través de la interfaz. Por lo tanto, para los usuarios que no son DHCP, sólo los mensajes de entradas MAC estáticas configuradas manualmente por los administradores pueden fluir, mientras que otros serán descartados.

Instrucciones:

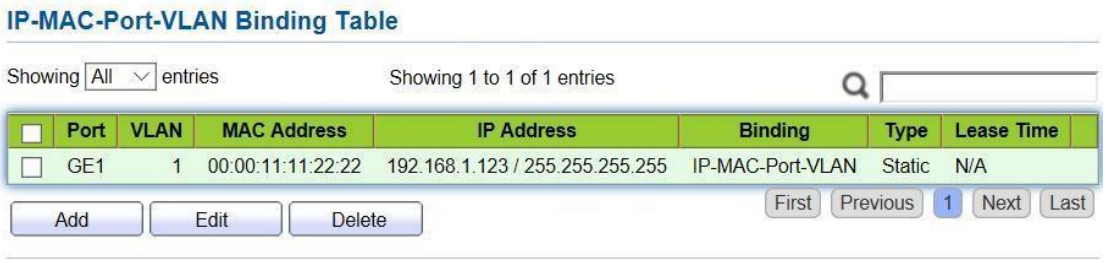
1. Haga clic en "Security > IP Source Guard > IMPV Binding", "Add" un nuevo grupo de enlace de IP-MAC-Port-VLAN de la siguiente manera:



Los campos de la interfaz son como a continuación.

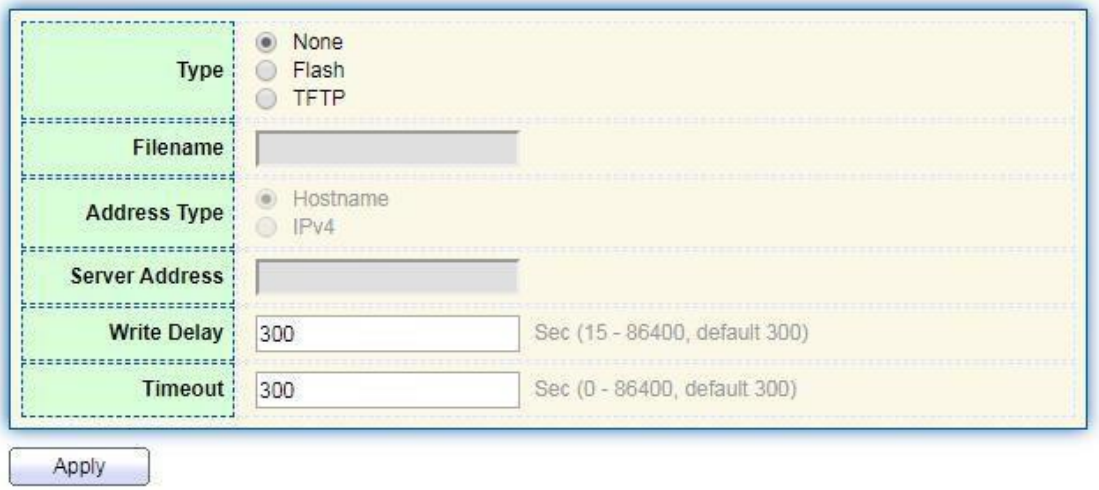
Elementos de configuración	Descripción
Port	El puerto No. del grupo de enlace
VLAN	ID de VLAN enlazado
Binding	Seleccione la relación de enlace entre IPMV e IPV
MAC Address	Dirección MAC enlazada
IP Address	Dirección IP enlazada

2. Completa los elementos de configuración correspondientes.
3. "Aplicar" y terminar de la siguiente manera.



4. Haga clic en "Security > IP Source Guard > Save Database" ingrese a la

base de datos. interfaz de la siguiente manera:



15 ACL

La expansión de la escala de la red y el flujo de montaje fortalecen la posición del control de seguridad de la red y la asignación de ancho de banda. El filtrado de paquetes evita el acceso de usuarios ilegales, controla el flujo y ahorra recursos de red. ACL (Lista de control de acceso) filtra los paquetes configurando los mensajes que coinciden con los procedimientos y los métodos de procesamiento.

El puerto del switch que recibe mensajes analiza el campo de acuerdo con las reglas actuales de ACL. Una vez que se identifica un mensaje específico, se permitirá o prohibirá que fluya de acuerdo con políticas predeterminadas.

Las reglas de apareo de paquetes definidas por ACL también pueden ser referenciadas por otras funciones que requieren distinción de flujo, como la definición de reglas de clasificación de flujo QoS.

ACL puede filtrar paquetes estableciendo reglas coincidentes y métodos de procesamiento. ACL es una colección de condiciones de permiso y denegación aplicables a los paquetes. Cuando la interfaz recibe los paquetes, el conmutador compara los campos y la ACL para determinar los paquetes permitidos y denegados sujetos a estándares especificados. ACL clasifica los paquetes por condiciones de control, que pueden ser la dirección MAC de origen/destino, la dirección IP de origen/destino, el puerto No. y así sucesivamente. ACL clasifica los paquetes por condiciones coincidentes, que pueden ser la dirección de origen/destino, el número de puerto, etc. ACL se puede dividir en las siguientescategorías de acuerdo con los propósitos de aplicación:

La ACL IP básica formula reglas basadas únicamente en la dirección IP de origen de los paquetes. El ID de ACL varía de 100 a 999. Advanced IP ACL prepara reglas de acuerdo con la dirección IP de origen/destino de los paquetes, los tipos de protocolo transportados por
IP, e información de capa 3 o 4, como las características del protocolo. El ID de ACL varía de 100 a 999.
ACL L2: Las reglas se realizan de acuerdo con la dirección MAC de origen/destino de los paquetes, la prioridad 802.1p y la información L2, como el tipo de protocolo. El ID de ACL varía de 1 a 99.

15.1 ACL MAC

ACL L2: las reglas se realizan de acuerdo con la dirección MAC de origen/destino, la prioridad VLAN y la información L2, como el tipo de protocolo.

Instrucciones:

1. Haga clic en “ACL > MAC ACL" en el menú de navegación de la siguiente manera.

Los campos de la interfaz son como a continuación.

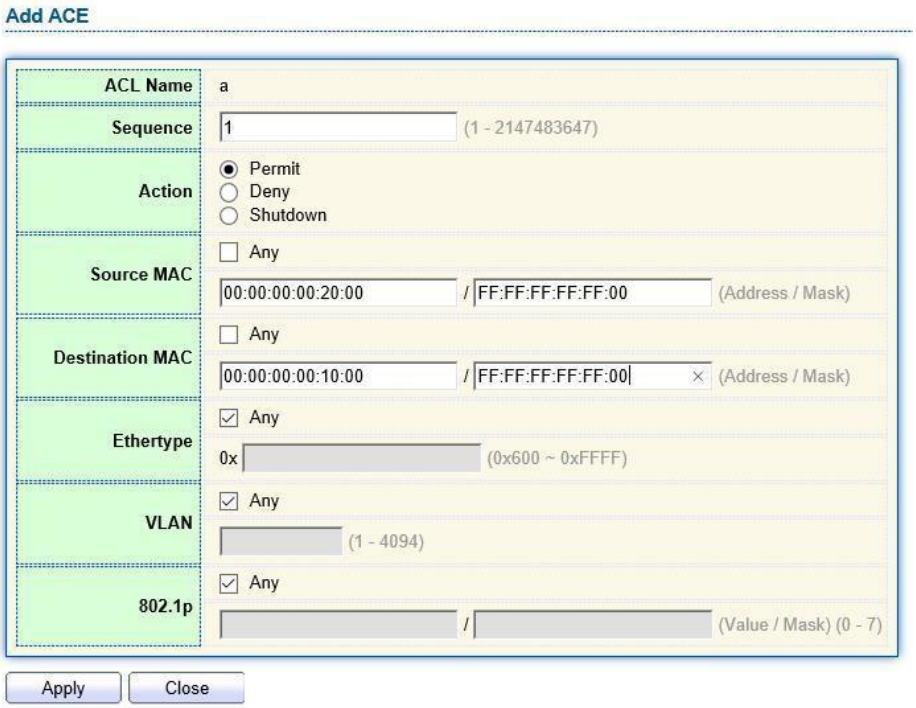
Elementos de configuración	Descripción
ACL Name	Asigne un nombre a las reglas de ACL de MAC

2. Haga clic en “ACL > MAC ACE" en el menú de navegación, "Agregar" el nombre de ACL de la siguiente manera:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Nombre de ACL	La lista de reglas de ACL se prepara en función de la configuración de ACL de MAC.

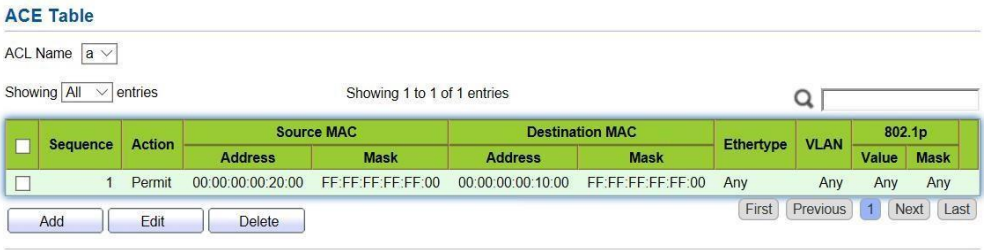
3. Completa los elementos de configuración correspondientes.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
ACL Name	La lista de reglas de ACL se prepara en función de la configuración de ACL de MAC.
Sequence	La ACL MAC varía de 1 a 2.147.483.647
Action	Las acciones de ACL se dividen en "Permitir" o "Denegar", así como "Cerrar".
Source MAC	Introduzca la dirección MAC de origen y la máscara de las reglas de ACL con el formato H.H.H.H.H.H. Seleccione "Cualquiera" para representar cualquier dirección MAC
Destination MAC	Introduzca la dirección MAC de destino y la máscara de las reglas ACL con el formato H.H.H.H.H.H . Seleccione "Cualquiera" para representar cualquier dirección MAC
EtherType	Ingrese el tipo Ethernet de reglas ACL que van desde 0 x 600 a 0 x FFFF, seleccione "Cualquiera" para representar cualquier tipo.
VLAN	Ingrese la VLAN de las reglas de ACL que van de 1 a 4,094, seleccione "Cualquiera" para representar cualquier VLAN
802.1p	Ingrese la prioridad VLAN y la máscara de las reglas de ACL que van del 1 al 7, seleccione "Cualquiera" para representar cualquier prioridad de VLAN

4. "Aplicar" y Finalizar de la siguiente manera.



15.2 ACL IPv4

La ACL (ACL de IP básica) basada en IPv4 formula reglas según la dirección IP de origen de los paquetes solamente. El ID de ACL varía de 100 a 999.

Las reglas avanzadas de ACL IP se realizan de acuerdo con la dirección IP de origen/destino de los paquetes, el tipo de protocolo transportado por IP y la información de capa 3 o 4, como las características del protocolo. El ID de ACL varía de 100 a 999.

Instrucciones

1. Haga clic en “ACL > IPv4 ACL" en el menú de navegación de la siguiente manera.

Los campos de la interfaz son como a continuación.

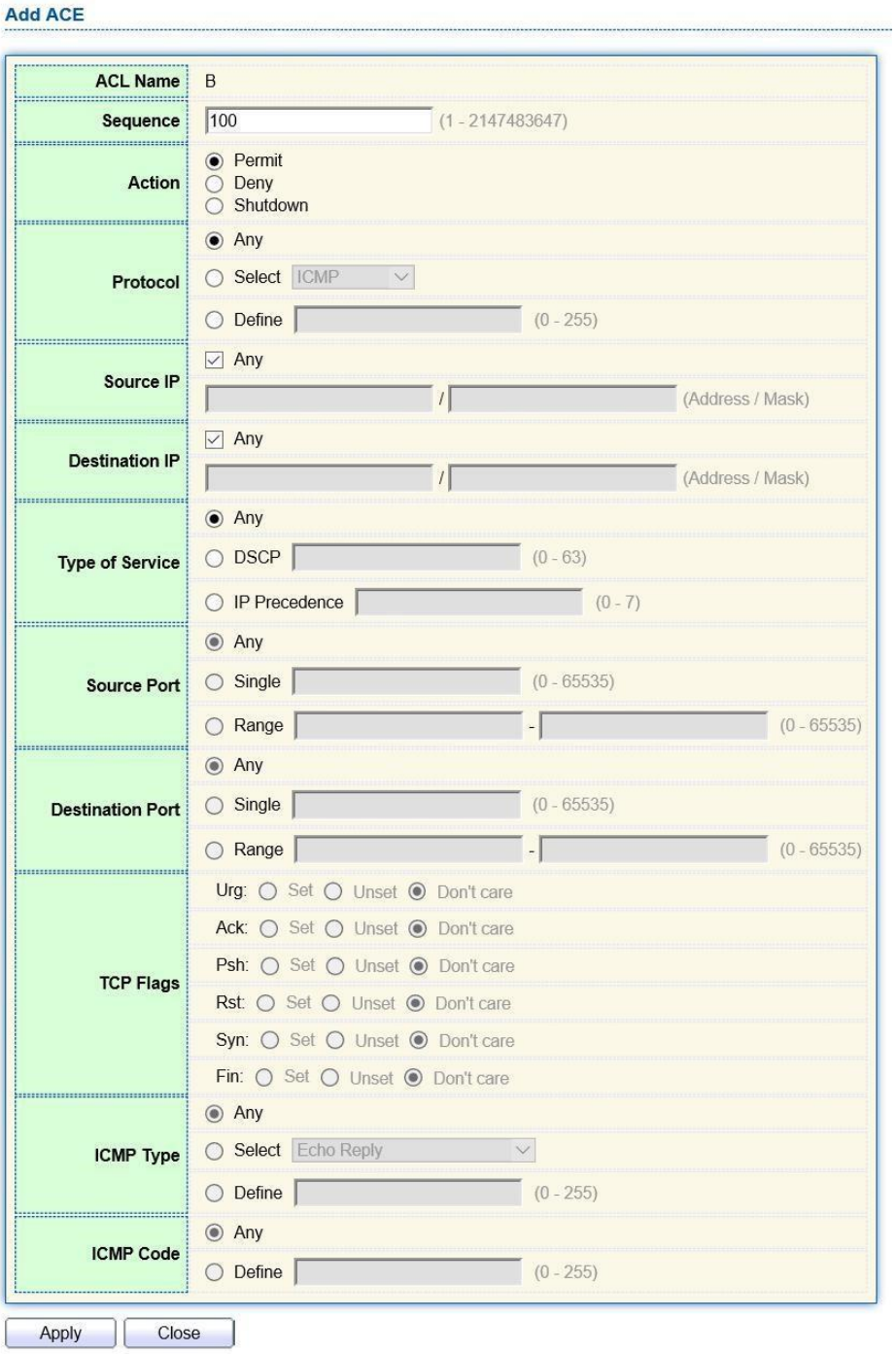
Elementos de configuración	Descripción
ACL Name	Asigne un nombre a las reglas de ACL IPv4

