

# Switch POE-GSH2404M

24 Puertas PoE Gigabits + 4 Puertos SFP Gigabits

## Manual Web

Ver. Español 1.0



### Historial de revisiones

Fecha	Versión	Descripción
Diciembre 29, 2020	Sp-V 1.0	Primera edición español. LS.

# Contenido

Switch.....	1
POE-GSH2404M .....	1
<i>24 Puertas PoE Gigabits + 4 Puertos SFP Gigabits .....</i>	<i>1</i>
Manual Web .....	1
<i>Ver. Español 1.0.....</i>	<i>1</i>
Contenido.....	2
1.1 <i>Público objetivo .....</i>	<i>8</i>
12 <i>Manual de Convención .....</i>	<i>8</i>
.....	9
2. Inicio de sesión en la página web .....	9
21 <i>Inicie sesión en el cliente de administración de red.....</i>	<i>9</i>
22 <i>Constitución de la interfaz de cliente .....</i>	<i>9</i>
23 <i>Barra de navegación en la interfaz web.....</i>	<i>10</i>
3. Estado .....	17
31 <i>Información del sistema .....</i>	<i>17</i>
32 <i>Estadística.....</i>	<i>18</i>
33 <i>Tabla de direcciones MAC .....</i>	<i>19</i>
34 <i>Reiniciar.....</i>	<i>20</i>
4 Red.....	21
41 <i>Dirección IP .....</i>	<i>21</i>
42 <i>DNS .....</i>	<i>22</i>
43 <i>Hora del sistema .....</i>	<i>24</i>
5 Puerto .....	26
51 <i>Configuración del puerto.....</i>	<i>26</i>
52 <i>Error deshabilitado .....</i>	<i>27</i>
53 <i>Agregación de enlaces .....</i>	<i>28</i>
531 <i>Grupo.....</i>	<i>30</i>
532 <i>Configuración del puerto.....</i>	<i>32</i>
533 <i>LACP .....</i>	<i>33</i>
54 <i>EEE .....</i>	<i>36</i>

55	<i>Trama Jumbo</i> .....	37
56	<i>Seguridad portuaria</i> .....	37
57	<i>Puerto protegido</i> .....	38
58	<i>Control de tormentas</i> .....	40
59	<i>Espejado</i> .....	41
6	<i>Configuración de POE</i> .....	44
61	<i>Configuración del puerto PoE</i> .....	44
62	<i>Configuración del temporizador de puerto POE</i> .....	45
63	<i>Configuración de reinicio del temporizador de puerto POE</i> .....	46
7	<i>VLAN</i> .....	48
7.1	<i>VLAN</i> .....	49
7.1.1	<i>Crear VALN</i> .....	49
7.1.2	<i>Configuración de VLAN</i> .....	50
7.1.3	<i>Membresía</i> .....	51
7.1.4	<i>Configuración del puerto</i> .....	52
7.2	<i>VLAN de voz</i> .....	55
	<i>OUI de VLAN de voz</i> .....	55
7.3	<i>VLAN de protocolo</i> .....	61
7.4	<i>VLAN de Mac</i> .....	66
7.5	<i>VLAN de vigilancia</i> .....	69
7.6	<i>GVRP</i> .....	71
7.6.1	<i>Propiedad</i> .....	72
7.6.2	<i>Membresía</i> .....	74
7.6.3	<i>Estadística</i> .....	74
8	<i>Tabla de direcciones MAC</i> .....	75
8.1	<i>Dirección dinámica</i> .....	75
8.2	<i>Dirección estática</i> .....	77
8.3	<i>Dirección de filtrado</i> .....	78
8.4	<i>Dirección de seguridad del puerto</i> .....	78
9	<i>Árbol de expansión</i> .....	80
9.1	<i>Propiedad</i> .....	80

<b>92</b>	<b>Configuración del puerto.....</b>	<b>83</b>
<b>93</b>	<b>Instancia de MST.....</b>	<b>85</b>
<b>94</b>	<b>Configuración del puerto MST.....</b>	<b>86</b>
	Ejemplo de configuración de la función MSTP:.....	88
<b>95</b>	<b>Estadística.....</b>	<b>91</b>
<b>10</b>	<b>Descubrimiento.....</b>	<b>92</b>
<b>101</b>	<b>LLDP.....</b>	<b>93</b>
<b>102</b>	<b>Configuración del puerto.....</b>	<b>94</b>
<b>103</b>	<b>Política de red MED.....</b>	<b>96</b>
<b>104</b>	<b>Configuración del puerto MED.....</b>	<b>97</b>
<b>105</b>	<b>Vista de paquetes.....</b>	<b>98</b>
<b>106</b>	<b>Información local.....</b>	<b>99</b>
<b>107</b>	<b>Vecino.....</b>	<b>99</b>
<b>108</b>	<b>Estadística.....</b>	<b>100</b>
<b>11</b>	<b>DHCP.....</b>	<b>101</b>
	Breve introducción al servidor DHCP.....	101
	Asignación de direcciones IP de la estrategia de asignación de direcciones IP DHCP.....	101
<b>112</b>	<b>Configuración del grupo de direcciones IP.....</b>	<b>105</b>
<b>113</b>	<b>Configuración del grupo de direcciones IF de VLAN.....</b>	<b>106</b>
<b>114</b>	<b>Lista de clientes.....</b>	<b>107</b>
<b>115</b>	<b>Tabla de enlace estático de cliente.....</b>	<b>107</b>
<b>12</b>	<b>Multidifusión.....</b>	<b>108</b>
<b>121</b>	<b>General.....</b>	<b>108</b>
<b>1211</b>	<b>Propiedad.....</b>	<b>108</b>
<b>1212</b>	<b>Dirección del grupo.....</b>	<b>108</b>
<b>1213</b>	<b>Puerto del router.....</b>	<b>110</b>
<b>1214</b>	<b>Reenviar todo.....</b>	<b>110</b>
<b>1215</b>	<b>Regulación.....</b>	<b>111</b>
<b>1216</b>	<b>Perfil de filtrado.....</b>	<b>111</b>
<b>12.2</b>	<b>IGMP Snooping.....</b>	<b>112</b>
<b>1221</b>	<b>Propiedad.....</b>	<b>113</b>
<b>1222</b>	<b>Consulta.....</b>	<b>114</b>

12.2.3	<i>Estadística</i> .....	115
12.3	<i>MLD Fisgoneo</i> .....	116
1231	<i>Propiedad</i> .....	117
1232	<i>Estadística</i> .....	118
12.4	<i>MVR</i> .....	119
1241	<i>Propiedad</i> .....	120
1242	<i>Configuración del puerto</i> .....	121
12.4.3	<i>Dirección del grupo</i> .....	122
13	<i>Enrutamiento</i> .....	124
131	<i>Gestión e interfaces IPv4</i> .....	124
131.1	<i>Interfaz IPv4</i> .....	124
131.2	<i>Rutas IPv4</i> .....	125
131.3	<i>ARP</i> .....	126
132	<i>Administración e interfaces IPv6</i> .....	127
132.1	<i>Interfaz IPv6</i> .....	127
132.2	<i>Dirección IPv6</i> .....	128
132.3	<i>Rutas IPv6</i> .....	129
132.4	<i>Vecinos</i> .....	130
14	<i>Seguridad</i> .....	131
141	<i>RADIO</i> .....	131
142	<i>TACACS+</i> .....	132
14.3	<i>AAA</i> .....	134
1431	<i>Lista de métodos</i> .....	134
14.3.2	<i>Autenticación de inicio de sesión</i> .....	135
14.4	<i>Acceso de administración</i> .....	135
14.4.1	<i>VLAN de administración</i> .....	135
14.4.2	<i>Servicio de Gestión</i> .....	136
14.4.3	<i>ACL de administración</i> .....	138
14.5	<i>Administrador de autenticación</i> .....	140
1451	<i>Propiedad</i> .....	140
14.5.2	<i>Configuración del puerto</i> .....	141

14.5.3	<i>Cuenta local basada en MAC</i> .....	143
14.5.4	<i>Cuenta local basada en web</i> .....	143
14.5.5	<i>Sesiones</i> .....	143
14.6	<i>DoS</i> .....	144
14.6.1	<i>Propiedad</i> .....	144
14.6.2	<i>Configuración del puerto</i> .....	144
14.7	<i>Inspección ARP dinámica</i> .....	145
14.7.1	<i>Propiedad</i> .....	145
14.7.2	<i>Estadística</i> .....	146
14.8	<i>Espionaje DHCP</i> .....	147
14.8.1	<i>Propiedad</i> .....	147
14.8.2	<i>Estadística</i> .....	149
14.8.3	<i>Propiedad Opción82</i> .....	150
	Mecanismo de compatibilidad con la retransmisión DHCP de la opción 82 .....	151
14.9	<i>Protección de origen IP</i> .....	155
14.9.1	<i>Configuración del puerto</i> .....	156
14.9.2	<i>Enlace IMPV</i> .....	157
15	<i>ACL</i> .....	159
15.1	<i>ACL MAC</i> .....	159
15.2	<i>ACL IPv4</i> .....	162
15.3	<i>ACL IPv6</i> .....	165
15.4	<i>Enlace de ACL</i> .....	168
16	<i>QoS</i> .....	169
16.1	<i>General</i> .....	171
16.1.1	<i>Propiedad</i> .....	171
16.1.2	<i>Programación de colas</i> .....	172
16.1.3	<i>Mapeo de CoS</i> .....	173
16.1.4	<i>Mapeo DSCP</i> .....	174
16.1.5	<i>Asignación de precedencia IP</i> .....	175
16.2	<i>Límite de tarifa</i> .....	176
16.2.1	<i>Puerto de entrada / salida</i> .....	176

16.2.2	<i>Cola de salida</i> .....	177
17	<b>Diagnósticos</b> .....	178
17.1	<i>Registro</i> .....	178
17.2	<i>Ping</i> .....	179
17.3	<i>Traceroute</i> .....	180
17.4	<i>Prueba de cobre</i> .....	181
17.5	<i>Módulo de fibra</i> .....	182
17.6	<i>UDLD</i> .....	182
17.6.1	<i>Propiedad</i> .....	182
17.6.2	<i>Vecino</i> .....	184
18	<b>Administración</b> .....	185
18.1	<i>Cuenta de usuario</i> .....	185
18.2	<i>Firmware</i> .....	186
18.3	<i>Configuración</i> .....	186
18.3.1	<i>Actualizar</i> .....	186
18.3.2	<i>Guardar configuración</i> .....	187
18.4	<b>SNMP</b> .....	188
18.4.1	<i>Vista</i> .....	190
18.4.2	<i>Grupo</i> .....	191
18.4.3	<i>Comunidad</i> .....	192
18.4.4	<i>Usuario</i> .....	193
18.4.5	<i>ID del Equipo</i> .....	194
18.4.6	<i>Evento Trap</i> .....	194
18.4.7	<i>Notificación</i> .....	195
18.5	<b>RMON</b> .....	196
18.5.1	<i>Estadística</i> .....	197
18.5.2	<i>Historia</i> .....	198
18.5.3	<i>Evento</i> .....	199
18.5.4	<i>Alarma</i> .....	200

## 1.1 Público objetivo

Este manual está preparado para los instaladores y administradores de sistemas responsables de la instalación, configuración y mantenimiento de la red. Asume que el usuario ha entendido todos los protocolos de comunicación y gestión de la red, así como los términos técnicos, los principios teóricos, las habilidades prácticas y la experiencia de los dispositivos, protocolos e interfaces relacionados con las redes. También se requiere experiencia laboral en interfaz gráfica de usuario (GUI), interfaz de línea de comandos, protocolo simple de administración de red (SNMP) y web explorer.

## 1.2 Manual de Convención

Deben prevalecer los siguientes enfoques.

Convención GUI	Descripción
Interpretación	Describa las operaciones y agregue la información necesaria.
Cautela	Recuerde al usuario las precauciones, ya que las operaciones incorrectas provocarán la pérdida de datos o daños en el equipo.



## 2. Inicio de sesión en la página web

### 2.1 Inicie sesión en el cliente de administración de red

Escriba la dirección predeterminada del Switch: <http://192.168.2.1> y presione "Enter".

#### Descripción:

Estándares del navegador: superior a IE 9.0, Chrome 23.0 y Firefox 20.0

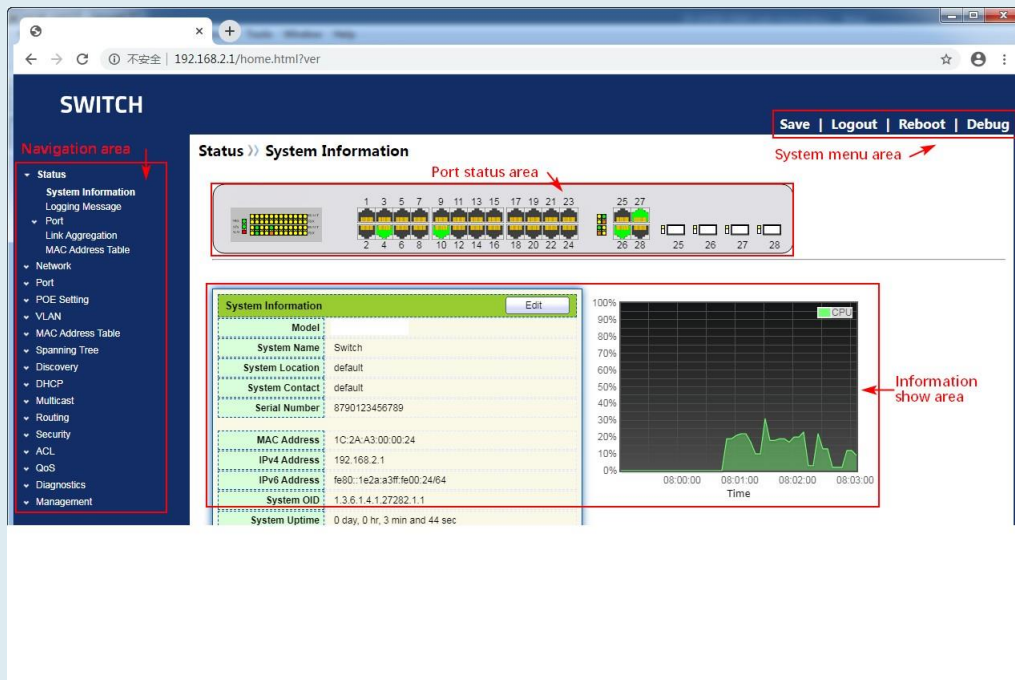
Mantenga el segmento de red IP de la PC consistente con el del conmutador, pero diferencie la dirección IP al iniciar sesión. Establezca la dirección IP del PC de 192.168.2.x y la máscara de subred de 255.255.255.0 para el primer inicio de sesión ( $1 < x \leq 254$ ).

Aparecerá una ventana de inicio de sesión como sigue. Type en el nombre de usuario predeterminado de "admin" y la contraseña de "admin". Haga clic en "Iniciar sesión" para ver el sistema de conmutación.

A screenshot of a web-based login interface. The background is a dark blue gradient. At the top center, the word "Login" is written in a large, white, sans-serif font. Below this, there are two white input fields. The first is labeled "Username:" and the second is labeled "Password:". Both labels are in a small, white, sans-serif font. Below the input fields, there is a white button with the word "LOGIN" in a small, blue, sans-serif font. The entire form is centered on the page.

### 2.2 Constitución de la interfaz de cliente

La interfaz de operación típica del sistema de administración de red web es la siguiente.



## 23 Barra de navegación en la interfaz web

Los elementos de menú como Estado, Red, Puerto, Configuración de PoE, VLAN, Tabla de direcciones MAC, Árbol de expansión, Detección, DHCP, Multidifusión, Enrutamiento, Seguridad, ACL, QoS, Diagnóstico y Administración están disponibles en el cliente de administración de red web. Cada elemento contiene submenús. La barra de navegación se detalla de la siguiente manera:

Menú	Submenús	Submenús secundarios	Descripción	
Status	System Information		Mostrar el estado del puerto y la información del producto	
	Logging Message		Mostrar los registros de funcionamiento y ejecución del dispositivo	
	Port	Statistics		Mostrar las estadísticas detalladas del puerto
		Error Disabled		Mostrar los errores que se producen en los puertos
		Bandwidth Utilization		Mostrar la utilización del ancho de banda por unidad de tiempo de todos los puertos
	Link Aggregation		Mostrar el estado y los miembros del grupo de agregación	
MAC Address Table		Mostrar la tabla de direcciones MAC del dispositivo actual		
Network DNS	IP Address		Configurar y ver la dirección IP de administración	
			Configurar y ver la configuración de DNS y servidor	
			Configurar y ver el servidor DNS y la tabla de asignación dinámica de host	
	Hosts		Configurar y ver la hora actual del sistema	

Menu	Submenus	Secondary Submenus	Descripción	
Port	Port Setting		Configurar y ver todos los puertos	
	Error Disabled		Configurar y ver la protección de deshabilitación de errores de puerto	
	Link Aggregation	Group		Configurar y ver los algoritmos de equilibrio de puertos y estrategias contenidos en LAG
		Post Setting		Configurar y ver el LAG
		LACP		Compruebe la prioridad del sistema LACP y la configuración del puerto
	EEE		Configurar y ver el estado y la información de EEE	
	Jumbo Frame		Configurar y ver la longitud del mensaje máximo reenviado por el sistema	
	Port Security		Configurar y ver la limitación de velocidad de la 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 tormentas portuarias	
Mirroring		Configurar y ver la duplicación de puertos		
POE Setting	POE Port Setting		Configurar y ver el puerto POE	
	POE Port Timer Setting		Configurar y ver el Switch de temporización del puerto POE	
	POE Port Timer Reboot Setting		Configurar y ver el reinicio programado del puerto Poe	
VLAN	VLAN	Create VLAN	Configurar y ver la información de VLAN del dispositivo	
		VLAN Configuration	Configurar y ver la configuración de VLAN de todos los puertos	
		Membership	Configurar y ver la información de puerto de las VLAN	
		Port Setting	Configurar y ver los atributos PVID y VLAN de los puertos	
	Voice VLAN	Property	Configurar y ver la función Voice-VLAN y la información de estado del puerto	
		Voice OUI	Configurar y ver información de OUI de Voice-VLAN	
	Protocol VLAN	Protocol Group	Configurar y ver el grupo VLAN de protocolo	
		Group Binding	Configurar y ver el puerto VLAN de protocolo y el enlace de grupo	
	MAC VLAN	MAC Group	Configurar y ver el grupo VLAN de MAC	
		Group Binding	Configurar y ver el puerto MAC VLAN y el enlace de grupo	
	Surveillance VLAN	Property	Configurar y ver la función Surveillance-VLAN y la información del estado del puerto	
		Surveillance OUI	Configurar y ver la información de OUI de Surveillance-VLAN	
	GVRP	Property	Configurar y ver el estado funcional global y del puerto	
		Membership	Configurar y ver las VLAN aprendidas y los miembros del puerto	

		Statistics	Configurar y ver las estadísticas de mensajes relacionadas con los puertos
MAC Address Table	Dynamic Address		Configurar y ver las direcciones MAC dinámicas y el tiempo de caducidad del dispositivo
	Static Address		Configurar y ver las tablas de direcciones MAC estáticas del dispositivo
	Filtering Address		Configurar y ver las tablas de direcciones MAC que se van a filtrar
	Port Security Address		Configurar y ver la tabla de direcciones MAC aprendida por la seguridad del puerto
Spanning Tree	Port Security		Configurar y ver el estado y los atributos de STP
	Port Setting		Configurar y ver las atribuciones de puerto de STP
	MST Instance		Configurar y ver los atributos de instancia de los STP
	MST Port Setting		Configurar y ver las instancias (incluida la información del puerto) de los STP
	Statistics		Configurar y ver las estadísticas de mensajes STP de cada puerto
Discovery	LLDP	Property	Configurar y ver los atributos relacionados con LLDP
		Port Setting	Configurar y ver el estado de transmisión y recepción de LLDP en cada puerto
		MED Network Policy	Configurar y ver la entrada de la tabla de estrategia de red MED
		Packet View	Configurar y ver los mensajes LLDP detallados en cada puerto
		Local Information	Configurar y ver el estado LLDP y LLDP-MED
		Neighbor	Configurar y ver la información del vecino LLDP
		Statistics	Configurar y ver el estado de transmisión y recepción del mensaje LLDP en cada puerto
DHCP	Property		Configurar y ver conmutadores de servicio DHCP y conmutadores de puerto
	IP Pool Setting		Configurar y ver el grupo de direcciones IP del servidor DHCP
	VLAN IF Address Group Setting		Configurar y ver la relación de enlace de grupo de servidores VLANIF y DHCP
	Client List		Ver la lista de clientes DHCP
	Client Static Binding Table		Configurar y ver entradas de tabla de enlace estático de cliente DHCP
Multicast	General	Property	Configurar y ver la configuración de la función
		Group Address	Configurar y ver la información de multidifusión estática relevante
		Router Port	Configurar y ver la información del puerto enrutado de multidifusión
		Forwarding All	Configurar y ver la información del puerto de reenvío de multidifusión
		Throttling	Configurar y ver el límite de multidifusión en cada puerto

		Filtering Profile	Configurar y ver las direcciones de multidifusión filtradas
		Filtering Binding	Configurar y ver la información de enlace relacionada con la regla de filtrado y los puertos
	IGMP Snooping	Property	Configure y vea el switch, la versión, etc.
		Querier	Configurar y ver el estado de la consulta
		Statistics	Configurar y ver los mensajes de protocolo
	MLD Snooping	Property	Configurar y ver el protocolo, switch, etc.
		Statistics	Configurar y ver los mensajes de protocolo
	MVR	Property	Configurar y ver la información del atributo, como el modificador
		Port Setting	Configurar y ver el estado en cada puerto
		Group Address	Configurar y ver la función, VLAN y dirección de grupo
Routing	IPv4 Management and Interfaces	IPv4 Interface	Configurar y ver la información de la dirección IPv4 de VLANIF
		IPv4 Routes	Configurar y ver rutas estáticas IPv4
		ARP	Configurar y ver la tabla ARP
	IPv6 Management and Interfaces	IPv6 Interface	Configurar y ver la información de la interfaz IPv6 de VLANIF
		IPv6 Address	Configurar y ver la información de la dirección IPv6 de VLANIF
		IPv6 Routes	Configurar y ver rutas estáticas IPv6
		IPv6 Neighbors	Configurar y ver la tabla de vecinos IPv6

Security	RADIUS		Configurar para ver información relacionada con el servidor RADIUS	
	TACACS+		Configurar para ver información relacionada con el servidor TACACS+	
	AAA	Method List		Configurar y ver el método de autenticación de inicio de sesión
		Login Authentication		Configurar y ver los métodos de autenticación de terminales
	Management Access	Management VLAN		Configurar y ver VLAN de administración
		Management Service		Configurar y ver el modo de administración de servicios y los atributos relevantes
		Management ACL		Configurar y ver la ACL con el objetivo de administrar canales
		Management ACE		Configurar y ver la configuración de ACE de los canales de administración
	Authentication Management	Property		Configurar y ver los atributos de autenticación
		Port Setting		Configurar y ver la información de autenticación en cada puerto
		MAC Local Account		Configurar y ver la lista de cuentas locales MAC
		Web Local Account		Configurar y ver la lista de cuentas locales web
		Sessions		Configurar y ver la información relacionada con la autenticación de sesión
	DoS	Property		Configurar y ver la opción de conmutador
		Port Setting		Configurar y ver la opción de conmutador en los puertos
	Dynamic ARP Inspection	Property		Configurar y ver la inspección ARP dinámica
		Statistics		Configurar y ver las estadísticas de mensajes en estado de inspección APR en cada puerto
	DHCP Snooping	Property		Configurar y ver el conmutador y el estado
		Statistics		Configurar y ver las estadísticas de mensajes DHCP recibidas por 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 la opción 82
	IP Source Guard	Port Setting		Configurar y ver el estado en los puertos
		IMPV Binding		Configurar y ver las tablas de enlace de IP, MAC, Puerto y VLAN
Save Database			Configurar y ver el almacenamiento y la información de la entrada de la tabla de enlace	

ACL	MAC ACL		Configurar para ver información relacionada con el servidor RADIUS
	MAC ACE		Configurar y ver el método de autenticación de inicio de sesión
	IPv4 ACL		Configurar y ver el método de autenticación de inicio de sesión
	IPv4 ACE		Configurar y ver VLAN de administración
	IPv6 ACL		Configurar y ver los atributos de autenticación
	ACL Binding		Configurar y ver la opción de conmutador
Qos	General	Property	Configurar y ver el conmutador QoS y el estado
		Queue Scheduling	Configurar y ver el algoritmo de programación de colas
		CoS Mapping	Configurar y ver la tabla de asignación de colas locales y de prioridad
		DSCP Mapping	Configurar y ver la tabla de asignación de colas locales y de prioridad
		IP Precedence Mapping	Configurar y ver la tabla de asignación de colas locales y de prioridad
	Rate Limit	Ingress/ Egress Port	Configurar y ver la configuración de la limitación de velocidad de puerto
		Egress Queue	Configurar y ver la configuración de limitación de velocidad basada en la cola de salida
Diagnostics	Logging	Property	Configurar y ver el conmutador y el estado
		Remote Server	Configurar y ver la dirección de los servidores remotos
	Ping		Diagnóstico de red por Ping
	Traceroute		Diagnósticos de red por traceroute
	Copper Test		Diagnóstico de enlace de interfaz eléctrica por APV
	Fiber Module		Compruebe el módulo SFP en interfaces ópticas
	UDLD	Property	Configurar y ver el conmutador y el estado
		Neighbor	Configurar y ver el estado del vecino
Management	User Account		Configurar y ver la información del usuario
	Firmware	Upgrade	Actualizar software
	Configuration	Upgrade	Actualizar archivos de configuración
		Save Configuration	Guarde los archivos de configuración compatibles con el dispositivo en ejecución
	SNMP	View	Configurar y ver la entrada de tabla de vista de función SNMP
		Group	Configurar y ver el grupo SNMP
		Community	Configurar y ver la comunidad SNMP
		User	Configurar y ver los atributos de usuario SNMP
		Engine ID	Configurar y ver el SNMP y los ID de motor remotos
		Trap Event	Configurar y ver el estado y el conmutador de captura SNMP

		Notification	Configurar y ver el estado del servidor de notificaciones SNMP
	RMON	Statistics	Configurar y ver el historial de estadísticas de mensajes de todos los puertos
		History	Configurar y ver el estado del registro del historial
		Event	Configurar y ver el estado del evento
		Alarm	Configurar y ver el estado de alarma



# 3. Estado



## 3.1 Información del sistema

De acuerdo con el switch conectado, el panel de administración de la red web muestra directamente la información del puerto y del producto, incluido: número de puertos, estados del puerto, información del producto, estados del dispositivo, estados de encendido y apagado de la función, etc.

Instrucciones:

1. Haga clic en "Estado > información del sistema" en la barra de navegación de la siguiente manera:

The screenshot shows a network switch management interface. At the top, there is a port status bar with 28 ports numbered 1 to 28. Ports 1-24 are in a 4x6 grid, and ports 25-28 are in a 2x4 grid. Ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 26, and 28 are shown as active (green). Below the port bar is a 'System Information' panel with an 'Edit' button. The panel contains the following data:

<b>Model</b>	
<b>System Name</b>	Switch
<b>System Location</b>	default
<b>System Contact</b>	default
<b>Serial Number</b>	8790123456789
<b>MAC Address</b>	1C:2A:A3:00:00:24
<b>IPv4 Address</b>	192.168.2.1
<b>IPv6 Address</b>	fe80::1e2a:a3ff:fe00:24/64
<b>System OID</b>	1.3.6.1.4.1.27282.1.1
<b>System Uptime</b>	0 day, 0 hr, 3 min and 22 sec
<b>Current Time</b>	2020-01-01 08:02:52 UTC+8
<b>Loader Version</b>	3.2.0.30
<b>Loader Date</b>	Oct 09 2020 - 10:40:51
<b>Firmware Version</b>	1.0.0.24
<b>Firmware Date</b>	Oct 09 2020 - 10:44:27
<b>Telnet</b>	Disabled
<b>SSH</b>	Disabled
<b>HTTP</b>	Enabled
<b>HTTPS</b>	Disabled
<b>SNMP</b>	Disabled

To the right of the system information panel are two performance graphs. The top graph is labeled 'CPU' and shows CPU usage percentage over time from 07:59:00 to 08:02:00. The usage is mostly low, with a peak of approximately 30% around 08:01:00. The bottom graph is labeled 'MEM' and shows memory usage percentage over the same time period. Memory usage is low until 08:01:00, where it spikes to about 60% and then remains relatively stable.

Descripción:

Pase el ratón sobre un puerto para comprobar el número de puerto, el tipo, la velocidad y el estado. "Edite" el "Nombre del sistema", "Ubicación" y "Contacto" en la información del producto. "Aplicar" y terminar.

## 3.2 Estadística

Introduzca las estadísticas de flujo detalladas en un puerto y la información que los usuarios deben actualizar o borrar manualmente.

1. Haga clic en "Estado >> estadísticas de puerto" en la barra de navegación de la siguiente manera:

<b>Port</b>	GE3 ▼
<b>MIB Counter</b>	<input checked="" type="radio"/> All <input type="radio"/> Interface <input type="radio"/> Etherlike <input type="radio"/> RMON
<b>Refresh Rate</b>	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

Interface	
<b>ifInOctets</b>	60938
<b>ifInUcastPkts</b>	210
<b>ifInNUcastPkts</b>	318
<b>ifInDiscards</b>	0
<b>ifOutOctets</b>	185965
<b>ifOutUcastPkts</b>	212
<b>ifOutNUcastPkts</b>	1422
<b>ifOutDiscards</b>	0
<b>ifInMulticastPkts</b>	160
<b>ifInBroadcastPkts</b>	158
<b>ifOutMulticastPkts</b>	770
<b>ifOutBroadcastPkts</b>	652

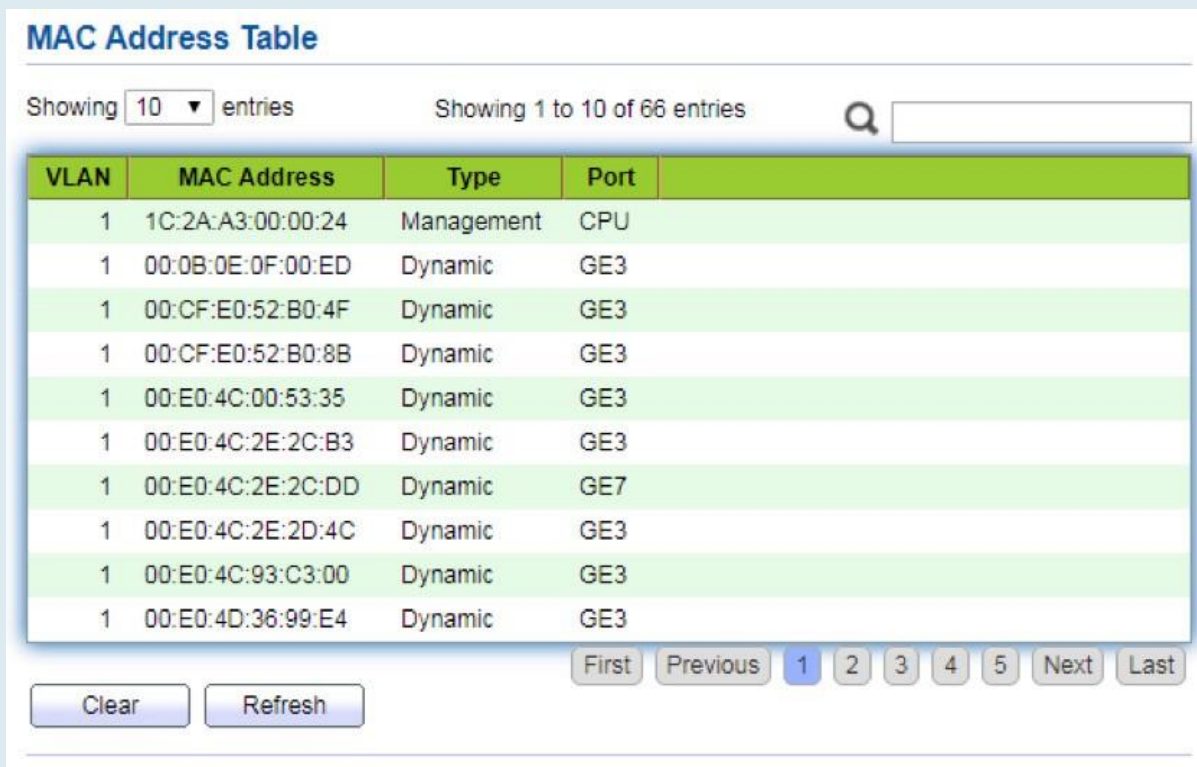
Descripción:

"Borre" las estadísticas de flujo en el puerto actual y refrescar la página.

### 3.3 Tabla de direcciones MAC

Ver información de la tabla de direcciones MAC Instrucciones:

1. Haga clic en "Estado > tabla de direcciones MAC " en la barra de navegación de la siguiente manera:



**MAC Address Table**

Showing 10 entries      Showing 1 to 10 of 66 entries     

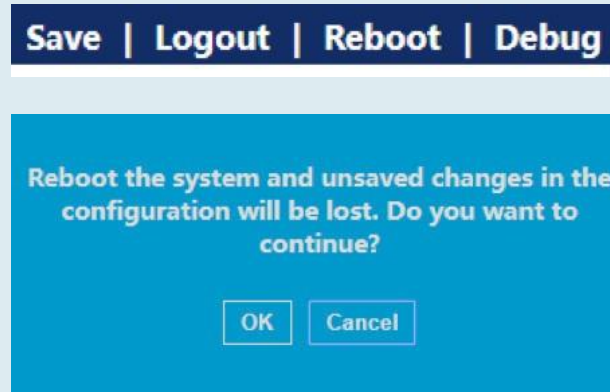
VLAN	MAC Address	Type	Port
1	1C:2A:A3:00:00:24	Management	CPU
1	00:0B:0E:0F:00:ED	Dynamic	GE3
1	00:CF:E0:52:B0:4F	Dynamic	GE3
1	00:CF:E0:52:B0:8B	Dynamic	GE3
1	00:E0:4C:00:53:35	Dynamic	GE3
1	00:E0:4C:2E:2C:B3	Dynamic	GE3
1	00:E0:4C:2E:2C:DD	Dynamic	GE7
1	00:E0:4C:2E:2D:4C	Dynamic	GE3
1	00:E0:4C:93:C3:00	Dynamic	GE3
1	00:E0:4D:36:99:E4	Dynamic	GE3

Los datos de la interfaz son los siguientes.

Elementos de consulta	Descripción
Mac	Dirección MAC de destino
VLAN	ID de VLAN que pertenece a la dirección MAC
Puerto	Salida de mensajes correspondiente a la dirección MAC
Tipo	<p>La dirección MAC dinámica se refiere a la entrada que envejecerá con el tiempo de envejecimiento establecido. Los conmutadores pueden agregar entradas basadas en el mecanismo de aprendizaje de la dirección MAC o la creación manual.</p> <p>La dirección MAC estática se refiere a la tabla especificada que se configura manualmente y no envejece.</p> <p>La dirección MAC de administración se refiere a la dirección en el puerto de administración.</p>

## 3.4 Reiniciar

1. Haga clic en "Reiniciar" en la parte superior derecha como se indica a continuación.



# 4 Red



## 4.1 Dirección IP

Cambie la dirección IP de administración en la interfaz web.  
Instrucciones:

1. Haga clic en "Dirección IP de > de red" en la barra de navegación para descubrir la dirección IPv4 de 192.168.2.1/24 de forma predeterminada de la siguiente manera:
2. Repita este paso, seleccione el tipo de dirección "Estática", ingrese la dirección IPv4 de 192.168.2.1, la máscara de subred de 255.255.255.0 y la administración de red de 192.168.2.254. "Aplicar" y terminar.

IPv4 Address	
Address Type	<input checked="" type="radio"/> Static <input type="radio"/> Dynamic
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254

Sub IPv4 Address	
Enabled	<input type="checkbox"/> Enable
IP Address	0.0.0.0
Subnet Mask	0.0.0.0

IPv6 Address	
Auto Configuration	<input checked="" type="checkbox"/> Enable
DHCPv6 Client	<input type="checkbox"/> Enable
IPv6 Address	
Prefix Length	0 (0 - 128)
IPv6 Gateway	

Operational Status	
IPv4 Address	192.168.2.1
IPv4 Default Gateway	192.168.2.254
Sub IPv4 Address	0.0.0.0
IPv6 Address	::
IPv6 Gateway	::
Link Local Address	fe80::1e2a:a3ff:fe00:24/64

Apply

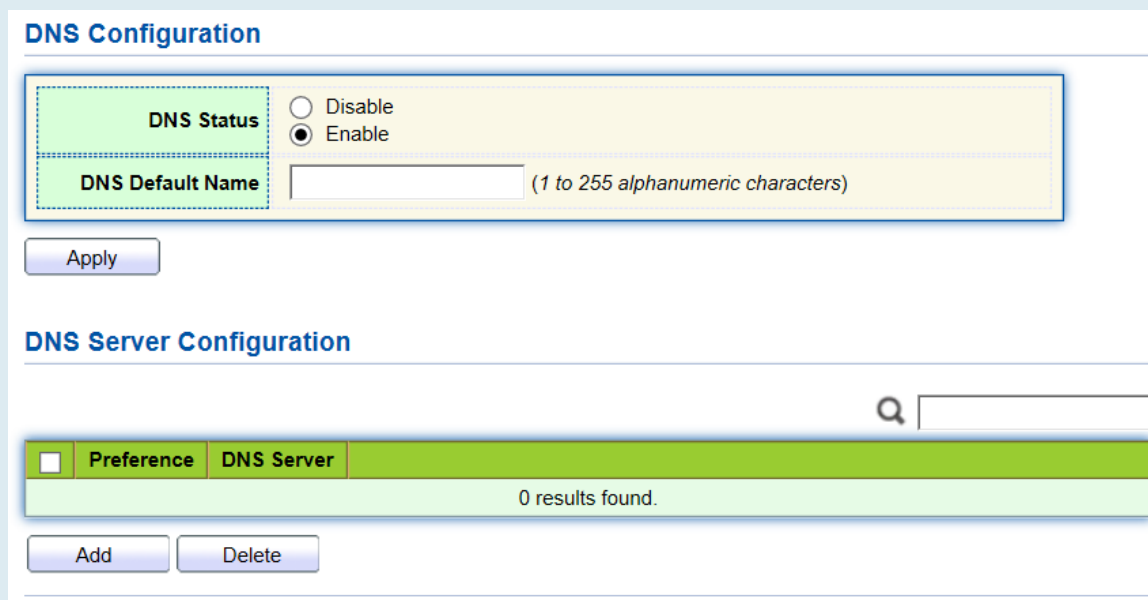
## 4.2 DNS

DNS es la abreviatura de Sistema de nombres de dominio para nombrar equipos y servicios de red de unidades a jerarquías de dominio.

Un nombre de dominio consiste en los puntos separados por una serie de palabras o abreviaturas, cada una correspondiente a una dirección IP única. DNS es el servidor en Internet que resuelve los nombres de dominio. Aplicable a Internet y otras redes TCP/IP, el nombre DNS recupera equipos y servicios a través de nombres descriptivos. Como uno de los principales servicios de Internet, DNS es una base de datos distribuida que mapea nombres de dominio y direcciones IP mutuamente.

