NETGEAR®

Manual del usuario principal

Línea AV de switches totalmente administrables Serie M4250

Versión de firmware 13.0.0 y posteriores

Febrero de 2023
202-12091-05

NETGEAR, Inc.
350 E. Plumeria Drive
San Jose, CA 95134, USA

Soporte y comunidad
Visite netgear.com/support para resolver sus dudas y acceder a las descargas más recientes.

También puede consultar la Comunidad NETGEAR para obtener consejos útiles en community.netgear.com.

Normativa y aspectos legales
Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/download/.

(Si este producto se vende en Canadá, puede acceder a este documento en francés canadiense en https://www.netgear.com/support/download/.)

Para información de cumplimiento normativo, incluida la Declaración de conformidad de la UE, visite https://www.netgear.com/about/regulatory/.

Consulte el documento de cumplimiento normativo antes de conectar la fuente de alimentación.
Para la Política de privacidad de NETGEAR, visite https://www.netgear.com/about/privacy-policy.

Al usar este dispositivo, acepta los Términos y condiciones de NETGEAR en https://www.netgear.com/about/terms-and-conditions. Si no está de acuerdo, devuelva el dispositivo al lugar de compra dentro del periodo de devolución.

No use este dispositivo en exteriores. La fuente PoE está diseñada solo para conexiones dentro del edificio.

Aplica solo a dispositivos de 6 GHz: Use el dispositivo solo en interiores. La operación de dispositivos de 6 GHz está prohibida en plataformas petroleras, automóviles, trenes, barcos y aeronaves, excepto que se permite en aeronaves grandes que vuelen a más de 10,000 pies. Se prohíbe operar transmisores en la banda de 5.925-7.125 GHz para controlar o comunicarse con sistemas de aeronaves no tripuladas.

Marcas comerciales
© NETGEAR, Inc., NETGEAR y el logotipo de NETGEAR son marcas comerciales de NETGEAR, Inc. Las marcas comerciales que no son de NETGEAR se usan solo como referencia.

Historial de revisiones

Número de parte de la publicación	Fecha de publicación	Comentarios
202-12091-05	Febrero de 2023	Corregimos el valor de la clase de dispositivo 6 en la Tabla 38 de la sección Conceptos de PoE en la página 136.
202-12091-04	Mayo de 2022	Modificamos Switches compatibles en la página 23.

(Continuación)

Número de parte de la publicación	Fecha de publicación	Comentarios
202-12091-03	Noviembre de 2021	Modificamos las siguientes secciones: Iniciar sesión en la UI principal con un navegador web en la página 24 Iniciar sesión en la UI principal con la IP predeterminada del switch en la página 25 Configurar el puerto de servicio IPv4 en la página 48 Agregar una cuenta de usuario SNMPv3 en la página 158 Configurar los requisitos de contraseña de usuario en la página 497 Configurar el acceso HTTPS en la página 526 Administrar certificados para acceso HTTPS en la página 528 Generar un certificado SSL en la página 529 Eliminar un certificado SSL en la página 531 Transferir un certificado HTTPS existente de un servidor al switch en la página 531
		Agregamos las siguientes secciones: Mostrar el estado de los certificados SSL en la página 528 Activar un certificado en la página 530
		Hicimos otros cambios menores. Publicamos el manual en un nuevo formato.
202-12091-02	Marzo de 2021	Esta segunda publicación es una revisión mayor.
		Agregamos lo siguiente: Información sobre los modelos PoE+ y PoE++ de 24 puertos y los modelos PoE+ y PoE++ de 40 puertos (consulte Switches compatibles en la página 23). Información sobre la función Auto-Trunk (consulte Descripción general de Auto-Trunk en la página 194 y Habilitar o deshabilitar Auto-Trunks en la página 195). Información sobre la función Auto-LAG (consulte Descripción general de Auto-LAG en la página 302, Habilitar o deshabilitar Auto-LAGs en la página 303 y Configurar el modo de hash de Auto-LAGs en la página 304).
		Revisamos gran parte del manual y agregamos varias secciones nuevas para ofrecer información más completa y correcta.
		Reemplazamos el apéndice anterior de valores predeterminados por uno nuevo que también incluye especificaciones de hardware (consulte Valores predeterminados de software y especificaciones de hardware en la página 784).
		Hicimos varias correcciones en todo el manual.
202-12091-01	Octubre de 2020	Primera publicación.

Contenido

Capítulo 1 Introducción a la UI principal

Switches compatibles....23
Publicaciones disponibles y ayuda en línea....23
Registre su producto....23
Descripción general de la UI local del navegador....24
Iniciar sesión en la UI principal con un navegador web....24
Iniciar sesión en la UI principal con la IP predeterminada del switch..25
Iniciar sesión en la UI principal con una IP conocida....26
Botones y campos definidos por el usuario de la UI principal....26
Convenciones de nombres de interfaces....27
Guardar la configuración en la configuración en ejecución....28
Ayuda en línea de la UI principal....28
Usar la vista de dispositivo (Device View) en la UI principal....29
Configurar el acceso SNMP....31

Capítulo 2 Configurar la información del sistema del switch

Información del sistema del switch....35
Ver y configurar la información del sistema del switch....35
Ver el estado de los ventiladores....38
Ver la información del sensor de temperatura....39
Ver el estado del dispositivo y la versión de firmware....40
Ver el estado de la CPU del sistema....41
Configurar los umbrales de CPU....42
Ver o borrar las estadísticas del switch....43
Ver la información del dispositivo USB....45
Interfaz de loopback....46
Interfaces y VLAN de administración IPv4....47
Configurar el puerto de servicio IPv4....48
Configurar una VLAN de administración IPv4....49
Configurar una interfaz de administración IPv4....52
Interfaces y VLAN de administración IPv6....53
Configurar un puerto de servicio IPv6....54
Administrar direcciones IPv6 del puerto de servicio IPv6....55
Configurar una VLAN de administración IPv6....56
Administrar direcciones IPv6 de la VLAN de administración IPv6..59

Administrar las rutas predeterminadas IPv6 de la VLAN de administración IPv6....60
Configurar una interfaz de administración IPv6....61
Administrar direcciones IPv6 de la interfaz de administración IPv6..63
Administrar las rutas predeterminadas IPv6 de la interfaz de administración IPv6....64
Configuración de hora y SNTP....65
Configurar la hora manualmente....65
Configurar la hora con SNTP y configurar los parámetros SNTP globales....66
Ver el estado global de SNTP....69
Configurar servidores SNTP....71
Agregar un servidor SNTP....72
Cambiar la configuración de un servidor SNTP existente....74
Eliminar un servidor SNTP....74
Configurar el horario de verano....75
Ver el estado del horario de verano....77
Precision Time Protocol....79
Administrar la configuración global de PTP....79
Administrar la configuración de interfaz de PTP....80
Domain Name System....81
Configurar los ajustes globales de DNS y agregar un servidor DNS...81
Eliminar un servidor DNS....83
Configurar y ver la información de nombre de host a dirección IP...84
Agregar una entrada estática a la tabla de asignación dinámica de hosts...84
Eliminar una entrada de la tabla de asignación dinámica de hosts...85
Cambiar el nombre de host o la dirección IP de una entrada de la tabla de asignación dinámica, ver todas las entradas o borrarlas todas...85
Plantilla de administración de la base de datos del switch....86
Configuración de Green Ethernet....88
Configurar los ajustes globales de Green Ethernet....88
Configurar los ajustes de interfaz de Green Ethernet....89
Configurar y mostrar los ajustes detallados de Green Ethernet de una interfaz....90
Mostrar la información de Green Ethernet del enlace asociado de una interfaz....93
Mostrar el resumen de estadísticas de Green Ethernet....94
Configurar y mostrar el historial EEE LPI de Green Ethernet de una interfaz....96
Configuración de Bonjour....97
Habilitar o deshabilitar Bonjour....98
Mostrar la información de Bonjour....98
Servidor DHCP IPv4....99
Configurar un servidor DHCP....99
Administrar pools DHCP....101

Crear un pool DHCP....101
Cambiar un pool DHCP....104
Eliminar un pool DHCP....105
Configurar las opciones del pool DHCP....105
Mostrar las estadísticas del servidor DHCP....106
Mostrar los enlaces (bindings) DHCP....108
Eliminar uno o todos los enlaces DHCP dinámicos....109
Ver enlaces con conflictos DHCP....109
Eliminar uno o todos los enlaces DHCP con conflictos....111
Retransmisión DHCP (relay) y estadísticas....112
Retransmisión DHCP de capa 2 (Layer 2 relay)....113
Configurar los ajustes globales de DHCP L2 relay....114
Configurar una interfaz de DHCP L2 relay....114
Mostrar las estadísticas de interfaz de DHCP L2 relay....116
Retransmisión UDP (UDP relay)....117
Configurar los ajustes globales de UDP relay y agregar una configuración UDP del switch....117
Cambiar una configuración UDP del switch....119
Eliminar una configuración UDP del switch....119
Agregar una configuración UDP de interfaz....120
Cambiar una configuración UDP de interfaz....121
Eliminar una configuración UDP del switch....122
Servidor DHCPv6....123
Habilitar el servidor DHCPv6....123
Administrar pools DHCPv6....124
Crear un pool DHCPv6....124
Cambiar un pool DHCPv6....124
Eliminar un pool DHCPv6....125
Administrar la delegación de prefijos DHCPv6 para pools....126
Crear una configuración de delegación de prefijos DHCPv6 para un pool....126
Cambiar una configuración de delegación de prefijos DHCPv6 de un pool....127
Eliminar una configuración de delegación de prefijos DHCPv6 de un pool....128
Configurar los ajustes de DHCPv6 de una interfaz....129
Mostrar los enlaces (bindings) DHCPv6....130
Mostrar las estadísticas del servidor DHCPv6....131
Eliminar las estadísticas DHCPv6 de una o todas las interfaces....134
Interfaz de retransmisión DHCPv6 (relay)....135
Power over Ethernet....136
Conceptos de PoE....136
Configurar los ajustes globales de PoE....138
Configurar los ajustes de los puertos PoE....139
Reiniciar la alimentación de uno o más puertos PoE....143

Programaciones de temporizador....144
Crear una programación de temporizador....144
Definir los ajustes de una programación absoluta....145
Definir los ajustes de una programación recurrente....146
Cambiar los ajustes de una entrada de programación recurrente...148
Eliminar una entrada de programación de temporizador....149
Eliminar una programación de temporizador....150
Simple Network Management Protocol....151
Administrar comunidades SNMPv1 y SNMPv2....151
Agregar una comunidad SNMPv1 y SNMPv2....151
Cambiar una comunidad SNMPv1 y SNMPv2 existente....152
Eliminar una comunidad SNMPv1 y SNMPv2....153
Administrar la configuración de traps SNMPv1 y SNMPv2....153
Agregar una configuración de traps SNMPv1 o SNMPv2 para un host
Cambiar una configuración de traps SNMPv1 o SNMPv2 de un host....155
Eliminar una configuración de traps SNMPv1 o SNMPv2 de un host....155
Configurar los indicadores de traps SNMPv1 y SNMPv2....156
Mostrar las MIB compatibles....158
Administrar usuarios SNMPv3....158
Agregar una cuenta de usuario SNMPv3....158
Cambiar una cuenta de usuario SNMPv3....159
Eliminar una cuenta de usuario SNMPv3....160
Link Layer Discovery Protocol....161
Configurar los ajustes globales de LLDP....161
Configurar los ajustes de interfaz de LLDP....162
Mostrar o borrar las estadísticas de LLDP....163
Mostrar la información del dispositivo local LLDP....165
Mostrar la información del dispositivo remoto LLDP....166
Mostrar el inventario del dispositivo remoto LLDP....168
Link Layer Discovery Protocol for Media Endpoint Devices....169
Configurar los ajustes globales de LLDP-MED....169
Configurar los ajustes de interfaz de LLDP-MED....170
Mostrar la información del dispositivo local LLDP-MED....172
Mostrar la información del dispositivo remoto LLDP-MED....174
Mostrar el inventario del dispositivo remoto LLDP-MED....178
Dependencia de enlaces....179
Configurar un grupo de dependencia de enlaces....179
Configurar o mostrar las interfaces ascendentes y descendentes de un grupo de dependencia de enlaces....180
Borrar todas las interfaces de un grupo de dependencia de enlaces....182
Industry Standard Discovery Protocol....183
Configurar los ajustes globales de ISDP....183
Configurar los ajustes de ISDP de una interfaz....185

Mostrar o borrar la información de vecinos ISDP.....186
Mostrar o borrar las estadísticas de ISDP.....187

Capítulo 3 Configurar la información de switching

VLAN.....190
Administrar la configuración de VLAN en el switch.....190
Agregar una VLAN.....190
Cambiar una VLAN.....191
Eliminar una o más VLAN.....192
Restablecer toda la configuración de VLAN a valores predeterminados...193
Cambiar la asignación interna de VLAN.....193
Descripción general de Auto-Trunk.....194
Habilitar o deshabilitar Auto-Trunks.....195
Configurar el modo de puerto del switch para interfaces.....196
Configurar las interfaces miembro de una VLAN.....199
Ver el estado de las VLAN en el switch.....201
Cambiar los ajustes de ID de VLAN del puerto.....202
Configurar una VLAN basada en MAC.....205
Agregar una configuración de VLAN basada en MAC.....205
Eliminar una configuración de VLAN basada en MAC.....206
Configurar un grupo de VLAN basada en protocolo.....206
Agregar un grupo de VLAN basada en protocolo.....207
Cambiar un grupo de VLAN basada en protocolo.....208
Eliminar un grupo de VLAN basada en protocolo.....209
Configurar las interfaces miembro de un grupo de VLAN basada en protocolo.....209
Configurar una VLAN basada en subred IP.....211
Agregar una VLAN basada en subred IP.....211
Eliminar una VLAN basada en subred IP.....212
Configurar una VLAN doble.....212
Configurar una VLAN de voz.....214
Configurar Generic Attribute Registration Protocol.....215
Configurar los ajustes de GARP del switch.....216
Configurar los ajustes de GARP de una o más interfaces.....217
Auto-VoIP.....218
Configurar los ajustes de Auto-VoIP basados en protocolo.....219
Configurar las propiedades de Auto-VoIP basadas en OUI.....220
Configurar los ajustes de interfaz basados en OUI.....221
Administrar la tabla OUI.....222
Agregar un prefijo OUI.....223
Eliminar uno o más prefijos OUI.....223
Mostrar el estado de Auto-VoIP.....224
Spanning Tree Protocol.....225
Configurar los ajustes de STP y mostrar el estado de STP.....226

Configurar los ajustes de CST y mostrar el estado de CST.....229
Configurar los ajustes de interfaz de CST.....231
Mostrar el estado de interfaz de CST.....234
Administrar instancias MST.....236
Agregar una instancia MST y mostrar el estado de MST.....236
Cambiar una instancia MST.....238
Eliminar una instancia MST.....238
Configurar y mostrar los ajustes de interfaz de una instancia MST.....239
Mostrar las estadísticas de interfaz de STP.....242
Configurar los ajustes de VLAN de PVST/RPVST.....243
Cambiar una configuración de VLAN de PVST/RPVST.....245
Eliminar una configuración de VLAN de PVST/RPVST.....246
Configurar los ajustes de interfaz de PVST y RPVST.....246
Mostrar las estadísticas de PVST y RPVST.....248
Base de datos de reenvío multicast.....249
Mostrar las entradas de la base de datos de reenvío multicast...249
Eliminar las entradas de IGMP snooping de la base de datos de reenvío multicast.....250
Eliminar todas las entradas MAC multicast conocidas de la base de datos de reenvío multicast.....251
Mostrar las estadísticas de la base de datos de reenvío multicast...252
Internet Group Management Protocol snooping.....253
Configurar IGMP snooping automáticamente con el modo IGMP Plus.....254
Configurar IGMP snooping manualmente.....255
Configurar los ajustes de IGMP snooping de las interfaces.....257
Configurar IGMP snooping para VLAN automáticamente con el modo IGMP Plus.....259
Configurar IGMP snooping para VLAN manualmente.....260
Configurar una interfaz de router multicast IGMP.....262
Configurar una VLAN de router multicast IGMP.....263
Descripción general del querier de IGMP snooping.....264
Configurar los ajustes globales del querier de IGMP snooping...264
Configurar un querier de IGMP snooping para una VLAN.....265
Eliminar los ajustes del querier de IGMP snooping de una VLAN...267
Mostrar el estado del querier de IGMP snooping.....268
Multicast Listener Discovery snooping.....269
Configurar MLD snooping automáticamente con el modo MLD Plus
Configurar MLD snooping manualmente.....271
Configurar los ajustes de MLD snooping de las interfaces.....272
Configurar MLD snooping para VLAN automáticamente con el modo MLD Plus.....274
Configurar MLD snooping para VLAN manualmente.....275
Eliminar los ajustes del querier de MLD snooping de una VLAN...277

Configurar una interfaz de router multicast MLD.....278
Configurar una VLAN de router multicast MLD.....279
Configurar los ajustes globales del querier de MLD snooping...280
Configurar un querier de MLD snooping para una VLAN.....281
Eliminar los ajustes del querier de MLD snooping de una VLAN...283
Registro de VLAN multicast (MVR).....283
Configurar los ajustes globales de MVR.....284
Configurar un grupo MVR.....285
Eliminar un grupo MVR.....286
Configurar una interfaz MVR.....287
Configurar las interfaces miembro de un grupo MVR.....288
Mostrar las estadísticas de MVR.....289
Tabla de direcciones MAC.....290
Ver, buscar o borrar la tabla de direcciones MAC.....290
Establecer el intervalo de envejecimiento de direcciones dinámicas.....292
Agregar una dirección MAC estática a la tabla de direcciones MAC...293
Eliminar una dirección MAC estática de la tabla de direcciones MAC...293
Configuración de puertos.....294
Configurar y mostrar los ajustes de puertos.....294
Agregar descripciones de puertos, LAG y VLAN.....297
Mostrar la información del módulo transceptor.....299
Configurar los ajustes de link flap del puerto.....300
Grupos de agregación de enlaces (LAG).....301
Descripción general de Auto-LAG.....302
Habilitar o deshabilitar Auto-LAGs.....303
Configurar el modo hash para Auto-LAGs.....304
Configurar los ajustes de LAG.....305
Configurar un LAG individual y sus miembros.....307
Temporización y sincronización 802.1AS.....309
Configurar y ver los ajustes globales de 802.1AS.....309
Configurar los ajustes de interfaz de 802.1AS.....311
Ver las estadísticas de 802.1AS.....313
Multiple Registration Protocol y ajustes de 802.1Qav.....315
Configurar los ajustes globales de MRP.....316
Configurar la asignación de 802.1Qav.....318
Configurar los ajustes de interfaz de MRP.....319
Ver o borrar las estadísticas de MMRP.....321
Ver o borrar las estadísticas de MVRP.....322
Ver o borrar las estadísticas de MSRP.....324
Ver los ajustes de reservación de MSRP.....326
Configurar y ver los ajustes de Qav de las interfaces.....328
Ver la información de flujos MSRP.....330
Protección contra bucles.....332
Acerca de la protección contra bucles.....332
Configurar los ajustes globales de protección contra bucles.....334

Configurar la protección contra bucles de las interfaces y mostrar el estado de protección contra bucles....335

Capítulo 4 Administrar el enrutamiento

Conceptos de enrutamiento....338
Tabla de enrutamiento, rutas y preferencias de ruta....338
Configurar una ruta y mostrar las rutas aprendidas....338
Eliminar una ruta....340
Especificar las preferencias de ruta....341
Enrutamiento IPv4....342
Administrar los ajustes globales de enrutamiento IPv4....342
Mostrar las estadísticas de IPv4....344
Configurar interfaces de enrutamiento IPv4....347
Eliminar la dirección IP de una interfaz de enrutamiento IPv4....350
Configurar una dirección IP secundaria para una interfaz de enrutamiento IPv4....351
Eliminar la dirección IP secundaria de una interfaz de enrutamiento IPv4....352
Enrutamiento IPv6....353
Administrar los ajustes globales de enrutamiento IPv6....353
Mostrar la tabla de rutas IPv6....354
Configurar interfaces de enrutamiento IPv6....355
Configurar prefijos de una interfaz de enrutamiento IPv6....358
Eliminar un prefijo de una interfaz de enrutamiento IPv6....360
Mostrar las estadísticas de IPv6 e ICMPv6 de una interfaz de enrutamiento IPv6....361
Mostrar la tabla de vecinos IPv6 o borrar entradas de vecinos IPv6....366
Configurar rutas estáticas IPv6....368
Eliminar una ruta estática IPv6....370
Configurar la preferencia de ruta IPv6 del switch....370
Configurar túneles IPv6....371
Eliminar un túnel IPv6....373
VLAN de enrutamiento....373
Crear una VLAN de enrutamiento con el asistente de rutas estáticas....374
Configurar el enrutamiento de una VLAN existente....375
Quitar la función de enrutamiento de una VLAN....376
Address Resolution Protocol (ARP)....377
Mostrar las entradas de la caché ARP....378
Agregar o cambiar una entrada estática en la tabla ARP....379
Eliminar una entrada ARP estática....380
Configurar los ajustes de la tabla ARP o eliminar entradas de la tabla....381
Routing Information Protocol (RIP)....383
Habilitar o deshabilitar RIP en el switch....384

Configurar los ajustes globales de RIP del switch.....384
Configurar los ajustes de interfaz RIP.....386
Configurar la redistribución de rutas RIP y mostrar el resumen de redistribución de rutas.....388
Descubrimiento de routers y anuncios de router.....390

Capítulo 5 Configurar el enrutamiento multicast

Enrutamiento multicast IPv4 y tabla de rutas multicast IPv4.....394
Mostrar la tabla de rutas multicast IPv4.....394
Agregar entradas multicast estáticas a la tabla Mroute IPv4.....395
Eliminar una entrada multicast estática de la tabla Mroute IPv4....396
Configurar los ajustes globales de multicast del switch.....397
Configurar una interfaz multicast.....398
IGMP para enrutamiento multicast IPv4.....399
Configurar los ajustes globales de IGMP del switch.....399
Configurar una interfaz de enrutamiento IGMP.....400
Mostrar las estadísticas de las interfaces de enrutamiento IGMP.....402
Mostrar los grupos IGMP y buscar en la base de datos de grupos IGMP.....403
Mostrar la información de membresía IGMP y buscar en la base de datos de membresía IGMP.....405
Configurar una interfaz proxy IGMP.....407
Mostrar las estadísticas de la interfaz proxy IGMP.....408
Mostrar la membresía del proxy IGMP y buscar en la base de datos de membresía del proxy IGMP.....410
PIM para enrutamiento multicast IPv4.....411
Configurar los ajustes globales de PIM IPv4 en el switch.....412
Agregar grupos PIM-SSM IPv4.....412
Eliminar un grupo PIM-SSM IPv4.....413
Configurar una interfaz PIM IPv4.....414
Mostrar los vecinos PIM IPv4 y buscar en la base de datos de vecinos PIM.....416
Agregar una configuración de punto de encuentro candidato PIM IPv4....417
Eliminar una configuración de punto de encuentro candidato PIM IPv4....418
Configurar una interfaz como candidato a router bootstrap PIM IPv4.....419
Eliminar una configuración de candidato a router bootstrap PIM IPv4....420
Configurar un punto de encuentro PIM IPv4 estático para un grupo....421
Eliminar una configuración de punto de encuentro PIM IPv4 estático....422
Rutas multicast estáticas para direcciones IPv4.....422
Configurar rutas multicast estáticas para direcciones IPv4.....422
Eliminar una ruta multicast estática de una dirección IPv4.....423
Límites administrativos multicast para direcciones IPv4.....424
Configurar una interfaz como límite administrativo multicast....424

Eliminar una configuración de límite administrativo multicast de una interfaz....425
Enrutamiento multicast IPv6 y tabla de rutas multicast IPv6....426
Mostrar la tabla de rutas multicast IPv6....426
PIM para enrutamiento multicast IPv6....428
Configurar los ajustes globales de PIM IPv6 en el switch....428
Agregar grupos PIM-SSM IPv6....429
Eliminar un grupo PIM-SSM IPv6....430
Configurar una interfaz PIM IPv6....430
Mostrar los vecinos PIM IPv6 y buscar en la base de datos de vecinos PIM....432
Agregar una configuración de punto de encuentro candidato PIM IPv6....433
Eliminar una configuración de punto de encuentro candidato PIM IPv6....434
Configurar una interfaz como candidato a router bootstrap PIM IPv6....435
Eliminar una configuración de candidato a router bootstrap PIM IPv6....436
Configurar un punto de encuentro PIM IPv6 estático para un grupo....437
Eliminar una configuración de punto de encuentro PIM IPv6 estático....438
MLD para enrutamiento multicast IPv6....439
Configurar los ajustes globales de MLP del switch....439
Configurar una interfaz de enrutamiento MLD....440
Mostrar las estadísticas de las interfaces de enrutamiento MLD....442
Mostrar los grupos MLD y buscar en la base de datos de grupos MLD....443
Mostrar o borrar las estadísticas de tráfico MLD....445
Configurar una interfaz proxy MLD....446
Mostrar las estadísticas de la interfaz proxy MLD....447
Mostrar la membresía del proxy MLD y buscar en la base de datos de membresía del proxy MLD....449
Rutas multicast estáticas para direcciones IPv6....450
Configurar rutas multicast estáticas para direcciones IPv6....451
Eliminar una ruta multicast estática de una dirección IPv6....452

Capítulo 6 Configurar la calidad de servicio

Conceptos de calidad de servicio (QoS)....454
Clase de servicio (CoS)....454
Conceptos de configuración de CoS....454
Configurar el modo de confianza CoS de forma global o para una interfaz específica....455
Asignar prioridades 802.1p a colas....456
Asignar valores DSCP a colas....458
Configurar los ajustes de interfaz CoS de una interfaz....458
Configurar los ajustes de colas CoS de una interfaz....460
Configurar la precedencia WRED de CoS para el descarte de paquetes....462

Servicios diferenciados (DiffServ).....464
Definición de DiffServ.....464
Descripción general del asistente DiffServ.....465
Usar el asistente DiffServ para crear una clase de tráfico y una política para una o más interfaces.....466
Configurar el modo DiffServ y mostrar las entradas de las tablas MIB privadas de DiffServ.....467
Configurar una clase DiffServ.....468
Agregar y configurar una clase DiffServ.....469
Cambiar el nombre de una clase DiffServ existente.....473
Cambiar los criterios de una clase DiffServ existente.....473
Eliminar una clase DiffServ.....474
Configurar una clase DiffServ IPv6.....475
Agregar y configurar una clase DiffServ IPv6.....475
Cambiar el nombre de una clase DiffServ IPv6 existente.....478
Cambiar los criterios de una clase DiffServ IPv6 existente....478
Eliminar una clase DiffServ IPv6.....479
Configurar una política DiffServ.....480
<<TBD>>Crear y configurar una política DiffServ.....480
Cambiar el nombre de una política DiffServ existente.....486
Cambiar los atributos de una política DiffServ existente.....487
Cambiar o quitar una clase de una política DiffServ existente....488
Eliminar una política DiffServ.....488
Configurar la interfaz de servicio DiffServ.....489
Asociar políticas DiffServ a una interfaz.....489
Cambiar una o ambas políticas DiffServ de una interfaz.....490
Quitar una o ambas políticas DiffServ de una interfaz.....491
Mostrar las estadísticas de servicio DiffServ.....492

Capítulo 7 Administrar la seguridad del switch

Cuentas de usuario y contraseñas.....495
Agregar o cambiar una cuenta de usuario.....495
Eliminar una cuenta de usuario.....496
Configurar los requisitos de contraseña de usuario.....497
Cambiar la contraseña CLI de EXEC privilegiado.....498
Cambiar la contraseña de consola, Telnet o SSH.....499
Servidores RADIUS.....500
Configurar los ajustes globales del servidor RADIUS.....500
Configurar un servidor de autenticación RADIUS en el switch....503
Agregar un servidor de autenticación RADIUS al switch.....503
Modificar los ajustes de un servidor de autenticación RADIUS en el switch.....505
Quitar un servidor de autenticación RADIUS del switch....506
Configurar un servidor de contabilidad RADIUS.....507

Agregar un servidor de contabilidad RADIUS al switch.....507
Modificar los ajustes de un servidor de contabilidad RADIUS en el switch.....509
Quitar un servidor de contabilidad RADIUS del switch....510
Servidores TACACS+.....510
Configurar los ajustes globales de TACACS+.....511
Agregar un servidor TACACS+ al switch.....512
Modificar los ajustes de un servidor TACACS+ en el switch....513
Quitar un servidor TACACS+ del switch.....514
Listas de autenticación.....514
Configurar una lista de autenticación de inicio de sesión.....514
Eliminar una lista de autenticación de inicio de sesión.....516
Configurar una lista de autenticación enable.....517
Eliminar una lista de autenticación enable.....519
Configurar la lista de autenticación Dot1x.....520
Configurar la lista de autenticación HTTP.....521
Configurar la lista de autenticación HTTPS.....522
Sesiones de inicio de sesión actuales.....523
Acceso de administración por HTTP y HTTPS.....524
Configurar los ajustes de acceso HTTP.....524
Configurar los ajustes de acceso HTTPS.....526
Mensaje de seguridad del navegador con acceso HTTPS.....527
Administrar certificados para el acceso HTTPS.....528
Mostrar el estado de los certificados SSL.....528
Generar un certificado SSL.....529
Activar un certificado.....530
Eliminar un certificado SSL.....531
Transferir un certificado HTTPS existente de un servidor al switch.....531
Acceso de administración por SSH.....533
Configurar los ajustes globales de acceso SSH.....534
Administrar claves RSA y DSA para el acceso SSH.....535
Generar una clave RSA o DSA.....535
Eliminar una clave RSA o DSA.....536
Transferir claves SSH existentes de un servidor TFTP al switch....537
Acceso de administración por Telnet.....539
Seleccionar listas de autenticación de Telnet.....539
Configurar los ajustes de Telnet entrante.....540
Configurar los ajustes de Telnet saliente.....541
Acceso de administración por el puerto de consola.....542
Denegación de servicio.....544
Perfiles y reglas de acceso de administración.....546
Agregar un perfil de acceso.....546
Agregar una regla al perfil de acceso.....547
Activar el perfil de acceso.....548

Mostrar el resumen del perfil de acceso y el número de paquetes filtrados....549
Desactivar un perfil de acceso....550
Quitar un perfil de acceso....551
Autenticación de puertos....552
Configurar los ajustes globales de 802.1X....552
Administrar la autenticación en puertos individuales....554
Configurar los ajustes 802.1X de un puerto....554
Inicializar 802.1X en un puerto....558
Mostrar el resumen de puertos....559
Mostrar el resumen de clientes....561
Filtros MAC para el control de tráfico....563
Crear un filtro MAC....563
Eliminar un filtro MAC....565
Mostrar el resumen de filtros MAC....566
Seguridad de puertos....567
Configurar el modo global de seguridad de puertos....567
Configurar una interfaz de seguridad de puertos....568
Mostrar las direcciones MAC aprendidas y convertirlas en direcciones estáticas....569
Agregar una dirección MAC estática a la tabla de direcciones MAC para la seguridad de puertos....571
Quitar una dirección MAC estática de la tabla de direcciones MAC para la seguridad de puertos....571
Grupos de puertos privados....572
Agregar un grupo de puertos privados....572
Quitar un grupo de puertos privados....573
Configurar la membresía de un grupo de puertos privados....574
Proteger puertos....575
VLAN privadas....576
Resumen de tareas para configurar VLAN privadas....577
Asignar un tipo de VLAN privada a una VLAN....578
Configurar una asociación de VLAN privada con una VLAN primaria y secundaria....579
Eliminar una asociación de VLAN privada existente....581
Configurar el modo de puerto de VLAN privada....581
Interfaz host de VLAN privada: asignar la interfaz a VLAN primarias y secundarias....583
Interfaz host de VLAN privada: quitar la interfaz de VLAN primarias y secundarias....585
Interfaz promiscua de VLAN privada: asignar la interfaz a VLAN primarias y secundarias....586
Interfaz promiscua de VLAN privada: quitar la interfaz de VLAN primarias y secundarias....587

Interfaz troncal promiscua de VLAN privada: agregar VLAN primarias y secundarias al troncal....589
Interfaz troncal promiscua de VLAN privada: quitar VLAN primarias y secundarias del troncal....590
Interfaz troncal aislada de VLAN privada: agregar VLAN primarias y secundarias al troncal....591
Interfaz troncal aislada de VLAN privada: quitar VLAN primarias y secundarias del troncal....592
Configurar VLAN nativas y permitidas en una interfaz troncal de VLAN privada....593
Control de tormentas....595
Configurar el control de tormentas global....595
Configurar el control de tormentas para uno o más puertos....597
DHCP snooping....599
Habilitar DHCP snooping para el switch....600
Habilitar DHCP snooping para una VLAN....600
Configurar DHCP snooping en interfaces....601
Agregar un enlace DHCP estático y mostrar enlaces DHCP dinámicos....603
Eliminar un enlace DHCP estático....604
Configurar la persistencia de DHCP snooping....605
Mostrar o borrar estadísticas de DHCP snooping....606
DHCPv6 snooping....607
Habilitar DHCPv6 snooping para el switch....607
Habilitar DHCPv6 snooping para una VLAN....608
Configurar DHCPv6 snooping en interfaces....609
Agregar un enlace DHCPv6 estático y mostrar enlaces DHCPv6 dinámicos....611
Eliminar un enlace DHCPv6 estático....612
Configurar la persistencia de DHCPv6 snooping....613
Mostrar o borrar estadísticas de DHCPv6 snooping....614
Interfaces de IP source guard....615
Configurar IP source guard en una interfaz....615
Agregar un enlace estático de IP source guard y mostrar enlaces dinámicos de IP source guard....617
Eliminar un enlace estático de IP source guard....618
Interfaces de IPv6 source guard....619
Configurar IPv6 source guard en una interfaz....619
Agregar un enlace estático de IPv6 source guard y mostrar enlaces dinámicos de IPv6 source guard....621
Eliminar un enlace estático de IPv6 source guard....622
Inspección dinámica de ARP....623
Configurar los ajustes globales de DAI....623
Configurar VLAN de DAI....624
Configurar interfaces de DAI....625

Crear una lista de control de acceso de DAI....627
Configurar una regla para una ACL de DAI existente....627
Eliminar una regla de una ACL de DAI existente....628
Eliminar una lista de control de acceso de DAI....629
Mostrar las estadísticas de DAI....630
Portales cautivos....631
Configurar los ajustes globales del portal cautivo....632
Configurar un portal cautivo....633
Eliminar un portal cautivo....637
Configurar un enlace de portal cautivo....637
Mostrar o eliminar enlaces en la tabla de enlaces del portal cautivo....638
Configurar grupos de portal cautivo....639
Agregar un grupo de portal cautivo....639
Eliminar un grupo de portal cautivo....640
Configurar usuarios del portal cautivo....641
Agregar o modificar una cuenta de usuario del portal cautivo....641
Eliminar una cuenta de usuario del portal cautivo....643
Configurar los indicadores de trap del portal cautivo....644
Mostrar o borrar estadísticas de clientes del portal cautivo....645
Listas de control de acceso....646
Usar el asistente ACL para crear una ACL simple....647
Usar el asistente ACL para crear una ACL....647
Modificar una regla ACL creada con el asistente ACL.652
Eliminar una regla ACL creada con el asistente ACL.652
Ejemplo del asistente ACL....653
Configurar una ACL MAC....653
Agregar una ACL MAC....654
Cambiar el nombre de una ACL MAC....655
Eliminar una ACL MAC....655
Configurar reglas de ACL MAC....656
Agregar una regla a una ACL MAC....656
Cambiar los criterios de coincidencia de una regla MAC....659
Eliminar una regla de una ACL MAC....659
Configurar enlaces MAC....660
Mostrar o eliminar enlaces de ACL MAC en la tabla de enlaces MAC....662
Configurar una ACL IPv4 básica o extendida....663
Agregar una ACL IPv4....664
Cambiar el número o nombre de una ACL IPv4....665
Eliminar una ACL IPv4....666
Configurar reglas para una ACL IP básica....666
Agregar una regla a una ACL IPv4 básica....667
Modificar los criterios de una regla de ACL IPv4 básica....669
Eliminar una regla de ACL IPv4 básica....670

Configurar reglas para una ACL IPv4 extendida....671
Agregar una regla a una ACL IPv4 extendida....671
Modificar los criterios de una regla de ACL IPv4 extendida...678
Eliminar una regla de ACL IPv4 extendida....679
Configurar una ACL IPv6....679
Agregar una ACL IPv6....680
Cambiar el nombre de una ACL IPv6....681
Eliminar una ACL IPv6....681
Configurar reglas para una ACL IPv6....682
Agregar una regla a una ACL IPv6....682
Modificar los criterios de una regla de ACL IPv6....687
Eliminar una regla de ACL IPv6....688
Configurar enlaces de ACL IP a interfaces....688
Mostrar o eliminar enlaces en la tabla de enlaces de ACL IP.690
Configurar enlaces de ACL de VLAN....692
Agregar un enlace de ACL de VLAN....692
Eliminar un enlace de ACL de VLAN....693

Capítulo 8 Monitorear el switch y la red

Estadísticas de puertos y paquetes EAP....695
Mostrar o borrar estadísticas de puertos....695
Mostrar o borrar estadísticas detalladas de un puerto....696
Mostrar o borrar estadísticas de EAP y EAPoL....703
Realizar una prueba de cable....705
Registros....706
Administrar y mostrar el registro de memoria....707
Formato de los mensajes de registro....709
Habilitar o deshabilitar el registro de configuración de comandos....709
Habilitar o deshabilitar el registro en consola....710
Configuración de syslog y del servidor de registros....712
Configurar syslog....712
Agregar un servidor syslog....713
Modificar la configuración de un servidor syslog....715
Eliminar la configuración de un servidor syslog....715
Registro de traps....716
Registro de eventos....717
Duplicación de puertos....718
VLAN RSPAN y switches de origen y destino....721
Configurar una VLAN existente como VLAN RSPAN....721
Configurar el switch como switch de origen RSPAN....722
Configurar el switch como switch de destino RSPAN....724
Monitoreo sFlow....725
Descripción general del agente sFlow....726
Configurar la interfaz de origen del agente sFlow....726

Configurar un receptor sFlow....727
Configurar el sondeo y muestreo sFlow en una interfaz....729
Mostrar información de la licencia....730
Mostrar información de la clave de licencia....730
Mostrar las funciones a las que se aplica la licencia....731

Capítulo 9 Mantenimiento y solución de problemas

Guardar la configuración....734
Instalación automática del archivo de configuración....734
Configurar el proceso de instalación automática....734
Requisitos del servidor DHCP con opción 125 para obtener un archivo de configuración mediante instalación automática....736
Reiniciar el switch desde la interfaz web local principal....737
Restablecer el switch a la configuración de fábrica....738
Exportar un archivo desde el switch....739
Exportar un archivo del switch a un servidor....739
Usar HTTP para exportar un archivo del switch a una computadora....741
Exportar un archivo del switch a un dispositivo de almacenamiento USB....742
Actualizar el software o descargar un archivo....744
Actualizar la imagen de software o descargar un archivo de un servidor al switch....744
Usar HTTP para descargar un archivo al switch o actualizar la imagen de software....747
Descargar un archivo de un dispositivo de almacenamiento USB al switch....749
Usar una sesión HTTP para descargar e instalar un archivo de certificado de seguridad SSL en el switch....750
Administrar imágenes de software....752
Copiar una imagen de software....752
Configurar la imagen dual....753
Cambiar la imagen de software que se carga al iniciar o reiniciar el switch....753
Eliminar una imagen de software....754
Diagnóstico y solución de problemas....755
Hacer ping a una dirección IPv4....755
Hacer ping a una dirección IPv6....757
Enviar un traceroute IPv4....758
Enviar un traceroute IPv6....760
Capturar paquetes....762
Realizar un volcado completo de memoria....763

Apéndice A Ejemplos de configuración

Redes de área local virtuales (VLAN)....766
Ejemplos de configuración de VLAN....767
Listas de control de acceso (ACL)....768

Configuración de ejemplo de ACL MAC....769
Configuración de ejemplo de ACL IP básica....770
Servicios diferenciados (DiffServ)....771
Clase....772
Clases de tráfico DiffServ....772
Crear políticas....773
Política de acondicionamiento de tráfico....773
Configuración de ejemplo de DiffServ....774
Control de acceso 802.1X....775
Configuración de ejemplo de 802.1X....777
Multiple Spanning Tree Protocol....779
Configuración de ejemplo de MSTP....780
Interfaces de enrutamiento de VLAN....782

Apéndice B Configuración predeterminada del software y especificaciones de hardware

Acceso predeterminado a la interfaz del switch....785
Valores predeterminados de funciones del sistema....785
Valores predeterminados de funciones de conmutación....790
Valores predeterminados de enrutamiento y multicast....800
Valores predeterminados de QoS....805
Valores predeterminados de seguridad....807
Valores predeterminados de monitoreo....816
Especificaciones técnicas de hardware por modelo....818
Modelo M4250-10G2F-PoE+ (SKU GSM4212P)....818
Modelo M4250-10G2XF-PoE+ (SKU GSM4212PX)....819
M4250-10G2XF-PoE++ (SKU GSM4212UX)....819
M4250-26G4F-PoE+ (SKU GSM4230P)....820
M4250-26G4XF-PoE+ (SKU GSM4230PX)....821
M4250-26G4F-PoE++ (SKU GSM4230UP)....821
M4250-40G8F-PoE+ (SKU GSM4248P)....822
M4250-40G8XF-PoE+ (SKU GSM4248PX)....823
M4250-40G8XF-PoE++ (SKU GSM4248UX)....823
M4250-12M2XF (SKU MSM4214X)....824
M4250-16XF (SKU XSM4216F)....824
Especificaciones técnicas generales de hardware....825

1

Introducción a la interfaz principal

Este manual del usuario es para la línea AV de switches totalmente administrados serie M4250 y abarca todos los modelos de switch M4250.

Este capítulo ofrece una descripción general de cómo usar su switch y acceder a la interfaz de usuario (UI) web local principal.

El capítulo contiene las siguientes secciones:

- Switches compatibles
- Publicaciones disponibles y ayuda en línea
- Registre su producto
- Descripción general de la interfaz web local principal
- Iniciar sesión en la interfaz principal con un navegador web
- Usar Device View en la interfaz principal
- Configurar el acceso SNMP

Nota: Para más información sobre los temas de este manual, visite el sitio web de soporte en netgear.com/support.

Nota: Periódicamente se publican actualizaciones de firmware con nuevas funciones y correcciones en netgear.com/support/download/. Algunos productos pueden revisar el sitio regularmente y descargar el firmware nuevo, o usted puede buscarlo y descargarlo manualmente. Si las funciones o el comportamiento de su producto no coinciden con lo descrito en esta guía, es posible que deba actualizar el firmware.

Switches compatibles

Este manual del usuario principal corresponde a los modelos NETGEAR AV Line of Fully Managed Switches M4250 Series. Para ver la lista de modelos M4250, visite kb.netgear.com/000064904.

Publicaciones disponibles y ayuda en línea

Puede descargar las siguientes publicaciones y más para AV Line of Fully Managed Switches M4250 Series en netgear.com/support/download/.

- Guía de instalación
- Guía de instalación del hardware
- Manual del usuario principal (este manual)
- Manual del usuario de audio y video
- Manual de administración del software
- Manual de referencia de comandos CLI

Cuando haya iniciado sesión en la interfaz web local principal, puede consultar la documentación en línea seleccionando Help > Online Help > User Guide. Consulte Ayuda en línea de la interfaz principal en la página 28

Además, la interfaz web local principal ofrece ayuda en línea contextual.

Registre su producto

Para recibir actualizaciones y la garantía del producto, le recomendamos registrar su producto. La primera vez que inicie sesión en el switch, puede registrarse con NETGEAR haciendo clic en el botón Register now.

El registro confirma que sus alertas por correo electrónico funcionan, reduce el tiempo de resolución del soporte técnico y asegura la exactitud de su dirección de envío. También deseamos incorporar sus comentarios en el desarrollo de futuros productos. Nunca vendemos ni rentamos su correo electrónico y puede darse de baja de las comunicaciones.

Para registrar su switch con NETGEAR:

1. Visite el sitio web de registro de NETGEAR en https://my.netgear.com/registration/login.aspx.

2. Haga clic en el botón Login y siga las instrucciones en pantalla para registrar el switch con su dirección de correo electrónico y contraseña de NETGEAR.

Si aún no ha creado una cuenta de NETGEAR, haga clic en el enlace Create account, siga las instrucciones en pantalla para crear una cuenta y, después, registre el switch con su dirección de correo electrónico y contraseña de NETGEAR.

Descripción general de la UI principal del navegador local

Su switch contiene un servidor web integrado y software de administración para administrar y supervisar las funciones del switch. El switch funciona como un switch simple sin el software de administración. Sin embargo, puede usar el software de administración para configurar funciones más avanzadas que pueden mejorar la eficiencia del switch y el rendimiento general de la red.

El software del switch incluye un conjunto completo de funciones de administración para configurar y supervisar el sistema mediante uno de los siguientes métodos:

- Interfaz de usuario principal del navegador local (UI principal), ya sea a través de un puerto de red Ethernet o a través del puerto fuera de banda (OOB) (también llamado puerto de servicio)
- Interfaz de usuario de audio y video del navegador local (UI AV), ya sea a través de un puerto de red Ethernet o a través del puerto OOB
- Simple Network Management Protocol (SNMP)
- Interfaz de línea de comandos (CLI)

Cada uno de estos métodos de administración basados en estándares le permite configurar y monitorear los componentes del switch. El método que use depende del tamaño y los requisitos de su red, y de su preferencia.

Este manual describe cómo usar la interfaz de usuario (UI) principal del navegador local para administrar y supervisar el switch. Abreviamos la UI principal del navegador local como UI principal.

La UI principal es una herramienta de administración basada en web que le permite supervisar, configurar y controlar su switch de forma remota con un navegador web estándar. Desde su navegador web, puede supervisar el rendimiento de su switch y optimizar su configuración para su red. Puede configurar todas las funciones disponibles del switch, como VLAN, QoS y ACL, mediante la UI principal.

Iniciar sesión en la UI principal con un navegador web

Si es la primera vez que inicia sesión en el switch y debe usar la dirección IP predeterminada del switch, consulte la información de la guía de instalación.

Puede usar un navegador web para acceder al switch e iniciar sesión. Debe poder hacer ping a la dirección IP de la interfaz de administración o del puerto fuera de banda (OOB) desde su computadora para que el acceso web esté disponible.

De forma predeterminada, no se establece ninguna dirección IP para el puerto OOB, pero su cliente DHCP está habilitado para que el puerto pueda recibir una dirección IP de un servidor DHCP de su red. Si el puerto OOB no recibe una dirección IP de un servidor DHCP de su red, la dirección IP del puerto se establece en 192.168.0.239 con 255.255.255.0 como máscara de subred. Lo mismo ocurre si conecta el puerto OOB directamente a una computadora y reinicia el switch.

Nota: La primera vez que inicie sesión como usuario administrador en la UI principal, no se requiere contraseña (es decir, la contraseña está en blanco). Después de iniciar sesión por primera vez, deberá especificar una contraseña local del dispositivo que deberá usar cada vez que inicie sesión. (Puede volver a cambiar la contraseña).

Iniciar sesión en la UI principal con la dirección IP predeterminada del switch

Para usar la dirección IP predeterminada del switch para acceder al switch a través de la UI principal:

1. Prepare su computadora con una dirección IP estática:

   • Para acceder a través de un puerto de red Ethernet, use una dirección IP estática en la subred 169.254.0.0 con máscara de subred 255.255.0.0.
   Por ejemplo, use 169.254.100.201 para su computadora.
   • Para acceder a través del puerto OOB, use una dirección IP estática en la subred 192.168.0.0 con máscara de subred 255.255.0.0.
   Por ejemplo, use 192.168.0.201 para su computadora.

2. Conecte un cable Ethernet desde un puerto Ethernet de su computadora a un puerto de red Ethernet del switch o al puerto OOB del switch.

3. Si usa el puerto OOB, reinicie el switch para que la dirección IP del puerto OOB se establezca en 192.168.0.239 con 255.255.255.0 como máscara de subred.

4. Abra un navegador web como Google Chrome, Mozilla Firefox o Microsoft Edge.
5. Ingrese la dirección IP predeterminada del switch en el campo de dirección del navegador web:

   • Para acceder a través de un puerto de red Ethernet, ingrese 169.254.100.100.
   • Para acceder a través del puerto OOB, ingrese 192.168.0.239. Se muestra la página de inicio de sesión.

6. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

7. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

Iniciar sesión en la UI principal con una dirección IP conocida

Si no asignó una dirección IP estática al switch, sino que dejó que un servidor DHCP de su red le asignara una, determine la dirección IP consultando el servidor DHCP o con una utilidad de escaneo de IP.

Los procedimientos de este manual suponen que usted conoce la dirección IP de su switch.

Para usar una dirección IP conocida para acceder al switch a través de la UI principal:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

Botones y campos definidos por el usuario de la UI principal

La siguiente tabla muestra los botones de comando que se usan en las páginas de la UI principal:

Tabla 1. Botones de comando de la UI principal

Botón	Función
Add	Al hacer clic en el botón Add, se agrega el nuevo elemento configurado en la fila de encabezado de una tabla.
Apply	Al hacer clic en el botón Apply, se envía la configuración actualizada al switch. Los cambios de configuración surten efecto de inmediato.
Cancel	Al hacer clic en el botón Cancel, se cancela la configuración de la página y se restablecen los datos de la página a los valores anteriores del switch.
Delete	Al hacer clic en el botón Delete, se elimina el elemento seleccionado.
Refresh	Al hacer clic en el botón Refresh, se actualiza la página con la información más reciente del dispositivo.

Tabla 1. Botones de comando de la UI principal (continuación)

Botón	Función
Save	Al hacer clic en el botón Save, se guarda la configuración.
Logout	Al hacer clic en el botón Logout, se termina la sesión.

Los campos definidos por el usuario pueden contener de 1 a 159 caracteres, a menos que se indique otra cosa en la página web de configuración. Se pueden usar todos los caracteres excepto los siguientes (a menos que se indique específicamente para esa función):

Tabla 2. Caracteres no válidos para campos definidos por el usuario

Caracteres no válidos para campos definidos por el usuario
\ | / < > * ?

Convenciones de nomenclatura de interfaces

El switch admite interfaces físicas y lógicas. Las interfaces se identifican por su tipo y su número de interfaz. Los puertos físicos son interfaces Gigabit Ethernet o Ethernet multivelocidad de 10G y están numerados en el panel frontal. Usted configura las interfaces lógicas.

La siguiente tabla describe la convención de nomenclatura de todas las interfaces disponibles en el switch.

Tabla 3. Convenciones de nomenclatura de interfaces

Interfaz	Descripción	Ejemplo
Interfaces físicas	Según el modelo, los puertos físicos son interfaces Ethernet de 1G, 2.5G o 10G o interfaces de fibra de 1G o 10G. El número de interfaz consiste en el número del switch (siempre 0) seguido de una barra diagonal y el número de puerto, que es un número secuencial que empieza en 1.	0/1, 0/2, 0/3, etc.
Grupo de agregación de enlaces (LAG)	Las interfaces LAG son interfaces lógicas que se usan solo para funciones de puenteo.	LAG 1, LAG 2, LAG 3, etc.

Tabla 3. Convenciones de nomenclatura de interfaces (continuación)

Interfaz	Descripción	Ejemplo
Interfaz de administración de la CPU	Esta es la interfaz interna del switch responsable de la dirección MAC base del switch. Esta interfaz no es configurable y siempre aparece en la tabla MAC Address Table.	5/1
Interfaces VLAN de enrutamiento	Esta es una interfaz que se usa para la funcionalidad de enrutamiento.	VLAN 1, VLAN 2, VLAN 3, etc.

Guardar la configuración en la configuración en ejecución

Cuando hace clic en el botón Apply, los cambios se guardan para la sesión de administración web, pero no se conservan al reiniciar el switch. Para guardar los cambios en la configuración en ejecución (es decir, de forma permanente), haga clic en el ícono Save en la parte superior derecha de una página.

También puede hacer primero varios cambios sin hacer clic en el ícono Save después de cada cambio (aunque debe hacer clic en el botón Apply después de cada cambio) y, después, guardar la configuración en la configuración en ejecución. Para obtener más información, consulte Guardar la configuración en la página 734).

Ayuda en línea de la UI principal

Cuando inicia sesión en el switch, cada página contiene un enlace a la ayuda en línea, que contiene información para ayudarle a configurar y administrar el switch. Las ventanas emergentes de la ayuda en línea dependen del contexto. Por ejemplo, si la página IP Addressing está abierta, se muestra el tema de ayuda de esa página al hacer clic en el botón Help.

Puede conectarse al sitio de soporte en línea en netgear.com/support cuando haya iniciado sesión en el switch.

Para acceder al enlace de soporte en línea:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Help > Online Help > Support.

6. Para conectarse al sitio de soporte de NETGEAR para los switches de la serie M4250, haga clic en el botón Apply.

Usar Device View en la UI principal

Device View es un applet HTML que muestra los puertos del switch. Este gráfico ofrece otra forma de navegar a las opciones de configuración y supervisión. El gráfico también proporciona información sobre los puertos del dispositivo, la configuración y el estado actuales, tablas y componentes de funciones.

Para usar Device View:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

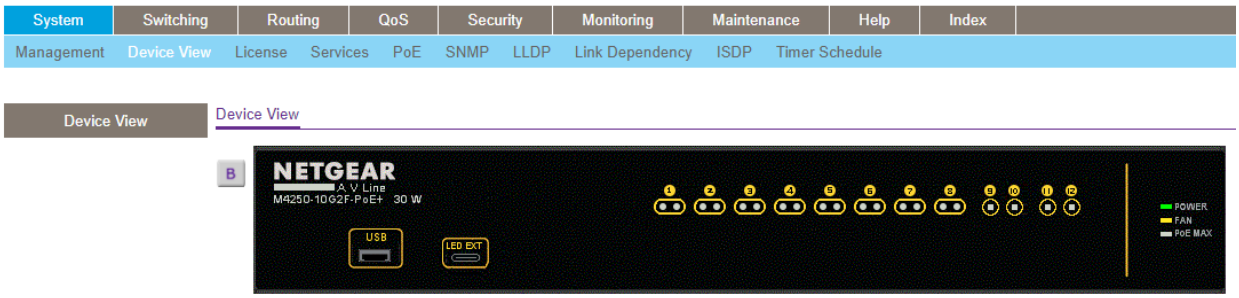
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

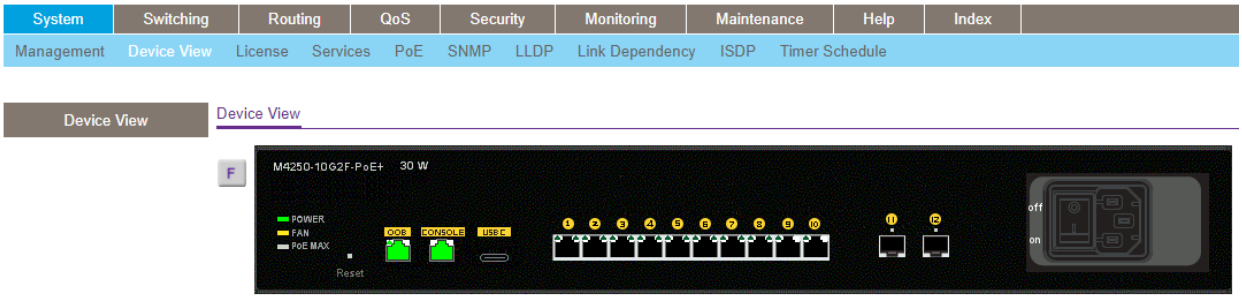
5. Seleccione System > Device View.
Se muestra la vista frontal del switch en Device View.

Como ejemplo, la siguiente figura muestra la vista frontal del modelo M4250-10G2F-PoE+.



6. Para mostrar la vista posterior, haga clic en el botón B.
El botón B cambia al botón F. (Al hacer clic en el botón F, se vuelve a mostrar la vista frontal).

Como ejemplo, la siguiente figura muestra la vista posterior del modelo M4250-10G2F-PoE+.



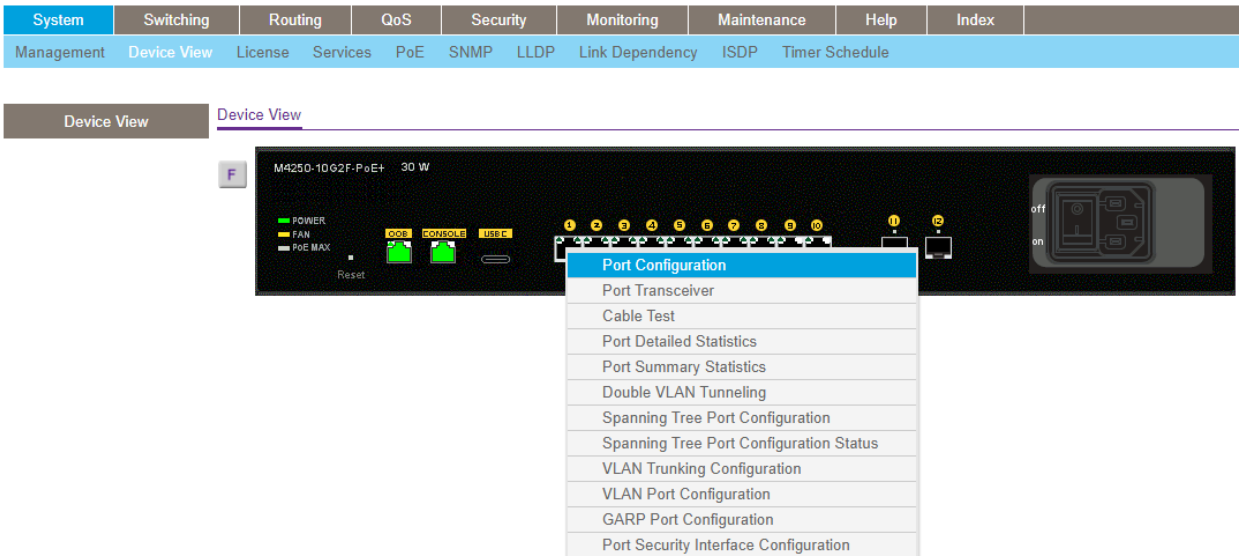
El color del puerto indica su estado:

- Negro. El puerto no está conectado a un dispositivo o está deshabilitado.
- Verde. El puerto está conectado a un dispositivo o habilitado.
- Rojo. Se produjo un error en el puerto.

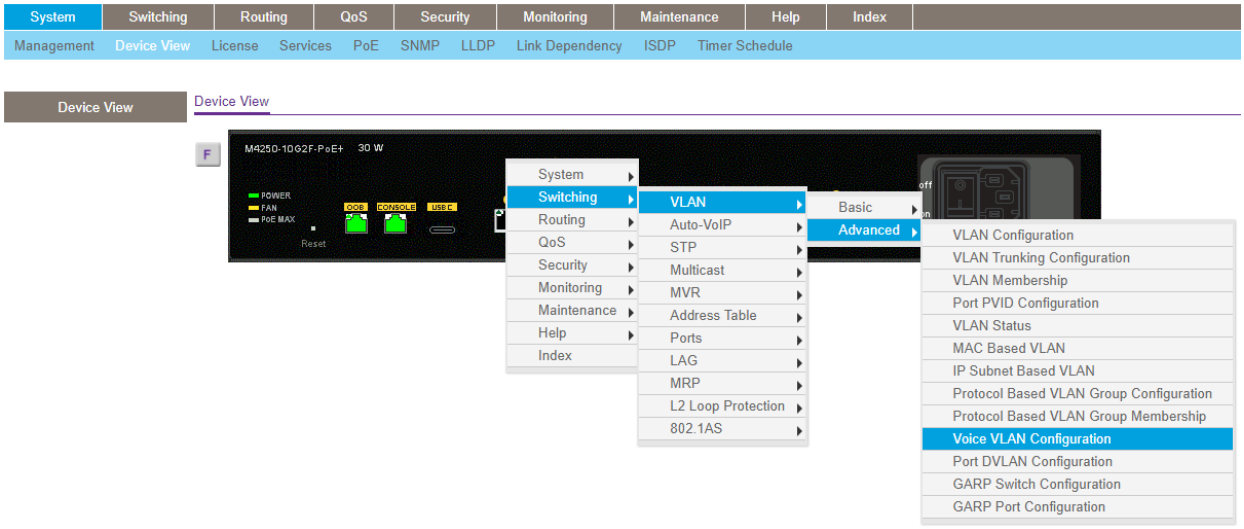
Los LED del sistema indican el estado del sistema. Para obtener más información, consulte la guía de instalación del hardware, que puede descargar en netgear.com/support/download/.

7. Para mostrar los menús que le permiten configurar puertos, haga clic con el botón derecho en un puerto.

Como ejemplo, la siguiente figura muestra la vista posterior del modelo M4250-10G2F-PoE+ con una vista parcial de los menús que le permiten configurar un puerto.



8. Para mostrar los menús que le permiten configurar los ajustes globales del switch, haga clic con el botón derecho en la vista posterior en cualquier lugar que no sea un puerto. Como ejemplo, la siguiente figura muestra la vista posterior del modelo M4250-10G2F-PoE+ con los menús que le permiten configurar los ajustes globales del switch.



Configurar el acceso SNMP

El software del switch admite la configuración de grupos y usuarios SNMP que pueden administrar las traps que genera el agente SNMP.

El switch usa tanto MIB públicas estándar para la funcionalidad estándar como MIB privadas que admiten funcionalidad adicional del switch. Todas las MIB privadas empiezan con el prefijo “-”. El objeto principal para la configuración de interfaces está en -SWITCHING-MIB, que es una MIB privada. Algunas configuraciones de interfaz también implican objetos de la MIB pública IF-MIB.

SNMP está habilitado de forma predeterminada. La página System Information, que es la página que se muestra al iniciar sesión, muestra la información que necesita para configurar un administrador SNMP para acceder al switch.

Cualquier usuario puede conectarse al switch mediante el protocolo SNMP v3, pero para la autenticación y el cifrado, el switch admite solo un usuario, que es el usuario admin; por lo tanto, solo se puede crear o modificar un perfil.

No puede acceder al switch mediante SNMPv3 hasta que inicie sesión en el switch como admin y cambie la contraseña predeterminada (consulte Iniciar sesión en la UI principal con un navegador web en la página 24). Después de hacerlo, SNMPv3 se configura automáticamente con el protocolo de autenticación MD5 y la nueva contraseña del usuario admin.

Para el acceso al switch mediante SNMPv3, el protocolo de autenticación debe ser MD5 o SHA. No puede usar la opción “none” para el protocolo de autenticación.

Para obtener más información sobre SNMP, consulte Simple Network Management Protocol en la página 151.

Para configurar los ajustes de autenticación y cifrado del perfil admin de SNMPv3:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP v3 User Configuration. Se muestra la página User Configuration.

6. Para habilitar la autenticación, seleccione una opción de Authentication Protocol, que puede ser MD5 o SHA.

7. Para habilitar el cifrado, seleccione la opción DES en la lista Encryption Protocol. Después, ingrese un código de cifrado de ocho o más caracteres alfanuméricos en el campo Encryption Key.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Nota: Para acceder a la información de configuración de SNMP V1 o SNMP V2, seleccione System > SNMP > SNMPv1/v2 y seleccione la página que contiene la información que desea configurar.

2

Configurar la información del sistema del switch

Este capítulo trata los siguientes temas:

- Información del sistema del switch
- Interfaz loopback
- Interfaces y VLAN de administración IPv4
- Interfaces y VLAN de administración IPv6
- Configuración de hora y SNTP
- Precision Time Protocol
- Domain Name System
- Plantilla de administración de la base de datos del switch
- Configuración de Green Ethernet
- Configuración de Bonjour
- Servidor DHCP IPv4
- Relay DHCP y estadísticas de relay
- Relay DHCP de capa 2
- Relay UDP
- Servidor DHCPv6
- Interfaz de relay DHCPv6
- Power over Ethernet
- Programaciones de temporizador
- Simple Network Management Protocol
- Link Layer Discovery Protocol
- Link Layer Discovery Protocol for Media Endpoint Devices
- Dependencia de enlaces
- Industry Standard Discovery Protocol

Información del sistema del switch

Puede ver y configurar la información del sistema del switch.

Ver y configurar la información del sistema del switch

Cuando inicia sesión, se muestra la página System Information. Puede configurar y ver información general del dispositivo.

Para ver y definir la información del sistema:

1. Abra un navegador web.

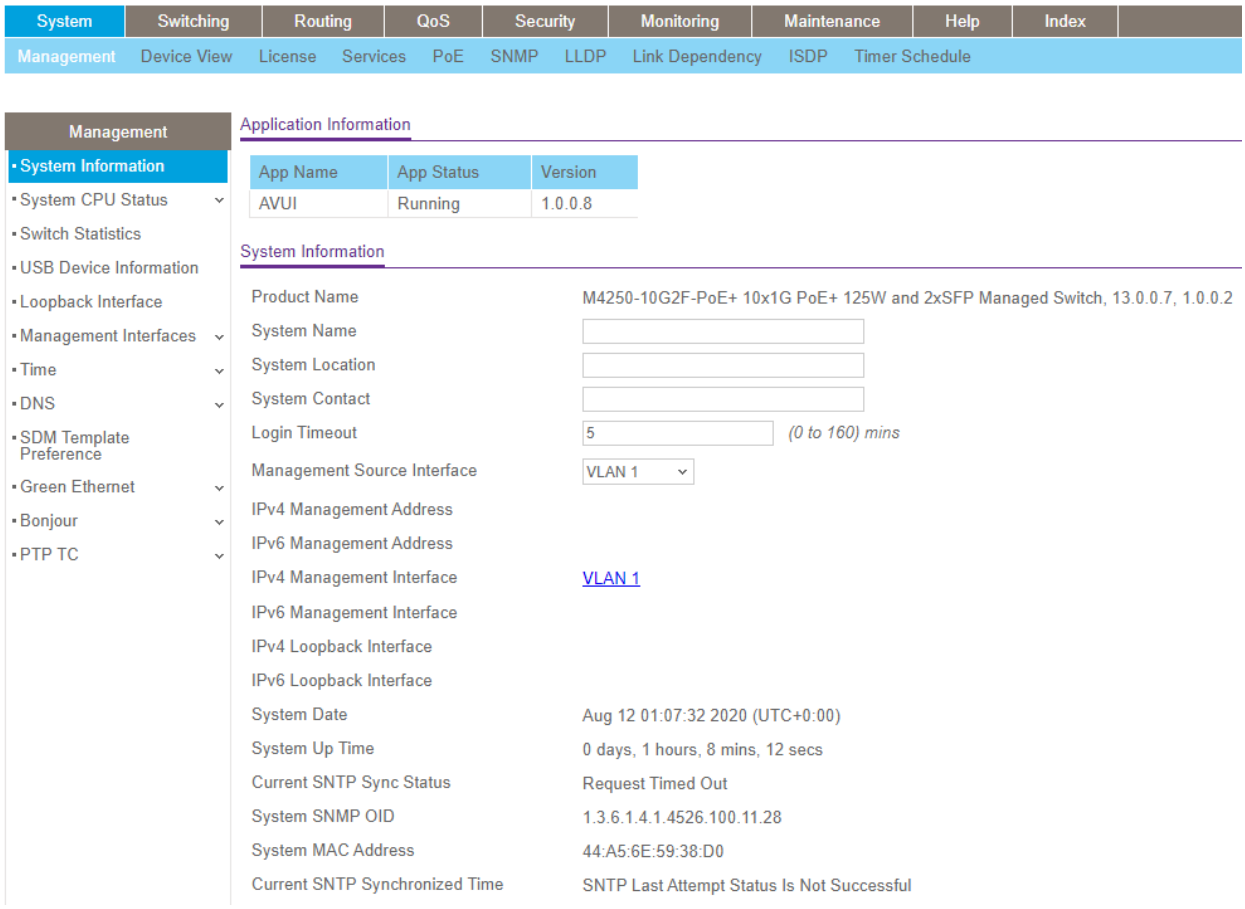
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > System Information.



6. Defina los siguientes campos:

• System Name: Ingrese el nombre para identificar este switch. Puede usar hasta 255 caracteres alfanuméricos. El valor predeterminado de fábrica es en blanco.
• System Location: Ingrese la ubicación de este switch. Puede usar hasta 255 caracteres alfanuméricos. El valor predeterminado de fábrica es en blanco.
• System Contact: Ingrese la persona de contacto de este switch. Puede usar hasta 255 caracteres alfanuméricos. El valor predeterminado de fábrica es en blanco.
• Login Timeout: Especifique cuántos minutos de inactividad pueden transcurrir en una conexión de puerto serie antes de que el switch cierre la conexión. Ingrese un número entre 0 y 160 minutos. El valor predeterminado de fábrica es 5. Ingresar 0 deshabilita el tiempo de espera.
• Management Source Interface: Seleccione la interfaz de administración que se usa como interfaz de origen para las aplicaciones SNMP trap, syslog, DNS, TACACS+, RADIUS, sflow y SNTP. Los valores posibles son los siguientes:

- **None**
- **Routing Interface**
- **Routing VLAN**

- **Routing Loopback Interface**
- **Service Port**
- Different. Para algunas aplicaciones de la lista, la interfaz de origen se configura por separado. Solo aparecen en la lista si este es el caso.

De forma predeterminada, se usa VLAN 1 como interfaz de origen.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información de estado de las secciones Application Information y System Information de la página.

Tabla 4. Application Information y System Information

Campo	Descripción
Application Information	
App Name	El nombre de la aplicación que funciona como agente Universal Plug and Play (UPnP).
App Status	El estado de la aplicación.
Version	La versión de la aplicación.
System Information	
Product Name	El nombre de producto de este switch.
IPv4 Management Address	La dirección IPv4 y la máscara asignadas a la interfaz VLAN de administración.
IPv6 Management Address	La dirección IPv6 y la máscara asignadas a la interfaz VLAN de administración.
IPv4 Management Interface	El ID de VLAN de administración IPv4 del switch. Haga clic en el valor de Management VLAN ID que se muestra para ir a la página de configuración. Consulte Configurar una VLAN de administración IPv4 en la página 49.
IPv6 Management Interface	El ID de VLAN de administración IPv6 del switch. Haga clic en el valor de Management VLAN ID que se muestra para ir a la página de configuración. Consulte Configurar una VLAN de administración IPv6 en la página 56.
IPv4 Loopback Interface	La dirección IPv4 y la máscara asignadas a la interfaz loopback.
IPv6 Loopback Interface	El prefijo IPv6 y la longitud de prefijo asignados a la interfaz loopback.
System Date	La fecha actual.
System Up Time	El tiempo en días, horas y minutos desde que se reinició el switch.

Tabla 4. Application Information y System Information (continuación)

Campo	Descripción
Current SNTP Sync Status	El estado actual de sincronización SNTP.
System SNMP OID	El ID de objeto base de la MIB empresarial del switch.
System Mac Address	Dirección de red asignada universalmente.
Current SNTP Synchronized Time	La hora sincronizada por SNTP.

Ver el estado de los ventiladores

Esta página muestra el estado de los ventiladores de todas las unidades. Estos ventiladores eliminan el calor generado por la fuente de alimentación, la CPU y otros chipsets, y permiten que los chipsets funcionen normalmente.

Para ver el estado de los ventiladores:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Desplácese hacia abajo hasta la sección Fan Status.
6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe la información no configurable de Fan Status.

   La cantidad de ventiladores depende del modelo de switch.

Tabla 5. Fan Status

Campo	Descripción
Unit ID	El ID de unidad del switch en el que está instalado el ventilador. Este ID siempre es 1.
FAN	El ID del ventilador (1, 2 o 3)

Tabla 5. Fan Status (continuación)

Campo	Descripción
Description	La descripción del ventilador (FAN-1, FAN-2 o FAN-3).
Type	El tipo de ventilador siempre es Fixed.
Speed	La velocidad del ventilador. Para obtener más información, consulte la guía de instalación del hardware, que puede descargar en netgear.com/support/download/.
Duty Level	El nivel de trabajo del ventilador en porcentaje.
FAN Status	El estado del ventilador: • Operational: El ventilador funciona normalmente. • Failure: El ventilador falló. • Not Present: El ventilador no está presente. (La cantidad de ventiladores depende del modelo de switch). • Stop: El ventilador se detuvo porque la temperatura del switch es baja. El ventilador arrancará si la temperatura del switch aumenta.

Ver la información de los sensores de temperatura

Puede ver la temperatura actual de los distintos sensores del sistema en la tabla Temperature Status.

Para ver la información de temperatura:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Desplácese hacia abajo hasta la sección Temperature Status.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe la información no configurable de Temperature Status.

Tabla 6. Información de Temperature Status

Campo	Descripción
Unit ID	El ID de unidad del switch en el que está instalado el sensor. Este ID siempre es 1.
Sensor	El ID del sensor.
Description	La descripción del sensor.
Temperature (C)	La temperatura del sensor en grados Celsius.
State	El estado del sensor: Operational o Failure.
Max Temp (C)	La temperatura de funcionamiento máxima admitida en grados Celsius.

Ver el estado del dispositivo y la versión de firmware

Puede ver el estado del dispositivo y la versión de firmware.

Para ver el estado del dispositivo y la versión de firmware:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Desplácese hacia abajo hasta la sección Temperature Status.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe la información no configurable de Device Status.

Tabla 7. Device Status

Campo	Descripción
Firmware Version	El número de versión principal, versión y mantenimiento del firmware que se ejecuta en el switch. Por ejemplo, si la versión principal es 1, la versión es 2 y el número de mantenimiento es 4, el formato es 1.2.4.
Boot Version	La versión del código de arranque que está en la memoria flash para cargar el firmware en la memoria.
CPLD Version	La versión del software del dispositivo lógico programable complejo (CPLD) del switch.
Serial Number	El número de serie del switch.
PS-1	El estado de la fuente de alimentación del switch: • Operational: La fuente de alimentación está presente y funciona correctamente. • Failed: La fuente de alimentación está presente, pero el cable de alimentación no está conectado o hay un cable defectuoso conectado.
PoE MÁX.	El estado del sistema PoE del switch: • ON: Hay menos de 10 W de alimentación PoE disponibles para otro PD. • OFF: Hay al menos 10 W de alimentación PoE disponibles para otro PD. • N/A: El switch no admite PoE.
System Up Time	El tiempo en días, horas y minutos desde que se reinició el switch.

Ver el estado de la CPU del sistema

Para ver el estado de la CPU del sistema:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > Management > System CPU Status. Se muestra la página System CPU Status.

El estado de memoria de la CPU incluye la memoria total del switch en KBytes y el espacio de memoria disponible del switch en KBytes.

La utilización de CPU muestra el uso de la CPU por los distintos procesos del switch.

Configurar los umbrales de CPU

Puede configurar umbrales de CPU que, al superarse, generan una notificación. La notificación se envía mediante traps SNMP y mensajes de syslog.

Para configurar los umbrales de CPU:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > System CPU Status > CPU Threshold. Se muestra la página CPU Threshold.

6. Configure los siguientes ajustes de umbral de CPU:

- Rising Threshold: Configure el valor del umbral ascendente. Se genera una notificación cuando el uso total de CPU supera este valor durante el período de tiempo configurado. El rango es un porcentaje de 1 a 100.
- Rising Interval: Configure el valor del intervalo ascendente. Configure este período de monitoreo de uso de 5 a 86400 segundos, en múltiplos de 5 segundos.
- Falling Threshold: Configure el umbral descendente. Se genera una notificación cuando el uso total de CPU baja de este nivel durante un período configurado.

El umbral descendente debe ser igual o menor que el valor del umbral ascendente. La notificación del umbral descendente solo se genera si antes se generó una notificación del umbral ascendente. Configurar el umbral descendente y su período es opcional. Si no se configuran los valores descendentes de uso de CPU, toman los mismos valores que los ascendentes. El rango es un porcentaje de 1 a 100.
• Falling Interval: Configure el intervalo descendente. Puede configurar el período de monitoreo de uso de 5 a 86400 segundos, en múltiplos de 5 segundos.
• Free Memory Threshold: Configure el umbral de memoria libre de la CPU en KB.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Ver o borrar las estadísticas del switch

Para ver o borrar las estadísticas del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Switch Statistics. Se muestra la página Switch Statistics.

6. Para borrar todos los contadores y restablecer las estadísticas resumidas y detalladas a sus valores predeterminados, haga clic en el botón Clear.
El conteo de paquetes descartados no se puede borrar.

7. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información de estadísticas del switch.

Tabla 8. Información de estadísticas del switch

Campo	Descripción
ifIndex	El ifIndex de la entrada de la tabla de interfaces asociada con el procesador de este switch.
Octetos recibidos	Número total de octetos de datos recibidos por el procesador (sin incluir bits de trama, pero incluyendo octetos FCS).
Paquetes recibidos sin errores	Número total de paquetes (incluidos paquetes broadcast y multicast) recibidos por el procesador.
Paquetes unicast recibidos	Número de paquetes unicast de subred entregados a un protocolo de capa superior.
Paquetes multicast recibidos	Número total de paquetes recibidos dirigidos a una dirección multicast. Este número no incluye los paquetes dirigidos a la dirección de broadcast.
Paquetes broadcast recibidos	Número total de paquetes recibidos dirigidos a la dirección de broadcast. No incluye paquetes multicast.
Paquetes recibidos descartados	Número de paquetes entrantes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Una posible razón para descartar un paquete es liberar espacio de búfer.
Octetos transmitidos	Número total de octetos transmitidos por la interfaz, incluidos los caracteres de trama.
Paquetes transmitidos sin errores	Número total de paquetes transmitidos por la interfaz.
Paquetes unicast transmitidos	Número total de paquetes que los protocolos de nivel superior solicitaron transmitir a una dirección unicast de subred, incluidos los que se descartaron o no se enviaron.
Paquetes multicast transmitidos	Número total de paquetes que los protocolos de nivel superior solicitaron transmitir a una dirección multicast, incluidos los que se descartaron o no se enviaron.
Paquetes broadcast transmitidos	Número total de paquetes que los protocolos de nivel superior solicitaron transmitir a la dirección de broadcast, incluidos los que se descartaron o no se enviaron.
Paquetes transmitidos descartados	Número de paquetes salientes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Una posible razón para descartar un paquete es liberar espacio de búfer.
Máximo de entradas de direcciones usadas	Mayor número de entradas de la tabla de direcciones de la base de datos de reenvío aprendidas por este switch desde el último reinicio.
Entradas de direcciones en uso	Número de entradas aprendidas y estáticas en la tabla de direcciones de la base de datos de reenvío de este switch.
Máximo de entradas VLAN	Número máximo de LAN virtuales (VLAN) permitidas en este switch.

Tabla 8. Información de estadísticas del switch (continuación)

Campo	Descripción
Máximo de entradas VLAN usadas	Mayor número de VLAN que estuvieron activas en este switch desde el último reinicio.
Entradas VLAN estáticas	Número de entradas VLAN activas actualmente en este switch que se crearon de forma estática.
Entradas VLAN dinámicas	Número de entradas VLAN activas actualmente en este switch que se crearon mediante registro GVRP.
VLAN eliminadas	Número de VLAN de este switch que se crearon y luego se eliminaron desde el último reinicio.
Tiempo desde el último borrado de contadores	Tiempo transcurrido, en días, horas, minutos y segundos, desde que se borraron por última vez las estadísticas de este switch.

Ver la información del dispositivo USB

Para mostrar la información del dispositivo USB:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Management > USB Device Information. Se muestra la página USB Device Information.

   El campo Device Status muestra el estado actual del dispositivo. El estado es uno de los siguientes:

   • Active: El dispositivo USB está conectado y el switch lo reconoce.
   • Inactive: El dispositivo no está montado.
   • Invalid: El dispositivo no está presente o se conectó un dispositivo no válido.

6. Para actualizar la página, haga clic en el botón Refresh.

La siguiente tabla describe la información de la sección USB Memory Statistics.

Tabla 9. Información de USB Memory Statistics

Campo	Descripción
Tamaño total	Tamaño de almacenamiento del dispositivo flash USB en bytes.
Bytes usados	Cantidad de memoria usada en el dispositivo flash USB.
Bytes libres	Cantidad de memoria libre en el dispositivo flash USB.

La siguiente tabla describe la información de la sección USB Directory Details.

Tabla 10. Información de USB Directory Details

Campo	Descripción
Nombre de archivo	Nombre del archivo almacenado en la unidad flash USB.
Tamaño de archivo	Tamaño en bytes del archivo almacenado en la unidad flash USB
Hora de modificación	Hora de la última modificación del archivo almacenado en la unidad flash USB.

Interfaz loopback

Puede crear, configurar y eliminar interfaces loopback.

Para configurar una interfaz loopback:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Loopback Interface. Se muestra la página Loopback Interface.

6. En el menú Loopback Interface Type, seleccione IPv4 o IPv6.
7. En el menú Loopback ID, seleccione una interfaz.
8. Configure los siguientes ajustes, según el tipo de interfaz loopback:
• IPv4: Para una interfaz IPv4, configure los siguientes ajustes:

- Primary IP Address: Ingrese la dirección IPv4 principal de esta interfaz en notación decimal con puntos.
- Primary IP Subnet Mask: Ingrese la máscara de subred IPv4 principal en notación decimal con puntos.

• IPv6: Para una interfaz IPv6, configure los siguientes ajustes:

- IPv6 mode: Seleccione Enable para usar la dirección IPv6 después de especificarla. Solo puede seleccionar esta opción antes de especificar la dirección IPv6.
- IPv6 Prefix: Ingrese el prefijo IPv6.
- Prefix Length: Ingrese la longitud del prefijo IPv6.
- EUI64: Opcionalmente, especifique el identificador único extendido de 64 bits (EUI-64).

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Interfaces y VLAN de administración IPv4

La interfaz principal ofrece opciones separadas para la administración IP por interfaz IPv4 y por puerto.

Si configura la administración IP basada en puerto, se desactiva la basada en VLAN. Del mismo modo, si configura la administración IP basada en VLAN, se desactiva la basada en puerto.

De forma predeterminada, la interfaz de origen de las aplicaciones es la VLAN 1. Si cambia la VLAN y el puerto de administración IPv4 a un valor no predeterminado, la interfaz de origen de la VLAN 1 predeterminada y el puerto también cambian automáticamente.

Puede acceder al switch mediante la interfaz principal con uno de los siguientes métodos:

- Puerto de servicio IPv4: El puerto de servicio es un puerto Ethernet dedicado para la administración fuera de banda (OOB) del switch. El tráfico en este puerto está separado del

tráfico de la red operativa en los puertos del switch y no se puede conmutar ni enrutar a la red operativa.

- Interfaz VLAN de administración: La VLAN de administración es la interfaz lógica usada para la conectividad en banda con el switch a través de cualquiera de sus interfaces de red. Para acceder al switch por una red, primero debe configurar una dirección IP y una máscara de subred para el switch.
- Interfaz de administración única opcional: De forma predeterminada, puede usar cualquier interfaz de red del switch como interfaz de administración. Sin embargo, puede restringir la administración IPv4 a una interfaz de red específica.

Configurar el puerto de servicio IPv4

Puede configurar la información de red del puerto de servicio IPv4, también llamado puerto fuera de banda (OOB). El puerto de servicio es un puerto Ethernet dedicado para la administración fuera de banda del switch. Su tráfico está separado del tráfico de la red operativa en los puertos del switch y no se puede conmutar ni enrutar a la red operativa.

De forma predeterminada, no se establece ninguna dirección IP para el puerto OOB, pero su cliente DHCP está habilitado para que el puerto pueda recibir una dirección IP de un servidor DHCP de su red. Si el puerto OOB no recibe una dirección IP de un servidor DHCP de su red, la dirección IP del puerto se establece en 192.168.0.239 con 255.255.255.0 como máscara de subred. Lo mismo ocurre si conecta el puerto OOB directamente a una computadora y reinicia el switch.

Para configurar el puerto de servicio IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv4 Service Port Configuration.
Se muestra la página IPv4 Service Port Configuration.

6. Seleccione un botón de opción de Service Port Configuration Protocol:

• Bootp: En el siguiente ciclo de arranque, el cliente BootP del dispositivo difunde una solicitud BootP para obtener información de un servidor BootP de la red. Los campos IP Address, Subnet Mask y Default Gateway muestran la información obtenida dinámicamente.
• DHCP: En el siguiente ciclo de arranque, el cliente DHCP del dispositivo difunde una solicitud DHCP para obtener información de un servidor DHCP de la red. Los campos IP Address, Subnet Mask y Default Gateway muestran la información obtenida dinámicamente.
• None: El dispositivo no intenta obtener la información de red dinámicamente. Debe configurar las direcciones manualmente:

- IP Address: Especifique la dirección IP de la interfaz.
- Subnet Mask: Especifique la máscara de subred IP de la interfaz.
- Default Gateway: Especifique la puerta de enlace predeterminada de la interfaz IP.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 11. Información de configuración del puerto de servicio IPv4

Campo	Descripción
Dirección MAC grabada	Dirección MAC grabada de fábrica usada para la conectividad fuera de banda.
Estado de la interfaz	Indica si el estado del enlace está activo o inactivo.
Identificador de cliente DHCP	Si se seleccionó DHCP, el ID de cliente DHCP.

Configurar una VLAN de administración IPv4

Para administrar el switch mediante la interfaz principal, debe definir la dirección IP de administración. De forma predeterminada se crea una interfaz VLAN de administración que obtiene una dirección IP si hay un servidor DHCP. Si no puede obtener una dirección IP, la dirección IPv4 de respaldo asignada automáticamente es 169.254.100.100 y la máscara de subred es 255.255.0.0.

La VLAN de administración se usa como interfaz de origen predeterminada para syslog, el registro de mensajes, un cliente SNMP, etc. La interfaz de red está desactivada de forma predeterminada.

La VLAN de administración es la interfaz lógica usada para la conectividad en banda con el switch a través de cualquiera de los puertos del panel frontal. Los parámetros de configuración

asociados con la VLAN de administración del switch no afectan la configuración de los puertos del panel frontal por los que se conmuta o enruta el tráfico.

Para acceder al switch por una red, primero debe configurar una dirección IP y máscara de subred para el switch. Puede configurar la información IP mediante cualquiera de estos:

- DHCP
- Interfaz de terminal a través del puerto EIA-232

Después de establecer la conectividad en banda, puede cambiar la información IP mediante cualquiera de estos:

- Interfaz de terminal a través del puerto EIA-232
- Interfaz de terminal a través de Telnet
- Administración basada en SNMP
- Administración basada en web

Para configurar o restablecer la VLAN de administración IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv4 Management VLAN Configuration.
Se muestra la página IPv4 Management VLAN Configuration.

6. En el campo Management VLAN ID, especifique el ID de la VLAN de administración del switch. La VLAN de administración IPv4 se usa para administrar el switch. Puede configurar cualquier valor en el rango de 1 a 4093.

7. Seleccione el botón de opción Routing Mode Enable o Disable para activar o desactivar el enrutamiento global en el switch.
El valor predeterminado es Enable.

8. Seleccione el botón de opción Configuration Method DHCP o Manual para especificar la acción de arranque del switch:

- DHCP: El switch solicita la información de dirección IP a un servidor DHCP.
- Manual: El switch carga la información de dirección IP que usted especifique:

  - IP Address: Especifique la dirección IP de la interfaz.
    El valor predeterminado es 169.254.100.100.
  - Subnet Mask: Especifique la máscara de subred IP de la interfaz. También se llama máscara de subred/red y define la parte de la dirección IP de la interfaz que identifica la red conectada.
    El valor predeterminado es 255.255.0.0.
  - Gateway: Especifique la puerta de enlace de la interfaz.
    El valor predeterminado es 0.0.0.0.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Nota: Si necesita restablecer la VLAN de administración IPv4, en la sección Reset IPv4 Management Interface de la página, marque la casilla Set Management Interface to Default y haga clic en el botón Apply. Esto elimina la configuración de la interfaz de administración IPv4 basada en puerto y restablece la interfaz de administración IPv4 a la VLAN 1 predeterminada.

La sección Current IPv4 Management Interface Status muestra los siguientes campos no configurables.

Tabla 12. Información no configurable del estado de la interfaz de administración IPv4

Campo	Descripción
Interfaz de administración	Muestra la VLAN de administración IPv4 actual.
Estado del enlace	Indica si el estado del enlace está activo o inactivo.
Estado de la interfaz de enrutamiento	Indica si el estado del enlace está activo o inactivo para la interfaz de administración.
Dirección MAC	Dirección MAC asignada a la interfaz de administración.
Método de configuración de dirección IP	Indica si el método de configuración de la dirección IP es DHCP o manual.
Dirección IP	Dirección IP de la interfaz de administración.

Tabla 12. Información no configurable del estado de la interfaz de administración IPv4 (continuación)

Campo	Descripción
Máscara de subred	Máscara de subred IP de la interfaz de administración.
Puerta de enlace	Puerta de enlace predeterminada especificada para la interfaz de administración.

Configurar una interfaz de administración IPv4

Puede restringir la administración IPv4 a una interfaz específica. De forma predeterminada, puede usar cualquiera de las interfaces como interfaz de administración IPv4.

Para configurar una interfaz de administración IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv4 Management Interface Configuration.
Se muestra la página IPv4 Management Interface Configuration.

6. En el menú Interface, seleccione la interfaz que será la interfaz de administración IPv4.

7. Marque la casilla Set Management Interface para poder configurar los ajustes de dirección IP de la interfaz

8. Seleccione un botón de opción de Configuration Method:

• DHCP: El switch obtiene la configuración de dirección IP de la interfaz de administración de un servidor DHCP de la red.
• Manual: Configure manualmente la dirección IP de la interfaz de administración:

- IP Address: Especifique la dirección IP de la interfaz de administración.
- Subnet Mask: Especifique la máscara de subred de la interfaz de administración.

- Gateway: Especifique la dirección IP de la puerta de enlace predeterminada de la interfaz de administración.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Nota: Si necesita restablecer la interfaz de administración IPv4, en la sección Reset IPv4 Management Interface de la página, marque la casilla Set Management Interface to Default y haga clic en el botón Apply. Esto elimina la configuración de la interfaz de administración IPv4 y la restablece a su configuración predeterminada.

La sección Current IPv4 Management Interface muestra los siguientes campos no configurables.

Tabla 13. Información no configurable del estado de la interfaz de administración IPv4

Campo	Descripción
Interfaz de administración	Muestra la interfaz de administración IPv4 actual
Estado del enlace	Indica si el estado del enlace está activo o inactivo.
Estado de la interfaz de enrutamiento	Indica si el estado del enlace está activo o inactivo para la interfaz de administración.
Dirección MAC	Dirección MAC asignada a la interfaz de administración.
Método de configuración de dirección IP	Indica si el método de configuración de la dirección IP es DHCP o manual.
Dirección IP	Dirección IP de la interfaz de administración.
Máscara de subred	Máscara de subred IP de la interfaz de administración.
Puerta de enlace	Puerta de enlace predeterminada especificada para la interfaz de administración.

Interfaces y VLAN de administración IPv6

La interfaz principal ofrece opciones separadas para la administración IP por interfaz IPv6 y por puerto.

Si configura la administración IP basada en puerto, se desactiva la basada en VLAN. Del mismo modo, si configura la administración IP basada en VLAN, se desactiva la basada en puerto.

De forma predeterminada, la interfaz de origen de las aplicaciones es la VLAN 1. Si cambia la VLAN y el puerto de administración IPv6 a un valor no predeterminado, la interfaz de origen de la VLAN 1 predeterminada y el puerto también cambian automáticamente.

Puede acceder al switch mediante la interfaz principal con uno de los siguientes métodos:

- Puerto de servicio IPv6: El puerto de servicio es un puerto Ethernet dedicado para la administración fuera de banda del switch. Su tráfico está separado del tráfico de la red operativa en los puertos del switch y no se puede conmutar ni enrutar a la red operativa.
- Interfaz VLAN de administración: La VLAN de administración es la interfaz lógica usada para la conectividad en banda con el switch a través de cualquiera de sus interfaces de red. Para acceder al switch por una red, primero debe configurar una dirección IP y máscara de subred para el switch. Para la VLAN de administración IPv6, puede usar la misma VLAN que para la administración IPv4 u otra distinta. El switch no ofrece una VLAN de administración IPv6 predeterminada. Si desea usar una, debe crearla manualmente.
- Interfaz de administración única opcional: De forma predeterminada, puede usar cualquier interfaz de red del switch como interfaz de administración. Sin embargo, puede restringir la administración IPv6 a una interfaz de red específica.

Configurar un puerto de servicio IPv6

Puede configurar la información de red IPv6 en el puerto de servicio. El puerto de servicio es un puerto Ethernet dedicado para la administración fuera de banda del switch. Su tráfico está separado del tráfico de la red operativa en los puertos del switch y no se puede conmutar ni enrutar a la red operativa.

Para configurar el puerto de servicio IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Service Port Configuration.
Se muestra la página IPv6 Service Port Configuration.

6. Seleccione el botón de opción IPv6 mode Enable o Disable. Esto especifica el modo administrativo IPv6 en el puerto de servicio.

7. Seleccione el botón de opción Service Port Configuration Protocol None o DHCP. Esto especifica si el dispositivo obtiene la información de red de un servidor DHCPv6. Al seleccionar None se desactiva el cliente DHCPv6 en el puerto de servicio.

Si selecciona el botón de opción DHCP, el campo DHCPv6 Client DUID muestra el identificador de cliente que usa el cliente DHCPv6 al enviar mensajes al servidor DHCPv6.

8. Seleccione el botón de opción IPv6 Stateless Address AutoConfig mode Enable o Disable:

• Enable: El puerto de servicio puede obtener una dirección IPv6 mediante el protocolo Neighbor Discovery Protocol (NDP) de IPv6 y mensajes de anuncio de router.
• Disable: El puerto de servicio no usa la función nativa de autoconfiguración de direcciones IPv6 para obtener una dirección IPv6.

Esto establece el modo de autoconfiguración de direcciones IPv6 sin estado en el puerto de servicio.

9. Para configurar la puerta de enlace IPv6, haga lo siguiente:

a. Marque la casilla Change IPv6 Gateway.

La puerta de enlace IPv6 es la puerta de enlace predeterminada de la interfaz del puerto de servicio IPv6.

b. En el campo IPv6 Gateway, especifique la puerta de enlace predeterminada de la interfaz del puerto de servicio IPv6.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Administrar direcciones IPv6 del puerto de servicio IPv6

Puede agregar una dirección IPv6 estática específica del puerto de servicio IPv6. También puede eliminar una dirección IPv6 que ya no necesite para el puerto de servicio IPv6.

Para agregar o eliminar una dirección IPv6 del puerto de servicio IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Service Port Configuration.
Se muestra la página IPv6 Service Port Configuration.

La tabla Add/Delete IPv6 Address muestra las direcciones IPv6 estáticas que agregó manualmente a la interfaz del puerto de servicio.

6. Para agregar una dirección IPv6, en la sección Add/Delete IPv6 Address, haga lo siguiente: a. En el campo IPv6 Address, especifique la dirección IPv6 que desea agregar. b. En el menú EUI FLAG, seleccione True para habilitar el indicador Extended Universal Identifier

(EUI) de la dirección IPv6, o seleccione False para omitirlo. c.
Haga clic en el botón Agregar (Add).
La dirección IPv6 se agrega al puerto de servicio IPv6.

7. Para eliminar una dirección IPv6, en la sección Add/Delete IPv6 Address, haga lo siguiente: a. Active la casilla de la dirección IPv6 que desea eliminar. b. Haga clic en el botón Eliminar (Delete).

La dirección IPv6 se elimina del puerto de servicio IPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una VLAN de administración IPv6

Para administrar el switch mediante la interfaz principal, debe definir la dirección IP de administración. De forma predeterminada se crea una interfaz VLAN de administración que obtiene una dirección IP si hay un servidor DHCP. Si no puede obtener una dirección IP, la dirección IPv4 de respaldo asignada automáticamente es 169.254.100.100 y la máscara de subred es 255.255.0.0.

La VLAN de administración se usa como interfaz de origen predeterminada para syslog, el registro de mensajes, un cliente SNMP, etc. La interfaz de red está desactivada de forma predeterminada.

La VLAN de administración es la interfaz lógica que se usa para la conectividad en banda con el switch a través de cualquiera de los puertos del panel frontal. Los parámetros de configuración asociados a la VLAN de administración del switch no afectan la configuración de los puertos del panel frontal por los que se conmuta o enruta el tráfico.

Para acceder al switch por una red, primero debe configurar una dirección IP y máscara de subred para el switch. Puede configurar la información IP mediante cualquiera de estos:

- DHCP
- Interfaz de terminal a través del puerto EIA-232

Después de establecer la conectividad en banda, puede cambiar la información IP mediante cualquiera de estos:

- Interfaz de terminal a través del puerto EIA-232
- Interfaz de terminal a través de Telnet
- Administración basada en SNMP
- Administración basada en web

Para configurar una VLAN de administración IPv6, puede usar la misma VLAN que se usa para la administración IPv4 o una VLAN distinta. El switch no incluye una VLAN de administración IPv6 predeterminada. Si desea usar una, debe crearla manualmente.

Para configurar o restablecer la VLAN de administración IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Management VLAN Configuration.
Se muestra la página IPv6 Management VLAN Configuration.

6. En el campo Management VLAN ID, especifique el ID de la VLAN de administración del switch.

La VLAN de administración IPv6 se usa para administrar el switch. Puede configurar cualquier valor en el rango de 1 a 4093.

7. Seleccione el botón de opción Enable o Disable de IPv6 Enable Mode para especificar el modo de administración de la VLAN de administración IPv6.

8. Seleccione el botón de opción Enable o Disable de Address Autoconfigure Mode para especificar el modo de autoconfiguración de direcciones.
Si habilita este modo, la configuración de red IPv6 (prefijo IPv6 y longitud de prefijo) se configura automáticamente para la interfaz de la VLAN de administración. De forma predeterminada, para la VLAN 1, el modo está habilitado y la configuración es automática.

Nota: La opción Address Autoconfigure Mode solo está disponible si el enrutamiento unicast está deshabilitado globalmente.

9. Seleccione el botón de opción Enable o Disable de Address DHCP Mode para especificar si la configuración IPv6 se obtiene de un servidor DHCP.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Nota: Si necesita restablecer la interfaz de administración IPv6, en la sección Reset IPv6 Management Interface de la página, active la casilla Set Management Interface to Default y haga clic en el botón Aplicar (Apply). Esto elimina la configuración de la interfaz de administración IPv6.

La sección Current IPv6 Management Interface Status muestra los siguientes campos no configurables.

Tabla 14. Información del estado actual de la interfaz de administración IPv6

Campo	Descripción
Management Interface	La interfaz de administración IPv6. (De forma predeterminada, no hay ninguna interfaz de administración IPv6 configurada).
Link State	Indica si el estado del enlace es activo o inactivo.
IPv6 Routing Interface Status/Operational Mode	Indica si el estado del enlace de la interfaz de administración IPv6 es activo o inactivo.
MAC Address	La dirección MAC asignada a la interfaz de administración IPv6.
IPv6 Enable Mode	Indica si IPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.

Tabla 14. Información del estado actual de la interfaz de administración IPv6 (continuación)

Campo	Descripción
IPv6 Routing Mode	Indica si el enrutamiento IPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
Stateless Address Autoconfig Mode	Indica si el modo de autoconfiguración de direcciones IPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
DHCPv6 Client Mode	Indica si el modo de cliente DHCPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
IPv6 Default Gateway	La dirección IPv6 de la puerta de enlace predeterminada del switch.
IPv6 Next Hop Interface	La dirección IPv6 de la interfaz de siguiente salto del switch.
IPv6 Prefix/Prefix Length	El prefijo IPv6 y la longitud de prefijo usados en la interfaz de administración IPv6.
EU164	El indicador EUI-64 de la dirección IPv6 en la interfaz de administración IPv6.
Current State	El estado actual de la dirección IPv6 en la interfaz de administración IPv6.

Administrar direcciones IPv6 de la VLAN de administración IPv6

Puede agregar una dirección IPv6 estática específica de la VLAN de administración IPv6. También puede eliminar una dirección IPv6 que ya no necesite para la VLAN de administración IPv6.

Para agregar o eliminar una dirección IPv6 de la VLAN de administración IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Management VLAN Configuration.
Se muestra la página IPv6 Management VLAN Configuration.

Si Address Autoconfigure Mode está habilitado, el prefijo IPv6 y la longitud de prefijo autoconfigurados se muestran en la sección IPv6 VLAN Interface Configuration.

6. Para agregar una dirección IPv6, en la sección IPv6 VLAN Interface Configuration, haga lo siguiente:

a. En el campo IPv6 Prefix/Prefix Length, especifique la dirección IPv6 y la longitud de prefijo que desea agregar.
b. En el menú EUI64, seleccione True para habilitar el indicador Extended Universal Identifier (EUI) de la dirección IPv6, o seleccione False para omitirlo. c. Haga clic en el botón Agregar (Add).
La dirección IPv6 se agrega a la VLAN de administración IPv6.

7. Para eliminar una dirección IPv6, en la sección IPv6 VLAN Interface Configuration, haga lo siguiente:

a. Active la casilla de la dirección IP y el prefijo que desea eliminar. b. Haga clic en el botón Eliminar (Delete).
La dirección IPv6 se elimina de la VLAN de administración IPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar las direcciones de ruta predeterminada IPv6 de la VLAN de administración IPv6

Puede agregar una dirección de ruta predeterminada IPv6 específica de la VLAN de administración IPv6. También puede eliminar una dirección de ruta predeterminada IPv6 que ya no necesite para la VLAN de administración IPv6.

Para agregar o eliminar una dirección de ruta predeterminada IPv6 de la VLAN de administración IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Management VLAN Configuration.
Se muestra la página IPv6 Management VLAN Configuration.

6. Para agregar una dirección de ruta predeterminada IPv6, en la sección IPv6 Default Route Configuration, haga lo siguiente:

a. Active la casilla Change IPv6 Default Route.

b. En el campo IPv6 Default Route Address, especifique la dirección IPv6 y la longitud de prefijo que desea agregar.
c. Haga clic en el botón Agregar (Add).
La dirección de ruta predeterminada IPv6 se agrega a la VLAN de administración IPv6.

7. Para eliminar una dirección de ruta predeterminada IPv6, en la sección IPv6 Default Route Configuration, haga lo siguiente:

a. Active la casilla de la dirección de ruta predeterminada IPv6 que desea eliminar. b. Haga clic en el botón Eliminar (Delete).
La dirección de ruta predeterminada IPv6 se elimina de la VLAN de administración IPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz de administración IPv6

Puede restringir la administración IPv6 a una interfaz específica. De forma predeterminada, puede usar cualquiera de las interfaces como interfaz de administración IPv6.

Para configurar una interfaz de administración IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Management Interface Configuration.
Se muestra la página IPv6 Management Interface Configuration.

6. En el menú Interface, seleccione la interfaz que será la interfaz de administración IPv6.

7. Active la casilla Set Management Interface para poder configurar los ajustes de la interfaz.

8. Seleccione el botón de opción Enable o Disable de Routing Mode para habilitar o deshabilitar el enrutamiento en la interfaz de administración IPv6.

9. Seleccione el botón de opción Enable o Disable de IPv6 Enable Mode para habilitar o deshabilitar IPv6 en la interfaz de administración IPv6.

10. Seleccione el botón de opción Enable o Disable de Stateless Address Autoconfigure Mode para habilitar o deshabilitar este modo en la interfaz de administración IPv6.
Solo puede habilitar este modo si el enrutamiento unicast está deshabilitado globalmente.

11. Seleccione el botón de opción Enable o Disable de DHCPv6 Client Mode para habilitar o deshabilitar el modo de cliente DHCPv6 en la interfaz de administración IPv6.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Nota: Si necesita restablecer la interfaz de administración IPv6, en la sección Reset IPv6 Management Interface de la página, active la casilla Set Management Interface to Default y haga clic en el botón Aplicar (Apply). Esto elimina la configuración de la interfaz de administración IPv6.

La sección Current IPv6 Management Interface Status muestra los siguientes campos no configurables.

Tabla 15. Información del estado actual de la interfaz de administración IPv6

Campo	Descripción
Management Interface	La interfaz de administración IPv6. (De forma predeterminada, no hay ninguna interfaz de administración IPv6 configurada).
Link State	Indica si el estado del enlace es activo o inactivo.
IPv6 Routing Interface Status/Operational Mode	Indica si el estado del enlace de la interfaz de administración IPv6 es activo o inactivo.
MAC Address	La dirección MAC asignada a la interfaz de administración IPv6.

Tabla 15. Información del estado actual de la interfaz de administración IPv6 (continuación)

Campo	Descripción
IPv6 Enable Mode	Indica si IPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
IPv6 Routing Mode	Indica si el enrutamiento IPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
Stateless Address Autoconfig Mode	Indica si el modo de autoconfiguración de direcciones IPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
DHCPv6 Client Mode	Indica si el modo de cliente DHCPv6 está habilitado o deshabilitado en la interfaz de administración IPv6.
IPv6 Default Gateway	La dirección IPv6 de la puerta de enlace predeterminada del switch.
IPv6 Next Hop Interface	La dirección IPv6 de la interfaz de siguiente salto del switch.
IPv6 Prefix/Prefix Length	El prefijo IPv6 y la longitud de prefijo usados en la interfaz de administración IPv6.
EU164	El indicador EUI-64 de la dirección IPv6 en la interfaz de administración IPv6.
Current State	El estado actual de la dirección IPv6 en la interfaz de administración IPv6.

Administrar direcciones IPv6 de la interfaz de administración IPv6

Puede agregar una dirección IPv6 estática específica de la interfaz de administración IPv6. También puede eliminar una dirección IPv6 que ya no necesite para la interfaz de administración IPv6.

Para agregar o eliminar una dirección IPv6 de la interfaz de administración IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Management Interface Configuration.

Se muestra la página IPv6 Management Interface Configuration.

6. Para agregar una dirección IPv6, en la sección IPv6 Management Interface Configuration, haga lo siguiente:

a. Active la casilla Set Management Interface.
Probablemente ya lo hizo al iniciar la configuración de la interfaz de administración IPv6.

b. En el campo IPv6 Prefix, especifique la dirección IPv6 que desea agregar. c. En el campo Prefix Length, especifique la longitud de prefijo de la dirección IPv6 que desea agregar.
d. En el menú EUI64, seleccione Enable para habilitar el indicador Extended Universal Identifier (EUI) de la dirección IPv6, o seleccione Disable para omitirlo. e. Haga clic en el botón Agregar (Add).
La dirección IPv6 se agrega a la interfaz de administración IPv6.

7. Para eliminar una dirección IPv6, en la sección IPv6 Management Interface Configuration, haga lo siguiente:

a. Active la casilla de la dirección IPv6 que desea eliminar. b. Haga clic en el botón Eliminar (Delete).
La dirección IPv6 se elimina de la interfaz de administración IPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar las direcciones de ruta predeterminada IPv6 de la interfaz de administración IPv6

Puede agregar una dirección de ruta predeterminada IPv6 específica de la interfaz de administración IPv6. También puede eliminar una dirección de ruta predeterminada IPv6 que ya no necesite para la interfaz de administración IPv6.

Para agregar o eliminar una dirección de ruta predeterminada IPv6 de la interfaz de administración IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Management Interfaces > IPv6 Management Interface Configuration.
Se muestra la página IPv6 Management Interface Configuration.

6. Para agregar una dirección de ruta predeterminada IPv6, en la sección IPv6 Default Route Configuration, haga lo siguiente:

a. Active la casilla Change IPv6 Default Route.

b. En el campo IPv6 Default Route Address, especifique la dirección IPv6 y la longitud de prefijo que desea agregar.
c. Haga clic en el botón Agregar (Add).
La dirección de ruta predeterminada IPv6 se agrega a la interfaz de administración IPv6.

7. Para eliminar una dirección de ruta predeterminada IPv6, en la sección IPv6 Default Route Configuration, haga lo siguiente:

a. Active la casilla de la dirección de ruta predeterminada IPv6 que desea eliminar. b. Haga clic en el botón Eliminar (Delete).
La dirección de ruta predeterminada IPv6 se elimina de la interfaz de administración IPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configuración de hora y SNTP

El switch admite el Simple Network Time Protocol (SNTP). Como su nombre lo indica, es una versión menos compleja del Network Time Protocol (NTP), un sistema para sincronizar los relojes de computadoras en red, principalmente cuando la transferencia de datos se realiza por Internet. También puede establecer la hora del sistema manualmente.

Configurar la hora manualmente

Para configurar la hora manualmente

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > Time Configuration. Se muestra la página Time Configuration.

6. Seleccione el botón de opción Local de Clock Source. El valor predeterminado es SNTP.

7. En el campo Date, especifique la fecha actual en meses, días y años.
8. En el campo Time, especifique la hora actual en horas, minutos y segundos.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar la hora con SNTP y la configuración global de SNTP

Para configurar la hora con SNTP y la configuración global de SNTP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > Time Configuration. Se muestra la página Time Configuration.

6. Seleccione el botón de opción SNTP de Clock Source. El valor predeterminado es SNTP.

En la sección SNTP Global Configuration de la página, configure lo siguiente.

7. Seleccione un botón de opción de Client Mode para especificar el modo de operación del cliente SNTP en el switch:

- Disable: SNTP no está operativo. El cliente no envía solicitudes SNTP y no se procesan los mensajes SNTP recibidos.
- Unicast: SNTP opera en modo punto a punto. Un cliente unicast envía una solicitud a un servidor designado en su dirección unicast y espera una respuesta con la que pueda determinar la hora y, opcionalmente, el retardo de ida y vuelta y el desfase del reloj local respecto al servidor.
  La selección predeterminada es Unicast. Puede agregar la dirección IP o el nombre DNS de uno o más servidores SNTP que el switch consultará. Para más información, consulte Configurar servidores SNTP en la página 71.
- Broadcast: SNTP usa una dirección de broadcast local en lugar de una dirección multicast. La dirección de broadcast tiene alcance de una sola subred, mientras que una dirección multicast tiene alcance en todo Internet.

8. En el campo Port, especifique el puerto UDP local en el que el cliente SNTP recibe los paquetes del servidor.
El número de puerto es 123 o un valor de 1025 a 65535. El valor predeterminado es 123. Cuando se configura el valor predeterminado, el sistema operativo asigna el puerto de cliente real usado en los paquetes SNTP.

9. En el menú Source Interface, seleccione la interfaz que debe usar el cliente SNTP:

- None: Se usa como dirección de origen la dirección IP principal de la interfaz de salida.
- Routing interface: Se usa como dirección de origen la dirección IP principal de un puerto físico.
- Routing VLAN: Se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento VLAN.
- Routing loopback interface: Se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.
- Tunnel interface: La interfaz de túnel IPv6.
- Service port: Se usa como dirección de origen la dirección IP del puerto de administración.

De forma predeterminada, se usa VLAN 1 como interfaz de origen.

10. En el campo Unicast Poll Interval, especifique los segundos entre solicitudes de consulta unicast, expresados como potencia de 2. El rango es de 6 a 10. El valor predeterminado es 6.

11. En el campo Broadcast Poll Interval, especifique los segundos entre solicitudes de consulta broadcast, expresados como potencia de 2.
Los broadcasts recibidos antes de que venza este intervalo se descartan. El rango es de 6 a 10. El valor predeterminado es 6.

12. En el campo Unicast Poll Timeout, especifique los segundos que se espera una respuesta SNTP a una solicitud de consulta unicast.
El rango es de 1 a 30. El valor predeterminado es 5.

13. En el campo Unicast Poll Retry, especifique cuántas veces se reintenta una solicitud de consulta unicast a un servidor SNTP después del primer tiempo de espera, antes de que el switch intente usar el siguiente servidor configurado.
El rango es de 0 a 10. El valor predeterminado es 1.

14. En el campo Time Zone Name, especifique una zona horaria.
En los campos Offset Hours y Offset Minutes, también puede especificar el número de horas y minutos de diferencia de la zona horaria respecto al Tiempo Universal Coordinado (UTC). La zona horaria puede afectar la visualización de la hora actual del sistema.

> Nota: Cuando usa un servidor de hora SNTP o NTP, la hora recibida del servidor se basa en UTC, que es igual a la hora media de Greenwich (GMT). Esta puede no ser la zona horaria en la que se encuentra el switch.

15. En el campo Offset Hours, especifique el número de horas de diferencia de la zona horaria respecto a UTC.
El rango es de -12 a 14. El valor predeterminado es 0.

16. En el campo Offset Minutes, especifique el número de minutos de diferencia de la zona horaria respecto a UTC.
El rango es de 0 a 59. El valor predeterminado es 0.

17. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

18. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Ver el estado global de SNTP

Cuando selecciona la opción SNTP como fuente de reloj, puede ver el estado global de SNTP.

Para ver el estado global de SNTP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Management > Time > Time Configuration. Se muestra la página Time Configuration.

   La sección SNTP Global Status muestra los siguientes campos no configurables:

Tabla 16. Información del estado global de SNTP

Campo	Descripción
Version	La versión de SNTP que admite el cliente.
Supported mode	Los modos SNTP que admite el cliente. Un cliente puede admitir varios modos.
Last Update Time	La fecha y hora local (UTC) en que el cliente SNTP actualizó por última vez el reloj del sistema.
Last Attempt Time	La fecha y hora local (UTC) de la última solicitud SNTP o recepción de un mensaje no solicitado.

Tabla 16. Información del estado global de SNTP (continuación)

Campo	Descripción
Last Attempt Status	El estado de la última solicitud SNTP o mensaje no solicitado en los modos unicast y broadcast. Si no se recibió ningún mensaje de un servidor, se muestra el estado Other. Estos valores son válidos para todos los modos de operación. • Other: Ninguno de los siguientes valores. • Success: La operación SNTP se realizó correctamente y se actualizó la hora del sistema. • Request Timed Out: Una solicitud SNTP dirigida agotó el tiempo de espera sin recibir respuesta del servidor SNTP. • Bad Date Encoded: La hora proporcionada por el servidor SNTP no es válida. • Version Not Supported: La versión de SNTP que admite el servidor no es compatible con la versión que admite el cliente. • Server Unsynchronized: El servidor SNTP no está sincronizado con sus pares. Esto se indica en el campo leap indicator del mensaje SNTP. • Server Kiss Of Death: El servidor SNTP indicó que no se le deben enviar más consultas. Esto se indica con un campo stratum igual a 0 en un mensaje recibido de un servidor.
Server IP Address	La dirección IP del servidor del último paquete válido recibido. Si no se recibió ningún mensaje de ningún servidor, se muestra una cadena vacía.
Address Type	El tipo de dirección del servidor SNTP del último paquete válido recibido.
Server Stratum	El estrato declarado del servidor del último paquete válido recibido.
Reference Clock ID	El identificador del reloj de referencia del servidor del último paquete válido recibido.
Server mode	El modo del servidor del último paquete válido recibido.
Unicast Server Max Entries	El número máximo de entradas de servidores unicast que se pueden configurar en este cliente.

Tabla 16. Información del estado global de SNTP (continuación)

Campo	Descripción
Unicast Server Current Entries	El número de entradas de servidores unicast válidas configuradas actualmente para este cliente.
Broadcast Count	El número de mensajes SNTP broadcast no solicitados que el cliente SNTP recibió y procesó desde el último reinicio.

Configurar servidores SNTP

SNTP garantiza una sincronización precisa del reloj de los dispositivos de red, hasta el milisegundo. La sincronización la realiza un servidor SNTP de la red. El switch funciona solo como cliente SNTP y no proporciona servicios de hora a otros dispositivos.

Las fuentes de hora se organizan por estratos. Los estratos definen la precisión del reloj de referencia. Cuanto más alto el estrato (cero es el más alto), más preciso es el reloj. El switch recibe la hora de dispositivos de estrato 1 o estrato 0 porque el propio switch es un dispositivo de estrato 2.

Los siguientes son ejemplos de estratos:

- Estrato 0: Se usa un reloj en tiempo real como fuente de hora, por ejemplo, un sistema GPS.
- Estrato 1: Se usa un servidor conectado directamente a una fuente de hora de estrato 0. Los servidores de estrato 1 proporcionan los estándares de hora principales de la red.
- Estrato 2: La fuente de hora está alejada del servidor de estrato 1 por una ruta de red. Por ejemplo, un servidor de estrato 2 recibe la hora por un enlace de red, mediante NTP, desde un servidor de estrato 1.

La información recibida de los servidores SNTP se evalúa según el nivel de tiempo y el tipo de servidor.

Las definiciones de tiempo SNTP se evalúan y determinan con los siguientes niveles de tiempo:

- T1: Hora en que el cliente envió la solicitud original.
- T2: Hora en que el servidor recibió la solicitud original.
- T3: Hora en que el servidor envió una respuesta.
- T4: Hora en que el cliente recibió la respuesta del servidor.

El switch puede consultar la hora a servidores de tipo unicast. El switch consulta información unicast para detectar un servidor cuya dirección IP es conocida. Solo se consultan para obtener información de sincronización los servidores SNTP que configure en el switch. T1 a T4 se usan para determinar la hora del servidor. Este es el método preferido para

sincronizar la hora del dispositivo porque es el más seguro. Si se selecciona este método, solo se acepta información SNTP de los servidores SNTP configurados en el switch.

El switch obtiene información de sincronización, ya sea solicitándola activamente o en cada intervalo de sondeo.

Agregar un servidor SNTP Para agregar un servidor SNTP:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > SNTP Server Configuration. Se muestra la página SNTP Server Configuration.

6. En el menú Server Type, seleccione el tipo de dirección SNTP que introducirá en el campo de dirección.
La dirección puede ser IPv4, IPv6 o un nombre de host (DNS). El valor predeterminado es DNS.

7. En el campo Address, especifique la dirección IP o el nombre de host del servidor SNTP. Es una dirección IP o una cadena de texto de hasta 64 caracteres que contiene la dirección IP unicast codificada o el nombre de host de un servidor SNTP. Las solicitudes SNTP unicast se envían a esta dirección. Si la dirección es un nombre de host DNS, este se resuelve en una dirección IP cada vez que se le envía una solicitud SNTP.

8. En el campo Port, especifique el número de puerto.
Es el puerto UDP del servidor SNTP al que se envían las solicitudes SNTP. El rango es de 1 a 65535. El valor predeterminado es 123.

9. En el campo Priority, especifique el orden de prioridad en que el switch debe consultar los servidores.
El cliente SNTP del switch sigue enviando solicitudes SNTP a distintos servidores hasta recibir una respuesta correcta o hasta haber probado todos. La prioridad indica el orden en que el switch debe consultar los servidores. Primero envía una solicitud

al servidor SNTP con prioridad 1, luego al servidor con prioridad 2, y así sucesivamente. Si varios servidores tienen la misma prioridad, el cliente SNTP los contacta en el orden en que aparecen en la tabla. El rango de prioridad es de 1 a 3. De forma predeterminada, el primer servidor que agregue recibe la prioridad 1, el segundo la prioridad 2 y el tercero la prioridad 3.

10. En el campo NTP Version, especifique la versión de NTP que admite el switch. El rango es de 1 a 4. El valor predeterminado es 4.

11. Haga clic en el botón Add.
Se agrega la entrada del servidor SNTP.

12. Para agregar más servidores SNTP, repita los pasos anteriores. Puede configurar hasta tres servidores SNTP.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La tabla SNTP Server Status muestra la siguiente información.

Tabla 17. Información de estado del servidor SNTP

Campo	Descripción
Address	La dirección IP del servidor SNTP.
Last Update Time	La fecha y hora local (UTC) en que se usó la respuesta del servidor para actualizar el reloj del sistema.
Last Attempt Time	La fecha y hora local (UTC) de la última consulta al servidor SNTP.
Last Attempt Status	El estado de la última solicitud NTP al servidor: • Other: No se recibió ningún paquete del servidor. • Success: La operación SNTP se realizó correctamente y se actualizó la hora del sistema. • Request Timed Out: Una solicitud SNTP dirigida agotó el tiempo de espera sin recibir respuesta del servidor SNTP. • Bad Date Encoded: La hora proporcionada por el servidor SNTP no es válida. • Version Not Supported: La versión de SNTP que admite el servidor no es compatible con la versión que admite el cliente. • Server Unsynchronized: El servidor SNTP no está sincronizado con sus pares. Esto se indica en el campo leap indicator del mensaje SNTP. • Server Kiss Of Death: El servidor SNTP indicó que no se le deben enviar más consultas. Esto se indica con un campo stratum igual a 0 en un mensaje recibido de un servidor.

Tabla 17. Información de estado del servidor SNTP (continuación)

Campo	Descripción
Requests	El número de solicitudes SNTP enviadas al servidor desde el último reinicio.
Failed Requests	El número de solicitudes SNTP fallidas enviadas al servidor desde el último reinicio.

Cambiar la configuración de un servidor SNTP existente Para cambiar la configuración de un servidor SNTP existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > SNTP Server Configuration. Se muestra la página SNTP Server Configuration.

6. Marque la casilla junto al servidor configurado.
7. Cambie la configuración según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un servidor SNTP Para eliminar un servidor SNTP:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > SNTP Server Configuration. Se muestra la página SNTP Server Configuration.

6. Marque la casilla junto al servidor configurado que desea eliminar.

7. Haga clic en el botón
Delete. Se elimina el servidor.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el horario de verano

Puede configurar el horario de verano. Utilizado en algunos países del mundo, el horario de verano consiste en adelantar temporalmente los relojes durante los meses de verano. Normalmente, los relojes se adelantan una o más horas a inicios de la primavera y se atrasan en otoño.

Para configurar el horario de verano:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > Daylight Saving Configuration. Se muestra la página Daylight Saving Configuration.

6. Seleccione uno de los siguientes botones de opción Daylight Saving (DST):
• Disable: Deshabilita el horario de verano.

• Recurring: El horario de verano ocurre en las mismas fechas cada año. Debe configurar manualmente las horas y fechas de inicio y fin del cambio de hora. Configure los ajustes descritos en el paso 7.
• Recurring EU: El reloj del sistema usa los ajustes estándar recurrentes de horario de verano de los países de la Unión Europea. Con esta opción, los demás campos aplicables de la página se completan automáticamente y no se pueden cambiar. Configure los ajustes descritos en el paso 7.
• Recurring USA: El reloj del sistema usa los ajustes estándar recurrentes de horario de verano de Estados Unidos. Con esta opción, los demás campos aplicables de la página se completan automáticamente y no se pueden cambiar. Configure los ajustes descritos en el paso 7.
• Non Recurring: El horario de verano solo está vigente entre la fecha de inicio y la fecha de fin del año especificado. Con esta opción, el horario de verano no se repite anualmente.
Configure los ajustes descritos en el paso 8.

7. Si selecciona el botón de opción Recurring, Recurring EU o Recurring USA, configure los campos que se muestran en la siguiente tabla.

Campo	Descripción
Begins At	Estos campos configuran los valores de inicio del día y la hora. • Week: Configure la semana de inicio. • Day: Configure el día de inicio. • Month: Configure el mes de inicio. • Hours: Configure las horas de inicio. • Minutes: Configure los minutos de inicio.
Ends At	Estos campos configuran los valores de fin del día y la hora. • Week: Configure la semana de fin. • Day: Configure el día de fin. • Month: Configure el mes de fin. • Hours: Configure las horas de fin. • Minutes: Configure los minutos de fin.
Offset	Configure el desfase recurrente en minutos. El rango válido es 1-1440 minutos.
Zone	Configure la zona horaria.

8. Si selecciona Non Recurring, configure los campos que se muestran en la siguiente tabla.

Campo	Descripción
Begins At	Estos campos configuran los valores de inicio de la fecha y la hora. • Month: Configure el mes de inicio. • Date: Configure la fecha de inicio. • Year: Configure el año de inicio. • Hours: Configure las horas de inicio. • Minutes: Configure los minutos de inicio.
Ends At	Estos campos configuran los valores de fin de la fecha y la hora. • Month: Configure el mes de fin. • Date: Configure la fecha de fin. • Year: Configure el año de fin. • Hours: Configure las horas de fin. • Minutes: Configure los minutos de fin.
Offset	Configure el desfase no recurrente en minutos. El rango válido es 1-1440 minutos.
Zone	Configure la zona horaria.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Ver el estado del horario de verano

Puede mostrar información sobre la configuración del horario de verano y si el cambio de hora está vigente actualmente.

Para ver el estado del horario de verano:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Time > Daylight Saving Configuration. Se muestra la página Daylight Saving Configuration.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla muestra la información de estado del horario de verano (DST), que no es configurable.

Tabla 18. Información de estado del horario de verano

Campo	Descripción
Daylight Saving (DST)	El valor de Daylight Saving, que es uno de los siguientes: • **Disable** • **Recurring** • **Recurring EU** • **Recurring USA** • **Non Recurring**
Begins At	Muestra cuándo comienza el horario de verano. Este campo no se muestra cuando el horario de verano está deshabilitado.
Ends At	Muestra cuándo termina el horario de verano. Este campo no se muestra cuando el horario de verano está deshabilitado.
Offset (in Minutes)	El valor de desfase en minutos. Este campo no se muestra cuando el horario de verano está deshabilitado.

Tabla 18. Información de estado del horario de verano (continuación)

Campo	Descripción
Zone	El acrónimo de la zona. Este campo no se muestra cuando el horario de verano está deshabilitado.
Daylight Saving (DST) in Effect	Muestra si el horario de verano está vigente.

Precision Time Protocol

Precision Time Protocol (PTP, IEEE 1588) es un protocolo que permite sincronizar relojes con precisión inferior a un microsegundo en una red basada en paquetes. PTP permite que dispositivos de red con distinta precisión y resolución se sincronicen con un reloj grandmaster mediante el intercambio de paquetes en la red. El switch admite un reloj transparente PTP de extremo a extremo, habilitado de forma predeterminada tanto globalmente como a nivel de puerto.

Nota: PTP no afecta al switch en sí.

Administrar la configuración global de PTP

De forma predeterminada, PTP está habilitado globalmente en el switch. Puede deshabilitarlo globalmente, en cuyo caso el switch no admite el paso de PTP (pass-through).

Para configurar globalmente el reloj transparente PTP de extremo a extremo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > PTP TC > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción Admin Mode Enable o Disable. El valor predeterminado es Enable.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar la configuración de PTP en las interfaces

En un switch independiente, PTP está habilitado de forma predeterminada en todas las interfaces. En una pila de switches, PTP está deshabilitado de forma predeterminada en todas las interfaces. Puede seleccionar interfaces individuales para habilitar o deshabilitar PTP. Si deshabilita PTP en una interfaz, esta no admite el paso de PTP (pass-through).

Para configurar el reloj transparente PTP de extremo a extremo en una o más interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > PTP TC > Interface Configuration. Se muestra la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.

• Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Configured Mode, seleccione Enable o Disable. El valor predeterminado es Enable.

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Operational Mode indica si PTP está habilitado o deshabilitado en una interfaz.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Domain Name System

Puede configurar información sobre los servidores Domain Name System (DNS) que usa la red y cómo funciona el switch como cliente DNS.

Configurar los ajustes globales de DNS y agregar un servidor DNS

Puede configurar los ajustes globales de DNS y la información de los servidores DNS.

Para configurar los ajustes globales de DNS y agregar un servidor DNS:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > DNS > DNS Configuration. Se muestra la página DNS Configuration.

6. Seleccione el botón de opción DNS Status Disable o Enable:

- Enable: Permite que el switch envíe consultas DNS a un servidor DNS para resolver un nombre de dominio DNS. El valor predeterminado es Enable.
- Disable: Impide que el switch envíe consultas DNS.

7. En el campo DNS Default Name, introduzca el nombre que se debe incluir en las consultas DNS. Cuando el switch busca un nombre de host no calificado, este campo proporciona el nombre de dominio. Por ejemplo, si el nombre de dominio predeterminado es netgear.com y escribe test, test se cambia a test.netgear.com para resolver el nombre. La longitud máxima del nombre es de 255 caracteres.

8. En el campo Retry Number, especifique cuántas veces debe reintentar el switch enviar consultas DNS al servidor DNS.
Introduzca un número de 0 a 100. El valor predeterminado es 2.

9. En el campo Response Timeout (secs), especifique el tiempo en segundos que el switch debe esperar una respuesta a una consulta DNS.
Introduzca un número de 0 a 3600. El valor predeterminado es 3.

10. En el menú Source Interface, seleccione la interfaz que será la interfaz de origen para DNS:

- None: Se usa como dirección de origen la dirección IP principal de la interfaz de salida.
- Routing interface: Se usa como dirección de origen la dirección IP principal de un puerto físico.
- Routing VLAN: Se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento VLAN.
- Routing loopback interface: Se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.
- Tunnel interface: La interfaz de túnel IPv6.
- Service port: Se usa como dirección de origen la dirección IP del puerto de administración.

De forma predeterminada, se usa VLAN 1 como interfaz de origen.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

13. Para agregar un servidor DNS al que el switch envíe consultas DNS, haga lo siguiente:
a. En el campo DNS Server Address de la tabla DNS Server Configuration, introduzca

una dirección IP en notación estándar IPv4 o IPv6. b.
Haga clic en el botón Add.

El servidor se agrega a la tabla. Puede especificar hasta ocho servidores DNS. La precedencia se establece según el orden en que agregue los servidores.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla muestra información no configurable de los servidores DNS.

Tabla 19. Información de configuración de servidores DNS

Campo	Descripción
Serial No	El número de secuencia del servidor DNS.
Preference	La preferencia del servidor DNS. La preferencia se determina por el orden en que agrega los servidores.

Eliminar un servidor DNS

Puede eliminar un servidor DNS que ya no necesite.

Para eliminar un servidor DNS:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > DNS > DNS Configuration. Se muestra la página DNS Configuration.

6. En la tabla DNS Server Configuration, marque la casilla del servidor DNS.

Nota: Si no selecciona un servidor DNS, se eliminan todos los servidores DNS al hacer clic en el botón Delete.

7. Haga clic en el botón Delete.
Se elimina el servidor DNS.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar y ver la asignación de nombres de host a direcciones IP

Puede asignar manualmente nombres de host a direcciones IP o ver las asignaciones dinámicas de hosts.

Agregar una entrada estática a la tabla de asignación dinámica de hosts Para agregar una entrada estática a la tabla local de asignación dinámica de hosts:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > DNS > Host Configuration. Se muestra la página Host Configuration.

6. En el campo Host Name, especifique el nombre de host estático. La longitud máxima del nombre es de 255 caracteres.

7. En el campo IP Address, introduzca la dirección IP que se asociará al nombre de host.

8. Haga clic en el botón Add.
La entrada aparece en la tabla Dynamic Host Mapping.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una entrada de la tabla de asignación dinámica de hosts Para eliminar una entrada de la tabla de asignación dinámica de hosts:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > DNS > Host Configuration. Se muestra la página Host Configuration.

6. Marque la casilla junto a la entrada que desea eliminar.

7. Haga clic en el botón
Delete. Se elimina la entrada.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar el nombre de host o la dirección IP de una entrada de la tabla de asignación dinámica de hosts, ver o borrar todas las entradas Para cambiar el nombre de host o la dirección IP de una entrada de la tabla de asignación dinámica de hosts, ver todas las entradas o borrar todas las entradas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > DNS > Host Configuration. Se muestra la página Host Configuration.

6. Marque la casilla junto a la entrada que desea actualizar.
7. Introduzca la nueva información en el campo correspondiente.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para borrar todas las entradas dinámicas de nombres de host de la lista, haga clic en el botón Clear.
10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La tabla de asignación dinámica de hosts muestra las entradas de nombre de host a dirección IP que el switch aprendió. La siguiente tabla describe los campos de hosts dinámicos.

Tabla 20. Información de Dynamic Host Mapping

Campo	Descripción
Host	Muestra el nombre de host que asigna a la dirección IP especificada.
Total	Tiempo transcurrido desde que la entrada dinámica se agregó por primera vez a la tabla.
Elapsed	Tiempo transcurrido desde la última actualización de la entrada dinámica.
Type	El tipo de entrada dinámica.
Addresses	Muestra la dirección IP asociada al nombre de host.

Plantilla de administración de la base de datos del switch

Una plantilla de administración de la base de datos del switch (SDM) determina los recursos máximos que el switch puede usar para diversas funciones. Las plantillas SDM permiten distintas combinaciones de factores de escala y, por lo tanto, de asignación de recursos, según el uso del switch. Es decir, permiten reasignar los recursos del switch para admitir otra combinación de funciones según los requisitos de su red.

La siguiente tabla muestra cómo se dividen los recursos de hardware.

Tabla 21. Recursos de hardware de SDM

Nombre de plantilla	Modelos compatibles	Número de entradas IPv4	Número de entradas IPv6
IPv4-Basic	Todos los modelos	90% del total disponible	10% del total disponible
IPv6-Basic	Todos los modelos	10% del total disponible	90% del total disponible
IPv4-Advanced	M4250-16XF	90% del total disponible	10% del total disponible
IPv6-Advanced	M4250-16XF	10% del total disponible	90% del total disponible

La Main UI ofrece más información sobre las plantillas (consulte los pasos de esta tarea). La plantilla SDM predeterminada es IP4v-Basic. Puede cambiar la plantilla SDM del switch.

Para cambiar la plantilla SDM

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > SDM Template Preference. Se muestra la página SDM Template Preference.

6. En el menú SDM Next Template ID, seleccione una plantilla. De forma predeterminada, está seleccionada la plantilla IPv4-Basic.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

9. Para activar la nueva plantilla, reinicie el switch. La siguiente tabla muestra la información de resumen.

Tabla 22. Información de resumen de la plantilla SDM

Campo	Descripción
SDM Template	Identifica la plantilla.
ARP Entries	El número máximo de entradas en la caché de Address Resolution Protocol (ARP) para interfaces de enrutamiento.
IPv4 Unicast Routes	El número máximo de entradas de la tabla de reenvío unicast IPv4.
IPv6 NDP Entries	El número máximo de entradas en la caché de IPv6 Neighbor Discovery Protocol (NDP).
IPv6 Unicast Routes	El número máximo de entradas de la tabla de reenvío unicast IPv6.
ECMP Next Hops	El número máximo de saltos siguientes que se pueden instalar en las tablas de reenvío unicast IPv4 e IPv6.
IPv4 Multicast Routes	El número máximo de entradas de la tabla de reenvío multicast IPv4.
IPv6 Multicast Routes	El número máximo de entradas de la tabla de reenvío multicast IPv6.
Maximum VLAN Entries	El número máximo de entradas VLAN, que es 4093 para cualquier plantilla SDM.