2. Haga clic en “ACL > IPv4 ACE" en el menú de navegación, "Agregar" el nombre de ACL de la siguiente manera:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
ACL Name	La lista de reglas de ACL se realiza en función de la configuración de ACL IPv4.

3. Completa los elementos de configuración correspondientes.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
ACL Name	La lista de reglas de ACL se realiza en función de la configuración de ACL IPv4.
Sequence	La ACL IPv4 oscila entre 1 y 2.147.483.647.
Action	Las acciones de ACL se dividen en "Permitir" o "Denegar", así como "Cerrar".
Protocol	Es necesario seleccionar el tipo de protocolo, como ICMP, TCP y UDP. Seleccione "Cualquiera" para representar cualquier protocolo.
Source IP	Introduzca la IP de origen y la máscara de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier IP de origen.
Destination IP	Introduzca la IP de destino y la máscara de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier IP de destino.
Type of Service	Introduzca el tipo de servicio de las reglas de ACL, como DSCP (0-63) y IP priority (0-7). Seleccione "Cualquiera" para representar cualquier tipo de servicio .
Source Port	Introduzca el puerto de origen de las reglas de ACL, como el puerto único No. o segmento de rango (0-65,535). Seleccione "Cualquiera" para representar cualquier puerto de origen.
Destination Port	Introduzca el puerto de destino de las reglas de ACL, como el puerto único No. o segmento de rango (0-65,535). Seleccione "Cualquiera" para representar cualquier puerto de destino.
TCP Flags	Ingrese las banderas TCP de las reglas de ACL, COMO URG, ACK, PSH, RST, SYN, FIN, con acciones como "Establecer", "Desestablecer" y "No me importa".
ICMP Type	Introduzca el tipo de mensaje ICMP de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier tipo de ICMP.
ICMP Code	Introduzca el valor de código ICMP de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier valor de campo.

3. " Aplicar" y finalizar de la siguiente manera.

ACE Table

ACL Name B

Showing All entries Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
	100	Permit	Any (IP)	Any		Any					Any	Any		

Add Edit Delete

First Previous 1 Next Last

15.3 ACL IPv6

Instrucciones

1. Haga click en “ACL > IPv6 ACL” en el menú de navegación como se indica a continuación.

Los campos de la interfaz son como a continuación.

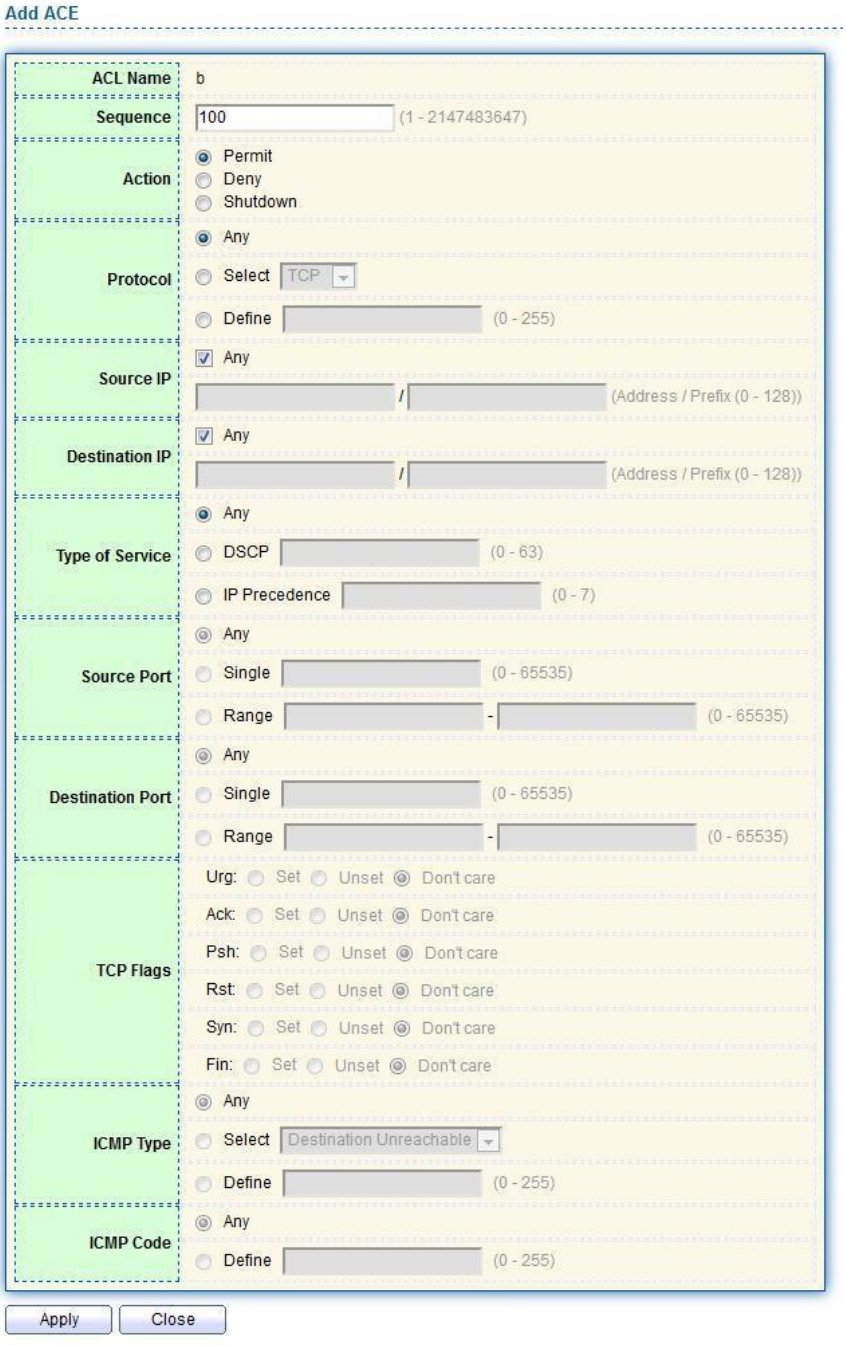
Elementos de configuración	Descripción
Nombre de ACL	Asigne un nombre a las reglas de ACL IPv6

2. Haga clic en "ACL > IPv6 ACE" en el menú de navegación, "Add" the ACL Name de la siguiente manera:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Nombre de ACL	La lista de reglas de ACL se realiza en función de la configuración de ACL IPv6.

3. Completa los elementos de configuración correspondientes.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
ACL Name	La lista de reglas de ACL se realiza en función de la configuración de ACL IPv6.
Sequence	La ACL IPv6 oscila entre 1 y 2.147.483.647.
Action	Las acciones de ACL se dividen en "Permitir" o "Denegar", así como "Cerrar".
Protocol	Es necesario seleccionar el tipo de protocolo, como ICMP, TCP y UDP. Seleccione "Cualquiera" para representar cualquier protocolo.
Source IP	Introduzca la IP de origen y la máscara de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier IP de origen.
Destination IP	Introduzca la IP de destino y la máscara de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier IP de destino.
Type of Service	Introduzca el tipo de servicio de las reglas de ACL, como DSCP (0-63) y IP priority (0-7). Seleccione "Cualquiera" para representar cualquier servicio tipo.
Source Port	Introduzca el puerto de origen de las reglas de ACL, como el puerto único No. o segmento de rango (0-65,535). Seleccione "Cualquiera" para representar cualquier puerto de origen.
Destination Port	Introduzca el puerto de destino de las reglas de ACL, como el puerto único No. o segmento de rango (0-65,535). Seleccione "Cualquiera" para representar cualquier puerto de destino.
TCP Flags	Ingrese las banderas TCP de las reglas de ACL, COMO URG, ACK, PSH, RST, SYN, FIN, con acciones como "Establecer", "Desestablecer" y "No me importa".
ICMP Type	Introduzca el tipo de mensaje ICMP de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier tipo de ICMP.
ICMP Code	Introduzca el valor del código ICMP de las reglas ACL. Seleccione "Cualquiera" para representar cualquier valor de campo.

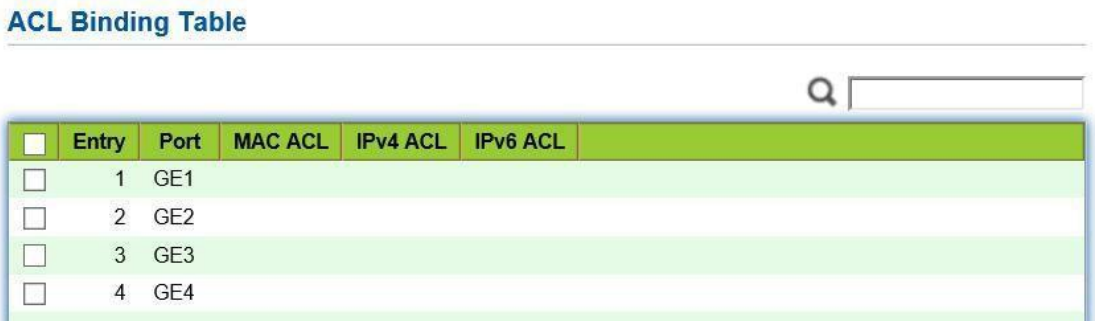
4. "Aplicar" y Finalizar de la siguiente manera.

15.4 Enlace de ACL

Una vez creada la lista, debe estar vinculada a cada interfaz requerida.

Instrucciones:

1. Haga click en “ACL > ACL Binding” en el menú de navegación.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
MAC ACL	Nombre de ACL MAC enlazado al puerto
IPv4 ACL	Nombre de ACL IPv4 enlazado al puerto (mutuamente excluyente con IPv6 ACL)
IPv6 ACL	Nombre de ACL IPv6 enlazado al puerto (mutuamente excluyente con ACL IPv4)

2. Completa los elementos de configuración correspondientes, tomando como ejemplos los MAC ACL a, IPv4 ACL b, IPv6 ACL c creados.

3. "Aplicar" y Finalizar de la siguiente manera.

16 QoS

QoS (Quality of Service) evalúa la capacidad de los proveedores de servicios para satisfacer las necesidades de los clientes y la capacidad de transmitir paquetes a través de Internet. Los servicios diversificados se pueden evaluar en función de diferentes aspectos. QoS generalmente se refiere a la evaluación de las capacidades de servicio que admiten requisitos básicos como ancho de banda, retraso, variación de retraso y tasa de pérdida de paquetes durante la entrega. El ancho de banda, también conocido como rendimiento, se refiere al flujo comercial promedio dentro de un cierto período de tiempo, con la unidad de Kbit / s. El retraso se refiere al tiempo promedio requerido para que el negocio fluya a través de la red. Para un dispositivo de red, los siguientes son niveles generales de requisitos de retardo. Hay dos niveles de retraso, es decir, el negocio de alta prioridad se puede servir lo antes posible mediante el método de programación de la cola de prioridad, mientras que el negocio de baja prioridad obtiene servicios después de eso. La variación de retardo se refiere al cambio de tiempo del negocio que fluye a través de la red. La tasa de pérdida de paquetes se refiere al porcentaje de flujo de negocios perdido durante la transmisión. Como los sistemas de transmisión modernos son muy confiables, la información a menudo se pierde en la congestión de la red. La pérdida de paquetes debido al desbordamiento de la cola es la situación más común.

Todos los mensajes en una red IP tradicional se tratan por igual. Cada dispositivo de red procesa los mensajes sobre una base FIFO, y hace todo lo posible para transmitirlos a destinos sin garantizar la fiabilidad, el retraso de la transferencia u otro rendimiento.