Instrucciones:

1. Haga clic en "Network > DNS" en la barra de navegación de la siguiente manera.



**DNS Configuration**

**DNS Status**  Disable  Enable

**DNS Default Name**  (1 to 255 alphanumeric characters)

Apply

**DNS Server Configuration**

Q

<input type="checkbox"/>	Preference	DNS Server
0 results found.		

Add Delete

Los datos de la interfaz son los siguientes.

Elementos de configuración	Descripción
DNS State	Conmutador DNS
DNS Default Name	Introduzca el nombre predeterminado de DNS

2. "Agregar" para configurar el servidor DNS.



**Add DNS Server**

**IPv4/IPv6 Address**

Apply Close

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

### DNS Server Configuration

---

<input type="checkbox"/>	Preference	DNS Server
<input type="checkbox"/>	1	114.114.114.114

## 4.3 Hora del sistema

Se utiliza principalmente para configurar la hora del sistema y seleccionar la fuente de tiempo, el horario de verano, etc.

Instrucciones

1. Haga clic en "Hora de red > sistema" en la barra de navegación de la siguiente manera.

<b>Source</b>	<input type="radio"/> SNTP <input type="radio"/> From Computer <input checked="" type="radio"/> Manual Time
<b>Time Zone</b>	UTC +8:00 ▾
<b>SNTP</b>	
<b>Address Type</b>	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
<b>Server Address</b>	<input type="text"/>
<b>Server Port</b>	123 (1 - 65535, default 123)
<b>Manual Time</b>	
<b>Date</b>	2019-01-01 YYYY-MM-DD
<b>Time</b>	09:07:05 HH:MM:SS
<b>Daylight Saving Time</b>	
<b>Type</b>	<input checked="" type="radio"/> None <input type="radio"/> Recurring <input type="radio"/> Non-recurring <input type="radio"/> USA <input type="radio"/> European
<b>Offset</b>	60 Min (1 - 1440, default 60)
<b>Recurring</b>	From: Day <input type="text" value="Sun"/> ▾ Week <input type="text" value="First"/> ▾ Month <input type="text" value="Jan"/> ▾ Time <input type="text"/>
	To: Day <input type="text" value="Sun"/> ▾ Week <input type="text" value="First"/> ▾ Month <input type="text" value="Jan"/> ▾ Time <input type="text"/>
<b>Non-recurring</b>	From: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM
	To: <input type="text"/> YYYY-MM-DD <input type="text"/> HH:MM
<b>Operational Status</b>	
<b>Current Time</b>	2019-01-01 09:07:05 UTC+8



Los datos de la interfaz son los siguientes.

Elementos de configuración	Descripción
Time Source	Seleccione la fuente de tiempo en SNTP, PC o modos manuales
Time Zone	Establecer la zona horaria
Address Type	Nombre de host o dirección IPv4 (con origen de tiempo establecido por SNTP)
Server Address	Dirección del servidor (con origen de tiempo establecido por SNTP)
Server Port No.	Número de puerto del servidor (con origen de tiempo establecido por SNTP)
Date	Información de fecha: DD/MM/AAAA (con la fuente de tiempo configurada en modo manual)
Time	Información de tiempo: SS / MM / HH (con fuente de tiempo configurada en modo manual)
Type	Los tipos de horario de verano se dividen en Ninguno, cíclico, no cíclico, Estados Unidos y Europa.
Reimbursed Time	Tiempo de verano reembolsado
Cyclic Mode	Configurar el modo cíclico del horario de verano
Non-cyclic Mode	Configurar el modo no cíclico del horario de verano

# 5 Puerto



## 5.1 Configuración del puerto

Las interfaces deben identificarse para que los usuarios puedan consultar y configurar las interfaces Ethernet como deseen.

Instrucciones:

1. Haga clic en "Configuración de puerto > puerto" en la barra de navegación:

Port Setting Table

Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	1	GE1	1000M Copper	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	2	GE2	1000M Copper	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	3	GE3	1000M Copper	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	4	GE4	1000M Copper	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	5	GE5	1000M Copper	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	6	GE6	1000M Copper	Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	7	GE7	1000M Copper	Enabled	Down	Auto	Auto	Disabled

2. Seleccione los puertos que desea configurar y "Editar" de la siguiente manera:

Edit Port Setting

Port	GE1-GE3
Description	<input type="text"/>
State	<input checked="" type="checkbox"/> Enable
Speed	<input checked="" type="radio"/> Auto <input type="radio"/> 10M <input type="radio"/> Auto - 10M <input type="radio"/> 100M <input type="radio"/> Auto - 100M <input type="radio"/> 1000M <input type="radio"/> Auto - 1000M <input type="radio"/> 10G <input type="radio"/> Auto - 10M/100M
Duplex	<input checked="" type="radio"/> Auto <input type="radio"/> Full <input type="radio"/> Half
Flow Control	<input type="radio"/> Auto <input type="radio"/> Enable <input checked="" type="radio"/> Disable

Los datos de la interfaz son los siguientes.

Elementos de configuración	Descripción
Port	Lista de puertos
Description	Alias de puerto
State	Habilitar o deshabilitar el puerto
Speed	Negociación automática configurable con estados obligatorios de 10 Mb, 100 Mb y 1.000 Mb. Las velocidades de interfaz que incluyen 10 Mbit/s, 100 Mbit/s y 1.000 Mbit/s están disponibles para las interfaces eléctricas Ethernet y son opcionales según sea necesario.
Duplex	Negociación automática configurable con dúplex completo o medio.
Flow Control	Después de habilitarlo tanto en la red local como en los dispositivos de red opuestos, el local notificará al otro que deje de transmitir mensajes en presencia de congestión de la red. El opuesto ejecutará el comando temporalmente para garantizar que no haya ningún mensaje. Recepción y transmisión de discapacitados y transmisión de la trama PAUSE; Habilitado para habilitar la recepción y transmisión de la trama PAUSE; Negociación automática: negocie automáticamente la trama PAUSE con dispositivos de red opuestos.

## 5.2 Error deshabilitado

En general, si el software del switch detecta algunos errores en el puerto, el puerto se cerrará inmediatamente. En otras palabras, cuando el sistema operativo del switch detecta algunos eventos de error en el puerto del switch, el switch cerrará automáticamente el port Instrucciones:

1. Haga clic en "Error de > de puerto deshabilitado" en la barra de navegación para habilitar o deshabilitar la configuración de la siguiente manera:

<b>Recovery Interval</b>	<input type="text" value="300"/>	Sec (30 - 86400)
<b>BPDU Guard</b>	<input type="checkbox"/>	Enable
<b>UDLD</b>	<input type="checkbox"/>	Enable
<b>Self Loop</b>	<input type="checkbox"/>	Enable
<b>Broadcast Flood</b>	<input type="checkbox"/>	Enable
<b>Unknown Multicast Flood</b>	<input type="checkbox"/>	Enable
<b>Unicast Flood</b>	<input type="checkbox"/>	Enable
<b>ACL</b>	<input type="checkbox"/>	Enable
<b>Port Security</b>	<input type="checkbox"/>	Enable
<b>DHCP Rate Limit</b>	<input type="checkbox"/>	Enable
<b>ARP Rate Limit</b>	<input type="checkbox"/>	Enable

### 5.3 Agregación de enlaces

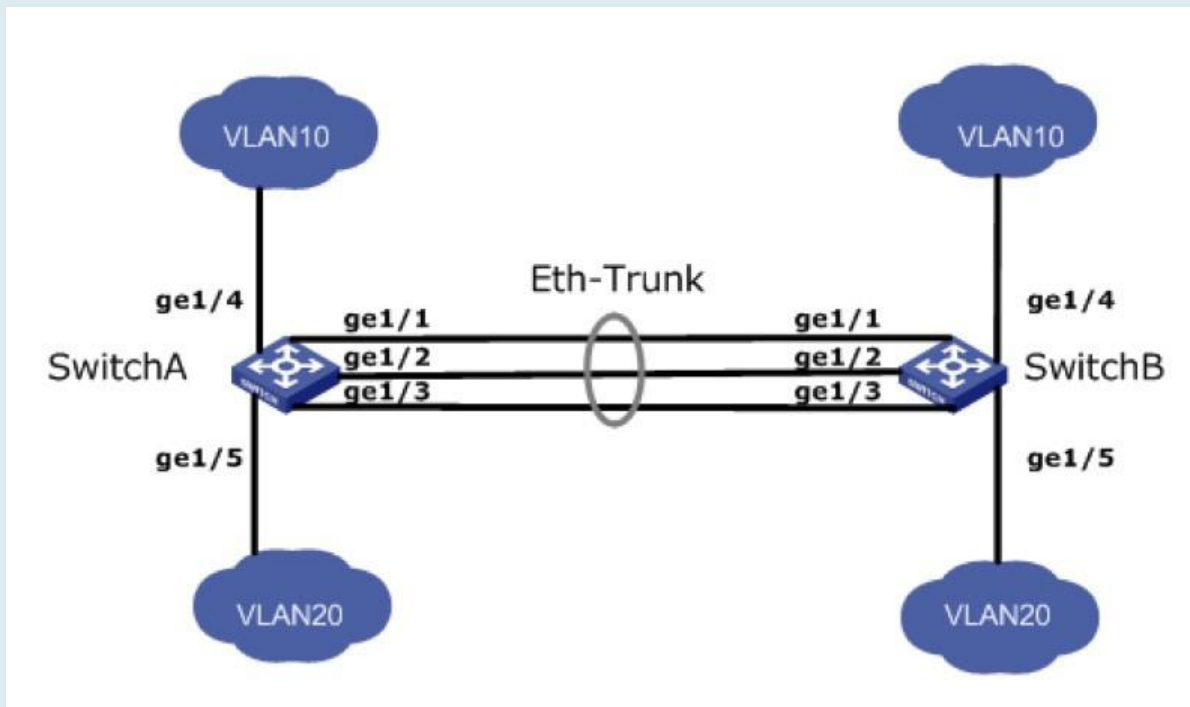
La agregación de enlaces amplía el ancho de banda y la fiabilidad al agrupar un grupo de interfaces físicas en una única interfaz lógica.

LAG (Link Aggregation Group) es un enlace lógico agrupado por múltiples enlaces Ethernet (Eth-Trunk).

La expansión incesante del tamaño de la red aumenta las demandas de los usuarios de ancho de banda de enlace y confiabilidad. Tradicionalmente, la placa de interfaz de alta velocidad o el equipo compatible generalmente se reemplaza para optimizar el ancho de banda, que es costoso e inflexible.

La tecnología de agregación de enlaces agrupa múltiples interfaces físicas en una sola interfaz lógica sin actualizar el hardware. Su mecanismo de respaldo no solo mejora la confiabilidad, sino que también comparte la carga de flujo en diferentes enlaces físicos.

Como se muestra a continuación, el conmutador A está vinculado con el conmutador B a través de tres enlaces Ethernet que se agrupan en un enlace lógico Eth-Trunk. Su ancho de banda es igual al de los tres enlaces en total, ampliando así el ancho de banda. Mientras tanto, estos tres enlaces se respaldan mutuamente para ser más confiables.



La agregación de enlaces puede satisfacer las siguientes demandas:

- Ancho de banda insuficiente de dos switches conectados con un enlace.
- Fiabilidad insuficiente de dos Switches conectados con un enlace.

La agregación de enlaces se puede dividir en modo manual y modo LACP de acuerdo con el estado del protocolo de control de agregación de enlaces (LACP).

En el primer modo, establecimiento Eth-Trunk, el acceso a la interfaz miembro debe agregarse manualmente sin LACP. También se llama modo de uso compartido de carga porque todos los enlaces están involucrados en el reenvío de datos y el uso compartido de carga. En caso de que falle algún enlace activo, LAG promediará la carga con los restantes. Este modo se prefiere bajo la circunstancia de que dos dispositivos conectados directamente requieren un ancho de banda de enlace mayor pero no tienen acceso a LACP.

## 5.3.1 Grupo

Instrucciones para agregar una agregación de vínculos estáticos:

1. Haga clic en "Grupo de > agregación de > de puertos", seleccione un algoritmo de equilibrio de carga con un botón de opción. "Aplicar" y terminar de la siguiente manera:

**Load Balance Algorithm**
 MAC Address  
 IP-MAC Address

### Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
<input type="radio"/>	LAG 1	---	---		
<input type="radio"/>	LAG 2	---	---		
<input type="radio"/>	LAG 3	---	---		
<input type="radio"/>	LAG 4	---	---		
<input type="radio"/>	LAG 5	---	---		
<input type="radio"/>	LAG 6	---	---		
<input type="radio"/>	LAG 7	---	---		
<input type="radio"/>	LAG 8	---	---		

2. Seleccione uno de los 8 LAG disponibles, "Edite" la página de configuración de la siguiente manera:

### Edit Link Aggregation Group

<b>LAG</b>	1
<b>Name</b>	<input type="text"/>
<b>Type</b>	<input checked="" type="radio"/> Static <input type="radio"/> LACP
<b>Member</b>	<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <p>Available Port</p> <ul style="list-style-type: none"> <li>GE1</li> <li>GE2</li> <li>GE3</li> <li>GE4</li> <li>GE5</li> <li>GE6</li> <li>GE7</li> <li>GE8</li> </ul> </div> <div style="margin-right: 10px;"> <input type="button" value="➤"/>   <input type="button" value="➤"/> </div> <div> <p>Selected Port</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> </div> </div>

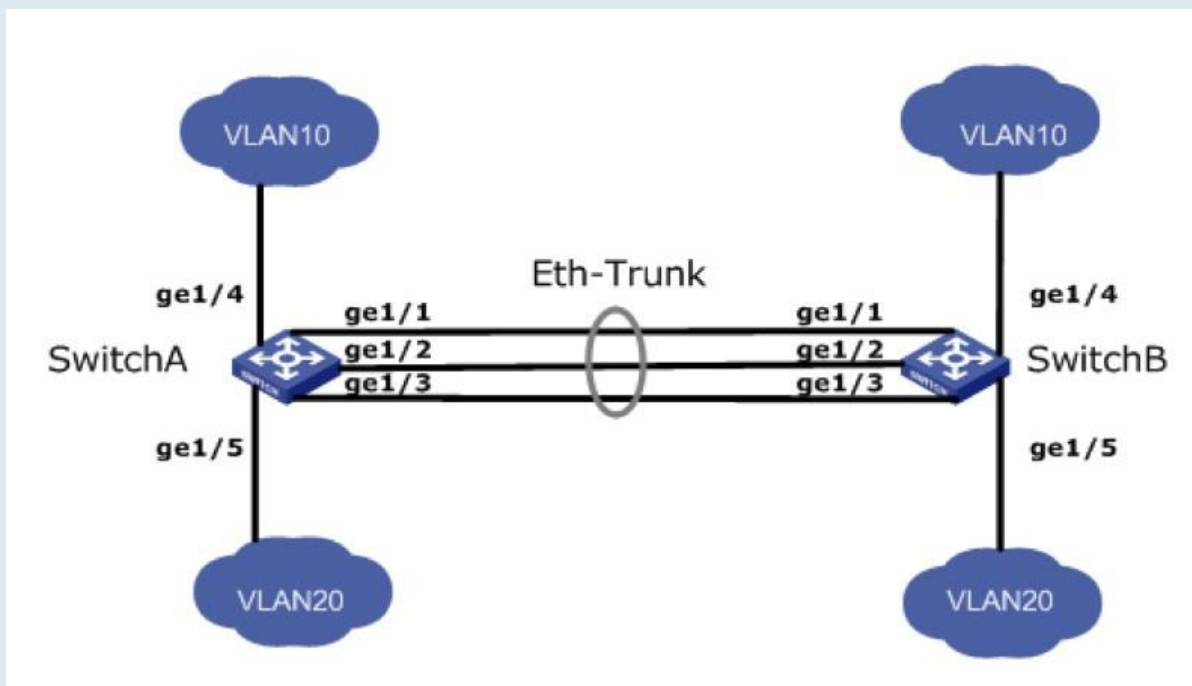
Los datos de la interfaz son los siguientes.

Elementos de configuración	Descripción
LAG	Hay 8 GAL numerados del 1 al 8.
Name	Descripción del GAL, que puede modificarse según sea necesario.
Type	Seleccione entre el modo manual y el modo LACP.
Member	Hasta 8 puertos miembro están disponibles en LAG.

Ilustración:

Como se muestra a continuación, el conmutador A y el conmutador B conectan VLAN 10 y 20 a través de Ethernet respectivamente, con un gran flujo de datos entre ellos. Se espera que tanto el conmutador A como el B proporcionen un ancho de banda de enlace superior para la comunicación VLAN. Mientras tanto, debería haber redundancia para la transmisión de datos y enlaces confiables.

Diagrama de red LAG en modo manual



Instrucciones:

1. Cree la interfaz troncal ETH en SwitchA y agregue una interfaz miembro para aumentar el ancho de banda del enlace. La configuración de SwitchB es como la de SwitchA. Haga clic en "Port > Link Aggregation > Group", elija "LAG 1" y los puertos GE1, 2 y 3 y muévalos a los puertos seleccionados a la derecha. "Aplicar" y terminar de la siguiente manera.

### Link Aggregation Table

	LAG	Name	Type	Link Status	Active Member	Inactive Member
<input type="radio"/>	LAG 1		Static	Up	GE3	GE1-GE2
<input type="radio"/>	LAG 2		---	---		
<input type="radio"/>	LAG 3		---	---		
<input type="radio"/>	LAG 4		---	---		

## 5.3.2 Configuración del puerto

Configuración de atributos del puerto miembro del grupo de agregación

1. Haga clic en "Configuración de puerto > vincular agregación > puerto" para ingresar a la interfaz de configuración de atributos del puerto miembro del grupo de agregación de la siguiente manera:

### Port Setting Table

<input type="checkbox"/>	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
<input type="checkbox"/>	LAG 1			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 2			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 3			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 4			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 5			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 6			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 7			Enabled	Down	Auto	Auto	Disabled
<input type="checkbox"/>	LAG 8			Enabled	Down	Auto	Auto	Disabled

Edit



### 5.3.3 LACP

LACP (Link Aggregation Control Protocol), basado en el estándar IEEE 802.3ad, agrega y desagrega dinámicamente los enlaces. Intercambia información con los dispositivos de red opuestos a través de LACPDU (Link Aggregation Control Protocol Data Unit).

Después de que un puerto utiliza LACP, informará al dispositivo de red opuesto de la prioridad del sistema, MAC del sistema, prioridad de puerto y No., y clave de operación mediante la transmisión de un LACPDU. El dispositivo opuesto comparará dicha información con la guardada por otros puertos después de recibirla, llegando así a un acuerdo sobre la participación del puerto o la salida de una agregación dinámica.

La agregación dinámica de LACP es creada o eliminada automáticamente por el sistema, es decir, los puertos internos se pueden agregar o eliminar por sí mismos. Solo se pueden agregar los puertos conectados a un mismo dispositivo con la misma velocidad, dúplex y configuración básica.

Instrucciones para agregar una agregación de enlaces dinámicos:

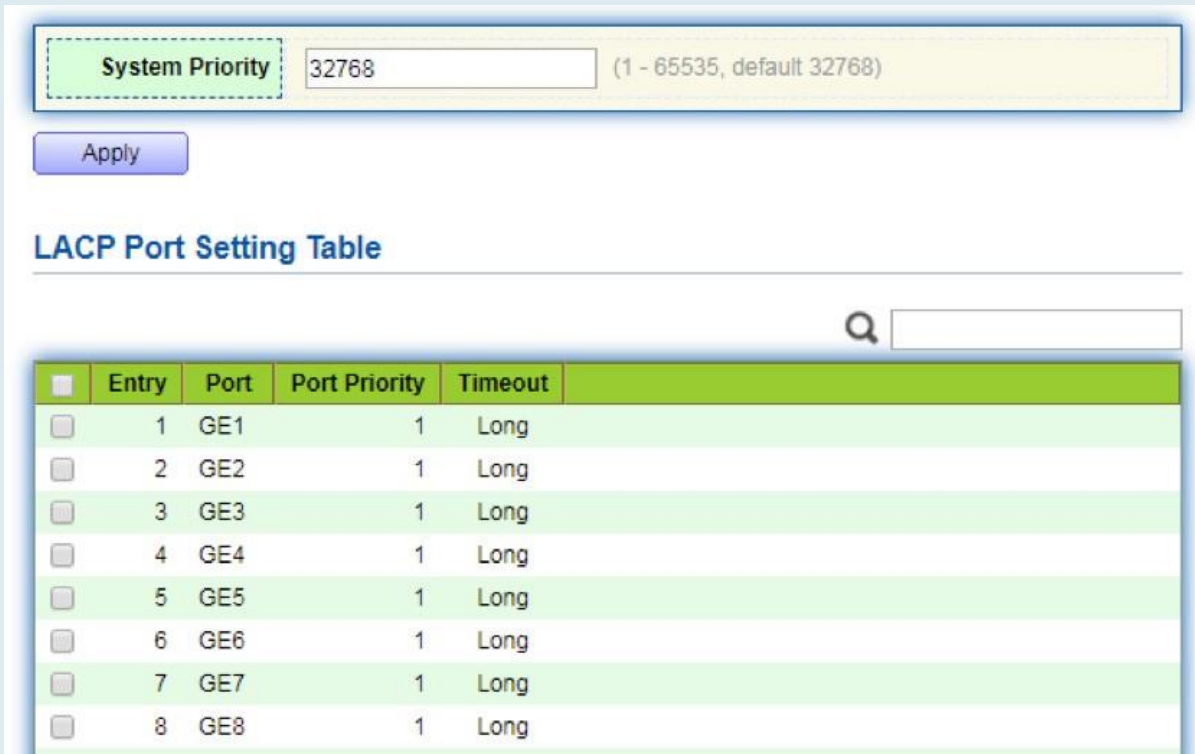
1. Haga clic en "Port > Link Aggregation > Group" en la barra de navegación, seleccione el LAG ID y el modo LACP, "Edite" de la siguiente manera:

**Edit Link Aggregation Group**

<b>LAG</b>	2	
<b>Name</b>	<input type="text"/>	
<b>Type</b>	<input type="radio"/> Static <input checked="" type="radio"/> LACP	
<b>Member</b>	Available Port GE1 GE2 GE3 GE7 GE8 GE9 GE10 GE11	Selected Port GE4 GE5 GE6

Apply Close

2. Haga clic en "Port >Link Aggregation > LACP" en la barra de navegación para configurar los atributos LACP, como la prioridad del sistema, la prioridad del puerto y el método de tiempo de espera de la siguiente manera:



**System Priority**  (1 - 65535, default 32768)

**LACP Port Setting Table**

Q

<input type="checkbox"/>	Entry	Port	Port Priority	Timeout
<input type="checkbox"/>	1	GE1	1	Long
<input type="checkbox"/>	2	GE2	1	Long
<input type="checkbox"/>	3	GE3	1	Long
<input type="checkbox"/>	4	GE4	1	Long
<input type="checkbox"/>	5	GE5	1	Long
<input type="checkbox"/>	6	GE6	1	Long
<input type="checkbox"/>	7	GE7	1	Long
<input type="checkbox"/>	8	GE8	1	Long

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
System Priority	LACP determina los modos activo y pasivo entre dos dispositivos sujetos al estándar de prioridad.
Port	Lista de puertos
Port Priority	LACP determina el modo de miembro dinámico del GAL sujeto a la prioridad del puerto con un sistema superior.
Timeout	Decide la frecuencia de transmisión de los mensajes LACP.

Descripción:

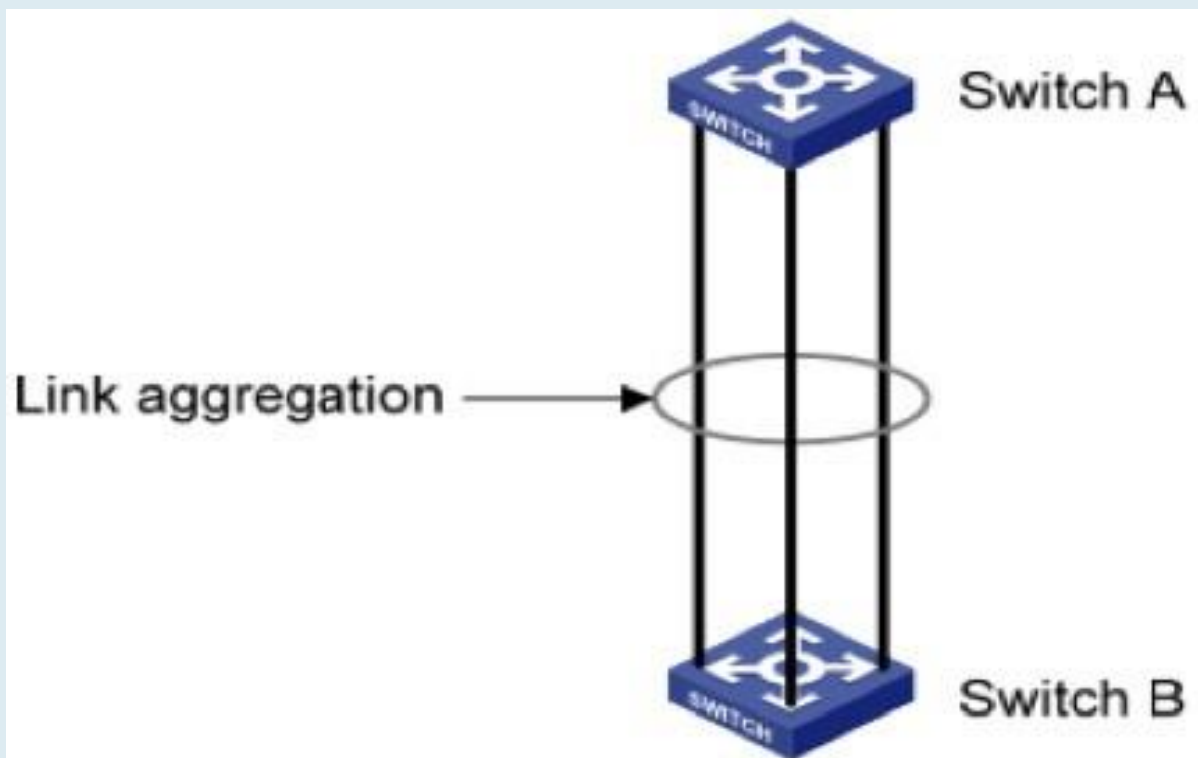
Asegúrese de que no haya ninguna interfaz de miembro que acceda al Eth-Trunk antes de cambiar su patrón de trabajo, de lo contrario falla.

El patrón de trabajo de los dispositivos de red local debe ser coherente con el de los dispositivos de red opuestos.

Ilustración

Ethernet Switch A agrega 3 puertos de GE1 a GE3 al conmutador B, para compartir la carga por cada puerto miembro.

Las siguientes configuraciones se ilustran mediante agregación dinámica.



Descripción:

La siguiente es la configuración del conmutador A solamente, que debe permanecer igual que la del conmutador B para la agregación de puertos.

Instrucciones:

1. Haga clic en "Port > Link Aggregation > Group" en la barra de navegación, "Editar" con LAG 2, seleccione GE1-GE3 en modo LACP. "Aplicar" y terminar de la siguiente manera:

**Edit Link Aggregation Group**

---

<b>LAG</b>	2	
<b>Name</b>	<input type="text"/>	
<b>Type</b>	<input type="radio"/> Static <input checked="" type="radio"/> LACP	
<b>Member</b>	Available Port GE4 GE5 GE6 GE7 GE8 GE9 GE10 GE11	Selected Port GE1 GE2 GE3

## 5.4 EEE

La alimentación del puerto se apagará en caso de flujo cero o menor.

Instrucciones:

1. Haga clic en "Port > EEE" en la barra de navegación, seleccione el puerto y "Editar" para ingresar a la interfaz de configuración de la siguiente manera:

**EEE Setting Table**

Q

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled
<input type="checkbox"/>	5	GE5	Disabled
<input type="checkbox"/>	6	GE6	Disabled
<input type="checkbox"/>	7	GE7	Disabled

**Edit EEE Setting**

Port GE1-GE2

State  Enable

Apply Close

2. Establezca la etiqueta de habilitación de puerto y "Aplicar" para completar la configuración de la siguiente manera:

**EEE Setting Table**

Q

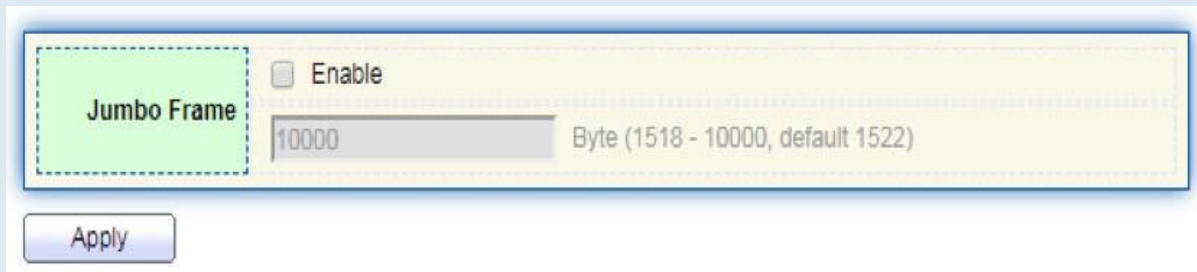
<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Enabled
<input type="checkbox"/>	2	GE2	Enabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled

## 5.5 Trama Jumbo

Configure la MTU (Unidad de transmisión máxima) del puerto.

Instrucciones:

1. Haga clic en "Port > Jumbo Frame" en la barra de navegación, ingrese a la interfaz de configuración de Jumbo Frame de la siguiente manera:



## 5.6 Seguridad portuaria

La función de seguridad del puerto registra la dirección MAC Ethernet conectada al puerto del conmutador a través de la tabla de direcciones MAC, y sólo una dirección MAC puede comunicarse a través de este puerto. Cuando los paquetes enviados por otras direcciones MAC pasan a través de este puerto, las características 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 características de seguridad de puertos también se pueden utilizar para evitar que la tabla de direcciones MAC se llene debido a la inundación de direcciones MAC Instrucciones:

1. Haga clic en "Port > Port Security" en la barrade navegación, ingrese a la interfaz de configuración de seguridad de puertos de la siguiente manera:



1. Haga clic en "Port > Port Security" en la barra de navegación, seleccione el puerto y "Editar" para ingresar a la interfaz de configuración de nivel de puerto de la siguiente manera:

### Port Security Table

<input type="checkbox"/>	Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
<input type="checkbox"/>	1	GE1	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	2	GE2	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	3	GE3	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	4	GE4	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	5	GE5	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	6	GE6	Disabled	1	0	0	0	Protect	Disabled
<input type="checkbox"/>	7	GE7	Disabled	1	0	0	0	Protect	Disabled

### Edit Port Security

<b>Port</b>	GE1-GE2
<b>State</b>	<input type="checkbox"/> Enable
<b>Address Limit</b>	<input type="text" value="1"/> (1 - 256, default 1)
<b>Violate Action</b>	<input checked="" type="radio"/> Protect <input type="radio"/> Restrict <input type="radio"/> Shutdown
<b>Sticky</b>	<input type="checkbox"/> Enable

## 5.7 Puerto protegido

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

Instrucciones:

1. Haga clic en "Puerto > puerto protegido" en la barra de navegación, marque los puertos que desea aislar, "Editar" para cambiar esta función de la siguiente manera:

## Protected Port Table



<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Unprotected
<input type="checkbox"/>	2	GE2	Unprotected
<input type="checkbox"/>	3	GE3	Unprotected
<input type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected
<input type="checkbox"/>	6	GE6	Unprotected
<input type="checkbox"/>	7	GE7	Unprotected

### Edit Protected Port

<b>Port</b>	GE1-GE4
<b>State</b>	<input checked="" type="checkbox"/> Protected

Instrucciones para lograr el aislamiento del puerto:

1. Haga clic en "Puerto > puerto protegido" en la barra de navegación, marque y "Edite" los GE1, 2 y 3 que desea aislar. "Aplicar" y terminar de la siguiente manera:

## Protected Port Table



<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Protected
<input type="checkbox"/>	2	GE2	Protected
<input type="checkbox"/>	3	GE3	Protected
<input type="checkbox"/>	4	GE4	Unprotected
<input type="checkbox"/>	5	GE5	Unprotected

2. GE1, 2 y 3 no se comunican mutuamente como otros puertos no aislados.

## 5.8 Control de tormentas

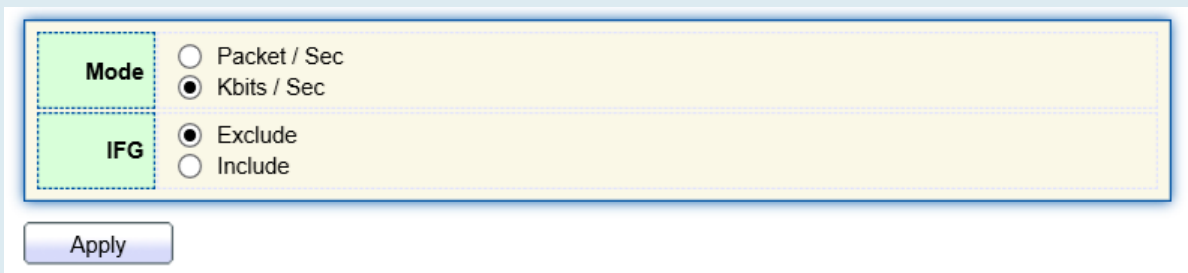
Las tormentas generadas a través de mensajes de transmisión, multidifusión desconocida y unidifusión se evitan de la siguiente manera. Estos mensajes se suprimirán sujetos a las tasas de paquetes respectivamente. La tasa media de los mensajes recibidos por las interfaces de supervisión se comparará con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

Cuando una interfaz Ethernet L2 recibe los 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, puede ocurrir una tormenta de transmisión para degradar el rendimiento de operación del dispositivo.

Tres tipos de flujo de mensajes pueden ser controlados por las características de la policía de tormentas para mantenerse alejado de las tormentas de transmisión.

Instrucciones:

1. Haga clic en "Port > Storm Control" en la barra de navegación para configurar los atributos relacionados con la vigilancia de tormentas, como el modo de la siguiente manera:



2. Seleccione el puerto apropiado y "Edite" configurando las tasas de vigilancia de las tormentas de transmisión, multidifusión desconocida y unidifusión en cada puerto.

**Port Setting Table**

Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action	
			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)		
<input type="checkbox"/>	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop



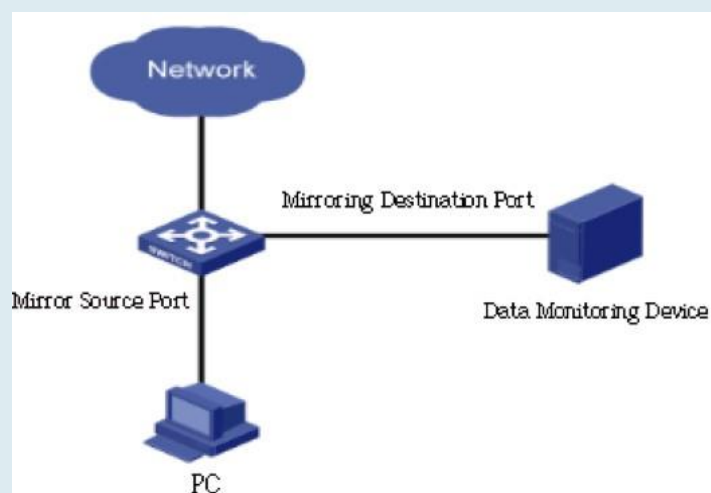
3. Configure información como Switch de tormenta y tasa, "Aplicar" y finalice de la siguiente manera:

**Port Setting Table**

Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
			State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
<input type="checkbox"/>	1	GE1	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	2	GE2	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	3	GE3	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	4	GE4	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	5	GE5	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	6	GE6	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	7	GE7	Disabled	10000	Disabled	10000	Disabled	10000	Drop
<input type="checkbox"/>	8	GE8	Disabled	10000	Disabled	10000	Disabled	10000	Drop

## 5.9 Espejado

La duplicación de puertos copia el mensaje de un puerto de conmutador especificado en el 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 supervisar 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 clic en "Port > Mirroring" en la barra de navegación. Se pueden configurar 4 conjuntos de reglas de duplicación de flujo de la siguiente manera:

## Mirroring Table

	Session ID	State	Monitor Port	Ingress Port	Egress Port
<input type="radio"/>	1	Disabled	---	---	---
<input type="radio"/>	2	Disabled	---	---	---
<input type="radio"/>	3	Disabled	---	---	---
<input type="radio"/>	4	Disabled	---	---	---

\*\*\* Allow the monitor port to send or receive normal packets

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

## Edit Mirroring

<b>Session ID</b>	1	
<b>State</b>	<input checked="" type="checkbox"/> Enable	
<b>Monitor Port</b>	GE1 <input type="button" value="v"/>	
	<input checked="" type="checkbox"/> Send or Receive Normal Packet	
<b>Ingress Port</b>	Available Port	Selected Port
	<div style="border: 1px solid #ccc; padding: 5px;">             GE1 GE5 GE6 GE7 GE8 GE9 GE10 GE11           </div>	<div style="border: 1px solid #ccc; padding: 5px;">             GE2 GE3 GE4           </div>
<b>Egress Port</b>	Available Port	Selected Port
	<div style="border: 1px solid #ccc; padding: 5px;">             GE1 GE5 GE6 GE7 GE8 GE9 GE10 GE11           </div>	<div style="border: 1px solid #ccc; padding: 5px;">             GE2 GE3 GE4           </div>

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Session ID	El conmutador tiene 4 ID de sesión de forma predeterminada.
State	El grupo de creación de reflejo se puede habilitar o no.
Monitor Port	Solo se puede seleccionar un puerto físico ordinario, excluyendo el puerto de agregación de vínculos y el puerto de origen.
Ingress Port	Cualquier mensaje recibido se reflejará en el puerto de destino.
Egress Port	Cualquier mensaje transmitido se reflejará en el puerto de destino.

# 6 Configuración de 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 red Cat-5 existente. Garantiza un cableado estructurado seguro y un funcionamiento normal de la red para minimizar el costo.