Configuración de Green Ethernet

Puede configurar las funciones de Green Ethernet para reducir el consumo de energía.

Configurar los ajustes globales de Green Ethernet

Puede configurar los ajustes globales de Green Ethernet.

Para configurar los ajustes globales de Green Ethernet:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > Management > Green Ethernet > Green Ethernet Configuration. Se muestra la página Green Ethernet Configuration.

6. Seleccione el botón de opción Auto Power Down Mode Disable o Enable. De forma predeterminada, este modo está deshabilitado. Cuando el enlace de un puerto está inactivo, la capa física subyacente se desactiva por un breve periodo y luego vuelve a buscar pulsos de enlace para que la autonegociación siga siendo posible. Así, el switch ahorra energía cuando no hay un dispositivo enlazado en el puerto.

7. Seleccione el botón de opción EEE Mode Disable o Enable.
De forma predeterminada, este modo está deshabilitado. Energy Efficient Ethernet (EEE) combina la MAC con una familia de capas físicas que admiten el funcionamiento en modo de bajo consumo. Está definido por el estándar IEEE 802.3az. El modo de bajo consumo permite que los lados de envío y recepción del enlace desactiven algunas funciones para ahorrar energía cuando la carga es baja. La transición al modo de bajo consumo no cambia el estado del enlace. Las tramas en tránsito no se descartan ni se corrompen al entrar o salir del modo de bajo consumo. El tiempo de transición es transparente para los protocolos y aplicaciones de capas superiores.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar Green Ethernet en las interfaces

Puede configurar Green Ethernet en interfaces individuales.

Para configurar Green Ethernet en las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Green Ethernet > Green Ethernet Interface Configuration.
Se muestra la página Green Ethernet Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

7. En el menú Auto Power Down mode, seleccione Enable o Disable. De forma predeterminada, este modo está deshabilitado en la interfaz. Cuando un enlace de puerto cae, la capa física subyacente se apaga por un breve periodo y luego vuelve a buscar pulsos de enlace para que la autonegociación siga siendo posible. Así, el switch ahorra energía cuando el puerto no tiene ningún dispositivo enlazado.

8. En el menú EEE mode, seleccione Enable o Disable.
De forma predeterminada, este modo está deshabilitado en la interfaz. Cuando un enlace de puerto cae, la capa física subyacente se apaga por un breve periodo y luego vuelve a buscar pulsos de enlace para que la autonegociación siga siendo posible. Así, el switch ahorra energía cuando el puerto no tiene ningún dispositivo enlazado.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar y mostrar la configuración detallada de green Ethernet de una interfaz

Puede seleccionar una sola interfaz y configurar y mostrar su configuración detallada de green Ethernet.

Para configurar y mostrar la configuración detallada de green Ethernet de una sola interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Green Ethernet > Green Ethernet Details. Se muestra la página Green Ethernet Details.

6. En el menú Interface, seleccione la interfaz.

7. En el menú Energy Detect Admin Mode, habilite o deshabilite este modo. De forma predeterminada, este modo está deshabilitado en la interfaz. Cuando un enlace de puerto cae, la capa física subyacente se apaga por un breve periodo y luego vuelve a buscar pulsos de enlace para que la autonegociación siga siendo posible. Así, el switch ahorra energía cuando el puerto no tiene ningún dispositivo enlazado.

8. En el menú EEE Admin Mode, habilite o deshabilite este modo. Con el modo Energy Efficient Ethernet (EEE) habilitado, el puerto pasa a modo de bajo consumo cuando el enlace está inactivo. El valor predeterminado es Disabled.

9. En el campo EEE Transmit Idle Time, introduzca el tiempo que la interfaz debe permanecer inactiva (sin recibir paquetes para transmitir) antes de entrar en el estado de inactividad de bajo consumo (LPI).
El rango es de 600 a 4294967295 segundos. El valor predeterminado es 600 segundos.

10. En el campo EEE Transmit Wake Time, introduzca el tiempo que la interfaz debe permanecer en el estado LPI antes de volver al estado activo tras recibir un paquete para transmitir.
El rango es de 8 a 65535 segundos. El valor predeterminado es 17 segundos.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables.

Tabla 23. Información del dispositivo local de green Ethernet

Campo	Descripción
Cumulative Energy Saved on this port due to Green mode(s) (Watts * Hours)	La energía acumulada ahorrada en el puerto gracias a los modos green habilitados en el puerto, en watts * horas.
Energy Detect Operational Status	El estado operativo (Active o Inactive) del modo Energy Detect.
Reason	El motivo del estado operativo que se muestra en el campo anterior.
Rx Low Power Idle Event Count	El número total de veces que el puerto entró en el estado de inactividad de bajo consumo (LPI) desde que se restablecieron los contadores EEE.
Rx Low Power Idle Duration (uSec)	El tiempo total (en incrementos de 10 us) que el puerto permaneció en el estado LPI desde que se restablecieron los contadores EEE.
Tx Low Power Idle Event Count	El número total de veces que el dispositivo enlazado al puerto entró en el estado LPI desde que se restablecieron los contadores EEE.
Tx Low Power Idle Duration (uSec)	El tiempo total (en incrementos de 10 us) que el dispositivo enlazado al puerto permaneció en el estado LPI desde que se restablecieron los contadores EEE.
Tw_sys_tx (uSec)	El valor de ‘Tw_sys’ que admite el puerto.
Tw_sys_tx Echo (uSec)	El ‘transmit Tw_sys’ del dispositivo enlazado que el puerto usa para calcular el ‘Tw_sys’ que solicita a su dispositivo enlazado.
Tw_sys_rx (uSec)	El valor de ‘Tw_sys’ que el puerto solicitó a su dispositivo enlazado.
Tw_sys_rx Echo (uSec)	El ‘receive Tw_sys’ del dispositivo enlazado que el puerto usa para calcular el ‘Tw_sys’ que puede admitir.
Fallback Tw_sys (uSec)	El valor de ‘fallback Tw_sys’ que el puerto solicitó a su dispositivo enlazado.
Tx_dll_enabled	El estado de inicialización de la función de transmisión EEE de capa de enlace de datos (DLL) en el puerto.
Tx_dll_ready	El estado de DLL de transmisión, que indica si la inicialización de ‘tx system’ está completa y si el puerto está listo para recibir o actualizar LLDPDU que contienen TLV de EEE.
Rx_dll_enabled	El estado de la negociación de capacidad EEE en el puerto.

Tabla 23. Información del dispositivo local de green Ethernet (continuación)

Campo	Descripción
Rx_dll_ready	El estado de DLL de recepción, que indica si la inicialización de 'rx system' está completa y si el puerto está listo para recibir o actualizar LLDPDU que contienen TLV de EEE.
Time Since Counters Last Cleared	El tiempo transcurrido desde que se restablecieron los contadores.

Mostrar la información de green Ethernet del dispositivo enlazado a una interfaz

El switch puede detectar la información de green Ethernet del dispositivo enlazado a una interfaz, es decir, del dispositivo remoto.

Para mostrar la información de green Ethernet del dispositivo enlazado a una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Green Ethernet > Green Ethernet Details. Se muestra la página Green Ethernet Details.

6. Desplácese hacia abajo hasta la sección Remote Device Information.

7. En el menú Interface, seleccione la interfaz. La siguiente tabla describe los campos no configurables.

Tabla 24. Información del dispositivo remoto de green Ethernet

Campo	Descripción
Remote ID	El identificador asignado al dispositivo enlazado al puerto.
Remote Tw_sys_tx (uSec)	El valor de ‘Tw_sys’ que admite el dispositivo enlazado.
Remote Tw_sys_tx Echo (uSec)	El valor de ‘transmit Tw_sys’ que el dispositivo enlazado devuelve al puerto.
Remote Tw_sys_rx (uSec)	El valor de ‘Tw_sys’ que el dispositivo enlazado solicita al puerto.
Remote Tw_sys_rx Echo (uSec)	El valor de ‘receive Tw_sys’ que el dispositivo enlazado devuelve al puerto.
Remote Fallback Tw_sys (uSec)	El valor de ‘fallback Tw_sys’ que el dispositivo enlazado devuelve al puerto.

Mostrar el resumen de estadísticas de green Ethernet

El resumen de estadísticas de green Ethernet muestra información tanto del switch como de las interfaces.

Para mostrar el resumen de estadísticas de green Ethernet:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Green Ethernet > Green Ethernet Summary. Se muestra la página Green Ethernet Summary.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la sección Green Ethernet Statistics Summary.

Tabla 25. Información del resumen de estadísticas de green Ethernet

Campo	Descripción
Current Power Consumption (mW)	El consumo de energía de todos los puertos del switch en mW.
Percentage Power Saving (%)	El porcentaje de energía ahorrada en todos los puertos del switch con el modo green Ethernet habilitado.
Cumulative Energy Saving (W*H)	La energía acumulada ahorrada en el switch (en watts * hora) con todas las funciones green habilitadas.

La siguiente tabla describe los campos no configurables de la sección Green Ethernet Feature Summary.

Tabla 26. Información del resumen de funciones de green Ethernet

Campo	Descripción
Unit	La unidad siempre es 1.
Green Features supported on this unit	Las funciones green compatibles con el switch: • Energy-Detect • EEE (Energy Efficient Ethernet) • LPI-History (historial de inactividad de bajo consumo EEE) • LLDP-Cap-Exchg (intercambio de capacidades LLDP de EEE) • Pwr-Usg-Est (estimaciones de consumo de energía).

La siguiente tabla describe los campos no configurables de la sección Green Ethernet Interface Summary.

Tabla 27. Información del resumen de interfaces de green Ethernet

Campo	Descripción
Interface	La interfaz cuya información se muestra.
Energy Detect Admin Mode	Indica el estado del modo (Enable o Disable). Si el modo está habilitado y un enlace de puerto cae, la capa física subyacente se apaga por un breve periodo y luego vuelve a buscar pulsos de enlace para que la autonegociación siga siendo posible. Así, el switch ahorra energía cuando el puerto no tiene ningún dispositivo enlazado.
Energy Detect Operational Status	El estado operativo (Active o Inactive) del modo Energy Detect.
EEE Admin mode	Indica el estado del modo (Enable o Disable). Si este modo está habilitado, el puerto pasa a modo de bajo consumo cuando el enlace está inactivo.

Configurar y mostrar el historial LPI de EEE de green Ethernet de una interfaz

Puede configurar y mostrar el historial de inactividad de bajo consumo (LPI) de EEE de green Ethernet de una interfaz.

Para configurar y mostrar el historial LPI de EEE de green Ethernet de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Green Ethernet > Green Ethernet LPI History. Se muestra la página Green Ethernet LPI History.

6. En el menú Interface, seleccione la interfaz.

7. En el campo Sampling Interval, introduzca el intervalo de recopilación de datos LPI de EEE. El rango es de 30 a 36000 segundos. El valor predeterminado es 3600 segundos.

8. En el campo Max Samples To Keep, introduzca el número máximo de muestras que se conservan. El rango es de 1 a 168. El valor predeterminado es 168.

El campo Percentage LPI time muestra el tiempo que la interfaz estuvo en modo LPI desde que se restablecieron los contadores EEE.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

11. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables.

Tabla 28. Información del historial LPI de EEE del modo green de la interfaz

Campo	Descripción
Sample No.	El índice de la muestra.
Time Since The Sample Was Recorded	El tiempo transcurrido desde que se registró la muestra.
Percentage Time spent in LPI mode since last sample	El porcentaje de tiempo que la interfaz estuvo en modo LPI desde que se registró la última muestra.
Percentage Time spent in LPI mode since last reset	El porcentaje de tiempo que la interfaz estuvo en modo LPI desde que se restablecieron los contadores EEE.

Configuración de Bonjour

Una Mac compatible con Bonjour puede detectar el switch en la red para que usted encuentre la dirección IP del switch e inicie sesión en su UI principal. Bonjour está habilitado de forma predeterminada. Puede deshabilitar Bonjour por motivos de seguridad.

Habilitar o deshabilitar Bonjour

Para habilitar o deshabilitar Bonjour:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Management > Bonjour > Bonjour Configuration. Se muestra la página Bonjour Configuration.

6. Seleccione uno de los siguientes botones de opción:

- Enable. Bonjour está habilitado. Es la configuración predeterminada.
- Disable. Bonjour está deshabilitado.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar la información de Bonjour

Para mostrar la información de Bonjour:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > Management > Bonjour > Bonjour Details. Se muestra la página Bonjour Details.

El campo Bonjour Administration Mode indica si Bonjour está habilitado o deshabilitado.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 29. Servicios publicados de Bonjour

Campo	Descripción
Service Name	Los nombres de los servicios Bonjour del switch.
Type	Los nombres de tipo de los servicios Bonjour del switch.
Domain	El dominio del servicio Bonjour del switch.
Port	El número de puerto del servicio Bonjour.
TXT Data	El texto del servicio Bonjour.

Servidor DHCP IPv4

Puede configurar un servidor DHCP IPv4, pools DHCP y asignaciones (bindings) DHCP. También puede ver las estadísticas DHCP y, si se producen, los conflictos DHCP.

Configurar un servidor DHCP

Para configurar un servidor DHCP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Server Configuration. Se muestra la página DHCP Server Configuration.

6. Seleccione el botón de opción Admin Mode Disable o Enable. Esta opción indica si el servicio DHCP está habilitado o deshabilitado.

El valor predeterminado es Disable.

7. En el campo Ping Packet Count, especifique el número de paquetes que un servidor envía a una dirección del pool para comprobar si está duplicada mediante ping. El valor puede ser 0 o de 2 a 10. El valor 0 deshabilita la función. El valor predeterminado es 2.

8. Seleccione el botón de opción Conflict Logging Mode Disable o Enable. Esta opción indica si el registro de conflictos en un servidor DHCP está habilitado o deshabilitado. El valor predeterminado es Enable.

9. Seleccione el botón de opción BootP Automatic Mode Disable o Enable. Esta opción indica si BootP para pools dinámicos está habilitado o deshabilitado. El valor predeterminado es Disable.

10. Para excluir direcciones, haga lo siguiente:
a. En el campo IP Range From, introduzca la dirección más baja del rango o una sola dirección que se excluirá.
b. En el campo IP Range To, para excluir un rango, introduzca la dirección más alta del rango. Para excluir una sola dirección, introduzca la misma IP que en el campo IP Range From, o déjelo como 0.0.0.0.
c. Haga clic en el botón Agregar (Add).
Las direcciones que se deben excluir se agregan al switch.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Administrar los pools DHCP

Puede configurar y administrar distintos tipos de pools de direcciones IP que el servidor DHCP puede asignar.

Crear un pool DHCP Para crear un pool DHCP:
1. Abra un navegador web.

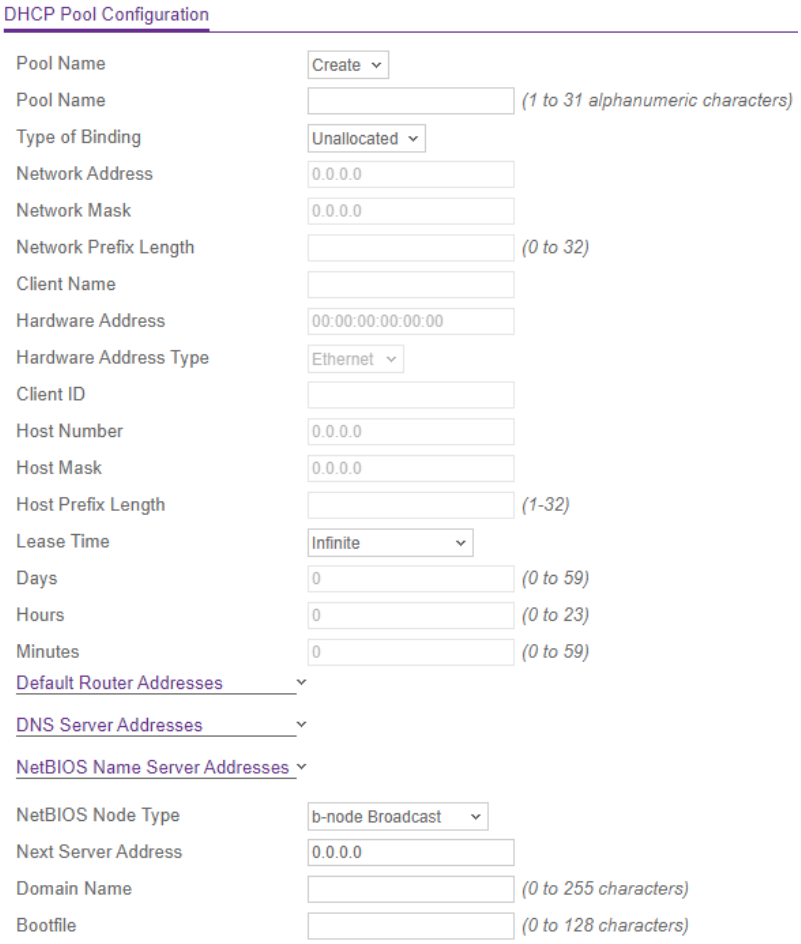
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Pool Configuration.



6. En el menú Pool Name, seleccione Create.
Se muestra el campo Pool Name.

7. En el campo Pool Name, escriba un nombre para el nuevo pool. El nombre puede tener hasta 31 caracteres.

8. Seleccione el tipo de asignación del pool:

- Unallocated: No se requiere más configuración. Continúe con el siguiente paso.
- Dynamic: Configure lo siguiente:
  - Network Address. La dirección IP de subred del pool DHCP dinámico.
  - Network Mask: La máscara de red del pool DHCP dinámico.
  - Network Prefix Length: El número de subred del pool DHCP dinámico. El rango es de 0 a 32.

Nota: Para un pool DHCP dinámico, puede configurar la máscara de red o la longitud de prefijo.

• Manual: Configure lo siguiente:

- Client Name: El nombre del cliente DHCP.
- Hardware Address: La dirección MAC de hardware del cliente DHCP.
- Hardware Address Type: El protocolo de la dirección MAC del cliente DHCP. Puede ser Ethernet o IEEE802. El valor predeterminado es Ethernet.
- Client ID: El ID del cliente DHCP.
- Host Number: La dirección IP de la asignación manual del cliente DHCP.
- Host Mask: La máscara de subred de la asignación manual del cliente DHCP.
- Host Prefix Length: La máscara de subred de la asignación manual del cliente DHCP. El rango es de 0 a 32.

Nota: Para un cliente DHCP agregado manualmente, puede configurar la máscara de red o la longitud de prefijo.

9. En el menú Lease Time, seleccione cómo se concede la asignación:

• Infinite: Para una asignación dinámica, infinito equivale a una concesión de 60 días. Para una asignación manual, la concesión es indefinida. No se requiere más configuración. Continúe con el siguiente paso.
• Specified Duration: Configure lo siguiente:

- Days: El número de días de la concesión. El rango es de 0 a 59. El valor predeterminado es 1.
- Hours: El número de horas de la concesión. El rango es de 0 a 22.
- Minutes: El número de minutos de la concesión. El rango es de 0 a 86399.

10. Para configurar las direcciones de router predeterminado, haga clic en el enlace Default Router Addresses y agregue hasta ocho direcciones IP de routers predeterminados, en orden de preferencia.

11. Para configurar las direcciones de servidores DNS, haga clic en el enlace DNS Server Addresses y agregue hasta ocho direcciones IP de servidores DNS, en orden de preferencia.

12. Para configurar las direcciones de servidores de nombres NetBIOS, haga clic en el enlace NetBIOS name server addresses y agregue hasta ocho direcciones IP de servidores de nombres NetBIOS, en orden de preferencia.

13. En el menú NetBIOS Node Type, seleccione uno de los siguientes tipos de nodo NetBIOS para los clientes DHCP:

- b-node Broadcast
- p-node Peer-to-Peer
- m-node Mixed
- h-node Hybrid

14. En el campo Next Server Address, introduzca la dirección IP del siguiente servidor en el proceso de arranque de un cliente DHCP.

15. En el campo Domain Name, introduzca el nombre de dominio en el proceso de arranque de un cliente DHCP.
El nombre de dominio puede tener hasta 255 caracteres.

16. En el campo Bootfile, introduzca el nombre de la imagen de arranque predeterminada para un cliente DHCP.
El nombre puede tener hasta 128 caracteres.

17. Haga clic en el botón Add.
Se agrega la configuración del pool.

18. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Cambiar un pool DHCP Puede cambiar un pool DHCP existente.
Para cambiar un pool DHCP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Pool Configuration. Se muestra la página DHCP Pool Configuration.

6. En el menú Pool Name, seleccione el pool.

7. Cambie la configuración según sea necesario.
Para más información, consulte Crear un pool DHCP en la página 101.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un pool DHCP Puede eliminar un pool DHCP que ya no necesite. Para eliminar un pool DHCP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Pool Configuration. Se muestra la página DHCP Pool Configuration.

6. En el menú Pool Name, seleccione el pool.

7. Haga clic en el botón
Delete. Se elimina el pool.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar las opciones del pool DHCP

Puede especificar la información que se incluye en el campo “options” de un mensaje DHCP que envía el switch.

Para configurar las opciones del pool DHCP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server> DHCP Pool Options. Se muestra la página DHCP Pool Options.

6. En el menú Pool Name, seleccione el nombre del pool.

7. En el campo Option Code, especifique el código de opción configurado para el pool. El rango es de 1 a 254. Para información sobre las opciones y su formato, consulte la RFC 2132 en https://tools.ietf.org/html/rfc2132.

8. En el menú Option Type, seleccione uno de los siguientes tipos de opción para el pool:

- ASCII: Introduzca la información en el campo Option Value en formato ASCII.
- Hex: Introduzca la información en el campo Option Value en formato hexadecimal. Los formatos posibles son xx:xx y xxxx.xxxx.
- IP Address: En el campo Option Value, introduzca una dirección IPv4.

9. En el campo Option Value, especifique el valor de la opción para el pool según lo que seleccionó en el paso anterior.

10. Haga clic en el botón Add.
Se agrega el código de opción al pool.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar las estadísticas del servidor DHCP

Para mostrar las estadísticas del servidor DHCP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Server Statistics. Se muestra la página DHCP Server Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 30. Información de estadísticas del servidor DHCP

Campo	Descripción
Detalles de asignaciones (Binding Details)	
Automatic Bindings	El número de asignaciones automáticas en el servidor DHCP.
Expired Bindings	El número de asignaciones vencidas en el servidor DHCP.
Malformed Messages	El número de mensajes con formato incorrecto en el servidor DHCP.
Mensajes recibidos (Message Received)	
DHCPDISCOVER	El número de mensajes DHCPDISCOVER recibidos por el servidor DHCP.
DHCPREQUEST	El número de mensajes DHCPREQUEST recibidos por el servidor DHCP.
DHCPDECLINE	El número de mensajes DHCPDECLINE recibidos por el servidor DHCP.
DHCPRELEASE	El número de mensajes DHCPRELEASE recibidos por el servidor DHCP.
DHCPINFORM	El número de mensajes DHCPINFORM recibidos por el servidor DHCP.
Mensajes enviados (Message Sent)	
DHCPOFFER	El número de mensajes DHCPOFFER enviados por el servidor DHCP.

Tabla 30. Información de estadísticas del servidor DHCP (continuación)

Campo	Descripción
DHCPACK	El número de mensajes DHCPACK enviados por el servidor DHCP.
DHCPNAK	El número de mensajes DHCPNAK enviados por el servidor DHCP.

Mostrar las asignaciones DHCP

Para mostrar las asignaciones DHCP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Bindings Information. Se muestra la página DHCP Bindings Information. La tabla muestra información de todas las asignaciones.

6. Para buscar una asignación por dirección IP, introdúzcala en el campo Search Binding IP y haga clic en el botón Go.
Se muestra la información de la asignación.

   La siguiente tabla describe los campos no configurables de la página.

Tabla 31. Información de asignaciones DHCP

Campo	Descripción
IP Address	La dirección IP del cliente.
Hardware Address	La dirección de hardware del cliente.

Tabla 31. Información de asignaciones DHCP (continuación)

Campo	Descripción
Lease Time Left	El tiempo de concesión restante en días, horas y minutos (formato dd:hh:mm).
Type	El tipo de asignación (Dynamic o Manual).

Eliminar una o todas las asignaciones DHCP dinámicas

Para eliminar una o todas las asignaciones DHCP dinámicas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Bindings Information. Se muestra la página DHCP Bindings Information.

6. Seleccione uno de los siguientes botones de opción:

- All Dynamic Bindings: Se borran todas las asignaciones dinámicas.
- Specific Dynamic Binding: En el campo, especifique la dirección IP de la asignación dinámica que se borrará.

7. Haga clic en el botón Clear.
Se eliminan la asignación o asignaciones seleccionadas.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Ver asignaciones con conflictos DHCP

Puede ver información sobre dispositivos con conflictos de dirección IP. Puede ocurrir un conflicto cuando la misma dirección IP se asigna a dos o más dispositivos de la red.

Para ver las asignaciones DHCP con conflictos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Conflicts Information.
Aparece la página DHCP Conflicts Information. La tabla muestra información de todas las asociaciones (bindings) con conflictos.

6. Para buscar una asociación con conflicto de dirección IP, escriba la dirección IP en el campo Search Conflict IP Address y haga clic en el botón Go.
Se muestra la información de la asociación.

   La siguiente tabla describe los campos no configurables de la página.

Tabla 32. Información de conflictos DHCP

Campo	Descripción
IP Address	La dirección IP del cliente DHCP.
Hardware Address	La dirección de hardware del cliente DHCP.

Tabla 32. Información de conflictos DHCP (continuación)

Campo	Descripción
Detection Method	El método con el que se detectó la dirección IP del cliente DHCP en el servidor DHCP.
Detection Time	El momento en que se detectó el conflicto, en formato días;horas;minutos;segundos desde el último reinicio del switch.

Eliminar una o todas las asociaciones DHCP con conflictos

Para eliminar una o todas las asociaciones DHCP con conflictos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Services > DHCP Server > DHCP Conflicts Information. Aparece la página DHCP Conflicts Information.

6. Seleccione uno de los siguientes botones de opción:

   • All Address Conflicts: Se borran todas las asociaciones con conflictos de dirección IP.
   • Specific Address Conflict: En el campo, especifique la dirección IP de la asociación con conflicto que se debe borrar.

7. Haga clic en el botón Clear.
Se eliminan la asignación o asignaciones seleccionadas.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Retransmisión DHCP y sus estadísticas

Si el switch funciona como dispositivo de capa 3, puede habilitar el agente de retransmisión DHCP de capa 3 para que el switch retransmita mensajes DHCP entre clientes y servidores DHCP ubicados en una subred IP diferente.

Para configurar una retransmisión DHCP y mostrar sus estadísticas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP Relay. Aparece la página DHCP Relay.

6. En el campo Maximum Hop Count, escriba el número máximo de saltos que puede dar una solicitud de cliente antes de descartarse.
El rango es de 1 a 16. El valor predeterminado es 4.

7. Seleccione el botón de opción Admin mode Disable o Enable para deshabilitar o habilitar la retransmisión DHCP en el switch.

8. En el campo Minimum Wait Time, escriba el tiempo mínimo en segundos que la retransmisión DHCP debe esperar antes de reenviar solicitudes.
Este tiempo se compara con la marca de tiempo de los paquetes de solicitud DHCP del cliente, que representa el tiempo desde que se encendió el cliente. Los paquetes solo se reenvían cuando la marca de tiempo supera el tiempo mínimo de espera. El rango es de 0 a 100.

9. Seleccione uno de los siguientes botones de opción de Circuit ID Option Mode:

- Enable: Las opciones del agente de retransmisión se agregan a las solicitudes antes de reenviarlas al servidor y se eliminan de las respuestas antes de reenviarlas a los clientes.
- Disable: Las opciones del agente de retransmisión no se agregan a las solicitudes antes de reenviarlas al servidor ni se eliminan de las respuestas antes de reenviarlas a los clientes.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para actualizar la información de la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 33. Información de estado de la retransmisión DHCP

Campo	Descripción
Requests Received	El número total de solicitudes DHCP recibidas de todos los clientes desde que se inició el switch.
Requests Relayed	El número total de solicitudes DHCP reenviadas al servidor desde que se inició el switch.
Packets Discarded	El número total de paquetes DHCP descartados por el agente de retransmisión desde que se inició el switch.

Retransmisión DHCP de capa 2

Si habilita y configura un agente de retransmisión DHCP en el switch, algunos dispositivos de capa 2 (L2) no necesitan conectarse a un servidor DHCP en la red física. Un agente de retransmisión completa automáticamente el campo de dirección IP de puerta de enlace (giaddr) y agrega la opción Relay Agent Information a los mensajes DHCP. Un servidor DHCP usa esta opción para direcciones IP y otras políticas de asignación. Un agente de retransmisión DHCP suele ser un dispositivo con enrutamiento IP, también llamado agente de retransmisión de capa 3. En algunas configuraciones de red, los dispositivos L2 deben agregar la opción Relay Agent Information porque están más cerca de los hosts finales.

Un dispositivo L2 puede operar solo como puente de una red y podría no tener una dirección IPv4 en esa red. Si un dispositivo L2 no tiene dirección IPv4 de origen, no puede retransmitir paquetes directamente a un servidor DHCP ubicado en otra red. En esa situación, el dispositivo L2 puede agregar la opción Relay Agent Information y difundir el mensaje DHCP.

Configurar los ajustes globales de retransmisión DHCP L2

Para configurar los ajustes globales de retransmisión DHCP L2:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration. Aparece la página DHCP L2 Relay Global Configuration.

6. Seleccione el botón de opción Admin mode Disable o Enable para deshabilitar o habilitar la retransmisión DHCP L2 en el switch.
El valor predeterminado es Disable.

7. En la sección DHCP L2 Relay VLAN Configuration, configure los siguientes ajustes:

- VLAN ID: El ID de una VLAN ya configurada en el switch. Esta página no permite agregar VLAN. Para agregar VLAN, consulte VLAN en la página 190.
- Admin mode: Habilita o deshabilita la retransmisión DHCP L2 en la VLAN.
- Circuit ID mode: Habilita o deshabilita la subopción Circuit ID de DHCP Option-82.
- Remote ID String: Especifique el Remote ID si la opción Remote ID está habilitada.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz de retransmisión DHCP L2

Puede habilitar la retransmisión DHCP L2 en una interfaz.

Para configurar una interfaz de retransmisión DHCP L2:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration.
Aparece la página DHCP L2 Relay Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin mode, seleccione si desea habilitar o deshabilitar la retransmisión DHCP L2 en la interfaz.
El valor predeterminado es Disable.

9. En el menú 82 Option Trust Mode, seleccione si desea habilitar o deshabilitar la interfaz como interfaz de confianza para la opción Relay Agent Information (Option 82).

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar las estadísticas de interfaz de retransmisión DHCP L2

Para mostrar las estadísticas de interfaz de retransmisión DHCP L2:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics. Aparece la página DHCP L2 Relay Interface Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es el ajuste predeterminado.
- VLANS: Solo se muestran las VLAN.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Para actualizar la información de la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 34. Información de estadísticas de interfaz de retransmisión DHCP L2

Campo	Descripción
Interface	La interfaz por la que se recibe el mensaje DHCP.
UntrustedServerMsgsWithOpt82	El número de mensajes DHCP con Option 82 recibidos de un servidor no confiable.

Tabla 34. Información de estadísticas de interfaz de retransmisión DHCP L2 (continuación)

Campo	Descripción
UntrustedClientMsgsWithOpt82	El número de mensajes DHCP con Option 82 recibidos de un servidor cliente.
TrustedServerMsgsWithoutOpt82	El número de mensajes DHCP sin Option 82 recibidos de un servidor de confianza no confiable.
TrustedClientMsgsWithoutOpt82	El número de mensajes DHCP sin Option 82 recibidos de un servidor de confianza cliente.

Retransmisión UDP

Puede habilitar el switch para que funcione como retransmisor UDP, lo que le permite reenviar paquetes de difusión User Datagram Protocol (UDP) de un router a una dirección IP en una subred local o no local.

Configurar los ajustes globales de retransmisión UDP y agregar una configuración UDP del switch

Para configurar los ajustes globales de retransmisión UDP y agregar una configuración UDP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > UDP Relay > UDP Relay Global Configuration. Aparece la página UDP Relay Global Configuration.

6. Seleccione el botón de opción Admin mode Disable o Enable para deshabilitar o habilitar la retransmisión UDP en el switch.
El valor predeterminado es Disable.

7. En la sección UDP Relay Global Configuration, configure los siguientes ajustes:

- Server Address: Escriba la dirección IPv4 del servidor de retransmisión UDP.
- UDP Port: Seleccione uno de los siguientes tipos de puerto UDP de destino:
  - Other: Se habilita el campo UDP Port Other Value para que pueda escribir un número de puerto UDP personalizado.
  - dhcp: Retransmite paquetes DHCP (puerto UDP 67).
  - domain: Retransmite paquetes DNS (puerto UDP 53).
  - isakmp: Retransmite paquetes ISAKMP (puerto UDP 500).
  - mobile-ip: Retransmite paquetes Mobile IP (puerto UDP 434)
  - nameserver: Retransmite paquetes IEN-116 Name Service (puerto UDP 42)
  - netbios-dgm: Retransmite paquetes NetBIOS Datagram Server (puerto UDP 138)
  - netbios-ns: Retransmite paquetes NetBIOS Name Server (puerto UDP 137)
  - ntp: Retransmite paquetes de network time protocol (puerto UDP 123).
  - pim-auto-rp: Retransmite paquetes PIM auto RP (puerto UDP 496).
  - rip: Retransmite paquetes Routing Image Protocol (RIP) (puerto UDP 520)
  - tacacs: Retransmite paquetes TACACS (puerto UDP 49)
  - tftp: Retransmite paquetes TFTP (puerto UDP 69)
  - time: Retransmite paquetes del servicio de hora (puerto UDP 37)
- UDP Port Other Value: Si selecciona Other en el menú UDP Port, escriba un número de puerto UDP personalizado de 0 a 65535.

8. Haga clic en el botón Add.
Se agrega la configuración UDP del switch.

El campo Hit Count muestra el número de paquetes UDP detectados en la interfaz UDP.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar una configuración UDP del switch

Para cambiar una configuración UDP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > UDP Relay > UDP Relay Global Configuration. Aparece la página UDP Relay Global Configuration.

6. En la sección UDP Relay Global Configuration, seleccione la casilla de la configuración UDP del switch.

7. Cambie los ajustes según sea necesario.
Para obtener más información, consulte Configurar los ajustes globales de retransmisión UDP y agregar una configuración UDP del switch en la página 117.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una configuración UDP del switch

Para eliminar una configuración UDP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > UDP Relay > UDP Relay Global Configuration. Aparece la página UDP Relay Global Configuration.

6. En la sección UDP Relay Global Configuration, seleccione la casilla de la configuración UDP del switch.

7. Haga clic en el botón Delete.
Se elimina la configuración UDP del switch.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Agregar una configuración UDP de interfaz

Para agregar una configuración de interfaz de retransmisión UDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > UDP Relay > UDP Relay Interface Configuration. Aparece la página UDP Relay Interface Configuration.

6. En el menú Interface, seleccione la interfaz o VLAN a la que agregará la configuración UDP.

7. En el campo Server Address, escriba la dirección IPv4 del servidor de retransmisión UDP.
8. En el menú UDP Port, seleccione uno de los siguientes tipos de puerto UDP de destino:

• Other: Se habilita el campo UDP Port Other Value para que pueda escribir un número de puerto UDP personalizado.
• dhcp: Retransmite paquetes DHCP (puerto UDP 67).
• domain: Retransmite paquetes DNS (puerto UDP 53).
• isakmp: Retransmite paquetes ISAKMP (puerto UDP 500).
• mobile-ip: Retransmite paquetes Mobile IP (puerto UDP 434)
• nameserver: Retransmite paquetes IEN-116 Name Service (puerto UDP 42)
• netbios-dgm: Retransmite paquetes NetBIOS Datagram Server (puerto UDP 138)
• netbios-ns: Retransmite paquetes NetBIOS Name Server (puerto UDP 137)
• ntp: Retransmite paquetes de network time protocol (puerto UDP 123).
• pim-auto-rp: Retransmite paquetes PIM auto RP (puerto UDP 496).
• rip: Retransmite paquetes Routing Image Protocol (RIP) (puerto UDP 520)
• tacacs: Retransmite paquetes TACACS (puerto UDP 49)
• tftp: Retransmite paquetes TFTP (puerto UDP 69)
• time: Retransmite paquetes del servicio de hora (puerto UDP 37)

9. Si selecciona Other en el menú UDP Port, escriba un número de puerto UDP personalizado en el campo UDP Port Other Value.
El número de puerto puede estar entre 0 y 65535.

10. En el menú Discard, seleccione si se descartan los paquetes que cumplen la condición:

• Enable: Los paquetes se descartan. Esta opción solo funciona si escribe 0.0.0.0 como dirección IP del servidor.
• Discard: Los paquetes no se descartan. Esta opción funciona si la dirección IP del servidor no es 0.0.0.0.

11. Haga clic en el botón Add.
Se agrega la configuración UDP de la interfaz.

El campo Hit Count muestra el número de paquetes UDP detectados en la interfaz UDP.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Cambiar una configuración UDP de interfaz

Para cambiar una configuración UDP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > UDP Relay > UDP Relay Interface Configuration. Aparece la página UDP Relay Interface Configuration.

6. En el menú Interface, seleccione la interfaz o VLAN.

7. Cambie los ajustes según sea necesario.
Para obtener más información, consulte Agregar una configuración UDP de interfaz en la página 120.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una configuración UDP del switch

Para eliminar una configuración UDP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > UDP Relay > UDP Relay Interface Configuration. Aparece la página UDP Relay Interface Configuration.

6. En el menú Interface, seleccione la interfaz o VLAN.

7. Haga clic en el botón Delete.
Se elimina la configuración UDP del switch.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Servidor DHCPv6

Puede configurar ajustes de servidor DHCPv6, pools DHCPv6, delegación de prefijos DHCPv6, interfaces DHCPv6 y asociaciones DHCPv6. También puede ver estadísticas de DHCPv6.

Habilitar el servidor DHCPv6

De forma predeterminada, el servidor DHCPv6 está deshabilitado. Puede habilitarlo para que el switch asigne información de configuración de red a clientes IPv6.

Para habilitar el servidor DHCPv6 en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Server Configuration. Aparece la página DHCPv6 Server Configuration.

6. Seleccione el botón de opción Admin mode
Enable. El valor predeterminado es Disable.

7. Haga clic en el botón Apply.
La configuración se guarda.

El campo DHCPv6 Server DUID muestra el identificador único DHCP (DUID) del servidor DHCPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar pools DHCPv6

Un pool DHCPv6 proporciona información de configuración de red disponible para los clientes DHCPv6 que la solicitan. Puede agregar, cambiar y eliminar pools DHCPv6.

Crear un pool DHCPv6 Un pool DHCPv6 proporciona información de configuración de red disponible para los clientes DHCPv6 que la solicitan. Para crear un pool DHCPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Pool Configuration. Aparece la página DHCPv6 Pool Configuration.

6. En el menú Pool Name, seleccione Create.

7. En el campo Pool Name, escriba un nombre que identifique el pool del servidor DHCPv6. El nombre puede tener hasta 31 caracteres.

8. Haga clic en el enlace Default Router Addresses y especifique la lista de direcciones IPv6 de router predeterminado del pool.
Puede especificar hasta ocho direcciones de router predeterminado en orden de preferencia.

9. Haga clic en el enlace Domain Name y especifique la lista de nombres de dominio IPv6 del pool. Un nombre de dominio puede tener hasta 255 caracteres alfanuméricos.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Cambiar un pool DHCPv6 Puede cambiar un pool DHCPv6 existente.

Para cambiar un pool DHCPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Pool Configuration. Aparece la página DHCPv6 Pool Configuration.

6. En el menú Pool Name, seleccione el nombre del pool. No puede cambiar el nombre del pool.

7. Haga clic en el enlace Default Router Addresses y cambie la lista de direcciones IPv6 de router predeterminado del pool.
Puede especificar hasta ocho direcciones de router predeterminado en orden de preferencia.

8. Haga clic en el enlace Domain Name y cambie la lista de nombres de dominio IPv6 del pool. Un nombre de dominio puede tener hasta 255 caracteres alfanuméricos.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar un pool DHCPv6 Puede eliminar un pool DHCPv6 que ya no necesite. Para eliminar un pool DHCPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Pool Configuration. Aparece la página DHCPv6 Pool Configuration.

6. En el menú Pool Name, seleccione el nombre del pool.

7. Haga clic en el botón
Delete. Se elimina el pool.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar la delegación de prefijos DHCPv6 para pools

Una configuración de delegación de prefijos asigna un prefijo IPv6 y una longitud de prefijo a un pool DHCPv6 que proporciona información de configuración de red a los clientes DHCPv6 que la solicitan.

Un cliente DHCPv6 puede solicitar varios prefijos IPv6 y también prefijos IPv6 específicos. Si un pool DHCPv6 contiene el prefijo específico que solicita un cliente DHCPv6, el prefijo se delega al cliente. De lo contrario, se delega al cliente el primer prefijo IPv6 disponible del pool.

Crear una configuración de delegación de prefijos DHCPv6 para un pool Para crear una configuración de delegación de prefijos DHCPv6 para un pool:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration.

Aparece la página DHCPv6 Prefix Delegation Configuration.

6. En el menú Pool Names, seleccione un pool.
7. En el campo Prefix, especifique el prefijo IPv6.
8. En el campo Prefix Length, especifique la longitud asociada al prefijo IPv6.

9. En el campo DUID, especifique el identificador único DHCP (DUID) asociado al prefijo IPv6.

Nota: El DUID y el nombre del cliente solo se usan si un dispositivo solicita un prefijo. De esta forma, el dispositivo recibe un prefijo IPv6 en lugar de una dirección IPv6 específica. Si asigna una dirección IPv6 específica al dispositivo, puede dejar en blanco los campos DUID y Client Name.

10. En el campo Client Name, escriba un nombre de cliente asociado al prefijo IPv6. El nombre, útil para registros o rastreo, puede tener hasta 31 caracteres.

11. En el campo Valid Lifetime, escriba el tiempo en segundos tras el cual expira el prefijo IPv6.
Escriba un valor entre 0 y 4294967295.

12. En el campo Prefer Lifetime, escriba el tiempo preferido en segundos tras el cual expira el prefijo IPv6.
Escriba un valor entre 0 y 4294967295.

13. Haga clic en el botón Add.
Se agrega la configuración de delegación de prefijos para el pool seleccionado.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Cambiar una configuración de delegación de prefijos DHCPv6 para un pool
Puede cambiar una configuración existente de delegación de prefijos DHCPv6.
Para cambiar una configuración de delegación de prefijos DHCPv6 para un pool:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration.
Aparece la página DHCPv6 Prefix Delegation Configuration.

6. En el menú Pool Names, seleccione el pool.

7. Cambie los ajustes según sea necesario.
Para obtener más información, consulte Crear una configuración de delegación de prefijos DHCPv6 para un pool en la página 126.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una configuración de delegación de prefijos DHCPv6 para un pool Puede eliminar una configuración existente de delegación de prefijos DHCPv6 que ya no necesite. Para eliminar una configuración de delegación de prefijos DHCPv6 para un pool:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration.
Aparece la página DHCPv6 Prefix Delegation Configuration.

6. En el menú Pool Names, seleccione el pool.

7. Haga clic en el botón Delete.
Se elimina la configuración de delegación de prefijos.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes DHCPv6 de una interfaz

Puede configurar los ajustes DHCPv6 de una interfaz para que esta proporcione servicios DHCPv6 a los dispositivos conectados.

Para configurar los ajustes DHCPv6 de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Interface Configuration. Aparece la página DHCPv6 Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

7. En el menú Admin mode, seleccione si desea habilitar o deshabilitar el modo de servidor DHCPv6 en la interfaz.

Nota: Las funciones de servidor DHCPv6 y de retransmisión DHCPv6 son mutuamente excluyentes. Para configurar una interfaz como retransmisión DHCPv6, consulte Interfaz de retransmisión DHCPv6 en la página 135.

8. En el campo Pool Name, seleccione un pool DHCPv6. Para obtener más información, consulte Administrar pools DHCPv6 en la página 124.

9. En el menú Rapid Commit, seleccione si desea habilitar o deshabilitar un intercambio abreviado entre el dispositivo que solicita información IPv6 y el servidor DHCPv6. Este ajuste es opcional.

10. En el campo Preference, especifique el valor de preferencia que un dispositivo puede usar para determinar la preferencia de esta interfaz respecto a otros servidores DHCPv6. Puede escribir un valor de 0 a 4294967295. El valor predeterminado es 0.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Mostrar las asociaciones DHCPv6

Después de que un cliente obtiene información de configuración IPv6 de un servidor DHCPv6, el servidor agrega una entrada a la tabla de asociaciones DHCPv6.

Para mostrar la información de asociaciones DHCPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Bindings Information. Aparece la página DHCPv6 Bindings Information.

6. Para buscar una asociación, escriba la dirección IPv6 en el campo Search Binding IP y haga clic en el botón Go.
Se muestra la información de la asociación.

7. La siguiente tabla describe los campos no configurables de la página.

8. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 35. Información de asociaciones DHCPv6

Campo	Descripción
Client Address	La dirección IPv6 del cliente asociado a la asociación.
Client Interface	El número de interfaz en la que se produjo la asociación del cliente.
Client DUID	El identificador único DHCPv6 (DUID) del cliente. El DUID es una combinación de la dirección de hardware y el identificador del cliente.
Prefix	La dirección IPv6 del prefijo delegado asociado a esta asociación.
Prefix Length	La longitud de máscara IPv6 del prefijo delegado asociado a esta asociación.
Prefix Type	El tipo de prefijo IPv6 asociado a esta asociación.
Expiry Time	El número de segundos hasta que expira el prefijo asociado a una asociación.
Valid Lifetime	El tiempo máximo en segundos que el cliente puede usar el prefijo.
Prefer Lifetime	El tiempo preferido en segundos que el cliente puede usar el prefijo.

Mostrar las estadísticas del servidor DHCPv6

Puede mostrar las estadísticas del servidor DHCPv6, incluida información sobre los mensajes DHCPv6 enviados, recibidos y descartados de forma global y en cada interfaz.

Para mostrar las estadísticas del servidor DHCPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Server Statistics. Se muestra la página DHCPv6 Server Statistics.

6. Realice una de las siguientes acciones:

- Mostrar estadísticas de una interfaz: en el menú Interface, seleccione la interfaz.
- Mostrar estadísticas de todas las interfaces: en el menú Interface, seleccione All.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 36. Información de estadísticas del servidor DHCPv6

Campo	Descripción
Mensajes recibidos	
Total de paquetes DHCPv6 recibidos	Número de mensajes DHCPv6 recibidos. Los mensajes DHCPv6 enviados de un cliente DHCP v6 a un servidor DHCP v6 incluyen solicit, request, confirm, renew, rebind, release, decline e information-request. Además, un agente de retransmisión DHCP v6 puede reenviar mensajes relay-forward a un servidor DHCP v6.
Paquetes DHCPv6 Solicit recibidos	Número de mensajes DHCPv6 Solicit recibidos. Este tipo de mensaje lo envía un cliente para localizar servidores DHCPv6.
Paquetes DHCPv6 Request recibidos	Número de solicitudes recibidas.
Paquetes DHCPv6 Confirm recibidos	Número de mensajes DHCPv6 Confirm recibidos. Este tipo de mensaje lo envía un cliente a todos los servidores DHCPv6 para determinar si su configuración es válida para el enlace conectado.
Paquetes DHCPv6 Renew recibidos	Número de mensajes DHCPv6 Renew recibidos. Este tipo de mensaje lo envía un cliente para extender y actualizar la información de configuración proporcionada por el servidor DHCPv6.
Paquetes DHCPv6 Rebind recibidos	Número de mensajes DHCPv6 Rebind recibidos. Este tipo de mensaje lo envía un cliente a cualquier servidor DHCPv6 cuando no recibe respuesta a un mensaje Renew.
Paquetes DHCPv6 Release recibidos	Número de mensajes DHCPv6 Release recibidos. Este tipo de mensaje lo envía un cliente para indicar que ya no necesita la dirección asignada.

Tabla 36. Información de estadísticas del servidor DHCPv6 (continuación)

Campo	Descripción
Paquetes DHCPv6 Decline recibidos	Número de mensajes DHCPv6 Decline recibidos. Este tipo de mensaje lo envía un cliente al servidor DHCPv6 para indicar que una dirección asignada ya está en uso en el enlace.
Paquetes DHCPv6 Inform recibidos	Número de mensajes DHCP v6 information-request recibidos. Este tipo de mensaje lo envía un cliente para solicitar información de configuración distinta de la asignación de dirección IP.
Paquetes DHCPv6 Relay-forward recibidos	Número de mensajes DHCPv6 relay-forward recibidos. Este tipo de mensaje lo envía un agente de retransmisión para reenviar mensajes a servidores.
Paquetes DHCPv6 Relay-reply recibidos	Número de mensajes DHCP v6 relay-reply recibidos. Este tipo de mensaje lo envía un servidor a un agente de retransmisión DHCP v6 y contiene el mensaje que el agente de retransmisión debe entregar al cliente.
Paquetes DHCPv6 mal formados recibidos	Número de mensajes DHCPv6 recibidos pero descartados por estar mal formados.
Paquetes DHCPv6 recibidos descartados	Número de paquetes descartados.
Mensajes enviados	
Total de paquetes DHCPv6 enviados	Número de mensajes DHCPv6 enviados. Los mensajes DHCPv6 enviados de un servidor DHCPv6 a un cliente DHCPv6 incluyen Advertise, Reply, Reconfigure y Relay-Reply.
Paquetes DHCPv6 Advertisement transmitidos	Número de mensajes DHCPv6 Advertise enviados. Este tipo de mensaje lo envía un servidor a un cliente DHCPv6 en respuesta a un mensaje Solicit e indica que está disponible para dar servicio.
Paquetes DHCPv6 Reply transmitidos	Número de mensajes DHCPv6 Reply enviados a un cliente DHCPv6 en respuesta a un mensaje solicit, request, renew, rebind, information-request, confirm, release o decline.
Paquetes DHCPv6 Reconfig transmitidos	Número de mensajes DHCPv6 reconfigure enviados. Este tipo de mensaje lo envía un servidor a un cliente DHCPv6 para informarle que el servidor tiene información nueva o actualizada. Normalmente, el cliente inicia entonces una transacción renew/reply o Information-request/reply con el servidor para recibir la información actualizada.

Tabla 36. Información de estadísticas del servidor DHCPv6 (continuación)

Campo	Descripción
Paquetes DHCPv6 Relay-forward transmitidos	Número de mensajes DHCPv6 Relay-Forward enviados. Este tipo de mensaje lo envía un agente de retransmisión para reenviar mensajes a servidores.
Paquetes DHCPv6 Relay-reply transmitidos	Número de mensajes DHCPv6 Relay-Reply enviados. Este tipo de mensaje lo envía un servidor a un agente de retransmisión DHCPv6 y contiene el mensaje que el agente de retransmisión debe entregar al cliente.

Eliminar las estadísticas DHCPv6 de una o todas las interfaces

Para eliminar las estadísticas DHCPv6 de una o todas las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Server > DHCPv6 Server Statistics. Se muestra la página DHCPv6 Server Statistics.

6. Realice una de las siguientes acciones:

   - Eliminar estadísticas de una interfaz: en el menú Interface, seleccione la interfaz.
   - Eliminar estadísticas de todas las interfaces: en el menú Interface, seleccione All.

7. Haga clic en el botón Clear (Borrar).
Se eliminan las estadísticas seleccionadas.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Interfaz de retransmisión DHCPv6 (relay)

Un agente de retransmisión DHCPv6 permite adjuntar subopciones a los mensajes que el switch retransmite a un servidor DHCPv6. A su vez, el servidor DHCPv6 puede usar esta información para determinar la dirección que asignará a un cliente DHCPv6.

Para configurar una interfaz como retransmisión DHCPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Services > DHCPv6 Relay. Se muestra la página DHCPv6 Relay.

Se muestra la página DHCPv6 Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

7. En el menú Admin mode, seleccione si desea habilitar o deshabilitar el modo de retransmisión DHCPv6 en la interfaz.

Nota: Las funciones de retransmisión DHCPv6 y de servidor DHCPv6 son mutuamente excluyentes. Para obtener información sobre cómo configurar una interfaz como servidor DHCPv6, consulte Configurar los ajustes de DHCPv6 de una interfaz en la página 129.

8. En el menú Relay Interface, seleccione la interfaz, el LAG o la VLAN conectada al servidor de retransmisión DHCPv6.

9. En el campo Destination IP Address, especifique la dirección IPv6 del servidor de retransmisión DHCPv6.

10. En el campo Remote ID, especifique la opción de información del agente de retransmisión. El ID remoto se deriva del DUID del servidor DHCPv6 y del número de la interfaz de retransmisión, o bien puede especificarlo como una cadena definida por el usuario.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Power over Ethernet

Puede establecer la configuración global de Power over Ethernet (PoE) y la configuración PoE de cada puerto.

Conceptos de PoE

Los modelos Power over Ethernet (PoE) admiten ocho puertos PoE+ o PoE++ con las capacidades por puerto y presupuestos que se describen en la siguiente tabla.

Tabla 37. Capacidades y presupuestos de los puertos PoE

Modelo	Puertos PoE	Capacidad del puerto	Presupuesto PoE del switch
M4250-10G2F-PoE+	8 PoE+ (802.3at)	30W	125W
M4250-10G2XF-PoE+	8 PoE+ (802.3at)	30W	240W
M4250-10G2XF-PoE++	8 PoE++ (802.3bt)	90W	720W
M4250-26G4F-PoE+	8 PoE+ (802.3at)	30W	300W
M4250-26G4XF-PoE+	8 PoE+ (802.3at)	30W	480W
M4250-26G4F-PoE++	8 PoE++ (802.3bt)	90W	1440W con ambas PSU internas conectadas
M4250-40G8F-PoE+	8 PoE+ (802.3at)	30W	480W

Tabla 37. Capacidades y presupuestos de los puertos PoE (continuación)

Modelo	Puertos PoE	Capacidad del puerto	Presupuesto PoE del switch
M4250-40G8XF-PoE+	8 PoE+ (802.3at)	30W	960W
M4250-40G8XF-PoE++	8 PoE++ (802.3bt)	90W	2880W con tres PSU internas conectadas

La alimentación suministrada se prioriza según el orden de los puertos, hasta el presupuesto total de energía del dispositivo. El puerto 1 recibe la prioridad PoE más alta y el puerto 8 la más baja.

Si los requisitos de energía de los dispositivos alimentados (PD) conectados superan el presupuesto total del switch, se deshabilita la energía PoE del dispositivo en el puerto PoE activo con el número más alto, para garantizar que los dispositivos conectados a los puertos PoE de mayor prioridad y número más bajo reciban energía primero.

Aunque un dispositivo figure como alimentado por 802.3bt PoE++ o por 802.3at PoE+, es posible que no requiera el límite máximo de potencia que especifica su estándar IEEE. Muchos dispositivos requieren menos potencia, lo que permite que los 8 puertos PoE estén activos a la vez si los dispositivos informan correctamente su clase PoE.

La siguiente tabla muestra los rangos de potencia estándar, calculados con la longitud máxima de cable de 328 pies (100 metros). Si un dispositivo recibe energía PoE insuficiente del switch, considere usar un cable más corto.

Tabla 38. Clases PoE y asignaciones de potencia PoE

Clase del dispositivo	Norma PoE compatible	Descripción de la clase	Potencia máxima reservada para el PD	Potencia entregada al PD
0	PoE, PoE+ y PoE++	Potencia predeterminada (completa)	15.4W	0.44W–15.8W
1	PoE, PoE+ y PoE++	Potencia muy baja	4.0W	0.44W–3.84W
2	PoE, PoE+ y PoE++	Potencia baja	7.0W	3.84W–7.2W
3	PoE, PoE+ y PoE++	Potencia media	15.4W	6.49W–15.9W
4	PoE+ y PoE++	Potencia alta	30.0W	12.95W–30.8W
5	PoE++	Potencia ultra alta	45.0W	25.5W–47.0W
6	PoE++	Potencia ultra alta	60.0W	51.0W–64.4W

Tabla 38. Clases PoE y asignaciones de potencia PoE (continuación)

Clase del dispositivo	Norma PoE compatible	Descripción de la clase	Potencia máxima reservada para el PD	Potencia entregada al PD
7	PoE++	Potencia ultra alta	75.0W	62.0W–81.1W
8	PoE++	Potencia ultra alta	90.0W	71.0W–96.5W

Configurar los ajustes globales de PoE

Para configurar los ajustes globales de PoE:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > PoE > Basic > PoE Configuration. Se muestra la página PoE Configuration.

6. En el campo System Usage Threshold, introduzca un número de 1 a 99 para establecer el umbral a partir del cual se envía un trap si la potencia consumida supera la potencia de umbral.

7. En el menú Power Management mode, seleccione el algoritmo de administración de energía que usa el switch para suministrar energía a los PD solicitantes:

- Static: seleccione Static para que la potencia asignada a cada puerto dependa del tipo de umbral de potencia configurado en el puerto.
- Dynamic: seleccione Dynamic para que el consumo de energía de cada puerto se mida y calcule en tiempo real. Esta es la configuración predeterminada.

8. Para configurar los traps, en la sección PoE Trap Configuration, seleccione uno de los siguientes botones de opción:

- Enable: activa los traps de PoE. Esta es la configuración predeterminada.
- Disable: desactiva los traps de PoE.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 39. Información de PoE

Campo	Descripción
Versión de firmware	Versión de firmware del software PoE.
Estado de alimentación	Estado de la alimentación.
Potencia total disponible (W)	Potencia máxima en vatios que el switch puede suministrar a todos los puertos.
Potencia de umbral (W)	Si la potencia consumida es inferior a la potencia de umbral, el switch puede alimentar otro puerto. La potencia consumida puede estar entre la potencia nominal y la de umbral. La potencia de umbral se muestra en vatios. Nota: El valor de la potencia de umbral lo determina el valor que introduzca en el campo System Usage Threshold.
Potencia consumida (W)	Potencia total en vatios que se suministra a todos los puertos.

Configurar los ajustes de los puertos PoE

Para configurar los ajustes de los puertos PoE:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > PoE > Advanced > PoE Port Configuration. Se muestra la página PoE Port Configuration.

6. Seleccione uno o más puertos mediante una de las siguientes acciones:

• Para configurar un solo puerto, marque la casilla del puerto o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varios puertos con la misma configuración, marque la casilla de cada puerto.
• Para configurar todos los puertos con la misma configuración, marque la casilla de la fila de encabezado.

7. En el menú Port Power, seleccione el modo PoE administrativo del puerto:

• Enable: se habilita la capacidad del puerto de suministrar energía. Es la opción predeterminada.
• Disable: se deshabilita la capacidad del puerto de suministrar energía.

8. En el menú Port Priority, seleccione la prioridad del puerto con respecto a los demás para cuando la potencia total que el switch puede suministrar supere el presupuesto total de energía:

• Low: prioridad baja. Esta es la configuración predeterminada.
• Medium: prioridad media.
• High: prioridad alta.
• Critical: prioridad crítica.

La prioridad del puerto determina qué puertos pueden seguir suministrando energía cuando la potencia total suministrada por el switch supera el presupuesto total. (En esa situación, es posible que el switch no pueda alimentar todos los dispositivos conectados). Si dos puertos tienen la misma prioridad, el puerto con el número más bajo recibe mayor prioridad.

9. En el menú Power Mode, seleccione el modo PoE en el que debe funcionar el puerto:

• 802.3af: el puerto se alimenta en modo IEEE 802.3af y está limitado a él. Un PD que requiere IEEE 802.3at no recibe energía si el puerto funciona en modo IEEE 802.3af.
• Legacy: el puerto se alimenta con corriente de arranque alta, usada por PD heredados que requieren más de 15W para encenderse.
• Pre-802.3at: el puerto se alimenta inicialmente en modo IEEE 802.3af y, antes de 75 ms, cambia al modo de alta potencia IEEE 802.3at. Seleccione este modo si el PD no realiza clasificación de capa 2 o si el switch realiza clasificación de capa 1 de 2 eventos.
• 802.3at: el puerto se alimenta en modo IEEE 802.3at y es compatible con versiones anteriores de IEEE 802.3af. El modo 802.3at es el predeterminado. En este modo, si el switch detecta que el PD conectado solicita más potencia que IEEE 802.3af pero no es un dispositivo IEEE 802.3at clase 4, el PD no recibe energía del switch.
• Pre-802.3bt: el puerto admite dispositivos clase 4 que usan PoE de 4 pares (4PPoE) para recibir más de 30W, pero que no cumplen con IEEE 802.3bt. El puerto también admite los modos IEEE 802.3at e IEEE 802.3af.

• 802.3bt-Type3. El puerto admite el modo IEEE 802.3bt tipo 3, el modo IEEE 802.3at y el modo IEEE 802.3af.
• 802.3bt: el puerto se alimenta en modo IEEE 802.3bt y es compatible con versiones anteriores de IEEE 802.3at e IEEE 802.3af. En este modo, si el switch detecta que el PD conectado solicita más potencia que IEEE 802.3at pero no es un dispositivo IEEE 802.3bt, el PD no recibe energía del switch.

10. En el menú Power Limit Type, seleccione cómo controla el puerto la potencia máxima que puede suministrar:

• None: en los puertos PoE+ (802.3at), el puerto consume hasta la potencia máxima de clase 0 en modo de baja potencia. En modo de alta potencia, se aplica lo siguiente:

- Puertos PoE+ (802.3at): el puerto consume hasta la potencia máxima de clase 4.
- Puertos PoE++ (802.3bt): el puerto consume hasta la potencia máxima de clase 8.

• Class: el límite de potencia del puerto es igual a la clase del PD conectado. Esta es la configuración predeterminada. El límite superior es la potencia que un puerto puede suministrar a un PD. La clase se detecta según el PD conectado al puerto, y se aplica lo siguiente:

- Puertos PoE+ (802.3at): los valores posibles van de clase 0 a clase 4.
- Puertos PoE++ (802.3bt): los valores posibles van de clase 0 a clase 8.

• User: el límite de potencia del puerto es igual al valor especificado en el campo Power Limit (W).

Nota: Si un PD no informa correctamente su clase, estas opciones pueden ahorrar potencia PoE adicional al evitar que el switch suministre más potencia de la que requiere el PD. Sin embargo, según la opción que seleccione, es posible que un PD que no informa correctamente su clase no se encienda en absoluto.

11. En el campo Power Limit (W), introduzca la potencia máxima (en W) que el puerto puede suministrar.
Se aplica lo siguiente:

• Puertos PoE+ (802.3at): el rango es de 3.0W a 30.0W.
• Puertos 802.3bt-Type3 (opción del menú Power Mode): el rango es de 3.0W a 60.0W.
• Puertos PoE++ (802.3bt): el rango es de 3.0W a 99.9W.

12. En el menú Detection Type, seleccione cómo detecta el puerto el PD conectado:

• IEEE 802: el puerto realiza una detección resistiva de 4 puntos. Esta es la configuración predeterminada.

• 4pt 802.3af + Legacy: el puerto realiza una detección resistiva de 4 puntos y, si es necesario, continúa con la detección heredada (legacy).
• Legacy: el puerto realiza la detección heredada.

13. En el menú Timer Schedule, seleccione una programación de temporizador o seleccione None, que es la opción predeterminada.
Para obtener información sobre cómo establecer y configurar programaciones de temporizador PoE, consulte Programaciones de temporizador en la página 144.

14. Haga clic en el botón Apply (Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 40. Información de los puertos PoE

Campo	Descripción
Alta potencia	Todos los puertos admiten el modo de alta potencia.
Potencia máx. (W)	Potencia máxima en vatios que puede suministrar el puerto.
Clase	La clase define el rango de potencia que un dispositivo alimentado (PD) consume del switch. Las clases se definen de la siguiente manera: • 0: 0.44W–15.8W • **1**: 0.44W–3.84W • **2**: 3.84W–7.2W • **3**: 6.49W–15.9W • **4**: 12.95W–30.8W • **5**: 25.5W–47.0W • **6**: 51.0W–64.4W • **7**: 62.0W–81.1W • **8**: 71.0W–96.5W • Unknown: no se puede detectar la clase o no hay ningún PD conectado al puerto.
Voltaje de salida (V)	Voltaje suministrado al PD, en voltios.
Corriente de salida (mA)	Corriente suministrada al PD, en mA.
Potencia de salida (W)	Potencia suministrada al PD, en vatios.

Tabla 40. Información de los puertos PoE (continuación)

Campo	Descripción
Estado	Estado operativo del puerto: • Disabled: no se suministra energía. • Delivering Power. El PD está consumiendo energía. • Requesting Power: el puerto está solicitando energía. • Fault: se produjo un problema con la alimentación. • Test: el puerto está en modo de prueba. • Other Fault: el puerto está inactivo debido a una condición de error. • Searching: el puerto no está en ninguno de los demás estados de esta lista.
Estado de falla	Descripción del error cuando el puerto PoE está en estado de falla: • No Error: el puerto no está en ningún estado de error y puede suministrar energía. • MPS Absent: el puerto detectó la ausencia de la fuente de alimentación principal, lo que le impide suministrar energía. • Short: el puerto detectó un cortocircuito, lo que le impide suministrar energía. • Overload: el PD conectado al puerto intenta consumir más potencia de la permitida por la configuración del puerto, lo que impide que el puerto suministre energía. • Power Denied: se negó la energía al puerto por falta de potencia o por una condición administrativa. En esta condición,

Reiniciar la alimentación de uno o más puertos PoE

Puede reiniciar la alimentación de uno o más puertos PoE. Esto puede ser útil si los puertos PoE no funcionan como se espera.

Para reiniciar la alimentación de uno o más puertos PoE:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > PoE > Advanced > PoE Port Configuration. Se muestra la página PoE Port Configuration.

6. Seleccione uno o más puertos mediante una de las siguientes acciones:

• Para reiniciar un solo puerto, marque la casilla del puerto o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para reiniciar varios puertos con la misma configuración, marque la casilla de cada puerto.
• Para reiniciar todos los puertos con la misma configuración, marque la casilla de la fila de encabezado.

7. Haga clic en el botón Power-Cycle Port(s).
Se reinicia la alimentación de los puertos.

Programaciones de temporizador

Puede definir varias programaciones de temporizador (cada una con un nombre único) para el suministro de energía PoE a los PD conectados y para listas de control de acceso:

- Programaciones de temporizador para PoE:
  Después de crear una programación, puede asociarla con uno o más puertos PoE (consulte Configurar los ajustes de los puertos PoE en la página 139). También puede usar una programación distinta para cada puerto PoE.
  Después de asociar una programación a un puerto PoE, la fecha y hora de inicio obligan al puerto PoE a dejar de suministrar energía, y la fecha y hora de fin permiten que el puerto PoE vuelva a suministrar energía.
- Programaciones de temporizador para listas de control de acceso:
  Después de crear una programación, puede asociarla con una o más listas de control de acceso (consulte Listas de control de acceso en la página 646). También puede usar una programación distinta para cada lista de control de acceso.

Puede crear programaciones absolutas, que se aplican a fechas y horas específicas, y programaciones recurrentes. Para cada programación puede agregar varias entradas que se aplican solo a la programación seleccionada.

Crear una programación de temporizador

Puede agregar un máximo de 100 programaciones de temporizador.

Para crear una programación de temporizador:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Timer Schedule > Basic > Global Configuration. Se muestra la página Timer Schedule Name.

6. En el campo Timer Schedule Name, especifique el nombre de la programación.

7. Haga clic en el botón Add (Agregar).
La programación se agrega a la tabla de la página Timer Schedule Name y se le asigna un ID.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Definir los ajustes de una programación absoluta

Una programación absoluta se aplica a fechas y horas específicas. La programación se ejecuta una sola vez.

Para definir los ajustes de una programación que usa fechas y horas específicas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Timer Schedule > Advanced > Timer Schedule Configuration. Se muestra la página Timer Schedule Configuration.

6. En la sección Timer Schedule Selection, realice sus selecciones en los siguientes menús:

a. Timer Schedule Name. Seleccione el nombre de la programación que desea configurar.
Solo puede seleccionar nombres de programaciones que haya creado (consulte Crear una programación de temporizador en la página 144).

b. Timer Schedule Type. Seleccione Absolute.

Los campos de la sección Timer Schedule Configuration pueden ajustarse para permitirle configurar una programación para fechas y horas específicas.

c. Timer Schedule Entry. Para agregar una entrada nueva, seleccione new. Si selecciona una entrada existente, puede modificarla.

7. En la sección Timer Schedule Configuration, especifique las horas y fechas: a. En el campo Time Start, introduzca la hora del día en formato HH:MM para indicar cuándo debe iniciar la programación.
b. En el campo Time End, introduzca la hora del día en formato HH:MM para indicar cuándo debe detenerse la programación.
c. Junto al campo Date Start, haga clic en el icono de calendario y use los menús de la ventana emergente para introducir la fecha en formato DD-Mon-YYY e indicar cuándo debe iniciar la programación.

d. Junto al campo Date End, haga clic en el icono de calendario y use los menús de la ventana emergente para introducir la fecha en formato DD-Mon-YYY e indicar cuándo debe detenerse la programación.

8. Haga clic en el botón Add (Agregar).
Se agrega la entrada de la programación.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Definir los ajustes de una programación recurrente

Un programa recurrente le permite configurar un solo programa que inicia en una fecha determinada y se repite hasta una fecha de fin específica o de forma indefinida.

Para un solo programa de temporizador recurrente, puede agregar una configuración diaria, semanal y mensual. Es decir, estas configuraciones no son mutuamente excluyentes, sino que se complementan.

Para especificar la configuración de un programa de temporizador con patrón de recurrencia:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Timer Schedule > Advanced > Timer Schedule Configuration. Se muestra la página Timer Schedule Configuration.

6. En la sección Timer Schedule Selection, realice sus selecciones en los siguientes menús:

a. Timer Schedule Name: seleccione el nombre del programa de temporizador que desea configurar.
Solo puede seleccionar nombres de programaciones que haya creado (consulte Crear una programación de temporizador en la página 144).

b. Timer Schedule Type: seleccione Periodic.
Los campos de la sección Timer Schedule Configuration pueden ajustarse para permitirle configurar un programa de temporizador con patrón de recurrencia.

c. Timer Schedule Entry: para agregar una entrada nueva, seleccione new. Si selecciona una entrada existente, puede modificarla.

7. En la sección Timer Schedule Configuration, especifique el patrón de recurrencia: a. En el campo Time Start, introduzca la hora del día en formato HH:MM para indicar cuándo debe iniciar la programación.
b. En el campo Time End, introduzca la hora del día en formato HH:MM para indicar cuándo debe detenerse la programación.

c. Junto al campo Date Start, haga clic en el icono de calendario y use los menús de la ventana emergente para introducir la fecha en formato DD-Mon-YYY e indicar cuándo debe iniciar la programación.

d. Seleccione el botón de opción No End Date o el botón de opción End Date y, junto al campo End Date, haga clic en el ícono de calendario y use los menús de la ventana emergente para introducir la fecha en formato DD-Mon-YYY e indicar cuándo debe detenerse el programa.

e. En el menú Recurrence Pattern, seleccione el patrón:

- Daily: el programa se repite diariamente. Los campos se ajustan.
  Seleccione el botón de opción Every Weekday para que el programa opere de lunes a viernes, o seleccione el botón de opción Every Day(s) e introduzca un número de 0 a 255 en el campo.
  En este último caso, el programa se activa cada número de días especificado. Si no se especifica el número de días o si introduce 0, el programa se activa una sola vez.
- Weekly: el programa se repite semanalmente. Los campos se ajustan.
  En el campo Every Week(s), introduzca un número de 0 a 255 para que el programa se active cada número de semanas especificado. Si no se especifica el número de semanas o si introduce 0, el programa se activa una sola vez.
  Seleccione una, varias o todas las casillas Week Day para especificar el día o los días de la semana en que debe operar el programa.
- Monthly: el programa se repite mensualmente. Los campos se ajustan.
  En el campo Day, introduzca un número de 1 a 31 para indicar el día del mes en que debe activarse el programa.
  En el campo Every Month(s), introduzca un número de 0 a 99 para que el programa se active cada número de meses especificado. Si no se especifica el número de meses o si introduce 0, el programa se activa una sola vez.

8. Haga clic en el botón Add (Agregar).
Se agrega la entrada de la programación.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar la configuración de una entrada de programa de temporizador recurrente

Puede cambiar la configuración de una entrada de programa recurrente existente. (No puede hacerlo con un programa de temporizador absoluto existente).

Para cambiar la configuración de una entrada de programa de temporizador recurrente existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Timer Schedule > Advanced > Timer Schedule Configuration. Se muestra la página Timer Schedule Configuration.

6. En el menú Timer Schedule Name, seleccione el nombre del programa.
7. En el menú Timer Schedule Type, seleccione el tipo de programa.
8. En el menú Timer Schedule Entry, seleccione la entrada del programa.

9. Realice los cambios en la entrada del programa.
Para más información, consulte Especificar la configuración de un programa de temporizador recurrente en la página 146.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar una entrada de programa de temporizador

Puede eliminar una entrada de programa de temporizador que ya no necesite.

Para eliminar una entrada de programa de temporizador:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Timer Schedule > Advanced > Timer Schedule Configuration. Se muestra la página Timer Schedule Configuration.

6. En el menú Timer Schedule Name, seleccione el nombre del programa.
7. En el menú Timer Schedule Type, seleccione el tipo de programa.
8. En el menú Timer Schedule Entry, seleccione la entrada del programa.
9. Haga clic en el botón Delete. Se elimina la entrada.
10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar un programa de temporizador

Puede eliminar un programa de temporizador que ya no necesite. También se eliminan todas sus entradas.

Para eliminar un programa de temporizador:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Timer Schedule > Basic > Global Configuration. Se muestra la página Timer Schedule Name.

6. Seleccione la casilla del programa que desea eliminar.
7. Haga clic en el botón Delete.

Se elimina el programa.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Simple Network Management Protocol

Puede configurar SNMP para SNMPv1, SNMPv2 y SNMPv3. El switch admite la configuración de grupos y usuarios SNMP que pueden administrar los traps que genera el agente SNMP.

El switch usa MIB públicas estándar para la funcionalidad estándar y MIB privadas que admiten funciones adicionales del switch.

Administrar comunidades SNMPv1 y SNMPv2

De forma predeterminada, no existen comunidades SNMP. Las comunidades que defina pueden acceder al switch mediante SNMPv1 y SNMPv2. Solo las comunidades con acceso de lectura/escritura pueden usarse para cambiar la configuración mediante SNMP.

Agregar una comunidad SNMPv1 y SNMPv2 Puede agregar una comunidad SNMPv1 y SNMPv2, que permite el acceso tanto SNMPv1 como SNMPv2. Para agregar una comunidad SNMPv1 y SNMPv2:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Community Configuration. Se muestra la página Community Configuration.

6. En el campo Community Name, escriba un nombre para la nueva comunidad. El nombre puede tener hasta 16 caracteres.

7. Especifique la dirección IP y la máscara IP del cliente:

• Client Address: introduzca la dirección IP del cliente.
• Client IP Mask: introduzca la máscara IP del cliente.

La dirección IP y la máscara IP del cliente indican juntas un rango de direcciones IP desde el que los clientes SNMP pueden usar la comunidad para acceder al switch.

Si la dirección IP o la máscara IP del cliente es 0.0.0.0, se permite el acceso desde cualquier dirección IP. De lo contrario, se aplica un AND entre la dirección IP de cada cliente y la máscara, al igual que con la dirección IP del cliente. Si los valores coinciden, se permite el acceso.

Por ejemplo, si la dirección IP y la máscara IP del cliente son 192.168.1.0/255.255.255.0, se permite el acceso a cualquier cliente con una dirección IP de 192.168.1.0 a 192.168.1.255 (inclusive). Para permitir el acceso desde una sola estación, use una máscara IP de 255.255.255.255 y use la dirección IP de esa computadora como dirección del cliente.

8. En el menú Access Mode, seleccione el nivel de acceso de esta comunidad: Read/ Write o Read Only.

9. Haga clic en el botón Add.
Se agrega la comunidad.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Cambiar una comunidad SNMPv1 y SNMPv2 existente Puede cambiar una comunidad SNMPv1 y SNMPv2 existente.
Para modificar una comunidad SNMPv1 y SNMPv2 existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Community Configuration. Se muestra la página Community Configuration.

6. Seleccione la casilla junto a la comunidad.
7. Cambie la configuración según sea necesario.

Para más información sobre la configuración, consulte Agregar una comunidad SNMPv1 y SNMPv2 en la página 151.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una comunidad SNMPv1 y SNMPv2 Puede eliminar una comunidad SNMPv1 y SNMPv2 que ya no necesite.
Para eliminar una comunidad SNMPv1 y SNMPv2:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Community Configuration. Se muestra la página Community Configuration.

6. Seleccione la casilla junto a la comunidad.

7. Haga clic en el botón Delete.
Se elimina la comunidad.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar la configuración de traps SNMPv1 y SNMPv2

Para cada comunidad SNMP, puede especificar la interfaz de origen que debe usarse en el switch, el nombre de la comunidad, la dirección IP asociada y otros parámetros.

Agregar una configuración de trap SNMPv1 o SNMPv2 para un host Puede agregar una configuración de trap para un host, lo que le permite recibir traps SNMPv1 o SNMPv2.

Para agregar una configuración de trap SNMPv1 o SNMPv2 para un host:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Trap Configuration. Se muestra la página Trap Configuration.

6. En el menú Source Interface, seleccione la interfaz de origen que debe usarse para el receptor de traps SNMP:

- None: Se usa como dirección de origen la dirección IP principal de la interfaz de salida.
- Routing interface: Se usa como dirección de origen la dirección IP principal de un puerto físico.
- Routing VLAN: Se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento VLAN.
- Routing loopback interface: Se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.
- Tunnel interface: La interfaz de túnel IPv6.
- Service port: Se usa como dirección de origen la dirección IP del puerto de administración.

De forma predeterminada, se usa VLAN 1 como interfaz de origen.

7. En el campo Community Name, especifique el nombre de la comunidad SNMP que incluye el host de administración SNMP y el agente SNMP del dispositivo. El nombre puede tener hasta 16 caracteres y distingue mayúsculas y minúsculas.

8. En el menú Version, seleccione la versión de SNMP que usará el receptor:

- SNMPv1: el switch usa SNMPv1 para enviar traps al receptor. El valor predeterminado es SNMPv1.
- SNMPv2: el switch usa SNMPv2 para enviar traps al receptor.

9. En el menú Protocol, seleccione el protocolo que usará el receptor: Seleccione IPv4 si la dirección del receptor es IPv4 o IPv6 si la dirección del receptor es IPv6. También puede seleccionar DNS e introducir un nombre de dominio.

10. En el campo Address, introduzca la dirección IPv4 o IPv6 o el nombre de dominio, según lo seleccionado en el menú Protocol.

11. Haga clic en el botón Add.
Se agrega la configuración de trap.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Cambiar una configuración de trap SNMPv1 o SNMPv2 para un host Puede cambiar una configuración de trap SNMPv1 o SNMPv2 existente para un host. Para cambiar una configuración de trap SNMPv1 o SNMPv2 para un host:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Trap Configuration. Se muestra la página Trap Configuration.

6. Seleccione la casilla junto a la configuración de trap.

7. Cambie la configuración según sea necesario.
Para más información, consulte Agregar una configuración de trap SNMPv1 o SNMPv2 para un host en la página 153.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una configuración de trap SNMPv1 o SNMPv2 para un host Puede eliminar una configuración de trap SNMPv1 o SNMPv2 que ya no necesite para un host.

Para eliminar una configuración de trap SNMPv1 o SNMPv2 para un host:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Trap Configuration. Se muestra la página Trap Configuration.

6. Seleccione la casilla junto a la configuración de trap.

7. Haga clic en el botón Delete.
Se elimina la configuración de trap.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los indicadores de trap SNMPv1 y SNMPv2

Puede habilitar o deshabilitar traps específicos. Cuando ocurre en el switch la condición identificada por un trap activo, se envía un mensaje de trap a todos los receptores SNMP habilitados y se escribe un mensaje en el registro de traps.

Para configurar los indicadores de trap:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Trap Flags. Se muestra la página Trap Flags.

6. Seleccione el botón de opción Authentication Disable o Enable.
Esto habilita o deshabilita los traps por fallas de autenticación. El valor predeterminado es Enable.

Si está habilitado, se envían traps SNMP cuando ocurren eventos de autenticación, por ejemplo, cuando un usuario intenta acceder a la interfaz principal del switch sin un nombre de usuario y contraseña válidos.

7. Seleccione el botón de opción Link Up/Down Disable o Enable
Esto habilita o deshabilita los traps de estado del enlace. El valor predeterminado es Enable.

Si está habilitado, se envían traps SNMP cuando cambia el estado administrativo u operativo de un enlace físico o lógico

8. Seleccione el botón de opción Multiple Users Disable o Enable
Esto habilita o deshabilita los traps de múltiples usuarios. El valor predeterminado es Enable. Este trap se activa cuando el mismo ID de usuario inicia sesión en el switch más de una vez al mismo tiempo (por Telnet o por el puerto serie).

9. Seleccione el botón de opción Spanning Tree Disable o Enable.
Esto habilita o deshabilita los traps de spanning tree. El valor predeterminado es Enable.

10. Seleccione el botón de opción ACL Disable o Enable.
Esto habilita o deshabilita los traps de ACL. El valor predeterminado es Disable.

11. Seleccione el botón de opción Captive Portal Disable o Enable.
Esto habilita o deshabilita los traps del portal cautivo. El valor predeterminado es Disable.

12. Seleccione el botón de opción PIM Disable o Enable.
Esto habilita o deshabilita los traps de PIM. El valor predeterminado es Disable.

13. Seleccione el botón de opción PoE Disable o Enable.
Esto habilita o deshabilita los traps de PoE. El valor predeterminado es Enable.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Mostrar las MIB compatibles

Para mostrar las MIB compatibles con el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V1/V2 > Supported MIBs. Se muestra la página Supported MIBs.

   El campo Name muestra el número de RFC, si corresponde, y el nombre de la MIB. El campo Description muestra el título del RFC o la descripción de la MIB.

Administrar usuarios SNMPv3

Puede administrar cuentas de usuario SNMPv3 y configurar la autenticación y el cifrado.

Agregar una cuenta de usuario SNMPv3 Puede agregar una cuenta de usuario SNMPv3. Para agregar una cuenta de usuario SNMPv3:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V3 > User Configuration. Se muestra la página User Configuration.

6. En el campo User Name, escriba un nombre para la cuenta de usuario. El nombre puede tener hasta 30 caracteres.

7. En el menú SNMP v3 Access Mode, seleccione Read-Only o Read/Write para especificar los privilegios de acceso SNMPv3 de la cuenta.
Los privilegios de acceso SNMPv3 de la cuenta admin son Read/Write.

8. En el menú Authentication Protocol, seleccione SHA512 para la autenticación.
SHA512 es la única opción disponible en el menú.

9. En el menú Authentication Protocol, especifique una contraseña (clave) en el campo Authentication Key.
La contraseña puede tener hasta 32 caracteres.

10. En el menú Encryption Protocol, seleccione None o AES128 para el cifrado:

- None: la información no se cifra.
- AES128: debe especificar una contraseña de cifrado para el acceso SNMPv3 (consulte el paso siguiente).

11. Si selecciona AES128 en el menú Encryption Protocol, especifique una contraseña (clave) en el campo Encryption Key.
La contraseña puede tener hasta 32 caracteres.

12. Haga clic en el botón Add.
Se agrega la cuenta de usuario SNMPv3.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Cambiar una cuenta de usuario SNMPv3 Puede cambiar una cuenta de usuario SNMPv3 existente.
Para cambiar una cuenta de usuario SNMPv3 existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V3 > User Configuration. Se muestra la página User Configuration.

6. Seleccione la casilla junto a la cuenta de usuario SNMPv3.

7. Cambie la configuración según sea necesario.
Para más información, consulte Agregar una cuenta de usuario SNMPv3 en la página 158.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una cuenta de usuario SNMPv3 Puede eliminar una cuenta de usuario SNMPv3 que ya no necesite.
Para eliminar una cuenta de usuario SNMPv3:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > SNMP > SNMP V3 > User Configuration. Se muestra la página User Configuration.

6. Seleccione la casilla junto a la cuenta de usuario SNMPv3.

7. Haga clic en el botón Delete.
Se elimina la cuenta de usuario SNMPv3.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP), definido en IEEE 802.1AB, permite que los dispositivos de una LAN anuncien sus capacidades principales y descripciones físicas. Puede ver esta información para identificar la topología del sistema y detectar configuraciones problemáticas en la LAN.

LLDP es un protocolo unidireccional sin secuencias de solicitud y respuesta. La información la anuncian los dispositivos configurados para transmitir LLDP y la reciben y procesan los dispositivos configurados para recibir LLDP. Puede habilitar y deshabilitar la transmisión y la recepción por separado en cada puerto. De forma predeterminada, ambas funciones están deshabilitadas en todos los puertos.

Configurar los ajustes globales de LLDP

Puede especificar parámetros de LLDP que se aplican globalmente al switch.

Para configurar los ajustes globales de LLDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > Global Configuration.
Se muestra la página Global Configuration.

6. En el campo TLV Advertised Interval, introduzca el intervalo en segundos para transmitir tramas LLDP.
El rango es de 5 a 32768 s. El valor predeterminado es 30 segundos.

7. En el campo Hold Multiplier, introduzca el multiplicador del valor del campo TLV Advertised Interval, que determina el tiempo de vida (TTL) de las notificaciones LLDP. El rango es de 2 a 10 s. El valor predeterminado es 4. Por ejemplo, si el valor de TLV Advertised Interval es 30 y el valor de Hold Multiplier es 4, el TTL de las notificaciones LLDP es de 120 segundos.

8. En el campo Reinitialization Delay, introduzca el retardo antes de iniciar la reinicialización. El rango es de 1 a 10 s. El valor predeterminado es 2 segundos.

9. En el campo Notification Interval, introduzca el intervalo en segundos para la transmisión de notificaciones.
El rango es de 5 a 3600 s. El valor predeterminado es 5 segundos.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar LLDP en interfaces

Puede especificar parámetros de LLDP que se aplican a una o más interfaces.

Para configurar LLDP en interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > Interface Configuration.
Se muestra la página Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.

• Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

El campo Link Status indica si la interfaz está activa o inactiva.

7. En el menú Transmit, seleccione si la interfaz puede transmitir notificaciones LLDP. El valor predeterminado es Enable.

8. En el menú Receive, seleccione si la interfaz puede recibir notificaciones LLDP. El valor predeterminado es Enable.

9. En el menú Notify, seleccione si la interfaz admite notificaciones LLDP. El valor predeterminado es Disable.

10. Opcionalmente, configure la siguiente información Type Length Value (TLV), toda habilitada de forma predeterminada:

• Port Description: seleccione si la interfaz puede enviar una descripción del puerto en una trama LLDP.
• System Name: seleccione si la interfaz puede enviar el nombre del sistema en una trama LLDP.
• System Description: seleccione si la interfaz puede enviar la descripción del sistema en una trama LLDP.
• System Capabilities: seleccione si la interfaz puede enviar las capacidades del sistema en una trama LLDP.

11. En el menú Management Information, seleccione si la dirección de administración se transmite en las tramas LLDP.

12. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar o borrar estadísticas de LLDP

Para mostrar o borrar estadísticas de LLDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP >
Statistics. Se muestra la página Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.

7. Para borrar todas las estadísticas de LLDP, haga
clic en el botón Clear. Se borran todas las estadísticas.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 41. Información de estadísticas de LLDP

Campo	Descripción
Estadísticas LLDP Estas estadísticas son del switch.	
Last Update	Momento en que se creó, modificó o eliminó una entrada en las tablas asociadas con el sistema remoto.
Total Inserts	Número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) concreto se insertó en las tablas asociadas con los sistemas remotos.
Total Deletes	Número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) concreto se eliminó de las tablas asociadas con los sistemas remotos.
Total Drops	Número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) concreto no pudo introducirse en las tablas asociadas con los sistemas remotos por falta de recursos.
Total Ageouts	Número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) concreto se eliminó de las tablas asociadas con los sistemas remotos porque expiró el intervalo de vigencia de la información.
Estadísticas LLDP Estas estadísticas son de las interfaces.	
Interface	La interfaz.

Tabla 41. Información de estadísticas de LLDP (continuación)

Campo	Descripción
Transmit Total	Número de tramas LLDP transmitidas por el agente LLDP.
Receive Total	Número de tramas LLDP válidas recibidas por este agente LLDP.
Discards	Número de TLV LLDP descartados por cualquier motivo por el agente LLDP.
Errors	Número de tramas LLDP no válidas recibidas por el agente LLDP.
Ageouts	Número de expiraciones ocurridas. Una expiración es el número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) concreto se eliminó de las tablas asociadas con las entradas remotas porque expiró el intervalo de vigencia de la información.
TLV Discards	Número de TLV LLDP descartados por el agente LLDP.
TLV Unknowns	Número de TLV LLDP recibidos que el agente LLDP no reconoció.
TLV MED	Número total de TLV LLDP-MED recibidos.
TLV 802.1	Número total de TLV LLDP recibidos de tipo 802.1.
TLV 802.3	Número total de TLV LLDP recibidos de tipo 802.3.
TLV UPOE	Número total de TLV LLDP recibidos de tipo UPOE.
TLV NTGR	Número total de TLV LLDP recibidos de tipo NTGR.

Mostrar la información del dispositivo local LLDP

Puede mostrar la información del dispositivo local LLDP, es decir, la información que anuncia el propio switch o una de sus interfaces.

Para mostrar la información del dispositivo local LLDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > Local Device Information.
Se muestra la página Local Device Information.

6. En el menú Interface, seleccione una interfaz con la transmisión de tramas LLDP habilitada.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 42. Información del dispositivo local LLDP

Campo	Descripción
Chassis ID Subtype	El identificador del switch es la dirección MAC del switch (consulte el siguiente campo).
Chassis ID	Dirección MAC del switch.
Port ID Subtype	El identificador del puerto es la dirección MAC de la interfaz (consulte el siguiente campo).
Port ID	Dirección MAC de la interfaz del switch.
System Name	Nombre del sistema del switch, si existe.
System Description	Descripción del switch.
Port Description	Nombre de la interfaz del switch, si existe.
System Capabilities Supported	Capacidades del sistema del switch.
System Capabilities Enabled	Capacidades del sistema del switch que están habilitadas.
Management Address Type	Tipo de dirección IP de administración del switch.
Management Address	Dirección IP de administración anunciada del switch.

Mostrar la información de dispositivos remotos LLDP

Puede mostrar la información de dispositivos remotos LLDP, es decir, la información que anuncia el dispositivo conectado a una interfaz.

Para mostrar la información de dispositivos remotos LLDP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > Remote Device Information.
Se muestra la página Remote Device Information.

6. En el menú Interface, seleccione una interfaz con la recepción de tramas LLDP habilitada.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 43. Información de dispositivos remotos LLDP

Campo	Descripción
ID remoto	ID del dispositivo remoto.
ID del switch	Dirección MAC del dispositivo remoto.
Subtipo de ID del switch	El identificador del switch es la dirección MAC del dispositivo remoto (vea el campo anterior).
ID de puerto	Identificador asociado con la interfaz del dispositivo remoto.
Subtipo de ID de puerto	Tipo del identificador de puerto en el dispositivo remoto.
Nombre del sistema	Nombre del sistema del dispositivo remoto, si existe.
Descripción del sistema	Descripción del dispositivo remoto.
Descripción del puerto	Nombre de la interfaz del dispositivo remoto, si existe.
Capacidades del sistema compatibles	Capacidades del sistema compatibles con el dispositivo remoto.
Capacidades del sistema habilitadas	Capacidades del sistema habilitadas en el dispositivo remoto.
Tiempo de vida	Período de vida (TTL) en segundos de la entrada remota recibida.

Tabla 43. Información de dispositivos remotos LLDP (continuación)

Campo	Descripción
Tipo de dirección de administración	Tipo de dirección IP de administración del dispositivo remoto.
Dirección de administración	Dirección IP de administración anunciada por el dispositivo remoto.

Mostrar el inventario de dispositivos remotos LLDP

El inventario LLDP consta de los dispositivos que LLDP detecta.

Para mostrar el inventario de dispositivos remotos LLDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > LLDP > Remote Device Inventory. Se muestra la página Remote Device Inventory.

6. Para buscar una interfaz, ingrese el número de interfaz con el formato 0/x, donde x es el número de interfaz, en el campo Search Interface y haga clic en el botón Go. Se muestra la información de la interfaz.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 44. Información del inventario de dispositivos remotos LLDP

Campo	Descripción
Puerto	Interfaz del switch en la que se recibe la información LLDP.
ID del dispositivo remoto	ID del dispositivo remoto.
Dirección de administración	Dirección de administración anunciada por el dispositivo remoto.
Dirección MAC	Dirección MAC del dispositivo remoto.
Nombre del sistema	Nombre del sistema del dispositivo remoto.
ID de puerto remoto	Número de interfaz del dispositivo remoto.
OUI	Identificador único organizacional (OUI) Type-Length-Value (TLV) del dispositivo remoto.
Subtipo de OUI	Subtipo del OUI TLV del dispositivo remoto.

Link Layer Discovery Protocol para dispositivos de punto final multimedia

Link Layer Discovery Protocol for Media Endpoint Discovery (LLDP-MED) es una mejora de LLDP que admite las siguientes funciones:

- Detección automática de políticas LAN (como VLAN, prioridad de capa 2 y DiffServ), lo que permite redes plug-and-play.
- Detección de la ubicación de dispositivos, que permite crear bases de datos de ubicación.
- Administración de energía extendida y automatizada de puntos finales Power over Ethernet.
- Administración de inventario, que le permite rastrear sus dispositivos de red y conocer sus características, como fabricante, versiones de software y hardware, y números de serie o de activo.

Configurar los ajustes globales de LLDP-MED

Puede especificar ajustes de LLDP-MED que se aplican globalmente al switch.

Para configurar los ajustes globales de LLDP-MED:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > LLDP-MED > Global Configuration. Se muestra la página Global Configuration.

6. En el campo Fast Start Repeat Count, ingrese el número de PDU LLDP que se transmiten al habilitar el protocolo.
El rango es de 1 a 10. El valor predeterminado es 3.

El campo Device Class muestra la clasificación MED del switch. El switch es un dispositivo de conectividad de red.

Existen los siguientes cuatro tipos de dispositivos MED, de los cuales los tres primeros son puntos finales:

- Clase I: Dispositivos genéricos, como controladores de comunicación IP.
- Clase II: Dispositivos multimedia, como puentes de conferencia.
- Clase III: Dispositivos de comunicación, como teléfonos IP.
- Clase IV: Dispositivos de conectividad de red, como switches LAN, routers, puentes IEEE 802.1 y puntos de acceso WiFi IEEE 802.11.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de interfaz de LLDP-MED

Puede especificar ajustes de LLDP-MED que se aplican a una o más interfaces.

Para configurar los ajustes de interfaz de LLDP-MED:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > LLDP-MED > Interface Configuration. Se muestra la página Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

Los siguientes dos campos de la página no son configurables:

- El campo Link Status indica si la interfaz está activa o inactiva.
- El campo Operational Status indica si se transfieren TLV de LLDP-MED en esta interfaz.

7. En el menú MED Status, seleccione si el modo LLDP-MED está habilitado o deshabilitado en la interfaz.
El valor predeterminado es Enable.

8. En el menú Receive, seleccione si la interfaz puede recibir notificaciones LLDP.
El valor predeterminado es Enable.

9. En el menú Notification Status, seleccione si la interfaz admite notificaciones LLDP-MED.
El valor predeterminado es Disable.

10. Configure si se transmite la siguiente información Type Length Value (TLV), toda habilitada de forma predeterminada, para LLDP-MED en tramas PDU LLDP:

- MED Capabilities. Seleccione si la interfaz puede enviar las capacidades MED en una trama LLDP.

• Network Policy: Seleccione si la interfaz puede enviar la política de red en una trama LLDP.
• Location Identification: Seleccione si la interfaz puede enviar información de ubicación en una trama LLDP.
• Extended MDI-PSE: Seleccione si la interfaz puede enviar información del equipo de alimentación (PSE) en una trama LLDP.
• Inventory Information: Seleccione si la interfaz puede enviar información de inventario en una trama LLDP.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Mostrar la información del dispositivo local LLDP-MED

Puede mostrar la información del dispositivo local LLDP-MED, es decir, la información que anuncia el propio switch o una de sus interfaces.

Para mostrar la información del dispositivo local LLDP-MED:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > LLDP-MED > Local Device Information. Se muestra la página Local Device Information.

6. En el menú Interface, seleccione una interfaz con la transmisión de tramas LLDP-MED habilitada.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 45. Información del dispositivo local LLDP-MED

Campo	Descripción
Información de política de red Indica si hay un TLV de política de red en las tramas LLDP-MED transmitidas.	
Tipo de aplicación multimedia	El tipo de aplicación, que puede ser uno de los siguientes: • desconocido • señalización de voz • voz de invitado • señalización de voz de invitado • voz de softphone • videoconferencia • streaming de video • señalización de video Cada tipo de aplicación transmitido incluye el ID de VLAN, la prioridad, el DSCP, el estado del bit etiquetado y el del bit desconocido. Una interfaz puede recibir uno o varios de estos tipos de aplicación. Esta información solo se muestra si se transmite un TLV de política de red.
ID de VLAN	ID de VLAN transmitido.
Prioridad	Prioridad transmitida.
DSCP	DSCP transmitido.
Estado del bit desconocido	Estado del bit desconocido transmitido.
Estado del bit etiquetado	Estado del bit etiquetado transmitido.
Información de inventario Indica si hay un TLV de inventario en las tramas LLDP-MED transmitidas.	
Revisión de hardware	Versión de hardware transmitida.
Revisión de firmware	Versión de firmware transmitida.
Revisión de software	Versión de software transmitida.
Número de serie	Número de serie transmitido.

Tabla 45. Información del dispositivo local LLDP-MED (continuación)

Campo	Descripción
Nombre del fabricante	Nombre del fabricante transmitido.
Nombre del modelo	Nombre del modelo transmitido.
ID de activo	ID de activo transmitido.
Información de ubicación	
Indica si hay un TLV de ubicación en las tramas LLDP-MED transmitidas.	
Subtipo	Tipo de información de ubicación transmitida.
Información de ubicación	Información de ubicación transmitida.
PoE extendido	
Indica si hay información de dispositivos PoE en las tramas LLDP-MED transmitidas.	
Tipo de dispositivo	Tipo de dispositivo PoE transmitido. El switch puede suministrar PoE, por lo que es un equipo de alimentación (PSE).
Fuente de alimentación	Tipo de fuente de alimentación transmitido.
Prioridad de alimentación	Tipo de prioridad de alimentación transmitido.
Valor de potencia	Potencia en watts transmitida; es decir, se transmite la información, no la potencia real.

Mostrar la información de dispositivos remotos LLDP-MED

Puede mostrar la información de dispositivos remotos LLDP-MED, es decir, la información que anuncia el dispositivo conectado a una interfaz.

Para mostrar la información de dispositivos remotos LLDP-MED:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > LLDP > LLDP-MED > Remote Device Information. Se muestra la página Remote Device Information.

6. En el menú Interface, seleccione una interfaz con la recepción de tramas LLDP-MED habilitada.
El campo Remote ID muestra el ID asignado al dispositivo remoto.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 46. Información de dispositivos remotos LLDP-MED

Campo	Descripción
Información de capacidades	
Muestra las capacidades compatibles recibidas en las tramas LLDP-MED.	
Capacidades compatibles	Capacidades del sistema compatibles con el dispositivo remoto.
Capacidades habilitadas	Capacidades del sistema habilitadas en el dispositivo remoto.
Clase de dispositivo	Clase de dispositivo anunciada por el dispositivo remoto. La clase de dispositivo puede ser Generic, Media, Communication o Network Connectivity.
Información de políticas de red	
Muestra la información de políticas de red recibida en las tramas LLDP-MED.	

Tabla 46. Información de dispositivos remotos LLDP-MED (continuación)

Campo	Descripción
Tipo de aplicación multimedia	Tipo de aplicación del dispositivo remoto, que puede ser uno de los siguiente: • desconocido • señalización de voz • voz de invitado • señalización de voz de invitado • voz de softphone • videoconferencia • streaming de video • señalización de video Cada tipo de aplicación recibido incluye el ID de VLAN, la prioridad, el DSCP, el estado del bit etiquetado y el del bit desconocido. Una interfaz puede recibir uno o varios de estos tipos de aplicación. Esta información solo se muestra si se recibe un TLV de política de red.
ID de VLAN	ID de VLAN del dispositivo remoto.
Prioridad	Prioridad del dispositivo remoto.
DSCP	DSCP del dispositivo remoto.
Estado del bit desconocido	Estado del bit desconocido del dispositivo remoto.
Estado del bit etiquetado	Estado del bit etiquetado del dispositivo remoto.
Información de inventario Muestra la información de inventario recibida en las tramas LLDP-MED.	
Revisión de hardware	Versión de hardware del dispositivo remoto.
Revisión de firmware	Versión de firmware del dispositivo remoto.
Revisión de software	Versión de software del dispositivo remoto.
Número de serie	Número de serie del dispositivo remoto.
Nombre del fabricante	Nombre del fabricante del dispositivo remoto.
Nombre del modelo	Nombre del modelo del dispositivo remoto.

Tabla 46. Información de dispositivos remotos LLDP-MED (continuación)

Campo	Descripción
ID de activo	ID de activo del dispositivo remoto.
Información de ubicación Muestra la información de ubicación recibida en las tramas LLDP-MED.	
Subtipo	Tipo de información de ubicación del dispositivo remoto.
Información de ubicación	Información de ubicación del dispositivo remoto.
Información de ubicación Indica si hay un TLV de ubicación en las tramas LLDP-MED transmitidas.	
Subtipo	Tipo de información de ubicación del dispositivo remoto.
Información de ubicación	Información de ubicación del dispositivo remoto.
PoE extendido Indica si se recibe información de PoE extendido en las tramas LLDP-MED.	
Tipo de dispositivo	Tipo de dispositivo PoE del dispositivo remoto.
PoE PSE extendido: Indica si se recibe información de PoE PSE extendido en las tramas LLDP-MED.	
Tipo de dispositivo	Tipo de dispositivo PoE del dispositivo remoto.
Fuente de alimentación	Tipo de fuente de alimentación del dispositivo remoto.
Prioridad de alimentación	Tipo de prioridad de alimentación del dispositivo remoto.
Valor de potencia	Potencia en watts que transmite el dispositivo remoto; es decir, se transmite la información, no la potencia real.
PoE PD extendido: Indica si se recibe información de PoE PD extendido en las tramas LLDP-MED.	
Tipo de dispositivo	Tipo de dispositivo PoE del dispositivo remoto.
Fuente de alimentación	Tipo de fuente de alimentación del dispositivo remoto.

Tabla 46. Información de dispositivos remotos LLDP-MED (continuación)

Campo	Descripción
Prioridad de alimentación	Tipo de prioridad de alimentación del dispositivo remoto.
Valor de potencia	Potencia en watts que transmite el dispositivo remoto; es decir, se transmite la información, no la potencia real.

Mostrar el inventario de dispositivos remotos LLDP-MED

El inventario LLDP consta de los dispositivos que LLDP detecta y que admiten MED.

Para mostrar el inventario de dispositivos remotos LLDP-MED:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > LLDP > LLDP-MED > Remote Device Inventory. Se muestra la página Remote Device Inventory.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 47. Información del inventario de dispositivos remotos LLDP-MED

Campo	Descripción
Puerto	Interfaz del switch en la que se recibe la información LLDP-MED.
Dirección de administración	Dirección de administración anunciada por el dispositivo remoto.
Dirección MAC	Dirección MAC del dispositivo remoto.

Tabla 47. Información del inventario de dispositivos remotos LLDP-MED (continuación)

Campo	Descripción
Nombre del sistema	Nombre del sistema del dispositivo remoto.
ID de puerto remoto	Número de interfaz del dispositivo remoto.

Dependencia de enlace

La dependencia de enlace le permite habilitar o deshabilitar una o más interfaces según el estado de enlace de otras interfaces. Es decir, si habilita la dependencia de enlace en una interfaz, el estado de enlace de esa interfaz depende del estado de enlace de otra interfaz. Por ejemplo, si el puerto 0/2 depende del puerto 0/4 y el switch detecta una pérdida de enlace en el puerto 0/4, el switch puede desactivar automáticamente el enlace del puerto 0/2. Cuando se restablece el enlace del puerto 0/4, el switch puede restablecer automáticamente el del puerto 0/2.

También es posible lo contrario: si el puerto 0/2 depende del puerto 0/4 y el switch detecta una pérdida de enlace en el puerto 0/4, el switch puede activar automáticamente el enlace del puerto 0/2. Cuando se restablece el enlace del puerto 0/4, el switch puede desactivar automáticamente el enlace del puerto 0/2.

Configurar un grupo de dependencia de enlace

Un grupo de dependencia de enlace incluye una lista de interfaces ascendentes, una lista de interfaces descendentes y una acción configurada para el grupo. Si todas las interfaces ascendentes de la lista se desactivan, todas las interfaces descendentes se desactivan o se activan, según la acción que configure para el grupo de dependencia de enlace.

Después de configurar el grupo de dependencia de enlace, configure sus interfaces ascendentes y descendentes (vea Configurar o mostrar las interfaces ascendentes y descendentes de un grupo de dependencia de enlace en la página 180).

Para configurar un grupo de dependencia de enlace:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > Link Dependency > Link Dependency Group Configuration. Se muestra la página Link Dependency Group Configuration.

6. Marque una o más casillas de ID de grupo. El switch admite 16 ID de grupo.

Nota: Los ID de grupo no están asociados con los números de interfaz.

7. En el menú Link Action, especifique la acción que debe ocurrir en las interfaces descendentes del grupo cuando todas las interfaces ascendentes del grupo están inactivas:

- Link Down: Cuando todas las interfaces ascendentes del grupo están inactivas, todas las descendentes también se desactivan. Cuando cualquiera de las interfaces ascendentes está activa, todas las descendentes también se activan.
- Link Up: Cuando todas las interfaces ascendentes del grupo están inactivas, todas las descendentes se activan. Cuando cualquiera de las interfaces ascendentes está activa, todas las descendentes se desactivan.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar o mostrar las interfaces ascendentes y descendentes de un grupo de dependencia de enlace

En un grupo de dependencia de enlace, si agrega interfaces descendentes, estas se desactivan hasta que agregue una o más interfaces ascendentes al grupo. Después, el estado de enlace de las descendentes depende del estado de enlace de las ascendentes y de la acción configurada para el grupo. Le recomendamos configurar primero las interfaces ascendentes y después las descendentes.

En un grupo de dependencia de enlace, una interfaz puede ser miembro de la lista ascendente o de la descendente, pero no de ambas.

Para configurar o mostrar las interfaces ascendentes y descendentes de un grupo de dependencia de enlace:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Link Dependency > Link Dependency Interface Configuration. Se muestra la página Link Dependency Interface Configuration.

6. En la sección Link Dependency Group ID, en el menú Group ID, seleccione el ID de grupo cuya configuración desea mostrar o configurar.

Nota: Los ID de grupo no están asociados con los números de interfaz.

7. En la sección Link Dependency Interface Configuration, seleccione si desea mostrar interfaces físicas, LAG o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

8. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

9. En el menú Downstream Interface, seleccione si la interfaz es miembro de la lista descendente del grupo.

• False: La interfaz no es miembro de la lista descendente del grupo. Es la configuración predeterminada.
• True: La interfaz es miembro de la lista descendente del grupo.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. En el menú Upstream Interface, seleccione si la interfaz es miembro de la lista ascendente del grupo.

• False. La interfaz no es miembro de la lista ascendente del grupo. Es la configuración predeterminada.
• True: La interfaz es miembro de la lista ascendente del grupo.

12. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

El campo Link Status indica si el enlace de la interfaz o LAG correspondiente está activo o inactivo.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

14. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables que se muestran en la sección Link Dependency Group Statistic.

Tabla 48. Información estadística del grupo de dependencia de enlace

Campo	Descripción
ID de grupo	ID del grupo. El rango es de 1 a 16.
Acción de enlace	Acción que se realiza en las interfaces descendentes cuando todas las interfaces de la lista ascendente se desactivan.
Estado del grupo	Estado actual del grupo.
Transiciones del grupo	Número de transiciones del grupo.
Hora de la última transición	Hora de la última transición del grupo.

Borrar todas las interfaces de un grupo de dependencia de enlace

Puede borrar todas las interfaces de un grupo de dependencia de enlace. Después, las listas ascendente y descendente del grupo no incluyen ninguna interfaz.

Para borrar todas las interfaces de un grupo de dependencia de enlace:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > Link Dependency > Link Dependency Interface Configuration. Se muestra la página Link Dependency Interface Configuration.

6. En la sección Link Dependency Group ID, en el menú Group ID, seleccione el ID de grupo cuya configuración desea mostrar o configurar.
El rango del ID de grupo es de 1 a 16.

Nota: Los ID de grupo no están asociados con los números de interfaz.

7. Haga clic en el botón Clear.
Las interfaces se eliminan del grupo.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Industry Standard Discovery Protocol

Industry Standard Discovery Protocol (ISDP) es un protocolo que permite a los dispositivos compartir información en una red.

Puede configurar los ajustes globales y de interfaz de ISDP.

Configurar los ajustes globales de ISDP

Puede configurar los ajustes de ISDP que se aplican globalmente al switch.

Para configurar los ajustes globales de ISDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > ISDP > Basic > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción Admin mode Disable o Enable para especificar si el servicio ISDP está deshabilitado o habilitado.
El valor predeterminado es Enabled.

7. En el campo Timer, especifique el período en segundos entre transmisiones de paquetes ISDP.
El rango es de 5 a 254 segundos. El valor predeterminado es 30 segundos.

8. En el campo Hold Time, especifique el tiempo de retención de los paquetes ISDP que transmite el switch. El tiempo de retención indica cuánto tiempo debe guardar un dispositivo receptor la información del paquete ISDP antes de descartarla. El rango es de 10 a 255 segundos. El valor predeterminado es 180 segundos.

9. Seleccione el botón de opción Version 2 Advertisements Disable o Enable para especificar si el switch puede enviar paquetes ISDPv2.
El valor predeterminado es Enabled.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 49. Información de configuración global de ISDP

Campo	Descripción
Último cambio de la tabla de vecinos	Hora en que cambió la información de la tabla de vecinos.
ID de dispositivo	ID de dispositivo de este switch.
Capacidad de formato de ID de dispositivo	Capacidad de formato del ID de dispositivo.
Formato de ID de dispositivo	Formato del ID de dispositivo.

Configurar los ajustes de ISDP de una interfaz

Puede configurar si una interfaz puede comunicar paquetes ISDP.

Para configurar los ajustes de ISDP de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > ISDP > Advanced > Interface Configuration. Se muestra la página Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

7. En el menú Admin mode, seleccione Enable o Disable para especificar si la interfaz puede comunicar información ISDP.
El valor predeterminado es Enable.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar o borrar la información de vecinos ISDP

Puede ver o borrar la información sobre los vecinos ISDP.

Para mostrar o borrar la información de vecinos ISDP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > ISDP > Advanced > Neighbor. Se muestra la página Neighbor.

6. Para buscar un vecino, en el menú Search, seleccione Device ID o Interface, y en el campo, ingrese el ID de dispositivo o el número de interfaz.

7. Para actualizar la página, haga clic en el botón Refresh.

8. Para borrar la información de vecinos ISDP, haga clic en el botón Borrar (Clear). Se borra toda la información de la página.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 50. Información de vecinos ISDP

Campo	Descripción
Device ID	El ID de dispositivo del vecino ISDP.
Interface	La interfaz en la que se descubre el vecino.
Address	La dirección IP del vecino.
Capability	La capacidad del vecino, que puede ser una de las siguientes: • Router • Trans Bridge • Source Route • Switch • Host • IGMP • Repeater
Platform	El tipo de modelo del vecino.
Port ID	El ID de puerto en el vecino.
Hold Time	El tiempo de retención de los paquetes ISDP que transmite el vecino.
Advertisement Version	La versión de ISDP que envía el vecino.
Entry Last Changed Time	El tiempo transcurrido desde el último cambio de la entrada.
Software Version	La versión de software del vecino.

Mostrar o borrar las estadísticas de ISDP

Puede mostrar o borrar las estadísticas de ISDP.

Para mostrar o borrar las estadísticas de ISDP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > ISDP > Advanced > Statistics. Se muestra la página Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.

7. Para borrar las estadísticas de ISDP, haga clic en el botón Borrar (Clear). Se borran las estadísticas.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 51. Información de estadísticas de ISDP

Campo	Descripción
ISDP Packets Received	Los paquetes ISDPv2 e ISDPv3 recibidos en el switch.
ISDP Packets Transmitted	Los paquetes ISDPv2 e ISDPv3 transmitidos en el switch.
ISDPv1 Packets Received	Los paquetes ISDPv1 recibidos en el switch.
ISDPv1 Packets Transmitted	Los paquetes ISDPv1 transmitidos en el switch.
ISDPv2 Packets Received	Los paquetes ISDPv2 recibidos en el switch.
ISDPv2 Packets Transmitted	Los paquetes ISDPv2 transmitidos en el switch.
ISDP Bad Header	Los paquetes ISDP con encabezados incorrectos recibidos en el switch.
ISDP Checksum Error	Los paquetes ISDP con errores de suma de verificación recibidos en el switch.
ISDP Transmission Failure	El número de paquetes ISDP que el switch no pudo transmitir.
ISDP Invalid Format	El número de paquetes ISDP con formato no válido que recibió el switch.
ISDP Table Full	El tamaño de la tabla ISDP.
ISDP IP Address Table Full	El tamaño de la tabla de direcciones IP de ISDP.

3

Configurar la información de conmutación

Este capítulo trata los siguientes temas:

- VLAN
- Auto-VoIP
- Spanning Tree Protocol
- Base de datos de reenvío multicast
- IGMP snooping (Internet Group Management Protocol)
- MLD snooping (Multicast Listener Discovery)
- Registro de VLAN multicast
- Tabla de direcciones MAC
- Configuración de puertos
- Grupos de agregación de enlaces
- Temporización y sincronización 802.1AS
- Multiple Registration Protocol y configuración de 802.1Qav
- Protección contra bucles

VLAN

Agregar compatibilidad con LAN virtuales (VLAN) a un switch de capa 2 ofrece algunas de las ventajas tanto del puenteo como del enrutamiento. Como un puente, un switch con VLAN reenvía el tráfico según el encabezado de capa 2, lo cual es rápido, y como un router, divide la red en segmentos lógicos, lo que mejora la administración, la seguridad y la gestión del tráfico multicast.

De forma predeterminada, todos los puertos del switch están en el mismo dominio de broadcast. Las VLAN separan electrónicamente los puertos de un mismo switch en dominios de broadcast distintos, para que los paquetes de broadcast no se envíen a todos los puertos de un switch. Al usar una VLAN, los usuarios pueden agruparse por función lógica en lugar de por ubicación física.

A cada VLAN de una red se le asigna un ID de VLAN, que aparece en la etiqueta IEEE 802.1Q del encabezado de capa 2 de los paquetes transmitidos en una VLAN. Una estación final puede omitir la etiqueta, o la parte de VLAN de la etiqueta; en ese caso, el primer puerto del switch que reciba el paquete puede rechazarlo o insertar una etiqueta con su ID de VLAN predeterminado. Un puerto puede manejar tráfico de más de una VLAN, pero solo admite un ID de VLAN predeterminado.

Puede definir grupos de VLAN almacenados en la tabla de membresía de VLAN. Cada switch admite hasta 1024 VLAN. La VLAN 1 se crea de forma predeterminada y es la VLAN predeterminada de la que todos los puertos son miembros.

Administrar la configuración de VLAN del switch

Puede agregar, cambiar y eliminar VLAN, o restablecer toda la configuración de VLAN del switch a los valores predeterminados.

Agregar una VLAN Puede agregar varias VLAN para adaptar el switch a su red. Una VLAN interna está reservada por una interfaz de enrutamiento basada en puerto y es invisible para el usuario final. Después de que la interfaz de enrutamiento basada en puerto asigna una VLAN interna, esa VLAN no se puede asignar a una interfaz VLAN de enrutamiento.

Para agregar una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Basic > VLAN Configuration. Se muestra la página VLAN Configuration.

6. En la sección VLAN Configuration, especifique la configuración de la nueva VLAN:

• VLAN ID: Especifique el identificador de la nueva VLAN. El ID de VLAN puede ir de 1 a 4093.
• VLAN Name: Escriba un nombre para la nueva VLAN. El nombre puede tener hasta 32 caracteres, incluidos espacios. De forma predeterminada, el nombre de la VLAN ID 1 es Default.

Nota: Cuando agrega una VLAN manualmente (como en este procedimiento), el campo VLAN Type siempre muestra Static. Una VLAN creada por registro GVRP usa inicialmente el tipo dinámico, pero puede cambiarlo a estático (consulte Cambiar una VLAN en la página 191). El tipo de la VLAN predeterminada (VLAN ID 1) siempre es Default.

7. Haga clic en el botón Agregar (Add). Se agrega la VLAN.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar una VLAN Puede cambiar el nombre de una VLAN agregada estática o dinámicamente. En una VLAN agregada dinámicamente (por ejemplo, una VLAN creada por registro GVRP), puede cambiar el tipo de VLAN a estático.
Para cambiar una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Basic > VLAN Configuration.

Se muestra la página VLAN Configuration.

6. En la sección VLAN Configuration, active la casilla del ID de VLAN.

7. Para cambiar el nombre de la VLAN, en el campo VLAN Name, escriba un nombre nuevo. El nombre puede tener hasta 32 caracteres, incluidos espacios.

8. Para cambiar el tipo de VLAN de dinámico a estático, en el menú Make Static, seleccione Enable.
Una VLAN creada por registro GVRP usa inicialmente el tipo dinámico, pero puede cambiarlo a estático. No puede cambiar el tipo de una VLAN que agregó manualmente. El tipo de la VLAN predeterminada (VLAN ID 1) siempre es Default.

9. Haga clic en el botón Aplicar
(Apply). Se guardan los cambios.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una o más VLAN Puede eliminar una o más VLAN que ya no necesite. No puede eliminar la VLAN predeterminada (VLAN 1).
Para eliminar una o más VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Basic > VLAN Configuration. Se muestra la página VLAN Configuration.

6. En la sección VLAN Configuration, active las casillas de los ID de VLAN.

7. Haga clic en el botón Eliminar
(Delete). Se eliminan las VLAN.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Restablecer toda la configuración de VLAN a los valores predeterminados Puede restablecer toda la configuración de VLAN del switch a los valores de fábrica, con excepción de la VLAN predeterminada (VLAN 1). Los valores de fábrica son los siguientes:

- Todos los puertos se asignan a la VLAN predeterminada 1.
- Todos los puertos se configuran con un PVID de 1.
- Todos los puertos se configuran con “Acceptable Frame Types” en el valor “Admit All Frames”.
- Todos los puertos se configuran con el filtrado de entrada deshabilitado.
- Todos los puertos se configuran para transmitir solo tramas sin etiqueta.
- GVRP se deshabilita en todos los puertos y se borran todas las entradas dinámicas.

Para restablecer toda la configuración de VLAN a los valores predeterminados:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > VLAN Configuration. Se muestra la página VLAN Configuration.

6. Active la casilla Reset Configuration. Se muestra una ventana de confirmación.

ADVERTENCIA: Si selecciona este botón y confirma su selección, toda la configuración de VLAN del switch se restablece a los valores de fábrica.

7. Haga clic en el botón OK.
Se eliminan todas las VLAN, excepto la VLAN predeterminada.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar la configuración de asignación de VLAN internas En la mayoría de los casos, no necesita cambiar la configuración de asignación de VLAN internas.

Para cambiar la configuración de asignación de VLAN internas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Basic > VLAN Configuration. Se muestra la página VLAN Configuration.

6. En el campo Internal VLAN Allocation Base, especifique la base de asignación de VLAN para la interfaz de enrutamiento.
El rango base predeterminado de la VLAN interna es de 1 a 4093.

7. Seleccione el botón de opción Ascending o Descending de Internal VLAN Allocation Policy para especificar la política de asignación de VLAN internas:

- Ascending: Las VLAN se asignan en orden ascendente de 2 a 4093.
- Descending: Las VLAN se asignan en orden descendente de 4093 a 2.

La VLAN 1 es la VLAN predeterminada.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Descripción general de Auto-Trunk

Auto-Trunk es una función que permite al switch habilitar automáticamente el modo Trunk en enlaces físicos e interfaces LAG compatibles entre dispositivos asociados. Una troncal puede transportar todas las VLAN activas. De forma predeterminada, la función Auto-Trunk está habilitada en el switch.

Si el switch configura automáticamente un puerto como troncal (es decir, un Auto-Trunk), todas las VLAN del switch pasan a formar parte de la troncal, lo que permite la configuración automática de todas las VLAN en el switch y en el dispositivo asociado con el que se establece la troncal.

Antes de configurar un Auto-Trunk, el switch primero detecta los enlaces físicos con el dispositivo asociado que también admite la función Auto-Trunk y, después, configura automáticamente los puertos que están conectados y que pueden formar una troncal en ambos extremos.

Una troncal transporta varias VLAN y acepta paquetes etiquetados y sin etiquetar. Normalmente, una conexión entre el switch y un dispositivo asociado, como un router, un punto de acceso o otro switch, funciona como troncal.

Para que el switch forme un Auto-Trunk con un dispositivo asociado, se requiere lo siguiente:

- La función Auto-Trunk debe ser compatible y estar habilitada globalmente en el switch y en el dispositivo asociado. (En todos los modelos de switch M4250, la función Auto-Trunk está habilitada de forma predeterminada).
- Los puertos interconectados del switch y del dispositivo asociado deben estar habilitados. (En todos los modelos de switch M4250, todos los puertos están habilitados de forma predeterminada).
- LLDP debe estar habilitado en los puertos interconectados del switch y del dispositivo asociado. (En todos los modelos M4250, LLDP está habilitado de forma predeterminada en todos los puertos).
- Los puertos interconectados del switch y del dispositivo asociado deben estar en el modo de puerto predeterminado del switch, que es el modo General. Si los puertos están en modo Access o ya están en modo Trunk, no se puede formar un Auto-Trunk en un Auto-LAG.

En un Auto-Trunk, el PVID se establece automáticamente en la VLAN de administración. Si desea cambiar el PVID de un Auto-Trunk, cambie la VLAN de administración.

La función Auto-Trunk funciona junto con la función Auto-LAG (consulte Descripción general de Auto-LAG en la página 302). Después de formarse un Auto-LAG, el switch aplica automáticamente el modo trunk (es decir, un Auto-Trunk) al LAG en ambos extremos. Es decir, después de formarse un Auto-LAG, el modo de los puertos que participan en él cambia automáticamente del modo de puerto de switch predeterminado al modo trunk, y el Auto-LAG se convierte en un Auto-Trunk.

Después de que un puerto o un Auto-LAG se convierte en Auto-Trunk, todas las VLAN del switch pasan a formar parte de la troncal, y todas las VLAN del switch y del dispositivo asociado pueden configurarse automáticamente.

Habilitar o deshabilitar Auto-Trunks

De forma predeterminada, la función Auto-Trunk está habilitada globalmente, pero puede deshabilitarla globalmente.

Para habilitar o deshabilitar Auto-Trunks:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching> VLAN > Advanced > VLAN Trunking Configuration. Se muestra la página VLAN Trunking Configuration.

6. En la sección Global Auto-Trunk Mode, seleccione el botón de opción Enable o Disable de Admin Mode.
De forma predeterminada, la función Auto-Trunk está habilitada globalmente.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el modo de puerto de switch de las interfaces

Puede configurar el modo de puerto de switch en las interfaces. El modo de puerto de switch define la función del puerto según el tipo de dispositivo al que se conecta y restringe en consecuencia la configuración de VLAN del puerto. Asignar el modo de puerto de switch adecuado ayuda a simplificar la configuración de VLAN y a minimizar errores.

El switch admite los siguientes tipos de puertos de switch:

- Access: Este modo es para puertos conectados a dispositivos finales. Los puertos de acceso participan en una sola VLAN. Aceptan paquetes con y sin etiqueta, pero siempre transmiten paquetes sin etiqueta.
- General: Este modo permite una configuración personalizada del puerto. Puede configurar los atributos de VLAN del puerto general, como la membresía (consulte Configurar las interfaces miembro de una VLAN en la página 199) y el PVID, el etiquetado, el filtro de entrada, etc. (consulte Cambiar la configuración del ID de VLAN de puerto en la página 202). De forma predeterminada, todos los puertos se configuran inicialmente en modo general.
- Trunk: Este modo es para puertos conectados a otros switches o a un router. Un puerto trunk puede participar en varias VLAN y aceptar paquetes con y sin etiqueta.

En el siguiente procedimiento, los puertos se denominan interfaces.

Para configurar el modo de puerto de switch de las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > VLAN Trunking Configuration. Se muestra la página VLAN Trunking Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Switch port Mode, seleccione una de las siguientes opciones:

- Access: Seleccione este modo si la interfaz está conectada a dispositivos finales. Las interfaces de acceso participan en una sola VLAN. Aceptan paquetes con y sin etiqueta, pero siempre transmiten paquetes sin etiqueta.
- General: Seleccione este modo para poder configurar la interfaz. Puede configurar los atributos de VLAN del puerto general, como la membresía (consulte Configurar las interfaces miembro de una VLAN en la página 199) y el PVID, el etiquetado, el filtro de entrada, etc. (consulte Cambiar la configuración del ID de VLAN de puerto en la página 202). Esta es la selección predeterminada.

• Trunk: Seleccione este modo si la interfaz está conectada a otro switch o a un router. Una interfaz trunk puede participar en varias VLAN y aceptar paquetes con y sin etiqueta.

9. Según su selección en el paso anterior, haga lo siguiente:

• Access: Si seleccionó Access en el menú Switch port Mode, en el menú Access VLAN ID, seleccione la VLAN de acceso de la interfaz.
• Trunk: Si seleccionó Trunk en el menú Switch port Mode, haga lo siguiente:

a. En el menú Native VLAN ID, seleccione la VLAN nativa de la interfaz. b. En el campo Trunk Allowed VLANs, introduzca las VLAN de las que la interfaz puede

ser miembro cuando su modo de puerto de switch es Trunk. De forma predeterminada, el campo incluye todas las VLAN, aunque aún no estén creadas. Los ID de VLAN van de 1 a 4093. Use un guion (-) para especificar un rango de VLAN o una coma (,) para separar los ID de VLAN de una lista. No se permiten espacios. Un valor cero borra las VLAN permitidas. Si introduce All, se incluyen todas las VLAN de 1 a 4093.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Campo	Definición
Native VLAN Tagging	Muestra si el etiquetado de VLAN está habilitado: • Disable: Cuando el etiquetado de VLAN está habilitado, si el puerto trunk recibe tramas sin etiqueta, las reenvía en la VLAN nativa sin etiqueta de VLAN. • Enable: Cuando el etiquetado de VLAN está deshabilitado, si el puerto trunk recibe tramas sin etiqueta, incluye el ID de la VLAN nativa en la etiqueta de VLAN al reenviarlas.
Auto-Trunk Operational Status	Muestra si Auto-Trunk está configurado en la interfaz: • Disable: Auto-Trunk no está configurado en la interfaz. • Enable: Auto-Trunk está configurado en la interfaz.
Auto-Trunk Member VLAN List	Las VLAN que son miembros del Auto-Trunk, si hay un Auto-Trunk configurado en la interfaz.

Configurar las interfaces miembro de una VLAN

Para configurar las interfaces miembro de una VLAN:

1. Abra un navegador web.

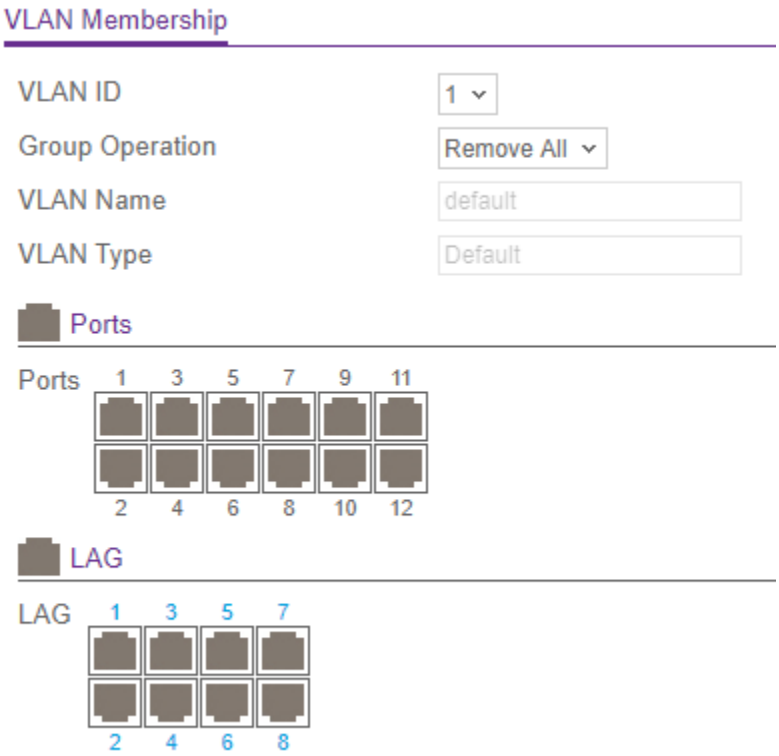
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > VLAN Membership.



La figura anterior muestra la página de un modelo de 12 puertos. Según su modelo de switch, el ícono Ports (sobre la tabla Ports) puede aparecer como el ícono Unit 1.

6. En el menú VLAN ID, seleccione el ID de VLAN.

7. Para agregar o quitar todos los puertos y LAG a la vez (también puede seleccionarlos individualmente), seleccione una de las siguientes opciones en el menú Group Operation:

- Untag All: Todos los puertos y LAG se agregan como miembros sin etiqueta de la VLAN.
- Tag All: Todos los puertos y LAG se agregan como miembros con etiqueta de la VLAN.
- Remove All: Todos los puertos y LAG se excluyen de la VLAN.

8. En la tabla Ports, haga clic en un puerto una, dos o tres veces para configurar uno de los siguientes modos:

- Miembro T (con etiqueta): El puerto se agrega como miembro con etiqueta de la VLAN.
- Miembro U (sin etiqueta): El puerto se agrega como miembro sin etiqueta de la VLAN.
- Miembro excluido: De forma predeterminada, la selección está en blanco, lo que significa que el puerto está excluido de la VLAN. Un puerto excluido aún puede agregarse dinámicamente a la VLAN mediante GVRP.

9. En la tabla LAG, haga clic en un LAG una, dos o tres veces para configurar uno de los siguientes modos:

- Miembro T (con etiqueta): El LAG se agrega como miembro con etiqueta de la VLAN.
- Miembro U (sin etiqueta): El LAG se agrega como miembro sin etiqueta de la VLAN.
- Miembro excluido: De forma predeterminada, la selección está en blanco, lo que significa que el LAG está excluido de la VLAN. Un LAG excluido aún puede agregarse dinámicamente a la VLAN mediante GVRP.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 52. Membresía de VLAN avanzada

Campo	Definición
VLAN Name	El nombre de la VLAN.
VLAN Type	El tipo de la VLAN seleccionada: • Default (VLAN ID = 1): Siempre presente. • Static: Una VLAN que agregó manualmente. • Dynamic: Una VLAN creada mediante registro GVRP que no convirtió a estática y que, por lo tanto, GVRP puede eliminar.

Ver el estado de las VLAN del switch

Puede ver el estado de todas las VLAN configuradas.

Para ver el estado de las VLAN del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login. La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > VLAN Status. Se muestra la página VLAN Status.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 53. Estado de VLAN

Campo	Definición
VLAN ID	El identificador (VID) de la VLAN. El ID de VLAN va de 1 a 4093.
VLAN Name	El nombre de la VLAN. La VLAN ID 1 siempre se llama Default.
VLAN Type	El tipo de la VLAN seleccionada: • Default (VLAN ID = 1): Siempre presente. • Static: Una VLAN que agregó manualmente. • Dynamic: Una VLAN creada mediante registro GVRP que no convirtió a estática y que, por lo tanto, GVRP puede eliminar.
Routing Interface	La interfaz asociada a la VLAN, si el enrutamiento VLAN está configurado para esta VLAN.
Member Ports	Las interfaces y LAG que son miembros de la VLAN.

Cambiar la configuración del ID de VLAN de puerto

De forma predeterminada, a cada interfaz se le asigna un ID de VLAN de puerto (PVID) de 1 porque está asociada a la VLAN predeterminada, VLAN ID 1.

Si desea cambiar el PVID de una interfaz, la interfaz debe ser miembro de al menos otra VLAN además de la VLAN predeterminada.

Además del PVID, puede configurar otros ajustes relacionados con el PVID.

Para configurar el PVID y los ajustes relacionados:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Port PVID Configuration. Se muestra la página Port PVID Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el campo PVID, especifique el ID de VLAN que se asignará a las tramas sin etiqueta o con etiqueta de prioridad recibidas en esta interfaz.
El valor predeterminado es 1.

9. En el campo VLAN Member, especifique el ID de VLAN o la lista de VLAN de una interfaz miembro.
Los ID de VLAN van de 1 a 4093. El valor predeterminado es 1. Use un guion (-) para especificar un rango o una coma (,) para separar los ID de VLAN de una lista. No se permiten espacios ni ceros.

10. En el campo VLAN Tag, especifique el ID de VLAN o la lista de VLAN de una interfaz con etiqueta. Los ID de VLAN van de 1 a 4093. Use un guion (-) para especificar un rango o una coma (,) para separar los ID de VLAN de una lista. No se permiten espacios ni ceros. Para restablecer la configuración de etiquetas de VLAN a los valores predeterminados, use la palabra clave None. El etiquetado de puerto de la VLAN solo se puede establecer si la interfaz es miembro de esta VLAN.