La calidad del servicio de red se mejora constantemente a medida que siguen surgiendo nuevas aplicaciones en la red IP que cambia rápidamente. Por ejemplo, VoIP, vídeo y otros servicios sensibles al retraso han establecido normas más estrictas sobre el retraso en la transmisión de mensajes. La transmisión de mensajes en un corto período ha sido la tendencia común. Para soportar servicios de voz, vídeo y datos con diferentes requisitos, la red necesita identificar los tipos de negocio y proporcionar los servicios correspondientes.

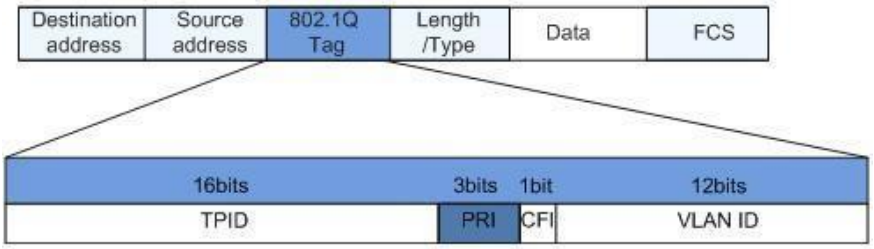
La capacidad de distinguir los tipos de negocio es el requisito previo para proporcionar los servicios correspondientes, por lo que el servicio tradicional de mejor esfuerzo ya no satisface las necesidades de la aplicación. Por lo tanto, QoS nace. Regula el flujo de la red para evitar y manejar la congestión de la red y reducir la tasa de pérdida de paquetes. Mientras tanto, los usuarios pueden disfrutar de anchos de banda dedicados, mientras que las empresas pueden mejorar la calidad del servicio, perfeccionando así la capacidad de servicio de la red.

Las prioridades de QoS varían según los tipos de mensaje. Por ejemplo, el mensaje VLAN utiliza 802.1p, también conocido como el campo CoS (clase de servicio), mientras que el mensaje IP utiliza DSCP. Para mantener la prioridad, estos campos deben asignarse a la puerta de enlace conectada con varias redes cuando los mensajes fluyen a través de la red.

Prioridad 802.1p en el encabezado de trama VLAN

Normalmente, las tramas VLAN interactúan entre dispositivos de capa 2. El campo PRI (es decir, prioridad 802.1p), o campo CoS, en el encabezado de trama VLAN identifica los requisitos de calidad de servicio de acuerdo con las definiciones de IEEE 802.1Q.

Prioridad 802.1p en el marco VLAN

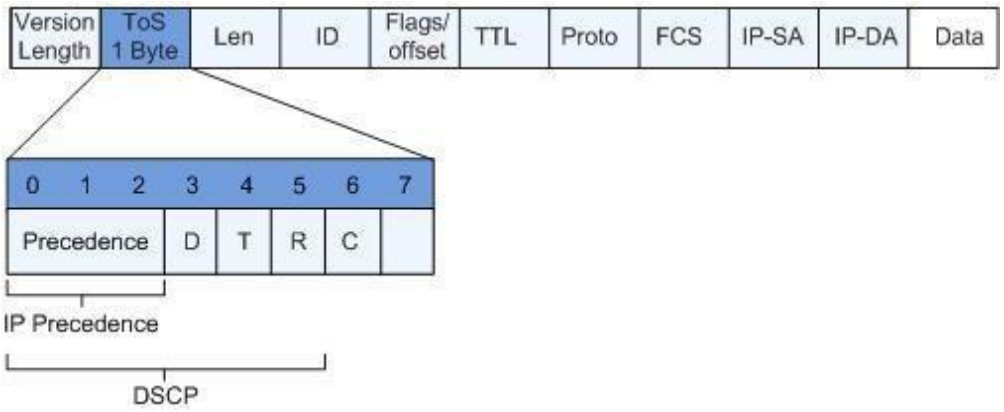


El encabezado 802.1Q contiene campos PRI de 3 bits. El campo PRI define 8 CoS de prioridad empresarial que van de 7 a 0 de mayor a menor.

Campo de precedencia IP/DSCP

Según la definición RFC791, el dominio ToS (Tipo de servicio) en el encabezado del mensaje IP se compone de 8 bits. Entre ellos, el campo Precedencia de 3 bits de longitud, como se encuentra a continuación, identifica la prioridad del mensaje IP.

Campo de precedencia IP/DSCP



0 a 2 bits son campos de precedencia que representan las 8 prioridades de transmisión de mensajes que van de 7 a 0 de mayor a menor, con el nivel 7 o 6 como el más alto. Prioridad que generalmente se reserva para enrutar o actualizar la comunicación de control de red. Las aplicaciones de nivel de usuario solo tienen acceso a los niveles 0 a 5.

El dominio ToS, además de los campos de precedencia, también incluye bits D, T y R: D-bit representa el requisito de retraso (0 para retraso normal y 1 para retraso bajo). T-bit representa el rendimiento (0 para el rendimiento normal y 1 para el rendimiento alto). R- bit representa la fiabilidad (0 para fiabilidad normal y 1 para alta fiabilidad). El dominio ToS reserva los bits 6 y 7.

RFC1349 redefine el dominio ToS agregando un bit C para representar el costo monetario. A continuación, el grupo IETF DiffServ redefine el dominio ToS de 0 a 5 bits en el encabezado de mensaje IPv4 de RFC2474 como DSCP y lo renombra como byte DS (servicio diferenciado) como se muestra en la figura anterior.
Los primeros 6 bits (0-5 bits) del campo DS distinguen el DSCP (DS Code Point), y los 2 bits superiores (6-7 bits) están reservados. Los 3 bits inferiores (0-2 bits) son CSCP (Class Selector Code Point), con el mismo valor CSCP que representa el DSCP de la misma clase. Los nodos DS seleccionan el PHB (comportamiento por salto) correspondiente según los valores DSCP.

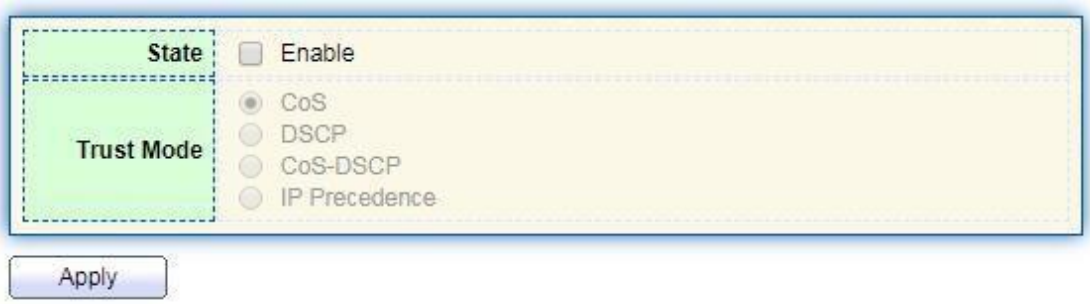
16.1 General

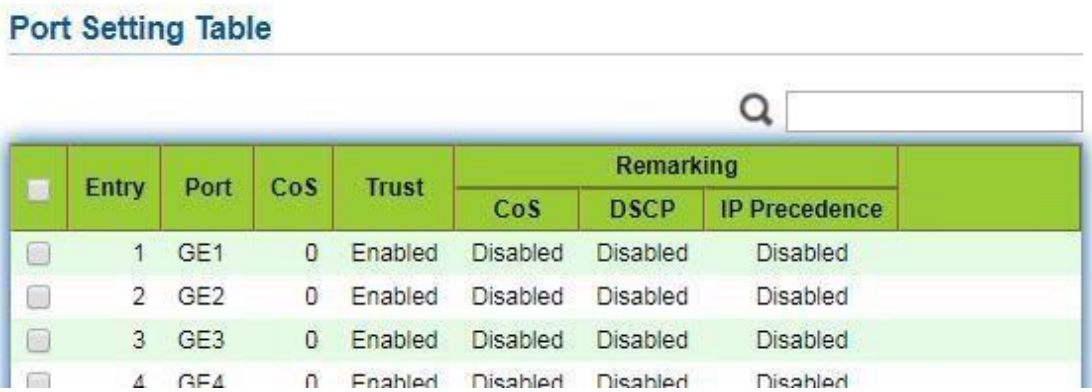
16.1.1 Propiedad

La congestión de la red resultante de la competencia por los derechos de uso de recursos entre mensajes al mismo tiempo generalmente se resuelve mediante la programación de colas, evitando así congestiones intermitentes. Las tecnologías de programación de colas incluyen SP (prioridad estricta), WFQ (cola justa ponderada), WRR (round robin ponderado) y DRR (Deficit Round Robin, que también se amplía a partir de la tecnología RR).

Instrucciones para la configuración de programación global y de puertos

1. Haga click en “QoS > General > Property” en el menú de navegación.





Los datos de interfaz de la configuración global son los siguientes.

Elementos de configuración	Descripción
State	Conmutador de la función QoS global
Trust Mode	Se puede dividir en CoS, DSCP, CoS-DSCP y prioridad IP

Los datos de interfaz de la configuración del puerto son los siguientes.

Elementos de configuración	Descripción
CoS	De 0 a 7
Port Trust Mode	Conmutador de la función QoS del puerto
CoS	Marcar el campo CoS
DSCP	Marcar el campo DSCP
IP Priority	Marque el campo Prioridad IP

16.1.2 Programación de colas

1. Haga clic en "QoS > General > Queue Scheduling". "Aplicar" y terminar de la siguiente manera.

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Strict Priority	Modo SP
WRR	Modo WRR
Weight	Porcentaje de ancho de banda de WRR contabilizado por Queue

16.1.3 Mapeo de CoS

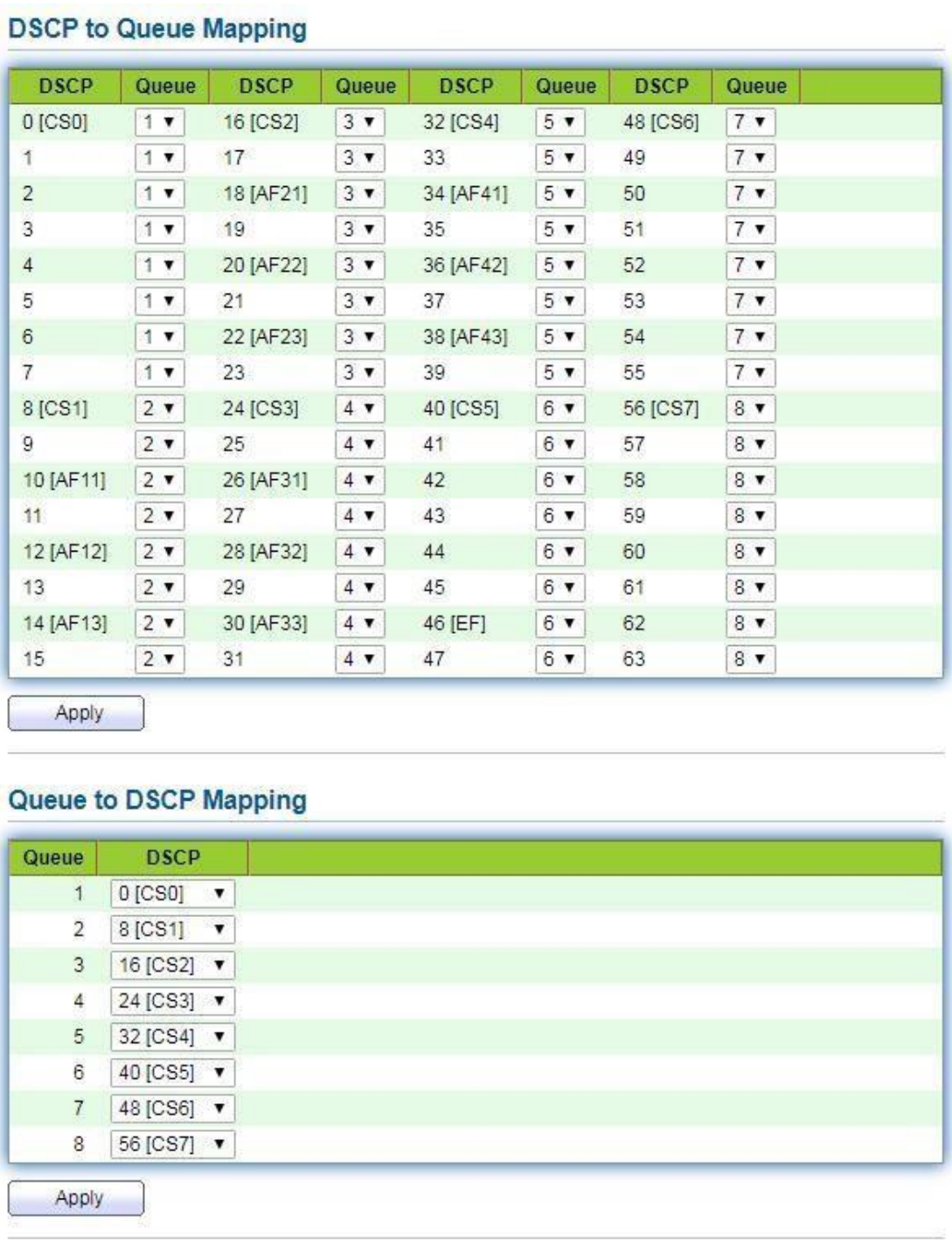
1. Haga clic en "QoS > General > CoS Mapping" en el menú de navegación. "Aplicar y terminar de la siguiente manera.