## 6.1 Configuración del puerto PoE

Instrucciones:

1. Haga clic en "Configuración de POE > Configuración de puerto POE" en la barra de navegación de la siguiente manera:

**System info**

System Power(mW)	0
System Temperature(C)	62
Refresh Rate	<input type="radio"/> None <input type="radio"/> 5 sec <input checked="" type="radio"/> 10 sec <input type="radio"/> 30 sec

**Port Setting Table**

Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)	WatchDog	
<input type="checkbox"/>	1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	2	GE2	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	3	GE3	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	5	GE5	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	6	GE6	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	7	GE7	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled
<input type="checkbox"/>	8	GE8	Enabled	Off	AF(U)	0	N/A	N/A	N/A	Disabled

2. Seleccione los puertos que desea configurar y "Editar" de la siguiente manera:

**Edit Port Setting**

Port	GE1-GE2
PortEnable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WatchDog	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

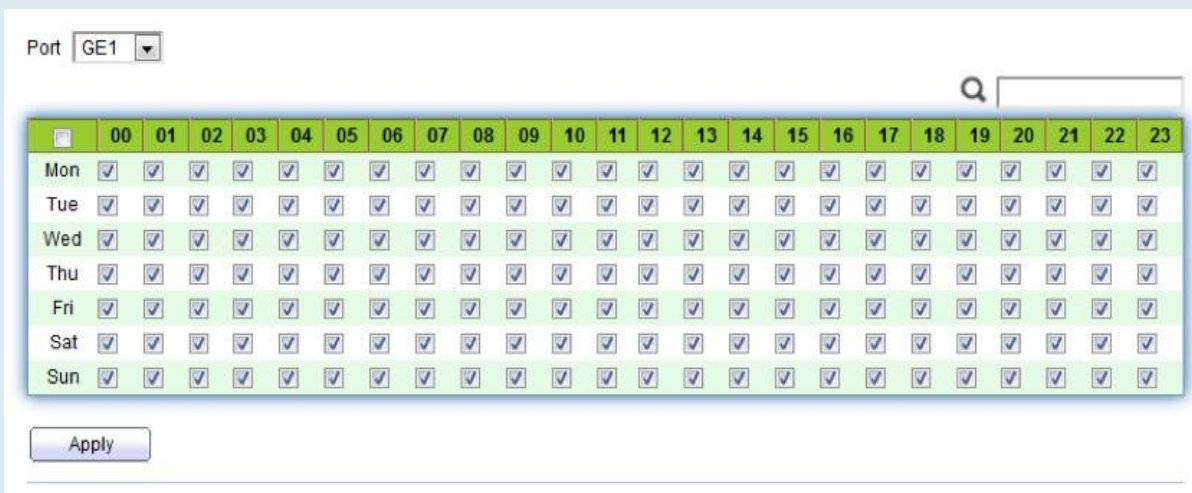
Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
PortEnable	Activar/desactivar la alimentación del puerto Poe
WatchDog	Activar/desactivar 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 total de detección es 5 veces

## 6.2 Configuración del temporizador de puerto POE

Instrucciones:

1. Haga clic en "Configuración de POE > Configuración del temporizador de puerto POE", seleccione el tiempo de suministro de energía de la programación de Poe. "Aplicar" y terminar de la siguiente manera



Port

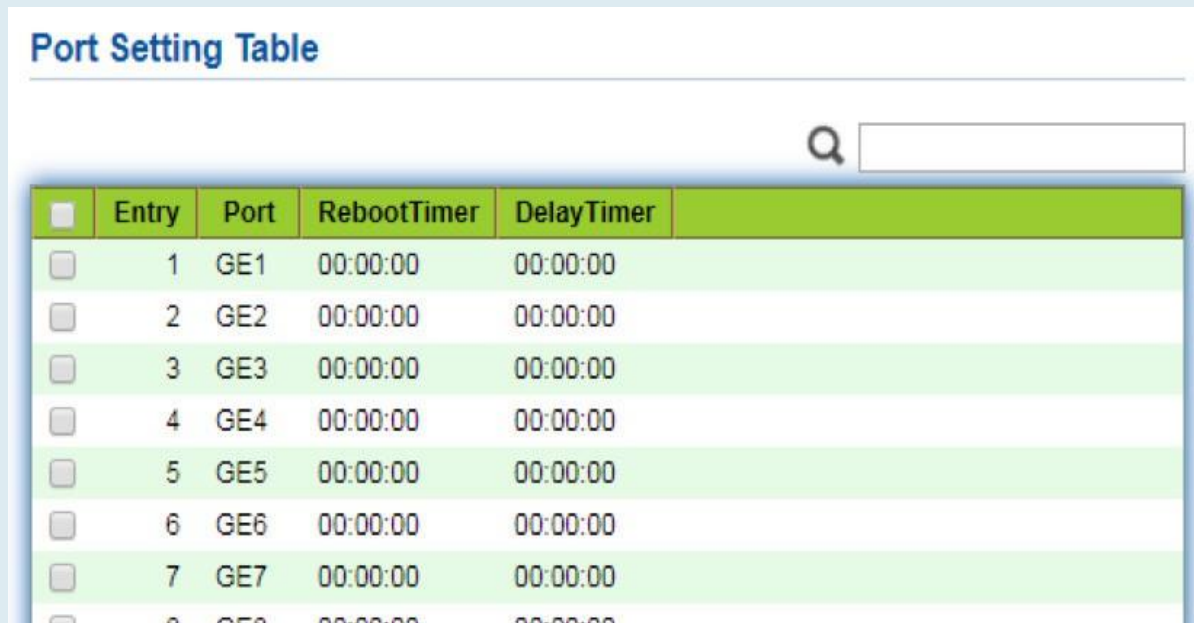
Q

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Thu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fri	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Sun	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## 6.3 Configuración de reinicio del temporizador de puerto POE

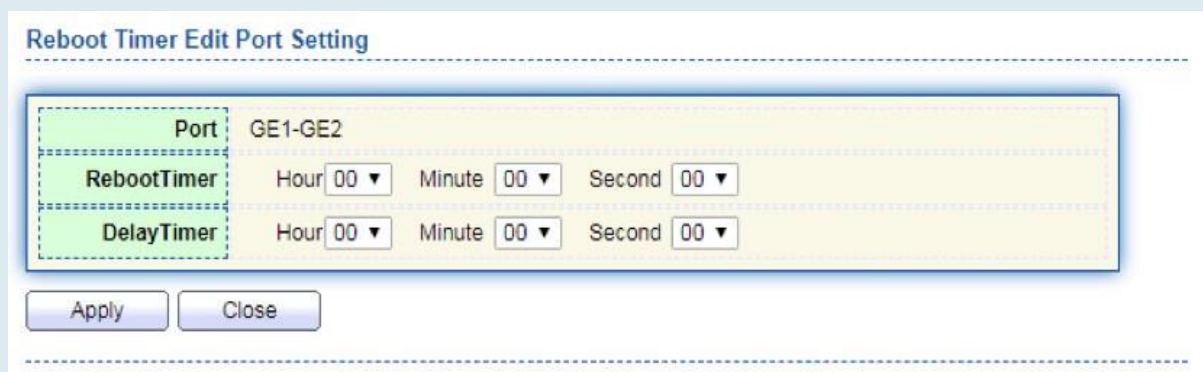
Al configurar, la fuente de alimentación se puede reiniciar periódicamente según el puerto.  
Instrucciones:

1. Haga clic en "Configuración de POE > Configuración de reinicio del temporizador de puerto POE" en la barra de navegación de la siguiente manera:



Entry	Port	RebootTimer	DelayTimer
1	GE1	00:00:00	00:00:00
2	GE2	00:00:00	00:00:00
3	GE3	00:00:00	00:00:00
4	GE4	00:00:00	00:00:00
5	GE5	00:00:00	00:00:00
6	GE6	00:00:00	00:00:00
7	GE7	00:00:00	00:00:00
8	GE8	00:00:00	00:00:00

2. Seleccione el puerto y "Editar" para entrar en la interfaz de configuración



Reboot Timer Edit Port Setting

Port: GE1-GE2

RebootTimer: Hour 00 Minute 00 Second 00

DelayTimer: Hour 00 Minute 00 Second 00

Apply Close

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Port	Lista de puertos
RebootTimer	Establezca 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 apagar la fuente de alimentación PoE en el momento del reinicio, el tiempo de retraso para reiniciar y encender la fuente de alimentación solo se puede establecer en minutos

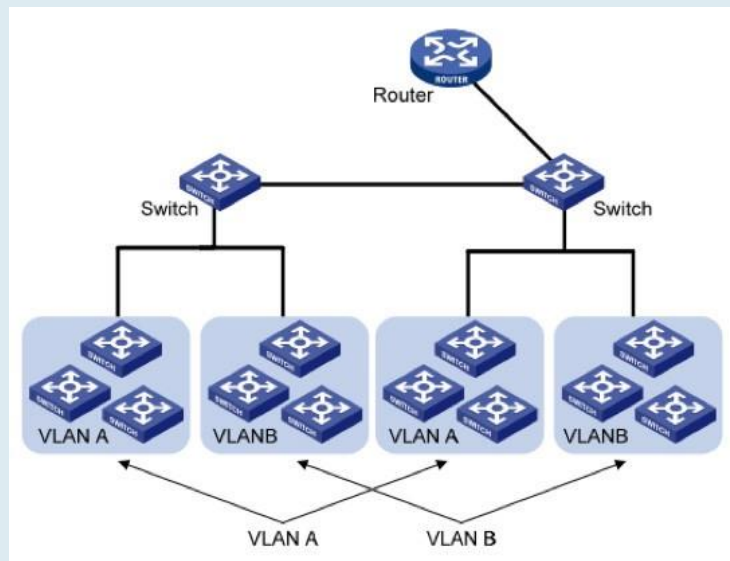


Nota:

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

# 7 VLAN

VLAN está formulado no restringido 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 mediante comunicación tradicional. Para los hosts en diferentes VLAN, el dispositivo como el enrutador o el conmutador L3 es imprescindible.



VLAN es superior a la Ethernet tradicional en términos de:

- Cobertura del 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 LAN: los hosts VLAN no se comunican entre sí ya que los mensajes están separados por el dominio de difusión 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 ámbito. Este switch de administración 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 del puerto es

sujeto dividido a la interfaz de un Switch No. El administrador de red le da a cada interfaz de switch 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 eliminará una etiqueta adicional, aunque la interfaz tenga un PVID.

- La solución para una trama VLAN depende del tipo de interfaz, lo que facilita la definición de miembros, pero reconfigura VLAN en caso de movilidad de miembros.

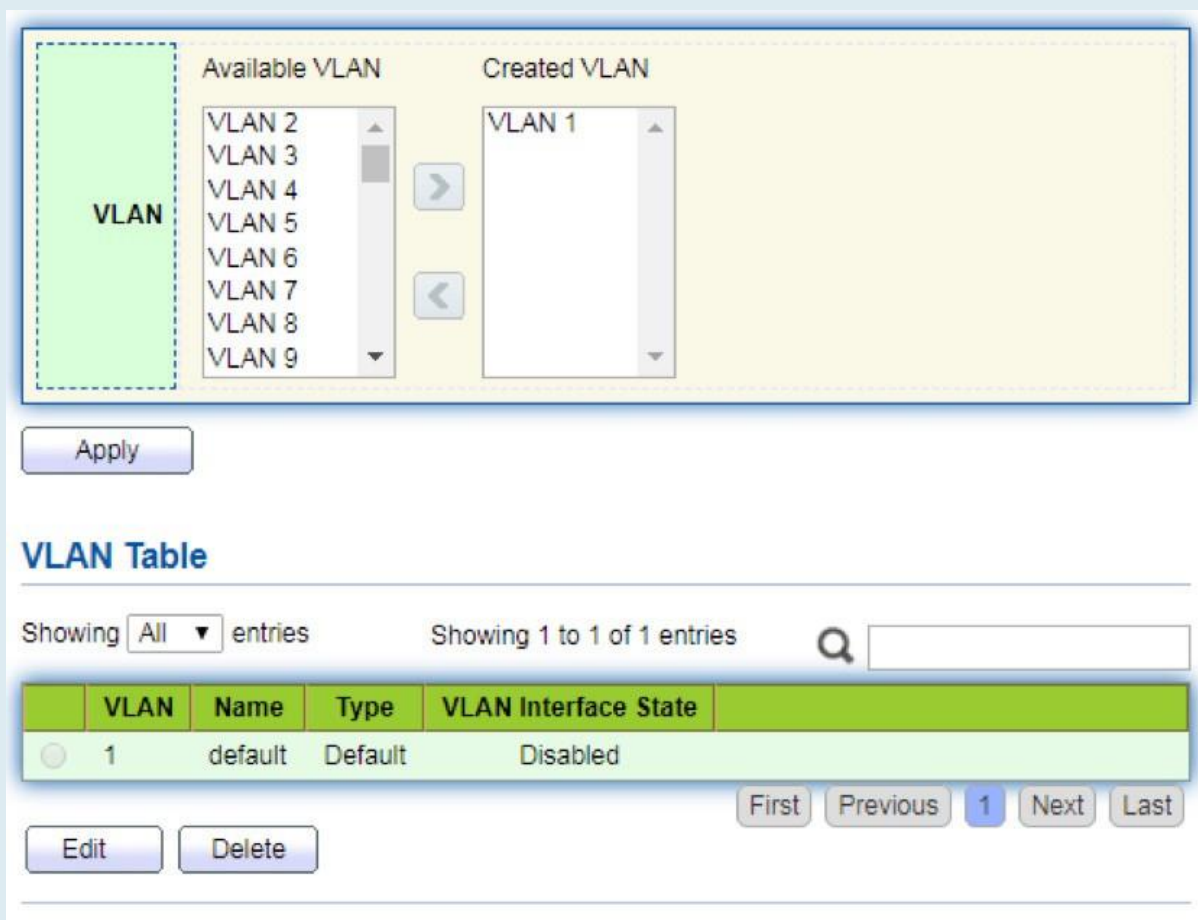


## 7.1 VLAN

### 7.1.1 Crear VALN

Instrucciones para crear una nueva VLAN:

1. Haga clic en "VLAN > VLAN > Crear VLAN" para seleccionar un nombre en el cuadro VLAN válido, muévelo al cuadro de creación de VLAN a la derecha (se pueden crear hasta 256 VLAN). "Aplicar" y terminar de la siguiente manera:



**VLAN**

Available VLAN

- VLAN 2
- VLAN 3
- VLAN 4
- VLAN 5
- VLAN 6
- VLAN 7
- VLAN 8
- VLAN 9

Created VLAN

- VLAN 1

Apply

**VLAN Table**

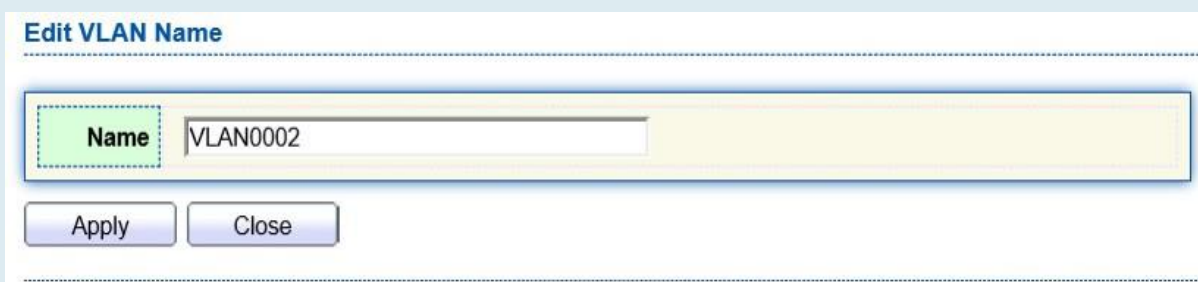
Showing All entries      Showing 1 to 1 of 1 entries

VLAN	Name	Type	VLAN Interface State
1	default	Default	Disabled

First Previous 1 Next Last

Edit Delete

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



**Edit VLAN Name**

Name: VLAN0002

Apply Close

Los datos de la interfaz son los siguientes

Elementos de configuración	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.

## 7.12 Configuración de VLAN

Hay dos métodos. Una es agregar múltiples puertos bajo una sola VLAN. La otra es agregar un puerto a múltiples VLAN. Se configuran de acuerdo con diferentes propósitos. Instrucciones para el primer método para agregar el puerto actual a una VLAN especificada

1. Haga clic en “VLAN > VLAN > VLAN Configuration” en la barra de navegación, seleccione el ID de VLAN en la parte superior izquierda y, a continuación, haga clic en la información del puerto de la siguiente manera:

**VLAN Configuration Table**

VLAN

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	GE2	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	GE3	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	GE4	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	GE5	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	GE6	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	GE7	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	GE8	Trunk	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
Port	Lista de puertos
Mode	Modo de puerto VLAN
Membership	Roles de miembro 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 no etiquetado de esta VLAN
PVID	Si esta VLAN es el PVID del puerto
Forbidden	Si el mensaje VLAN está prohibido reenviarse en este puerto

## 7.13 Membresía

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

1. Haga clic en "VLAN > VLAN > Membership" en la barra de navegación, seleccione el puerto a configurar y "Editar" para configurar sus atributos:

**Membership Table**

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
<input type="radio"/>	1	GE1	Trunk	1UP	1UP
<input type="radio"/>	2	GE2	Trunk	1UP	1UP
<input type="radio"/>	3	GE3	Trunk	1UP	1UP
<input type="radio"/>	4	GE4	Trunk	1UP	1UP
<input type="radio"/>	5	GE5	Trunk	1UP	1UP
<input type="radio"/>	6	GE6	Trunk	1UP	1UP
<input type="radio"/>	7	GE7	Trunk	1UP	1UP

**Edit Port Setting**

<b>Port</b>	GE2
<b>Mode</b>	Trunk
<b>Membership</b>	<div style="display: flex; align-items: center;"> <div style="border: 1px solid gray; padding: 2px; margin-right: 5px;">10</div> <div style="margin: 0 5px;">➤</div> <div style="border: 1px solid gray; padding: 2px;">         1UP 2T 3T 4T 5T 6T 7T 8T       </div> </div>
	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged <input type="checkbox"/> PVID

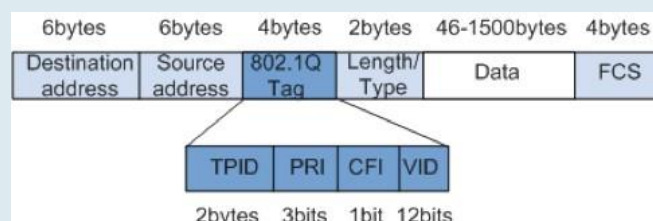
Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Puerto	Lista de puertos
Modo	Modo de puerto VLAN
Membresía	El puerto es el atributo de VLAN ID y VLAN: Prohibido: no reenviar el mensaje VLAN Excluido: el puerto que sale de la VLAN Etiquetado: El miembro etiquetado de la VLAN Untagged: El miembro sin etiquetar de la VLAN PVID: si la VLAN es el puerto PVLAN

## 7.1.4 Configuración del puerto

Configuración del tronco. Conectadas con otros switches, las interfaces troncales conectan principalmente enlaces troncales para permitir que las tramas VLAN fluyan a través. IEEE 802.1q es el protocolo de encapsulación del enlace troncal y considera el estándar formal para las redes de área local con puente virtual. Cambia el formato de trama de Ethernet agregando una etiqueta 802.1q de 4 bits entre el campo de dirección MAC de origen y el campo de protocolo.

Formato de fotografía 802.1q



### Significado de los campos de etiqueta 802.1q

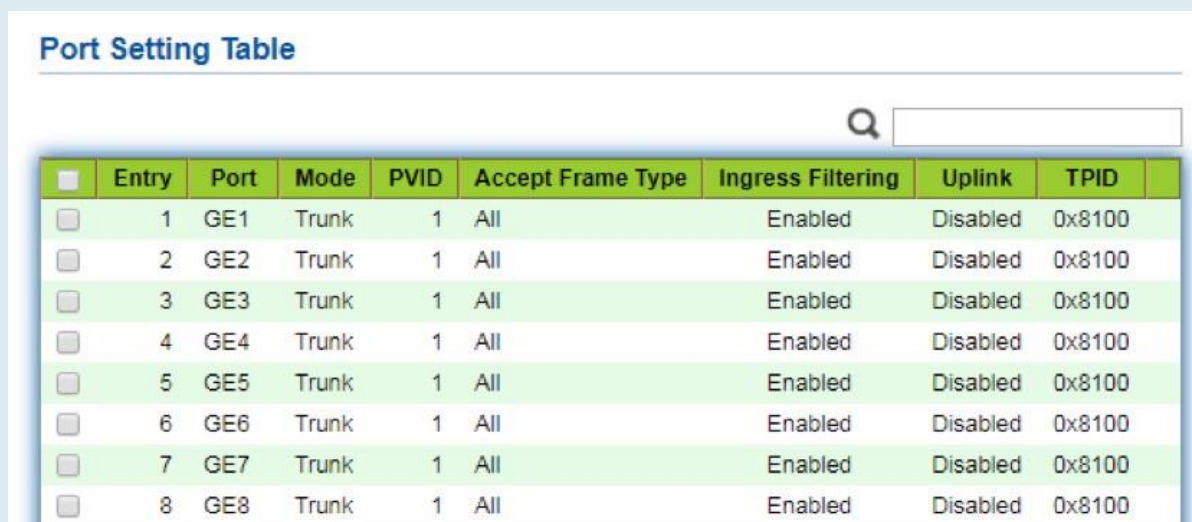
Campo	Largura	Nombre	Análisis
TPID	2 bytes	Tag Protocol Identifier to describe the frame type	Se refiere al marco de etiqueta 802.1q cuando el valor es 0x8100, que se descartará si el equipo relevante no lo recibe.
PRI	3 bits	Frame Priority	Varía de 0 a 7, con la prioridad más alta representada por un número mayor. El marco de datos con mayor prioridad se enviará preferentemente en caso de congestión del switch.
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.	Varía de 0 a 4.095, con 1 a 4.094 válidos ya que 0 y 4.095 son los valores de retención del protocolo.

Los paquetes enviados por cada switch que soporta el protocolo 802.1q contienen un ID de VLAN para indicar la VLAN a la que pertenece el switch. Por lo tanto, las tramas Ethernet se dividen en dos tipos de la siguiente manera en una red de conmutación VLAN:

- Marco etiquetado: se refiere al marco que agrega una etiqueta 802.1q de 4 bits.
- Marco sin etiquetar: se refiere al marco original sin una etiqueta 802.1q de 4 bits. Conectadas con otros switches, las interfaces troncales conectan principalmente enlaces troncales para permitir que las tramas VLAN fluyan a través.

Instrucciones para la configuración de la interfaz troncal:

1. Haga clic en "VLAN > VLAN > Port Setting" en la barra de navegación, seleccione el puerto y "Editarlo" para configurar los atributos:



Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
8	GE8	Trunk	1	All	Enabled	Disabled	0x8100

**Edit Port Setting**

<b>Port</b>	GE4-GE8
<b>Mode</b>	<input checked="" type="radio"/> Hybrid <input type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/> Tunnel
<b>PVID</b>	<input type="text" value="1"/> (1 - 4094)
<b>Accept Frame Type</b>	<input checked="" type="radio"/> All <input type="radio"/> Tag Only <input type="radio"/> Untag Only
<b>Ingress Filtering</b>	<input checked="" type="checkbox"/> Enable
<b>Uplink</b>	<input type="checkbox"/> Enable
<b>TPID</b>	<input type="text" value="v"/>

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Port	Puerto No. a configurar
Mode	Modo de puerto VLAN Híbrido: el puerto en este modo sirve como miembro de los puertos etiquetados y no etiquetados de VLAN Acceso: el puerto en este modo sirve como el único miembro de VLAN Trunk: 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
Port	VLAN nativa del puerto
Accept Frame Type	Tipos de mensajes recibidos por los puertos Todos: todos los mensajes Solo etiqueta: solo se recibirán los mensajes etiquetados Solo des etiquetar: solo se recibirán los mensajes sin etiquetar
Ingress Filtering	Un switch para decidir filtrar los mensajes VLAN excluidos en el puerto
Uplink	Ya sea en modo de enlace ascendente o no
TPID	N.º de identificación de etiqueta VLAN

## 7.2 VLAN de voz

Tradicionalmente, se aplicará ACL (Access Control List) para distinguir los datos de voz y se utilizará QoS (Quality of Service) para garantizar la calidad de la transmisión, mejorando así la prioridad. Con el fin de simplificar la configuración del usuario y facilitar la gestión del flujo de voz, surge la VLAN de voz. La interfaz habilitada juzga si es flujo de datos de voz o no de acuerdo con al 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 de la organización) 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, simplificando así la configuración del usuario y la gestión de datos de voz.

### OUI de VLAN de voz

OUI representa un campo de dirección MAC. Su dirección se puede calcular en función de la dirección MAC de 48 bits y el bit de máscara correspondiente. El número de bits de la dirección MAC de entrada y la OUI correspondiente está determinado por la longitud de todos los bits "1" de 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 entrada coinciden con los de OUI, la interfaz VLAN de voz habilitada identifica el flujo de datos y el dispositivo de entrada 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 en su 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 tienen una prioridad más alta que otros datos empresariales durante la transmisión para reducir el posible retraso y la pérdida de paquetes.

1. Haga clic en "VLAN > Voice VLAN > Property" en la barra de navegación de la siguiente manera.

<b>State</b>	<input type="checkbox"/> Enable
<b>VLAN</b>	None ▾
<b>CoS / 802.1p Remarking</b>	<input type="checkbox"/> Enable 6 ▾
<b>Aging Time</b>	1440 Min (30 - 65536, default 1440)

Apply

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
State	Compruebe y habilite la VLAN de voz
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
Accept Frame Type	Tiempo de envejecimiento de la tabla

### Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Voice Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Voice Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Voice Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Voice Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Voice Packet

### Edit Port Setting

<b>Port</b>	GE1
<b>State</b>	<input type="checkbox"/> Enable
<b>Mode</b>	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
<b>QoS Policy</b>	<input checked="" type="radio"/> Voice Packet <input type="radio"/> All

Apply
Close



Los datos de la interfaz son los siguientes

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

2. Haga clic en "VLAN > VLAN de voz > OUI de voz" en la barra de navegación para configurar el segmento de direcciones de OUI de VLAN de voz de la siguiente manera:

**Voice OUI Table**

Showing  entries      Showing 1 to 8 of 8 entries     

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:03:6B	Cisco
<input type="checkbox"/>	00:E0:75	Veritel
<input type="checkbox"/>	00:D0:1E	Pingtel
<input type="checkbox"/>	00:01:E3	Siemens
<input type="checkbox"/>	00:60:B9	NEC/Philips
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:09:6E	Avaya

**Add Voice OUI**

**OUI**  :  :

**Description**

3. Rellene los elementos de configuración correspondientes.
4. "Aplicar" y terminar de la siguiente manera.

### Voice OUI Table

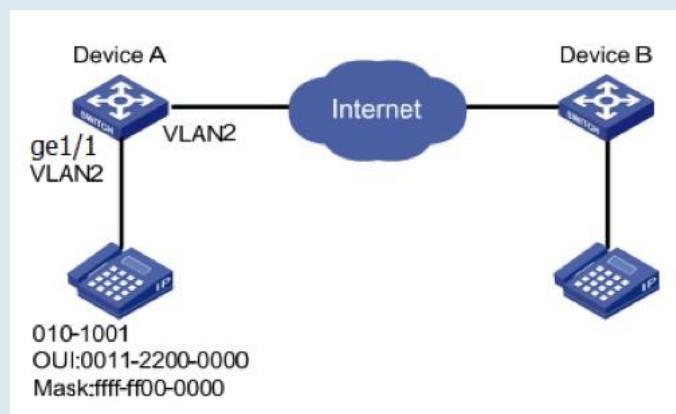
Showing  entries      Showing 1 to 9 of 9 entries     

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:03:6B	Cisco
<input type="checkbox"/>	00:E0:75	Veritel
<input type="checkbox"/>	00:D0:1E	Pingtel
<input type="checkbox"/>	00:01:E3	Siemens
<input type="checkbox"/>	00:60:B9	NEC/Philips
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:09:6E	Avaya
<input type="checkbox"/>	98:00:36	H7650

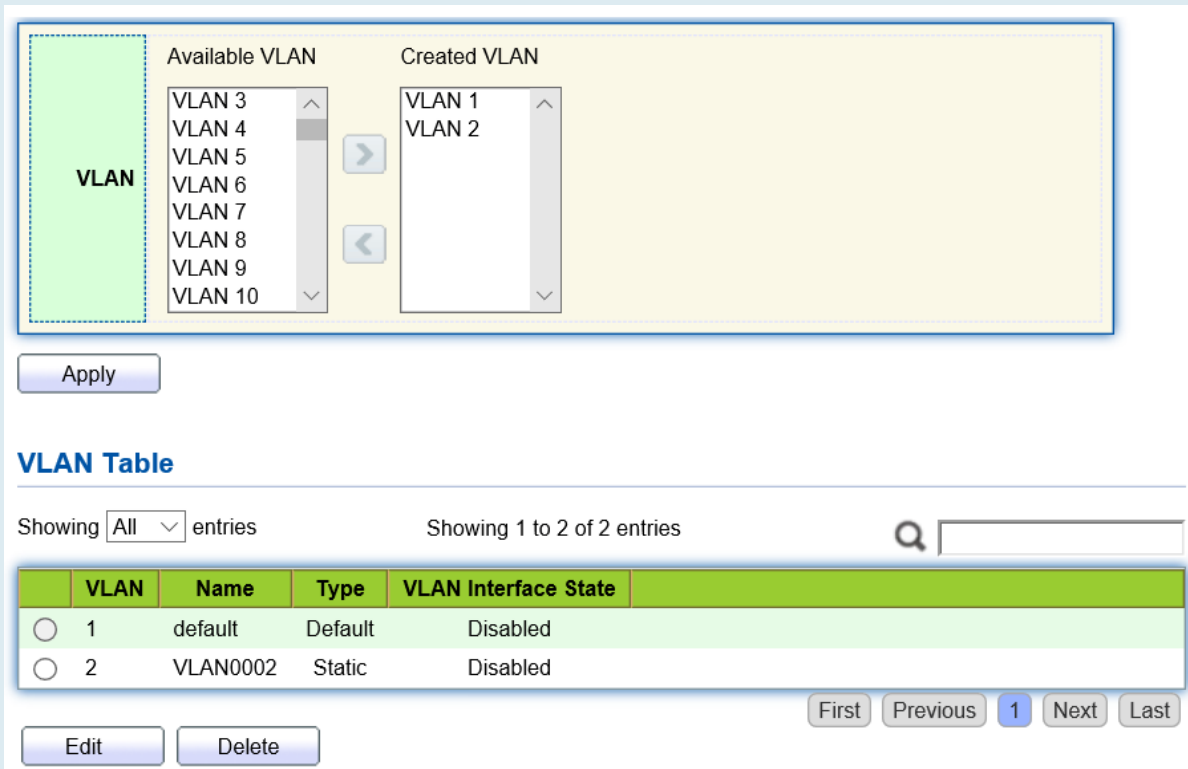
Por ejemplo, configure la VLAN de voz en modo manual para que los puertos que acceden a la telefonía IP puedan ingresar/salir de la VLAN de voz y transmitir el flujo de voz dentro de ella. Cree VLAN2 para operar VLAN de voz de forma segura, lo que permite que solo fluyan los datos de voz.

La telefonía IP transmite el flujo de voz sin etiquetar a GE1, el puerto troncal de entrada. Los usuarios deben personalizar una OUI (0011-2231-05e1) y configurar el diagrama de red VLAN de voz en modo automático.



Instrucciones:

1. Cree una VLAN para reconocer las VLAN a las que pertenecen los empleados. Haga clic en "VLAN > VLAN > Crear VLAN" en la barra de navegación para agregar VLAN 2 a la lista VLAN de la derecha. "Aplicar" y finalizar:



**VLAN**

Available VLAN

- VLAN 3
- VLAN 4
- VLAN 5
- VLAN 6
- VLAN 7
- VLAN 8
- VLAN 9
- VLAN 10

Created VLAN

- VLAN 1
- VLAN 2

Apply

**VLAN Table**

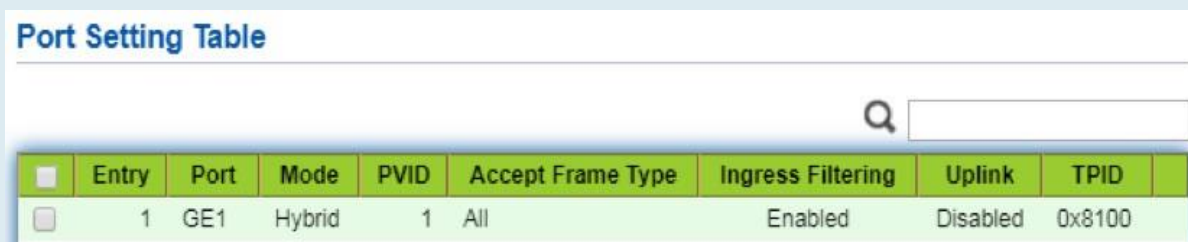
Showing All entries      Showing 1 to 2 of 2 entries

VLAN	Name	Type	VLAN Interface State
<input type="radio"/> 1	default	Default	Disabled
<input type="radio"/> 2	VLAN0002	Static	Disabled

First Previous 1 Next Last

Edit Delete

2. Configure la interfaz Ethernet GE1 del conmutador A en modo híbrido. Haga clic en "VLAN > VLAN > Port Setting" en la barra de navegación, "Edit" GE1 en modo híbrido:



**Port Setting Table**

Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	GE1	Hybrid	1	All	Enabled	Disabled	0x8100

3. Haga clic en "VLAN > Voice VLAN > Voice OUI" en la barra de navegación para configurar y agregar el rango de dirección MAC 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:

**Voice OUI Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	00:11:22	aaa

4. Habilite la VLAN de voz del puerto GE1. Haga clic en "VLAN > Voice VLAN > Property" en la barra 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:

<b>State</b>	<input checked="" type="checkbox"/> Enable
<b>VLAN</b>	<input type="text" value="VLAN0002"/>
<b>CoS / 802.1p Remarking</b>	<input type="checkbox"/> Enable <input type="text" value="6"/>
<b>Aging Time</b>	<input type="text" value="1440"/> Min (30 - 65536, default 1440)

**Port Setting Table**

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Enabled	Auto	Voice Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Voice Packet

Nota:

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

## 7.3 VLAN de protocolo

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

Los administradores deben preparar el esquema de asignación entre el dominio de protocolo de la trama Ethernet y el ID de VLAN, que se agregará si se reciben tramas sin etiquetar.

Fortaleza: Este método de división mejorará la gestión y el mantenimiento al vincular los servicios netos 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 lleva a una velocidad más baja debido a la gran cantidad de recursos consumidos.

Instrucciones:

1. Haga clic en "VLAN > Protocol VLAN > Protocol Group" en la barra de navegación de la siguiente manera:

**Protocol Group Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	Group ID	Frame Type	Protocol Value
<input type="checkbox"/>	1	Ethernet_II	0x8888

**Add Protocol Group**

0x  (0x600 ~ 0xFFFFE)

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Group ID	Grupo VLAN de protocolo
Frame Type	Tipos de marcos: Ether2, LLC, RFC 1042
Protocol Value	Va de 0x600 a 0xFFFFE

2. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

**Protocol Group Table**

Showing  entries      Showing 1 to 2 of 2 entries     

<input type="checkbox"/>	Group ID	Frame Type	Protocol Value
<input type="checkbox"/>	1	Ethernet_II	0x8888
<input type="checkbox"/>	2	RFC_1042	0x8889

4. Haga clic en "VLAN > Protocol VLAN > Group Binding" en la barra de navegación para enlazar el protocolo No., puerto No. y VLAN ID, para que la configuración surta efecto de la siguiente manera:

**Group Binding Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	Port	Group ID	VLAN
<input type="checkbox"/>	GE1	1	10

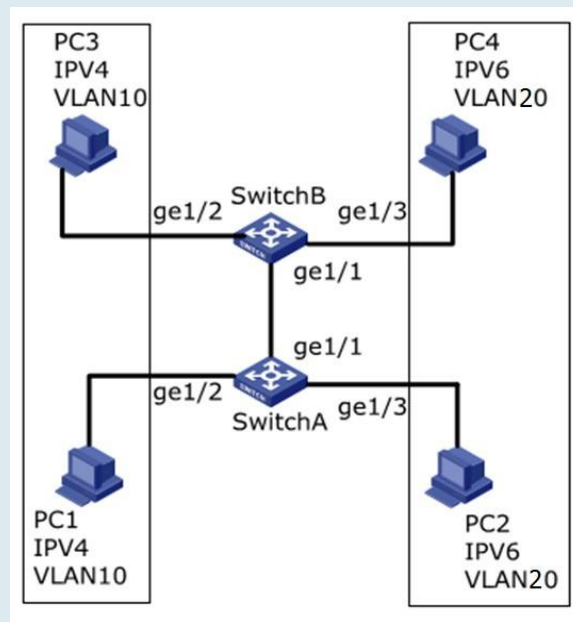
          
                

Descripción:

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 > Create VLAN", agregue VLAN10 y 20 a la lista de creación de VLAN a la derecha, "Aplicar" y finalice:

VLAN

Available VLAN

- VLAN 2
- VLAN 3
- VLAN 4
- VLAN 5
- VLAN 6
- VLAN 7
- VLAN 8
- VLAN 9

Created VLAN

- VLAN 1
- VLAN 10
- VLAN 20

### VLAN Table

Showing All entries Showing 1 to 3 of 3 entries

VLAN	Name	Type	VLAN Interface State
<input type="radio"/> 1	default	Default	Disabled
<input type="radio"/> 10	VLAN0010	Static	Disabled
<input type="radio"/> 20	VLAN0020	Static	Disabled

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

### Port Setting Table

<input type="checkbox"/>	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
<input type="checkbox"/>	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	2	GE2	Hybrid	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	3	GE3	Hybrid	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100

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:

### VLAN Configuration Table

VLAN

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
2	GE2	Hybrid	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
3	GE3	Hybrid	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

### VLAN Configuration Table

VLAN

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
2	GE2	Hybrid	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
3	GE3	Hybrid	<input type="radio"/> Excluded	<input type="radio"/> Tagged	<input checked="" type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>
4	GE4	Trunk	<input checked="" type="radio"/> Excluded	<input type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

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 en la lista para seleccionar VLAN10 y el miembro etiquetado de GE1. Configure VLAN20 de manera similar.