11. En el menú Acceptable Frame Types, seleccione los tipos de tramas que se pueden recibir en la interfaz:

• VLAN only: Se descartan las tramas sin etiqueta y con etiqueta de prioridad recibidas en la interfaz. Las tramas con etiqueta de VLAN se reenvían de acuerdo con la especificación VLAN 802.1Q.
• Admit All: Se aceptan las tramas sin etiqueta y con etiqueta de prioridad recibidas en la interfaz y se les asigna el ID de VLAN de puerto de la interfaz. Las tramas con etiqueta de VLAN se reenvían de acuerdo con la especificación VLAN 802.1Q.
• Admit Untagged Only: Se aceptan las tramas sin etiqueta recibidas en la interfaz. Las tramas con etiqueta de VLAN se reenvían de acuerdo con la especificación VLAN 802.1Q.

12. En el menú Ingress Filtering, seleccione una de las siguientes opciones:

• Enabled: La trama se descarta si la interfaz no es miembro de la VLAN a la que está asociada la trama. En una trama con etiqueta, la VLAN se identifica por el ID de VLAN de la etiqueta. En una trama sin etiqueta, la VLAN es el ID de VLAN de puerto de la interfaz que recibe la trama.
• Disabled: Todas las tramas se reenvían de acuerdo con la especificación de puente VLAN 802.1Q. El valor predeterminado es Disabled.

13. En el campo Port Priority, especifique la prioridad 802.1p predeterminada asignada a los paquetes sin etiqueta que llegan al puerto.
Puede introducir un número de 0 a 7.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 54. Información de configuración de PVID

Campo	Descripción
Current Ingress Filtering	Indica si el filtrado de entrada está habilitado en la interfaz.
Untagged VLANs	El número de VLAN sin etiqueta de las que la interfaz es miembro.
Tagged VLANs	El número de VLAN con etiqueta de las que la interfaz es miembro.

Tabla 54. Información de configuración de PVID (continuación)

Campo	Descripción
Forbidden VLANs	El número de VLAN prohibidas de las que la interfaz es miembro.
Dynamic VLANs	El número de VLAN agregadas dinámicamente de las que la interfaz es miembro.

Configurar una VLAN basada en MAC

Una VLAN basada en MAC permite asignar los paquetes entrantes sin etiqueta a una VLAN y clasificar el tráfico según la dirección MAC de origen del paquete.

Para definir una asignación de MAC a VLAN, configure una entrada en la tabla MAC-to-VLAN. Una entrada se define por su dirección MAC de origen y un ID de VLAN. Las configuraciones MAC-to-VLAN se comparten en todas las interfaces (es decir, hay una tabla para todo el sistema con asignaciones de dirección MAC a ID de VLAN).

Cuando llegan al switch paquetes sin etiquetar o con etiqueta de prioridad y existen entradas en la tabla MAC-to-VLAN, el switch intenta encontrar la dirección MAC de origen del paquete: Si el switch encuentra una entrada, se asigna al paquete el ID de VLAN correspondiente. Si el paquete ya tiene etiqueta de prioridad, conserva este valor; de lo contrario, la prioridad se establece en cero. El ID de VLAN asignado se verifica con la tabla de VLAN: si la VLAN es válida, continúa el procesamiento de entrada del paquete; de lo contrario, el paquete se descarta. Esto implica que puede configurar manualmente una asignación de dirección MAC a ID de VLAN.

Agregar una configuración de VLAN basada en MAC Para agregar una configuración de VLAN basada en MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > MAC Based VLAN. Se muestra la página MAC Based VLAN.

6. En el campo MAC Address, escriba una dirección MAC que debe vincularse a un ID de VLAN.

7. En el campo VLAN ID, especifique el ID de VLAN en el rango de 1 a 4093.

8. Haga clic en el botón Add.
Se agrega la configuración de VLAN basada en MAC.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una configuración de VLAN basada en MAC Para eliminar una configuración de VLAN basada en MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > MAC Based VLAN. Se muestra la página MAC Based VLAN.

6. Marque la casilla de la configuración de VLAN basada en MAC

7. Haga clic en el botón Delete.
Se elimina la configuración de VLAN basada en MAC.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar un grupo de VLAN basada en protocolo

Puede usar una VLAN basada en protocolo para definir criterios de filtrado para paquetes sin etiquetar. De forma predeterminada, si no configura una VLAN basada en puerto (IEEE 802.1Q) o basada en protocolo, los paquetes sin etiquetar se asignan a la VLAN 1. Puede anular este comportamiento definiendo VLAN basadas en puerto, VLAN basadas en protocolo, o ambas. Los paquetes etiquetados siempre se manejan según el estándar IEEE 802.1Q y no se incluyen en las VLAN basadas en protocolo.

Si asigna una interfaz a una VLAN basada en protocolo para un protocolo específico, a las tramas sin etiquetar recibidas en la interfaz para ese protocolo se les asigna el ID de la VLAN basada en protocolo. A las tramas sin etiquetar recibidas en la interfaz para otros protocolos se les asigna el Port

VLAN ID, ya sea el PVID predeterminado (1) o un PVID asignado específicamente a la interfaz (consulte Cambiar la configuración del ID de VLAN del puerto en la página 202).

Una VLAN basada en protocolo se define creando un grupo. Cada grupo tiene una relación uno a uno con un ID de VLAN, puede incluir de una a tres definiciones de protocolo y puede incluir varias interfaces. Cuando crea un grupo, especifica un nombre. El ID de grupo se asigna automáticamente.

Agregar un grupo de VLAN basada en protocolo Puede agregar un grupo de VLAN basada en protocolo. Para agregar un grupo de VLAN basada en protocolo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.
Se muestra la página Protocol Based VLAN Group Configuration.

6. En el campo Group ID, especifique un ID numérico.
Puede ingresar un ID en el rango de 1 a 128.

7. En el campo Group Name, especifique un nombre para el nuevo grupo. Puede ingresar hasta 16 caracteres.

8. En el campo Protocol, especifique uno o más de los siguientes protocolos que se asociarán con el grupo:

- IP: IP es un protocolo de capa de red que ofrece un servicio sin conexión para la entrega de datos.
- ARP: Address Resolution Protocol (ARP) es un protocolo de bajo nivel que asigna dinámicamente direcciones de capa de red a direcciones físicas de control de acceso al medio (MAC).
- IPX: Internetwork Packet Exchange (IPX) es un protocolo de datagramas sin conexión de capa de red que reenvía datos a través de una red.

Separe los protocolos con una coma (,). Por ejemplo, para especificar los tres protocolos, ingrese lo siguiente: ip,arp,ipx

También puede ingresar valores hexadecimales o decimales en el rango de 0x0600(1536) a 0xFFFF(65535).

9. En el campo VLAN ID, especifique el ID de VLAN.
El ID debe ser un número en el rango de 1 a 4093. Una interfaz del grupo asigna este ID de VLAN a los paquetes sin etiquetar que recibe para los protocolos que incluya en este grupo.

10. Haga clic en el botón Add.
Se agrega el grupo de VLAN basada en protocolo.

El campo Ports muestra los puertos de interfaz que pertenecen al grupo.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Cambiar un grupo de VLAN basada en protocolo Puede cambiar un grupo existente de VLAN basada en protocolo.
Para cambiar un grupo de VLAN basada en protocolo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.
Se muestra la página Protocol Based VLAN Group Configuration.

6. Marque la casilla del ID de grupo.

7. Cambie la configuración según sea necesario.
Para obtener más información, consulte Agregar un grupo de VLAN basada en protocolo en la página 207.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un grupo de VLAN basada en protocolo Puede eliminar un grupo de VLAN basada en protocolo que ya no necesite.
Para eliminar un grupo de VLAN basada en protocolo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.
Se muestra la página Protocol Based VLAN Group Configuration.

6. Marque la casilla del ID de grupo.

7. Haga clic en el botón Delete.
Se elimina el grupo de VLAN basada en protocolo.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar las interfaces miembro de un grupo de VLAN basada en protocolo

Para un protocolo, una interfaz solo puede pertenecer a un grupo de VLAN basada en protocolo. Si ya agregó una interfaz a un grupo para IP, no puede agregar la interfaz a otro grupo que también incluya IP, pero puede agregarla a un nuevo grupo para IPX.

Para configurar las interfaces miembro de un grupo de VLAN basada en protocolo:

1. Abra un navegador web.

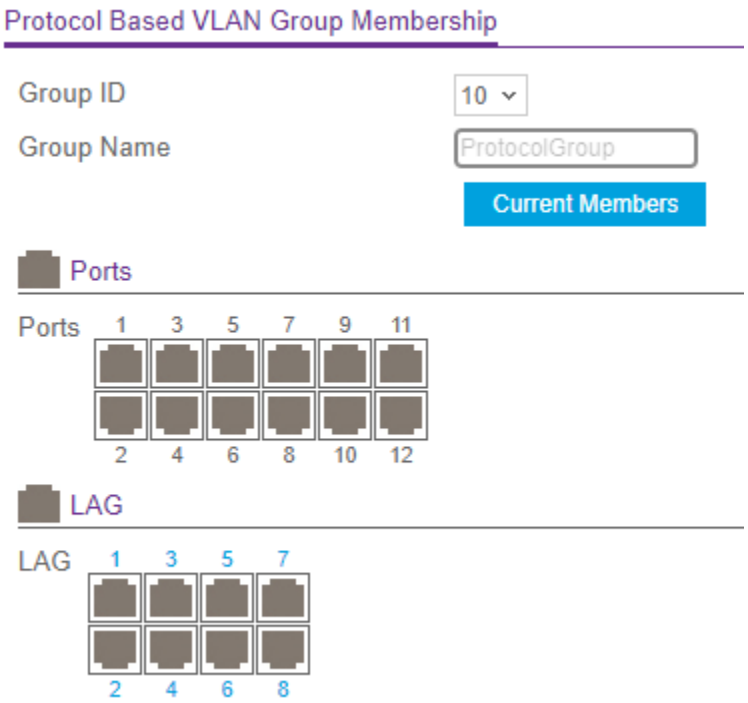
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Protocol Based VLAN Group Membership.



La figura anterior muestra la página de un modelo de 12 puertos. Según su modelo de switch, el ícono Ports (sobre la tabla Ports) puede aparecer como el ícono Unit 1.

6. En el menú Group ID, seleccione el ID del grupo de VLAN basada en protocolo. El campo Group Name muestra el nombre de la VLAN basada en protocolo que seleccionó.

7. Para mostrar los miembros actuales del grupo de VLAN basada en protocolo seleccionado, haga clic en el botón Current Members.
Una ventana emergente muestra los miembros.

8. Para seleccionar interfaces físicas para la VLAN, realice una de las siguientes acciones:

- Seleccionar todas las interfaces físicas: Haga clic en el ícono Ports o Unit 1 encima de la tabla Ports.
- Seleccionar interfaces físicas individuales: En la tabla Ports, haga clic en uno o más puertos individualmente.

9. Para seleccionar LAG para la VLAN, realice una de las siguientes acciones:

- Seleccionar todos los LAG: Haga clic en el ícono LAG encima de la tabla LAG.
- Seleccionar LAG individuales: En la tabla LAG, haga clic en uno o más LAG individualmente.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar una VLAN basada en subred IP

Una asignación de subred IP a VLAN se configura especificando una dirección IP de origen, una máscara de red y el ID de VLAN. Las configuraciones de subred IP a VLAN se comparten entre todas las interfaces del switch.

Agregar una VLAN basada en subred IP Puede agregar una VLAN basada en subred IP. Para agregar una VLAN basada en subred IP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > IP Subnet Based VLAN. Se muestra la página IP Subnet Based VLAN.

6. En el campo IP Address, especifique una dirección IP.
Ingrese la dirección IP en notación decimal con puntos.

7. En el campo Subnet Mask, especifique una máscara de subred asociada con la dirección IP. Ingrese la máscara de subred en notación decimal con puntos.

8. En el campo VLAN ID, especifique el ID de VLAN al que debe vincularse la configuración IP.
El ID de VLAN puede estar en el rango de 1 a 4093.

9. Haga clic en el botón Add.
Se agrega la VLAN basada en subred IP.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una VLAN basada en subred IP Puede eliminar una VLAN basada en subred IP que ya no necesite.
Para eliminar una VLAN basada en subred IP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching> VLAN > Advanced > IP Subnet Based VLAN. Se muestra la página IP Subnet Based VLAN.

6. Marque la casilla de la VLAN basada en subred IP.

7. Haga clic en el botón Delete.
Se elimina la VLAN basada en subred IP.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una VLAN doble

Una VLAN doble (DVLAN) le permite configurar una etiqueta de VLAN EtherType dentro de una etiqueta de VLAN. La etiqueta de VLAN EtherType puede ser una etiqueta 802.1Q, una etiqueta de red de área metropolitana virtual (vMAN) o una etiqueta personalizada.

Para configurar el EtherType global de la DVLAN y configurar la DVLAN en una o más interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Port DVLAN Configuration. Se muestra la página Port DVLAN Configuration.

6. En el menú Global EtherType, seleccione un tipo de etiqueta que determina los primeros 16 bits de la etiqueta DVLAN:

- 802.1Q Tag: La etiqueta dot1q que representa 0x8100.
- vMAN Tag: La etiqueta de red de área metropolitana virtual (vMAN) que representa 0x88A8.
- Custom Tag: Una etiqueta EtherType personalizada en el rango de 0 a 65535. Con esta opción se muestra el campo Custom Value.

7. Si selecciona Custom Tag en el menú Global EtherType, ingrese la etiqueta EtherType personalizada en el campo Custom Value.
La etiqueta puede estar en el rango de 0 a 65535.

8. Seleccione si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes enlaces encima del encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

9. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

10. En el menú Admin Mode, seleccione Enabled o Disabled para especificar si la etiqueta DVLAN seleccionada se agrega a las tramas que se procesan en la interfaz. El valor predeterminado es Disabled y la etiqueta DVLAN seleccionada no se agrega a las tramas.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar una VLAN de voz

Puede configurar una VLAN de voz para usarla con tráfico de voz. Por ejemplo, habilite la VLAN de voz en una interfaz conectada a teléfonos IP. Una VLAN de voz puede garantizar que la calidad de sonido del tráfico de teléfonos IP siga siendo buena cuando el tráfico de datos en la misma interfaz es alto.

Para configurar una VLAN de voz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > Voice VLAN Configuration. Se muestra la página Voice VLAN Configuration.

6. Seleccione el botón de opción Admin Mode Disable o Enable para deshabilitar o habilitar el modo global de VLAN de voz en el switch.
El valor predeterminado es Disable. Si desea usar una VLAN de voz, debe habilitar el modo global de VLAN de voz.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Interface Mode, seleccione el modo de VLAN de voz:

• Disable: Este es el valor predeterminado.
• None: Permite que un teléfono IP use su propia configuración para enviar tráfico de voz sin etiquetar.
• VLAN ID: Un teléfono IP debe configurarse para enviar tráfico de voz etiquetado.
• Dot1p: Configure el etiquetado de prioridad 802.1p de la VLAN de voz para el tráfico de voz. Si selecciona este modo, ingrese el valor dot1p en el campo Value.
• Untagged: Un teléfono IP debe configurarse para enviar tráfico de voz sin etiquetar.

9. En el menú CoS Override Mode, seleccione una de las siguientes opciones:

• Enable: La interfaz ignora (es decir, anula) el valor de prioridad 802.1p de las tramas Ethernet que recibe de los dispositivos conectados. El campo DSCP anula el valor CoS.
• Disable: La interfaz confía en el valor de prioridad de la trama recibida. El valor predeterminado es Disable.

10. En el menú Authentication Mode, seleccione una de las siguientes opciones:

• Enable: Se permite el tráfico de voz en una interfaz de VLAN de voz no autorizada. El valor predeterminado es Enable.
• Disable: El tráfico de voz solo se permite en una interfaz de VLAN de voz autorizada, para la cual debe estar habilitado dot1x (consulte Administrar la autenticación de puertos en puertos individuales en la página 554).

11. En el campo DSCP Value, configure el valor DSCP para la interfaz.
El rango es de 0 a 64. El valor predeterminado es 0.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

El campo Operational State muestra el estado operativo de la VLAN de voz en la interfaz.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar Generic Attribute Registration Protocol

Generic Attribute Registration Protocol (GARP) permite que los dispositivos de red compartan información como ID de VLAN y membresía de grupos multicast a través de una LAN con puentes. Es decir, los participantes de GARP pueden registrar y anular el registro de valores de atributos dentro de la LAN. Cuando un participante de GARP declara o retira un atributo, el valor del atributo se registra para ese atributo y para la interfaz desde la que se hizo la declaración o el retiro.

Lo siguiente se aplica a GARP:

- El registro solo ocurre en interfaces que reciben una PDU de GARP con una declaración o un retiro.
- La anulación del registro solo ocurre si todos los participantes de GARP conectados al mismo segmento de LAN que la interfaz retiran la declaración.

Configurar los ajustes de GARP del switch Puede habilitar globalmente GARP VLAN registration protocol (GVRP) y GARP multicast registration protocol (GMRP) en el switch. Para configurar los ajustes de GARP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > GARP Switch Configuration. Se muestra la página GARP Switch Configuration.

6. Seleccione el botón de opción GVRP Mode Disable o Enable para deshabilitar o habilitar GARP VLAN registration protocol (GVRP) globalmente para el switch.
Si GVRP está habilitado, el switch puede compartir ID de VLAN con dispositivos de la red. El valor predeterminado es Disable.

7. Seleccione el botón de opción GMRP Mode Disable o Enable para deshabilitar o habilitar GARP multicast registration protocol (GMRP) globalmente para el switch. Si GMRP está habilitado, el switch puede compartir información multicast con dispositivos de la red. El valor predeterminado es Disable.

8. Haga clic en el botón Apply.
La configuración se guarda.

Los cambios en la configuración de GARP pueden tardar hasta 10 segundos en surtir efecto.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de GARP para una o más interfaces Puede configurar los ajustes de GARP para interfaces individuales. Estos ajustes surten efecto solo si el modo GVRP, el modo GMRP o ambos modos están habilitados en el switch.
Para configurar los ajustes de GARP para una o más interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > VLAN > Advanced > GARP Port Configuration.
Se muestra la página GARP Port Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú GVRP Mode, seleccione Enable o Disable para especificar el modo GARP VLAN registration protocol del puerto.
Si selecciona Disable, GVRP no está activo y las opciones join time, leave time y leave all time no tienen efecto. El valor predeterminado es Disable.

9. En el menú GMRP Mode, seleccione Enable o Disable para especificar el modo GARP multicast registration protocol del puerto.

Si selecciona Disable, GMRP no está activo y las opciones join time, leave time y leave all time no tienen efecto. El valor predeterminado es Disable.

10. En el campo Join Timer, especifique el tiempo en centésimas de segundo entre la transmisión de PDU de GARP que registran la membresía de una VLAN o un grupo multicast. Ingrese un número entre 10 y 100 (0.1 a 1.0 segundos). El valor predeterminado es 20 centésimas de segundo (0.2 segundos). Existe una instancia de este temporizador para cada participante de GARP en cada puerto.

11. En el campo Leave Timer, especifique el tiempo en centésimas de segundo que se espera después de recibir una solicitud de anulación de registro de una VLAN o un grupo multicast antes de eliminar la entrada asociada.
Esto da tiempo para que otra estación afirme el registro del mismo atributo y mantenga un servicio ininterrumpido. Ingrese un número entre 20 y 600 (0.2 a 6.0 segundos). El valor predeterminado es 60 centésimas de segundo (0.6 segundos). Existe una instancia de este temporizador para cada participante de GARP en cada puerto.

12. En el campo Leave All Timer, especifique con qué frecuencia (en centésimas de segundo) se generan las PDU LeaveAll.
Una PDU LeaveAll indica que todos los registros se anularán pronto. Para mantener el registro, los participantes deben volver a unirse. El temporizador del periodo leave all se establece en un valor aleatorio en el rango de LeaveAllTime a 1.5 * LeaveAllTime. El temporizador se especifica en centésimas de segundo. Ingrese un número entre 200 y 6000 (2 a 60 segundos). El valor predeterminado es 1000 centésimas de segundo (10 segundos). Existe una instancia de este temporizador para cada participante de GARP en cada puerto.

13. Haga clic en el botón Apply.
La configuración se guarda.

Los cambios en la configuración de GARP pueden tardar hasta 10 segundos en surtir efecto.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Auto-VoIP

Voice over Internet Protocol (VoIP) permite hacer llamadas telefónicas a través de una red de datos. Como el tráfico de voz suele ser más sensible al tiempo que el tráfico de datos, Auto-VoIP ofrece clasificación de los paquetes de voz para que puedan priorizarse sobre los paquetes de datos y lograr una mejor calidad de servicio (QoS). Con Auto-VoIP, la priorización de voz se basa en protocolos de control de llamadas como SIP, H.323 y SCCP en las interfaces o en los bits de identificador único de organización (OUI).

Configurar los ajustes de Auto-VoIP basados en protocolo

Para priorizar el tráfico de voz sensible al tiempo sobre el tráfico de datos, Auto-VoIP basado en protocolo determina si los paquetes transportan los siguientes protocolos VoIP:

- Session Initiation Protocol (SIP)
- H.323
- Signalling Connection Control Part (SCCP)

Los paquetes VoIP que entran por una interfaz en la que Auto-VoIP está habilitado se marcan con el valor de clase de tráfico CoS especificado.

Para configurar los ajustes basados en protocolo para una o más interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Auto-VoIP > Protocol-based > Port Settings. Se muestra la página Port Settings.

6. En la sección Protocol Based Global Settings, especifique los siguientes ajustes globales:

a. En el menú Prioritization Type, seleccione Traffic Class o Remark.

Esto especifica el tipo de priorización.

b. En el menú Class Value, especifique el valor de clase CoS que se reasignará a los paquetes que recibe la VLAN de voz. Puede seleccionar un valor en el rango de 0 a 7.

7. En la sección Protocol Based Global Settings, especifique los ajustes de Auto VoIP para las interfaces:

a. Seleccione si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes enlaces encima del encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Esta es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

b. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

c. En el menú Auto VoIP Mode, seleccione habilitar o deshabilitar el modo Auto VoIP para la interfaz.
Auto-VoIP está deshabilitado de forma predeterminada.

8. Haga clic en el botón Apply.
La configuración se guarda.

El campo Operational Status muestra si la interfaz está activa o inactiva.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar las propiedades de Auto-VoIP basadas en OUI

Con Auto-VoIP basado en el identificador único de organización (OUI), la priorización de voz se proporciona según los bits OUI.

Para configurar las propiedades de Auto-VoIP basadas en OUI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Auto-VoIP > OUI-based > Properties. Se muestra la página Properties.

6. En el campo Auto-VoIP VLAN ID, ingrese el ID de VLAN VoIP del switch. No existe una VLAN predeterminada para Auto-VoIP; debe crear una VLAN para Auto-VoIP.

7. En el menú OUI-based priority, seleccione la prioridad basada en OUI del switch. El valor predeterminado es 7.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de interfaz basados en OUI

Puede configurar los ajustes de interfaz OUI.

Para configurar los ajustes de interfaz basados en OUI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Auto-VoIP > OUI-based > Port Settings. Se muestra la página Port Settings.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

• 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
• LAG: Solo se muestran los LAG.
• All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
• Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú Auto VoIP Mode, seleccione habilitar o deshabilitar el modo Auto VoIP para la interfaz.
Auto-VoIP está deshabilitado de forma predeterminada.

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Operational Status muestra si la interfaz está activa o inactiva.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Administrar la tabla OUI

Los fabricantes de hardware pueden incluir un OUI en un adaptador de red para ayudar a identificar un dispositivo de hardware. El OUI es un número único de 24 bits asignado por la autoridad de registro del IEEE. El switch viene preconfigurado con los siguientes OUI que identifican al fabricante del teléfono IP:

- 00:01:E3: SIEMENS
- 00:03:6B: CISCO1
- 00:12:43: CISCO2
- 00:0F:E2: H3C
- 00:60:B9: NITSUKO
- 00:D0:1E: PINTEL
- 00:E0:75: VERILINK
- 00:E0:BB: 3COM
- 00:04:0D: AVAYA1
- 00:1B:4F: AVAYA2

- 00:04:13: SNOM
- 00:1D:C1: Dante

Puede seleccionar un OUI existente o agregar un nuevo OUI y una descripción para identificar los teléfonos IP de la red.

Agregar un prefijo OUI Para agregar un prefijo OUI:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Auto-VoIP > OUI-based > OUI Table. Se muestra la página OUI Table.

6. En el campo Telephony OUI(s), especifique el nuevo prefijo OUI de VoIP con el formato AA:BB:CC.
La tabla puede incluir hasta 128 OUI.

7. En el campo Description, ingrese la descripción del OUI. La longitud máxima es de 32 caracteres.

8. Haga clic en el botón Add.
Se agrega la entrada de OUI de telefonía.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar uno o más prefijos OUI Para eliminar uno o más prefijos OUI:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Auto-VoIP > OUI-based > OUI Table. Se muestra la página OUI Table.

6. Marque la casilla junto a cada prefijo OUI que desea eliminar.

7. Haga clic en el botón Delete.
Se eliminan las entradas de OUI de telefonía.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar el estado de Auto-VoIP

Para mostrar el estado de Auto-VoIP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Auto-VoIP > Auto-VoIP Status. Se muestra la página Auto-VoIP Status.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 55. Información de estado de Auto-VoIP

Campo	Descripción
ID de VLAN de Auto-VoIP	El ID de VLAN de Auto-VoIP.
Número máximo de canales de voz admitidos	El número máximo de canales de voz admitidos.
Número de canales de voz detectados	El número de canales VoIP priorizados correctamente.

Spanning Tree Protocol

El Spanning Tree Protocol (STP) proporciona una topología de árbol para cualquier disposición de dispositivos de red. STP también proporciona una sola ruta entre estaciones finales de una red, eliminando los bucles. STP (también llamado STP “clásico”) proporciona una sola ruta entre estaciones finales, evitando y eliminando bucles. Para configurar los ajustes globales de STP del switch, consulte Configurar los ajustes de STP y mostrar el estado de STP en la página 226.

El switch admite las siguientes versiones de spanning tree:

- CST: STP común. Para configurar CST, consulte Configurar los ajustes de CST y mostrar el estado de CST en la página 229 y Configurar los ajustes de interfaz CST en la página 231.
- MSTP: Multiple Spanning Tree Protocol (MSTP, también llamado MST) admite varias instancias de spanning tree para canalizar de forma eficiente el tráfico VLAN por distintas interfaces. Para configurar MSTP, consulte Administrar instancias MST en la página 236 y Configurar y mostrar los ajustes de interfaz de una instancia MST en la página 239.
- RSTP: STP rápido. Cada instancia del spanning tree se comporta según lo especificado en IEEE 802.1w, Rapid Spanning Tree (RSTP), con ligeras modificaciones en el funcionamiento pero no en el efecto final (el efecto principal es la transición rápida del puerto al estado de reenvío).
  La diferencia entre RSTP y el STP tradicional (IEEE 802.1D) es la capacidad de configurar y reconocer la conectividad full-duplex y los puertos conectados a estaciones finales, lo que produce una transición rápida del puerto al estado de reenvío y la supresión de los mensajes de notificación de cambio de topología. Estas funciones se representan con los parámetros ‘pointtopoint’ y ‘edgeport’. MSTP es compatible con RSTP y STP. Se comporta de forma adecuada para bridges STP y RSTP

Un bridge MSTP puede configurarse para comportarse totalmente como un bridge RSTP o como un bridge STP.

- PVST: Per-VLAN Spanning Tree (PVST) proporciona una instancia única de spanning tree para cada VLAN. Para configurar PVST, consulte Configurar los ajustes de VLAN PVST/RPVST en la página 243 y Configurar los ajustes de interfaz PVST y RPVST en la página 246.
- RPVST: Rapid Per-VLAN Spanning Tree (RPVST) proporciona una instancia única de spanning tree para cada VLAN, y cada instancia se comporta según lo especificado en IEEE 802.1w, Rapid Spanning Tree (RSTP). En comparación con PVST, RPVST ofrece una convergencia de spanning tree más rápida ante cambios de topología de capa 2. Para configurar RPVST, consulte Configurar los ajustes de VLAN PVST/RPVST en la página 243 y Configurar los ajustes de interfaz PVST y RPVST en la página 246.

Nota: Para que dos bridges estén en la misma región, la versión forzada debe ser 802.1s y sus nombres de configuración, claves digest y niveles de revisión deben coincidir. Para más información sobre las regiones y su efecto en la topología de red, consulte el estándar IEEE 802.1Q.

Configurar los ajustes de STP y mostrar el estado de STP

Puede configurar los ajustes del Spanning Tree Protocol (STP) y mostrar el estado de STP en el switch.

Para configurar los ajustes de STP y mostrar el estado de STP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Basic > STP Configuration. Se muestra la página STP Configuration.

6. Seleccione el botón de opción Spanning Tree Admin Mode Disable o Enable.

Esto especifica si la operación de spanning tree está habilitada en el switch.

7. Seleccione uno de los siguientes botones de opción Force Protocol Version para especificar la versión de STP que debe usar el switch:

- IEEE 802.1d: Spanning Tree Protocol tradicional (clásico).
- IEEE 802.1w: Rapid Spanning Tree Protocol.
- IEEE 802.1s: Multiple Spanning Tree Protocol.
- PVST: Per-VLAN Spanning Tree Protocol.
- RPVST: Rapid Per-VLAN Spanning Tree Protocol.

8. En el campo Configuration Name, especifique un ID o nombre que permita identificar la configuración.
El nombre puede tener hasta 32 caracteres. El valor predeterminado es la dirección MAC del switch.

9. En el campo Configuration Revision Level, especifique un ID que permita identificar la configuración.
Por ejemplo, si cambia la configuración, puede cambiar el ID en el campo Configuration Revision Level para llevar el control de las distintas configuraciones. Puede introducir un ID de 0 a 65535. El valor predeterminado es 0.

10. Seleccione uno de los siguientes botones de opción Forward BPDU while STP Disabled:

- Disabled: Las BPDU de spanning tree no se reenvían si spanning-tree está deshabilitado en el switch. El valor predeterminado es Disable.
- Enabled: Las BPDU de spanning tree se reenvían si spanning-tree está deshabilitado en el switch.

11. Seleccione uno de los siguientes botones de opción BPDU Guard:

- Disabled: La función BPDU guard está deshabilitada, que es el ajuste predeterminado.
- Enabled: La función BPDU guard está habilitada y refuerza los límites del dominio STP para mantener la topología activa coherente y predecible. Los switches detrás de puertos de borde con BPDU guard habilitado no afectan la topología STP general. Al recibir BPDU, el puerto con BPDU guard habilitado pasa al estado deshabilitado.

12. Seleccione uno de los siguientes botones de opción BPDU Filter:

- Disabled: La función BPDU Filter está deshabilitada, que es el ajuste predeterminado.
- Enabled: La función BPDU Filter está habilitada y se aplica a todos los puertos de borde operativos. Un puerto de borde operativo se conecta a hosts que normalmente descartan las BPDU. Si un puerto de borde operativo recibe una BPDU, pierde su estado operativo. Si un puerto con filtrado de BPDU habilitado recibe BPDU, el puerto descarta las BPDU y sigue operativo.

13. Seleccione uno de los siguientes botones de opción Fast Backbone:

- Disabled: La función Fast Backbone está deshabilitada, que es el ajuste predeterminado.
- Enabled: La función Fast Backbone está habilitada. Si falla un enlace indirecto, el switch puede seleccionar automáticamente un nuevo enlace indirecto. Con PVST, el switch no ignora las BPDU inferiores (como ocurre con STP), sino que deja que expiren en el puerto donde se recibieron. Después, el switch envía consultas de enlace raíz por otros puertos no designados. Si el switch recibe una respuesta positiva, selecciona un nuevo enlace indirecto.

14. Seleccione uno de los siguientes botones de opción Fast Uplink:

- Disabled: La función Fast Uplink está deshabilitada, que es el ajuste predeterminado.
- Enabled: La función Fast Uplink está habilitada. Si el puerto raíz principal se cae, se reduce el tiempo de recuperación al seleccionar un nuevo puerto raíz.

15. Si habilitó Fast Uplink en el paso anterior, en el campo Max Update Rate, introduzca la tasa máxima de actualización en paquetes por segundo. Introduzca de 0 a 32000 paquetes por segundo. El valor predeterminado es 150.

16. Haga clic en el botón Apply. Se guardan los ajustes.

17. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 56. Información de configuración y estado de STP

Campo	Descripción
Configuración de STP	
Configuration Digest Key	El identificador de la configuración de STP.
Configuration Format Selector	La versión del formato de configuración para el intercambio de BPDU.
Estado de STP	
MST ID	La instancia de multiple spanning tree (MST) o common spanning tree (CST).

Tabla 56. Información de configuración y estado de STP (continuación)

Campo	Descripción
VID ID	El ID de VLAN (VID).
FID ID	El ID de filtrado (FID).

Configurar los ajustes de CST y mostrar el estado de CST

Puede configurar el common spanning tree (CST) y mostrar el estado de CST en el switch.

Para configurar los ajustes de CST y mostrar el estado de CST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > CST Configuration. Se muestra la página CST Configuration.

6. En el campo Bridge Priority, especifique el valor de prioridad del bridge para el common spanning tree (CST) y el common and internal spanning tree (CIST).
El rango es de 0 a 61440. La prioridad del bridge es un múltiplo de 4096. La prioridad predeterminada es 32768.

Cuando los switches o bridges ejecutan STP, a cada uno se le asigna una prioridad. Después de intercambiar BPDU, el switch con el valor de prioridad más bajo se convierte en el bridge raíz. Si especifica una prioridad que no es múltiplo de 4096, la prioridad se establece automáticamente en la siguiente prioridad inferior que sea múltiplo de 4096. Por ejemplo, si establece la prioridad en un valor entre 0 y 4095, se establece automáticamente en 0.

7. En el campo Bridge Max Age (secs), especifique el período en segundos que un bridge espera antes de implementar un cambio de topología.

El rango es de 6 a 40 segundos, y el valor debe ser menor o igual que lo siguiente: (2 * Bridge Forward Delay) – 1 y mayor o igual que 2 * (Bridge Hello Time +1).

El valor predeterminado es 20 segundos.

Nota: El campo Bridge Hello Time (secs) muestra el período fijo en segundos que un bridge raíz espera entre mensajes de configuración. El período fijo es de 2 segundos.

8. En el campo Bridge Forward Delay (secs), especifique el período en segundos que un bridge permanece en estado de escucha y aprendizaje antes de reenviar paquetes. El período es de 4 a 30 segundos, y el valor debe ser mayor o igual que lo siguiente: (Bridge Max Age / 2) + 1.

El valor predeterminado es 15 segundos.

9. En el campo Spanning Tree Maximum Hops, especifique el número máximo de saltos de bridge que puede recorrer la información de una instancia CST determinada antes de descartarse.
El rango es de 6 a 40 saltos. El valor predeterminado es 20 saltos.

10. En el campo Spanning Tree Tx Hold Count, especifique el número máximo de BPDU que el bridge puede enviar dentro de la ventana de tiempo hello.
El rango es de 1 a 10. El valor predeterminado es 6.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 57. Información de estado de CST

Campo	Descripción
Bridge identifier	El identificador de bridge del CST, que consta de la prioridad del bridge y la dirección MAC base del bridge.
Time Since Topology Change	El tiempo en segundos desde que cambió la topología del CST.
Topology Change Count	El número de veces que cambió la topología del CST.
Topology Change	Este campo indica si hay un cambio de topología en curso en algún puerto asignado al CST. (True o False.)

Tabla 57. Información de estado de CST (continuación)

Campo	Descripción
Designated Root	El identificador de bridge del bridge raíz, que consta de la prioridad del bridge y la dirección MAC base del bridge.
Root Path Cost	El costo de ruta hacia la raíz designada del CST.
Root Port	El puerto a través del cual se accede a la raíz designada del CST.
Max Age (secs)	El período en segundos que transcurre antes de que un puerto de bridge guarde su información de BPDU de configuración.
Forward Delay (secs)	El período en segundos que el bridge del puerto raíz retrasa el proceso de reenvío. Este período es un valor derivado.
Hold Time (secs)	El período mínimo entre transmisiones de BPDU de configuración.
CST Regional Root	La prioridad y la dirección MAC base de la raíz regional del CST.
CST Path Cost	El costo de ruta hacia la raíz regional del CST.
Port Triggered TC	El puerto en el que se activa el cambio de topología (TC).

Configurar los ajustes de interfaz CST

Puede configurar un common spanning tree (CST) e internal spanning tree en una interfaz específica del switch.

Una interfaz puede quedar deshabilitada por diagnóstico (D-Disable) cuando ocurre una condición de error grave de DOT1S. La causa más común es una inundación de BPDU. El criterio de inundación es que DOT1S reciba más de 15 BPDU en un intervalo de 3 segundos. (Otras causas de una condición D-Disable de DOT1S son muy raras.)

Para configurar los ajustes de interfaz CST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > CST Port Configuration. Se muestra la página CST Port Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el campo Port Priority, especifique la prioridad del puerto en el CST. Especifique la prioridad en múltiplos de 16. Por ejemplo, si establece la prioridad del puerto en un valor entre 0 y 15, se establece automáticamente en 0. Si la establece en un valor entre 16 y (2*16-1), se establece automáticamente en 16, y así sucesivamente. El valor predeterminado es 128.

9. En el menú Admin Edge Port, seleccione Enable o Disable para especificar si el puerto funciona como puerto de borde en el CIST.
El valor predeterminado es Disable.

10. En el campo Port Path Cost, especifique un valor de costo de ruta para el puerto en el CIST. El valor puede estar en el rango de 1 a 200000000. El valor predeterminado es 0.

11. En el menú Auto Calculated Port Path Cost, seleccione Enable o Disable para especificar si el costo de ruta externo se calcula automáticamente.
Si el valor del campo Port Path Cost es cero y el costo de ruta se calcula automáticamente, el valor se basa en la velocidad de enlace del puerto.

El valor predeterminado es Disable.

12. En el campo External Port Path Cost, especifique un valor de costo de ruta externo para el puerto en el CIST.
El valor puede estar en el rango de 1 a 200000000. El valor predeterminado es 0.

13. En el menú Auto Calculated External Port Path Cost, seleccione Enable o Disable para especificar si el costo de ruta externo se calcula automáticamente.

Si el valor del campo External Port Path Cost es cero y el costo de ruta externo se calcula automáticamente, el valor se basa en la velocidad de enlace del puerto.

El valor predeterminado es Disable.

14. En el menú BPDU Filter, seleccione Enable o Disable para especificar si el tráfico BPDU se filtra en el puerto cuando STP está habilitado en el puerto.
El valor predeterminado es Disable.

15. En el menú BPDU Forwarding, seleccione Enable o Disable para especificar si el tráfico BPDU que llega al puerto puede inundarse si STP está deshabilitado en el puerto. El valor predeterminado es Disable.

16. En el menú Auto Edge, seleccione Enable o Disable para especificar si el puerto puede convertirse en puerto de borde si no recibe BPDU durante un período. El valor predeterminado es Enable.

17. En el menú Root Guard, seleccione Enable o Disable para especificar si el puerto puede descartar cualquier información superior que reciba y, de este modo, evitar que cambie la raíz del dispositivo.
Si habilita esta opción, el puerto se coloca en estado de descarte y no reenvía ningún paquete. El valor predeterminado es Disable.

18. En el menú Loop Guard, seleccione Enable o Disable para especificar si el puerto está protegido contra bucles de reenvío de capa 2.
Si habilita esta opción, el puerto pasa del estado ‘listening/learning/forwarding’ al ‘STP loop inconsistent blocking state’. El valor predeterminado es Disable

19. En el menú TCN Guard, seleccione Enable o Disable para especificar si se impide que el puerto propague la información de cambio de topología que recibe. El valor predeterminado es Disable.

20. En el menú Port Mode, seleccione Enable o Disable para especificar si STP está habilitado o deshabilitado en el puerto.
El valor predeterminado es Disable.

21. Haga clic en el botón
Apply. Se guardan los ajustes.

22. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 58. Información de configuración de puertos CST

Campo	Descripción
Hello Timer	El ajuste del temporizador Hello del CST. De forma predeterminada, es 2.
BPDU Guard Effect	Indica si un puerto de borde que recibe paquetes BPDU está habilitado o deshabilitado.
Port Forwarding State	Indica el estado STP actual de la interfaz. Si está habilitado, el estado del puerto determina qué acción de reenvío se aplica al tráfico. Los estados posibles son los siguientes: • Disabled: STP está deshabilitado en la interfaz. La interfaz reenvía tráfico mientras aprende direcciones MAC. • Blocking: La interfaz está bloqueada y no puede usarse para reenviar tráfico ni aprender direcciones MAC. • Listening: La interfaz está en modo de escucha. La interfaz no puede reenviar tráfico ni aprender direcciones MAC. • Learning: La interfaz está en modo de aprendizaje. No puede reenviar tráfico, pero sí puede aprender nuevas direcciones MAC. • Forwarding: La interfaz está en modo de reenvío. La interfaz puede reenviar tráfico y aprender nuevas direcciones MAC • Manual forwarding: La interfaz está en modo de reenvío manual. La interfaz puede reenviar tráfico y aprender nuevas direcciones MAC

Mostrar el estado de interfaz CST

Puede mostrar la información de estado de Common Spanning Tree (CST) de las interfaces del switch.

Para mostrar el estado de interfaz CST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > CST Port Status.

Se muestra la página CST Port Status.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Para actualizar la página, haga clic en el botón Refresh.

La siguiente tabla describe los campos no configurables de la página.

Tabla 59. Información de estado de interfaz CST

Campo	Descripción
Interface	La interfaz física o LAG asociada al CST.
Port ID	El identificador del puerto en el CST, que se crea a partir de la prioridad del puerto y el número de interfaz.
Port Forwarding State	Indica el estado STP actual de la interfaz. Si está habilitado, el estado del puerto determina qué acción de reenvío se aplica al tráfico. Los estados posibles son los siguientes: • Disabled: STP está deshabilitado en la interfaz. La interfaz reenvía tráfico mientras aprende direcciones MAC. • Blocking: La interfaz está bloqueada y no puede usarse para reenviar tráfico ni aprender direcciones MAC. • Listening: La interfaz está en modo de escucha. La interfaz no puede reenviar tráfico ni aprender direcciones MAC. • Learning. La interfaz está en modo de aprendizaje. La interfaz no puede reenviar tráfico. Sin embargo, puede aprender nuevas direcciones MAC. • Forwarding: La interfaz está en modo de reenvío. La interfaz puede reenviar tráfico y aprender nuevas direcciones MAC. • Manual forwarding: La interfaz está en modo de reenvío manual. La interfaz puede reenviar tráfico y aprender nuevas direcciones MAC
Port Role	A cada puerto de bridge MST habilitado se le asigna un rol de puerto para cada spanning tree. El rol es uno de los siguientes: Root, Designated, Alternate, Backup, Master o Disabled.
Designated Root	El bridge raíz del CST, que se crea a partir de la prioridad del bridge y la dirección MAC base del bridge.
Designated Cost	El costo de ruta que ofrece el puerto designado a la LAN.
Designated Bridge	El identificador del bridge que tiene el puerto designado. Este identificador se crea a partir de la prioridad del bridge y la dirección MAC base del bridge.

Tabla 59. Información de estado de interfaz CST (continuación)

Campo	Descripción
Designated Port	El identificador de puerto en el bridge designado que ofrece el menor costo a la LAN. Este identificador se crea a partir de la prioridad del puerto y el número de interfaz del puerto.
Topology Change Acknowledge	Indica si el indicador de reconocimiento de cambio de topología está activado para la siguiente BPDU que se transmitirá por el puerto. (True o False.)
Edge port	Indica si el puerto está habilitado como puerto de borde.
Point-to-Point MAC	El estado punto a punto, que indica si el enlace del puerto es un enlace punto a punto (True) o no (False).
CST Regional Root	El identificador de bridge de la raíz regional del CST. Este identificador se crea a partir de la prioridad del bridge y la dirección MAC base del bridge.
CST Path Cost	El costo de ruta hacia la raíz regional del CST.
Port Up Time Since Counters Last Cleared	El tiempo transcurrido desde que se borraron los contadores por última vez.
Loop Inconsistent State	Indica si la interfaz está en estado de bucle inconsistente. (False o True.)
Transitions Into Loop Inconsistent State	El número de veces que la interfaz pasó al estado de bucle inconsistente.
Transitions Out Of Loop Inconsistent State	El número de veces que la interfaz salió del estado de bucle inconsistente.

Administrar instancias MST

Puede agregar, cambiar o eliminar instancias de multiple spanning tree (MST) en el switch. La instancia MST consta de un ID, un valor de prioridad y un ID de VLAN.

Agregar una instancia MST y mostrar el estado de MST Puede agregar una instancia MST y mostrar el estado de MST.
Para agregar una instancia MST y mostrar el estado de MST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > MST Configuration. Se muestra la página MST Configuration.

6. Configure los ajustes de la instancia MST:

• MST ID: En el campo MST ID, especifique el ID de la MST. El ID puede estar en el rango de 1 a 4094.
• Priority: En el campo Priority, especifique el valor de prioridad del puente para la instancia MST. Cuando los switches o puentes ejecutan STP, a cada uno se le asigna una prioridad. Tras intercambiar BPDU, el switch con el valor de prioridad más bajo se convierte en el puente raíz. La prioridad del puente es un múltiplo de 4096. Si especifica una prioridad que no es múltiplo de 4096, la prioridad se establece automáticamente en la siguiente prioridad inferior que sea múltiplo de 4096. Por ejemplo, si establece la prioridad en cualquier valor entre 0 y 4095, el switch establece automáticamente el valor en 0. El rango es de 0 a 61440. El valor predeterminado es 32768.
• VLAN ID: En el menú VLAN ID, seleccione la VLAN que debe asociarse con la instancia MST.

7. Haga clic en el botón Add. Se agrega la MST.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

9. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 60. Información de configuración de MST

Campo	Descripción
Bridge Identifier	El identificador de puente de la instancia MST, que se crea con la prioridad del puente y la dirección MAC base del puente.
Last TCN	El tiempo en segundos desde que cambió la topología de la instancia MST.
Topology Change Count	El número de veces que cambió la topología de la instancia MST.
Topology Change	Indica si hay un cambio de topología en curso en una interfaz de la MST. (True o False.)

Tabla 60. Información de configuración de MST (continuación)

Campo	Descripción
Designated Root	El identificador de puente del puente raíz, que se crea con la prioridad del puente y la dirección MAC base del puente
Root Path Cost	El costo de ruta hacia la raíz designada de la instancia MST.
Root Port	El puerto a través del cual se puede acceder a la raíz designada de la instancia MST.

Cambiar una instancia MST Puede cambiar una instancia MST existente.
Para cambiar una instancia MST existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > MST Configuration. Se muestra la página MST Configuration.

6. Marque la casilla asociada con la instancia MST.

7. Cambie la configuración según sea necesario.
Para obtener más información, consulte Agregar una instancia MST y mostrar el estado de MST en la página 236.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una instancia MST Puede eliminar una instancia MST que ya no necesite.

Para eliminar una instancia MST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > MST Configuration. Se muestra la página MST Configuration.

6. Marque la casilla asociada con la instancia MST.

7. Haga clic en el botón Delete.
Se elimina la instancia MST.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar y mostrar la configuración de interfaz de una instancia MST

Puede configurar y mostrar la configuración de interfaz de una instancia de Multiple Spanning Tree (MST).

Una interfaz puede quedar deshabilitada por diagnóstico (D-Disable) cuando ocurre una condición de error grave de DOT1S. La causa más común es una inundación de BPDU. El criterio de inundación es que DOT1S reciba más de 15 BPDU en un intervalo de 3 segundos. (Otras causas de una condición D-Disable de DOT1S son muy raras.)

Para configurar y mostrar la configuración de puertos de una instancia MST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > MST Port Configuration. Se muestra la página MST Port Configuration.

6. En el menú Select MST, seleccione una instancia MST.
Para obtener información sobre cómo agregar instancias MST, consulte Administrar instancias MST en la página 236.

7. Seleccione si desea mostrar interfaces físicas, LAG o ambas haciendo clic en uno de los siguientes enlaces sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

8. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

9. Configure los valores de MST para la interfaz o las interfaces seleccionadas:

- Port Priority: En el campo Port Priority, especifique la prioridad de la interfaz en la instancia MST. La prioridad del puerto se establece en múltiplos de 16. Si especifica un valor que no es múltiplo de 16, la prioridad se establece automáticamente en la siguiente prioridad inferior que sea múltiplo de 16. Por ejemplo, si establece un valor entre 0 y 15, la prioridad se establece en 0. Si especifica un número entre 16 y 31, la prioridad se establece en 16. Especifique un valor en el rango de 0 a 240. El valor predeterminado es 128.
- Port Path Cost: En el campo Port Path Cost, especifique el costo de ruta en el rango de 0 a 200000000. El valor predeterminado es 0.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 61. Información de configuración de interfaces MST

Campo	Descripción
Operational Port Path Cost	El costo de ruta que usa la interfaz.
Auto Calculated Port Path Cost	Indica si el costo de ruta se calcula automáticamente (Enable) o no (Disable). Si está habilitado, el costo de ruta se calcula según la velocidad de enlace del puerto si el valor configurado de Port Path Cost es cero.
Port ID	El identificador del puerto en la instancia MST, que se crea con la prioridad del puerto y el número de interfaz.
Port Uptime Since Last Clear Counters	El tiempo transcurrido desde que se borraron los contadores.
Port Mode	Indica si STP está habilitado para la interfaz.
Port Forwarding State	Indica el estado STP actual de la interfaz. Si está habilitado, el estado del puerto determina qué acción de reenvío se aplica al tráfico. Los estados de puerto posibles son los siguientes: • Disabled: STP está deshabilitado en la interfaz. La interfaz reenvía tráfico mientras aprende direcciones MAC. • Blocking: La interfaz está bloqueada y no se puede usar para reenviar tráfico ni aprender direcciones MAC. • Listening: La interfaz está en modo de escucha. La interfaz no puede reenviar tráfico ni aprender direcciones MAC. • Learning: La interfaz está en modo de aprendizaje. La interfaz no puede reenviar tráfico. Sin embargo, puede aprender nuevas direcciones MAC. • Forwarding: La interfaz está en modo de reenvío. La interfaz puede reenviar tráfico y aprender nuevas direcciones MAC. • Manual forwarding: La interfaz está en modo de reenvío manual. La interfaz puede reenviar tráfico y aprender nuevas direcciones MAC.
Port Role	A cada puerto de puente MST habilitado se le asigna un rol de puerto para cada árbol de expansión. El rol de puerto es uno de los siguientes: Root, Designated, Alternate, Backup, Master o Disabled.

Tabla 61. Información de configuración de interfaces MST (continuación)

Campo	Descripción
Designated Root	El identificador de puente del puente raíz, que se crea con la prioridad del puente y la dirección MAC base del puente
Designated Cost	El costo de ruta que ofrece el puerto designado a la LAN.
Designated Bridge	El identificador de puente del puente con el puerto designado. Este identificador se crea a partir de la prioridad del puente y la dirección MAC base del puente.
Designated Port	El identificador de puerto en el puente designado que ofrece el costo más bajo hacia la LAN. Este identificador se crea a partir de la prioridad del puerto y el número de interfaz del puerto.
Loop Inconsistent State	Indica si la interfaz está en estado de bucle inconsistente. (False o True.)
Transitions Into Loop Inconsistent State	El número de veces que la interfaz pasó al estado de inconsistencia de bucle.
Transitions Out Of Loop Inconsistent State	El número de veces que la interfaz salió del estado de inconsistencia de bucle de bucle.

Mostrar las estadísticas STP de las interfaces

Puede mostrar información sobre el número y tipo de unidades de datos de protocolo de puente (BPDU) que se transmiten y reciben en cada interfaz.

Para mostrar las estadísticas STP de las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > STP Statistics. Se muestra la página STP Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

La configuración se guarda.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 62. Información de estadísticas STP de las interfaces

Campo	Descripción
STP BPDUs Received	El número de BPDU STP recibidas en la interfaz.
STP BPDUs Transmitted	El número de BPDU STP transmitidas desde la interfaz
RSTP BPDUs Received	El número de BPDU RSTP recibidas en la interfaz.
RSTP BPDUs Transmitted	El número de BPDU RSTP transmitidas desde la interfaz.
MSTP BPDUs Received	El número de BPDU MSTP recibidas en la interfaz.
MSTP BPDUs Transmitted	El número de BPDU MSTP transmitidas desde la interfaz.

Configurar los ajustes de VLAN de PVST/RPVST

Puede configurar los ajustes de Per-VLAN Spanning Tree Protocol (PVST) y Rapid PVST (RPVST) para una VLAN.

PVST y RPVST deben estar habilitados. Para obtener más información, consulte Configurar los ajustes de STP y mostrar el estado de STP en la página 226.

Para configurar los ajustes de VLAN de PVST/RPVST del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > PVST
VLAN. Se muestra la página PVST VLAN.

6. En el campo VLAN ID, especifique un ID de VLAN único.
Solo puede especificar VLAN en las que STP esté habilitado y en las que PVST o RPVST esté habilitado.

7. En el menú Root, seleccione None, Primary o Secondary:

- None: El valor predeterminado es None. El switch no funciona como puente raíz ni como puente de reserva para la VLAN.
- Primary: El switch funciona como puente raíz para la VLAN. La prioridad del puente cambia del valor predeterminado de 32768 a un valor menor para asegurar la configuración de puente raíz.
- Secondary: El switch funciona como puente de reserva para la VLAN. La prioridad del puente cambia del valor predeterminado de 32768 a un valor menor para asegurar la configuración de puente de reserva.

8. En el campo Hello Time, ingrese el intervalo de hello time del árbol de expansión para las VLAN. El hello time es el intervalo entre el envío de BPDU sucesivas. Ingrese un valor en el rango de 1 a 10 segundos. El valor predeterminado es 2 segundos.

9. En el campo Forward Time, ingrese el intervalo de retardo de reenvío del árbol de expansión para la VLAN.
Este intervalo es el período durante el cual el switch detecta el estado antes de pasar un puerto de interfaz al estado de reenvío. El rango es de 4 a 30 segundos. El valor predeterminado es 15 segundos.

10. En el campo Max Age, ingrese el tiempo de antigüedad máxima del árbol de expansión para la VLAN. Este tiempo es el período después del cual una interfaz de puente guarda su información de configuración. El rango es de 6 a 40 segundos. El valor predeterminado es 20 segundos.

11. En el campo Priority, ingrese la prioridad de la VLAN.
Los valores permitidos están entre 0 y 61440. Los valores válidos se enumeran en la siguiente tabla.

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

El valor predeterminado es 32768. Si el valor que ingresa no está entre los valores especificados, se redondea automáticamente al valor válido más cercano.

12. Haga clic en el botón Add.
Se agrega la configuración de VLAN de PVST/RPVST.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Cambiar una configuración de VLAN de PVST/RPVST

Puede cambiar una configuración de VLAN de PVST/RPVST existente.

Para cambiar una configuración de VLAN de PVST/RPVST existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > PVST VLAN. Se muestra la página PVST VLAN.

6. Marque la casilla asociada con la configuración de VLAN de PVST/RPVST.
7. Cambie la configuración según sea necesario.

Para obtener más información, consulte Configurar los ajustes de VLAN de PVST/RPVST en la página 243.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una configuración de VLAN de PVST/RPVST

Puede eliminar una configuración de VLAN de PVST/RPVST que ya no necesite.

Para eliminar una configuración de VLAN de PVST/RPVST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > PVST VLAN. Se muestra la página PVST VLAN.

6. Marque la casilla asociada con la configuración de VLAN de PVST/RPVST.

7. Haga clic en el botón Delete.
Se elimina la configuración de VLAN de PVST/RPVST.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de interfaz de PVST y RPVST

Puede configurar los ajustes de Per-VLAN Spanning Tree Protocol (PVST) y Rapid PVST (RPVST) para una interfaz.

PVST y RPVST deben estar habilitados. Para obtener más información, consulte Configurar los ajustes de STP y mostrar el estado de STP en la página 226.

Para configurar los ajustes de interfaz de PVST y RPVST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > PVST Interface. Se muestra la página PVST Interface.

6. En el menú VLAN ID, seleccione una VLAN en la que STP y PVST o RPVST ya estén habilitados, o seleccione Other para configurar un nuevo ID de VLAN ingresándolo.

7. Seleccione si desea mostrar interfaces físicas, LAG o ambas haciendo clic en uno de los siguientes enlaces sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

8. En el campo Priority, ingrese la prioridad de la interfaz.
Establezca un número menor para que la interfaz reenvíe tramas. La prioridad se usa cuando la interfaz está configurada como enlace punto a punto. El valor puede ser de 0 a 240 y debe ser múltiplo de 16.

0	16	32
48	64	80
96	112	128 (predeterminado)
144	160	176

(Continuación)

192	208	224
240	-	-

El valor predeterminado es 128. Si el valor que ingresa no está entre los valores especificados, se redondea automáticamente al valor válido más cercano.

9. En el campo Cost, ingrese el costo de ruta de la interfaz al puente raíz. De forma predeterminada, el costo no se configura manualmente. Puede ingresar un valor de 1 a 200,000,000. Ingrese 0 para deshabilitar el ajuste. Si no se configura el costo por VLAN, el costo de ruta se establece según la velocidad de enlace.

10. En el menú Auto Calculated Cost, seleccione Enable o Disable para especificar si el costo se calcula automáticamente.
El valor predeterminado es Enable.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 63. Información de configuración de interfaces PVST/RPVST

Campo	Descripción
Role	El rol de la interfaz, que puede ser Disabled, Root, Designated, Alternate, Backup o Master. Nota: Para una interfaz que no es miembro de la VLAN seleccionada, el campo está en blanco.
Estado	El estado de la interfaz, que puede ser Discarding, Learning, Forwarding o Disabled. Nota: Para una interfaz que no es miembro de la VLAN seleccionada, el campo está en blanco.

Mostrar las estadísticas de PVST y RPVST

Puede mostrar las estadísticas de Per-VLAN Spanning Tree Protocol (PVST) y Rapid PVST (RPVST).

PVST y RPVST deben estar habilitados. Para obtener más información, consulte Configurar los ajustes de STP y mostrar el estado de STP en la página 226.

Para mostrar las estadísticas de PVST y RPVST:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > STP > Advanced > PVST Statistics. Se muestra la página PVST/RPVST Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.
Si PVST o RPVST está habilitado, la página muestra información estadística.

Base de datos de reenvío multicast

El tráfico IP multicast es tráfico destinado a un grupo de hosts. Los grupos de hosts se identifican con direcciones IP de clase D, que van de 224.0.0.0 a 239.255.255.255.

Mostrar las entradas de la base de datos de reenvío multicast

La base de datos de reenvío multicast (MFDB) contiene la información de membresía de puertos de todas las entradas de direcciones multicast activas. La clave de una entrada es una combinación de un ID de VLAN y una dirección MAC. Las entradas pueden contener datos de más de un protocolo.

Para mostrar las entradas de la base de datos de reenvío multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MFDB > MFDB Table. Se muestra la página MFDB Table.

6. Para buscar una entrada, en el campo Search by MAC Address, ingrese una dirección MAC y haga clic en el botón Go.
Si la dirección existe, se muestra esa entrada. Se requiere una coincidencia exacta.

La siguiente tabla describe los campos no configurables de la página.

Tabla 64. Información de MFDB

Campo	Descripción
MAC Address	La dirección MAC multicast para la que solicitó datos.
VLAN ID	El ID de VLAN con el que se relaciona la dirección MAC multicast.
Component	El componente responsable de esta entrada en la MFDB. El componente puede ser IGMP snooping, GMRP, Static Filtering o MLD snooping.
Type	El tipo de entrada. Las entradas estáticas son las que usted configura. Las entradas dinámicas se agregan a la tabla como resultado de un proceso de aprendizaje o protocolo.
Description	La descripción de esta entrada de la tabla multicast. La descripción puede ser Management Configured, Network Configured o Network Assisted.
Forwarding Interfaces	La lista de reenvío que se obtiene al combinar todas las interfaces de reenvío y quitar las interfaces que figuran como interfaces de filtrado estático.

Eliminar las entradas de IGMP snooping de la base de datos de reenvío multicast

Puede eliminar las entradas de IGMP snooping de la base de datos de reenvío multicast.

Para eliminar las entradas de IGMP snooping de la base de datos de reenvío multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MFDB > MFDB Table. Se muestra la página MFDB Table.

6. Haga clic en el botón Clear.
Se guarda la configuración.

7. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar todas las entradas MAC multicast conocidas de la base de datos de reenvío multicast

Puede eliminar todas las entradas MAC multicast conocidas de la base de datos de reenvío multicast.

Para eliminar todas las entradas MAC multicast conocidas de la base de datos de reenvío multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MFDB > MFDB Table. Se muestra la página MFDB Table.

6. Marque la casilla Reset Known Multicast MAC Entries. Se muestra una ventana emergente de confirmación.

7. Seleccione el botón OK. Se cierra la ventana emergente.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar las estadísticas de la base de datos de reenvío multicast

Puede mostrar las estadísticas de la base de datos de reenvío multicast

Para mostrar las estadísticas de la base de datos de reenvío multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MFDB > MFDB Statistics. Se muestra la tabla MFDB Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 65. Información de estadísticas de MFDB

Campo	Descripción
Max MFDB Table Entries	El número máximo de entradas que puede contener la tabla de la base de datos de reenvío multicast.
Most MFDB Entries Since Last Reset	El mayor número de entradas presentes en la tabla de la base de datos de reenvío multicast desde el último restablecimiento. Este valor también se conoce como el nivel máximo de la MFDB.
Current Entries	El número actual de entradas en la tabla de la base de datos de reenvío multicast.

Internet Group Management Protocol snooping

Internet Group Management Protocol (IGMP) snooping permite que un switch reenvíe tráfico multicast de forma inteligente. El tráfico IP multicast se destina a un grupo de hosts. Los grupos de hosts se identifican con direcciones IP de clase D, que van de 224.0.0.0 a 239.255.255.255. Con base en los mensajes IGMP de consulta y reporte, el switch reenvía tráfico solo a los puertos que solicitan el tráfico multicast. Esto evita que el switch difunda el tráfico a todos los puertos y posiblemente afecte el rendimiento de la red.

Una red Ethernet tradicional puede dividirse en distintos segmentos de red para evitar colocar demasiados dispositivos en el mismo medio compartido. Los puentes y switches conectan estos segmentos. Cuando se recibe un paquete con una dirección de destino broadcast o multicast, el switch reenvía una copia a cada uno de los demás segmentos de red de acuerdo con el estándar IEEE MAC Bridge. Finalmente, el paquete queda accesible para todos los nodos conectados a la red.

Este enfoque funciona bien para paquetes broadcast destinados a ser vistos o procesados por todos los nodos conectados. Sin embargo, en el caso de paquetes multicast, este enfoque podría hacer un uso menos eficiente del ancho de banda de la red, sobre todo cuando el paquete está destinado solo a unos pocos nodos. Los paquetes inundan segmentos de red donde ningún nodo los recibe. Aunque los nodos rara vez incurren en sobrecarga de procesamiento al filtrar paquetes dirigidos a direcciones de grupo no solicitadas, no pueden transmitir nuevos paquetes al medio compartido mientras el paquete multicast inunda la red. El problema del desperdicio de ancho de banda es aún peor cuando el segmento LAN no es compartido, por ejemplo, en enlaces full-duplex.

Permitir que los switches hagan snooping de paquetes IGMP es una solución creativa a este problema. El switch usa la información de los paquetes IGMP a medida que se reenvían por la red para determinar qué segmentos reciben paquetes dirigidos a la dirección de grupo.

Configurar IGMP snooping automáticamente con el modo IGMP Plus

El modo IGMP Plus le permite configurar automáticamente IGMP snooping, que se usa para crear listas de reenvío para el tráfico multicast IPv4.

También puede configurar IGMP snooping manualmente (consulte Configurar IGMP snooping manualmente en la página 255).

Para configurar IGMP snooping automáticamente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Configuration. Se muestra la página Configuration.

6. Seleccione el botón de opción IGMP Plus Mode Enable o Disable. Si está habilitado, los siguientes modos de IGMP snooping se habilitan automáticamente:

- Admin mode
- Proxy Querier mode
- Report Flood Mode
- Exclude Mrouter Interface Mode
- Fast Leave Auto-assignment Mode

El valor predeterminado es Enable.
Si está deshabilitado, estos modos de IGMP snooping se deshabilitan automáticamente.

Nota: Para obtener información sobre otros ajustes de la página, consulte Configurar IGMP snooping manualmente en la página 255.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

9. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 66. Información de configuración de IGMP snooping

Campo	Descripción
Multicast Control Frame Count	El número de tramas de control multicast que procesa el switch.
Interfaces Enabled for IGMP Snooping	Las interfaces en las que IGMP snooping está habilitado.
Operational Mode	Indica si IGMP snooping está habilitado o deshabilitado globalmente en el switch.
VLAN IDs Enabled For IGMP Snooping	Las VLAN en las que IGMP snooping está habilitado.

Configurar IGMP snooping manualmente

Puede configurar manualmente los ajustes de IGMP snooping, que se usa para crear listas de reenvío para el tráfico multicast IPv4.

También puede configurar IGMP snooping automáticamente (consulte Configurar IGMP snooping automáticamente con el modo IGMP Plus en la página 254).

Para configurar manualmente los ajustes de IGMP snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Configuration. Se muestra la página Configuration.

6. Seleccione el botón de opción Admin Mode Enable o Disable.
Esta selección habilita o deshabilita el modo administrativo de IGMP snooping del switch. El valor predeterminado es Disable.

7. Seleccione el botón de opción Validate IGMP IP header Enable o Disable. Esta selección habilita o deshabilita la validación de encabezados para todas las versiones de IGMP en el switch. Si está habilitado, el encabezado IP de un paquete IGMP valida la opción Router Alert, ToS y TTL. El valor predeterminado es Enable.

8. Seleccione el botón de opción Proxy Querier Mode Enable o Disable. Esta opción habilita o deshabilita el consultor proxy IGMP del switch. Si está deshabilitado, la consulta proxy IGMP con dirección IP de origen 0.0.0.0 no se envía en respuesta a un paquete IGMP leave. El valor predeterminado es Enable.

9. Seleccione el botón de opción Report Flood Mode Enable o Disable. Esta opción habilita o deshabilita el modo de inundación de informes en el switch. Si está habilitado, las PDU IGMP Join/Leave que el switch recibe de un host en un puerto descendente se reenvían a todos los demás puertos de la VLAN asociada. El valor predeterminado es Enable.

10. Seleccione el botón de opción Exclude Mrouter Interface Mode Enable o Disable. Esta opción especifica el tipo de información que se reenvía a la interfaz del router multicast ascendente.

Si está habilitado, el switch reenvía las PDU IGMP Join/Leave que recibe en un puerto descendente a una interfaz mrouter ascendente. Además, el switch reenvía un flujo de datos multicast a una interfaz mrouter ascendente solo si ese puerto ya recibió un mensaje de membresía IGMPv1 o IGMPv2. El switch descarta los flujos multicast desconocidos. El valor predeterminado es Enable.

Si está deshabilitado, el switch reenvía las PDU IGMP Join/Leave, los flujos multicast conocidos y los flujos multicast desconocidos a la interfaz mrouter ascendente.

11. Seleccione el botón de opción Fast Leave Auto-Assignment Mode Enable o Disable. Esta opción habilita o deshabilita la asignación automática de mensajes fast-leave a todos los puertos y LAG del switch. El valor predeterminado es Enable.

Nota: Para obtener información sobre el modo IGMP ~~Plus, consulte Configurar IGMP snooping automáticamente c~~on el modo IGMP Plus en la página 254.

12. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

14. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 67. Información de configuración de IGMP snooping

Campo	Descripción
Multicast Control Frame Count	El número de tramas de control multicast que procesa el switch.
Interfaces Enabled for IGMP Snooping	Las interfaces en las que IGMP snooping está habilitado.
Operational Mode	Indica si IGMP snooping está habilitado o deshabilitado globalmente en el switch.
VLAN IDs Enabled For IGMP Snooping	Las VLAN en las que IGMP snooping está habilitado.

Configurar los ajustes de IGMP snooping de las interfaces

Puede configurar los ajustes de IGMP snooping de las interfaces.

Para configurar los ajustes de IGMP snooping de las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Interface Configuration. Aparece la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, seleccione Disable o Enable.
Esta opción habilita o deshabilita el modo administrativo de IGMP snooping de la interfaz. El valor predeterminado es Disable.

9. En el campo Membership Interval, especifique el tiempo que el switch espera un informe de grupo antes de quitar la interfaz como miembro del grupo. Escriba un valor entre 1 y 3600 segundos. El valor predeterminado es 600 segundos.

10. En el campo Max Response Time, especifique el tiempo que el switch espera después de enviar una consulta en una interfaz por no haber recibido un informe de un grupo en esa interfaz.
Escriba un valor igual o mayor que 1, pero menor que el del campo Membership Interval. El valor predeterminado es 120 segundos.

11. En el campo Expiration Time, especifique el tiempo que el switch espera recibir una consulta en la interfaz antes de quitarla de la lista de interfaces con routers multicast conectados.
Escriba un valor de 0 a 3600 segundos. El valor predeterminado es 300 segundos. Si escribe 0, configura un tiempo de espera infinito (sin expiración).

12. En el menú Fast Leave, seleccione si desea habilitar o deshabilitar el modo fast leave de IGMP snooping en la interfaz. Esta opción habilita o deshabilita la asignación automática de mensajes fast-leave en la interfaz. El valor predeterminado es Disable. El campo Fast Leave Operational Mode muestra el estado de la interfaz.

13. En el menú Proxy Querier, seleccione si desea habilitar o deshabilitar el consultor proxy en la interfaz.

Si está deshabilitado, la consulta proxy IGMP con dirección IP de origen 0.0.0.0 no se envía en respuesta a un paquete IGMP leave. El valor predeterminado es Enable.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar IGMP snooping para VLAN automáticamente con el modo IGMP Plus

El modo IGMP Plus le permite configurar automáticamente IGMP snooping para VLAN, que se usa para crear listas de reenvío del tráfico multicast.

También puede configurar IGMP snooping para VLAN manualmente (consulte Configurar IGMP snooping manualmente en la página 255).

Para configurar IGMP snooping para VLAN automáticamente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration. Aparece la página IGMP VLAN Configuration.

6. Seleccione la casilla junto al VLAN ID.

7. En el menú IGMP Plus Mode, a la derecha de la página, seleccione si desea habilitar o deshabilitar el modo IGMP Plus en la VLAN.
Si está habilitado, los siguientes modos de IGMP snooping se habilitan automáticamente en la VLAN y ocurre lo siguiente:

- Admin mode
- Fast-Leave

- Proxy Querier
- Report Flood Mode
- Exclude Mrouter Interface Mode
- Se instalan en el sistema las direcciones MAC multicast reservadas.

Si está deshabilitado, estos modos de IGMP snooping se deshabilitan automáticamente en la VLAN.

Nota: Para obtener información sobre otros ajustes de la página, consulte Configurar IGMP snooping para VLAN manualmente en la página 260.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar IGMP snooping para VLAN manualmente

Puede configurar manualmente los ajustes de IGMP snooping para VLAN, que se usa para crear listas de reenvío del tráfico multicast.

También puede configurar IGMP snooping para VLAN automáticamente (consulte Configurar IGMP snooping para VLAN automáticamente con el modo IGMP Plus en la página 259).

Para configurar manualmente los ajustes de IGMP snooping de una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration. Aparece la página IGMP VLAN Configuration.

6. Seleccione la casilla junto al VLAN ID.

7. En el menú Admin Mode, seleccione si desea habilitar o deshabilitar IGMP snooping en la VLAN.
El valor predeterminado es Disable.

8. En el menú Fast Leave, seleccione si desea habilitar o deshabilitar el modo fast leave de IGMP snooping en la VLAN.
Esta opción habilita o deshabilita la asignación automática de mensajes fast-leave para todos los miembros de la VLAN. El valor predeterminado es Enable.

9. En el campo Membership Interval, escriba el intervalo de membresía de grupo de IGMP snooping para la VLAN.
El valor debe ser el del campo Maximum Response Time más un valor de 1 a 3600 segundos. El valor predeterminado es 600 segundos.

10. En el campo Maximum Response Time, escriba el tiempo máximo de respuesta de IGMP snooping para la VLAN.
El rango debe ser de 1 al valor del campo Group Membership Interval menos
1. El valor del campo Maximum Response Time debe ser mayor que el valor del campo Group Membership Interval. El valor predeterminado es 120 segundos.

11. En el campo Multicast Router Expiry Time, escriba el tiempo de expiración del router multicast de IGMP snooping para la VLAN.
El rango debe ser de 0 a 3600 segundos. El valor predeterminado es 300 segundos.

12. En el menú Report Suppression, seleccione si desea habilitar o deshabilitar el modo de supresión de informes de IGMP snooping en la VLAN.
Este modo permite suprimir los informes IGMP enviados por hosts multicast. Para ello, el switch crea una tabla de membresía de capa 3 y envía solo los informes esenciales a los routers IGMP que deben recibir el tráfico multicast. Como resultado, se reduce el tráfico de informes multicast enviado a los routers IGMP. El valor predeterminado es Disable.

13. En el menú Proxy Querier, seleccione si desea habilitar o deshabilitar el consultor proxy en la VLAN.
Si está deshabilitado, la consulta proxy IGMP con dirección IP de origen 0.0.0.0 no se envía en respuesta a un paquete IGMP leave. El valor predeterminado es Enable.

14. En el menú Report Flood Mode, seleccione si desea habilitar o deshabilitar el modo de inundación de informes en la VLAN.
Si está habilitado, las PDU IGMP Join/Leave que la VLAN recibe de un host en un puerto descendente se reenvían a todos los demás puertos de la VLAN. El valor predeterminado es Enable.

15. En el menú Exclude Mrouter Interface Mode, seleccione si desea habilitar o deshabilitar el Exclude Mrouter Interface Mode.

Esta opción especifica el tipo de información que se reenvía a la interfaz del router multicast ascendente:

• Enable. La VLAN reenvía las PDU IGMP Join/Leave que recibe en un puerto descendente a una interfaz mrouter ascendente. Además, la VLAN reenvía un flujo de datos multicast a una interfaz mrouter ascendente solo si ese puerto ya recibió un mensaje de membresía IGMPv1 o IGMPv2. La VLAN descarta los flujos multicast desconocidos. El valor predeterminado es Enable.
• Disable: La VLAN reenvía las PDU IGMP Join/Leave, los flujos multicast conocidos y los desconocidos a la interfaz mrouter ascendente.

Nota: Para obtener información sobre el modo IGMP Plus para VLAN, consulte Configurar IGMP snooping para VLAN automáticamente con el modo IGMP Plus en la página 259.

16. Haga clic en el botón
Apply. Se guardan los ajustes.

17. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

Configurar una interfaz de router multicast IGMP

Puede configurar una interfaz como la interfaz designada a la que está conectado un router multicast. Todos los paquetes IGMP detectados por el switch se reenvían al router multicast accesible desde esta interfaz. A esta interfaz la llamamos router multicast.

En la mayoría de los casos, esta configuración no es necesaria porque el switch detecta automáticamente un router multicast y reenvía los paquetes IGMP según corresponda. Puede ser necesaria en una red compleja si desea asegurarse de que el router multicast siempre reciba paquetes IGMP del switch.

Para configurar una interfaz de router multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Multicast Router Configuration. Aparece la página Multicast Router Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Multicast Router, seleccione si desea habilitar o deshabilitar la opción de router multicast.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar una VLAN de router multicast IGMP

Puede configurar una VLAN específica para una interfaz específica a fin de reenviar los paquetes IGMP detectados al router multicast conectado a la interfaz.

En la mayoría de los casos, esta configuración no es necesaria porque el switch detecta automáticamente un router multicast y reenvía los paquetes IGMP según corresponda. Puede ser necesaria en una red compleja si desea asegurarse de que el router multicast siempre reciba paquetes IGMP del switch.

Para configurar una VLAN de router multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration.
Aparece la página Multicast Router VLAN Configuration.

6. En el menú Interface, seleccione la interfaz.
7. En el campo VLAN ID, escriba el ID de VLAN.

8. En el menú Multicast Router, seleccione Enable o Disable para especificar si la VLAN es una VLAN de router multicast.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Descripción general del consultor de IGMP snooping

IGMP snooping requiere que un switch o router central consulte periódicamente a todos los dispositivos finales de la red para que anuncien sus membresías multicast. Este dispositivo central es el consultor IGMP (querier). Las respuestas a las consultas IGMP, llamadas informes IGMP, mantienen al switch actualizado con la membresía actual de los grupos multicast puerto por puerto. Si el switch no recibe información de membresía actualizada a tiempo, deja de reenviar multicast al puerto donde se encuentra el dispositivo final.

Puede configurar y mostrar información de los consultores de IGMP snooping en la red y, por separado, en las VLAN.

Configurar los ajustes globales del consultor de IGMP snooping

Puede configurar los ajustes globales de un consultor de IGMP snooping en el switch.

Para configurar los ajustes globales de un consultor de IGMP snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Querier Configuration. Aparece la página Querier Configuration.

6. Seleccione el botón de opción Querier Admin Mode Enable o Disable para especificar si IGMP snooping está habilitado en el switch.
El valor predeterminado es Disable.

7. En el campo Snooping Querier IP Address, especifique la dirección IP del consultor de snooping que se usará como dirección de origen en las consultas IGMP periódicas. Esta dirección se usa cuando no hay ninguna dirección configurada en la VLAN en la que se envían las consultas.

8. En el campo IGMP Version, especifique la versión del protocolo IGMP usada en las consultas IGMP periódicas.
La versión puede ser 1 o 2. El valor predeterminado es 2.

9. En el campo Query Interval (secs), especifique el tiempo en segundos entre las consultas periódicas enviadas por el consultor de snooping.
El rango es de 1 a 1800 segundos. El valor predeterminado es 60 segundos.

10. En el campo Querier Expiry Interval (secs), especifique el tiempo en segundos tras el cual se elimina la información del último consultor.
El rango es de 60 a 300 segundos. El valor predeterminado es 180 segundos.

11. Haga clic en el botón Apply.
Se guarda la configuración.

La página muestra los VLAN ID habilitados para el consultor de IGMP snooping.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar un consultor de IGMP snooping para una VLAN

Puede configurar un consultor IGMP para usarlo con una VLAN de la red.

Para configurar un consultor de IGMP snooping para una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Querier VLAN Configuration. Aparece la página Querier VLAN Configuration.

6. Especifique una VLAN nueva o cambie una VLAN existente:

- Especificar una VLAN nueva: En el campo VLAN ID, escriba el ID de la nueva VLAN.
- Cambiar una VLAN existente: Seleccione la casilla de una VLAN existente.

7. En el menú Querier Election Participate Mode, seleccione si desea habilitar o deshabilitar el modo de participación en la elección del consultor:

- Disabled. Si el switch detecta otro consultor de la misma versión en la VLAN, el consultor de snooping pasa al estado de no consultor.
- Enabled: El consultor de snooping participa en la elección, en la que la dirección IP más baja opera como consultor en esa VLAN. El otro consultor pasa al estado de no consultor.

De forma predeterminada, el modo de participación en la elección del consultor está habilitado en la VLAN 1.

8. En el campo Snooping Querier VLAN Address, especifique la dirección IP que se usará como dirección IP de origen en las consultas IGMP periódicas enviadas en la VLAN.

9. Agregue la nueva VLAN o guarde los ajustes de la VLAN existente:

- **Agregar la nueva VLAN: Haga clic en el botón Add.**
  Se agrega la VLAN.
- **Guardar los ajustes de la VLAN existente: Haga clic en el botón Apply. Se guardan los ajustes.**

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 68. Información de configuración de VLAN del consultor

Campo	Descripción
Operational State	El estado operativo del consultor de IGMP snooping en una VLAN: • Querier: El switch de snooping es el consultor en la VLAN. El switch envía consultas periódicas con un intervalo igual al intervalo de consulta configurado. Si el switch encuentra un mejor consultor en la VLAN, pasa al modo de no consultor. • Non-Querier: El switch de snooping está en modo de no consultor en la VLAN. Si vence el temporizador del intervalo de expiración del consultor, el switch pasa al modo de consultor. • Disabled: El consultor de snooping no está operativo en la VLAN. El consultor pasa al modo deshabilitado cuando IGMP snooping no está operativo en la VLAN o cuando no están configuradas ni la dirección del consultor ni la dirección de administración de red.
Operational Version	La versión operativa del protocolo IGMP del consultor.
Last Querier Address	La dirección IP del último consultor del que se detectó una consulta en la VLAN.
Last Querier Version	La versión del protocolo IGMP del último consultor del que se detectó una consulta en la VLAN.
Operational Max Response Time	El tiempo máximo de respuesta que se usará en las consultas enviadas por el consultor de snooping.

Eliminar los ajustes del consultor de IGMP snooping de una VLAN

Puede eliminar los ajustes del consultor de IGMP snooping de una VLAN.

Para eliminar los ajustes del consultor de IGMP snooping de una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping > Querier VLAN Configuration. Aparece la página Querier VLAN Configuration.

6. Seleccione la VLAN cuyos ajustes del consultor de IGMP snooping desea eliminar.

7. Haga clic en el botón Delete.
Se guardan los ajustes. (La VLAN en sí no se elimina.)

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar el estado del consultor de IGMP snooping

Puede mostrar el estado del consultor de IGMP snooping de una interfaz o una VLAN.

Para mostrar el estado del consultor de IGMP snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > IGMP Snooping Querier > IGMP Snooping Group Table.
Aparece la página IGMP Snooping Group Table.

6. Para mostrar información de una VLAN o interfaz específica, haga lo siguiente: a. En el menú Search, seleccione VLAN ID o interfaz. b. En el campo, escriba el VLAN ID o el número de interfaz. c. Haga clic en el botón GO.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 69. Información de grupos de IGMP snooping

Campo	Descripción
VLAN ID	El ID de la VLAN en la que el host envía solicitudes de unión IGMP.
Subscriber	La dirección IP y la dirección MAC del host que envía solicitudes de unión IGMP.
MC Group	La dirección IP multicast y la dirección MAC en las que está registrado el suscriptor.
Interface	La interfaz en la que se detectan las solicitudes de unión IGMP.
Type	La versión del protocolo IGMP.
Timeout (secs)	El momento en que expira la actualización más reciente de este host.

Multicast Listener Discovery snooping

En redes IPv6, Multicast Listener Discovery (MLD) snooping cumple una función similar a IGMP en redes IPv4. Con MLD snooping, los datos multicast IPv6 se reenvían selectivamente a los puertos configurados para recibirlos, en lugar de inundarse a todos los puertos de una VLAN. Los puertos se determinan detectando los paquetes de control multicast IPv6.

Un oyente multicast es un dispositivo configurado para recibir paquetes multicast IPv6. Los routers multicast IPv6 usan MLD para descubrir la presencia de oyentes multicast en sus enlaces directamente conectados y para descubrir qué paquetes multicast interesan a los dispositivos vecinos.

El protocolo MLD se deriva de IGMP. MLD versión 1 (MLDv1) equivale a IGMPv2, y MLD versión 2 (MLDv2) equivale a IGMPv3. MLD es un subprotocolo de Internet Control Message Protocol versión 6 (ICMPv6), y los mensajes MLD son un subconjunto de los mensajes ICMPv6, identificados en los paquetes IPv6 por un valor Next Header previo de 58.

Configurar MLD snooping automáticamente con el modo MLD Plus

El modo MLD Plus le permite configurar automáticamente MLD snooping, que se usa para crear listas de reenvío del tráfico multicast IPv6.

También puede configurar MLD snooping manualmente (consulte Configurar MLD snooping manualmente en la página 271).

Para configurar MLD snooping automáticamente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Configuration. Aparece la página Configuration.

6. Seleccione el botón de opción MLD Plus Mode Enable o Disable. Si está habilitado, los siguientes modos de MLD snooping se habilitan automáticamente:

- MLD Snooping Admin mode
- Exclude Mrouter Interface Mode

El valor predeterminado es Enable.
Si está deshabilitado, estos modos de MLD snooping se deshabilitan automáticamente.

Nota: Para obtener información sobre otros ajustes de la página, consulte Configurar MLD snooping manualmente en la página 271.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

9. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 70. Información de configuración de MLD snooping

Campo	Definición
Multicast Control Frame Count	El número de tramas de control multicast procesadas.
Interfaces Enabled for MLD Snooping	La interfaz en la que MLD snooping está habilitado administrativamente. MLD snooping debe estar habilitado globalmente y en la interfaz para que esta pueda detectar paquetes MLD y determinar qué segmentos deben recibir los paquetes multicast dirigidos a la dirección del grupo.
VLAN IDs Enabled For MLD Snooping	La VLAN en la que MLD snooping está habilitado administrativamente.

Configurar MLD snooping manualmente

Puede configurar manualmente los ajustes de MLD snooping, que se usa para crear listas de reenvío del tráfico multicast IPv6.

También puede configurar MLD snooping automáticamente (consulte Configurar MLD snooping automáticamente con el modo MLD Plus en la página 269).

Para configurar manualmente los ajustes de MLD snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Configuration. Aparece la página Configuration.

6. Seleccione el botón de opción MLD Snooping Admin Mode Enable o Disable para especificar el modo administrativo de MLD snooping en el switch. El valor predeterminado es Disable.

7. Seleccione el botón de opción Proxy Querier Mode Enable o Disable.

Esto habilita o deshabilita un consultor proxy MLD en el sistema. Si está deshabilitado, no se envía una consulta proxy MLD con IP de origen 0::0 en respuesta a un paquete MLD leave. Si está habilitado, se envían consultas proxy MLD. El valor predeterminado es Enable.

8. Seleccione el botón de opción Exclude Mrouter Interface Mode Enable o Disable.
Esta opción especifica el tipo de información que se reenvía a la interfaz del router multicast ascendente.

Si está habilitado, el switch bloquea todos los datos multicast desconocidos a través del puerto mrouter, ya sea que el puerto esté configurado de forma dinámica o estática. Solo las PDU MLD pueden pasar por el puerto mrouter hacia la interfaz del router ascendente.

El valor predeterminado es Enable. Si está deshabilitado, el switch reenvía tanto los datos multicast desconocidos como las PDU MLD a la interfaz del router multicast ascendente.

Nota: Para obtener información sobre el modo MLD Plus, consulte Configurar MLD snooping automáticamente con el modo MLD Plus en la página 269.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

11. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 71. Información de configuración de MLD snooping

Campo	Definición
Multicast Control Frame Count	El número de tramas de control multicast procesadas.
Interfaces Enabled for MLD Snooping	La interfaz en la que MLD snooping está habilitado administrativamente. MLD snooping debe estar habilitado globalmente y en la interfaz para que esta pueda detectar paquetes MLD y determinar qué segmentos deben recibir los paquetes multicast dirigidos a la dirección del grupo.
VLAN IDs Enabled For MLD Snooping	La VLAN en la que MLD snooping está habilitado administrativamente.

Configurar MLD snooping en las interfaces

Puede configurar los ajustes de MLD snooping en las interfaces.

Para configurar MLD snooping en las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Interface Configuration. Se muestra la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, habilite o deshabilite MLD snooping en la interfaz.
El valor predeterminado es Disable.

9. En el campo Membership Interval, especifique el tiempo que el switch debe esperar un informe de un grupo determinado en una interfaz determinada antes de eliminar esa interfaz del grupo.
El rango válido es de 2 a 3600 segundos. El valor configurado debe ser mayor que el tiempo máximo de respuesta. El valor predeterminado es 260 segundos.

10. En el campo Max Response Time, especifique el tiempo que el switch debe esperar tras enviar una consulta en una interfaz porque no recibió un informe de un grupo determinado en esa interfaz.
Introduzca un valor mayor o igual que 1 y menor que el intervalo de membresía en segundos. El valor predeterminado es 10 segundos. El valor configurado debe ser menor que el intervalo de membresía.

11. En el campo Expiration Time, especifique el tiempo que el switch debe esperar para recibir una consulta en una interfaz antes de quitarla de la lista de interfaces con routers multicast conectados.
Introduzca un valor entre 0 y 3600 segundos. El valor predeterminado es 300 segundos. Un valor de cero indica un tiempo de espera infinito, es decir, sin expiración.

12. En el menú Fast Leave, seleccione Enable o Disable para habilitar o deshabilitar Fast Leave en la interfaz.
Si Fast Leave está habilitado, la interfaz se puede quitar de inmediato de la tabla de reenvío de capa 2 cuando el switch recibe un mensaje MLD leave de un grupo multicast sin enviar primero consultas generales basadas en MAC. El valor predeterminado es Disable.

13. En el menú Proxy Querier Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo proxy querier en la interfaz.
Si el modo está deshabilitado, no se envía una consulta proxy MLD con IP de origen 0::0 en respuesta a un paquete MLD leave. Si está habilitado, se envían consultas proxy MLD. El valor predeterminado es Enable.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar MLD snooping en VLAN automáticamente con el modo MLD Plus

El modo MLD Plus permite configurar automáticamente MLD snooping en las VLAN, que se usa para crear listas de reenvío para el tráfico multicast IPv6.

También puede configurar MLD snooping en las VLAN manualmente (consulte Configurar IGMP snooping manualmente en la página 255).

Para configurar MLD snooping en las VLAN automáticamente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > MLD VLAN Configuration. Se muestra la página MLD VLAN Configuration.

6. Marque la casilla del VLAN ID en el que se debe habilitar MLD snooping.

7. En el menú MLD Plus Mode, habilite o deshabilite el modo MLD Plus en la VLAN.
Si se habilita, se activan automáticamente los siguientes modos de MLD snooping en la VLAN:

- Admin mode
- Fast-Leave
- Exclude Mrouter Interface Mode

Si se deshabilita, estos modos de MLD snooping se desactivan automáticamente en la VLAN.

Nota: Para obtener información sobre otros ajustes de la página, consulte Configurar MLD snooping en VLAN manualmente en la página 275.

8. Haga clic en Add para habilitar MLD Snooping en la VLAN especificada.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar MLD snooping en VLAN manualmente

Puede configurar manualmente los ajustes de MLD snooping en las VLAN, que se usa para crear listas de reenvío para el tráfico multicast IPv6.

También puede configurar MLD snooping en las VLAN automáticamente (consulte Configurar MLD snooping en VLAN automáticamente con el modo MLD Plus en la página 274).

Para configurar manualmente MLD snooping en una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > MLD VLAN Configuration. Se muestra la página MLD VLAN Configuration.

6. Especifique una VLAN nueva o cambie una VLAN existente:

- Especificar una VLAN nueva: En el campo VLAN ID, escriba el ID de la nueva VLAN.
- Cambiar una VLAN existente: Seleccione la casilla de una VLAN existente.

7. En el menú Fast Leave, habilite o deshabilite el modo Fast Leave de MLD snooping.

8. En el campo Membership Interval, especifique el intervalo de membresía de grupo de MLD snooping.
El rango va del valor especificado en el campo Maximum Response Time más 1 hasta 3600 segundos. El valor predeterminado es 260 segundos.

9. En el campo Maximum Response Time, especifique el tiempo máximo de respuesta de MLD snooping.
El rango va de 1 segundo al valor especificado en Membership Interval menos 1. El valor predeterminado es 10 segundos.

10. En el campo Multicast Router Expiry Time, especifique el tiempo de expiración del router multicast de MLD Snooping.
El rango es de 0 a 3600 segundos. El valor predeterminado es 300 segundos.

11. En el menú Proxy Querier Mode, habilite o deshabilite el modo proxy querier.
Si selecciona Disable, no se envía la consulta proxy MLD con IP de origen 0::0 en respuesta a un paquete MLD leave. El valor predeterminado es Enable.

12. En el menú Exclude Mrouter Interface Mode, habilite o deshabilite el modo de interfaz mrouter.
Esta opción especifica el tipo de información que se reenvía a la interfaz del router multicast ascendente.

Si se habilita, la interfaz bloquea todos los datos multicast desconocidos a través del puerto mrouter, ya sea que el puerto esté configurado de forma dinámica o estática. Solo las PDU MLD pueden pasar por el puerto mrouter hacia la interfaz del router ascendente.

El valor predeterminado es Enable. Si se deshabilita, la interfaz reenvía tanto los datos multicast desconocidos como las PDU MLD a la interfaz del router multicast ascendente.

Nota: Para obtener información sobre el modo MLD Plus en VLAN, consulte Configurar MLD snooping en VLAN automáticamente con el modo MLD Plus en la página 274.

13. Agregue la nueva VLAN o guarde la configuración de la VLAN existente:

• Agregar la nueva VLAN: Haga clic en el botón Add.
Se agrega la VLAN.
• Guardar los ajustes de la VLAN existente: Haga clic en el botón Apply. Se guardan los ajustes.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar la configuración del querier de MLD snooping de una VLAN

Puede eliminar la configuración del querier de MLD snooping de una VLAN.

Para eliminar la configuración del querier de MLD snooping de una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Querier VLAN Configuration. Se muestra la página Querier VLAN Configuration.

6. Seleccione la VLAN cuyos ajustes del consultor de IGMP snooping desea eliminar.

7. Haga clic en el botón Delete.
Se guardan los ajustes. (La VLAN en sí no se elimina.)

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz de router multicast MLD

Puede configurar una interfaz como la interfaz designada a la que se conecta un router multicast. Todos los paquetes MLD detectados por el switch se reenvían al router multicast accesible desde esta interfaz. A esta interfaz la llamamos router multicast.

En la mayoría de los casos, esta configuración no es necesaria porque el switch detecta automáticamente un router multicast y reenvía los paquetes MLD en consecuencia. Esta configuración puede ser necesaria en una red compleja si desea asegurarse de que el router multicast siempre reciba los paquetes MLD del switch.

Para configurar una interfaz de router multicast MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Multicast Router Configuration. Se muestra la página Multicast Router Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Multicast Router, seleccione si desea habilitar o deshabilitar la opción de router multicast.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar una VLAN de router multicast MLD

Puede configurar una VLAN específica para una interfaz específica a fin de reenviar los paquetes MLD detectados al router multicast conectado a la interfaz.

En la mayoría de los casos, esta configuración no es necesaria porque el switch detecta automáticamente un router multicast y reenvía los paquetes MLD en consecuencia. Esta configuración puede ser necesaria en una red compleja si desea asegurarse de que el router multicast siempre reciba los paquetes MLD del switch.

Para configurar una VLAN de router multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration.
Se muestra la página Multicast Router VLAN Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo VLAN ID, escriba el ID de VLAN.

8. En el menú Multicast Router, seleccione Enable o Disable para especificar si la VLAN es una VLAN de router multicast.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar los ajustes globales del querier de MLD snooping

Puede configurar los ajustes globales de un querier de MLD snooping en el switch.

Para configurar los ajustes globales de un querier de MLD snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Multicast > MLD Snooping > Querier Configuration. Se muestra la página Querier Configuration.

6. Seleccione el botón de opción Querier Admin Mode Enable o Disable para indicar si MLD snooping está habilitado en el switch.
El valor predeterminado es Disable.

7. En el campo Querier Address, especifique la dirección IP del querier de snooping que se usará como dirección de origen en las consultas MLD periódicas.
Esta dirección se usa cuando no hay ninguna dirección configurada en la VLAN en la que se envían las consultas. Los formatos IPv6 admitidos son x:x:x:x:x:x:x:x y x::x.

Nota: El campo MLDP Version siempre indica la versión 1 del protocolo MLD. Esta es la versión que se usa en las consultas MLD periódicas.

8. En el campo Query Interval (secs), especifique el tiempo en segundos entre las consultas periódicas que envía el querier de snooping.
El rango es de 1 a 1800 segundos. El valor predeterminado es 60 segundos.

9. En el campo Querier Expiry Interval (secs), especifique el tiempo en segundos tras el cual se elimina la información del último querier.
El rango es de 60 a 300 segundos. El valor predeterminado es 60 segundos.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

La página muestra los VLAN ID habilitados para el querier de MLD snooping.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar un querier de MLD snooping para una VLAN

Puede configurar un querier MLD para usarlo con una VLAN de la red.

Para configurar un querier de MLD snooping para una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching> Multicast > MLD Snooping > Querier VLAN Configuration. Se muestra la página Querier VLAN Configuration.

6. Especifique una VLAN nueva o cambie una VLAN existente:

- Especificar una nueva VLAN. En el campo VLAN ID, introduzca el ID de la nueva VLAN.
- Cambiar una VLAN existente. Marque la casilla de una VLAN existente.

7. En el menú Querier Election Participate Mode, seleccione si desea habilitar o deshabilitar el modo de participación en la elección del consultor:

• Disabled: Si el switch detecta otro querier de la misma versión en la VLAN, el querier de snooping pasa al estado non-querier.
• Enabled: El querier de snooping participa en la elección de querier, en la que la dirección IPv6 más baja funciona como querier en esa VLAN. El otro querier pasa al estado non-querier.

8. En el campo Querier VLAN Address, especifique la dirección IPv6 que se usará como dirección de origen en las consultas IGMP periódicas que se envían en la VLAN.

9. Agregue la nueva VLAN o guarde los ajustes de la VLAN existente:

• Agregar la nueva VLAN: Haga clic en el botón Add.
Se agrega la VLAN.
• Guardar los ajustes de la VLAN existente: Haga clic en el botón Apply. Se guardan los ajustes.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 72. Información de configuración de Querier VLAN

Campo	Descripción
Operational State	El estado operativo del querier de MLD snooping en una VLAN: • Querier: El switch de snooping es el querier de la VLAN. El switch envía consultas periódicas con un intervalo igual al intervalo de consulta configurado. Si el switch encuentra un querier mejor en la VLAN, pasa al modo non-querier. • Non-Querier: El switch de snooping está en modo non-querier en la VLAN. Si vence el temporizador del intervalo de expiración del querier, el switch pasa al modo querier. • Disabled: El querier de snooping no está operativo en la VLAN. El querier pasa al modo deshabilitado cuando MLD snooping no está operativo en la VLAN o cuando no está configurada la dirección del querier ni la dirección de administración de red.
Operational Version	La versión operativa del protocolo MLD del querier.
Last Querier Address	La dirección IP del último consultor del que se detectó una consulta en la VLAN.

Tabla 72. Información de configuración de Querier VLAN (continuación)

Campo	Descripción
Last Querier Version	La versión del protocolo MLD del último querier cuya consulta se detectó en la VLAN.
Operational Max Response Time	El tiempo máximo de respuesta que se usará en las consultas enviadas por el consultor de snooping.

Eliminar la configuración del querier de MLD snooping de una VLAN

Puede eliminar la configuración del querier de MLD snooping de una VLAN.

Para eliminar la configuración del querier de MLD snooping de una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching> Multicast > MLD Snooping > Querier VLAN Configuration. Se muestra la página Querier VLAN Configuration.

6. Seleccione la VLAN cuyos ajustes del consultor de IGMP snooping desea eliminar.

7. Haga clic en el botón Delete.
Se guardan los ajustes. (La VLAN en sí no se elimina.)

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Registro de VLAN multicast

IGMP y MLD snooping ayudan a limitar el tráfico multicast cuando los puertos miembro están en la misma VLAN. Sin embargo, cuando los puertos pertenecen a VLAN distintas, se envía una copia del flujo multicast a cada VLAN con puertos miembro del grupo multicast. El registro de VLAN

multicast (MVR) elimina la necesidad de duplicar el tráfico multicast cuando los puertos miembro del grupo multicast pertenecen a VLAN distintas.

MVR usa una VLAN multicast dedicada para reenviar el tráfico multicast en la red L2. Solo puede configurar una VLAN de origen multicast (MVLAN) en el switch. Esta MVLAN se usa solo para cierto tráfico multicast, como el de una aplicación IPTV, para evitar la duplicación de flujos multicast para clientes en VLAN distintas. Los clientes pueden unirse o salir de la MVLAN dinámicamente sin afectar su membresía en otras VLAN.

MVR, al igual que IGMP y MLD snooping, permite que un switch de capa 2 escuche los mensajes IGMP y MLD para conocer la membresía de los grupos multicast.

Puede configurar los ajustes globales, de grupo, de interfaz y de membresía de grupo.

Configurar los ajustes globales de MVR

Puede configurar los ajustes globales de MVR que se aplican al switch.

Para configurar los ajustes globales de MVR:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MVR > Basic > MVR Configuration. Se muestra la página MVR Configuration.

6. En el menú MVR Running, seleccione Enable o Disable para indicar si MVR está habilitado o deshabilitado globalmente en el switch.
El valor predeterminado es Disable.

7. En el campo MVR Multicast VLAN, especifique la VLAN en la que se reciben los datos multicast de MVR.
Todos los puertos de origen pertenecen a esta VLAN. El rango es de 1 a 4093. El valor predeterminado es 1.

8. En el campo MVR Global Query Response Time, establezca el tiempo que el switch debe esperar un informe de membresía de grupo IGMP de una interfaz antes de quitar la interfaz como miembro del grupo multicast.
Este tiempo solo se aplica a la eliminación de la interfaz del puerto receptor en el switch. Cuando se envía una consulta IGMP desde un puerto receptor, el switch espera el tiempo de consulta MVR predeterminado o configurado un informe de membresía IGMP antes de quitar la interfaz como miembro del grupo multicast. El tiempo se expresa en décimas de segundo. El rango es de 1 a 100 décimas. El valor predeterminado es 5 décimas, o medio segundo.

9. En el menú MVR Mode, seleccione compatible o dynamic para especificar el modo de funcionamiento de MVR.
Seleccione compatible (modo predeterminado) para bloquear los informes de membresía IGMP en los puertos de origen. Seleccione dynamic para permitir los informes de membresía IGMP en los puertos de origen.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 73. Información de configuración de MVR

Campo	Definición
MVR Max Multicast Groups	El número máximo de grupos multicast que admite MVR.
MVR Current Multicast Groups	El número de grupos MVR asignados.

Configurar un grupo MVR

Puede configurar un grupo MVR. Después de configurar interfaces para MVR, puede agregarlas como miembros del grupo MVR.

Para configurar un grupo MVR:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MVR > Advanced > MVR Group Configuration. Se muestra la página MVR Group Configuration.

6. En el campo MVR Group IP, especifique la dirección IP del nuevo grupo MVR.

7. En el campo Count, especifique el número de grupos MVR contiguos. Este número permite crear varios grupos MVR con un solo clic en el botón Add. Si el campo está vacío, al hacer clic en el botón se crea un solo grupo nuevo. El campo se muestra vacío para cada grupo. El rango es de 1 a 256.

8. Haga clic en el botón Add.
Se agrega el grupo MVR.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 74. Información de configuración de grupos MVR

Campo	Definición
Status	El estado del grupo MVR específico.
Members	La lista de interfaces que participan en el grupo MVR.

Eliminar un grupo MVR

Puede eliminar un grupo MVR que ya no necesite.

Para eliminar un grupo MVR:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MVR > Advanced > MVR Group Configuration. Se muestra la página MVR Group Configuration.

6. Marque la casilla del grupo MVR.

7. Haga clic en el botón Delete.
Se elimina el grupo MVR.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz MVR

Le recomendamos configurar primero una interfaz MVR antes de agregarla como miembro de un grupo MVR.

Para configurar una interfaz MVR:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MVR > Advanced > MVR Interface Configuration. Se muestra la página MVR Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.

• All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, indique si MVR está habilitado en la interfaz seleccionando Enable o Disable.
El valor predeterminado es Disable.

9. En el menú Type, indique si la interfaz es un receptor MVR o un origen MVR seleccionando receiver o source.
El tipo de puerto predeterminado es none.

10. En el menú Immediate Leave, indique si la función Immediate Leave está habilitada seleccionando Enable o Disable.
El valor predeterminado es Disable.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

13. Para actualizar la página, haga clic en el botón Refresh.
El campo Status muestra el estado de cada interfaz.

Configurar las interfaces miembro de un grupo MVR

Puede agregar o quitar interfaces como miembros de un grupo MVR.

Para configurar las interfaces miembro de un grupo MVR:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MVR > Advanced > MVR Group Membership. Se muestra la página MVR Group Membership.

6. En el menú Group IP, seleccione la dirección IP del grupo MVR.

7. En la tabla Ports, haga clic en cada puerto que desee hacer miembro del grupo MVR. Un puerto seleccionado se indica con una marca de verificación.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar las estadísticas de MVR

Puede mostrar las estadísticas de MVR del switch. Estas estadísticas están asociadas a IGMP.

Para mostrar las estadísticas de MVR:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MVR > Advanced > MVR Statistics. Se muestra la página MVR Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 75. Información de estadísticas de MVR

Campo	Definición
IGMP Query Received	El número de consultas IGMP recibidas.
IGMP Report V1 Received	El número de informes IGMP V1 recibidos.
IGMP Report V2 Received	El número de informes IGMP V2 recibidos.
IGMP Leave Received	El número de mensajes IGMP leave recibidos.
IGMP Query Transmitted	El número de consultas IGMP transmitidas.
IGMP Report V1 Transmitted	El número de informes IGMP V1 transmitidos.
IGMP Report V2 Transmitted	El número de informes IGMP V2 transmitidos.
IGMP Leave Transmitted	El número de mensajes IGMP leave transmitidos.
IGMP Packet Receive Failures	El número de fallas de recepción de paquetes IGMP.
IGMP Packet Transmit Failures	El número de fallas de transmisión de paquetes IGMP.

Tabla de direcciones MAC

Puede ver o configurar la tabla de direcciones MAC. Esta tabla contiene información sobre las entradas unicast para las que el switch guarda información de reenvío o filtrado. Esta información permite que la función de puenteo transparente determine cómo se debe propagar una trama entrante.

Ver, buscar o borrar la tabla de direcciones MAC

Si borra las entradas de la tabla de direcciones MAC, solo se eliminan las entradas dinámicas.

Para ver, buscar o borrar la tabla de direcciones MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Address Table > Basic > Address Table. Se muestra la página Address Table.

6. Use el menú y el campo Search para buscar una dirección MAC, un VLAN ID o un número de interfaz:

• Buscar por dirección MAC: En el menú Search, seleccione MAC Address e introduzca la dirección MAC hexadecimal de 6 bytes en grupos de dos dígitos separados por dos puntos, por ejemplo, 01:23:45:67:89:AB. Luego haga clic en el botón Go.
Si la dirección existe, esa entrada se muestra primero, seguida de las demás direcciones MAC (mayores). Se requiere una coincidencia exacta.
• Buscar por VLAN ID: En el menú Search, seleccione VLAN ID e introduzca el VLAN ID, por ejemplo, 100. Luego haga clic en el botón Go.
• Buscar por interfaz: En el menú Search, seleccione Port e introduzca el ID de interfaz con la convención de nombres correspondiente (por ejemplo, 0/2). Luego haga clic en el botón Go.

7. Para eliminar las entradas dinámicas de la tabla de direcciones MAC, haga clic en el botón Clear.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

9. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 76. Información de la tabla de direcciones MAC

Campo	Descripción
Total MAC Address	El número total de direcciones MAC aprendidas o configuradas.
MAC Address	La dirección MAC unicast para la que el switch guarda información de reenvío, de filtrado o ambas. El formato es una dirección MAC de 6 bytes separada por dos puntos, por ejemplo, 01:23:45:67:89:AB.
VLAN ID	El VLAN ID asociado a la dirección MAC.

Tabla 76. Información de la tabla de direcciones MAC (continuación)

Campo	Descripción
Port	La interfaz en la que se aprendió la dirección.
Estado	El estado de esta entrada: • Static: El switch o un usuario agregó la dirección MAC y no se puede volver a aprender. • Learned: La dirección MAC se aprendió y está en uso. • Management: La dirección MAC de administración.

Establecer el intervalo de envejecimiento de direcciones dinámicas

Puede establecer el intervalo de envejecimiento de direcciones de la base de datos de reenvío. Es el tiempo de espera en segundos para que caduque la información de reenvío aprendida dinámicamente.

Para establecer el intervalo de envejecimiento de direcciones dinámicas:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Switching > Address Table > Advanced > Dynamic Addresses. Se muestra la página Dynamic Addresses.

6. En el campo Address Aging Timeout (seconds), especifique el tiempo de espera en segundos para que caduque la información de reenvío aprendida dinámicamente.
El rango es de 10 a 1000000 segundos. El valor predeterminado es 3000 segundos.
7. Haga clic en el botón Apply.
La configuración se guarda.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Agregar una dirección MAC estática a la tabla de direcciones MAC

Las entradas de dirección MAC estática son las que agrega manualmente a la tabla de direcciones MAC para una interfaz y una VLAN específicas.

Para agregar una dirección MAC estática a la tabla de direcciones MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Address Table > Advanced > Static MAC Address. Se muestra la página Static MAC Address.

6. En el menú Interface, seleccione la interfaz o el LAG.
7. En el campo Static MAC Address, introduzca la dirección MAC.

8. En el menú VLAN ID, seleccione el ID de VLAN que se asociará con la dirección MAC.

9. Haga clic en el botón Add.
La dirección MAC estática se agrega a la tabla de direcciones MAC.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una dirección MAC estática de la tabla de direcciones MAC

Puede eliminar una dirección MAC estática que ya no necesite.

Para eliminar una dirección MAC estática de la tabla de direcciones MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Address Table > Advanced > Static MAC Address. Se muestra la página Static MAC Address.

6. En el menú Interface, seleccione la interfaz o el LAG.
7. Seleccione la casilla de la dirección MAC.

8. Haga clic en el botón Delete.
La dirección MAC estática se elimina de la tabla de direcciones MAC.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configuración de puertos

Para los puertos físicos y los LAG del switch, puede configurar y mostrar los ajustes, incluido el modo administrativo de un puerto o LAG (habilitado de forma predeterminada) y la velocidad de un puerto (detectada automáticamente de forma predeterminada), agregar descripciones, mostrar información de los transceptores opcionales que haya instalado y configurar los ajustes de link flap del puerto.

Configurar y mostrar la configuración de puertos

Puede configurar y mostrar la información del puerto físico del switch. Algunos ajustes que aplican a los puertos físicos no aplican a los LAG.

Nota: Si cambia la autonegociación, la velocidad o el modo dúplex de un puerto físico, el switch podría quedar inaccesible durante algunos segundos mientras se aplican los nuevos ajustes.

Para configurar y mostrar la configuración de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Ports > Port Configuration.
Se muestra la página Port Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú STP Mode, habilite o deshabilite el modo administrativo de Spanning Tree Protocol para el puerto o LAG.
El valor predeterminado es Enable.

9. En el menú Admin Mode, habilite o deshabilite el modo administrativo del puerto o LAG.
Para que el puerto o LAG participe en la red, debe seleccionar Enable. El valor predeterminado es Enable.

10. En el menú LACP Mode, habilite o deshabilite el modo administrativo de Link Aggregation Control Protocol para el puerto.
El modo debe estar habilitado para que el puerto participe en la agregación de enlaces. El valor predeterminado es Enable.

11. En el menú Autonegotiation, habilite o deshabilite el modo de autonegociación de velocidad del puerto.

El valor predeterminado es Enable.

12. Para cambiar la velocidad del puerto, en el menú Speed, seleccione una de las siguientes velocidades:

• Auto: La velocidad se establece mediante autonegociación. Es la configuración predeterminada.
• 100: La velocidad se limita a 100 Mbits/segundo.

Los caracteres delimitadores para establecer distintos valores de velocidad son la coma (,), el punto (.) y el espacio ( ). Para establecer la velocidad de autonegociación, el modo de autonegociación debe estar en Enable.

Nota: Puede establecer la velocidad de los puertos Ethernet. En los puertos SFP, la velocidad se detecta automáticamente y no se puede cambiar.

13. Para cambiar el modo dúplex del puerto, en el menú Duplex Mode, seleccione uno de los siguientes valores:

• Auto: El modo dúplex se establece mediante autonegociación. Es la configuración predeterminada.
• Full: La transmisión entre los dispositivos ocurre en ambos sentidos simultáneamente.
• Half: La transmisión entre los dispositivos ocurre en un solo sentido a la vez.

14. En el menú Link Trap, habilite o deshabilite el envío de un trap cuando cambie el estado del enlace del puerto o LAG.
Para puertos, el valor predeterminado es Enable. Para LAG, es Disable.

15. En el campo Frame Size, especifique el tamaño máximo de trama Ethernet que admite el puerto o LAG, incluidos el encabezado Ethernet, el CRC y la carga útil. El rango es de 1500 a 12270. El valor predeterminado es 9198.

16. En el campo Debounce Time, especifique el tiempo de espera de debounce del puerto o LAG. Especifique el tiempo como múltiplo de 100 milisegundos (msec) en el rango de 100 a 5000. El valor predeterminado es 0 segundos, lo que significa que el debounce está deshabilitado.

17. En el menú Flow Control, seleccione la configuración de control de flujo IEEE 802.3x para el puerto:

• Disable: Si los búferes del puerto se llenan, el switch no envía tramas de pausa y podría haber pérdida de datos. Es la configuración predeterminada.
• Symmetric: Si los búferes del puerto se llenan, el switch envía tramas de pausa para detener el tráfico.
El control de flujo ayuda a evitar la pérdida de datos cuando el puerto no puede procesar el número de tramas que se conmutan. Al habilitar el control de flujo, el switch puede enviar una trama de pausa para detener el tráfico en el puerto si la memoria usada por los paquetes del puerto supera un umbral preconfigurado, y responde a las solicitudes

de pausa de los dispositivos asociados. El puerto en pausa no reenvía paquetes durante el tiempo especificado en la trama de pausa. Cuando transcurre ese tiempo, o el uso vuelve a un umbral bajo especificado, el switch permite que el puerto vuelva a transmitir tramas. El switch también respeta las tramas de pausa entrantes deteniendo temporalmente la transmisión.
• Asymmetric: Si los búferes del puerto se llenan, el switch no envía tramas de pausa y podría haber pérdida de datos. Sin embargo, el switch sí respeta las tramas de pausa entrantes deteniendo temporalmente la transmisión.

18. En el campo Load Interval, especifique el intervalo de carga del puerto o LAG. Es el periodo cuyos datos se usan para calcular las estadísticas de carga. Introduzca el periodo en múltiplos de 30 segundos, de 30 a 600. El valor predeterminado es 300 segundos. Cuanto menor sea el intervalo, más precisa será la tasa instantánea de las estadísticas de carga.

19. Haga clic en el botón Apply.
Se guarda la configuración.

20. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 77. Información de configuración de puertos

Campo	Descripción
Media Type	El tipo de medio que admite el puerto.
Port Type	Para puertos normales, este campo es Normal. De lo contrario, los valores posibles son los siguientes: • Mirrored: El puerto es un puerto duplicado cuyo tráfico se copia al puerto de sondeo. • Probe: Use este puerto para supervisar un puerto duplicado. • Trunk Member: El puerto es miembro de un trunk de agregación de enlaces. Consulte las páginas de LAG para más información.
Physical Status	La velocidad y el modo dúplex del puerto.
Link Status	Indica si el enlace del puerto o LAG está activo o inactivo.
ifIndex	El ifIndex de la entrada de la tabla de interfaces asociada al puerto o LAG.

Agregar descripciones de puertos, LAG y VLAN

Puede agregar una descripción a un puerto, LAG y VLAN.

Para agregar descripciones de puertos, LAG y VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Ports > Port Description.
Se muestra la página Port Description.

6. Elija si desea mostrar interfaces físicas, VLAN, LAG o todo haciendo clic en uno de los siguientes enlaces sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas, las VLAN y los LAG.

7. Seleccione una o más interfaces o VLAN mediante una de las siguientes acciones:

- Para configurar una sola interfaz o VLAN, seleccione su casilla o escriba el número de interfaz o VLAN en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces o VLAN con la misma configuración, seleccione la casilla de cada interfaz o VLAN.
- Para configurar todas las interfaces, VLAN o ambas con la misma configuración, seleccione la casilla de la fila de encabezado.

8. En el campo Description, introduzca una descripción de hasta 64 caracteres.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 78. Información de descripción de puertos

Campo	Descripción
MAC Address	La dirección MAC de la interfaz o VLAN.
PortList Bit Offset	El valor de desplazamiento de bit que corresponde a la interfaz o VLAN cuando se usa el tipo de objeto MIB PortList para la administración por SNMP.
ifIndex	El índice de interfaz asociado a la interfaz o VLAN.

Mostrar la información de los módulos transceptores

Para permitir conexiones de fibra de alta velocidad y Gigabit Ethernet de corta y larga distancia en el switch, los puertos de fibra SFP y SFP+ admiten módulos transceptores estándar 1G SFP y 10G SFP+. Puede ver la información de los módulos transceptores de todos los puertos de fibra del switch.

Para ver la información de los módulos transceptores:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Ports > Port Transceiver.
Se muestra la página Port Transceiver.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 79. Información de transceptores de puertos

Campo	Descripción
Port	El puerto en el que está instalado el módulo transceptor.
Vendor Name	El nombre del fabricante del módulo transceptor.
Link Length 50 µm [m]	La longitud de enlace admitida para fibra de 50 µm.
Link Length 62, 5 µm [m]	La longitud de enlace admitida para fibra de 62, 5 µm.
Serial Number	El número de serie del módulo transceptor.
Part Number	El número de parte del módulo transceptor.
Nominal Bit Rate [Mpbs]	La velocidad de señalización nominal del módulo transceptor.
Revision	La revisión del fabricante del módulo transceptor.
Compliance	La conformidad del módulo transceptor.
Supported	Indica si el módulo transceptor insertado es compatible (Yes o No).
Possible Speed Detected	La velocidad potencial que admite el módulo transceptor.

Configurar los ajustes de link flap del puerto

Puede configurar los ajustes de link flap del puerto, que determinan cuándo un puerto pasa automáticamente al estado deshabilitado. También puede configurar la recuperación automática, que permite que un puerto se vuelva a activar automáticamente.

Para configurar los ajustes de link flap del puerto:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > Ports > Link Flap Configuration.
Se muestra la página Link Flap Configuration.

6. Seleccione el botón de opción Admin Mode Enable o Disable para habilitar o deshabilitar el modo administrativo de link flap.
Para poder configurar los ajustes de link flap, debe seleccionar Enable. El valor predeterminado es Disable.

7. En el campo Max-Count, introduzca el número máximo de flaps permitidos antes de que el puerto pase al estado deshabilitado.
Puede introducir un número de 2 a 10. El valor predeterminado es 5.

8. En el campo Duration, introduzca el periodo máximo en segundos durante el cual se cuenta el número de link flaps.
Si el número de link flaps del puerto es mayor o igual al número que introdujo en el campo Max-Count, el puerto pasa al estado deshabilitado. De forma predeterminada, el periodo es de 10 segundos. Puede introducir un periodo de 3 a 200 segundos.

9. Seleccione el botón de opción Auto-Recovery Admin Mode Enable o Disable para habilitar o deshabilitar el modo administrativo de recuperación automática.
Para habilitar la recuperación automática, debe seleccionar Enable. Si está habilitada, el puerto sale automáticamente del estado deshabilitado al cumplirse el intervalo. El valor predeterminado es Disable.

10. En el campo Auto-Recovery Interval, introduzca el periodo en segundos tras el cual el puerto sale automáticamente del estado deshabilitado.
Puede introducir un periodo de 30 a 8640 segundos. El valor predeterminado es 300 segundos.

11. Haga clic en el botón Apply.
Se guarda la configuración.

La sección D-Disabled Ports due to Link Flap muestra los puertos que están en estado deshabilitado.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Grupos de agregación de enlaces

Los grupos de agregación de enlaces (LAG), también llamados port channels, le permiten combinar varios enlaces Ethernet full-duplex en un solo enlace lógico. Los dispositivos de red tratan la agregación como si fuera un solo enlace, lo que aumenta la tolerancia a fallas y

permite compartir la carga. La pertenencia a VLAN del LAG se asigna después de crearlo. De forma predeterminada, el LAG pasa a ser miembro de la VLAN de administración.

Una interfaz LAG puede ser estática o dinámica, pero no ambas. Todos los miembros de un LAG deben participar en los mismos protocolos. Una interfaz port-channel estática no requiere un sistema asociado para poder agregar sus puertos miembro.

El switch admite LAG estáticos. Cuando un puerto se agrega como miembro estático de un LAG, el puerto no transmite ni recibe LACPDU.

Descripción general de Auto-LAG

Un Auto-LAG es un LAG que se forma automáticamente entre dos dispositivos que admiten la función Auto-LAG. Un Auto-LAG es un LAG dinámico de capa 2 basado en el protocolo Link Aggregation Control Protocol (LACP).

Nota: Un LAG también se conoce como port channel o EtherChannel.

El switch puede detectar los enlaces físicos con un dispositivo asociado y configurar automáticamente un LAG (es decir, un Auto-LAG) en puertos interconectados y compatibles en ambos extremos. El switch solo puede formar un Auto-LAG con cada dispositivo asociado.

La función Auto-LAG funciona junto con la función Auto-Trunk, que también debe ser compatible y estar habilitada en el dispositivo asociado con el que se forma el LAG. Una vez formado un Auto-LAG, el switch aplica automáticamente el modo trunk (es decir, un Auto-Trunk) al LAG en ambos extremos. Es decir, tras formarse un Auto-LAG, el modo de los puertos que participan en él cambia del modo de puerto predeterminado al modo de puerto trunk. Para más información sobre la función Auto-Trunk, consulte Descripción general de Auto-Trunk en la página 194.

Para que el switch forme un Auto-LAG con un dispositivo asociado, se requiere lo siguiente:

- Las funciones Auto-LAG y Auto-Trunk deben ser compatibles y estar habilitadas globalmente en el switch y en el dispositivo asociado. (En todos los modelos de switch M4250, las funciones Auto-LAG y Auto-Trunk están habilitadas de forma predeterminada).
- Deben establecerse al menos dos enlaces entre el switch y el dispositivo asociado, y estos enlaces deben admitir la misma velocidad y el mismo modo dúplex.
- Los enlaces no pueden ser miembros de un LAG estático o dinámico configurado manualmente.
- LLDP debe estar habilitado en los puertos interconectados del switch y del dispositivo asociado. (En todos los modelos de switch M4250, LLDP está habilitado de forma predeterminada en todos los puertos).
- Los puertos interconectados del switch y del dispositivo asociado deben estar en el modo de puerto predeterminado, que es el modo General. Si los puertos están en modo Access o ya en modo Trunk, no se puede formar un Auto-Trunk en el Auto-LAG.

Un Auto-LAG puede formarse con hasta ocho interfaces como miembros. Las interfaces se seleccionan automáticamente para el Auto-LAG según si están activas y disponibles y según las siguientes condiciones:

- La interfaz no está ya configurada manualmente como miembro de un LAG.
- La interfaz no está configurada manualmente como puerto troncal ni como puerto de acceso. Es decir, la interfaz debe ser una interfaz general.

Nota: El switch admite varios LAG estáticos y dinámicos, pero con cada dispositivo asociado, el switch solo admite un Auto-LAG.

Habilitar o deshabilitar Auto-LAGs

De forma predeterminada, la función Auto-LAG está habilitada globalmente, pero puede deshabilitarla globalmente.

Para habilitar o deshabilitar Auto-LAGs:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Switching > LAG > LAG Configuration.
Se muestra la página LAG Configuration.

6. En la sección LAG Global Configuration, seleccione el botón de opción Auto-LAG Admin Mode Enable o Disable.
De forma predeterminada, la función Auto-LAG está habilitada globalmente.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el modo de hash de Auto-LAGs

De forma predeterminada, la función Auto-LAG está habilitada y usa un modo de hash que configura automáticamente un LAG según la dirección MAC de destino, la VLAN, el EtherType y el puerto de entrada del paquete (es decir, el modo de hash llamado 2 Dest MAC, VLAN, EType, incoming port). Puede cambiar el modo de hash (es decir, el modo de balanceo de carga) de la función Auto-LAG.

El switch balancea el tráfico en un LAG seleccionando uno de los enlaces del canal por el que deben transmitirse los paquetes. El switch selecciona el enlace creando un patrón binario a partir de campos seleccionados de un paquete y asociando ese patrón con un enlace específico. El modo hash determina qué campos del paquete selecciona el switch.

Para cambiar el modo hash de los Auto-LAGs:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > LAG > LAG Configuration.
Se muestra la página LAG Configuration.

6. En la sección LAG Global Configuration, en el menú Auto-LAG Global Hash Mode, seleccione el modo de hash para los Auto-LAGs:

- 1 Src MAC, VLAN, EType, incoming port: Dirección MAC de origen, VLAN, EtherType y puerto de entrada asociados al paquete.
- 2 Dest MAC, VLAN, EType, incoming port: Dirección MAC de destino, VLAN, EtherType y puerto de entrada asociados al paquete. Es el modo predeterminado.
- 3 Src/Dest MAC, VLAN, EType, incoming port: Direcciones MAC de origen y destino, VLAN, EtherType y puerto de entrada asociados al paquete.
- 4 Src IP and Src TCP/UDP Port fields: Campos de dirección IP de origen y puerto TCP/UDP de origen del paquete.
- 5 Dest IP and Dest TCP/UDP Port fields: Campos de dirección IP de destino y puerto TCP/UDP de destino del paquete.

• 6 Src/Dest IP and TCP/UDP Port fields: Campos de direcciones IP de origen y destino y de puertos TCP/UDP de origen y destino del paquete.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de LAG

Puede agrupar uno o más enlaces Ethernet full-duplex para agregarlos y formar un grupo de agregación de enlaces, también llamado port-channel. El switch trata el LAG como si fuera un solo enlace.

Para configurar los ajustes de LAG:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > LAG > LAG Configuration.
Se muestra la página LAG Configuration.

6. Para cambiar el nombre predeterminado del LAG, en el campo LAG Name, introduzca el nombre que se asignará al LAG.
De forma predeterminada, los nombres son ch1, ch2, ch3, etc. Puede introducir un nombre de hasta 15 caracteres.

Para información sobre cómo agregar un nombre en el campo Description, consulte Agregar descripciones de puertos, LAG y VLAN en la página 297 o Configurar un solo LAG y sus miembros en la página 307.

7. En el menú Admin Mode, habilite o deshabilite el LAG. Cuando el LAG está deshabilitado, no fluye tráfico y se descartan las LACPDU, pero los enlaces que forman el LAG no se liberan. El valor predeterminado es Enable.

8. En el menú Hash Mode, seleccione el modo de hash (es decir, el modo de balanceo de carga) para el LAG:

- 1 Src MAC, VLAN, EType, incoming port: Dirección MAC de origen, VLAN, EtherType y puerto de entrada asociados al paquete.
- 2 Dest MAC, VLAN, EType, incoming port: Dirección MAC de destino, VLAN, EtherType y puerto de entrada asociados al paquete. Es el modo predeterminado.
- 3 Src/Dest MAC, VLAN, EType, incoming port: Direcciones MAC de origen y destino, VLAN, EtherType y puerto de entrada asociados al paquete.
- 4 Src IP and Src TCP/UDP Port fields: Campos de dirección IP de origen y puerto TCP/UDP de origen del paquete.
- 5 Dest IP and Dest TCP/UDP Port fields: Campos de dirección IP de destino y puerto TCP/UDP de destino del paquete.
- 6 Src/Dest IP and TCP/UDP Port fields: Campos de direcciones IP de origen y destino y de puertos TCP/UDP de origen y destino del paquete.

Nota: El switch balancea el tráfico de un LAG seleccionando uno de los enlaces del canal por el que se transmitirán los paquetes. El switch selecciona el enlace creando un patrón binario a partir de campos seleccionados del paquete y asociando ese patrón a un enlace concreto. El modo de hash determina qué campos del paquete selecciona el switch.

9. En el menú STP Mode, habilite o deshabilite el modo administrativo de Spanning Tree Protocol (STP) para el LAG.
El valor predeterminado es Enable.

10. En el menú Static Mode, habilite o deshabilite el LAG como LAG estático. Con el modo estático habilitado, el LAG no transmite ni procesa LACPDU entrantes. Es decir, un puerto miembro del LAG no transmite LACPDU, y las LACPDU que recibe se descartan. El valor predeterminado es Disable.

11. En el menú Link Trap, habilite o deshabilite el envío de un trap cuando cambie el estado del enlace del LAG.
El valor predeterminado es Enable, que permite enviar un trap.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 80. Información de configuración de LAG

Campo	Descripción
LAG Description	La descripción que haya agregado al LAG (consulte Agregar descripciones de puertos, LAG y VLAN en la página 297 o Configurar un solo LAG y sus miembros en la página 307).
LAG ID	El ID del LAG.
Configured Ports	Las interfaces que son miembros del LAG.
Down Ports	Las interfaces que son miembros del LAG pero están inactivas.
LAG State	Indica si el enlace del LAG está activo o inactivo.
Automatic LAG	Indica si el LAG se creó manualmente (No) o automáticamente (Yes).

Configurar un solo LAG y sus miembros

Puede configurar un solo LAG y agregarle interfaces físicas como miembros.

La información sobre la configuración del LAG es idéntica a la de Configurar los ajustes de LAG en la página 305, pero la información sobre cómo agregar miembros al LAG es exclusiva de la siguiente sección.

Para configurar un solo LAG y sus miembros:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > LAG > LAG Membership.
Se muestra la página LAG Membership.

6. En el menú LAG ID, seleccione el LAG.

7. Para cambiar el nombre predeterminado del LAG, en el campo LAG Name, introduzca el nombre que se asignará al LAG.
De forma predeterminada, los nombres son ch1, ch2, ch3, etc. Puede introducir un nombre de hasta 15 caracteres.

8. Para introducir una descripción del LAG, en el campo LAG Description, escriba una descripción de hasta 64 caracteres.

9. En el menú Admin Mode, habilite o deshabilite el LAG. Cuando el LAG está deshabilitado, no fluye tráfico y se descartan las LACPDU, pero los enlaces que forman el LAG no se liberan. El valor predeterminado es Enable.

10. En el menú Link Trap, habilite o deshabilite el envío de un trap cuando cambie el estado del enlace del LAG.
El valor predeterminado es Enable, que permite enviar un trap.

11. En el menú STP Mode, habilite o deshabilite el modo administrativo de Spanning Tree Protocol (STP) para el LAG.
El valor predeterminado es Enable.

12. En el menú Static Mode, seleccione si habilita o deshabilita el LAG como LAG estático. Con el modo estático habilitado, el LAG no transmite ni procesa LACPDU entrantes. Es decir, un puerto miembro del LAG no transmite LACPDU y descarta las LACPDU que recibe. El valor predeterminado es Disable.

13. En el menú Hash Mode, seleccione el modo de balanceo de carga del LAG:

- Src MAC, VLAN, EType, incoming port: dirección MAC de origen, VLAN, EtherType y puerto de entrada asociados con el paquete.
- Dest MAC, VLAN, EType, incoming port: dirección MAC de destino, VLAN, EtherType y puerto de entrada asociados con el paquete. Es el modo predeterminado.
- Src/Dest MAC, VLAN, EType, incoming port: direcciones MAC de origen y destino, VLAN, EtherType y puerto de entrada asociados con el paquete.
- Src IP and Src TCP/UDP Port fields: campos de dirección IP de origen y puerto TCP/UDP de origen del paquete.
- Dest IP and Dest TCP/UDP Port fields: campos de dirección IP de destino y puerto TCP/UDP de destino del paquete.
- Src/Dest IP and TCP/UDP Port fields: campos de direcciones IP de origen y destino y de puertos TCP/UDP de origen y destino del paquete.

Nota: El switch balancea el tráfico de un LAG seleccionando uno de los enlaces del canal por el que deben transmitirse los paquetes. El switch selecciona el enlace creando un patrón binario a partir de campos seleccionados del paquete y asociando ese patrón a un enlace determinado.

14. En la tabla Ports, haga clic en cada puerto que desea hacer miembro del LAG.

15. Haga clic en el botón Apply.
Se guarda la configuración.

16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Temporización y sincronización 802.1AS

La temporización y sincronización 802.1AS es una función de audio video bridging (AVB). La función 802.1AS requiere una licencia. Para comprar una licencia, comuníquese con NETGEAR o con su distribuidor local de NETGEAR.

El estándar IEEE 802.1AS especifica el protocolo y los procedimientos usados para garantizar los requisitos de QoS en aplicaciones sensibles al tiempo, como audio y video.

El Precision Time Protocol (PTP) IEEE 1588 es la base del estándar IEEE 802.1AS. PTP especifica un protocolo de sincronización de reloj preciso basado en paquetes con marca de tiempo. Para configurar PTP, consulte Precision Time Protocol en la página 79.

El protocolo PTP se aplica a sistemas distribuidos formados por uno o más nodos que se comunican a través de medios de comunicación. La información de tiempo síncrono se distribuye de forma jerárquica, con un reloj grandmaster en la raíz de la jerarquía. El grandmaster proporciona una referencia de tiempo común y precisa a uno o más dispositivos conectados directamente mediante el intercambio periódico de información de temporización. Es decir, todos los dispositivos sincronizan sus relojes con el reloj grandmaster. A su vez, los dispositivos pueden actuar como maestros para otras capas jerárquicas de dispositivos.

Configurar y ver los ajustes globales de 802.1AS

Puede habilitar 802.1AS globalmente en el switch y configurar las prioridades del reloj local. La función 802.1AS calcula el retardo entre dispositivos de un enlace y mantiene una vista precisa del reloj de la red.

Para configurar y ver los ajustes globales de 802.1AS en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > 802.1AS > Basic > 802.1AS Configuration. Se muestra la página 802.1AS Configuration.

6. Para habilitar la función, seleccione el botón de opción Enable de 802.1AS status.

7. En el campo Local Clock Priority1, especifique el primer valor de prioridad del reloj local. El reloj local es el reloj del switch como puente sensible al tiempo. Introduzca un número de 0 a 255 segundos. El valor predeterminado es 255 segundos.

8. En el campo Local Clock Priority2, especifique el segundo valor de prioridad del reloj local. Introduzca un número de 0 a 255 segundos. El valor predeterminado es 248 segundos.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 81. Información de configuración de 802.1AS

Campo	Descripción
GrandMaster Capable	Indica si el reloj grandmaster está activo. El valor predeterminado es False.
Best Clock Identity	Dirección MAC del mejor reloj detectado por el switch.
Best Clock Priority1	Primer valor de prioridad del mejor reloj detectado por el switch.
Best Clock Priority2	Segundo valor de prioridad del mejor reloj detectado por el switch.
Steps to Best Clock	Número de enlaces entre el mejor reloj y el switch. Si el propio switch es el mejor reloj, el valor es cero.
Local Clock Identity	Dirección MAC del reloj local del switch.

Tabla 81. Información de configuración de 802.1AS (continuación)

Campo	Descripción
GM Change Count	Número de veces que cambió el reloj grandmaster.
Last GM Change Timestamp	Momento en que ocurrió el cambio más reciente de reloj grandmaster.

Configurar 802.1AS en interfaces

Puede configurar 802.1AS para interfaces individuales.