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
CoS	Prioridad 802.1p
Queue	Cola de puertos

16.1.4 Mapeo DSCP

1. Haga clic en "QoS > General > DSCP Mapping". "Aplicar" y terminar de la siguiente manera.

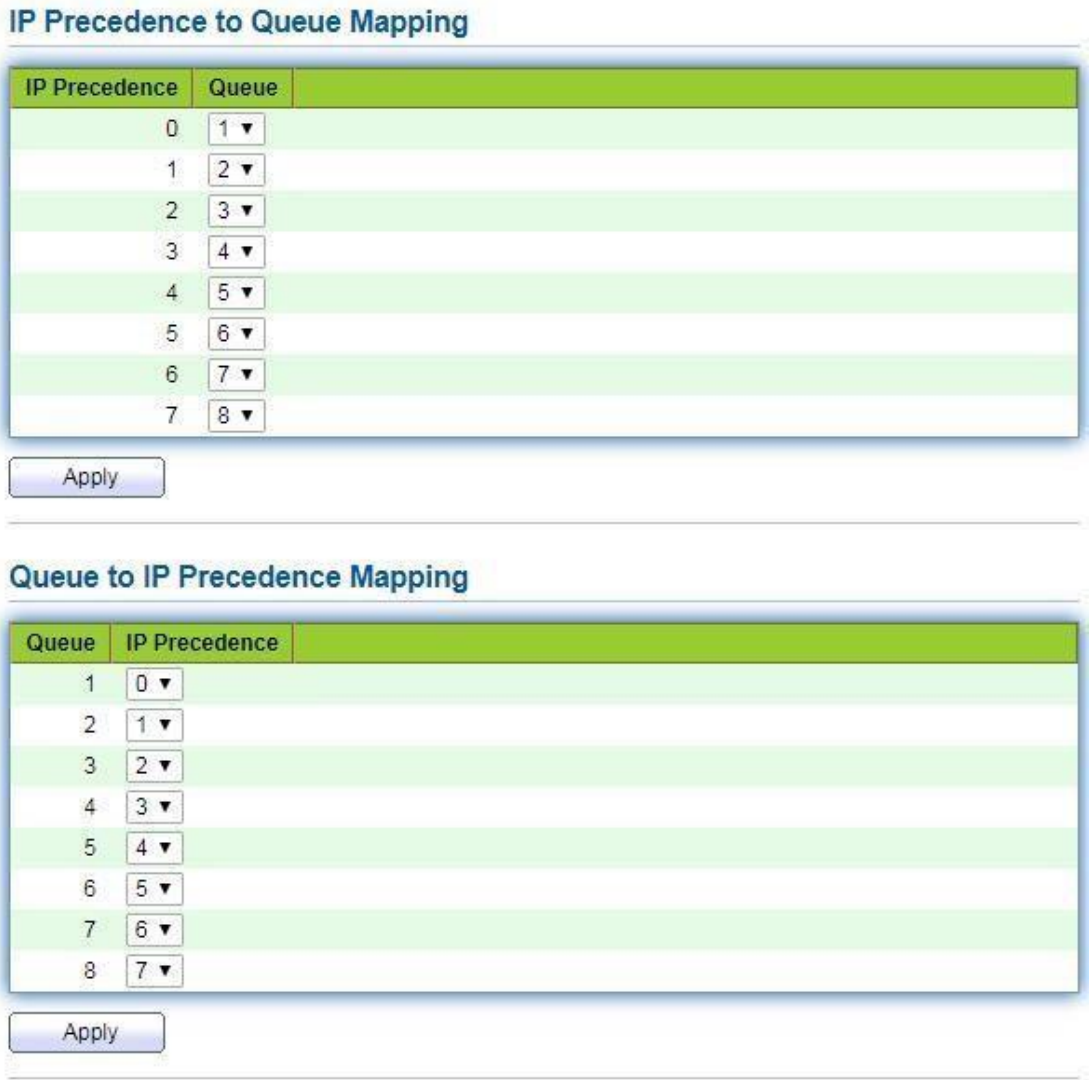


Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
CoS	Valor de la prioridad de dominio IP DHCP
Queue	Cola de puertos

16.1.5 Asignación de precedencia IP

1. Haga clic en "QoS > General > IP Precedence Mapping", ingrese a esta página y haga clic en "Aplicar", Finalizar de la siguiente manera.



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
IP Precedence	Valor de la prioridad de dominio IP TOS
Queue	Cola de puertos

16.2 Límite de tarifa

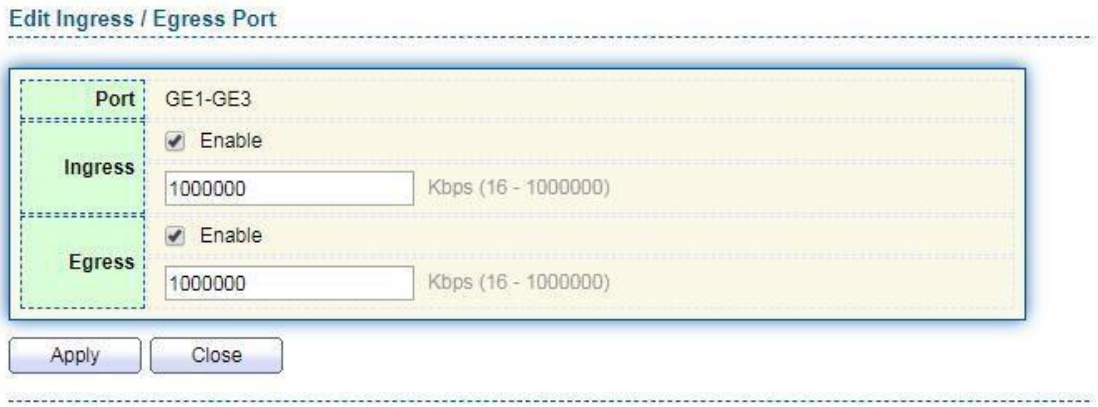
16.2.1 Puerto de entrada / salida

Se refiere a la restricción de velocidad en la transmisión y recepción de datos en interfaces físicas. Restringir la limitación de velocidad en la salida antes del flujo de transmisión, controlando así todo el flujo de mensajes salientes;
Restringir la limitación de velocidad en la entrada antes del flujo de recepción, controlando así todo el flujo de mensajes entrantes;

Instrucciones:

1. Haga clic en "QoS > Rate Limit > Ingress / Egress Port" en el menú de navegación para elegir un puerto limitante de velocidad y comprobar la configuración actual de la siguiente manera:

2. Seleccione el puerto (s) para limitar la velocidad, "Editar" en la parte inferior para cambiar la función y especificar la velocidad. "Aplicar" y Finalizar de la siguiente manera:



Los campos de la interfaz son como a continuación.

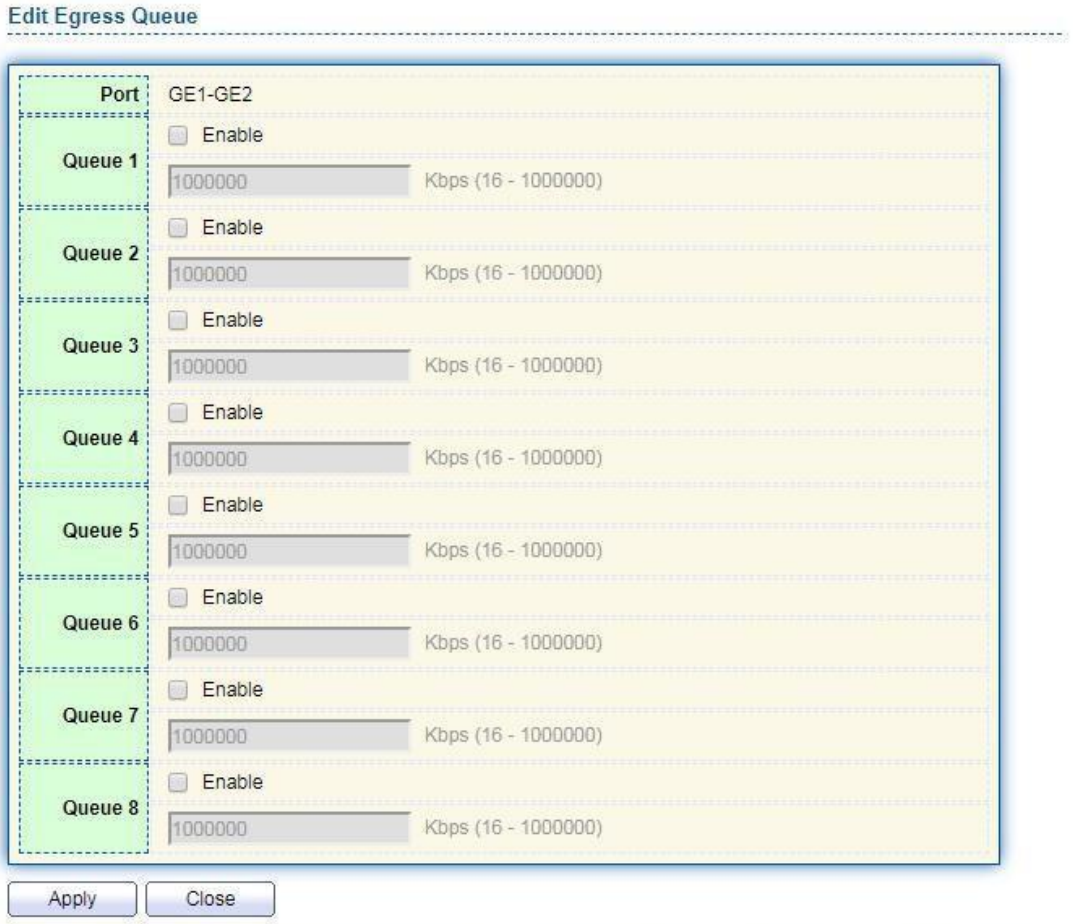
Elementos de configuración		Descripción
Ingress	Habilitado	Interruptor de limitación de velocidad
	Tasa	La tarifa oscila entre 16 y 1.000.000 Kbps
Egress	Habilitado	Interruptor de limitación de velocidad
	Tasa	La tarifa oscila entre 16 y 1.000.000 Kbps

16.2.2 Cola de salida

Instrucciones para la configuración de la cola de salida

1. Haga clic en "QoS > Rate Limit > Egress Queue" en el menú de navegación de la siguiente manera.

2. Seleccione el puerto y "Editar" para ingresar a la interfaz de configuración del puerto de la



siguiente manera.

17 Diagnósticos

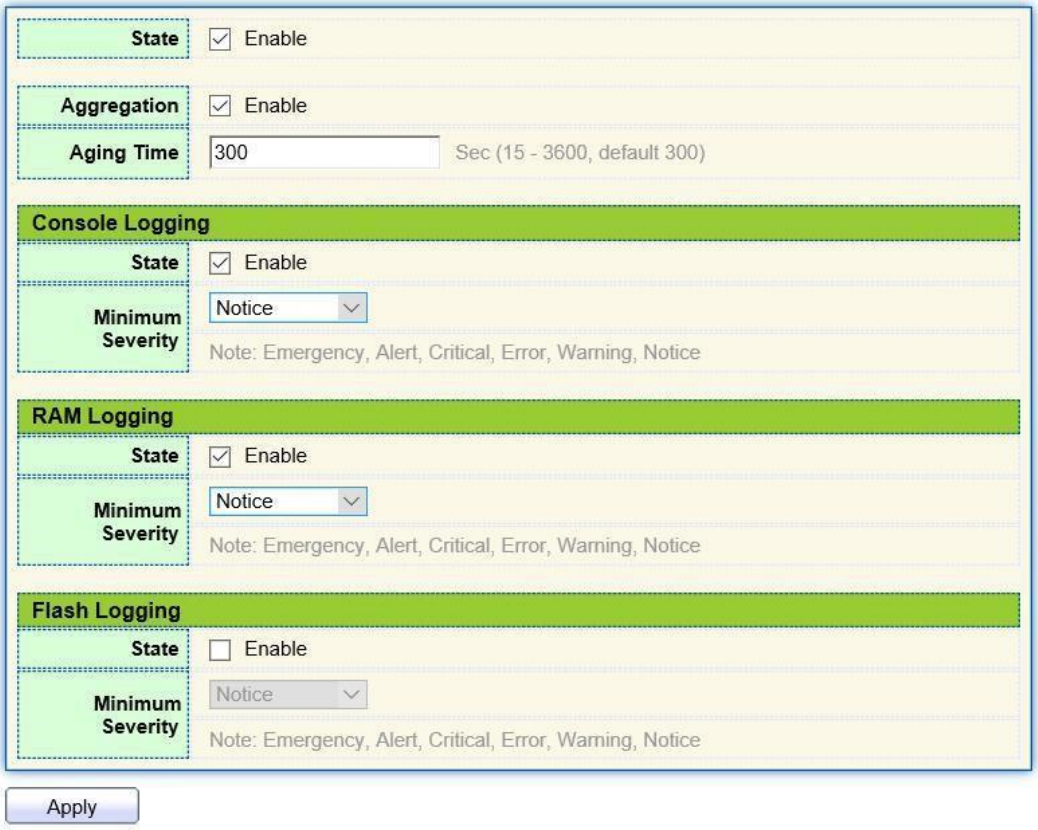
14.1 Registro

Configura el interruptor de registro, la integración de información, el tiempo de envejecimiento y el nivel de configuración. También carga los registros de trabajo del switch en el servidor TFTP.