### VLAN Configuration Table

VLAN

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input type="radio"/> Excluded	<input checked="" type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

### VLAN Configuration Table

VLAN

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	<input type="radio"/> Excluded	<input checked="" type="radio"/> Tagged	<input type="radio"/> Untagged	<input type="checkbox"/>	<input type="checkbox"/>

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 la barra de navegación para agregar 2 reglas para las listas de Protocol Groups:

### Protocol Group Table

Showing  entries

Showing 1 to 2 of 2 entries

<input type="checkbox"/>	Group ID	Frame Type	Protocol Value
<input type="checkbox"/>	1	Ethernet_II	0x0800
<input type="checkbox"/>	2	Ethernet_II	0x86DD

7. Puerto, 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:

### Group Binding Table

Showing  entries

Showing 1 to 2 of 2 entries

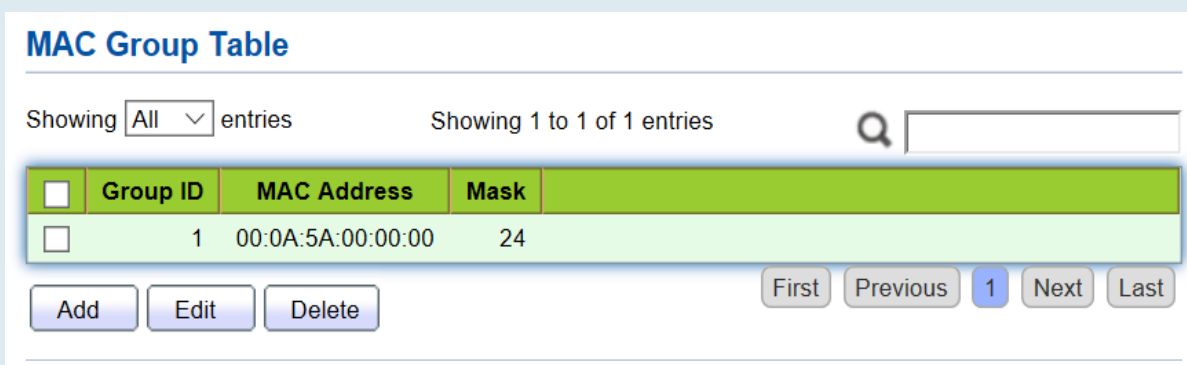
<input type="checkbox"/>	Port	Group ID	VLAN
<input type="checkbox"/>	GE2	1	10
<input type="checkbox"/>	GE3	2	20

## 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 la VLAN cuando cambia la ubicación 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 por adelantado. Instrucciones:

1. Haga clic en "VLAN > MAC VLAN > MAC Group" en la barra de navegación y "Agregar" un nuevo grupo MAC de la siguiente manera:

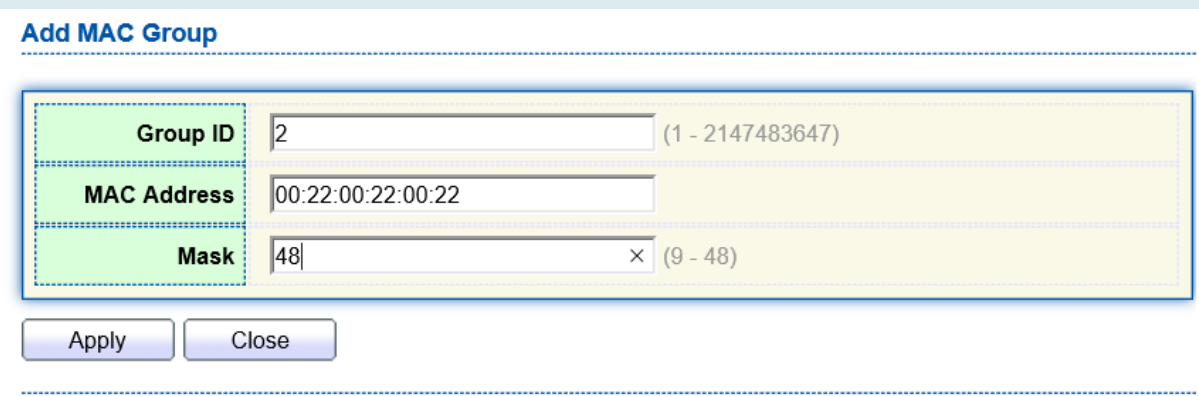


**MAC Group Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	Group ID	MAC Address	Mask
<input type="checkbox"/>	1	00:0A:5A:00:00:00	24



**Add MAC Group**

**Group ID**  (1 - 2147483647)

**MAC Address**

**Mask**  × (9 - 48)

Los datos de la interfaz son los siguientes

Elementos de configuración	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 del conmutador A y el conmutador, mientras que otros 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 la instancia de 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 la barra de navegación, agregue VLAN10 a la lista de creación de VLAN a la derecha, "Aplicar" y finalice de la siguiente manera:

**VLAN Table**

Showing  entries      Showing 1 to 3 of 3 entries     

<input type="radio"/>	VLAN	Name	Type	VLAN Interface State
<input type="radio"/>	1	default	Default	Disabled
<input type="radio"/>	10	VLAN0010	Static	Disabled
<input type="radio"/>	100	VLAN0100	Static	Disabled

2. Configure el GE1 del switch en modo híbrido con PVID de 100 para que actúe como miembro no etiquetado de VLAN10. Configure GE2 en modo troncal para que actúe como miembro etiquetado de VLAN10.

**Port Setting Table**

<input type="checkbox"/>	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
<input type="checkbox"/>	1	GE1	Hybrid	100	All	Enabled	Disabled	0x8100
<input type="checkbox"/>	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100

### Membership Table

Q

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
<input type="radio"/>	1	GE1	Hybrid	1U, 10U, 100P	1U, 10U, 100P
<input type="radio"/>	2	GE2	Trunk	1UP, 10T	1UP, 10T
<input type="radio"/>	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 > grupo MAC" en la barra 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  entries      Showing 1 to 3 of 3 entries      Q

<input type="checkbox"/>	Group ID	MAC Address	Mask
<input type="checkbox"/>	1	00:22:00:22:00:22	48
<input type="checkbox"/>	2	00:33:00:33:00:33	48
<input type="checkbox"/>	3	00:44:00:44:00:44	48

4. Haga clic en "VLAN > MAC VLAN > Group Binding" en la barra de navegación, "Add" para seleccionar el puerto híbrido solamente, el ID de grupo MAC que se enlazará y el ID de VLAN especificado. "Aplicar" y finalizar:

### MAC Group Table

Showing  entries      Showing 1 to 3 of 3 entries      Q

<input type="checkbox"/>	Group ID	MAC Address	Mask
<input type="checkbox"/>	1	00:22:00:22:00:22	48
<input type="checkbox"/>	2	00:33:00:33:00:33	48
<input type="checkbox"/>	3	00:44:00:44:00:44	48

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 alto que los paquetes ordinarios Instrucciones:

1. Haga clic en "VLAN > Surveillance VLAN > Property" en la barra de navegación de la siguiente manera.

<b>State</b>	<input type="checkbox"/> Enable
<b>VLAN</b>	None <input type="text"/>
<b>CoS / 802.1p Remarking</b>	<input type="checkbox"/> Enable 6 <input type="text"/>
<b>Aging Time</b>	1440 <input type="text"/> Min (30 - 65536, default 1440)

Elementos de configuración	Descripción
Estado	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

### Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Mode	QoS Policy
<input type="checkbox"/>	1	GE1	Disabled	Auto	Video Packet
<input type="checkbox"/>	2	GE2	Disabled	Auto	Video Packet
<input type="checkbox"/>	3	GE3	Disabled	Auto	Video Packet
<input type="checkbox"/>	4	GE4	Disabled	Auto	Video Packet
<input type="checkbox"/>	5	GE5	Disabled	Auto	Video Packet
<input type="checkbox"/>	6	GE6	Disabled	Auto	Video Packet
<input type="checkbox"/>	7	GE7	Disabled	Auto	Video Packet

### Edit Port Setting

Port	GE1-GE2
State	<input type="checkbox"/> Enable
Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
QoS Policy	<input checked="" type="radio"/> Video Packet <input type="radio"/> All

Apply Close

Los datos de la interfaz son los siguientes

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	Compruebe y habilite la VLAN de vigilancia

2. Haga clic en "VLAN > VLAN de vigilancia > OUI de vigilancia" en la barra de navegación para configurar el segmento de direcciones de OUI de VLAN de vigilancia de la siguiente manera:

### Surveillance OUI Table

Showing All entries Showing 0 to 0 of 0 entries

OUI	Description
0 results found.	

First Previous 1 Next Last

Add Edit Delete

### Add Voice OUI

OUI	<input type="text"/> : <input type="text"/> : <input type="text"/>
Description	<input type="text"/>

Apply Close

3. Rellene los elementos de configuración correspondientes.
4. "Aplicar" y terminar de la siguiente manera.

### Surveillance OUI Table

Showing All entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	OUI	Description
<input type="checkbox"/>	98:00:36	H7650

First Previous 1 Next Last

Add Edit Delete

## 7.6 GVRP

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

Los switches GVRP pueden intercambiar configuraciones VLAN en información entre sí, cortar la difusión innecesaria y el tráfico de unidifusión desconocido, y crear y administrar VLAN dinámicamente en los switches conectados a través del troncal 802.1Q.


GID y GIP se utilizan en GVRP, que proporcionan la descripción del mecanismo de estado general y el mecanismo de difusión de información para aplicaciones basadas en GRP, 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 switch. La información de actualización de GVRP y el temporizador se pueden cambiar. Los puertos GVRP tienen una variedad de modos de funcionamiento para controlar cómo adaptan las VLAN. GVRP puede agregar y administrar dinámicamente VLAN para la base de datos VLAN

GVRP admite la propagación de información VLAN entre dispositivos. En GVRP, la información de VLAN de un switch se puede configurar manualmente, y todos los demás switches 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. Se puede configurar una NIC compatible con GVRP para unirse a la VLAN necesaria y, a continuación, acceder a un conmutador habilitado para GVRP. Se establece la conexión de comunicación entre la NIC y el switch, y la conectividad VLAN se realiza entre la NIC y el switch.

## 7.6.1 Propiedad

Instrucciones de configuración global y de puertos:

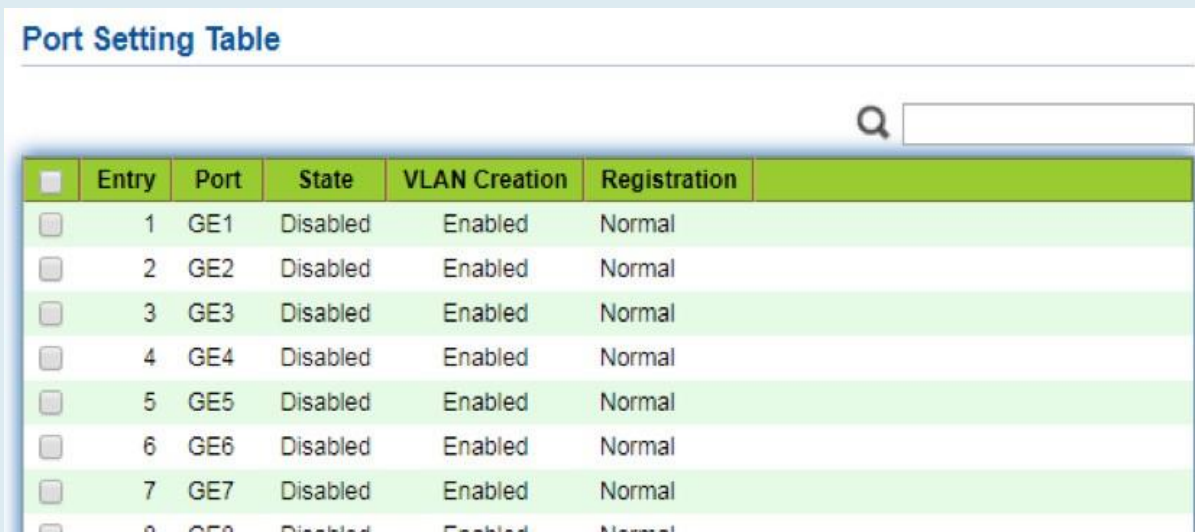
1. Haga clic en " VLAN > GVRP > Property" en la barra de navegación de la siguiente manera.



Los datos de la interfaz son los siguientes

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

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



	Entry	Port	State	VLAN Creation	Registration
<input type="checkbox"/>	1	GE1	Disabled	Enabled	Normal
<input type="checkbox"/>	2	GE2	Disabled	Enabled	Normal
<input type="checkbox"/>	3	GE3	Disabled	Enabled	Normal
<input type="checkbox"/>	4	GE4	Disabled	Enabled	Normal
<input type="checkbox"/>	5	GE5	Disabled	Enabled	Normal
<input type="checkbox"/>	6	GE6	Disabled	Enabled	Normal
<input type="checkbox"/>	7	GE7	Disabled	Enabled	Normal
<input type="checkbox"/>	8	GE8	Disabled	Enabled	Normal



**Edit Port Setting**

---

<b>Port</b>	GE1-GE2
<b>State</b>	<input type="checkbox"/> Enable
<b>VLAN Creation</b>	<input checked="" type="checkbox"/> Enable
<b>Registration</b>	<input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden

Apply    Close

---

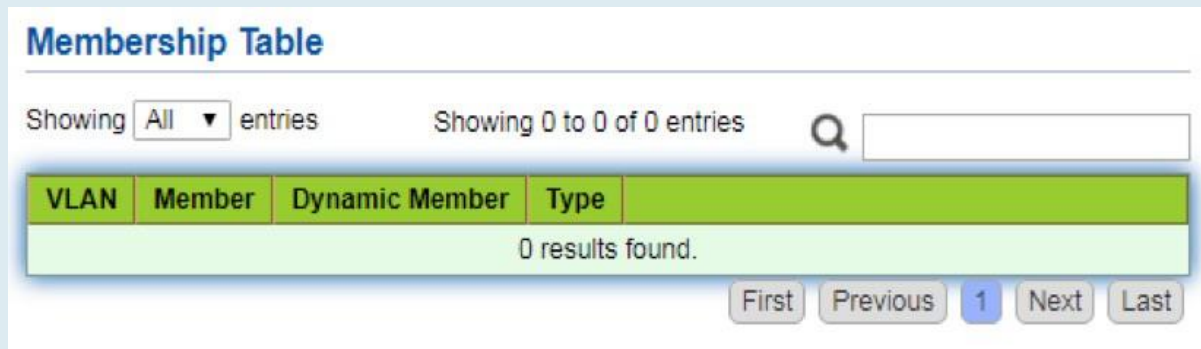
Los datos de la interfaz son los siguientes

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

## 7.6.2 Membresía

Ver información dinámica de miembros de GVRP Instrucciones:

1. Haga clic en " VLAN > GVRP > Membership" en la barra de navegación de la siguiente manera.



**Membership Table**

Showing  entries      Showing 0 to 0 of 0 entries     

VLAN	Member	Dynamic Member	Type
0 results found.			

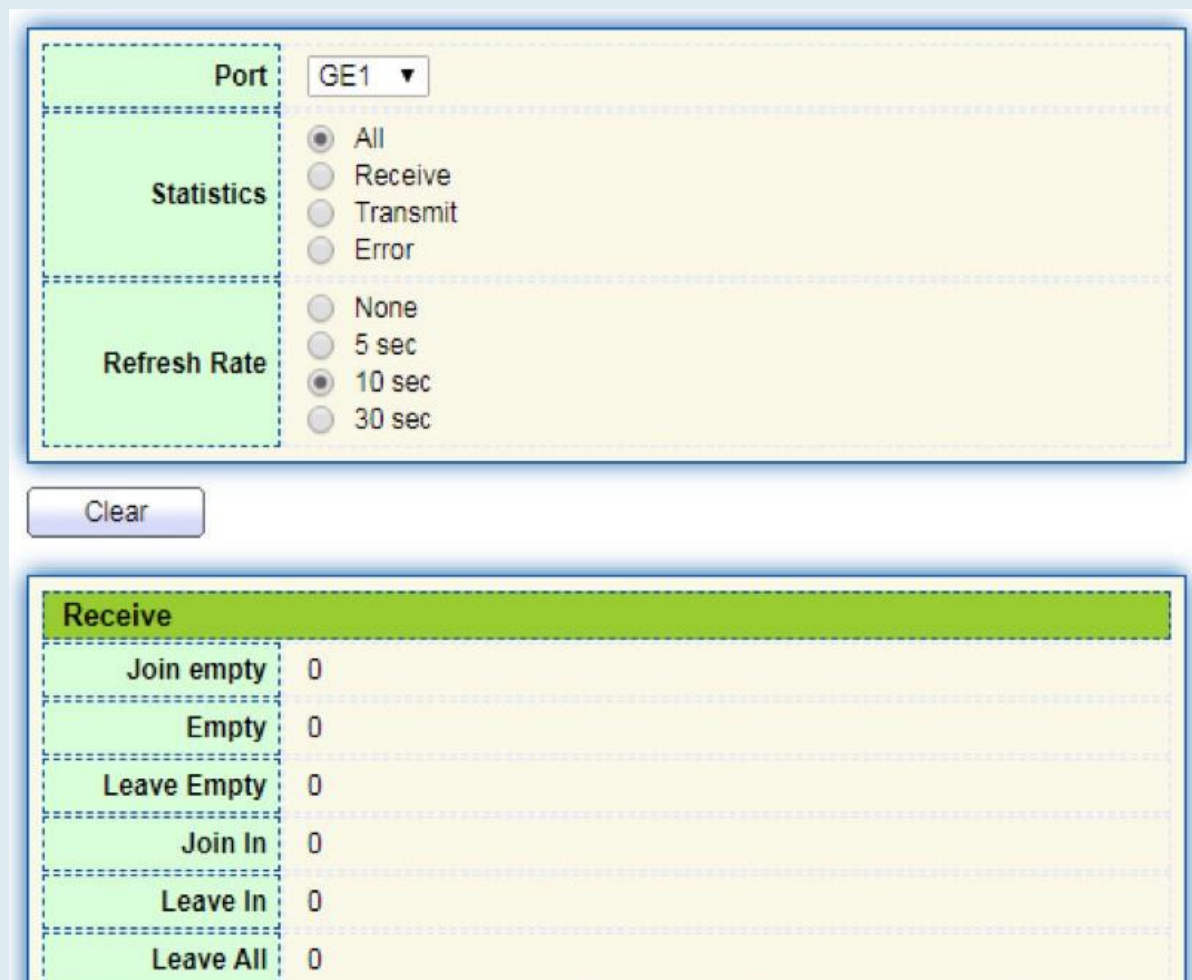
First Previous **1** Next Last

## 7.6.3 Estadística

Ver estadísticas de mensajes GVRP de puerto Instrucciones:

1. Haga clic en "VLAN > GVRP > Statistics" en la barra de navegación de la siguiente manera.

72



**Port**

**Statistics**

- All
- Receive
- Transmit
- Error

**Refresh Rate**

- None
- 5 sec
- 10 sec
- 30 sec

Receive	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0

# 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 de acuerdo con 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 que pertenece al puerto
- Reenvío de entrada No. de este dispositivo

Hay dos tipos de mensajes según la información de la tabla de direcciones MAC:

- Modo de unidifusión: el conmutador transmite directamente los mensajes de la salida de la tabla cuando la tabla de reenvío de direcciones MAC contiene las 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 MAC en la tabla de reenvío, el switch reenviará los mensajes a todos los puertos excluyendo el puerto de recepción de esta manera.

## 8.1 Dirección dinámica

El tiempo de caducidad y la información de la tabla de las direcciones MAC se pueden configurar y verificar en este [página](#).

La tabla de direcciones MAC necesita actualizaciones constantes para atender los cambios de red. Eso

Genera automáticamente entradas que están limitadas a su vida útil (es decir, el tiempo de envejecimiento). Aquellas entradas que no se actualicen después de la expiración se eliminarán. El tiempo de caducidad de una entrada se volverá a calcular si su registro se actualiza antes de su vencimiento.

El tiempo de envejecimiento adecuado ayuda a lograr el objetivo de envejecimiento de la dirección MAC. La escasez de tiempo de envejecimiento puede llevar a muchos switches de difusión a descubrir los paquetes de direcciones MAC de destino, influyendo así en el rendimiento del switch.

Envejecer demasiado puede hacer que el conmutador no 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 de red.

El conmutador puede eliminar entradas válidas de la tabla de direcciones MAC debido a un tiempo de envejecimiento demasiado corto, lo que reduce la eficiencia del reenvío. En general, el tiempo de envejecimiento recomendado es de 300 segundos por defecto.

Instrucciones para la configuración del tiempo de envejecimiento:

1. Haga clic en la "Tabla de direcciones MAC > dirección dinámica" en la barra de navegación de la interfaz de configuración y vista:

**Aging Time**

Sec (10 - 630, default 300)

### Dynamic Address Table

Showing 10 entries
Showing 1 to 10 of 65 entries

<input type="checkbox"/>	VLAN	MAC Address	Port
<input type="checkbox"/>	1	00:0B:0E:0F:00:ED	GE3
<input type="checkbox"/>	1	00:CF:E0:52:B0:4F	GE3
<input type="checkbox"/>	1	00:CF:E0:52:B0:8B	GE3
<input type="checkbox"/>	1	00:E0:4C:00:53:35	GE3
<input type="checkbox"/>	1	00:E0:4C:2E:2C:B3	GE3
<input type="checkbox"/>	1	00:E0:4C:2E:2C:DD	GE7
<input type="checkbox"/>	1	00:E0:4C:2E:2D:4C	GE3
<input type="checkbox"/>	1	00:E0:4C:93:C3:00	GE3
<input type="checkbox"/>	1	00:E0:4D:36:99:E4	GE3
<input type="checkbox"/>	1	00:E0:66:70:A6:CB	GE3

1
2
3
4
5

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
MAC Aging Time	Introduzca el tiempo de caducidad de la dirección MAC

2. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

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 el número de VLAN. tabla de consulta de tramas Ethernet.

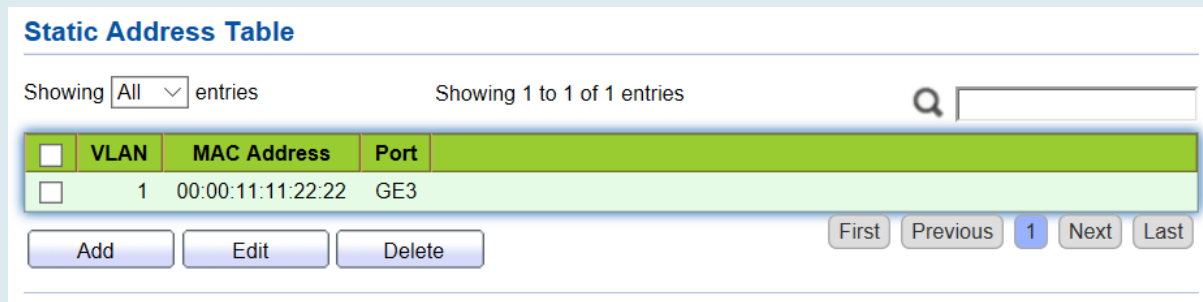
Para ver la tabla de direcciones MAC, consulte la Sección 3.3 del Capítulo 3.

## 8.2 Dirección estática

La tabla estática es configurada manualmente por los usuarios y distribuida a cada placa de interfaz, que no envejecerá.

Instrucciones:

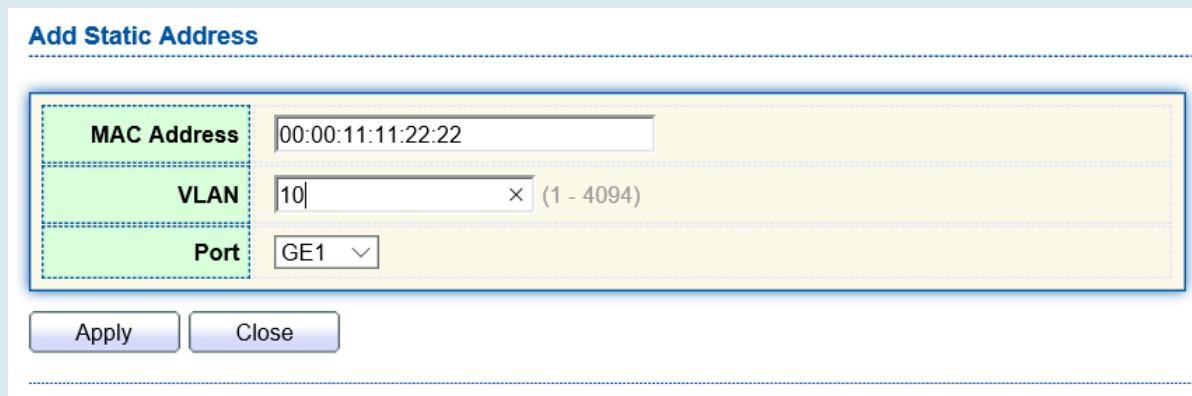
1. Haga clic en la "Tabla de direcciones MAC > dirección estática" de la siguiente manera:



**Static Address Table**

Showing  entries      Showing 1 to 1 of 1 entries

<input type="checkbox"/>	VLAN	MAC Address	Port
<input type="checkbox"/>	1	00:00:11:11:22:22	GE3



**Add Static Address**

MAC Address	<input type="text" value="00:00:11:11:22:22"/>
VLAN	<input type="text" value="10"/> × (1 - 4094)
Port	<input type="text" value="GE1"/>

Los datos de la interfaz son los siguientes

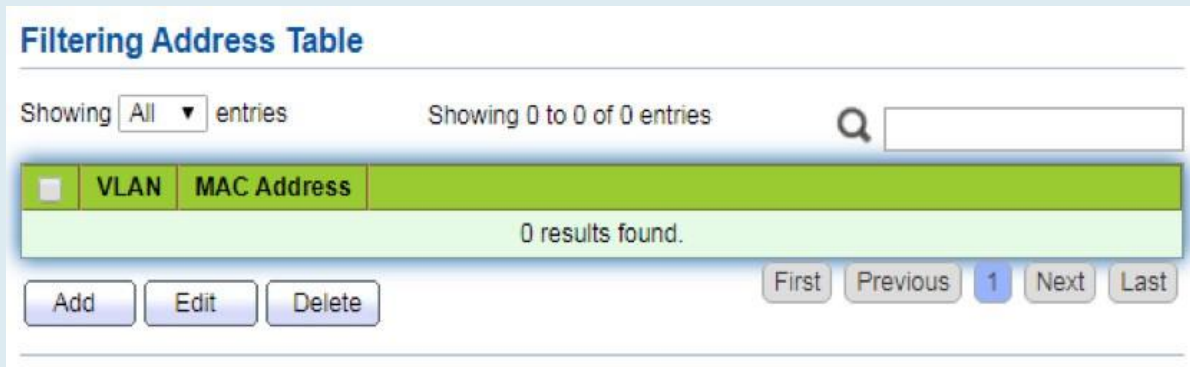
Elementos de configuración	Descripción
MAC	Obligatorio. Introduzca la nueva dirección MAC, por ejemplo: HH:HH:HH:HH:HH:HH
VLAN	Obligatorio. Especifique el ID de VLAN
Port	Obligatorio. Seleccione el tipo de interfaz e introduzca el nombre de la interfaz Descripción: debe ser el puerto miembro de las VLAN configuradas.

2. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

## 8.3 Dirección de filtrado

El conmutador descarta el marco de datos coincidente mediante instrucciones de configuración:

1. Haga clic en la "Tabla de direcciones MAC > dirección de filtrado" de la siguiente manera:




Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
MAC Address	Dirección MAC que se va a filtrar
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 la "Tabla de direcciones MAC > dirección de seguridad del puerto" de la siguiente manera:

### Port Security Address Table

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	VLAN	MAC Address	Type	Port
0 results found.				

### Add Port Security Address

MAC Address	<input type="text"/>
VLAN	<input type="text"/> (1 - 4094)
Port	<input type="text" value="GE1"/>

Los datos de la interfaz son los siguientes

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

# 9 Árbol de expansión



Los enlaces redundantes se utilizan a menudo para la copia de seguridad de enlaces y la fiabilidad de la red en la red de conmutación Ethernet. Sin embargo, estos enlaces generarán bucles en la red de conmutación, lo que provocará una tormenta de difusión, una lista de direcciones MAC inestable y otros fallos, empeorando así la calidad de la comunicación de los usuarios o incluso interrumpiendo la comunicación. Como resultado, aparece STP (Spanning Tree Protocol).

Lo mismo con el desarrollo de otros protocolos, desde el STP original definido en IEEE 802.1D, hasta RSTP (Rapid Spanning Tree Protocol) definido en IEEE802.1W y hasta MSTP (Multiple Spanning Tree Protocol) definido en IEEE 802.1S, STP sigue actualizándose.

MSTP es compatible con RSTP y STP, mientras que RSTP es compatible con STP. El contraste entre estos 3 protocolos se muestra en la tabla.

Stp	Característica	Aplicación
Stp	Un árbol libre de bucles como solución para difundir tormentas y copias de seguridad redundantes. Converge lentamente.	Un árbol libre de bucles como solución para difundir tormentas y copias de seguridad redundantes. Converge lentamente.
RSTP	Un árbol libre de bucles como solución para difundir tormentas y copias de seguridad redundantes. Converge rápidamente.	
MSTP	Un árbol libre de bucles como solución para difundir tormentas y copias de seguridad redundantes. Converge rápidamente. Los árboles de expansión equilibran la carga entre las VLAN. El flujo de diferentes VLAN se reenviará sujeto a rutas.	Distinguir el flujo de usuario y de negocio para el flujo de carga. Diferentes VLAN reenvían el flujo a través de árboles de expansión separados.

Después de implementar STP, se pueden lograr los siguientes objetivos calculando los bucles con topología:

- Eliminación de bucles: elimine posibles bucles de comunicación bloqueando redundantes Enlaces.

- Copias de seguridad de enlaces: active enlaces redundantes para restaurar la conectividad de red si el

Se produce un error en la ruta de acceso.

## 9.1 Propiedad

Configurar 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 clic en " Spanning Tree > Property" en la barra de navegación de la siguiente manera:

<b>State</b>	<input type="checkbox"/> Enable
<b>Operation Mode</b>	<input type="radio"/> STP <input checked="" type="radio"/> RSTP <input type="radio"/> MSTP
<b>Path Cost</b>	<input checked="" type="radio"/> Long <input type="radio"/> Short
<b>BPDU Handling</b>	<input type="radio"/> Filtering <input checked="" type="radio"/> Flooding
<b>Priority</b>	32768 (0 - 61440, default 32768)
<b>Hello Time</b>	2 Sec (1 - 10, default 2)
<b>Max Age</b>	20 Sec (6 - 40, default 20)
<b>Forward Delay</b>	15 Sec (4 - 30, default 15)
<b>Tx Hold Count</b>	6 (1 - 10, default 6)
<b>Region Name</b>	1C:2A:A3:00:00:24
<b>Revision</b>	0 (0 - 65535, default 0)
<b>Max Hop</b>	20 (1 - 40, default 20)

Los datos de la interfaz son los siguientes

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 de puerto
Hello Time	Intervalos entre mensajes Hello
Max Age	Tiempo máximo de envejecimiento
Forward Delay	Tiempo de retardo hacia adelante
Tx Hold Count	Especifique el recuento de retención Tx utilizado para limitar el número máximo de transmisión de paquetes 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 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 de MSTP
Max Hop	Especificar el número de saltos en una región MSTP antes de descartar la BPDU

2. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

## 9.2 Configuración del 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 la barra 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
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000

Edit Port Setting

**Port** GE1

**State**  Enable

**Path Cost**  (0 - 200000000) (0 = Auto)

**Priority**

**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

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
State	El puerto No. Para configurar atributos
Port	Habilitar STP o no
State	En modo largo y modo corto
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.
Edge Port	En lugar de otro conmutador o segmento de red, el puerto perimetral debe conectarse directamente a los terminales de usuario. Puede transitar rápidamente al estado de reenvío ya que los cambios de topología crean Sin bucles. STP puede pasar rápidamente a un puerto perimetral bajo configuración. Para lograr esto, se recomienda que los puertos Ethernet conectados directamente a los terminales de usuario se configuren como puertos de borde.
BPDU Filter	Habilitar filtro BPDU o no
BPDU Guard	Habilite BPDU Guard o no. Sin marcar de forma predeterminada. Si BPDU Guard está habilitado, el dispositivo apagará las interfaces que reciben BPDU y notificará al NMS. Dichas interfaces solo pueden ser restauradas manualmente por los administradores de red.
Point-to-Point	Seleccione habilitado, apagados y modos automáticos. 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 de apagado: indica que el puerto específico no puede conectar los enlaces punto a punto.

2. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

## 9.3 Instancia de MST

Una red de conmutación se divide en múltiples dominios por MSTP, con árboles de expansión independientes formados dentro de cada dominio. Cada árbol de expansión se denomina MSTI (Multiple Spanning Tree Instance), y cada dominio se denomina región MST: Multiple Spanning Tree Region).

Descripción:

Una instancia es un grupo de VLAN que reduce el costo de comunicación y la tasa de utilización de recursos. Cada instancia, calculada independientemente con topología, puede equilibrar la carga. Las VLAN con la misma topología se pueden asignar a una misma instancia y se reenvían de acuerdo con el estado del puerto en las instancias 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 la barra de navegación, "Editar" las instancias de árbol de expansión seleccionadas que se configurarán de la siguiente manera:

**MST Instance Table**

MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
0	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	1-4094
1	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
2	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
3	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
4	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
5	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
6	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
7	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
8	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
9	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
10	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
11	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
12	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
13	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
14	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
15	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	

**Edit MST Instance Setting**

---

<b>MSTI</b>	0
<b>Priority</b>	32768 (0 - 61440, default 32768)
<b>Bridge Identifier</b>	32768-1C:2A:A3:00:00:24
<b>Designated Root Bridge</b>	0-00:00:00:00:00:00
<b>Root Port</b>	
<b>Root Path Cost</b>	0
<b>Remaining Hop</b>	0

Apply Close

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
MSTI	Instancia No. de árboles de expansión varía de 0 a 15
VLAN	VLAN No. Asignado a partir de instancias
Priority	Establezca la prioridad de un múltiplo de 4.096 para la instancia especificada, que va de 0 a 65.535 con 32.768 como valor predeterminado.

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

## 9.4 Configuración del puerto MST

Instrucciones:

1. Haga clic en "Spanning Tree > MST Port Setting" en la barra de navegación, marque 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:

**MST Port Setting Table**

MSTI

Q

Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
<input type="checkbox"/>	1 GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	0	20
<input type="checkbox"/>	2 GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	0	20
<input type="checkbox"/>	3 GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	0	20
<input type="checkbox"/>	4 GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	0	20
<input type="checkbox"/>	5 GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	0	20
<input type="checkbox"/>	6 GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	0	20
<input type="checkbox"/>	7 GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	0	20
<input type="checkbox"/>	8 GE8	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-8	0	20
<input type="checkbox"/>	9 GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	0	20

**Edit MST Port Setting**

---

<b>MSTI</b>	0
<b>Port</b>	GE1-GE2
<b>Path Cost</b>	<input type="text" value="0"/> (0 - 200000000) (0 = Auto)
<b>Priority</b>	128 <input type="button" value="v"/>
<b>Port Role</b>	Disabled
<b>Port State</b>	Disabled
<b>Mode</b>	RSTP
<b>Type</b>	Boundary
<b>Designated Bridge</b>	0-00:00:00:00:00:00
<b>Designated Port ID</b>	128-1
<b>Designated Cost</b>	20000
<b>Remaining Hop</b>	20

---

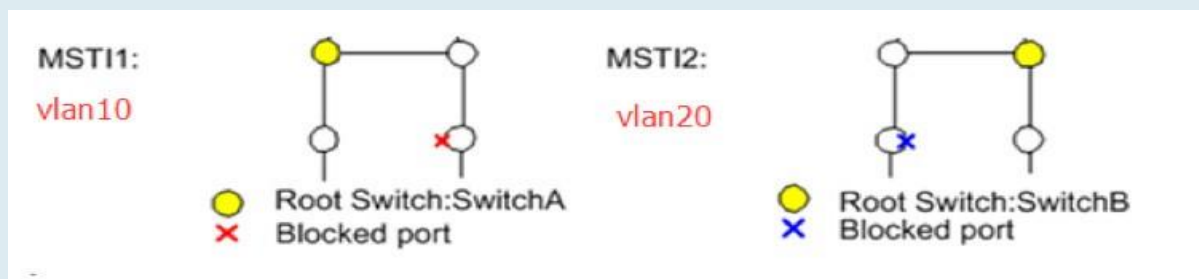
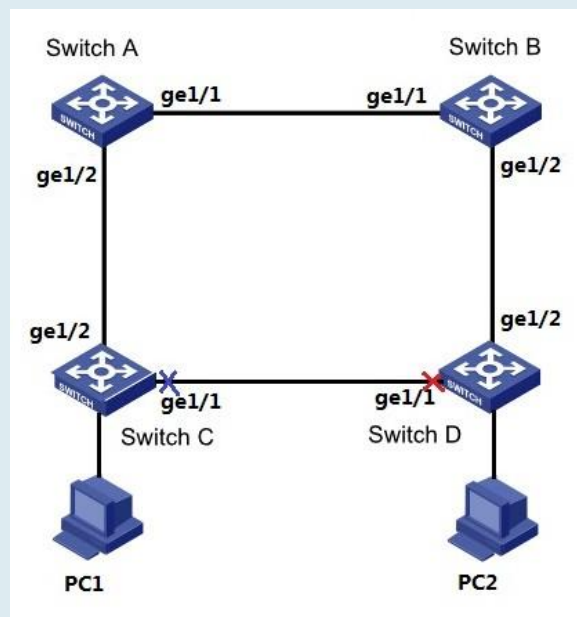
Los datos de la interfaz son los siguientes

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 LED de desactivación.
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. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

### 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 VLANs con abarcando instancias de árbol 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 > Crear VLAN" en la barra de navegación, complete las configuraciones correspondientes. "Aplicar" y terminar de la siguiente manera.



VLAN

Available VLAN

- VLAN 2
- VLAN 3
- VLAN 4
- VLAN 5
- VLAN 6
- VLAN 7
- VLAN 8
- VLAN 9

Created VLAN

- VLAN 1
- VLAN 10
- VLAN 20

---

### VLAN Table

Showing All entries Showing 1 to 3 of 3 entries

VLAN	Name	Type	VLAN interface State
<input type="radio"/> 1	default	Default	Disabled
<input type="radio"/> 10	VLAN0010	Static	Disabled
<input type="radio"/> 20	VLAN0020	Static	Disabled

2. Las VLAN se agregan a los bucles de entrada de los puertos del switch. Haga clic en "VLAN > VLAN > Membership" en la barra de navegación, seleccione el puerto de anillo a configurar, mueva VLAN10 y 20 al cuadro derecho y márkuelos con "Etiquetado".

### Edit Port Setting

**Port** GE1

**Mode** Trunk

Membership

- 10
- 20

- 1UP

Forbidden  
 Excluded  
 Tagged  
 Untagged  
 PVID

"Aplicar" y finalizar:

3. Haga clic en la "Propiedad de > de árbol de expansión" en la barra de navegación y elija el modo MSTP de la siguiente manera:

<b>State</b>	<input checked="" type="checkbox"/> Enable
<b>Operation Mode</b>	<input type="radio"/> STP <input type="radio"/> RSTP <input checked="" type="radio"/> MSTP
<b>Path Cost</b>	<input checked="" type="radio"/> Long <input type="radio"/> Short
<b>BPDU Handling</b>	<input type="radio"/> Filtering <input checked="" type="radio"/> Flooding
<b>Priority</b>	32768 (0 - 61440, default 32768)
<b>Hello Time</b>	2 Sec (1 - 10, default 2)
<b>Max Age</b>	20 Sec (6 - 40, default 20)
<b>Forward Delay</b>	15 Sec (4 - 30, default 15)
<b>Tx Hold Count</b>	6 (1 - 10, default 6)
<b>Region Name</b>	1C:2A:A3:00:00:24
<b>Revision</b>	0 (0 - 65535, default 0)
<b>Max Hop</b>	20 (1 - 40, default 20)

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 "Agregarlos" de la siguiente manera:

**MST Instance Table**

MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
0	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	1-9,11-19,21-4094
1	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	10
2	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	20
3	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
4	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
5	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	
6	32768	32768-1C:2A:A3:00:00:24	0-00:00:00:00:00:00	N/A	0	0	

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 la barra de navegación, estadísticas del puerto de entrada de la siguiente manera

**Statistics Table**

Refresh Rate  sec

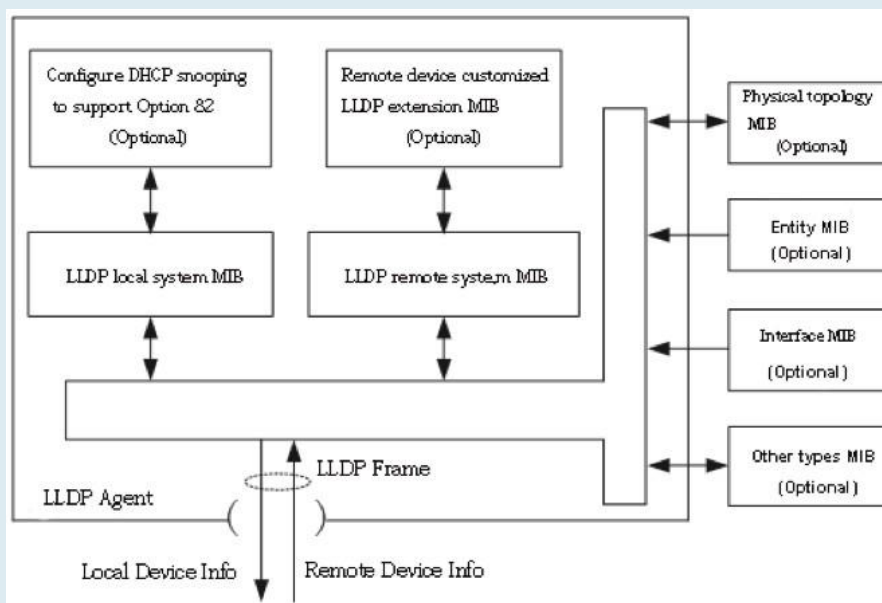
	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0

# 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 network local se mantendrá en forma de MIB. A continuación, se muestra cómo funciona.