Para configurar 802.1AS en interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > 802.1AS > Advanced > 802.1AS Port Settings. Se muestra la página 802.1AS Port Settings.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, seleccione Enable o Disable.
Para que la configuración de 802.1AS surta efecto en la interfaz, seleccione Enable. El valor predeterminado es Disable.

9. En el campo Pdelay Threshold, especifique el umbral de retardo de propagación de la interfaz.
El umbral determina si el puerto puede participar en el protocolo 802.1AS. Si el retardo de propagación de la interfaz supera el umbral configurado, se considera que la interfaz no puede participar en el protocolo 802.1AS. El retardo del par debe ser menor que el umbral configurado en la interfaz. El rango es de 0 a 1,000,000,000 nanosegundos (ns). El valor predeterminado es 2500 ns.

10. En el campo Allowed Lost Responses, especifique el valor de respuestas perdidas permitidas. Si la interfaz no recibe respuestas válidas a mensajes PDELAY_REQ por encima de este valor, se considera que el puerto no está intercambiando mensajes de retardo con su vecino. El rango es de 0 a 65,535. El valor predeterminado es 3.

11. En el campo Initial Sync Interval, especifique la tasa de transmisión de mensajes SYNC. Este valor es el logaritmo en base 2 del intervalo medio entre mensajes SYNC sucesivos enviados en esta interfaz. El intervalo inicial configurado pasa a ser el intervalo actual solo después de inicializar o reinicializar el puerto para operar con 802.1AS. El rango es de –5 a 5. El valor predeterminado es –3.

12. En el campo Initial Pdelay Interval, especifique la tasa de transmisión de mensajes PDELAY_REQ.
Este valor es el logaritmo en base 2 del intervalo medio entre mensajes PDELAY_REQ sucesivos enviados en esta interfaz. El intervalo inicial configurado pasa a ser el intervalo actual solo después de inicializar o reinicializar el puerto para operar con 802.1AS. El rango es de –5 a 5. El valor predeterminado es –3.

13. En el campo Initial Announce Interval, especifique la tasa de transmisión de mensajes ANNOUNCE.
Este valor es el logaritmo en base 2 del intervalo medio entre mensajes ANNOUNCE sucesivos enviados en esta interfaz. El intervalo inicial configurado pasa a ser el intervalo actual solo después de inicializar o reinicializar el puerto para operar con 802.1AS. El rango es de –5 a 5. El valor predeterminado es –3.

14. En el campo SyncRx Timeout, especifique el número de intervalos SYNC. Este valor define cuántos intervalos SYNC deben transcurrir sin recibir información SYNC antes de que el switch detecte que el reloj maestro ya no transmite.

15. En el campo AnnounceRx Timeout, especifique el número de intervalos ANNOUNCE.

Este valor define cuántos intervalos ANNOUNCE deben transcurrir sin recibir una PDU ANNOUNCE antes de que el switch detecte que el reloj maestro ya no transmite.

16. Haga clic en el botón
Apply. Se guardan los ajustes.

17. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 82. Información de 802.1AS en interfaces

Campo	Descripción
Port Role	Rol 802.1AS de la interfaz. Los roles posibles son: • Disabled (predeterminado) • Master • Slave • Passive
Propagation Delay	Retardo medio de propagación en la interfaz.
Measuring Pdelay	Indica si la interfaz recibe mensajes de respuesta PDELAY del otro extremo del enlace.
802.1AS Capable	Indica si la interfaz es compatible con 802.1AS. De forma predeterminada, la interfaz no es compatible con 802.1AS.
Neighbor Rate Ratio	Relación estimada entre la frecuencia del reloj local del dispositivo sensible al tiempo en el otro extremo del enlace de la interfaz y la frecuencia del reloj local del switch.
Current Sync Interval	Intervalo medio actual entre mensajes SYNC sucesivos enviados por el enlace, en formato de logaritmo en base 2.
Current Pdelay Interval	Intervalo medio actual entre mensajes PDELAY_REQ sucesivos enviados por el enlace, en formato de logaritmo en base 2.
Current Announce Interval	Intervalo medio actual entre mensajes ANNOUNCE sucesivos enviados por el enlace, en formato de logaritmo en base 2.

Ver las estadísticas de 802.1AS

Puede ver las estadísticas de 802.1AS de las interfaces.

Para ver las estadísticas de 802.1AS de las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > 802.1AS > Advanced > 802.1AS Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 83. Información de estadísticas de 802.1AS

Campo	Descripción
Interface	La interfaz cuya información se muestra.
Sync Tx	Número total de paquetes SYNC transmitidos sin errores.
Sync Rx	Número total de paquetes SYNC recibidos sin errores.
Followup Tx	Número total de paquetes FOLLOWUP transmitidos sin errores.
Followup Rx	Número total de paquetes FOLLOWUP recibidos sin errores.
Announce Tx	Número total de paquetes ANNOUNCE transmitidos sin errores.
Announce Rx	Número total de paquetes ANNOUNCE recibidos sin errores.
Pdelay Req Tx	Número total de paquetes PDELAY_REQ transmitidos sin errores.

Tabla 83. Información de estadísticas de 802.1AS (continuación)

Campo	Descripción
Pdelay Req Rx	Número total de paquetes PDELAY_REQ recibidos sin errores.
Pdelay Resp Tx	Número total de paquetes PDELAY_RESP transmitidos sin errores.
Pdelay Resp Rx	Número total de paquetes PDELAY_RESP recibidos sin errores.
Pdelay Resp Followup Tx	Número total de paquetes PDELAY_RESP_FOLLOWUP transmitidos sin errores.
Pdelay Resp Followup Rx	Número total de paquetes PDELAY_RESP_FOLLOWUP recibidos sin errores.
Signaling Tx	Número total de paquetes SIGNALING transmitidos sin errores.
Signaling Rx	Número total de paquetes SIGNALING recibidos sin errores.
Sync Timeouts	Número total de tiempos de espera agotados en la recepción de SYNC.
Sync Discards	Número total de paquetes SYNC descartados.
Announce Timeouts	Número total de tiempos de espera agotados en la recepción de ANNOUNCE.
Announce Discards	Número total de paquetes ANNOUNCE descartados.
Pdelay Timeouts	Número total de tiempos de espera agotados en la recepción de PDELAY.
Pdelay Discards	Número total de paquetes PDELAY descartados.
Bad Headers	Número total de paquetes recibidos con encabezado incorrecto.

Configuración de Multiple Registration Protocol y 802.1Qav

Multiple Registration Protocol (MRP) es una función de audio video bridging (AVB). MRP es un protocolo de registro base que permite a los dispositivos con una aplicación MRP registrar atributos en otros dispositivos de la red. MRP ofrece una aplicación para registrar atributos como el ancho de banda de un stream de audio y video (AV) y la información de direcciones MAC. Diversas aplicaciones usan esta función para propagar el registro.

Nota: El marco MRP debe estar disponible y habilitado en todos los dispositivos intermedios para asegurar que los atributos se propaguen por toda la red.

El switch admite las siguientes aplicaciones MRP:

- Multiple MAC Registration Protocol (MMRP): MMRP permite propagar la información de direcciones MAC en la red, así como registrar y anular el registro de direcciones MAC individuales y de la pertenencia a grupos de direcciones MAC. Las estaciones finales pueden solicitar unirse o salir de un grupo multicast, o registrar una dirección MAC individual en una VLAN específica. Las entradas de direcciones MAC pueden registrarse y anularse dinámicamente si MMRP está habilitado administrativamente en el switch.
- Multiple VLAN Registration Protocol (MVRP): MVRP registra las VLAN en la red, lo que permite la configuración automática de VLAN en el switch. En una red típica, el etiquetado VLAN es común. Muchos nodos requieren que el tráfico de entrada lleve un ID de VLAN específico, y otros requieren que el tráfico de salida se transmita con un ID de VLAN específico. Con MVRP en la entrada y la salida, no se requiere configurar VLAN manualmente para que el tráfico etiquetado pase por la red.
- Multiple Stream Reservation Protocol (MSRP): MSRP reserva recursos en la red para que el tráfico sensible al tiempo fluya de extremo a extremo. Una red típica incluye varios talkers (dispositivos que transmiten streams) y varios listeners (dispositivos que reciben streams de uno o varios talkers). Cada flujo tiene requisitos específicos de ancho de banda, frecuencia de tramas y sincronización. MSRP garantiza estos recursos en todos los dispositivos intermedios entre cualquier talker y listener.

Con MRP, los atributos de red se declaran, registran, retiran y eliminan dinámicamente sin intervención del usuario. Esta naturaleza dinámica es especialmente útil en redes donde ocurre lo siguiente:

- Es probable que los atributos de red cambien con frecuencia, lo que exige reconfigurar los dispositivos intermedios.
- El número de destinatarios de estos atributos aumenta o disminuye con frecuencia.
- Sin un marco dinámico de autoajuste, cada uno de estos cambios requeriría atención constante de un administrador de red.

Configurar los ajustes globales de MRP

Puede configurar ajustes globales de MRP para el switch.

Para configurar los ajustes globales de MRP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Basic > MRP Configuration. Se muestra la página MRP Configuration.

6. Seleccione el botón de opción MVRP Mode Enable o Disable para especificar el modo administrativo global de MVRP en el switch.
Al habilitarlo, MVRP registra las VLAN en la red, lo que permite la configuración automática de VLAN en el dispositivo. El valor predeterminado es Disable.

7. Seleccione el botón de opción MMRP Enable o Disable para especificar el modo administrativo global de MMRP en el switch.
Al habilitarlo, se permite propagar la información de direcciones MAC en la red. A su vez, esto permite registrar y anular el registro de direcciones MAC individuales y de la pertenencia a grupos de direcciones MAC. El valor predeterminado es Disable.

8. Seleccione el botón de opción MSRP Enable o Disable para especificar el modo administrativo global de MSRP en el switch.
Al habilitarlo, el switch puede reservar recursos en la red para que el tráfico sensible al tiempo fluya de extremo a extremo. El valor predeterminado es Disable.

9. Seleccione el botón de opción Periodic State Machine (MVRP Mode) Enable o Disable. Al habilitarlo, se puede limitar el efecto de los cambios de topología de MVRP y reducir el número de unidades de datos de protocolo (PDU) transmitidas entre dispositivos. El valor predeterminado es Disable.

10. Seleccione el botón de opción Periodic State Machine (MMRP) Enable o Disable.
Al habilitarlo, se puede limitar el efecto de los cambios de topología de MMRP y reducir el número de unidades de datos de protocolo (PDU) transmitidas entre dispositivos. El valor predeterminado es Disable.

11. En el campo MSRP Max Fan In Ports, especifique el número máximo de interfaces en las que se permiten registros MSRP.
El rango es de 0 a 12. El valor predeterminado es 0, que significa que no hay límite en el número de interfaces.

12. Seleccione el botón de opción MSRP Boundary Propagation Enable o Disable.

Al habilitar la propagación de límite MSRP, según la configuración, se puede permitir que una reserva de stream atraviese un puerto de límite.

El valor predeterminado es Disable.

13. Haga clic en el botón Apply.
La configuración se guarda.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar el mapeo 802.1Qav

Puede definir las prioridades QoS globales para los streams Ethernet audio video (EAV) de tráfico clase A y clase B. Los streams de clase A reciben mayor prioridad que los de clase B.

Para cambiar las prioridades de mapeo 802.1Qav:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Basic > MRP Configuration. Se muestra la página MRP Configuration.

6. Desplácese a la sección 802.1qav Mapping.
De forma predeterminada, la prioridad EAV del tráfico clase A es 3, con prioridad de reasignación 1.

De forma predeterminada, la prioridad EAV del tráfico clase B es 2, con prioridad de reasignación 1.

7. En la columna EAV Stream, seleccione la casilla de la clase.
8. En el campo EAV Priority, especifique una prioridad de 0 a 7.
9. En el campo EAV Remap Priority, especifique una prioridad de 0 a 7.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar MRP en interfaces

Puede configurar el modo MRP y los temporizadores para una o más interfaces. Los temporizadores controlan cuándo y con qué frecuencia se transmiten los mensajes en cada interfaz.

Para configurar MRP en interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > MRP Port Settings. Se muestra la página MRP Port Settings.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú MVRP Mode, seleccione Enable o Disable para especificar el modo administrativo de MVRP en la interfaz.
Al habilitarlo, MVRP registra las VLAN en la red, lo que permite la configuración automática de VLAN en la interfaz. El valor predeterminado es Disable.

9. En el menú MMRP Mode, seleccione Enable o Disable para especificar el modo administrativo de MMRP en la interfaz.
Al habilitarlo, se permite propagar la información de direcciones MAC en la interfaz. A su vez, esto permite registrar y anular el registro de direcciones MAC individuales y de la pertenencia a grupos de direcciones MAC. El valor predeterminado es Disable.

10. En el menú MSRP Mode, seleccione Enable o Disable para especificar el modo administrativo de MSRP en la interfaz.
Al habilitarlo, la interfaz puede reservar recursos en la red para que el tráfico sensible al tiempo fluya de extremo a extremo. El valor predeterminado es Disable.

11. En el campo Join Timer, especifique el tiempo que la interfaz debe esperar mensajes JoinIn de otros participantes MRP después de enviar un mensaje Join. Si transcurre ese tiempo antes de que la interfaz reciba un mensaje JoinIn, la interfaz reenvía el mensaje Join. El rango es de 10 a 100 centisegundos. El valor predeterminado es 20.

12. En el campo Leave Timer, especifique el tiempo que la interfaz debe esperar antes de anular el registro de atributos de otros participantes MRP.
Si la interfaz recibe mensajes Join de otros participantes antes de que expire ese tiempo, los atributos no se anulan. El rango es de 20 a 600 centisegundos. El valor predeterminado es 300.

13. En el campo Leave All Timer, especifique el tiempo que la interfaz debe esperar tras iniciar el proceso de registro MRP, antes de que los participantes actualicen y vuelvan a registrar sus atributos.
El rango es de 200 a 6000 centisegundos. El valor predeterminado es 2000.

14. En el campo MSRP SR class PVID, especifique el ID de VLAN predeterminado que la interfaz debe usar para el tráfico de streams MSRP.

15. Haga clic en el botón Apply.
Se guarda la configuración.

16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 84. Información de configuración de MRP en interfaces

Campo	Descripción
MSRP Class A Boundary Port	Indica si la interfaz es un puerto de límite para el tráfico clase A.
MSRP Class B Boundary Port	Indica si la interfaz es un puerto de límite para el tráfico clase B.

Ver o borrar estadísticas de MMRP

Puede ver y borrar la información sobre las tramas MMRP transmitidas y recibidas por el switch y por cada interfaz.

Para ver y borrar las estadísticas de MMRP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > MMRP Statistics. Se muestra la página MMRP Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Para actualizar la página, haga clic en el botón Refresh.
8. Para borrar las estadísticas, haga lo siguiente:
a. Seleccione la casilla junto a la interfaz o interfaces o, para borrar las estadísticas de todas las interfaces, seleccione la casilla del encabezado de la tabla. b. Haga clic en el botón Clear.

Se borran las estadísticas.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 85. Información de estadísticas de MMRP

Campo	Descripción
Estadísticas globales de MMRP	
Frames Received	Número de tramas MMRP recibidas en el switch.
Bad Header	Número de tramas MMRP con encabezado incorrecto recibidas en el switch.
Bad Format	Número de tramas MMRP con formato de cuerpo de PDU incorrecto recibidas en el switch.
Frames Transmitted	Número de tramas MMRP transmitidas en el switch.
Fallas de transmisión	Número de tramas MMRP que el switch no transmitió.
Estadísticas de MMRP	
Interface	La interfaz cuya información se muestra.
Tramas recibidas	Número de tramas MMRP recibidas en la interfaz.
Encabezado incorrecto	Número de tramas MMRP con encabezados incorrectos recibidas en la interfaz.
Formato incorrecto	Número de tramas MMRP con formato de cuerpo de PDU incorrecto recibidas en la interfaz.
Tramas transmitidas	Número de tramas MMRP transmitidas en la interfaz.
Fallas de transmisión	Número de tramas MMRP que la interfaz no pudo transmitir.

Ver o borrar las estadísticas de MVRP

Puede ver y borrar la información de las tramas MVRP transmitidas y recibidas por el switch y por cada interfaz.

Para ver y borrar las estadísticas de MVRP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > MVRP Statistics. Se muestra la página MVRP Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Para actualizar la página, haga clic en el botón Refresh.
8. Para borrar las estadísticas, haga lo siguiente:
a. Seleccione la casilla junto a la interfaz o interfaces o, para borrar las estadísticas

de todas las interfaces, seleccione la casilla del encabezado de la tabla. b. Haga clic en el botón Clear.
Se borran las estadísticas.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 86. Información de estadísticas de MVRP

Campo	Descripción
Estadísticas globales de MVRP	
Frames Received	Número de tramas MMRP recibidas en el switch.
Bad Header	Número de tramas MMRP con encabezado incorrecto recibidas en el switch.
Bad Format	Número de tramas MMRP con formato de cuerpo de PDU incorrecto recibidas en el switch.
Frames Transmitted	Número de tramas MMRP transmitidas en el switch.

Tabla 86. Información de estadísticas de MVRP (continuación)

Campo	Descripción
Fallas de transmisión	Número de tramas MMRP que el switch no transmitió.
Fallas de cola de mensajes	Número de mensajes MMRP que no se agregaron a la cola.
Estadísticas de MVRP	
Interface	La interfaz cuya información se muestra.
Tramas recibidas	Número de tramas MVRP recibidas en la interfaz.
Encabezado incorrecto	Número de tramas MVRP con encabezados incorrectos recibidas en la interfaz.
Formato incorrecto	Número de tramas MVRP con formato de cuerpo de PDU incorrecto recibidas en la interfaz.
Tramas transmitidas	Número de tramas MVRP transmitidas en la interfaz.
Fallas de transmisión	Número de tramas MVRP que la interfaz no pudo transmitir.
Fallas de registro	Número de tramas MVRP que no se pudieron registrar en un dispositivo o en una interfaz específica.

Ver o borrar las estadísticas de MSRP

Puede ver y borrar la información de las tramas MSRP transmitidas y recibidas por el switch y por cada interfaz.

Para ver y borrar las estadísticas de MSRP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > MSRP Statistics. Se muestra la página MSRP Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Para actualizar la página, haga clic en el botón Refresh.
8. Para borrar las estadísticas, haga lo siguiente:
a. Seleccione la casilla junto a la interfaz o interfaces o, para borrar las estadísticas

de todas las interfaces, seleccione la casilla del encabezado
de la tabla. b. Haga clic en el botón Clear.
Se borran las estadísticas.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 87. Información de estadísticas de MSRP

Campo	Descripción
Estadísticas globales de MSRP	
Tramas recibidas	Número de tramas MSRP recibidas en el switch.
Encabezado incorrecto	Número de tramas MSRP con encabezados incorrectos recibidas en el switch.
Formato incorrecto	Número de tramas MSRP con formato de cuerpo de PDU incorrecto recibidas en el switch.
Tramas transmitidas	Número de tramas MSRP transmitidas en el switch.
Fallas de transmisión	Número de tramas MSRP que el switch no transmitió.
Fallas de mensajes	Número de mensajes MSRP que no se agregaron a la cola.
Estadísticas de MSRP	
Interface	La interfaz cuya información se muestra.
Tramas recibidas	Número de tramas MSRP recibidas en la interfaz.
Encabezado incorrecto	Número de tramas MSRP con encabezado incorrecto recibidas en la interfaz.
Formato incorrecto	Número de tramas MSRP con formato de cuerpo de PDU incorrecto recibidas en la interfaz.

Tabla 87. Información de estadísticas de MSRP (continuación)

Campo	Descripción
Tramas transmitidas	Número de tramas MSRP transmitidas en la interfaz.
Fallas de transmisión	Número de tramas MSRP que la interfaz no pudo transmitir.
Fallas de registro	Número de tramas MSRP que no se pudieron registrar en un dispositivo o en una interfaz específica.

Ver los ajustes de reservación de MSRP

Puede ver información sobre el estado de talker, listener y dispositivo intermedio de los dispositivos que participan en cada flujo MSRP que pasa por el switch.

Para ver los ajustes de reservación de MSRP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > MSRP Reservation Parameters. Se muestra la página MSRP Reservation Parameters.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 88. Información de parámetros de reservación de MSRP

Campo	Descripción
Interface	La interfaz cuya información se muestra.
ID de flujo	Valor entero sin signo de 16 bits, que es un ID único para distinguir el flujo entre varios flujos del mismo dispositivo.
Estado de declaración del listener	Estado de declaración MSRP del atributo listener.
Tipo de declaración del listener	Tipo de declaración MSRP del atributo listener.
Estado de declaración del talker	Estado de declaración MSRP del atributo talker.
Tipo de declaración del talker	Tipo de declaración MSRP del atributo talker.
Latencia acumulada	Latencia, en nanosegundos, del flujo en su trayecto desde el talker hasta un listener. La latencia empieza en cero y aumenta en uno por cada dispositivo de la red por el que se propaga el flujo.
Interfaz del puente con falla	Si ocurrió una falla, la interfaz del dispositivo en el que ocurrió.
MAC del puente con falla	Si ocurrió una falla, la dirección MAC del dispositivo en el que ocurrió.

Tabla 88. Información de parámetros de reservación de MSRP (continuación)

Campo	Descripción
Código de falla	Si ocurrió una falla, el número que representa el motivo de la falla. El switch admite los siguientes códigos: • 1: Ancho de banda insuficiente • 3: Ancho de banda insuficiente para la clase de tráfico • 5: La dirección de destino del flujo ya está en uso • 7: Cambió la latencia informada • 8: El puerto de salida no admite audio video bridging (AVB) • 9: Use otra dirección de destino (por ejemplo, si la tabla hash de MAC DA está llena) • 12: No se puede almacenar la dirección de destino (por ejemplo, si el dispositivo se quedó sin recursos de MAC DA) • 13: La prioridad solicitada no es una prioridad de clase SR • 14: MaxFrameSize es demasiado grande para el medio • 15: Se alcanzó el límite de msrpMaxFanInPorts • 16: Cambios en FirstValue para un StreamID registrado • 17: La VLAN está bloqueada en este puerto de salida (Registration Forbidden)
Antigüedad del flujo	Tiempo, en segundos, desde que la dirección de destino del flujo se agregó a la tabla Dynamic Reservations Entries. Un valor de cero indica que la dirección de destino no se agregó a la tabla.

Configurar y ver los ajustes de Qav de las interfaces

Puede configurar y ver los ajustes de IEEE 802.1Qav de las interfaces. El estándar IEEE 802.1Qav admite flujos de tráfico sensibles al tiempo al regular todo el tráfico del switch, incluido el tráfico Ethernet asíncrono heredado, mediante colas y reenvío. Cuando un talker declara un flujo, 802.1Qav identifica si el flujo es de clase A o clase B y especifica los requisitos de ancho de banda del flujo. El tráfico de clase A recibe mayor prioridad de transmisión que el de clase B.

Puede configurar y ver las asignaciones de ancho de banda seleccionadas para el tráfico de clase A y clase B.

Para configurar y ver los ajustes de Qav de las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > Qav Parameters. Se muestra la página Qav Parameters.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla de la interfaz.
- Para configurar varias interfaces con la misma configuración, marque la casilla de cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

7. En el campo Class A MSRP Delta Bandwidth, especifique el ancho de banda adicional, expresado como porcentaje de la velocidad de transmisión de la interfaz, reservado para el tráfico de clase A y clase B.
El tráfico de clase A recibe mayor prioridad que el de clase B. El rango es de 0 a 100. El valor predeterminado es 75.

8. En el campo Class B MSRP Delta Bandwidth, especifique el ancho de banda adicional, expresado como porcentaje de la velocidad de transmisión de la interfaz, reservado para el tráfico de clase B.
El rango es de 0 a 100. El valor predeterminado es 0.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 89. Información de ajustes de Qav

Campo	Descripción
Ancho de banda asignado clase A	Velocidad actual (en Bps) del tráfico de clase A en la interfaz.
Ancho de banda restante clase A	Velocidad máxima (en Bps) de clase A que admite la interfaz.
Ancho de banda asignado clase B	Velocidad actual (en Bps) del tráfico de clase B en la interfaz.
Ancho de banda restante clase B	Velocidad máxima (en Bps) de clase B que admite la interfaz.
Ancho de banda total asignado	Suma de las velocidades de tráfico asignadas de clase A y clase B (en Bps) en la interfaz.
Ancho de banda total restante	75 por ciento de la velocidad de la interfaz menos el ancho de banda total asignado (en Bps/s).

Ver la información de flujos MSRP

Puede ver información sobre los flujos MSRP que pasan por cada interfaz.

Para ver la información de flujos MSRP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > MRP > Advanced > MSRP Streams Information. Se muestra la página MSRP Streams Information.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 90. Información de flujos MSRP

Campo	Descripción
ID de flujo	Valor entero sin signo de 16 bits, que es un ID único para distinguir el flujo entre varios flujos del mismo dispositivo.
Dirección MAC de origen del flujo	Dirección MAC del origen del flujo de tráfico.
Latencia acumulada recibida	Valor de latencia acumulada sin signo de 32 bits que se usa para determinar la latencia en el peor caso que puede sufrir un flujo en su trayecto del talker a un listener. La latencia empieza en cero y aumenta en uno por cada dispositivo de la red por el que se propaga el flujo.
Clase de tráfico	Indica si el flujo es de clase A o clase B. El tráfico de clase A recibe mayor prioridad que el de clase B.
Rango	Valor de rango sin signo de 5 bits que usan los dispositivos para determinar qué flujos se pueden seguir atendiendo cuando los registros MSRP superan la capacidad de una interfaz para transportar los flujos de datos correspondientes. Si un dispositivo queda sobresuscrito (por ejemplo, por una reconfiguración de la red o una reducción del ancho de banda 802.11), el valor de rango también se usa para determinar qué flujos se descartan. Un valor numérico menor es más importante que uno mayor.
Tamaño máx. de trama TSpec	Valor de ancho de banda sin signo de 32 bits que se usa para asignar recursos y ajustar la selección de colas para ofrecer la calidad de servicio solicitada por un talker MSRP. El valor representa la velocidad máxima, en unidades de 1024 octetos por segundo, a la que se pueden transmitir las tramas del flujo referido por el talker.
Tramas máx. por intervalo TSpec	Valor de velocidad de tramas sin signo de 32 bits que se usa para asignar recursos y ajustar la selección de colas para ofrecer la calidad de servicio solicitada por un talker MSRP. El valor representa el número máximo de tramas que el talker puede transmitir en un segundo.
VLAN del flujo	ID de VLAN del flujo de tráfico.
MAC de destino	Dirección MAC del destino del flujo de tráfico.
Información de falla recibida Interfaz del puente	Si ocurrió una falla, la interfaz del dispositivo en el que ocurrió.

Tabla 90. Información de flujos MSRP (continuación)

Campo	Descripción
Información de falla recibida Código de falla	Si ocurrió una falla, el número que representa el motivo de la falla. El switch admite los siguientes códigos: • 1: Ancho de banda insuficiente • 3: Ancho de banda insuficiente para la clase de tráfico • 5: La dirección de destino del flujo ya está en uso • 7: Cambió la latencia informada • 8: El puerto de salida no admite audio video bridging (AVB) • 9: Use otra dirección de destino (por ejemplo, si la tabla hash de MAC DA está llena) • 12: No se puede almacenar la dirección de destino (por ejemplo, si el dispositivo se quedó sin recursos de MAC DA) • 13: La prioridad solicitada no es una prioridad de clase SR • 14: MaxFrameSize es demasiado grande para el medio • 15: Se alcanzó el límite de msrpMaxFanInPorts • 16: Cambios en FirstValue para un StreamID registrado • 17: La VLAN está bloqueada en este puerto de salida (Registration Forbidden)
Información de falla recibida MAC del puente	Si ocurrió una falla, la dirección MAC del dispositivo en el que ocurrió.
Interfaz del talker	Interfaz en la que se encuentra el talker.
Listeners	Interfaz en la que se encuentran los listeners.

Protección contra bucles

La protección contra bucles puede detectar bucles físicos y lógicos entre los puertos Ethernet de un dispositivo.

Acerca de la protección contra bucles

Los bucles en una red son costosos porque consumen recursos y reducen el rendimiento de la red. Detectar bucles manualmente puede ser complicado.

El switch puede identificar automáticamente los bucles en la red. Puede habilitar la protección contra bucles por puerto o de forma global.

Si la protección contra bucles está habilitada, el switch envía paquetes de unidad de datos de protocolo (PDU) predefinidos a una dirección de destino multicast de capa 2 (09:00:09:09:13:A6) en todos los puertos en los que la función está habilitada. Puede deshabilitar selectivamente la transmisión de PDU de protección contra bucles en puertos específicos aunque la protección esté habilitada. Si el switch recibe un paquete con dicha dirección de destino multicast, la dirección MAC de origen del paquete se compara con la dirección MAC del switch. Si no coinciden, el paquete se reenvía a todos los puertos miembros de la misma VLAN, como cualquier otro paquete multicast. El paquete no se reenvía al puerto por el que se recibió.

Si la dirección MAC de origen coincide con la dirección MAC del switch, este puede realizar una de las siguientes acciones, según cómo configure la acción:

- Se apaga el puerto.
- Se genera un mensaje de registro. (Si hay un servidor syslog configurado, el mensaje puede enviarse al servidor syslog).
- Se apaga el puerto y se genera un mensaje de registro.

Si la protección contra bucles está deshabilitada, el paquete multicast se descarta sin aviso.

La protección contra bucles no está pensada para puertos que funcionan como uplinks entre switches compatibles con spanning tree. Está diseñada para switches no administrables que descartan las unidades de datos de protocolo de puente (BPDU) de spanning tree.

Debe habilitar la función de forma global antes de habilitarla a nivel de puerto para que se pueda instalar el filtro de políticas del sistema.

La protección contra bucles trata la transmisión de paquetes PDU y el protocolo spanning tree de las siguientes maneras:

- Protección contra bucles y transmisión de paquetes PDU: la protección envía paquetes del protocolo de bucles desde todos los puertos en los que está habilitada. Puede configurar el intervalo (de 1 a 5 segundos) entre dos paquetes PDU consecutivos. El intervalo predeterminado es de 5 segundos. Si el switch recibe un paquete del protocolo en un puerto cuya acción es apagar el puerto, el puerto ya no puede recibir ni enviar tramas.
  La protección contra bucles funciona a nivel de puerto, independientemente de la asignación y pertenencia a VLAN, y detecta bucles entre VLAN.
- Protección contra bucles y Spanning Tree Protocol: la protección contra bucles no afecta a los nodos finales y no está pensada para puertos que funcionan como uplinks entre switches compatibles con spanning tree. Puede coexistir con Spanning Tree Protocol (STP). Puede habilitar la protección contra bucles y STP en un puerto, ya que estas funciones funcionan de forma independiente. STP no desactiva un puerto al detectar un bucle, sino que lo mantiene en estado de bloqueo. Como se permiten PDU en el

estado de bloqueo, se reciben los paquetes de protección y esta desactiva el puerto involucrado en el bucle (si la acción configurada es apagar el puerto).

Configurar los ajustes globales de protección contra bucles

Antes de configurar la protección contra bucles en puertos individuales (consulte Configurar los ajustes de protección contra bucles de las interfaces y mostrar su estado en la página 335), debe habilitarla y configurarla de forma global.

Para habilitar y configurar la protección contra bucles de forma global:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > L2 Loop Protection > L2 Loop Protection Configuration. Se muestra la página L2 Loop Protection Configuration.

6. En la sección Global L2 Loop Protection Configuration, configure los siguientes ajustes:

- Junto a Admin Mode, seleccione el botón de opción Enable o Disable para especificar el modo administrativo de la protección contra bucles en el switch.
De forma predeterminada, la protección contra bucles está deshabilitada globalmente.
- En el menú TLV Advertized Interval, seleccione el intervalo entre las transmisiones de paquetes de bucle en un puerto.
El rango es de 1 a 5 segundos. El valor predeterminado es 5 segundos. El intervalo seleccionado se aplica a todos los puertos en los que habilite la protección.
- En el menú Max PDU Receive, seleccione el número máximo de paquetes que un puerto puede recibir antes de que se tome una acción.
El valor predeterminado es 1 paquete. El número seleccionado se aplica a todos los puertos en los que habilite la protección contra bucles.

7. Haga clic en el botón Apply.

La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de protección contra bucles de las interfaces y mostrar el estado de la protección

Antes de configurar la protección contra bucles en puertos individuales, debe habilitarla de forma global (consulte Configurar los ajustes globales de protección contra bucles en la página 334).

Para habilitar y configurar la protección contra bucles de una interfaz y mostrar su estado en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Switching > L2 Loop Protection > L2 Loop Protection Configuration. Se muestra la página L2 Loop Protection Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Keep Alive, seleccione Enable para habilitar la protección contra bucles en el puerto.
De forma predeterminada, la protección contra bucles está deshabilitada en los puertos.

9. En el menú RX Action, seleccione la acción que realiza el switch cuando se detecta un bucle en el puerto:

- Log: registra el mensaje cuando se detecta un bucle en el puerto.
- Disable: deshabilita el puerto cuando se detecta un bucle. Esta es la configuración predeterminada.
- Both: registra el mensaje y deshabilita el puerto cuando se detecta un bucle.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 91. Información de configuración de protección contra bucles de la interfaz

Campo	Descripción
Bucle detectado	Indica (Yes o No) si se detectó un bucle en la interfaz.
Conteo de bucles	Número de paquetes recibidos en la interfaz después de que el bucle se la detecta.
Tiempo desde el último bucle	Tiempo transcurrido desde que se detectó el bucle.
Estado del puerto	Estado de la interfaz (Enabled o Disabled).
Motivo de Errdisable	Motivo por el que se deshabilitó la interfaz. Además de deshabilitarse por la protección contra bucles, la interfaz puede deshabilitarse por Unidirectional Link Detection (UDLD), una tormenta de broadcast, una tormenta de unicast, etc.
Tiempo restante de recuperación automática (s)	Tiempo restante antes de que la interfaz se vuelva a habilitar mediante el proceso de recuperación automática. El tiempo va de 30 a 604800 segundos.

4

Administrar el enrutamiento

Este capítulo trata los siguientes temas:

- Conceptos de enrutamiento
- Tabla de enrutamiento, rutas y preferencias de ruta
- Enrutamiento IPv4
- Enrutamiento IPv6
- VLAN de enrutamiento
- Address Resolution Protocol
- Routing Information Protocol
- Descubrimiento de routers y anuncios de router

Conceptos de enrutamiento

El switch admite enrutamiento IP. Cuando un paquete entra en el switch, este revisa la dirección MAC de destino para determinar si coincide con alguna de las interfaces de enrutamiento configuradas. Si coincide, el switch busca en la tabla de hosts una dirección IP de destino coincidente. Si encuentra una entrada, el paquete se enruta al host. Si no hay coincidencia, el switch busca la coincidencia de prefijo más larga para la IP de destino. Si encuentra una entrada, el paquete se enruta al siguiente salto. Si no hay coincidencia, el paquete se enruta al siguiente salto especificado en la ruta predeterminada. Si no existe una ruta predeterminada, el paquete se descarta.

Tabla de enrutamiento, rutas y preferencias de ruta

La tabla de enrutamiento reúne rutas de varios orígenes y enumera todas: rutas estáticas, rutas locales, rutas agregadas dinámicamente, etc. Las rutas estáticas son las que usted agrega manualmente. La tabla puede aprender varias rutas al mismo destino desde varios orígenes, por ejemplo, rutas agregadas dinámicamente por protocolos de enrutamiento.

Configurar una ruta y mostrar las rutas aprendidas

Puede agregar o cambiar una ruta en la tabla de enrutamiento y mostrar las rutas aprendidas automáticamente en la tabla.

Para agregar o cambiar una ruta y mostrar las rutas aprendidas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Routing> Routing Table > Basic > Route Configuration. Se muestra la página Route Configuration.

6. Si va a cambiar una ruta existente, marque la casilla de la ruta.
7. En el menú Route Type, seleccione uno de los siguientes tipos de ruta:

- Default: especifique la dirección del siguiente salto y la preferencia.
- Static: especifique la dirección de red, la máscara de subred, la dirección del siguiente salto y la preferencia.
- Static Reject: especifique la dirección de red, la máscara de subred y la preferencia.

8. En el campo Network Address, introduzca el prefijo de ruta IP del destino.

9. En el campo Subnet Mask, introduzca la parte de la dirección IP de la interfaz que identifica la red conectada.
También se conoce como máscara de subred o de red.

10. En el campo Next Hop IP Address, introduzca la dirección IP del router de salida que se debe usar al reenviar el tráfico al siguiente router (si lo hay) en la ruta hacia el destino.
El siguiente router es siempre uno de los vecinos adyacentes o la dirección IP de la interfaz local en el caso de una red conectada directamente.

11. En el campo Preference, introduzca un valor de 1 a 255.
Puede especificar el valor de preferencia (a veces llamado distancia administrativa) de una ruta estática individual. Entre las rutas al mismo destino, la ruta con el valor de preferencia más bajo es la que se introduce en la base de datos de reenvío. Al especificar la preferencia de una ruta estática, puede controlar si se prefiere más o menos que las rutas de protocolos de enrutamiento dinámico. La preferencia también controla si una ruta estática se prefiere más o menos que otras rutas estáticas al mismo destino.

12. En el campo Description, introduzca una descripción que identifique esta ruta. La descripción debe constar de caracteres alfanuméricos, guiones o guiones bajos y puede tener hasta 31 caracteres.

13. Realice una de las siguientes acciones:

- Si va a agregar una ruta nueva, haga clic en el botón Add. Se guarda la configuración. La ruta se agrega a la tabla de enrutamiento.
- Si va a cambiar una ruta existente, haga clic en el botón Apply. Se guarda la configuración.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 92. Información de rutas aprendidas

Campo	Descripción
Dirección de red	Prefijo de ruta IP del destino.
Máscara de subred	Máscara de subred/red, que indica la parte de la dirección de la interfaz IP que identifica la red conectada.
Protocolo	Protocolo que creó la ruta: Local, Static o RIP.
Tipo de ruta	Tipo de ruta, según el protocolo: Connected, Static o Dynamic.
Interfaz del siguiente salto	Interfaz de salida del router que debe usarse al reenviar el tráfico al destino.
Dirección del siguiente salto	Dirección IP de la interfaz de salida del router que debe usarse al reenviar el tráfico al siguiente router (si lo hay) en la ruta hacia el destino.
Preferencia	Preferencia, un valor de 0 a 255.
Métrica	Costo administrativo de la ruta al destino. El valor predeterminado es 1. El rango es de 0 a 255.

Eliminar una ruta

Puede eliminar una ruta que ya no necesite.

Para eliminar una ruta:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Routing Table > Basic > Route Configuration. Se muestra la página Route Configuration.

6. Marque la casilla de la ruta.

7. Haga clic en el botón Delete.
Se guarda la configuración. La ruta se elimina.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Especificar las preferencias de ruta

Puede configurar la preferencia predeterminada de cada protocolo, por ejemplo, 60 para rutas estáticas o 120 para RIP. Son valores arbitrarios en el rango de 1 a 255 e independientes de las métricas de ruta. La mayoría de los protocolos usan una métrica para determinar la ruta más corta conocida por el protocolo, independientemente de otros protocolos.

La mejor ruta a un destino es la que tiene el valor de preferencia más bajo. Si existen varias rutas a un destino, los valores de preferencia se usan para determinar la ruta preferida. Si aún hay empate, se elige la ruta con la mejor métrica. Para evitar problemas con métricas incompatibles, como protocolos que no son directamente comparables, debe configurar valores de preferencia distintos para cada protocolo.

Para especificar las preferencias de ruta

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Routing Table > Advanced > Route Preferences. Se muestra la página Route Preferences.

6. En el campo Static, especifique la preferencia de rutas estáticas en el switch. El valor predeterminado es 1. El rango es de 1 a 255.

7. En el campo RIP, especifique la preferencia de rutas RIP en el switch. El valor predeterminado es 120. El rango es de 1 a 255.

8. Haga clic en el botón Apply.
La configuración se guarda.

El campo Local muestra el valor de preferencia de rutas locales.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Enrutamiento IPv4

Puede habilitar o deshabilitar el modo de enrutamiento IPv4, configurar los ajustes globales de enrutamiento IPv4, configurar interfaces de enrutamiento IPv4, agregar una dirección IP secundaria a una interfaz de enrutamiento IPv4 y ver las estadísticas de enrutamiento IPv4.

Administrar los ajustes globales de enrutamiento IPv4

Puede configurar los ajustes de enrutamiento IPv4 del switch, a diferencia de los ajustes de enrutamiento IPv4 de una interfaz.

Para configurar los ajustes globales de enrutamiento IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IP > Basic > IP Configuration. Se muestra la página IP Configuration.

6. Seleccione el botón de opción Routing Mode Enable o Disable.
Esto habilita o deshabilita el modo administrativo de enrutamiento IPv4 del switch. El valor predeterminado es Enable.

7. Seleccione el botón de opción ICMP Echo Replies Enable o Disable. El valor predeterminado es Enable, lo que significa que el switch responde a las solicitudes de eco ICMP.

8. Seleccione el botón de opción ICMP Redirects Enable o Disable.
El valor predeterminado es Disable. Si habilita ICMP Redirects, el switch puede reenviar redirecciones ICMP.

9. En el campo ICMP Rate Limit Interval, especifique el número de paquetes de error ICMP permitidos por intervalo de ráfaga.
De forma predeterminada, el intervalo es de 1000 ms (límite de 100 paquetes/s). El intervalo va de 0 a 2147483647 ms. Ingrese 0 para que el switch ignore el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

10. En el campo ICMP Rate Limit Burst Size, especifique el número de paquetes de error ICMP permitidos para el tamaño de ráfaga.
De forma predeterminada, el tamaño de ráfaga es de 100 paquetes. El rango es de 1 a 200. Ingrese 0 para que el switch ignore el número de paquetes de error ICMP permitidos para el tamaño de ráfaga.

11. Para configurar una puerta de enlace predeterminada global, marque la casilla Select to configure Global Default Gateway. Después, en el campo Global Default Gateway, ingrese la dirección IP. La puerta de enlace que especifique tiene mayor preferencia que una puerta de enlace predeterminada aprendida de un servidor DHCP. Solo puede configurar una puerta de enlace predeterminada, pero puede cambiarla.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 93. Información de configuración del enrutamiento IPv4

Campo	Descripción
Tiempo de vida predeterminado	Valor predeterminado que se inserta en el campo Time-To-Live del encabezado IP de los datagramas originados por el switch, si el protocolo de capa de transporte no proporciona un valor TTL.
Máximo de siguientes saltos	Número máximo de saltos admitidos por el switch.

Tabla 93. Información de configuración del enrutamiento IPv4 (continuación)

Campo	Descripción
Máximo de rutas	Número máximo de rutas admitidas por el switch.
Máximo de rutas estáticas	Número máximo de rutas estáticas admitidas por el switch.

Mostrar las estadísticas IPv4

Puede mostrar las estadísticas de enrutamiento IPv4 del switch.

Para mostrar las estadísticas de enrutamiento IPv4 del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Routing> IP > Basic > Statistics. Se muestra la página Statistics.

   La siguiente tabla describe los campos no configurables de la página.

Tabla 94. Información de estadísticas IP

Campo	Descripción
IpInReceives	Número total de datagramas de entrada recibidos de las interfaces, incluidos los recibidos con errores.
IpInHdrErrors	Número de datagramas de entrada descartados por errores en sus encabezados IP, como sumas de verificación incorrectas, versión no coincidente, otros errores de formato, tiempo de vida excedido, errores al procesar sus opciones IP, etc.

Tabla 94. Información de estadísticas IP (continuación)

Campo	Descripción
IpInAddrErrors	Número de datagramas de entrada descartados porque la dirección IP del campo de destino del encabezado IP no era válida para recibirse en esta entidad. Incluye direcciones no válidas (por ejemplo, 0.0.0.0) y direcciones de clases no admitidas (Clase E). En entidades que no son gateways IP y que por lo tanto no reenvían datagramas, incluye los datagramas descartados porque la dirección de destino no era una dirección local.
IpForwDatagrams	Número de datagramas de entrada para los que esta entidad no era su destino IP final, por lo que se intentó encontrar una ruta para reenviarlos a ese destino final. En entidades que no actúan como gateways IP, solo incluye los paquetes enrutados en origen a través de esta entidad cuyo procesamiento de la opción source-route fue exitoso.
IpInUnknownProtos	Número de datagramas dirigidos localmente recibidos correctamente pero descartados por un protocolo desconocido o no admitido.
IpInDiscards	Número de datagramas IP de entrada que no presentaron problemas que impidieran continuar su procesamiento, pero que se descartaron (por falta de espacio de búfer). No incluye datagramas descartados mientras esperaban reensamblaje.
IpInDelivers	Número total de datagramas de entrada entregados correctamente a protocolos de usuario IP (incluido ICMP).
IpOutRequests	Número total de datagramas IP que los protocolos de usuario IP locales (incluido ICMP) entregaron a IP en solicitudes de transmisión. No incluye datagramas contados en ipForwDatagrams.
IpOutDiscards	Número de datagramas IP de salida que no presentaron problemas que impidieran su transmisión al destino, pero que se descartaron por razones como falta de espacio de búfer. Este contador incluiría datagramas contados en ipForwDatagrams si alguno cumpliera este criterio (discrecional) de descarte.
IpOutNoRoutes	Número de datagramas IP descartados porque no se encontró ninguna ruta para transmitirlos a su destino. Incluye los paquetes contados en ipForwDatagrams que cumplen este criterio de falta de ruta. Incluye los datagramas que un host no puede enrutar porque todas sus puertas de enlace predeterminadas están inactivas.

Tabla 94. Información de estadísticas IP (continuación)

Campo	Descripción
IpReasmTimeout	Número máximo de segundos que se retienen los fragmentos recibidos mientras esperan reensamblaje en esta entidad.
IpReasmReqds	Número de fragmentos IP recibidos que se reensamblaron en esta entidad.
IpReasmOKs	Número de datagramas IP reensamblados correctamente.
IpReasmFails	Número de fallas detectadas por el algoritmo de reensamblaje IP (por cualquier motivo: tiempo agotado, errores, etc.). No es necesariamente un conteo de fragmentos IP descartados, ya que algunos algoritmos pierden la cuenta de fragmentos al combinarlos conforme se reciben.
IpFragOKs	Número de datagramas IP fragmentados en esta entidad.
IpFragFails	Número de datagramas IP descartados porque debían fragmentarse en esta entidad pero no fue posible, por ejemplo porque tenían activado el indicador Don’t Fragment.
IpFragCreates	Número de fragmentos de datagramas IP generados como resultado de la fragmentación en esta entidad.
IpRoutingDiscards	Número de entradas de enrutamiento descartadas aunque eran válidas. Una posible razón para descartarlas es liberar espacio de búfer para otras entradas de enrutamiento.
IcmpInMsgs	Número total de mensajes ICMP que recibió la entidad. Este contador incluye todos los contados por icmpInErrors.
IcmpInErrors	Número de mensajes ICMP que la entidad recibió pero que determinó que tenían errores específicos de ICMP (sumas de verificación ICMP incorrectas, longitud incorrecta, etc.).
IcmpInDestUnreachs	Número de mensajes ICMP de destino inalcanzable recibidos.
IcmpInTimeExcds	Número de mensajes ICMP de tiempo excedido recibidos.
IcmpInParmProbs	Número de mensajes ICMP de problema de parámetros recibidos.
IcmpInSrcQuenchs	Número de mensajes ICMP de source quench recibidos.
IcmpInRedirects	Número de mensajes ICMP de redirección recibidos.
IcmpInEchos	Número de mensajes ICMP de eco (solicitud) recibidos.

Tabla 94. Información de estadísticas IP (continuación)

Campo	Descripción
IcmpInEchoReps	Número de mensajes ICMP de respuesta de eco recibidos.
IcmpInTimestamps	Número de mensajes ICMP de marca de tiempo (solicitud) recibidos.
IcmpInTimestampReps	Número de mensajes ICMP de respuesta de marca de tiempo recibidos.
IcmpInAddrMasks	Número de mensajes ICMP de solicitud de máscara de dirección recibidos.
IcmpInAddrMaskReps	Número de mensajes ICMP de respuesta de máscara de dirección recibidos.
IcmpOutMsgs	Número total de mensajes ICMP que esta entidad intentó enviar. Este contador incluye todos los contados por icmpOutErrors.
IcmpOutErrors	Número de mensajes ICMP que esta entidad no envió debido a problemas detectados dentro de ICMP, como falta de búferes. Este valor no incluye errores detectados fuera de la capa ICMP, como la imposibilidad de IP de enrutar el datagrama resultante. En algunas implementaciones puede no haber tipos de error que contribuyan al valor de este contador.
IcmpOutDestUnreachs	Número de mensajes ICMP de destino inalcanzable enviados.
IcmpOutTimeExcds	Número de mensajes ICMP de tiempo excedido enviados.
IcmpOutParmProbs	Número de mensajes ICMP de problema de parámetros enviados.
IcmpOutSrcQuenchs	Número de mensajes ICMP de source quench enviados.
IcmpOutRedirects	Número de mensajes ICMP de redirección enviados. En un host, siempre es cero, ya que los hosts no envían redirecciones.
IcmpOutEchos	Número de mensajes ICMP de eco (solicitud) enviados.
IcmpOutEchoReps	Número de mensajes ICMP de respuesta de eco enviados.
IcmpOutTimestamps	Número de mensajes ICMP de marca de tiempo (solicitud).
IcmpOutTimestampReps	Número de mensajes ICMP de respuesta de marca de tiempo enviados.
IcmpOutAddrMasks	Número de mensajes ICMP de solicitud de máscara de dirección enviados.

Configurar interfaces de enrutamiento IPv4

Puede configurar una o más interfaces de enrutamiento IPv4.

Para configurar una o más interfaces de enrutamiento IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IP > Advanced > IP Interface Configuration. Se muestra la página IP Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el campo Description, ingrese una descripción para la interfaz.

9. En el menú IP Address Configuration Method, seleccione el método con el que se configura la dirección IP en la interfaz: None, Manual o DHCP. El método predeterminado es None. Use el método None para restablecer el método DHCP.

Nota: Al cambiar el método de configuración de DHCP a None, hay un breve retraso antes de que se actualice la página.

10. Si selecciona None en el menú IP Address Configuration Method, haga lo siguiente:

a. En el campo IP Address, ingrese la dirección IP de la interfaz. b. En el campo Subnet Mask, ingrese la máscara de subred de la interfaz.

También se llama máscara de subred/red y define la parte de la dirección IP de la interfaz que identifica la red conectada.

11. En el menú Routing Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de enrutamiento de la interfaz.
El valor predeterminado es Enable.

12. En el menú Administrative Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo administrativo de la interfaz.
El valor predeterminado es Enable.

13. En el menú Forward Net Directed Broadcasts, seleccione Enable o Disable para habilitar o deshabilitar el reenvío de paquetes broadcast dirigidos a la red. El valor predeterminado es Disable, lo que significa que estos paquetes no se reenvían, sino que se descartan.

14. En el menú Encapsulation Type, seleccione el tipo de encapsulamiento de capa de enlace de los paquetes transmitidos desde la interfaz especificada.
Puede seleccionar Ethernet o SNAP (Subnetwork Access Protocol). El valor predeterminado es Ethernet.

15. En el menú Proxy Arp, seleccione Enable o Disable para habilitar o deshabilitar el proxy ARP de la interfaz.
El valor predeterminado es Enable.

16. En el menú Local Proxy Arp, seleccione Enable o Disable para habilitar o deshabilitar el proxy ARP local de la interfaz.
El valor predeterminado es Disable.

17. En el campo Bandwidth (kbps), especifique el ancho de banda de la interfaz. Este valor indica la velocidad de la interfaz a los protocolos de nivel superior. Algunos protocolos usan el ancho de banda para calcular el costo del enlace. El rango es de 1 a 10000000.

18. En el menú ICMP Destination Unreachables, seleccione Enable o Disable para permitir o impedir que la interfaz envíe mensajes ICMP de destino inalcanzable. El valor predeterminado es Enable.

19. En el menú ICMP Redirects, seleccione Enable o Disable para habilitar o deshabilitar el modo de redirección ICMP.
La interfaz envía un mensaje de redirección ICMP solo si esta función está habilitada tanto globalmente como en la interfaz. El valor predeterminado es Enable.

20. En el campo IP MTU, especifique el tamaño máximo de los paquetes IP enviados por la interfaz.
La MTU IP es el tamaño máximo de trama menos la longitud del encabezado de capa 2. El rango va de 68 bytes al tamaño de MTU que admite el enlace de la interfaz. El valor predeterminado es 1500. Un valor de 0 indica que la MTU IP no está configurada, en cuyo caso la interfaz usa el tamaño de MTU que admite el enlace de la interfaz.

21. Haga clic en el botón
Apply. Se guardan los ajustes.

22. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 95. IP Interface Configuration

Campo	Descripción
ID de VLAN	ID de VLAN de la interfaz.
Velocidad de datos del enlace	Velocidad de datos del enlace físico de la interfaz.
Estado activo	Estado activo o inactivo de la interfaz (Active o Inactive).
Dirección MAC	Dirección MAC asociada con la interfaz.
Estado del enlace	Estado de enlace activo o inactivo de la interfaz (Link UP o Link Down). Una interfaz se considera activa si el enlace está activo y la interfaz está en estado de reenvío.
Estado de la interfaz de enrutamiento	Estado del enlace de la interfaz de enrutamiento (Up o Down).

Eliminar la dirección IP de enrutamiento de una interfaz de enrutamiento IPv4

Puede eliminar la dirección IP de enrutamiento de una o más interfaces de enrutamiento IPv4.

Para eliminar la dirección IP de enrutamiento de una o más interfaces de enrutamiento IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IP > Advanced > IP Interface Configuration. Se muestra la página IP Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para eliminar la dirección IP de una sola interfaz, marque la casilla asociada con la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para eliminar la dirección IP de varias interfaces, marque la casilla asociada con cada interfaz.

8. Haga clic en el botón Delete.
Se guarda la configuración. La dirección IP de enrutamiento se elimina de la interfaz de enrutamiento IPv4.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una dirección IP secundaria para una interfaz de enrutamiento IPv4

Puede configurar una dirección IP secundaria para una interfaz de enrutamiento IPv4.

Para configurar la dirección IP secundaria:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IP > Advanced > Secondary IP. Se muestra la página Secondary IP.

6. En el menú Routing Interface, seleccione la interfaz.
7. En el campo Secondary IP Address, agregue una dirección IPv4 secundaria a la interfaz.

8. En el campo Secondary IP Subnet Mask, ingrese la máscara de subred asociada con la dirección IP secundaria.

9. Haga clic en el botón Add.
Se agrega la dirección IP secundaria.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 96. Información de la dirección IP secundaria

Campo	Descripción
ID de VLAN	ID de VLAN asociado con la interfaz seleccionada.
Dirección IP principal	Dirección IP principal de la interfaz.

Eliminar la dirección IP secundaria de una interfaz de enrutamiento IPv4

Puede eliminar la dirección IP secundaria de una interfaz de enrutamiento IPv4.

Para eliminar la dirección IP secundaria de una interfaz de enrutamiento IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IP > Advanced > Secondary IP. Se muestra la página Secondary IP.

6. En el menú Routing Interface, seleccione la interfaz.
7. En la tabla Secondary IP Address, marque la casilla de la dirección IP.

8. Haga clic en el botón Delete.
Se guarda la configuración. La dirección IP secundaria se elimina de la interfaz de enrutamiento IPv4.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Enrutamiento IPv6

Puede habilitar o deshabilitar el modo de enrutamiento IPv6, configurar los ajustes globales de enrutamiento IPv6, configurar interfaces de enrutamiento IPv6, agregar prefijos IPv6, agregar rutas estáticas y preferencias de ruta IPv6, agregar túneles IPv6 y ver las estadísticas, rutas y vecinos de enrutamiento IPv6.

Administrar los ajustes globales de enrutamiento IPv6

Puede configurar los ajustes de enrutamiento IPv6 del switch, a diferencia de los ajustes de enrutamiento IPv6 de una interfaz.

Para configurar los ajustes globales de enrutamiento IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Basic > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción IPv6 Unicast Routing Enable o Disable. Esto habilita o deshabilita el modo administrativo de enrutamiento IPv6 del switch. El valor predeterminado es Disable.

7. En el campo Hop Limit, ingrese el número de saltos unicast que se usa para los paquetes IPv6 originados en el switch.
El número de saltos también se incluye en los anuncios de router y va de 1 a 255, inclusive. El valor predeterminado es 64.

8. En el campo ICMPv6 Rate Limit Error Interval, especifique el número de paquetes de error ICMP permitidos por intervalo de ráfaga.
De forma predeterminada, el intervalo es de 1000 ms (límite de 100 paquetes/s). El intervalo va de 0 a 2147483647 ms. Ingrese 0 para que el switch ignore el número de paquetes de error ICMPv6 permitidos por intervalo de ráfaga.

9. En el campo ICMPv6 Rate Limit Burst Size, especifique el número de paquetes de error ICMP permitidos para el tamaño de ráfaga.
De forma predeterminada, el tamaño de ráfaga es de 100 paquetes. El rango es de 1 a 200. Ingrese 0 para que el switch ignore el número de paquetes de error ICMPv6 permitidos para el tamaño de ráfaga.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar la tabla de rutas IPv6

La tabla de rutas IPv6 incluye todas las rutas, incluidas las mejores rutas y las configuradas. Puede seleccionar qué rutas mostrar.

Para mostrar la tabla de rutas IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Basic > Route Table. Se muestra la página Route Table.

6. En el menú Routes Displayed, seleccione qué rutas se deben mostrar en la tabla:

- All Routes: Todas las rutas IPv6 activas.
- Best Routes Only: Solo las mejores rutas activas.
- Configured Routes Only: Solo las rutas configuradas manualmente.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 97. Información de la tabla de rutas IPv6

Campo	Descripción
Number of Routes	El número total de rutas activas en la tabla de rutas.
IPv6 Prefix	El prefijo de red de la ruta activa.
Prefix Length	La longitud de prefijo de la ruta activa.
Protocol	El tipo de protocolo de la ruta activa.
Next Hop Interface	La interfaz por la que la ruta está activa. En una ruta de rechazo, el siguiente salto es una interfaz nula (Null0).
Next Hop IP Address	La dirección IPv6 del siguiente salto de la ruta activa.
Preference	La preferencia de la ruta configurada.

Configurar interfaces de enrutamiento IPv6

Puede configurar una o más interfaces de enrutamiento IPv6.

Para configurar una o más interfaces de enrutamiento IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Interface Configuration.
Se muestra la página Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú IPv6 Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de enrutamiento IPv6 de la interfaz.
Cuando el modo de enrutamiento IPv6 está habilitado, la interfaz puede operar con IPv6 sin una dirección global. En este caso, se usa una dirección link-local basada en EUI-64. El valor predeterminado es Disable.

9. En el menú DHCPv6 Client Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de cliente DHCPv6 en la interfaz.
Solo una interfaz puede funcionar como cliente DHCPv6. El valor predeterminado es Disable.

10. En el menú Stateless Address AutoConfig Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de configuración automática de direcciones sin estado en la interfaz.
El valor predeterminado es Disable.

11. En el menú Routing Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de enrutamiento de la interfaz.
El valor predeterminado es Disable.

12. En la lista Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo administrativo de la interfaz.
El valor predeterminado es Enable.

13. En el campo MTU, especifique la unidad máxima de transmisión de la interfaz. El rango es de 1280 a 1500. El valor predeterminado es 1500. Si introduce 0, deshabilita el enrutamiento en la interfaz.

14. En el campo Duplicate Address Detection Transmits, especifique el número de transmisiones de detección de direcciones duplicadas (DAD) de la interfaz.
El valor debe estar en el rango de 0 a 600. El valor predeterminado es 1.

15. En el campo Life Time Interval, especifique el intervalo de vida útil que la interfaz transmite en los anuncios de router.
Es la información sobre el periodo durante el cual los vecinos IPv6 pueden usar la interfaz como router predeterminado.

El rango es de 0 a 9000. El valor predeterminado es 1800. El valor debe ser mayor o igual al intervalo máximo de anuncio. Si introduce 0, la interfaz no se puede usar como interfaz de enrutamiento predeterminada.

16. En el campo Adv NS Interval, especifique la información del intervalo de retransmisión que la interfaz transmite en los anuncios de router.
Es la información sobre el intervalo entre retransmisiones de solicitudes de vecino.

El rango es de 1000 a 4294967295.

17. En el campo Adv Reachable Interval, especifique la información del intervalo de alcanzabilidad que la interfaz transmite en los anuncios de router.
Es la información sobre el periodo durante el cual un dispositivo IPv6 remoto se considera alcanzable tras recibir un mensaje de confirmación de descubrimiento de vecinos.

El rango es de 0 a 3600000. El valor predeterminado es 0.

18. En el campo Adv Interval, especifique el periodo entre anuncios de router de la interfaz.

El rango es de 4 a 1800. El valor predeterminado es 600.

19. En el menú Adv Management Config Flag, seleccione Enable o Disable para habilitar o deshabilitar el indicador “managed address configuration flag” del anuncio de router en la interfaz.
Si está habilitado, los nodos finales usan DHCPV6. Si está deshabilitado, los nodos finales configuran las direcciones automáticamente. El valor predeterminado es Disable.

20. En el menú Adv Other Config Flag, seleccione Enable o Disable para habilitar o deshabilitar el indicador “other stateful configuration flag” del anuncio de router en la interfaz. El valor predeterminado es Disable.

21. En el menú Router Preference, seleccione la preferencia de router que anuncia la interfaz.
Puede seleccionar High, Medium o Low. El valor predeterminado es Medium.

22. En la lista Adv Suppress Flag, seleccione Enable o Disable para habilitar o deshabilitar la supresión de anuncios de router en la interfaz.
El valor predeterminado es Disable.

23. En el menú Destination Unreachables, seleccione Enable o Disable para habilitar o deshabilitar la transmisión de mensajes ICMPv6 de destino inalcanzable en la interfaz.
El valor predeterminado es Enable.

24. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

25. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 98. Información de configuración de interfaces IPv6

Campo	Descripción
Operational Mode	El estado operativo de una interfaz. El valor predeterminado es Disable.
Link State	Indica si el enlace está activo o inactivo (Link Up o Link Down).

Configurar los prefijos de una interfaz de enrutamiento IPv6

Puede agregar o cambiar uno o más prefijos y su configuración asociada en una interfaz de enrutamiento IPv6.

Para agregar o cambiar la configuración de prefijos de una interfaz de enrutamiento IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 > Advanced > Prefix Configuration. Se muestra la página Prefix Configuration.

6. En el menú Interface, seleccione la interfaz.

7. Si va a cambiar un prefijo existente de la interfaz, active la casilla del prefijo.

8. Si va a agregar un prefijo nuevo, en el campo IPv6 Prefix, especifique el prefijo IPv6 de la interfaz.

9. Si va a agregar un prefijo nuevo, en el campo Prefix Length, especifique la longitud de prefijo IPv6 de la interfaz.

10. En el menú EUI64, seleccione Enable o Disable para habilitar o deshabilitar el prefijo unicast de 64 bits.

11. En el campo Valid Life Time, especifique el periodo válido de los anuncios de router del prefijo en la interfaz.
Es el periodo durante el cual el prefijo es válido para determinar si está en el enlace (on-link). El rango es de 0 a 4294967295.

12. En el campo Preferred Life Time, especifique el periodo preferido de los anuncios de router del prefijo en la interfaz.
Es el periodo durante el cual el prefijo es preferido para determinar si está en el enlace. Una dirección autoconfigurada generada a partir del prefijo es una dirección preferida. El rango es de 0 a 4294967295.

13. En el menú Onlink Flag, seleccione Enable o Disable para permitir o impedir que el prefijo se use para la configuración autónoma de direcciones.
Si está habilitado, el prefijo puede usarse para determinar si está en el enlace.

14. En el menú Autonomous Flag, permita o impida que el prefijo se use para determinar si está en el enlace.
Si está habilitado, el prefijo puede usarse para la configuración autónoma de direcciones.

15. Realice una de las siguientes acciones:

• Si va a agregar un prefijo nuevo, haga clic en el botón Agregar (Add). Se guarda la configuración. El prefijo se agrega a la interfaz.
• Si va a cambiar un prefijo existente, haga clic en el botón Aplicar (Apply). Se guarda la configuración.

El campo Current State muestra el estado de la dirección IPV6. El estado es TENT (tentativo) si el enrutamiento está deshabilitado o si falla DAD (Duplicate Address Detection). El estado es Active si la interfaz está activa y DAD se completa correctamente.

16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un prefijo de una interfaz de enrutamiento IPv6

Puede eliminar un prefijo y su configuración asociada que ya no necesite en una interfaz de enrutamiento IPv6.

Para eliminar la configuración de un prefijo de una interfaz de enrutamiento IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Prefix Configuration. Se muestra la página Prefix Configuration.

6. En el menú Interface, seleccione la interfaz.
7. Active la casilla del prefijo.

8. Haga clic en el botón Eliminar (Delete).
Se guarda la configuración. Se elimina el prefijo.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar las estadísticas de IPv6 e ICMPv6 de una interfaz de enrutamiento IPv6

Puede mostrar las estadísticas de IPv6 e ICMPv6 de una interfaz de enrutamiento IPv6.

Para mostrar las estadísticas de IPv6 e ICMPv6 de una interfaz de enrutamiento IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Statistics. Se muestra la página Statistics.

6. En el menú Interface, seleccione la interfaz de enrutamiento IPv6.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 99. Información de estadísticas de interfaces IPv6

Campo	Descripción
Total Datagrams Received	El número total de datagramas de entrada recibidos por la interfaz, incluidos los recibidos con errores.
Received Datagrams Locally Delivered	El número total de datagramas entregados correctamente a los protocolos de usuario IPv6 (incluido ICMP). Este contador se incrementa en la interfaz a la que se dirigieron estos datagramas, que puede no ser la interfaz de entrada de algunos de ellos.

Tabla 99. Información de estadísticas de interfaces IPv6 (continuación)

Campo	Descripción
Received Datagrams Discarded Due To Header Errors	El número de datagramas de entrada descartados por errores en sus encabezados IPv6, como discrepancia del número de versión, otros errores de formato, límite de saltos excedido, errores al procesar sus opciones IPv6, etc.
Received Datagrams Discarded Due To MTU	El número de datagramas de entrada que no se pudieron reenviar porque su tamaño superaba la MTU del enlace de la interfaz de salida.
Received Datagrams Discarded Due To No Route	El número de datagramas de entrada descartados porque no se encontró ninguna ruta para transmitirlos a su destino.
Received Datagrams With Unknown Protocol	El número de datagramas dirigidos localmente recibidos correctamente pero descartados por un protocolo desconocido o no compatible. Este contador se incrementa en la interfaz a la que se dirigieron estos datagramas, que puede no ser la interfaz de entrada de algunos de ellos.
Received Datagrams Discarded Due To Invalid Address	El número de datagramas de entrada descartados porque la dirección IPv6 del campo de destino de su encabezado IPv6 no era una dirección válida para recibir en esta entidad. Incluye direcciones no válidas (por ejemplo, ::0) y direcciones no compatibles (como direcciones con prefijos no asignados). En entidades que no son routers IPv6 y, por lo tanto, no reenvían datagramas, este contador incluye los datagramas descartados porque la dirección de destino no era una dirección local.
Received Datagrams Discarded Dut To Truncated Data	El número de datagramas de entrada descartados porque la trama del datagrama no contenía suficientes datos.
Received Datagrams Discarded Other	El número de datagramas IPv6 de entrada sin problemas que se que impidieran continuar su procesamiento, pero que se descartaron por motivos como falta de espacio en búfer. Este contador no incluye los datagramas descartados en espera de reensamblado.
Received Datagrams Reassembly Required	El número de fragmentos IPv6 recibidos que necesitaban reensamblarse en esta interfaz. Este contador se incrementa en la interfaz a la que se dirigieron estos fragmentos, que puede no ser la interfaz de entrada de algunos de ellos.
Datagrams Reassembled	El número de datagramas IPv6 reensamblados correctamente. Este contador se incrementa en la interfaz a la que se dirigieron estos datagramas, que puede no ser necesariamente la interfaz de entrada de algunos de los fragmentos.

Tabla 99. Información de estadísticas de interfaces IPv6 (continuación)

Campo	Descripción
Datagrams Failed To Reassemble	El número de fallas detectadas por el algoritmo de reensamblado IPv6 (por cualquier motivo: tiempo agotado, errores, etc.). No es necesariamente un número de fragmentos IPv6 descartados, ya que algunos algoritmos (en especial el algoritmo de RFC 815) pueden perder la cuenta de los fragmentos al combinarlos a medida que se reciben. Este contador se incrementa en la interfaz a la que se dirigieron estos fragmentos, que puede no ser la interfaz de entrada de algunos de ellos.
Datagrams Forwarded	El número de datagramas de salida que esta entidad recibió y reenvió a su destino final. En entidades que no actúan como routers IPv6, este contador solo incluye los paquetes con enrutamiento de origen a través de esta entidad cuyo procesamiento de ruta de origen fue correcto. Por cada datagrama reenviado correctamente, se incrementa el contador de la interfaz de salida.
Datagrams Locally Transmitted	El número de datagramas que esta entidad transmitió correctamente desde esta interfaz de salida.
Datagrams Transmit Failed	El número de datagramas que esta entidad no pudo transmitir correctamente.
Datagrams Fragmented	El número de datagramas IPv6 que se fragmentaron en esta interfaz de salida del puerto de servicio IPv6.
Datagrams Failed To Fragment	El número de datagramas de salida que no se pudieron fragmentar en esta del puerto de servicio IPv6.
Datagrams Fragments Created	El número de fragmentos de datagramas de salida generados como resultado de la fragmentación en esta interfaz de salida.
Multicast Datagrams Received	El número de paquetes multicast recibidos por la interfaz.
Multicast Datagrams Transmitted	El número de paquetes multicast transmitidos por la interfaz.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 100. Información de estadísticas ICMPv6 de interfaces

Campo	Descripción
Total ICMPv6 Messages Received	El número total de mensajes ICMP recibidos por la interfaz, que incluye todos los contados por IPv6IfIcmpInErrors. Esta interfaz es la interfaz a la que se dirigieron los mensajes ICMP, que puede no ser la interfaz de entrada de los mensajes.
ICMPv6 Messages With Errors recibidos	El número de mensajes ICMP que la interfaz recibió pero determinó que tenían errores específicos de ICMP (suma de verificación ICMP incorrecta, longitud incorrecta, etc.).
ICMPv6 Destination Unreachable Mensajes recibidos	El número de mensajes ICMP Destination Unreachable recibidos por la interfaz.
ICMPv6 Messages Prohibited Administratively Received	El número de mensajes ICMP de destino inalcanzable/comunicación prohibida administrativamente recibidos por la interfaz.
ICMPv6 Time Exceeded Messages recibidos	El número de mensajes ICMP Time Exceeded recibidos por la interfaz.
ICMPv6 Parameter Problem Mensajes recibidos	El número de mensajes ICMP Parameter Problem recibidos por la del puerto de servicio IPv6.
ICMPv6 Packet Too Big Messages recibidos	El número de mensajes ICMP Packet Too Big recibidos por la interfaz.
ICMPv6 Echo Request Messages recibidos	El número de mensajes ICMP Echo (solicitud) recibidos por la interfaz.
ICMPv6 Echo Reply Messages recibidos	El número de mensajes ICMP Echo Reply recibidos por la interfaz.
ICMPv6 Router Solicit Messages recibidos	El número de mensajes ICMP Router Solicit recibidos por la interfaz.
ICMPv6 Router Advertisement Mensajes recibidos	El número de mensajes ICMP Router Advertisement recibidos por la del puerto de servicio IPv6.
ICMPv6 Neighbor Solicit Messages recibidos	El número de mensajes ICMP Neighbor Solicit recibidos por la interfaz.
ICMPv6 Neighbor Advertisement Mensajes recibidos	El número de mensajes ICMP Neighbor Advertisement recibidos por la interfaz.

Tabla 100. Información de estadísticas ICMPv6 de interfaces (continuación)

Campo	Descripción
ICMPv6 Redirect Messages recibidos	El número de mensajes ICMPv6 Redirect recibidos por la interfaz.
ICMPv6 Group Membership Query Mensajes recibidos	El número de mensajes ICMPv6 Group Membership Query recibidos por la interfaz.
ICMPv6 Group Membership Response Messages Received	El número de mensajes ICMPv6 Group Membership Response recibidos por la interfaz.
ICMPv6 Group Membership Reduction Messages Received	El número de mensajes ICMPv6 Group Membership Reduction recibidos por la interfaz.
Total ICMPv6 Messages transmitidos	El número total de mensajes ICMP que esta interfaz intentó enviar. Este contador incluye todos los contados por icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	El número de mensajes ICMP que esta interfaz no envió porque problemas detectados dentro de ICMP, como falta de búferes. Este valor no incluye errores detectados fuera de la capa ICMP, como la IPv6 no pudo enrutar el datagrama resultante. En algunas implementaciones puede que ningún tipo de error contribuya al valor de este contador.
ICMPv6 Destination Unreachable Messages Transmitted	El número de mensajes ICMP Destination Unreachable enviados por la del puerto de servicio IPv6.
ICMPv6 Messages Prohibited Administratively Transmitted	Número de mensajes ICMP de destino inalcanzable/ comunicación prohibida administrativamente enviados.
ICMPv6 Time Exceeded Messages transmitidos	El número de mensajes ICMP Time Exceeded enviados por la interfaz.
ICMPv6 Parameter Problem Messages Transmitted	El número de mensajes ICMP Parameter Problem enviados por la interfaz.
ICMPv6 Packet Too Big Messages transmitidos	El número de mensajes ICMP Packet Too Big enviados por la interfaz.
ICMPv6 Echo Request Messages transmitidos	El número de mensajes ICMP Echo (solicitud) enviados por la interfaz.
ICMPv6 Echo Reply Messages transmitidos	El número de mensajes ICMP Echo Reply enviados por la interfaz.

Tabla 100. Información de estadísticas ICMPv6 de interfaces (continuación)

Campo	Descripción
ICMPv6 Router Solicit Messages transmitidos	El número de mensajes ICMP Neighbor Solicitation enviados por la del puerto de servicio IPv6.
ICMPv6 Router Advertisement Messages Transmitted	El número de mensajes ICMP Router Advertisement enviados por la del puerto de servicio IPv6.
ICMPv6 Neighbor Solicit Messages transmitidos	El número de mensajes ICMP Neighbor Solicitation enviados por la del puerto de servicio IPv6.
ICMPv6 Neighbor Advertisement Messages Transmitted	El número de mensajes ICMP Neighbor Advertisement enviados por la del puerto de servicio IPv6.
ICMPv6 Redirect Messages transmitidos	El número de mensajes Redirect enviados.
ICMPv6 Group Membership Query Messages Transmitted	El número de mensajes ICMPv6 Group Membership Query enviados.
ICMPv6 Group Membership Response Messages Transmitted	El número de mensajes ICMPv6 Group Membership Response enviados.
ICMPv6 Group Membership Reduction Messages Transmitted	El número de mensajes ICMPv6 Group Membership Reduction enviados.
ICMPv6 Duplicate Address Detects	El número de direcciones duplicadas detectadas por la interfaz.

Mostrar la tabla de vecinos IPv6 o borrar entradas de vecinos IPv6

Puede mostrar los dispositivos vecinos IPv6 que detecta el switch o borrar entradas de vecinos IPv6 de la tabla de vecinos.

Para mostrar la tabla de vecinos IPv6 o borrar entradas de vecinos IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Neighbor Table. Se muestra la página Neighbor Table.

6. En el menú Search By, seleccione uno de los siguientes métodos para buscar vecinos IPv6:

- IPv6 Address: Introduzca la dirección IPv6 hexadecimal de 128 bytes en grupos de cuatro dígitos separados por dos puntos, por ejemplo, 2001:231F:::1. Luego haga clic en el botón Go. Si la dirección existe, se muestra esa entrada. Se requiere una coincidencia exacta.
- Interface: Introduzca el ID de interfaz en formato unidad/puerto, por ejemplo, 0/4. Luego haga clic en el botón Go. Si la dirección existe, se muestra esa entrada.

7. Para borrar los vecinos IPv6 que se muestran, haga clic en el botón Borrar (Clear).
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

9. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 101. Tabla de vecinos IPv6 avanzada

Campo	Descripción
Interface	La interfaz cuya configuración se muestra.
IPv6 Address	La dirección IPv6 del vecino o de la interfaz.
MAC Address	La dirección MAC asociada a una interfaz.
isRtr	Indica si el vecino es un router. Si el vecino es un router, el campo muestra True. Si el vecino no es un router, el campo muestra False.

Tabla 101. Tabla de vecinos IPv6 avanzada (continuación)

Campo	Descripción
Neighbor State	El estado de la entrada de la caché de vecinos. Los estados de las entradas dinámicas en la caché de descubrimiento de vecinos IPv6 son los siguientes: • Incmp: Se está realizando la resolución de dirección de la entrada. Se envió un mensaje de solicitud de vecino a la dirección multicast de nodo solicitado del destino, pero aún no se ha recibido el mensaje de anuncio de vecino correspondiente. • Reach: Se recibió confirmación positiva dentro de los últimos “ReachableTime” milisegundos de que la ruta de reenvío al vecino funcionaba correctamente. En estado REACH, el dispositivo no realiza ninguna acción especial al enviar paquetes. • Stale: Transcurrieron más de “ReachableTime” milisegundos desde la última confirmación positiva de que la ruta de reenvío funcionaba correctamente. En estado STALE, el dispositivo no realiza ninguna acción hasta que se envía un paquete. • Delay: Transcurrieron más de “ReachableTime” milisegundos desde la última confirmación positiva de que la ruta de reenvío funcionaba correctamente. Se envió un paquete en los últimos DELAY_FIRST_PROBE_TIME segundos. Si no se recibe confirmación de alcanzabilidad en DELAY_FIRST_PROBE_TIME segundos tras entrar en el estado DELAY, se envía un mensaje de solicitud de vecino y el estado cambia a PROBE. • Probe: Se busca activamente una confirmación de alcanzabilidad reenviando mensajes de solicitud de vecino cada “RetransTimer” milisegundos hasta recibir una confirmación de alcanzabilidad.
Last Updated	El tiempo transcurrido desde que se confirmó que la dirección era alcanzable.

Configurar rutas estáticas IPv6

Puede agregar o cambiar una ruta estática IPv6.

Para agregar o cambiar una ruta estática IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Static Route Configuration. Se muestra la página Static Route Configuration.

6. Si va a cambiar una ruta existente, active la casilla de la ruta. El único campo que puede cambiar es la preferencia de la ruta.

7. Si va a agregar una ruta nueva, en el campo IPv6 Prefix, especifique el prefijo IPv6 de la ruta.

8. Si va a agregar una ruta nueva, en el campo Prefix Length, especifique la longitud de prefijo IPv6 de la ruta.

9. Si va a agregar una ruta nueva, en el menú Next Hop IPv6 Address Type, seleccione una de las siguientes opciones:

- Global: Cree una ruta IPv6 global especificando la interfaz de la ruta.
- Link-Local: Cree una dirección IPv6 link-local especificando la interfaz y la dirección del siguiente salto de la ruta.
- Static-Reject: Cree una ruta de rechazo estática para un prefijo de destino. No puede especificar una interfaz ni una dirección de siguiente salto para la ruta.

10. Si está agregando una nueva ruta y seleccionó Global o Link-Local en el menú Next Hop IPv6 Address Type, especifique la dirección IPv6 del siguiente salto en el campo Next Hop IPv6 Address.

11. Si está agregando una nueva ruta y seleccionó Link-Local en el menú Next Hop IPv6 Address Type, especifique la interfaz para la ruta.

12. En el campo Preference, especifique la preferencia de la ruta.
El rango es de 1 a 255. Puede agregar la preferencia para una nueva ruta o cambiar la preferencia de una ruta existente.

13. Realice una de las siguientes acciones:

- Si está agregando una nueva ruta, haga clic en el botón Add.
La configuración se guarda. Se agrega la ruta.
- Si está cambiando una ruta existente, haga clic en el botón Apply. La configuración se guarda.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una ruta estática IPv6

Puede eliminar una ruta estática IPv6 que ya no necesite.

Para eliminar una ruta estática IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Static Route Configuration. Se muestra la página Static Route Configuration.

6. Marque la casilla de la ruta.

7. Haga clic en el botón Delete.
Se guarda la configuración. La ruta se elimina.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar la preferencia de rutas IPv6 del switch

Puede configurar la preferencia predeterminada del switch, que es un valor en el rango de 1 a 255 y es independiente de las métricas de ruta. La mayoría de los protocolos de enrutamiento usan una métrica de ruta para determinar la ruta más corta conocida por el protocolo, independientemente de cualquier otro protocolo. La mejor ruta a un destino se selecciona automáticamente determinando la ruta con el valor de preferencia más bajo. Si existen varias rutas a un destino, el valor de preferencia se usa para determinar la ruta preferida. Si hay un empate, se selecciona la ruta con la mejor métrica.

Configurar la preferencia de rutas IPv6 del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Route Preference. Se muestra la página Route Preference.

6. En el campo Static, especifique el valor de preferencia de rutas estáticas del switch. El rango es de 1 a 255. El valor predeterminado es 1.

7. Haga clic en el botón Apply.
La configuración se guarda.

El campo Local muestra la preferencia local.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar túneles IPv6

Puede agregar un nuevo túnel IPv6 o cambiar un túnel IPv6 existente.

Para agregar un nuevo túnel IPv6 o cambiar un túnel IPv6 existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Tunnel Configuration. Se muestra la página Tunnel Configuration.

6. Si está cambiando un túnel existente, marque la casilla de la ruta.
7. En el menú Tunnel ID, seleccione un ID de túnel.
8. En el menú Mode, seleccione uno de los siguientes modos:

- 6-in-4-configured: Este modo encapsula paquetes IPv6 en una interfaz IPv4.
- 6-to-4: Este modo encapsula paquetes IPv6 y deriva la dirección IPv4 del extremo a partir de las direcciones IPv6 del paquete IPv6.

9. En el menú IPv6 Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de enrutamiento IPv6 de la interfaz.
Cuando el modo de enrutamiento IPv6 está habilitado, la interfaz puede operar con IPv6 sin una dirección global. En este caso, se usa una dirección link-local basada en EUI-64. El valor predeterminado es Disable.

10. En el menú IPv6 Unreachables, seleccione Enable o Disable para habilitar o deshabilitar la transmisión de mensajes ICMPv6 Destination Unreachable. Si selecciona Enable, se pueden enviar mensajes ICMPv6 de destino inalcanzable.

11. En el campo IPv6 Address/Prefix Length, especifique una dirección IPv6 y una longitud de prefijo. Especifique la dirección con el formato prefijo/longitud.

12. En el menú EUI64, seleccione Enable o Disable para habilitar o deshabilitar el prefijo unicast de 64 bits.
Para túneles 6to4, configure la dirección IPv6 con los primeros 48 bits con el formato 2002:tunnel-source-IPv4-address::/48.

13. En el campo Source Address, especifique la dirección IPv4 de origen del túnel. Ingrese la dirección en notación decimal con puntos.

14. En el menú Source Interface, seleccione la interfaz para el túnel. La dirección IPv6 asociada con la interfaz seleccionada se usa como dirección de origen.

15. En el campo Destination Address, ingrese la dirección IPv4 de destino del túnel. Ingrese la dirección en notación decimal con puntos.

16. Realice una de las siguientes acciones:

- Si está agregando un nuevo túnel, haga clic en el botón Add.
La configuración se guarda. Se agrega la ruta.
- Si está cambiando un túnel existente, haga clic en el botón Apply. La configuración se guarda.

El campo Interface Link Status indica si la interfaz del túnel está activa o inactiva.

17. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

Eliminar un túnel IPv6

Puede eliminar un túnel IPv6 que ya no necesite.

Para eliminar un túnel IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> IPv6 > Advanced > Tunnel Configuration. Se muestra la página Tunnel Configuration.

6. Marque la casilla del túnel.

7. Haga clic en el botón Delete.
La configuración se guarda. Se elimina el túnel.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

VLAN de enrutamiento

Puede configurar algunas interfaces para admitir VLAN y otras interfaces para admitir enrutamiento. También puede configurar una VLAN para que funcione como si fuera una interfaz de enrutamiento.

Cuando una interfaz está habilitada para puenteo (la configuración predeterminada) en lugar de enrutamiento, se realiza todo el procesamiento normal de puente para un paquete entrante, que luego se asocia con una VLAN. Su dirección MAC de destino (MAC DA) y su ID de VLAN se usan para buscar en la tabla de direcciones MAC. Si el enrutamiento está habilitado para la VLAN y la MAC DA de un paquete unicast entrante es la de la interfaz interna puente-router, el paquete se enruta. Un paquete multicast entrante se reenvía a todos los puertos de la VLAN, además de la interfaz interna puente-router, si se recibió en una VLAN enrutada.

Como una interfaz puede pertenecer a más de una VLAN, el enrutamiento de VLAN puede estar habilitado para todas las VLAN de la interfaz o para un subconjunto. El enrutamiento de VLAN puede usarse para permitir que más de un puerto físico resida en la misma subred. También puede usarse cuando una VLAN abarca varias redes físicas, o cuando se requiere segmentación o seguridad adicional.

Una interfaz puede ser una interfaz VLAN o una interfaz de enrutamiento, pero no ambas. Sin embargo, una interfaz VLAN puede formar parte de una VLAN que funciona como interfaz de enrutamiento.

Crear una VLAN de enrutamiento con el asistente de enrutamiento estático de VLAN

El asistente de enrutamiento estático de VLAN le permite crear una VLAN y agregarle interfaces. El asistente también le permite agregar interfaces seleccionadas como un grupo de agregación de enlaces (LAG). Con el asistente, puede hacer lo siguiente:

- Crear una VLAN y generar un nombre único para la VLAN.
- Agregar interfaces seleccionadas a la VLAN recién creada o quitar interfaces seleccionadas de la VLAN predeterminada.
- Agregar interfaces seleccionadas a un LAG y agregar el LAG a una VLAN recién creada.
- Habilitar el etiquetado en las interfaces seleccionadas si la interfaz es miembro de otra VLAN. O deshabilitar el etiquetado si la interfaz seleccionada no es miembro de otra VLAN.
- Excluir puertos de la VLAN.
- Habilitar el enrutamiento en la VLAN y especificar una dirección IP y una máscara de subred para el enrutamiento.

Para crear una VLAN de enrutamiento con el asistente de enrutamiento estático de VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Routing> VLAN > VLAN Static Routing Wizard. Se muestra la página VLAN Static Routing Wizard.

6. En el campo VLAN ID, especifique el identificador de VLAN (VID) que debe asociarse con la VLAN.
El rango es de 1 a 4093.

7. En el campo IP Address, especifique la dirección IPv4 de la interfaz de enrutamiento de la VLAN.
8. En el campo Network Mask, especifique la máscara de subred de la interfaz de enrutamiento de la VLAN.

9. En la tabla Ports, haga clic en un puerto una, dos o tres veces para configurar uno de los siguientes modos:

- Miembro T (con etiqueta): El puerto se agrega como miembro con etiqueta de la VLAN.
- Miembro U (sin etiqueta): El puerto se agrega como miembro sin etiqueta de la VLAN.
- Miembro excluido: De forma predeterminada, la selección está en blanco, lo que significa que el puerto está excluido de la VLAN. Un puerto excluido aún puede agregarse dinámicamente a la VLAN mediante GVRP.

10. En la tabla LAG, haga clic en un LAG una, dos o tres veces para configurar uno de los siguientes modos:

- Miembro T (con etiqueta): El LAG se agrega como miembro con etiqueta de la VLAN.
- Miembro U (sin etiqueta): El LAG se agrega como miembro sin etiqueta de la VLAN.
- Miembro excluido: De forma predeterminada, la selección está en blanco, lo que significa que el LAG está excluido de la VLAN. Un LAG excluido aún puede agregarse dinámicamente a la VLAN mediante GVRP.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar el enrutamiento para una VLAN existente

Para una VLAN existente, puede agregar o cambiar una dirección IPv4 y una máscara de subred y configurar el enrutamiento para la VLAN.

Para agregar o cambiar el enrutamiento de una VLAN existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing> VLAN > VLAN
Routing. Se muestra la página VLAN Routing.

6. Si está cambiando una VLAN de enrutamiento existente, marque la casilla de la VLAN.

7. Si está agregando una nueva VLAN de enrutamiento, en el menú VLAN ID, seleccione el ID de VLAN. Este menú muestra los ID de todas las VLAN configuradas en este switch.

8. En el campo IP Address, especifique la dirección IP de la VLAN de enrutamiento.
9. En el campo Subnet Mask, especifique la máscara de subred de la VLAN de enrutamiento.
10. Realice una de las siguientes acciones:

- Si está agregando una nueva VLAN de enrutamiento, haga clic en el botón Add. La configuración se guarda. Se agrega la VLAN de enrutamiento.
- Si está cambiando una VLAN de enrutamiento existente, haga clic en el botón Apply. La configuración se guarda.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 102. Información de configuración del enrutamiento de VLAN

Campo	Descripción
Port	La interfaz de la VLAN de enrutamiento.
MAC Address	La dirección MAC de la interfaz de la VLAN de enrutamiento.

Quitar la función de enrutamiento de una VLAN

Puede quitar la función de enrutamiento de una VLAN. Es decir, puede quitar la dirección IP de enrutamiento y la máscara de subred de la VLAN. La VLAN en sí no se elimina.

Para quitar la función de enrutamiento de una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> VLAN > VLAN
Routing. Se muestra la página VLAN Routing.

6. Marque la casilla de la VLAN.

7. Haga clic en el botón Delete.
La configuración se guarda. Se quita la función de enrutamiento de la VLAN, pero la VLAN en sí no se elimina.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Address Resolution Protocol

Address Resolution Protocol (ARP) asocia una dirección MAC de capa 2 con una dirección IPv4 de capa 3. El switch admite la configuración de ARP dinámica y manual. Con la configuración manual de ARP, puede agregar entradas estáticas a la tabla ARP.

ARP es una parte obligatoria del Internet Protocol (IP) y se usa para traducir una dirección IP a una dirección de medio (MAC), definida por una LAN como una LAN Ethernet. Un dispositivo que envía paquetes IP debe conocer la dirección MAC del destino IP, o del router del siguiente salto, si el destino no está en la misma subred. Esto se logra difundiendo un paquete de solicitud ARP, al que el destinatario previsto responde enviando por unicast una respuesta ARP que contiene su dirección MAC. Una vez conocida, la dirección MAC se usa en el campo de dirección de destino del encabezado de capa 2 que se antepone al paquete IP.

La caché ARP es una tabla que se mantiene localmente en cada dispositivo de una red. Las entradas de la caché ARP se aprenden examinando la información de origen en los campos de carga útil del paquete ARP, independientemente de si es una solicitud o una respuesta ARP. Así, cuando se difunde una solicitud ARP a todos los dispositivos de una LAN o VLAN, cada destinatario puede almacenar la IP y la dirección MAC del remitente en su caché ARP. La respuesta ARP (que es un mensaje unicast) normalmente solo la detecta el solicitante, que almacena la información del remitente en su caché ARP. La información más reciente siempre reemplaza el contenido existente en la caché ARP.

La cantidad de entradas ARP admitidas depende del dispositivo.

Un dispositivo puede moverse dentro de una red, lo que significa que la dirección IP del dispositivo que estaba asociada con una dirección MAC ahora está asociada con otra dirección MAC. Un dispositivo también puede desaparecer de la red por completo (por ejemplo, porque se reconfiguró, se desconectó o se apagó). Estas situaciones causan información obsoleta en la caché ARP. Por lo tanto, las entradas se actualizan o se renuevan periódicamente para determinar si una dirección todavía existe. Si una entrada se identificó como remitente de un paquete ARP, la entrada puede eliminarse de la caché ARP. Puede configurar un intervalo de caducidad que determina cuánto tiempo permanece en la caché ARP una entrada que no se actualiza.

Mostrar las entradas ARP de la caché ARP

Puede ver las entradas ARP de la caché ARP. La caché ARP es una tabla que enumera las conexiones remotas que el switch detectó recientemente

Para mostrar las entradas ARP de la caché ARP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> ARP > Basic > ARP Cache. Se muestra la página ARP Cache.

La página muestra la siguiente información:

• IP Address: Muestra la dirección IP asociada con la dirección MAC del sistema. Esta dirección debe ser la dirección IP de un dispositivo en una subred conectada a una de las interfaces de enrutamiento existentes del switch.
• Port: Muestra la unidad/ranura/puerto asociado de la conexión.
• MAC Address: Muestra la dirección MAC unicast del dispositivo. La dirección consiste en seis números hexadecimales de 2 dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40.

La caché ARP puede ser grande. El menú de navegación de paginación funciona de la siguiente manera:

• Rows per page: Seleccione cuántas entradas de la tabla se muestran por página. Los valores posibles son 20, 50, 100, 200 y All. Si selecciona All, el navegador puede tardar en mostrar la información.
• <. Muestra la página anterior de entradas de datos de la tabla.
• >. Muestra la página siguiente de entradas de datos de la tabla.

6. Para actualizar la página, haga clic en el botón Refresh.

Agregar o cambiar una entrada estática en la tabla ARP

Puede agregar una nueva entrada estática a la tabla ARP o cambiar una entrada existente que haya agregado manualmente.

Para agregar una nueva entrada estática o cambiar una entrada existente en la tabla ARP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> ARP > Advanced > ARP Create. Se muestra la página ARP Create.

6. Si está cambiando una entrada ARP existente, marque la casilla de la entrada.

7. En el campo IP Address, especifique la dirección IP que desea agregar.
La dirección debe ser la dirección IP de un dispositivo en una subred conectada a una de las interfaces de enrutamiento existentes del switch.

8. En el campo MAC Address, especifique la dirección MAC unicast del dispositivo. Ingrese la dirección como seis números hexadecimales de 2 dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40.

9. Realice una de las siguientes acciones:

• Si está agregando una nueva entrada ARP, haga clic en el botón Add. La configuración se guarda. Se agrega la entrada ARP.

• Si está cambiando una entrada ARP existente, haga clic en el botón Apply. La configuración se guarda.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La tabla ARP puede ser grande. El menú de navegación de paginación funciona de la siguiente manera:

- Rows per page: Seleccione cuántas entradas de la tabla se muestran por página. Los valores posibles son 20, 50, 100, 200 y All. Si selecciona All, el navegador puede tardar en mostrar la información.
- <. Muestra la página anterior de entradas de datos de la tabla.
- >. Muestra la página siguiente de entradas de datos de la tabla.

La siguiente tabla describe los campos no configurables de la página.

Tabla 103. Información de la caché ARP

Campo	Descripción
IP Address	La dirección IP del dispositivo.
Port	La interfaz asociada (con el formato unidad/puerto) para la conexión del dispositivo.
MAC Address	La dirección MAC unicast del dispositivo.
Type	El tipo de entrada ARP. Los valores posibles son los siguientes: • Local: Una entrada ARP asociada con una de las direcciones MAC de las interfaces de enrutamiento del switch. • Gateway: Una entrada ARP dinámica cuya dirección IP es la de un router. • Static: Una entrada ARP que usted agregó. • Dynamic: Una entrada ARP que el switch aprendió.
Age	El tiempo (en segundos) desde la última actualización de la entrada en la tabla ARP.

Eliminar una entrada ARP estática

Puede eliminar una entrada ARP estática que ya no necesite.

Para eliminar una entrada ARP estática:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> ARP > Advanced > ARP Create. Se muestra la página ARP Create.

6. Marque la casilla de la entrada.

7. Haga clic en el botón Delete.
La configuración se guarda. Se elimina la entrada.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de la tabla ARP o eliminar entradas de la tabla

Puede cambiar los ajustes de configuración de la tabla ARP. También puede eliminar entradas de la tabla, por ejemplo, todas las entradas dinámicas.

Para configurar los ajustes de la tabla ARP o eliminar entradas de la tabla:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing> ARP > Advanced > Global ARP Configuration. Se muestra la página Global ARP Configuration.

6. En el campo Age Time, especifique el periodo en segundos que una entrada ARP dinámica permanece en la tabla ARP antes de caducar.

El rango es de 15 a 21600 segundos. El valor predeterminado es 1200 segundos.

7. En el campo Response Time, especifique el periodo en segundos que el switch espera una respuesta ARP a una solicitud ARP que envía.
El rango es de 1 a 10 segundos. El valor predeterminado es 1 segundo.

8. En el campo Retries, especifique el número máximo de veces que se reintenta una solicitud ARP cuando el switch no recibe una respuesta ARP.
Este número incluye la solicitud ARP inicial. El rango es de 0 a 10. El valor predeterminado es 4.

9. En el campo Cache Size, especifique el número máximo de entradas permitidas en la tabla ARP.
Este número incluye todas las entradas ARP estáticas y dinámicas. El rango es de 384 a 4096. El valor predeterminado es 4096.

10. Seleccione el botón de opción Dynamic Renew Enable o Disable para habilitar o deshabilitar que las entradas ARP dinámicas intenten renovarse automáticamente después de caducar. El valor predeterminado es Enable.

11. Para eliminar ciertas entradas de la tabla ARP, seleccione una de las siguientes opciones en el menú Remove From Table:

- All Dynamic Entries: Se eliminarán todas las entradas dinámicas.
- All Dynamic and Gateway Entries: Se eliminarán todas las entradas dinámicas y de gateway.
- Specific Dynamic/Gateway Entry: Debe especificar la dirección IP de la entrada dinámica o de gateway específica en el campo Remove IP Address.
- Specific Static Entry: Debe especificar la dirección IP de la entrada estática específica en el campo Remove IP Address.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 104. ARP Table Configuration

Campo	Descripción
Total Entry Count	El número total de entradas en la tabla ARP.
Peak Total Entries	El valor más alto alcanzado en el campo Total Entry Count. Este contador se reinicia cuando cambia el tamaño de la caché de la tabla ARP.
Active Static Entries	El número total de entradas estáticas activas en la tabla ARP.
Configured Static Entries	El número total de entradas estáticas configuradas en la tabla ARP.
Maximum Static Entries	El número máximo de entradas estáticas que se pueden definir.

Routing Information Protocol

Routing Information Protocol (RIP) es un protocolo que los switches y routers pueden usar para intercambiar información de topología de red. RIP se clasifica como protocolo de gateway interior y se usa normalmente en redes pequeñas y medianas. Un dispositivo que ejecuta RIP envía el contenido de su tabla de enrutamiento a cada uno de sus dispositivos adyacentes. Cuando una ruta se elimina de la tabla de enrutamiento, los demás dispositivos la marcan como inutilizable y, después de cierto periodo, la eliminan de su enrutamiento.

Existen dos versiones de RIP:

- RIPv1 (definido en RFC 1058):
  - Las rutas se especifican por red IP de destino y número de saltos.
  - La tabla de enrutamiento se difunde a todos los dispositivos de la red conectada.

  RIPv2 (definido en RFC 1723):
  - La especificación de ruta también incluye la máscara de subred y el gateway.
  - La tabla de enrutamiento se envía a una dirección multicast, lo que reduce el tráfico de red.
  - Se usa autenticación por seguridad.

Puede configurar una interfaz para hacer lo siguiente:

- Recibir paquetes en uno o ambos formatos.
- Enviar paquetes con formato RIPv1 o RIPv2, o enviar paquetes RIPv2 a la dirección de difusión de RIPv1.
- Impedir que se reciban paquetes RIP.

- Impedir que se envíen paquetes RIP.

Habilitar o deshabilitar RIP en el switch

De forma predeterminada, RIP está habilitado en el switch.

Para habilitar o deshabilitar RIP en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > RIP > Basic > RIP Configuration. Se muestra la página RIP Configuration.

6. Seleccione el botón de opción RIP Admin Mode Enable o Disable para habilitar o deshabilitar RIP en el switch.
El valor predeterminado es Enable.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes globales de RIP del switch

Puede configurar los ajustes globales de RIP del switch, a diferencia de los ajustes de RIP de interfaces individuales.

Para configurar los ajustes globales de RIP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > RIP > Advanced > RIP Configuration. Se muestra la página RIP Configuration.

6. Seleccione el botón de opción RIP Admin Mode Enable o Disable para habilitar o deshabilitar RIP en el switch.
El valor predeterminado es Enable.

7. Seleccione uno de los siguientes botones de opción de Split Horizon Mode:

- None: No se habilita ningún procesamiento especial.
- Simple: Una ruta no se incluye en las actualizaciones que se envían al dispositivo del que se aprendió. El valor predeterminado es Simple.
- Poison Reverse: Una ruta se incluye en las actualizaciones enviadas al dispositivo del que se aprendió, pero la métrica se establece en infinito.

El horizonte dividido (split horizon) es una técnica para evitar problemas que podrían causarse al incluir rutas en las actualizaciones enviadas a un dispositivo del que la ruta se aprendió originalmente.

8. Seleccione el botón de opción Auto Summary Mode Enable o Disable para habilitar o deshabilitar que grupos de rutas adyacentes se resuman en entradas únicas. Si selecciona el botón de opción Enable, las rutas adyacentes se resumen en entradas únicas para reducir el número total de entradas. El valor predeterminado es Disable.

9. Seleccione el botón de opción Host Routes Accept Mode Enable o Disable para habilitar o deshabilitar que el switch acepte rutas de host.
Si selecciona el botón de opción Enable, el switch acepta rutas de host. El valor predeterminado es Enable.

10. Seleccione el botón de opción Default Information Originate Enable o Disable para habilitar o deshabilitar los anuncios de ruta predeterminada.
El valor predeterminado es Disable.

11. En el campo Default Metric, especifique un valor de métrica para las rutas redistribuidas. El rango es de 1 a 15. El valor predeterminado es 0.

12. Haga clic en el botón Apply.

La configuración se guarda.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 105. Información de configuración de RIP

Campo	Descripción
Global Route Changes	El número de cambios de ruta realizados por RIP en la base de datos de rutas IP. Esto no incluye la actualización de una ruta después de caducar.
Global Queries	El número de respuestas enviadas a consultas RIP de otros dispositivos.

Configurar los ajustes de interfaz RIP

Puede configurar ajustes de RIP que se aplican a interfaces individuales.

Para configurar los ajustes de interfaz RIP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > RIP > Advanced > Interface Configuration. Se muestra la página Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Send Version, seleccione la versión de los paquetes de control RIP que envía la interfaz:

- None. No se envían paquetes de control RIP.
- RIP-1: Envía paquetes con formato RIP versión 1 por broadcast.
- RIP-1c: Envía paquetes en modo de compatibilidad con RIP versión 1 y paquetes con formato RIP versión 2 por broadcast.
- RIP-2: Envía paquetes RIP versión 2 por multicast. El valor predeterminado es RIP-2.

9. En el menú Receive Version, seleccione la versión de los paquetes de control RIP que acepta la interfaz:

- RIP-1: Acepta solo paquetes con formato RIP versión 1.
- RIP-2: Acepta solo paquetes con formato RIP versión 2.
- Both: Acepta paquetes en formato RIP versión 1 o versión 2. El valor predeterminado es Both.
- None: No se aceptan paquetes de control RIP.

10. En el menú RIP Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo RIP de la interfaz.
Antes de habilitar RIP versión 1 o 1c en una interfaz, primero debe habilitar el modo de broadcast dirigido a la red (es decir, el modo RIP) en la interfaz. El valor predeterminado es Disable.

11. En el menú Authentication Type, seleccione el tipo de autenticación:

- None: No se configura ningún protocolo de autenticación. Es el ajuste predeterminado.
- Simple: Se le pide introducir una clave de autenticación. Esta clave se incluye (en formato no cifrado) en el encabezado RIP de todos los paquetes enviados a la red. Todos los dispositivos de la red deben configurarse con la misma clave.
- Encrypt: Se le pide introducir una clave de autenticación y un ID de autenticación. El cifrado usa el algoritmo MD5 Message-Digest. Todos los dispositivos de la red deben configurarse con la misma clave e ID.

12. Si selecciona Simple o Encrypt en el menú Authentication Type, en el campo Authentication Key introduzca la clave de autenticación RIP de la interfaz. La clave puede tener hasta 16 octetos.

13. Si selecciona Encrypt en el menú Authentication Type, en el campo Authentication Key ID introduzca el ID de clave de autenticación RIP de la interfaz.
El ID de clave puede ser de 0 a 255.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para actualizar la página, haga clic en el botón Refresh.
16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 106. Información de configuración de interfaz RIP

Campo	Descripción
Bad Packets Received	El número de paquetes de respuesta RIP recibidos por el proceso RIP que se descartaron posteriormente por cualquier motivo.
Bad Routes Received	El número de rutas en paquetes RIP válidos que se ignoraron por cualquier motivo (por ejemplo, familia de direcciones desconocida o métrica no válida).
Updates Sent	El número de actualizaciones RIP activadas enviadas por la interfaz. Esto explícitamente no incluye las actualizaciones completas enviadas con información nueva.
IP Address	La dirección IP de la interfaz del router.
Link State	Indica si la interfaz del router RIP está activa o inactiva.

Configurar la redistribución de rutas RIP y mostrar el resumen de redistribución de rutas

Puede configurar los ajustes de redistribución de rutas RIP y mostrar el resumen de redistribución de rutas.

Para configurar la redistribución de rutas RIP y mostrar el resumen de redistribución de rutas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > RIP > Advanced > Route Redistribution. Se muestra la página Route Redistribution.

Las opciones del menú Source incluyen solo las rutas de origen que ya están configuradas para redistribución por RIP. Esto le permite configurar otra ruta de origen entre las rutas de origen disponibles.

6. En el menú Source, seleccione uno de los siguientes tipos de rutas de origen:

- Connected: Permite configurar los ajustes de las rutas conectadas.
- Static: Permite configurar los ajustes de las rutas estáticas.

7. En el menú Redistribute Mode, seleccione Enable o Disable para habilitar o deshabilitar el modo de redistribución RIP para el tipo de ruta de origen seleccionado.
El valor predeterminado es Disable.

8. En el campo Metric, especifique el valor de métrica de las rutas redistribuidas del tipo de ruta de origen seleccionado.
El rango es de 0 a 15. El valor predeterminado es 0, que significa que no hay ningún valor de métrica en vigor.

9. En el campo Distribute List, especifique la lista de acceso que debe filtrar las rutas que redistribuirá el protocolo de destino.
Solo se redistribuyen las rutas permitidas. Si este campo hace referencia a una lista de acceso inexistente, se permiten todas las rutas. El rango de ID de lista de acceso es de 0 a 199. (Para más información, consulte Listas de control de acceso en la página 646.)
El valor predeterminado es 0, que significa que no hay ninguna lista de acceso en vigor.

Cuando usa una lista de acceso para filtrar rutas, solo se usan los siguientes campos de la lista de acceso:

- Dirección IP de origen y máscara de red
- Dirección IP de destino y máscara de red
- Acción (permit o deny)

Todos los demás campos (como puerto de origen y destino, precedencia, ToS, etc.) se ignoran.

La dirección IP de origen se compara con la dirección IP de destino de la ruta. La máscara de red IP de origen de la regla de la lista de acceso se trata como máscara comodín e indica qué bits de la dirección IP de origen deben coincidir con la dirección de destino de la ruta.

Nota: Un 1 en la máscara indica que no importa el bit de dirección correspondiente.

Cuando una regla de lista de acceso incluye una dirección IP de destino y máscara de red (lista de acceso extendida), la dirección IP de destino se compara con la máscara de red del destino de la ruta. La máscara de red de destino de la lista de acceso sirve como máscara comodín e indica qué bits de la máscara de destino de la ruta son significativos para la operación de filtrado.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 107. Información de resumen de redistribución de rutas RIP

Campo	Descripción
Source Protocol	El tipo de ruta de origen que redistribuirá RIP: • Connected • Static
Redistribute Mode	Indica si se redistribuye la ruta de un protocolo de origen. De forma predeterminada, la distribución de rutas está deshabilitada.
Metric	La métrica de las rutas redistribuidas para la ruta de origen. El campo muestra 0 si la métrica no está configurada.
Distribute List	La lista de acceso que filtra las rutas que redistribuirá el protocolo de destino. El campo muestra 0 si no hay una ACL configurada para ello.
Match Internal	Indica si se redistribuye una ruta OSPF interna.
Match External Type 1	Indica si se redistribuye una ruta OSPF externa tipo 1.
Match External Type 2	Indica si se redistribuye una ruta OSPF externa tipo 2.
Match NSSA External Type 1	Indica si se redistribuye una ruta OSPF NSSA tipo 1.
Match NSSA External Type 2	Indica si se redistribuye una ruta OSPF NSSA tipo 2.

Descubrimiento de routers y anuncios de router

De forma predeterminada, una interfaz de enrutamiento no envía anuncios de router. Puede habilitar los anuncios de router de una interfaz de enrutamiento y configurar los ajustes de los anuncios de router.

Para configurar el descubrimiento de routers de una interfaz de enrutamiento:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Router Discovery > Router Discovery Configuration. Se muestra la página Router Discovery Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Advertise Mode, seleccione Enable o Disable para habilitar o deshabilitar la transmisión de anuncios de router en la interfaz.
El valor predeterminado es Disable.

9. En el campo Advertise Address, especifique la dirección IPv4 que debe usar la interfaz para los anuncios de router.

10. En el campo Maximum Advertise Interval, especifique el período máximo en segundos permitido entre los anuncios de router enviados desde la interfaz. El período debe estar en el rango de 4 a 1800. El valor predeterminado es 600.

11. En el campo Minimum Advertise Interval, especifique el período mínimo en segundos permitido entre los anuncios de router enviados desde la interfaz. El período debe estar en el rango de 3 a 1800. El valor predeterminado es 450.

12. En el campo Advertise Lifetime, especifique el período máximo en segundos durante el cual los hosts consideran la dirección anunciada por la interfaz como una dirección de router válida.
El período debe estar en el rango de 4 a 9000. El valor predeterminado es 1800.

13. En el campo Preference Level, especifique el nivel de preferencia de la interfaz del router como router predeterminado respecto a otros routers de la misma subred.
Un número más alto significa que la dirección anunciada recibe mayor preferencia. El valor predeterminado es 0.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

5

Configurar el enrutamiento multicast

Este capítulo trata los siguientes temas:

- Enrutamiento multicast IPv4 y tabla de rutas multicast IPv4
- IGMP para enrutamiento multicast IPv4
- PIM para enrutamiento multicast IPv4
- Rutas multicast estáticas para direcciones IPv4
- Límites administrativos multicast para direcciones IPv4
- Enrutamiento multicast IPv6 y tabla de rutas multicast IPv6
- PIM para enrutamiento multicast IPv6
- MLD para enrutamiento multicast IPv6
- Rutas multicast estáticas para direcciones IPv6

Enrutamiento multicast IPv4 y tabla de rutas multicast IPv4

Multicast es ideal para tráfico de video y audio que requiere control de paquetes multicast para un funcionamiento óptimo. Multicast para IPv4 admite IGMPv1, IGMPv2 e IGMPv3. La comunicación de punto a multipunto se denomina multicast. El host de origen (punto) transmite un mensaje a un grupo de cero o más hosts (multipunto) identificados por una sola dirección IPv4 de destino. Aunque la tarea puede lograrse enviando mensajes unicast (punto a punto) a cada host de destino, multicast es el método preferido para este tipo de transmisión. Un mensaje multicast se entrega a todos los miembros de su grupo de hosts de destino con la misma fiabilidad de mejor esfuerzo que los mensajes IPv4 unicast normales. No se garantiza que el mensaje llegue intacto a todos los miembros del grupo de destino ni en el mismo orden respecto a otros mensajes.

Mostrar la tabla de rutas multicast IPv4

La tabla de enrutamiento multicast (Mroute) incluye información sobre la dirección IPv4 de origen, las direcciones IPv4 de destino del grupo, las interfaces de entrada y salida, los siguientes saltos a los que debe reenviarse el paquete IPv4 y los protocolos admitidos.

Para mostrar la tabla Mroute IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Mroute Table. Se muestra la página Mroute Table.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 108. Información de la tabla Mroute IPv4 multicast

Campo	Descripción
Group IP	La dirección IPv4 del grupo de destino.
Source IP	La dirección IPv4 del origen del paquete multicast, que se combina con la IPv4 del grupo para identificar por completo una sola ruta.
Incoming Interface	La interfaz de entrada por la que llegan los paquetes multicast de este origen/grupo.
Outgoing Interfaces	La lista de interfaces de salida por las que se reenvían los paquetes multicast de este origen/grupo.
Up Time (hh:mm:ss)	El tiempo en segundos desde que se creó la entrada.
Expiry Time (hh:mm:ss)	El tiempo en segundos antes de que esta entrada caduque y se elimine de la tabla.
RPF Neighbor	La dirección IPv4 del vecino de reenvío por ruta inversa (RPF).
Protocol	El protocolo de enrutamiento multicast que creó dinámicamente esta entrada. Los valores posibles son los siguientes: • PIM-DM • PIM-SM
Flags	El valor de este campo es válido si el protocolo de enrutamiento multicast es PIM-SM. Los valores posibles son RPT y SPT. Para otros protocolos se muestra “------”.

Agregar entradas multicast estáticas a la tabla Mroute IPv4

Puede agregar una entrada multicast estática a la tabla Mroute IPv4.

Para agregar una entrada multicast estática a la tabla Mroute IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Mroute Static-Multicast Configuration.
Se muestra la página Mroute Static-Multicast Configuration.

6. En el campo Group IP, especifique la dirección IP del grupo multicast.

7. En el campo Egress VLAN List, especifique la VLAN o VLAN a las que pertenece la dirección IP del grupo multicast.

8. Haga clic en el botón Add.
Se guardan los ajustes. Se agrega la entrada multicast.

9. Para actualizar la página, haga clic en el botón Refresh.
10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 109. Información de configuración de Mroute multicast estático

Campo	Descripción
Maximum Multicast Static Address Count	El número máximo de direcciones multicast estáticas que puede contener la tabla Mroute.
Current Multicast Static Address Count	El número de direcciones multicast estáticas que agregó a la tabla Mroute.

Eliminar una entrada multicast estática de la tabla Mroute IPv4

Puede eliminar de la tabla de rutas IPv4 una entrada multicast estática que ya no necesite.

Para eliminar una entrada multicast estática de la tabla Mroute IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Mroute Static-Multicast Configuration.
Se muestra la página Mroute Static-Multicast Configuration.

6. Seleccione la casilla de la entrada multicast.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la entrada multicast.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes globales de multicast del switch

Puede configurar los ajustes globales de multicast del switch, a diferencia de los ajustes multicast de una interfaz.

Para configurar los ajustes globales de multicast del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Global Configuration.
Se muestra la página Global Configuration.

6. Seleccione el botón de opción Admin Mode Enable o Disable para habilitar o deshabilitar el estado administrativo del reenvío multicast en el switch.
El valor predeterminado es Disable.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 110. Información de configuración global de multicast

Campo	Descripción
Protocol State	El estado operativo del reenvío multicast.
Table Maximum Entry Count	El número máximo de entradas de la tabla Mroute.
Protocol	El protocolo de enrutamiento multicast activo en el switch, si hay algún protocolo activo.
Table Entry Count	El número de entradas de rutas multicast presentes en la tabla Mroute.

Configurar una interfaz multicast

Puede configurar una o más interfaces multicast.

Para configurar una interfaz multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Interface Configuration.
Se muestra la página Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el campo TTL Threshold, especifique el umbral por debajo del cual un paquete de datos multicast no se reenvía desde la interfaz.
Introduzca un número entre 0 y 255. El valor predeterminado es 1. Si introduce 0, se reenvían todos los paquetes multicast de la interfaz. Debe configurar al menos una interfaz de router antes de que este campo esté disponible.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

IGMP para enrutamiento multicast IPv4

Puede configurar los ajustes de Internet Group Management Protocol (IGMP) y ver las estadísticas de IGMP.

IGMP snooping permite al switch reenviar el tráfico multicast de forma inteligente. Según los mensajes de consulta y reporte IGMP, el switch reenvía el tráfico solo a los puertos que solicitan el tráfico multicast, en lugar de a todos los puertos.

IGMP snooping ayuda a optimizar el rendimiento multicast y es especialmente útil para aplicaciones IP multicast con alto consumo de ancho de banda, como el streaming de medios en línea.

Configurar los ajustes globales de IGMP del switch

Puede configurar los ajustes globales de IGMP del switch, a diferencia de los ajustes IGMP de una interfaz.

Para configurar los ajustes globales de IGMP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción Admin Mode Enable o Disable para habilitar o deshabilitar IGMP en el switch.
El valor predeterminado es Disable.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz de enrutamiento IGMP

Puede configurar una o más interfaces de enrutamiento IGMP.

Para configurar una interfaz de enrutamiento IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > Routing Interface Configuration. Se muestra la página Routing Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar IGMP en la interfaz.
El valor predeterminado es Disable.

9. En el campo Version, especifique la versión de IGMP de la interfaz. La versión puede ser 1, 2 o 3. El valor predeterminado es 3. Este campo solo es configurable cuando el modo IGMP Interface está habilitado.

10. En el campo Robustness, introduzca el valor de robustez de la interfaz. Este valor permite ajustar la pérdida de paquetes esperada en una subred. Si espera que la subred tenga pérdidas, introduzca un número más alto. IGMP tolera (variable de robustez –1) pérdidas de paquetes. El valor es de 1 a 255. El valor predeterminado es 2.

11. En el campo Query Interval, introduzca la frecuencia en segundos con la que se transmiten los paquetes de consulta de host IGMP en la interfaz.
El valor es de 1 a 3600. El valor predeterminado es 125.

12. En el campo Query Max Response Time, introduzca el tiempo máximo de respuesta a consultas, en décimas de segundo, que se anunciará en las consultas IGMPv2 de la interfaz. El valor es de 0 a 255. El valor predeterminado es 100.

13. En el campo Startup Query Interval, introduzca el número de segundos entre las transmisiones de consultas de inicio en la interfaz.
El valor es de 1 a 300. El valor predeterminado es 31.

14. En el campo Startup Query Count, introduzca el número de consultas que se enviarán al inicio, separadas por el intervalo de consultas de inicio.
El valor es de 1 a 20. El valor predeterminado es 2.

15. En el campo Last Member Query Interval, introduzca el intervalo de consulta del último miembro en décimas de segundo.

Este valor es el tiempo máximo de respuesta que se inserta en las consultas específicas de grupo enviadas en respuesta a mensajes de abandono de grupo, y también es el período entre mensajes de consulta específicos de grupo. El valor es de 0 a 255. El valor predeterminado es 10. Este valor no se usa en IGMP versión 1.

16. En el campo Last Member Query Count, introduzca el número de consultas que se enviarán al recibir un reporte de abandono de grupo.
El valor es de 1 a 20. El valor predeterminado es 2.

17. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

18. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar las estadísticas de las interfaces de enrutamiento IGMP

Puede mostrar las estadísticas de las interfaces de enrutamiento IGMP.

Para mostrar las estadísticas de las interfaces de enrutamiento IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > Routing Interface Statistics. Se muestra la página Routing Interface Statistic.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Para actualizar la página, haga clic en el botón Refresh.

La siguiente tabla describe los campos no configurables de la página.

Tabla 111. Información de estadísticas de interfaz de enrutamiento IGMP

Campo	Descripción
Interface	La interfaz en la que está habilitado IGMP.
IP Address	La dirección IP de la interfaz.
Subnet Mask	La máscara de subred de la dirección IP de la interfaz.
Protocol State	El estado operativo de IGMP en la interfaz (Operational o Non-Operational).
Querier IP	La dirección del consultor (querier) IGMP en la subred IP a la que está conectada la interfaz.
Querier Status	Indica si la interfaz está en modo querier o non-querier.
Querier Up Time	El período en segundos desde el último cambio del querier de la interfaz IGMP.
Querier Expiry Time	El período en segundos que falta para que caduque el temporizador de presencia de otro querier. Si el switch es el querier, es cero.
Wrong Version Queries Received	El número de consultas recibidas en la interfaz con una versión de IGMP que no coincide con la versión de IGMP configurada para la interfaz, durante la vida útil de la entrada. IGMP requiere que todos los routers o interfaces de enrutamiento de una LAN estén configurados con la misma versión de IGMP. Por lo tanto, si se reciben consultas con un número de versión incorrecto, se indica un error de configuración.
Number of Joins Received	El número de veces que se agregó una membresía de grupo en la interfaz; es decir, el número de veces que se agregó una entrada de la interfaz a la tabla de caché. Esto da una idea de la cantidad de actividad IGMP en la del puerto de servicio IPv6.
Number of Groups	El número actual de entradas de la interfaz en la tabla de caché.

Mostrar los grupos IGMP y buscar en la base de datos de grupos IGMP

Puede mostrar la información de grupos IGMP y buscar en la base de datos de grupos IGMP por interfaz o por grupo.

Para mostrar los grupos IGMP y buscar en la base de datos de grupos IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > IGMP Groups. Se muestra la página IGMP Groups.

6. Para buscar entradas de grupos IGMP por interfaz o grupo, seleccione una de las siguientes opciones del menú Search:

• Interface: Seleccione Interface en el menú, especifique la interfaz en formato unidad/puerto (por ejemplo, 0/8) y haga clic en el botón Go.
Si la entrada existe, se muestra como la primera entrada, seguida de las demás entradas.
• Group: Seleccione Group en el menú, especifique la dirección IPv4 del grupo multicast y haga clic en el botón Go.
Si la entrada existe, la entrada con la dirección IPv4 de grupo coincidente se muestra como la primera, seguida de las demás. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 112. Información de grupos IGMP

Campo	Descripción
Interface	La interfaz en la que está habilitado IGMP.
Multicast Group IP	La dirección del grupo multicast IP.
Last Reporter	La dirección IP del origen del último informe de membresía recibido para la dirección del grupo multicast IP en la interfaz.

Tabla 112. Información de grupos IGMP (continuación)

Campo	Descripción
Up Time	El tiempo transcurrido desde que se creó esta entrada.
Expiry Time	El tiempo restante antes de que esta entrada caduque.
Version 1 Host Timer	El tiempo restante hasta que el switch determina que no hay miembros de IGMP versión 1 en la subred IP conectada a la interfaz. Al recibir un informe de membresía IGMPv1, este temporizador se restablece al temporizador de membresía del grupo. Mientras no llegue a cero, el switch ignora los mensajes IGMPv2 leave de este grupo que reciba en la interfaz. Este campo solo aparece si la interfaz está configurada para IGMP versión 1.
Version 2 Host Timer	El tiempo restante hasta que el switch determina que no hay miembros de IGMP versión 2 en la subred IP conectada a la interfaz. Al recibir un informe de membresía IGMPv2, este temporizador se restablece al temporizador de membresía del grupo. Mientras no llegue a cero, el switch ignora los mensajes IGMPv1 e IGMPv3 leave de este grupo que reciba en la interfaz seleccionada. Este campo solo aparece si la interfaz está configurada para IGMP versión 2.
Compatibility	El modo de compatibilidad (v1, v2 o v3) del grupo en la interfaz.
Filter Mode	El modo de filtro de origen (Include, Exclude o NA) del grupo en la interfaz. Si el modo es NA, el campo está en blanco.

Mostrar la información de membresía IGMP y buscar en la base de datos de membresía IGMP

Puede mostrar la información de membresía IGMP y buscar en la base de datos de membresía IGMP por interfaz o por grupo.

Para mostrar la información de membresía IGMP y buscar en la base de datos de membresía IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > IGMP Membership. Aparece la página IGMP Membership.

6. Para buscar la membresía IGMP por interfaz o grupo, seleccione una de las siguientes opciones del menú Search:

• Interface: Seleccione Interface en el menú, especifique la interfaz en formato unidad/puerto (por ejemplo, 0/8) y haga clic en el botón Go.
Si la entrada existe, se muestra como la primera entrada, seguida de las demás entradas.
• Group: Seleccione Group en el menú, especifique la dirección IP del grupo multicast y haga clic en el botón Go.
Si la entrada existe, la entrada con la dirección IP de grupo coincidente se muestra como la primera, seguida de las demás. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 113. Información de membresía IGMP

Campo	Descripción
Interface	La interfaz por la que se reenvían los paquetes multicast.
Group IP	La dirección del grupo multicast IP.
Compatibility Mode	El modo de compatibilidad (v1, v2 o v3) del grupo en la interfaz.
Source Filter Mode	El modo de filtro de origen (Include, Exclude o NA) del grupo en la interfaz. Si el modo es NA, el campo está en blanco.

Tabla 113. Información de membresía IGMP (continuación)

Campo	Descripción
Source Hosts	Las direcciones IP de origen que son miembros de la dirección multicast.
Expiry Time	El tiempo de expiración de cada dirección IP de origen que es miembro del grupo multicast. Es el tiempo tras el cual caduca la entrada de origen.

Configurar una interfaz proxy IGMP

Puede configurar una interfaz proxy IGMP. Se aplican los siguientes requisitos:

- El enrutamiento, IGMP y multicast deben estar habilitados globalmente en el switch.
- Debe configurar al menos una interfaz de enrutamiento.
- La interfaz proxy IGMP no puede ser la misma que una interfaz de enrutamiento IGMP.

Para configurar una interfaz proxy IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > Proxy Interface Configuration. Aparece la página Proxy Interface Configuration.

6. En el menú Interface, seleccione la interfaz que funcionará como interfaz proxy IGMP.

7. En el menú Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar la función de proxy IGMP en la interfaz.
El valor predeterminado es Disable.

8. En el campo Unsolicited Report Interval, especifique el tiempo en segundos entre repeticiones del informe inicial de membresía de un host en un grupo. El rango es de 1 a 260. El valor predeterminado es 1.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 114. Información de configuración de la interfaz proxy IGMP

Campo	Descripción
IP Address	La dirección IP de la interfaz proxy IGMP.
Subnet Mask	La máscara de subred de la dirección IP de la interfaz proxy IGMP.
Operational Mode	El estado operativo de la interfaz proxy IGMP (Disable o Enable).
Querier Address on Proxy Interface	La dirección del consultor en la interfaz proxy.
Number of Groups	El número de entradas de grupos multicast de la interfaz proxy IGMP en la tabla de caché.
Version	La versión de IGMP configurada en la interfaz de enrutamiento IGMP que convirtió en interfaz proxy IGMP. Para obtener más información, consulte Configurar una interfaz de enrutamiento IGMP en la página 400.
Version 1 Querier Timeout	El tiempo de espera del consultor IGMPv1 en segundos. Si un host recibe una consulta IGMPv1, establece temporalmente su temporizador de consultor IGMPv1 presente al intervalo del consultor IGMPv1. Después de leer la consulta IGMPv1, el tiempo de espera indica el periodo tras el cual el host vuelve a IGMPv3.
Version 2 Querier Timeout	El tiempo de espera del consultor IGMPv2 en segundos. Si un host recibe una consulta IGMPv2, establece temporalmente su temporizador de consultor IGMPv2 presente al intervalo del consultor IGMPv2. Después de leer la consulta IGMPv2, el tiempo de espera indica el periodo tras el cual el host vuelve a IGMPv3.
Proxy Start Frequency	El número de veces que se inició el proxy.

Mostrar las estadísticas de la interfaz proxy IGMP

Puede mostrar las estadísticas de la interfaz proxy IGMP.

Para mostrar las estadísticas de la interfaz proxy IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > Proxy Interface Statistics. Aparece la página Proxy Interface Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 115. Estadísticas de la interfaz proxy IGMP

Campo	Descripción
Proxy Interface	La interfaz en la que se reciben los paquetes IGMP.
Version	La versión de los paquetes IGMP recibidos.
Queries Received	El número de consultas IGMP recibidas.
Report Received	El número de informes IGMP recibidos.
Reports Sent	El número de informes IGMP enviados.

Tabla 115. Estadísticas de la interfaz proxy IGMP (continuación)

Campo	Descripción
Leaves Received	El número de mensajes IGMP leave recibidos.
Leaves Sent	El número de mensajes IGMP leave enviados.

Mostrar la membresía del proxy IGMP y buscar en la base de datos de membresía del proxy IGMP

Puede mostrar la información de membresía del proxy IGMP y buscar en la base de datos de membresía del proxy IGMP por grupo.

Para mostrar la información de membresía del proxy IGMP y buscar en la base de datos de membresía del proxy IGMP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > IGMP > Proxy Membership. Aparece la página Proxy Membership.

6. Para buscar la membresía del proxy IGMP por grupo, especifique la dirección IPv4 del grupo multicast y haga clic en el botón Go.
Si la entrada existe, la entrada con la dirección IPv4 de grupo coincidente se muestra como la primera, seguida de las demás. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 116. Información de membresía del proxy IGMP

Campo	Descripción
Proxy Interface	La interfaz en la que está habilitado el proxy IGMP.
Group IP	La dirección IPv4 del grupo multicast.
Source Hosts	Las direcciones de origen que son miembros del grupo multicast.
Last Reporter	La dirección IPv4 de origen que envió el último informe de membresía del grupo multicast en la interfaz proxy IGMP.
Up Time	El tiempo transcurrido desde que se creó la entrada.
Expiry Time	El intervalo de expiración de cada dirección de origen que es miembro del grupo multicast. Es el tiempo tras el cual caduca la entrada de origen.
State	El estado de la entrada del host: • Non-member state: El host no pertenece al grupo en la del puerto de servicio IPv6. • Delaying member state: El host pertenece al grupo en la interfaz y su temporizador de informes está activo. (Este temporizador se usa para enviar informes.) • Idle member state: El host pertenece al grupo en la interfaz pero su temporizador de informes está inactivo.
Filter Mode	El modo de filtro (Include, Exclude o None) del grupo en la interfaz proxy IGMP.
Number of Sources	El número de hosts de origen en el grupo multicast.

PIM para enrutamiento multicast IPv4

Protocol-Independent Multicast (PIM) es un protocolo estándar de enrutamiento multicast que proporciona enrutamiento multicast escalable entre dominios en Internet, independiente de cualquier protocolo de enrutamiento unicast.

Puede configurar los diversos ajustes de PIM para el enrutamiento multicast IPv4 y mostrar las estadísticas de PIM.

Configurar los ajustes globales de PIM IPv4 en el switch

Según las necesidades de su red IPv4, puede habilitar globalmente PIM Sparse Mode (PIM-SM) o PIM Dense Mode (PIM-DM) en el switch.

Para configurar los ajustes globales de PIM IPv4 en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > Global Configuration. Aparece la página Global Configuration.

6. Seleccione uno de los siguientes botones de opción de Admin Mode:

- Disable: PIM está deshabilitado en el switch. Es el ajuste predeterminado.
- PIM-SM: PIM Sparse Mode está habilitado en el switch.
- PIM-DM: PIM Dense Mode está habilitado en el switch.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Agregar grupos PIM-SSM IPv4

Mientras PIM emplea un router de punto de encuentro (RP) configurado especialmente que sirve como punto de reunión entre emisores y receptores multicast, PIM Single-Source Multicast (PIM-SSM) no usa un punto de encuentro (RP). PIM-SSM solo admite árboles de distribución de ruta de origen. Se usa entre routers (incluidas las interfaces de router del switch) para que puedan saber qué paquetes multicast reenviarse entre sí y a sus LAN directamente conectadas. Puede implementar PIM-SSM con un subconjunto estricto de los mecanismos de PIM. El multicast IPv4 normal y SSM pueden coexistir en un mismo router, y ambos pueden implementarse con el protocolo PIM. Un rango de direcciones multicast, 232.0.0.0/8 para IPv4, está reservado para SSM.

Para agregar un grupo PIM-SSM IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > SSM Configuration. Aparece la página SSM Configuration.

6. En el campo SSM Group Address, especifique la dirección IPv4 del grupo multicast de origen específico.

7. En el campo SSM Group Mask, especifique la máscara de la dirección IPv4 del grupo multicast de origen específico.

8. Haga clic en el botón Add.
Se guardan los ajustes. Se agrega el grupo.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un grupo PIM-SSM IPv4

Puede eliminar un grupo PIM-SSM IPv4 que ya no necesite.

Para eliminar un grupo PIM-SSM IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Mroute Static-Multicast Configuration.
Se muestra la página Mroute Static-Multicast Configuration.

6. Seleccione la casilla del grupo PIM-SSM.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina el grupo PIM-SSM.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz PIM IPv4

Puede configurar una interfaz IPv4 para PIM.

Para configurar una interfaz PIM IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > Interface Configuration. Aparece la página Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar PIM en la interfaz.
El valor predeterminado es Disable.

9. En el campo Hello Interval, especifique el tiempo en segundos entre la transmisión de mensajes PIM hello en la interfaz.
El rango es de 0 a 18000. El valor predeterminado es 30.

10. En el campo Join/Prune Interval, especifique el intervalo en segundos con el que se transmiten los mensajes PIM Join/Prune en la interfaz.
El rango es de 0 a 18000. El valor predeterminado es 60.

11. En el menú BSR Border, seleccione Enable o Disable para habilitar o deshabilitar el borde del router bootstrap (BSR) en la interfaz.
El valor predeterminado es Disable.

12. En el campo DR Priority, especifique la prioridad del router designado (DR) de la interfaz. El rango es de 0 a 2147483647. El valor predeterminado es 1.

13. Haga clic en el botón Apply.
La configuración se guarda.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe el campo no configurable de la página.

Tabla 117. Información de configuración de la interfaz PIM IPv4

Campo	Descripción
Protocol State	El estado de PIM en la interfaz (Operational o Non-Operational).
IP Address	La dirección IPv4 de la interfaz PIM.

Tabla 117. Información de configuración de la interfaz PIM IPv4 (continuación)

Campo	Descripción
Designated Router	La dirección IPv4 del router designado en la interfaz PIM.
Neighbor Count	El número de vecinos PIM en la interfaz PIM.

Mostrar los vecinos PIM IPv4 y buscar en la base de datos de vecinos PIM

Puede mostrar la información de vecinos PIM IPv4 y buscar en la base de datos de vecinos PIM por interfaz o por dirección IP del vecino.

Para mostrar los vecinos PIM IPv4 y buscar en la base de datos de vecinos PIM:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > PIM Neighbor. Aparece la página PIM Neighbor.

6. Para buscar entradas de grupos IGMP por interfaz o grupo, seleccione una de las siguientes opciones del menú Search:

- Interface: Seleccione Interface en el menú, especifique la interfaz en formato unidad/puerto (por ejemplo, 0/8) y haga clic en el botón Go.
Si la entrada existe, se muestra como la primera entrada, seguida de las demás entradas.
- Neighbor IP: Seleccione Neighbor IP en el menú, especifique la dirección IPv4 del vecino y haga clic en el botón Go.
Si la entrada existe, la entrada con la dirección IPv4 de vecino coincidente se muestra como la primera, seguida de las demás. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 118. Información de vecinos PIM IPv4

Campo	Descripción
Interface	La interfaz en la que está conectado el vecino PIM.
Neighbor IP	La dirección IPv4 del vecino PIM.
Up Time (hh:mm:ss)	El tiempo transcurrido desde que el dispositivo PIM se convirtió en vecino de la del puerto de servicio IPv6.
Expiry Time (hh:mm:ss)	El tiempo restante antes de que caduque el vecino PIM.
DR Priority	La prioridad de router designado (DR) del vecino PIM.