Instrucciones:

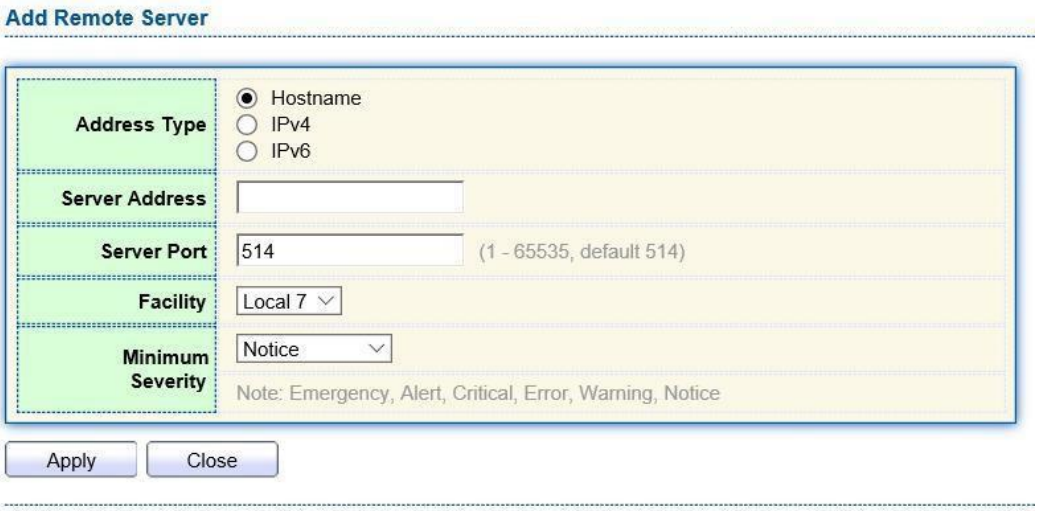
1. Haga clic en "Diagnostics > Logging > Property" en el menú de navegación para activar / desactivar los registros, seleccionar el terminal de salida, configurar el nivel de gravedad, etc. como

   Sigue:



2. Haga clic en "Diagnostics > Logging > Remote Server" en el menú de navegación para agregar y ver la configuración del servidor de la siguiente manera:

3. "Agregar" un nuevo servidor de registro remoto y "Editar" la configuración seleccionada. "Aplicar" y Finalizar de la siguiente manera:



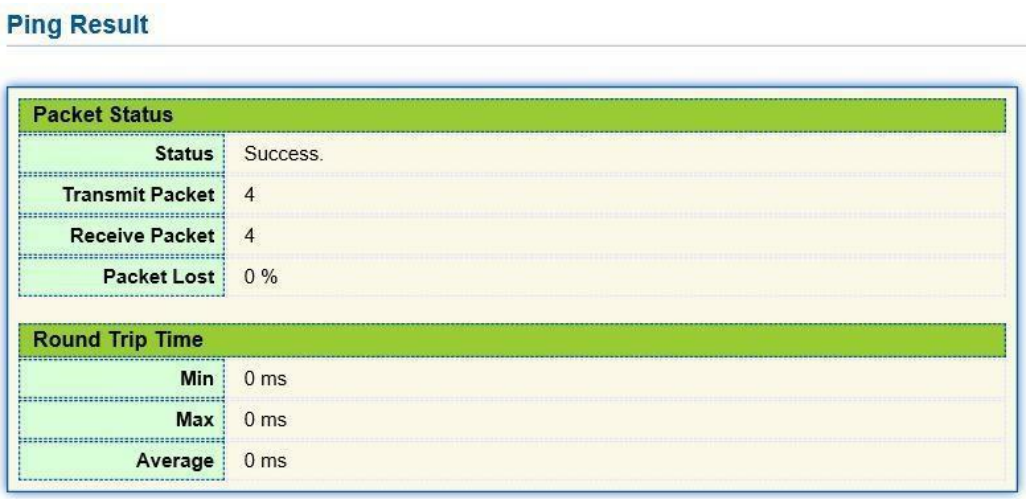
17.2 Ping

El comando ping comprueba la disponibilidad de direcciones IP y nombres de host especificados y transmite estadísticas en consecuencia.

Instrucciones:

1. Haga clic en "Diagnostics > Ping" en el menú de navegación para introducir un nombre de host o una dirección IP, así como el número de pruebas de la siguiente manera:

2. Haga clic en "Ping" para aceptar la prueba de transmisión de paquetes del sistema para verificar la validez de la dirección y generar el resultado de la siguiente manera:

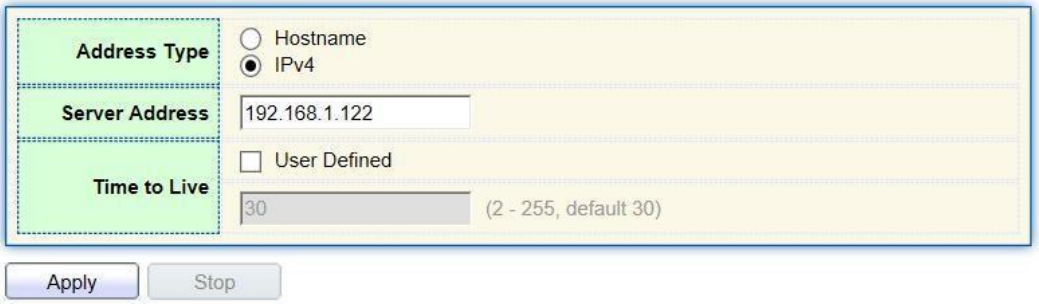


17.3 Traceroute

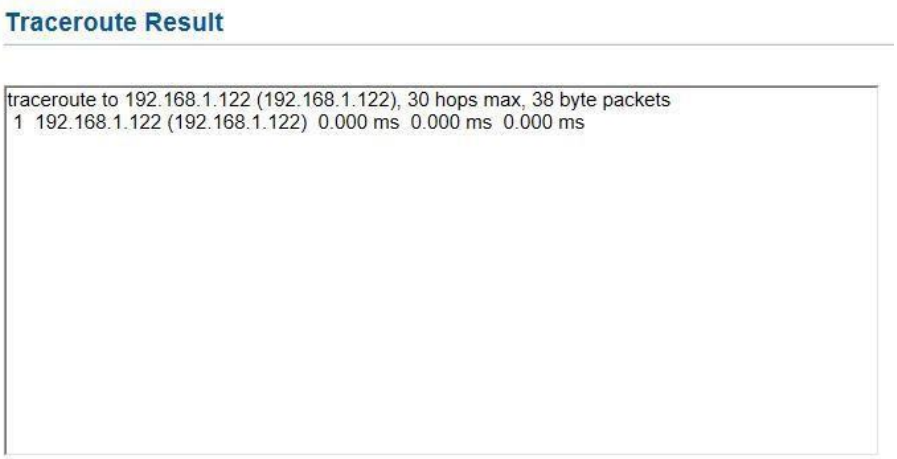
Traceroute mide la duración desde la transmisión de un pequeño paquete hasta su recepción desde el dispositivo de destino.

Instrucciones:

1. Haga clic en "Diagnostics > Traceroute" en el menú de navegación para introducir un nombre de host o dirección IP para definir el tiempo de existencia del mensaje de la siguiente manera:



2. "Aplicar" para probar y generar el resultado de la siguiente manera:



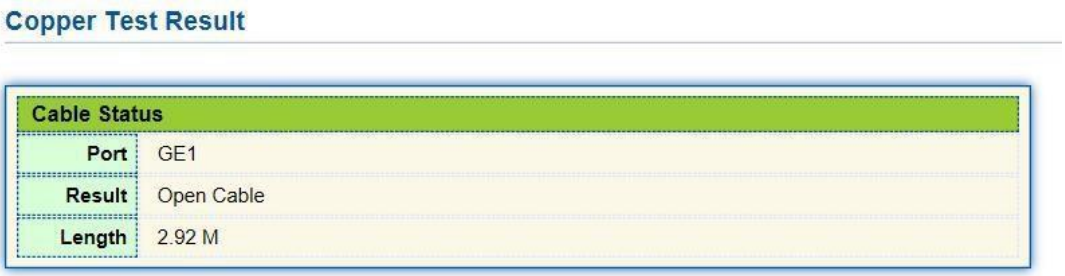
17.4 Prueba de cobre

La prueba de cobre evalúa el estado del cable de entrada y localiza las fallas (aproximadamente 5 m por error) de acuerdo con la intensidad de voltaje reflejada.

Instrucciones:

1. Haga clic en "Diagnostics > Copper Test" en el menú de navegación para seleccionar un puerto para probar de la siguiente manera:

2. Haga clic en "Prueba de cobre" y genere el resultado de la siguiente manera:

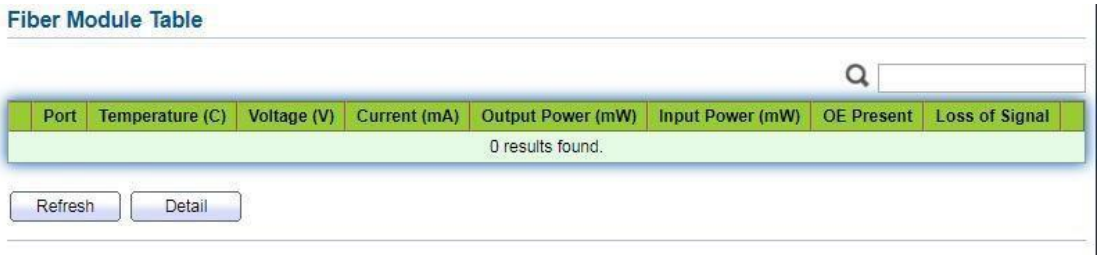


17.5 Módulo de fibra

Se puede utilizar para ver información DDM del módulo óptico.

Instrucciones:

1. Haga clic en "Diagnostics > Fiber Module" en el menú de navegación para seleccionar un puerto para probar de la siguiente manera:



Nota:

La información del módulo óptico solo se puede ver cuando el estado de la interfaz está activo.

17.6 UDLD

UDLD (Unidirectional Link Detection): es un protocolo privado de capa 2 de Cisco, que se utiliza para monitorizar la configuración física del enlace Ethernet conectado por fibra óptica o par trenzado. Cuando aparece un enlace unidireccional (solo puede transmitir a una dirección, por ejemplo, puedo enviarte datos, tú también puedes recibirlos, pero no puedo recibir los datos que me enviaste), UDLD puede detectar esta situación, cerrar la interfaz correspondiente y enviarle un mensaje de advertencia. Los enlaces unidireccionales pueden causar muchos problemas, especialmente árboles de expansión, lo que puede causar un bucle invertido. Nota: Los dispositivos UDLD deben ser compatibles con ambos extremos del enlace para que se ejecute normalmente.

17.6.1 Propiedad

Instrucciones de configuración del
switch global y de puerto:

1. Haga clic en "Diagnostics > UDLD > Property" en el menú de navegación para seleccionar un puerto para probar de la siguiente manera:

2. Seleccione el puerto y haga clic en "Editar" para ingresar a la interfaz Editar de la siguiente

manera:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Port	ID de puerto
Mode	Modo de puerto UDLD Deshabilitado: Desactivar la función de puerto Normal: UDLD puede detectar vínculos unidireccionales y marcar el puerto como indeterminado para generar registros del sistema Agresivo: UDLD puede detectar el enlace unidireccional. Intentará reconstruir el enlace y enviar mensajes UDLD durante 8 segundos continuamente. Si no hay respuesta de eco UDLD, el puerto se colocará en el estado errable

17.6.2 Vecino

UDLD envía periódicamente paquetes de hola (también conocidos como sonda de publicidad o sonda) en cada interfaz activa.

Cuando el conmutador recibe el paquete Hello, el mensaje se almacena hasta que expira el tiempo de caducidad. Cuando Hello se recibe de nuevo antes de la expiración del tiempo de envejecimiento, el tiempo de envejecimiento se actualiza.