Diagrama de bloques de los principios LLDP



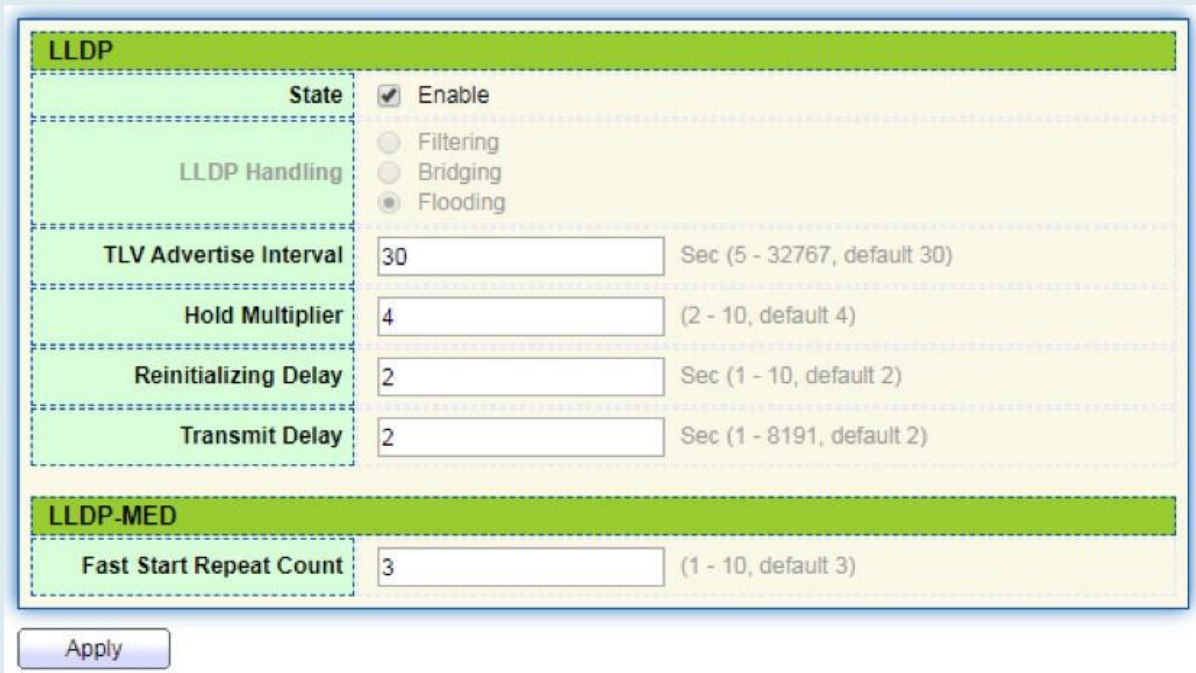
LLDP se realiza en base a:

- 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 de servicio 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 la falla y profundiza la comprensión precisa de la topología de red por parte del sistema de gestión.

## 10.1 LLDP

Instrucciones:

1. Haga clic en "Discovery > LLDP > Property" en la barra de navegación de la siguiente manera.



Los datos de la interfaz son los siguientes

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. Rellene los elementos de configuración correspondientes
3. "Aplicar" y terminar.

## 10.2 Configuración del puerto

Instrucciones:

1. Haga clic en "Discovery > LLDP > Port Setting" en la barra de navegación de la siguiente manera.

Port Setting Table					
<input type="checkbox"/>	Entry	Port	Mode	Selected TLV	
<input type="checkbox"/>	1	GE1	Normal	802.1 PVID	
<input type="checkbox"/>	2	GE2	Normal	802.1 PVID	
<input type="checkbox"/>	3	GE3	Normal	802.1 PVID	
<input type="checkbox"/>	4	GE4	Normal	802.1 PVID	

Los datos de la interfaz son los siguientes

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.

**Edit Port Setting**

<b>Port</b>	GE1				
<b>Mode</b>	<input type="radio"/> Transmit <input type="radio"/> Receive <input checked="" type="radio"/> Normal <input type="radio"/> Disable				
<b>Optional TLV</b>	<table style="width: 100%;"> <tr> <th>Available TLV</th> <th>Selected TLV</th> </tr> <tr> <td>           Port Description            System Name            System Description            System Capabilities            802.3 MAC-PHY         </td> <td>802.1 PVID</td> </tr> </table>	Available TLV	Selected TLV	Port Description System Name System Description System Capabilities 802.3 MAC-PHY	802.1 PVID
Available TLV	Selected TLV				
Port Description System Name System Description System Capabilities 802.3 MAC-PHY	802.1 PVID				
<b>802.1 VLAN Name</b>	<table style="width: 100%;"> <tr> <th>Available VLAN</th> <th>Selected VLAN</th> </tr> <tr> <td>VLAN 1</td> <td></td> </tr> </table>	Available VLAN	Selected VLAN	VLAN 1	
Available VLAN	Selected VLAN				
VLAN 1					

Los datos de la interfaz son los siguientes

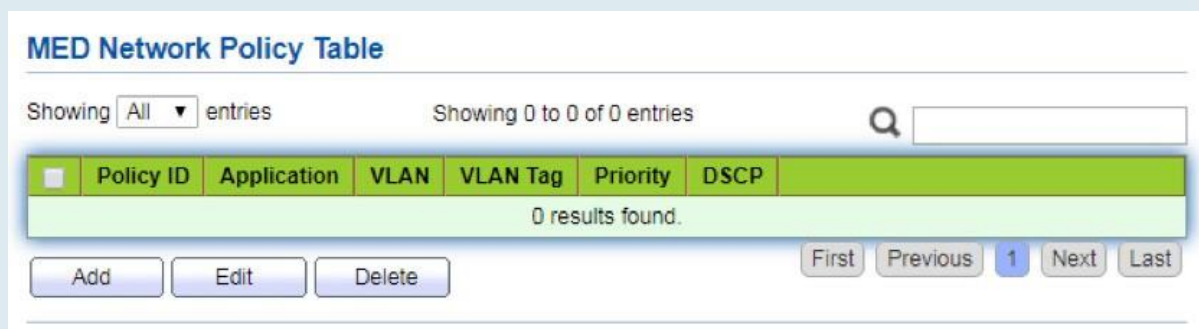
Elementos de configuración	Descripción
Port	Lista de puertos
Mode	El modo LLDP incluye: Transmitir, Recibir, Normal, Deshabilitar, el valor predeterminado es Normal Transmitir: transmitir mensajes LLDP solamente; Recibir: recibir mensajes LLDP solamente; Normal: transmitir y recibir mensajes LLDP; Desactivar: 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 fallos y permitir que los sistemas de gestión comprendan con precisión la topología de la red.

Instrucciones

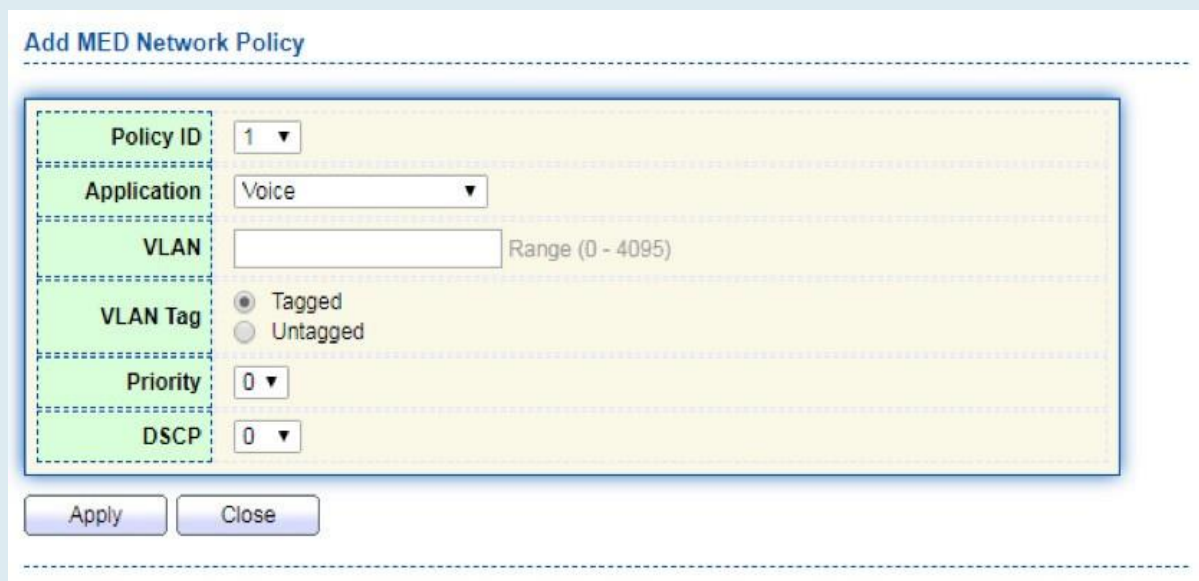
1. Haga clic en "Discovery > LLDP > MED Network Policy" en la barra de navegación de la siguiente manera.



**MED Network Policy Table**

Showing  entries      Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP
0 results found.						



**Add MED Network Policy**

Policy ID:   
 Application:   
 VLAN:  Range (0 - 4095)  
 VLAN Tag:  Tagged  Untagged  
 Priority:   
 DSCP:

Los datos de la interfaz son los siguientes

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 clic en "Discovery > LLDP > MED Port Setting" en la barra de navegación de la siguiente manera.

### MED Port Setting Table

□	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
<input type="checkbox"/>	1	GE1	Enabled	Yes		No	No
<input type="checkbox"/>	2	GE2	Enabled	Yes		No	No
<input type="checkbox"/>	3	GE3	Enabled	Yes		No	No
<input type="checkbox"/>	4	GE4	Enabled	Yes		No	No
<input type="checkbox"/>	5	GE5	Enabled	Yes		No	No
<input type="checkbox"/>	6	GE6	Enabled	Yes		No	No
<input type="checkbox"/>	7	GE7	Enabled	Yes		No	No

### Edit MED Port Setting

**Port** GE1-GE2

**State**  Enable

**Optional TLV**

**Available TLV**  

Location

Inventory

**Selected TLV**  

Network Policy

**Network policy**

**Available Policy**

**Selected Policy**

**Location**

**Coordinate**  (16 pairs of hexadecimal characters)

**Civic**  (6 - 160 pairs of hexadecimal characters)

**ECS ELIN**  (10 - 25 pairs of hexadecimal characters)

Los datos de la interfaz son los siguientes

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 clic en "Discovery > LLDP > Packet View" en la barra de navegación de la siguiente manera.

**Packet View Table**

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
<input type="radio"/>	1	GE1	38	1450	Not Overloading
<input type="radio"/>	2	GE2	38	1450	Not Overloading
<input type="radio"/>	3	GE3	38	1450	Not Overloading
<input type="radio"/>	4	GE4	38	1450	Not Overloading
<input type="radio"/>	5	GE5	38	1450	Not Overloading
<input type="radio"/>	6	GE6	38	1450	Not Overloading
<input type="radio"/>	7	GE7	38	1450	Not Overloading
<input type="radio"/>	8	GE8	38	1450	Not Overloading

## 10.6 Información local

Instrucciones para el resumen del dispositivo:

1. Haga clic en "Discovery > LLDP > Local Information" en la barra de navegación de la siguiente manera.

**Device Summary**

<b>Chassis ID Subtype</b>	MAC address
<b>Chassis ID</b>	1C:2A:A3:00:00:24
<b>System Name</b>	Switch
<b>System Description</b>	HR-AFGM-2444S
<b>Supported Capabilities</b>	Bridge, Router
<b>Enabled Capabilities</b>	Bridge, Router
<b>Port ID Subtype</b>	Local

Instrucciones para la tabla de estado del puerto:

2. Haga clic en "Discovery > LLDP > Local Information" en la barra de navegación de la siguiente manera.

**Port Status Table**

	Entry	Port	LLDP State	LLDP-MED State
<input type="radio"/>	1	GE1	Normal	Enabled
<input type="radio"/>	2	GE2	Normal	Enabled
<input type="radio"/>	3	GE3	Normal	Enabled
<input type="radio"/>	4	GE4	Normal	Enabled
<input type="radio"/>	5	GE5	Normal	Enabled
<input type="radio"/>	6	GE6	Normal	Enabled

## 10.7 Vecino

Instrucciones para la visualización de vecinos LLDP

1. Haga clic en "Discovery > LLDP > Neighbor" en la barra de navegación de la siguiente manera.

### Neighbor Table

Showing  entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
<input type="checkbox"/>	GE9	MAC address	00:E0:41:00:00:02	Local	gi13		118

## 10.8 Estadística

Instrucciones:

- Haga clic en "Discovery > LLDP > Statistics" en la barra de navegación de la siguiente manera.

### Global Statistics

Insertions	11
Deletions	7
Drops	0
AgeOuts	0

### Statistics Table

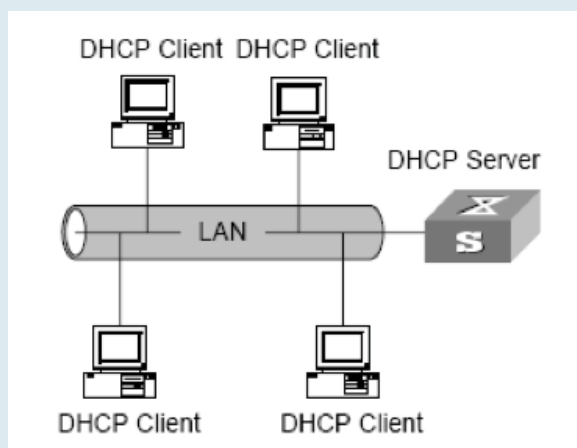
<input type="checkbox"/>	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor Timeout
			Total	Total	Discard	Error	Discard	Unrecognized	
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	278	29	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0	0

## 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 del equipo cambia (como un equipo portátil o una red inalámbrica) y el número de equipos supera la resolución de adición de 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 de acuerdo con la política.

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.



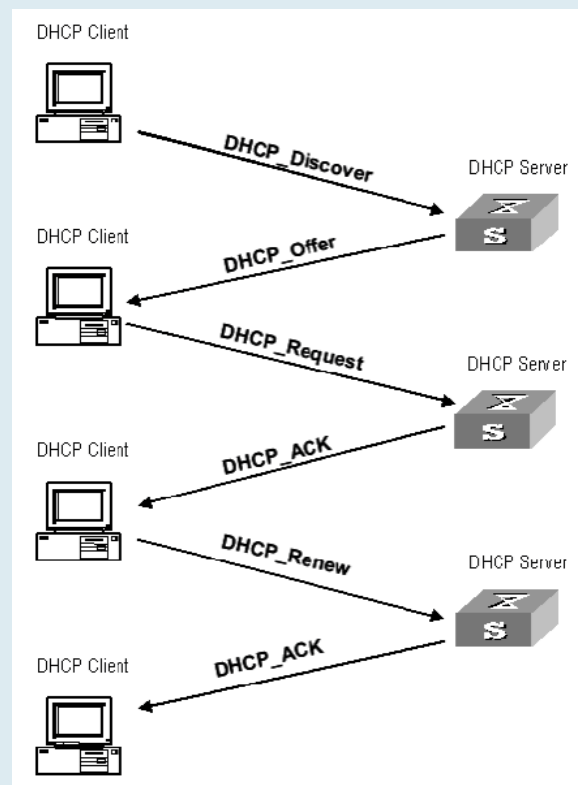
## Asignación de direcciones IP de la estrategia de asignación de direcciones IP DHCP

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). Envía 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 asignación de direcciones dinámica.

### 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.



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 de detección DHCP en modo de difusión y solo responderá el servidor DHCP.
- 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 solicitud de IP address desde el 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 la edad del desorden de confirmación dhcp-ack que contiene la dirección IP y otras configuraciones proporcionadas por el cliente; de lo contrario, devolverá el mensaje dhcp-nak, indicando 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 asignada)

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, solo necesita difundir el mensaje de solicitud DHCP que contiene la dirección IP asignada la última vez, y no es necesario volver a enviar el mensaje de descubrimiento 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, se ha 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

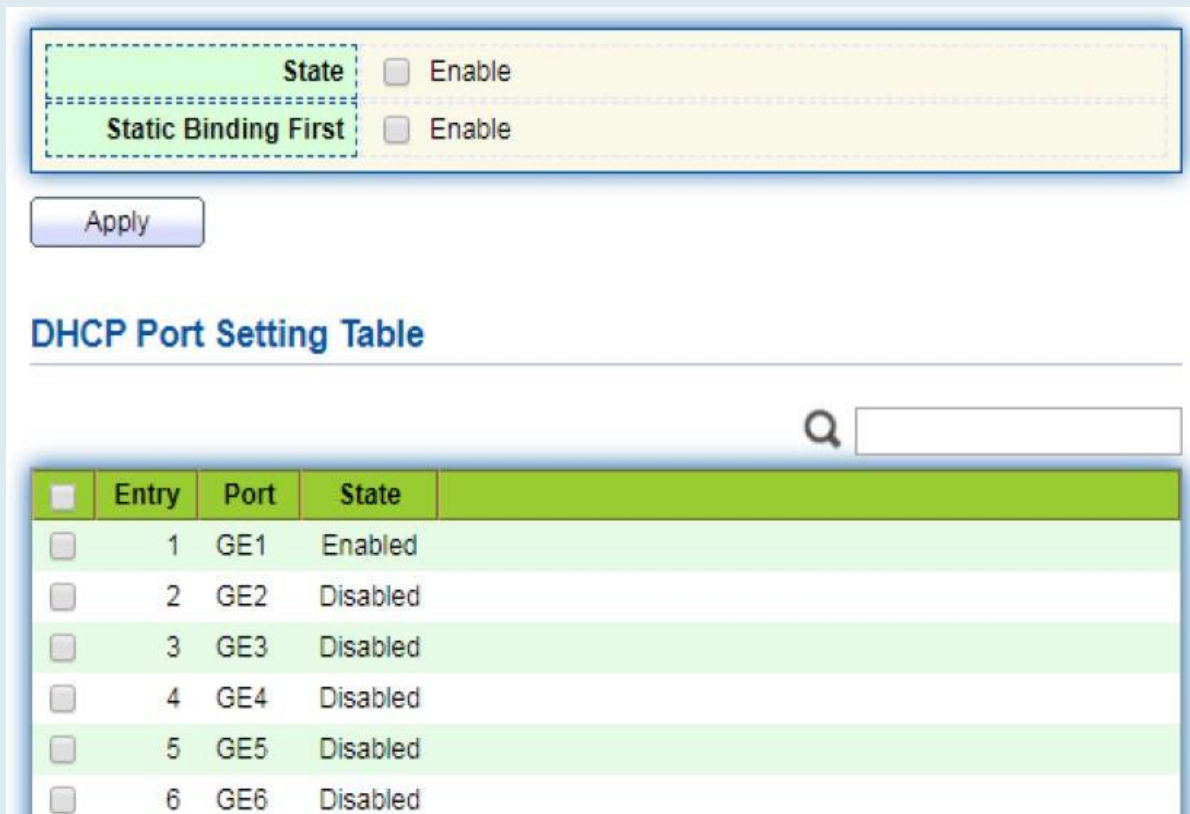
La dirección IP dinámica asignada por el servidor DHCP al cliente suele tener un plazo de concesión determinado. Después de la expiración, el servidor recuperará la dirección IP. Si el cliente DHCP desea seguir utilizando la dirección, es necesario actualizar la concesión de IP.

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 clic en "DHCP > Property" en la barra de navegación de la siguiente manera.

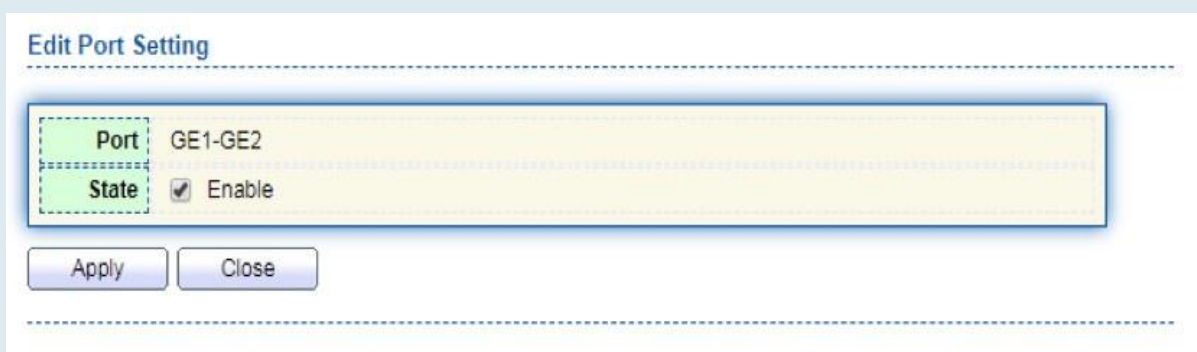


The screenshot shows the DHCP configuration interface. At the top, there are two settings: "State" and "Static Binding First", both with "Enable" checkboxes. Below these is an "Apply" button. Underneath is the "DHCP Port Setting Table" with a search bar. The table lists six entries with their respective ports and states.

Entry	Port	State
1	GE1	Enabled
2	GE2	Disabled
3	GE3	Disabled
4	GE4	Disabled
5	GE5	Disabled
6	GE6	Disabled

Instrucciones para la configuración del puerto DHCP:

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



The screenshot shows the "Edit Port Setting" dialog box. It has two fields: "Port" with the value "GE1-GE2" and "State" with a checked "Enable" checkbox. Below the fields are "Apply" and "Close" buttons.

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 el grupo de IP de la siguiente manera.

**IP Pool Table**

Showing  entries Showing 0 to 0 of 0 entries

Pool	Section			Gateway	Mask	DNS Primary Server	DNS Second Server	Lease time
	Section	Start Address	End Address					
0 results found.								

**IP Pool Table**

<b>Pool</b>	<input type="text" value=""/> (1 to 32 alphanumeric characters)
<b>Gateway</b>	<input type="text" value=""/>
<b>Mask</b>	<input type="text" value=""/>
<b>IP Address Section</b>	Section <input type="text" value="1"/>
	Start Address <input type="text" value=""/>
	End Address <input type="text" value=""/>
<b>DNS Primary Server</b>	<input type="checkbox"/> Enable <input type="text" value=""/>
<b>DNS Second Server</b>	<input type="checkbox"/> Enable <input type="text" value=""/>
<b>Lease time</b>	<input type="text" value="1"/> Day <input type="text" value="00"/> Hour <input type="text" value="00"/> Minute

Nota:

- La dirección inicial 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:

- 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.

**DHCP Server Group Table**

Q

Group ID	Group IP Address	Bind VLAN Interface
0 results found.		

**DHCP Server Group Table**

DHCP Server Group

Group IP Address

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

- Haga clic en "Configuración del grupo de direcciones DHCP > VLAN IF", ingrese a la tabla de grupo de direcciones de interfaz VLAN, seleccione la interfaz y el grupo de servidores, y luego haga clic en "Aplicar" de la siguiente manera.

**Vlan Interface Address Pool Table**

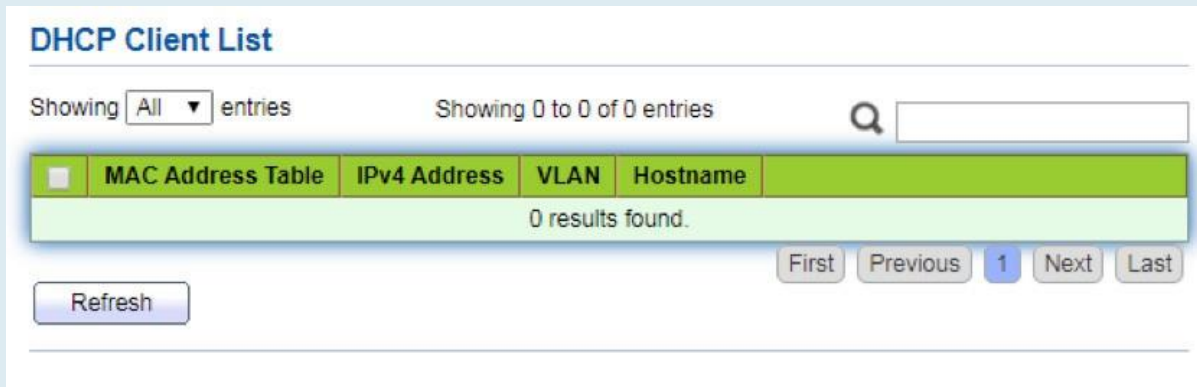
Interface

DHCP Server Group

## 11.4 Lista de clientes

Información de la lista de clientes Instrucciones:

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



**DHCP Client List**

Showing **All** entries      Showing 0 to 0 of 0 entries     

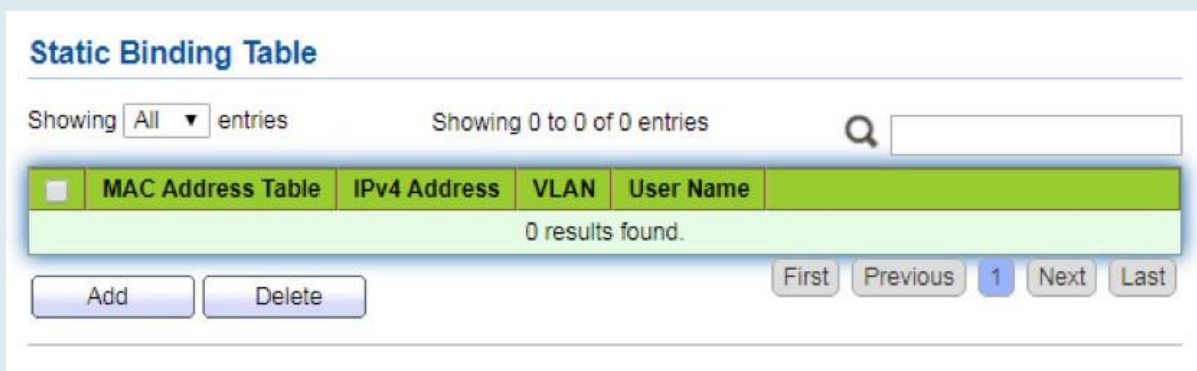
<input type="checkbox"/>	MAC Address Table	IPv4 Address	VLAN	Hostname
0 results found.				

First Previous **1** Next Last

## 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.



**Static Binding Table**

Showing **All** entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	MAC Address Table	IPv4 Address	VLAN	User Name
0 results found.				

First Previous **1** Next Last

Nota:

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

# 12 Multidifusión



## 121 General

### 121.1 Propiedad

Instrucciones:

1. Haga clic en "Multicast > General > Property" en la barra de navegación de la siguiente manera.

**Unknown Multicast Action**

- Flood
- Drop
- Forward to Router Port

**Multicast Forward Method**

Protocol	Method
IPv4	<input checked="" type="radio"/> DMAC-VID
	<input type="radio"/> DIP-VID
IPv6	<input checked="" type="radio"/> DMAC-VID
	<input type="radio"/> DIP-VID

Apply

### 121.2 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 una gran cantidad 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:

**Group Address Table**

IP Version: IPv4

Showing: All entries      Showing 0 to 0 of 0 entries

VLAN	Group Address	Member	Type	Life (Sec)
0 results found.				

Buttons: Add, Edit, Delete, Refresh

Pagination: First, Previous, 1, Next, Last

### Add Group Address

<b>VLAN</b>	1				
<b>IP Version</b>	IPv4				
<b>Group Address</b>					
<b>Member</b>	<table border="1"> <tr> <th>Available Port</th> <th>Selected Port</th> </tr> <tr> <td> <ul style="list-style-type: none"> <li>GE1</li> <li>GE2</li> <li>GE3</li> <li>GE4</li> <li>GE5</li> <li>GE6</li> <li>GE7</li> <li>GE8</li> </ul> </td> <td></td> </tr> </table>	Available Port	Selected Port	<ul style="list-style-type: none"> <li>GE1</li> <li>GE2</li> <li>GE3</li> <li>GE4</li> <li>GE5</li> <li>GE6</li> <li>GE7</li> <li>GE8</li> </ul>	
Available Port	Selected Port				
<ul style="list-style-type: none"> <li>GE1</li> <li>GE2</li> <li>GE3</li> <li>GE4</li> <li>GE5</li> <li>GE6</li> <li>GE7</li> <li>GE8</li> </ul>					

Los datos de la interfaz son los siguientes

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

### Group Address Table

IP Version

Showing  entries      Showing 1 to 1 of 1 entries

<input type="checkbox"/>	VLAN	Group Address	Member	Type	Life (Sec)
<input type="checkbox"/>	1	<a href="#">224.1.1.111</a>	GE1-GE8	Static	

## 121.3 Puerto del router

Configurar y ver el puerto del router de multidifusión Instrucciones:

1. Haga clic en "Multicast > General > Router Port" en la barra de navegación de la siguiente manera.

### Router Port Table

IP Version IPv4 ▾

Showing All ▾ entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
0 results found.					

First Previous 1 Next Last

Add   Edit   Refresh

## 121.4 Reenviar todo

Configurar y ver el puerto de reenvío de multidifusión Instrucciones:

1. Haga clic en "Multidifusión > General > Adelante todo" en la barra de navegación de la siguiente manera.

### Forward All Table

IP Version IPv4 ▾

Showing All ▾ entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	VLAN	Static Port	Forbidden Port
0 results found.			

First Previous 1 Next Last

Add   Edit   Delete

## 121.5 Regulación

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

1. Haga clic en "Multicast > General > Throttling" en la barra de navegación de la siguiente manera.

**Throttling Table**

IP Version

Q

<input type="checkbox"/>	Entry	Port	Max Group	Exceed Action
<input type="checkbox"/>	1	GE1	256	Deny
<input type="checkbox"/>	2	GE2	256	Deny
<input type="checkbox"/>	3	GE3	256	Deny
<input type="checkbox"/>	4	GE4	256	Deny
<input type="checkbox"/>	5	GE5	256	Deny
<input type="checkbox"/>	6	GE6	256	Deny

## 121.6 Perfil de filtrado

Configurar y ver el perfil de filtrado de multidifusión del puerto Instrucciones:

1. Haga clic en "Multicast > General > Filtering Profile" en la barra de navegación de la siguiente manera.

**Filtering Profile Table**

IP Version

Showing  entries Showing 0 to 0 of 0 entries

Q

<input type="checkbox"/>	Profile ID	Start Address	End Address	Action
0 results found.				

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

2. Haga clic en "Multicast > General > Filtering Binding" en la barra de navegación de la siguiente manera.

**Filtering Binding Table**

IP Version

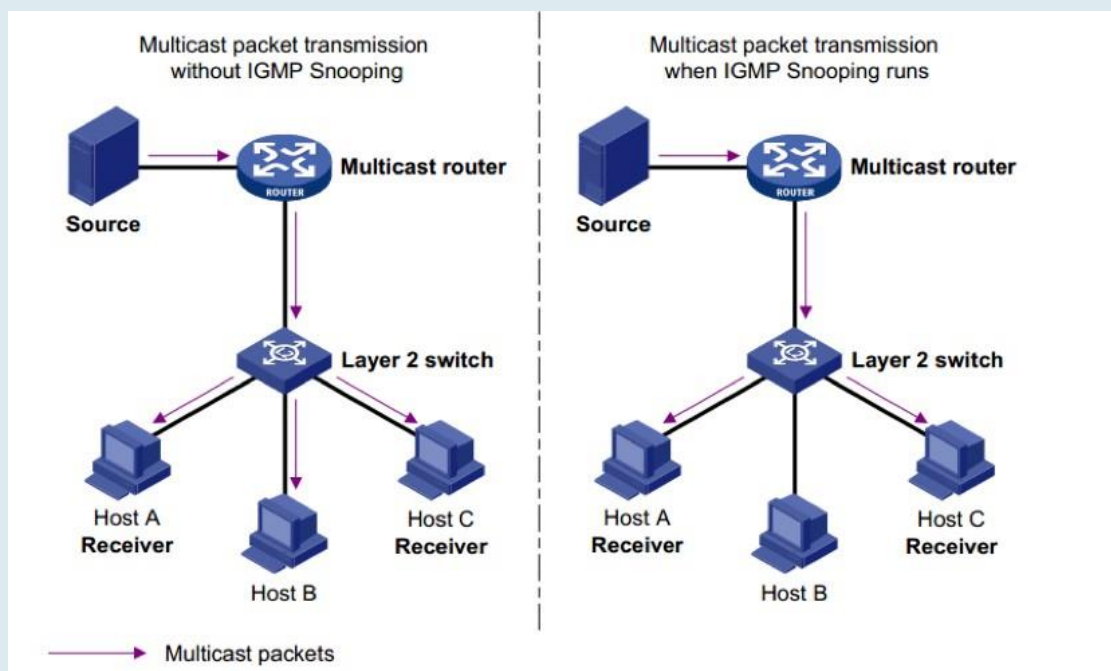
Q

<input type="checkbox"/>	Entry	Port	Profile ID
<input type="checkbox"/>	1	GE1	
<input type="checkbox"/>	2	GE2	
<input type="checkbox"/>	3	GE3	
<input type="checkbox"/>	4	GE4	
<input type="checkbox"/>	5	GE5	
<input type="checkbox"/>	6	GE6	

## 12.2 IGMP Snooping

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 puertos y 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 espionaje IGMP. Cuando se ejecuta el espionaje IGMP, los datos de grupos de multidifusión conocidos se transmiten a receptores especificados, mientras que los datos de multidifusión no conocidos todavía están en la capa 2.