Agregar una configuración de punto de encuentro candidato PIM IPv4

Puede agregar una configuración de punto de encuentro (RP) candidato PIM IPv4 en una interfaz.

Para agregar una configuración de RP candidato PIM IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > Candidate RP Configuration. Aparece la página Candidate RP Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo Group Address, especifique la dirección IPv4 del grupo que se transmite en los anuncios de RP candidato.

8. En el campo Group Mask, escriba la máscara de la dirección del grupo que se transmite en los anuncios de RP candidato.

9. En el campo C-RP Advertisement Interval, especifique el intervalo en segundos con el que se envían los anuncios de RP candidato como tráfico unicast al router bootstrap (BSR). El rango es de 1 a 16383 segundos.

10. Haga clic en el botón Add.
Se guardan los ajustes. Se agrega el RP candidato PIM.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar una configuración de punto de encuentro candidato PIM IPv4

Puede eliminar una configuración de punto de encuentro (RP) candidato PIM IPv4 que ya no necesite.

Para eliminar una configuración de RP candidato PIM IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > Candidate RP Configuration. Aparece la página Candidate RP Configuration.

6. En el menú Interface, seleccione la interfaz.
7. Seleccione la casilla del RP candidato PIM.

8. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la entrada del RP candidato PIM.

Configurar una interfaz como candidato a router bootstrap PIM IPv4

Puede configurar una interfaz como candidato a router bootstrap (BSR) PIM IPv4.

Para configurar una interfaz como candidato a BSR PIM IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > BSR Candidate Configuration. Aparece la página BSR Candidate Configuration.

6. En el menú Interface, seleccione una interfaz.

7. En el campo Hash Mask Length, especifique la longitud de la máscara hash que se anunciará en los mensajes bootstrap.
La longitud de la máscara hash se usa en el algoritmo hash para seleccionar el RP de un grupo específico. El rango es de 0 a 32. El valor predeterminado es 30.

8. En el campo Priority, especifique la prioridad del candidato a BSR. El rango es de 0 a 255. El valor predeterminado es 0.

9. En el campo Advertisement Interval, especifique el tiempo en segundos entre anuncios.
El rango es de 1 a 16383. El valor predeterminado es 60.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 119. Información de configuración del candidato a BSR PIM IPv4

Campo	Descripción
BSR Expiry Time (hh:mm:ss)	El tiempo (en horas, minutos y segundos) tras el cual expira el BSR elegido aprendido.
IP Address	La dirección IPv4 del BSR elegido.
Next bootstrap Message (hh:mm:ss)	El tiempo (en horas, minutos y segundos) tras el cual se espera el siguiente mensaje bootstrap del BSR.
Next Candidate RP Advertisement (hh:mm:ss)	El tiempo (en horas, minutos y segundos) tras el cual se envía el siguiente anuncio de RP candidato.

Eliminar una configuración de candidato a router bootstrap PIM IPv4

Puede eliminar una configuración de candidato a router bootstrap (BSR) PIM IPv4 de una interfaz.

Para eliminar una configuración de candidato a BSR PIM IPv4 de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > BSR Candidate Configuration. Aparece la página BSR Candidate Configuration.

6. En el menú Interface, seleccione la interfaz.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la configuración del candidato a BSR PIM de la interfaz.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar un punto de encuentro PIM IPv4 estático para un grupo

Puede agregar un punto de encuentro (RP) PIM IPv4 estático nuevo o cambiar uno existente para un grupo.

Para agregar o cambiar un RP PIM IPv4 estático para un grupo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > Static RP Configuration. Aparece la página Static RP Configuration.

6. Si va a cambiar un RP estático existente, seleccione su casilla.
7. En el campo RP Address, especifique la dirección IPv4 del RP estático.

8. En el campo Group Address, especifique la dirección IPv4 del grupo al que se aplica el RP estático.

9. En el campo Group Mask, especifique la máscara del grupo al que se aplica el RP estático.

10. En el menú Override, seleccione Enable o Disable para habilitar o deshabilitar la capacidad de un RP estático de anular un RP aprendido de un BSR.
Si selecciona Enable y ocurre un conflicto, el RP estático anula el RP aprendido de un BSR.

11. Realice una de las siguientes acciones:

- Si va a agregar un RP estático nuevo, haga clic en el botón Add.
Se guardan los ajustes. Se agrega el RP estático.
- Si va a cambiar un RP estático existente, haga clic en el botón Apply. Se guardan los ajustes.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una configuración de punto de encuentro PIM IPv4 estático

Puede eliminar una configuración de punto de encuentro (RP) PIM IPv4 estático que ya no necesite para un grupo.

Para eliminar una configuración de RP PIM IPv4 estático para un grupo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > PIM > Static RP Configuration. Aparece la página Static RP Configuration.

6. Seleccione la casilla del RP estático.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la configuración del RP estático para el grupo.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Rutas multicast estáticas para direcciones IPv4

Si un protocolo de enrutamiento multicast como PIM-SM o PIM-DM está habilitado y configurado, las rutas multicast se crean dinámicamente. Sin embargo, también puede configurar una o más rutas multicast IPv4 estáticas. Una ruta estática puede facilitar el procesamiento del tráfico multicast cuando hay un router vecino de reenvío por ruta inversa (RPF) entre el switch y el origen multicast.

Configurar rutas multicast estáticas para direcciones IPv4

Puede agregar una ruta multicast IPv4 estática nueva o cambiar una existente.

Para agregar o cambiar una ruta multicast IPv4 estática:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Static Routes Configuration. Aparece la página Static Routes Configuration.

6. Si va a cambiar una ruta multicast estática existente, seleccione la casilla de la ruta.
En una ruta estática existente, solo puede cambiar la métrica.

7. En el campo Source IP, especifique la dirección IPv4 del origen de los paquetes multicast.
8. En el campo Source Mask, especifique la máscara de subred del origen de los paquetes multicast.

9. En el campo RPF Neighbor, especifique la dirección IPv4 del router RPF vecino ubicado entre el switch y el origen multicast.

10. En el campo Metric, especifique el costo de estado de enlace de la ruta desde el origen multicast hasta el switch.
El rango es de 0 a 255.

11. Realice una de las siguientes acciones:

- Si va a agregar una ruta multicast estática nueva, haga clic en el botón Add. Se guardan los ajustes. Se agrega la ruta multicast estática.
- Si va a cambiar una ruta multicast estática existente, haga clic en el botón Apply. Se guardan los ajustes.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una ruta multicast estática de una dirección IPv4

Puede eliminar una ruta multicast IPv4 estática que ya no necesite.

Para eliminar una ruta multicast IPv4 estática:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Static Routes Configuration. Aparece la página Static Routes Configuration.

6. Marque la casilla de la ruta estática.

7. Haga clic en el botón Delete.
Se guarda la configuración. Se elimina la ruta estática.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Límites administrativos multicast para direcciones IPv4

Un límite administrativo (admin boundary) multicast puede detener el tráfico multicast de entrada y salida de un rango de direcciones multicast en una interfaz de enrutamiento. Con los límites administrativos, puede definir los bordes de una región multicast, más allá de los cuales el tráfico multicast no debe pasar.

Configurar una interfaz como límite administrativo multicast

Puede configurar una interfaz como límite administrativo multicast.

Para configurar una interfaz como límite administrativo multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Admin Boundary Configuration.
Se muestra la página Admin Boundary Configuration.

6. En el menú Interface, seleccione la interfaz del router.

7. En el campo Group IP, especifique la dirección de grupo multicast que inicia el rango de direcciones que se deben excluir.
La dirección debe estar en el rango de 239.0.0.0 a 239.255.255.255.

8. En el campo Group Mask, introduzca la máscara de la dirección de grupo multicast. La combinación de la máscara y la IP de grupo define el rango del límite administrativo multicast.

9. Haga clic en el botón Add.
Se guarda la configuración. Se agrega el límite administrativo multicast.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar la configuración de límite administrativo multicast de una interfaz

Puede eliminar la configuración de límite administrativo multicast que ya no necesite en una interfaz.

Para eliminar una configuración de límite administrativo multicast:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > Multicast > Admin Boundary Configuration.
Se muestra la página Admin Boundary Configuration.

6. Marque la casilla de la interfaz.

7. Haga clic en el botón Delete.
Se guarda la configuración. Se elimina la ruta estática de la interfaz.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Enrutamiento multicast IPv6 y tabla de rutas multicast IPv6

Multicast es ideal para tráfico de video y audio que requiere control de paquetes multicast para un funcionamiento óptimo. Multicast para IPv6 incluye compatibilidad con Multicast Listener Discovery (MLD). La comunicación de punto a multipunto se denomina multidifusión. El host de origen (punto) transmite un mensaje a un grupo de cero o más hosts (multipunto) identificados por una sola dirección IPv6 de destino. Aunque esto puede lograrse enviando mensajes unicast (punto a punto) a cada host de destino, la multidifusión es el método preferido para este tipo de transmisión. Un mensaje multicast se entrega a todos los miembros de su grupo de hosts de destino con la misma confiabilidad de mejor esfuerzo que los mensajes IPv6 unicast normales. No se garantiza que el mensaje llegue intacto a todos los miembros del grupo de destino ni en el mismo orden respecto de otros mensajes.

Mostrar la tabla de rutas multicast IPv6

La tabla de enrutamiento multicast (Mroute) incluye información sobre la dirección IPv6 de origen, las direcciones IPv6 de destino del grupo, las interfaces de entrada y salida, los saltos siguientes a los que se deben reenviar los paquetes IPv6 y los protocolos admitidos.

Para mostrar la tabla Mroute IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > Mroute Table. Se muestra la página Mroute Table.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 120. Información de la tabla Mroute IPv6 multicast

Campo	Descripción
Group IP	La dirección IPv6 del grupo de destino.
Source IP	La dirección IPv6 del origen del paquete multicast, que se combina con la IPv6 del grupo para identificar por completo la ruta.
Incoming Interface	La interfaz de entrada por la que llegan los paquetes multicast de este origen/grupo.
Outgoing Interfaces	La lista de interfaces de salida por las que se reenvían los paquetes multicast de este origen/grupo.
Up Time (hh:mm:ss)	El tiempo en segundos desde que se creó la entrada.
Expiry Time (hh:mm:ss)	El tiempo en segundos antes de que esta entrada caduque y se elimine de la tabla.
RPF Neighbor	La dirección IPv6 del vecino de reenvío por ruta inversa (RPF).

Tabla 120. Información de la tabla Mroute IPv6 multicast (continuación)

Campo	Descripción
Protocol	El protocolo de enrutamiento multicast que creó dinámicamente esta entrada. Los valores posibles son los siguientes: • PIM-DM • PIM-SM
Flags	El valor de este campo es válido si el protocolo de enrutamiento multicast es PIM-SM. Los valores posibles son RPT y SPT. Para otros protocolos se muestra “------”.

PIM para enrutamiento multicast IPv6

Protocol-Independent Multicast (PIM) es un protocolo estándar de enrutamiento multicast que ofrece enrutamiento multicast escalable entre dominios en Internet, independiente de cualquier protocolo de enrutamiento unicast.

Puede configurar los distintos ajustes de PIM para el enrutamiento multicast IPv6 y mostrar las estadísticas de PIM.

Configurar los ajustes globales de PIM IPv6 en el switch

Según las necesidades de su red IPv6, puede habilitar globalmente PIM Sparse Mode (PIM-SM) o PIM Dense Mode (PIM-DM) en el switch.

Para configurar los ajustes globales de PIM IPv6 en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > Global Configuration.

Se muestra la página Global Configuration.

6. Seleccione uno de los siguientes botones de opción de Admin Mode:

- Disable: PIM está deshabilitado en el switch. Es el ajuste predeterminado.
- PIM-SM: PIM Sparse Mode está habilitado en el switch.
- PIM-DM: PIM Dense Mode está habilitado en el switch.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Agregar grupos PIM-SSM IPv6

Mientras que PIM usa un router de punto de encuentro (RP) configurado especialmente que sirve como punto de reunión para emisores y receptores multicast, PIM Single-Source Multicast (PIM-SSM) no usa un punto de encuentro (RP). PIM-SSM solo admite árboles de distribución por ruta de origen. Se usa entre routers (incluidas las interfaces de router del switch) para que puedan saber qué paquetes multicast reenviarse entre sí y a sus LAN directamente conectadas. Puede implementar PIM-SSM con un subconjunto estricto de los mecanismos del protocolo PIM. El multicast IPv6 normal y SSM pueden coexistir en un solo router, y ambos se pueden implementar con el protocolo PIM. Un rango de direcciones multicast, FF3x::/32 para IPv6, está reservado para SSM.

Para agregar un grupo PIM-SSM IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > SSM Configuration. Se muestra la página SSM Configuration.

6. En el campo SSM Group Address, introduzca la dirección IPv6 del grupo multicast de origen específico.

7. En el campo SSM Group Mask, introduzca el prefijo de la dirección IPv6 del grupo multicast de origen específico.

8. Haga clic en el botón Add.
Se guardan los ajustes. Se agrega el grupo.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un grupo PIM-SSM IPv6

Puede eliminar un grupo PIM-SSM IPv6 que ya no necesite.

Para eliminar un grupo PIM-SSM IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > SSM Configuration. Se muestra la página SSM Configuration.

6. Seleccione la casilla del grupo PIM-SSM.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina el grupo PIM-SSM.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz PIM IPv6

Puede configurar una interfaz IPv6 para PIM.

Para configurar una interfaz PIM IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration. Se muestra la página Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar PIM en la interfaz.
El valor predeterminado es Disable.

9. En el campo Hello Interval, especifique el tiempo en segundos entre la transmisión de mensajes PIM hello en la interfaz.
El rango es de 0 a 18000. El valor predeterminado es 30.

10. En el campo Join/Prune Interval, especifique el intervalo en segundos con el que se transmiten los mensajes PIM Join/Prune en la interfaz.
El rango es de 0 a 18000. El valor predeterminado es 60.

11. En el menú BSR Border, seleccione Enable o Disable para habilitar o deshabilitar el borde de bootstrap router (BSR) en la interfaz.

El valor predeterminado es Disable.

12. En el campo DR Priority, especifique la prioridad del router designado (DR) de la interfaz. El rango es de 0 a 2147483647. El valor predeterminado es 1.

13. Haga clic en el botón Apply.
La configuración se guarda.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe el campo no configurable de la página.

Tabla 121. Información de configuración de interfaces PIM IPv6

Campo	Descripción
Protocol State	El estado de PIM en la interfaz (Operational o Non-Operational).
IPv6 Prefix/Length	La dirección IPv6 y la longitud de prefijo de la interfaz PIM.
Designated Router	La dirección IPv6 del router designado en la interfaz PIM.
Neighbor Count	El número de vecinos PIM en la interfaz PIM.

Mostrar los vecinos PIM IPv6 y buscar en la base de datos de vecinos PIM

Puede mostrar la información de vecinos PIM IPv6 y buscar en la base de datos de vecinos PIM por interfaz o por dirección IP del vecino.

Para mostrar los vecinos PIM IPv6 y buscar en la base de datos de vecinos PIM:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > PIM Neighbor. Se muestra la página PIM Neighbor.

6. Para buscar entradas de grupos IGMP por interfaz o grupo, seleccione una de las siguientes opciones del menú Search:

- Interface: Seleccione Interface en el menú, especifique la interfaz en formato unidad/puerto (por ejemplo, 0/8) y haga clic en el botón Go.
  Si la entrada existe, se muestra primero, seguida de las demás entradas.
- Neighbor IP: Seleccione Neighbor IP en el menú, especifique la dirección IPv6 del vecino y haga clic en el botón Go.
  Si la entrada existe, la entrada con la dirección IPv6 de vecino coincidente se muestra primero, seguida de las demás entradas. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 122. Información de vecinos PIM IPv6

Campo	Descripción
Interface	La interfaz en la que está conectado el vecino PIM.
Neighbor IP	La dirección IPv6 del vecino PIM.
Up Time (hh:mm:ss)	El tiempo transcurrido desde que el dispositivo PIM se convirtió en vecino de la del puerto de servicio IPv6.
Expiry Time (hh:mm:ss)	El tiempo restante antes de que caduque el vecino PIM.
DR Priority	La prioridad de router designado (DR) del vecino PIM.

Agregar una configuración de punto de encuentro candidato PIM IPv6

Puede agregar una configuración de punto de encuentro (RP) candidato PIM IPv6 en una interfaz.

Para agregar una configuración de RP candidato PIM IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > Candidate RP Configuration. Se muestra la página Candidate RP Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo Group Address, especifique la dirección IPv6 de grupo que se transmite en los anuncios candidate-RP-advertisements.

8. En el campo Prefix Length, introduzca la longitud de prefijo IPv6 del grupo que se transmite en los anuncios candidate-RP-advertisements.

9. En el campo C-RP Advertisement Interval, especifique el intervalo en segundos con el que se envían los anuncios de RP candidato como tráfico unicast al router bootstrap (BSR). El rango es de 1 a 16383 segundos.

10. Haga clic en el botón Add.
Se guardan los ajustes. Se agrega el RP candidato PIM.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar una configuración de punto de encuentro candidato PIM IPv6

Puede eliminar una configuración de punto de encuentro (RP) candidato PIM IPv6 que ya no necesite.

Para eliminar una configuración de RP candidato PIM IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > Candidate RP Configuration. Se muestra la página Candidate RP Configuration.

6. En el menú Interface, seleccione la interfaz.
7. Seleccione la casilla del RP candidato PIM.

8. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la entrada del RP candidato PIM.

Configurar una interfaz como candidato a bootstrap router PIM IPv6

Puede configurar una interfaz como candidato a bootstrap router (BSR) PIM IPv6.

Para configurar una interfaz como candidato a BSR PIM IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > BSR Candidate Configuration. Se muestra la página BSR Candidate Configuration.

6. En el menú Interface, seleccione una interfaz.

7. En el campo Hash Mask Length, especifique la longitud de máscara hash que se anunciará en los mensajes bootstrap.
La longitud de máscara hash se usa en el algoritmo hash para seleccionar el RP de un grupo determinado. El rango es de 0 a 128. El valor predeterminado es 126.

8. En el campo Priority, especifique la prioridad del candidato a BSR. El rango es de 0 a 255. El valor predeterminado es 0.

9. En el campo Advertisement Interval, especifique el tiempo en segundos entre anuncios.
El rango es de 1 a 16383. El valor predeterminado es 60.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 123. Información de configuración de candidatos BSR PIM IPv6

Campo	Descripción
BSR Expiry Time (hh:mm:ss)	El tiempo (en horas, minutos y segundos) tras el cual expira el BSR elegido aprendido.
IP Address	La dirección IPv6 del BSR elegido.
Next bootstrap Message (hh:mm:ss)	El tiempo (en horas, minutos y segundos) tras el cual se espera el siguiente mensaje bootstrap del BSR.
Next Candidate RP Advertisement (hh:mm:ss)	El tiempo (en horas, minutos y segundos) tras el cual se envía el siguiente anuncio de RP candidato.

Eliminar una configuración de candidato a bootstrap router PIM IPv6

Puede eliminar una configuración de candidato a bootstrap router (BSR) PIM IPv6 de una interfaz.

Para eliminar una configuración de candidato a BSR PIM IPv6 de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > BSR Candidate Configuration. Se muestra la página BSR Candidate Configuration.

6. En el menú Interface, seleccione la interfaz.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la configuración del candidato a BSR PIM de la interfaz.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar un punto de encuentro PIM IPv6 estático para un grupo

Puede agregar un punto de encuentro (RP) PIM IPv6 estático nuevo o cambiar uno existente para un grupo.

Para agregar o cambiar un RP PIM IPv6 estático para un grupo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > Static RP Configuration. Se muestra la página Static RP Configuration.

6. Si va a cambiar un RP estático existente, seleccione su casilla.
7. En el campo RP Address, especifique la dirección IPv6 del RP estático.

8. En el campo Group Address, especifique la dirección IPv6 del grupo al que se aplica el RP estático.

9. En el campo Prefix Length, especifique la longitud de prefijo IPv6 del grupo al que se aplica el RP estático.

10. En el menú Override, seleccione Enable o Disable para habilitar o deshabilitar la capacidad de un RP estático de anular un RP aprendido de un BSR.
Si selecciona Enable y ocurre un conflicto, el RP estático anula el RP aprendido de un BSR.

11. Realice una de las siguientes acciones:

- Si va a agregar un RP estático nuevo, haga clic en el botón Add.
Se guardan los ajustes. Se agrega el RP estático.
- Si va a cambiar un RP estático existente, haga clic en el botón Apply. Se guardan los ajustes.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una configuración de punto de encuentro PIM IPv6 estático

Puede eliminar una configuración de punto de encuentro (RP) PIM IPv6 estático que ya no necesite para un grupo.

Para eliminar una configuración de RP PIM IPv6 estático de un grupo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > IPv6 PIM > Static RP Configuration. Se muestra la página Static RP Configuration.

6. Seleccione la casilla del RP estático.
7. Haga clic en el botón Delete.

Se guarda la configuración. Se elimina la configuración de RP estático del grupo.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

MLD para enrutamiento multicast IPv6

Puede configurar los ajustes de Multicast Listener Discovery (MLD) y ver las estadísticas de MLD.

MLD es un protocolo que usan los routers multicast IPv6 para detectar la presencia de receptores multicast (nodos configurados para recibir paquetes multicast IPv6) en sus enlaces directamente conectados y para saber qué paquetes multicast interesan a los nodos vecinos. MLD deriva de IGMP; MLD versión 1 (MLDv1) equivale a IGMPv2 y MLD versión 2 (MLDv2) equivale a IGMPv3. MLD es un subprotocolo de Internet Control Message Protocol version 6 (ICMPv6), y los mensajes MLD son un subconjunto de los mensajes ICMPv6, identificados en los paquetes IPv6 por un valor Next Header anterior de 58.

El switch puede detectar paquetes de los protocolos MLDv1 y MLDv2 y puentear datos multicast IPv6 según las direcciones MAC multicast IPv6 de destino. El switch puede admitir MLD snooping e IGMP snooping simultáneamente.

Configurar los ajustes globales de MLP del switch

Puede configurar los ajustes globales de MLDP del switch, a diferencia de los ajustes MLD de una interfaz.

Para configurar los ajustes globales de MLP del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción Admin Mode Enable o Disable para habilitar o deshabilitar MLD en el switch.
El valor predeterminado es Disable.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una interfaz de enrutamiento MLD

Puede configurar una o más interfaces de enrutamiento MLD.

Para configurar una interfaz de enrutamiento MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > Routing Interface Configuration. Se muestra la página Routing Interface Configuration.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.

• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar MLD en la interfaz.
El valor predeterminado es Disable.

9. En el campo Version, especifique la versión de MLD de la interfaz. La versión puede ser 1 o 2. El valor predeterminado es 2.

10. En el campo Query Interval, introduzca la frecuencia en segundos con la que se transmiten los paquetes MLD host-query en la interfaz.
El valor es de 1 a 3600. El valor predeterminado es 125.

11. En el campo Query Max Response Time, introduzca el tiempo máximo de respuesta a consultas, en milisegundos, que se anuncia en las consultas MLDv2 de la interfaz. El valor es de 0 a 65535. El valor predeterminado es 10000 milisegundos.

12. En el campo Startup Query Interval, introduzca el número de segundos entre la transmisión de consultas de inicio en la interfaz.
El valor es de 1 a 300. El valor predeterminado es 31.

13. En el campo Startup Query Count, introduzca el número de consultas que se envían al inicio, separadas por el intervalo de consultas de inicio.
El valor es de 1 a 20. El valor predeterminado es 2.

14. En el campo Last Member Query Interval, introduzca el intervalo de consulta del último miembro en milisegundos.
Este valor es el tiempo máximo de respuesta que se inserta en las consultas específicas de grupo enviadas en respuesta a mensajes leave group, y también es el tiempo entre mensajes de consulta específicos de grupo. El valor es de 0 a 655355. El valor predeterminado es 1000 milisegundos.

15. En el campo Last Member Query Count, introduzca el número de consultas que se envían al recibir un informe leave group.
El valor es de 1 a 20. El valor predeterminado es 2.

16. Haga clic en el botón Apply. Se guardan los ajustes.

17. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 124. Configuración de interfaces de enrutamiento MLD

Campo	Descripción
Operational Mode	El estado operativo de MLD en la interfaz.
Robustness	El ajuste de robustez de la interfaz. El valor predeterminado es 2.

Mostrar las estadísticas de las interfaces de enrutamiento MLD

Puede mostrar las estadísticas de las interfaces de enrutamiento MLD.

Para mostrar las estadísticas de las interfaces de enrutamiento MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > Routing Interface Statistics. Se muestra la página Routing Interface Statistics.

6. Seleccione si desea mostrar interfaces físicas, VLAN o ambas haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- VLANS: Solo se muestran las VLAN.
- All: Se muestran tanto las interfaces físicas como las VLAN.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 125. Información de estadísticas de interfaces de enrutamiento MLD

Campo	Descripción
Interface	La interfaz en la que está habilitado MLD.
Querier Status	Indica si la interfaz es un querier o non-querier MLD en la subred IPv6 a la que está asociada.
Querier IP	La dirección IPv6 del querier MLD en la subred IPv6 a la que está conectada la interfaz.
Querier Up Time	El tiempo en segundos desde el último cambio del querier de la interfaz MLD.
Querier Expiry Time	El período en segundos que falta para que caduque el temporizador de presencia de otro querier. Si el switch es el querier, es cero.
Wrong Version Queries Received	El número de consultas recibidas en la interfaz con una versión de MLD que no coincide con la versión de MLD configurada para la tabla de caché
Number of Joins Received	El número de veces que se agregó una membresía de grupo en la interfaz; es decir, el número de veces que se agregó una entrada de la interfaz a la de la interfaz.
Number of Groups	El número actual de entradas de la interfaz en la tabla de caché.

Mostrar los grupos MLD y buscar en la base de datos de grupos MLD

Puede mostrar la información de grupos MLD y buscar en la base de datos de grupos MLD por interfaz o por grupo.

Para mostrar los grupos MLD y buscar en la base de datos de grupos MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > MLD Groups. Se muestra la página MLD Groups.

6. Para buscar entradas de grupos IGMP por interfaz o grupo, seleccione una de las siguientes opciones del menú Search:

• Interface: Seleccione Interface en el menú, especifique la interfaz en formato unidad/puerto (por ejemplo, 0/8) y haga clic en el botón Go.
Si la entrada existe, se muestra primero, seguida de las demás entradas.
• Group: Seleccione Group en el menú, especifique la dirección IPv6 del grupo multicast y haga clic en el botón Go.
Si la entrada existe, la entrada con la dirección IPv6 de grupo coincidente se muestra primero, seguida de las demás entradas. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 126. Información de grupos MLD

Campo	Descripción
Interface	La interfaz en la que está habilitado MLD.
Group IP	La dirección del grupo multicast IP.
Last Reporter	La dirección IP del origen del último informe de membresía recibido para la dirección de grupo multicast IP en la interfaz.
Up Time	El tiempo transcurrido desde que se creó esta entrada.
Expiry Time	El tiempo restante antes de que esta entrada caduque.
Filter Mode	El modo de filtro de origen (Include, Exclude o NA) del grupo en la interfaz. Si el modo es NA, el campo está vacío.
Version 1 Host Timer	El tiempo restante hasta que el switch determine que no hay miembros de MLD versión 1 conectados a la interfaz.
Group Compat Mode	El modo de compatibilidad (MLDv1 o MLDv2) del grupo multicast en la del puerto de servicio IPv6.

Tabla 126. Información de grupos MLD (continuación)

Campo	Descripción
Source Hosts	Las direcciones de origen que son miembros de la dirección multicast.
Source Address (Expiry Time)	El tiempo de expiración tras el cual caduca cada dirección de origen que es miembro del grupo multicast.

Mostrar o borrar las estadísticas de tráfico MLD

Puede ver y borrar las estadísticas de tráfico MLD.

Para ver o borrar las estadísticas de tráfico MLD IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > MLD Traffic. Se muestra la página MLD Traffic.

6. Para actualizar la página, haga clic en el botón Refresh.
7. Para restablecer (borrar) todas las estadísticas de tráfico MLD, haga clic en el botón Clear.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 127. Información de estadísticas de tráfico MLD

Campo	Descripción
Valid MLD Packets Received	El número de paquetes MLD válidos recibidos por el switch.
Valid MLD Packets Sent	El número de paquetes MLD válidos enviados por el switch.
Queries Received	El número de consultas MLD válidas recibidas por el switch.
Queries Sent	El número de consultas MLD válidas enviadas por el switch.
Reports Received	El número de informes MLD válidos recibidos por el switch.
Reports Sent	El número de informes MLD válidos enviados por el switch.
Leaves Received	El número de mensajes MLD leave válidos recibidos por el switch.
Leaves Sent	El número de mensajes MLD leave válidos enviados por el switch.

Configurar una interfaz proxy MLD

Puede configurar una interfaz proxy MLD. Se aplican los siguientes requisitos:

- El enrutamiento, MLD y multicast deben estar habilitados globalmente en el switch.
- Debe configurar al menos una interfaz de enrutamiento.
- La interfaz proxy MLD no puede ser la misma que una interfaz de enrutamiento MLD.

Para configurar una interfaz proxy MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > Proxy Interface Configuration. Se muestra la página Proxy Interface Configuration.

6. En el menú Interface, seleccione la interfaz que funcionará como interfaz proxy IGMP.

7. En el menú Admin Mode, seleccione Enable o Disable para habilitar o deshabilitar la función de proxy IGMP en la interfaz.
El valor predeterminado es Disable.

8. En el campo Unsolicited Report Interval, especifique el tiempo en segundos entre repeticiones del informe inicial de membresía de un host en un grupo. El rango es de 1 a 260. El valor predeterminado es 1.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 128. Información de configuración de la interfaz proxy MLD

Campo	Descripción
IPv6 Prefix	La dirección IPv6 de la interfaz proxy MLD.
Prefix Length	La longitud de prefijo de la dirección IPv6 de la interfaz proxy MLD.
Operational Mode	El estado operativo de la interfaz proxy IGMP (Disable o Enable).
Querier Address on Proxy Interface	La dirección del consultor en la interfaz proxy.
Number of Groups	El número de entradas de grupos multicast de la interfaz proxy MLD en la tabla de caché.
Version	La versión de MLD configurada en la interfaz de enrutamiento MLD que convirtió en interfaz proxy MLD. Para obtener más información, consulte Configurar una interfaz de enrutamiento MLD en la página 440.
Version 1 Querier Timeout	El tiempo de espera del querier MLDv1 en segundos. Si un host recibe una consulta MLDv1, establece temporalmente su temporizador de querier MLDv1 presente en el intervalo del querier MLDv1. Después de que el host lee la consulta MLDv1, el tiempo de espera del querier MLDv1 indica el tiempo tras el cual el host vuelve a MLDv2.
Proxy Start Frequency	El número de veces que se inició el proxy.

Mostrar las estadísticas de la interfaz proxy MLD

Puede mostrar las estadísticas de la interfaz proxy MLD.

Para mostrar las estadísticas de la interfaz proxy MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > Proxy Interface Statistics. Se muestra la página Proxy Interface Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 129. Información de estadísticas de la interfaz proxy MLD

Campo	Descripción
Proxy Interface	La interfaz en la que se reciben los paquetes proxy MLD.
Version	La versión de los paquetes proxy MLD recibidos.
Queries Received	El número de consultas proxy MLD recibidas.
Reports Received	El número de informes proxy MLD recibidos.
Reports Sent	El número de informes proxy MLD enviados.

Tabla 129. Información de estadísticas de la interfaz proxy MLD (continuación)

Campo	Descripción
Leaves Received	El número de mensajes proxy MLD leave recibidos.
Leaves Sent	El número de mensajes proxy MLD leave enviados.

Mostrar la membresía proxy MLD y buscar en la base de datos de membresía proxy MLD

Puede mostrar la información de membresía proxy MLD y buscar en la base de datos de membresía proxy MLD por grupo.

Para mostrar la información de membresía proxy MLD y buscar en la base de datos de membresía proxy MLD:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > MLD > Proxy Membership. Se muestra la página Proxy Membership.

6. Para buscar la membresía de proxy MLD por grupo, especifique la dirección IPv6 del grupo multicast y haga clic en el botón Go.
Si la entrada existe, la entrada con la dirección IPv6 de grupo coincidente se muestra como la primera, seguida del resto de las entradas. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 130. Información de membresía de proxy MLD

Campo	Descripción
Proxy Interface	La interfaz en la que está habilitado el proxy MLD.
Group IP	La dirección de grupo multicast IPv6.
Source Hosts	Las direcciones de origen que son miembros del grupo multicast.
Last Reporter	La dirección IPv6 de origen que envió el último informe de membresía del grupo multicast en la interfaz de proxy MLD.
Up Time	El tiempo transcurrido desde que se creó esta entrada.
Expiry Time	El intervalo de expiración de cada dirección de origen que es miembro del grupo multicast. Es el tiempo tras el cual caduca la entrada de origen.
State	El estado de la entrada del host: • Non-member state: El host no pertenece al grupo en la del puerto de servicio IPv6. • Delaying member state: El host pertenece al grupo en la interfaz y su temporizador de informes está activo. (Este temporizador se usa para enviar informes.) • Idle member state: El host pertenece al grupo en la interfaz pero su temporizador de informes está inactivo.
Filter Mode	El modo de filtro (Include, Exclude o None) del grupo en la interfaz de proxy MLD.
Number of Sources	El número de hosts de origen en el grupo multicast.

Rutas multicast estáticas para direcciones IPv6

Si se habilita y configura un protocolo de enrutamiento multicast como PIM-SM o PIM-DM, las rutas multicast se crean dinámicamente. Sin embargo, también puede configurar una o más rutas multicast IPv6 estáticas. Una ruta estática puede facilitar el procesamiento del tráfico multicast cuando hay un router vecino de reenvío por ruta inversa (RPF) entre el switch y la fuente multicast.

Configurar rutas multicast estáticas para direcciones IPv6

Puede agregar una ruta multicast IPv6 estática nueva o cambiar una existente.

Para agregar o cambiar una ruta multicast IPv6 estática:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > Static Routes Configuration. Se muestra la página Static Routes Configuration.

6. Si va a cambiar una ruta multicast estática existente, seleccione la casilla de la ruta.
En una ruta estática existente, solo puede cambiar la métrica.

7. En el campo Source IP, especifique la dirección IPv6 de la fuente de los paquetes multicast.

8. En el campo Prefix Length, especifique la longitud de prefijo IPv6 de la fuente de los paquetes multicast.

9. En el campo RPF Neighbor, especifique la dirección IPv6 del router RPF vecino ubicado entre el switch y la fuente multicast.

10. En el campo Metric, especifique el costo de estado de enlace de la ruta desde el origen multicast hasta el switch.
El rango es de 0 a 255.

11. En el menú RPF Interface, seleccione la interfaz conectada al vecino RPF.

12. Realice una de las siguientes acciones:

- Si va a agregar una ruta multicast estática nueva, haga clic en el botón Add. Se guardan los ajustes. Se agrega la ruta multicast estática.
- Si va a cambiar una ruta multicast estática existente, haga clic en el botón Apply. Se guardan los ajustes.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar una ruta multicast estática de una dirección IPv6

Puede eliminar una ruta multicast IPv6 estática que ya no necesite.

Para eliminar una ruta multicast estática:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Routing > IPv6 Multicast > Static Routes Configuration. Se muestra la página Static Routes Configuration.

6. Marque la casilla de la ruta estática.

7. Haga clic en el botón Delete.
Se guarda la configuración. Se elimina la ruta estática.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

6

Configurar la calidad de servicio

Este capítulo trata los siguientes temas:

- Conceptos de calidad de servicio
- Clase de servicio
- Servicios diferenciados

Conceptos de calidad de servicio

En un switch, cada puerto físico tiene una o más colas para transmitir paquetes a la red conectada. A menudo se ofrecen varias colas por puerto para dar preferencia a ciertos paquetes sobre otros según criterios definidos por el usuario. Cuando un paquete se encola para transmitirse en un puerto, la velocidad con que se atiende depende de cómo esté configurada la cola y, posiblemente, de la cantidad de tráfico en las demás colas del puerto. Si se requiere un retardo, los paquetes se retienen en la cola hasta que el planificador autoriza la transmisión de la cola. Cuando las colas se llenan, los paquetes ya no pueden retenerse para su transmisión y el switch los descarta.

La calidad de servicio (QoS) permite una entrega de datos constante y predecible distinguiendo los paquetes con requisitos de tiempo estrictos de aquellos que toleran mejor el retardo. En una red con QoS, los paquetes con requisitos de tiempo estrictos reciben un trato especial. Por ello, todos los elementos de la red deben admitir QoS. Un solo nodo sin QoS crea una deficiencia en la ruta de red y compromete el rendimiento de todo el flujo de paquetes.

Clase de servicio

La función de colas de clase de servicio (CoS) le permite configurar directamente ciertos aspectos de las colas del switch. Esto proporciona el comportamiento QoS deseado para distintos tipos de tráfico de red cuando no se requiere la complejidad de DiffServ. La prioridad de un paquete que llega a una interfaz puede usarse para dirigirlo a la cola CoS de salida adecuada mediante una tabla de asignación. Las características de las colas CoS que afectan la asignación, como el ancho de banda mínimo garantizado o la limitación de la velocidad de transmisión, son configurables a nivel de cola (o de puerto).

Se admiten ocho colas por puerto.

Conceptos de configuración de CoS

Puede establecer el modo de confianza de clase de servicio de una interfaz. Cada puerto del switch puede configurarse para confiar en uno de los campos del paquete (802.1p o IP DSCP), o para no confiar en la designación de prioridad de ningún paquete (modo no confiable). Si el puerto está en modo de confianza, usa la tabla de asignación correspondiente al campo de confianza utilizado. Esta tabla indica la cola CoS a la que se debe reenviar el paquete en el puerto de salida correspondiente. Por supuesto, el campo de confianza debe existir en el paquete para que la tabla sea útil. Si no es así, se realizan acciones predeterminadas. Estas acciones consisten en dirigir el paquete a un nivel CoS específico configurado para el puerto de entrada en su conjunto, según la prioridad predeterminada del puerto asignada a una clase de tráfico por la tabla de asignación 802.1p actual.

Por otro lado, cuando un puerto se configura como no confiable, no confía en ninguna designación de prioridad de los paquetes entrantes y usa en su lugar la prioridad predeterminada del puerto. Todos los paquetes que llegan a un puerto no confiable se dirigen a una cola CoS específica en los puertos de salida correspondientes, según la prioridad predeterminada configurada del puerto de entrada. Este proceso también se usa cuando no se puede respetar la asignación de un puerto de confianza, como cuando llega un paquete no IP a un puerto configurado para confiar en el valor IP DSCP.

Configurar el modo de confianza CoS globalmente o para una interfaz específica

Una configuración global del modo de confianza CoS se aplica a todas las interfaces del switch.

Una configuración del modo de confianza CoS de una interfaz se aplica solo a la interfaz seleccionada. Para configurar el modo de confianza CoS en más de una interfaz, repita el procedimiento para cada interfaz.

Para configurar el modo de confianza CoS en todas las interfaces o en una interfaz específica:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > CoS > Basic > CoS Configuration.
Se muestra la página CoS Configuration.

6. Configure el mismo modo de confianza CoS para todas las interfaces configurables con CoS o configure CoS por interfaz.
De forma predeterminada, está seleccionado el botón de opción Global.

• Para configurar el mismo modo de confianza CoS en todas las interfaces configurables con CoS, haga lo siguiente:

a. Seleccione el botón de opción Global.
b. En el menú Global Trust Mode, seleccione una de las siguientes opciones de modo de confianza para el tráfico de entrada del switch:

- untrusted: No confiar en ninguna marca CoS de los paquetes de entrada.
- trust dot1p: Las ocho etiquetas de prioridad especificadas en IEEE 802.1p son de p0 a p7. La configuración de QoS le permite asignar cada uno de los ocho niveles de prioridad a una de las ocho colas de prioridad internas del hardware.
- trust IP-DSCP: Los seis bits más significativos del campo DiffServ se denominan bits Differentiated Services Code Point (DSCP). El modo predeterminado es IP-DSCP.

• Para configurar CoS en una interfaz, haga lo siguiente: a. Seleccione el botón de opción Interface.
b. En el menú, seleccione la interfaz.

La configuración se aplica solo a la interfaz seleccionada. c. En el menú Interface Trust Mode, seleccione una de las siguientes opciones de modo de confianza:

- untrusted: No confiar en ninguna marca CoS de los paquetes de entrada.
- trust dot1p: Las ocho etiquetas de prioridad especificadas en IEEE 802.1p son de p0 a p7. La configuración de QoS le permite asignar cada uno de los ocho niveles de prioridad a una de las siete colas de prioridad internas del hardware.
- trust IP-DSCP: Los seis bits más significativos del campo DiffServ se denominan bits Differentiated Services Code Point (DSCP). El modo predeterminado es IP-DSCP.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Asignar prioridades 802.1p a colas

Puede ver o cambiar qué clases de tráfico internas se asignan a los valores de clase de prioridad 802.1p de las tramas Ethernet que recibe el dispositivo. Las asignaciones de prioridad a clase de tráfico pueden aplicarse globalmente (a todas las interfaces) o a cada interfaz. La

asignación permite al switch agrupar distintos tipos de tráfico (por ejemplo, datos o voz) según sus requisitos de latencia y dar preferencia al tráfico sensible al tiempo.

Para asignar prioridades 802.1p a colas en todas las interfaces o en interfaces individuales:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > CoS > Advanced > 802.1p to Queue Mapping. Se muestra la página 802.1p to Queue Mapping.

6. En el menú Interface, seleccione All para aplicar la asignación a todas las interfaces o seleccione una interfaz individual.

7. En la tabla 802.1p to Queue Mapping, asigne cada una de las ocho prioridades 802.1p a una cola (clase de tráfico interna) de 0 a 7.
La fila 802.1p Priority contiene selectores de clase de tráfico para cada una de las ocho prioridades 802.1p. La prioridad va de baja (0) a alta (7). Por ejemplo, el tráfico con prioridad 0 corresponde a la mayoría del tráfico de datos y se envía con el mejor esfuerzo. El tráfico con mayor prioridad, como 7, puede ser tráfico sensible al tiempo, como voz o video.

Tabla 131. Valores predeterminados de asignación de 802.1p a colas

Prioridad 802.1p	0	1	2	3	4	5	6	7
Cola predeterminada	1	0	0	1	2	2	3	3

Los valores del menú bajo cada prioridad representan la clase de tráfico. La clase de tráfico es la cola de hardware de un puerto. Los valores más altos indican una posición de cola más alta. Antes de enviarse, el tráfico de una cola inferior debe esperar a que se envíe el tráfico de las colas superiores.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Asignar valores DSCP a colas

Puede asignar una clase de tráfico interna a un valor DSCP.

Para asignar valores DSCP a colas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > CoS > Advanced > IP DSCP to Queue Mapping. Se muestra la página IP DSCP to Queue Mapping.

El campo IP DSCP muestra un valor IP DSCP de 0 a 63.

6. Para cada valor DSCP, especifique a qué clase de tráfico interna se asigna el valor IP DSCP correspondiente.
El número de cola depende del hardware específico.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de interfaz CoS de una interfaz

Puede configurar el modo de confianza de una o más interfaces y aplicar una velocidad de limitación (shaping) a todas las interfaces o a una interfaz específica.

Para configurar CoS en una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > CoS > Advanced > CoS Interface Configuration. Se muestra la página CoS Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú Interface Trust Mode, seleccione una de las siguientes opciones de modo de confianza para el tráfico de entrada en las interfaces seleccionadas:

- Untrusted: No confiar en ninguna marca CoS de los paquetes de entrada.
- 802.1p: Las ocho etiquetas de prioridad especificadas en IEEE 802.1p son de p0 a p7. La configuración de QoS le permite asignar cada uno de los ocho niveles de prioridad a una de las siete colas de prioridad internas del hardware. El valor predeterminado es 802.1p.
- IP-DSCP: Los seis bits más significativos del campo DiffServ se denominan bits Differentiated Services Code Point (DSCP).

9. En el campo Interface Shaping Rate, especifique el ancho de banda máximo de transmisión de salida en kbps.
Este ajuste limita la velocidad de transmisión de salida en incrementos de 1 por ciento en un rango de 0–100. Este valor se controla de forma independiente de cualquier configuración

de ancho de banda máximo por cola. Es, en efecto, un mecanismo de limitación de segundo nivel. El valor predeterminado es 0. El valor 0 significa que el máximo es ilimitado.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar las colas CoS de una interfaz

Puede definir el comportamiento de una cola configurando las colas de salida del switch. Puede controlar cuánto ancho de banda usa la cola, la profundidad de la cola durante la congestión y la planificación de la transmisión de paquetes de todas las colas de un puerto. Cada puerto tiene su propia configuración de colas CoS.

Para información sobre la configuración global de las colas CoS, consulte Configurar el modo de confianza CoS globalmente o para una interfaz específica en la página 455.

Para configurar las colas CoS de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > CoS > Advanced > Interface Queue Configuration. Se muestra la página Interface Queue Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú Queue ID, seleccione la cola.
Puede seleccionar una cola de 0 a 7.

9. En el campo Minimum Bandwidth, especifique el ancho de banda mínimo garantizado asignado a la cola en la interfaz.
Si este valor es mayor que el ancho de banda máximo correspondiente, el máximo aumenta automáticamente al mismo valor. El valor predeterminado es 0. El rango es de 0 a 100 en incrementos de 1. El valor 0 significa que no se aplica ningún ancho de banda mínimo garantizado. La suma de los anchos de banda mínimos de todas las colas de la interfaz seleccionada no puede superar el máximo (100).

El ajuste se aplica solo a la cola seleccionada en el menú Queue ID.

10. En el menú Scheduler Type, seleccione el tipo de planificación que se usa para la cola en la interfaz:

- Strict: La interfaz atiende primero el tráfico de mayor prioridad de una cola.
- Weighted: La interfaz usa round robin ponderado para asociar un peso a cada cola. Es la configuración predeterminada.

El ajuste se aplica solo a la cola seleccionada en el menú Queue ID.

11. En el menú Queue Management Type, seleccione el método de administración de la profundidad de cola que se usa para la cola en la interfaz:

- TailDrop: El método Taildrop descarta los paquetes si la cola está llena. Cuando se libera espacio en la cola, los paquetes vuelven a aceptarse. Es el método predeterminado.
- WRED: El método Weighted Random Early Detection (WRED) le permite refinar la administración de colas para descartar paquetes de forma selectiva (consulte Configurar la precedencia WRED de CoS para descartar paquetes en la página 462).

El ajuste se aplica solo a la cola seleccionada en el menú Queue ID.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar la precedencia WRED de CoS para descartar paquetes

Si usa el método Weighted Random Early Detection (WRED) para administrar la profundidad de cola (consulte Configurar las colas CoS de una interfaz en la página 460), puede configurar la precedencia para descartar paquetes si una cola está llena. Estos ajustes se aplican a una interfaz y una cola seleccionadas. Puede configurar ajustes distintos para cada cola y cada nivel de precedencia en una interfaz.

Para configurar la precedencia WRED de CoS para descartar paquetes:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > CoS> Advanced > CoS Queue Drop Precedence Configuration. Se muestra la página CoS Queue Drop Precedence Configuration.

6. En el menú Interface, seleccione una interfaz.
7. En el menú Queue ID, seleccione una cola de 0 a 7.

8. En el menú Drop Precedence Level, seleccione el nivel de precedencia de descarte de 1 a 4.
Los paquetes con nivel 1 son los que tienen más probabilidad de descartarse. Los paquetes con nivel 4 son los que tienen menos probabilidad de descartarse.

La siguiente tabla muestra los valores predeterminados de cada nivel de precedencia de descarte. Puede modificar estos ajustes.

Tabla 132. Valores predeterminados de los niveles de precedencia de descarte

Nivel de precedencia de descarte	WRED Minimum Threshold	WRED Maximum Threshold	WRED Drop Probability Scale
1	40	100	10
2	30	90	10
3	20	80	10
4	99	100	10

9. En el campo WRED Minimum Threshold, especifique el umbral mínimo de cola WRED por debajo del cual no se descarta ningún paquete para el nivel de precedencia seleccionado. El rango es de 0 a 100.

10. En el campo WRED Maximum Threshold, especifique el umbral máximo de cola de RED ponderado por encima del cual se descartan todos los paquetes para el nivel de precedencia actual.
El rango es de 0 a 100.

11. En el campo WRED Drop Probability Scale, especifique la probabilidad de descarte de paquetes para el nivel de precedencia actual.
El rango es de 0 a 100.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 133. Estado de precedencia de descarte de colas de interfaz CoS

Campo	Descripción
Interface	La interfaz CoS.
Queue ID	El ID de la cola.
Drop Precedence Level	El nivel de precedencia de descarte.
WRED Minimum Threshold	El valor del umbral mínimo de cola WRED.

Tabla 133. Estado de precedencia de descarte de colas de interfaz CoS (continuación)

Campo	Descripción
WRED Maximum Threshold	El valor del umbral máximo de cola WRED.
WRED Drop Probability Scale	El valor de probabilidad de descarte de paquetes WRED.

Servicios diferenciados

La función QoS incluye compatibilidad con servicios diferenciados (DiffServ), que permite clasificar el tráfico en flujos y darle un tratamiento QoS según comportamientos por salto (per-hop behaviors) definidos.

Las redes IP estándar ofrecen un servicio de entrega de datos de mejor esfuerzo. Este servicio implica que la red entrega los datos a tiempo, aunque sin garantía. Si hay congestión, los paquetes pueden retrasarse, enviarse de forma esporádica o descartarse. Para las aplicaciones de Internet típicas, como el correo electrónico y la transferencia de archivos, una ligera degradación del servicio es aceptable y en muchos casos imperceptible. Sin embargo, cualquier degradación puede afectar negativamente a las aplicaciones con requisitos de tiempo estrictos, como voz y multimedia.

Definición de DiffServ

Para usar DiffServ para QoS, primero debe definir las siguientes categorías y sus criterios:
1. Clase: Cree clases y defina sus criterios.
2. Política: Cree políticas, asocie clases a las políticas y defina las instrucciones de las políticas.
3. Servicio: Agregue una política a una interfaz de entrada.

Los paquetes se clasifican y procesan según criterios definidos. Los criterios de clasificación los define una clase. El procesamiento lo definen los atributos de una política. Los atributos de la política pueden definirse por instancia de clase, y son estos atributos los que se aplican cuando hay una coincidencia. Una política puede contener varias clases. Cuando la política está activa, las acciones dependen de la clase que coincida con el paquete.

Tenga en cuenta lo siguiente sobre el proceso DiffServ:

- Los paquetes se filtran y procesan según criterios definidos. Los criterios de filtrado los define una clase. El procesamiento lo definen los atributos de una política. Los atributos de la política

pueden definirse por instancia de clase, y son estos atributos los que se aplican cuando hay una coincidencia.

- El proceso de configuración comienza definiendo uno o más criterios de coincidencia para una clase. Luego se agregan una o más clases a una política. Después, las políticas se agregan a las interfaces.

El procesamiento de paquetes comienza evaluando los criterios de coincidencia de un paquete. La opción de tipo de clase All especifica que todos los criterios de una clase deben cumplirse para que un paquete coincida con esa clase. La opción Any especifica que al menos un criterio debe cumplirse para que un paquete coincida con esa clase. Las clases se evalúan en el orden en que se agregaron a la política. Una política se aplica a un paquete cuando se encuentra una coincidencia de clase en esa política.

Descripción general del asistente DiffServ

El asistente DiffServ habilita DiffServ en el switch creando una clase de tráfico, agregando la clase de tráfico a una política y luego agregando la política a los puertos que seleccione. El asistente DiffServ hace lo siguiente:

- Crea una clase DiffServ y define criterios de coincidencia que sirven de filtro para determinar si el tráfico entrante cumple los requisitos para pertenecer a la clase.
- Establece los criterios de coincidencia de la clase DiffServ según el tipo de tráfico seleccionado:
  - VOIP: Establece el criterio de coincidencia en protocolo UDP.
  - HTTP: Establece el criterio de coincidencia en puerto de destino HTTP.
  - FTP: Establece el criterio de coincidencia en puerto de destino FTP.
  - Telnet: Establece el criterio de coincidencia en puerto de destino Telnet.
  - Every: Establece el criterio de coincidencia para todo el tráfico.
- Crea una política DiffServ y la agrega a la clase DiffServ creada.
- Marca el tráfico de la siguiente manera:
  - Policing habilitado: Si el policing está habilitado, el estilo de la política DiffServ se establece en simple. El tráfico que cumple los criterios de la clase se procesa según la prioridad de salida seleccionada. La prioridad de salida configura el manejo del tráfico conforme de la siguiente manera:
  - High: Establece la acción de policing en markdscp ef.
  - Medium: Establece la acción de policing en markdscp af31.
  - Low: Establece la acción de policing en send.

- Policing deshabilitado: Si el policing está deshabilitado, todo el tráfico se marca así:
  - High: Establece la marca de la política en ipdscp ef.
  - Medium: Establece la marca de la política en ipdscp af31.
  - Low: Establece la marca de la política en ipdscp be.
- Agrega cada puerto y LAG seleccionado a la política.

Usar el asistente DiffServ para crear una clase de tráfico y una política para una o más interfaces

Para usar el asistente DiffServ para crear una clase de tráfico y una política para una o más interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > DiffServ Wizard. Se muestra la página DiffServ Wizard.

6. En el menú Traffic Type, defina la clase DiffServ seleccionando VOIP, HTTP, FTP, Telnet o Every.

7. En el campo Committed Rate (Kbps), especifique la tasa en Kbps que se aplica al tráfico de la clase.
El rango es de 1 al ancho de banda máximo admitido en la interfaz. El valor predeterminado es 1 Kbps.

La tasa comprometida se aplica si policing está habilitado (como lo está de forma predeterminada):

• Policing habilitado: La tasa comprometida se aplica a la política y la acción de policing se establece en conform.
• Policing deshabilitado: La tasa comprometida no se aplica y la política se establece en markdscp.

8. Para deshabilitar policing, desmarque la casilla Policing.
De forma predeterminada, policing está habilitado.

9. En el menú Outbound Priority, seleccione la prioridad para el tráfico saliente:
• High: La forma en que se aplica este ajuste depende de si policing está habilitado:

- Policing habilitado: High establece la acción en mark dscp ef.
- Policing deshabilitado: High establece la acción en mark ipdscp ef.

• Medium: La forma en que se aplica este ajuste depende de si policing está habilitado:

- Policing habilitado: Medium establece la acción en mark dscp af31.
- Policing deshabilitado: Medium establece la acción en mark ipdscp af31.

• Low: La forma en que se aplica este ajuste depende de si policing está habilitado:

- Policing habilitado: Low establece la acción en send.
- Policing deshabilitado: Low establece la acción en mark ipdscp be.

10. En la tabla Ports, haga clic en cada puerto al que desee agregar la política DiffServ.
11. En la tabla LAG, haga clic en cada LAG al que desee agregar la política DiffServ.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar el modo DiffServ y mostrar las entradas de las tablas MIB privadas de DiffServ

Puede habilitar o deshabilitar DiffServ y mostrar el número actual y máximo de filas en cada una de las principales tablas MIB privadas de DiffServ.

Para configurar el modo DiffServ y mostrar las entradas de las tablas MIB privadas de DiffServ:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Basic > DiffServ Configuration. Se muestra la página DiffServ Configuration.

6. Seleccione el modo administrativo de DiffServ:

- Enable: Los servicios diferenciados están activos. Este es el ajuste predeterminado.
- Disable: Los servicios diferenciados están inactivos. La configuración DiffServ existente se conserva y puede cambiarse, pero no está activa.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 134. Información de DiffServ Status

Campo	Descripción
Class table	El número de clases DiffServ configuradas del total permitido en el switch.
Class Rule table	El número de reglas de clase configuradas del total permitido en el switch.
Policy table	El número de políticas configuradas del total permitido en el switch.
Policy Instance table	El número de instancias de clase de política configuradas del total permitido en el switch.
Policy Attributes table	El número de atributos de política configurados (vinculados a las instancias de clase de política) del total permitido en el switch.
Service table	El número de servicios configurados (vinculados a las políticas en interfaces especificadas) del total permitido en el switch.

Configurar una clase DiffServ

Puede agregar un nuevo nombre de clase DiffServ, o cambiar el nombre o eliminar una clase existente. También puede definir los criterios que se asocian con una clase DiffServ. A medida que se reciben paquetes, estas clases DiffServ se usan para priorizarlos. Puede usar varios criterios de coincidencia en una clase. La lógica es un AND lógico booleano para estos criterios.

Agregar y configurar una clase DiffServ Para agregar y configurar una clase DiffServ:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Class Configuration. Se muestra la página Class Configuration.

6. En el campo Class Name, ingrese un nombre de clase.
El campo Class Name también enumera todos los nombres de clases DiffServ existentes, de los que puede seleccionar uno para modificarlo o eliminarlo. El nombre de clase puede tener de 1 a 31 caracteres alfanuméricos.

7. En el menú Class Type, seleccione una de las siguientes opciones:

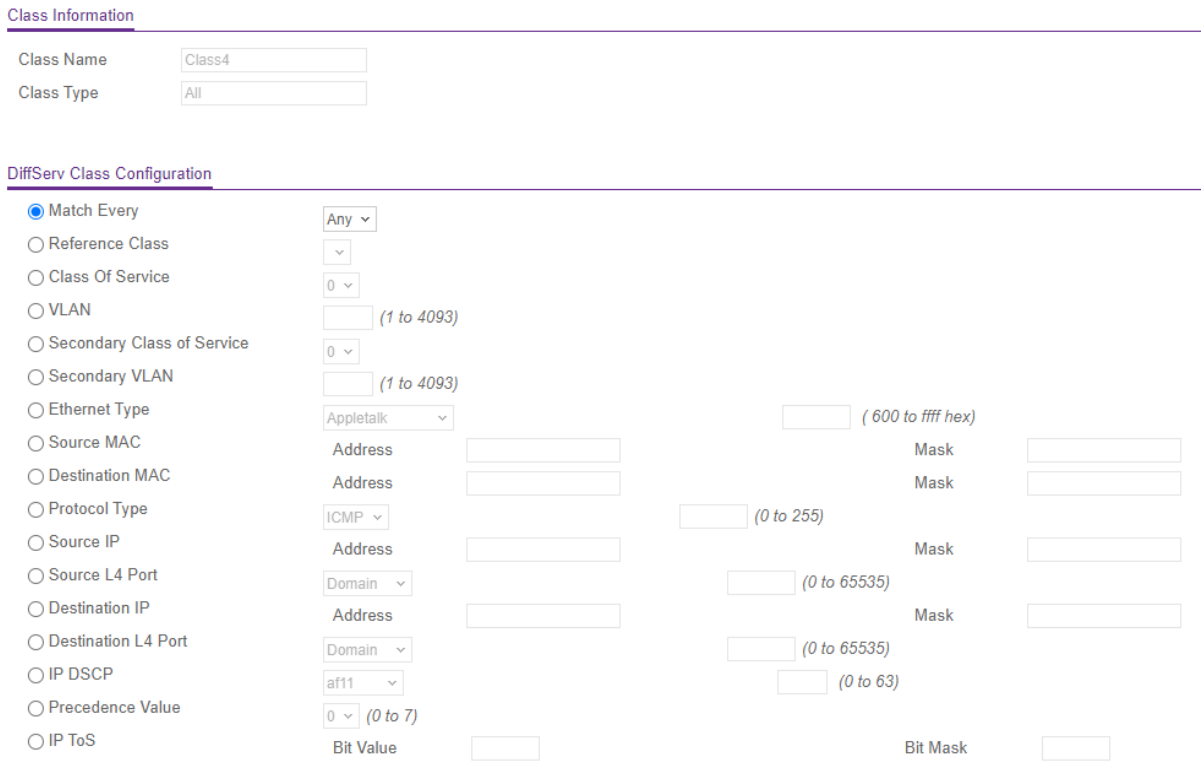
• All: Se deben cumplir todos los criterios de coincidencia definidos para la clase para que un paquete coincida. All significa el AND lógico de todos los criterios de coincidencia.
Por ejemplo, si la clase incluye un criterio para una dirección IP y otro criterio para una dirección MAC, el tráfico debe coincidir con ambos criterios.
• Any: Se debe cumplir cualquiera de los criterios de coincidencia definidos para la clase para que un paquete coincida.
Por ejemplo, si la clase incluye un criterio para una dirección IP y otro criterio para una dirección MAC, el tráfico debe coincidir con uno de los criterios, pero no necesita coincidir con ambos.

Solo puede seleccionar el tipo de clase al crear una clase nueva. Una vez creada la clase, no puede modificar su tipo.

8. Haga clic en el botón Add.
Se agrega la nueva clase.

9. Después de crear la clase, haga clic en el nombre de la clase.

El nombre de la clase es un hipervínculo a la página en la que puede definir la configuración de la clase (consulte la siguiente figura).



10. Defina los criterios que deben asociarse con la clase DiffServ seleccionando uno de los siguientes botones de opción:

- Match Every: Seleccione este botón de opción para agregar una condición de coincidencia que considera que todos los paquetes pertenecen a la clase. La única opción del menú Match Every es Any.
- Reference Class: Seleccione este botón de opción para hacer referencia a otra clase para los criterios. Los criterios de coincidencia definidos en la clase de referencia funcionan como criterios de coincidencia además de los que defina para la clase seleccionada. Después de seleccionar el botón de opción, se muestran las clases a las que se puede hacer referencia. Seleccione la clase de referencia. Una clase solo puede hacer referencia a otra clase del mismo tipo.
- Class of Service: Seleccione este botón de opción para exigir que el valor de Class of Service (CoS) en el encabezado de una trama Ethernet coincida con el valor CoS especificado. Esta opción enumera todos los valores del criterio Class of Service en el rango de 0 a 7, de los que puede seleccionar uno.
- VLAN: Seleccione este botón de opción para exigir que el ID de VLAN de un paquete coincida con un ID de VLAN. El valor de VLAN está en el rango de 1 a 4093.
- Secondary Class of Service: Seleccione este botón de opción para exigir que el valor secundario de Class of Service (CoS) en el encabezado de una trama Ethernet coincida con el valor CoS secundario especificado.

• Secondary VLAN: Seleccione este botón de opción para exigir que el ID de VLAN de un paquete coincida con un ID de VLAN secundario. El valor de VLAN está en el rango de 1 a 4093.
• Ethernet Type: Seleccione este botón de opción para exigir que el valor EtherType del encabezado de la trama Ethernet coincida con el valor EtherType especificado. Después de seleccionar el botón de opción, seleccione la palabra clave EtherType en el menú de protocolos comunes asignados a su valor EtherType. También puede seleccionar User Value en el menú e ingresar un valor hexadecimal en el rango de 600 a ffff.
• Source MAC: Seleccione este botón de opción para exigir que la dirección MAC de origen de un paquete coincida con la dirección MAC especificada. Después de seleccionarlo, use los siguientes campos para configurar los criterios de coincidencia de la dirección MAC de origen:

- Address: La dirección MAC de origen que debe coincidir. La dirección MAC de origen se especifica como seis números hexadecimales de dos dígitos separados por dos puntos.
- Mask: La máscara MAC, que especifica los bits de la dirección MAC de origen que se comparan con la trama Ethernet. Use F y ceros para configurar la máscara MAC. Una F significa que el bit se verifica, y un cero en una posición de bit significa que el dato no es significativo. Por ejemplo, si la dirección MAC es aa:bb:cc:dd:ee:ff y la máscara es ff:ff:00:00:00:00, todas las direcciones MAC con aa:bb:xx:xx:xx:xx coinciden (donde x es cualquier número hexadecimal). Tenga en cuenta que esta no es una máscara comodín como la que usan las ACL.

• Destination MAC: Seleccione este botón de opción para exigir que la dirección MAC de destino de un paquete coincida con la dirección MAC especificada. Después de seleccionar el botón de opción, use los siguientes campos para configurar los criterios de coincidencia de la dirección MAC de destino:

- Address: La dirección MAC de destino que debe coincidir. La dirección MAC de destino se especifica como seis números hexadecimales de dos dígitos separados por dos puntos.
- Mask: La máscara MAC, que especifica los bits de la dirección MAC de destino que se comparan con una trama Ethernet. Use F y ceros para configurar la máscara MAC. Una F significa que el bit se verifica, y un cero en una posición de bit significa que el dato no es significativo. Por ejemplo, si la dirección MAC es aa:bb:cc:dd:ee:ff y la máscara es ff:ff:00:00:00:00, todas las direcciones MAC con aa:bb:xx:xx:xx:xx coinciden (donde x es cualquier número hexadecimal). Tenga en cuenta que esta no es una máscara comodín como la que usan las ACL.

• Protocol Type: Seleccione este botón de opción para exigir que el protocolo de capa 4 de un paquete coincida con el protocolo especificado, que debe seleccionar en el menú. También puede seleccionar Other en el menú e ingresar un número de protocolo de 0 a 255.
• Source IP: Seleccione este botón de opción para exigir que la dirección IP de origen de un paquete coincida con la dirección IP especificada. Después de seleccionar el botón de opción, use los siguientes campos para configurar los criterios de coincidencia de la dirección IP de origen:

- Address: El formato de dirección IP de origen que debe coincidir, en notación decimal con puntos.

- Mask: La máscara de bits en formato IP decimal con puntos que indica qué partes de la dirección IP de origen se usan para comparar con el contenido del paquete.

• Source L4 Port: Seleccione este botón de opción para exigir que el puerto de origen TCP/UDP de un paquete coincida con el protocolo especificado, que debe seleccionar en el menú. También puede seleccionar Other en el menú e ingresar un número de puerto de 0 a 65535.
• Destination IP: Seleccione este botón de opción para exigir que la dirección IP de destino de un paquete coincida con la dirección IP especificada. Después de seleccionar el botón de opción, use los siguientes campos para configurar los criterios de coincidencia de la dirección IP de destino:

- Address: El formato de dirección IP de destino que debe coincidir, en notación decimal con puntos.
- Mask: La máscara de bits en formato IP decimal con puntos que indica qué partes de la dirección IP de destino se usan para comparar con el contenido del paquete.

• Destination L4 Port: Seleccione este botón de opción para exigir que el puerto TCP/UDP de destino de un paquete coincida con el protocolo especificado. También puede seleccionar Other en el menú e ingresar un número de puerto de 0 a 65535.
• IP DSCP: Seleccione este botón de opción para exigir que el valor IP DiffServ Code Point (DSCP) del paquete coincida con el código de palabra clave IP DSCP especificado, que debe seleccionar en el menú. También puede seleccionar Other en el menú e ingresar un valor IP DSCP de 0 a 63. El valor DSCP se define como los 6 bits de orden superior del octeto Service Type en el encabezado IP.
• Precedence Value: Seleccione este botón de opción para exigir que el valor de precedencia IP del paquete coincida con el número especificado de 0 a 7, que debe seleccionar en el menú. El campo IP Precedence de un paquete se define como los 3 bits de orden superior del octeto Service Type en el encabezado IP.
• IP ToS: Seleccione este botón de opción para exigir que los bits Type of Service (ToS) del paquete en el encabezado IP coincidan con el valor especificado. El campo IP ToS de un paquete se define como los 8 bits del octeto de tipo de servicio en el encabezado IP. Después de seleccionar el botón de opción, use los siguientes campos para configurar los criterios de coincidencia de ToS:

- Bit Value: Ingrese un valor de octeto hexadecimal de dos dígitos en el rango de 00 a ff para que coincida con los bits del campo ToS de un paquete.
- Bit Mask: Especifique las posiciones de bits que se usan para comparar con el campo IP ToS de un paquete.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la sección Class Summary.

Tabla 135. Información de DiffServ Class Configuration, Class Summary

Campo	Descripción
Match Criteria	Los criterios de coincidencia configurados para la clase especificada.
Values	Los valores de los criterios de coincidencia configurados.

Cambiar el nombre de una clase DiffServ existente Para cambiar el nombre de una clase DiffServ existente:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Class Configuration. Se muestra la página Class Configuration.

6. Marque la casilla junto al nombre de la clase.
7. En el campo Class Name, especifique el nuevo nombre.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar los criterios de una clase DiffServ existente Para cambiar los criterios de una clase DiffServ existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Class Configuration. Se muestra la página Class Configuration.

6. Haga clic en el nombre de la clase, que es un hipervínculo.
Se muestra la página en la que puede cambiar la configuración de la clase.

7. Cambie la configuración de la clase según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una clase DiffServ Para eliminar una clase DiffServ:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Class Configuration. Se muestra la página Class Configuration.

6. Marque la casilla junto al nombre de la clase.

7. Haga clic en el botón
Delete. Se elimina la clase.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una clase DiffServ IPv6

El switch admite la funcionalidad de ACL de QoS y DiffServ para IPv6 al ofrecer compatibilidad con la clasificación de paquetes IPv6. Una ACL IPv6 cumple la misma función que una ACL IPv4.

Un paquete Ethernet IPv6 se distingue de un paquete IPv4 por su valor EtherType único, por lo que todos los clasificadores IPv6 incluyen el campo EtherType, aunque no puede configurar su valor para una clase IPv6 en el switch.

Las direcciones IPv6 de destino y de origen usan un valor de longitud de prefijo en lugar de una máscara individual para calificarlas como direcciones de subred o de host. Los paquetes que coinciden con un clasificador IPv6 pueden marcarse con el campo IP DSCP del octeto de clase de tráfico.

También puede asignar una ACL IPv6 con una asignación DiffServ a interfaces LAG.

Puede agregar un nuevo nombre de clase DiffServ, o cambiar el nombre o eliminar una clase existente. A medida que se reciben paquetes, estas clases DiffServ se usan para priorizarlos. Puede usar varios criterios de coincidencia en una clase. La lógica es un AND lógico booleano para estos criterios.

Agregar y configurar una clase DiffServ IPv6 Para configurar una clase DiffServ IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > IPv6 Class Configuration. Se muestra la página Class Configuration.

6. En el campo Class Name, ingrese un nombre de clase.
El campo Class Name también enumera todos los nombres de clases DiffServ existentes, de los que puede seleccionar uno para modificarlo o eliminarlo. El nombre de clase puede tener de 1 a 31 caracteres alfanuméricos.

7. En el menú Class Type, seleccione una de las siguientes opciones:

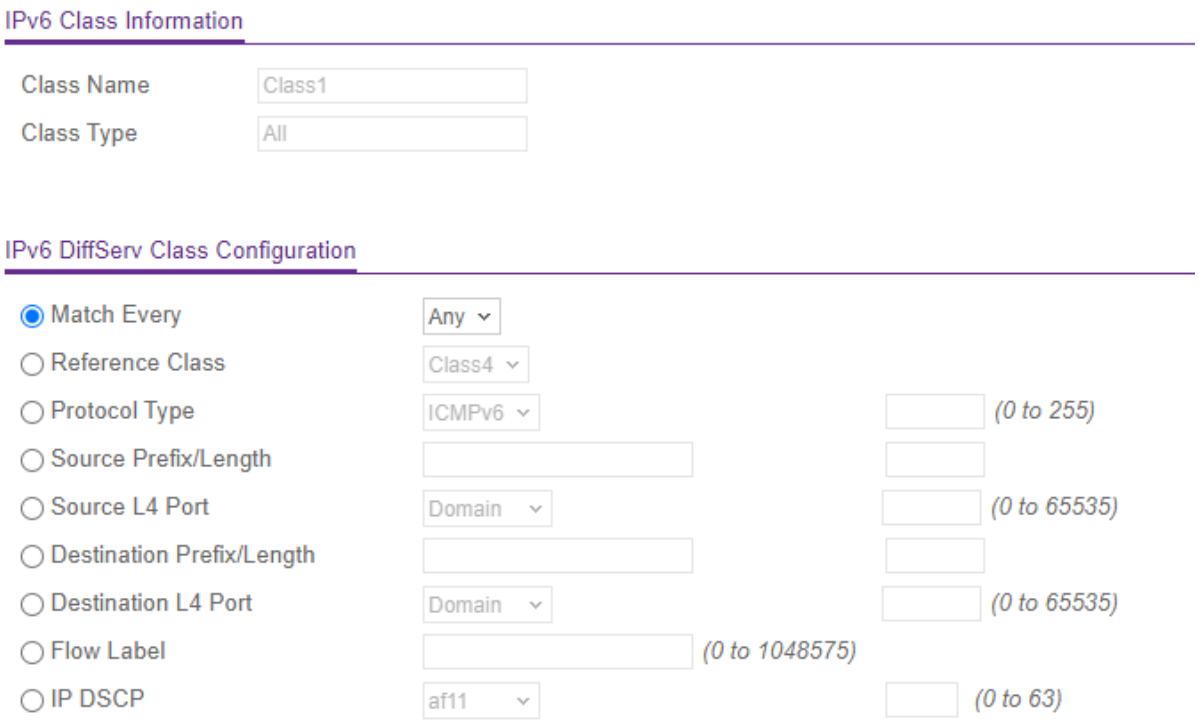
- All: Se deben cumplir todos los criterios de coincidencia definidos para la clase para que un paquete coincida. All significa el AND lógico de todos los criterios de coincidencia.

Por ejemplo, si la clase incluye un criterio para una dirección IP y otro criterio para una dirección MAC, el tráfico debe coincidir con ambos criterios.
• Any: Se debe cumplir cualquiera de los criterios de coincidencia definidos para la clase para que un paquete coincida.
Por ejemplo, si la clase incluye un criterio para una dirección IP y otro criterio para una dirección MAC, el tráfico debe coincidir con uno de los criterios, pero no necesita coincidir con ambos.

Solo puede seleccionar el tipo de clase al crear una clase nueva. Una vez creada la clase, no puede modificar su tipo.

8. Haga clic en el botón Add.
Se agrega la nueva clase.

9. Después de crear la clase, haga clic en el nombre de la clase.
El nombre de la clase es un hipervínculo a la página en la que puede definir la configuración de la clase (consulte la siguiente figura).



10. Defina los criterios que se asocian con una clase DiffServ:

• Match Every: Seleccione este botón de opción para agregar una condición de coincidencia que considera que todos los paquetes pertenecen a la clase. La única opción del menú Match Every es Any.

• Reference Class: Seleccione este botón de opción para hacer referencia a otra clase para los criterios. Los criterios de coincidencia definidos en la clase de referencia funcionan como criterios de coincidencia además de los que defina para la clase seleccionada. Después de seleccionar esta opción, se muestran las clases a las que se puede hacer referencia. Seleccione la clase de referencia. Una clase puede hacer referencia a otra clase del mismo tipo.
• Protocol Type: Seleccione este botón de opción para exigir que el protocolo de capa 4 de un paquete coincida con el protocolo especificado, que debe seleccionar en el menú. El menú incluye la opción Other, que le permite ingresar un número de protocolo de 0 a 255.
• Source Prefix/Length: Seleccione este botón de opción para exigir que el prefijo de origen de un paquete y su longitud coincidan con el prefijo IPv6 de origen y la longitud de prefijo especificados. El prefijo siempre debe especificarse con la longitud de prefijo. El prefijo puede estar en el rango hexadecimal de 0 a FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF y la longitud de prefijo puede estar en el rango de 0 a 128.
• Source L4 Port: Seleccione este botón de opción para exigir que el puerto de origen TCP/UDP de un paquete coincida con el protocolo especificado, que debe seleccionar en el menú. El rango es de 0 a 65535. El menú incluye Other como opción para puertos sin nombre.
• Destination Prefix/Length: Seleccione este botón de opción para exigir que el prefijo de destino de un paquete y su longitud coincidan con el prefijo IPv6 de origen y la longitud de prefijo especificados. El prefijo siempre debe especificarse con la longitud de prefijo. El prefijo puede estar en el rango hexadecimal de 0 a FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF y la longitud de prefijo puede estar en el rango de 0 a 128.
• Destination L4 Port: Seleccione este botón de opción para exigir que el puerto TCP/UDP de destino de un paquete coincida con el protocolo especificado, que debe seleccionar en el menú. El rango es de 0 a 65535. El menú incluye Other como opción para puertos sin nombre.
• Flow Label: Seleccione este botón de opción para exigir que la etiqueta de flujo de un paquete coincida con la etiqueta de flujo especificada. La etiqueta de flujo es un número de 20 bits exclusivo de un paquete IPv6 que las estaciones finales usan para indicar el tratamiento de QoS en los routers. La etiqueta de flujo puede especificarse en el rango de 0 a 1048575.
• IP DSCP: Seleccione este botón de opción para exigir que el valor IP DiffServ Code Point (DSCP) del paquete coincida con el código de palabra clave IP DSCP especificado, que debe seleccionar en el menú. El menú incluye la opción Other, que le permite ingresar un valor IP DSCP de 0 a 63. El valor DSCP se define como los 6 bits de orden superior del octeto Service Type en el encabezado IP.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra en la sección Class Summary.

Tabla 136. Resumen de clases de la configuración de clases DiffServ IPv6

Campo	Descripción
Match Criteria	Los criterios de coincidencia configurados para la clase especificada.
Values	Los valores de los criterios de coincidencia configurados.

Cambiar el nombre de una clase DiffServ IPv6 existente Para cambiar el nombre de una clase DiffServ IPv6 existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > IPv6 Class Configuration. Se muestra la página Class Configuration.

6. Marque la casilla junto al nombre de la clase.
7. En el campo Class Name, especifique el nuevo nombre.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar los criterios de una clase DiffServ IPv6 existente Para cambiar los criterios de una clase DiffServ IPv6 existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > IPv6 Class Configuration. Se muestra la página Class Configuration.

6. Haga clic en el nombre de la clase, que es un hipervínculo.
Se muestra la página en la que puede cambiar la configuración de la clase.

7. Cambie la configuración de la clase según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una clase DiffServ IPv6

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > IPv6 Class Configuration. Se muestra la página Class Configuration.

6. Marque la casilla junto al nombre de la clase.

7. Haga clic en el botón
Delete. Se elimina la clase.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una política DiffServ

Puede asociar un conjunto de clases con una o más políticas.

<<TBD>>Crear y configurar una política DiffServ Para crear y configurar una política DiffServ:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Policy Configuration. Se muestra la página Policy Configuration.

6. En el campo Policy Name, ingrese un nombre de política.
El nombre de la clase de política puede tener de 1 a 31 caracteres alfanuméricos.

7. En el menú Policy Type, seleccione la dirección del flujo de tráfico a la que debe aplicarse la política:

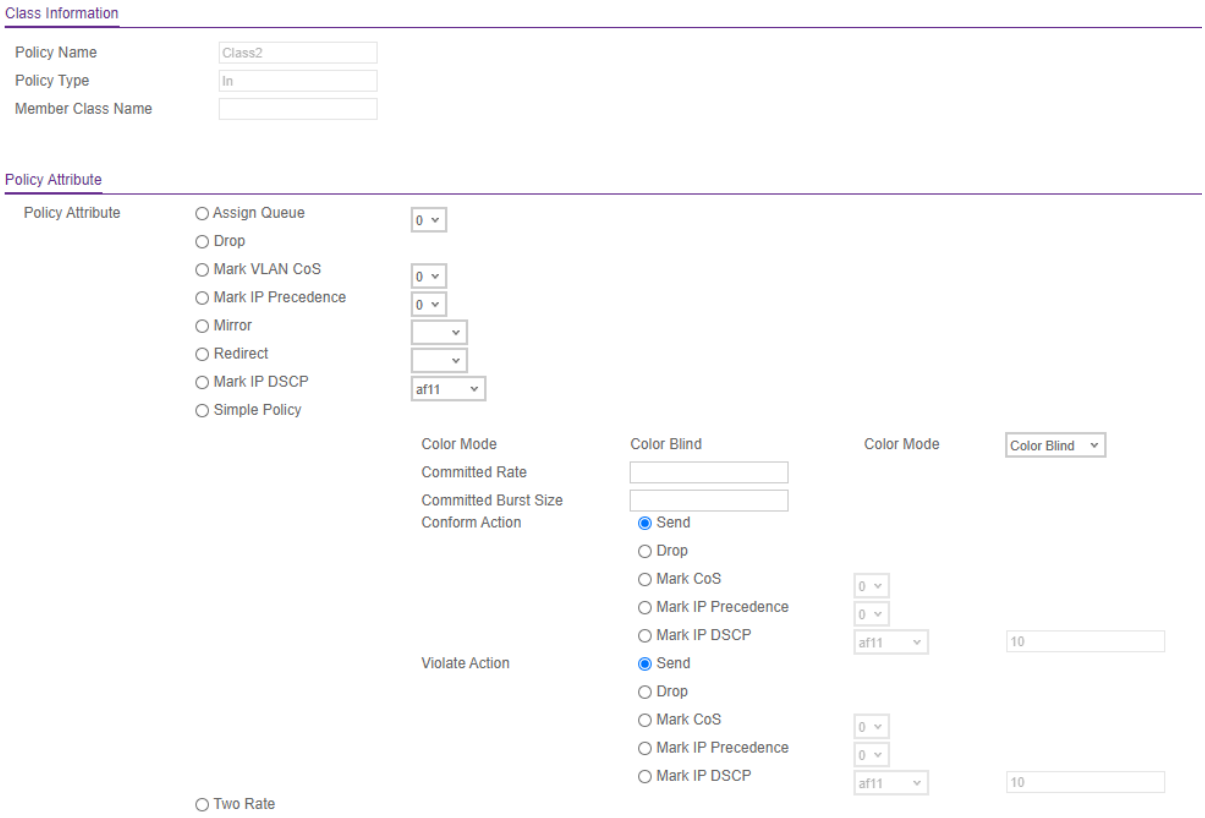
- In: La política se aplica al tráfico entrante.
- Out: La política se aplica al tráfico saliente.

8. En el menú Member Class, seleccione una clase existente que desee asociar con la nueva política.

9. Haga clic en el botón Add.
Se agrega la nueva política.

10. Después de crear la política, haga clic en el nombre de la política.
El nombre de la política es un hipervínculo a la página en la que puede definir los atributos de la política (consulte la siguiente figura, que no muestra la sección Two Rate de

la página). <<TBD, cambiar captura de pantalla. No hay menú Color Mode. Agregar botón Mark QoS as secondary CoS, pero solo para M4300.>>



11. Configure los atributos de la política seleccionando uno de los siguientes botones de opción:

    • Assign Queue: Seleccione este botón de opción para especificar que el tráfico se asigne a una cola, que debe seleccionar en el menú. La cola se expresa como un valor en el rango de 0 a 7.
    • Drop: Seleccione este botón de opción para exigir que se descarte cada paquete.
    • Mark VLAN CoS: Seleccione este botón de opción para especificar la prioridad de VLAN, que debe seleccionar en el menú. La prioridad de VLAN se expresa como un valor en el rango de 0 a 7.
    • Mark CoS As Secondary CoS: Seleccione este botón de opción para especificar que los bits de prioridad de la etiqueta VLAN externa de los paquetes se establezcan como la prioridad de la etiqueta VLAN interna. Es decir, para estos paquetes, el CoS de la etiqueta VLAN interna se copia al CoS de la etiqueta VLAN externa.
    • Mark IP Precedence: Seleccione este botón de opción para exigir que los paquetes se marquen con un valor de precedencia IP antes de reenviarse. Debe seleccionar un valor de precedencia IP de 0 a 7 en el menú.
    • Mirror: Seleccione este botón de opción para exigir que los paquetes se reflejen en una interfaz o LAG, que debe seleccionar en el menú.
    • Redirect: Seleccione este botón de opción para exigir que los paquetes se redirijan a una interfaz o LAG, que debe seleccionar en el menú.

• Mark IP DSCP: seleccione este botón de opción para que el paquete se marque con un código de palabra clave IP DSCP, que debe seleccionar en el menú. El valor DSCP se define como los 6 bits de orden superior del octeto Service Type del encabezado IP.
• Simple Policy: seleccione este botón de opción para definir el estilo de vigilancia de tráfico simple para la clase. De forma predeterminada, la política simple es ciega al color y no se aplican clases de color. Puede hacer que la política simple reconozca el color y seleccionar una clase de color. Una política simple admite una sola tasa de datos y aplica una acción a los paquetes que cumplen la política y otra a los paquetes que la infringen.

a. <<TBD if Color Aware is out.>> Especifique la clase de color para la política simple:

- Color Blind: es la selección predeterminada. No se aplican clases de color.
- Color Aware: seleccione este botón de opción para exigir una clase de color válida para esta instancia de política. Después de seleccionar Color Aware en el menú Color Mode, se muestra el menú Color Conform Class. En este menú, seleccione otra clase (una que ya haya creado; consulte Configurar una clase DiffServ en la página 468 o Configurar una clase DiffServ IPv6 en la página 475). En el contexto de esta política, a esta clase seleccionada la llamamos clase de color. Una clase de color válida contiene un solo criterio de coincidencia no excluyente, siempre que dicho criterio no entre en conflicto con el clasificador de la propia instancia de política:

b. Especifique la tasa de tráfico y el tamaño de ráfaga para los paquetes que cumplen la política simple.

- Committed Rate: especifique la tasa comprometida que se aplica a los paquetes conformes introduciendo un valor de 1 a 4294967295 kilobits por segundo (Kbps). La tasa comprometida se usa para limitar la tasa de llegada del tráfico conforme.
- Committed Burst Size: especifique el tamaño de ráfaga que se aplica a los paquetes conformes introduciendo un valor de 1 a 128 KBytes (KB). El tamaño de ráfaga comprometido se usa para limitar la cantidad de tráfico conforme.

c. Especifique una acción de política para los paquetes que cumplen la política simple.

- Send: los paquetes se reenvían sin modificar. Es la acción predeterminada para paquetes conformes.
- Drop: los paquetes se descartan.
- Mark CoS: DiffServ marca los paquetes con el valor CoS especificado antes de reenviarlos. Esta opción requiere que el campo Mark CoS esté configurado. Debe seleccionar en el menú un valor CoS de 0 a 7.
- Mark CoS As Secondary CoS: en estos paquetes, los bits de prioridad de la etiqueta VLAN externa se establecen igual a la prioridad de la etiqueta VLAN interna. Es decir, en estos paquetes, el CoS de la etiqueta VLAN interna se copia al CoS de la etiqueta VLAN externa.

- Mark IP Precedence: DiffServ marca estos paquetes con el valor IP Precedence especificado antes de reenviarlos. Esta opción requiere que el campo Mark IP Precedence esté configurado. Debe seleccionar en el menú un valor de IP Precedence de 0 a 7.
- Mark IP DSCP: DiffServ marca los paquetes con el valor DSCP especificado antes de reenviarlos. Esta opción requiere que el campo DSCP esté configurado. Debe seleccionar un código DSCP en el menú o introducir un valor IP DSCP de 0 a 63 en el campo junto al menú. Un valor que introduzca en el campo anula cualquier selección del menú. El valor DSCP se define como los seis bits de orden superior del octeto Service Type del encabezado IP.

d. Especifique una acción de política para los paquetes que infringen la política simple.

- Send: los paquetes se reenvían sin modificar. Es la acción predeterminada para infracciones.
- Drop: los paquetes se descartan.
- Mark CoS: DiffServ marca los paquetes con el valor CoS especificado antes de reenviarlos. Esta opción requiere que el campo Mark CoS esté configurado. Debe seleccionar en el menú un valor CoS de 0 a 7.
- Mark CoS As Secondary CoS: en estos paquetes, los bits de prioridad de la etiqueta VLAN externa se establecen igual a la prioridad de la etiqueta VLAN interna. Es decir, en estos paquetes, el CoS de la etiqueta VLAN interna se copia al CoS de la etiqueta VLAN externa.
- Mark IP Precedence: DiffServ marca estos paquetes con el valor IP Precedence especificado antes de reenviarlos. Esta opción requiere que el campo Mark IP Precedence esté configurado. Debe seleccionar en el menú un valor de IP Precedence de 0 a 7.
- Mark IP DSCP: DiffServ marca los paquetes con el valor DSCP especificado antes de reenviarlos. Esta opción requiere que el campo DSCP esté configurado. Debe seleccionar un código DSCP en el menú o introducir un valor IP DSCP de 0 a 63 en el campo junto al menú. Un valor que introduzca en el campo anula cualquier selección del menú. El valor DSCP se define como los seis bits de orden superior del octeto Service Type del encabezado IP.

• Two Rate: seleccione este botón de opción para definir un estilo de vigilancia de tráfico de dos tasas para la clase. Una política de dos tasas se diferencia de una simple en que permite definir una tasa pico y un tamaño de ráfaga pico, además de la tasa y el tamaño de ráfaga comprometidos.
De forma predeterminada, la política de dos tasas es ciega al color y no se aplican clases de color. Puede hacer que reconozca el color y seleccionar una clase de color.

Una política de dos tasas admite dos tasas de datos y aplica una acción a los paquetes que cumplen la política y otra a los paquetes que la infringen.

a. Especifique la clase de color:

- Color Blind: es la selección predeterminada. No se aplican clases de color.
- Color Aware: seleccione este botón de opción para exigir una clase de color válida para esta instancia de política. Después de seleccionar Color Aware en el menú Color Mode, se muestra el menú Color Conform Class. En este menú, seleccione otra clase (una que ya haya creado; consulte Configurar una clase DiffServ en la página 468 o Configurar una clase DiffServ IPv6 en la página 475). En el contexto de esta política, a esta clase seleccionada la llamamos clase de color. Una clase de color válida contiene un solo criterio de coincidencia no excluyente, siempre que dicho criterio no entre en conflicto con el clasificador de la propia instancia de política:

b. Especifique las tasas de tráfico y los tamaños de ráfaga para los paquetes que cumplen la política simple.

- Committed Rate: especifique la tasa comprometida que se aplica a los paquetes conformes introduciendo un valor de 1 a 4294967295 kilobits por segundo (Kbps). La tasa comprometida se usa para garantizar el ancho de banda permitido del tráfico conforme.
- Committed Burst Size: especifique el tamaño de ráfaga que se aplica a los paquetes conformes introduciendo un valor de 1 a 128 KBytes (KB). El tamaño de ráfaga comprometido limita el número máximo de bytes en una ráfaga (un instante muy breve) de tráfico conforme.
- Peak Rate: especifique la tasa pico que se aplica a los paquetes conformes introduciendo un valor de 1 a 4294967295 kilobits por segundo (Kbps). La tasa pico limita cuánto puede superar una ráfaga de tráfico conforme la tasa comprometida.
- Peak Burst Size: especifique el tamaño de ráfaga pico que se aplica a los paquetes conformes introduciendo un valor de 1 a 128 KBytes (KB). El tamaño de ráfaga pico limita cuánto puede superar una ráfaga de tráfico conforme la tasa pico.

c. Especifique una acción de política para los paquetes que cumplen la política de dos tasas.

- Send: los paquetes se reenvían sin modificar. Es la acción predeterminada para paquetes conformes.
- Drop: los paquetes se descartan.
- Mark CoS: DiffServ marca los paquetes con el valor CoS especificado antes de reenviarlos. Esta opción requiere que el campo Mark CoS esté configurado. Debe seleccionar en el menú un valor CoS de 0 a 7.

- Mark CoS As Secondary CoS: en estos paquetes, los bits de prioridad de la etiqueta VLAN externa se establecen igual a la prioridad de la etiqueta VLAN interna. Es decir, en estos paquetes, el CoS de la etiqueta VLAN interna se copia al CoS de la etiqueta VLAN externa.
- Mark IP Precedence: DiffServ marca estos paquetes con el valor IP Precedence especificado antes de reenviarlos. Esta opción requiere que el campo Mark IP Precedence esté configurado. Debe seleccionar en el menú un valor de IP Precedence de 0 a 7.
- Mark IP DSCP: DiffServ marca los paquetes con el valor DSCP especificado antes de reenviarlos. Esta opción requiere que el campo DSCP esté configurado. Debe seleccionar un código DSCP en el menú o introducir un valor IP DSCP de 0 a 63 en el campo junto al menú. Un valor que introduzca en el campo anula cualquier selección del menú.
  El valor DSCP se define como los seis bits de orden superior del octeto Service Type del encabezado IP.

d. Especifique una acción de política para los paquetes que exceden la política de dos tasas.

- Send: los paquetes se reenvían sin modificar. Es la acción predeterminada para infracciones.
- Drop: los paquetes se descartan.
- Mark CoS: DiffServ marca los paquetes con el valor CoS especificado antes de reenviarlos. Esta opción requiere que el campo Mark CoS esté configurado. Debe seleccionar en el menú un valor CoS de 0 a 7.
- Mark CoS As Secondary CoS: en estos paquetes, los bits de prioridad de la etiqueta VLAN externa se establecen igual a la prioridad de la etiqueta VLAN interna. Es decir, en estos paquetes, el CoS de la etiqueta VLAN interna se copia al CoS de la etiqueta VLAN externa.
- Mark IP Precedence: DiffServ marca estos paquetes con el valor IP Precedence especificado antes de reenviarlos. Esta opción requiere que el campo Mark IP Precedence esté configurado. Debe seleccionar en el menú un valor de IP Precedence de 0 a 7.
- Mark IP DSCP: DiffServ marca los paquetes con el valor DSCP especificado antes de reenviarlos. Esta opción requiere que el campo DSCP esté configurado. Debe seleccionar un código DSCP en el menú o introducir un valor IP DSCP de 0 a 63 en el campo junto al menú. Un valor que introduzca en el campo anula cualquier selección del menú.
  El valor DSCP se define como los seis bits de orden superior del octeto Service Type del encabezado IP.

e. Especifique una acción de política para los paquetes que infringen la política de dos tasas.

- Send: los paquetes se reenvían sin modificar. Es la acción predeterminada para infracciones.
- Drop: los paquetes se descartan.

- Mark CoS: DiffServ marca los paquetes con el valor CoS especificado antes de reenviarlos. Esta opción requiere que el campo Mark CoS esté configurado. Debe seleccionar en el menú un valor CoS de 0 a 7.
- Mark CoS As Secondary CoS: en estos paquetes, los bits de prioridad de la etiqueta VLAN externa se establecen igual a la prioridad de la etiqueta VLAN interna. Es decir, en estos paquetes, el CoS de la etiqueta VLAN interna se copia al CoS de la etiqueta VLAN externa.
- Mark IP Precedence: DiffServ marca estos paquetes con el valor IP Precedence especificado antes de reenviarlos. Esta opción requiere que el campo Mark IP Precedence esté configurado. Debe seleccionar en el menú un valor de IP Precedence de 0 a 7.
- Mark IP DSCP: DiffServ marca los paquetes con el valor DSCP especificado antes de reenviarlos. Esta opción requiere que el campo DSCP esté configurado. Debe seleccionar un código DSCP en el menú o introducir un valor IP DSCP de 0 a 63 en el campo junto al menú. Un valor que introduzca en el campo anula cualquier selección del menú.
  El valor DSCP se define como los seis bits de orden superior del octeto Service Type del encabezado IP.

12. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 137. Configuración de políticas DiffServ, atributos de política

Campo	Descripción
Policy Name	Nombre de la política DiffServ.
Policy Type	Tipo de política (In u Out).
Member Class Name	Instancias de clase asociadas a la política.

Cambiar el nombre de una política DiffServ existente Para cambiar el nombre de una política DiffServ existente:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Policy Configuration. Se muestra la página Policy Configuration.

6. Seleccione la casilla junto al nombre de la política.
7. En el campo Policy Name, especifique el nuevo nombre.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar los atributos de una política DiffServ existente Para cambiar los atributos de una política DiffServ existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Policy Configuration. Se muestra la página Policy Configuration.

6. Haga clic en el nombre de la política, que es un hipervínculo.
Se muestra la página donde puede cambiar los atributos de la política.

7. Cambie los atributos de la política según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar o quitar una clase de una política DiffServ existente Para cambiar o quitar una clase de una política DiffServ existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Policy Configuration. Se muestra la página Policy Configuration.

6. Seleccione la casilla junto al nombre de la política.
7. Realice una de las siguientes acciones:

- Para cambiar la clase, seleccione otra clase en el menú Member Class.
- Para quitar la clase, seleccione None en el menú Member Class.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una política DiffServ Para eliminar una política DiffServ:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Policy Configuration. Se muestra la página Policy Configuration.

6. Seleccione la casilla junto al nombre de la política.

7. Haga clic en el botón Delete. Se elimina la política.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar la interfaz de servicio DiffServ

Puede asignar (adjuntar) una política de entrada y una de salida a una interfaz.
Adjuntar políticas DiffServ a una interfaz Para adjuntar políticas DiffServ a una interfaz:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Service Interface Configuration. Se muestra la página Service Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
• Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú Policy In Name, seleccione el nombre de una política para el tráfico de entrada.
9. En el menú Policy Out Name, seleccione el nombre de una política para el tráfico de salida.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 138. Información de Service Interface Configuration

Campo	Descripción
Direction	Dirección del tráfico (In, Out o ambas) de la política o políticas en la interfaz de servicio.
Operational Status	Estado operativo de esta interfaz de servicio (Up o Down). El estado operativo se muestra como Up si se cumplen todas estas condiciones: • La clase adjunta es válida e incluye al menos una regla de coincidencia. • La política adjunta es válida e incluye al menos un atributo. • El puerto está habilitado, es decir, el enlace físico del puerto está activo.

Cambiar una o ambas políticas DiffServ de una interfaz Para cambiar una o ambas políticas DiffServ de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Service Interface Configuration. Se muestra la página Service Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione la casilla de la interfaz.

8. Para seleccionar otra política de entrada, seleccione otro nombre de política en el menú Policy In Name.

9. Para seleccionar otra política de salida, seleccione otro nombre de política en el menú Policy Out Name.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Quitar una o ambas políticas DiffServ de una interfaz Para quitar una o ambas políticas DiffServ de una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Service Interface Configuration. Se muestra la página Service Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

• 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
• LAG: Solo se muestran los LAG.
• All: Se muestran las interfaces físicas y los LAG.

7. Seleccione la casilla de la interfaz.
8. Para quitar la política de entrada, seleccione None en el menú Policy In Name.
9. Para quitar la política de salida, seleccione None en el menú Policy Out Name.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar estadísticas de servicio DiffServ

Puede mostrar información estadística de nivel de servicio de todas las interfaces con políticas DiffServ adjuntas.

Para mostrar estadísticas de servicio DiffServ:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione QoS > DiffServ > Advanced > Service Statistics. Se muestra la página Service Statistics.

6. Use el menú Search para buscar estadísticas DiffServ por interfaz o clase miembro:

• Para buscar por interfaz, seleccione Interface, introduzca la interfaz en formato unidad/ranura/puerto (por ejemplo, 1/0/13) y haga clic en el botón Go.
Si la entrada existe, se muestra como la primera entrada, seguida del resto de las entradas.

• Para buscar por clase miembro, seleccione Member Class, introduzca la clase miembro y haga clic en el botón Go.
Si existe una entrada con esa clase miembro, se muestra como la primera entrada, seguida del resto. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh (Actualizar).
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 139. Información de DiffServ Service Statistics

Campo	Descripción
Interface	Interfaz con una política DiffServ adjunta.
Direction	Dirección (In u Out) en la que se adjunta la política DiffServ.
Policy Name	Nombre de la política DiffServ. Si hay más de una clase adjunta a la política, se muestra cada instancia de política (con el mismo nombre de política).
Operational Status	Estado operativo de la política DiffServ (Up o Down). El estado se muestra como Up si se cumplen todas estas condiciones: • La clase adjunta es válida e incluye al menos una regla de coincidencia. • La política adjunta es válida e incluye al menos un atributo. • El puerto está habilitado, es decir, el enlace físico del puerto está activo.
Member Classes	Todas las clases DiffServ definidas como miembros de la política seleccionada. Seleccione un nombre de clase miembro para ver sus estadísticas. Si no hay ninguna clase asociada a la política seleccionada, la lista está vacía.
Offered Packets	Número total de paquetes ofrecidos a todas las instancias de clase de esta política de servicio antes de aplicar el tratamiento DiffServ definido. Es el total para la interfaz y la dirección.
Discarded Packets	Número total de paquetes descartados por cualquier motivo en todas las instancias de clase de esta política de servicio al aplicar el tratamiento DiffServ. Es el total para la interfaz y la dirección.

7

Administrar la seguridad del switch

Este capítulo trata los siguientes temas:

- Cuentas de usuario y contraseñas
- Servidores RADIUS
- Servidores TACACS+
- Listas de autenticación
- Sesiones de inicio de sesión actuales
- Acceso de administración HTTP y HTTPS
- Acceso de administración SSH
- Acceso de administración Telnet
- Acceso de administración por puerto de consola
- Denegación de servicio
- Perfiles y reglas de acceso de administración
- Autenticación de puertos
- Filtros MAC para control de tráfico
- Seguridad de puertos
- Grupos de puertos privados
- Protección de puertos
- VLAN privadas
- Control de tormentas
- DHCP snooping
- DHCPv6 snooping
- Interfaces de IP source guard
- Interfaces de IPv6 source guard
- Inspección dinámica de ARP
- Portales cautivos
- Listas de control de acceso

Cuentas de usuario y contraseñas

Puede configurar cuentas de usuario y contraseñas de inicio de sesión. De forma predeterminada, existen dos cuentas de usuario:

- admin, con privilegios de lectura y escritura (read/write)
- guest, con privilegios de solo lectura

Los nombres de cuenta no distinguen mayúsculas y minúsculas.

La primera vez que inicia sesión como admin en la interfaz principal, no se requiere contraseña (es decir, la contraseña está en blanco). Después del primer inicio de sesión, debe especificar una contraseña local del dispositivo, que deberá usar para volver a iniciar sesión. En cada inicio de sesión posterior, debe usar la contraseña local del dispositivo.

Un usuario guest no puede iniciar sesión hasta que el usuario admin le asigne una contraseña.

Si inicia sesión como admin con privilegios de lectura/escritura, puede asignar contraseñas, definir parámetros de seguridad de las cuentas predeterminadas y agregar y eliminar cuentas (excepto la cuenta admin), hasta un máximo de seis cuentas. Como admin con privilegios de lectura/escritura, puede modificar todos los datos de las páginas de la interfaz principal.

Agregar o cambiar una cuenta de usuario

Para agregar o cambiar una cuenta de usuario:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security> Management Security > Local User > User Management. Se muestra la página User Management.

6. Si cambia la configuración de una cuenta de usuario existente, seleccione la casilla de esa cuenta.

Si cambia la configuración, no puede cambiar el nombre de usuario.

7. Si agrega una cuenta de usuario nueva, introduzca un nombre en el campo User Name. Solo puede introducir un nombre de usuario al crear una cuenta. Los nombres de usuario tienen hasta 64 caracteres y no distinguen mayúsculas y minúsculas. Se admiten todos los caracteres alfanuméricos, así como el guion (-) y el guion bajo (_). El nombre de usuario default no es válido. Una vez creados, los nombres de usuario no se pueden cambiar ni modificar.

8. En el menú Edit Password, seleccione Enable.
De forma predeterminada, la selección es Disable. Habilite esta opción solo si va a definir o cambiar la contraseña.

9. En el campo Password, introduzca la contraseña de la cuenta.
Los caracteres no se muestran al escribirlos; solo aparecen asteriscos (*). Las contraseñas tienen hasta ocho caracteres alfanuméricos y distinguen mayúsculas y minúsculas.

10. En el campo Confirm Password, vuelva a introducir la contraseña para confirmar que la escribió correctamente.
Este campo no muestra la contraseña al escribirla, sino asteriscos (*).

11. En el menú Access Mode, seleccione Read_Write o Read_Only.
12. Realice una de las siguientes acciones:

- Si agrega una cuenta de usuario nueva, haga clic en el botón Add. Se guarda la configuración y se agrega la cuenta de usuario.
- Si cambia la configuración de una cuenta de usuario, haga clic en el botón Apply. Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 140. Información de administración de usuarios

Campo	Descripción
Lockout Status	Indica si la cuenta de usuario está bloqueada (True o False).
Password Expiration Date	Fecha de vencimiento de la contraseña, si existe.

Eliminar una cuenta de usuario

Puede eliminar una cuenta de usuario que ya no se necesite.

Para eliminar una cuenta de usuario:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security> Management Security > Local User > User Management. Se muestra la página User Management.

6. Seleccione la casilla del usuario.

7. Haga clic en el botón
Delete. Se elimina el usuario.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los requisitos de contraseña de usuario

Para configurar los requisitos de contraseña de usuario:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security> Management Security > Local User > User Password Configuration.

Se muestra la página User Password Configuration.

6. En el campo Password Minimum Length, escriba la longitud mínima de caracteres para cualquier contraseña de usuario local nueva.
El valor predeterminado es ocho caracteres. El rango es de 0 a 64 caracteres.

7. En el campo Password Aging (days), escriba el número máximo de días durante los cuales una contraseña de usuario es válida, contados desde el día en que se define. Cuando una contraseña vence, el usuario debe definir una nueva al iniciar sesión. El valor predeterminado es 0, que significa que las contraseñas no vencen. El rango es de 0 a 365 días.

8. En el campo Password History, escriba el número de contraseñas anteriores que el switch almacena para impedir que los usuarios las reutilicen.
El valor predeterminado es 0, que significa que el switch no almacena contraseñas anteriores. El rango es de 0 a 10 contraseñas.

9. En el campo Lockout Attempts, especifique el número de intentos fallidos de autenticación local permitidos antes de que se bloquee la cuenta del usuario. El valor predeterminado es 5. Si introduce 0, un intento fallido de autenticación local no bloquea la cuenta. El rango es de 0 a 5 intentos.

10. En el campo Unlock Time, especifique el tiempo en minutos tras el cual se desbloquea una cuenta bloqueada.
El valor predeterminado es 5 minutos. El rango es de 1 a 60 minutos.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Cambiar la contraseña EXEC privilegiada de la CLI

Puede cambiar la contraseña EXEC privilegiada para acceder al modo EXEC privilegiado en la interfaz de línea de comandos (CLI). Las contraseñas tienen un máximo de 64 caracteres alfanuméricos y distinguen mayúsculas y minúsculas.

Para cambiar la contraseña EXEC privilegiada para usarla en la CLI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security> Management Security > Enable Password. Se muestra la página Enable Password.

6. En el campo Password, escriba la contraseña.
La contraseña puede tener un máximo de 64 caracteres alfanuméricos.

7. En el campo Confirm Password, vuelva a escribir la contraseña para confirmar que la escribió correctamente.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar la contraseña de consola, Telnet o SSH

Una contraseña de línea es la que se usa para el acceso por consola, Telnet o SSH.

Para configurar la contraseña de consola, Telnet o SSH:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security> Management Security > Line Password. Se muestra la página Line Password.

6. Para cambiar la contraseña de consola, haga lo siguiente: a. En el campo Console Password, escriba la contraseña de consola.

La contraseña puede tener un máximo de 64 caracteres alfanuméricos.

b. En el campo Confirm Console Password, vuelva a escribir la contraseña para confirmar que la escribió correctamente.

7. Para cambiar la contraseña de Telnet, haga lo siguiente: a. En el campo Telnet Password, escriba la contraseña de Telnet.

La contraseña puede tener un máximo de 64 caracteres alfanuméricos.

b. En el campo Confirm Telnet Password, vuelva a escribir la contraseña para confirmar que la escribió correctamente.

8. Para cambiar la contraseña de SSH, haga lo siguiente: a. En el campo SSH Password, escriba la contraseña de SSH.

La contraseña puede tener un máximo de 64 caracteres alfanuméricos.

b. En el campo Confirm SSH Password, vuelva a escribir la contraseña para confirmar que la escribió correctamente.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Servidores RADIUS

Los servidores RADIUS brindan seguridad adicional a las redes. El servidor RADIUS mantiene una base de datos de usuarios con información de autenticación por usuario. El switch envía información al servidor RADIUS configurado, que puede autenticar un nombre de usuario y contraseña antes de autorizar el uso de la red. Los servidores RADIUS ofrecen un método de autenticación centralizado para lo siguiente:

- Acceso web
- Control de acceso de puertos (802.1X)

Configurar los ajustes globales del servidor RADIUS

Puede agregar información sobre uno o más servidores RADIUS de la red.

Si configura varios servidores RADIUS, considere el retardo máximo al especificar el número máximo de retransmisiones (es decir, el valor del campo Max Number of Retransmits en el procedimiento siguiente) y el tiempo de espera (es decir, el valor del campo Timeout Duration en el procedimiento siguiente) para RADIUS:

- Para un servidor RADIUS, no hay retransmisión hasta que expira el tiempo de espera configurado sin respuesta del servidor RADIUS. Además, debe agotarse el número máximo de retransmisiones para un servidor RADIUS antes de que el switch intente con el siguiente servidor RADIUS.
- Por lo tanto, el retardo máximo para recibir una respuesta RADIUS en el switch es igual al número máximo de retransmisiones multiplicado por el tiempo de espera multiplicado por el número de servidores RADIUS configurados. Si la solicitud RADIUS se generó por un intento de inicio de sesión, todas las interfaces de usuario se bloquean hasta que el switch recibe una respuesta RADIUS.

Para configurar los ajustes globales del servidor RADIUS:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Management Security > RADIUS > Global Configuration. Se muestra la página Global Configuration.

   El campo Current Server IP Address está en blanco si no hay servidores configurados (consulte Configurar un servidor de autenticación RADIUS en el switch en la página 503).

   El switch admite hasta tres servidores RADIUS configurados. Si hay más de un servidor RADIUS configurado, el servidor actual es el principal. Si ningún servidor está configurado como principal, el servidor actual es el servidor RADIUS agregado más recientemente.

6. En el menú Source Interface, seleccione la interfaz que debe usar el switch para comunicarse con los servidores RADIUS.

• None: se usa como dirección de origen la dirección IP principal de la interfaz de origen (saliente).
• Routing interface: se usa como dirección de origen la dirección IP principal de un puerto físico.
• Routing VLAN: se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento VLAN.
• Routing loopback interface: se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.
• Service port: se usa como dirección de origen la IP de origen del puerto de administración.

De forma predeterminada, se usa la VLAN 1 como interfaz de origen.

PRECAUCIÓN: El retraso máximo para recibir una respuesta RADIUS en el switch equivale al número máximo de retransmisiones multiplicado por el tiempo de espera multiplicado por el número de servidores RADIUS configurados. Si la solicitud RADIUS se generó por un intento de inicio de sesión, todas las interfaces de usuario se bloquean hasta que el switch reciba una respuesta RADIUS.

7. En el campo Max Number of Retransmits, especifique el número máximo de veces que se retransmite un paquete de solicitud al servidor RADIUS.
El rango es de 1 a 15. El valor predeterminado es 4.

8. En el campo Timeout Duration, especifique el tiempo de espera, en segundos, para las retransmisiones de solicitudes.
El rango es de 1 a 30. El valor predeterminado es 5.

9. Seleccione el botón de opción Accounting Mode Disable o Enable. Esta opción especifica si el modo de contabilidad (accounting) RADIUS está habilitado en el servidor actual. De forma predeterminada, la opción es Disable.

10. Seleccione el botón de opción RADIUS Attribute 4 Mode Disable o Enable. Esta opción especifica si el atributo 4 de RADIUS está habilitado en el servidor actual. De forma predeterminada, la opción es Disable. Si selecciona Enable, aparece el campo RADIUS Attribute 4 Value, que le permite introducir una dirección IPv4 para la opción del atributo 4 de RADIUS.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 141. Información de configuración de RADIUS

Campo	Descripción
Dirección del servidor actual	Dirección del servidor RADIUS actual. Este campo está vacío si no hay servidores configurados.
Número de servidores de autenticación configurados	Número de servidores RADIUS de autenticación configurados. El valor puede ir de 0 a 32.
Número de servidores de contabilidad configurados	Número de servidores RADIUS de contabilidad configurados. El valor puede ir de 0 a 32.
Número de grupos de servidores de autenticación con nombre	Número de grupos con nombre de servidores RADIUS de autenticación configurados.
Número de grupos de servidores de contabilidad con nombre	Número de grupos con nombre de servidores RADIUS de contabilidad configurados.

Configurar un servidor de autenticación RADIUS en el switch

Puede mostrar y configurar diversos ajustes de un servidor RADIUS configurado en el switch.

Agregar un servidor de autenticación RADIUS al switch Para agregar un servidor de autenticación RADIUS al switch y mostrar o restablecer las estadísticas del servidor de autenticación RADIUS:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > RADIUS > Server Configuration. Se muestra la página Server Configuration.

6. En el campo Radius Server IP Address, especifique la dirección IP del servidor RADIUS.
7. En el campo Radius Server Name, especifique un nombre para el servidor RADIUS.

Este nombre le ayuda a identificar el servidor RADIUS.

8. En el campo Port, especifique el número de puerto UDP que usa el servidor para verificar la autenticación del servidor RADIUS.
El rango es de 1 a 65535.

9. En el menú Secret Configured, seleccione Yes.
Debe seleccionar Yes antes de configurar el secreto RADIUS. Después de agregar el servidor RADIUS, este campo indica si se configuró el secreto compartido de este servidor.

10. En el campo Secret, escriba la cadena de texto del secreto compartido que se usa para autenticar y cifrar todas las comunicaciones RADIUS entre el switch y el servidor RADIUS. Este secreto debe coincidir con el configurado en el servidor RADIUS.

11. En el menú Primary Server, seleccione una de las siguientes opciones:

- Yes: el servidor funciona como servidor de autenticación RADIUS principal.
- No: el servidor funciona como servidor de autenticación RADIUS secundario.

12. En el menú Message Authenticator, seleccione Enable o Disable para especificar si el atributo message authenticator del servidor seleccionado está habilitado. El message authenticator agrega protección a los mensajes RADIUS mediante un hash MD5 que cifra cada mensaje. El secreto compartido se usa como clave y, si el servidor RADIUS no puede verificar el mensaje, este se descarta.

13. En el menú Server Type, seleccione una de las siguientes opciones:

- Netgear: un servidor RADIUS específico de NETGEAR.
- Standard: un servidor RADIUS de terceros.

14. Haga clic en el botón Add (Agregar).
El servidor se agrega al switch.

15. Para restablecer el servidor de autenticación y las estadísticas RADIUS a sus valores predeterminados, haga clic en el botón Clear Counters (Borrar contadores).

16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

El campo Current indica si el servidor se está usando actualmente como servidor de autenticación RADIUS.
En la siguiente tabla se describen los campos no configurables de la página.

Tabla 142. Información de estadísticas del servidor de autenticación RADIUS

Campo	Descripción
Servidor RADIUS	Dirección o nombre del servidor RADIUS cuyas estadísticas se muestran.
Tiempo de ida y vuelta	Intervalo de tiempo, en centésimas de segundo, entre el access-reply/ access-challenge más reciente y el access-request correspondiente de este servidor de autenticación RADIUS.
Solicitudes de acceso	Número de paquetes RADIUS access-request enviados a este servidor. Este número no incluye las retransmisiones.
Retransmisiones de acceso	Número de paquetes RADIUS access-request retransmitidos a este servidor.
Accesos aceptados	Número de paquetes RADIUS access-accept, tanto válidos como no válidos, recibidos de este servidor.
Accesos rechazados	Número de paquetes RADIUS access-reject, tanto válidos como no válidos, recibidos de este servidor.
Desafíos de acceso	Número de paquetes RADIUS access-challenge, tanto válidos como no válidos, recibidos de este servidor.
Respuestas de acceso mal formadas	Número de paquetes RADIUS access-response mal formados recibidos de este servidor. Incluyen paquetes con longitud no válida. Los autenticadores o atributos de firma incorrectos o los tipos desconocidos no se incluyen en las respuestas de acceso mal formadas.
Autenticadores incorrectos	Número de paquetes RADIUS access-response con autenticadores o atributos de firma no válidos recibidos de este servidor.
Solicitudes pendientes	Número de paquetes RADIUS access-request destinados a este servidor que aún no han agotado el tiempo de espera ni recibido respuesta.
Tiempos de espera agotados	Número de tiempos de espera agotados de autenticación con este servidor.
Tipos desconocidos	Número de paquetes RADIUS de tipo desconocido recibidos de este servidor en el puerto de autenticación.
Paquetes descartados	Número de paquetes RADIUS recibidos de este servidor en el puerto de autenticación y descartados por algún otro motivo.

Modificar los ajustes de un servidor de autenticación RADIUS en el switch Para modificar los ajustes de un servidor de autenticación RADIUS en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security> RADIUS > Server Configuration. Se muestra la página Server Configuration.

6. Marque la casilla junto a la dirección IP del servidor.
7. Modifique la configuración del servidor seleccionado.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un servidor de autenticación RADIUS del switch Para eliminar un servidor de autenticación RADIUS del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > RADIUS > Server Configuration. Se muestra la página Server Configuration.

6. Marque la casilla junto a la dirección IP del servidor.

7. Haga clic en el botón Delete (Eliminar).
Se elimina el servidor RADIUS.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar un servidor de contabilidad RADIUS

Puede mostrar y configurar diversos ajustes de un servidor de contabilidad RADIUS en la red.

Agregar un servidor de contabilidad RADIUS al switch Para agregar un servidor de contabilidad RADIUS al switch y mostrar o borrar sus estadísticas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > RADIUS > Accounting Server Configuration.
Se muestra la página Accounting Server Configuration.

6. En el campo Accounting Server IP Address, especifique la dirección IP del servidor de contabilidad RADIUS.

7. En el campo Accounting Server Name, introduzca el nombre del servidor de contabilidad.

8. En el campo Port, especifique el número de puerto UDP que usa el servidor para verificar el servidor de contabilidad RADIUS.
El rango es de 1 a 65535.

9. En el menú Secret Configured, seleccione Yes para agregar un secreto RADIUS en el siguiente campo.
Después de agregar el servidor de contabilidad RADIUS, este campo indica si el secreto compartido de este servidor está configurado.

10. En el campo Secret, escriba el secreto compartido que se usará con el servidor de contabilidad especificado.

11. En el menú Accounting Mode, seleccione si desea habilitar o deshabilitar el modo de contabilidad RADIUS:

- Enable: se habilitan todos los servidores de contabilidad RADIUS configurados.
- Disable: se deshabilitan todos los servidores de contabilidad RADIUS configurados.

Nota: La opción que seleccione en el menú Accounting Mode se aplica a todos los servidores de contabilidad configurados, no solo al servidor que está agregando.

12. Haga clic en el botón Add (Agregar).
El servidor se agrega al switch.

13. Para restablecer el servidor de autenticación y las estadísticas RADIUS a sus valores predeterminados, haga clic en el botón Clear Counters (Borrar contadores).

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 143. Información de estadísticas del servidor de contabilidad RADIUS

Campo	Descripción
Servidor de contabilidad	Servidor de contabilidad asociado a las estadísticas.
Tiempo de ida y vuelta	Intervalo de tiempo, en centésimas de segundo, entre el accounting-response más reciente y el accounting-request correspondiente de este servidor de contabilidad RADIUS.
Solicitudes de contabilidad	Número de paquetes RADIUS accounting-request enviados, sin incluir las retransmisiones.
Retransmisiones de contabilidad	Número de paquetes RADIUS accounting-request retransmitidos a este servidor de contabilidad RADIUS.
Respuestas de contabilidad	Número de paquetes RADIUS recibidos en el puerto de contabilidad desde este servidor.
Respuestas de contabilidad mal formadas	Número de paquetes RADIUS accounting-response mal formados recibidos de este servidor. Incluyen paquetes con longitud no válida. Los autenticadores incorrectos y los tipos desconocidos no se incluyen como respuestas de contabilidad mal formadas.
Autenticadores incorrectos	Número de paquetes RADIUS accounting-response con autenticadores no válidos recibidos de este servidor de contabilidad.
Solicitudes pendientes	Número de paquetes RADIUS accounting-request enviados a este servidor que aún no han agotado el tiempo de espera ni recibido respuesta.
Tiempos de espera agotados	Número de tiempos de espera agotados de contabilidad con este servidor.

Tabla 143. Información de estadísticas del servidor de contabilidad RADIUS (continuación)

Campo	Descripción
Tipos desconocidos	Número de paquetes RADIUS de tipo desconocido recibidos de este servidor en el puerto de contabilidad.
Paquetes descartados	Número de paquetes RADIUS recibidos de este servidor en el puerto de contabilidad y descartados por algún otro motivo.

Modificar los ajustes de un servidor de contabilidad RADIUS en el switch Para modificar los ajustes de un servidor de contabilidad RADIUS en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > RADIUS > Accounting Server Configuration.
Se muestra la página Accounting Server Configuration.

6. Marque la casilla junto a la dirección IP del servidor.
7. Modifique la configuración del servidor de contabilidad.

Nota: Si cambia la opción del menú Accounting Mode, los cambios se aplican a todos los servidores de contabilidad configurados, no solo al servidor cuya casilla marcó.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un servidor de contabilidad RADIUS del switch Para eliminar un servidor de contabilidad RADIUS del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > RADIUS > Accounting Server Configuration.
Se muestra la página Accounting Server Configuration.

6. Marque la casilla junto a la dirección IP del servidor.

7. Haga clic en el botón Delete (Eliminar).
Se guarda la configuración. Se elimina el servidor de contabilidad RADIUS.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Servidores TACACS+

TACACS+ ofrece un sistema centralizado de administración de usuarios, manteniendo la coherencia con RADIUS y otros procesos de autenticación. TACACS+ ofrece los siguientes servicios:

- Autenticación: proporciona autenticación durante el inicio de sesión mediante nombres de usuario y contraseñas definidas por el usuario.
- Autorización: se realiza al iniciar sesión. Cuando finaliza la sesión de autenticación, inicia una sesión de autorización con el nombre de usuario autenticado. El servidor TACACS+ verifica los privilegios del usuario.

El protocolo TACACS+ garantiza la seguridad de la red mediante intercambios cifrados entre el dispositivo y el servidor TACACS+.

Configurar los ajustes globales de TACACS+

Puede configurar los ajustes globales de TACACS+ para la comunicación entre el switch y un servidor TACACS+.

Para configurar los ajustes globales de TACACS+:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > TACACS > TACACS+ Configuration. Se muestra la página TACACS+ Configuration.

6. En el campo Key String, especifique la clave de autenticación y cifrado para las comunicaciones TACACS+ entre el switch y el servidor TACACS+. El rango es de 0 a 128. La clave debe coincidir con la configurada en el servidor TACACS+.

7. En el campo Connection Timeout, especifique el número máximo de segundos permitido para establecer una conexión TCP entre el switch y el servidor TACACS+. El rango es de 1 a 30 segundos. El valor predeterminado es 5 segundos.

8. En el menú Source Interface, seleccione la interfaz de origen que debe usarse para la comunicación TACACS+:

- None: se usa como dirección de origen la dirección IP principal de la interfaz de origen (saliente).
- Routing interface: se usa como dirección de origen la dirección IP principal de un puerto físico.
- Routing VLAN: se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento VLAN.
- Routing loopback interface: se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.

• Service port: se usa como dirección de origen la dirección IP de origen del puerto de administración.

De forma predeterminada, se usa la VLAN 1 como interfaz de origen.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Agregar un servidor TACACS+ al switch

Puede agregar hasta cinco servidores TACACS+ con los que el switch puede comunicarse.

Para agregar un servidor TACACS+ al switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security> TACACS > TACACS+ Server Configuration.
Se muestra la página TACACS+ Server Configuration.

6. En el campo TACACS+ Server, introduzca la dirección IP del servidor TACACS+.

7. En el campo Priority, especifique la prioridad del servidor TACACS+. La prioridad determina el orden en que se contacta a los servidores TACACS+ al intentar autenticar a un usuario. El valor 0 es la prioridad más alta. El rango es de 0 a 65535.

8. En el campo Port, especifique el número de puerto de autenticación para las sesiones del servidor TACAS+. El valor debe estar en el rango de 0 a 65535.

9. En el campo Key String, especifique la clave de autenticación y cifrado para las comunicaciones TACACS+ entre el dispositivo y el servidor TACACS+.

La clave puede tener de 0 a 128 caracteres. Debe coincidir con la clave usada en el servidor TACACS+.

10. En el campo Connection Timeout, especifique el tiempo que transcurre antes de que se agote el tiempo de espera de la conexión entre el dispositivo y el servidor TACACS+. El rango es de 1 a 30 segundos.

11. Haga clic en el botón Add (Agregar).
El servidor se agrega al switch.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Modificar los ajustes de un servidor TACACS+ en el switch

Para modificar los ajustes de un servidor TACACS+ en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > TACACS+ > TACACS+ Server Configuration.
Se muestra la página TACACS+ Server Configuration.

6. Marque la casilla junto a la dirección IP del servidor.
7. Modifique la configuración del servidor TACACS+ seleccionado.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un servidor TACACS+ del switch

Para eliminar un servidor TACACS+ del switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > TACACS+ > TACACS+ Server Configuration.
Se muestra la página TACACS+ Server Configuration.

6. Marque la casilla junto a la dirección IP del servidor.

7. Haga clic en el botón Delete (Eliminar).
Se elimina el servidor TACACS+.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Listas de autenticación

Una lista de autenticación de inicio de sesión especifica uno o más métodos de autenticación para validar el acceso al switch o puerto de un usuario admin o guest. El acceso puede ser HTTP o HTTPS a la main UI o AV UI, o acceso de línea (es decir, Telnet, SSH o consola) a la CLI.

Configurar una lista de autenticación de inicio de sesión

Una lista de inicio de sesión especifica los métodos de autenticación que se usan para validar el acceso al switch o puerto. Una lista de autenticación puede aplicarse a usuarios que acceden al switch mediante uno de los siguientes métodos:

- Secure Shell (SSH): para obtener información sobre cómo seleccionar una lista de autenticación para el acceso SSH, consulte Acceso de administración SSH en la página 533.

- Telnet: para obtener información sobre cómo seleccionar una lista de autenticación para el acceso Telnet, consulte Acceso de administración Telnet en la página 539.
- Puerto de consola: para obtener información sobre cómo seleccionar una lista de autenticación para el acceso por puerto de consola, consulte Acceso de administración por puerto de consola en la página 542.

Hay dos listas predeterminadas: defaultList y networkList. No puede eliminarlas. De forma predeterminada, los usuarios preconfigurados (admin y guest) se asignan a ambas listas de la siguiente manera:

- Para el acceso SSH y Telnet, de forma predeterminada, los usuarios preconfigurados se asignan a la defaultList.
- Para el acceso por consola, de forma predeterminada, los usuarios preconfigurados se asignan a la networkList.

Todos los usuarios agregados también se asignan a la defaultList hasta que los asigne expresamente a otra lista (consulte Configurar los ajustes globales de 802.1X en la página 552).

Para configurar una lista de autenticación de inicio de sesión:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > Login Authentication List.
Se muestra la página Login Authentication List.

6. Realice una de las siguientes acciones:

   • Crear una lista nueva: en el campo List Name, especifique un nombre.
   El nombre puede tener hasta 15 caracteres alfanuméricos y no distingue mayúsculas de minúsculas.
   • Modificar una lista existente: marque la casilla asociada a la lista.

7. En el menú de la columna 1, seleccione el método de autenticación que debe usarse primero en la lista de autenticación de inicio de sesión seleccionada.

Si selecciona como primer método uno que no agota el tiempo de espera, como Local, no se intenta ningún otro método, aunque haya especificado más de uno. La autenticación del usuario se realiza en el orden en que seleccione los métodos:

• Local: se usan el nombre y la contraseña del usuario almacenados localmente para la autenticación. Como el método Local no agota el tiempo de espera, si lo selecciona como primer método, no se intenta ningún otro, aunque haya especificado más de uno. Esta es la opción predeterminada para el método 1.
• Enable: se usa la contraseña de EXEC privilegiado para la autenticación.
• Line: se usa la contraseña de línea para la autenticación.
• None: se permite el acceso al usuario sin autenticación.
• Radius: el nombre y la contraseña del usuario se autentican mediante el servidor RADIUS en lugar del servidor local.
• Tacacs: el nombre y la contraseña del usuario se autentican mediante el servidor TACACS en lugar del servidor local.

8. En los menús de las columnas 2, 3, 4, 5 y 6, seleccione los métodos de autenticación, si los hay, que deben usarse en la lista de autenticación de inicio de sesión seleccionada. Si un método anterior agota el tiempo de espera, se usa el siguiente. Por ejemplo, el método que seleccione en la columna 2 se intenta después del método que seleccionó en la columna 1 en el paso anterior. Del mismo modo, el método que seleccione en la columna 3 se intenta después del método que seleccione en la columna 2, y así sucesivamente. Si selecciona un método que no agota el tiempo de espera, no se intenta el siguiente método.

En los menús de las columnas 2, 3, 4, 5 y 6, además de las opciones descritas en el paso anterior, también puede seleccionar N/A. Con la opción N/A (que es la opción predeterminada), no se usa el método de autenticación. Esta opción no está disponible en el menú de la columna 1.

9. Realice una de las siguientes acciones:

• Si va a agregar una lista nueva, haga clic en el botón Add (Agregar). Se guarda la configuración. La lista se agrega a la tabla.
• Si va a cambiar una lista existente, haga clic en el botón Apply (Aplicar). Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una lista de autenticación de inicio de sesión

Puede eliminar una lista de autenticación de inicio de sesión personalizada que ya no necesite. No puede eliminar defaultList ni networkList.

Para eliminar una lista de autenticación de inicio de sesión:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > Login Authentication List.
Se muestra la página Login Authentication List.

6. Marque la casilla asociada a la lista.

7. Haga clic en el botón Delete (Eliminar).
Se guarda la configuración. Se elimina la lista.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una lista de autenticación enable

Una lista enable especifica los métodos de autenticación para validar el acceso EXEC privilegiado en la CLI. Una lista enable se puede aplicar a usuarios que acceden a la CLI del switch mediante uno de los siguientes métodos:

- Secure Shell (SSH): Para obtener información sobre cómo seleccionar una lista enable para el acceso SSH, consulte Acceso de administración SSH en la página 533.
- Telnet: Para obtener información sobre cómo seleccionar una lista enable para el acceso Telnet, consulte Acceso de administración Telnet en la página 539.
- Puerto de consola: Para obtener información sobre cómo seleccionar una lista enable para el puerto de consola, consulte Acceso de administración por puerto de consola en la página 542.

Existen dos listas predeterminadas: enableList y enableNetList. No puede eliminar estas listas.

Los usuarios preconfigurados (admin y guest) se asignan a enableList hasta que seleccione específicamente otra lista.

Todos los usuarios nuevos también se asignan a enableList hasta que seleccione específicamente otra lista.

Para configurar una lista de autenticación enable:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > Enable Authentication List.
Se muestra la página Enable Authentication List.

6. Realice una de las siguientes acciones:

- Crear una lista nueva: en el campo List Name, especifique un nombre.
El nombre puede tener hasta 15 caracteres alfanuméricos y no distingue mayúsculas de minúsculas.
- Modificar una lista existente: marque la casilla asociada a la lista.

7. En el menú de la columna 1, seleccione el método de autenticación que se debe usar primero en la lista de inicio de sesión seleccionada.
Si selecciona como primer método uno que no agota el tiempo, como Local, no se prueba ningún otro método, aunque haya especificado más de uno. La autenticación del usuario se realiza en el orden en que seleccione los métodos:

- Enable: Se usa la contraseña de EXEC privilegiado para la autenticación.
- Line: Se usa la contraseña de línea para la autenticación.
- None: Se permite el acceso al usuario sin autenticación.
- Radius: El nombre y la contraseña del usuario se autentican con el servidor RADIUS en lugar del servidor local.
- Tacacs: El nombre y la contraseña del usuario se autentican con el servidor TACACS en lugar del servidor local.
- Deny: Siempre se niega el acceso al usuario.

8. En los menús de las columnas 2, 3, 4 y 5, seleccione los métodos de autenticación, si los hay, que se deben usar en la lista de inicio de sesión seleccionada.

Si se agota el tiempo de un método anterior, se usa el siguiente. Por ejemplo, el método que seleccione en la columna 2 se prueba después del método que seleccionó en la columna 1 en el paso anterior. Del mismo modo, el método que seleccione en la columna 3 se prueba después del método que seleccione en la columna 2, y así sucesivamente. Si selecciona un método que no agota el tiempo, no se prueba el siguiente método.

En los menús de las columnas 2, 3, 4 y 5, además de las opciones descritas en el paso anterior, también puede seleccionar N/A. Con la opción N/A (selección predeterminada) no se usa el método de autenticación. Esta opción no está disponible en el menú de la columna 1.

9. Realice una de las siguientes acciones:

• Si va a agregar una lista nueva, haga clic en el botón Add (Agregar). Se guarda la configuración. La lista se agrega a la tabla.
• Si va a cambiar una lista existente, haga clic en el botón Apply (Aplicar). Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una lista de autenticación enable

Puede eliminar una lista de autenticación personalizada que ya no necesite. No puede eliminar enableList ni enableNetList.

Para eliminar una lista de autenticación enable:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > Enable Authentication List.
Se muestra la página Enable Authentication List.

6. Marque la casilla asociada a la lista.

7. Haga clic en el botón Delete (Eliminar).
Se guarda la configuración. Se elimina la lista.

Configurar la lista de autenticación Dot1x

Puede configurar la lista de autenticación dot1x, que especifica los métodos de autenticación para validar el acceso a puertos de los usuarios asociados con la lista dot1x. Solo existe una lista dot1x. Para esa lista, solo puede seleccionar un método de acceso. De forma predeterminada, el acceso a los puertos no requiere autenticación, por lo que no existe un método predeterminado.

Para configurar la lista de autenticación dot1x:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > Dot1x Authentication List.
Se muestra la página Dot1x Authentication List.

6. Marque la casilla de la lista dot1x.
7. Seleccione el método de autenticación que se debe usar:

- Ias: Se usan el ID y la contraseña del usuario de la base de datos del servidor de autenticación interno (IAS).
- Local: Se usan el nombre y la contraseña del usuario almacenados localmente.
- None: Se permite el acceso al usuario sin autenticación.
- Radius: El nombre y la contraseña del usuario se autentican con el servidor RADIUS en lugar del servidor local.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar la lista de autenticación HTTP

Puede configurar la lista de autenticación HTTP, que especifica los métodos de autenticación para validar el acceso al switch o a puertos mediante HTTP, por ejemplo, en una sesión de navegador web. Solo existe una lista de autenticación HTTP, que de forma predeterminada usa autenticación local.

Para configurar la lista de autenticación HTTP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > HTTP Authentication List.
Se muestra la página HTTP Authentication List.