Cuando un nuevo vecino o un vecino solicita volver a sincronizar la memoria caché, se envía una serie de paquetes de sondeo/eco (Hello) UDLD.
Instrucciones:

1. Haga clic en "Diagnostics > UDLD > Neighbor" en el menú de navegación para seleccionar un puerto para probar de la siguiente manera:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Entry	Nº de serie de vecino
Expiration Time	Tiempo restante de envejecimiento
Current Neighbor State	Situación de los vecinos
Device ID	Id. de dispositivo de los vecinos
Device Name	Nombre del dispositivo de los vecinos
Port ID	El ID de la interfaz conectada
Message Interval	Intervalo de mensajes para vecinos
Timeout Interval	Intervalo de tiempo de espera para vecinos

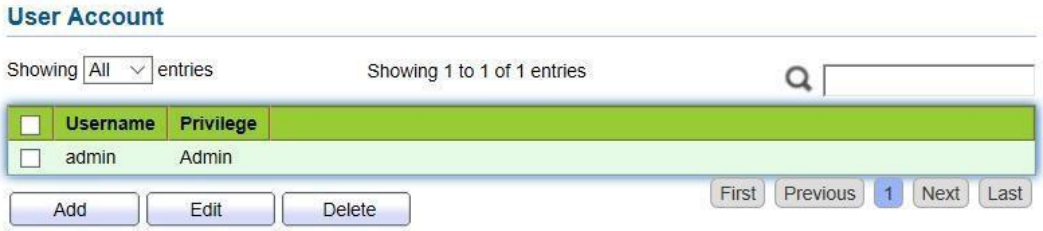
18 Administración

18.1 Cuenta de usuario

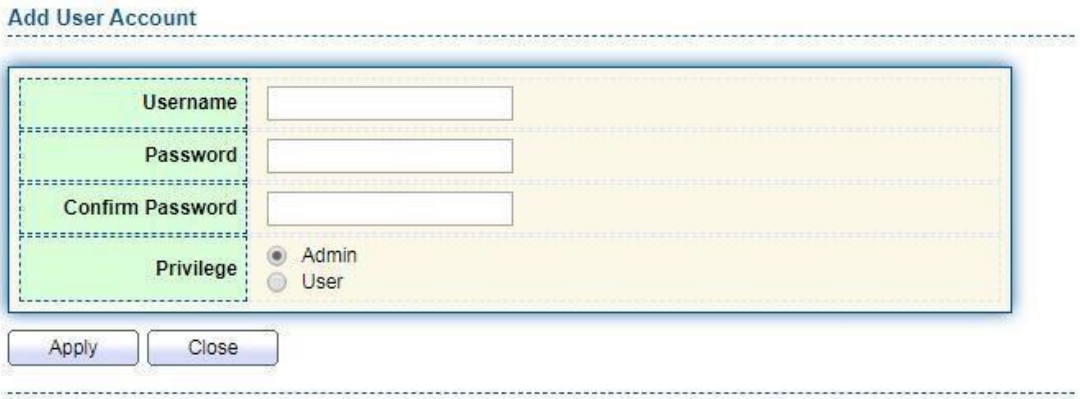
Los usuarios pueden comprobar y modificar el nombre de usuario, la contraseña y la autoridad actuales del conmutador.

Instrucciones:

1. Haga clic en "Management > User Account" en el menú de navegación para descubrir el nombre de usuario de "admin" y el privilegio de "Admin" por defecto de la siguiente manera:



2. "Agregar" una nueva cuenta de usuario y "Editar" el atributo de usuario seleccionado de la siguiente manera:



18.2 Firmware

Instrucciones de actualización del
firmware de la versión del sistema:

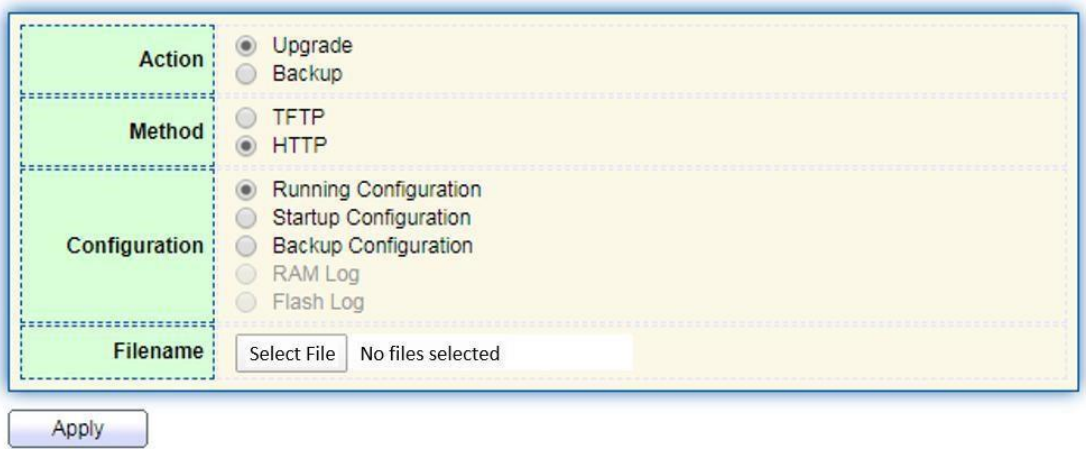
1. Haga click en “Management > Firmware > Upgrade” en el menú de navegación:

18.3 Configuración

18.3.1 Actualizar

Actualización o copia de seguridad de la
configuración del sistema Instrucciones para la
actualización del archivo de configuración:

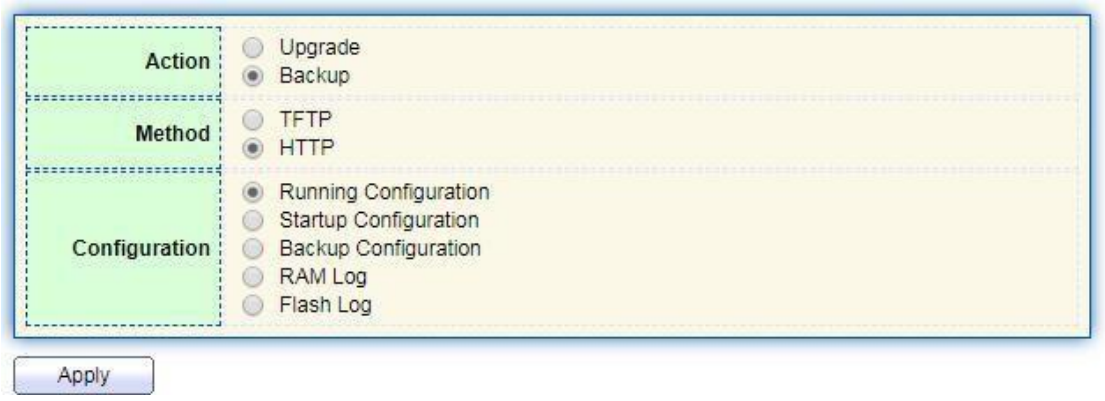
1. Haga clic en "Management > Configuration > Upgrade" Haga clic en "Upgrade" en modo de "TFTP” o "HTTP", seleccione los archivos correspondientes a actualizar (los servidores deben ser
   ilustrado en modo TFTP). "Aplicar" y terminar de la siguiente manera:



Instrucciones para la configuración de la copia de seguridad de archivos:

2. Haga clic en "Copia de seguridad" en modo “TFTP" o “HTTP", seleccione los archivos o registros a actualizar (los servidores deben ilustrarse en modo TFTP). "Aplicar" y

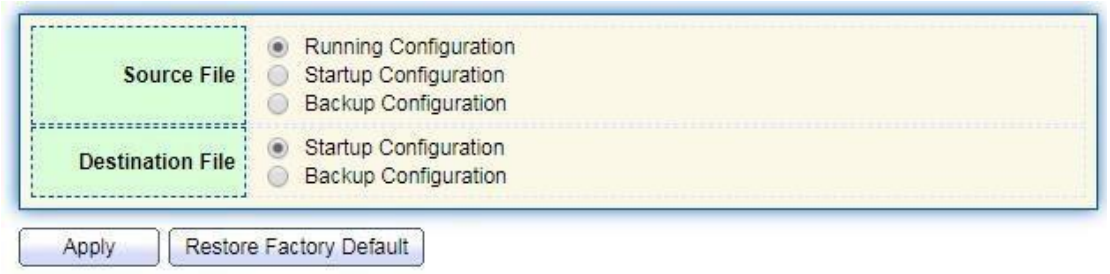
   Termine de la siguiente manera.



18.3.2 Guardar configuración

Guarde la configuración del sistema o restaure la configuración a los valores predeterminados de fábrica. Instrucciones:

1. Haga click en “Management > Configuration > Save Configuration” en el menú de navegación as follows:



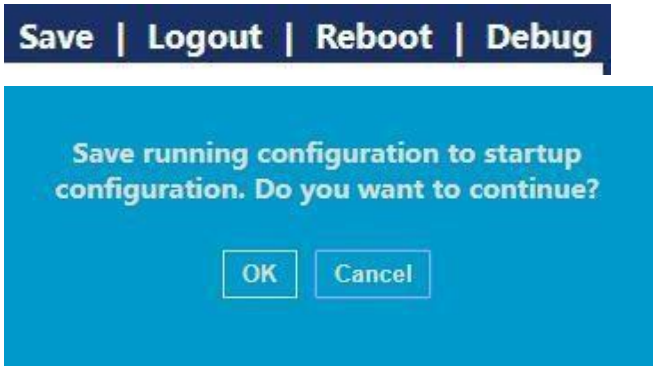
Nota:

- Haga clic en "Restablecimiento de fábrica” y "Reinicio del dispositivo" para restaurar la configuración de fábrica.

Guarde la "Configuración en ejecución" como “Configuración de inicio" (que se puede guardar como "Configuración de copia de seguridad" o "Configuración en ejecución") y la "Configuración de copia de seguridad" (que se puede guardar como "Configuración de inicio" o "Configuración en ejecución “).

Instrucciones para el segundo método de conservación del sistema:

2. Haga clic en "Guardar" en la parte superior derecha para guardar la configuración en ejecución como la configuración de inicio de la siguiente manera.

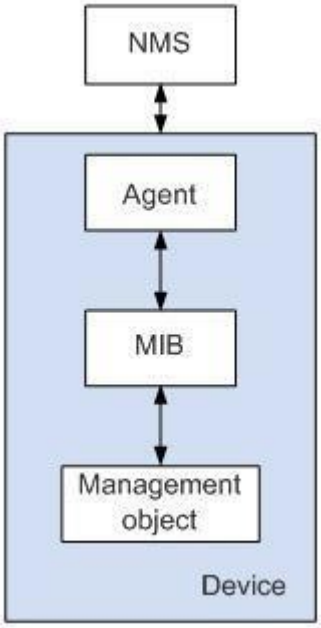


18.4 SNMP

SNMP (Simple Network Management Protocol) es ampliamente utilizado en redes TCP/IP. Administra los dispositivos mediante la computadora central que opera el software de administración network (es decir, la estación de trabajo de administración de red). SNMP es:

- Simple: El SNMP de sondeo tiene el conjunto de funcionalidades fundamentales que es aplicable a entornos de pequeña escala con alta velocidad y bajo costo. Además, SNMP impulsado por UDP es compatible con la mayoría de los dispositivos. Potente: SNMP tiene como objetivo garantizar la transmisión de información de administración entre dos nodos para que los administradores puedan recuperar, modificar y solucionar problemas de la información fácilmente. Hay 3 versiones comunes, a saber, SNMPv1, v2c y v3. Su sistema contiene NMS (Network Management System), Agente, Objeto de gestión y MIB (Base de información de gestión).
- NMS, como centro de administración, administrará todos los dispositivos. Cada dispositivo bajo administración incluye el agente residente, MIB y objetos de administración. NMS actúa con el agente ejecutándose en el objeto de gestión que operará el MIB para ejecutar órdenes NMS.

Modelo de gestión SNMP



Nms

- Como administrador de red , NMS administra/monitorea los dispositivos de red mediante SNMP en su servidor. Puede solicitar al agente que consulte o modifique los parámetros especificados. NMS puede recibir la captura enviada activamente por el agente para actualizarla con los estados de los dispositivos administrados.

Agente

- Como proceso de agente de los dispositivos administrados, mantiene los datos del dispositivo y responde a las solicitudes de NMS informando de los datos de administración. El agente cumplirá con los pedidos relevantes a través de MIB Table y transmitirá los resultados a NMS después de recibir su solicitud. Devices tomará la iniciativa de transmitir información relacionada con los estatutos actuales de los dispositivos a NMS a través del Agente una vez que ocurra una falla u otro evento.

Objeto de administración

- Se refiere al objeto bajo gestión. Cada dispositivo puede tener más de un objeto, incluida una pieza de hardware (por ejemplo, una placa de interfaz), hardware y software parciales (por ejemplo, protocolo de enrutamiento), así como otros conjuntos de elementos de configuración.

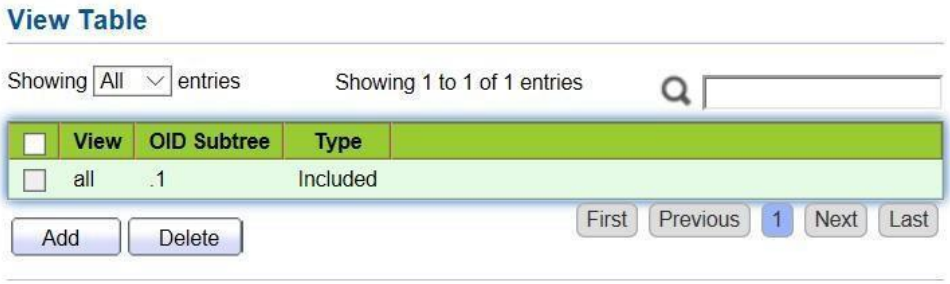
Mib

- MIB es una base de datos que especifica las variables mantenidas por el objeto de gestión (es decir, la información que puede ser consultada y establecida por el agente). MIB define los atributos del objeto de administración, incluidos el nombre, el estado, el derecho de acceso y el tipo de datos. Las siguientes funciones se pueden realizar a través de MIB:

  El agente dominará la información instantánea del dispositivo consultando MIB y establecerá los elementos de configuración de estado cambiando MIB.

18.4.1 Vista

1. Haga click en “Management > SNMP > View” en el menú de navegación:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
View	Nombre de la vista
OID Subtree	Ver OID
Type	Tipo de vista: "Incluido” o "Excluido"

2. "Agregar" la configuración correspondiente, "Aplicar" y Finalizar.