## 12.21 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 husmear los mensajes IGMP / MLD transmitidos entre enrutadores y hosts, y para establecer una tabla de reenvío L2 para datos de multidifusión, con el fin de administrar y controlar el reenvío de datos de multidifusión 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 el VLAN que se configurará a partir de la información de VLAN creada y "Edite" los detalles de la siguiente manera:

<b>State</b>	<input type="checkbox"/> Enable
<b>Version</b>	<input checked="" type="radio"/> IGMPv2 <input type="radio"/> IGMPv3
<b>Report Suppression</b>	<input checked="" type="checkbox"/> Enable

**VLAN Setting Table**

☐	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	10	Disabled	Enabled	2	125	10	2	1	Disabled
<input type="checkbox"/>	20	Disabled	Enabled	2	125	10	2	1	Disabled

**Edit VLAN Setting**

<b>VLAN</b>	20
<b>State</b>	<input type="checkbox"/> Enable
<b>Router Port Auto Learn</b>	<input checked="" type="checkbox"/> Enable
<b>Immediate leave</b>	<input type="checkbox"/> Enable
<b>Query Robustness</b>	<input type="text" value="2"/> (1 - 7, default 2)
<b>Query Interval</b>	<input type="text" value="125"/> Sec (30 - 18000, default 125)
<b>Query Max Response Interval</b>	<input type="text" value="10"/> Sec (5 - 20, default 10)
<b>Last Member Query Counter</b>	<input type="text" value="2"/> (1 - 7, default 2)
<b>Last Member Query Interval</b>	<input type="text" value="1"/> Sec (1 - 25, default 1)
<b>Operational Status</b>	
<b>Status</b>	Disabled
<b>Query Robustness</b>	2
<b>Query Interval</b>	125 (Sec)
<b>Query Max Response Interval</b>	10 (Sec)
<b>Last Member Query Counter</b>	2
<b>Last Member Query Interval</b>	1 (Sec)

Los datos de la interfaz son los siguientes

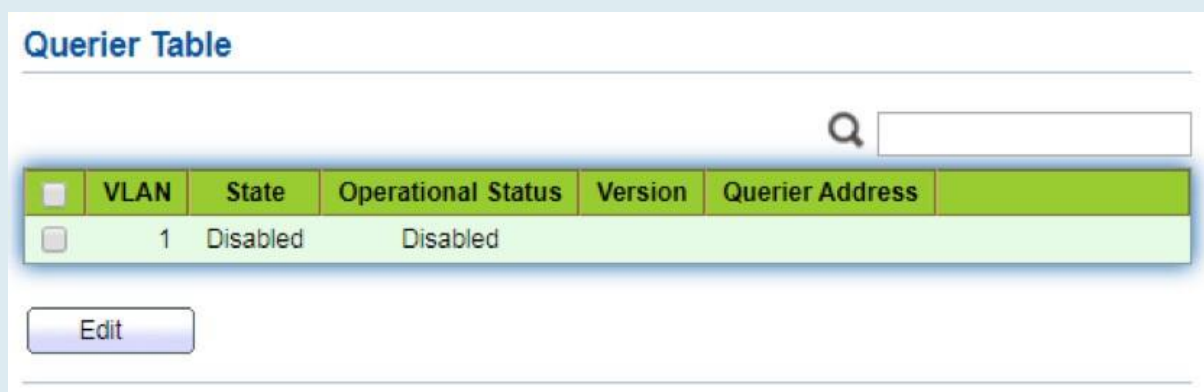
Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
State	Habilitar o deshabilitar el IGMP Snooping en esta VLAN
Router Port Auto Learn	Habilitar o deshabilitar el aprendizaje automático del puerto de ruta
Immediate leave	Los miembros de multidifusión se van rápidamente
Query 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. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

## 12.2.2 Consulta

Configurar y ver IGMP snooping  
Instrucciones de Querier:

1. Haga clic en "Multicast > IGMP Snooping > Querier" en la barra de navegación de la siguiente manera.



**Querier Table**

Q

<input type="checkbox"/>	VLAN	State	Operational Status	Version	Querier Address
<input type="checkbox"/>	1	Disabled	Disabled		

Los datos de la interfaz son los siguientes

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

Configurar y ver las estadísticas de espionaje IGMP Instrucciones:

1. Haga clic en "Multicast > IGMP Snooping > statistics" en la barra de navegación de la siguiente manera.

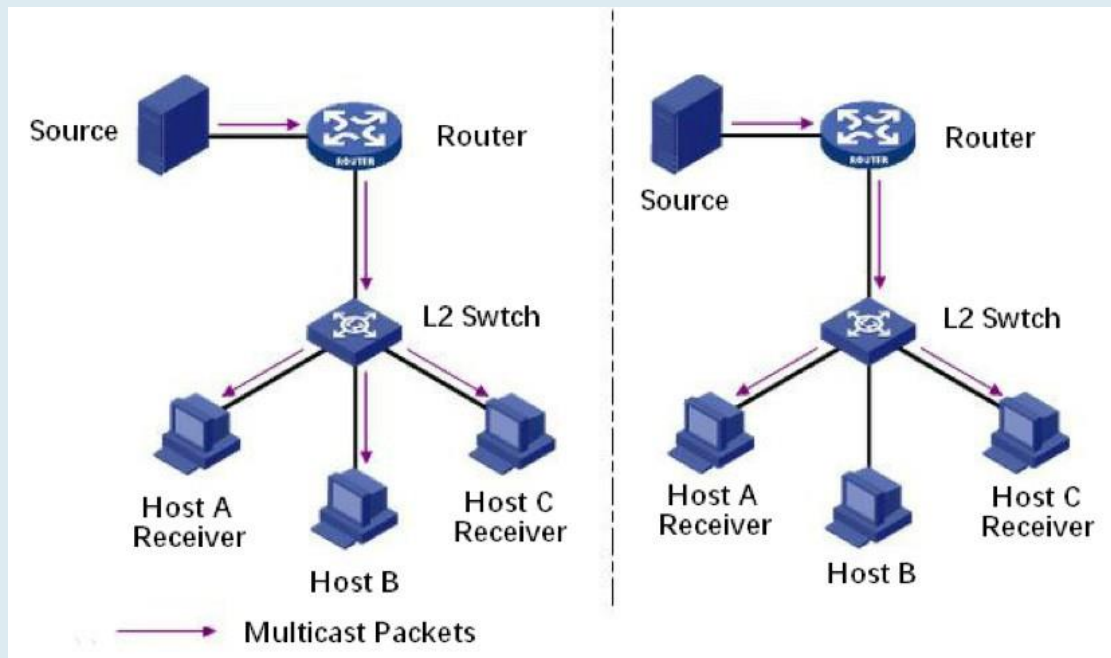
Receive Packet		
Total		0
Valid		0
InValid		0
Other		0
Leave		0
Report		0
General Query		0
Special Group Query		0
Source-specific Group Query		0
Transmit Packet		
Leave		0
Report		0
General Query		0
Special Group Query		0
Source-specific Group Query		0

## 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 figura siguiente, 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 transmitirán a los múltiples 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:

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

## 123.1 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:

**State**  Enable

**Version**  MLDv1  MLDv2

**Report Suppression**  Enable

**VLAN Setting Table**

■	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
<input type="checkbox"/>	1	Disabled	Enabled	2	125	10	2	1	Disabled

**Edit VLAN Setting**

---

**VLAN** 1

**State**  Enable

**Router Port Auto Learn**  Enable

**Immediate leave**  Enable

**Query Robustness**  (1 - 7, default 2)

**Query Interval**  Sec (30 - 18000, default 125)

**Query Max Response Interval**  Sec (5 - 20, default 10)

**Last Member Query Counter**  (1 - 7, default 2)

**Last Member Query Interval**  Sec (1 - 25, default 1)

**Operational Status**

**Status** Disabled

**Query Robustness** 2

**Query Interval** 125 (Sec)

**Query Max Response Interval** 10 (Sec)

**Last Member Query Counter** 2

**Last Member Query Interval** 1 (Sec)

Los datos de la interfaz son los siguientes

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. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

## 12.3.2 Estadística

Configurar y ver estadísticas de espionaje

MLD Instrucciones:

1. Haga clic en "Multicast > MLD Snooping > statistics" en la barra de navegación de la siguiente manera.

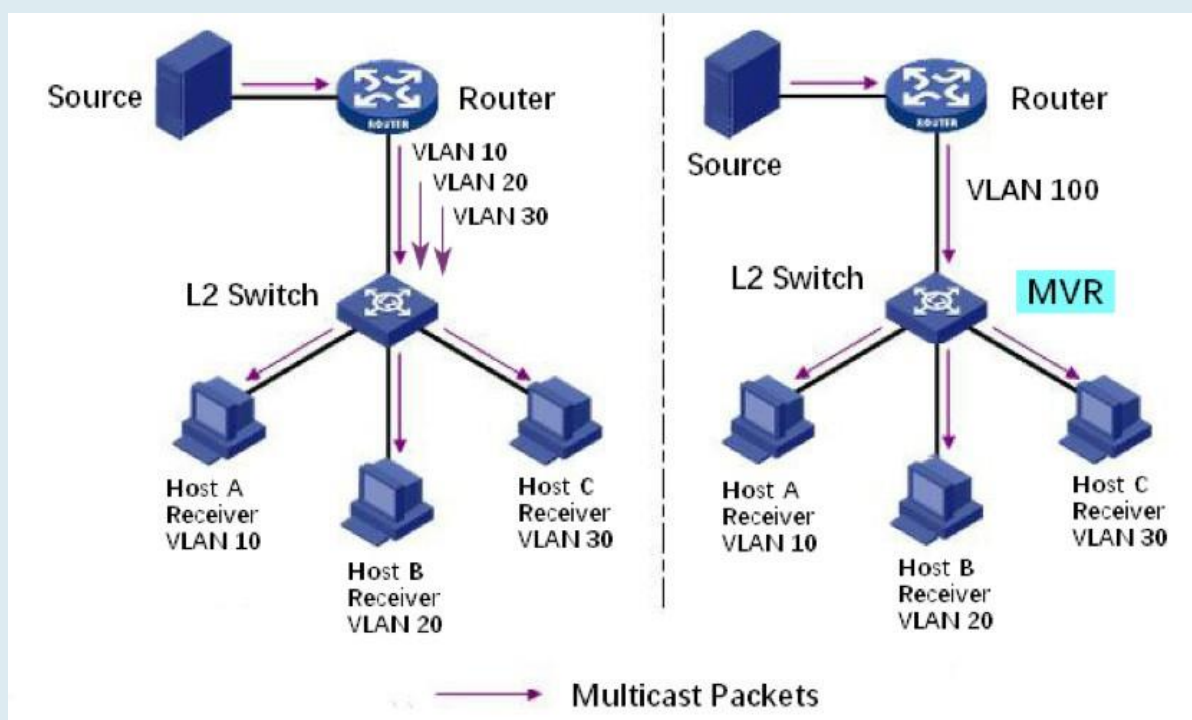
Receive Packet		
Total	0	
Valid	0	
InValid	0	
Other	0	
Leave	0	
Report	0	
General Query	0	
Special Group Query	0	
Source-specific Group Query	0	
Transmit Packet		
Leave	0	
Report	0	
General Query	0	
Special Group Query	0	
Source-specific Group Query	0	

Clear Refresh

## 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.

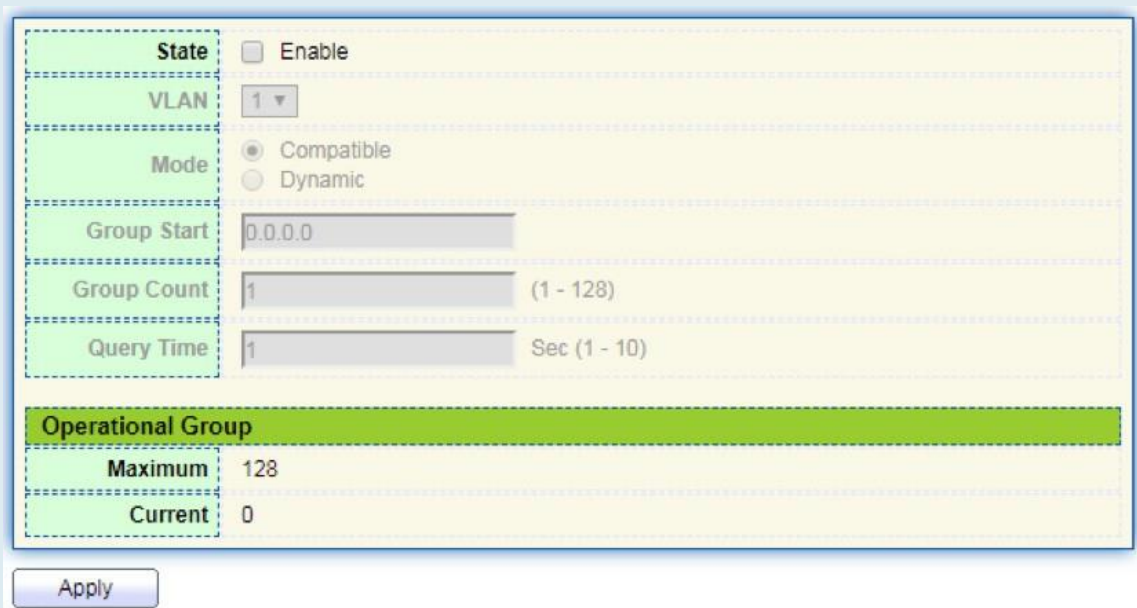
Sin embargo, IGMP snooping solo puede controlar efectivamente el tráfico de la misma VLAN multicast, pero no el tráfico VLAN cruzado. Como resultado, la eficiencia de la replicación múltiple de la misma multidifusión en diferentes VLAN sigue existiendo. Para resolver el problema de inundación de VLAN cruzada, adoptamos la VLAN de multidifusión dedicada del tráfico de fuente de multidifusión, como se muestra en la figura siguiente.



## 12.4.1 Propiedad

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

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



Los datos de la interfaz son los siguientes

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 la parte superior externa 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 inicial del grupo de multidifusión
Group Count	Número de direcciones de grupo de multidifusión
Query Time	Tiempo de consulta de grupo de multidifusión



2. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar.

## 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:

### Port Setting Table

<input type="checkbox"/>	Entry	Port	Role	Immediate Leave
<input type="checkbox"/>	1	GE1	None	Disabled
<input type="checkbox"/>	2	GE2	None	Disabled
<input type="checkbox"/>	3	GE3	None	Disabled
<input type="checkbox"/>	4	GE4	None	Disabled
<input type="checkbox"/>	5	GE5	None	Disabled
<input type="checkbox"/>	6	GE6	None	Disabled

#### Edit Port Setting

<b>Port</b>	GE1
<b>Role</b>	<input checked="" type="radio"/> None <input type="radio"/> Receiver <input type="radio"/> Source
<b>Immediate Leave</b>	<input type="checkbox"/> Enable

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Port	Lista de puertos
Role	<p>Modo de puerto</p> <p>Receptor: Representa el puerto del conmutador al que está conectado el host de multidifusión, que se utiliza para recibir el flujo de multidifusión.</p> <p>Fuente: El puerto de origen se refiere al puerto de origen del flujo de multidifusión del equipo de capa superior, es decir, el acceso a la fuente de multidifusión port</p>
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:

**Group Address Table**

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	VLAN	Group Address	Member	Type	Life (Sec)
0 results found.					

**Add Group Address**

**VLAN** 1

**Group Address**  (0.0.0.0 - 0.0.0.0)

**Member**

Available Port:

Selected Port:

Los datos de la interfaz son los siguientes

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 VLANIF, primero se debe crear la VLAN correspondiente. Con la ayuda de la interfaz VLANIF, 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 a la configuración de la interfaz IPv4 de capa 3 de la siguiente manera:

**IPv4 Interface Table**

Q

<input type="checkbox"/>	Interface	IP Address Type	IP Address	Mask	Status
0 results found.					

**Add IPv4 Interface**

**Interface**  VLAN

Loopback

**Address Type**  Dynamic  Static

**IP Address**

**Mask**  Network Mask   Prefix Length  (8 - 30)

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
VLAN	ID de VLAN que se va a configurar
Loopback	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:

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

**IPv4 Routing Table**

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
<input type="checkbox"/>	192.168.2.0	24	Directly Connected				MGMT VLAN*

**Add IPv4 Static Route**

<b>IP Address</b>	<input type="text"/>
<b>Mask</b>	<input checked="" type="radio"/> Network Mask <input type="text"/> <input type="radio"/> Prefix Length <input type="text"/> (0 - 32)
<b>Next Hop Router IP Address</b>	<input type="text"/>
<b>Metric</b>	<input type="text" value="1"/> (1 - 255, default 1)

Los datos de la interfaz son los siguientes

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

### 13.1.3 ARP

Instrucciones:

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

ARP Entry Age Out

Sec (15 - 21600, default 1200)

Clear ARP Table Entries

All  
 Dynamic  
 Static  
 Normal Age Out

#### ARP Table

<input type="checkbox"/>	Interface	IP Address	MAC Address	Status
<input type="checkbox"/>	VLAN 1	192.168.0.20	00:e0:4c:2e:2c:dd	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.15	00:e0:4c:2e:2c:dd	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.71	04:d4:c4:49:63:fb	Dynamic
<input type="checkbox"/>	VLAN 1	192.168.1.80	b0:6e:bf:c6:dc:1a	Dynamic

---

#### Add ARP

Interface

VLAN

Note: Only interfaces with an valid IPv4 address are available for selection

IP Address

MAC Address

Los datos de la interfaz son los siguientes

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 a la configuración de la interfaz IPv6 de capa 3 de la siguiente manera:

IPv6 Unicast Routing  Enable

#### IPv6 Interface Table

Interface	DHCPv6 Client			Auto Configuration	DAD Attempts
	Stateless	Information Refresh Time	Minimum Information Refresh Time		
0 results found.					

#### Add IPv6 Interface

**Interface**

VLAN

**Auto Configuration**

Enable

**DAD Attempts**

(0 - 600, default 1)

**DHCPv6 Client**

**Stateless**

Enable

**Information Refresh Time**

(86400 - 4294967294, default 86400)

**Minimum Information Refresh Time**

(600 - 4294967294, default 600)

Los datos de la interfaz son los siguientes

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:

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

### IPv6 Address Table

Interface VLAN 5 ▼

<input type="checkbox"/>	IPv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
<input type="checkbox"/>	Link Local	fe80::1e2a:a3ff:fe00:24	64	Tentative
<input type="checkbox"/>	Multicast	ff02::1		
<input type="checkbox"/>	Multicast	ff01::1		

---

### Add IPv6 Interface

**Interface** VLAN 5

**IPv6 Address Type**

Global

Link Local

**IPv6 Address**

**Prefix Length**  (3 - 128)

**EUI-64**  Enable



Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Interface	Interfaz VLANIF
IPv6 Address Type	Global: dirección IPv6 global Link 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:

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

**IPv6 Routing Table**

Q

<input type="checkbox"/>	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
0 results found.							

Add Edit Delete

---

**Add IPv6 Static Route**

<b>IPv6 Prefix</b>	<input type="text"/>	
<b>IPv6 Prefix Length</b>	<input type="text"/>	(0 - 128)
<b>Next Hop Router IP Address</b>	<input type="text"/>	
<b>Metric</b>	<input type="text" value="1"/>	(1 - 255, default 1)

Apply Close

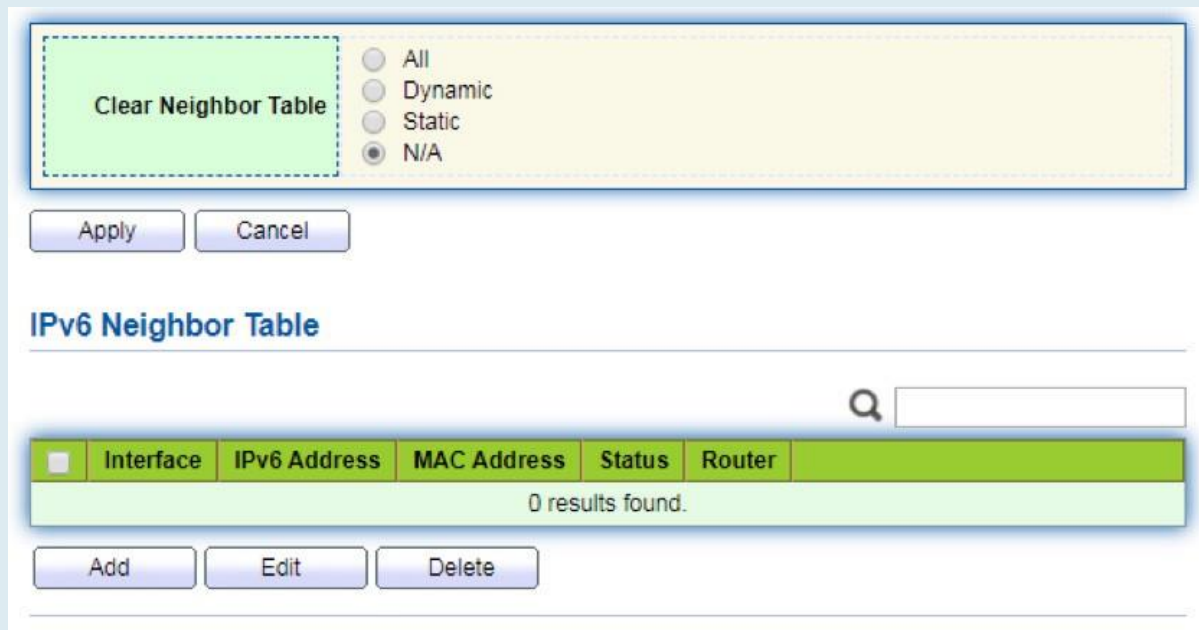
Los datos de la interfaz son los siguientes

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	Salto 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:



Clear Neighbor Table

All  
 Dynamic  
 Static  
 N/A

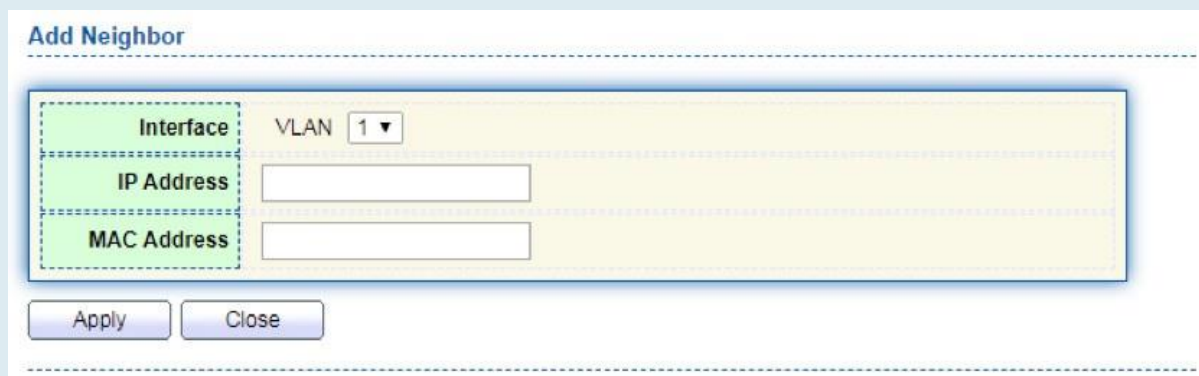
Apply Cancel

### IPv6 Neighbor Table

Q

<input type="checkbox"/>	Interface	IPv6 Address	MAC Address	Status	Router
0 results found.					

Add Edit Delete



### Add Neighbor

Interface VLAN

IP Address

MAC Address

Apply Close

Los datos de la interfaz son los siguientes

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 Elementos

# 14 Seguridad



## 14.1 RADIO

Instrucciones:

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

**Use Default Parameter**

Retry	<input type="text" value="3"/>	(1 - 10, default 3)
Timeout	<input type="text" value="3"/>	Sec (1 - 30, default 3)
Key String	<input type="text"/>	

**RADIUS Table**

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	Server Address	Server Port	Priority	Retry	Timeout	Usage
0 results found.						

**Add RADIUS Server**

Address Type	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
Server Address	<input type="text"/>
Server Port	<input type="text" value="1812"/> (0 - 65535, default 1812)
Priority	<input type="text"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Retry	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 10, default 3)
Timeout	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> Sec (1 - 30, default 3)
Usage	<input type="radio"/> Login <input type="radio"/> 802.1X <input checked="" type="radio"/> All

Los datos de la interfaz son los siguientes

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:

**Use Default Parameter**

**Timeout**

Sec (1 - 30, default 5)

**Key String**

### TACACS+ Table

Showing All entries
Showing 0 to 0 of 0 entries

☐	Server Address	Server Port	Priority	Timeout
0 results found.				

**Add TACACS+ Server**

---

<b>Address Type</b>	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Server Address</b>	<input type="text"/>
<b>Server Port</b>	<input type="text" value="49"/> (0 - 65535, default 49)
<b>Priority</b>	<input type="text"/> (0 - 65535)
<b>Key String</b>	<input checked="" type="checkbox"/> Use Default <input type="text"/>
<b>Timeout</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="5"/> Sec (1 - 30, default 5)

---

Los datos de la interfaz son los siguientes

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:

**Method List Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	Name	Sequence
<input type="checkbox"/>	default	(1) Local

**Add Method List**

Name

Method 1

- Empty
- None
- Local
- Enable
- RADIUS
- TACACS+

Method 2

- Empty
- None
- Local
- Enable
- RADIUS
- TACACS+

Method 3

- Empty
- None
- Local
- Enable
- RADIUS
- TACACS+

Method 4

- Empty
- None
- Local
- Enable
- RADIUS
- TACACS+

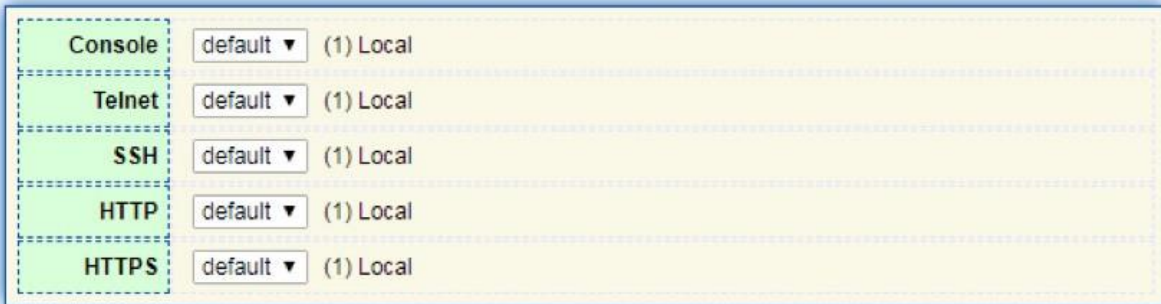
Los datos de la interfaz son los siguientes

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 autenticar Habilitar: Usar la base de datos de contraseñas de habilitación local para autenticar RADIUS: Usar el servidor Radius remoto para autenticar TACACS+: Usar el servidor remoto TACACS+ para autenticarse

## 14.3.2 Autenticación de inicio de sesión

Instrucciones:

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



Console default (1) Local

Telnet default (1) Local

SSH default (1) Local

HTTP default (1) Local

HTTPS default (1) Local


Apply

## 14.4 Acceso de administración

### 14.4.1 VLAN de administración

Instrucciones:

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



Management VLAN 1 - default

Note: Change Management VLAN may cause connection interrupted

Apply

## 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:

Management Service		
Telnet	<input checked="" type="checkbox"/>	Enable
SSH	<input type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input type="checkbox"/>	Enable
SNMP	<input type="checkbox"/>	Enable

Session Timeout		
Console	<input type="text" value="10"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

Instrucciones para SSH:

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

Management Service		
Telnet	<input type="checkbox"/>	Enable
SSH	<input checked="" type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input type="checkbox"/>	Enable
SNMP	<input type="checkbox"/>	Enable

Session Timeout		
Console	<input type="text" value="10"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)



Instrucciones para HTTPS:

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

Management Service		
Telnet	<input type="checkbox"/>	Enable
SSH	<input type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input checked="" type="checkbox"/>	Enable
SNMP	<input type="checkbox"/>	Enable

Session Timeout		
Console	<input type="text" value="10"/>	Min (0 - 65535, default 10)
Telnet	<input type="text" value="10"/>	Min (0 - 65535, default 10)
SSH	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTP	<input type="text" value="10"/>	Min (0 - 65535, default 10)
HTTPS	<input type="text" value="10"/>	Min (0 - 65535, default 10)

Instrucciones para SNMP:

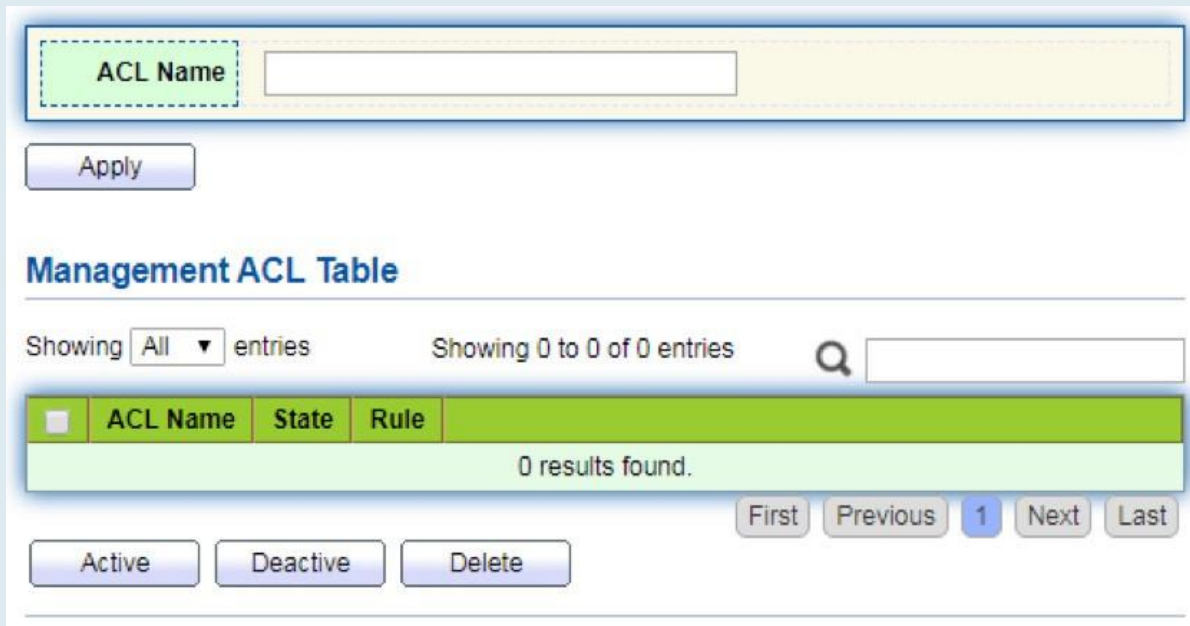
- Haga clic en "Security > Management Access > Management Service", ingrese a la interfaz del servicio de administración de la siguiente manera:

Management Service		
Telnet	<input type="checkbox"/>	Enable
SSH	<input type="checkbox"/>	Enable
HTTP	<input checked="" type="checkbox"/>	Enable
HTTPS	<input type="checkbox"/>	Enable
SNMP	<input checked="" type="checkbox"/>	Enable

### 14.4.3 ACL de administración

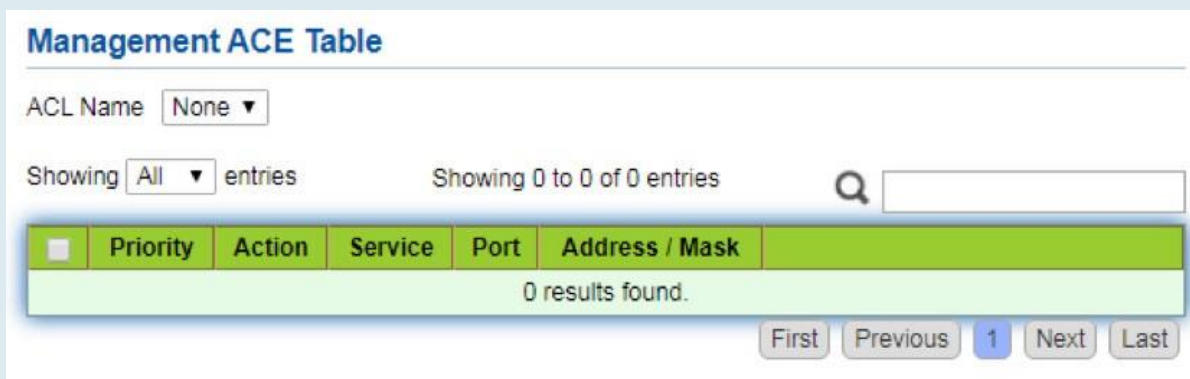
ACLs aplicado a las instrucciones de gestión:

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



The screenshot shows the 'Management ACL Table' interface. At the top, there is a text input field labeled 'ACL Name' with a dashed border, followed by an 'Apply' button. Below this is the title 'Management ACL Table'. The interface includes a filter section with 'Showing All entries' and 'Showing 0 to 0 of 0 entries', along with a search icon and a search input field. A table with a green header is shown, containing the text '0 results found.'. Below the table are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'. At the bottom, there are three buttons: 'Active', 'Deactive', and 'Delete'.

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



The screenshot shows the 'Management ACE Table' interface. At the top, there is a dropdown menu for 'ACL Name' set to 'None'. Below this is the title 'Management ACE Table'. The interface includes a filter section with 'Showing All entries' and 'Showing 0 to 0 of 0 entries', along with a search icon and a search input field. A table with a green header is shown, containing the text '0 results found.'. Below the table are navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

**Add Management ACE**

<b>ACL Name</b>	a	
<b>Priority</b>	1	(1 - 65535)
<b>Service</b>	<input type="radio"/> All <input type="radio"/> Http <input type="radio"/> Https <input checked="" type="radio"/> Snmp <input type="radio"/> SSH <input type="radio"/> Telnet	
<b>Action</b>	<input type="radio"/> Permit <input checked="" type="radio"/> Deny	
<b>Port</b>	Available Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	Selected Port  
<b>IP Version</b>	<input checked="" type="radio"/> All <input type="radio"/> IPv4 <input type="radio"/> IPv6	
<b>IPv4</b>	/ 255.255.255.255	
<b>IPv6</b>	/ 128 (1 - 128)	

Apply Close

Los datos de la interfaz son los siguientes

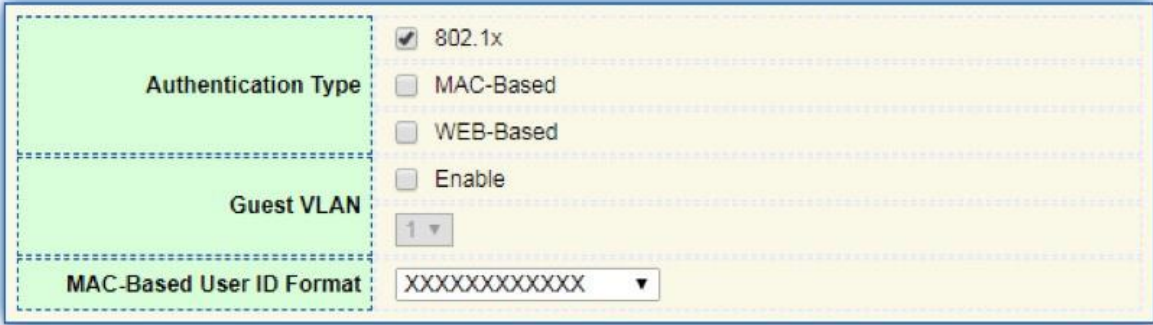
Elementos de configuración	Descripción
ACL Name	Nombre de ACL
Priority	Prioridad de ACL
Service	Tipo de servicio utilizado
Action	Acción del partido
Port	El puerto en el que se aplica esta ACL
IP Version	Administrar la versión de la dirección IP
IPv4	Dirección IPv4
IPv6	Dirección IPv6

## 14.5 Administrador de autenticación

### 14.5.1 Propiedad

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

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



**Authentication Type**

- 802.1x
- MAC-Based
- WEB-Based

**Guest VLAN**

- Enable
- 1

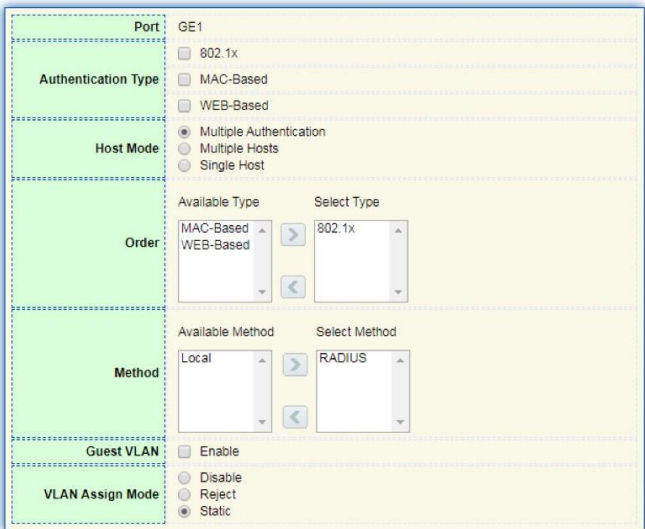
**MAC-Based User ID Format**

- XXXXXXXXXXXX

Apply

Port Mode Table

Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode	
		802.1x	MAC-Based	WEB-Based						
<input type="checkbox"/>	1	GE1	Enabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static



**Port** GE1

**Authentication Type**

- 802.1x
- MAC-Based
- WEB-Based

**Host Mode**

- Multiple Authentication
- Multiple Hosts
- Single Host

**Order**

Available Type: MAC-Based, WEB-Based | Select Type: 802.1x

**Method**

Available Method: Local | Select Method: RADIUS

**Guest VLAN**

- Enable

**VLAN Assign Mode**

- Disable
- Reject
- Static

Apply Close

Los datos de la interfaz son los siguientes

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. Single Host: 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:

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

Port Setting Table

Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters			Web-Based Parameters	
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
<input type="checkbox"/>	1 GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	2 GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	3 GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	4 GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	5 GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	6 GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	7 GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
<input type="checkbox"/>	8 GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

**Edit Port Setting**

Port: GE1-GE2

**Port Control**

Disabled  
 Force Authorized  
 Force Unauthorized  
 Auto

**Reauthentication**

Enable

**Max Hosts**

256 (1 - 256, default 256)

**Common Timer**

**Reauthentication**

3600 Sec (300 - 2147483647, default 3600)

**Inactive**

60 Sec (60 - 65535, default 60)

**Quiet**

60 Sec (0 - 65535, default 60)

**802.1x Parameters**

**TX Period**

30 Sec (1 - 65535, default 30)

**Supplicant Timeout**

30 Sec (1 - 65535, default 30)

**Server Timeout**

30 Sec (1 - 65535, default 30)

**Max Request**

2 (1 - 10, default 2)

**Web-Based Parameters**

Infinite

**Max Login**

3 (3 - 10, default 3)

Apply Close

Los datos de la interfaz son los siguientes

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 automáticos: necesitan pasar el procedimiento de autenticación para obtener accesibilidad de red
Reauthentication	Habilitar la Re autenticación de puertos
Max Hosts	El número máximo de hosts del puerto para el modo de autenticación múltiple
Reauthentication	El valor del período de Re autenticación del puerto con una unidad de segundo si la base de datos local o el servidor de autenticación remota no asignan el tiempo de Re autenticación
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
Inicio de sesión máximo	El valor numérico de intento de inicio de sesión máximo de autenticación WEB del puerto WEB

### 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:

**MAC-Based Local Account Table**

Showing  entries      Showing 0 to 0 of 0 entries     

MAC Address	Control	VLAN	Timeout (Sec)	
			Reauthentication	Inactive
0 results found.				

### 14.5.4 Cuenta local basada en web

Instrucciones:

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

**WEB-Based Local Account Table**

Showing  entries      Showing 0 to 0 of 0 entries     

Username	VLAN	Timeout (Sec)	
		Reauthentication	Inactive
0 results found.			

### 14.5.5 Sesiones

Instrucciones:

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

**Sessions Table**

Showing  entries      Showing 0 to 0 of 0 entries     

Session ID	Port	MAC Address	Current Type	Status	Operational Information				Authorized Information		
					VLAN	Session Time	Inactivated Time	Quiet Time	VLAN	Reauthentication Period	Inactive Timeout
0 results found.											

## 14.6 DoS

### 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.

POD	<input checked="" type="checkbox"/>	Enable
Land	<input checked="" type="checkbox"/>	Enable
UDP Blat	<input checked="" type="checkbox"/>	Enable
TCP Blat	<input checked="" type="checkbox"/>	Enable
DMAC = SMAC	<input checked="" type="checkbox"/>	Enable
Null Scan Attack	<input checked="" type="checkbox"/>	Enable
X-Mas Scan Attack	<input checked="" type="checkbox"/>	Enable
TCP SYN-FIN Attack	<input checked="" type="checkbox"/>	Enable
TCP SYN-RST Attack	<input checked="" type="checkbox"/>	Enable
ICMP Fragment	<input checked="" type="checkbox"/>	Enable
TCP-SYN	<input checked="" type="checkbox"/>	Enable Note: Source Port < 1024
TCP Fragment	<input checked="" type="checkbox"/>	Enable Note: Offset = 1
Ping Max Size	<input checked="" type="checkbox"/>	Enable IPv4
	<input checked="" type="checkbox"/>	Enable IPv6
	<input type="text" value="512"/>	Byte (0 - 65535, default 512)
TCP Min Hdr size	<input checked="" type="checkbox"/>	Enable
	<input type="text" value="20"/>	Byte (0 - 31, default 20)
IPv6 Min Fragment	<input checked="" type="checkbox"/>	Enable
	<input type="text" value="1240"/>	Byte (0 - 65535, default 1240)
Smurf Attack	<input checked="" type="checkbox"/>	Enable
	<input type="text" value="0"/>	Netmask Length (0 - 32, default 0)

Apply

### 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:

**Port Setting Table**

<input type="checkbox"/>	Entry	Port	State
<input type="checkbox"/>	1	GE1	Disabled
<input type="checkbox"/>	2	GE2	Disabled
<input type="checkbox"/>	3	GE3	Disabled
<input type="checkbox"/>	4	GE4	Disabled



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

**Edit Port Setting**

<b>Port</b>	GE1
<b>State</b>	<input checked="" type="checkbox"/> Enable

## 14.7 Inspección ARP dinámica

### 14.7.1 Propiedad

Instrucciones

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

<b>State</b>	<input type="checkbox"/> Enable	
<b>VLAN</b>	<b>Available VLAN</b>	<b>Selected VLAN</b>
	VLAN 1 VLAN 5	

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

### Port Setting Table

<input type="checkbox"/>	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited

### Edit Port Setting

<b>Port</b>	GE1-GE2
<b>Trust</b>	<input type="checkbox"/> Enable
<b>Source MAC Address</b>	<input type="checkbox"/> Enable
<b>Destination MAC Address</b>	<input type="checkbox"/> Enable
<b>IP Address</b>	<input type="checkbox"/> Enable <input type="checkbox"/> Allow Zero (0.0.0.0)
<b>Rate Limit</b>	<input type="text" value="0"/> pps (1 - 50, default 0), 0 is Unlimited

## 14.7.2 Estadística

Instrucciones

- Haga clic en "Security > Dynamic ARP Inspection > Statistics" (Estadísticas de inspección ARP dinámicas) vea las estadísticas de DAI de la siguiente manera:

### Statistics Table

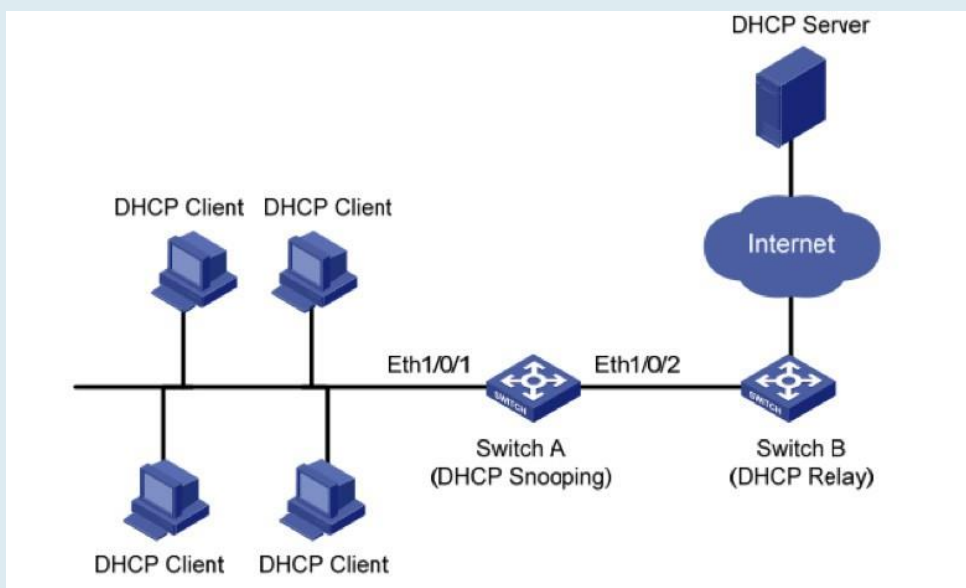
<input type="checkbox"/>	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
<input type="checkbox"/>	1	GE1	0	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0	0
<input type="checkbox"/>	8	GE8	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 monitor 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 divide los puertos en Puerto de confianza y Puerto no confiable.