6. Marque la casilla de la lista HTTP.

7. En el menú de la columna 1, seleccione el método de autenticación que se debe usar primero en la lista de inicio de sesión seleccionada.
Si selecciona como primer método uno que no agota el tiempo, como Local, no se prueba ningún otro método, aunque haya especificado más de uno. La autenticación del usuario se realiza en el orden en que seleccione los métodos:

- Local: Se usan el nombre y la contraseña del usuario almacenados localmente. Como el método Local no agota el tiempo, si lo selecciona como primer método, no se prueba ningún otro, aunque haya especificado más de uno. Es la selección predeterminada para el método 1.
- None: Se permite el acceso al usuario sin autenticación.
- Radius: El nombre y la contraseña del usuario se autentican con el servidor RADIUS en lugar del servidor local.
- Tacacs: El nombre y la contraseña del usuario se autentican con el servidor TACACS en lugar del servidor local.

8. En los menús de las columnas 2, 3 y 4, seleccione los métodos de autenticación, si los hay, que se deben usar en la lista de inicio de sesión seleccionada. Si se agota el tiempo de un método anterior, se usa el siguiente. Por ejemplo, el método que seleccione en la columna 2 se prueba después del método que seleccionó en la columna 1 en el paso anterior. Del mismo modo, el método que seleccione en la columna 3 se prueba después del método que seleccione en la columna 2, y así sucesivamente. Si selecciona un método que no agota el tiempo, no se prueba el siguiente método.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar la lista de autenticación HTTPS

Puede configurar la lista de autenticación HTTPS, que especifica los métodos de autenticación para validar el acceso al switch o a puertos mediante HTTP seguro (HTTPS), por ejemplo, en una sesión de navegador web. Solo existe una lista de autenticación HTTPS, que de forma predeterminada usa autenticación local.

Para configurar la lista de autenticación HTTPS:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Authentication List > HTTPS Authentication List.
Se muestra la página HTTPS Authentication List.

6. Marque la casilla de la lista HTTPS.

7. En el menú de la columna 1, seleccione el método de autenticación que debe usarse primero en la lista de autenticación de inicio de sesión seleccionada.

Si selecciona como primer método uno que no agota el tiempo de espera, como Local, no se intenta ningún otro método, aunque haya especificado más de uno. La autenticación del usuario se realiza en el orden en que seleccione los métodos:

• Local: Se usan el nombre y la contraseña del usuario almacenados localmente. Como el método Local no agota el tiempo, si lo selecciona como primer método, no se prueba ningún otro, aunque haya especificado más de uno. Es la selección predeterminada para el método 1.
• None: Se permite el acceso al usuario sin autenticación.
• Radius: El nombre y la contraseña del usuario se autentican con el servidor RADIUS en lugar del servidor local.
• Tacacs: El nombre y la contraseña del usuario se autentican con el servidor TACACS en lugar del servidor local.

8. En los menús de las columnas 2, 3 y 4, seleccione los métodos de autenticación, si los hay, que se deben usar en la lista de inicio de sesión seleccionada. Si se agota el tiempo de un método anterior, se usa el siguiente. Por ejemplo, el método que seleccione en la columna 2 se prueba después del método que seleccionó en la columna 1 en el paso anterior. Del mismo modo, el método que seleccione en la columna 3 se prueba después del método que seleccione en la columna 2, y así sucesivamente. Si selecciona un método que no agota el tiempo, no se prueba el siguiente método.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Sesiones de inicio de sesión actuales

Para mostrar las sesiones de inicio de sesión actuales:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Management Security > Login Sessions. Se muestra la página Login Sessions.

La siguiente tabla describe los campos que se muestran en la tabla.

Tabla 144. Login Sessions

Campo	Descripción
ID	Identifica el ID de esta fila.
Nombre de usuario	Nombre del usuario cuya sesión está abierta.
Conexión desde	Equipo desde el que está conectado el usuario.
Tiempo inactivo	Tiempo de inactividad de la sesión.
Tiempo de sesión	Tiempo total de la sesión.
Tipo de sesión	Tipo de sesión: Telnet, Serial, SSH, HTTP o HTTPS.

Acceso de administración HTTP y HTTPS

Puede configurar el acceso HTTP y HTTP seguro (HTTPS) a la interfaz de administración del switch.

Configurar los ajustes de acceso HTTP

Puede configurar los ajustes de acceso HTTP del switch. Si accede a la interfaz del switch, HTTP es el método de acceso predeterminado.

Para configurar los ajustes de acceso HTTP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTP > HTTP Configuration. Se muestra la página HTTP Configuration.

6. Seleccione el botón de opción HTTP Access Disable o Enable:

• Disable: No puede acceder a la interfaz del switch desde una sesión HTTP en un navegador web.
• Enable: Puede acceder a la interfaz del switch desde una sesión HTTP en un navegador web. Es la configuración predeterminada.

7. En el campo HTTP Port, ingrese el número de puerto HTTP.
El rango válido es 80 y de 1025 a 65535. El puerto predeterminado es 80.

8. En el campo HTTP Session Soft Timeout (Minutes), especifique los minutos que una sesión HTTP puede estar inactiva antes de que se agote el tiempo.
El valor debe estar entre 0 y 60 minutos. El valor predeterminado es 5 minutos.

Cuando la sesión está inactiva y se agota el tiempo, se cierra automáticamente la sesión y debe volver a ingresar la contraseña para acceder a la interfaz. Un valor de cero significa que la sesión no expira.

9. En el campo HTTP Session Hard Timeout (Hours), especifique el tiempo de espera absoluto de las sesiones HTTP.
Este tiempo no depende de la actividad de la sesión. El valor debe estar en el rango de 0 a 168 horas. Un valor de cero significa que la sesión no expira. El valor predeterminado es 24 horas.

10. En el campo Maximum Number of HTTP Sessions, especifique el número máximo de sesiones HTTP simultáneas.
El valor debe estar en el rango de 0 a 16. El valor predeterminado es 16.

11. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Authentication List muestra HttpList, la lista predeterminada para el acceso HTTP.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar los ajustes de acceso HTTPS

HTTP seguro (HTTPS) permite transmitir HTTP a través de una conexión cifrada Secure Sockets Layer (SSL) o Transport Layer Security (TLS). Al administrar el switch mediante su interfaz, HTTPS ayuda a proteger la comunicación entre el sistema de administración y el switch contra escuchas y ataques de intermediario (man-in-the-middle).

Para configurar los ajustes de acceso HTTPS:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > HTTPS Configuration. Se muestra la página HTTPS Configuration.

6. Seleccione el botón de opción Admin Mode Disable o Enable:

- Disable: No puede acceder a la interfaz del switch desde una sesión HTTPS en un navegador web.

  Nota: Solo puede descargar certificados SSL cuando HTTPS está deshabilitado.

- Enable: Puede acceder a la interfaz del switch desde una sesión HTTPS en un navegador web. Es la configuración predeterminada.

El campo Operational Status indica si HTTPS está habilitado o deshabilitado operativamente. Por ejemplo, si todos los certificados expiran, HTTPS se deshabilita operativamente.

El campo TLS Version muestra la versión de TLS, que siempre es 1.2.

7. En el campo HTTPS Port, especifique el número de puerto HTTPS. El rango válido es de 1025 a 65535. El puerto predeterminado es 443.

8. En el campo HTTPS Session Soft Timeout (Minutes), especifique los minutos que una sesión HTTPS puede estar inactiva antes de que se agote el tiempo.

El valor debe estar entre 0 y 60 minutos. El valor predeterminado es 5 minutos.

Cuando la sesión está inactiva y se agota el tiempo, se cierra automáticamente la sesión y debe volver a ingresar la contraseña para acceder a la interfaz. Un valor de cero significa que la sesión no expira.

9. En el campo HTTPS Session Hard Timeout (Hours), especifique el tiempo de espera absoluto de las sesiones HTTPS.
Este tiempo no depende de la actividad de la sesión. El valor debe estar en el rango de 0 a 168 horas. Un valor de cero significa que la sesión no expira. El valor predeterminado es 24 horas.

10. En el campo Maximum Number of HTTPS Sessions, especifique el número máximo de sesiones HTTPS simultáneas.
El valor debe estar en el rango de 0 a 16. El valor predeterminado es 16.

11. Haga clic en el botón Apply.
Se guarda la configuración.

El campo TLS Version muestra 1.2, la versión predeterminada del switch.

El campo Authentication List muestra HttpsList, la lista predeterminada para el acceso HTTPS.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Mensaje de seguridad del navegador con acceso HTTPS

Después de habilitar el acceso HTTPS (consulte Configurar los ajustes de acceso HTTP en la página 524), al intentar acceder a la interfaz, el navegador puede mostrar una advertencia de seguridad debido al certificado autofirmado del switch. Es un comportamiento esperado. Puede continuar o agregar una excepción para la advertencia de seguridad.

Para continuar con una advertencia de seguridad o agregar una excepción:

- Google Chrome: Haga clic en el vínculo ADVANCED. Después, haga clic en el vínculo Proceed to x.x.x.x (unsafe), donde x.x.x.x es la dirección IP del switch.
- Apple Safari: Haga clic en el botón Show Details. Después, haga clic en el vínculo visit this website. Si aparece una ventana emergente de advertencia, haga clic en el botón Visit Website. Si aparece otra ventana emergente para confirmar cambios en la configuración de confianza del certificado, ingrese su nombre de usuario y contraseña de Mac y haga clic en el botón Update Setting.
- Mozilla Firefox: Haga clic en el botón ADVANCED. Después, haga clic en el botón Add Exception. En la ventana emergente, haga clic en el botón Confirm Security Exception.
- Microsoft Edge: Seleccione Details > Go on to the webpage.

- Microsoft Internet Explorer: Haga clic en el vínculo Continue to this website (not recommended).

Nota: Para obtener información sobre cómo instalar un certificado de seguridad específico en el switch, consulte Administrar certificados para el acceso HTTPS en la página 528 y Usar una sesión HTTP para descargar e instalar un archivo de certificado de seguridad SSL en el switch en la página 750.

Administrar certificados para el acceso HTTPS

Puede administrar certificados SSL para el acceso HTTPS. El switch admite dos certificados, uno de los cuales puede ser el certificado activo.

Puede generar un certificado en el switch o transferirlo desde un servidor al switch.

Mostrar el estado de los certificados SSL El switch puede contener certificados autogenerados que usted agregó y certificados que transfirió al switch. Para mostrar el estado de los certificados SSL:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > Certificate Management. Se muestra la página Certificate Management.

6. En el menú Certificate Number, seleccione el certificado, es decir, 1 o 2.

   Nota: A un certificado que transfiera (cargue) al switch se le asigna el número 1.

   El campo Certificate Present indica si el certificado seleccionado está presente en el switch.

   El campo Certificate Expire indica si el certificado seleccionado expiró.

La sección Certificate Status muestra lo siguiente para todos los certificados del switch:

- Active Certificate: Los certificados activos del switch. Si HTTPS está deshabilitado, se muestra None. De lo contrario, se muestran los números de certificado.
- Expired Certificate(s): Los certificados expirados del switch.

Generar un certificado SSL Puede generar hasta dos certificados SSL autofirmados para la comunicación HTTPS.

Nota: Antes de generar un certificado, debe deshabilitar HTTPS (consulte Configurar los ajustes de acceso HTTPS en la página 526) y volver a iniciar sesión en la interfaz mediante una sesión HTTP. Después de generar el certificado, puede volver a habilitar HTTPS e iniciar sesión en la interfaz mediante una sesión HTTPS.

Para generar un certificado SSL:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > Certificate Management. Se muestra la página Certificate Management.

6. En el menú Certificate Number, seleccione el certificado, es decir, 1 o 2. Su selección determina si se genera el primer o el segundo certificado.

7. Seleccione el botón de opción Generate Certificates.

8. Haga clic en el botón Apply.
El switch genera un certificado SSL.

El campo Certificate Generation Status indica que el switch está generando un certificado.

9. Haga clic en el botón Refresh.

El campo Certificate Present muestra Yes, lo que indica que el certificado está presente.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Activar un certificado Después de agregar un certificado SSL autogenerado o transferir (cargar) al switch un certificado firmado por una autoridad de certificación (CA) externa, puede activar el certificado.
Para activar un certificado:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > Certificate Management. Se muestra la página Certificate Management.

6. En el menú Certificate Number, seleccione el certificado, es decir, 1 o 2. Su selección determina si se activa el primer o el segundo certificado.

7. Seleccione el botón de opción Activate Certificate.

8. Haga clic en el botón Apply.
Se guarda la configuración y el certificado queda activo.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un certificado SSL

Nota: Antes de eliminar un certificado, debe deshabilitar HTTPS (consulte Configurar los ajustes de acceso HTTPS en la página 526) y volver a iniciar sesión en la interfaz mediante una sesión HTTP. Después de eliminar el certificado, puede volver a habilitar HTTPS e iniciar sesión en la interfaz mediante una sesión HTTPS.

Para eliminar un certificado SSL:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > Certificate Management. El campo Certificate Present muestra Yes.

6. En el menú Certificate Number, seleccione el certificado, es decir, 1 o 2. Su selección determina si se elimina el primer o el segundo certificado.

7. Seleccione el botón de opción Delete Certificates.

8. Haga clic en el botón Apply.
Se elimina el certificado.

Transferir un certificado HTTPS existente de un servidor al switch Puede transferir un archivo de certificado de un servidor seguro al switch. A un certificado que transfiera al switch se le asigna el número 1.

Nota: Para obtener información sobre cómo descargar e instalar un certificado SSL mediante una sesión HTTP, consulte Usar una sesión HTTP para descargar e instalar un archivo de certificado de seguridad SSL en el switch en la página 750.

Para que el switch acepte conexiones HTTPS de un dispositivo, requiere un certificado de clave pública. Puede generar un certificado externamente (por ejemplo, sin conexión) u obtener un certificado firmado por una autoridad de certificación (CA) y transferirlo al switch.

Antes de transferir un archivo de un servidor al switch, se deben cumplir las siguientes condiciones:

- El archivo que transfiere está en el servidor, en el directorio adecuado.
- El archivo tiene el formato correcto.
- El switch tiene una ruta al servidor.

Nota: Antes de transferir un certificado, debe deshabilitar HTTPS (consulte Configurar los ajustes de acceso HTTPS en la página 526) y volver a iniciar sesión en la interfaz mediante una sesión HTTP. Después de transferir el certificado, puede volver a habilitar HTTPS e iniciar sesión en la interfaz mediante una sesión HTTPS.

Para transferir un certificado HTTPS al switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > Certificate Download. Se muestra la página Certificate Update.

6. En el menú File Type, seleccione el tipo de certificado SSL que desea descargar:

• SSL Trusted Root Certificate PEM File: Archivo de certificado raíz de confianza SSL (codificado PEM)
• SSL Server Certificate PEM File: Archivo de certificado de servidor SSL (codificado PEM)
• SSL DH Weak Encryption Parameter PEM File: Archivo de parámetros de cifrado débil Diffie-Hellman SSL (codificado PEM)
• SSL DH Strong Encryption Parameter PEM File: Archivo de parámetros de cifrado fuerte Diffie-Hellman SSL (codificado PEM)

7. En el menú Transfer Mode, seleccione el protocolo que se debe usar para transferir el archivo:

- **TFTP**: Trivial File Transfer Protocol

- **SFTP**: Secure File Transfer Protocol
- **SCP**: Secure Copy Protocol

8. En el menú Server Address Type, seleccione IPv4, IPv6 o DNS para indicar el formato del campo TFTP Server IP.
El valor predeterminado es IPv4.

9. En el campo Server Address, especifique la dirección o el nombre de host del servidor. La dirección puede ser una dirección IP en formato IPv4 o IPv6 estándar o un nombre de host. El nombre de host debe comenzar con una letra.

10. En el campo Remote File Path, ingrese la ruta del archivo que desea descargar. Puede ingresar hasta 96 caracteres. El valor predeterminado es vacío.

11. En el campo Remote File Name, ingrese el nombre del archivo del servidor TFTP que desea descargar.
Puede ingresar hasta 32 caracteres. El valor predeterminado es vacío.

12. Si selecciona SFTP o SCP en el menú Transfer Mode, especifique los siguientes ajustes:

- User Name: Especifique el nombre de usuario para iniciar sesión en el servidor.
- Password: Especifique la contraseña para iniciar sesión en el servidor.

13. Haga clic en el botón Apply. Se inicia la transferencia del archivo.

Se muestra un mensaje de estado durante la transferencia y al completarse correctamente.

Al terminar la transferencia, se asigna el número 1 al certificado.

14. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Acceso de administración SSH

Puede mostrar y modificar los ajustes del servidor Secure Shell (SSH) del switch. SSH es un protocolo de red que permite acceder a la interfaz de administración CLI mediante un cliente SSH en un sistema de administración remoto. SSH es más seguro que Telnet porque cifra la comunicación entre el sistema de administración y el dispositivo. Puede descargar o generar claves de host SSH para la administración segura por CLI.

Configurar los ajustes globales de acceso SSH

Puede configurar los ajustes globales de acceso SSH.

Para configurar los ajustes de SSH:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > SSH > SSH Configuration. Se muestra la página SSH Configuration.

6. Seleccione el botón de opción SSH Admin Mode Disable o Enable. Esta opción habilita o deshabilita el modo administrativo global de SSH. Cuando está habilitado, puede acceder al switch con un cliente SSH en un sistema remoto. El valor predeterminado es Disable.

7. En el campo SSH Session Timeout, especifique el tiempo de espera por inactividad de las sesiones SSH al switch.
Si una sesión SSH está inactiva y se excede el tiempo de espera, la sesión se termina. El rango es de 1 a 160 minutos. El valor predeterminado es 5 minutos.

8. En el campo Maximum Number of SSH Sessions, especifique el número máximo de sesiones SSH que pueden establecerse simultáneamente con el switch.
El rango es de 0 a 5. El valor predeterminado es 5 sesiones.

9. En el menú Authentication List, seleccione una lista de autenticación de inicio de sesión. Esta lista se usa para autenticar a los usuarios que intentan iniciar sesión en el switch. La lista predeterminada es networkList. Para obtener más información sobre las listas de autenticación de inicio de sesión, consulte Configurar una lista de autenticación de inicio de sesión en la página 514.

10. En el menú Enable Authentication List, seleccione una lista de autenticación enable.

Esta lista se usa para autenticar a los usuarios que intentan obtener acceso EXEC privilegiado. La lista predeterminada es enableList. Para obtener más información sobre las listas de autenticación enable, consulte Configurar una lista de autenticación enable en la página 517.

11. En el campo SSH Port, especifique el puerto para el acceso SSH.
El rango es de 1 a 65535. El número de puerto predeterminado es 22.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables que se muestran en la página.

Tabla 145. Información de configuración de SSH

Campo	Descripción
SSH Version	El switch puede aceptar conexiones de un cliente SSH con el nivel de protocolo 2 de SSH (SSH-2). El nivel de protocolo 2 de SSH está habilitado de forma predeterminada.
Current Number of SSH Sessions	El número de sesiones SSH activas entre clientes SSH remotos y el switch.
Keys Present	Muestra si una o ambas (si las hay) de las siguientes claves están presentes en el dispositivo: • Archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (codificado en PEM) • Archivo de clave SSH-2 Digital Signature Algorithm (DSA) (codificado en PEM) Si no hay claves, se muestra No.

Administrar las claves RSA y DSA para el acceso SSH

Puede administrar las claves Rivest-Shamir-Adelman (RSA) y Digital Signature Algorithm (DSA) para el acceso SSH al switch.

Generar una clave RSA o DSA

Nota: Para generar un archivo de clave SSH, SSH debe estar deshabilitado (consulte Configurar los ajustes globales de acceso SSH en la página 534).

Para generar una clave RSA o DSA:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > SSH > Host Keys Management. Se muestra la página Host Keys Management.

El campo Keys Present muestra si hay un certificado en el switch.

6. Realice una de las siguientes acciones:

- Clave RSA: En la sección RSA Keys Management, seleccione el botón de opción Generate RSA Keys.
- Clave DSA: En la sección DSA Keys Management, seleccione el botón de opción Generate DSA Keys.

7. Haga clic en el botón Apply.
El switch genera una clave. El campo Key Generation In Progress muestra información sobre el progreso.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables que se muestran en la página.

Tabla 146. Información de Host Key Status

Campo	Descripción
Keys Present	Muestra cuál de las siguientes claves, o ambas (si las hay), están presentes en el dispositivo: • Archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (codificado en PEM) • Archivo de clave SSH-2 Digital Signature Algorithm (DSA) (codificado en PEM)
Key Generation In Progress	Muestra qué clave se está generando (si la hay): RSA, DSA o None.

Eliminar una clave RSA o DSA

Nota: Para eliminar un archivo de clave SSH, SSH debe estar deshabilitado (consulte Configurar los ajustes globales de acceso SSH en la página 534).

Para eliminar una clave RSA o DSA:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > SSH > Host Keys Management. Se muestra la página Host Keys Management.

El campo Keys Present muestra Yes.

6. Realice una de las siguientes acciones:

• Clave RSA: En la sección RSA Keys Management, seleccione el botón de opción Delete RSA Keys.
• Clave DSA: En la sección DSA Keys Management, seleccione el botón de opción Delete DSA Keys.

7. Haga clic en el botón Apply. Se eliminan las claves.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Transferir claves SSH existentes de un servidor TFTP al switch Puede transferir un archivo de clave SSH-2 RSA o DSA de un switch o una computadora remotos al switch. Antes de transferir un archivo de un servidor TFTP al switch, deben cumplirse las siguientes condiciones:

- El archivo que transfiere desde un servidor TFTP está en el servidor, en el directorio adecuado.
- El archivo tiene el formato correcto.
- El switch contiene una ruta al servidor TFTP.

Nota: Para descargar un archivo de clave SSH al switch, SSH debe estar deshabilitado (consulte Configurar los ajustes globales de acceso SSH en la página 534).

Para transferir claves SSH al switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > SSH > Host Keys Download. Se muestra la página Host Keys Download.

6. En el menú File Type, seleccione el tipo de archivo de clave que desea descargar:

• SSH-2 RSA Key PEM File: Archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (codificado en PEM)
• SSH-2 DSA Key PEM File: Archivo de clave SSH-2 Digital Signature Algorithm (DSA) (codificado en PEM)

7. En el menú Transfer Mode, seleccione el protocolo que se debe usar para transferir el archivo:

- **TFTP**: Trivial File Transfer Protocol
- **SFTP**: Secure File Transfer Protocol
- **SCP**: Secure Copy Protocol

8. En el menú Server Address Type, seleccione IPv4, IPv6 o DNS para indicar el formato del campo TFTP Server IP.
El valor predeterminado es IPv4.

9. En el campo Server IP, especifique la dirección o el nombre de host del servidor. La dirección puede ser una dirección IP en el formato estándar IPv4 o IPv6, o un nombre de host. El nombre de host debe empezar con una letra del alfabeto.

10. En el campo Remote File Path, ingrese la ruta del archivo que desea descargar. Puede ingresar hasta 96 caracteres. El valor predeterminado es vacío.

11. En el campo Remote File Name, ingrese el nombre del archivo del servidor TFTP que desea descargar.

Puede ingresar hasta 32 caracteres. El valor predeterminado es en blanco.

12. Si selecciona SFTP o SCP en el menú Transfer Mode, ingrese el nombre de usuario en el campo Username.
Este es el nombre de usuario con el que accede al servidor SFTP o SCP.

13. Si selecciona SFTP o SCP en el menú Transfer Mode, ingrese la contraseña en el campo Password.
Esta es la contraseña necesaria para acceder al servidor SFTP o SCP.

14. Haga clic en el botón Apply.
Se inicia la transferencia del archivo. Se muestra un mensaje de estado durante la transferencia y al finalizar correctamente la transferencia.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Acceso de administración por Telnet

Puede configurar las listas de autenticación de Telnet y administrar Telnet de salida y de entrada.

Seleccionar las listas de autenticación de Telnet

Puede seleccionar una lista de autenticación de inicio de sesión y una lista de autenticación enable:

- Lista de autenticación de inicio de sesión: La lista de inicio de sesión especifica los métodos de autenticación que se usan para validar el acceso al switch o al puerto de los usuarios asociados con la lista. Para obtener más información, consulte Configurar una lista de autenticación de inicio de sesión en la página 514.
- Lista de autenticación enable: La lista enable especifica los métodos de autenticación que se usan para validar el acceso EXEC privilegiado de los usuarios asociados con la lista. Para obtener más información, consulte Configurar una lista de autenticación enable en la página 517.

Para configurar las listas de autenticación de Telnet:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Access > Telnet. Se muestra la página Telnet.

6. En el menú Authentication List, seleccione qué lista de autenticación de inicio de sesión debe usarse para establecer una sesión Telnet.
El valor predeterminado es networkList.

7. En el menú Enable Authentication List, seleccione qué lista de autenticación enable debe usarse para acceder al modo EXEC privilegiado en una sesión Telnet establecida. El valor predeterminado es enableList.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de Telnet de entrada

Si habilita las sesiones Telnet de entrada y permite que se establezcan nuevas sesiones Telnet, los usuarios autorizados pueden establecer nuevas sesiones Telnet con el switch hasta que se exceda el número máximo de sesiones Telnet. Una sesión Telnet establecida permanece activa hasta que se termina la sesión o se excede el tiempo de espera de la sesión.

Para configurar los ajustes de Telnet de entrada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Telnet. Se muestra la página Telnet.

6. En la sección Inbound Telnet, configure los siguientes ajustes: a.
Seleccione el botón de opción Telnet Server Admin Mode Disable o Enable.

Esta opción especifica si el switch acepta sesiones Telnet de entrada. De forma predeterminada, está seleccionado el botón de opción Enable.

b. Junto a Allow new telnet sessions, seleccione el botón de opción Disable o Enable.

Esta opción especifica si el switch acepta nuevas sesiones Telnet, es decir, nuevas además de una sesión Telnet actual. De forma predeterminada, está seleccionado el botón de opción Enable. Si deshabilita esta opción, una sesión establecida permanece activa hasta que se termina, después de lo cual no se puede establecer ninguna nueva sesión Telnet.

c. En el campo Session Timeout (Minutes), especifique el tiempo en minutos después del cual una sesión Telnet inactiva se termina automáticamente. El rango es de 1 a 160 minutos. El valor predeterminado es 5 minutos.

d. En el campo Maximum Number of Sessions, especifique cuántas sesiones Telnet de entrada simultáneas se permiten. El máximo es 5, que también es el valor predeterminado.

7. Haga clic en el botón Apply.
La configuración se guarda.

El campo Current Number of Sessions de la sección Inbound Telnet muestra el número de sesiones Telnet de entrada actuales.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de Telnet de salida

Si habilita las sesiones Telnet de salida y permite que se establezcan nuevas sesiones Telnet, los usuarios autorizados pueden establecer nuevas sesiones Telnet desde el switch a otro dispositivo hasta que se exceda el número máximo de sesiones Telnet. Una sesión Telnet establecida permanece activa hasta que se termina la sesión o se excede el tiempo de espera de la sesión.

Para configurar los ajustes de Telnet de salida:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Telnet. Se muestra la página Telnet.

6. En la sección Outbound Telnet, configure los siguientes ajustes: a. Junto a Allow new telnet sessions, seleccione el botón de opción Disable o Enable.

Esta opción especifica si el switch permite nuevas sesiones Telnet de salida. De forma predeterminada, está seleccionado el botón de opción Enable. Si deshabilita esta opción, una sesión establecida permanece activa hasta que se termina.

b. En el campo Session Timeout (Minutes), especifique el tiempo en minutos después del cual una sesión Telnet inactiva se termina automáticamente. El rango es de 1 a 160 minutos. El valor predeterminado es 5 minutos.

c. En el campo Maximum Number of Sessions, especifique cuántas sesiones Telnet de salida simultáneas se permiten. El máximo es 5, que también es el valor predeterminado.

7. Haga clic en el botón Apply.
La configuración se guarda.

El campo Current Number of Sessions de la sección Outbound Telnet muestra el número de sesiones Telnet de salida actuales.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Acceso de administración por el puerto de consola

Puede configurar los ajustes de una conexión por puerto serie (puerto de consola) al switch.

Para configurar los ajustes del puerto de consola:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Console Port. Se muestra la página Console Port.

6. En el campo Serial Port Login Timeout (minutes), especifique el tiempo en minutos después del cual una conexión inactiva del puerto de consola se termina automáticamente. El rango es de 1 a 160 minutos. El valor predeterminado es 5 minutos. Ingresar 0 deshabilita el tiempo de espera.

7. En el menú Baud Rate (bps), seleccione la velocidad en baudios predeterminada para la conexión del puerto de consola.
Puede elegir entre 1200, 2400, 4800, 9600, 19200, 38400, 57600 y 115200 baudios. El valor predeterminado es 115200 baudios.

8. En el menú Authentication List, seleccione una lista de autenticación de inicio de sesión. Esta lista se usa para autenticar a los usuarios que intentan iniciar sesión en el switch. El valor predeterminado es defaultList. Para obtener más información sobre las listas de autenticación de inicio de sesión, consulte Configurar una lista de autenticación de inicio de sesión en la página 514.

9. En el menú Enable Authentication List, seleccione una lista de autenticación enable. Esta lista se usa para autenticar a los usuarios que intentan obtener acceso EXEC privilegiado. La lista predeterminada es enableList. Para obtener más información sobre las listas de autenticación enable, consulte Configurar una lista de autenticación enable en la página 517.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe la información no configurable que se muestra.

Tabla 147. Información del puerto de consola

Campo	Descripción
Character Size (bits)	El número de bits de un carácter. Este ajuste siempre es 8.
Flow Control	Muestra si el control de flujo por hardware está habilitado o deshabilitado. Este ajuste siempre está deshabilitado.
Stop Bits	El número de bits de parada por carácter. Este ajuste siempre es 1.
Parity	El método de paridad que se usa en el puerto de consola. Este ajuste siempre es None.

Denegación de servicio

Puede seleccionar qué tipos de ataques de denegación de servicio (DoS) supervisa y bloquea el switch.

Para configurar los ajustes de DoS individuales:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Access > Denial of Service Configuration.
Se muestra la página Denial of Service Configuration.

6. Seleccione los tipos de ataques DoS que el switch debe supervisar y bloquear, y configure los valores asociados:

   • Denial of Service Min TCP Header Size: Especifique el tamaño mínimo de encabezado TCP permitido. Si selecciona el botón de opción Denial of Service TCP Fragment, el switch descarta el primer fragmento TCP con un paquete de carga útil TCP cuyo tamaño mínimo de encabezado TCP es mayor que la longitud de la carga útil IP menos el tamaño del encabezado IP. El rango del tamaño mínimo de encabezado TCP es de 0 a 255. El valor predeterminado es 20.

• Denial of Service ICMPv4: Al habilitar la prevención de DoS ICMPv4, el switch descarta los paquetes ICMPv4 con el tipo ECHO_REQ (ping) y un tamaño mayor que el tamaño de paquete ICMPv4 configurado. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service Max ICMPv4 Packet Size: Especifique el tamaño máximo de paquete ICMPv4 permitido. Si la prevención de DoS ICMPv4 está habilitada, el switch descarta los paquetes ping ICMPv4 con un tamaño mayor que el valor configurado. El rango es de 0 a 16376. El valor predeterminado es 512.
• Denial of Service ICMPv6: Al habilitar la prevención de DoS ICMPv6, el switch descarta los paquetes ICMPv6 con el tipo ECHO_REQ (ping) y un tamaño mayor que el tamaño de paquete ICMPv6 configurado. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service Max ICMPv6 Packet Size: Especifique el tamaño máximo de paquete ICMPv6 permitido. Si la prevención de DoS ICMPv6 está habilitada, el switch descarta los paquetes ping ICMPv6 con un tamaño mayor que el valor configurado. El rango es de 0 a 16376. El valor predeterminado es 512.
• Denial of Service First Fragment: Al habilitar la prevención de DoS del primer fragmento, el switch verifica las opciones de DoS en el primer fragmento de un paquete IP fragmentado. De lo contrario, el switch ignora el primer fragmento de un paquete IP fragmentado. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service ICMP Fragment: Al habilitar la prevención de DoS de fragmentos ICMP, el switch descarta los paquetes ICMP fragmentados. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service SIP=DIP: Al habilitar la prevención de DoS SIP=DIP, el switch descarta los paquetes cuya dirección IP de origen es igual a la dirección IP de destino. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service SMAC=DMAC: Al habilitar la prevención de DoS SMAC=DMAC, el switch descarta los paquetes cuya dirección MAC de origen es igual a la dirección MAC de destino. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service TCP FIN&URG&PSH: Al habilitar la prevención de DoS TCP FIN & URG & PSH, el switch descarta los paquetes con los indicadores TCP FIN, URG y PSH activados y el número de secuencia TCP igual a 0. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service TCP Flag&Sequence: Al habilitar la prevención de DoS de indicadores TCP, el switch descarta los paquetes con los indicadores de control TCP en 0 y el número de secuencia TCP en 0. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service TCP Fragment: Al habilitar la prevención de DoS de fragmentos TCP, el switch descarta los paquetes con una carga útil TCP cuya longitud de carga útil IP menos el tamaño del encabezado IP es menor que el tamaño mínimo de encabezado TCP permitido. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service TCP Offset: Al habilitar la prevención de DoS TCP Offset, el switch descarta los paquetes con un desplazamiento de encabezado TCP igual a 1. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service TCP Port: Al habilitar la prevención de DoS de puerto TCP, el switch descarta los paquetes cuyo puerto TCP de origen es igual al puerto TCP de destino. De forma predeterminada, esta opción está deshabilitada.

• Denial of Service TCP SYN: Al habilitar la prevención de DoS TCP SYN, el switch descarta los paquetes con el indicador TCP SYN activado. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service TCP SYN&FIN: Al habilitar la prevención de DoS TCP SYN & FIN, el switch descarta los paquetes con los indicadores TCP SYN y FIN activados. De forma predeterminada, esta opción está deshabilitada.
• Denial of Service UDP Port: Al habilitar la prevención de DoS de puerto UDP, el switch descarta los paquetes cuyo puerto UDP de origen es igual al puerto UDP de destino. De forma predeterminada, esta opción está deshabilitada.
• Stacked VLAN0 tag drop mode: Al habilitar el modo de descarte de etiquetas para la VLAN 0 apilada, el switch reenvía o descarta los paquetes etiquetados con VLAN 0 y reenvía o descarta los paquetes SNAP. (SNAP significa Stateful Network-Wide Abstractions for Packet Processing). De forma predeterminada, esta opción está deshabilitada.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Perfiles y reglas de acceso de administración

El control de acceso le permite configurar un perfil de control de acceso y establecer reglas para el acceso a la UI del dispositivo, el acceso de estaciones SNMP y el acceso de clientes a un servidor TFTP. Nos referimos a un perfil de control de acceso como perfil de acceso. Puede agregar un solo perfil de acceso, que puede configurar, activar o desactivar.

PRECAUCIÓN: Si configura incorrectamente un perfil de acceso de seguridad y activa el perfil de acceso, es posible que ya no pueda acceder a la UI del dispositivo del switch. Si esto ocurre, debe restablecer el switch a la configuración predeterminada de fábrica (consulte Restablecer el switch a la configuración predeterminada de fábrica en la página 738).

Agregar un perfil de acceso

Puede configurar un solo perfil de acceso de seguridad con el que puede asociar una configuración de reglas de acceso.

Para agregar un perfil de acceso:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Access Control > Access Profile Configuration. Se muestra la página Access Profile Configuration.

6. En el campo Access Profile Name, ingrese el nombre del perfil de acceso que desea agregar. La longitud máxima es de 32 caracteres.

7. Haga clic en el botón Apply.
La configuración se guarda. De forma predeterminada, el perfil de acceso está desactivado. Después de agregar reglas, puede activar el perfil de acceso.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Agregar una regla al perfil de acceso

Después de agregar el perfil de acceso, puede agregar una o más reglas de acceso de seguridad al perfil de acceso.

Si accede al switch desde una computadora, asegúrese de agregar una regla de permiso para el tipo de servicio que usa (por ejemplo, HTTPS), la dirección IP de su computadora y la máscara de subred de su computadora.

PRECAUCIÓN: Debe agregar una regla de permiso para su dispositivo y método de acceso; de lo contrario, quedará bloqueado del switch después de activar el perfil de acceso. Si esto ocurre, debe restablecer el switch a la configuración predeterminada de fábrica (consulte Restablecer el switch a la configuración predeterminada de fábrica en la página 738).

Para agregar una regla al perfil de acceso:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Access > Access Control > Access Rule Configuration. Se muestra la página Access Rule Configuration.

6. En el menú Rule Type, seleccione Permit o Deny para permitir o denegar el acceso cuando se cumplan las reglas seleccionadas.
Una regla Permit permite el acceso desde un dispositivo que cumple los criterios de la regla. Una regla Deny bloquea un dispositivo que cumple los criterios de la regla.

7. En el menú Service Type, seleccione el método de acceso al que se aplica la regla. A menos que permita cualquier método de acceso, la política se restringe al método de acceso seleccionado. Los métodos de acceso posibles son Any, TELNET, TFTP, HTTP, Secure HTTP (SSL), SNMP, Secure Telnet (SSH) y SNTP.

8. En el campo Source IP Address, ingrese la dirección IP de origen desde la que se origina el tráfico de administración.

9. En el campo Mask, especifique la máscara de subred desde la que se origina el tráfico de administración.

10. En el campo Priority, asigne una prioridad a la regla.
Las reglas se validan contra la solicitud de administración entrante en orden ascendente de sus prioridades. Si una regla coincide, se realiza la acción y se ignoran las reglas posteriores. Por ejemplo, si una dirección IP de origen 10.10.10.10 se configura con prioridad 1 para permitir, y la misma dirección IP de origen 10.10.10.10 también se configura con prioridad 2 para denegar, el acceso se permite si el perfil está activo, y la segunda regla se ignora.

11. Haga clic en el botón Add.
Se agrega la regla de acceso.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Activar el perfil de acceso

Después de agregar reglas al perfil de acceso, puede activar el perfil de acceso.

PRECAUCIÓN: Si configura incorrectamente un perfil de acceso de seguridad y activa el perfil de acceso, es posible que ya no pueda acceder a la UI del dispositivo del switch. Si esto ocurre, debe restablecer el switch a la configuración predeterminada de fábrica (consulte Restablecer el switch a la configuración predeterminada de fábrica en la página 738).

Para activar el perfil de acceso:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Access Control > Access Profile Configuration. Se muestra la página Access Profile Configuration. La casilla Deactivate Profile está marcada.

6. Marque la casilla Activate Profile.

7. Haga clic en el botón Apply.
La configuración se guarda y el perfil de acceso queda activo.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar el resumen del perfil de acceso y el número de paquetes filtrados

Después de agregar reglas al perfil activo, puede mostrar las entradas en el resumen. Si el perfil de acceso está activo, también puede mostrar el número de paquetes filtrados.

Para mostrar el resumen del perfil de acceso y el número de paquetes filtrados:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Access > Access Control > Access Profile Configuration. Se muestra la página Access Profile Configuration.

El campo Packets Filtered muestra el número de paquetes filtrados.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh).
La siguiente tabla describe los datos no configurables que se muestran.

Tabla 148. Resumen de la configuración del perfil de acceso

Campo	Descripción
Rule Type	La acción que se realiza cuando coinciden las reglas.
Service Type	El tipo de servicio seleccionado. La política se restringe al tipo de servicio seleccionado.
Source IP Address	La dirección IP de origen del cliente que origina el tráfico de administración.
Mask	La máscara de subred de la dirección IP.
Priority	La prioridad de la regla.

Desactivar un perfil de acceso

Puede desactivar un perfil de acceso.

Para desactivar un perfil de acceso:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Access Control > Access Profile Configuration. Se muestra la página Access Profile Configuration. La casilla Activate Profile está activada.

6. Active la casilla Deactivate Profile.

7. Haga clic en el botón Aplicar (Apply).
Se guarda la configuración y el perfil de acceso queda desactivado.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un perfil de acceso

Puede eliminar un perfil de acceso que ya no necesite. Antes de eliminar el perfil de acceso, debe desactivarlo (consulte Desactivar un perfil de acceso en la página 550).

Para eliminar un perfil de acceso:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > Access Control > Access Profile Configuration. Se muestra la página Access Profile Configuration. La casilla Deactivate Profile está marcada.

6. Active la casilla Remove Profile.

7. Haga clic en el botón Aplicar
(Apply). Se elimina el perfil de acceso.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Autenticación de puertos

Con la autenticación basada en puerto, cuando 802.1X está habilitado globalmente y en el puerto, la autenticación correcta de cualquier solicitante conectado al puerto permite que todos los usuarios usen el puerto sin restricciones. En este modo, solo se permite que un solicitante a la vez intente autenticarse en un puerto. Los puertos en este modo tienen control bidireccional. 802.1X es el modo de autenticación predeterminado. 802.1X también se conoce como dot1x.

Nota: En la autenticación de puertos, cuando hablamos de un puerto, nos referimos a una interfaz física.

Una red 802.1X incluye tres componentes:

- Autenticador: El puerto que se autentica antes de permitir el acceso a los servicios del sistema.
- Solicitante: El host conectado al puerto autenticado que solicita acceso a los servicios del sistema.
- Servidor de autenticación: El servidor externo, por ejemplo, el servidor RADIUS, que realiza la autenticación en nombre del autenticador e indica si el solicitante está autorizado para acceder a los servicios del sistema.

Configurar los ajustes globales de 802.1X

Puede habilitar 802.X en el switch y configurar los ajustes globales de 802.1X que se aplican al switch y a usuarios específicos.

Si habilita 802.1X, la autenticación debe realizarla un servidor RADIUS:

- Servidor RADIUS: Configure un servidor RADIUS (consulte Servidores RADIUS en la página 500).
- Método de autenticación principal: Establezca RADIUS como método de autenticación principal; es decir, RADIUS debe ser el método 1 del ajuste defaultList de la lista de autenticación de inicio de sesión (consulte Configurar una lista de autenticación de inicio de sesión en la página 514).

Para configurar los ajustes globales de 802.1X:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Port Authentication > Basic > 802.1X Configuration. Se muestra la página 802.1X Configuration.

6. Seleccione el botón de opción Disable o Enable de Dot1x Admin Mode:

- Enabled: La autenticación 802.1X basada en puerto está habilitada globalmente en el switch.
- Disabled: La autenticación 802.1X basada en puerto está deshabilitada globalmente en el switch. Esta es la configuración predeterminada. El switch no comprueba la autenticación 802.1X antes de permitir el tráfico en ningún puerto, aunque algunos puertos estén configurados para permitir solo usuarios autenticados.

7. Seleccione el botón de opción Disable o Enable de Authentication Admin Mode:

- Enabled: El modo de administración de autenticación está habilitado y requiere que la autenticación la realice un servidor RADIUS. Esto significa que el método de autenticación principal debe ser RADIUS. Para establecer el método, seleccione Security > Management Security > Authentication List > Authentication List y seleccione Radius como método 1 de defaultList. Para más información, consulte Configurar una lista de autenticación de inicio de sesión en la página 514.
- Disabled: El modo de administración de autenticación está deshabilitado (configuración predeterminada). El switch no comprueba la autenticación 802.1X antes de permitir el tráfico en ningún puerto, aunque la autenticación 802.1X basada en puerto esté habilitada globalmente (consulte el paso anterior) y los puertos estén configurados para permitir solo usuarios autenticados.

8. Seleccione el botón de opción Disable o Enable de VLAN Assignment Mode. Si está habilitada, esta función permite colocar un puerto en una VLAN específica según el resultado de la autenticación o el tipo de autenticación 802.1X que usa un cliente al acceder al dispositivo. El servidor de autenticación puede indicar al dispositivo qué VLAN asignar al solicitante. El valor predeterminado es Disable.

9. Seleccione el botón de opción Disable o Enable de EAPOL Flood Mode. Esta selección especifica si la inundación de Extensible Authentication Protocol (EAP) over LAN (EAPoL) está habilitada en el switch. El valor predeterminado es Disable.

10. En el menú Dynamic VLAN Creation Mode, seleccione Disable o Enable. Si las VLAN asignadas por RADIUS están habilitadas, el servidor RADIUS incluye el ID de VLAN en los atributos de túnel 802.1X de su mensaje de respuesta al dispositivo. Si la creación dinámica de VLAN está habilitada en el dispositivo y la VLAN asignada por RADIUS no existe,

la VLAN asignada se crea dinámicamente. Esto significa que el cliente puede conectarse desde cualquier puerto y se asigna a la VLAN adecuada. Esta función da flexibilidad a los clientes para moverse por la red sin requerir mucha configuración adicional. El valor predeterminado es Disable.

11. En el menú Monitor Mode, seleccione Disable o Enable.
Si está habilitada, esta opción permite que el switch supervise el proceso de autenticación dot1x y puede ayudarle a diagnosticar fallas de autenticación, si ocurren. El valor predeterminado es Disable.

12. En el menú Users, seleccione el nombre de usuario al que debe aplicarse la lista de inicio de sesión que seleccionará en el paso siguiente.

13. En el menú Login, seleccione la lista de inicio de sesión que se aplica al nombre de usuario seleccionado en el paso anterior.
Si 802.1X está habilitado, se aplica la lista dot1xList predeterminada para la autenticación, como se muestra en el campo Authentication List.

El campo Software Version siempre muestra 0.

14. Haga clic en el botón Apply
(Aplicar). Se guarda la configuración.

15. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Administrar la autenticación en puertos individuales

Puede habilitar y configurar el control de acceso a puertos en uno o más puertos físicos.

Configurar los ajustes 802.1X de un puerto Puede configurar los ajustes de control de acceso a puertos 802.1X de uno o más puertos.
Para configurar los ajustes 802.1X de un puerto:

1. Abra un navegador web.

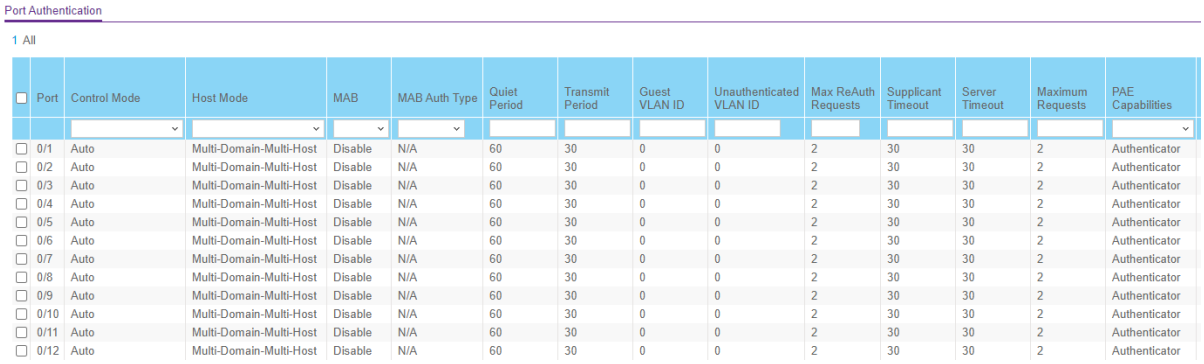
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Port Authentication > Advanced > Port Authentication.



Port	Control Mode	Host Mode	MAB	MAB Auth Type	Quiet Period	Transmit Period	Guest VLAN ID	Unauthenticated VLAN ID	Max ReAuth Requests	Supplicant Timeout	Server Timeout	Maximum Requests	PAE Capabilities
0/1	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/2	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/3	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/4	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/5	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/6	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/7	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/8	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/9	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/10	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/11	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator
0/12	Auto	Multi-Domain-Multi-Host	Disable	N/A	60	30	0	0	2	30	30	2	Authenticator

La figura anterior muestra solo una parte de la página.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

7. En el menú Control Mode, seleccione una opción:

- Auto: La entidad de acceso a puerto (PAE) del autenticador establece el modo del puerto controlado según el resultado de los intercambios de autenticación entre el solicitante, el autenticador y el servidor de autenticación. Esta es la configuración predeterminada.
- Force Authorized: La PAE del autenticador establece incondicionalmente el puerto controlado como autorizado.
- Force Unauthorized: La PAE del autenticador establece incondicionalmente el puerto controlado como no autorizado.

8. En el menú Host Mode, seleccione una opción para especificar el número y el tipo de clientes que pueden autenticarse y autorizarse en el puerto:

- Single-Host: Solo un cliente de datos puede autenticarse en el puerto. Tras una autenticación correcta, se concede acceso solo a este cliente y no a otros clientes. Solo cuando este cliente cierra sesión, otro cliente puede autenticarse, autorizarse en el puerto y obtener acceso.
- Multi-Host: Inicialmente, solo un cliente de datos puede autenticarse en el puerto. Tras una autenticación correcta, se concede acceso a todos los clientes conectados al puerto. Por ejemplo, use esta opción cuando un punto de acceso WiFi esté conectado a un puerto con control de acceso de un NAS. Después de que el NAS autentica el punto de acceso, el puerto queda autorizado para el tráfico no solo del punto de acceso, sino también de todos los clientes WiFi conectados a él.

• Multi-Domain: Un cliente de datos y un cliente de voz pueden autenticarse en el puerto. Tras una autenticación correcta, se concede acceso a ambos clientes. Por ejemplo, use esta opción cuando un teléfono IP esté conectado a un puerto del NAS y una laptop esté conectada al puerto hub del teléfono IP. Ambos dispositivos deben autenticarse para acceder a los servicios de red detrás del NAS. Los dominios de voz y datos están separados. (El atributo del servidor RADIUS Cisco-AVPair = device-traffic-class=voice se usa para identificar un cliente de voz).
• Multi-Auth: Un cliente de voz y varios clientes de datos pueden autenticarse en el puerto. Tras una autenticación correcta, se concede acceso a todos los clientes. Por ejemplo, use esta opción cuando una red de laptops y un teléfono IP estén conectados a un puerto del NAS mediante un hub.
• Multi-Domain-Multi-Host: Inicialmente, un cliente de voz y un cliente de datos pueden autenticarse en el puerto. Una vez autenticado el cliente de datos, se concede acceso a todos los clientes conectados al puerto, que se consideran clientes de datos. Por ejemplo, use esta opción cuando un teléfono IP esté conectado a un puerto del NAS y un controlador de máquinas virtuales (VM) esté conectado al puerto hub del teléfono IP. El controlador aloja varias VM. Tanto el controlador de VM como el teléfono IP deben autenticarse para acceder a los servicios de red detrás del NAS. Los dominios de voz y datos están separados. Una vez autenticado el controlador de VM, se permite el tráfico de todas las VM que aloja. Tenga en cuenta que si el cliente de datos se autentica primero, el cliente de voz solo puede autenticarse mediante 802.1x.

9. En el menú MAB, habilite o deshabilite la omisión de autenticación basada en MAC (MAB) para clientes que no admiten 802.1x.
MAB solo funciona si el modo de control del puerto es MAC-based. La selección predeterminada es Disable.

10. En el menú MAB Auth Type, seleccione una opción de autenticación MAB:

• EAP-MD5: El hash MD5 de la dirección MAC se envía como contraseña en el mensaje EAP (atributo RADIUS 79) al servidor de autenticación.
• PAP: La dirección MAC del cliente se envía como contraseña, con un formato similar al del atributo 1, en texto sin cifrar como parte del mensaje User-Password (atributo RADIUS 2).
• CHAP: Se envía un desafío de 16 octetos generado aleatoriamente como mensaje CHAP-Challenge (atributo RADIUS 60) junto con el mensaje CHAP-Password (atributo RADIUS 3). El CHAP ID es un número único que identifica la sesión. La dirección MAC del cliente se obtiene y se formatea con el formato configurado del atributo 1. Luego, esta información se usa como secreto para derivar la información del mensaje CHAP-Password. La información del mensaje CHAP-Password se calcula como MD5 (con el CHAP-ID, el secreto y el CHAP-Challenge).

11. En el campo Quiet Period, introduzca el periodo en segundos durante el cual la interfaz no intenta adquirir un solicitante después de que falló un intercambio de autenticación anterior.
Introduzca un valor de 0 a 65535. Un periodo de 0 significa que la interfaz no adquiere ningún solicitante. El valor predeterminado es 60 segundos.

12. En el campo Transmit Period, introduzca el periodo en segundos tras el cual la interfaz envía una trama EAPOL EAP Request/Identity al solicitante. Introduzca un valor de 0 a 65535. El valor predeterminado es 30 segundos.

13. En el campo GuestVLAN ID, introduzca el ID de la VLAN de invitados. Introduzca un valor de 0 a 4093. El valor predeterminado es 0.

14. En el campo Unauthenticated VLAN ID, introduzca el ID de la VLAN no autenticada.
El usuario tiene tres intentos para introducir las credenciales correctas. De lo contrario, el cliente se coloca en la VLAN no autenticada. Introduzca un valor de 0 a 4093. El valor predeterminado es 0.

15. En el campo Max ReAuth Requests, introduzca el número máximo de solicitudes de reautenticación permitidas.
Introduzca un valor de 1 a 20. El valor predeterminado es 2.

16. En el campo Supplicant Timeout, introduzca el periodo en segundos tras el cual la interfaz agota el tiempo de espera del solicitante.
Introduzca un valor de 0 a 65535. El valor predeterminado es 30 segundos.

17. En el campo Server Timeout, introduzca el periodo tras el cual la interfaz agota el tiempo de espera del servidor de autenticación.
Introduzca un valor de 0 a 65535. El valor predeterminado es 30 segundos.

18. En el campo Maximum Requests, introduzca el número máximo de veces que la interfaz envía una solicitud EAPOL EAP request/identity al solicitante antes de agotar el tiempo de espera.
Introduzca un valor de 1 a 10. El valor predeterminado es 2.

19. En el menú PAE Capabilities, seleccione Authenticator o Supplicant para especificar la función de la entidad de acceso a puerto (PAE).
El valor predeterminado es Authenticator.

20. En el menú Periodic Reauthentication, habilite o deshabilite la reautenticación periódica del solicitante.
El valor predeterminado es Disable.

21. Si habilita la reautenticación periódica, en el campo Reauthentication Period, introduzca el periodo en segundos tras el cual el solicitante debe reautenticarse. Introduzca un valor de 0 a 65535. El valor predeterminado es 3600 segundos.

22. En el menú User Privileges, seleccione admin o guest para limitar el tipo de usuarios a los que se puede conceder acceso.
De forma predeterminada, se puede conceder acceso tanto a usuarios admin como guest.

23. En el campo Max Users, introduzca el número máximo de solicitantes que la interfaz puede admitir.
El valor predeterminado es 48.

24. En las columnas Authentication Order, introduzca el orden en que debe realizarse la autenticación, con hasta tres métodos:

- Method 1: La selección predeterminada es DOT1X. Las otras opciones son MAB y CAPTIVE PORTAL. No puede deshabilitar Method 1.
- Method 2: La selección predeterminada es MAB. Las otras opciones son None, DOT1X y CAPTIVE PORTAL. Para deshabilitar Method 2, seleccione None.
- Method 3: La selección predeterminada es CAPTIVE PORTAL. Las otras opciones son None, DOT1X y MAB. Para deshabilitar Method 3, seleccione None.

Por ejemplo, si un cliente intenta la autenticación 802.1X (según las credenciales del usuario y del cliente) y falla, la interfaz continúa con la autenticación MAB. Si ese método también falla, la interfaz continúa con la autenticación por portal cautivo. Si ese método también falla, el cliente no puede autenticarse.

25. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

26. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Inicializar 802.1X en un puerto Solo puede inicializar un puerto si el modo de control es Auto. Esta es la configuración predeterminada, en la que la entidad de acceso a puerto (PAE) del autenticador establece el modo del puerto controlado según el resultado de los intercambios de autenticación entre el solicitante, el autenticador y el servidor de autenticación. Para inicializar 802.1X en un puerto:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Port Authentication > Advanced > Port Authentication. Se muestra la página Port Authentication.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

7. Haga clic en el botón Initialize.
802.1X en el puerto seleccionado se restablece al estado de inicialización. El tráfico hacia y desde el puerto se bloquea durante el proceso de autenticación. Este botón solo está disponible si el modo de control es auto. Al hacer clic en este botón, la acción es inmediata. No necesita hacer clic en el botón Aplicar (Apply) para que se realice.

Mostrar el resumen de puertos

Puede mostrar información resumida sobre la configuración de autenticación basada en puerto de cada puerto.

Para mostrar el resumen de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Port Authentication > Advanced > Port Summary. Se muestra la página Port Summary.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 149. Información del resumen de puertos

Campo	Descripción
Port	El puerto cuya configuración se muestra.
Control Mode	El modo de control configurado para el puerto: • Force Unauthorized: La entidad de acceso a puerto (PAE) del autenticador establece incondicionalmente el puerto controlado como no autorizado. • Force Authorized: La PAE del autenticador establece incondicionalmente el puerto controlado como autorizado. • Auto: La PAE del autenticador establece el modo del puerto controlado según el resultado de los intercambios de autenticación entre el solicitante, el autenticador y el servidor de autenticación.
Operating Control Mode	El modo de control en el que opera realmente el puerto. Las opciones son las siguientes: • ForceUnauthorized • ForceAuthorized • Auto • MAC Based • N/A: Si el puerto está desconectado, el valor es N/A porque el puerto no puede participar en el control de acceso a puertos.
Reauthentication Enabled	Indica si se permite la reautenticación del solicitante. Si el valor es True, se permite la reautenticación. De lo contrario, no se permite.
Control Direction	La dirección de control, que determina en qué medida se producen intercambios de protocolo entre un solicitante y el autenticador. La dirección determina si el puerto controlado no autorizado controla la comunicación en ambas direcciones (deshabilitando tramas entrantes y salientes) o solo en la dirección de entrada (deshabilitando solo la recepción de tramas entrantes).

Tabla 149. Información del resumen de puertos (continuación)

Campo	Descripción
PAE Capabilities	La función de la entidad de acceso a puerto (PAE), que puede ser Authenticator o Supplicant.
Authenticator PAE State	El estado de la PAE del autenticador: • Initialize • Authenticating • Authenticated • Held • Unauthenticated
Key Transmission Enabled	Indica si la transmisión de claves está habilitada. Si el valor es False, no se transmiten claves. De lo contrario, se admite la transmisión de claves.
Port Status	El estado de autorización del puerto: • N/A: Si el puerto está desconectado, el valor es N/A porque el puerto no puede participar en el control de acceso a puertos. • Authorized • Unauthorized
Protocol Version	La versión del protocolo siempre es 2, que corresponde a la segunda versión de la especificación 802.1X.

Mostrar el resumen de clientes

Puede mostrar información sobre los dispositivos solicitantes conectados a los puertos del autenticador local. Si no hay sesiones 802.1X activas, la tabla está vacía.

Para mostrar el resumen de clientes:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Port Authentication > Advanced > Client Summary. Se muestra la página Client Summary.

6. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe los campos no configurables de la página.

Tabla 150. Información del resumen de clientes

Campo	Descripción
Port	El puerto cuya información se muestra.
User Name	El nombre que representa la identidad del dispositivo solicitante.
Supplicant Mac Address	La dirección MAC del dispositivo solicitante.
Session Time	El tiempo en segundos desde que el solicitante inició sesión.
Filter ID	El ID de filtro de política que el autenticador asignó al dispositivo solicitante.
VLAN ID	El ID de VLAN que el autenticador asignó al dispositivo solicitante.
VLAN Assigned	El motivo del ID de VLAN que el autenticador asignó al dispositivo solicitante: • Default Assigned VLAN: El cliente se autenticó en la VLAN predeterminada del puerto y el servidor de autenticación no era un servidor RADIUS. • Radius Assigned VLAN: Se usó RADIUS para autenticar al cliente. • Unauthenticated VLAN: El cliente se autenticó en la VLAN no autenticada. • Guest VLAN: El cliente se autenticó en la VLAN de invitados. • Voice VLAN: El cliente se autenticó en la VLAN de voz. • Monitor Mode VLAN: El cliente se autenticó en modo Monitor y el servidor RADIUS lo asignó a una VLAN de supervisión. • Not Assigned: El cliente no se asignó a ninguna VLAN.
Session Timeout	El tiempo de espera de sesión que impone el servidor RADIUS al dispositivo solicitante.

Tabla 150. Información del resumen de clientes (continuación)

Campo	Descripción
Termination Action	La acción de terminación que impone el servidor RADIUS al dispositivo solicitante.
Time left for Session Termination Action	El tiempo restante antes de que se termine la sesión por el motivo que se muestra en el campo Termination Action.

Filtros MAC para control de tráfico

Puede crear filtros MAC que limiten el tráfico permitido hacia y desde puertos específicos del switch. Las limitaciones de tráfico se basan en direcciones MAC.

Crear un filtro MAC

Puede crear filtros MAC que limiten el tráfico permitido hacia y desde puertos específicos del sistema.

Para crear un filtro MAC:

1. Abra un navegador web.

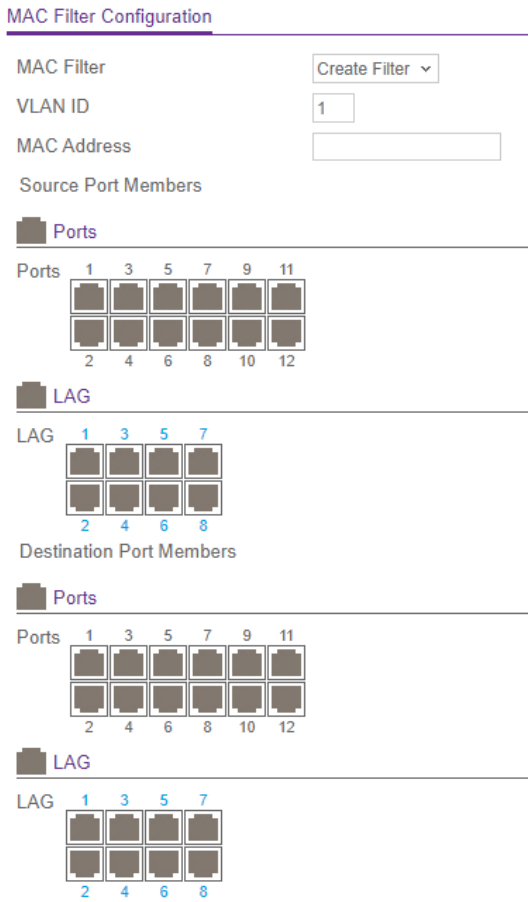
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > MAC Filter.



La figura anterior muestra la página de un modelo de 12 puertos.

6. En el menú MAC Filter, seleccione Create Filter.
Si no configuró ningún filtro, esta es la única opción disponible.

7. En el menú VLAN ID, seleccione la VLAN que se usará con la dirección MAC.

8. En el campo MAC Address, especifique la dirección MAC del filtro en el formato XX:XX:XX:XX:XX:XX.
No puede definir filtros para las siguientes direcciones MAC:

- 00:00:00:00:00:00
- 01:80:C2:00:00:00 a 01:80:C2:00:00:0F
- 01:80:C2:00:00:20 a 01:80:C2:00:00:21
- FF:FF:FF:FF:FF:FF

9. En las tablas Port y LAG de la sección Source Port Members, seleccione los puertos y LAG que se incluirán en el filtro de entrada.

Si se recibe un paquete con la dirección MAC y el VLAN ID especificados en un puerto que no forma parte del filtro de entrada, el paquete se descarta.

10. En las tablas Port y LAG de la sección Destination Port Members, seleccione los puertos y LAG que se incluirán en el filtro de salida.
Un paquete con la dirección MAC y el VLAN ID especificados solo puede transmitirse desde un puerto que forme parte del filtro de salida.

Nota: Los puertos de destino solo pueden incluirse en un filtro multicast. Un filtro multicast se determina por la dirección MAC que escriba en el campo MAC Address.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar un filtro MAC

Puede eliminar un filtro MAC existente que ya no necesite.

Para eliminar un filtro MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > MAC Filter. Aparece la página MAC Filter Configuration.

6. En el menú MAC Filter, seleccione el filtro MAC.

7. Haga clic en el botón Delete. Se elimina el filtro.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar el resumen de filtros MAC

Puede mostrar los filtros MAC configurados en el switch.

Para mostrar el resumen de filtros MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Traffic Control > MAC Filter > MAC Filter Summary. Aparece la página MAC Filter Summary.

   La siguiente tabla describe los campos no configurables de la página.

Tabla 151. Información del resumen de filtros MAC

Campo	Descripción
MAC Address	La dirección MAC del filtro en el formato XX:XX:XX:XX:XX:XX.
VLAN ID	El VLAN ID usado con la dirección MAC para identificar por completo los paquetes que desea filtrar.

Tabla 151. Información del resumen de filtros MAC (continuación)

Campo	Descripción
Source Port Members	Los puertos que se usan para filtrar los paquetes entrantes.
Destination Port Members	Los puertos que se usan para filtrar los paquetes salientes.

Seguridad de puertos

La seguridad de puertos le permite bloquear uno o más puertos del switch. Cuando un puerto está bloqueado, solo puede reenviar paquetes con direcciones MAC de origen que usted haya permitido específicamente. El puerto descarta todos los demás paquetes.

Configurar el modo global de seguridad de puertos

Para configurar el modo global de seguridad de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Port Security > Port Administration. Aparece la página Port Administration.

6. Para habilitar la seguridad de puertos en el switch, seleccione el botón de opción Port Security Mode Enable.
El valor predeterminado es Disable.

   La tabla Port Security Violations muestra información sobre las infracciones ocurridas en los puertos con seguridad de puertos habilitada.

Tabla 152. Información de infracciones de seguridad de puertos

Campo	Descripción
Port	La interfaz.
Last Violation MAC	La dirección MAC de origen del último paquete descartado en un puerto bloqueado.
VLAN ID	El VLAN ID correspondiente a la última infracción de dirección MAC.

Configurar una interfaz de seguridad de puertos

Una dirección MAC puede definirse como permitida mediante uno de dos métodos: dinámico o estático. Ambos métodos se usan simultáneamente cuando un puerto está bloqueado.

El bloqueo dinámico implementa un mecanismo de primera llegada para la seguridad de puertos. Usted especifica cuántas direcciones se pueden aprender en el puerto bloqueado. Si no se alcanza el límite, un paquete con una dirección MAC de origen desconocida se aprende y se reenvía normalmente. Si se alcanza el límite, no se aprenden más direcciones en el puerto. Se descartan los paquetes con direcciones MAC de origen que aún no se hayan aprendido. Puede deshabilitar en la práctica el bloqueo dinámico estableciendo en cero el número de entradas dinámicas permitidas.

El bloqueo estático le permite especificar una lista de direcciones MAC permitidas en un puerto. El comportamiento de los paquetes es el mismo que en el bloqueo dinámico: solo se pueden reenviar paquetes con una dirección MAC de origen permitida.

Para configurar los ajustes de seguridad de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Port Security > Interface Configuration. Aparece la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada a la interfaz, o escriba el número de interfaz en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
- Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. Especifique los siguientes ajustes:

- Security Mode: Habilita o deshabilita la seguridad de puertos. El valor predeterminado es Disable.
- Max Learned MAC Address: Especifique el número máximo de direcciones MAC aprendidas dinámicamente. El valor predeterminado es 4096. Si especifica 0, la interfaz no aprende ninguna dirección MAC.
- Max Static MAC Address: Especifique el número máximo de direcciones MAC bloqueadas estáticamente. El valor predeterminado es 48.
- Violation Shutdown: Habilita o deshabilita el apagado si se recibe un paquete con una dirección MAC no permitida. El valor predeterminado es Disable.
- Violation Traps: Habilita o deshabilita el envío de traps de infracción si se recibe un paquete con una dirección MAC no permitida. El valor predeterminado es Disable.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Mostrar las direcciones MAC aprendidas y convertirlas en direcciones estáticas

Después de habilitar la seguridad de puertos globalmente (consulte Configurar el modo global de seguridad de puertos en la página 567) y en interfaces específicas (consulte Configurar una interfaz de seguridad de puertos en la página 568), puede convertir una dirección MAC aprendida dinámicamente en una dirección bloqueada estáticamente.

Para mostrar las direcciones MAC aprendidas de una interfaz o LAG y convertirlas en direcciones MAC estáticas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Port Security > Dynamic MAC Address. Aparece la página Dynamic MAC Address.

6. Para mostrar las direcciones MAC aprendidas de una interfaz, en el menú Port List, seleccione la interfaz o LAG.
El campo Number of Dynamic MAC Addresses Learned muestra el número de direcciones MAC aprendidas dinámicamente en un puerto específico.

La siguiente tabla muestra las direcciones MAC y sus VLAN asociadas aprendidas en la interfaz seleccionada.

Campo	Descripción
VLAN ID	El VLAN ID correspondiente a la dirección MAC.
MAC Address	Las direcciones MAC aprendidas en el puerto.

7. Para convertir las direcciones MAC aprendidas dinámicamente en la interfaz en direcciones bloqueadas estáticamente, seleccione la casilla Convert Dynamic Address to Static. Las entradas de direcciones MAC dinámicas se convierten en entradas estáticas en orden numérico ascendente hasta alcanzar el límite estático.

8. Para actualizar la página, haga clic en el botón Refresh.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Agregar una dirección MAC estática a la tabla de direcciones MAC para la seguridad de puertos

Las entradas de direcciones MAC estáticas son las que usted agrega manualmente a la tabla de direcciones MAC para la seguridad de puertos de una interfaz y VLAN específicas.

Para agregar una dirección MAC estática a la tabla de direcciones MAC para la seguridad de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Port Security > Static MAC Address. Aparece la página Static MAC Address.

6. En el menú Interface, seleccione la interfaz o el LAG.
7. En el campo Static MAC Address, introduzca la dirección MAC.

8. En el menú VLAN ID, seleccione el ID de VLAN que se asociará con la dirección MAC.

9. Haga clic en el botón Add.
La dirección MAC estática se agrega a la tabla de direcciones MAC.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una dirección MAC estática de la tabla de direcciones MAC para la seguridad de puertos

Puede eliminar una dirección MAC estática que ya no necesite para la seguridad de puertos.

Para eliminar una dirección MAC estática de la tabla de direcciones MAC para la seguridad de puertos:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Port Security > Static MAC Address. Aparece la página Static MAC Address.

6. En el menú Interface, seleccione la interfaz o el LAG.
7. Seleccione la casilla de la dirección MAC.

8. Haga clic en el botón Delete.
La dirección MAC estática se elimina de la tabla de direcciones MAC.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Grupos de puertos privados

Para agregar un nivel de seguridad, puede crear un grupo privado de puertos físicos (no LAG) que funcione en modo aislado o de comunidad:

- Grupo en modo aislado: Un puerto que agregue como miembro del grupo no puede reenviar su tráfico de salida a ningún otro miembro del mismo grupo.
- Grupo en modo comunidad: Un puerto que agregue como miembro del grupo puede reenviar su tráfico de salida a otros miembros del mismo grupo, pero no a miembros de otros grupos.

Agregar un grupo de puertos privado

Después de agregar un grupo privado, puede agregarle miembros (consulte Configurar la membresía de un grupo de puertos privado en la página 574).

Para agregar un grupo de puertos privado:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private Group > Private Group Configuration. Aparece la página Private Group Configuration.

6. En el campo Group Name, escriba el nombre del grupo privado. El nombre puede tener hasta 24 caracteres.

7. En el menú Group Mode, seleccione el modo del grupo privado:

- Isolated: Un puerto que agregue como miembro del grupo no puede reenviar su tráfico de salida a ningún otro miembro del mismo grupo.
- Community: Un puerto que agregue como miembro del grupo puede reenviar su tráfico de salida a otros miembros del mismo grupo, pero no a miembros de otros grupos.

8. Haga clic en el botón Add.
Se agrega el grupo privado.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un grupo de puertos privado

Puede eliminar un grupo de puertos privado que ya no necesite.

Para eliminar un grupo de puertos privado:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private Group > Private Group Configuration. Aparece la página Private Group Configuration.

6. Seleccione la casilla junto al grupo privado.

7. Haga clic en el botón Delete.
Se elimina el grupo privado.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar la membresía de un grupo de puertos privado

Después de agregar un grupo de puertos privado, puede agregarle miembros (consulte Agregar un grupo de puertos privado en la página 572).

Para configurar la membresía de un grupo de puertos privado:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private Group > Private Group Membership. Aparece la página Private Group Membership.

6. En el menú Group ID, seleccione el ID del grupo.
7. En la tabla Ports, seleccione los puertos que serán miembros del grupo.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información no configurable de la página.

Tabla 153. Información de membresía de grupos privados

Campo	Descripción
Group Name	El nombre del grupo privado.
Group Mode	El modo del grupo privado (Community o Isolated).

Proteger puertos

Si un puerto está configurado como protegido, no reenvía tráfico a ningún otro puerto protegido del switch, pero sí a los puertos no protegidos. Puede configurar puertos como protegidos o no protegidos.

Para configurar puertos protegidos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Protected Ports. Aparece la página Protected Ports.

6. En la lista Group ID, seleccione 0, 1 o 2 para combinar los puertos protegidos seleccionados en un grupo lógico.
El tráfico puede fluir entre puertos protegidos de grupos distintos, pero no dentro del mismo grupo. El ID de grupo puede ser 0, 1 o 2.

7. Para asociar un nombre al grupo de puertos protegidos, especifíquelo en el campo Group Name.
El nombre puede tener hasta 32 caracteres alfanuméricos, incluidos espacios.

8. En la tabla Ports, seleccione los puertos que serán puertos protegidos y miembros del grupo de puertos protegidos.
De forma predeterminada, todos los puertos están desprotegidos.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

VLAN privadas

Una VLAN privada contiene puertos del switch que no pueden comunicarse entre sí, pero sí acceder a otra red. Estos puertos se llaman puertos privados. Cada VLAN privada contiene uno o más puertos privados y un único puerto uplink o grupo de agregación uplink. Tenga en cuenta que todo el tráfico entre puertos privados se bloquea en todas las capas, no solo el de capa 2, sino también tráfico como FTP, HTTP y Telnet.

Una VLAN privada separa un dominio VLAN normal en dos o más subdominios. Cada subdominio se define (representa) mediante una VLAN principal y una VLAN secundaria:

- VLAN principal: El ID de VLAN principal es el mismo para todos los subdominios que pertenecen a una VLAN privada.
- VLAN secundaria: El ID de VLAN secundaria diferencia los subdominios entre sí y proporciona aislamiento de capa 2 entre puertos de la misma VLAN privada.

Dentro de una VLAN privada pueden existir tres tipos de VLAN:

- VLAN principal: La VLAN reenvía tráfico de los puertos promiscuos a los puertos aislados, puertos de comunidad y otros puertos promiscuos de la misma VLAN privada. En una VLAN privada, solo puede configurar una VLAN principal. Todos los puertos de una VLAN privada comparten la misma VLAN principal.
- VLAN aislada: Es una VLAN secundaria que transporta tráfico de los puertos aislados a los puertos promiscuos. En una VLAN privada, solo puede configurar una VLAN aislada.
- VLAN de comunidad: Es una VLAN secundaria que reenvía tráfico entre puertos de la misma comunidad y hacia los puertos promiscuos. En una VLAN privada, puede configurar varias VLAN de comunidad.

Dentro de una VLAN privada, el switch admite cinco tipos de designación de puertos:

- Puerto promiscuo: Es miembro de una VLAN principal (dentro de la VLAN privada) y puede comunicarse con todos los tipos de puertos de la VLAN privada, incluidos otros puertos promiscuos, puertos de comunidad y puertos aislados.

- Puerto de comunidad: Es un puerto host miembro de una VLAN de comunidad (una VLAN secundaria dentro de la VLAN privada) que puede comunicarse con otros puertos de comunidad y con puertos promiscuos.
- Puerto aislado: Es un puerto host miembro de una VLAN aislada (una VLAN secundaria dentro de la VLAN privada) que solo puede comunicarse con puertos promiscuos.
- Puerto troncal promiscuo: Es a la vez un puerto troncal uplink (por ejemplo, puede conectar un router) y un puerto promiscuo que puede ser miembro de varias VLAN principales (dentro de la VLAN privada) y de VLAN normales. Procesa tráfico etiquetado para comunicarse con todos los tipos de puertos de las VLAN privadas (incluidos puertos promiscuos, de comunidad y aislados) y con puertos de VLAN normales.
- Puerto troncal aislado: Es un puerto troncal downlink (por ejemplo, puede conectarse a varios dispositivos descendentes) y puede ser miembro de varias VLAN aisladas (VLAN secundarias dentro de VLAN privadas) y de VLAN normales. Procesa tráfico etiquetado para comunicarse con puertos de VLAN aisladas y con puertos de VLAN normales. Los dispositivos descendentes conectados al puerto troncal aislado no necesitan ser compatibles con VLAN privadas.

Descripción general de las tareas de configuración de VLAN privadas

Para configurar una VLAN privada que permita la comunicación entre switches de una red, realice las tareas descritas en las siguientes secciones:

1. Asignar un tipo de VLAN privada a una VLAN en la página 578.
De forma predeterminada, una VLAN es una VLAN normal, por lo que debe asignarle un tipo de VLAN privada.

2. Configurar una asociación de VLAN privada con una VLAN principal y secundaria en la página 579.
Una VLAN privada debe constar de una sola VLAN principal y una o más VLAN secundarias.

3. Configurar el modo de puerto de VLAN privada en la página 581.
Un puerto debe estar en el modo correcto para participar en una VLAN privada. Por ejemplo, para que un puerto sea miembro de una VLAN aislada o de comunidad, primero debe configurarlo como puerto host.

4. Interfaz host de VLAN privada: Asignar la interfaz a VLAN principales y secundarias en la página 583.
Para un puerto configurado en modo host, configure una sola VLAN principal y una sola VLAN secundaria.

5. Interfaz promiscua de VLAN privada: Asignar la interfaz a VLAN principales y secundarias en la página 586.
Para un puerto configurado en modo promiscuo, configure una sola VLAN principal y una o más VLAN secundarias.

6. Interfaz troncal promiscua de VLAN privada: Agregar VLAN principales y secundarias a la troncal en la página 589.
Para un puerto configurado en modo troncal promiscuo, agregue VLAN principales y secundarias a la troncal.

7. Interfaz troncal aislada de VLAN privada: Agregar VLAN principales y secundarias a la troncal en la página 591
Para un puerto configurado en modo troncal aislado, agregue VLAN principales y secundarias a la troncal.

8. Configurar VLAN nativas y permitidas en una interfaz troncal de VLAN privada en la página 593 Para un puerto configurado en un modo troncal de VLAN privada (ya sea troncal promiscuo o troncal aislado), configure las VLAN nativas para el tráfico sin etiqueta y las VLAN privadas permitidas.

Asignar un tipo de VLAN privada a una VLAN

A cada VLAN puede asignarle un tipo de VLAN privada: Primary, Isolated o Community. De forma predeterminada, una VLAN es una VLAN normal con el tipo de VLAN privada Unconfigured.

Para asignar un tipo de VLAN privada a una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Type Configuration.

Aparece la página Private VLAN Type Configuration.

6. Marque la casilla de la VLAN.
7. En el menú Private VLAN Type, seleccione el tipo de VLAN privada:

• Unconfigured: La VLAN no es una VLAN privada sino una VLAN normal. Es el ajuste predeterminado.
• Primary: Es una VLAN principal que reenvía tráfico de los puertos promiscuos a los puertos aislados, de comunidad y otros puertos promiscuos de la misma VLAN privada. En una VLAN privada, solo puede configurar una VLAN principal. Todos los puertos de una VLAN privada comparten la misma VLAN principal.
• Isolated: Es una VLAN secundaria que transporta tráfico de los puertos aislados a los puertos promiscuos. En una VLAN privada, solo puede configurar una VLAN aislada.
• Community: Es una VLAN secundaria que reenvía tráfico entre puertos de la misma comunidad y hacia los puertos promiscuos. En una VLAN privada, puede configurar varias VLAN de comunidad.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una asociación de VLAN privada con una VLAN principal y secundaria

Puede configurar una VLAN privada asociando una sola VLAN principal con una o más VLAN secundarias.

Para configurar una asociación de VLAN privada con una VLAN principal y secundaria:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Association Configuration.
Aparece la página Private VLAN Association Configuration.

6. Si va a cambiar una asociación de VLAN privada existente, seleccione la casilla de la asociación.

7. En el menú Primary VLAN, seleccione el ID de VLAN principal de la VLAN privada.
Esta opción especifica la VLAN principal dentro de la VLAN privada. Puede asociar VLAN secundarias de la VLAN privada con esta VLAN principal.

Para configurar una VLAN principal para la VLAN privada, consulte Asignar un tipo de VLAN privada a una VLAN en la página 578.

8. En el campo Secondary VLANs, especifique una o más VLAN secundarias para la VLAN privada.
Esta opción especifica las VLAN secundarias (VLAN aisladas, de comunidad o una combinación de ambas) dentro de la VLAN privada. Las VLAN secundarias se asocian con la VLAN principal de la VLAN privada.

Puede especificar un solo VLAN ID, un rango de VLAN ID o una combinación de ambos en secuencia separados por coma (,):

- Puede especificar un VLAN ID individual, como 10.
- Puede especificar un rango de VLAN separado por guion, por ejemplo, 10-13.
- Puede especificar una combinación de ambos separada por comas, por ejemplo: 12,15,40–43,1000–1005, 2000.

Para configurar una VLAN aislada o de comunidad para la VLAN privada, consulte Asignar un tipo de VLAN privada a una VLAN en la página 578.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 154. Asociación de VLAN privada

Campo	Descripción
Isolated VLAN	La única VLAN aislada asociada a la VLAN principal seleccionada.
Community VLAN(s)	La lista de VLAN de comunidad asociadas a la VLAN principal seleccionada.

Eliminar una asociación de VLAN privada existente

Puede eliminar una asociación de VLAN privada que ya no necesite.

Para eliminar una asociación de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Association Configuration.
Aparece la página Private VLAN Association Configuration.

6. Seleccione la casilla de la asociación de VLAN privada.

7. Haga clic en el botón Delete.
Se guardan los ajustes. Se elimina la asociación de VLAN privada.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el modo de puerto de VLAN privada

Un puerto debe estar en el modo correcto para participar en una VLAN privada.

El modo de puerto de VLAN privada determina si un puerto (o LAG) funciona en modo Host para una VLAN principal o secundaria (dentro de una VLAN privada) o en modo Promiscuous para una VLAN promiscua (dentro de una VLAN privada).

También puede configurar un puerto (o LAG) para que funcione como troncal promiscua para un uplink a un router o como troncal aislada para un downlink a varios dispositivos. Estos tipos de puertos troncales de VLAN privada pueden transportar varias VLAN privadas y VLAN normales.

Para configurar el modo de puerto de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration.
Aparece la página Private VLAN Port Mode Configuration.

6. En el menú Port VLAN Mode, seleccione el modo de puerto de VLAN privada:

• General: El puerto funciona en modo general y no como puerto de una VLAN privada. Es el ajuste predeterminado.
• Host: El puerto funciona en modo host en una VLAN privada. En este modo, el puerto puede ser miembro de una VLAN de comunidad o de una VLAN aislada:

- Community VLAN: El puerto es miembro de una VLAN secundaria (dentro de la VLAN privada) y puede comunicarse con otros puertos community y puertos promiscuos.
- Isolated VLAN: El puerto es miembro de una VLAN secundaria (dentro de la VLAN privada) y solo puede comunicarse con puertos promiscuos.

Para configurar un puerto host como miembro de VLAN específicas, consulte Interfaz host de VLAN privada: Asignar la interfaz a VLAN primarias y secundarias en la página 583.
• Promiscuous: El puerto funciona en modo promiscuo en una VLAN privada. En este modo, el puerto puede comunicarse con todos los tipos de puertos de la VLAN privada, incluidos otros puertos promiscuos, puertos community y puertos aislados.

Para configurar un puerto promiscuo como miembro de VLAN específicas, consulte Interfaz promiscua de VLAN privada: Asignar la interfaz a VLAN primarias y secundarias en la página 586.

• Promiscuous trunk port: El puerto funciona en modo trunk promiscuo como puerto trunk de enlace ascendente (por ejemplo, puede conectar un router) y como puerto promiscuo que puede ser miembro de varias VLAN primarias (dentro de la VLAN privada) y de VLAN normales. En este modo, el puerto procesa tráfico etiquetado para comunicarse con todos los tipos de puertos de las VLAN privadas (incluidos puertos promiscuos, community y aislados) y con puertos de VLAN normales.
Para asignar un puerto trunk promiscuo a VLAN específicas, consulte Interfaz trunk promiscua de VLAN privada: Agregar VLAN primarias y secundarias al trunk en la página 589.

• Isolated trunk port: El puerto funciona en modo trunk aislado (por ejemplo, puede conectarse a varios dispositivos descendentes) y puede ser miembro de varias VLAN aisladas (VLAN secundarias dentro de VLAN privadas) y de VLAN normales. En este modo, el puerto procesa tráfico etiquetado para comunicarse con puertos de VLAN aisladas y con puertos de VLAN normales. Los dispositivos descendentes conectados al puerto trunk aislado no necesitan ser compatibles con VLAN privadas.
Para asignar un puerto trunk aislado a VLAN específicas, consulte Interfaz trunk aislada de VLAN privada: Agregar VLAN primarias y secundarias al trunk en la página 591.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Interfaz host de VLAN privada: Asignar la interfaz a VLAN primarias y secundarias

Si configura el modo de puerto de VLAN privada de una interfaz como Host (consulte Configurar el modo de puerto de VLAN privada en la página 581), puede asignar la interfaz a una sola VLAN primaria y una sola VLAN secundaria.

Para asignar una interfaz host de VLAN privada a una VLAN primaria y una secundaria:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.
Se muestra la página Private VLAN Host Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, seleccione la casilla asociada al puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, seleccione la casilla asociada a cada interfaz.

La interfaz que seleccione debe estar configurada en modo Host (consulte Configurar el modo de puerto de VLAN privada en la página 581).

8. En el campo Host Primary VLAN, especifique un ID de VLAN primaria.
Puede seleccionar una VLAN cuyo tipo configuró como Primary (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

9. En el campo Host Secondary VLAN, especifique un ID de VLAN secundaria. Puede seleccionar una VLAN cuyo tipo configuró como Isolated o Community, ambos tipos de VLAN secundaria dentro de una VLAN privada (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

El campo Operational VLAN(s) muestra las VLAN primarias y secundarias que operan en la interfaz host.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Interfaz host de VLAN privada: Quitar la interfaz de VLAN primarias y secundarias

Puede quitar una interfaz host de VLAN privada de las VLAN primarias y secundarias.

Para quitar una interfaz host de VLAN privada de las VLAN primarias y secundarias:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.
Se muestra la página Private VLAN Host Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, seleccione la casilla asociada al puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, seleccione la casilla asociada a cada interfaz.

La interfaz que seleccione debe estar configurada en modo Host (consulte Configurar el modo de puerto de VLAN privada en la página 581).

8. Haga clic en el botón Delete.
Se guardan los ajustes. La interfaz se quita de las VLAN primarias y secundarias.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Interfaz promiscua de VLAN privada: Asignar la interfaz a VLAN primarias y secundarias

Si configura el modo de puerto de VLAN privada de una interfaz como Promiscuous (consulte Configurar el modo de puerto de VLAN privada en la página 581), puede asignar la interfaz a una sola VLAN primaria y a una o más VLAN secundarias.

Para asignar una interfaz promiscua de VLAN privada a una VLAN primaria y a VLAN secundarias:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration.
Se muestra la página Private VLAN Promiscuous Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, seleccione la casilla asociada al puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, seleccione la casilla asociada a cada interfaz.

La interfaz que seleccione debe estar configurada en modo Promiscuous (consulte Configurar el modo de puerto de VLAN privada en la página 581).

8. En el campo Promiscuous Primary VLAN, especifique un ID de VLAN primaria.
Puede seleccionar una VLAN cuyo tipo configuró como Primary (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

9. En el campo Promiscuous Secondary VLAN IDs, especifique uno o más IDs de VLAN secundaria.
Puede especificar VLAN cuyo tipo configuró como Isolated o Community, ambos tipos de VLAN secundaria dentro de una VLAN privada (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

Puede especificar un solo VLAN ID, un rango de VLAN ID o una combinación de ambos en secuencia separados por coma (,):

- Puede especificar un VLAN ID individual, como 10.
- Puede especificar un rango de VLAN separado por guion, por ejemplo, 10-13.
- Puede especificar una combinación de ambos separada por comas, por ejemplo: 12,15,40–43,1000–1005, 2000.

Nota: Los IDs de VLAN que especifique sobrescriben las VLAN secundarias que configuró en la página Private VLAN Association Configuration (consulte Configurar una asociación de VLAN privada con una VLAN primaria y secundaria en la página 579).

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

El campo Operational VLAN(s) muestra las VLAN primarias y secundarias que operan en la interfaz promiscua.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Interfaz promiscua de VLAN privada: Quitar la interfaz de VLAN primarias y secundarias

Puede quitar una interfaz promiscua de VLAN privada de las VLAN primarias y secundarias.

Para quitar una interfaz promiscua de VLAN privada de las VLAN primarias y secundarias:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration.
Se muestra la página Private VLAN Promiscuous Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, seleccione la casilla asociada al puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, seleccione la casilla asociada a cada interfaz.

La interfaz que seleccione debe estar configurada en modo Promiscuous (consulte Configurar el modo de puerto de VLAN privada en la página 581).

8. Haga clic en el botón Delete.
Se guardan los ajustes.

Se guardan los ajustes. La interfaz se quita de las VLAN primarias y secundarias.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Interfaz trunk promiscua de VLAN privada: Agregar VLAN primarias y secundarias al trunk

Si configura el modo de puerto de VLAN privada de una interfaz como Promiscuous Trunk (consulte Configurar el modo de puerto de VLAN privada en la página 581), puede agregar varias configuraciones de VLAN al trunk. Cada configuración de VLAN consta de una sola VLAN primaria y una o más VLAN secundarias.

Para agregar una VLAN primaria y VLAN secundarias a una interfaz trunk promiscua de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Trunk Interface Configuration.
Se muestra la página Private VLAN Promiscuous Trunk Interface Configuration.

6. En el menú Interface, seleccione una interfaz o LAG cuyo modo de puerto VLAN configuró como Promiscuous Trunk.
Para más información sobre los modos VLAN de puerto, consulte Configurar el modo de puerto de VLAN privada en la página 581.

7. En el campo Promiscuous Trunk Primary VLAN, especifique un ID de VLAN primaria. Puede seleccionar una VLAN cuyo tipo configuró como Primary (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

8. En el campo Promiscuous Trunk Secondary VLAN(s), especifique uno o más IDs de VLAN secundaria.
Puede especificar VLAN cuyo tipo configuró como Isolated o Community, ambos tipos de VLAN secundaria dentro de una VLAN privada (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

Puede especificar un solo VLAN ID, un rango de VLAN ID o una combinación de ambos en secuencia separados por coma (,):

• Puede especificar un VLAN ID individual, como 10.
• Puede especificar un rango de VLAN separado por guion, por ejemplo, 10-13.
• Puede especificar una combinación de ambos separada por comas, por ejemplo: 12,15,40–43,1000–1005, 2000.

Nota: Los IDs de VLAN que especifique sobrescriben las VLAN secundarias que configuró en la página Private VLAN Association Configuration (consulte Configurar una asociación de VLAN privada con una VLAN primaria y secundaria en la página 579).

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Operational VLAN(s) muestra las VLAN primarias y secundarias que operan en la interfaz trunk promiscua.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Interfaz trunk promiscua de VLAN privada: Quitar VLAN primarias y secundarias del trunk

Puede quitar VLAN primarias y secundarias de una interfaz trunk promiscua de VLAN privada.

Para quitar VLAN primarias y secundarias de una interfaz trunk promiscua de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Trunk Interface Configuration.
Se muestra la página Private VLAN Promiscuous Trunk Interface Configuration.

6. En el menú Interface, seleccione una interfaz o LAG cuyo modo de puerto VLAN configuró como Promiscuous Trunk.
Para más información sobre los modos VLAN de puerto, consulte Configurar el modo de puerto de VLAN privada en la página 581.

7. Seleccione la casilla de la configuración de VLAN.

8. Haga clic en el botón Delete.
Se guardan los ajustes.

Las VLAN primarias y secundarias se quitan de la interfaz seleccionada. Las VLAN en sí no se eliminan.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Interfaz trunk aislada de VLAN privada: Agregar VLAN primarias y secundarias al trunk

Si configura el modo de puerto de VLAN privada de una interfaz como Isolated Trunk (consulte Configurar el modo de puerto de VLAN privada en la página 581), puede agregar varias configuraciones de VLAN al trunk. Cada configuración de VLAN consta de una sola VLAN primaria y una o más VLAN secundarias.

Para agregar una VLAN primaria y VLAN secundarias a una interfaz trunk aislada de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Isolated Trunk Interface Configuration.

Se muestra la página Private VLAN Isolated Trunk Interface Configuration.

6. En el menú Interface, seleccione una interfaz o LAG cuyo modo de puerto VLAN configuró como Isolated Trunk.
Para más información sobre los modos VLAN de puerto, consulte Configurar el modo de puerto de VLAN privada en la página 581.

7. En el campo Isolated Trunk Primary VLAN, especifique un ID de VLAN primaria.
Puede seleccionar una VLAN cuyo tipo configuró como Primary (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

8. En el campo Isolated Trunk Secondary VLAN(s), especifique uno o más IDs de VLAN secundaria.
Puede especificar VLAN cuyo tipo configuró como Isolated o Community, ambos tipos de VLAN secundaria dentro de una VLAN privada (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

Puede especificar un solo VLAN ID, un rango de VLAN ID o una combinación de ambos en secuencia separados por coma (,):

- Puede especificar un VLAN ID individual, como 10.
- Puede especificar un rango de VLAN separado por guion, por ejemplo, 10-13.
- Puede especificar una combinación de ambos separada por comas, por ejemplo: 12,15,40–43,1000–1005, 2000.

Nota: Los IDs de VLAN que especifique sobrescriben las VLAN secundarias que configuró en la página Private VLAN Association Configuration (consulte Configurar una asociación de VLAN privada con una VLAN primaria y secundaria en la página 579).

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Operational VLAN(s) muestra las VLAN primarias y secundarias que operan en la interfaz trunk aislada.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Interfaz trunk aislada de VLAN privada: Quitar VLAN primarias y secundarias del trunk

Puede quitar VLAN primarias y secundarias de una interfaz trunk aislada de VLAN privada.

Para quitar VLAN primarias y secundarias de una interfaz trunk aislada de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Isolated Trunk Interface Configuration.
Se muestra la página Private VLAN Isolated Trunk Interface Configuration.

6. En el menú Interface, seleccione una interfaz o LAG cuyo modo de puerto VLAN configuró como Isolated Trunk.
Para más información sobre los modos VLAN de puerto, consulte Configurar el modo de puerto de VLAN privada en la página 581.

7. Seleccione la casilla de la configuración de VLAN.

8. Haga clic en el botón Delete.
Se guardan los ajustes.

Las VLAN primarias y secundarias se quitan de la interfaz seleccionada. Las VLAN en sí no se eliminan.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar VLAN nativas y permitidas en una interfaz trunk de VLAN privada

Si configura una interfaz como interfaz promiscua de VLAN privada o como interfaz trunk aislada de VLAN privada, también puede permitir tráfico sin etiquetar de una VLAN nativa en la misma interfaz trunk. De forma predeterminada, la VLAN 1 es la VLAN predeterminada y la nativa, pero puede configurar otra VLAN como nativa (consulte Configurar los ajustes de modo de puerto del switch para interfaces en la página 196).

Si no especifica una VLAN nativa en la interfaz trunk privada, todos los paquetes sin etiquetar se descartan en la interfaz trunk de VLAN privada.

Para configurar VLAN nativas y permitidas en una interfaz trunk de VLAN privada:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Trunk Interface Configuration.
Se muestra la página Private VLAN Trunk Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, seleccione la casilla asociada al puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con los mismos ajustes, seleccione la casilla asociada a cada interfaz.

La interfaz que seleccione debe estar configurada en modo Promiscuous Trunk o Isolated Trunk (consulte Configurar el modo de puerto de VLAN privada en la página 581).

8. En el campo Trunk Native VLAN, especifique un ID de VLAN para la VLAN nativa. De forma predeterminada, la VLAN 1 es la VLAN predeterminada y la nativa, pero puede configurar otra VLAN como nativa (consulte Configurar los ajustes de modo de puerto del switch para interfaces en la página 196).

9. En el campo Trunk Allowed VLAN, especifique uno o más IDs de VLAN para configuraciones de VLAN privada que constan de una VLAN primaria y VLAN secundarias. Puede especificar VLAN cuyo tipo configuró como Promiscuous, Isolated o Community dentro de una VLAN privada (consulte Asignar un tipo de VLAN privada a una VLAN en la página 578).

Puede especificar un solo VLAN ID, un rango de VLAN ID o una combinación de ambos en secuencia separados por coma (,):

- Puede especificar un VLAN ID individual, como 10.
- Puede especificar un rango de VLAN separado por guion, por ejemplo, 10-13.
- Puede especificar una combinación de ambos separada por comas, por ejemplo: 12,15,40–43,1000–1005, 2000.

Nota: Los IDs de VLAN que especifique sobrescriben las VLAN secundarias que configuró en la página Private VLAN Association Configuration (consulte Configurar una asociación de VLAN privada con una VLAN primaria y secundaria en la página 579).

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

El campo Operational VLAN(s) muestra las VLAN que operan en la interfaz trunk de VLAN privada.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Control de tormentas

Una tormenta de broadcast es el resultado de un número excesivo de mensajes de broadcast transmitidos simultáneamente por la red desde un solo puerto. Las respuestas a los mensajes reenviados pueden sobrecargar los recursos de red, provocar tiempos de espera agotados, o ambos.

El switch mide la tasa de paquetes entrantes por puerto para paquetes broadcast, multicast, desconocidos y unicast, y descarta paquetes si la tasa supera el valor definido. Puede habilitar el control de tormentas por interfaz definiendo el tipo de paquete y la tasa a la que se transmiten los paquetes.

Configurar los ajustes globales de control de tormentas

Los ajustes globales de control de tormentas se aplican a todos los puertos. Después de configurar los ajustes globales, puede especificar ajustes de control de tormentas para uno o más puertos.

Para configurar los ajustes globales de control de tormentas:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Storm Control > Storm Control Global Configuration.
Se muestra la página Storm Control Global Configuration.

Los siguientes tres ajustes le permiten habilitar o deshabilitar globalmente la limitación de tasa de cada tipo de paquete en todos los puertos. Para puertos individuales, consulte Configurar los ajustes de control de tormentas para uno o más puertos en la página 597.

6. Configure los ajustes de control de tormentas seleccionando un botón de opción:
• Broadcast Storm Control All: Habilite o deshabilite esta opción:

- Enable: Si el tráfico broadcast de un puerto supera el umbral configurado, el switch descarta el tráfico broadcast. El valor predeterminado es Enable.
- Disable: El control de tormentas de broadcast está deshabilitado en todos los puertos.

• Multicast Storm Control All: Habilite o deshabilite esta opción:

- Enable: Si el tráfico multicast de un puerto supera el umbral configurado, el switch descarta el tráfico multicast. El valor predeterminado es Enable.
- Disable: El control de tormentas multicast está deshabilitado en todos los puertos. El valor predeterminado es Disable.

• Unknown Unicast Storm Control All: Habilite o deshabilite esta opción:

- Enable: Si el tráfico unicast desconocido de un puerto supera el umbral configurado, el switch descarta el tráfico unicast desconocido. El valor predeterminado es Enable.
- Disable: El control de tormentas de unicast desconocido está deshabilitado en todos los puertos. El valor predeterminado es Disable.

7. Haga clic en el botón Apply.

La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de control de tormentas para uno o más puertos

Puede especificar ajustes de control de tormentas para uno o más puertos.

Para configurar los ajustes de control de tormentas para uno o más puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Traffic Control > Storm Control > Storm Control Interface Configuration.
Se muestra la página Storm Control Interface Configuration.

6. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
• Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

7. Configure los siguientes ajustes para tormentas de broadcast:
• Recovery Mode: Habilite o deshabilite esta opción para el tráfico broadcast:

- Enable: Si el tráfico broadcast supera el umbral configurado, el puerto descarta el tráfico broadcast. El valor predeterminado es Enable.
- Disable: Si el tráfico broadcast supera el umbral configurado, el broadcast no se descarta.

• Recovery Level Type: Especifique el nivel de recuperación en el campo Recovery Level como porcentaje de la velocidad de enlace del puerto o como paquetes por segundo:

- Percent: El nivel de recuperación se expresa como porcentaje de la velocidad de enlace.
- pps: El nivel de recuperación se expresa en paquetes por segundo (pps).

• Recovery Level: Especifique el umbral a partir del cual se activa el control de tormentas de broadcast. De forma predeterminada, el nivel de recuperación es el 5 por ciento de la velocidad de enlace del puerto o 5 pps.
• Control Action: Especifique una de las siguientes acciones:

- None: No se realiza ninguna otra acción. Es el ajuste predeterminado.
- Trap: Si el tráfico broadcast supera el umbral configurado, se envía un trap.
- Shutdown: Si el tráfico broadcast supera el umbral configurado, el puerto se apaga.

8. Configure los siguientes ajustes para tormentas multicast:
• Recovery Mode: Habilite o deshabilite esta opción para el tráfico multicast:

- Enable: Si el tráfico multicast supera el umbral configurado, el puerto descarta el tráfico multicast. El valor predeterminado es Enable.
- Disable: Si el tráfico multicast supera el umbral configurado, el multicast no se descarta.

• Recovery Level Type: Especifique el nivel de recuperación en el campo Recovery Level como porcentaje de la velocidad de enlace del puerto o como paquetes por segundo:

- Percent: El nivel de recuperación se expresa como porcentaje de la velocidad de enlace.
- pps: El nivel de recuperación se expresa en paquetes por segundo (pps).

• Recovery Level: Especifique el umbral a partir del cual se activa el control de tormentas multicast. De forma predeterminada, el nivel de recuperación es el 5 por ciento de la velocidad de enlace del puerto o 5 pps.
• Control Action: Especifique una de las siguientes acciones:

- None: No se realiza ninguna otra acción. Es el ajuste predeterminado.
- Trap: Si el tráfico multicast supera el umbral configurado, se envía un trap.
- Shutdown: Si el tráfico multicast supera el umbral configurado, el puerto se apaga.

9. Configure los siguientes ajustes para tormentas unicast:

• Recovery Mode: Habilite o deshabilite esta opción para el tráfico unicast:

- Enable: Si el tráfico unicast supera el umbral configurado, el puerto descarta el tráfico unicast. El valor predeterminado es Enable.
- Disable: Si el tráfico unicast supera el umbral configurado, el unicast no se descarta.

• Recovery Level Type: Especifique el nivel de recuperación en el campo Recovery Level como porcentaje de la velocidad de enlace del puerto o como paquetes por segundo:

- Percent: El nivel de recuperación se expresa como porcentaje de la velocidad de enlace.
- pps: El nivel de recuperación se expresa en paquetes por segundo (pps).

• Recovery Level: Especifique el umbral a partir del cual se activa el control de tormentas unicast. De forma predeterminada, el nivel de recuperación es el 5 por ciento de la velocidad de enlace del puerto o 5 pps.
• Control Action: Especifique una de las siguientes acciones:

- None: No se realiza ninguna otra acción. Es el ajuste predeterminado.
- Trap: Si el tráfico unicast supera el umbral configurado, se envía un trap.
- Shutdown: Si el tráfico unicast supera el umbral configurado, el puerto se apaga.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

DHCP snooping

DHCP snooping es una función que proporciona seguridad al filtrar mensajes DHCP no confiables y al crear y mantener una tabla de vinculaciones de DHCP snooping. Un mensaje no confiable es un mensaje recibido desde fuera de la red o del firewall que puede provocar ataques de tráfico dentro de su red. La tabla de vinculaciones de DHCP snooping contiene la dirección MAC, la dirección IP, el tiempo de concesión, el tipo de vinculación, el número de VLAN y la información de interfaz correspondientes a las interfaces locales no confiables de un switch. Una interfaz no confiable es una interfaz configurada para recibir mensajes desde fuera de la red o del firewall. Una interfaz confiable es una interfaz configurada para recibir solo mensajes desde dentro de la red.

DHCP snooping actúa como un firewall entre hosts no confiables y servidores DHCP. También permite diferenciar entre las interfaces no confiables conectadas al usuario final y las interfaces confiables conectadas al servidor DHCP o a otro switch.

Habilitar DHCP snooping en el switch

Puede habilitar DHCP snooping globalmente en el switch.

Para habilitar DHCP snooping globalmente en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción DHCP Snooping Mode Enable. El valor predeterminado es Disable.

7. Para habilitar la verificación de la dirección MAC del remitente en DHCP snooping, deje seleccionado el botón de opción MAC Address Validation Enable.
El valor predeterminado es Enable.

Cuando la validación de direcciones MAC está habilitada, el dispositivo revisa los paquetes recibidos en una interfaz no confiable para verificar que la dirección MAC y la dirección de hardware del cliente DHCP coincidan. Si las direcciones no coinciden, el dispositivo descarta el paquete.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Habilitar DHCP snooping en una VLAN

Para habilitar DHCP snooping en una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Global Configuration. Se muestra la página Global Configuration.

La tabla muestra las VLAN.

6. Marque la casilla de la VLAN.

7. En el menú DHCP Snooping Mode, seleccione Enable.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de interfaz de DHCP snooping

Puede mostrar y configurar cada puerto como confiable o no confiable. Todas las respuestas DHCP recibidas en un puerto confiable se reenvían. Si un puerto está configurado como no confiable, se descartan todas las respuestas DHCP (o BootP) recibidas en ese puerto.

Para configurar los ajustes de interfaz de DHCP snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Interface Configuration.

Se muestra la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

• 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
• LAG: Solo se muestran los LAG.
• All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
• Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú Trust Mode, seleccione el modo de confianza:

• Disabled. La interfaz se considera no confiable y podría usarse para lanzar un ataque a la red. Los mensajes del servidor DHCP se comparan con la base de datos de vinculaciones. En los puertos no confiables, DHCP snooping aplica las siguientes reglas de seguridad:

- Se descartan los paquetes DHCP procedentes de un servidor DHCP.
- Se descartan los mensajes DHCP si la dirección MAC está en la base de datos de snooping pero la interfaz de la vinculación es distinta de la interfaz en la que se recibió el mensaje.
- Se descartan los paquetes DHCP si la dirección MAC de origen no coincide con la dirección de hardware del cliente y la validación de direcciones MAC está habilitada globalmente.

• Enabled. La interfaz se considera de confianza y reenvía los mensajes del servidor DHCP sin validación.

9. En el menú Invalid Packets, seleccione el modo de registro de paquetes. Si está habilitado, la función DHCP snooping genera un mensaje de registro cuando la interfaz recibe y descarta un paquete no válido.

10. En el campo Rate Limit (pps), especifique el valor de límite de tasa para DHCP snooping. Si la tasa de entrada de paquetes DHCP por segundo supera el intervalo de ráfaga configurado por segundo, el puerto se apaga. Si el límite de tasa es None (valor predeterminado), el intervalo de ráfaga tampoco se aplica y la limitación de tasa está deshabilitada.

11. En el campo Burst Interval (secs), especifique el intervalo de ráfaga en segundos para la limitación de tasa en la interfaz.
Si el límite de tasa es N/A, el intervalo de ráfaga no se aplica.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Agregar un enlace DHCP estático y mostrar los enlaces DHCP dinámicos

Puede agregar un enlace estático a la base de datos de enlaces de DHCP snooping y mostrar o borrar los enlaces dinámicos de la tabla de enlaces.

Para agregar un enlace DHCP estático y mostrar o borrar los enlaces dinámicos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Binding Configuration. Se muestra la página Binding Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo MAC Address, especifique la dirección MAC del enlace que desea agregar. Es la clave de la base de datos de enlaces.

8. En el menú VLAN ID, seleccione el ID de la VLAN.
9. En el campo IP Address, especifique la dirección IP del enlace que desea agregar.

10. Haga clic en el botón Add.
La entrada de enlace de DHCP snooping se agrega a la base de datos.

La tabla Dynamic Binding Configuration muestra información sobre los enlaces DHCP aprendidos en cada interfaz con DHCP snooping habilitado. La siguiente tabla describe la información de los enlaces dinámicos.

Campo	Descripción
Interface	La interfaz en la que se recibió el mensaje del cliente DHCP.
MAC Address	La dirección MAC asociada al cliente DHCP que envió el mensaje. Es la clave de la base de datos de enlaces.
VLAN ID	El VLAN ID de la interfaz del cliente.
IP Address	La dirección IP asignada al cliente por el servidor DHCP.
Lease Time	El tiempo de concesión restante de la dirección IP del cliente.

11. Para borrar todos los enlaces dinámicos de la tabla Dynamic Binding Configuration, haga clic en el botón Clear.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar un enlace DHCP estático

Puede eliminar un enlace estático de la base de datos de enlaces de DHCP snooping.

Para eliminar un enlace DHCP estático:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Binding Configuration. Se muestra la página Binding Configuration.

6. En la tabla Static Binding Configuration, marque la casilla del enlace estático.
7. Haga clic en el botón Delete.

La entrada de enlace de DHCP snooping se elimina de la base de datos.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el almacenamiento persistente de DHCP snooping

Puede configurar la ubicación persistente de la base de datos de enlaces de DHCP snooping. La base de datos se puede almacenar localmente en el switch o en un dispositivo remoto de la red. El switch debe poder alcanzar la dirección IP del dispositivo remoto para enviar enlaces a una base de datos remota.

Para configurar el almacenamiento persistente de DHCP snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Persistent Configuration. Se muestra la página Persistent Configuration.

6. Especifique dónde se ubica la base de datos de enlaces de DHCP snooping.

- Local: La tabla de enlaces se almacena localmente en el switch.
- Remote: La tabla de enlaces se almacena en un servidor TFTP remoto. Si la base de datos se almacena en un servidor remoto, especifique la siguiente información:
  - Remote IP Address: Especifique la dirección IP del servidor TFTP.
  - Remote File Name: Especifique el nombre de archivo de la base de datos de enlaces de DHCP snooping en la que se almacenan los enlaces.

7. En el campo Write Delay, especifique el tiempo que el switch debe esperar después de escribir la información de enlaces en el almacenamiento persistente.
El retardo permite al switch reunir tantas entradas como sea posible (nuevas y eliminadas) antes de escribirlas en el archivo persistente. Puede especificar de 15 a 86400 segundos. De forma predeterminada, el retardo es de 300 segundos.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar o borrar las estadísticas de DHCP snooping

Puede mostrar y borrar las estadísticas por interfaz de los mensajes DHCP filtrados por la función DHCP snooping en interfaces que no son de confianza.

Para mostrar o borrar las estadísticas de DHCP snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCP Snooping > Statistics. Se muestra la página Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Haga clic en el botón Clear para borrar las estadísticas de todas las interfaces.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe las estadísticas de DHCP snooping.

Tabla 155. Información de estadísticas de DHCP Snooping

Campo	Descripción
MAC Verify Failures	El número de mensajes DHCP descartados porque la dirección MAC de origen y la dirección de hardware del cliente no coincidían. La verificación de direcciones MAC solo se realiza si está habilitada globalmente.
Client Ifc Mismatch	El número de paquetes descartados por DHCP snooping porque la interfaz y la VLAN en las que se recibió el paquete no coinciden con la información de interfaz y VLAN del cliente almacenada en la base de datos de enlaces.
DHCP Server Msgs	El número de mensajes del servidor DHCP descartados en un puerto que no es de confianza.

DHCPv6 snooping

DHCPv6 snooping es una función que proporciona seguridad al filtrar mensajes DHCPv6 que no son de confianza y al crear y mantener una tabla de enlaces de DHCPv6 snooping. Un mensaje que no es de confianza es aquel que se recibe desde fuera de la red o del firewall y que puede provocar ataques de tráfico dentro de su red. La tabla de enlaces de DHCPv6 snooping contiene la dirección MAC, la dirección IP, el tiempo de concesión, el tipo de enlace, el número de VLAN y la información de interfaz correspondientes a las interfaces locales que no son de confianza de un switch. Una interfaz que no es de confianza está configurada para recibir mensajes desde fuera de la red o del firewall. Una interfaz de confianza está configurada para recibir solo mensajes desde dentro de la red.

DHCPv6 snooping actúa como un firewall entre hosts que no son de confianza y servidores DHCPv6. También permite diferenciar entre interfaces que no son de confianza conectadas al usuario final e interfaces de confianza conectadas al servidor DHCPv6 o a otro switch.

Habilitar DHCPv6 snooping en el switch

Puede habilitar globalmente DHCPv6 snooping en el switch.

Para habilitar globalmente DHCPv6 snooping en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Global Configuration. Se muestra la página Global Configuration.

6. Seleccione el botón de opción DHCPv6 Snooping Mode Enable. El valor predeterminado es Disable.

7. Para habilitar la verificación de la dirección MAC del remitente en DHCPv6 snooping, deje seleccionado el botón de opción MAC Address Validation Enable. El valor predeterminado es Enable.

Cuando la validación de direcciones MAC está habilitada, el dispositivo revisa los paquetes recibidos en una interfaz que no es de confianza para verificar que la dirección MAC y la dirección de hardware del cliente DHCPv6 coincidan. Si no coinciden, el dispositivo descarta el paquete.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Habilitar DHCPv6 snooping en una VLAN

Para habilitar DHCPv6 snooping en una VLAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Global Configuration. Se muestra la página Global Configuration.

La tabla muestra las VLAN.

6. Marque la casilla de la VLAN.

7. En el menú DHCPv6 Snooping Mode, seleccione Enable.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar DHCPv6 snooping en las interfaces

Puede mostrar y configurar cada puerto como de confianza o no de confianza. Las respuestas DHCPv6 recibidas en un puerto de confianza se reenvían. Si un puerto está configurado como no de confianza, se descartan las respuestas DHCPv6 (o BootP) recibidas en ese puerto.

Para configurar DHCPv6 snooping en las interfaces:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Interface Configuration. Se muestra la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada al puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.

• Para configurar varias interfaces con los mismos ajustes, marque la casilla asociada a cada interfaz.
• Para configurar todas las interfaces con los mismos ajustes, marque la casilla de la fila de encabezado.

8. En el menú Trust Mode, seleccione el modo de confianza:

• Disabled. La interfaz se considera que no es de confianza y podría usarse para lanzar un ataque a la red. Los mensajes del servidor DHCPv6 se comparan con la base de datos de enlaces. En los puertos que no son de confianza, DHCPv6 snooping aplica las siguientes reglas de seguridad:

- Se descartan los paquetes DHCPv6 de un servidor DHCPv6.
- Se descartan los mensajes DHCPv6 si la dirección MAC está en la base de datos de snooping pero la interfaz del enlace es distinta de la interfaz en la que se recibió el mensaje.
- Se descartan los paquetes DHCPv6 si la dirección MAC de origen no coincide con la dirección de hardware del cliente y la validación de direcciones MAC está habilitada globalmente.

• Enabled. La interfaz se considera de confianza y reenvía los mensajes del servidor DHCPv6 sin validación.

9. En el menú Invalid Packets, seleccione el modo de registro de paquetes. Si está habilitado, la función DHCPv6 snooping genera un mensaje de registro cuando la interfaz recibe y descarta un paquete no válido.

10. En el campo Rate Limit (pps), especifique el valor de límite de tasa para DHCPv6 snooping. Si la tasa de entrada de paquetes DHCPv6 por segundo supera el intervalo de ráfaga configurado por segundo, el puerto se apaga. Si el límite de tasa es None (valor predeterminado), el intervalo de ráfaga tampoco se aplica y la limitación de tasa está deshabilitada.

11. En el campo Burst Interval (secs), especifique el intervalo de ráfaga en segundos para la limitación de tasa en la interfaz.
Si el límite de tasa es N/A, el intervalo de ráfaga no se aplica.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Agregar un enlace DHCPv6 estático y mostrar los enlaces DHCPv6 dinámicos

Puede agregar un enlace estático a la base de datos de enlaces de DHCPv6 snooping y mostrar o borrar los enlaces dinámicos de la tabla de enlaces.

Para agregar un enlace DHCPv6 estático y mostrar o borrar los enlaces dinámicos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Binding Configuration. Se muestra la página Binding Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo MAC Address, especifique la dirección MAC del enlace que desea agregar. Es la clave de la base de datos de enlaces.

8. En el menú VLAN ID, seleccione el ID de la VLAN.
9. En el campo IPv6 Address, especifique la dirección IPv6 del enlace que desea agregar.

10. Haga clic en el botón Add.
La entrada de enlace de DHCPv6 snooping se agrega a la base de datos.

La tabla Dynamic Binding Configuration muestra información sobre los enlaces DHCPv6 aprendidos en cada interfaz con DHCPv6 snooping habilitado. La siguiente tabla describe la información de los enlaces dinámicos.

Campo	Descripción
Interface	La interfaz en la que se recibió el mensaje del cliente DHCPv6.
MAC Address	La dirección MAC asociada al cliente DHCPv6 que envió el mensaje. Es la clave de la base de datos de enlaces.

(Continuación)

Campo	Descripción
VLAN ID	El VLAN ID de la interfaz del cliente.
IPv6 Address	La dirección IPv6 asignada al cliente por el servidor DHCPv6.
Lease Time	El tiempo de concesión restante de la dirección IP del cliente.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para borrar todos los enlaces dinámicos de la tabla Dynamic Binding Configuration, haga clic en el botón Clear.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar un enlace DHCPv6 estático

Puede eliminar un enlace estático de la base de datos de enlaces de DHCPv6 snooping.

Para eliminar un enlace DHCPv6 estático:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Binding Configuration. Se muestra la página Binding Configuration.

6. En la tabla Static Binding Configuration, marque la casilla del enlace estático.

7. Haga clic en el botón Delete.
La entrada de enlace de DHCPv6 snooping se elimina de la base de datos.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el almacenamiento persistente de DHCPv6 snooping

Puede configurar la ubicación persistente de la base de datos de enlaces de DHCPv6 snooping. La base de datos se puede almacenar localmente en el switch o en un dispositivo remoto de la red. El switch debe poder alcanzar la dirección IP del dispositivo remoto para enviar enlaces a una base de datos remota.

Para configurar el almacenamiento persistente de DHCPv6 snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Persistent Configuration. Se muestra la página Persistent Configuration.

6. Especifique dónde se ubica la base de datos de enlaces de DHCPv6 snooping.

- Local: La tabla de enlaces se almacena localmente en el switch.
- Remote: La tabla de enlaces se almacena en un servidor TFTP remoto. Si la base de datos se almacena en un servidor remoto, especifique la siguiente información:
  - Remote IP Address: Especifique la dirección IP del servidor TFTP.
  - Remote File Name: Especifique el nombre de archivo de la base de datos de enlaces de DHCPv6 snooping en la que se almacenan los enlaces.

7. En el campo Write Delay, especifique el tiempo que el switch debe esperar después de escribir la información de enlaces en el almacenamiento persistente.
El retardo permite al switch reunir tantas entradas como sea posible (nuevas y eliminadas) antes de escribirlas en el archivo persistente. Puede especificar de 15 a 86400 segundos. De forma predeterminada, el retardo es de 300 segundos.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar o borrar las estadísticas de DHCPv6 snooping

Puede mostrar y borrar las estadísticas por interfaz de los mensajes DHCPv6 filtrados por la función DHCPv6 snooping en interfaces que no son de confianza.

Para mostrar o borrar las estadísticas de DHCPv6 snooping:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > DHCPv6 Snooping > Statistics. Se muestra la página Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Haga clic en el botón Clear para borrar las estadísticas de todas las interfaces.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe las estadísticas de DHCPv6 snooping.

Tabla 156. Información de estadísticas de DHCPv6 Snooping

Campo	Descripción
MAC Verify Failures	El número de mensajes DHCPv6 descartados porque la dirección MAC de origen y la dirección de hardware del cliente no coincidían. La verificación de direcciones MAC solo se realiza si está habilitada globalmente.
Client Ifc Mismatch	El número de paquetes descartados por DHCPv6 snooping porque la interfaz y la VLAN en las que se recibió el paquete no coinciden con la información de interfaz y VLAN del cliente almacenada en la base de datos de enlaces.
DHCPv6 Server Msgs	El número de mensajes del servidor DHCPv6 descartados en un puerto que no es de confianza.

Interfaces de IP source guard

Puede configurar IP source guard (IPSG) en interfaces individuales. IPSG es una función de seguridad que filtra los paquetes IP según el ID de origen. Esta función ayuda a proteger la red de ataques que usan suplantación de direcciones IP para comprometer o saturar la red. El ID de origen puede ser la dirección IP de origen o una combinación de dirección IP de origen y dirección MAC de origen, denominada par. La base de datos de enlaces de DHCP snooping, junto con las entradas IPSG de la base de datos, identifica los ID de origen autorizados.

Si habilita IPSG en un puerto con DHCP snooping deshabilitado, o con DHCP snooping habilitado pero que no es de confianza, se descarta todo el tráfico IP recibido en ese puerto. Además, IPSG interactúa con la seguridad de puertos (consulte Seguridad de puertos en la página 567) para verificar la dirección MAC de origen de los paquetes entrantes. La seguridad de puertos controla cómo se aprenden las direcciones MAC de origen en la base de datos de reenvío de capa 2 (la tabla de direcciones MAC). Si un puerto recibe una trama con una dirección MAC de origen no aprendida, la seguridad de puertos usa IPSG para determinar si la dirección MAC pertenece a un enlace válido.

Configurar IP source guard en una interfaz

Puede configurar IP source guard en interfaces individuales.

Para configurar IP source guard en una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > IP Source Guard > Interface Configuration. Se muestra la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

• 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
• LAG: Solo se muestran los LAG.
• All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

• Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
• Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
• Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú IPSG Mode, especifique el modo administrativo de IPSG en la interfaz:

• Enable: IPSG está habilitado en la interfaz. Si la dirección IP de origen no está en la base de datos de enlaces de DHCP snooping, los paquetes no se reenvían.
• Disable: IPSG está deshabilitado en la interfaz. El valor predeterminado es Disable.

9. En el menú IPSG Port Security, especifique el modo administrativo de la seguridad de puertos de IPSG en la interfaz:

• Enable: La seguridad de puertos de IPSG está habilitada en la interfaz. Los paquetes no se reenvían si la dirección MAC de origen no está en la tabla de la base de datos de reenvío ni en la base de datos de enlaces de DHCP snooping. Para aplicar el filtrado por dirección MAC, también debe configurar las siguientes funciones:

- Habilitar la seguridad de puertos globalmente (consulte Configurar el modo global de seguridad de puertos en la página 567).
- Habilitar la seguridad de puertos en la interfaz (consulte Configurar una interfaz de seguridad de puertos en la página 568).

• Disable: La seguridad de puertos de IPSG está deshabilitada en la interfaz. El valor predeterminado es Disable.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Agregar un enlace estático de IP source guard y mostrar los enlaces dinámicos de IP source guard

Puede agregar un enlace estático a la base de datos de enlaces de IP source guard (IPSG) y mostrar o borrar los enlaces dinámicos de la tabla de enlaces.

Para agregar un enlace IPSG estático y mostrar o borrar los enlaces dinámicos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > IP Source Guard > Binding Configuration. Se muestra la página Binding Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo MAC Address, especifique la dirección MAC del enlace que desea agregar. Es la clave de la base de datos de enlaces.

8. En el menú VLAN ID, seleccione el ID de la VLAN.
9. En el campo IP Address, especifique la dirección IP del enlace que desea agregar.

10. Haga clic en el botón Add.
La entrada de enlace estático IPSG se agrega a la base de datos.

El campo Filter Type indica si IPSG está configurado para funcionar solo con la dirección IP de origen o, si la seguridad de puertos también está habilitada para IPSG, con la dirección IP de origen y la dirección MAC.

La tabla Dynamic Binding Configuration muestra información sobre los enlaces IPSG aprendidos en cada interfaz con IPSG habilitado. La siguiente tabla describe la información de los enlaces dinámicos.

Campo	Descripción
Interface	La interfaz en la que se aprendió el enlace de origen IPSG.
MAC Address	La dirección MAC asociada al dispositivo de origen IPSG. Es la clave de la base de datos de enlaces.
VLAN ID	El VLAN ID de la interfaz del dispositivo de origen IPSG.
IP Address	La dirección IP del dispositivo de origen IPSG.
Filter Type	El tipo de filtro usado en la interfaz del switch. IPSG está configurado para funcionar solo con la dirección IP de origen o, si la seguridad de puertos también está habilitada para IPSG, con la dirección IP de origen y la dirección MAC.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para borrar todos los enlaces dinámicos de la tabla Dynamic Binding Configuration, haga clic en el botón Clear.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar un enlace estático de IP source guard

Puede eliminar un enlace estático de la base de datos de enlaces de IP source guard (IPSG).

Para eliminar un enlace IPSG estático:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > IP Source Guard > Binding Configuration.

Se muestra la página Binding Configuration.

6. En la tabla Static Binding Configuration, marque la casilla del enlace estático.

7. Haga clic en el botón Delete.
La entrada de enlace IPSG se elimina de la base de datos.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Interfaces de IPv6 source guard

Puede configurar IPv6 source guard (IPv6SG) en interfaces individuales. IPv6SG es una función de seguridad que filtra los paquetes IPv6 según el ID de origen. Esta función ayuda a proteger la red de ataques que usan suplantación de direcciones IPv6 para comprometer o saturar la red. El ID de origen puede ser la dirección IPv6 de origen o una combinación de dirección IPv6 de origen y dirección MAC de origen, denominada par. La base de datos de enlaces de DHCP snooping, junto con las entradas IPv6SG de la base de datos, identifica los ID de origen autorizados.

Si habilita IPv6SG en un puerto con DHCP snooping deshabilitado, o con DHCP snooping habilitado pero que no es de confianza, se descarta todo el tráfico IPv6 recibido en ese puerto. Además, IPv6SG interactúa con la seguridad de puertos (consulte Seguridad de puertos en la página 567) para verificar la dirección MAC de origen de los paquetes entrantes. La seguridad de puertos controla cómo se aprenden las direcciones MAC de origen en la base de datos de reenvío de capa 2 (la tabla de direcciones MAC). Si un puerto recibe una trama con una dirección MAC de origen no aprendida, la seguridad de puertos usa IPv6SG para determinar si la dirección MAC pertenece a un enlace válido.

Configurar IPv6 source guard en una interfaz

Puede configurar IPv6 source guard en interfaces individuales.

Para configurar IPv6 source guard en una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > IPv6 Source Guard > Interface Configuration. Se muestra la página Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú IPv6SG Mode, especifique el modo administrativo de IPv6SG en la interfaz:

- Enable: IPv6SG está habilitado en la interfaz. Si la dirección IPv6 de origen no está en la base de datos de enlaces de DHCP snooping, los paquetes no se reenvían.
- Disable: IPv6SG está deshabilitado en la interfaz. El valor predeterminado es Disable.

9. En el menú IPv6SG Port Security, especifique el modo administrativo de la seguridad de puertos de IPv6SG en la interfaz:

- Enable: La seguridad de puertos de IPv6SG está habilitada en la interfaz. Los paquetes no se reenvían si la dirección MAC de origen no está en la tabla de la base de datos de reenvío ni en la base de datos de enlaces de DHCP snooping. Para aplicar el filtrado por dirección MAC, también debe configurar las siguientes funciones:
  - Habilitar la seguridad de puertos globalmente (consulte Configurar el modo global de seguridad de puertos en la página 567).
  - Habilitar la seguridad de puertos en la interfaz (consulte Configurar una interfaz de seguridad de puertos en la página 568).
- Disable: La seguridad de puertos de IPv6SG está deshabilitada en la interfaz. El valor predeterminado es Disable.

10. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Agregar un enlace estático de IPv6 source guard y mostrar los enlaces dinámicos de IPv6 source guard

Puede agregar un enlace estático a la base de datos de enlaces de IPv6 source guard (IPv6SG) y mostrar o borrar los enlaces dinámicos de la tabla de enlaces.

Para agregar un enlace IPv6SG estático y mostrar o borrar los enlaces dinámicos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > IPv6 Source Guard > Binding Configuration. Se muestra la página Binding Configuration.

6. En el menú Interface, seleccione la interfaz.

7. En el campo MAC Address, especifique la dirección MAC del enlace que desea agregar. Es la clave de la base de datos de enlaces.

8. En el menú VLAN ID, seleccione el ID de la VLAN.
9. En el campo IPv6 Address, especifique la dirección IPv6 del enlace que desea agregar.

10. Haga clic en el botón Add.
La entrada de enlace estático IPv6SG se agrega a la base de datos.

El campo Filter Type indica si IPv6SG está configurado para funcionar solo con la dirección IPv6 de origen o, si la seguridad de puertos también está habilitada para IPv6SG, con la dirección IPv6 de origen y la dirección MAC.

La tabla Dynamic Binding Configuration muestra información sobre los enlaces IPv6SG aprendidos en cada interfaz con IPv6SG habilitado. La siguiente tabla describe la información de los enlaces dinámicos.

Campo	Descripción
Interface	La interfaz en la que se aprendió el enlace de origen IPv6SG.
MAC Address	La dirección MAC asociada al dispositivo de origen IPv6SG. Es la clave de la base de datos de enlaces.
VLAN ID	El VLAN ID de la interfaz del dispositivo de origen IPv6SG.
IPv6 Address	La dirección IPv6 del dispositivo de origen IPv6SG.
Filter Type	El tipo de filtro usado en la interfaz del switch. IPv6SG está configurado para funcionar solo con la dirección IPv6 de origen o, si la seguridad de puertos también está habilitada para IPv6SG, con la dirección IPv6 de origen y la dirección MAC.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

12. Para borrar todos los enlaces dinámicos de la tabla Dynamic Binding Configuration, haga clic en el botón Clear.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar un enlace estático de IPv6 source guard

Puede eliminar un enlace estático de la base de datos de enlaces de IPv6 source guard (IPv6SG).

Para eliminar un enlace IPv6SG estático:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > IPv6 Source Guard > Binding Configuration. Se muestra la página Binding Configuration.

6. En la tabla Static Binding Configuration, marque la casilla del enlace estático.
7. Haga clic en el botón Delete.

Se elimina la entrada de enlace IPv6SG de la base de datos.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Inspección dinámica de ARP

La inspección dinámica de ARP (DAI) es una función de seguridad que rechaza paquetes ARP no válidos y maliciosos. La función impide un tipo de ataque man-in-the-middle en el que una estación hostil intercepta el tráfico de otras estaciones envenenando las cachés ARP de sus vecinos desprevenidos. La estación hostil envía solicitudes o respuestas ARP que asocian la dirección IP de otra estación con su propia dirección MAC.

DAI depende de DHCP snooping. DHCP snooping escucha los intercambios de mensajes DHCP y crea una base de datos de enlaces con direcciones MAC, direcciones IP, interfaces VLAN válidas, etc.

Si DAI está habilitado y la dirección MAC e IP del remitente no coinciden con una entrada de la base de datos de enlaces de DHCP snooping, el switch descarta el paquete ARP. Sin embargo, también puede crear asignaciones estáticas en la base de datos de enlaces de DHCP snooping. Las asignaciones estáticas son útiles cuando los hosts usan direcciones IP estáticas, el switch no puede ejecutar DHCP snooping u otros switches de la red no ejecutan la inspección dinámica de ARP. Una asignación estática asocia una dirección IP con una dirección MAC en una VLAN.

Puede configurar VLAN, interfaces y listas de control de acceso (ACL) de DAI con sus reglas asociadas.

Configurar los ajustes globales de DAI

Puede configurar los ajustes globales de la inspección dinámica de ARP (DAI).

Para configurar los ajustes globales de DAI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI Configuration. Se muestra la página DAI Configuration.

6. Seleccione el botón de opción Validate Source MAC Disable o Enable. Esto especifica el modo de validación de MAC de origen de DAI para el switch. Si selecciona Enable, se habilita la validación de MAC del remitente en los paquetes ARP. El valor predeterminado es Disable.

7. Seleccione el botón de opción Validate Destination MAC Disable o Enable Esto especifica el modo de validación de MAC de destino de DAI para el switch. Si selecciona Enable, se habilita la validación de MAC de destino en los paquetes de respuesta ARP. El valor predeterminado es Disable.

8. Seleccione el botón de opción Validate IP Disable o Enable.
Esto especifica el modo de validación de IP de DAI para el switch. Si selecciona Enable, se habilita la validación de direcciones IP en los paquetes ARP. El valor predeterminado es Disable.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar VLAN de DAI

Puede configurar una o más VLAN de inspección dinámica de ARP (DAI).

Para configurar una o más VLAN de DAI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration. Se muestra la página DAI VLAN Configuration.

La tabla muestra las VLAN.

6. Marque la casilla de la VLAN.

7. En el menú Admin Mode, seleccione Enable o Disable para indicar si DAI está habilitado para la VLAN.
El valor predeterminado es Disable.

8. En el menú Invalid Packets, seleccione Enable o Disable para indicar si el registro de DAI está habilitado para la VLAN.
El valor predeterminado es Enable.

9. En el campo ARP ACL Name, especifique el nombre de una ACL ARP existente (consulte Crear una lista de control de acceso de DAI en la página 627).
La ACL ARP se usa para validar paquetes ARP. Para quitar un nombre de ACL ARP del campo ARP ACL Name, introduzca N/A.

10. En el menú Static Flag, seleccione Enable o Disable para indicar si el paquete ARP debe validarse con la base de datos de DHCP snooping cuando no coincide la regla de ACL ARP.
Si está habilitado, el paquete ARP se valida solo con la regla de ACL ARP. Si está deshabilitado, el paquete ARP requiere una validación adicional con la base de datos de DHCP snooping. El valor predeterminado es Disable.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Configurar interfaces de DAI

Puede configurar una o más interfaces de inspección dinámica de ARP (DAI).

Para configurar una o más interfaces de DAI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.
Se muestra la página DAI Interface Configuration.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1 (el ID de unidad del switch): Solo se muestran las interfaces físicas. Es la configuración predeterminada.
- LAG: Solo se muestran los LAG.
- All: Se muestran las interfaces físicas y los LAG.

7. Seleccione una o más interfaces mediante una de las siguientes acciones:

- Para configurar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.
- Para configurar varias interfaces con la misma configuración, marque la casilla asociada con cada interfaz.
- Para configurar todas las interfaces con la misma configuración, marque la casilla de la fila de encabezado.

8. En el menú Trust Mode, especifique si la interfaz es de confianza para DAI. Si está habilitado, la interfaz es de confianza y los paquetes ARP que entran por ella se reenvían sin verificación. Si está deshabilitado, la interfaz no es de confianza y los paquetes ARP que entran por ella se someten a DAI. El valor predeterminado es Disable.