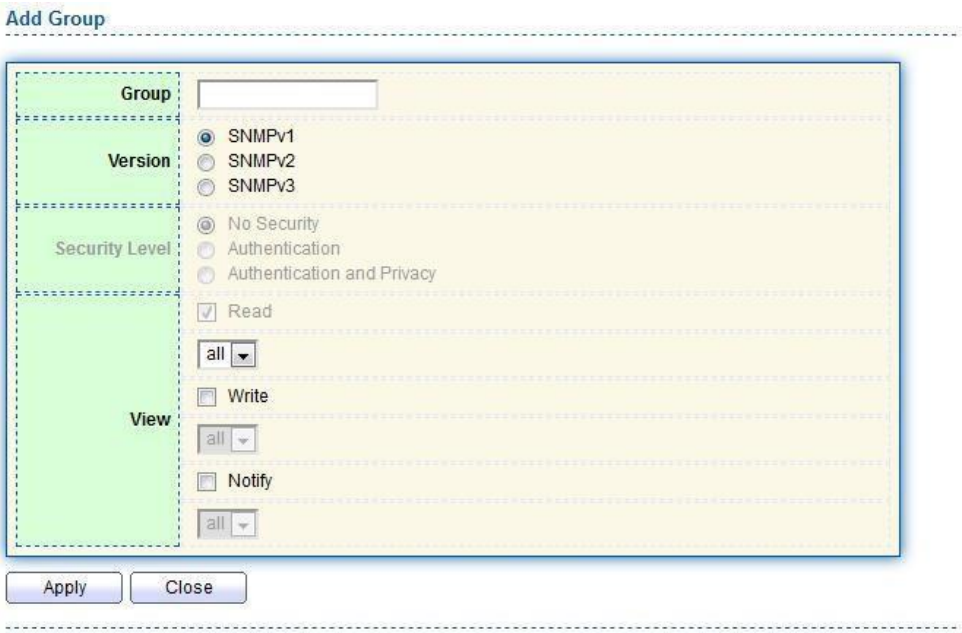
18.4.2 Grupo

1. Haga click en “Management > SNMP > Group” en el menú de navegación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Group	Nombre del grupo
Version	V1, V2, V3
Security Level	Nivel de seguridad
View	Las vistas se dividen en lectura de vistas, escritura y notificación.

2. Haga clic en "Agregar" para completar la configuración correspondiente. "Aplicar" y finalizar.



18.4.3 Comunidad

1. Haga click en “Management > SNMP > Community” en el menú de navegación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Community	Configuración de la comunidad
Group	Nombre del grupo
View	Nombre de la vista
Access:	Autoridad: solo lectura o lectura-escritura

2. "Agregar" la configuración correspondiente. "Aplicar" y finalizar.

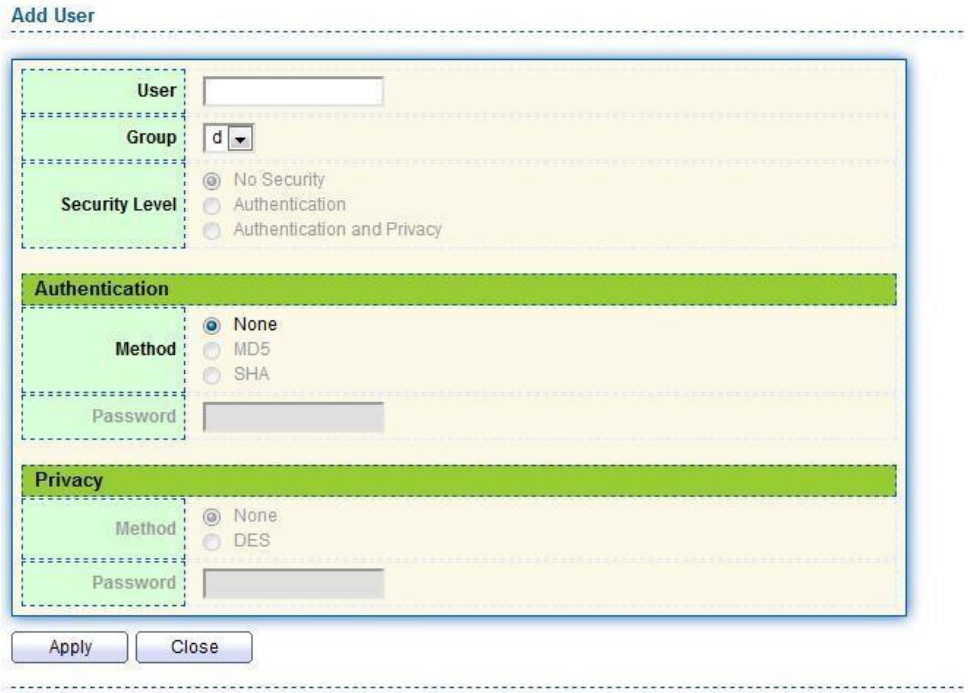
18.4.4 Usuario

1. Haga click en “Management > SNMP > User” en el menú de navegación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
User	Nombre de usuario
Group	Nombre del grupo
Security Level	Nivel de seguridad
Authentication Method	Modo de autenticación
Privacy Method	Modo de cifrado

2. "Agregar" la configuración correspondiente. "Aplicar" y finalizar.



18.4.5 ID del motor

1. Haga click en “Management > SNMP > Engine ID” en el menú de navegación:

2. Haga clic en "User Automation" para completar el valor de ID correspondiente . "Aplicar" y terminar.

18.4.6 Evento Trap

1. Haga click en “Management > SNMP > Trap Event” en el menú de navegación:

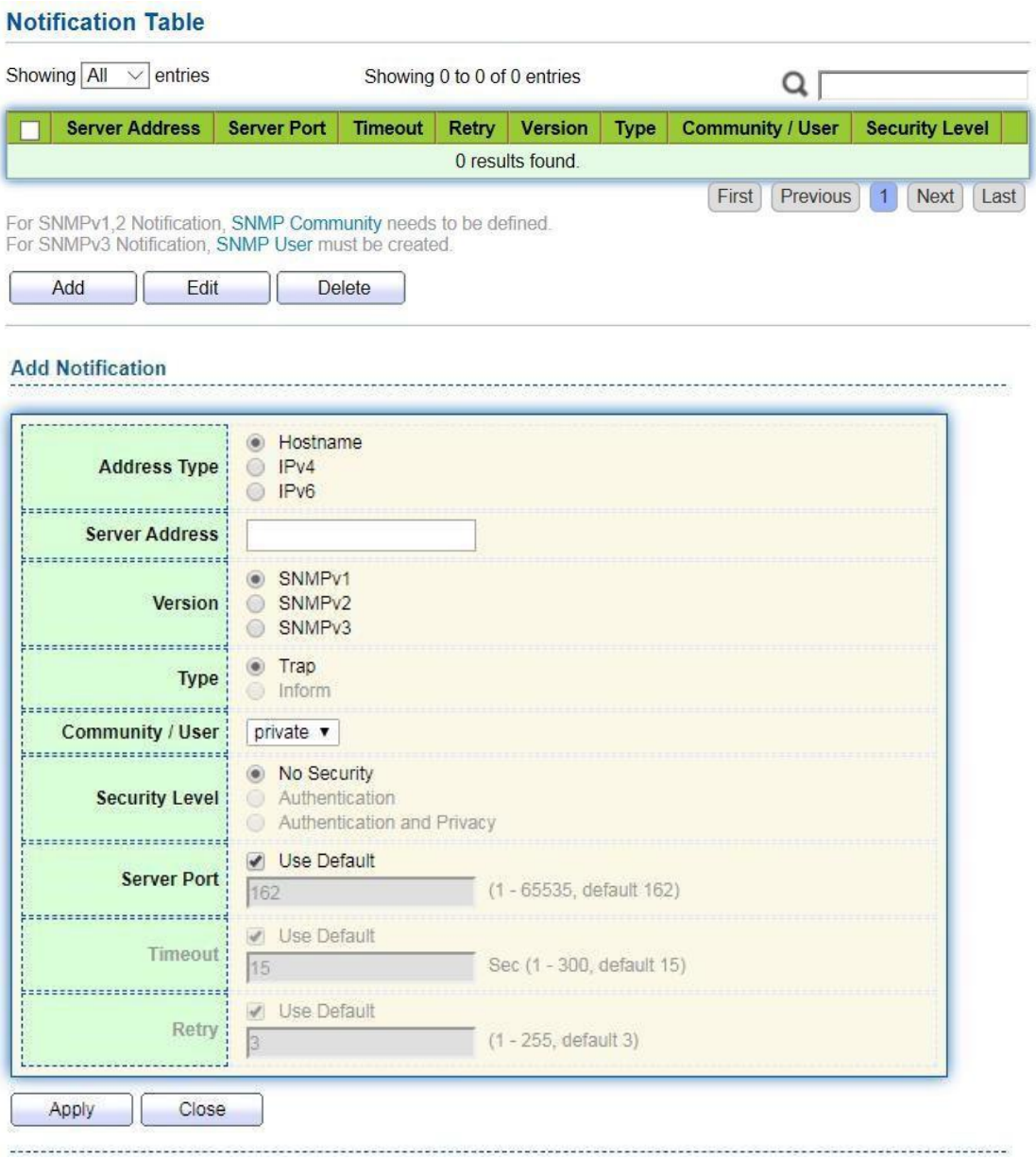
Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Authentication Failure	Error de autenticación
Link Up / Down	Enlace de puerto hacia arriba/hacia abajo
Cold start	Arranque en frío
Warm start	Arranque en caliente

2. "Aplicar" y finalizar.

18.4.7 Notificación

1. Haga click en “Management > SNMP > Notification” en el menú de navegación:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Address Type	Tipo de dirección: "Nombre de host", "IPv4" o "IPv6"
Server Address	Información de la dirección del servidor
Version	Versiones SNMP: v1, v2 y v3
Type	Tipo de notificación: "Trap" o "Informar"
Community / User	Comunidad o nombre de usuario
Security Level	Nivel de seguridad
Server port	162 por defecto van de 1 a 65.535
Timeout	Período de tiempo de espera: 15s por defecto que van de 1 a 300s.
Retry	El intervalo de reintento varía de 1 a 255s con 3s de forma predeterminada.

2. "Agregar" la configuración correspondiente. "Aplicar" y finalizar.

18.5 RMON

RMON (RemoteMonitoring) es un MIB definido por el IETF (Internet Engineering Task Force) y enfatiza significativamente el estándar MIB II. Supervisa principalmente el flujo de datos en un segmento de red o incluso en toda la red, que es uno de los estándares de gestión de red más utilizados. RMON incluye NMS (Network Management Station) y Agent que se ejecuta en varios dispositivos de red. El agente RMON que se ejecuta en monitores o detectores de red rastreará y contará la información de flujo (por ejemplo, el número total de mensajes en un segmento de red durante un cierto período de tiempo, o el de los mensajes correctos enviados a un host) en el segmento de red conectado al puerto. Basado en la arquitectura SNMP, RMON es compatible con el marco SNMP existente. SNMP supervisa los dispositivos de red remotos de una manera más eficiente y activa para supervisar el funcionamiento de la subred. RMON puede reducir el flujo de comunicación entre NMS y SNMP

Agente para gestionar la red de interconexión a gran escala de forma cómoda y eficaz. Varios monitores pueden recopilar datos por 2 medios: la sonda RMON exclusiva se utiliza para recopilar datos, y el NMS administra directamente la información y controla los recursos de la red. Se puede obtener toda la información

de RMON MIB. El agente RMON con acceso directo a dispositivos de red (enrutador, conmutador, HUB, etc.) se convertirá en la instalación de red con función de sonda RMON.

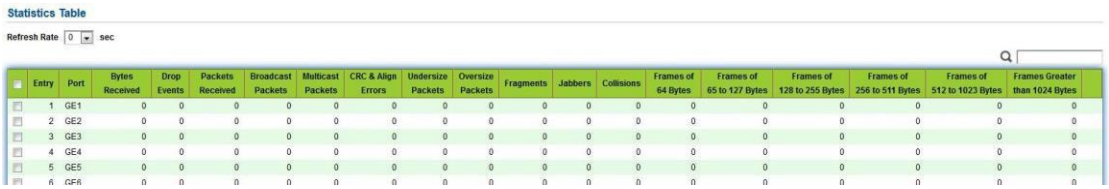
RMON NMS intercambia datos con el agente SNMP con el comando básico SNMP para recopilar información de administración de red. Sin embargo, limitado por los recursos del dispositivo, generalmente no puede obtener todos los datos de RMON MIB. La mayoría de los dispositivos recopilan datos de solo cuatro grupos: grupos de alarmas, eventos, historial y estadísticas. El interruptor de tipo de área realiza RMON de la segunda manera. El agente RMON que accede directamente a los switches se convertirá en la instalación de red con la función de sonda RMON. Al ejecutar el agente SNMP compatible con los conmutadores, NMS puede obtener el flujo general, estadísticas de errores, estadísticas de rendimiento y otra información sobre los segmentos de red conectados a los puertos, con el fin de administrar la red.