El puerto de confianza conecta directa o indirectamente el servidor DHCP legal. Reenvía los 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 es de confianza 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 del mensaje DHCPREQUEST
- Snooping del mensaje DHCPACK

### 14.8.1 Propiedad

Habilite las instrucciones de espionaje DHCP:

1. Haga clic en la "Propiedad > de espionaje de seguridad > DHCP". La interfaz DHCP Snooping 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:

**State**  Enable

**VLAN**

Available VLAN: VLAN 1, VLAN 10, VLAN 100

Selected VLAN:

Apply

### Port Setting Table

<input type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input type="checkbox"/>	1	GE1	Disabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	Disabled	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	Disabled	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	Disabled	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	Disabled	Unlimited

### Edit Port Setting

**Port** GE1-GE2

**Trust**  Enable

**Verify Chaddr**  Enable

**Rate Limit**  pps (1 - 300, default 0), 0 is Unlimited

Apply Close

Los datos de la interfaz son los siguientes

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

### Port Setting Table

<input type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input type="checkbox"/>	1	GE1	Enabled	Enabled	100
<input type="checkbox"/>	2	GE2	Enabled	Enabled	100
<input type="checkbox"/>	3	GE3	Disabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	Disabled	Unlimited

## 14.8.2 Estadística

Instrucciones

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

### Statistics Table

<input type="checkbox"/>	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
<input type="checkbox"/>	1	GE1	0	0	0	0	0
<input type="checkbox"/>	2	GE2	0	0	0	0	0
<input type="checkbox"/>	3	GE3	0	0	0	0	0
<input type="checkbox"/>	4	GE4	0	0	0	0	0
<input type="checkbox"/>	5	GE5	0	0	0	0	0
<input type="checkbox"/>	6	GE6	0	0	0	0	0
<input type="checkbox"/>	7	GE7	0	0	0	0	0

### 14.8.3 Propiedad Opción82

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 switch 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.

- El puerto de no Confianza 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 registra la 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.

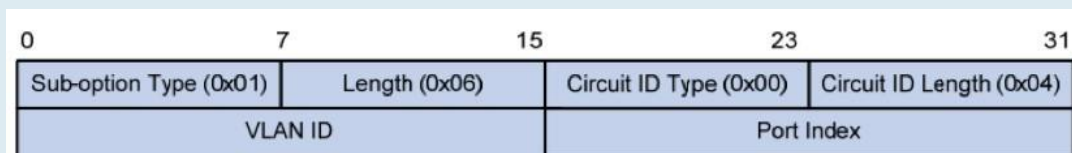
En la opción 82 figuran hasta 255 sub opciones. Se debe definir al menos una sub opción si se quiere definir Option 82. El dispositivo actual admite 2 sub opciones: Sub opción de ID de circuito y Sub opción de ID remoto.

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 ofrece los formatos de relleno extendidos para las sub opciones de la opción 82 y los valores predeterminados de relleno son los siguientes:

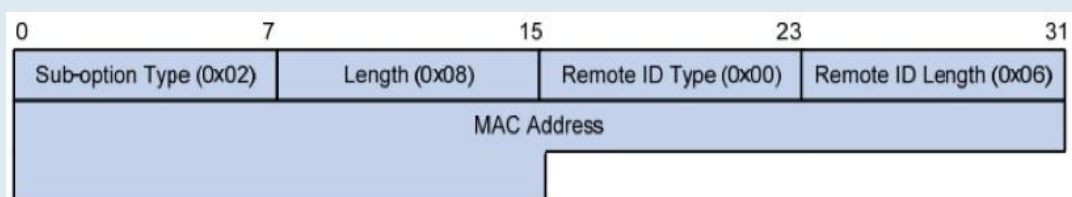
- Sub opción 1: VLAN No. y el índice de puerto (número físico del puerto menos 1) del puerto que recibe el mensaje de solicitud enviado por el cliente DHCP.

- Sub opción 2: dirección MAC puente del dispositivo de retransmisión DHCP que recibe el mensaje de solicitud de cliente DHCP.

Sub opción 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.



Sub opción 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 directivas de configuración (descartar, reemplazar con la opción 82 de retransmisión o mantener la opción 82 original) y, a continuación, reenviarla al servidor DHCP.

- 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.

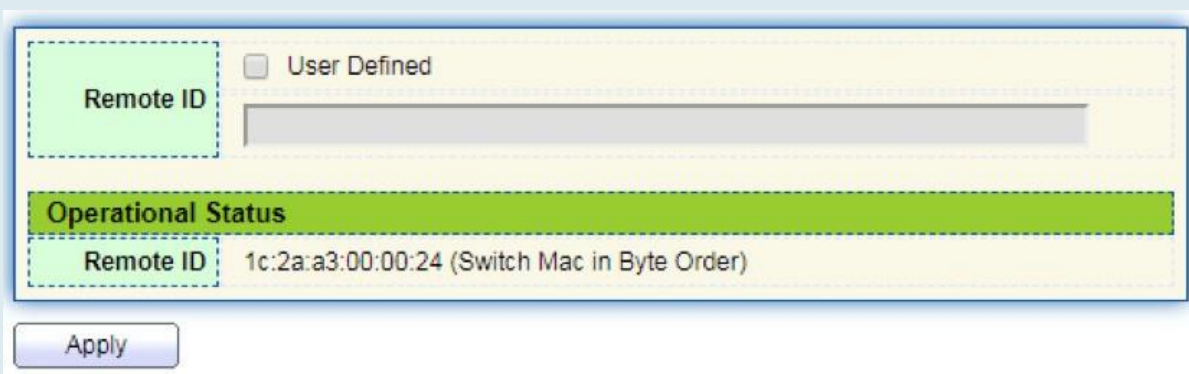
### Descripción:

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 configurado con las funciones DHCP 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 sub opciones.

### Instrucciones:

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



The screenshot shows a configuration window for DHCP Snooping Option 82. It includes a 'Remote ID' field with a 'User Defined' checkbox, an 'Operational Status' bar, and a 'Remote ID' field containing the MAC address '1c:2a:a3:00:00:24 (Switch Mac in Byte Order)'. An 'Apply' button is located at the bottom.

### Port Setting Table

<input type="checkbox"/>	Entry	Port	State	Allow Untrust
<input type="checkbox"/>	1	GE1	Disabled	Drop
<input type="checkbox"/>	2	GE2	Disabled	Drop
<input type="checkbox"/>	3	GE3	Disabled	Drop
<input type="checkbox"/>	4	GE4	Disabled	Drop
<input type="checkbox"/>	5	GE5	Disabled	Drop
<input type="checkbox"/>	6	GE6	Disabled	Drop
<input type="checkbox"/>	7	GE7	Disabled	Drop

### Edit Port Setting

<b>Port</b>	GE1-GE2
<b>State</b>	<input type="checkbox"/> Enable
<b>Allow Untrust</b>	<input type="radio"/> Keep
	<input checked="" type="radio"/> Drop
	<input type="radio"/> Replace

Los datos de la interfaz son los siguientes

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	Puerto que no confía 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 de acuerdo con la configuración del ID del circuito



**Descripción:**

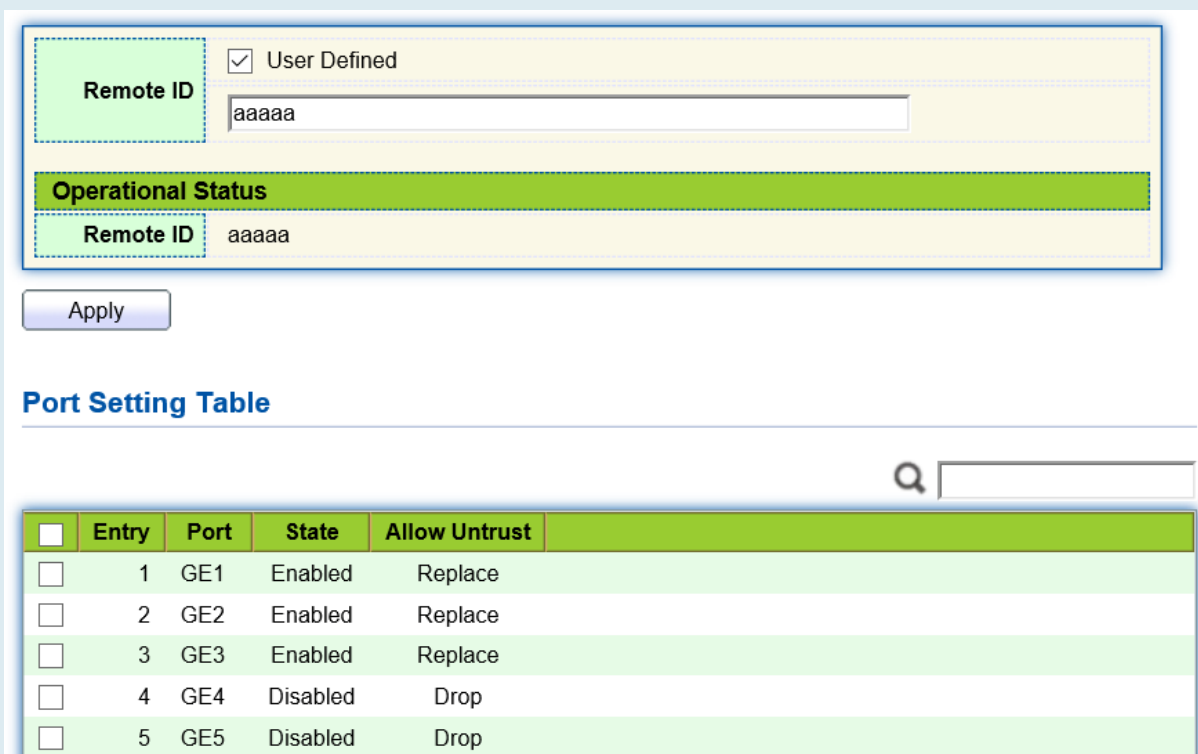
El campo de opción 82 configura independientemente las sub opciones de ID de circuito o ID remoto.

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 DHCP enviados 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. Rellene los elementos de configuración correspondientes.
3. "Aplicar" y terminar de la siguiente manera.



**Remote ID**  User Defined

aaaaa

**Operational Status**

**Remote ID** aaaaa

Apply

**Port Setting Table**

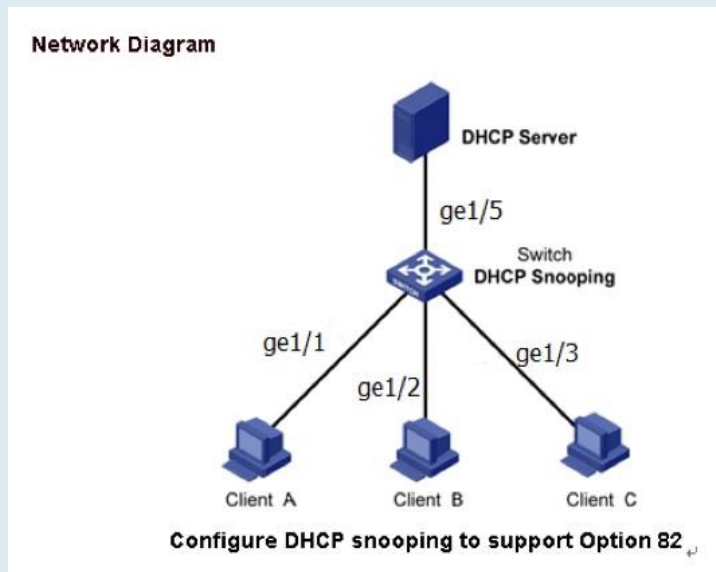
Q

<input type="checkbox"/>	Entry	Port	State	Allow Untrust
<input type="checkbox"/>	1	GE1	Enabled	Replace
<input type="checkbox"/>	2	GE2	Enabled	Replace
<input type="checkbox"/>	3	GE3	Enabled	Replace
<input type="checkbox"/>	4	GE4	Disabled	Drop
<input type="checkbox"/>	5	GE5	Disabled	Drop

**Ilustración de la configuración típica de DHCP Snooping**

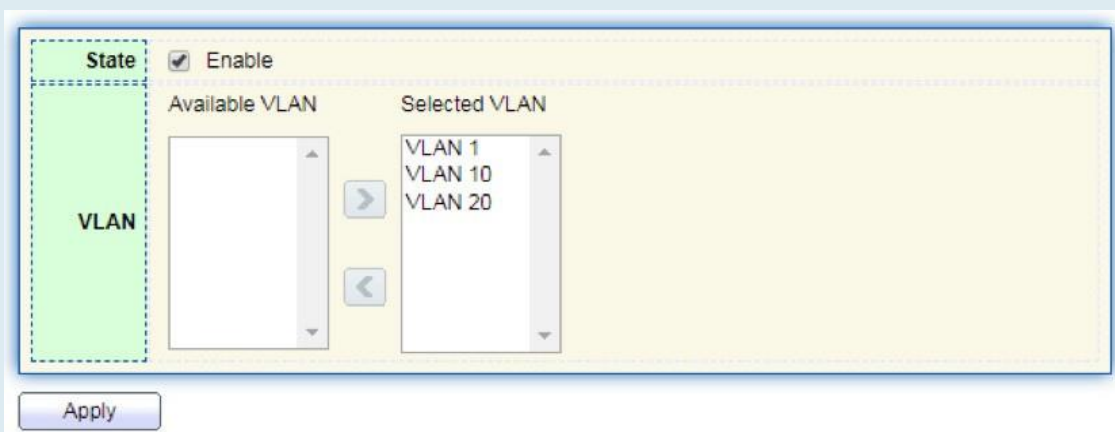
Como se muestra a continuación, el puerto del conmutador GE1-5 está conectado al servidor DHCP y los puertos GE1-1, 2 y 3 están conectados al cliente DHCP A, B y C respectivamente.

- Habilite DHCP Snooping en el switch.
- Establezca el GE1-5 como el puerto Trust 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.



Instrucciones:

1. Habilite el snooping DHCP del conmutador. Haga clic en la "Propiedad de > de espionaje DHCP > seguridad" en la barra de navegación para habilitar la función de la siguiente manera:



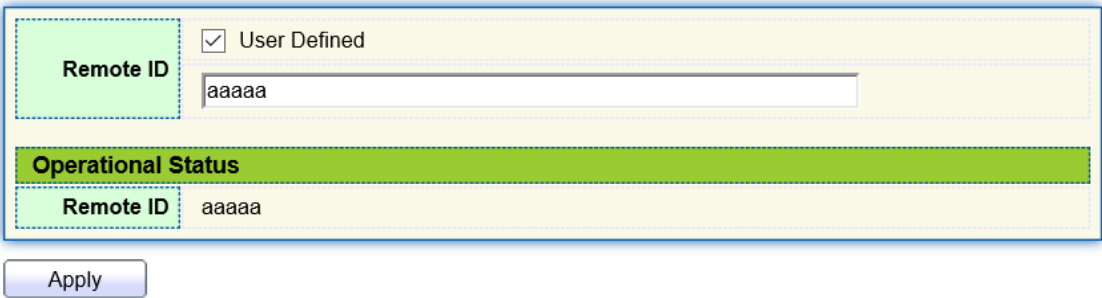
2. Establezca el GE1-5 como el puerto de confianza de DHCP Snooping, complete las configuraciones correspondientes y "Editar" de la siguiente manera:

#### Port Setting Table

<input type="checkbox"/>	Entry	Port	Trust	Verify Chaddr	Rate Limit
<input type="checkbox"/>	1	GE1	Enabled	Disabled	Unlimited
<input type="checkbox"/>	2	GE2	Enabled	Disabled	Unlimited
<input type="checkbox"/>	3	GE3	Enabled	Disabled	Unlimited
<input type="checkbox"/>	4	GE4	Enabled	Disabled	Unlimited
<input type="checkbox"/>	5	GE5	Enabled	Disabled	Unlimited

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

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



**Remote ID**  User Defined

aaaaa

**Operational Status**

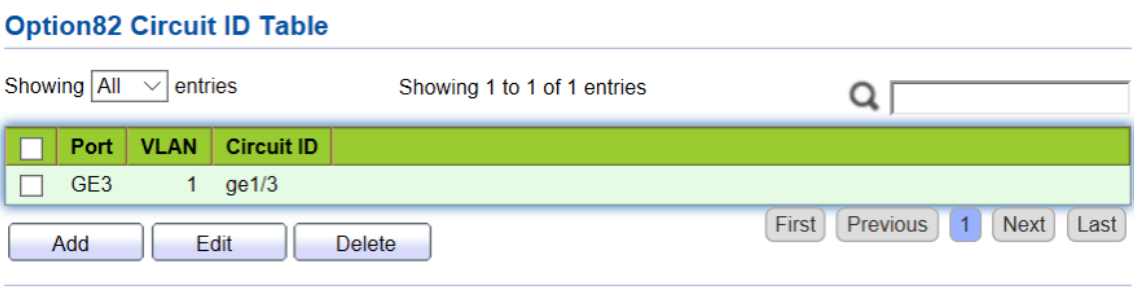
**Remote ID** aaaaa

Apply

**Port Setting Table**

Entry	Port	State	Allow Untrust
<input type="checkbox"/> 1	GE1	Disabled	Drop
<input type="checkbox"/> 2	GE2	Disabled	Drop
<input type="checkbox"/> 3	GE3	Enabled	Replace
<input type="checkbox"/> 4	GE4	Disabled	Drop
<input type="checkbox"/> 5	GE5	Disabled	Drop

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



**Option82 Circuit ID Table**

Showing All entries Showing 1 to 1 of 1 entries

Port	VLAN	Circuit ID
GE3	1	ge1/3

Add Edit Delete First Previous 1 Next Last

## 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 asegurar 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

Instrucciones

- Haga clic en "Security > IP Source Guard > Port Setting" ingrese a la interfaz de configuración del puerto de la siguiente manera:

**Port Setting Table**

<input type="checkbox"/>	Entry	Port	State	Verify Source	Current Entry	Max Entry
<input type="checkbox"/>	1	GE1	Disabled	IP	0	Unlimited
<input type="checkbox"/>	2	GE2	Disabled	IP	0	Unlimited
<input type="checkbox"/>	3	GE3	Disabled	IP	0	Unlimited
<input type="checkbox"/>	4	GE4	Disabled	IP	0	Unlimited
<input type="checkbox"/>	5	GE5	Disabled	IP	0	Unlimited
<input type="checkbox"/>	6	GE6	Disabled	IP	0	Unlimited
<input type="checkbox"/>	7	GE7	Disabled	IP	0	Unlimited
<input type="checkbox"/>	8	GE8	Disabled	IP	0	Unlimited

**Edit Port Setting**

<b>Port</b>	GE1-GE2
<b>State</b>	<input type="checkbox"/> Enable
<b>Verify Source</b>	<input checked="" type="radio"/> IP <input type="radio"/> IP-MAC
<b>Max Entry</b>	<input type="text" value="0"/> (1 - 50, default 0), 0 is Unlimited

Los datos de la interfaz son los siguientes

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 estáticas MAC 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 pueden fluir los mensajes de entradas MAC estáticas configuradas por los administradores, mientras que otros se descartarán.

Instrucciones:

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

**IP-MAC-Port-VLAN Binding Table**

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.							

**Add IP-MAC-Port-VLAN Binding**

<b>Port</b>	<input type="text" value="GE1"/>
<b>VLAN</b>	<input type="text" value=""/> (1 - 4094)
<b>Binding</b>	<input checked="" type="radio"/> IP-MAC-Port-VLAN <input type="radio"/> IP-Port-VLAN
<b>MAC Address</b>	<input type="text"/>
<b>IP Address</b>	<input type="text"/> / <input type="text" value="255.255.255.255"/>

Los datos de la interfaz son los siguientes

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

**IP-MAC-Port-VLAN Binding Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
<input type="checkbox"/>	GE1	1	00:00:11:11:22:22	192.168.1.123 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A

4. Haga clic en "Security > IP Source Guard > Save Database" ingrese a la interfaz de la base de datos de la siguiente manera:

<b>Type</b>	<input checked="" type="radio"/> None <input type="radio"/> Flash <input type="radio"/> TFTP
<b>Filename</b>	<input type="text"/>
<b>Address Type</b>	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4
<b>Server Address</b>	<input type="text"/>
<b>Write Delay</b>	<input type="text" value="300"/> Sec (15 - 86400, default 300)
<b>Timeout</b>	<input type="text" value="300"/> Sec (0 - 86400, default 300)

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 (Access Control List) filtra los paquetes configurando las reglas de coincidencia de mensajes 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 coincidencia 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 de 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 clasifique los paquetes mediante condiciones coincidentes, 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 siguientes categorías según los fines 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 y la información de capa 3 o 4, como las características de protocolo. El ID de ACL varía de 100 a 999.

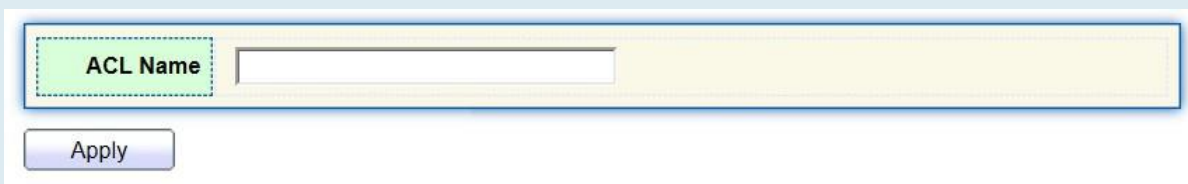
ACL L2: Las reglas se realizan de acuerdo con la dirección MAC de origen/destino de los paquetes, la prioridad 802.1p y la información L2, como el tipo de protocolo. El ID de ACL varía de 1 a 99.

## 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 la barra de navegación de la siguiente manera.



The screenshot shows a configuration window with a yellow background. At the top, there is a label 'ACL Name' next to a text input field. Below the input field is a button labeled 'Apply'.

Los datos de la interfaz son los siguientes

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

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

**ACE Table**

ACL Name

Showing  entries      Showing 0 to 0 of 0 entries

	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p		
			Address	Mask	Address	Mask			Value	Mask	
0 results found.											

Los datos de la interfaz son los siguientes

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

3. Rellene los elementos de configuración correspondientes.

**Add ACE**

ACL Name	a	
Sequence	<input type="text" value="1"/>	(1 - 2147483647)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown	
Source MAC	<input type="checkbox"/> Any <input type="text" value="00:00:00:00:20:00"/> / <input type="text" value="FF:FF:FF:FF:FF:00"/> (Address / Mask)	
Destination MAC	<input type="checkbox"/> Any <input type="text" value="00:00:00:00:10:00"/> / <input type="text" value="FF:FF:FF:FF:FF:00"/> × (Address / Mask)	
Ethertype	<input checked="" type="checkbox"/> Any 0x <input type="text"/> (0x600 ~ 0xFFFF)	
VLAN	<input checked="" type="checkbox"/> Any <input type="text"/> (1 - 4094)	
802.1p	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Value / Mask) (0 - 7)	



Los datos de la interfaz son los siguientes

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	Introduzca 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 terminar de la siguiente manera.

**ACE Table**

ACL Name

Showing  entries      Showing 1 to 1 of 1 entries     

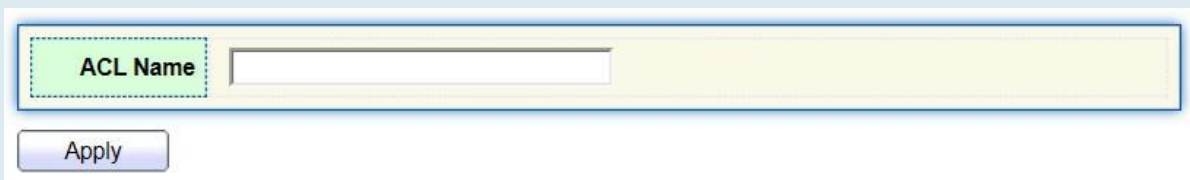
Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
		Address	Mask	Address	Mask			Value	Mask
<input type="checkbox"/>	1 Permit	00:00:00:00:20:00	FF:FF:FF:FF:FF:00	00:00:00:00:10:00	FF:FF:FF:FF:FF:00	Any	Any	Any	Any

## 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 de 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

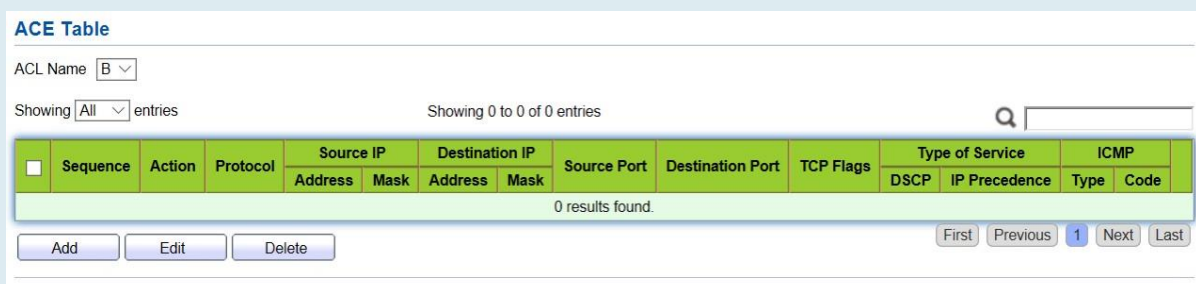
1. Haga clic en "ACL > IPv4 ACL" en la barra de navegación de la siguiente manera.



Los datos de la interfaz son los siguientes

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

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



Los datos de la interfaz son los siguientes

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

3. Rellene los elementos de configuración correspondientes.

### Add ACE

<b>ACL Name</b>	B
<b>Sequence</b>	100 (1 - 2147483647)
<b>Action</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
<b>Protocol</b>	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="ICMP"/> <small>▼</small> <input type="radio"/> Define <input type="text"/> (0 - 255)
<b>Source IP</b>	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
<b>Destination IP</b>	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Mask)
<b>Type of Service</b>	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text"/> (0 - 63) <input type="radio"/> IP Precedence <input type="text"/> (0 - 7)
<b>Source Port</b>	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)
<b>Destination Port</b>	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)
<b>TCP Flags</b>	Urg: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Ack: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Psh: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Rst: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Syn: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Fin: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care
<b>ICMP Type</b>	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="Echo Reply"/> <small>▼</small> <input type="radio"/> Define <input type="text"/> (0 - 255)
<b>ICMP Code</b>	<input checked="" type="radio"/> Any <input type="radio"/> Define <input type="text"/> (0 - 255)

Los datos de la interfaz son los siguientes

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 prioridad IP (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 sonó (0-65,535). Seleccione "Cualquiera" para representar cualquier puerto de seguridad.
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".
Tipo ICMP	Introduzca el tipo de mensaje ICMP de las reglas de ACL. Seleccione "Cualquiera" para representar cualquier tipo de ICMP.

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

**ACE Table**

ACL Name


Showing  entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	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
<input type="checkbox"/>	100	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		

## 15.3 ACL IPv6

### Instrucciones

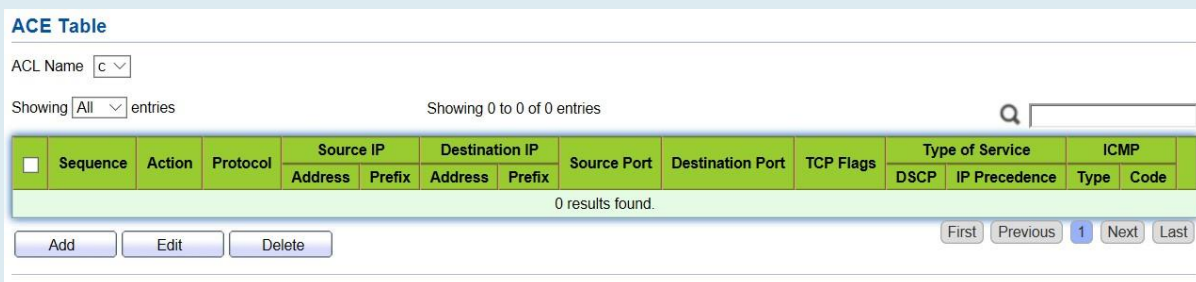
1. Haga clic en " ACL > IPv6 ACL" en la barra de navegación de la siguiente manera.



Los datos de la interfaz son los siguientes

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

2. Haga clic en "ACL > IPv6 ACE" en la barra de navegación, "Agregar" el nombre de ACL de la siguiente manera:



Los datos de la interfaz son los siguientes

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

3. Rellene los elementos de configuración correspondientes

### Add ACE

<b>ACL Name</b>	b
<b>Sequence</b>	100 (1 - 2147483647)
<b>Action</b>	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
<b>Protocol</b>	<input checked="" type="radio"/> Any <input type="radio"/> Select <input type="text" value="TCP"/> (0 - 255) <input type="radio"/> Define <input type="text"/> (0 - 255)
<b>Source IP</b>	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))
<b>Destination IP</b>	<input checked="" type="checkbox"/> Any <input type="text"/> / <input type="text"/> (Address / Prefix (0 - 128))
<b>Type of Service</b>	<input checked="" type="radio"/> Any <input type="radio"/> DSCP <input type="text"/> (0 - 63) <input type="radio"/> IP Precedence <input type="text"/> (0 - 7)
<b>Source Port</b>	<input type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)
<b>Destination Port</b>	<input type="radio"/> Any <input type="radio"/> Single <input type="text"/> (0 - 65535) <input type="radio"/> Range <input type="text"/> - <input type="text"/> (0 - 65535)
<b>TCP Flags</b>	Urg: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Ack: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Psh: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Rst: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Syn: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care Fin: <input type="radio"/> Set <input type="radio"/> Unset <input checked="" type="radio"/> Don't care
<b>ICMP Type</b>	<input type="radio"/> Any <input type="radio"/> Select <input type="text" value="Destination Unreachable"/> (0 - 255) <input type="radio"/> Define <input type="text"/> (0 - 255)
<b>ICMP Code</b>	<input checked="" type="radio"/> Any <input type="radio"/> Define <input type="text"/> (0 - 255)

Apply

Close

Los datos de la interfaz son los siguientes

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 prioridad IP (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", "Des establecer" 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 terminar de la siguiente manera.

**ACE Table**

ACL Name

Showing  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	Prefix	Address	Prefix				DSCP	IP Precedence	Type	Code
<input type="checkbox"/>	100	Permit	Any (IP)	Any	Any	Any				Any	Any		

## 15.4 Enlace de ACL

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

Instrucciones:

1. Haga clic en " ACL > ACL Binding" en la barra de navegación de la siguiente manera.

**ACL Binding Table**

<input type="checkbox"/>	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			

Los datos de la interfaz son los siguientes

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. Complete los elementos de configuración correspondientes, tomando como ejemplos la ACL a de MAC creada, la ACL b IPv4, la ACL c IPv6.
3. "Aplicar" y terminar de la siguiente manera.

**Add ACL Binding**

<b>Port</b>	GE3
	Note: ACL without any rules cannot be bound
<b>MAC ACL</b>	<input type="text" value="a"/>
<b>IPv4 ACL</b>	<input type="text" value="b"/>
<b>IPv6 ACL</b>	<input type="text" value="None"/>



QoS (Quality of Service) evalúa la capacidad de los proveedores de servicios para satisfacer las necesidades del cliente y la capacidad de transmitir paquetes a través de Internet. Los servicios diversificados pueden ser evaluado en base a 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 capacidad de transferencia, se refiere al flujo de carga promedio dentro de un cierto período de tiempo, con la unidad de Kbit/s. El retraso se refiere al tiempo promedio requerido para que la carga 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 tráfico de alta prioridad se puede servir tan pronto como sea posible mediante el método de programación de la cola de prioridad, mientras que el tráfico de baja prioridad obtiene servicios después de eso. La variación de retardo se refiere a la variación en tiempo que fluye el tráfico a través de la red. La tasa de paquetes se refiere al porcentaje de paquetes perdidos durante la transmisión. A pesar de que 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 causa más común de pérdida de información.

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 confiabilidad, el retraso de 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, video y otros servicios sensibles al retraso han establecido estándares más altos sobre el retraso de transmisión de mensajes. La transmisión de mensajes en un corto período ha sido la tendencia común. Para admitir servicios de voz, video y datos con diferentes requisitos, la red necesita identificar los tipos de negocio y proporcionar los servicios correspondientes.

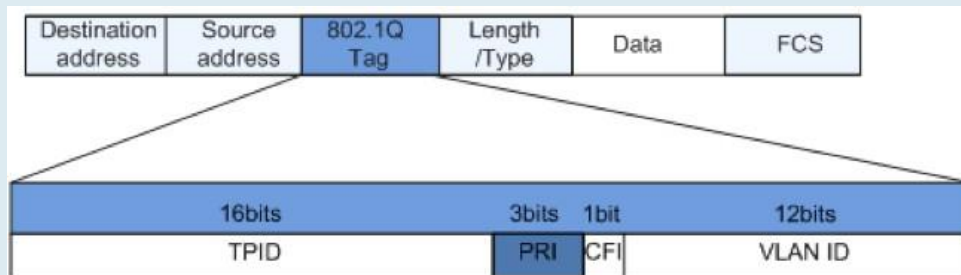
La capacidad de distinguir los tipos de paquetes es el requisito previo para proporcionar los servicios correspondientes, por lo que el servicio tradicional de mejor esfuerzo ya no satisface las necesidades de la aplicación. Por lo tanto, esa es la razón de QoS. Regula el flujo de la red para evitar 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 del servicio de 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 (Class of Service), 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, 802.1p priority), 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

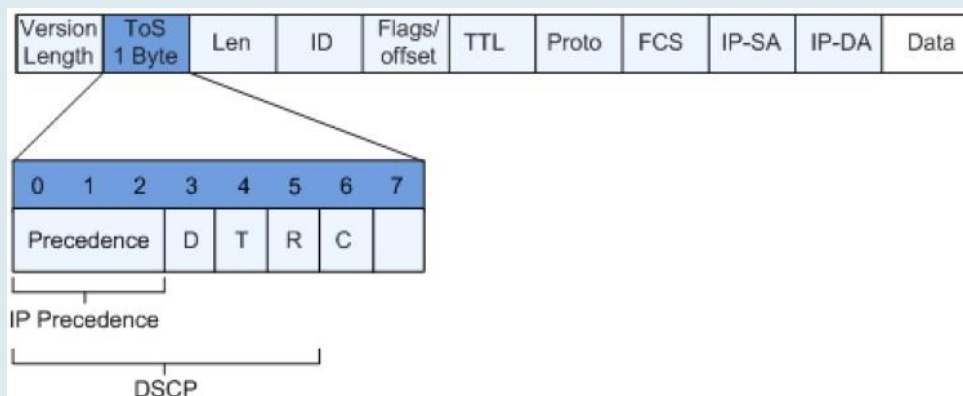


El encabezado 802.1Q contiene campos PRI de 3 bits. El campo PRI define 8 CoS de prioridad empresarial que van de 7 a 0 de mayor a menor.

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 la prioridad más alta 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 confiabilidad (0 para confiabilidad normal y 1 para alta confiabilidad). 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 los 0 a 5 bits del dominio ToS en el encabezado de mensaje IPv4 de RFC2474 como DSCP y le cambia el nombre como byte DS (servicio diferenciado) como se muestran 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 D.

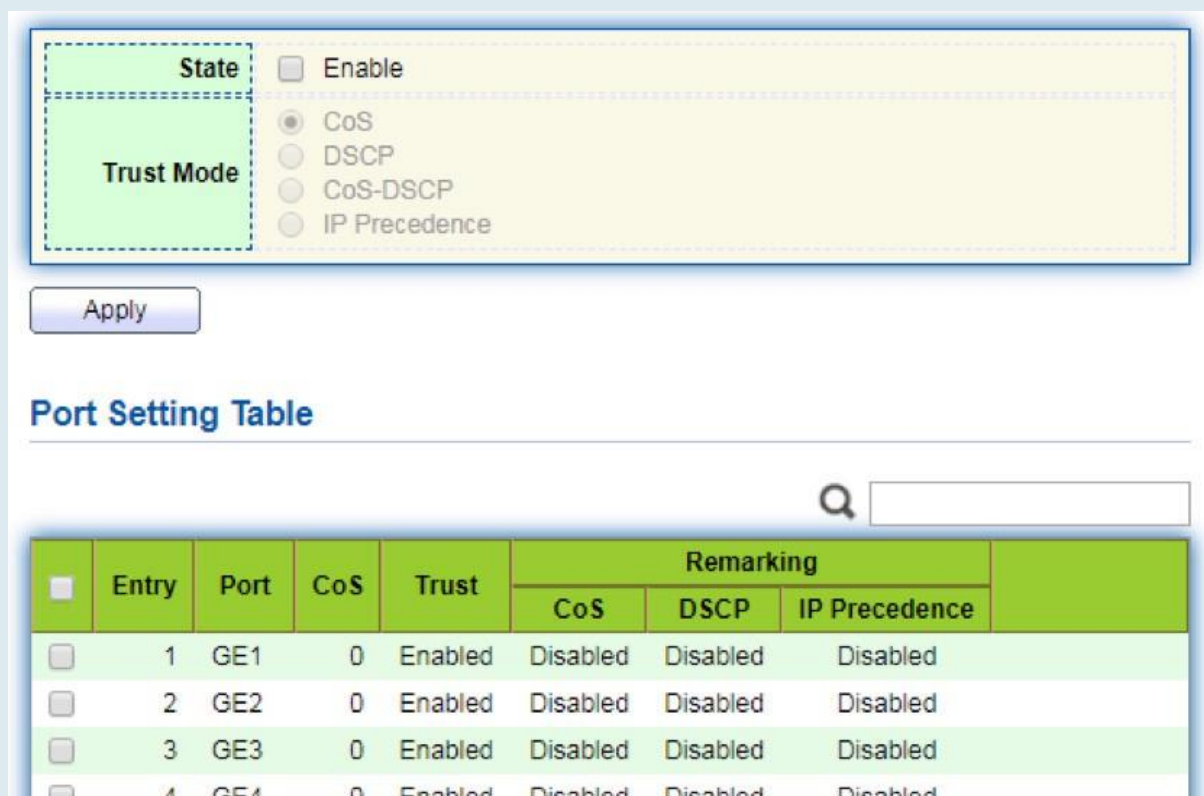
## 16.1 General

### 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 clic en "QoS > General > Property" en la barra de navegación de la siguiente manera.



The screenshot shows a configuration window with two main sections: 'State' and 'Trust Mode'. The 'State' section has an 'Enable' checkbox which is currently unchecked. The 'Trust Mode' section has four radio button options: 'CoS' (selected), 'DSCP', 'CoS-DSCP', and 'IP Precedence'. Below these options is an 'Apply' button. Underneath is a 'Port Setting Table' with a search bar. The table has columns for 'Entry', 'Port', 'CoS', 'Trust', and 'Remarking' (subdivided into 'CoS', 'DSCP', and 'IP Precedence').