9. En el campo Rate Limit (pps), especifique el límite de tasa para DAI. Si la tasa de paquetes ARP entrantes supera el valor especificado durante los segundos consecutivos del intervalo de ráfaga, los paquetes ARP se descartan. Si especifica N/A, no hay límite. El rango es de 0 a 300. El valor predeterminado es 15 paquetes por segundo (pps).

10. En el campo Burst Interval (secs), especifique el intervalo de ráfaga para el límite de tasa en la interfaz. Si especifica N/A, el intervalo de ráfaga no tiene efecto. El rango es de 1 a 15. El valor predeterminado es 1 segundo.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Crear una lista de control de acceso de DAI

Puede crear una lista de control de acceso (ACL) de inspección dinámica de ARP (DAI) a la que luego puede agregar reglas.

Para crear una ACL de DAI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI ACL Configuration. Se muestra la página DAI ACL Configuration.

6. En el campo Name, especifique un nombre de hasta 31 caracteres.

7. Haga clic en el botón Add.
Se agrega la ACL de DAI.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una regla para una ACL de DAI existente

Después de agregar una ACL de DAI (consulte Crear una lista de control de acceso de DAI en la página 627), puede configurar una regla para ella.

Para configurar una regla para una ACL de DAI existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.
Se muestra la página DAI ACL Rule Configuration.

6. En el menú ACL Name, seleccione la ACL de DAI para la que desea configurar la regla.

7. En el menú Action, seleccione la acción que debe ocurrir si un paquete cumple los criterios de la regla:

- Permit: el paquete se permite y se reenvía.
- Deny: el paquete se rechaza y se descarta.

8. En el campo Source IP Address, introduzca la dirección IP de origen que se usará como coincidencia para la regla.

9. En el campo Source MAC Address, introduzca la dirección MAC de origen que se usará como coincidencia para la regla.

10. Haga clic en el botón
Add. Se agrega la regla.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Eliminar una regla de una ACL de DAI existente

Puede eliminar una regla de una ACL de DAI existente.

Para eliminar una regla de una ACL de DAI existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.
Se muestra la página DAI ACL Rule Configuration.

6. En el menú ACL Name, seleccione la ACL de DAI de la que desea eliminar una regla.
7. Seleccione la casilla de la regla.

8. Haga clic en el botón
Delete. Se elimina la regla.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una lista de control de acceso de DAI

Puede eliminar una lista de control de acceso (ACL) de inspección dinámica de ARP (DAI) que ya no necesite.

Para eliminar una ACL de DAI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI ACL Configuration. Se muestra la página DAI ACL Configuration.

6. Seleccione la casilla de la ACL.

7. Haga clic en el botón Delete.
Se elimina la ACL de DAI.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar las estadísticas de DAI

Para mostrar las estadísticas de DAI:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Dynamic ARP Inspection > DAI Statistics. Se muestra la página DAI Statistic.

6. Para actualizar la página, haga clic en el botón Refresh.
7. Para borrar las estadísticas de DAI, haga clic en el botón Clear.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 157. Información de estadísticas de DAI

Campo	Descripción
VLAN	ID de la VLAN.
DHCP Drops	Número de paquetes ARP descartados por DAI porque no existe una entrada de enlace de DHCP snooping coincidente.
DHCP Permits	Número de paquetes ARP reenviados por DAI porque existe una entrada de enlace de DHCP snooping coincidente.
ACL Drops	Número de paquetes ARP descartados por DAI porque no existe una regla de ACL ARP coincidente para la VLAN y el indicador estático está activado en la VLAN.
ACL Permits	Número de paquetes ARP permitidos por DAI porque existe una regla de ACL ARP coincidente para la VLAN.

Tabla 157. Información de estadísticas de DAI (continuación)

Campo	Descripción
Bad Source MAC	Número de paquetes ARP descartados por DAI porque la dirección MAC del remitente en el paquete ARP no coincidía con la dirección MAC de origen del encabezado Ethernet.
Bad Dest MAC	Número de paquetes ARP descartados por DAI porque la dirección MAC de destino en los paquetes de respuesta ARP no coincidía con la dirección MAC de destino del encabezado Ethernet.
Invalid IP	Número de paquetes ARP descartados por DAI porque la dirección IP del remitente en los paquetes ARP o la dirección IP de destino en las respuestas ARP no es válida. Las direcciones no válidas incluyen 0.0.0.0, 255.255.255.255, direcciones IP multicast, direcciones de clase E (240.0.0.0/4) y direcciones loopback (127.0.0.0/8).
Forwarded	Número de paquetes ARP válidos reenviados por DAI.
Dropped	Número de paquetes ARP no válidos descartados por DAI.

Portales cautivos

La función de portal cautivo le permite impedir que los clientes accedan a la red hasta que se verifique el usuario. Puede configurar la verificación del portal cautivo para permitir el acceso a usuarios invitados y autenticados. Los usuarios autenticados deben validarse contra una base de datos de usuarios autorizados del portal cautivo antes de obtener acceso. La base de datos puede almacenarse localmente en el switch o en un servidor RADIUS.

El servidor de autenticación admite conexiones web HTTP y HTTPS. Además, puede configurar un portal cautivo para usar un puerto HTTP opcional (para redes con proxy HTTP). Si se configura, este puerto adicional lo usa exclusivamente el portal cautivo. Este puerto opcional se suma al puerto HTTP estándar 80, que se usa para todo el demás tráfico web.

Si habilita el portal cautivo en un puerto, el puerto descarta todo el tráfico de clientes no autenticados excepto los paquetes ARP, DHCP, DNS y NETBIOS, que se reenvían para que los clientes no autenticados puedan obtener una dirección IP y resolver nombres de host o de dominio. El tráfico de datos de los clientes autenticados pasa y las reglas no se aplican a esos paquetes.

En un puerto con el portal cautivo habilitado, si un cliente no autenticado abre un navegador web e intenta conectarse a la red, el portal cautivo redirige todo el tráfico HTTP y HTTPS de los clientes no autenticados al servidor de autenticación del switch. Se muestra una página web del portal cautivo al cliente no autenticado para que se autentique, tras lo cual obtiene acceso al puerto.

El portal cautivo no es compatible con interfaces VLAN, interfaces loopback ni interfaces lógicas. El portal cautivo usa autenticación basada en direcciones MAC

y no basada en puertos. Esto significa que todos los clientes conectados a la interfaz del portal cautivo deben autenticarse antes de obtener acceso a la red.

Configurar los ajustes globales del portal cautivo

Puede controlar el estado administrativo de la función de portal cautivo y configurar ajustes globales que afectan a todos los portales cautivos que configure en el switch.

Para configurar los ajustes globales del portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Global Configuration. Se muestra la página CP Global Configuration.

6. Seleccione el botón de opción Admin Mode Disable o Enable.
Esto define el modo administrativo de la función de portal cautivo. El valor predeterminado es Disable.

7. En el campo Additional HTTP Port, introduzca un número de puerto de 0 a 65535, excepto el 80.
El tráfico HTTP usa el puerto estándar 80, pero puede configurar un puerto adicional para el tráfico HTTP. El valor predeterminado es 0, que deshabilita esta opción.

8. En el campo Additional HTTP Secure Port, introduzca un número de puerto de 0 a 65535, excepto el 443.
El tráfico HTTP Secure (HTTPS) usa el puerto estándar 443, pero puede configurar un puerto adicional para el tráfico HTTPS. El valor predeterminado es 0, que deshabilita esta opción.

9. En el campo Authentication Timeout, introduzca el número de segundos que una sesión de autenticación permanece abierta mientras un cliente intenta acceder a la red a través de un portal cautivo.

Para acceder a la red mediante un portal cautivo, el cliente primero debe introducir sus datos de autenticación en una página web de autenticación. Cuando expira el tiempo de espera de la sesión y el cliente aún no se ha autenticado, el switch desconecta cualquier conexión TCP o SSL activa con el cliente. El rango es de 60 a 600 segundos. El valor predeterminado es 300 segundos.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe la información no configurable de la página.

Tabla 158. Información de configuración global del portal cautivo

Campo	Descripción
Operational Status	Estado operativo de la función de portal cautivo: Enabled o Disabled.
Disabled Reason	Si la función de portal cautivo está deshabilitada, el motivo: • Administrator Disabled • IP Address Not Configured • No IP Routing Interface • Routing Disabled
CP IP Address	Dirección IP que usa el portal cautivo.
Supported Captive Portals	Número total de portales cautivos admitidos en el switch.
Configured Captive Portals	Número de portales cautivos configurados en el switch.
Active Captive Portals	Número de portales cautivos habilitados operativamente (activos).
System Supported Users	Número total de usuarios que pueden autenticarse local y remotamente en el switch.
Local Supported Users	Número total de usuarios que pueden autenticarse localmente en el switch.
Configured Local Users	Número de usuarios locales configurados en el switch.
Authenticated Users	Número de usuarios autenticados en todos los portales cautivos del switch.

Configurar un portal cautivo

De forma predeterminada, el switch ofrece un portal cautivo predeterminado. Puede cambiar su configuración. También puede agregar y configurar hasta nueve portales adicionales.

Para configurar una instancia de portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Configuration. Se muestra la página CP Configuration.

6. Realice una de las siguientes acciones:

- Cambiar el portal cautivo predeterminado: junto al campo CP ID, seleccione la casilla 1.
- Agregar un portal cautivo nuevo: en el menú CP ID, seleccione un ID de 2 a 10.
- Cambiar un portal cautivo que agregó antes: junto al campo CP ID, seleccione la casilla asociada a ese portal cautivo.

7. En el campo CP Name, especifique un nombre para el portal cautivo. El nombre puede tener hasta 31 caracteres alfanuméricos.

8. En el menú Admin Mode, seleccione Enable o Disable.
Esto define el modo administrativo del portal cautivo. De forma predeterminada, un portal cautivo está deshabilitado.

9. En el campo Protocol, seleccione HTTP o HTTPS para la comunicación con los clientes durante la verificación:

- HTTP: no usa cifrado durante la verificación.
- HTTPS: usa Secure Sockets Layer (SSL), que requiere un certificado para el cifrado. El certificado se presenta al usuario al conectarse.

10. En el menú Verification, seleccione el tipo de autenticación de usuario que usa el portal cautivo cuando un cliente intenta conectarse:

- Guest: no se requiere autenticación de usuario.
- Local: el usuario se autentica mediante la base de datos local.
- RADIUS: el usuario se autentica mediante un servidor RADIUS.

11. Seleccione el estado de bloqueo, que permite controlar rápida y temporalmente un portal cautivo ante eventos inesperados, como ataques de denegación de servicio:

- Disable: la función de bloqueo está deshabilitada. No puede bloquear rápidamente el portal cautivo.
- Enable: el portal cautivo está bloqueado.
- Not Blocked: el portal cautivo no está bloqueado. El valor predeterminado es Not Blocked.

12. En el menú Group, seleccione un grupo de usuarios existente para el portal cautivo.
Todos los usuarios del grupo pueden acceder a la red a través del portal cautivo.

Esta opción solo está disponible si selecciona Local o RADIUS en el menú Verification.

13. En el campo Idle Timeout, introduzca el número de segundos que el switch espera antes de terminar una sesión inactiva y cerrar la sesión del usuario.
El rango es de 0 a 900 segundos. El valor predeterminado es 0 segundos, que significa que no se aplica el tiempo de espera.

14. En el menú User Logout, especifique si un cliente autenticado puede cerrar sesión en el portal cautivo y la red:

- Enable: el usuario puede cerrar sesión voluntariamente en el portal cautivo y la red.
- Disable: el usuario no puede cerrar sesión en el portal cautivo y la red, por lo que la conexión sigue autenticada hasta que el portal cautivo cancela la autenticación del usuario, por ejemplo, porque se supera el tiempo de inactividad o de sesión.

15. Si el modo de verificación es RADIUS (es decir, seleccionó RADIUS en el menú Verification), especifique la dirección IP del servidor RADIUS en el campo Radius Auth Server.

16. En el menú Redirect Mode, especifique si los clientes recién autenticados se redirigen a una URL:

- Enable: los clientes autenticados se redirigen a una URL que puede especificar en el campo Redirect URL.
- Disable: los clientes autenticados no se redirigen y se usa la página “welcome” local predeterminada. El valor predeterminado es Disable.

17. En el campo Redirect URL, especifique la URL a la que deben redirigirse los clientes recién autenticados.
La longitud máxima de la URL es de 512 caracteres alfanuméricos. La URL predeterminada es http://<ipaddress>/v1/security/captive_portal/cp_welcome.html.

Esta opción solo está disponible si selecciona Enable en el menú Redirect Mode.

18. En el campo Background Color, especifique el valor del color de fondo. El color predeterminado es #BFBFBF.

19. En el campo Foreground Color, especifique el valor del color de primer plano. El color predeterminado es #999999.

20. En el campo Separator Color, especifique el valor del color del separador. El color predeterminado es #B70024.

21. En el campo Max Bandwidth Down, especifique la tasa máxima a la que un cliente puede recibir datos de la red.
La tasa se expresa en bytes por segundo. El rango es de 0 a 536870911. El valor predeterminado es 0, que indica que no se aplica límite.

22. En el campo Max Bandwidth Up, especifique la tasa máxima a la que un cliente puede enviar datos a la red.
La tasa se expresa en bytes por segundo. El rango es de 0 a 536870911. El valor predeterminado es 0, que indica que no se aplica límite.

23. En el campo Max Input, especifique el número máximo de octetos que un cliente puede recibir.
Al alcanzar este límite, el cliente se desconecta. El rango es de 0 a 4294967295. El valor predeterminado es 0, que indica que no se aplica límite.

24. En el campo Max Output, especifique el número máximo de octetos que un cliente puede transmitir.
Al alcanzar este límite, el cliente se desconecta. El rango es de 0 a 4294967295. El valor predeterminado es 0, que indica que no se aplica límite.

25. En el campo Max Total, especifique el número máximo de octetos que un cliente puede transferir, es decir, la suma de octetos transmitidos y recibidos. Al alcanzar este límite, el cliente se desconecta. El rango es de 0 a 4294967295. El valor predeterminado es 0, que indica que no se aplica límite.

26. Realice una de las siguientes acciones:

- Si agrega un portal cautivo nuevo, haga clic en el botón Add. Se guarda la configuración y se agrega el portal cautivo.
- Si cambia el portal cautivo predeterminado o uno que agregó antes, haga clic en el botón Apply.
  Se guarda la configuración.

27. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un portal cautivo

Puede eliminar un portal cautivo que ya no necesite.

Para eliminar un portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Configuration. Se muestra la página CP Configuration.

6. Seleccione la casilla del portal cautivo.

7. Haga clic en el botón Delete.
Se elimina el portal cautivo.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar un enlace de portal cautivo

Puede asociar un portal cautivo con una o más interfaces. Aunque puede asociar varias interfaces a un portal cautivo, cada interfaz solo puede asociarse a un portal cautivo.

Para configurar un enlace de portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Binding Configuration. Se muestra la página CP Binding Configuration.

6. En el menú CP ID, seleccione el portal cautivo. El campo CP Name muestra el nombre del portal cautivo.

7. Para agregar el portal cautivo seleccionado a un puerto, en la tabla Ports, haga clic en el puerto para que aparezca una marca de verificación.
Puede agregar el portal cautivo a varios puertos.

La tabla Ports muestra las interfaces disponibles para enlaces de portal cautivo.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar o eliminar enlaces en la tabla de enlaces del portal cautivo

Puede mostrar o eliminar vinculaciones de portales cautivos.

Para mostrar o eliminar vinculaciones de portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Binding Table.

Se muestra la página CP Binding Table. Esta tabla muestra las vinculaciones de portal cautivo a interfaz.

6. Para eliminar una vinculación de portal cautivo a interfaz, haga lo siguiente: a. Marque la casilla junto a la interfaz.
b. Haga clic en el botón Eliminar (Delete).

Se elimina la vinculación.

7. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

8. Para actualizar la página, haga clic en el botón Refresh.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 159. Información de vinculación de portal cautivo

Campo	Descripción
Interface	La interfaz a la que está vinculado el portal cautivo.
CP ID	El ID del portal cautivo.
Operational Status	Indica si el portal está activo en la interfaz (Disable o Enable).
Block Status	Indica si el portal cautivo está bloqueado temporalmente para la autenticación.
Authenticated Users	El número de usuarios autenticados mediante el portal cautivo en la interfaz.

Configurar grupos de portal cautivo

Los grupos de portal cautivo le permiten organizar a los usuarios del portal cautivo, lo cual es útil si un gran número de usuarios debe poder acceder a un portal cautivo. Después de agregar un grupo de portal cautivo, puede agregar usuarios al grupo.

De forma predeterminada, todos los usuarios del portal cautivo se agregan al grupo predeterminado con ID 1. Puede agregar hasta 10 grupos.

Agregar un grupo de portal cautivo Después de agregar un grupo de portal cautivo, puede agregar usuarios del portal cautivo al grupo (consulte Configurar usuarios del portal cautivo en la página 641). Para agregar un grupo de portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Group Configuration. Se muestra la página CP Group Configuration.

6. En el menú Group ID, seleccione un ID para el grupo.
Puede seleccionar un ID de 1 a 10.

7. En el campo Group Name, especifique un nombre para el grupo.
El nombre puede contener de 1 a 31 caracteres alfanuméricos.

8. Haga clic en el botón
Add. Se agrega el grupo.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar un grupo de portal cautivo Para eliminar un grupo de portal cautivo:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Group Configuration. Se muestra la página CP Group Configuration.

6. En el menú Group ID, seleccione un ID para el grupo.
Puede seleccionar un ID de 1 a 10.

7. Marque la casilla del grupo que desea eliminar.

8. Haga clic en el botón
Delete. Se elimina el grupo.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar usuarios del portal cautivo

Puede configurar los ajustes de los usuarios del portal cautivo y agregarlos a un grupo de portal cautivo. De forma predeterminada, todos los usuarios se agregan al grupo predeterminado con ID 1. Después de agregar un grupo de portal cautivo personalizado (consulte Configurar grupos de portal cautivo en la página 639), también puede asignar usuarios del portal cautivo al grupo personalizado.

Los ajustes que puede configurar para un usuario individual del portal cautivo incluyen una contraseña, períodos de tiempo de espera, anchos de banda y cantidades máximas de tráfico.

Agregar o modificar una cuenta de usuario del portal cautivo Para agregar o modificar una cuenta de usuario del portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP User Configuration. Se muestra la página CP User Configuration.

6. Si cambia la configuración de una cuenta de usuario existente, marque la casilla de la cuenta de usuario.
Si cambia la configuración, no puede cambiar el ID ni el nombre de usuario.

7. Si agrega una cuenta de usuario, en el campo User ID, especifique un ID de 1 a 99 para identificar al usuario.
Después de agregar la cuenta de usuario, no puede cambiar el ID.

8. Si agrega una cuenta de usuario, en el campo User Name, ingrese un nombre para la cuenta de usuario.
El nombre puede contener hasta 31 caracteres alfanuméricos. Después de agregar la cuenta de usuario, no puede cambiar el nombre.

9. En el menú Edit Password, seleccione si desea usar una contraseña o ninguna para la nueva cuenta de usuario:

• Enable: Los campos Password y Confirm Password se habilitan para que pueda especificar una contraseña única para la nueva cuenta de usuario:

- En el campo Password, especifique una contraseña de 8 a 64 caracteres.
- En el campo Confirm Password, vuelva a especificar la contraseña.

• Disable: Los campos Password y Confirm Password se ocultan y no puede especificar una contraseña para la nueva cuenta de usuario.

De forma predeterminada, la selección es Disable, lo que significa que no se usa contraseña y los campos de contraseña están ocultos.

10. En el menú Group, seleccione al menos un grupo de portal cautivo. Para asignar una cuenta de usuario a más de un grupo, presione la tecla Control y haga clic en cada grupo. De forma predeterminada, una nueva cuenta de usuario se asigna al grupo predeterminado con ID 1.

11. En el campo Session Timeout, ingrese el período en segundos que un usuario puede permanecer conectado a la red.
Cuando se excede el tiempo de espera de la sesión, se cierra automáticamente la sesión del usuario. El valor predeterminado es 0, lo que significa que la sesión no expira. El rango es de 0 a 86400 segundos.

12. En el campo Idle Timeout, ingrese el período en segundos que el switch espera antes de finalizar una sesión inactiva y cerrar la sesión del usuario.
El valor predeterminado es 0, lo que significa que una sesión inactiva no expira. El rango es de 0 a 900 segundos.

13. En el campo Max Bandwidth Down, ingrese la tasa máxima, en bits por segundo, a la que un cliente puede recibir datos de la red.
Un valor de 0 indica que se debe usar la configuración global. El rango es de 0 a 536870911 bps.

14. En el campo Max Bandwidth Up, ingrese la tasa máxima, en bits por segundo, a la que un cliente puede enviar datos a la red.
Un valor de 0 indica que se debe usar la configuración global. El rango es de 0 a 536870911 bps.

15. En el campo Max Input, ingrese el número de octetos que el usuario puede recibir. Al alcanzar este límite, el usuario se desconecta. Un valor de 0 indica que se debe usar el límite global. El rango es de 0 a 4294967295.

16. En el campo Max Output, ingrese el número de octetos que el usuario puede transmitir. Al alcanzar este límite, el usuario se desconecta. Un valor de 0 indica que se debe usar el límite global. El rango es de 0 a 4294967295.

17. En el campo Max Total, ingrese el número de bytes que el usuario puede transmitir y recibir.
El número máximo de octetos es la suma de los octetos transmitidos y recibidos. Al alcanzar este límite, el usuario se desconecta. Un valor de 0 indica que se debe usar el límite global. El rango es de 0 a 4294967295.

18. Realice una de las siguientes acciones:

- Si agrega una cuenta de usuario nueva, haga clic en el botón Add. Se guarda la configuración y se agrega la cuenta de usuario.
- Si cambia la configuración de una cuenta de usuario, haga clic en el botón Apply. Se guarda la configuración.

19. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una cuenta de usuario del portal cautivo Puede eliminar una cuenta de usuario del portal cautivo que ya no se necesite.
Para eliminar una cuenta de usuario del portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP User Configuration. Se muestra la página CP User Configuration.

6. Marque la casilla de la cuenta de usuario.

7. Haga clic en el botón Delete.
Se elimina la cuenta de usuario.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los indicadores de trap del portal cautivo

Puede especificar si el switch envía traps SNMP para las acciones que ocurren en el portal cautivo. De forma predeterminada, el switch no envía traps para las acciones que ocurren en el portal cautivo.

Para configurar los indicadores de trap del portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Trap Flags. Se muestra la página CP Trap Flags.

6. Configure los siguientes indicadores de trap:

- CP Trap Mode: Habilite o deshabilite el modo de trap del portal cautivo.
- Client Authentication Failure: Habilite o deshabilite el envío de un trap si un cliente no logra autenticarse en un portal cautivo.
- Client Connect: Habilite o deshabilite el envío de un trap si un cliente se autentica en un portal cautivo y se conecta a él.
- Client Database Full: Habilite o deshabilite el envío de un trap cada vez que no se puede agregar una entrada a la base de datos de clientes porque está llena.
- Client Disconnect: Habilite o deshabilite el envío de un trap si un cliente se desconecta de un portal cautivo.

De forma predeterminada, estos indicadores de trap están deshabilitados.

7. Haga clic en el botón Apply.

La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Mostrar o borrar las estadísticas de clientes del portal cautivo

Puede mostrar o borrar las estadísticas de clientes del portal cautivo, incluidas las estadísticas del tráfico enviado y recibido por cada cliente.

Para mostrar o borrar las estadísticas de clientes del portal cautivo:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Control > Captive Portal > CP Client. Se muestra la página CP Client.

6. Para buscar un usuario del portal cautivo por dirección MAC, especifique la dirección MAC y haga clic en el botón Go.
Si la entrada existe, se muestra la información del usuario del portal cautivo. Se requiere una coincidencia exacta.

7. Para actualizar la página, haga clic en el botón Refresh.
8. Para borrar las estadísticas de clientes del portal cautivo, haga clic en el botón Clear.
9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 160. Estadísticas de clientes del portal cautivo

Campo	Descripción
MAC Address	La dirección MAC del cliente.
IP Address Drops	La dirección IP del cliente.
Protocol	El protocolo de conexión, que puede ser HTTP o HTTPS.
Verification	El tipo de autenticación, que puede ser Guest, Local o RADIUS.
Session Time	El tiempo transcurrido desde que se autorizó al cliente.
Interface	La interfaz que usa el cliente.
CP ID	El ID del portal cautivo.
User Name	El nombre de usuario (o ID de invitado) del cliente conectado.
Bytes Received	El número total de bytes que recibió el cliente.
Bytes Transmitted	El número total de bytes que transmitió el cliente.
Packets Received	El número total de paquetes que recibió el cliente.
Packets Transmitted	El número total de paquetes que transmitió el cliente.

Listas de control de acceso

Las listas de control de acceso (ACL) garantizan que solo los usuarios autorizados puedan acceder a recursos específicos y bloquean cualquier intento no autorizado de llegar a los recursos de red. Las ACL se usan para controlar el flujo de tráfico, restringir contenidos, decidir qué tipos de tráfico se reenvían o bloquean, y proporcionar seguridad a la red. El switch admite un total de 100 ACL, que pueden ser una combinación de ACL MAC, ACL IPv4 básicas, ACL IPv4 extendidas y ACL IPv6.

Para configurar una ACL:

1. Cree un ID de ACL basado en IPv4, IPv6 o MAC.
2. Cree una regla y asígnela a un ID de ACL único.

3. Defina las reglas, que pueden identificar protocolos, direcciones IP y MAC de origen y destino, y otros criterios de coincidencia de paquetes.

4. Use el número de ID para asignar la ACL a un puerto o a un LAG. Para ver ejemplos de configuración de ACL, consulte Listas de control de acceso (ACL) en la página 768.

Usar el ACL Wizard para crear una ACL simple

El ACL Wizard le ayuda a crear una ACL simple y aplicarla a los puertos seleccionados de forma fácil y rápida. Primero, seleccione el tipo de ACL que usará al crear una ACL. Después, agregue una regla de ACL a esta ACL y aplique esta ACL a los puertos seleccionados.

Nota: Los pasos del siguiente procedimiento describen cómo crear una ACL basada en la dirección MAC de destino. Si selecciona otro tipo de ACL (por ejemplo, una ACL basada en una IPv4 de origen), la página muestra información diferente.

Usar el ACL Wizard para crear una ACL Para usar el ACL Wizard para crear una ACL:
1. Abra un navegador web.

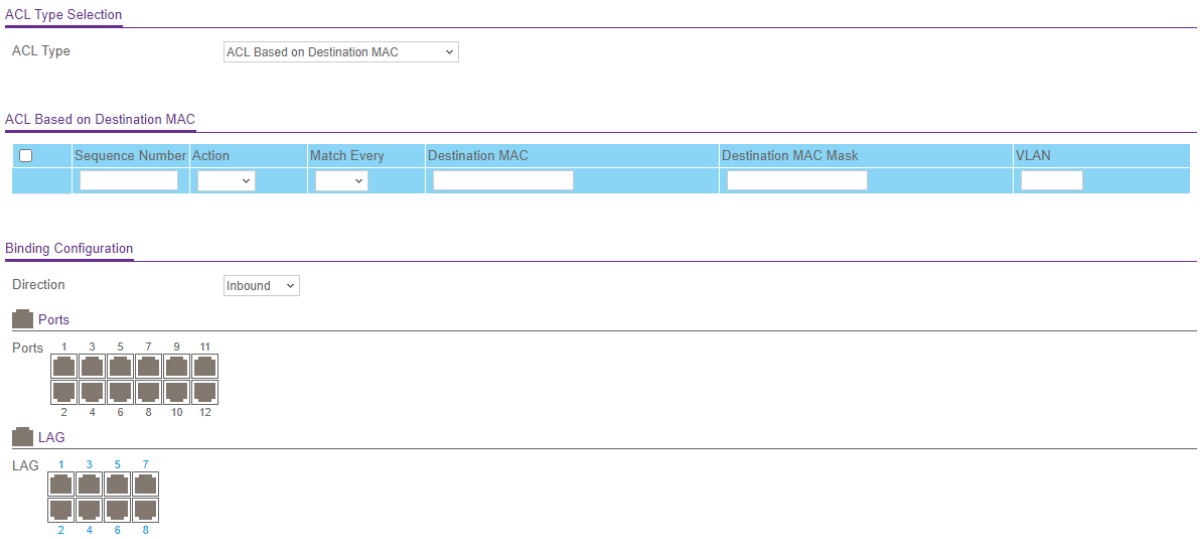
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > ACL Wizard.



La figura anterior muestra la página de un modelo de 12 puertos.

Nota: Los pasos de este procedimiento describen la creación de una ACL basada en la dirección MAC de destino. Si selecciona otro tipo de ACL, por ejemplo, una ACL basada en una IPv4 de origen, lo que se muestra en esta página varía según el paso actual del proceso de configuración de reglas.

6. En el menú ACL Type, seleccione el tipo de ACL.
Puede seleccionar entre los siguientes tipos de ACL:

- ACL Based on Destination MAC: Crea una ACL basada en la dirección MAC de destino, la máscara MAC de destino y la VLAN.
- ACL Based on Source MAC: Crea una ACL basada en la dirección MAC de origen, la máscara MAC de origen y la VLAN.
- ACL Based on Destination IPv4: Crea una ACL basada en la dirección IPv4 de destino y la máscara de dirección IPv4.
- ACL Based on Source IPv4: Crea una ACL basada en la dirección IPv4 de origen y la máscara de dirección IPv4.
- ACL Based on Destination IPv6: Crea una ACL basada en el prefijo IPv6 de destino y la longitud del prefijo IPv6.
- ACL Based on Source IPv6: Crea una ACL basada en el prefijo IPv6 de origen y la longitud del prefijo IPv6.
- ACL Based on Destination IPv4 L4 Port: Crea una ACL basada en el número de puerto de capa 4 IPv4 de destino.
- ACL Based on Source IPv4 L4 Port: Crea una ACL basada en el número de puerto de capa 4 IPv4 de origen.
- ACL Based on Destination IPv6 L4 Port: Crea una ACL basada en el número de puerto de capa 4 IPv6 de destino.
- ACL Based on Source IPv6 L4 Port: Crea una ACL basada en el número de puerto de capa 4 IPv6 de origen.

Nota: Para las opciones de puerto L4, se crean dos reglas (una para TCP y otra para UDP).

7. En el campo Sequence Number, ingrese un número entero en el rango de 1 a 2147483647 que se usa para identificar la regla.

8. En el menú Action, seleccione Permit o Deny para especificar la acción que debe aplicarse si un paquete coincide con los criterios de la regla.

9. En el menú Match Every, seleccione una de las siguientes opciones:

- False: No es necesario que los paquetes coincidan con la ACL y la regla seleccionadas. Con esta selección, puede agregar una dirección MAC de destino, una máscara MAC de destino y una VLAN.
- True: Todos los paquetes deben coincidir con la ACL y la regla seleccionadas y se permiten o se deniegan. En este caso, como todos los paquetes coinciden con la regla, no se ofrece la opción de configurar otros criterios de coincidencia.

10. Especifique los criterios de coincidencia adicionales para el tipo de ACL seleccionado. Los demás campos de criterios de coincidencia disponibles dependen del tipo de ACL seleccionado. Para obtener información sobre los posibles campos de criterios, consulte la siguiente tabla.

ACL basada en	Campos
Destination MAC	• Destination MAC: Especifique la dirección MAC de destino que se compara con una trama Ethernet. El formato es xx:xx:xx:xx:xx:xx. La palabra clave BPDU puede especificarse con una dirección MAC de destino de 01:80:C2:xx:xx:xx. • Destination MAC Mask: Especifique la máscara de dirección MAC de destino, que representa los bits de la dirección MAC de destino que se comparan con una trama Ethernet. El formato es xx:xx:xx:xx:xx:xx. La palabra clave BPDU puede especificarse con una máscara MAC de destino de 00:00:00:ff:ff:ff. • VLAN: Especifique el ID de VLAN que debe coincidir en la trama Ethernet.
Source MAC	• Source MAC: Especifique la dirección MAC de origen que se compara con una trama Ethernet. El formato es xx:xx:xx:xx:xx:xx. • Source MAC Mask: Especifique la máscara de dirección MAC de origen, que representa los bits de la dirección MAC de origen que se comparan con una trama Ethernet. El formato es (xx:xx:xx:xx:xx:xx). • VLAN: Especifique el ID de VLAN que debe coincidir en la trama Ethernet.
Destination IPv4	• Destination IP Address: Especifique la dirección IP de destino. • Destination IP Mask: Especifique la máscara de dirección IP de destino.
Source IPv4	• Source IP Address: Especifique la dirección IP de origen. • Source IP Mask: Especifique la máscara de dirección IP de origen.
Destination IPv6	• Destination Prefix: Especifique el prefijo de destino. • Destination Prefix Length: Especifique la longitud del prefijo de destino.
Source IPv6	• Source Prefix: Especifique el prefijo de origen. • Source Prefix Length: Especifique la longitud del prefijo de origen.
Destination IPv4 L4 Port	• Destination L4 port (protocol): Especifique el protocolo del puerto L4 IPv4 de destino. • Destination L4 port (value): Especifique el valor del puerto L4 IPv4 de destino.
Source IPv4 L4 Port	• Source L4 port (protocol): Especifique el protocolo del puerto L4 IPv4 de origen. • Source L4 port (value): Especifique el valor del puerto L4 IPv4 de origen.

(Continuación)

ACL basada en	Campos
Destination IPv6 L4 Port	• Destination L4 port (protocol): Especifique el protocolo del puerto L4 IPv6 de destino de destino. • Destination L4 port (value): Especifique el valor del puerto L4 IPv6 de destino.
Source IPv6 L4 Port	• Source L4 port (protocol): Especifique el protocolo del puerto L4 IPv6 de origen. • Source L4 port (value): Especifique el valor del puerto L4 IPv6 de origen.

11. A modo de ejemplo, los siguientes pasos describen cómo crear una ACL basada en la dirección MAC de destino:

a. En el campo Destination MAC, especifique la dirección MAC de destino que debe compararse con la información de una trama Ethernet.
El formato es xx:xx:xx:xx:xx:xx. La palabra clave BPDU puede especificarse con una dirección MAC de destino de 01:80:C2:xx:xx:xx.

b. En el campo Destination MAC Mask, especifique la máscara de dirección MAC de destino que debe compararse con la información de una trama Ethernet. El formato es xx:xx:xx:xx:xx:xx. La palabra clave BPDU puede especificarse con una máscara MAC de destino de 00:00:00:ff:ff:ff.

c. En el campo VLAN ID, especifique qué VLAN debe compararse con la información de una trama Ethernet.
El rango es de 1 a 4093. Se puede configurar un rango de VLAN o una VLAN.

12. En la sección Binding Configuration, en el menú Direction, seleccione la dirección de filtrado de paquetes de la ACL.

- Inbound: La vinculación MAC solo se puede aplicar al tráfico entrante.
- Outbound: La vinculación MAC solo se puede aplicar al tráfico saliente.

13. En las tablas Ports y LAG de la sección Binding Configuration, seleccione los puertos y LAG a los que debe aplicarse la ACL.

14. Haga clic en el botón Add.
Se agrega la regla a la ACL.

15. Haga clic en el botón Apply.
Se guarda la configuración.

16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Modificar una regla de ACL creada con el ACL Wizard Para modificar una regla de ACL creada con el ACL Wizard:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > ACL Wizard. Se muestra la página ACL Wizard.

6. Marque la casilla asociada con la regla.
7. Actualice los criterios de coincidencia según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una regla de ACL creada con el ACL Wizard Para eliminar una regla de ACL creada con el ACL Wizard:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

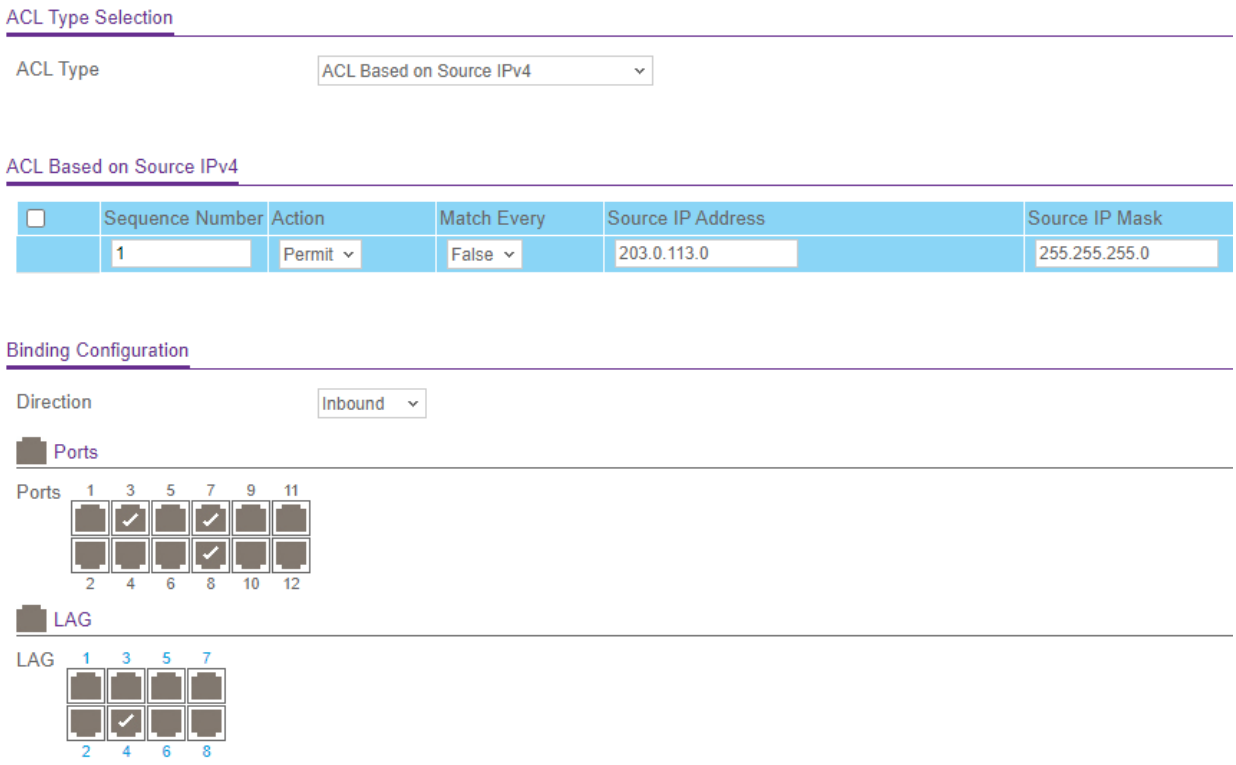
5. Seleccione Security > ACL > ACL
Wizard. Se muestra la página ACL Wizard.

6. Marque la casilla asociada con la regla.

7. Haga clic en el botón
Delete. Se elimina la regla.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Ejemplo de ACL Wizard En la siguiente figura, la regla de ACL está configurada para verificar coincidencias de paquetes en los puertos 3, 7 y 8 y en el LAG 4. Las interfaces pueden reenviar los paquetes que incluyen una dirección de origen en la red 203.0.113.0/24. Todos los demás paquetes se descartan porque cada ACL incluye una regla implícita deny all como última regla.



Para obtener información sobre el ACL Wizard, consulte Usar el ACL Wizard para crear una ACL simple en la página 647.

Configurar una ACL MAC

Una ACL MAC consiste en un conjunto de reglas que se comparan secuencialmente con un paquete. Cuando un paquete cumple los criterios de coincidencia de una regla, se aplica la acción especificada (Permit o Deny) y no se verifican las reglas adicionales.

Definir una ACL MAC y aplicarla al switch implica varios pasos:
1. Cree un ID de ACL MAC (consulte Agregar una ACL MAC en la página 654).
2. Cree una regla MAC (consulte Configurar reglas de ACL MAC en la página 656).

3. Asocie la ACL MAC con una o más interfaces (consulte Configurar vinculaciones MAC en la página 660).
Puede mostrar o eliminar configuraciones de ACL MAC en la tabla de vinculaciones MAC (consulte Mostrar o eliminar vinculaciones de ACL MAC en la tabla de vinculaciones MAC en la página 662).

Agregar una ACL MAC Para agregar una ACL MAC:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC ACL. Se muestra la página MAC ACL.

La tabla MAC ACL muestra el número de ACL configuradas actualmente en el switch y el número máximo de ACL que se pueden configurar. El tamaño actual es igual al número de ACL IPv4 e IPv6 configuradas más el número de ACL MAC configuradas.

6. En el campo Name, especifique un nombre para la ACL MAC.
El nombre solo puede incluir caracteres alfabéticos, numéricos, guiones, guiones bajos o espacios. El nombre debe comenzar con un carácter alfabético.

7. Haga clic en el botón Add.
Se agrega la ACL MAC.

Cada ACL configurada muestra la siguiente información:

- Rules: El número de reglas configuradas actualmente para la ACL MAC.
- Direction: La dirección del tráfico de paquetes afectado por la ACL MAC, que puede ser Inbound o estar en blanco. (Si la ACL no está vinculada a una interfaz, la dirección está en blanco).

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar el nombre de una ACL MAC Para cambiar el nombre de una ACL MAC:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC ACL. Se muestra la página MAC ACL.

6. Marque la casilla asociada con la ACL MAC.
7. En el campo Name, especifique el nuevo nombre.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una ACL MAC Para eliminar una ACL MAC:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC ACL.

Se muestra la página MAC ACL.

6. Marque la casilla asociada con la ACL MAC.

7. Haga clic en el botón Delete.
Se elimina la ACL MAC.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar reglas de ACL MAC

Puede definir reglas para ACL basadas en MAC. La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple los criterios se reenvía normalmente o se descarta. Una regla predeterminada deny all es la última regla de cada lista.

Agregar una regla a una ACL MAC Para agregar una regla a una ACL MAC:
1. Abra un navegador web.

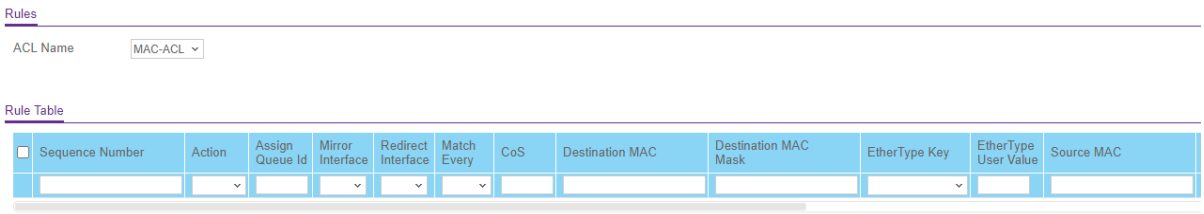
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC Rules.



6. En el menú ACL Name, seleccione la ACL MAC.

7. En el campo Sequence Number, ingrese un número entero en el rango de 1 a 2147483647 para identificar la regla.

8. En el menú Action, seleccione la acción que se realizará si un paquete cumple los criterios de la regla:

- Permit: Reenvía los paquetes que cumplen los criterios de la ACL.
- Deny: Descarta los paquetes que cumplen los criterios de la ACL.

9. En el campo Assign Queue, especifique el identificador de la cola de salida del hardware que se usará para manejar todos los paquetes que coincidan con esta regla de ACL.
El rango del ID de cola es de 0 a 7.

10. En el menú Mirror Interface, seleccione la interfaz de salida específica a la que se copiará el flujo de tráfico coincidente, además de reenviarse normalmente por el switch.
Este campo no se puede establecer si ya hay una interfaz de redirección configurada para la regla. Este campo aparece con la acción Permit.

11. En el menú Redirect Interface, seleccione la interfaz de salida a la que se redirigirá el flujo de tráfico coincidente, omitiendo cualquier decisión de reenvío que normalmente tome el switch. Este campo no se puede establecer si ya hay una interfaz de duplicación configurada para la regla.

12. En el menú Match Every, seleccione si cada paquete MAC de capa 2 debe compararse con la regla:

- True: Cada paquete debe coincidir con la regla de ACL seleccionada.
- False: No todos los paquetes deben coincidir con la regla de ACL seleccionada.

13. En el campo CoS, especifique la prioridad 802.1p que se comparará con la información de una trama Ethernet.
El rango de prioridad es de 0 a 7.

14. En el campo Destination MAC, especifique la dirección MAC de destino que se comparará con la información de una trama Ethernet.
El formato es xx:xx:xx:xx:xx:xx. La palabra clave BPDU puede especificarse con una dirección MAC de destino 01:80:C2:xx:xx:xx.

15. En el campo Destination MAC Mask, especifique la máscara de dirección MAC de destino que se comparará con la información de una trama Ethernet. El formato es xx:xx:xx:xx:xx:xx. La palabra clave BPDU puede especificarse con una máscara MAC de destino 00:00:00:ff:ff:ff.

16. En el menú EtherType Key, seleccione el valor EtherType que se comparará con la información de una trama Ethernet.
Los valores son los siguientes:

- **Apple Talk**
- **IBM SNA**
- **IPv4**

- **IPv6**
- **IPX**
- **MPLS Multicast**
- **MPLS Unicast**
- **NetBios**
- **Novell**
- **PPPOE**
- **RARP**
- **User Value**

17. Si selecciona User Value en el menú EtherType Key, en el campo EtherType User Value, especifique el valor EtherType personalizado que se usará. Este valor se compara con la información de una trama Ethernet. El rango es de 0x0600 a 0xFFFF.

18. En el campo Source MAC, especifique la dirección MAC de origen que se comparará con la información de una trama Ethernet.
El formato es xx:xx:xx:xx:xx:xx.

19. En el campo Source MAC Mask, especifique la máscara de dirección MAC de origen que se comparará con la información de una trama Ethernet.
El formato es xx:xx:xx:xx:xx:xx.

20. En el campo VLAN, especifique el ID de VLAN que se comparará con la información de una trama Ethernet.
El rango es de 1 a 4093. Puede configurar una sola VLAN o un rango de VLAN.

21. En el menú Logging, habilite o deshabilite el registro. Esta opción está disponible si en el menú Action se seleccionó Deny.

Si selecciona Enable, el registro se habilita para esta regla de ACL (sujeto a la disponibilidad de recursos del switch).

Si el indicador de trap de la lista de acceso también está habilitado, se generan traps periódicos que indican el número de veces que se invocó la regla durante el intervalo de informe, fijo en cinco minutos.

22. En el campo Rate Limit Conform Data Rate, especifique la velocidad de datos conforme, que es la velocidad a la que se limita el tráfico conforme. El rango es de 1 a 4294967295 Kbps.

23. En el campo Rate Limit Burst Size, especifique el tamaño de ráfaga, que es el tamaño hasta el cual se permiten ráfagas de tráfico por encima de la velocidad conforme. El rango es de 1 a 128 Kbps.

24. En el menú Time Range, opcionalmente, seleccione el nombre del programa de temporizador. Para información sobre programas de temporizador, consulte Programas de temporizador en la página 144.

El campo Rule Status de la tabla indica si la regla está activa o inactiva. En blanco significa que no hay ningún programa de temporizador asociado a la regla.

25. Haga clic en el botón
Add. Se agrega la regla.

26. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Cambiar los criterios de coincidencia de una regla MAC Para cambiar los criterios de una regla MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC Rules. Se muestra la página MAC Rules.

6. Seleccione la casilla asociada a la regla.
7. Modifique los campos según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una regla de una ACL MAC Para eliminar una regla de una ACL MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC Rules. Se muestra la página MAC Rules.

6. Seleccione la casilla asociada a la regla.

7. Haga clic en el botón
Delete. Se elimina la regla.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los enlaces (bindings) MAC

Cuando una ACL se enlaza a una interfaz, todas las reglas definidas se aplican a la interfaz seleccionada. Puede asignar ACL MAC a interfaces y LAG.

Para configurar el enlace MAC:

1. Abra un navegador web.

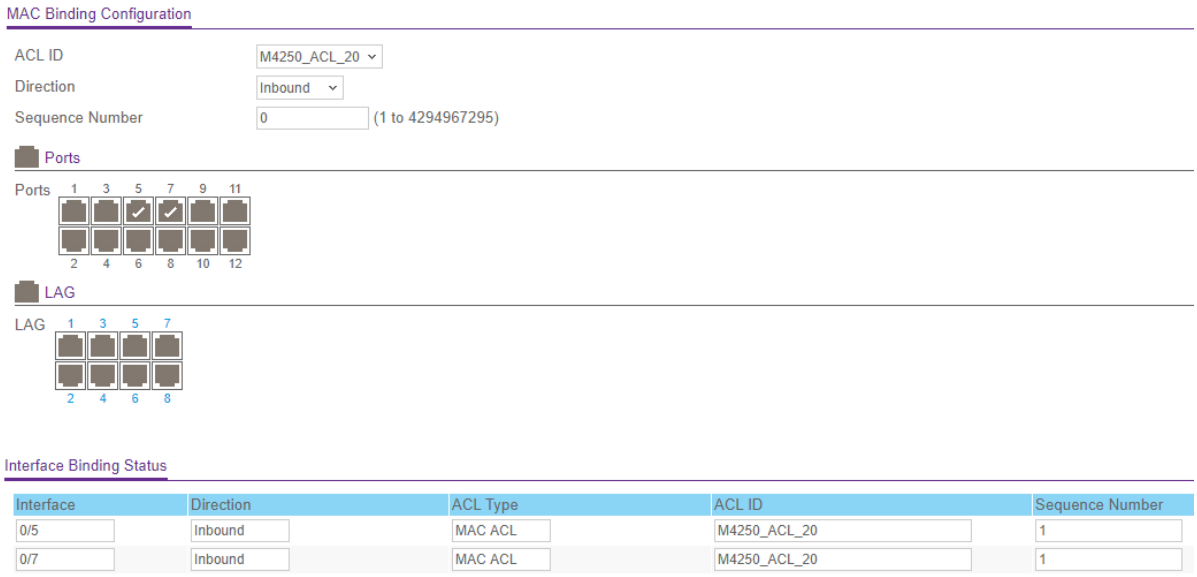
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > MAC Binding Configuration.



La figura anterior muestra la página de un modelo de 12 puertos e incluye algunos ejemplos.

6. En el menú ACL ID, seleccione una ACL.
7. En el menú Direction, seleccione la dirección del tráfico para el enlace MAC:

- Inbound: La vinculación MAC solo se puede aplicar al tráfico entrante.
- Outbound: La vinculación MAC solo se puede aplicar al tráfico saliente.

8. En el campo Sequence Number, opcionalmente, especifique un número que indique el orden de la lista de acceso respecto a otras listas ya asignadas a la interfaz y dirección.
Un número bajo indica mayor precedencia. Si un número de secuencia ya está en uso para la interfaz y dirección, la lista de acceso especificada reemplaza a la lista que usa ese número. Si no especifica el número de secuencia, se usa uno mayor en una unidad que el número de secuencia más alto en uso para la interfaz y dirección. El rango es de 1 a 4294967295.

9. Para agregar la ACL seleccionada a un puerto o LAG, en la tabla Ports o LAG, haga clic en el puerto o LAG para que aparezca una marca de verificación.
Puede agregar la ACL a varios puertos y LAG.

Las tablas Ports y LAG muestran las interfaces disponibles para enlaces de ACL.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe la información no configurable que se muestra.

Tabla 161. Información de Interface Binding Status

Campo	Descripción
Interface	La interfaz seleccionada.
Direction	La dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignado a la interfaz y dirección seleccionadas.
ACL ID	El número o nombre de la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL respecto a otras ACL asignadas a la interfaz y dirección seleccionadas.

Mostrar o eliminar enlaces de ACL MAC en la tabla de enlaces MAC

Puede mostrar o eliminar los enlaces de ACL MAC en la tabla de enlaces MAC.

Para mostrar o eliminar enlaces de ACL MAC:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Security > ACL > Basic > Binding Table.
Se muestra la página Binding Table. Esta tabla muestra los enlaces de ACL MAC a interfaces.

6. Para eliminar un enlace de ACL MAC a interfaz, haga lo siguiente: a. Marque la casilla junto a la interfaz. b. Haga clic en el botón Eliminar (Delete).

Se elimina la vinculación.

7. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información que se muestra en la tabla de enlaces MAC.

Tabla 162. Información de MAC Binding Table

Campo	Descripción
Interface	La interfaz de la ACL asignada.
Direction	La dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignado a la interfaz y dirección seleccionadas.
ACL ID	El nombre de la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL respecto a otras ACL asignadas a la interfaz y dirección seleccionadas.

Configurar una ACL IPv4 básica o extendida

Una ACL IPv4 consiste en un conjunto de reglas que se comparan secuencialmente con un paquete. Cuando un paquete cumple los criterios de una regla, se realiza la acción especificada (Permit o Deny) y no se evalúan las demás reglas. Debe especificar las interfaces a las que se aplica una ACL IPv4 y si se aplica al tráfico de entrada o de salida.

Definir una ACL IPv4 y aplicarla al switch implica varios pasos:

1. Agregue un ID de ACL IPv4 (consulte Agregar una ACL IPv4 en la página 664).
Las diferencias entre una ACL IPv4 básica y una extendida son las siguientes:

- ACL numerada de 1 a 99: Crea una ACL IPv4 básica, que le permite permitir o denegar el tráfico de una dirección IP de origen.
- ACL numerada de 100 a 199: Crea una ACL IPv4 extendida, que le permite permitir o denegar tipos específicos de tráfico de capa 3 o 4 de una dirección IP de origen a una de destino. Este tipo de ACL ofrece más granularidad y capacidad de filtrado que la ACL IP básica.
- ACL IP con nombre: Crea una ACL IPv4 extendida con un nombre de hasta 31 caracteres alfanuméricos. El nombre debe comenzar con un carácter alfabético.

2. Cree una regla IPv4 (consulte Configurar reglas para una ACL IP básica en la página 666 o Configurar reglas para una ACL IPv4 extendida en la página 671).

3. Asocie la ACL IPv4 a una o más interfaces (consulte Configurar los enlaces de ACL IP a interfaces en la página 688).
Puede mostrar o eliminar configuraciones de ACL IPv4 en la tabla IP ACL Binding (consulte Mostrar o eliminar enlaces de ACL IP en la tabla de enlaces de ACL IP en la página 690).

Agregar una ACL IPv4 Para agregar una ACL IPv4:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP ACL. Se muestra la página IP ACL.

La página IP ACL muestra el tamaño actual de la tabla de ACL en comparación con su tamaño máximo. El tamaño actual es igual al número de ACL IPv4 configuradas más el número de ACL MAC y ACL IPv6 configuradas. El número máximo de ACL en el switch es 100.

El campo Current Number of ACL muestra el número actual de ACL configuradas en el switch.

El campo Maximum ACL muestra el número máximo de ACL que puede configurar en el switch.

6. En el campo IP ACL ID, especifique el ID o el nombre de la ACL IP, según el tipo de ACL IP. El ID de ACL IP es un número entero en el siguiente rango:

• 1–99: Crea una ACL IP básica, que le permite permitir o denegar el tráfico de una dirección IP de origen.
• 100–199: Crea una ACL IP extendida, que le permite permitir o denegar tipos específicos de tráfico de capa 3 o 4 de una dirección IP de origen a una dirección IP de destino. Este tipo de ACL ofrece más granularidad y capacidad de filtrado que la ACL IP estándar.
• IP ACL Name: Crea una ACL IP extendida con un nombre de hasta 31 caracteres alfanuméricos. El nombre debe comenzar con un carácter alfabético.

Cada ACL configurada muestra la siguiente información:

- Rules: El número de reglas configuradas actualmente para la ACL IPv4.
- Type: Identifica la ACL como ACL IP básica (ID de 1 a 99), ACL IP extendida (ID de 100 a 199) o ACL con nombre (que también es extendida).

7. Haga clic en el botón
Add. Se agrega la ACL IP.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Cambiar el número o el nombre de una ACL IPv4 Para cambiar el número o el nombre de una ACL IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP
ACL. Se muestra la página IP ACL Configuration.

6. Seleccione la casilla asociada a la ACL IP.
7. En el campo IP ACL, especifique el nuevo número o nombre.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una ACL IPv4 Para eliminar una ACL IPv4:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP
ACL. Se muestra la página IP ACL Configuration.

6. Seleccione la casilla asociada a la ACL IP.

7. Haga clic en el botón
Delete. Se elimina la ACL IP.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar reglas para una ACL IP básica

Puede definir reglas para ACL estándar basadas en IP (ACL básicas). La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple los criterios se reenvía normalmente o se descarta.

Nota: Al final de una lista de ACL se incluye una regla implícita de denegar todo. Esto significa que si se aplica una ACL a un paquete y ninguna de las reglas explícitas coincide, se aplica la regla implícita final de denegar todo y el paquete se descarta.

Agregar una regla a una ACL IPv4 básica Para agregar una regla a una ACL IPv4 básica:
1. Abra un navegador web.

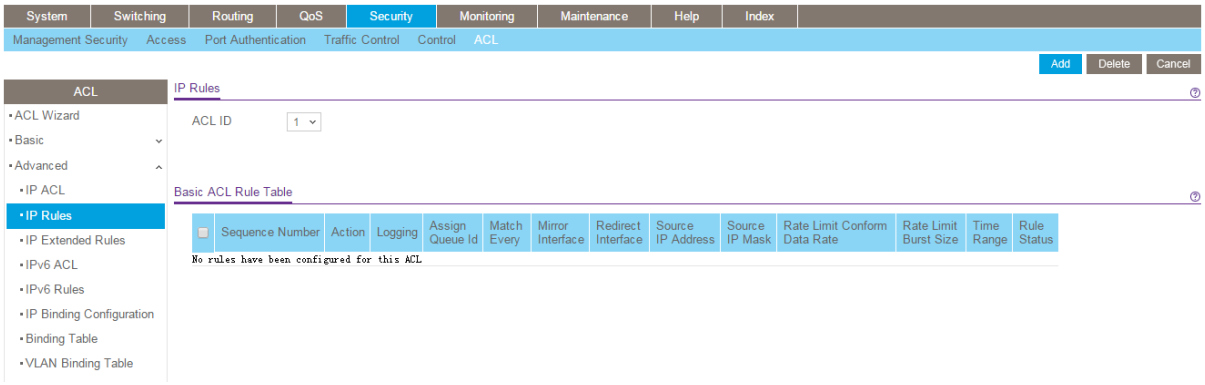
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

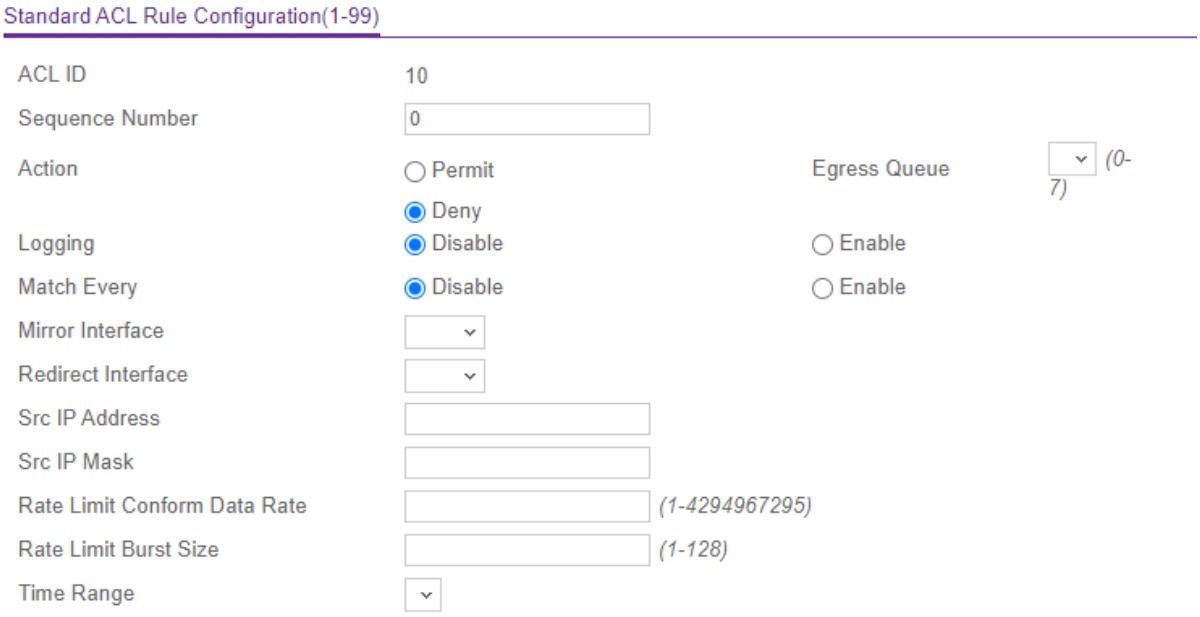
5. Seleccione Security > ACL > Advanced > IP Rules.



Si no hay reglas, la tabla Basic ACL Rule Table muestra el mensaje No rules have been configured for this ACL. Si existen una o más reglas para la ACL, se muestran en la tabla Basic ACL Rule Table.

6. En el menú ACL ID, seleccione la ACL IP a la que desea agregar o en la que desea cambiar una regla.
Para ACL IP básicas, debe ser un ID en el rango de 1 a 99.

7. Haga clic en el botón Add.



8. Especifique los siguientes criterios de coincidencia para la regla:

• Sequence Number: Introduzca un número de secuencia de ACL en el rango de 1 a 2147483647 que identifica la regla. Una ACL IP puede contener hasta 50 reglas.
• Action: Seleccione la acción de reenvío de la ACL, que puede ser una de las siguientes:

- Permit: Reenvía los paquetes que cumplen los criterios de la ACL.
  Egress Queue: Si en el menú Action se seleccionó Permit, puede especificar el identificador de la cola de salida del hardware que maneja todos los paquetes que coinciden con esta regla de ACL IP. El rango de ID de cola es de 0 a 7.
- Deny: Descarta los paquetes que cumplen los criterios de la ACL.
  Logging: Si en el menú Action se seleccionó Deny, puede habilitar el registro de la ACL seleccionando el botón de opción Enable. (El registro está sujeto a la disponibilidad de recursos del switch).

• Match Every: Seleccione uno de los botones de opción para especificar si todos los paquetes deben coincidir con la regla de ACL IP seleccionada:

- Enable: Todos los paquetes deben coincidir con la regla de ACL IP seleccionada y se permiten o se deniegan.
- Disable: No todos los paquetes deben coincidir con la regla de ACL IP seleccionada.

• Mirror Interface: En el menú, seleccione la interfaz de salida a la que se copiará el flujo de tráfico coincidente, además de reenviarse normalmente por el switch.

Puede seleccionar una interfaz de duplicación o una de redirección. Estas opciones son mutuamente excluyentes.
• Redirect Interface: En el menú, seleccione la interfaz de salida a la que se redirigirá el flujo de tráfico coincidente, omitiendo cualquier decisión de reenvío que normalmente tome el switch.
Puede seleccionar una interfaz de redirección o una de duplicación. Estas opciones son mutuamente excluyentes.
• Src IP Address: Especifique una dirección IP en notación decimal con puntos que se comparará con la dirección IP de origen del paquete como criterio de la regla de ACL IP seleccionada.
• Src IP Mask: Especifique la máscara IP en notación decimal con puntos que se usará con la dirección IP de origen.
• Rate Limit Conform Data Rate: Especifique la velocidad de datos conforme, que es la velocidad a la que se limita el tráfico conforme. El rango es de 1 a 4294967295 Kbps.
• Rate Limit Burst Size: Especifique el tamaño de ráfaga, que es el tamaño hasta el cual se permiten ráfagas de tráfico por encima de la velocidad conforme. El rango es de 1 a 128 Kbps.
• Time Range: En el menú Time Range, seleccione el programa de temporizador que se asociará a la regla. Para más información sobre programas de temporizador, consulte Programas de temporizador en la página 144. Si no configuró ningún programa, el menú no presenta opciones.

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Rule Status de la tabla indica si la regla está activa o inactiva. En blanco significa que no hay ningún programa de temporizador asociado a la regla.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Modificar los criterios de coincidencia de una regla de ACL IPv4 básica
Para modificar los criterios de una regla de ACL IPv4 básica:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP Rules. Se muestra la página IP Rules.

6. En el menú ACL ID, seleccione la ACL que incluye la regla que desea modificar.

7. En la tabla Basic ACL Rule Table, haga clic en la regla.
La regla es un hipervínculo. Se muestra la página Standard ACL Rule Configuration.

8. Modifique los criterios de la regla de ACL IP básica.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una regla de ACL IPv4 básica Para eliminar una regla de ACL IPv4 básica:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP Rules. Se muestra la página IP Rules.

6. En el menú ACL ID, seleccione la ACL que incluye la regla que desea modificar.
7. En la tabla Basic ACL Rule Table, seleccione la casilla asociada a la regla.

8. Haga clic en el botón
Delete. Se elimina la regla.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar reglas para una ACL IPv4 extendida

Puede definir reglas para ACL IPv4 extendidas. La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple los criterios se reenvía normalmente o se descarta.

Nota: Al final de una lista de ACL se incluye una regla implícita de denegar todo. Esto significa que si se aplica una ACL a un paquete y ninguna de las reglas explícitas coincide, se aplica la regla implícita final de denegar todo y el paquete se descarta.

Agregar una regla a una ACL IPv4 extendida Para agregar una regla a una ACL IPv4 extendida:
1. Abra un navegador web.

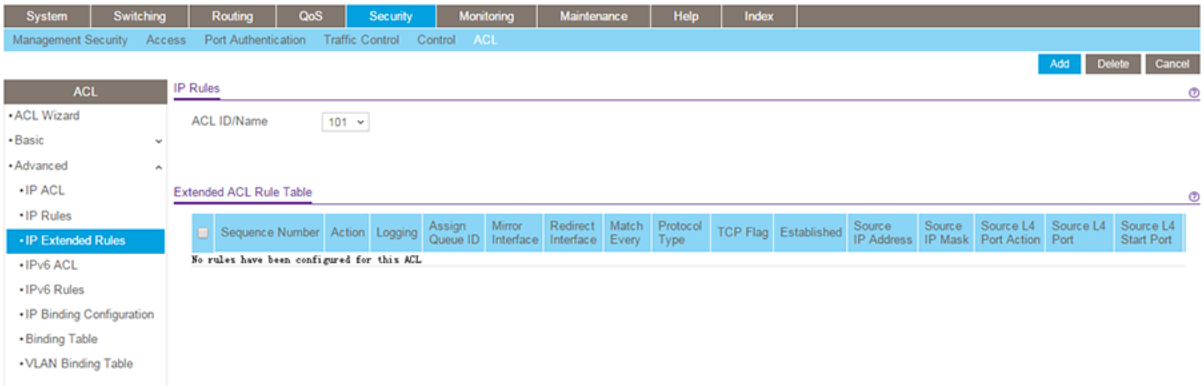
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

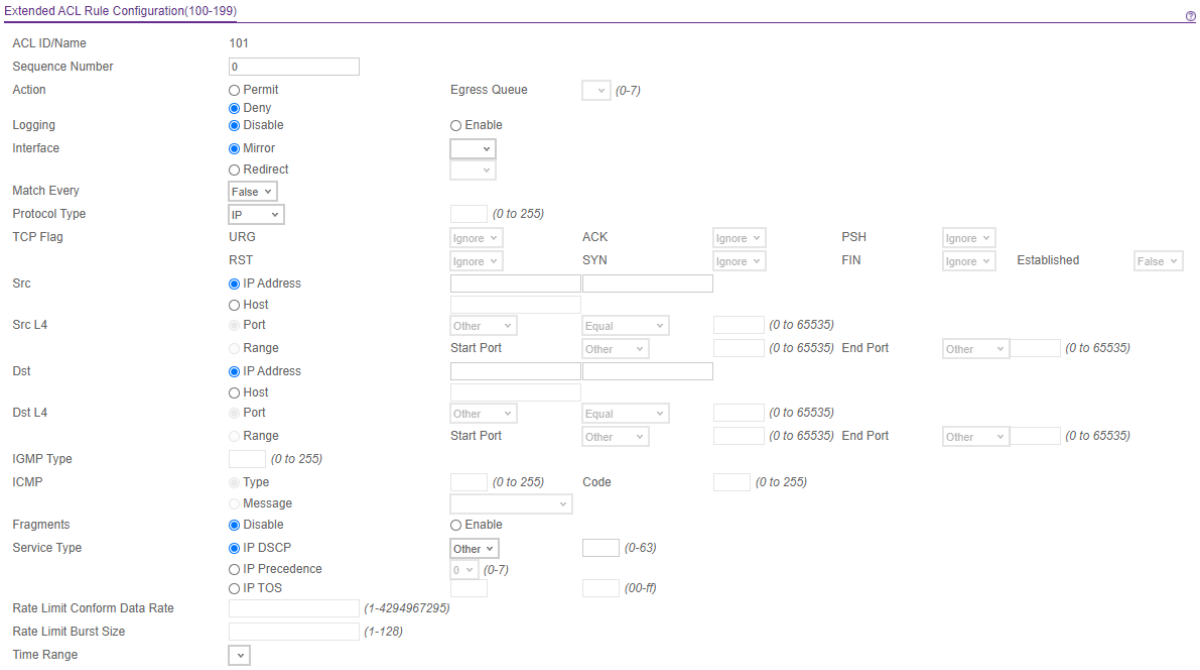
5. Seleccione Security > ACL > Advanced > IP Extended Rules.



Si no hay reglas, la tabla Extended ACL Rule Table muestra el mensaje No rules have been configured for this ACL. Si existen una o más reglas para la ACL, se muestran en la tabla Extended ACL Rule Table.

6. En el menú ACL ID/Name, seleccione la ACL IP a la que desea agregar una regla. Para ACL IP extendidas, debe ser un ID en el rango de 101 a 199 o un nombre.

7. Haga clic en el botón Add.



8. Configure las siguientes opciones para la regla:

• Sequence Number: Introduzca un número en el rango de 1 a 2147483647 que identifica la regla. Una ACL IP extendida puede contener hasta 1023 reglas.
• Action: Seleccione la acción de reenvío de la ACL, que puede ser una de las siguientes:

- Permit: Reenvía los paquetes que cumplen los criterios de la ACL.
  Egress Queue: Si en el menú Action se seleccionó Permit, seleccione el identificador de la cola de salida del hardware que maneja todos los paquetes que coinciden con esta regla de ACL IP. El rango de ID de cola es de 0 a 7.
- Deny: Descarta los paquetes que cumplen los criterios de la ACL.
  Esta opción está disponible si en el menú Action se seleccionó Deny.
  Si selecciona Enable, el registro se habilita para esta regla de ACL (sujeto a la disponibilidad de recursos del switch).
  Si el indicador de trap de la lista de acceso también está habilitado, se generan traps periódicos que indican el número de veces que se invocó la regla durante el intervalo de informe, fijo en cinco minutos.

• Interface: Para la acción Permit, use una interfaz de duplicación o una de redirección:

- Seleccione el botón de opción Mirror y use el menú para especificar la interfaz de salida a la que se copia el flujo de tráfico coincidente, además de reenviarse normalmente por el dispositivo.

- Seleccione el botón de opción Redirect y use el menú para especificar la interfaz de salida a la que se fuerza el flujo de tráfico coincidente, omitiendo cualquier decisión de reenvío que normalmente tome el dispositivo.

• Match Every: Seleccione uno de los botones de opción para especificar si todos los paquetes deben coincidir con la regla de ACL IP seleccionada:

- False: No todos los paquetes deben coincidir con la regla de ACL IP seleccionada. Puede configurar otros criterios de coincidencia en la página.
- True: Todos los paquetes deben coincidir con la regla de ACL IP seleccionada y se permiten o se deniegan. En este caso, no puede configurar otros criterios en la página.

• Protocol Type: En el menú, seleccione el protocolo con el que se comparará el protocolo IP del paquete: IP, ICMP, IGMP, TCP, UDP, EIGRP, GRE, IPINIP, OSPF, PIM o Other. Si selecciona Other, introduzca un número de protocolo de 0 a 255.
• TCP Flag: Si selecciona TCP en el menú Protocol Type, para cada indicador TCP puede especificar si el indicador TCP del paquete debe coincidir. Los indicadores TCP son URG, ACK, PSH, RST, SYN y FIN. Puede establecer cada indicador TCP por separado en una de las siguientes opciones:

- Ignore: Se ignora el indicador TCP del paquete. Es la configuración predeterminada.
- Set: Un paquete coincide con esta regla si el indicador TCP del paquete está activado.
- Clear: Un paquete coincide con esta regla si el indicador TCP del paquete no está activado.

Nota: Si los indicadores RST y ACK están activados, está disponible la opción Established, que indica que hay coincidencia si los bits RST o ACK están activados en el encabezado del paquete.

• Src: En el campo Src, introduzca una dirección IP de origen, en notación decimal con puntos, que se comparará con la dirección IP de origen del paquete como criterio de la regla de ACL IP seleccionada:

- Si selecciona el botón de opción IP Address, introduzca una dirección IP o un rango de direcciones IP. Puede introducir una máscara comodín para aplicar este criterio. Si este campo se deja vacío, significa cualquiera.
- Si selecciona el botón de opción Host, la máscara comodín se configura como 0.0.0.0. Si este campo se deja vacío, significa cualquiera.
  La máscara comodín determina qué bits se usan y cuáles se ignoran.
  Una máscara comodín de 0.0.0.0 indica que ninguno de los bits es importante. Una máscara de 255.255.255.255 indica que todos los bits son importantes.

• Src L4: Las opciones solo están disponibles si en el menú Protocol Type se seleccionó TCP o UDP. Use la opción de puerto L4 de origen para especificar condiciones de coincidencia de números de puerto L4 en la regla de ACL extendida.

Puede seleccionar el botón de opción Port o el botón de opción Range:

- Port: si selecciona el botón de opción Port, puede introducir usted mismo el número de puerto o seleccionar uno de los siguientes protocolos del menú:
  - Los protocolos de puerto TCP de IP de origen son Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3 y BGP.
  - Los protocolos de puerto UDP de IP de origen son Domain, Echo, SNMP, NTP, RIP, Time, Who y TFTP.

  Cada uno de estos valores se traduce en su número de puerto equivalente, que se usa como inicio y fin del rango de puertos.
  Seleccione Other en el menú para introducir un número de puerto. Si selecciona Other en el menú pero deja el campo vacío, significa cualquiera (any).
  Las condiciones de coincidencia aplicables a los números de puerto L4 son las siguientes:

  - Equal: la regla de ACL IP coincide si el número de puerto de origen de capa 4 es igual al número de puerto o clave de puerto especificado.
  - Not Equal: la regla de ACL IP coincide si el número de puerto de origen de capa 4 no es igual al número de puerto o clave de puerto especificado.
  - Less Than: la regla de ACL IP coincide si el número de puerto de origen de capa 4 es menor que el número de puerto o clave de puerto especificado.
  - Greater Than: la regla de ACL IP coincide si el número de puerto de origen de capa 4 es mayor que el número de puerto o clave de puerto especificado.

- Range: si selecciona el botón de opción Range, la regla de ACL IP coincide solo si el número de puerto de origen de capa 4 está dentro del rango especificado. El puerto inicial, el final y todos los intermedios forman parte del rango de puertos de capa 4. Los campos Start Port y End Port identifican el primer y el último puerto del rango. Los valores pueden ir de 0 a 65535.
  Puede introducir usted mismo el rango de puertos o seleccionar uno de los siguientes protocolos del menú:
  - Los protocolos de puerto TCP de IP de origen son Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3 y BGP.
  - Los protocolos de puerto UDP de IP de origen son Domain, Echo, SNMP, NTP, RIP, Time, Who y TFTP.

  Cada uno de estos valores se traduce en su número de puerto equivalente, que se usa como inicio y fin del rango de puertos. Seleccione Other en el menú para introducir un número de puerto. Si selecciona Other pero deja el campo vacío, significa cualquiera (any).

La máscara wildcard determina qué bits se usan y cuáles se ignoran. Una máscara wildcard de 0.0.0.0 indica que ninguno de los bits es importante. Una wildcard de 255.255.255.255 indica que todos los bits son importantes.

• Dst: en el campo Dst, introduzca una dirección IP de destino, en notación decimal con puntos, que se comparará con la dirección IP de destino del paquete como criterio de coincidencia de la regla de ACL IP seleccionada:

- Si selecciona el botón de opción IP Address, introduzca una dirección IP con su máscara wildcard para aplicar este criterio. Si deja este campo vacío, significa cualquiera.
- Si selecciona el botón de opción Host, la máscara comodín se configura como 0.0.0.0. Si este campo se deja vacío, significa cualquiera.
  La máscara comodín determina qué bits se usan y cuáles se ignoran.
  Una máscara comodín de 0.0.0.0 indica que ninguno de los bits es importante. Una máscara de 255.255.255.255 indica que todos los bits son importantes.

• Dst L4: las opciones solo están disponibles si en el menú Protocol Type se selecciona TCP o UDP. Use la opción de puerto L4 de destino para especificar las condiciones de coincidencia de los números de puerto L4 en la regla de ACL extendida. Puede seleccionar el botón de opción Port o el botón de opción Range:

- Port: si selecciona el botón de opción Port, puede introducir usted mismo el número de puerto o seleccionar uno de los siguientes protocolos del menú.
  - Los protocolos de puerto TCP de IP de destino son Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3 y BGP.
  - Los protocolos de puerto UDP de IP de destino son Domain, Echo, SNMP, NTP, RIP, Time, Who y TFTP.

  Cada uno de estos valores se traduce en su número de puerto equivalente, que se usa como inicio y fin del rango de puertos.
  Seleccione Other en el menú para introducir un número de puerto. Si selecciona Other en el menú pero deja el campo vacío, significa cualquiera (any).
  Las condiciones de coincidencia aplicables a los números de puerto L4 son las siguientes:

  - Equal: la regla de ACL IP coincide si el número de puerto de origen de capa 4 es igual al número de puerto o clave de puerto especificado.
  - Not Equal: la regla de ACL IP coincide si el número de puerto de origen de capa 4 no es igual al número de puerto o clave de puerto especificado.
  - Less Than: la regla de ACL IP coincide si el número de puerto de origen de capa 4 es menor que el número de puerto o clave de puerto especificado.
  - Greater Than: la regla de ACL IP coincide si el número de puerto de origen de capa 4 es mayor que el número de puerto o clave de puerto especificado.

- Range: si selecciona el botón de opción Range, la regla de ACL IP coincide solo si el número de puerto de destino de capa 4 está dentro del rango especificado. El puerto inicial, el final y todos los intermedios forman parte del rango de puertos de capa 4.
  Los campos Start Port y End Port identifican el primer y el último puerto del rango. Los valores pueden ir de 0 a 65535.
  Puede introducir usted mismo el rango de puertos o seleccionar uno de los siguientes protocolos del menú:
  - Los protocolos de puerto TCP de IP de destino son Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3 y BGP.
  - Los protocolos de puerto UDP de IP de destino son Domain, Echo, SNMP, NTP, RIP, Time, Who y TFTP.

  Cada uno de estos valores se traduce en su número de puerto equivalente, que se usa como inicio y fin del rango de puertos.
  Seleccione Other en el menú para introducir un número de puerto. Si selecciona Other en el menú pero deja el campo vacío, significa cualquiera (any).
  La máscara wildcard determina qué bits se usan y cuáles se ignoran. Una máscara wildcard de 0.0.0.0 indica que ninguno de los bits es importante. Una wildcard de 255.255.255.255 indica que todos los bits son importantes.

• IGMP Type: si en el menú Protocol Type seleccionó IGMP y especifica el tipo IGMP, la regla de ACL IP coincide con el tipo de mensaje IGMP especificado. El rango es de 0 a 255. Si deja este campo vacío, significa cualquiera.
• ICMP: si en el menú Protocol Type seleccionó ICMP, puede seleccionar el botón de opción Type o Message:

- Si selecciona el botón de opción Type, tenga en cuenta lo siguiente:
  - Los campos Type y Code solo se habilitan si el protocolo es ICMP. Use estos campos para especificar una condición de coincidencia para paquetes ICMP:
  - Si especifica información en el campo Type, la regla de ACL IP coincide con el tipo de mensaje ICMP especificado. El número de tipo puede ser de 0 a 255.
  - Si especifica información en el campo Code, la regla de ACL IP coincide con el código de mensaje ICMP especificado. El código puede ser de 0 a 255.
  - Si deja estos campos vacíos, significa cualquiera.

- Si selecciona el botón de opción Message, seleccione en el menú el tipo de mensaje ICMP que debe coincidir con la regla de ACL IP seleccionada. Especificar un tipo de mensaje implica especificar tanto el tipo ICMP como el código ICMP. El mensaje ICMP se decodifica en el tipo ICMP y el código ICMP correspondientes dentro del tipo ICMP.

Los tipos de mensaje ICMP de IPv4 son Echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, TTL-exceeded, time-exceeded y unreachable.

• Fragments: seleccione el botón de opción Enable para permitir fragmentos iniciales (es decir, con el bit de fragmento activado) o deje seleccionado el botón Disable predeterminado para impedir el uso de fragmentos iniciales.
Esta opción no es válida para reglas que coinciden con información L4, como un número de puerto TCP, ya que esa información se transporta en el paquete inicial.
• Service Type: seleccione una condición de coincidencia de tipo de servicio para la regla de ACL IP extendida. Los valores posibles son IP DSCP, IP precedence e IP TOS, que son métodos alternativos para especificar un criterio para el mismo campo de tipo de servicio del encabezado IP. Cada método usa una notación distinta. Después de hacer una selección, puede especificar los valores correspondientes.

- IP DSCP: configuración opcional. Especifique el campo IP DiffServ Code Point (DSCP). El DSCP se define como los 6 bits de orden superior del octeto de tipo de servicio del encabezado IP. Introduzca un entero de 0 a 63. Para seleccionar el IP DSCP, seleccione una de las palabras clave DSCP del menú. Para especificar un valor numérico, seleccione Other y aparecerá un campo en el que puede introducir el valor numérico del DSCP.
- IP Precedence: configuración opcional. El campo IP precedence de un paquete se define como los tres bits de orden superior del octeto de tipo de servicio del encabezado IP. Introduzca un entero de 0 a 7.
- IP TOS: configuración opcional. El campo IP ToS de un paquete se define como los 8 bits del octeto de tipo de servicio del encabezado IP. El valor de bits ToS es un número hexadecimal de 00 a 09 y de aa a ff. El valor de máscara ToS es un número hexadecimal de 00 a FF. La máscara ToS indica las posiciones de bits del valor de bits ToS que se usan para compararlo con el campo IP ToS de un paquete.
  Por ejemplo, para comprobar un valor IP ToS con el bit 7 activado como el más significativo, el bit 5 activado y el bit 1 desactivado, use un valor de bits ToS de 0xA0 y una máscara ToS de 0xFF.

• Rate Limit Conform Data Rate: especifique la velocidad de datos conforme, que es la velocidad a la que se limita el tráfico conforme. El rango es de 1 a 4294967295 Kbps.
• Rate Limit Burst Size: especifique el tamaño de ráfaga, que es el tamaño con el que se permiten ráfagas de tráfico por encima de la velocidad conforme. El rango es de 1 a 128 Kbps.
• Time Range: en el menú Time Range, seleccione la programación de temporizador que debe asociarse a la regla. Para obtener más información sobre las programaciones, consulte

Programaciones de temporizador en la página 144. Si no configuró ninguna programación, el menú no muestra opciones.

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Rule Status de la tabla indica si la regla está activa o inactiva. En blanco significa que no hay ningún programa de temporizador asociado a la regla.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Modificar los criterios de coincidencia de una regla de ACL IPv4 extendida Para modificar los criterios de coincidencia de una regla de ACL IPv4 extendida existente:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP Extended Rules. Se muestra la página IP Extended Rules.

6. En el menú ACL ID/Name, seleccione la ACL que incluye la regla que desea modificar.

7. En la tabla Extended ACL Rule Table, haga clic en la regla.
La regla es un hipervínculo. Se muestra la página Extended ACL Rule Configuration.

8. Modifique los criterios de la regla de ACL IP extendida.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una regla de ACL IPv4 extendida Para eliminar una regla de ACL IPv4 extendida:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP Extended Rules. Se muestra la página IP Extended Rules.

6. En el menú ACL ID/Name, seleccione la ACL que incluye la regla que desea eliminar.

7. En la tabla Extended ACL Rule Table, marque la casilla asociada a la regla.

8. Haga clic en el botón
Delete. Se elimina la regla.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar una ACL IPv6

Una ACL IPv6 consta de un conjunto de reglas que se comparan secuencialmente con un paquete. Cuando un paquete cumple los criterios de una regla, se aplica la acción especificada (Permit o Deny) y no se comprueban las demás reglas. Debe especificar las interfaces a las que se aplica una ACL IPv6, así como si se aplica al tráfico entrante o saliente.

Definir una ACL IPv6 y aplicarla al switch implica varios pasos:

1. Agregue un ID de ACL IPv6 (consulte Agregar una ACL IPv6 en la página 680). Una ACL IPv6 debe comenzar con una cadena de nombre de hasta 31 caracteres alfanuméricos. El nombre debe comenzar con una letra.

2. Cree una regla IPv6 (consulte Configurar reglas para una ACL IPv6 en la página 682).

3. Asocie la ACL IPv6 a una o más interfaces (consulte Configurar los enlaces de interfaz de ACL IP en la página 688).

Puede mostrar o eliminar configuraciones de ACL IPv6 en la tabla IP ACL Binding (consulte Mostrar o eliminar enlaces de ACL IP en la tabla de enlaces de ACL IP en la página 690).

Agregar una ACL IPv6 Para agregar una ACL IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IPv6 ACL. Se muestra la página IPv6 ACL.

6. En el campo IPv6 ACL, especifique un nombre para identificar la ACL IPv6. Es la cadena de nombre de la ACL IPv6, que admite solo hasta 31 caracteres alfanuméricos. El nombre debe comenzar con una letra.

7. Haga clic en el botón Add (Agregar).
La ACL IPv6 se agrega a la configuración del switch.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 163. Información de ACL IPv6

Campo	Descripción
Número actual de ACL	Número actual de ACL configuradas en el switch.
Máximo de ACL	Número máximo de ACL IP que se pueden configurar en el switch.

Tabla 163. Información de ACL IPv6 (continuación)

Campo	Descripción
Reglas	Número máximo de ACL que se pueden configurar en el switch.
Tipo	El tipo es IPv6 ACL.

Cambiar el nombre de una ACL IPv6 Para cambiar el nombre de una ACL IPv6:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IPv6 ACL. Se muestra la página IPv6 ACL.

6. Marque la casilla asociada a la ACL IPv6.
7. En el campo IPv6 ACL, especifique el nuevo nombre.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Eliminar una ACL IPv6 Para eliminar una ACL IPv6:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IPv6 ACL. Se muestra la página IPv6 ACL.

6. Marque la casilla asociada a la ACL IPv6.

7. Haga clic en el botón Delete (Eliminar). Se elimina la ACL IPv6.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar reglas para una ACL IPv6

Puede definir reglas para las ACL IPv6. La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple los criterios se reenvía normalmente o se descarta.

Agregar una regla para una ACL IPv6 Para agregar una regla para una ACL IPv6:

1. Abra un navegador web.

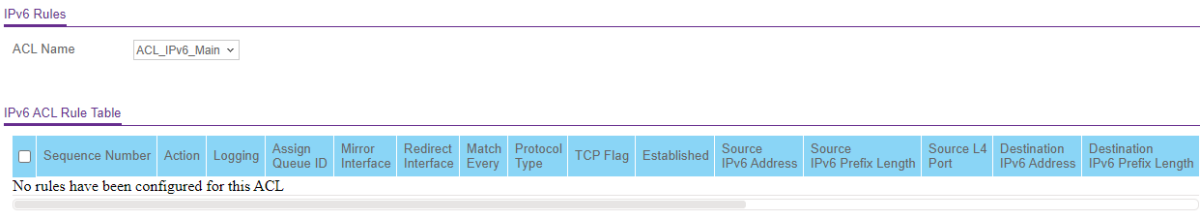
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

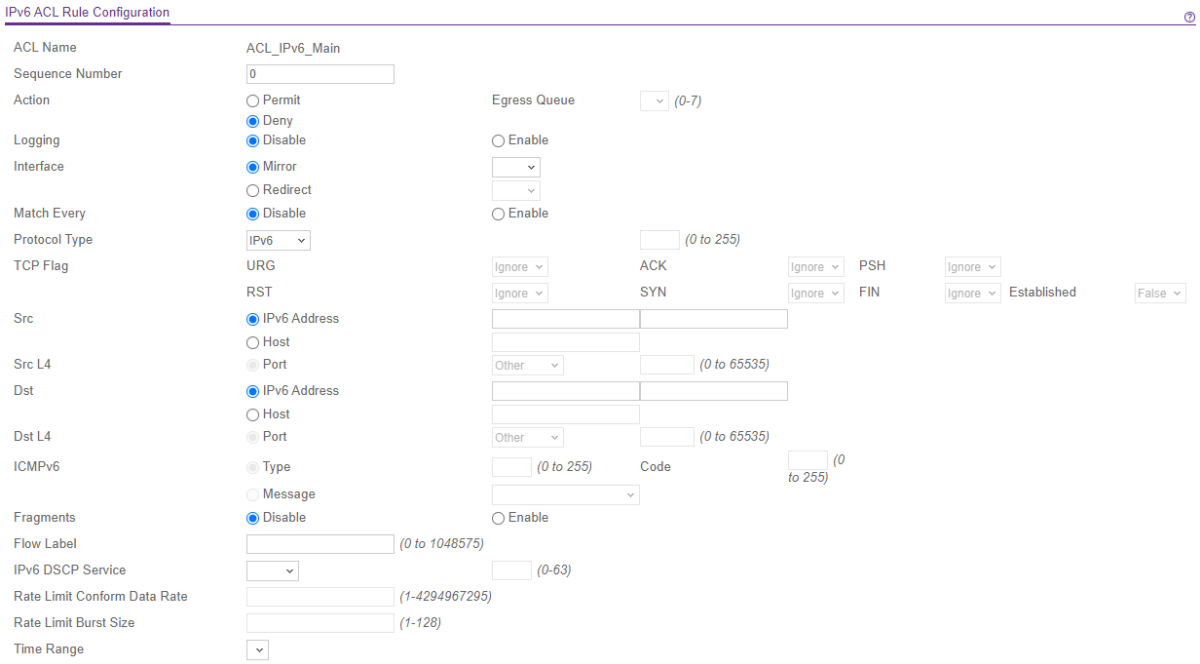
5. Seleccione Security > ACL > Advanced > IPv6 Rules.



Si no existen reglas, la tabla IPv6 ACL Rule Table muestra el mensaje No rules have been configured for this ACL. Si existen una o más reglas para la ACL, se muestran en la tabla IPv6 ACL Rule Table.

6. En el menú ACL Name, seleccione la ACL IPv6 para la que desea agregar o cambiar una regla.

7. Haga clic en el botón Add.



8. Configure las siguientes opciones para la regla:

• Sequence Number: introduzca un número entero de 1 a 2147483647. Este número identifica la regla. Una ACL IPv6 puede contener hasta 1023 reglas.
• Action: seleccione la acción de reenvío de la ACL mediante uno de los siguientes botones de opción:

- Permit: reenvía los paquetes que cumplen los criterios de la ACL.
- Deny: descarta los paquetes que cumplen los criterios de la ACL.

• Egress Queue: si selecciona el botón de opción Permit, seleccione el identificador de la cola de salida de hardware que se usa para todos los paquetes que coinciden con esta regla de ACL IPv6. El rango de ID de cola es de 0 a 7.
• Logging: si selecciona el botón de opción Deny, puede habilitar el registro de la ACL seleccionando el botón de opción Enable. (El registro depende de los recursos disponibles en el dispositivo).
Si el indicador de trap de lista de acceso también está habilitado, se generan traps periódicos que indican el número de veces que se invocó esta regla durante el intervalo de informe. El switch usa un intervalo de informe fijo de cinco minutos. No se emite un trap si el conteo de coincidencias de la regla es cero en el intervalo actual.

• Interface: si selecciona el botón de opción Permit, use una interfaz espejo o una interfaz de redirección:

- Seleccione el botón de opción Mirror Interface y use el menú para especificar la interfaz de salida a la que se copia el flujo de tráfico coincidente, además de reenviarse normalmente por el dispositivo.
- Seleccione el botón de opción Redirect Interface y use el menú para especificar la interfaz de salida a la que se fuerza el flujo de tráfico coincidente, omitiendo cualquier decisión de reenvío que normalmente toma el dispositivo.

• Match Every: seleccione si todos los paquetes deben coincidir con la regla de ACL IPv6 seleccionada:

- False: no todos los paquetes deben coincidir con la regla de ACL IPv6 seleccionada. Puede configurar otros criterios de coincidencia en la página.
- True: todos los paquetes deben coincidir con la regla de ACL IPv6 seleccionada y se permiten o deniegan. En este caso, no puede configurar otros criterios de coincidencia en la página.

• Protocol Type: especifique el tipo de protocolo IPv6 de una de las siguientes maneras:

- En el menú Protocol Type, seleccione IPv6, ICMPv6, TCP o UDP.
- En el menú Protocol Type, seleccione Other y, en el campo asociado, especifique un entero de 0 a 255. Este número representa el protocolo IPv6.

• TCP Flag: si selecciona TCP en el menú Protocol Type, para cada indicador TCP puede especificar si el indicador TCP del paquete debe coincidir o no. Los indicadores TCP son URG, ACK, PSH, RST, SYN y FIN. Puede establecer cada indicador TCP por separado en una de las siguientes opciones:

- Ignore: Se ignora el indicador TCP del paquete. Es la configuración predeterminada.
- Set: Un paquete coincide con esta regla si el indicador TCP del paquete está activado.
- Clear: Un paquete coincide con esta regla si el indicador TCP del paquete no está activado.

Nota: Si los indicadores RST y ACK están activados, está disponible la opción Established, que indica que hay coincidencia si los bits RST o ACK están activados en el encabezado del paquete.

• Src: en el campo Src, introduzca una dirección IPv6 de origen o un rango de direcciones IPv6 de origen que se comparará con la dirección IPv6 de origen del paquete como criterio de coincidencia de la regla de ACL IPv6 seleccionada:

- Si selecciona el botón de opción IPv6 Address, introduzca una dirección o un rango IPv6 para aplicar este criterio. Si deja este campo vacío, significa cualquiera.

- Si selecciona el botón de opción Host, introduzca una dirección IPv6 de origen de host que coincida con la dirección IPv6 especificada. Si deja este campo vacío, significa cualquiera.

El argumento de dirección IPv6 de origen debe tener el formato documentado en RFC 2373, en el que la dirección se especifica en números hexadecimales con valores de 16 bits separados por dos puntos.
• Src L4: las opciones solo están disponibles si en el menú Protocol Type se selecciona TCP o UDP. Use la opción de puerto L4 de origen para especificar las condiciones de coincidencia de los números de puerto L4 en la regla de ACL IPv6. Puede introducir usted mismo el número de puerto o seleccionar uno de los siguientes protocolos del menú:

- Los protocolos de puerto TCP de IP de origen son Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3 y BGP.
- Los protocolos de puerto UDP de IP de origen son Domain, Echo, SNMP, NTP, RIP, Time, Who y TFTP.

Cada uno de estos valores se traduce en su número de puerto equivalente, que se usa como inicio y fin del rango de puertos.
Seleccione Other en el menú para introducir un número de puerto. Si selecciona Other en el menú pero deja el campo vacío, significa cualquiera (any).
La única condición de coincidencia aplicable a los números de puerto L4 es igual. Esto significa que una regla de ACL IPv6 coincide solo si el número de puerto de origen de capa 4 es igual al número de puerto o protocolo de puerto especificado.
• Dst: en el campo Dst, introduzca una dirección IPv6 de destino que se comparará con la dirección IPv6 de destino del paquete como criterio de coincidencia de la regla de ACL IPv6 seleccionada:

- Si selecciona el botón de opción IPv6 Address, introduzca una dirección IPv6 para aplicar este criterio. Si deja este campo vacío, significa cualquiera.
- Si selecciona el botón de opción Host, introduzca una dirección IPv6 de origen de host que coincida con la dirección IPv6 especificada. Si deja este campo vacío, significa cualquiera.

El argumento de dirección IPv6 de origen debe tener el formato documentado en RFC 2373, en el que la dirección se especifica en números hexadecimales con valores de 16 bits separados por dos puntos.
• Dst L4: las opciones solo están disponibles si en el menú Protocol Type se selecciona TCP o UDP. Use la opción de puerto L4 de destino para especificar las condiciones de coincidencia de los números de puerto L4 en la regla de ACL IPv6. Puede introducir usted mismo el número de puerto o seleccionar uno de los siguientes protocolos del menú:

- Los protocolos de puerto TCP de IP de destino son Domain, Echo, FTP, FTP data, www-http, SMTP, Telnet, POP2, POP3 y BGP.
- Los protocolos de puerto UDP de IP de destino son Domain, Echo, SNMP, NTP, RIP, Time, Who y TFTP.

Cada uno de estos valores se traduce en su número de puerto equivalente, que se usa como inicio y fin del rango de puertos.
Seleccione Other en el menú para introducir un número de puerto. Si selecciona Other en el menú pero deja el campo vacío, significa cualquiera (any).
La única condición de coincidencia aplicable a los números de puerto L4 es igual. Esto significa que una regla de ACL IPv6 coincide solo si el número de puerto de destino de capa 4 es igual al número de puerto o protocolo de puerto especificado.
• ICMPv6: los campos Type y Message solo se habilitan si el protocolo es ICMPv6. Use estos campos para especificar una condición de coincidencia para paquetes ICMPv6. Seleccione el botón de opción Type o Message:

- Si selecciona el botón de opción Type, tenga en cuenta lo siguiente:
  - Los campos Type y Code solo se habilitan si el protocolo es ICMPv6. Use estos campos para especificar una condición de coincidencia para paquetes ICMPv6:
  - Si especifica información en el campo Type, la regla de ACL IPv6 coincide con el tipo de mensaje ICMPv6 especificado. El número de tipo puede ser de 0 a 255.
  - Si especifica información en el campo Code, la regla de ACL IPv6 coincide con el código de mensaje ICMPv6 especificado. El código puede ser de 0 a 255.
  - Si deja estos campos vacíos, significa cualquiera.
- Si selecciona el botón de opción Message, tenga en cuenta lo siguiente:
  - Seleccione el tipo de mensaje ICMPv6 que debe coincidir con la regla de ACL IPv6 seleccionada. Especificar un tipo de mensaje implica especificar tanto el tipo ICMPv6 como el código ICMPv6. El mensaje ICMPv6 se decodifica en el tipo ICMPv6 y el código ICMPv6 correspondientes dentro del tipo ICMP.
  - Los tipos de mensaje ISMPv6 son destination-unreachable, echo-reply, echo-request, header, hop-limit, MLD-query, MLD-reduction, MLD-report, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, unreachable, time-exceeded, nd-na y nd-ns.

• Fragments: seleccione el botón de opción Enable para permitir fragmentos iniciales (es decir, con el bit de fragmento activado) o deje seleccionado el botón Disable predeterminado para impedir el uso de fragmentos iniciales.
Esta opción no es válida para reglas que coinciden con información L4, como un número de puerto TCP, ya que esa información se transporta en el paquete inicial.
• Flow Label: el campo Flow Label solo se habilita si en el menú Protocol Type se selecciona ICMPv6. La etiqueta de flujo es un número de 20 bits único para un paquete IPv6 que usan las estaciones finales para indicar el tratamiento de calidad de servicio en los routers. El rango de la etiqueta de flujo es de 0 a 1048575.

• IPv6 DSCP Service: Especifique el campo IP DiffServ Code Point (DSCP). Esta configuración es opcional.
El DSCP se define como los seis bits de orden superior del octeto de tipo de servicio del encabezado IPv6. Ingrese un entero de 0 a 63. Para seleccionar el DSCP IPv6, elija una de las palabras clave DSCP. Para especificar un valor numérico, seleccione Other e ingrese el valor numérico del DSCP.
• Rate Limit Conform Data Rate: Especifique la velocidad de datos conforme, que es la velocidad a la que se limita el tráfico conforme. El rango es de 1 a 4294967295 Kbps.
• Rate Limit Burst Size: Especifique el tamaño de ráfaga, que es el tamaño hasta el que se permiten ráfagas de tráfico por encima de la velocidad conforme. El rango es de 1 a 128 Kbps.
• Time Range: En el menú Time Range, seleccione la programación de temporizador que se asociará con la regla. Para obtener más información, consulte Programaciones de temporizador en la página 144. Si no configuró ninguna, el menú no presenta opciones.

9. Haga clic en el botón Apply.
Se guarda la configuración.

El campo Rule Status de la tabla indica si la regla está activa o inactiva. En blanco significa que no hay ningún programa de temporizador asociado a la regla.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Modificar los criterios de coincidencia de una regla de ACL IPv6 Para modificar los criterios de coincidencia de una regla de ACL IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IPv6 Rules. Se muestra la página IPv6 Rules.

6. En el menú ACL Name, seleccione la ACL que incluye la regla que desea modificar.

7. En la tabla IPv6 ACL Rule Table, haga clic en la regla.
La regla es un hipervínculo. Se muestra la página IPv6 ACL Rule Configuration.

8. Modifique los criterios de la regla de ACL IPv6.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Eliminar una regla de ACL IPv6 Para eliminar una regla de ACL IPv6:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IPv6 Rules. Se muestra la página IPv6 Rules.

6. En el menú ACL Name, seleccione la ACL que incluye la regla que desea eliminar.

7. En la tabla IPv6 ACL Rule Table, marque la casilla asociada con la regla.

8. Haga clic en el botón
Delete. Se elimina la regla.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar las vinculaciones de ACL IP a interfaces

Al vincular una ACL IPv4 básica, IPv4 extendida o IPv6 a una interfaz, todas las reglas definidas para la ACL IP se aplican a la interfaz seleccionada.

Si los recursos del switch son insuficientes, falla el intento de vincular una ACL a una interfaz.

Para vincular una ACL IP a una o más interfaces:

1. Abra un navegador web.

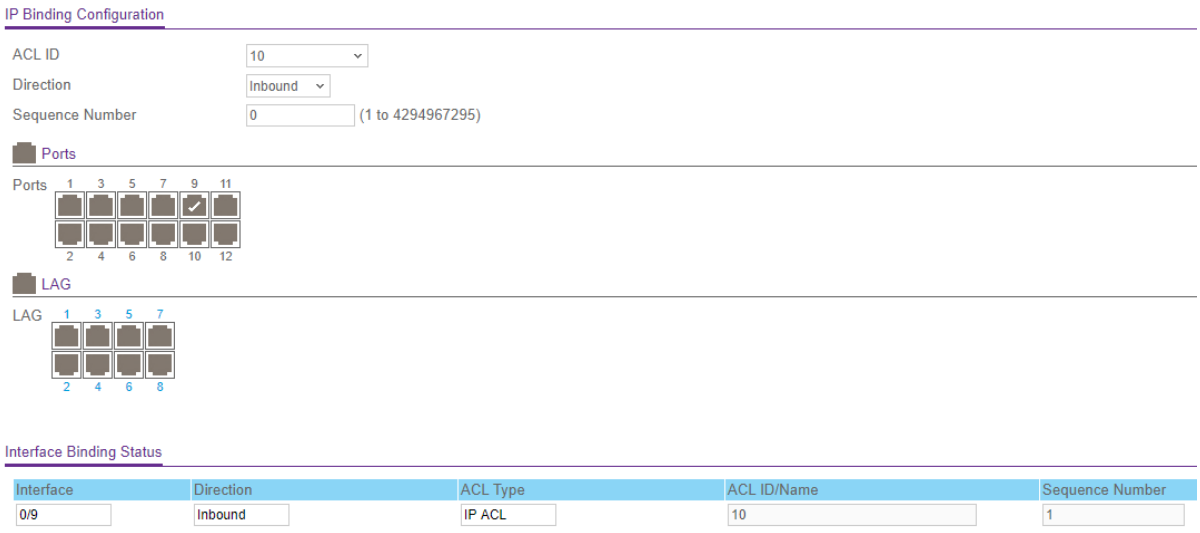
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > IP Binding Configuration.



La figura anterior muestra la página de un modelo de 12 puertos e incluye algunos ejemplos.

6. En el menú ACL ID, seleccione una ACL IP.

Nota: La vinculación de una ACL a una interfaz falla si el switch no tiene recursos para una nueva ACL. Además, no puede vincular una ACL IPv4 y una ACL IPv6 a la misma interfaz.

7. En el menú Direction, seleccione la dirección de filtrado de paquetes de la ACL:

- Inbound: La regla se aplica al tráfico que entra al puerto.
- Outbound: La regla se aplica al tráfico que sale del puerto.

8. En el campo Sequence Number, puede especificar un número que indique el orden de la lista de acceso respecto a otras ya asignadas a la interfaz y dirección.
Un número bajo indica mayor precedencia. Si un número de secuencia ya está en uso para la interfaz y dirección, la lista de acceso especificada reemplaza a la lista vinculada con ese número de secuencia. Si no especifica el número de secuencia (es decir, el valor es 0), se usa un número una unidad mayor que el número de secuencia más alto en uso para la interfaz y dirección. El rango es de 1 a 4294967295.

9. Para agregar la ACL seleccionada a un puerto o LAG, en la tabla Ports o LAG, haga clic en el puerto o LAG para que aparezca una marca de verificación.
Puede agregar la ACL a varios puertos y LAG.

Las tablas Ports y LAG muestran las interfaces disponibles para enlaces de ACL.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe la información no configurable que se muestra.

Tabla 164. Información de Interface Binding Status

Campo	Descripción
Interface	La interfaz seleccionada.
Direction	La dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignado a la interfaz y dirección seleccionadas.
ID/nombre de ACL	Número o nombre que identifica la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL respecto a otras ACL asignadas a la interfaz y dirección seleccionadas.

Mostrar o eliminar vinculaciones de ACL IP en la tabla de vinculaciones de ACL IP

Puede mostrar o eliminar vinculaciones de ACL IPv4 básicas, IPv4 extendidas e IPv6.

Para mostrar o eliminar vinculaciones de ACL IP:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > Binding Table.
Se muestra la página IP ACL Binding Table. La tabla muestra las vinculaciones de ACL IP a interfaces.

6. Para eliminar una vinculación de ACL IP a interfaz, haga lo siguiente: a. Marque la casilla junto a la interfaz. b. Haga clic en el botón Eliminar (Delete).

Se elimina la vinculación.

7. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 165. Información de Interface Binding Status

Campo	Descripción
Interface	La interfaz seleccionada.
Direction	La dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignado a la interfaz y dirección seleccionadas.

Tabla 165. Información de Interface Binding Status (continuación)

Campo	Descripción
ID/nombre de ACL	Número o nombre que identifica la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL respecto a otras ACL asignadas a la interfaz y dirección seleccionadas.

Configurar las vinculaciones de ACL a VLAN

Puede asociar una ACL MAC, cualquier tipo de ACL IPv4 o una ACL IPv6 con una VLAN. Al hacerlo, la ACL se aplica a todas las interfaces miembro de la VLAN.

Agregar una vinculación de ACL a VLAN Para agregar una vinculación de ACL a VLAN:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL> Advanced > VLAN Binding Table. Se muestra la página VLAN Binding Table.

6. En el campo VLAN ID, ingrese el ID de la VLAN a la que se aplicará la vinculación.
7. En el menú Direction, seleccione la dirección de filtrado de paquetes de la ACL:

- Inbound: La regla se aplica al tráfico que entra al puerto.
- Outbound: La regla se aplica al tráfico que sale del puerto.

8. En el campo Sequence Number, puede especificar un número que indique el orden de la lista de acceso respecto a otras ya asignadas a la VLAN y dirección. Un número bajo indica mayor precedencia. Si un número de secuencia ya está en uso para el ID de VLAN y dirección, la lista de acceso especificada reemplaza a la lista vinculada con ese número de secuencia. Si no especifica el número de secuencia (es decir, el valor es 0), se usa un número una unidad mayor

que el número de secuencia más alto en uso para el ID de VLAN y dirección. El rango es de 1 a 4294967295.

9. En el menú ACL Type, seleccione el tipo de ACL.
Puede seleccionar una ACL MAC, ACL IP o ACL IPv6.

10. En la lista ACL ID, seleccione el ID o nombre de la ACL que se vinculará a la VLAN especificada.

11. Haga clic en el botón Add.
Se agrega la vinculación de ACL a VLAN.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Quitar una vinculación de ACL a VLAN Para quitar una vinculación de ACL a VLAN:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > ACL > Advanced > VLAN Binding Table. Se muestra la página VLAN Binding Table.

6. Marque la casilla de la vinculación de VLAN que desea quitar.

7. Haga clic en el botón Delete.
Se quita la vinculación de ACL a VLAN.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

8

Monitorear el switch y la red

Este capítulo trata los siguientes temas:

- Estadísticas de puertos y paquetes EAP
- Realizar una prueba de cable
- Registros
- Ajustes de syslog y del host del servidor de registro
- Registro de traps
- Registro de eventos
- Duplicación de puertos
- VLAN RSPAN y switches de origen y destino
- Monitoreo sFlow
- Mostrar la información de licencias

Estadísticas de puertos y paquetes EAP

Puede ver las estadísticas de puertos, incluidas las detalladas, y las estadísticas de paquetes Extensible Authentication Protocol (EAP).

Mostrar o borrar las estadísticas de puertos

Puede mostrar un resumen de las estadísticas de tráfico por puerto del switch y borrar las estadísticas.

Para ver o borrar las estadísticas de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Ports > Port Statistics. Se muestra la página Port Statistics.

6. Elija si desea mostrar interfaces físicas, LAG o ambos haciendo clic en uno de los siguientes vínculos sobre el encabezado de la tabla:

- 1: Solo se muestran las interfaces físicas. Este es el valor predeterminado.
- LAG: Solo se muestran los LAG.
- All: Se muestran tanto las interfaces físicas como los LAG.

7. Para buscar una sola interfaz, marque la casilla asociada con el puerto, o escriba el número de puerto en el campo Go To Interface y haga clic en el botón Go.

8. Para borrar los contadores, realice una de las siguientes acciones:

- Para borrar todos los contadores de todos los puertos del switch, marque la casilla del encabezado y haga clic en el botón Clear.
- Para borrar los contadores de un puerto específico, marque la casilla del puerto y haga clic en el botón Clear.

9. Para actualizar la página, haga clic en el botón Refresh.
10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe las estadísticas por puerto que se muestran en la página.

Tabla 166. Información de estadísticas de puertos

Campo	Descripción
Interface	La interfaz.
Total de paquetes recibidos sin errores	Número total de paquetes recibidos sin errores.
Paquetes recibidos con error	Número de paquetes entrantes con errores que impidieron entregarlos a un protocolo de capa superior.
Paquetes broadcast recibidos	Número de paquetes válidos recibidos dirigidos a la dirección de broadcast. No incluye paquetes multicast.
Paquetes transmitidos sin errores	Número de tramas que este puerto transmitió a su segmento.
Errores de paquetes transmitidos	Número de paquetes salientes que no se pudieron transmitir debido a errores.
Tramas de colisión	Mejor estimación del número total de colisiones en este segmento Ethernet.
Eventos de enlace inactivo	Número total de eventos de enlace inactivo en el puerto.
Oscilaciones de enlace	Número de transiciones de enlace inactivo a activo (es decir, una oscilación de enlace) durante el tiempo de supresión de rebotes.
Velocidad de recepción (Mbps)	Velocidad de datos recibidos en Mbps.
Velocidad de transmisión (Mbps)	Velocidad de datos transmitidos en Mbps.
Tasa de errores de recepción	Velocidad de datos recibidos con errores en Mbps.
Tasa de errores de transmisión	Velocidad de datos transmitidos con errores en Mbps.
Paquetes recibidos por segundo	Número de paquetes recibidos por segundo.
Paquetes transmitidos por segundo	Número de paquetes transmitidos por segundo.
Tiempo desde el último borrado de contadores	Tiempo transcurrido en días, horas, minutos y segundos desde que se borraron por última vez las estadísticas de este puerto.

Mostrar o borrar las estadísticas detalladas de un puerto

Para un puerto específico, puede mostrar diversas estadísticas de tráfico o borrar las estadísticas.

Para mostrar y borrar las estadísticas detalladas de un puerto:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Ports > Port Detailed Statistics. Se muestra la página Port Detailed Statistics.

6. En el menú Interface, seleccione la interfaz (un puerto físico o LAG) cuyas estadísticas desea mostrar.

7. En el menú MST ID, seleccione el ID de MST asociado con la interfaz (si está disponible).
8. Para actualizar la página, haga clic en el botón Refresh.

9. Para borrar todos los contadores, haga clic en el botón Clear. Todas las estadísticas del puerto se restablecen a sus valores predeterminados.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

La siguiente tabla describe las estadísticas detalladas de puerto que se muestran en la página.

Tabla 167. Información de estadísticas detalladas de puerto

Campo	Descripción
ifIndex	El ifIndex de la entrada de la tabla de interfaces asociada con el puerto.
Port Type	El puerto es Normal o uno de los siguientes: • Mirrored: Este puerto es un puerto duplicado en una configuración de duplicación de puertos. • Probe: Este puerto es el puerto de sonda en una configuración de duplicación de puertos. • Port Channel: El puerto es miembro de un LAG.
ID de port channel	Si el puerto es miembro de un port channel, se muestran el ID de interfaz y el nombre del port channel. De lo contrario, se muestra Disable.

Tabla 167. Información de estadísticas detalladas de puerto (continuación)

Campo	Descripción
Port Role	A cada puerto de puente MST habilitado se le asigna una función por cada árbol de expansión. La función es uno de estos valores: Root, Designated, Alternate, Backup, Master o Disabled.
Modo STP	Modo administrativo de Spanning Tree Protocol asociado con el puerto o port channel. Las opciones son las siguientes: • Enable: Spanning tree está habilitado en el puerto. • Disable: Spanning tree está deshabilitado en el puerto.
Estado STP	Estado actual de Spanning Tree del puerto. Este estado controla la acción que realiza un puerto al recibir una trama. Si el puente detecta un puerto defectuoso, lo coloca en el estado Broken. Los estados se definen en IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Modo administrativo	Estado administrativo de control del puerto. El puerto debe estar habilitado para que se le permita entrar a la red. El valor predeterminado es habilitado.
Modo de control de flujo	Indica si el control de flujo está habilitado o deshabilitado en el puerto. Este campo no se aplica a los LAG.
Modo LACP	Indica el estado administrativo de Link Aggregation Control Protocol. El modo debe estar habilitado para que el puerto participe en la agregación de enlaces.
Modo físico	Indica la velocidad y el modo dúplex del puerto. En modo de autonegociación, el modo dúplex y la velocidad se establecen mediante el proceso de autonegociación.
Estado físico	Indica la velocidad y el modo dúplex del puerto.
Estado del enlace	Indica si el enlace está activo o inactivo.
Trap de enlace	Indica si el puerto envía o no un trap cuando cambia el estado del enlace.
Paquetes RX y TX de 64 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 64 octetos (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 65-127 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 65 a 127 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 128-255 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 128 a 255 octetos inclusive (sin bits de trama, pero con octetos FCS).

Tabla 167. Información de estadísticas detalladas de puerto (continuación)

Campo	Descripción
Paquetes RX y TX de 256-511 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 256 a 511 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 512-1023 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 512 a 1023 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 1024-1518 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 1024 a 1518 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 1519-2047 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 1519 a 2047 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 2048-4095 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 2048 a 4095 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes RX y TX de 4096-9216 octetos	Número total de paquetes (incluidos los defectuosos) recibidos o transmitidos con una longitud de 4096 a 9216 octetos inclusive (sin bits de trama, pero con octetos FCS).
Octetos recibidos	Número total de octetos de datos (incluidos los de paquetes defectuosos) recibidos en la red (sin bits de trama, pero con octetos FCS). Este objeto sirve como estimación razonable del uso de Ethernet. Si se requiere mayor precisión, los objetos etherStatsPkts y etherStatsOctets deben muestrearse antes y después de un intervalo común.
Paquetes recibidos de 64 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 64 octetos (sin bits de trama, pero con octetos FCS).
Paquetes recibidos de 65-127 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 65 a 127 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes recibidos de 128-255 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 128 a 255 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes recibidos de 256-511 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 256 a 511 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes recibidos de 512-1023 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 512 a 1023 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes recibidos de 1024-1518 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 1024 a 1518 octetos inclusive (sin bits de trama, pero con octetos FCS).

Tabla 167. Información de estadísticas detalladas de puerto (continuación)

Campo	Descripción
Paquetes recibidos > 1518 octetos	Número total de paquetes recibidos de más de 1518 octetos (sin bits de trama, pero con octetos FCS) y por lo demás bien formados.
Total de paquetes recibidos sin errores	Número total de paquetes recibidos sin errores.
Paquetes unicast recibidos	Número de paquetes unicast de subred entregados a un protocolo de capa superior.
Paquetes multicast recibidos	Número total de paquetes válidos recibidos dirigidos a una dirección multicast. No incluye paquetes dirigidos a la dirección de broadcast.
Paquetes broadcast recibidos	Número total de paquetes válidos recibidos dirigidos a la dirección de broadcast. No incluye paquetes multicast.
Paquetes recibidos descartados	Número de paquetes entrantes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Una posible razón para descartar un paquete es liberar espacio de búfer.
Total de paquetes recibidos con errores MAC	Número total de paquetes entrantes con errores que impidieron entregarlos a un protocolo de capa superior.
Jabbers recibidos	Número total de paquetes recibidos de más de 1518 octetos (sin bits de trama, pero con octetos FCS) que tenían una secuencia de verificación de trama (FCS) incorrecta con un número entero de octetos (error FCS) o una FCS incorrecta con un número no entero de octetos (error de alineación). Esta definición de jabber difiere de la de IEEE-802.3 sección 8.2.1.5 (10BASE5) y sección 10.3.1.4 (10BASE2). Esos documentos definen jabber como la condición en que un paquete excede 20 ms. El rango permitido para detectar jabber es de 20 ms a 150 ms.
Fragmentos recibidos	Número total de paquetes recibidos de menos de 64 octetos con CRC con ERROR (sin bits de trama, pero con octetos FCS).
Paquetes de tamaño insuficiente recibidos	Número total de paquetes recibidos de menos de 64 octetos con CRC CORRECTO (sin bits de trama, pero con octetos FCS).
Errores de alineación	Número total de paquetes recibidos con una longitud (sin bits de trama, pero con octetos FCS) de 64 a 1518 octetos inclusive, pero con una secuencia de verificación de trama (FCS) incorrecta con un número no entero de octetos.
Errores FCS de Rx	Número total de paquetes recibidos con una longitud (sin bits de trama, pero con octetos FCS) de 64 a 1518 octetos inclusive, pero con una secuencia de verificación de trama (FCS) incorrecta con un número entero de octetos
Desbordamientos	Número total de tramas descartadas porque este puerto estaba sobrecargado de paquetes entrantes y no pudo procesar el flujo.
Total de paquetes recibidos no reenviados	Conteo de tramas válidas recibidas que el proceso de reenvío descartó (es decir, filtró).

Tabla 167. Información de estadísticas detalladas de puerto (continuación)

Campo	Descripción
Tramas de pausa 802.3x recibidas	Conteo de tramas de control MAC recibidas en esta interfaz con un código de operación que indica la operación PAUSE. Este contador no aumenta cuando la interfaz opera en modo half-duplex.
Tipo de trama no aceptable	Número de tramas descartadas de este puerto por ser de un tipo de trama no aceptable.
Total de paquetes transmitidos (octetos)	Número total de octetos de datos (incluidos los de paquetes defectuosos) transmitidos en la red (sin bits de trama, pero con octetos FCS). Este objeto sirve como estimación razonable del uso de Ethernet. Si se requiere mayor precisión, los objetos etherStatsPkts y etherStatsOctets deben muestrearse antes y después de un intervalo común.
Paquetes transmitidos de 64 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 64 octetos (sin bits de trama, pero con octetos FCS).
Paquetes transmitidos de 65-127 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 65 a 127 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes transmitidos de 128-255 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 128 a 255 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes transmitidos de 256-511 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 256 a 511 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes transmitidos de 512-1023 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 512 a 1023 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes transmitidos de 1024-1518 octetos	Número total de paquetes (incluidos los defectuosos) recibidos con una longitud de 1024 a 1518 octetos inclusive (sin bits de trama, pero con octetos FCS).
Paquetes transmitidos > 1518 octetos	Número total de paquetes transmitidos de más de 1518 octetos (sin bits de trama, pero con octetos FCS) y por lo demás bien formados. Este contador tiene una tasa máxima de incremento de 815 conteos por segundo a 10 Mb/s.
Tamaño máximo de trama	Tamaño máximo de trama Ethernet que la interfaz admite o tiene configurado, incluidos el encabezado Ethernet, el CRC y la carga útil. El tamaño mínimo es 1500; el máximo es 12270; el predeterminado es 9198.
Total de paquetes transmitidos correctamente	Número de tramas que este puerto transmitió a su segmento.
Paquetes unicast transmitidos	Número total de paquetes que los protocolos de nivel superior solicitaron transmitir a una dirección unicast de subred, incluidos los que se descartaron o no se enviaron.

Tabla 167. Información de estadísticas detalladas de puerto (continuación)

Campo	Descripción
Paquetes multicast transmitidos	Número total de paquetes que los protocolos de nivel superior solicitaron transmitir a una dirección multicast, incluidos los que se descartaron o no se enviaron.
Paquetes broadcast transmitidos	Número total de paquetes que los protocolos de nivel superior solicitaron transmitir a la dirección de broadcast, incluidos los que se descartaron o no se enviaron.
Paquetes transmitidos descartados	Número total de paquetes salientes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Una posible razón para descartar un paquete es liberar espacio de búfer.
Total Transmit Errors	La suma de colisiones únicas, múltiples y excesivas.
Tx FCS Errors	El número total de paquetes transmitidos con una longitud (sin incluir los bits de entramado pero incluyendo los octetos FCS) de entre 64 y 1518 octetos, inclusive, y con una secuencia de verificación de trama (FCS) incorrecta con un número entero de octetos.
Total Transmit Packets Discarded	La suma de tramas de colisión única descartadas, tramas de colisión múltiple descartadas y tramas excesivas descartadas.
Single Collision Frames	El número de tramas transmitidas correctamente en una interfaz específica cuya transmisión se ve impedida por exactamente una colisión.
Multiple Collision Frames	El número de tramas transmitidas correctamente en una interfaz específica cuya transmisión se ve impedida por más de una colisión.
Excessive Collision Frames	El número de tramas cuya transmisión en una interfaz específica falla debido a colisiones excesivas.
STP BPDUs Received	El número de BPDU de STP recibidas en el puerto seleccionado.
STP BPDUs Transmitted	El número de BPDU de STP transmitidas desde el puerto seleccionado.
RSTP BPDUs Received	El número de BPDU de RSTP recibidas en el puerto seleccionado.
RSTP BPDUs Transmitted	El número de BPDU de RSTP transmitidas desde el puerto seleccionado.
MSTP BPDUs Received	El número de BPDU de MSTP recibidas en el puerto seleccionado.
MSTP BPDUs Transmitted	El número de BPDU de MSTP transmitidas desde el puerto seleccionado.
802.3x Pause Frames Transmitted	El número de tramas de control MAC transmitidas en esta interfaz con un código de operación que indica la operación PAUSE. Este contador no aumenta cuando la interfaz opera en modo half-duplex.
GVRP PDUs Received	El número de PDU de GVRP recibidas en la capa GARP.
GVRP PDUs Transmitted	El número de PDU de GVRP transmitidas desde la capa GARP.
GVRP Failed Registrations	El número de veces que no se pudieron completar los intentos de registro GVRP.
GMRP PDUs Received	El número de PDU de GMRP recibidas desde la capa GARP.

Tabla 167. Información de estadísticas detalladas de puerto (continuación)

Campo	Descripción
GMRP PDUs Transmitted	El número de PDU de GMRP transmitidas desde la capa GARP.
GMRP Failed Registrations	El número de veces que no se pudieron completar los intentos de registro GMRP.
EAPOL Frames Received	El número de tramas EAPOL válidas de cualquier tipo que recibió este autenticador.
EAPOL Frames Transmitted	El número de tramas EAPOL de cualquier tipo que transmitió este autenticador.
Load Interval	El periodo en segundos durante el cual se usan los datos para calcular las estadísticas de carga.
Velocidad de recepción (Mbps)	Velocidad de datos recibidos en Mbps.
Velocidad de transmisión (Mbps)	Velocidad de datos transmitidos en Mbps.
Tasa de errores de recepción	Velocidad de datos recibidos con errores en Mbps.
Tasa de errores de transmisión	Velocidad de datos transmitidos con errores en Mbps.
Packets Received Per Second	El número de paquetes recibidos por segundo.
Packets Transmitted Per Second	El número de paquetes transmitidos por segundo.
Percent Utilization Received	La utilización del tráfico recibido, redondeada al porcentaje entero más cercano.
Percent Utilization Transmitted	La utilización del tráfico transmitido, redondeada al porcentaje entero más cercano.
Time Since Counters Last Cleared	El tiempo transcurrido en días, horas, minutos y segundos desde que se borraron por última vez las estadísticas de este puerto.

Mostrar o borrar las estadísticas de EAP y EAPoL

Puede mostrar información sobre los paquetes Extensible Authentication Protocol (EAP) y EAP over LAN (EAPoL) que se reciben en los puertos físicos.

Para mostrar o borrar las estadísticas de EAP y EAPoL:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Ports > EAP Statistics. Se muestra la página EAP Statistics.

6. Para actualizar la página, haga clic en el botón Refresh.

7. Para borrar los contadores, lo que restablece las estadísticas de EAP y EAPoL a los valores predeterminados, realice una de las siguientes acciones:

- Para borrar los contadores de un puerto específico, marque la casilla asociada con el puerto y haga clic en el botón Clear.
- Para borrar los contadores de varios puertos, marque las casillas asociadas con los puertos y haga clic en el botón Clear.
- Para borrar todos los contadores de todos los puertos, marque la casilla del encabezado de fila y haga clic en el botón Clear.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe las estadísticas de EAP que se muestran en la página.

Tabla 168. Información de EAP Statistics

Campo	Descripción
Port	El número de puerto.
PAE Capabilities	Las capacidades PAE del puerto.
EAPOL Frames Received	El número de tramas EAPOL válidas de cualquier tipo que recibió este autenticador.
EAPOL Frames Transmitted	El número de tramas EAPOL de cualquier tipo que transmitió este autenticador.
EAPOL Start Frames Received	El número de tramas EAPOL start que recibió este autenticador.
EAPOL Logoff Frames Received	El número de tramas EAPOL logoff que recibió este autenticador.
EAPOL Last Frame Version	El número de versión del protocolo contenido en la trama EAPOL recibida más recientemente.
EAPOL Last Frame Source	La dirección MAC de origen contenida en la trama EAPOL recibida más recientemente.

Tabla 168. Información de EAP Statistics (continuación)

Campo	Descripción
EAPOL Invalid Frames Received	El número de tramas EAPOL recibidas por este autenticador en las que no se reconoce el tipo de trama.
EAPOL Length Error Frames Received	El número de tramas EAPOL recibidas por este autenticador en las que no se reconoce el tipo de trama.
EAP Response/ID Frames Received	El número de tramas EAP response/identity que recibió este autenticador.
EAP Response Frames Received	El número de tramas EAP response válidas (distintas de las tramas resp/ID) que recibió este autenticador.
EAP Request/ID Frames Transmitted	El número de tramas EAP request/identity que transmitió este autenticador.
EAP Request Frames Transmitted	El número de tramas EAP request (distintas de las tramas request/identity) que transmitió este autenticador.

Realizar una prueba de cable

Puede probar y mostrar información sobre los cables conectados a los puertos del switch.

Para realizar una prueba de cable:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Ports > Cable Test. Se muestra la página Cable Test.

6. Marque las casillas asociadas con los puertos físicos cuyos cables desea probar.

7. Haga clic en el botón Apply.
Se realiza una prueba de cable en la interfaz seleccionada. La prueba de cable puede tardar hasta dos segundos en completarse. Si el puerto tiene un enlace activo, el estado del cable siempre es Normal. El comando devuelve una estimación de la longitud del cable si el PHY admite esta función para la velocidad de enlace actual. Tenga en cuenta que si el enlace está inactivo y hay un cable conectado a un adaptador Ethernet 10/100, el estado del cable puede ser Open o Short porque algunos adaptadores Ethernet dejan los pares de hilos no usados sin terminar o conectados a tierra.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 169. Cable Test

Campo	Descripción
Cable Status	Indica el estado del cable: • Normal: El cable funciona correctamente. • Open: El cable está desconectado o hay un conector defectuoso. • Short: Existe un cortocircuito en el cable. • Cable Test Failed: No se pudo determinar el estado del cable. El cable podría en realidad estar funcionando. • Untested: El cable aún no se ha probado. • Invalid cable type: El tipo de cable no es compatible.
Cable Length	La longitud estimada del cable en metros. La longitud se muestra como un rango entre la longitud estimada más corta y la más larga. Se muestra Unknown si no se pudo determinar la longitud del cable. La longitud del cable solo se muestra si el estado del cable es Normal.
Failure Location	La distancia estimada en metros desde el extremo del cable hasta la ubicación de la falla. La ubicación de la falla solo se muestra si el estado del cable es Open o Short.

Registros

El switch genera mensajes en respuesta a eventos, fallas y errores, así como a cambios en la configuración u otros sucesos. Estos mensajes se almacenan localmente y pueden reenviarse a uno o más puntos centralizados de recopilación para fines de supervisión o almacenamiento de archivo a largo plazo (consulte Configuración de syslog y del host del servidor de registro en la página 712). La configuración local y remota de la función de registro incluye el filtrado de los mensajes registrados o reenviados según la gravedad y el componente que los genera.

Administrar y mostrar el registro en memoria

El registro en memoria almacena mensajes en la memoria según la configuración del componente y la gravedad del mensaje. Puede establecer el estado administrativo y el comportamiento de los registros en el búfer del sistema. Estos mensajes de registro se borran cuando se reinicia el switch.

Para administrar y mostrar el registro en memoria:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Memory Log. Se muestra la página Memory Log.

6. Seleccione uno de los siguientes botones de opción de Admin Status:

- Enable: Permite que el switch registre los mensajes predeterminados. Esta es la configuración predeterminada.
- Disable: Impide que el switch registre los mensajes predeterminados.

7. En el menú Behavior, especifique el comportamiento del registro cuando esté lleno:

- Wrap: Cuando el búfer está lleno, los mensajes de registro más antiguos se eliminan a medida que el sistema registra mensajes nuevos.
- Stop on Full: Cuando el búfer está lleno, el sistema deja de registrar mensajes nuevos y conserva todos los mensajes de registro existentes.

8. En el menú Severity Filter, seleccione el nivel de registro de los mensajes que deben registrarse.
Se registran los mensajes con el nivel de gravedad seleccionado y todos los mensajes de mayor gravedad. Por ejemplo, si selecciona Warning, los mensajes registrados incluyen Warning, Error, Critical, Alert y Emergency. El nivel de gravedad predeterminado es Informational (6).

La gravedad puede ser uno de los siguientes niveles:

- Emergency: Nivel 0, el nivel de advertencia más alto. Si el dispositivo está inactivo o no funciona correctamente, se guarda un registro de emergencia en el dispositivo.
- Alert: Nivel 1, el segundo nivel de advertencia más alto. Se guarda un registro de alerta si ocurre una falla grave del dispositivo, como que todas las funciones del dispositivo estén inactivas.
- Critical: Nivel 2, el tercer nivel de advertencia más alto. Se guarda un registro crítico si ocurre una falla crítica del dispositivo, por ejemplo, dos puertos del dispositivo no funcionan, mientras el resto de los puertos sigue funcionando.
- Error: Nivel 3, ocurrió un error en el dispositivo, como un puerto fuera de línea.
- Warning: Nivel 4, el nivel más bajo de advertencia del dispositivo.
- Notice: Nivel 5, proporciona información del dispositivo a los administradores de red.
- Informational: Nivel 6, proporciona información del dispositivo. Esta es la configuración predeterminada.
- Debug: Nivel 7, proporciona información detallada sobre el registro.

Nota: Un registro guarda los mensajes iguales o superiores a un umbral de gravedad configurado.

9. En el campo Threshold, ingrese el porcentaje de espacio de registro que, si se excede, hace que se detenga el registro.
Ingrese un porcentaje de 1 a 100. El valor predeterminado es 80.

El umbral solo se aplica si la opción seleccionada en el menú Behavior es Stop-on-Full. De forma predeterminada, la opción seleccionada en el menú Behavior es Wrap y el umbral no se aplica.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

La tabla Memory Log se muestra en la página Memory Log.

El campo Total number of Messages muestra el número de mensajes que el sistema registró en memoria. De forma predeterminada, se pueden mostrar en la página hasta 160 (80 por ciento del máximo de 200) de las entradas más recientes.

El resto de la página muestra los mensajes de Memory Log. El formato del mensaje de registro es el mismo para los mensajes que se muestran en el registro de mensajes, el registro persistente o el registro de consola. Los mensajes registrados en un recopilador o relay mediante syslog admiten el mismo formato.

El siguiente ejemplo muestra el formato estándar de un mensaje de registro:

```
<189> Jan 05 2021 00:00:18: AAA-5-CONNECT: New http connection
for user admin, source 192.168.1.111 ACCEPTED
```

El mensaje se generó con gravedad 189 (Notice, nivel 5) el 5 de enero de 2021 a las 00:00:18 a. m. por el componente AAA. El mensaje indica que el administrador inició sesión correctamente en la interfaz de administración HTTP desde un host con la dirección IP 192.168.1.111.

El número de gravedad del mensaje se genera mediante una combinación de la facility y la gravedad. En el ejemplo anterior, la facility predeterminada de 23 se multiplica por 8 y se suma la gravedad (5): (23 * 8) + 5 = 189

11. Para actualizar la página, haga clic en el botón Refresh.
12. Para borrar el registro, haga clic en el botón Clear.
13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Formato del registro de mensajes

Este tema se aplica al formato de todos los mensajes registrados que se muestran en el registro de mensajes, el registro persistente o el registro de consola.