18.5.1 Estadística

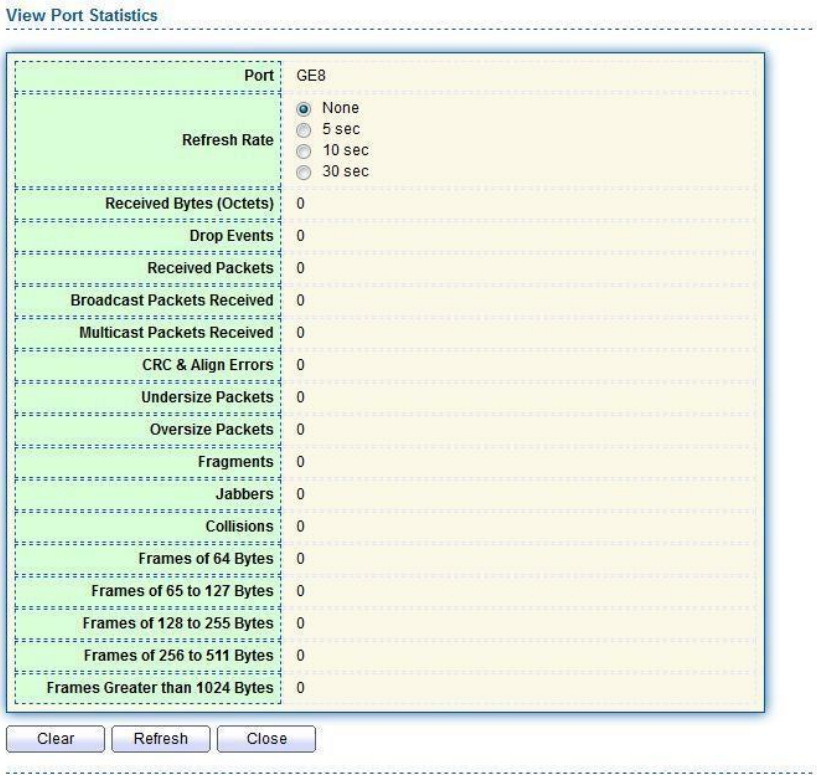
La información del grupo de estadísticas refleja las estadísticas de cada interfaz de supervisión en el conmutador, es decir, la información acumulada desde el comienzo de la creación del grupo. Las estadísticasincluyen el número de conflictos de red, mensajes de error CRC, mensajes de datos demasiado pequeños (demasiado grandes), mensajes de difusión/multidifusión, bytes y mensajes recibidos, etc. Con las estadísticas de RMON y las funciones de administración, el uso del puerto y los errores ocurridos se pueden monitorear y contar, respectivamente.

Instrucciones

1. Haga clic en "Management > RMON > Statistics" en el menú de navegación de la siguiente manera, que revela las estadísticas de mensajes relacionados con el puerto.



2. "Borrar" y "Actualizar" las estadísticas del puerto seleccionado. "Ver" dichas estadísticas de la siguiente manera.



3. Seleccione la frecuencia de actualización especificada para que funcione automáticamente.

18.5.2 Historia

Una vez configurado el grupo de historial RMON, los conmutadores recopilarán periódicamente y almacenarán temporalmente las estadísticas de red para facilitar el procesamiento, proporcionando datos históricos sobre el flujo del segmento de red, los paquetes de error, los paquetes de difusión, la utilización del ancho de banda y otras estadísticas. La gestión de datos históricos se puede utilizar para configurar dispositivos en términos de recopilación de datos históricos, incluida la recopilación periódica y el mantenimiento de los datos de puertos específicos.

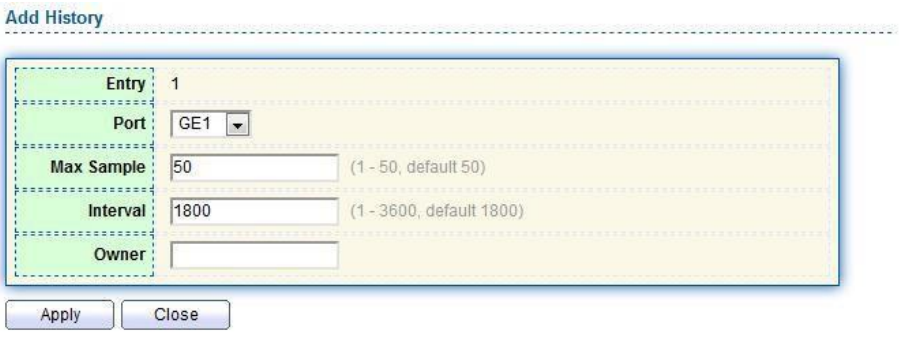
Instrucciones

1. Haga click en “Management > RMON > History” en el menú de navegación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Entry	Nº de serie Nº de grupos de eventos
Port	Puertos a contar
Interval	Intervalo de muestreo que varía de 1 a 3.600 (unidad: s), con 1.800s por defecto.
Owner	Dueño
Maximum	El número máximo de muestras varía de 0 a 50, con 50 por defecto.
Current	Número actual de muestras

2. "Agregar” los elementos de configuración correspondientes para configurar el grupo de



historial.

3. "Aplicar" y Finalizar de la siguiente manera.

18.5.3 Evento

Definición del evento No. y forma de proceso, el grupo de eventos es principalmente para los eventos desencadenados por los elementos de configuración del grupo de alarmas y los elementos de configuración del grupo de alarmas extendido. Hay varias soluciones para ellos: grabar en una tabla de registro; transmitir mensajes de captura a NMS; grabar un registro y transmitir un mensaje de captura; No me importa.

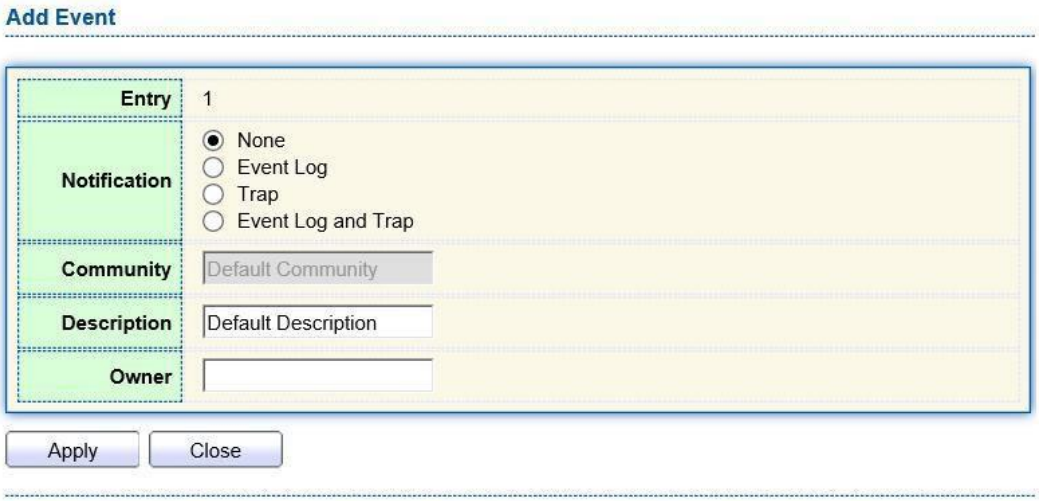
Instrucciones

1. Haga click en “Management > RMON > Event” en el menú de navegación:

Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Entry	Nº de serie Nº de grupos de eventos
Community	Nombre de la comunidad
Description	Descripción
Notification	Notificación
Timer	Hora
Owner	Dueño

2. "Agregar" los elementos de configuración correspondientes para configurar el grupo de



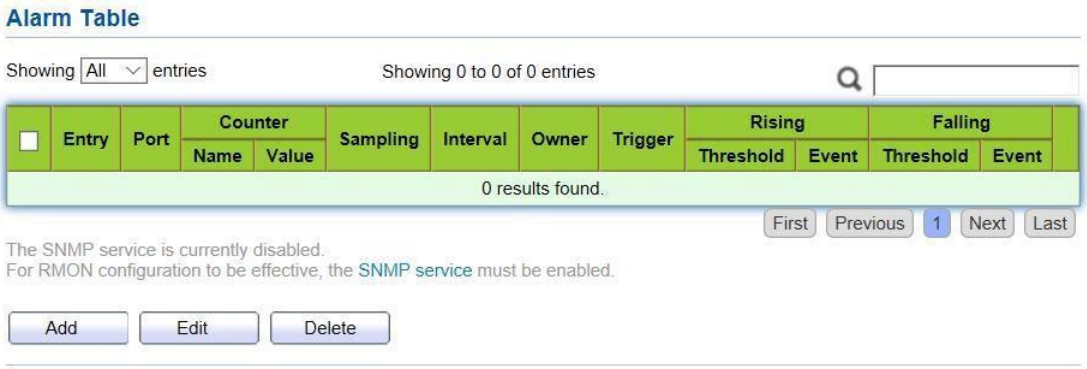
eventos.

3. "Agregar" y Terminar de la siguiente manera.

18.5.4 Alarma

La gestión de alarmas RMON supervisa variables de alarma específicas, como las estadísticas de puertos. Un evento de alarma ocurre cuando el valor de los datos monitoreados excede el umbral definido en la dirección correspondiente, que se tratará de acuerdo con el modo de tratamiento prescrito. La definición del evento se realiza en el grupo de eventos. Después de que el usuario defina la entrada de alarma, el sistema procesará lo siguiente: La variable de alarma definida por el tiempo de muestreo debe muestrearse y el valor debe compararse con el umbral. Para un umbral más alto, se activará el evento correspondiente.

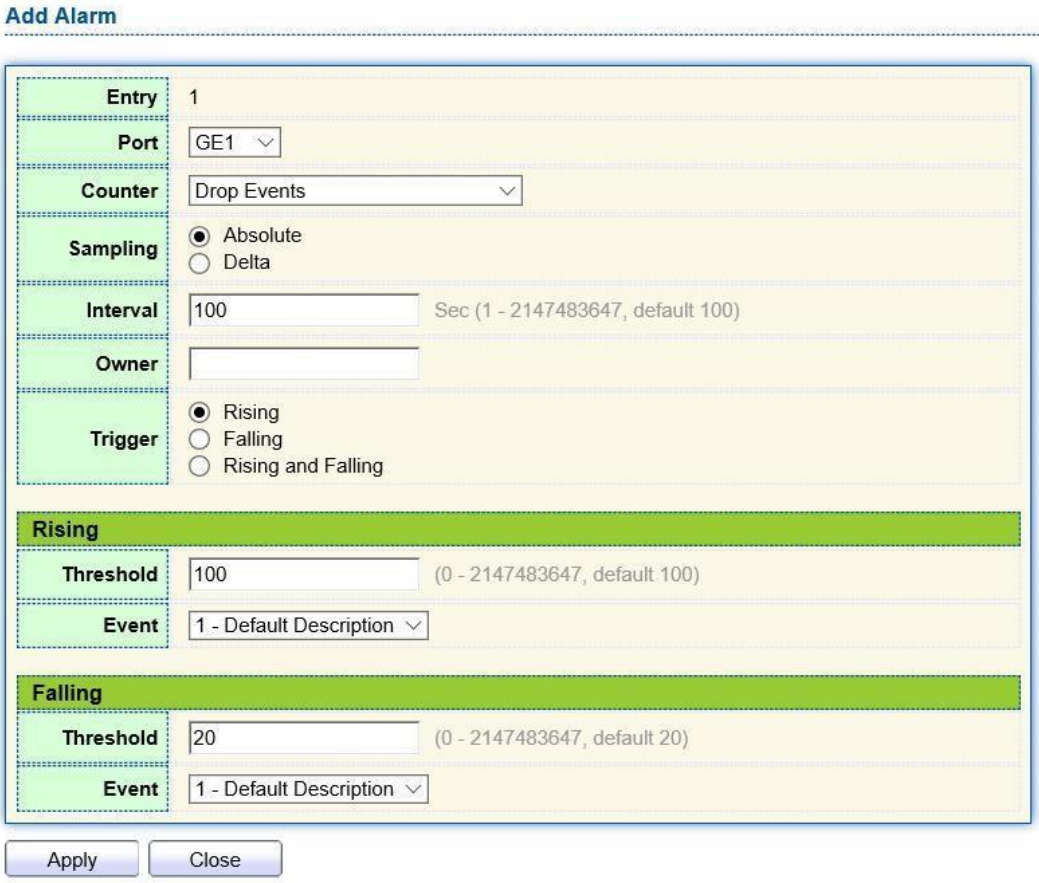
1. Haga click en “Management > RMON > Alarm” en el menú de navegación:



Los campos de la interfaz son como a continuación.

Elementos de configuración	Descripción
Entry	Nº de serie de grupos de alarma
Port	Introduzca los puertos que se contarán
Counter	Parámetros de muestra de alarmas
Interval	El intervalo de muestreo varía de 1 a 2.147.483.647 con la unidad de segundo. 100s por defecto.
Sampling	Tipos de muestra: Absoluto y Eliminar
Owner	Dueño
Threshold (Rising)	El umbral de borde ascendente varía de 0 a 2.147.483.647.
Event (Rising)	Índice de grupos de eventos . El evento correspondiente se activará cuando se active la alarma.
Threshold (Falling)	El umbral de borde descendente oscila entre 0 y 21.474.836.475.
Event (Falling)	Índice de grupos de eventos . El evento correspondiente se activará cuando se active la alarma.

2. "Agregar" los elementos de configuración correspondientes para configurar el grupo de alarmas



3. "Aplicar" y terminar de la siguiente manera.