	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
<input type="checkbox"/>	1	GE1	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	2	GE2	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	3	GE3	0	Enabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4	GE4	0	Enabled	Disabled	Disabled	Disabled

Los datos de la interfaz de la configuración del puerto 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

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

**Queue Scheduling Table**

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	<input checked="" type="radio"/>	<input type="radio"/>	1	
2	<input checked="" type="radio"/>	<input type="radio"/>	2	
3	<input checked="" type="radio"/>	<input type="radio"/>	3	
4	<input checked="" type="radio"/>	<input type="radio"/>	4	
5	<input checked="" type="radio"/>	<input type="radio"/>	5	
6	<input checked="" type="radio"/>	<input type="radio"/>	9	
7	<input checked="" type="radio"/>	<input type="radio"/>	13	
8	<input checked="" type="radio"/>	<input type="radio"/>	15	

Los datos de la interfaz son los siguientes

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

- Haga clic en "QoS > General > CoS Mapping" en la barra de navegación. "Aplicar" y terminar de la siguiente manera.

### CoS to Queue Mapping

CoS	Queue	
0	1 ▼	
1	2 ▼	
2	3 ▼	
3	4 ▼	
4	5 ▼	
5	6 ▼	
6	7 ▼	
7	8 ▼	

---

### Queue to CoS Mapping

Queue	CoS	
1	0 ▼	
2	1 ▼	
3	2 ▼	
4	3 ▼	
5	4 ▼	
6	5 ▼	
7	6 ▼	
8	7 ▼	

Los datos de la interfaz son los siguientes

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.

### DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 ▼	16 [CS2]	3 ▼	32 [CS4]	5 ▼	48 [CS6]	7 ▼
1	1 ▼	17	3 ▼	33	5 ▼	49	7 ▼
2	1 ▼	18 [AF21]	3 ▼	34 [AF41]	5 ▼	50	7 ▼
3	1 ▼	19	3 ▼	35	5 ▼	51	7 ▼
4	1 ▼	20 [AF22]	3 ▼	36 [AF42]	5 ▼	52	7 ▼
5	1 ▼	21	3 ▼	37	5 ▼	53	7 ▼
6	1 ▼	22 [AF23]	3 ▼	38 [AF43]	5 ▼	54	7 ▼
7	1 ▼	23	3 ▼	39	5 ▼	55	7 ▼
8 [CS1]	2 ▼	24 [CS3]	4 ▼	40 [CS5]	6 ▼	56 [CS7]	8 ▼
9	2 ▼	25	4 ▼	41	6 ▼	57	8 ▼
10 [AF11]	2 ▼	26 [AF31]	4 ▼	42	6 ▼	58	8 ▼
11	2 ▼	27	4 ▼	43	6 ▼	59	8 ▼
12 [AF12]	2 ▼	28 [AF32]	4 ▼	44	6 ▼	60	8 ▼
13	2 ▼	29	4 ▼	45	6 ▼	61	8 ▼
14 [AF13]	2 ▼	30 [AF33]	4 ▼	46 [EF]	6 ▼	62	8 ▼
15	2 ▼	31	4 ▼	47	6 ▼	63	8 ▼

Apply

### Queue to DSCP Mapping

Queue	DSCP
1	0 [CS0] ▼
2	8 [CS1] ▼
3	16 [CS2] ▼
4	24 [CS3] ▼
5	32 [CS4] ▼
6	40 [CS5] ▼
7	48 [CS6] ▼
8	56 [CS7] ▼

Apply

Los datos de la interfaz son los siguientes

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

## 16.1.5 Asignación de precedencia IP

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

### IP Precedence to Queue Mapping

IP Precedence	Queue
0	1 ▼
1	2 ▼
2	3 ▼
3	4 ▼
4	5 ▼
5	6 ▼
6	7 ▼
7	8 ▼

---

### Queue to IP Precedence Mapping

Queue	IP Precedence
1	0 ▼
2	1 ▼
3	2 ▼
4	3 ▼
5	4 ▼
6	5 ▼
7	6 ▼
8	7 ▼

Los datos de la interfaz son los siguientes

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:

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

**Ingress / Egress Port Table**

Entry	Port	Ingress		Egress	
		State	Rate (Kbps)	State	Rate (Kbps)
<input type="checkbox"/>	1 GE1	Disabled		Disabled	
<input type="checkbox"/>	2 GE2	Disabled		Disabled	
<input type="checkbox"/>	3 GE3	Disabled		Disabled	
<input type="checkbox"/>	4 GE4	Disabled		Disabled	
<input type="checkbox"/>	5 GE5	Disabled		Disabled	
<input type="checkbox"/>	6 GE6	Disabled		Disabled	
<input type="checkbox"/>	7 GE7	Disabled		Disabled	

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

**Edit Ingress / Egress Port**

<b>Port</b>	GE1-GE3
<b>Ingress</b>	<input checked="" type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)
<b>Egress</b>	<input checked="" type="checkbox"/> Enable <input type="text" value="1000000"/> Kbps (16 - 1000000)



Los datos de la interfaz son los siguientes

Elementos de configuración		Descripción
Ingress	Enabled	Switch de limitación de velocidad
	Rate	La tarifa oscila entre 16 y 1.000.000 Kbps
Egress	Enabled	Switch de limitación de velocidad
	Rate	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

- Haga clic en "QoS > Rate Limit > Egress Queue" en la barra de navegación de la siguiente manera.

Egress Queue Table

Q

Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8	
		State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
<input type="checkbox"/>	1 GE1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	2 GE2	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	3 GE3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	4 GE4	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	5 GE5	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	6 GE6	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	7 GE7	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	8 GE8	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

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

Edit Egress Queue

**Port** GE1-GE2

Enable

**Queue 1**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 2**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 3**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 4**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 5**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 6**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 7**  Enable  
1000000 Kbps (16 - 1000000)

**Queue 8**  Enable  
1000000 Kbps (16 - 1000000)

# 17 Diagnósticos



## 17.1 Registro

Configura el Switch 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 la barra de navegación para activar / deshabilitar los registros, seleccionar el terminal de salida, configurar el nivel de gravedad, etc. de la siguiente manera:

The screenshot shows a configuration page for logging. It includes the following sections:

- State:**  Enable
- Aggregation:**  Enable
- Aging Time:** 300 Sec (15 - 3600, default 300)
- Console Logging:**
  - State:  Enable
  - Minimum Severity: Notice (dropdown menu)
  - Note: Emergency, Alert, Critical, Error, Warning, Notice
- RAM Logging:**
  - State:  Enable
  - Minimum Severity: Notice (dropdown menu)
  - Note: Emergency, Alert, Critical, Error, Warning, Notice
- Flash Logging:**
  - State:  Enable
  - Minimum Severity: Notice (dropdown menu)
  - Note: Emergency, Alert, Critical, Error, Warning, Notice

An "Apply" button is located at the bottom of the form.

2. Haga clic en "Diagnóstico > registro > servidor remoto" en la barra de navegación para agregar y ver la configuración del servidor de la siguiente manera:

**Remote Server Table**

Search:

<input type="checkbox"/>	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					

Buttons: Add, Edit, Delete

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

**Add Remote Server**

<b>Address Type</b>	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Server Address</b>	<input type="text"/>
<b>Server Port</b>	<input type="text" value="514"/> (1 - 65535, default 514)
<b>Facility</b>	Local 7 ▾
<b>Minimum Severity</b>	<input type="text" value="Notice"/> ▾ Note: Emergency, Alert, Critical, Error, Warning, Notice

## 17.2 Ping

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

Instrucciones:

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

<b>Address Type</b>	<input type="radio"/> Hostname <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Server Address</b>	<input type="text" value="192.168.1.111"/>
<b>Count</b>	<input type="text" value="4"/> (1 - 65535)

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:

## Ping Result

Packet Status	
Status	Success.
Transmit Packet	4
Receive Packet	4
Packet Lost	0 %
Round Trip Time	
Min	0 ms
Max	0 ms
Average	0 ms

## 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 "Diagnóstico > Traceroute" en la barra de navegación para introducir un nombre de host o una dirección IP para definir el tiempo de existencia del mensaje de la siguiente manera:

Address Type	<input type="radio"/> Hostname <input checked="" type="radio"/> IPv4
Server Address	<input type="text" value="192.168.1.122"/>
Time to Live	<input type="checkbox"/> User Defined <input type="text" value="30"/> (2 - 255, default 30)

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

### Traceroute Result

```
tracert to 192.168.1.122 (192.168.1.122), 30 hops max, 38 byte packets
1 192.168.1.122 (192.168.1.122) 0.000 ms 0.000 ms 0.000 ms
```

## 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 "Diagnóstico > prueba de cobre " en la barra de navegación para seleccionar un puerto para la prueba de la siguiente manera:



2. Haga clic en "Copper Test" (Prueba de cobre)" y muestre el resultado de la siguiente manera:

### Copper Test Result

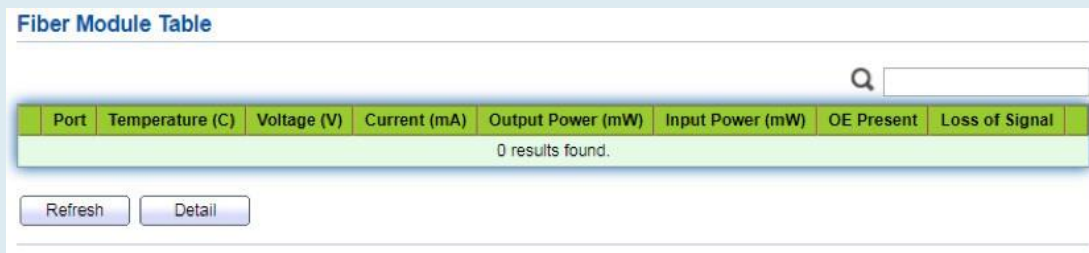
Cable Status	
Port	GE1
Result	Open Cable
Length	2.92 M

## 17.5 Módulo de fibra

Se puede utilizar para ver la información del módulo óptico DDM.

Instrucciones:

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



Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
0 results found.							

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

Configuración global y de conmutador de puerto

Instrucciones:

1. Haga clic en "Diagnóstico > propiedad > UDLD" en la barra de navegación para seleccionar un puerto para la prueba de la siguiente manera:

**Message Time**  Sec (1 - 90, default 15)

**Port Setting Table**

Q

<input type="checkbox"/>	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
<input type="checkbox"/>	1	GE1	Disabled	Unknown		0
<input type="checkbox"/>	2	GE2	Disabled	Unknown		0
<input type="checkbox"/>	3	GE3	Disabled	Unknown		0
<input type="checkbox"/>	4	GE4	Disabled	Unknown		0
<input type="checkbox"/>	5	GE5	Disabled	Unknown		0
<input type="checkbox"/>	6	GE6	Disabled	Unknown		0

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

**Edit Port Setting**

**Port**

**Mode**

Disabled

Normal

Aggressive

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
Port	ID de puerto
Mode	<p>Modo de puerto UDLD</p> <p>Deshabilitado: Desactivar la función de puerto</p> <p>Normal: UDLD puede detectar vínculos unidireccionales y marcar el puerto como indeterminado para generar registros del sistema</p> <p>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 deshabilitado de error.</p>

## 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 experiencia 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 "Diagnóstico > UDLD > vecino" en la barra de navegación para seleccionar un puerto para la prueba de la siguiente manera:



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

Elementos de configuración	Descripción
Entry	Nº de serie de vecino
Current Neighbor State	Tiempo restante de envejecimiento
Device ID	Situación de los vecinos
Device Name	Id. de 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

Instrucciones:

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

Instrucciones:

1. Haga clic en "Administración > cuenta de usuario" en la barra de navegación para descubrir el nombre de usuario de "admin" y el privilegio de "Admin" de forma predeterminada de la siguiente manera:

**User Account**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	Username	Privilege
<input type="checkbox"/>	admin	Admin

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

**Add User Account**

Username:

Password:

Confirm Password:

Privilege:  Admin    User

**Edit User Account**

Username: admin

Password:

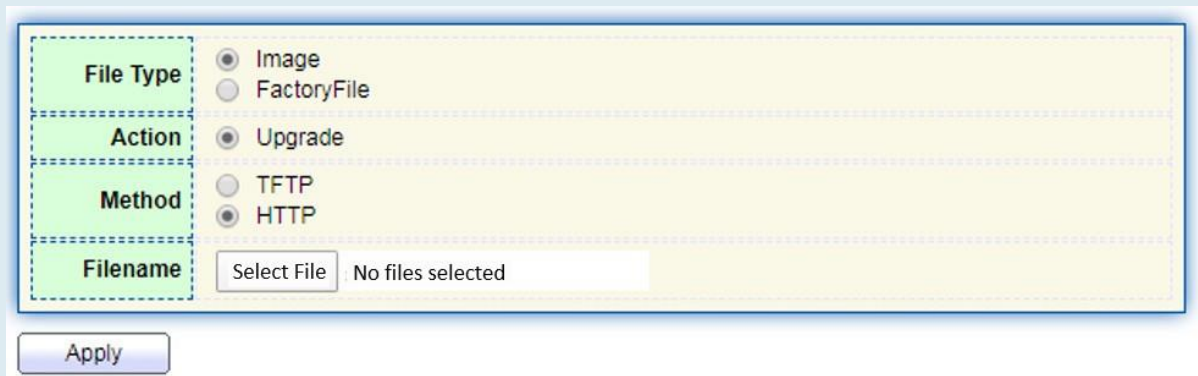
Confirm Password:

Privilege:  Admin    User

## 18.2 Firmware

Instrucciones para la actualización de la versión del firmware del sistema:

1. Haga clic en "Management > Firmware > Upgrade" en la barra de navegación de la siguiente manera:



The screenshot shows a configuration form for firmware upgrade. It has four sections: File Type, Action, Method, and Filename. Below the form is an 'Apply' button.

<b>File Type</b>	<input checked="" type="radio"/> Image <input type="radio"/> FactoryFile
<b>Action</b>	<input checked="" type="radio"/> Upgrade
<b>Method</b>	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
<b>Filename</b>	<input type="button" value="Select File"/> No files selected

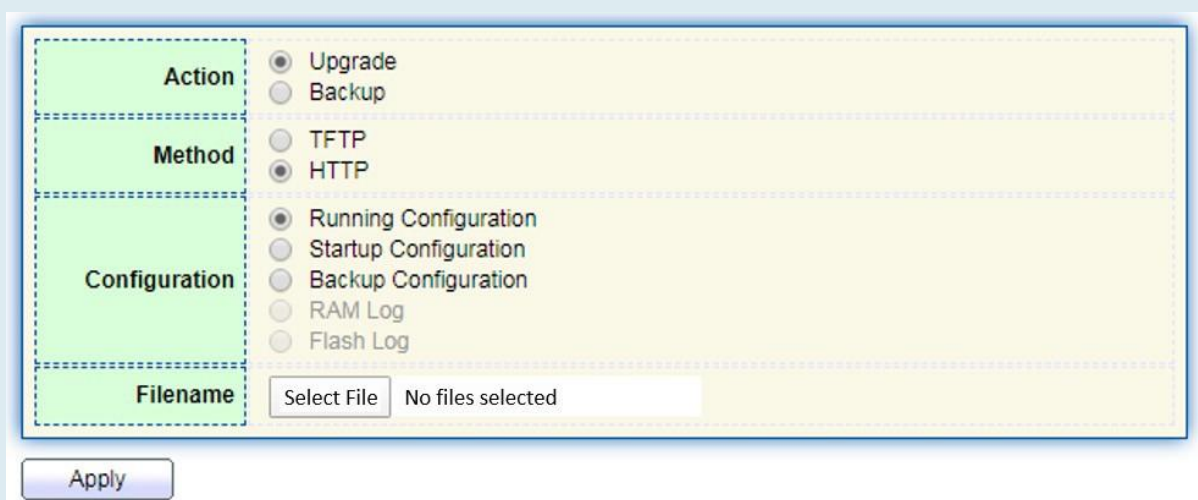
## 18.3 Configuración

### 18.3.1 Actualizar

Actualización o copia de seguridad (respaldo) de la configuración del sistema.

Instrucciones para la actualización del archivo de configuración:

1. Haga clic en "Management > Configuration > Upgrade" haga clic en "Actualizar" en modo de "TFTP" o "HTTP", seleccione los archivos correspondientes que desea actualizar (servers debe ilustrarse en modo TFTP). "Aplicar" y terminar de la siguiente manera:



The screenshot shows a configuration form for configuration upgrade. It has four sections: Action, Method, Configuration, and Filename. Below the form is an 'Apply' button.

<b>Action</b>	<input checked="" type="radio"/> Upgrade <input type="radio"/> Backup
<b>Method</b>	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
<b>Configuration</b>	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log
<b>Filename</b>	<input type="button" value="Select File"/> No files selected

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

- Haga clic en "Copia de seguridad" en modo "TFTP" o "HTTP", seleccione los archivos o registros que desea actualizar (los servidores deben ilustrarse en modo TFTP). "Aplicar" y terminar de la siguiente manera.

<b>Action</b>	<input type="radio"/> Upgrade <input checked="" type="radio"/> Backup
<b>Method</b>	<input type="radio"/> TFTP <input checked="" type="radio"/> HTTP
<b>Configuration</b>	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration <input type="radio"/> RAM Log <input type="radio"/> Flash Log

## 18.3.2 Guardar configuración

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

- Haga clic en "Management > Configuration > Save Configuration" en la barra de navegación de la siguiente manera:

<b>Source File</b>	<input checked="" type="radio"/> Running Configuration <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration
<b>Destination File</b>	<input checked="" type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration

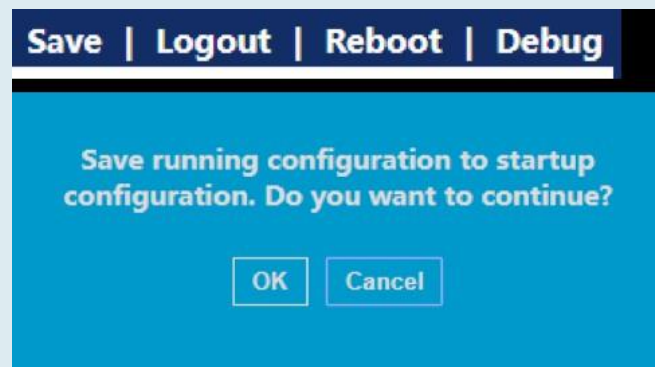
Nota:

- 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:

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



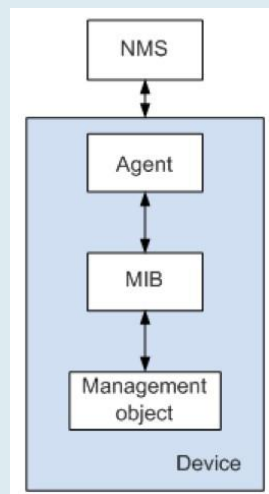
## 18.4 SNMP

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 de red (es decir, la estación de trabajo de administración de red). SNMP es:

- Simple: El SNMP de conducción de sondeos 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 gestión 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 interactúa con el agente que se ejecuta en el objeto de administración que operará el MIB para ejecutar órdenes NMS.

Modelo de gestión SNMP



### NMS

- Como administrador de red, NMS administra/supervisa 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. El dispositivo 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

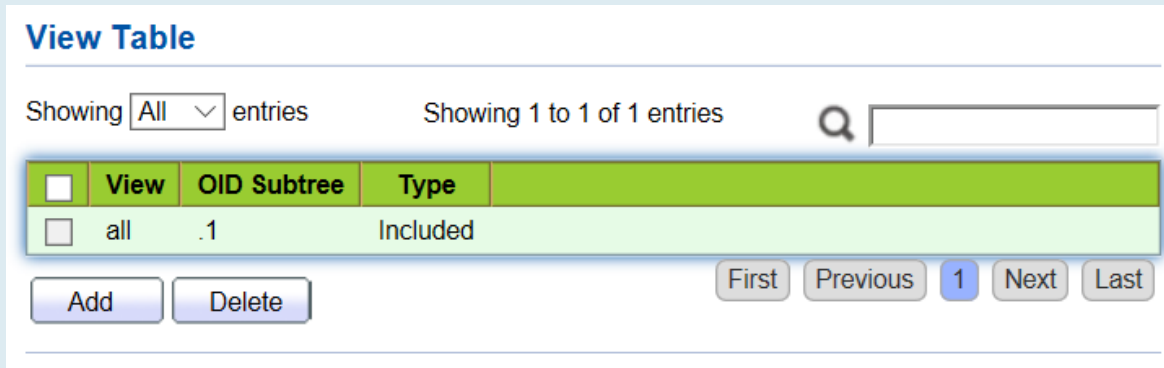
- Se refiere al objeto bajo gestión. Cada dispositivo puede tener más de un objeto, incluida una pieza de hardware (por ejemplo, una placa de interfaz), hardware y software parciales (por ejemplo, protocolo de enrutamiento), así como otros conjuntos de elementos de configuración.

### 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 clic en "Management > SNMP > View" en la barra de navegación de la siguiente manera.



**View Table**

Showing  entries      Showing 1 to 1 of 1 entries     

<input type="checkbox"/>	View	OID Subtree	Type
<input type="checkbox"/>	all	.1	Included

Los datos de la interfaz son los siguientes

Elementos de configuración	Descripción
View	Ver OID
OID Subtree	Cola de puertos
Type	Tipo de vista: "Incluido" o "Excluido"

2. "Añadir" la configuración correspondiente, "Aplicar" y finalizar.



**Add View**

Included     Excluded

## 18.4.2 Grupo

1. Haga clic en "Management > SNMP > Group" en la barra de navegación de la siguiente manera.



**Group Table**

Showing  entries      Showing 0 to 0 of 0 entries     

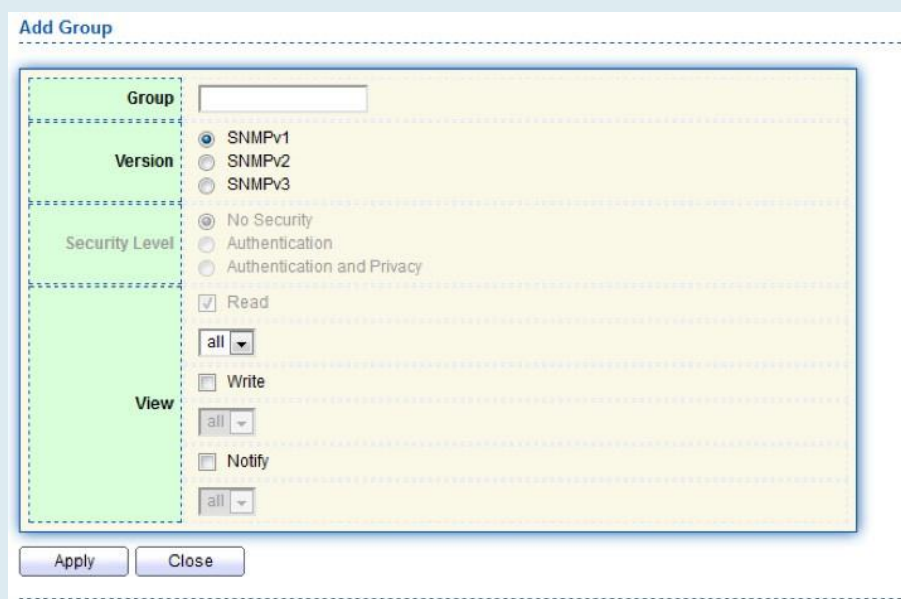
	Group	Version	Security Level	View		
				Read	Write	Notify
0 results found.						

Configure [SNMP View](#) to associate a non-default view with a group.

Los datos de la interfaz son los siguientes

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 terminar.



**Add Group**

Group:

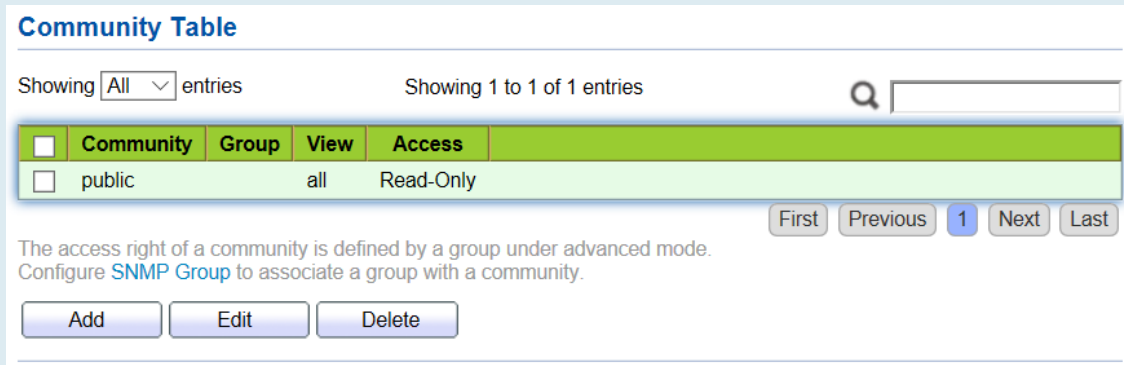
Version:
   
 SNMPv1
   
 SNMPv2
   
 SNMPv3

Security Level:
   
 No Security
   
 Authentication
   
 Authentication and Privacy

View:
   
 Read
   
 Write
   
 Notify

## 18.4.3 Comunidad

1. Haga clic en "Management > SNMP > Community" en la barra de navegación de la siguiente manera.



**Community Table**

Showing  entries      Showing 1 to 1 of 1 entries     

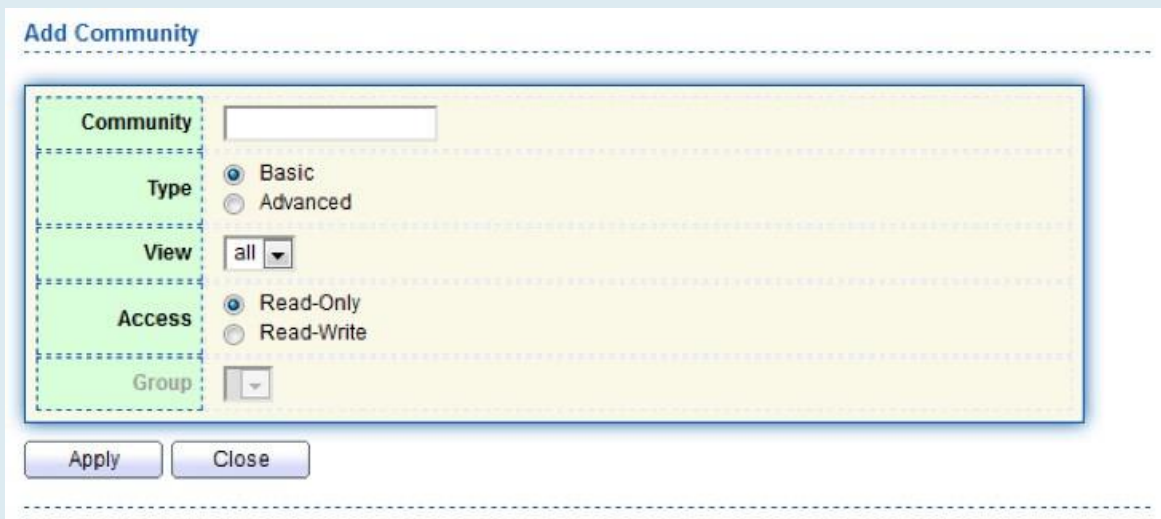
<input type="checkbox"/>	Community	Group	View	Access
<input type="checkbox"/>	public		all	Read-Only

The access right of a community is defined by a group under advanced mode. Configure [SNMP Group](#) to associate a group with a community.

Los datos de la interfaz son los siguientes

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 terminar.



**Add Community**

Community

Type  Basic  Advanced

View

Access  Read-Only  Read-Write

Group



## 18.4.4 Usuario

1. Haga clic en "Administración > SNMP > usuario" en la barra de navegación de la siguiente manera.

**User Table**

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	User	Group	Security Level	Authentication Method	Privacy Method
0 results found.					

Configure [SNMP Group](#) to associate an SNMPv3 group with an SNMPv3 user.

Los datos de la interfaz son los siguientes

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 terminar.

**Add User**

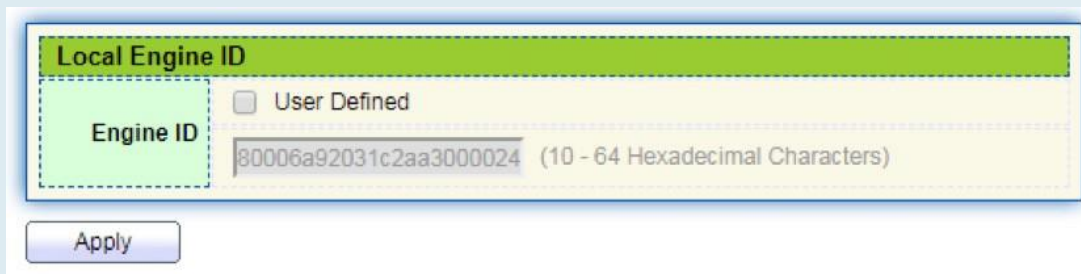
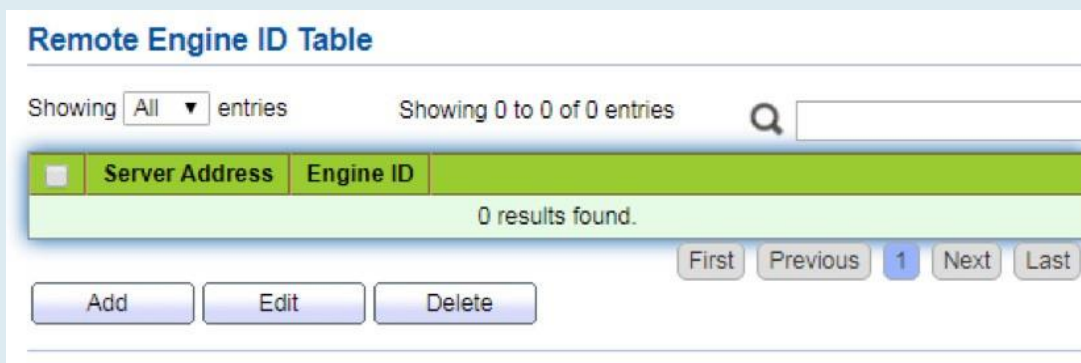
**User**   
**Group**   
**Security Level**
 No Security  
 Authentication  
 Authentication and Privacy

**Authentication**  
**Method**
 None  
 MD5  
 SHA  
**Password**

**Privacy**  
**Method**
 None  
 DES  
**Password**

## 18.4.5 ID del Equipo

1. Haga clic en "Management > SNMP > Engine ID" en la barra de navegación de la siguiente manera.

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

## 18.4.6 Evento Trap

1. Haga clic en "Management > SNMP > Trap Event" en la barra de navegación de la siguiente manera.



Los datos de la interfaz son los siguientes

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 clic en "Management > SNMP > Notification" en la barra de navegación de la siguiente manera.

**Notification Table**

Showing  entries      Showing 0 to 0 of 0 entries     

<input type="checkbox"/>	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								

For SNMPv1,2 Notification, [SNMP Community](#) needs to be defined.  
 For SNMPv3 Notification, [SNMP User](#) must be created.

**Add Notification**

<b>Address Type</b>	<input checked="" type="radio"/> Hostname <input type="radio"/> IPv4 <input type="radio"/> IPv6
<b>Server Address</b>	<input type="text"/>
<b>Version</b>	<input checked="" type="radio"/> SNMPv1 <input type="radio"/> SNMPv2 <input type="radio"/> SNMPv3
<b>Type</b>	<input checked="" type="radio"/> Trap <input type="radio"/> Inform
<b>Community / User</b>	<input type="text" value="private"/>
<b>Security Level</b>	<input checked="" type="radio"/> No Security <input type="radio"/> Authentication <input type="radio"/> Authentication and Privacy
<b>Server Port</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="162"/> (1 - 65535, default 162)
<b>Timeout</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="15"/> Sec (1 - 300, default 15)
<b>Retry</b>	<input checked="" type="checkbox"/> Use Default <input type="text" value="3"/> (1 - 255, default 3)

Los datos de la interfaz son los siguientes

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. "Añadir" la configuración correspondiente. "Aplicar" y terminar.

## 18.5 RMON

RMON (Remote Monitoring) 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 ampliamente 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 Agent para administrar la red de interconexión a gran escala de manera conveniente y efectiva. Varios monitores pueden recopilar datos por 2 medios: la exclusiva sonda RM ON 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. RMON Agent con acceso directo a dispositivos de red (enrutador, conmutador, HUB, etc.) se convertirá en la instalación de red con función RMON proba. 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: alarmas, eventos, historial y estadísticas. El Switch de tipo de área realiza RMON de la segunda manera. El agente RMON que se aloja en los switches se convertirá en la instalación de red con función de sonda RMON. Al ejecutar el agente SNMP compatible con los switches, NMS puede obtener todo el flujo, 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. La estadística incluya 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 gestión, el uso del puerto y los errores ocurridos se pueden controlar y contar, respectivamente.

Instrucciones

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

Statistics Table

Refresh Rate: 0 sec

Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes		
1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

View Port Statistics

Port: GE8

Refresh Rate:  None  5 sec  10 sec  30 sec

Received Bytes (Octets): 0

Drop Events: 0

Received Packets: 0

Broadcast Packets Received: 0

Multicast Packets Received: 0

CRC & Align Errors: 0

Undersize Packets: 0

Oversize Packets: 0

Fragments: 0

Jabbers: 0

Collisions: 0

Frames of 64 Bytes: 0

Frames of 65 to 127 Bytes: 0

Frames of 128 to 255 Bytes: 0

Frames of 256 to 511 Bytes: 0

Frames Greater than 1024 Bytes: 0

Clear Refresh Close

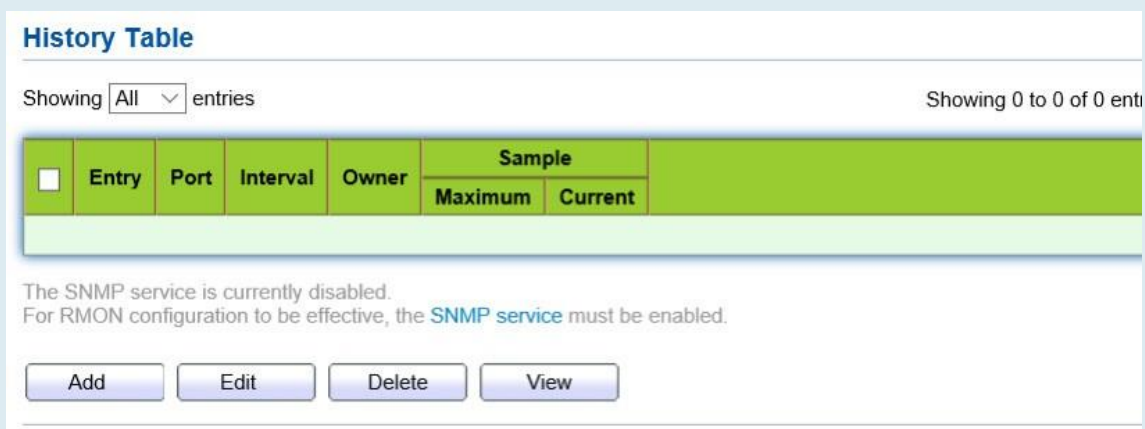
3. Seleccione la frecuencia de actualización especificada para que funcione automáticamente.

## 18.5.2 Historia

Una vez configurado el grupo de historial RMON, los conmutadores recopilarán periódicamente y almacenarán temporalmente las estadísticas de la 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 clic en "Management > RMON > History" en la barra de navegación de la siguiente manera.



**History Table**

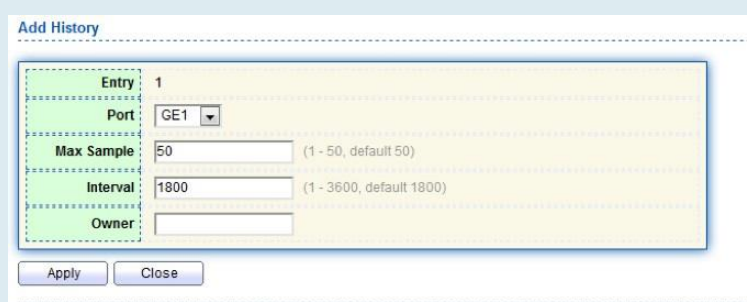
Showing  entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
The SNMP service is currently disabled. For RMON configuration to be effective, the <a href="#">SNMP service</a> must be enabled.						

Los datos de la interfaz son los siguientes

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
Security Level	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.



**Add History**

Entry: 1

Port:

Max Sample:  (1 - 50, default 50)

Interval:  (1 - 3600, default 1800)

Owner:

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

**History Table**

Showing  entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
<input type="checkbox"/>	1	GE1	1800		50	50

The SNMP service is currently disabled.  
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

### 18.5.3 Evento

El grupo de eventos se refiere principalmente a las actuaciones desencadenadas por los elementos de configuración del grupo de alarmas y los elementos de configuración del grupo de alarmas extendido. Hay varias formas de tratarlos: grabar el evento en una tabla de registro; transmitir un mensaje de captura a NMS; grabar un registro y transmitir un mensaje de captura; Condición "No me importa".

Instrucciones

1. Haga clic en "Management > RMON > Event" en la barra de navegación de la siguiente manera.

**Event Table**

Showing  entries Showing 0 to 0 of 0 entries

<input type="checkbox"/>	Entry	Community	Description	Notification	Time	Owner
0 results found.						

The SNMP service is currently disabled.  
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Los datos de la interfaz son los siguientes

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.

**Add Event**

---

<b>Entry</b>	1
<b>Notification</b>	<input checked="" type="radio"/> None <input type="radio"/> Event Log <input type="radio"/> Trap <input type="radio"/> Event Log and Trap
<b>Community</b>	Default Community
<b>Description</b>	Default Description
<b>Owner</b>	

Apply Close

---

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

**Event Table**

Showing All entries Showing 1 to 1 of 1 entries

<input type="checkbox"/>	Entry	Community	Description	Notification	Time	Owner
<input type="checkbox"/>	1	Default Community	Default Description	Event Log and Trap		

First Previous 1 Next Last

The SNMP service is currently disabled.  
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Add Edit Delete View

## 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 de la siguiente manera: 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 clic en "Management > RMON > Alarm" en la barra de navegación de la siguiente manera.



### Alarm Table

Showing  entries      Showing 0 to 0 of 0 entries     

Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
		Name	Value					Threshold	Event	Threshold	Event
0 results found.											

The SNMP service is currently disabled.  
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Los datos de la interfaz son los siguientes

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.

### Add Alarm

<b>Entry</b>	1	
<b>Port</b>	GE1	
<b>Counter</b>	Drop Events	
<b>Sampling</b>	<input checked="" type="radio"/> Absolute <input type="radio"/> Delta	
<b>Interval</b>	100	Sec (1 - 2147483647, default 100)
<b>Owner</b>		
<b>Trigger</b>	<input checked="" type="radio"/> Rising <input type="radio"/> Falling <input type="radio"/> Rising and Falling	
<b>Rising</b>		
<b>Threshold</b>	100	(0 - 2147483647, default 100)
<b>Event</b>	1 - Default Description	
<b>Falling</b>		
<b>Threshold</b>	20	(0 - 2147483647, default 20)
<b>Event</b>	1 - Default Description	

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

### Alarm Table

Showing All entries      Showing 1 to 1 of 1 entries     

	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
<input type="checkbox"/>	1	GE1	DropEvents	0	Absolute	100		Rising	100	Default Description	20	Default Description

The SNMP service is currently disabled.  
For RMON configuration to be effective, the [SNMP service](#) must be enabled.