Los mensajes registrados en un recopilador o relay mediante syslog usan un formato idéntico:

- <15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237%% Interface 12 transitioned to root state on message age timer expiry.
  Este ejemplo indica un mensaje con gravedad 7 (15 mod 8) (debug) en un switch, generado por el componente MSTP que se ejecuta en el ID de hilo 2110 el Aug 24 05:34:05 en la línea 318 del archivo mstp_api.c. Este es el mensaje número 237 registrado con la IP del sistema 0.0.0.0 y el ID de tarea 1.
- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237%% Interface 12 transitioned to root state on message age timer expiry.
  Este ejemplo indica un mensaje de nivel de usuario (1) con gravedad 7 (debug) en un sistema que no es un switch, generado por el componente MSTP que se ejecuta en el ID de hilo 2110 el Aug 24 05:34:05 en la línea 318 del archivo mstp_api.c. Este es el mensaje número 237 registrado. Los mensajes registrados en un recopilador o relay mediante syslog usan un formato idéntico al del mensaje anterior.
- Total number of Messages: Para el registro de mensajes, solo se muestran en la página las 200 entradas más recientes.

Habilitar o deshabilitar el registro de configuración de comandos

El switch puede registrar los cambios realizados con comandos de configuración de la CLI.

Para habilitar o deshabilitar el registro de configuración de comandos:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch.

Aparece la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Command Log Configuration.
Se muestra la página Command Log Configuration.

6. Seleccione uno de los siguientes botones de opción de Admin Status:

- Enable: Permite que el switch registre los comandos de configuración de la CLI. Esta es la configuración predeterminada.
- Disable: Impide que el switch registre los comandos de configuración de la CLI.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Habilitar o deshabilitar el registro en consola

El switch puede registrar mensajes en un dispositivo serie conectado al switch.

Para habilitar o deshabilitar el registro en consola:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Console Log Configuration.
Se muestra la página Console Log Configuration.

6. Seleccione uno de los siguientes botones de opción de Admin Status:

• Enable: Permite que el switch registre mensajes en un dispositivo serie. Esta es la configuración predeterminada.
• Disable: Impide que el switch registre mensajes en un dispositivo serie.

7. En el menú Severity Filter, seleccione el nivel de registro de los mensajes que deben registrarse.
Se registran los mensajes con el nivel de gravedad seleccionado y todos los mensajes de mayor gravedad. Por ejemplo, si selecciona Warning, los mensajes registrados incluyen Warning, Error, Critical, Alert y Emergency. El nivel de gravedad predeterminado es Error (3).

La gravedad puede ser uno de los siguientes niveles:

- Emergency: Nivel 0, el nivel de advertencia más alto. Si el dispositivo está inactivo o no funciona correctamente, se guarda un registro de emergencia en el dispositivo.
- Alert: Nivel 1, el segundo nivel de advertencia más alto. Se guarda un registro de alerta si ocurre una falla grave del dispositivo, como que todas las funciones del dispositivo estén inactivas.
- Critical: Nivel 2, el tercer nivel de advertencia más alto. Se guarda un registro crítico si ocurre una falla crítica del dispositivo, por ejemplo, dos puertos del dispositivo no funcionan, mientras el resto de los puertos sigue funcionando.
- Error: Nivel 3, ocurrió un error en el dispositivo, como un puerto fuera de línea. Esta es la configuración predeterminada.
- Warning: Nivel 4, el nivel más bajo de advertencia del dispositivo.
- Notice: Nivel 5, proporciona información del dispositivo a los administradores de red.
- Informational: Nivel 6, proporciona información del dispositivo.
- Debug: Nivel 7, proporciona información detallada sobre el registro.

Nota: Un registro guarda los mensajes iguales o superiores a un umbral de gravedad configurado.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configuración de syslog y del host del servidor de registro

Puede permitir que el switch envíe mensajes de registro a uno o más servidores, es decir, a hosts de registro remotos. Un servidor de registro remoto es lo mismo que un host syslog remoto.

Debe habilitar el registro en servidor en el switch y especificar uno o más hosts syslog remotos

Configurar los ajustes de syslog

Para configurar los ajustes de syslog:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Server Log. Se muestra la página Server Log.

6. Seleccione uno de los siguientes botones de opción de Admin Status:

- Enable: El switch envía mensajes de registro a todos los servidores syslog configurados.
- Disable: El switch deja de enviar mensajes de registro a todos los servidores syslog configurados.

7. En el campo Local UDP Port, especifique el número de puerto que usa el switch para enviar mensajes de registro a los servidores syslog.
El rango es de 1 a 65535. El puerto predeterminado es 514.

8. En el menú Source Interface, seleccione la interfaz de origen o la VLAN que debe usarse para la comunicación syslog:

- None: Se usa como dirección de origen la dirección IP principal de la interfaz de origen (de salida).
- Routing interface: Se usa como dirección de origen la dirección IP principal de un puerto físico.

• Routing VLAN: Se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento de VLAN.
• Routing loopback interface: Se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.
• Tunnel interface: La interfaz de túnel IPv6.
• Service port: Se usa como dirección de origen la dirección IP de origen del puerto de administración.

De forma predeterminada, se usa VLAN 1 como interfaz de origen.

Nota: La función syslog del switch puede guardar los mensajes de registro simultáneamente en un servidor remoto y en un dispositivo de almacenamiento USB.

9. Para guardar simultáneamente los mensajes de registro en un dispositivo de almacenamiento USB, en el campo USB Filename, especifique el nombre del archivo USB. El nombre de archivo no puede incluir los siguientes símbolos: V:*?”<>!. Se pueden ingresar hasta 64 caracteres. Los 64 caracteres corresponden solo a la longitud del nombre de archivo; la extensión se agrega automáticamente.

10. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

La siguiente tabla describe los campos no configurables de la página.

Tabla 170. Información de configuración de syslog

Campo	Descripción
Messages Received	El número de mensajes recibidos por el proceso de registro. Esto incluye los mensajes que se descartan o se ignoran.
Messages Relayed	El número de mensajes syslog retransmitidos.
Messages Ignored	El número de mensajes syslog ignorados.

Agregar un servidor syslog

Para agregar un servidor syslog:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Server Log. Se muestra la página Server Log.

6. En la tabla Server Configuration, configure los siguientes ajustes:

• IP Address Type: Especifique el tipo de dirección IP del servidor syslog, que puede ser IPv4, IPv6 o DNS.
• Host Address: Especifique la dirección IP o el nombre de host del servidor syslog.
• Port: Especifique el puerto del servidor syslog. El número de puerto predeterminado es 514.
• Severity Filter: Use el menú para seleccionar la gravedad de los registros que deben enviarse al servidor syslog. Se envían al host los registros con el nivel de gravedad seleccionado y todos los registros de mayor gravedad. Por ejemplo, si selecciona Error, los mensajes registrados incluyen Error, Critical, Alert y Emergency. La gravedad puede ser uno de los siguientes niveles:

- Emergency: Nivel 0, el nivel de advertencia más alto. Si el dispositivo está inactivo o no funciona correctamente, se guarda un registro de emergencia en el dispositivo.
- Alert: Nivel 1, el segundo nivel de advertencia más alto. Se guarda un registro de alerta si ocurre una falla grave del dispositivo, como que todas las funciones del dispositivo estén inactivas.
- Critical: Nivel 2, el tercer nivel de advertencia más alto. Se guarda un registro crítico si ocurre una falla crítica del dispositivo, por ejemplo, dos puertos del dispositivo no funcionan, mientras el resto de los puertos sigue funcionando.
- Error: Nivel 3, ocurrió un error en el dispositivo, como un puerto fuera de línea.
- Warning: Nivel 4, el nivel más bajo de advertencia del dispositivo.
- Notice: Nivel 5, proporciona información del dispositivo a los administradores de red.
- Informational: Nivel 6, proporciona información del dispositivo.
- Debug: Nivel 7, proporciona información detallada sobre el registro.

7. Haga clic en el botón Add.
Se agrega el servidor syslog.

El campo Status de la tabla Server Configuration muestra si el servidor syslog está activo actualmente.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Modificar la configuración de un servidor syslog

Para modificar la configuración de un host syslog remoto:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Server Log. Se muestra la página Server Log.

6. Marque la casilla asociada con el servidor syslog.
7. Cambie la configuración según sea necesario.

8. Haga clic en el botón Apply.
La configuración se guarda.

Eliminar la configuración de un servidor syslog

Para eliminar la configuración de un host syslog remoto:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Server Log. Se muestra la página Server Log.

6. Marque la casilla asociada con el servidor syslog.

7. Haga clic en el botón Delete.
Se elimina el servidor syslog.

Registro de traps

El registro de traps incluye información sobre las traps que envió el switch. Puede mostrar y borrar las entradas del registro de traps.

También puede recuperar el registro de traps y guardarlo como archivo. Para obtener más información, consulte Exportar un archivo desde el switch en la página 739.

Para mostrar o borrar el registro de traps:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Trap Logs. Se muestra la página Trap Logs.

6. Para actualizar la página, haga clic en el botón Refresh.
7. Para borrar el registro, haga clic en el botón Clear.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 171. Información del registro de traps

Campo	Descripción
Number of Traps Since Last Reset	El número de traps que ocurrieron desde el último reinicio del switch.
Trap Log Capacity	El número máximo de traps almacenadas en el registro. Si el número de traps excede la capacidad, las nuevas entradas sobrescriben las más antiguas.
Number of Traps since log last viewed	El número de traps que ocurrieron desde la última vez que se mostraron las traps. Nota: Si guarda el registro de traps en otro dispositivo (es decir, carga el archivo desde el switch), este contador se establece en 0.
Log	El número de secuencia de esta trap.
System Up Time	El momento en que ocurrió esta trap, expresado en días, horas, minutos y segundos desde el último reinicio del switch.
Trap	Información sobre la trap.

Registro de eventos

Puede mostrar y borrar el registro de eventos, que contiene mensajes de error del switch.

Nota: Si restablece el switch a la configuración predeterminada de fábrica, el registro de eventos no se borra.

Para mostrar o borrar el registro de eventos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Logs > Event Logs. Se muestra la página Event Logs.

6. Para actualizar la página, haga clic en el botón Refresh
7. Para borrar el registro, haga clic en el botón Clear.
8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe la información del registro de eventos que se muestra en la página.

Tabla 172. Información de los registros de eventos

Campo	Descripción
Entry	El número de secuencia del evento.
Type	El tipo de evento.
File Name	El archivo en el que se originó el evento.
Line	El número de línea del evento.
Task ID	El ID de tarea del evento.
Code	El código del evento.
Time	La hora en que ocurrió este evento.

Duplicación de puertos

La duplicación de puertos (port mirroring) le permite seleccionar el tráfico de red de puertos específicos del switch para que lo analice un analizador de red. En cada configuración de duplicación de puertos (el switch admite hasta cuatro), puede seleccionar muchos puertos como puertos de origen, pero solo un puerto como puerto de destino. En cada configuración, puede definir cómo se duplica el tráfico de un puerto de origen seleccionando los paquetes recibidos, transmitidos o ambos. También puede aplicar una ACL IP o una ACL MAC para filtrar el tráfico que se duplica.

Un paquete copiado al puerto de destino tiene el mismo formato que el paquete original. Es decir, si se copia un paquete recibido, la copia lleva o no etiqueta de VLAN tal como se recibió en el puerto de origen. Si se copia un paquete transmitido, la copia lleva o no etiqueta de VLAN tal como se transmite en el puerto de origen.

Para establecer una configuración de duplicación de puertos:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Mirroring > Multiple Port Mirroring. Se muestra la página Multiple Port Mirroring.

6. En el menú Session ID, seleccione 1, 2, 3 o 4 como ID de sesión de duplicación de puertos. Puede establecer cuatro configuraciones de duplicación de puertos que funcionan de forma independiente entre sí.

7. Habilite o deshabilite la configuración de duplicación de puertos seleccionando uno de los siguientes botones de opción de Admin Mode:

- True: Se duplican las interfaces de origen seleccionadas. Es decir, el tráfico que entra o sale de las interfaces de origen se copia (duplica) al puerto de destino seleccionado.
- False: No se duplican las interfaces de origen seleccionadas.

8. En el menú Destination Port, seleccione la interfaz de destino a la que se debe copiar el tráfico.
En cada configuración de duplicación de puertos, solo puede configurar un puerto de destino. El valor predeterminado es None.

9. Para filtrar el tráfico que se debe duplicar, haga lo siguiente:
a. En el menú Filter Type, seleccione IP ACL o MAC ACL.

Solo se duplica al puerto de destino el tráfico que coincide con las reglas de la ACL. De forma predeterminada, no se aplica ningún filtro; es decir, la selección es None.

b. En el campo Filter Name, especifique el ID de la ACL.
Para obtener información sobre la configuración de ACL, consulte Listas de control de acceso en la página 646.

10. En la sección Source Interface Configuration, seleccione una o más interfaces de origen y la dirección del tráfico:

a. Seleccione qué interfaces se muestran en la página:

- Unit ID: Muestra solo los puertos físicos.
- LAG: Muestra solo los LAG.
- CPU: Muestra solo la CPU.
- VLANS: Muestra solo las VLAN.
- All: Muestra todos los puertos físicos, LAG, la CPU y las VLAN.

b. Use uno de los siguientes métodos para seleccionar una interfaz:

- En el campo Go To Interface, introduzca la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.
- Junto a la columna Interface, active la casilla de la interfaz o interfaces que desea incluir.

Nota: Si una interfaz es miembro de una VLAN y de un LAG, no puede seleccionar la VLAN como VLAN de origen. Sin embargo, si una interfaz es miembro de una VLAN que selecciona como VLAN de origen, la interfaz puede ser miembro de un LAG.

c. En el menú Direction, seleccione la dirección del tráfico que se debe duplicar desde los puertos de origen configurados.

- None: El puerto (o la VLAN) no se duplica.
- Tx and Rx: Se duplica el tráfico de salida (transmitido) y de entrada (recibido). En una VLAN, esta opción selecciona la VLAN como VLAN de origen.
- Rx: Solo se duplica el tráfico de entrada (recibido). Esta opción no está disponible para una VLAN.
- Tx: Solo se duplica el tráfico de salida (transmitido). Esta opción no está disponible para una VLAN.

11. Haga clic en el botón Apply.
Se guarda la configuración.

Si el puerto está configurado como puerto de origen, el campo Status muestra Mirrored.
Si el puerto está configurado como puerto de destino, el campo Status muestra Probe.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

VLAN RSPAN y switches de origen y destino

Puede configurar una VLAN como VLAN de analizador de puertos conmutados remoto (RSPAN). RSPAN le permite duplicar el tráfico de varios puertos de origen (o de todos los puertos miembros de una VLAN) de distintos dispositivos de red y enviarlo a un puerto de destino (un puerto de sondeo conectado a un analizador de red) en un dispositivo remoto. El tráfico duplicado se etiqueta con el ID de VLAN RSPAN y se transmite por puertos trunk en la VLAN RSPAN.

Un switch puede funcionar como switch de origen RSPAN que envía tráfico a otro switch que funciona como switch de destino RSPAN. Como el switch admite varias configuraciones RSPAN, también puede funcionar como switch de destino RSPAN que recibe tráfico de otro switch que funciona como switch de origen RSPAN.

Configurar una VLAN existente como VLAN RSPAN

Puede configurar una VLAN existente como VLAN RSPAN.

Para configurar una VLAN existente como VLAN RSPAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Mirroring > RSPAN VLAN. Se muestra la página RSPAN VLAN.

6. Active la casilla de la VLAN que se convertirá en VLAN RSPAN.

7. En el menú Admin Mode, seleccione Enable para configurar la VLAN como VLAN RSPAN.
De forma predeterminada, la selección es Disable y la VLAN no es una VLAN RSPAN.

8. Haga clic en el botón Apply.
La configuración se guarda.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar el switch como switch de origen RSPAN

Puede configurar el switch como switch de origen RSPAN que envía tráfico a otro switch que funciona como switch de destino RSPAN.

Puede crear hasta cuatro configuraciones de switch de origen RSPAN.

Para configurar el switch como switch de origen RSPAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Mirroring > RSPAN Source Switch Configuration. Se muestra la página RSPAN Source Switch Configuration.

6. En el menú Session ID, seleccione 1, 2, 3 o 4 como ID de sesión del switch de origen RSPAN.
Puede establecer cuatro configuraciones de switch de origen RSPAN que funcionan de forma independiente entre sí.

7. Habilite o deshabilite la configuración de switch de origen RSPAN seleccionando uno de los siguientes botones de opción de Admin Mode:

- True: Se duplican las interfaces de origen seleccionadas. Es decir, el tráfico que entra o sale de las interfaces de origen se copia (duplica) a la VLAN de destino RSPAN seleccionada.
- False: No se duplican las interfaces de origen seleccionadas.

8. En el menú RSPAN Destination VLAN, seleccione la VLAN de destino a la que se debe copiar el tráfico.

En cada configuración de switch de origen RSPAN, solo puede configurar un puerto de VLAN de destino RSPAN. El valor predeterminado es None.

9. En el menú RSPAN Reflector Port, seleccione la interfaz conectada al switch de destino RSPAN.

10. Para filtrar el tráfico que se debe duplicar, haga lo siguiente:
a. En el menú Filter Type, seleccione IP ACL o MAC ACL.

Solo se duplica a la VLAN de destino RSPAN el tráfico que coincide con las reglas de la ACL.

De forma predeterminada, no se aplica ningún filtro; es decir, la selección es None.

b. En el campo Filter Name, especifique el ID de la ACL.
Para obtener información sobre la configuración de ACL, consulte Listas de control de acceso en la página 646.

11. En la sección RSPAN Source Interface Configuration, seleccione una o más interfaces de origen y la dirección del tráfico:

a. Seleccione qué interfaces se muestran en la página:

- Unit ID: Muestra solo los puertos físicos.
- LAG: Muestra solo los LAG.
- CPU: Muestra solo la CPU.
- VLANS: Muestra solo las VLAN.
- All: Muestra todos los puertos físicos, LAG, la CPU y las VLAN.

b. Use uno de los siguientes métodos para seleccionar una interfaz:

- En el campo Go To Interface, introduzca la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.
- Junto a la columna Interface, active la casilla de la interfaz o interfaces que desea incluir.

Nota: Si una interfaz es miembro de una VLAN y de un LAG, no puede seleccionar la VLAN como VLAN de origen. Sin embargo, si una interfaz es miembro de una VLAN que selecciona como VLAN de origen, la interfaz puede ser miembro de un LAG.

c. En el menú Direction, seleccione la dirección del tráfico que se debe duplicar desde los puertos de origen configurados.

- None: El puerto (o la VLAN) no se duplica.
- Tx and Rx: Se duplica el tráfico de salida (transmitido) y de entrada (recibido). En una VLAN, esta opción selecciona la VLAN como VLAN de origen.

- Rx: Solo se duplica el tráfico de entrada (recibido). Esta opción no está disponible para una VLAN.
- Tx: Solo se duplica el tráfico de salida (transmitido). Esta opción no está disponible para una VLAN.

12. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

Si el puerto está configurado como puerto de origen, el campo Status muestra Mirrored.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar el switch como switch de destino RSPAN

Puede configurar el switch como switch de destino RSPAN que recibe tráfico de otro switch que funciona como switch de origen RSPAN.

Puede crear hasta cuatro configuraciones de switch de destino RSPAN.

Para configurar el switch como switch de destino RSPAN:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring > Mirroring > RSPAN Destination Switch Configuration. Se muestra la página RSPAN Destination Switch Configuration.

6. En el menú Session ID, seleccione 1, 2, 3 o 4 como ID de sesión del switch de destino RSPAN.
Puede establecer cuatro configuraciones de switch de destino RSPAN que funcionan de forma independiente entre sí.

7. Habilite o deshabilite la configuración de switch de destino RSPAN seleccionando uno de los siguientes botones de opción de Admin Mode:

• True: El tráfico de la VLAN de origen RSPAN seleccionada se copia (duplica) al puerto de destino RSPAN seleccionado.
• False: El tráfico de la VLAN de origen RSPAN seleccionada no se duplica.

8. En el menú RSPAN Source VLAN, seleccione la VLAN de origen RSPAN desde la que se debe copiar el tráfico.

9. En el menú RSPAN Destination Port, seleccione el puerto de destino RSPAN al que se debe copiar el tráfico.
En cada configuración de switch de destino RSPAN, solo puede configurar un puerto de destino RSPAN. El valor predeterminado es None.

10. Para filtrar el tráfico que se debe duplicar, haga lo siguiente:
a. En el menú Filter Type, seleccione IP ACL o MAC ACL.

Solo se duplica al puerto de destino RSPAN el tráfico que coincide con las reglas de la ACL.

De forma predeterminada, no se aplica ningún filtro; es decir, la selección es None.

b. En el campo Filter Name, especifique el ID de la ACL.
Para obtener información sobre la configuración de ACL, consulte Listas de control de acceso en la página 646.

11. Haga clic en el botón Apply.
Se guarda la configuración.

12. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

Supervisión con sFlow

sFlow es un estándar para supervisar redes conmutadas y enrutadas de alta velocidad. La tecnología sFlow está integrada en el switch y en muchos otros dispositivos de red para dar visibilidad de la actividad de la red.

El sistema de supervisión sFlow consta de un agente sFlow integrado y un recolector sFlow central, también llamado receptor sFlow. El agente sFlow usa tecnología de muestreo para capturar estadísticas de tráfico del dispositivo que supervisa. Los datagramas sFlow se usan para reenviar las estadísticas muestreadas a un recolector sFlow para su análisis.

El agente sFlow usa dos formas de muestreo: muestreo estadístico basado en paquetes de flujos conmutados o enrutados, y muestreo de contadores basado en tiempo.

Descripción general del agente sFlow

El muestreo de flujos de paquetes y de contadores lo realizan instancias sFlow asociadas a fuentes de datos individuales dentro del agente sFlow. Las muestras de flujos y de contadores se combinan en datagramas sFlow. El muestreo de flujos genera un flujo constante pero aleatorio de datagramas sFlow hacia el recolector sFlow. Las muestras de contadores pueden tomarse según la oportunidad para completar estos datagramas.

Para realizar muestreo de flujos de paquetes, debe configurar una instancia de muestreador sFlow con una tasa de muestreo. Para realizar muestreo de contadores, debe configurar una instancia de sondeo sFlow con un intervalo de sondeo. El agente sFlow envía la información recopilada en forma de datagramas sFlow al receptor sFlow.

Configurar la interfaz de origen del agente sFlow

El switch puede funcionar como agente sFlow y reenviar el tráfico sondeado y muestreado a un receptor sFlow. Puede configurar la interfaz de origen que se conecta al dispositivo que funciona como receptor sFlow.

Para configurar la interfaz de origen del agente sFlow:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring> sFlow > Basic > sFlow Agent Information. Se muestra la página sFlow Agent Information.

6. En el menú Source Interface, seleccione la interfaz de administración que debe usar el agente sFlow:

- None: Se usa como dirección de origen la dirección IP principal de la interfaz de origen (de salida).
- Routing interface: Se usa como dirección de origen la dirección IP principal de un puerto físico.

• Routing VLAN: Se usa como dirección de origen la dirección IP principal de una interfaz de enrutamiento de VLAN.
• Routing loopback interface: Se usa como dirección de origen la dirección IP principal de una interfaz loopback de enrutamiento.
• Tunnel interface: La interfaz de túnel IPv6.
• Service port: Se usa como dirección de origen la dirección IP de origen del puerto de administración.

De forma predeterminada, se usa VLAN 1 como interfaz de origen.

7. Haga clic en el botón Apply.
La configuración se guarda.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

La siguiente tabla describe los campos no configurables de la página.

Tabla 173. Información del agente sFlow

Campo	Descripción
Agent Version	La versión e implementación de la MIB. La versión del agente consta de los siguientes componentes: • Versión de MIB: Por ejemplo, 1.3. • Organización: NETGEAR, Inc. • Revisión: Por ejemplo, 13.0.2.10.
Agent Address	La dirección IP asociada al agente. La dirección IP depende de la interfaz de origen seleccionada.

Configurar un receptor sFlow

Puede configurar uno o más dispositivos que funcionarán como receptores sFlow. La interfaz de origen sFlow proporciona la conexión a estos dispositivos.

Para configurar un receptor sFlow:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Monitoring> sFlow > Advanced > sFlow Receiver Configuration. Se muestra la página sFlow Receiver Configuration.

6. Active la casilla Receiver Index de un receptor.

7. En el campo Receiver Owner, especifique el propietario del receptor. Especifique el nombre del propietario o del dispositivo.

De forma predeterminada, la opción de tiempo de espera está habilitada, pero el periodo está configurado en 0, lo que significa que el muestreo sFlow no se detiene una vez habilitado.

8. Para configurar un periodo de tiempo de espera, haga lo siguiente:
a. En el campo Receiver Timeout, especifique el tiempo de espera en segundos tras el cual se detiene el muestreo.
El rango es de 0 a 2147483647. Un valor de cero significa que el muestreo sFlow no se detiene una vez habilitado.

b. En el menú No Timeout, seleccione False para habilitar el tiempo de espera del muestreo.

El valor predeterminado es False. Si selecciona True, el muestreo no vence y el periodo se establece automáticamente en el máximo de 2147483647.

9. En el campo Maximum Datagram Size, especifique el número máximo de bytes de datos que se pueden enviar en un solo datagrama de muestra.
El valor predeterminado es 1400. El rango es de 200 a 12188. Para evitar la fragmentación de los datagramas, le recomendamos no establecer un tamaño demasiado bajo.

10. En el campo Receiver Address, especifique la dirección IP del receptor sFlow.

11. En el campo Receiver Port, especifique el puerto de destino de los datagramas sFlow. El puerto predeterminado es 6343. El rango es de 1 a 65535.

12. Haga clic en el botón Aplicar (Apply). Se guarda la configuración.

El campo Receiver Datagram Version muestra 5 como versión de los datagramas sFlow.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Configurar el sondeo y muestreo sFlow en una interfaz

Si el switch está configurado como agente sFlow, puede hacer lo siguiente:

- Recopilar muestreo estadístico basado en paquetes de flujos conmutados y enviarlo a los receptores configurados. Una fuente de datos configurada para recopilar muestras de flujo se llama muestreador (sampler).
- Recopilar muestreo basado en tiempo de las estadísticas de interfaces de red y enviarlo a los receptores sFlow configurados. Una fuente de datos configurada para recopilar muestras de contadores se llama sondeador (poller).

Puede configurar el muestreo y el sondeo en una interfaz del switch. El tráfico de la interfaz se muestrea, se sondea y se reenvía al receptor sFlow.

Para configurar el sondeo y muestreo sFlow en una interfaz:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

5. Seleccione Monitoring> sFlow > Advanced > sFlow Interface Configuration. Se muestra la página sFlow Interface Configuration.

6. Use uno de los siguientes métodos para seleccionar una interfaz para el sondeador y el muestreador:

   • En el campo Go To Interface, introduzca la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.
   • Junto a la columna Interface, active la casilla de la interfaz que desea usar.

   Solo puede seleccionar puertos físicos.

7. En el campo Poller Receiver Index, especifique el receptor sFlow que se asociará al sondeador. Para obtener información sobre receptores sFlow, consulte Configurar un receptor sFlow en la página 727.

8. En el campo Poller Interval, especifique los segundos entre sondeos sucesivos.
Un intervalo de 0 deshabilita el muestreo. El rango es de 0 a 86400 segundos. El valor predeterminado es 0 segundos.

9. En el campo Sampler Receiver Index, especifique el receptor sFlow que se asociará al muestreador.
Para obtener información sobre receptores sFlow, consulte Configurar un receptor sFlow en la página 727.

10. En el campo Sampling Rate, especifique la tasa de muestreo estadístico de paquetes. Una tasa de 1 cuenta todos los paquetes. Una tasa de 0 deshabilita el muestreo. El rango permitido es de 1024 a 65536. El valor predeterminado es 0.

11. En el campo Maximum Header Size, especifique el número máximo de bytes que se copiarán de un paquete muestreado.
El rango es de 20 a 256 bytes. El valor predeterminado es 128 bytes.

12. Haga clic en el botón Aplicar
(Apply). Se guarda la configuración.

13. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Mostrar la información de la licencia

La interfaz principal le permite mostrar la información de la licencia, pero no agregarla ni administrarla. Para agregar y administrar una licencia, consulte el Manual del usuario de audio y video, que puede descargar en netgear.com/support/download/.

Mostrar la información de la clave de licencia

Puede mostrar información sobre la clave de licencia instalada.

Para mostrar la información de la clave de licencia:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.
3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.
4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione System > License > License Key. Se muestra la página License Key.

La siguiente tabla describe los campos no configurables de la página.

Tabla 174. Información de la clave de licencia

Campo	Descripción
License Date	La fecha en que se compró y emitió la licencia.
License Copy	El número de licencias (0 o 1).
License Status	Indica si la licencia es válida y si está activa o inactiva Nota: Puede haber una licencia válida instalada, pero es posible que deba activarla o reiniciar el switch para activarla.
Description	Indica si se debe reiniciar el switch para activar una licencia válida instalada en el switch.

Mostrar las funciones a las que se aplica la licencia

Puede ver las funciones que cubre la licencia. Sin una licencia válida, no puede usar las funciones MRP, MMRP, MVRP, MSRP y DOT1AS en el switch.

Para mostrar las funciones a las que se aplica la licencia:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione System > License > License Features. Se muestra la página License Features.

La tabla muestra si las funciones están habilitadas o deshabilitadas.

9

Mantenimiento y solución de problemas

Este capítulo trata los siguientes temas:

- Guardar la configuración
- Instalación automática del archivo de configuración
- Reiniciar el switch desde la interfaz principal del navegador local
- Restablecer el switch a los valores de fábrica
- Exportar un archivo desde el switch
- Actualizar el software o descargar un archivo
- Administrar imágenes de software
- Diagnóstico y solución de problemas

Guardar la configuración

Al guardar la configuración, el switch conserva los cambios realizados cuando se reinicia. También puede guardar la configuración en cada página de configuración de la interfaz principal haciendo clic en el ícono Guardar (Save).

Para guardar la configuración:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Save Config > Save Configuration. Se muestra la página Save Configuration.

6. Active la casilla.

7. Haga clic en el botón Aplicar (Apply).
Se guarda la configuración. Si reinicia el switch, se conserva la configuración guardada.

Instalación automática del archivo de configuración

Si el switch se inicializa sin un archivo de configuración, el proceso de instalación automática (auto install) puede cargar automáticamente la configuración del switch desde un servidor de la red.

Configurar el proceso de instalación automática

El proceso de instalación automática requiere que DHCP esté habilitado de forma predeterminada en el switch. Para guardar la configuración descargada en la configuración de inicio, debe guardar explícitamente el

archivo como tal. El proceso de instalación automática depende de la configuración de otros dispositivos de la red, como un servidor DHCP o BOOTP, un servidor TFTP y, si es necesario, un servidor DNS.

El proceso de instalación automática se realiza en tres fases:

1. Configuración o asignación de una dirección IP al switch: Para más información, consulte Interfaces de administración IPv4 y VLAN en la página 47 o Interfaces de administración IPv6 y VLAN en la página 53.

2. Asignación de un servidor TFTP: Si el switch funciona como cliente DHCP (como lo hace de forma predeterminada), el servidor DHCP puede proporcionarle automáticamente el servidor TFTP, por ejemplo, si el servidor DHCP está configurado con la opción 125 (consulte Requisitos del servidor DHCP con la opción 125 para obtener un archivo de configuración mediante auto install en la página 736).

3. Descarga de un archivo de configuración para el switch desde el servidor TFTP: Consulte el siguiente procedimiento.
Para configurar el proceso de instalación automática:

a. Abra un navegador web.
b. En el campo de dirección del navegador, introduzca la dirección IP del switch. Aparece la página de inicio de sesión.

c. Haga clic en el botón Main UI Login.

La página de inicio de sesión de la UI principal se abre en una nueva pestaña.

d. Introduzca admin como nombre de usuario, introduzca la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicia sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

e. Seleccione Maintenance > Save Config > Auto Install Configuration.

Se muestra la página Auto Install Configuration.

f. En el menú AutoInstall Mode, inicie o detenga el proceso de instalación automática:

- Start: Inicia el proceso de instalación automática (después de hacer clic en el botón Aplicar [Apply]).
- Stop: Detiene el proceso de instalación automática (después de hacer clic en el botón Aplicar [Apply]).

g. En el menú AutoInstall Persistent Mode, habilite o deshabilite el modo persistente del proceso de instalación automática:

- Enabled: El proceso de instalación automática guarda el archivo de configuración descargado y lo aplica después de reiniciar el switch. Esta es la configuración predeterminada.

- Disabled: El proceso de instalación automática no guarda el archivo de configuración descargado y, por lo tanto, no puede aplicarlo después de reiniciar el switch.

h. En el menú AutoSave Mode, habilite o deshabilite el guardado automático de la configuración en la configuración de inicio:

- Enabled: La configuración descargada automáticamente se guarda en la configuración de inicio.
- Disabled: La configuración descargada automáticamente no se guarda en la configuración de inicio. Si desea guardarla, debe hacerlo manualmente. Esta es la configuración predeterminada.

i. En el menú AutoInstall Retry Count, especifique el número de veces que el switch envía un mensaje unicast al servidor TFTP.
El servidor TFTP se especifica en la configuración DHCP (consulte Requisitos del servidor DHCP con opción 125 para obtener un archivo de configuración mediante instalación automática en la página 736). Al superarse el número de veces especificado, el switch envía mensajes broadcast al servidor TFTP. El rango es de 1 a 3. De forma predeterminada, el número es 3.

j. Haga clic en el botón Apply.
Se guardan los ajustes.
El campo Auto-Install State muestra el estado del proceso de instalación automática.

Requisitos del servidor DHCP con opción 125 para obtener un archivo de configuración mediante instalación automática

Puede usar la instalación automática para que el switch descargue un archivo de configuración (archivo de imagen) de un servidor TFTP mediante la opción 125 de DHCP. La actualización de imagen puede actualizar o revertir el firmware del switch.

Para que el switch pueda descargar una imagen de un servidor TFTP, el servidor DHCP debe incluir un archivo de descripción de imagen que indique la imagen que el switch debe descargar del servidor TFTP. Por ejemplo, el archivo de descripción de imagen autoinstall_dhcp del servidor DHCP indica la imagen M4XXX-v1.2.3.4.stk que el switch debe descargar del servidor TFTP.

La opción 125 del servidor DHCP debe contener la siguiente información (el ejemplo usa el archivo de descripción de imagen autoinstall_dhcp y la imagen M4XXX-v1.2.3.4.stk):

- Número de empresa (4 octetos). 0x0000 0x11ae
  En decimal, el número de empresa de NETGEAR es 4526.

- Longitud de datos (1 octeto): 0x12
  La longitud de datos incluye el código de SubOption más la longitud de SubOption más el archivo de descripción de imagen (no la imagen en sí): 1+1+16.
  - Código de SubOption (2 octetos): 0x05
  - Longitud de SubOption (1 octeto): 0x10
    La longitud del nombre del archivo de descripción de imagen.
  - Nombre del archivo de descripción de imagen (N octetos): 61.7574.6f69.6e73.7461.6c6c.5f64.6863.70
    En texto plano, el nombre del archivo de descripción de imagen es autoinstall_dhcp.

El contenido del archivo de descripción de imagen autoinstall_dhcp es M4XXX-v1.2.3.4.stk, que es la imagen que el switch debe descargar del servidor TFTP.

Puede cambiar el nombre del archivo de descripción de imagen, pero entonces también debe cambiar la longitud de datos de la opción 125, que se basa en el código de SubOption, la longitud de SubOption y el nombre del archivo de descripción de imagen.

Reiniciar el switch desde la UI principal del navegador local

Puede reiniciar el switch desde la UI principal.

Nota: Si tiene acceso físico al switch, puede reiniciarlo presionando el botón multifunción Reset del panel frontal durante menos de 5 segundos. (¡No presione el botón durante más de 5 segundos!)

Para reiniciar el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Reset > Device Reboot. Se muestra la página Device Reboot.

6. Seleccione uno de los siguientes botones de opción:

- Save prior to reboot: El switch guarda todos los cambios que realizó y para los que no hizo clic en el icono Save de la interfaz principal del navegador local.
- Don't save prior to reboot: El switch no guarda los cambios que realizó y para los que no hizo clic en el icono Save de la interfaz principal del navegador local.

7. Haga clic en el botón Apply.
Se muestra una ventana emergente de alerta.

8. Haga clic en el botón OK para confirmar. El switch se reinicia.

Restablecer el switch a los ajustes predeterminados de fábrica

Puede restablecer la configuración del switch a los valores predeterminados de fábrica. Se borran todos los cambios que realizó. Si cambia la dirección IP, su sesión web podría desconectarse.

Nota: Si restablece el switch a la configuración predeterminada, la dirección IP de administración se restablece a 169.254.100.100 y se habilita el cliente DHCP. No se establece ninguna dirección IP para el puerto OOB, pero su cliente DHCP se habilita. Si pierde la conectividad de red después de restablecer el switch a los valores de fábrica, consulte Iniciar sesión en la UI principal con un navegador web en la página 24.

Para restablecer el switch a los ajustes predeterminados de fábrica:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Reset > Factory Default. Se muestra la página Factory Default.

6. Active la casilla.

7. Haga clic en el botón Apply.
Se muestra una ventana emergente de confirmación.

8. Haga clic en el botón OK para confirmar.
La configuración se restablece a los ajustes predeterminados de fábrica.

Exportar un archivo desde el switch

Puede exportar archivos de configuración (ASCII) o de registro (ASCII log) desde el switch a un servidor de archivos mediante una sesión TFTP, SFTP, SCP o FTP, a una computadora mediante una sesión HTTP, o a un dispositivo de almacenamiento USB.

Exportar un archivo desde el switch a un servidor

Puede cargar (exportar) archivos de configuración (ASCII o log ASCII) y otros tipos de archivos desde el switch a un servidor TFTP, SFTP, SCP o FTP de la red.

Para exportar un archivo desde el switch a un servidor:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Export > File Export. Se muestra la página File Export.

6. En el menú File Type, seleccione el tipo de archivo que debe exportarse:

• Text Configuration: Un archivo de configuración de texto le permite editar un archivo de texto configurado (startup-config) sin conexión según sea necesario. El uso más común de la configuración de texto es cargar una configuración funcional desde un dispositivo, editarla sin conexión para personalizarla para otro dispositivo similar (por ejemplo, cambiar el nombre del dispositivo o la dirección IP) y descargarla en ese dispositivo. Es el ajuste predeterminado.
• Error Log: El registro persistente de errores del switch, también llamado registro de eventos.
• Buffered Log: El registro en búfer (en memoria) del sistema.
• Trap Log: El registro de traps con los registros de traps del switch.
• Script File: El archivo de script que debe especificar en el campo Local File Name.
• CLI Banner: El archivo de banner de CLI.
• Tech Support: El archivo de soporte técnico es un archivo de texto que contiene diversa información de hardware, software y configuración que puede ayudar a solucionar problemas del dispositivo y de la red.
• Crash Logs: Los registros de fallas del switch, si hay disponibles.
• Backup Configuration: El archivo de configuración de respaldo es un archivo de texto.
• CPU Packets Capture File: El archivo de captura de paquetes de CPU con los paquetes de CPU capturados y almacenados.
• Factory Default Configuration: El archivo de configuración predeterminada de fábrica es un archivo de texto con la configuración predeterminada de fábrica almacenada.
• DHCP Client Configuration File: El archivo de configuración del cliente DHCP con la información del servidor DHCP (host).

7. En el menú Transfer Mode, especifique el protocolo que debe usarse para transferir el archivo al servidor:

• TFTP: Trivial File Transfer Protocol.
• SFTP: Secure File Transfer Protocol. Esta opción requiere especificar un nombre de usuario y una contraseña.
• SCP: Secure Copy Protocol. Esta opción requiere especificar un nombre de usuario y una contraseña.
• FTP: File Transfer Protocol. Esta opción requiere especificar un nombre de usuario y una contraseña.

8. En el menú Server Address Type, seleccione el formato del campo Server Address:

• IPv4: Indica que la dirección del servidor es una dirección IPv4 en formato decimal con puntos. Es el ajuste predeterminado.
• IPv6: Indica que la dirección del servidor es una dirección IPv6 en números hexadecimales con valores de 16 bits separados por dos puntos.
• DNS: Indica que la dirección del servidor es un nombre de host.

9. En el campo Server Address, introduzca la dirección IP del servidor según el formato indicado por el tipo de dirección del servidor.
El valor predeterminado es la dirección IPv4 0.0.0.0.

10. En el campo Remote File Path, especifique la ruta del servidor donde desea guardar el archivo.
El nombre de ruta solo puede incluir caracteres alfabéticos, numéricos, barra diagonal, punto o guion bajo. Puede introducir hasta 160 caracteres.

11. En el campo Remote File Name, especifique un nombre de archivo de destino para el archivo que se exportará.
Puede introducir hasta 32 caracteres.

12. Si selecciona Script File en el menú File Type, especifique el nombre del archivo de script en el campo Local File Name.

13. Si selecciona SFTP, SCP o FTP en el menú Transfer Mode, especifique los siguientes ajustes:

- User Name: Especifique el nombre de usuario para el inicio de sesión remoto en el servidor.
- Password: Especifique la contraseña para el inicio de sesión remoto en el servidor.

14. Haga clic en el botón Apply.
El archivo se exporta (carga) al servidor. La página muestra información sobre el progreso de la transferencia del archivo.

Usar HTTP para exportar un archivo desde el switch a una computadora

Puede cargar (exportar) archivos de varios tipos desde el switch a una computadora mediante una sesión HTTP en su navegador web.

Para usar HTTP para exportar un archivo desde el switch a una computadora:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Export > HTTP File Export. Se muestra la página HTTP File Export.

6. En el menú File Type, seleccione el tipo de archivo que debe exportarse:

- Text Configuration: Un archivo de configuración de texto le permite editar un archivo de texto configurado (startup-config) sin conexión según sea necesario. El uso más común de la configuración de texto es cargar una configuración funcional desde un dispositivo, editarla sin conexión para personalizarla para otro dispositivo similar (por ejemplo, cambiar el nombre del dispositivo o la dirección IP) y descargarla en ese dispositivo. Es el ajuste predeterminado.
- Error Log: El registro persistente de errores del switch, también llamado registro de eventos.
- Buffered Log: El registro en búfer (en memoria) del sistema.
- Trap Log: El registro de traps con los registros de traps del switch.
- Script File: El archivo de script que debe especificar en el campo Local File Name.
- CLI Banner: El archivo de banner de CLI.
- Tech Support: El archivo de soporte técnico es un archivo de texto que contiene diversa información de hardware, software y configuración que puede ayudar a solucionar problemas del dispositivo y de la red.
- Crash Logs: Los registros de fallas del switch, si hay disponibles.
- Backup Configuration: El archivo de configuración de respaldo es un archivo de texto.
- CPU Packets Capture File: El archivo de captura de paquetes de CPU con los paquetes de CPU capturados y almacenados.
- Factory Default Configuration: El archivo de configuración predeterminada de fábrica es un archivo de texto con la configuración predeterminada de fábrica almacenada.
- DHCP Client Configuration File: El archivo de configuración del cliente DHCP con la información del servidor DHCP (host).

7. Si selecciona Script File en el menú File Type, especifique el nombre del archivo de script en el campo Local File Name.

8. Haga clic en el botón Apply.
El archivo se exporta (carga) a la computadora. La página muestra información sobre el progreso de la transferencia del archivo.

Exportar un archivo desde el switch a un dispositivo de almacenamiento USB

Solo puede cargar (exportar) un archivo de configuración de texto o una clave de licencia a un dispositivo de almacenamiento USB conectado al switch.

Para exportar un archivo desde el switch a un dispositivo de almacenamiento USB:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Export > USB File Export. Se muestra la página USB File Export.

6. En el menú File Type, seleccione el tipo de archivo que debe exportarse:

- Text Configuration: Un archivo de configuración de texto le permite editar un archivo de texto configurado (startup-config) sin conexión según sea necesario. El uso más común de la configuración de texto es cargar una configuración funcional desde un dispositivo, editarla sin conexión para personalizarla para otro dispositivo similar (por ejemplo, cambiar el nombre del dispositivo o la dirección IP) y descargarla en ese dispositivo. Es el ajuste predeterminado.
- DHCP Client Configuration File: El archivo de configuración del cliente DHCP con la información del servidor DHCP (host).

7. En el campo File Path, especifique la ruta en el dispositivo de almacenamiento USB. Puede usar hasta 146 caracteres. El valor predeterminado está en blanco.

8. En el campo USB File, especifique un nombre para el archivo. Es el nombre con el que se guardará el archivo en el dispositivo de almacenamiento USB.
Puede introducir hasta 32 caracteres.

9. Haga clic en el botón Apply.
El archivo se exporta (carga) al dispositivo de almacenamiento USB. La página muestra información sobre el progreso de la transferencia del archivo.

Actualizar el software o descargar un archivo

Puede descargar al switch archivos de firmware, configuración (ASCII), registro (ASCII log), SSL, PEM u otros tipos desde un servidor de archivos mediante una sesión TFTP, SFTP, SCP o FTP, desde una computadora mediante una sesión HTTP, o desde un dispositivo de almacenamiento USB.

Puede buscar manualmente la versión de software más reciente (también llamada versión de firmware), descargar el firmware a un servidor o computadora y luego descargar el firmware al switch. Si hay notas de la versión disponibles con el nuevo firmware, lea las notas para saber si debe reconfigurar el switch después de actualizar.

En este contexto, la descarga también se denomina actualización.
Tenga en cuenta lo siguiente sobre los archivos SSH y SSL:

- SSH: Para poder descargar archivos SSH al switch, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.
- SSL: Los archivos SSL contienen información para cifrar, autenticar y validar sesiones HTTPS. Para poder descargar archivos SSL al switch, HTTPS debe estar deshabilitado administrativamente.

Actualizar la imagen de software o descargar un archivo de un servidor al switch

Puede descargar al switch una imagen de software (firmware) y archivos de configuración, SSL, PEM u otros tipos desde un servidor TFTP, SFTP, SCP o FTP de su red.

Antes de descargar un archivo al switch, deben cumplirse las siguientes condiciones:

- El archivo que se descargará está en el servidor, en el directorio adecuado.
- El archivo tiene el formato correcto.
- El switch tiene una ruta al servidor.

Para descargar un archivo al switch desde un servidor:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión no se requiere contraseña. Sin embargo, después debe especificar una contraseña local del dispositivo para cada inicio de sesión posterior.

Se muestra la página System Information.

5. Seleccione Maintenance > Upgrade > File Upgrade. Se muestra la página File Upgrade.

6. En el menú File Type, seleccione el tipo de archivo:

• Software: La imagen del software del sistema, que se guarda en uno de dos sectores flash llamados imágenes (image1 e image2). La imagen activa almacena la copia activa, y la otra imagen almacena una segunda copia. El dispositivo arranca y funciona desde la imagen activa. Si la imagen activa está dañada, el sistema arranca automáticamente desde la imagen no activa. Es una función de seguridad ante fallas durante el proceso de actualización de arranque. Es el ajuste predeterminado.
• Text Configuration: Un archivo de configuración de texto le permite editar un archivo de texto configurado (startup-config) sin conexión según sea necesario. El uso más común de la configuración de texto es cargar una configuración funcional desde un dispositivo, editarla sin conexión para personalizarla para otro dispositivo similar (por ejemplo, cambiar el nombre del dispositivo o la dirección IP) y descargarla en ese dispositivo.
• SSH-2 RSA Key PEM File: Un archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (con codificación PEM).
• SSH-2 DSA Key PEM File: Un archivo de clave SSH-2 Digital Signature Algorithm (DSA) (con codificación PEM).
• SSL Trusted Root Certificate PEM File: Un archivo de certificado raíz de confianza SSL (con codificación PEM).
• SSL Server Certificate PEM File: Un archivo de certificado de servidor SSL (con codificación PEM) para el dispositivo.
• SSL DH 1024 Encryption Parameter PEM File: Un archivo de parámetros de cifrado SSL Diffie-Hellman de 1024 bits (con codificación PEM) para el dispositivo.
• SSL DH 2048 Encryption Parameter PEM File: Un archivo de parámetros de cifrado SSL Diffie-Hellman de 2048 bits (con codificación PEM) para el dispositivo.
• Script File: Un archivo de script de configuración de texto. Debe usar la interfaz de línea de comandos (CLI) para configurar, validar y activar el script.
• CLI Banner: El banner de CLI contiene el texto que se mostrará en la CLI antes del mensaje de inicio de sesión.
• IAS Users: El archivo de base de datos de usuarios del Internal Authentication Server (IAS). La base de datos de usuarios IAS almacena una lista de nombres de usuario y contraseñas (opcionales) para la autenticación local de usuarios basada en puertos.
• Factory Default Configuration: El archivo de configuración predeterminada de fábrica es un archivo de texto con la configuración predeterminada de fábrica almacenada.
• Public Key Configuration: El archivo de clave pública usado para validar scripts de configuración.

• Public Key Image: El archivo de clave pública usado para validar imágenes de código.
• Application: Archivos de una aplicación.
• Tech Support Commands File: Un archivo con comandos de soporte técnico.
• DHCP Client Configuration File: El archivo de configuración del cliente DHCP con la información del servidor DHCP (host).

7. Si la opción del menú File Type es Software, se muestra el menú Image Name y debe seleccionar la imagen de software que debe descargarse al switch:

• Image1: Seleccione image1 para cargar image1.
• Image2: Seleccione image2 para cargar image2.

Le recomendamos no sobrescribir la imagen activa.

8. Si la opción del menú File Type es Software, se muestran los botones de opción Verify para que pueda seleccionar una de las siguientes opciones:

• None: La verificación del archivo descargado está deshabilitada. Es el ajuste predeterminado.
• Verify: Se verifica la firma digital del archivo descargado.
• No Verify: No se verifica la firma digital del archivo descargado.

9. Si la opción del menú File Type es Application, se muestra el campo Application File Name y debe especificar el nombre del archivo de la aplicación.

10. En el menú Transfer Mode, especifique el protocolo que debe usarse para transferir el archivo al servidor:

• TFTP: Trivial File Transfer Protocol.
• SFTP: Secure File Transfer Protocol. Esta opción requiere especificar un nombre de usuario y una contraseña.
• SCP: Secure Copy Protocol. Esta opción requiere especificar un nombre de usuario y una contraseña.
• FTP: File Transfer Protocol. Esta opción requiere especificar un nombre de usuario y una contraseña.

11. En el menú Server Address Type, seleccione el formato del campo Server Address:

• IPv4: Indica que la dirección del servidor es una dirección IPv4 en formato decimal con puntos. Es el ajuste predeterminado.
• IPv6: Indica que la dirección del servidor es una dirección IPv6 en números hexadecimales con valores de 16 bits separados por dos puntos.
• DNS: Indica que la dirección del servidor es un nombre de host.

12. En el campo Server Address, introduzca la dirección IP del servidor según el formato indicado por el tipo de dirección del servidor.

El valor predeterminado es la dirección IPv4 0.0.0.0.

13. En el campo Remote File Path, especifique la ruta del servidor donde se encuentra el archivo. El nombre de ruta solo puede incluir caracteres alfabéticos, numéricos, barra diagonal, punto o guion bajo. Puede introducir hasta 160 caracteres.

14. En el campo Remote File Name, especifique el nombre del archivo que se descargará. Puede introducir hasta 32 caracteres.

15. Si selecciona SFTP, SCP o FTP en el menú Transfer Mode, especifique los siguientes ajustes:

- User Name: Especifique el nombre de usuario para el inicio de sesión remoto en el servidor.
- Password: Especifique la contraseña para el inicio de sesión remoto en el servidor.

16. Haga clic en el botón Apply.
El archivo se descarga del servidor al switch. La página muestra información sobre el progreso de la transferencia del archivo.

17. Para guardar los ajustes en la configuración en ejecución, haga clic en el icono Save.

Usar HTTP para descargar un archivo al switch o actualizar la imagen de software

Puede descargar archivos de varios tipos desde una computadora al switch mediante una sesión HTTP en su navegador web.

Para usar HTTP para descargar desde una computadora al switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Upgrade > HTTP File Upgrade. Se muestra la página HTTP File Upgrade.

• Software: La imagen del software del sistema, que se guarda en uno de dos sectores flash llamados imágenes (image1 e image2). La imagen activa almacena la copia activa, y la otra imagen almacena una segunda copia. El dispositivo arranca y funciona desde la imagen activa. Si la imagen activa está dañada, el sistema arranca automáticamente desde la imagen no activa. Es una función de seguridad ante fallas durante el proceso de actualización de arranque. Es el ajuste predeterminado.
• Text Configuration: Un archivo de configuración de texto le permite editar un archivo de texto configurado (startup-config) sin conexión según sea necesario. El uso más común de la configuración de texto es cargar una configuración funcional desde un dispositivo, editarla sin conexión para personalizarla para otro dispositivo similar (por ejemplo, cambiar el nombre del dispositivo o la dirección IP) y descargarla en ese dispositivo.
• SSH-2 RSA Key PEM File: Un archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (con codificación PEM).
• SSH-2 DSA Key PEM File: Un archivo de clave SSH-2 Digital Signature Algorithm (DSA) (con codificación PEM).
• SSL Trusted Root Certificate PEM File: Un archivo de certificado raíz de confianza SSL (con codificación PEM).
• SSL Server Certificate PEM File: Un archivo de certificado de servidor SSL (con codificación PEM) para el dispositivo.
• SSL DH 1024 Encryption Parameter PEM File: Un archivo de parámetros de cifrado SSL Diffie-Hellman de 1048 bits (con codificación PEM) para el dispositivo.
• SSL DH 2048 Encryption Parameter PEM File: Un archivo de parámetros de cifrado SSL Diffie-Hellman de 2048 bits (con codificación PEM) para el dispositivo.
• Config Script: Un archivo de script de configuración de texto. Debe usar la interfaz de línea de comandos (CLI) para configurar, validar y activar el script.
• CLI Banner: El banner de CLI contiene el texto que se mostrará en la CLI antes del mensaje de inicio de sesión.
• IAS Users: El archivo de base de datos de usuarios del Internal Authentication Server (IAS). La base de datos de usuarios IAS almacena una lista de nombres de usuario y contraseñas (opcionales) para la autenticación local de usuarios basada en puertos.
• Factory Default Configuration: El archivo de configuración predeterminada de fábrica es un archivo de texto con la configuración predeterminada de fábrica almacenada.
• Public Key Configuration: El archivo de clave pública usado para validar scripts de configuración.
• DHCP Client Configuration File: El archivo de configuración del cliente DHCP con la información del servidor DHCP (host).

6. Si la opción del menú File Type es Software, se muestra el menú Image Name y debe seleccionar la imagen de software que debe descargarse al switch:

• Image1: Seleccione image1 para cargar image1.
• Image2: Seleccione image2 para cargar image2.

Le recomendamos no sobrescribir la imagen activa.

7. Junto a Select File, haga clic en el botón Browse, vaya al archivo y selecciónelo para descargarlo.
Puede seleccionar un archivo con un nombre de hasta 80 caracteres.

8. Haga clic en el botón
Apply. Comienza la descarga.

El campo Download Status muestra el estado durante la transferencia del archivo al switch.

Nota: Después de iniciar una transferencia de archivo, espere a que la página se actualice. Cuando la página se actualiza, la opción Select File aparece en blanco, lo que indica que la transferencia del archivo se completó.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Descargar un archivo de un dispositivo de almacenamiento USB al switch

Solo puede descargar un archivo de configuración de texto o una clave de licencia de un dispositivo de almacenamiento USB al switch.

Para descargar un archivo de un dispositivo de almacenamiento USB al switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Upgrade > USB File Upgrade. Se muestra la página USB File Upgrade.

6. En el menú File Type, seleccione el tipo de archivo que debe descargarse:

• Software: La imagen del software del sistema, que se guarda en uno de dos sectores flash llamados imágenes (image1 e image2). La imagen activa almacena la copia activa, mientras que la otra almacena una segunda copia. El dispositivo arranca y funciona desde la imagen activa. Si la imagen activa está dañada, el sistema arranca automáticamente desde

la imagen no activa. Es una función de seguridad ante fallas durante el proceso de actualización de arranque. Es el ajuste predeterminado.
• Text Configuration: Un archivo de configuración de texto le permite editar un archivo de texto configurado (startup-config) sin conexión según sea necesario. El uso más común es cargar una configuración funcional desde un dispositivo, editarla sin conexión para adaptarla a otro dispositivo similar (por ejemplo, cambiar el nombre o la dirección IP) y descargarla a ese dispositivo. Es el ajuste predeterminado.
• DHCP Client Configuration File: El archivo de configuración del cliente DHCP con la información del servidor DHCP (host).

7. Si la opción del menú File Type es Software, se muestra el menú Image Name y debe seleccionar la imagen de software que debe descargarse al switch:

• Image1: Seleccione image1 para cargar image1.
• Image2: Seleccione image2 para cargar image2.

Le recomendamos no sobrescribir la imagen activa.

8. En el campo File Path, especifique la ruta en el dispositivo de almacenamiento USB. Puede usar hasta 146 caracteres. El valor predeterminado está en blanco.

9. En el campo USB File, especifique el nombre del archivo en el dispositivo de almacenamiento USB. Puede escribir hasta 32 caracteres.

10. Haga clic en el botón Apply.
El archivo se exporta (carga) al dispositivo de almacenamiento USB. La página muestra información sobre el progreso de la transferencia.

11. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Guardar (Save).

Usar una sesión HTTP para descargar e instalar un archivo de certificado de seguridad SSL en el switch

Si usa HTTPS en lugar de HTTP para acceder a la interfaz principal del navegador local, no necesita obtener un certificado SSL. La advertencia de seguridad que puede aparecer en su navegador le pide confirmar que el certificado autofirmado del switch es válido. Una vez que lo haga, es posible que la advertencia ya no aparezca al iniciar sesión.

Sin embargo, si obtiene un certificado de seguridad SSL de una autoridad de certificación, puede descargarlo e instalarlo mediante una sesión HTTP con su navegador web.

Para un certificado de seguridad SSL, debe descargar dos archivos Privacy Enhanced Mail (PEM) al switch:

- SSL Trusted Root Certificate PEM File: El archivo PEM del certificado raíz de confianza SSL, que debe tener el formato xxxxCERTxxxxx.pem.
- SSL Server Certificate PEM File: El archivo PEM del certificado del servidor SSL (archivo de clave), que debe tener el formato xxxxKEYxxxxx.pem.

Antes de descargar e instalar un certificado de seguridad SSL, debe deshabilitar HTTPS en el switch.

Para deshabilitar HTTPS y usar una sesión HTTP para descargar e instalar un archivo de certificado de seguridad SSL en el switch:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Security > Access > HTTPS > HTTPS Configuration. Se muestra la página HTTPS Configuration.

6. Seleccione el botón de opción Admin Mode Disable.

7. Haga clic en el botón Apply.
Se guardan los ajustes. Como cambió el modo de acceso de HTTPS a HTTP, se cierra su sesión en el switch.

8. Espere un minuto, actualice el navegador y vuelva a iniciar sesión en el switch.

9. Seleccione Maintenance > Upgrade > HTTP File Upgrade. Aparece la página HTTP Firmware/File Update.

10. En el menú File Type, seleccione SSL Trusted Root Certificate PEM File.

11. Seleccione el botón Select File Browse y ubique el archivo que desea descargar. Es el archivo de certificado, que debe tener el formato xxxxCERTxxxxx.pem.

12. Haga clic en el botón Apply.
Comienza la transferencia del archivo.

La página muestra información sobre el progreso de la transferencia. La página se actualiza automáticamente al completarse la transferencia (o si falla).

13. En el menú File Type, seleccione SSL Server Certificate PEM File.
Es el archivo de clave, que debe tener el formato xxxxKEYxxxxx.pem.

14. Seleccione el botón Select File Browse y ubique el archivo que desea descargar. El nombre del archivo puede tener hasta 80 caracteres.

15. Haga clic en el botón Apply.
Comienza la transferencia del archivo.

La página muestra información sobre el progreso de la transferencia. La página se actualiza automáticamente al completarse la transferencia.

16. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Administrar imágenes de software

El switch conserva dos versiones de su software en almacenamiento permanente. Una imagen es la activa y la otra es la de respaldo. La imagen activa se carga cuando el switch arranca o se reinicia. Esta función reduce el tiempo de inactividad del switch cuando actualiza su software.

Copiar una imagen de software

Puede copiar una imagen de software de una ubicación (principal o de respaldo) a otra.

Para copiar una imagen de software:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Image Management > Copy. Aparece la página Copy.

6. Seleccione el botón de opción Source Image Image1 o Image2 para especificar la imagen que se copiará.

7. Seleccione el botón de opción Destination Image Image1 o Image2 para especificar la imagen de destino.

8. Haga clic en el botón Apply. Se copia la imagen.

9. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Configurar los ajustes de imagen dual

La función Dual Image permite al switch conservar dos imágenes en almacenamiento permanente. Puede seleccionar qué imagen se cargará al reiniciar, especificar una descripción de la imagen o eliminar una imagen. Esta función reduce el tiempo de inactividad del switch al actualizar o revertir la imagen de software.

Cambiar la imagen de software que se carga al arrancar o reiniciar el switch

Para cambiar la imagen que se carga durante el arranque:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Image Management > Dual Image Configuration. Aparece la página Dual Image Configuration.

6. Seleccione la casilla de la imagen que no es la activa (es decir, la imagen cuyo campo Active Image muestra False) pero que desea que el switch ejecute después del reinicio.

7. En el menú Next Active Image, seleccione True.

8. Opcionalmente, especifique un nombre para la imagen seleccionada escribiéndolo en el campo Image Description.

9. Haga clic en el botón Apply.
Se guarda la configuración.

10. Para guardar la configuración en la configuración en ejecución, haga clic en el icono Save.

11. Después de activar la imagen, reinicie el switch (consulte Reiniciar el switch desde la interfaz principal del navegador local en la página 737).
Si no reinicia el switch, este sigue ejecutando la imagen que se muestra en el campo Current-active hasta el siguiente reinicio.

La siguiente tabla describe la información no configurable de la página.

Tabla 175. Información de configuración de imagen dual

Campo	Descripción
Image Name	El nombre de la imagen. De forma predeterminada, los nombres son image1 e image2.
Active Image	La imagen activa actual (True o False).
Version	La versión de firmware de la imagen.

Eliminar una imagen de software Para eliminar una imagen de software:
1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Image Management > Dual Image Configuration. Aparece la página Dual Image Configuration.

6. Seleccione la casilla de la imagen que no es la activa (es decir, la imagen cuyo campo Active Image muestra False)
No puede eliminar la imagen activa. Para la imagen activa actual, el campo Active Image muestra True.

7. Haga clic en el botón
Delete. Se elimina la imagen.

8. Para guardar la configuración en la configuración en ejecución, haga clic en el ícono Save.

Diagnóstico y solución de problemas

Puede enviar un ping, rastrear una ruta y realizar un volcado de memoria.

Hacer ping a una dirección IPv4

Puede configurar el switch para enviar una solicitud de ping a una dirección IPv4 especificada. Puede usar esta opción para comprobar si el switch puede comunicarse con un dispositivo IPv4 específico. Al enviar un ping, el switch envía un número especificado de solicitudes de ping y se muestran los resultados.

Si se recibe una respuesta al ping, aparece el siguiente mensaje:

```
PING x.y.z.w (x.y.z.w): size data bytes
```

```
size bytes from x.y.z.w: seq=0 ttl=xyz
```

```
--- x.y.z.w ping statistics ---
```

```
count packets transmitted, count packets received, x% packet loss
```

Si no se recibe respuesta al ping, aparece el siguiente mensaje:

```
PING x.y.z.w (x.y.z.w): size data bytes
```

```
--- x.y.z.w ping statistics ---
```

```
count packets transmitted, 0 packets received, 100% packet loss
```

Para hacer ping a una dirección IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Troubleshooting > Ping IPv4. Aparece la página Ping IPv4.

6. En el campo IP Address/Host Name, escriba la dirección IP o el nombre de host del dispositivo al que se hará ping.
El formato es x.x.x.x. El número máximo de caracteres es 255.

7. En el campo Count, escriba el número de solicitudes de eco que se enviarán. El valor predeterminado es 3. El rango es de 1 a 15.

8. En el campo Interval (secs), escriba el tiempo entre paquetes de ping en segundos. El valor predeterminado es 3 segundos. El rango es de 1 a 60.

9. En el campo Datagram Size, escriba el tamaño del paquete de ping. El valor predeterminado es 0 bytes. El rango es de 0 a 13000.

10. En el menú Source, opcionalmente, puede seleccionar la dirección IP o la interfaz que se usará para enviar los paquetes de solicitud de eco:

- None: La dirección de origen del paquete de ping es la de la interfaz de salida predeterminada.
- IP Address: La dirección IP de origen que se usará al enviar los paquetes de solicitud de eco. Con esta opción, aparece el campo IP Address y debe escribir la dirección IPv4 que se usará como origen.
- Interface: La interfaz que se usará al enviar los paquetes de solicitud de eco. Aparece el menú Interface, pero la única opción disponible es Network.

11. Haga clic en el botón Apply.
Se hace ping a la dirección especificada. Los resultados se muestran debajo de los datos configurables, en el campo Results.

Hacer ping a una dirección IPv6

Puede configurar el switch para enviar una solicitud de ping a una dirección IPv6 especificada. Puede usar esta opción para comprobar si el switch puede comunicarse con un dispositivo IPv6 específico. Al enviar un ping, el switch envía un número especificado de solicitudes de ping y se muestran los resultados.

Si se recibe una respuesta al ping, aparece el siguiente mensaje:

```
PING x:y::z:w (x:y::z:w): size data bytes
```

```
size bytes from x:y::z:w: seq=0 ttl=xyz
```

```
--- x:y::z:w ping statistics ---
```

```
count packets transmitted, count packets received, x% packet loss
```

Si no se recibe respuesta al ping, aparece el siguiente mensaje:

```
PING x:y::z:w (x:y::z:w): size data bytes
```

```
--- x:y::z:w ping statistics ---
```

```
count packets transmitted, 0 packets received, 100% packet loss
```

Para hacer ping a una dirección IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Troubleshooting > Ping IPv6. Aparece la página Ping IPv6.

6. En el menú Ping, seleccione el tipo de ping:
• Global: Hace ping a una dirección IPv6 global.

- Link Local: Hace ping a una dirección IPv6 link-local a través de una interfaz especificada. Con esta opción, aparece el menú Interface y debe seleccionar la interfaz.

7. En el campo IPv6 Address/Hostname, escriba la dirección IPv6 o el nombre de host de la estación a la que se hará ping.
El formato es xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. El número máximo de caracteres es 255.

8. En el campo Count, escriba el número de solicitudes de eco que se enviarán. El rango es de 1 a 15. El valor predeterminado es 3.

9. En el campo Interval (secs), escriba el tiempo en segundos entre paquetes de ping. El rango es de 1 a 60. El valor predeterminado es 3.

10. En el campo Datagram Size, escriba el tamaño del datagrama.
El rango válido es de 0 a 13000. El valor predeterminado es 0 bytes.

11. En el menú Source, opcionalmente, puede seleccionar la dirección IP o la interfaz que se usará para enviar los paquetes de solicitud de eco:

- None: La dirección de origen del paquete de ping es la de la interfaz de salida predeterminada.
- IPv6 Address: La dirección IP de origen que se usará al enviar los paquetes de solicitud de eco. Con esta opción, aparece el campo IPv6 Address y debe escribir la dirección IPv6 que se usará como origen.
- Interface: La interfaz que se usará al enviar los paquetes de solicitud de eco. Aparece el menú Interface y debe seleccionar la interfaz.

12. Haga clic en el botón Apply.
Se hace ping a la dirección especificada. Los resultados se muestran debajo de los datos configurables, en el campo Results.

Enviar un traceroute IPv4

Puede configurar el switch para enviar una solicitud de traceroute a una dirección IPv4 o nombre de host especificado. Así puede descubrir las rutas que siguen los paquetes hacia un destino remoto. Al enviar un traceroute, el switch muestra los resultados debajo de los datos configurables.

Si se recibe una respuesta al traceroute, aparece el siguiente mensaje:

```
traceroute to x.y.z.w (x.y.z.w), maxTTL hops max, size byte packets
```

```
initTTL x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

```
initTTL+1 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

```
initTTL+2 x.y.z.w (x.y.z.w) 0.000 ms * 0.000 ms
```

Para enviar un traceroute IPv4:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Troubleshooting > Traceroute IPv4. Aparece la página Traceroute IPv4.

6. En el campo IP Address/Hostname, escriba la dirección IP o el nombre de host del dispositivo cuya ruta desea descubrir.

7. En el campo Probes Per Hop, escriba el número de sondeos por salto. El valor predeterminado es 3. El rango es de 1 a 10.

8. En el campo Max TTL, escriba el tiempo de vida (TTL) máximo para el destino. El valor predeterminado es 30. El rango es de 1 a 255.

9. En el campo Init TTL, escriba el TTL inicial que se usará.
El valor predeterminado es 1. El rango es de 1 a 255.

10. En el campo MaxFail, escriba el número máximo de fallas permitidas en la sesión. El valor predeterminado es 5. El rango es de 1 a 255.

11. En el campo Interval (secs), escriba el tiempo entre sondeos en segundos. El valor predeterminado es 3. El rango es de 1 a 60.

12. En el campo Port, escriba el puerto UDP de destino de los paquetes de sondeo. El valor predeterminado es 33434. El rango es de 1 a 65535.

13. En el campo Size, escriba el tamaño de los paquetes de sondeo. El valor predeterminado es 0. El rango es de 0 a 39936.

14. En el menú Source, opcionalmente, puede seleccionar la dirección IP o la interfaz que se usará para enviar los paquetes de sondeo:

- None: La dirección de origen del paquete de sondeo es la de la interfaz de salida predeterminada.
- IP Address: La dirección IP de origen que se usará al enviar los paquetes de sondeo. Con esta opción, aparece el campo IP Address y debe escribir la dirección IPv4 que se usará como origen.
- Interface: La interfaz que se usará al enviar los paquetes de sondeo. Aparece el menú Interface, pero la única opción disponible es Network.

15. Haga clic en el botón Apply.
Se envía una solicitud de traceroute a la dirección IP o nombre de host especificado. Los resultados se muestran debajo de los datos configurables, en el campo Results.

Enviar un traceroute IPv6

Puede configurar el switch para enviar una solicitud de traceroute a una dirección IPv6 o nombre de host especificado. Así puede descubrir las rutas que siguen los paquetes hacia un destino remoto. Al enviar un traceroute, el switch muestra los resultados debajo de los datos configurables.

Si se recibe una respuesta al traceroute, aparece el siguiente mensaje:

```
traceroute to x:y::z:w (x:y::z:w), maxTTL hops max, size byte packets
```

```
initTTL x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

```
initTTL+1 x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

```
initTTL+2 x:y::z:w (x:y::z:w) 0.000 ms * 0.000 ms
```

Para enviar un traceroute IPv6:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Troubleshooting > Traceroute IPv6. Aparece la página Traceroute IPv6.

6. En el campo IPv6 Address/Host Name, escriba la dirección IPv6 o el nombre de host del dispositivo cuya ruta desea descubrir.

7. En el campo Probes Per Hop, escriba el número de sondeos por salto. El valor predeterminado es 3. El rango es de 1 a 10.

8. En el campo Max TTL, escriba el tiempo de vida (TTL) máximo para el destino. El valor predeterminado es 30. El rango es de 1 a 255.

9. En el campo Init TTL, escriba el TTL inicial que se usará.
El valor predeterminado es 1. El rango es de 1 a 255.

10. En el campo MaxFail, escriba el número máximo de fallas permitidas en la sesión. El valor predeterminado es 5. El rango es de 1 a 255.

11. En el campo Interval (secs), escriba el tiempo entre sondeos en segundos. El valor predeterminado es 3. El rango es de 1 a 60.

12. En el campo Port, escriba el puerto UDP de destino de los paquetes de sondeo. El valor predeterminado es 33434. El rango es de 1 a 65535.

13. En el campo Size, escriba el tamaño de los paquetes de sondeo. El valor predeterminado es 0. El rango es de 0 a 39936.

14. En el menú Source, opcionalmente, puede seleccionar la dirección IP o la interfaz que se usará para enviar los paquetes de sondeo:

- None: La dirección de origen del paquete de sondeo es la de la interfaz de salida predeterminada.
- IPv6 Address: La dirección IP de origen que se usará al enviar los paquetes de solicitud de eco. Con esta opción, aparece el campo IPv6 Address y debe escribir la dirección IPv6 que se usará como origen.

• Interface: La interfaz que se usará al enviar los paquetes de solicitud de eco. Aparece el menú Interface y debe seleccionar la interfaz.

15. Haga clic en el botón Apply.
Se envía una solicitud de traceroute a la dirección IP o nombre de host especificado. Los resultados se muestran debajo de los datos configurables, en el campo Results.

Capturar paquetes

Puede capturar y almacenar paquetes en un dispositivo de almacenamiento USB.

Para iniciar la captura de paquetes:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Troubleshooting > Packet Capturing. Aparece la página Packet Capturing.

6. Junto a RPCAP USB, seleccione el botón de opción Enable.
7. En el menú Capture Mode, seleccione el tipo de tráfico que se capturará:

• ALL: Captura todo el tráfico. Es el ajuste predeterminado.
• TX: Captura solo el tráfico transmitido.
• RX: Captura solo el tráfico recibido.

8. En el campo File Name, especifique el nombre del archivo USB.
El nombre no puede incluir los siguientes símbolos: '\/:*?”<>|'. Puede especificar hasta 64 caracteres, sin contar la extensión, que se agrega automáticamente.

9. Para iniciar la captura de paquetes, haga clic en el botón Apply. Los paquetes se capturan hasta que detenga el proceso.

10. Para detener la captura de paquetes, haga lo siguiente:
a. Junto a RPCAP USB, seleccione el botón de opción Disable. b. Haga clic en el botón Apply.

Se detiene la captura de paquetes.

Realizar un volcado completo de memoria

Puede realizar un volcado completo de memoria para obtener el core dump para la solución de problemas.

Para realizar un volcado completo de memoria:

1. Abra un navegador web.

2. En el campo de dirección de su navegador web, ingrese la dirección IP del switch. Se muestra la página de inicio de sesión.

3. Haga clic en el botón Main UI Login.
La página de inicio de sesión de la UI principal se muestra en una nueva pestaña.

4. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.
La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

5. Seleccione Maintenance > Troubleshooting > Full Memory Dump. Aparece la página Full Memory Dump.

6. En el menú Protocol, seleccione el protocolo con el que se transferirá el archivo de core dump:

- None: La función de core dump está deshabilitada.
- TFTP: Los resultados se transfieren a un servidor TFTP.
- USB: Los resultados se transfieren a un dispositivo de almacenamiento USB. Es la opción predeterminada.
- FTP: Los resultados se transfieren a un servidor FTP.

7. Si selecciona TFTP o FTP en el menú Protocol, aparecen campos adicionales en la página para especificar los ajustes del servidor:

- TFTP: En el campo Server Address, especifique la dirección IP del servidor TFTP.
- FTP: Especifique los siguientes ajustes del servidor:
  - Server Address: Especifique la dirección IP del servidor FTP.
  - User Name: Especifique el nombre de usuario para el inicio de sesión remoto en el servidor.

- Password: Especifique la contraseña para el inicio de sesión remoto en el servidor.

8. En el campo File Path, especifique la ruta de la ubicación donde se guardará el archivo de core dump.

9. En el campo File Name, especifique el nombre del archivo de core dump. El nombre predeterminado es core.

10. Para agregar el nombre de host al nombre del archivo de core dump, seleccione la casilla Hostname.

11. Para agregar una marca de tiempo al nombre del archivo de core dump, seleccione la casilla Time-stamp.
Esta casilla está seleccionada de forma predeterminada.

12. Para volcar el registro del chip del switch en caso de una excepción, seleccione la casilla Switch Register Dump.

13. Seleccione una de las siguientes casillas:

• Write Core Test: Para generar un core dump de prueba sin transferirlo al servidor ni al dispositivo USB, seleccione la casilla Write Core Test.
• Write Core: Para generar un core dump y transferirlo al servidor o al dispositivo USB, seleccione la casilla Write Core.

14. Si selecciona la casilla Write Core, para guardar los ajustes actuales, seleccione la casilla Save Current Settings.
Esta casilla está seleccionada de forma predeterminada.

PRECAUCIÓN: El switch se reinicia después de hacer clic en el botón Apply.

15. Haga clic en el botón Apply.
El volcado de memoria se envía a la ubicación especificada. El switch se reinicia. El proceso tarda unos 135 segundos.

A

Ejemplos de configuración

Este apéndice contiene información sobre cómo configurar las siguientes funciones:

- Redes de área local virtuales (VLAN)
- Listas de control de acceso (ACL)
- Differentiated Services (DiffServ)
- Control de acceso 802.1X
- Multiple Spanning Tree Protocol
- Interfaces de enrutamiento VLAN

Redes de área local virtuales (VLAN)

Una red de área local (LAN) puede definirse en general como un dominio de difusión. Hubs, puentes o switches en el mismo segmento o segmentos físicos conectan todos los dispositivos de nodo final. Los nodos finales pueden comunicarse entre sí sin necesidad de un router. Los routers conectan las LAN entre sí y enrutan el tráfico al puerto adecuado.

Una LAN virtual (VLAN) es una red de área local cuya definición agrupa estaciones de trabajo con un criterio distinto de la ubicación geográfica (por ejemplo, por departamento, tipo de usuario o aplicación principal). Para que el tráfico fluya entre VLAN, debe pasar por un router, como si las VLAN estuvieran en dos LAN separadas.

Una VLAN es un grupo de computadoras, servidores y otros recursos de red que se comportan como si estuvieran conectados a un solo segmento de red, aunque no lo estén. Por ejemplo, el personal de marketing puede estar repartido por todo un edificio. Pero si todos están asignados a una sola VLAN, pueden compartir recursos y ancho de banda como si estuvieran conectados al mismo segmento. Los recursos de otros departamentos pueden ser invisibles para los miembros de la VLAN de marketing, accesibles para todos o solo para personas específicas, según cómo el administrador de TI haya configurado las VLAN.

Las VLAN ofrecen varias ventajas:

- Facilitan la segmentación de la red. Los usuarios que se comunican con más frecuencia entre sí se pueden agrupar en VLAN comunes, sin importar su ubicación física. El tráfico de cada grupo se mantiene en gran parte dentro de la VLAN, lo que reduce el tráfico innecesario y mejora la eficiencia de toda la red.
- Son fáciles de administrar. La adición de nodos, así como los traslados y otros cambios, se pueden gestionar de forma rápida y cómoda desde una interfaz de administración en lugar de desde el gabinete de cableado.
- Ofrecen mayor rendimiento. Las VLAN liberan ancho de banda al limitar el tráfico nodo a nodo y de difusión en toda la red.
- Garantizan mayor seguridad de red. Las VLAN crean límites virtuales que solo se pueden atravesar mediante un router. Así, se pueden usar medidas de seguridad estándar basadas en router para restringir el acceso a cada VLAN.

Los paquetes que recibe el switch se tratan de la siguiente manera:

- Cuando un paquete sin etiqueta entra en un puerto, se etiqueta automáticamente con el número de VLAN ID predeterminado del puerto. Cada puerto admite un ajuste de VLAN ID predeterminado configurable (el valor predeterminado es 1). El VLAN ID predeterminado de cada puerto se puede cambiar en la página Port PVID Configuration. Consulte Cambiar la configuración de VLAN ID del puerto en la página 202.

- Cuando un paquete etiquetado entra en un puerto, su etiqueta no se ve afectada por el VLAN ID predeterminado. El paquete se dirige a la VLAN especificada por su número de etiqueta de VLAN ID.
- Si el puerto por el que entra el paquete no es miembro de la VLAN especificada por la etiqueta de VLAN ID, el paquete se descarta.
- Si el puerto es miembro de la VLAN especificada por el VLAN ID del paquete, el paquete se puede enviar a otros puertos con el mismo VLAN ID.
- Los paquetes que salen del switch van etiquetados (T) o sin etiqueta (U), según el ajuste de las propiedades de membresía VLAN de ese puerto. Una U en un puerto significa que los paquetes que salen del switch por ese puerto van sin etiqueta. Por el contrario, una T significa que los paquetes que salen del switch por ese puerto se etiquetan con el VLAN ID asociado al puerto.

El ejemplo de esta sección consta de numerosos pasos que ilustran una amplia gama de configuraciones para ayudar a comprender las VLAN etiquetadas.

Ejemplos de configuración de VLAN

Este ejemplo muestra varios escenarios de uso de VLAN y describe cómo el switch maneja el tráfico etiquetado y sin etiqueta.

En este ejemplo, se crean dos nuevas VLAN, se cambia la membresía de puertos de la VLAN 1 predeterminada y se asignan puertos miembro a las dos nuevas VLAN:

1. En la página Basic VLAN Configuration (consulte VLAN en la página 190), cree las siguientes VLAN:

   • Una VLAN con VLAN ID 10.
   • Una VLAN con VLAN ID 20.

2. En la página VLAN Membership (consulte Configurar las interfaces miembro de una VLAN en la página 199), especifique la membresía VLAN de la siguiente manera:

   • Para la VLAN predeterminada con VLAN ID 1, especifique los siguientes miembros: puerto 7 (U) y puerto 8 (U).
   • Para la VLAN con VLAN ID 10, especifique los siguientes miembros: puerto 1 (U), puerto 2 (U) y puerto 3 (T).
   • Para la VLAN con VLAN ID 20, especifique los siguientes miembros: puerto 4 (U), puerto 5 (T) y puerto 6 (U).

3. En la página Port PVID Configuration (consulte Cambiar la configuración de VLAN ID del puerto en la página 202), especifique el PVID de los puertos g1 y g4 para que los paquetes que entran por estos puertos se etiqueten con el VLAN ID del puerto:

   • Puerto 1: PVID 10

• Puerto 4: PVID 20

4. Con la configuración de VLAN establecida, las siguientes situaciones producen los resultados descritos:

• Si un paquete sin etiqueta entra por el puerto 1, el switch lo etiqueta con VLAN ID 10. El paquete puede acceder a los puertos 2 y 3. Al paquete saliente se le quita la etiqueta para salir por el puerto 2 como paquete sin etiqueta. Por el puerto 3, el paquete saliente sale como paquete etiquetado con VLAN ID 10.
• Si un paquete etiquetado con VLAN ID 10 entra por el puerto 3, puede acceder a los puertos 1 y 2. Si el paquete sale por el puerto 1 o 2, se le quita la etiqueta para salir del switch como paquete sin etiqueta.
• Si un paquete sin etiqueta entra por el puerto 4, el switch lo etiqueta con VLAN ID 20. El paquete puede acceder a los puertos 5 y 6. Al paquete saliente se le quita la etiqueta y se convierte en un paquete sin etiqueta al salir por el puerto 6. Por el puerto 5, el paquete saliente sale como paquete etiquetado con VLAN ID 20.

Listas de control de acceso (ACL)

Las ACL garantizan que solo los usuarios autorizados puedan acceder a recursos específicos y bloquean cualquier intento no autorizado de acceder a los recursos de la red.

Las ACL se usan para controlar el flujo de tráfico, restringir el contenido de las actualizaciones de enrutamiento, decidir qué tipos de tráfico se reenvían o bloquean, y proporcionar seguridad a la red. Normalmente se usan en routers firewall ubicados entre la red interna y una red externa, como Internet. También se pueden usar en un router ubicado entre dos partes de la red para controlar el tráfico que entra o sale de una parte específica de la red interna. El procesamiento adicional de paquetes que requiere la función ACL no afecta el rendimiento del switch. Es decir, el procesamiento de ACL ocurre a velocidad de línea.

Las listas de acceso son un conjunto secuencial de condiciones de permiso y denegación. Este conjunto de condiciones, llamado criterio de filtrado, se aplica a cada paquete que procesa el switch o el router. El reenvío o descarte de un paquete depende de si el paquete cumple o no el criterio especificado.

El filtrado de tráfico requiere los dos pasos básicos siguientes:

1. Crear una definición de lista de acceso.
La definición incluye reglas que especifican si el tráfico que cumple el criterio se reenvía normalmente o se descarta. Además, puede asignar el tráfico que cumple el criterio a una cola específica o redirigirlo a un puerto específico. Una regla predeterminada de denegar todo es la última regla de cada lista.

2. Aplicar la lista de acceso a una interfaz en dirección de entrada.

El switch permite vincular ACL a puertos físicos y LAG. El switch admite ACL MAC y ACL IP.

Ejemplo de configuración de ACL MAC

El siguiente ejemplo muestra cómo crear una ACL basada en MAC que permite el tráfico Ethernet del departamento de Ventas en puertos específicos y deniega el resto del tráfico en esos puertos.

1. En la página MAC ACL, cree una ACL con el nombre Sales_ACL para el departamento de Ventas de su red (consulte Configurar una ACL MAC en la página 653). De forma predeterminada, esta ACL se vincula en dirección de entrada, lo que significa que el switch examina el tráfico cuando entra en el puerto.

2. En la página MAC Rules, cree una regla para Sales_ACL con los siguientes ajustes:

- **Sequence Number**: 1
- **Action**: Permit
- **Assign Queue ID**: 0
- **Match Every**: False
- **CoS**: 0
- **Destination MAC**: 01:02:1A:BC:DE:EF
- **Destination MAC Mask**: 00:00:00:00:FF:FF
- **EtherType**: User Value
- **Source MAC**: 02:02:1A:BC:DE:EF
- **Source MAC Mask**: 00:00:00:00:FF:FF
- **VLAN ID**: 2

Para obtener más información sobre las reglas de ACL MAC, consulte Configurar reglas de ACL MAC en la página 656.

3. En la página MAC Binding Configuration, asigne Sales_ACL a 6, 7 y 8, y luego haga clic en el botón Apply. (Consulte Configurar vínculos MAC en la página 660). Puede asignar un número de secuencia opcional para indicar el orden de esta lista de acceso respecto de otras listas, si ya hay alguna asignada a esta interfaz y dirección.

4. La tabla MAC Binding Table muestra la información de la interfaz y del vínculo de ACL MAC. (Consulte Mostrar o eliminar vínculos de ACL MAC en la tabla de vínculos MAC en la página 662).

La ACL Sales_ACL busca tramas Ethernet con las direcciones MAC de destino y origen y las máscaras MAC definidas en la regla. Además, la trama debe estar etiquetada con VLAN ID 2, que es la VLAN del departamento de Ventas. El valor CoS de la trama debe ser 0, que es el valor predeterminado de las tramas Ethernet. Las tramas que cumplen este criterio se

permiten en las interfaces 6, 7 y 8 y se asignan a la cola de salida de hardware 0, que es la cola predeterminada. Todo el demás tráfico se deniega explícitamente en estas interfaces. Para permitir que entre tráfico adicional por estos puertos, debe agregar una nueva regla Permit con el criterio de coincidencia deseado y vincularla a las interfaces 6, 7 y 8.

Ejemplo de configuración de ACL IP básica

El siguiente ejemplo muestra cómo crear una ACL basada en IP que impide que el tráfico IP del departamento de Finanzas se permita en los puertos asociados a otros departamentos. El tráfico del departamento de Finanzas se identifica por la dirección IP de red de cada paquete.

1. En la página IP ACL, cree una nueva ACL IP con el IP ACL ID 1. (Consulte Configurar una ACL IPv4 básica o extendida en la página 663).

2. En la página IP Rules, cree una regla para la ACL IP 1 con los siguientes ajustes:

   • Sequence Number: 1
   • Action: Deny
   • Assign Queue ID: 0 (opcional: 0 es el valor predeterminado)
   • Match Every: False
   • Source IP Address: 192.168.187.0
   • Source IP Mask: 255.255.0

   Para obtener más información sobre las reglas de ACL IP, consulte Configurar reglas para una ACL IP básica en la página 666.

3. Haga clic en el botón Add.
4. En la página IP Rules, cree una segunda regla para la ACL IP 1 con los siguientes ajustes:

   - **Sequence Number**: 2
   - **Action**: Permit
   - **Match Every**: True

5. Haga clic en el botón Add.

6. En la página IP Binding Configuration, asigne el ACL ID 1 a los puertos 2, 3 y 4, y asigne el número de secuencia 1. (Consulte Configurar vínculos de interfaz de ACL IP en la página 688).
De forma predeterminada, esta ACL IP se vincula en dirección de entrada, por lo que examina el tráfico cuando entra en el switch.

7. Haga clic en el botón Apply.

8. En la página IP Binding Table, puede ver la información de las interfaces y los vínculos de ACL IP. (Consulte Mostrar o eliminar vínculos de ACL IP en la tabla de vínculos de ACL IP en la página 690).

La ACL IP de este ejemplo detecta todos los paquetes con la dirección IP de origen y la máscara de subred de la red del departamento de Finanzas y los deniega en las interfaces 2, 3 y 4 del switch. La segunda regla permite todo el tráfico que no es de Finanzas en los puertos. La segunda regla es necesaria porque existe una regla explícita de denegar todo como regla de menor prioridad.

Servicios diferenciados (DiffServ)

Las redes IP estándar están diseñadas para ofrecer un servicio de entrega de datos de mejor esfuerzo. El servicio de mejor esfuerzo implica que la red entrega los datos de manera oportuna, aunque no hay garantía de que lo haga. En momentos de congestión, los paquetes pueden retrasarse, enviarse esporádicamente o descartarse. En aplicaciones típicas de Internet, como el correo electrónico y la transferencia de archivos, una ligera degradación del servicio es aceptable y en muchos casos imperceptible. Sin embargo, cualquier degradación puede afectar negativamente a aplicaciones con requisitos de temporización estrictos, como voz o multimedia.

La calidad de servicio (QoS) puede ofrecer una entrega de datos uniforme y predecible al distinguir los paquetes con requisitos de temporización estrictos de los que son más tolerantes al retardo. Los paquetes con requisitos estrictos reciben un tratamiento especial en una red compatible con QoS. Por ello, todos los elementos de la red deben ser compatibles con QoS. Si un nodo no puede cumplir los requisitos de temporización, se crea una deficiencia en la ruta de red y se compromete el rendimiento de todo el flujo de paquetes.

Hay dos tipos básicos de QoS:

- Servicios integrados: Los recursos de red se reparten según la solicitud y se reservan (reserva de recursos) según la política de administración de la red (por ejemplo, RSVP).
- Servicios diferenciados: Los recursos de red se reparten según la clasificación y prioridad del tráfico, dando trato preferente a los datos con requisitos de temporización estrictos.

El switch admite DiffServ.

La función DiffServ contiene varios bloques conceptuales de QoS que puede usar para construir una red de servicios diferenciados. Use estos mismos bloques de distintas maneras para crear otros tipos de arquitecturas de QoS.

Debe configurar tres bloques clave de QoS para DiffServ:

- Clase
- Política
- Servicio (la asignación de una política a una interfaz direccional)

Clase

Puede clasificar los paquetes entrantes en las capas 2, 3 y 4 inspeccionando la siguiente información de un paquete:

- Dirección MAC de origen/destino
- EtherType
- Valor de clase de servicio (prioridad 802.1p) (primera/única etiqueta VLAN)
- Rango de VLAN ID (primera/única etiqueta VLAN)
- Valor de prioridad 802.1p secundario (segunda etiqueta VLAN/interna)
- Rango de VLAN ID secundario (segunda etiqueta VLAN/interna)
- Octeto IP Service Type (también llamado bits ToS, valor Precedence, valor DSCP)
- Protocolo de capa 4 (TCP, UDP, etc.)
- Puertos de origen/destino de capa 4
- Dirección IP de origen/destino

Desde el punto de vista de DiffServ, hay dos tipos de clases:

- Clases de tráfico DiffServ
- Niveles de servicio/clases de reenvío DiffServ

Clases de tráfico DiffServ

Con DiffServ, usted define qué clases de tráfico se rastrean en una interfaz de entrada. Puede definir clasificadores BA simples (DSCP) y una amplia variedad de clasificadores multicampo (MF):

- Capa 2; capas 3 y 4 (solo IP)
- Basados en protocolo
- Basados en dirección

Puede combinar estos clasificadores con operaciones lógicas AND u OR para crear clasificadores MF complejos (especificando un tipo de clase all o any, respectivamente). Es decir, dentro de una sola clase, varios criterios de coincidencia se agrupan como una expresión AND o una expresión OR secuencial, según el tipo de clase definido. Solo se pueden anidar clases del mismo tipo; el anidamiento de clases no permite la negación (opción exclude) de la clase referenciada.

Para configurar DiffServ, debe definir los niveles de servicio, es decir, las clases de reenvío/PHB identificadas por un valor DSCP, en la interfaz de salida. Estos niveles de servicio se definen configurando clases BA para cada uno.

Crear políticas

Use las políticas DiffServ para asociar un conjunto de clases que configure con una o más instrucciones de política de QoS. El resultado de esta asociación se denomina política.

Desde la perspectiva de DiffServ, hay dos tipos de políticas:

- Política de acondicionamiento de tráfico: Política aplicada a una clase de tráfico DiffServ
- Política de aprovisionamiento de servicio: Política aplicada a un nivel de servicio DiffServ

Debe configurar manualmente las distintas instrucciones y reglas usadas en las políticas de acondicionamiento de tráfico y aprovisionamiento de servicio para lograr el funcionamiento deseado de Traffic Conditioning Specification (TCS) y Service Level Specification (SLS), respectivamente.

Política de acondicionamiento de tráfico El acondicionamiento de tráfico se refiere a las acciones realizadas sobre el tráfico entrante. Varias acciones de QoS distintas están asociadas al acondicionamiento de tráfico:

- Descarte: Descarta un paquete al llegar. Es útil para emular el funcionamiento de listas de control de acceso con DiffServ, sobre todo cuando DiffServ y ACL no pueden coexistir en la misma interfaz.
- Marcado de IP DSCP o IP precedence: Marca/remarca el código DiffServ de un paquete con el valor DSCP que representa el nivel de servicio asociado a una clase de tráfico DiffServ determinada. Como alternativa, se puede marcar/remarcar el valor IP Precedence del paquete.
- Marcado de CoS (802.1p): Establece el campo de prioridad de tres bits del primer/único encabezado 802.1p en un valor especificado cuando se transmiten paquetes de la clase de tráfico. Si no existe un encabezado 802.1p, se inserta uno. Es útil para asignar un nivel de prioridad de capa 2 según la definición de una clase de reenvío DiffServ (como el valor DSCP o IP precedence) a fin de transmitir algunas características de QoS a los switches posteriores que no revisan normalmente el valor DSCP del encabezado IP.
- Vigilancia (policing): Método para restringir el tráfico entrante asociado a una clase determinada para que cumpla los términos de la TCS. Se puede aplicar un tratamiento especial a los paquetes fuera de perfil, ya sea que excedan la especificación de conformidad o no sean conformes.
  La función DiffServ admite los siguientes tratamientos de vigilancia de tráfico (acciones):
  - drop: Se descarta el paquete
  - mark cos: Se (re)marcan los bits de prioridad de usuario 802.1p y se reenvía
  - mark dscp: Se (re)marca el DSCP del paquete y se reenvía
  - mark prec: Se (re)marca el IP Precedence del paquete y se reenvía
  - send: El paquete se reenvía sin modificación DiffServ

- Reconocimiento del modo de color: La vigilancia en DiffServ usa el modo color blind o color aware. El modo color blind ignora la coloración (marcado) del paquete entrante. El modo color aware tiene en cuenta el marcado actual del paquete al determinar el resultado de la vigilancia. Se usa una clase de tráfico auxiliar junto con la definición de vigilancia para especificar un valor de uno de los campos 802.1p, 802.1p secundario, IP DSCP o IP Precedence que designa el valor de color entrante que se usará como color conforme. Opcionalmente, también puede especificar el color del tráfico excedente.
- Conteo: Actualiza las estadísticas de octetos y paquetes para llevar el control del manejo de datos en las rutas de tráfico de DiffServ. En esta función DiffServ, el usuario no configura los contadores explícitamente; el sistema los incorpora según la política DiffServ que se crea. Para obtener más información, consulte Estadísticas de puertos y paquetes EAP en la página 695.
- Asignación de cola de QoS: Dirige un flujo de tráfico a la cola de QoS especificada. Esto permite que un clasificador de tráfico especifique cuál de las colas de hardware admitidas se usa para manejar los paquetes de la clase.
- Redirección: Envía obligatoriamente un flujo de tráfico clasificado a un puerto de salida especificado (físico o LAG). Puede ocurrir además de cualquier acción de marcado o vigilancia. También se puede especificar junto con una asignación de cola de QoS.

Ejemplo de configuración de DiffServ

Para crear una clase/política DiffServ y vincularla a una interfaz del switch, siga estos pasos:
1. En la página QoS Class Configuration, cree una nueva clase con los siguientes ajustes:

   - **Class Name**: Class1
   - **Class Type**: All

   Para obtener más información sobre esta página, consulte Configurar una clase DiffServ en la página 468.

2. Haga clic en el hipervínculo Class1 para mostrar la página DiffServ Class Configuration de esta clase.

3. Configure los siguientes ajustes para Class1:

   • Protocol Type: UDP
   • Source IP Address: 192.12.1.0.
   • Source Mask: 255.255.255.0.
   • Source L4 Port: Other, e introduzca 4567 como valor de puerto de origen.
   • Destination IP Address: 192.12.2.0.
   • Destination Mask: 255.255.255.0.
   • Destination L4 Port: Other, e introduzca 4568 como valor de puerto de destino.

   Para obtener más información sobre esta página, consulte Configurar una clase DiffServ en la página 468.

4. Haga clic en el botón Apply.

5. En la página Policy Configuration, cree una nueva política con los siguientes ajustes:

- **Policy Selector**: Policy1
- **Member Class**: Class1

Para obtener más información sobre esta página, consulte Configurar una política DiffServ en la página 480.

6. Haga clic en el botón
Add. Se agrega la política.

7. Haga clic en el hipervínculo Policy1 para mostrar la página Policy Class Configuration de esta política.

8. Configure los atributos de la política de la siguiente manera:

- **Assign Queue**: 3
- **Policy Attribute**: Simple Policy
- **Color Mode**: Color Blind
- **Committed Rate**: 1000000 Kbps
- **Committed Burst Size**: 128 KB
- **Confirm Action**: Send
- **Violate Action**: Drop

Para obtener más información sobre esta página, consulte Configurar una política DiffServ en la página 480.

9. En la página Service Configuration, marque la casilla junto a las interfaces 7 y 8 para vincular la política a estas interfaces y luego haga clic en el botón Apply. (Consulte Configurar la interfaz de servicio DiffServ en la página 489).

Todos los flujos de paquetes UDP destinados a la red 192.12.2.0 con una dirección IP de origen de la red 192.12.1.0 que incluyan un puerto de origen de capa 4 4567 y un puerto de destino 4568 de este switch en los puertos 7 y 8 se asignan a la cola de hardware 3.

En esta red, el tráfico de las aplicaciones de streaming usa el puerto UDP 4567 como origen y 4568 como destino. Este tráfico en tiempo real es sensible al tiempo, por lo que se asigna a una cola de hardware de alta prioridad. De forma predeterminada, el tráfico de datos usa la cola de hardware 0, designada como cola de mejor esfuerzo.

Además, la acción de confirmación en este flujo es enviar los paquetes con una tasa comprometida de 1000000 Kbps y un tamaño de ráfaga de 128 KB. Los paquetes que exceden la tasa comprometida y el tamaño de ráfaga se descartan.

Control de acceso 802.1X

Las redes de área local (LAN) suelen implementarse en entornos que permiten conectar físicamente dispositivos no autorizados a la infraestructura LAN, o que permiten que usuarios no autorizados

intente acceder a la LAN a través de equipos ya conectados. En estos entornos, conviene restringir el acceso a los servicios de la LAN a los usuarios y dispositivos autorizados para usarlos.

El control de acceso a la red basado en puertos aprovecha las características físicas de la infraestructura LAN para autenticar y autorizar los dispositivos conectados a un puerto LAN con características de conexión punto a punto. Si el proceso de autenticación y autorización falla, el control de acceso impide el acceso a ese puerto. En este contexto, un puerto es un punto único de conexión a la LAN, como un puerto de un bridge MAC o una asociación entre estaciones o puntos de acceso en redes LAN inalámbricas IEEE 802.11.

El estándar IEEE 802.11 describe un marco de arquitectura en el que se realizan la autenticación y las acciones consiguientes. También establece los requisitos de un protocolo entre el autenticador (el sistema que pasa una solicitud de autenticación al servidor de autenticación) y el suplicante (el sistema que solicita la autenticación), así como entre el autenticador y el servidor de autenticación.

El switch admite una VLAN de invitados, que da a los usuarios no autenticados acceso limitado a los recursos de la red.

Nota: Puede usar funciones de QoS para limitar la tasa en la VLAN de invitados y así limitar los recursos de red que ofrece.

Otra función de 802.1X es la posibilidad de configurar un puerto para habilitar o deshabilitar el reenvío de paquetes EAPoL. Puede habilitar o deshabilitar el reenvío de EAPoL cuando 802.1X está deshabilitado en el dispositivo.

Los puertos de un switch autenticador 802.1X son el medio por el que ofrece servicios a otros sistemas accesibles a través de la LAN. El control de acceso a la red basado en puertos permite controlar el funcionamiento de los puertos del switch para que el acceso a sus servicios solo lo tengan los sistemas autorizados.

El control de acceso de puertos impide el acceso no autorizado de los suplicantes a los servicios de un sistema. Controlar el acceso a un switch y a la LAN a la que está conectado puede ser conveniente para restringir el acceso a puertos de bridge públicos o a las LAN de un departamento.

El control de acceso se logra exigiendo la autenticación de los suplicantes conectados a los puertos controlados de un autenticador. El resultado de la autenticación determina si el suplicante está autorizado a acceder a los servicios de ese puerto controlado.

Una Port Access Entity (PAE) puede adoptar uno de dos roles distintos en una interacción de control de acceso:

1. Autenticador: puerto que exige autenticación antes de permitir el acceso a los servicios disponibles a través de él.

2. Suplicante: puerto que intenta acceder a los servicios que ofrece el autenticador. Además, existe un tercer rol:

3. Servidor de autenticación: realiza la función de autenticación necesaria para verificar las credenciales del suplicante en nombre del autenticador.

Los tres roles son necesarios para completar un intercambio de autenticación.

El switch solo admite el rol de autenticador, en el que la PAE se encarga de comunicarse con el suplicante. La PAE autenticadora también se encarga de enviar la información recibida del suplicante al servidor de autenticación para verificar las credenciales, lo que determina el estado de autorización del puerto. La PAE autenticadora controla el estado autorizado/no autorizado del puerto controlado según el resultado del proceso de autenticación basado en RADIUS.

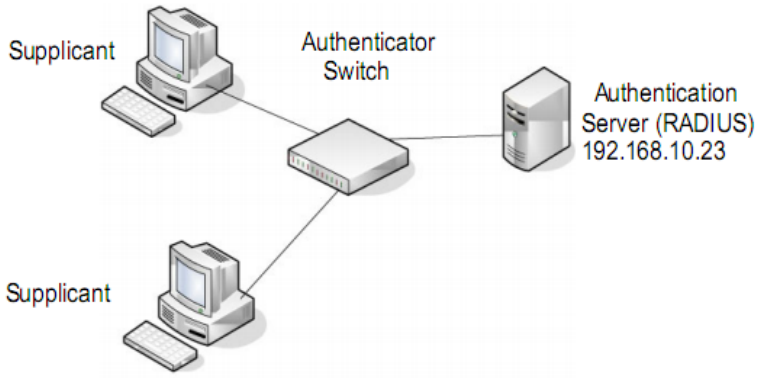


Figura 1. Roles de autenticación 802.1X

Configuración de ejemplo de 802.1X

Este ejemplo muestra cómo configurar el switch para exigir autenticación 802.1X en los puertos de una sala de juntas corporativa (5 a 8). Estos puertos están disponibles para visitantes, que deben autenticarse antes de obtener acceso a la red.

La autenticación la realiza un servidor RADIUS externo. Cuando el visitante se autentica correctamente, el tráfico se asigna automáticamente a la VLAN de invitados. Este ejemplo supone que se configuró una VLAN con ID 150 y nombre Guest.

1. En la página Port Authentication, seleccione los puertos 5, 6, 7 y 8.

2. En el menú Port Control, seleccione Unauthorized.
En todos los demás puertos que no requieren autenticación, la selección del menú Port Control debe ser Authorized. Cuando la selección del menú Port Control es Authorized, el puerto pasa incondicionalmente a un estado de autorización forzada y no requiere autenticación. Cuando la selección del menú Port Control es Auto, la PAE autenticadora define el modo del puerto controlado.

3. En el campo Guest VLAN de los puertos 5 a 8, introduzca 150 para asignar estos puertos a la VLAN de invitados.
Puede configurar parámetros adicionales para controlar el acceso a la red a través de los puertos. Consulte Configurar una interfaz de seguridad de puertos en la página 568 para más información sobre estos parámetros.

4. Haga clic en el botón Apply.

5. En la página 802.1X Configuration, establezca Port Based Authentication State y Guest VLAN mode en Enable y luego haga clic en el botón Apply (consulte Configurar el modo global de seguridad de puertos en la página 567).
Este ejemplo usa los valores predeterminados de autenticación de puertos, pero puede configurar varios parámetros adicionales. Por ejemplo, el campo EAPOL Flood Mode permite habilitar el reenvío de tramas EAPoL cuando 802.1X está deshabilitado en el dispositivo.

6. En la página RADIUS Server Configuration, configure un servidor RADIUS con los siguientes parámetros:

- **Server Address**: 192.168.10.23
- **Secret Configured**: Yes
- **Secret**: secret123
- **Active**: Primary

Para más información, consulte Servidores RADIUS en la página 500.

7. Haga clic en el botón Add.

8. En la página Authentication List, configure la lista predeterminada para usar RADIUS como primer método de autenticación (consulte Configurar una lista de autenticación de inicio de sesión en la página 514).

Este ejemplo habilita la seguridad de puertos 802.1X en el switch y solicita a los hosts conectados en los puertos 5 a 8 una autenticación 802.1X. El switch envía la información de autenticación al servidor RADIUS configurado.

Multiple Spanning Tree Protocol

Spanning Tree Protocol (STP) se ejecuta en redes con bridges para ayudar a eliminar bucles. Si se produce un bucle de bridge, la red puede saturarse de tráfico. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) admite varias instancias de spanning tree para canalizar eficientemente el tráfico VLAN por distintas interfaces. Cada instancia de spanning tree se comporta según lo especificado en IEEE 802.1w, Rapid Spanning Tree, con ligeras modificaciones en el funcionamiento pero no en el efecto final (principalmente, la transición rápida del puerto al estado de reenvío).

La diferencia entre RSTP y el STP tradicional (IEEE 802.1D) es la capacidad de configurar y reconocer la conectividad full-duplex y los puertos conectados a estaciones finales, lo que permite una transición rápida del puerto al estado Forwarding y la supresión de la notificación de cambio de topología. Estas funciones se representan con los parámetros pointtopoint y edgeport. MSTP es compatible con RSTP y STP, y se comporta de forma adecuada para bridges STP y RSTP.

Un bridge MSTP puede configurarse para comportarse totalmente como un bridge RSTP o STP. Por lo tanto, un bridge IEEE 802.1s también admite de forma inherente IEEE 802.1w e IEEE 802.1D.

El algoritmo y protocolo MSTP ofrecen conectividad simple y completa para las tramas asignadas a cualquier VLAN en una LAN con bridges formada por dispositivos de red interconectados arbitrariamente, cada uno con MSTP, STP o RSTP. MSTP permite que las tramas asignadas a distintas VLAN sigan rutas separadas, cada una basada en una Multiple Spanning Tree Instance (MSTI) independiente, dentro de regiones Multiple Spanning Tree (MST) formadas por LAN o bridges MSTP. Estas regiones y los demás bridges y LAN se conectan en un único Common Spanning Tree (CST). (IEEE DRAFT P802.1s/D13)

MSTP conecta todos los bridges y LAN con un único Common and Internal Spanning Tree (CIST). El CIST permite determinar automáticamente cada región MST, eligiendo su máxima extensión posible. La conectividad calculada para el CIST proporciona el CST para interconectar estas regiones y un Internal Spanning Tree (IST) dentro de cada región. MSTP garantiza que las tramas con un ID de VLAN se asignen a una sola MSTI o al IST dentro de la región, que la asignación sea coherente en todos los dispositivos de red de la región y que la conectividad estable de cada MSTI e IST en el límite de la región coincida con la del CST. Así, la topología activa estable de la LAN con bridges, respecto a las tramas clasificadas de forma coherente en cualquier VLAN, conecta de forma simple y completa todas las LAN y dispositivos de red de la red, aunque las tramas de distintas VLAN pueden seguir rutas diferentes dentro de una región, según IEEE DRAFT P802.1s/D13.

Todos los bridges, ya usen STP, RSTP o MSTP, envían información en mensajes de configuración mediante Bridge Protocol Data Units (BPDU) para asignar roles de puerto que determinan la participación de cada puerto en una topología activa simple y completamente conectada basada en uno o más spanning trees. La información comunicada se conoce como vector de prioridad de spanning tree. La estructura de BPDU es distinta para cada uno de estos protocolos. Un

bridge MSTP transmite la BPDU adecuada según el tipo de BPDU recibida en un puerto determinado.

Una región MST está formada por uno o más bridges MSTP con el mismo identificador de configuración MST, que usan las mismas MSTI y sin bridges conectados que no puedan recibir ni transmitir BPDU MSTP. El identificador de configuración MST incluye los siguientes componentes:

1. Selector de formato del identificador de configuración
2. Nombre de la configuración
3. Nivel de revisión de la configuración

4. Resumen de configuración: firma de 16 bytes de tipo HMAC-MD5 creada a partir de la tabla de configuración MST (asignación de ID de VLAN a MSTID)

Como existen varias instancias de spanning tree, el estado MSTP se mantiene por puerto y por instancia (o por puerto y por VLAN, ya que cada VLAN puede estar en una sola MSTI o CIST). Por ejemplo, el puerto A puede estar reenviando en la instancia 1 mientras descarta en la instancia 2. Los estados de puerto cambiaron respecto a la especificación IEEE 802.1D.

Para admitir varios spanning trees, configure un bridge MSTP con una asignación inequívoca de ID de VLAN (VID) a spanning trees. Para ello, asegúrese de lo siguiente:

1. La asignación de VID a FID es inequívoca.

2. Cada FID admitido por el bridge se asigna exactamente a una instancia de spanning tree.

La combinación de la asignación de VID a FID y de FID a MSTI define una asignación de VID a instancias de spanning tree, representada por la tabla de configuración MST.

Con esta asignación se garantiza que cada VLAN se asigne a una sola MSTI. El CIST también es una instancia de spanning tree, con MSTID 0.

Es posible que algunos VID no se asignen a una instancia, pero cada VLAN debe asignarse a una de las demás instancias de spanning tree.

La parte de la topología activa de la red que conecta dos bridges cualesquiera de la misma región MST atraviesa solo bridges MST y LAN de esa región, y nunca bridges de ningún tipo fuera de ella. Es decir, la conectividad dentro de la región es independiente de la conectividad externa.

Configuración de ejemplo de MSTP

Este ejemplo muestra cómo crear una instancia MSTP en el switch. La red de ejemplo incluye tres switches distintos que dan servicio a distintas ubicaciones de la red. En la siguiente figura, los puertos 1/0/1–1/0/5 están conectados a estaciones host, por lo que esos enlaces no están expuestos a bucles de red. Los puertos 1/0/6–1/0/8 están conectados entre los switches 1, 2 y 3.

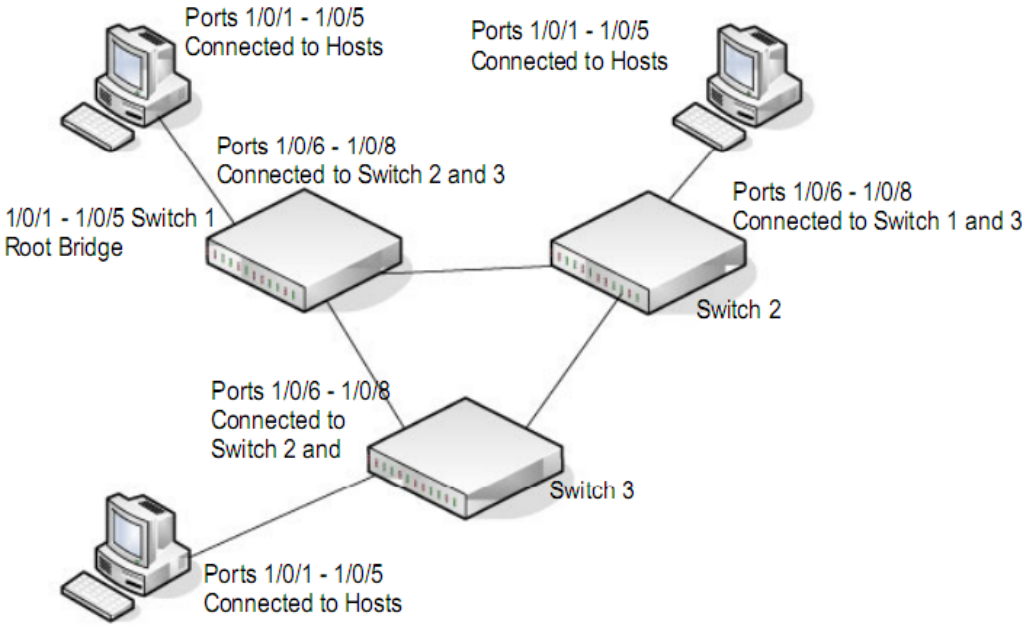


Figura 2. Configuración de ejemplo de MSTP

Realice los siguientes procedimientos en cada switch para configurar MSTP:

1. Use la página VLAN Configuration para crear las VLAN 300 y 500 (consulte Cambiar la asignación interna de VLAN en la página 193).

2. En la página VLAN Membership, incluya los puertos 1 a 8 como miembros etiquetados (T) o sin etiqueta (U) de la VLAN 300 y la VLAN 500 (consulte Cambiar la asignación interna de VLAN en la página 193).

3. En la página STP Configuration, habilite la opción Spanning Tree State (consulte Configurar CST en interfaces en la página 231).
Use los valores predeterminados para el resto de la configuración de STP. De forma predeterminada, el modo de operación STP es MSTP y el nombre de configuración es la dirección MAC del switch.

4. En la página CST Configuration, defina la prioridad de bridge de cada uno de los tres switches para forzar que Switch 1 sea el bridge raíz:

- **Switch 1**: 4096
- **Switch 2**: 12288
- **Switch 3**: 20480

Nota: Los valores de prioridad de bridge son múltiplos de 4096.

Si no especifica un bridge raíz y todos los switches tienen la misma prioridad de bridge, se elige como bridge raíz el switch con la dirección MAC más baja (consulte Configurar CST y mostrar el estado de CST en la página 229).

5. En la página CST Port Configuration, seleccione los puertos 1 a 8 y seleccione Enable en el menú STP Status (consulte Configurar CST en interfaces en la página 231).

6. Haga clic en el botón Aplicar (Apply).

7. Seleccione los puertos 1 a 5 (puertos de borde) y seleccione Enable en el menú Fast Link. Como los puertos de borde no corren riesgo de bucles, los puertos con Fast Link habilitado pasan directamente al estado de reenvío.

8. Haga clic en el botón Apply.
Puede usar la página CST Port Status para ver información de spanning tree de cada puerto.

9. En la página MST Configuration (Administrar instancias MST en la página 236), cree una instancia MST con los siguientes parámetros:

• MST ID: 1
• Priority: use el valor predeterminado (32768)
• VLAN ID: 300

10. Haga clic en el botón Add.
11. Cree una segunda instancia MST con los siguientes parámetros:

- **MST ID**: 2
- **Priority**: 49152
- **VLAN ID**: 500

12. Haga clic en el botón Add.

En este ejemplo, suponga que Switch 1 se convirtió en el bridge raíz de la instancia MST 1 y Switch 2 en el bridge raíz de la instancia MST 2. Switch 3 da servicio a hosts del departamento de ventas (puertos 1, 2 y 3) y de RR. HH. (puertos 4 y 5). Los switches 1 y 2 también incluyen hosts de ventas y de RR. HH. Los hosts conectados a Switch 2 usan la VLAN 500, instancia MST 2, para comunicarse con los hosts de Switch 3 directamente. Del mismo modo, los hosts de Switch 1 usan la VLAN 300, instancia MST 1, para comunicarse directamente con los hosts de Switch 3.

Los hosts usan distintas instancias de MSTP para aprovechar eficazmente los enlaces entre switches. El mismo concepto puede extenderse a otros switches y más instancias de MSTP.

Interfaces de enrutamiento de VLAN

Las VLAN dividen los dominios de broadcast en un entorno LAN. Cuando los hosts de una VLAN deben comunicarse con hosts de otra VLAN, el tráfico debe enrutarse entre ellas.

Esto se conoce como enrutamiento entre VLAN. En el switch, se logra creando interfaces de capa 3 (switch virtual interfaces [SVI]).

Cuando un puerto está habilitado para bridging (predeterminado) en lugar de enrutamiento, se realiza todo el procesamiento normal de bridge para un paquete entrante, que luego se asocia a una VLAN. Su dirección MAC de destino (MAC DA) y su ID de VLAN se usan para buscar en la tabla de direcciones MAC. Si el enrutamiento está habilitado para la VLAN y la MAC DA de un paquete unicast entrante es la de la interfaz interna bridge-router, el paquete se enruta. Un paquete multicast entrante se reenvía a todos los puertos de la VLAN, más la interfaz interna bridge-router, si se recibió en una VLAN enrutada.

Como un puerto puede pertenecer a más de una VLAN, el enrutamiento de VLAN puede habilitarse para todas las VLAN del puerto o para un subconjunto. El enrutamiento de VLAN puede usarse para que más de un puerto físico resida en la misma subred. También puede usarse cuando una VLAN abarca varias redes físicas o cuando se requiere segmentación o seguridad adicional. Un puerto puede ser un puerto VLAN o un puerto de router, pero no ambos. Sin embargo, un puerto VLAN puede formar parte de una VLAN que a su vez es un puerto de router.

Complete estos pasos para configurar un switch para el enrutamiento entre VLAN en IPv4:

1. Use la página IP Configuration para habilitar el enrutamiento IPv4 en el switch. De forma predeterminada, el enrutamiento IPv4 está habilitado. Para más información, consulte Administrar el enrutamiento IPv4 global en la página 342.

2. Determine las direcciones IP que desea asignar a la interfaz VLAN del switch. Para que el switch pueda enrutar entre VLAN, las interfaces VLAN deben tener una dirección IP. Cuando el switch recibe un paquete destinado a otra subred o VLAN, consulta la tabla de enrutamiento para determinar adónde reenviar el paquete. Luego, el paquete pasa a la interfaz VLAN de destino y se envía al puerto donde está conectado el dispositivo final.

3. Use la página VLAN Static Routing Wizard para crear una VLAN de enrutamiento, configurar la dirección IP y la máscara de subred, y agregar los puertos miembros. Para más información, consulte Crear una VLAN de enrutamiento con el asistente de enrutamiento estático de VLAN en la página 374.

B

Configuración predeterminada del software y especificaciones de hardware

Este apéndice contiene las siguientes secciones:

- Acceso predeterminado a la interfaz del switch
- Valores predeterminados de funciones del sistema
- Valores predeterminados de funciones de conmutación
- Valores predeterminados de enrutamiento y multicast
- Valores predeterminados de QoS
- Valores predeterminados de seguridad
- Valores predeterminados de monitoreo
- Especificaciones técnicas de hardware por modelo
- Especificaciones técnicas generales de hardware

Nota: Para más información sobre las especificaciones y capacidades del switch, incluidos los valores máximos de muchas funciones, consulte la hoja de datos, que puede descargar en netgear.com/support/download/.

Acceso predeterminado a la interfaz del switch

La siguiente tabla describe la configuración predeterminada de acceso a la interfaz del switch.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 176. Configuración predeterminada de acceso a la interfaz del switch

Función	Predeterminado
Dirección IP de la VLAN de administración	169.254.100.100
Dirección IP del puerto de servicio	192.168.0.239
Máscara de subred	255.255.0.0
Gateway predeterminado	0.0.0.0
ID de la VLAN de administración	1
Protocolo del puerto de servicio	Cliente DHCP habilitado
Usuario admin	admin (acceso de lectura/escritura) Sin contraseña (es decir, en blanco) En el primer inicio de sesión, el usuario admin debe definir una contraseña.
Usuario guest	guest (acceso de solo lectura) Sin contraseña (es decir, en blanco) En el primer inicio de sesión, el usuario guest debe definir una contraseña.
Longitud mínima de las contraseñas admin y guest	Ocho caracteres
Modo de administración IPv6	Habilitado
Autoconfiguración de direcciones IPv6	Deshabilitado
DHCPv6	Deshabilitado

Valores predeterminados de funciones del sistema

La siguiente tabla describe la configuración predeterminada de las funciones del sistema que puede configurar.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 177. Valores predeterminados de funciones del sistema

Nombre de función/parámetro	Predeterminado
Hora, global	
Fuente de reloj	SNTP
Modo de cliente SNTP	Unicast
Puerto	123
Interfaz de origen	VLAN 1
Intervalo de sondeo unicast	6
Intervalo de sondeo broadcast	6
Tiempo de espera de sondeo unicast	5
Reintentos de sondeo unicast	1
Horas de desfase	0
Minutos de desfase	0
Hora, servidor SNTP	
Tipo de servidor	DNS (para cada servidor predeterminado)
Dirección	time-a.netgear.com time-c.netgear.com
Puerto	123 (para cada servidor predeterminado)
Prioridad	1 (para cada servidor predeterminado)
Versión	4 (para cada servidor predeterminado)
Hora, horario de verano	
Horario de verano	Deshabilitado
DNS	
Estado de DNS	Habilitado
Número de reintentos	2
Tiempo de espera de respuesta	3
Interfaz de origen	VLAN 1
Servidor DNS	8.8.8.8
Preferencia de plantilla SDM	

Tabla 177. Valores predeterminados de funciones del sistema (continuación)

Nombre de función/parámetro	Predeterminado
Preferencia de plantilla SDM	IPv4- Basic
Green Ethernet, global	
Modo Auto Power Down	Deshabilitado
Modo EEE	Deshabilitado
Green Ethernet, interfaz	
Modo Auto Power Down	Deshabilitado
Modo EEE	Deshabilitado
Modo admin. de Energy Detect	Deshabilitado
Modo admin. de EEE	Deshabilitado
Tiempo de inactividad de transmisión EEE	600
Tiempo de activación de transmisión EEE	17
Historial LPI de Green Ethernet	
Intervalo de muestreo	3600
Máximo de muestras a conservar	168
Bonjour	
Modo administrativo	Habilitado
Precision Time Protocol, global e interfaz	
Modo administrativo/configurado	Deshabilitado
Servidor DHCP Sin servidores DHCP configurados	
Modo administrativo	Deshabilitado
Número de paquetes ping	2
Modo de registro de conflictos	Habilitado
Modo automático de Bootp	Deshabilitado
Relay DHCP Sin relays DHCP configurados	
Número máximo de saltos	4
Modo administrativo	Deshabilitado

Tabla 177. Valores predeterminados de funciones del sistema (continuación)

Nombre de función/parámetro	Predeterminado
Tiempo mínimo de espera	0
Modo de opción Circuit ID	Ninguno
Modo de anulación de servidor	Deshabilitado
Relay DHCP L2, global Sin relays DHCP L2 configurados	
Modo administrativo	Deshabilitado
Relay DHCP L2, interfaz	
Modo administrativo	Deshabilitado
Modo de confianza de opción 82	Deshabilitado
Relay UDP Sin relays UDP configurados	
Modo administrativo	Deshabilitado
Servidor DHCPv6, global e interfaz **Sin servidores DHCPv6 configurados**	
Modo administrativo	Deshabilitado
Relay DHCPv6 Sin relays DHCPv6 configurados	
Modo administrativo	Deshabilitado
PoE (solo modelos PoE+ y PoE++)	
Umbral de uso del sistema	90 por ciento
Modo de administración de energía	Dinámico
Traps	Habilitado
Potencia	Habilitado
Prioridad de puerto	Baja
Modo de potencia	• 802.3at para modelos PoE+ • 802.3bt para modelos PoE++
Tipo de límite de potencia	Clase
Tipo de detección	4ptdot3af
Programa de temporizador	Ninguno

Tabla 177. Valores predeterminados de funciones del sistema (continuación)

Nombre de función/parámetro	Predeterminado
SNMPv1/v2	
Configuración de comunidad	Ninguno
Configuración de traps	Ninguno
Indicadores de trap SNMPv1/v2	
Autenticación	Habilitado
Enlace activo/inactivo	Habilitado
Varios usuarios	Habilitado
Spanning tree	Habilitado
ACL	Deshabilitado
Portal cautivo	Deshabilitado
PIM	Deshabilitado
PoE	Habilitado
SNMPv3	
Nombre de usuario	admin
Modo de acceso SNMPv3	Lectura/escritura
Protocolo de autenticación	MD5
Clave de autenticación	password
Protocolo de cifrado	Ninguno
Clave de cifrado	
Configuración de traps	Ninguno
LLDP, global	
Intervalo de anuncio de TLV	30
Multiplicador de retención	4
Retardo de reinicialización	2
Retardo de transmisión	5
LLDP, interfaz	
Transmisión	Habilitado

Tabla 177. Valores predeterminados de funciones del sistema (continuación)

Nombre de función/parámetro	Predeterminado
Recepción	Habilitado
Notificar	Habilitado
TLV opcionales (descripción de puerto, nombre del sistema, descripción y capacidades del sistema)	Todos habilitados
Información de administración	Habilitado
LLDP-MED, global	
Número de repeticiones de inicio rápido	3
LLDP-MED, interfaz	
Estado de MED	Habilitado
Estado de notificación	Habilitado
Valores TLV de transmisión (capacidades MED, política de red, identificación de ubicación, MDI-PSE extendido, información de inventario)	Todos habilitados
Dependencias de enlace **Ninguno configurado**	
ISDP, global	
Modo administrativo	Habilitado
Temporizador	30
Tiempo de retención	180
Anuncios de versión 2	Habilitado
ISDP, interfaz	
Modo administrativo	Habilitado
Programas de temporizador Sin programas de temporizador configurados	

Configuración predeterminada de las funciones de conmutación

La siguiente tabla describe la configuración predeterminada de las funciones de conmutación que puede configurar.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 178. Configuración predeterminada de las funciones de conmutación

Nombre de función/parámetro	Predeterminado
VLAN, global	
Base de asignación de VLAN interna	4093
Política de asignación de VLAN interna	Ascendente
ID de VLAN predeterminada	1 (todos los puertos son miembros)
Nombre de VLAN predeterminada	default
Trunking de VLAN, global	
Modo administrativo	Habilitado
Puertos del switch, interfaz	
Modo de puerto del switch	General
ID de VLAN de acceso	1
ID de VLAN nativa	1
VLAN permitidas en trunk	1–4093
PVID de puertos, interfaz	
PVID	1
Miembro de VLAN	1
Etiqueta VLAN	Ninguno
Tramas aceptables	Admit All
Filtrado de entrada	Deshabilitado
Prioridad de puerto	0
DVLAN, interfaz	
Modo administrativo	Deshabilitado
VLAN de voz, global	
Modo administrativo	Deshabilitado
VLAN de voz, interfaz	
Modo de interfaz	Deshabilitado
Valor	0
Modo de anulación de CoS	Deshabilitado

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
Modo de autenticación	Habilitado
Valor DSCP	0
GARP, global	
Modo GVRP	Deshabilitado
Modo GMRP	Deshabilitado
GARP, interfaz	
Modo GVRP	Deshabilitado
Modo GMRP	Deshabilitado
Temporizador Join	20
Temporizador Leave	60
Temporizador Leave all	1000
Auto-VoIP basado en protocolo, global	
Tipo de priorización	Clase de tráfico
Valor de clase	7
Auto-VoIP basado en protocolo, interfaz	
Modo Auto-VoIP	Deshabilitado
Auto-VoIP basado en OUI, global	
ID de VLAN de Auto-VoIP	Ninguno (0)
Prioridad basada en OUI	7
Tabla OUI	00:01:E3 SIEMENS 00:03:6B CISCO1 00:12:43 CISCO2 00:0F:E2 H3C 00:60:B9 NITSUKO 00:D0:1E PINTEL 00:E0:75 VERILINK 00:E0:BB 3COM 00:04:0D AVAYA1 00:1B:4F AVAYA2 00:04:13 SNOM
Auto-VoIP basado en OUI, interfaz	
Modo Auto-VoIP	Deshabilitado

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
STP, global	
Modo administrativo de spanning tree	Habilitado
Forzar versión de protocolo	EEE 802.1w
Nombre de configuración	Dirección MAC
Nivel de revisión de configuración	0
Reenvío de BPDU con STP deshabilitado	Deshabilitado
BPDU guard	Deshabilitado
BPDU filter	Deshabilitado
Backbone rápido	Deshabilitado
Enlace ascendente rápido	Deshabilitado
Velocidad máxima de actualización	150
CST, global	
Prioridad del puente	32768
Antigüedad máxima del puente	20
Retardo de reenvío del puente	15
Saltos máximos de spanning tree	20
Conteo de retención Tx de spanning tree	6
CST, interfaz	
Prioridad de puerto	128
Puerto de borde administrativo	Deshabilitado
Costo de ruta del puerto	0
Costo de ruta de puerto calculado automáticamente	Habilitado
Costo de ruta de puerto externo	0
Costo de ruta de puerto externo calculado automáticamente	Habilitado
BPDU filter	Deshabilitado
Reenvío de BPDU	Deshabilitado
Borde automático	Habilitado

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
Root guard	Deshabilitado
Loop guard	Deshabilitado
TCN guard	Deshabilitado
Modo de puerto	Habilitado
MST, global	
MST ID	0
Prioridad	32768
VLAN ID	1
PVST, VLAN	
VLAN ID	1
Raíz	Ninguno
Tiempo de Hello	2
Tiempo de reenvío	15
Antigüedad máxima	20
Prioridad	32768
PVST, interfaz	
Prioridad	128
Costo	0
Costo calculado automáticamente	Habilitado
IGMP Snooping, global	
Modo administrativo	Habilitado
Validar encabezado IP de IGMP	Habilitado
Modo Proxy Querier	Habilitado
Modo de inundación de informes	Habilitado
Modo de exclusión de interfaz Mrouter	Habilitado
Modo de asignación automática de Fast Leave	Habilitado
Modo IGMP Plus	Habilitado

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
IGMP Snooping, interfaz	
Modo administrativo	Deshabilitado
Intervalo de membresía	600
Tiempo máximo de respuesta	120
Tiempo de vencimiento	300
Fast leave (salida rápida)	Deshabilitado
Proxy querier	Habilitado
IGMP Snooping, VLAN	
VLAN ID	1
Modo administrativo	Habilitado
Fast leave (salida rápida)	Habilitado
Intervalo de membresía	600
Tiempo máximo de respuesta	120
Tiempo de vencimiento del router multicast	300
Supresión de informes	Deshabilitado
Proxy querier	Habilitado
Modo de inundación de informes	Habilitado
Modo de exclusión de interfaz Mrouter	Habilitado
Modo IGMP Plus	Habilitado
IGMP Snooping, router multicast, interfaz	
Router multicast	Deshabilitado
IGMP Snooping, Querier, global	
Modo administrativo del Querier	Habilitado
Dirección del querier de snooping	Ninguno
Versión de IGMP	2
Intervalo de consulta	60
Intervalo de vencimiento del Querier	180

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
IGMP Snooping, Querier, VLAN	
VLAN ID	1
Modo de participación en la elección de Querier	Habilitado
Dirección VLAN del Querier	Ninguno
MLD Snooping, global	
Modo administrativo de MLD snooping	Habilitado
Modo Proxy Querier	Habilitado
Modo de inundación de informes	Habilitado
Modo de exclusión de interfaz Mrouter	Habilitado
Modo MLD Plus	Habilitado
MLD Snooping, interfaz	
Modo administrativo	Deshabilitado
Intervalo de membresía	260
Tiempo máximo de respuesta	10
Tiempo de vencimiento	300
Fast leave (salida rápida)	Deshabilitado
Proxy querier	Habilitado
MLD Snooping, VLAN	
VLAN ID	1
Fast leave (salida rápida)	Habilitado
Intervalo de membresía	260
Tiempo máximo de respuesta	10
Tiempo de vencimiento del router multicast	300
Modo Proxy Querier	Habilitado
Modo de exclusión de interfaz Mrouter	Habilitado
Modo MLD Plus	Habilitado
MLD Snooping, router multicast, interfaz	

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
Router multicast	Deshabilitado
MLD Snooping, Querier, global	
Modo administrativo del Querier	Deshabilitado
Dirección del Querier	Ninguno
Intervalo de consulta	60
Intervalo de vencimiento del Querier	60
MVR, global	
MVR en ejecución	Deshabilitado
VLAN multicast de MVR	1
Tiempo de respuesta de consulta global de MVR	5
Modo MVR	Compatible
MVR, interfaz	
Modo administrativo	Deshabilitado
Tipo	Ninguno
Salida inmediata	Deshabilitado
Tabla de direcciones	
Tiempo de envejecimiento de direcciones	3000
Puertos	
Modo STP	Habilitado
Modo administrativo	Habilitado
Modo LACP	Habilitado
Autonegociación	Habilitado
Velocidad	Auto
Modo dúplex	Auto
Trap de enlace	Habilitado
Tamaño de trama	9198
Tiempo de debounce	0

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
Control de flujo	Deshabilitado
Intervalo de carga	300
Puertos, link flaps	
Modo administrativo	Deshabilitado
Conteo máximo	5
Duración	10
Modo administrativo de recuperación automática	Deshabilitado
Intervalo de recuperación automática	300
LAG	
Modo administrativo de Auto-LAG	Habilitado
Modo de hash global de Auto-LAG	2 Dest MAC, VLAN, EType, incoming port
Nombre de LAG	ch<n>, donde n es de 1 a 8
Modo administrativo	Habilitado
Modo de hash	2 Dest MAC, VLAN, EType, incoming port
Modo STP	Deshabilitado
Modo estático	Deshabilitado
Trap de enlace	Habilitado
802.1AS, global	
Estado de 802.1AS	Deshabilitado
Prioridad2 del reloj local	248
802.1AS, interfaz	
Modo administrativo	Deshabilitado
Umbral de Pdelay	3000
Respuestas perdidas permitidas	3
Intervalo de sincronización inicial	–3
Intervalo Pdelay inicial	0
Intervalo de anuncio inicial	0

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
Tiempo de espera de SyncRx	3
Tiempo de espera de AnnounceRx	3
MRP, global	
Modo MVRP	Deshabilitado
Modo MMRP	Deshabilitado
Modo MSRP	Deshabilitado
Depuración de talkers MSRP	Deshabilitado
Máquina de estado periódica (modo MVRP)	Habilitado
Máquina de estado periódica (modo MMRP)	Habilitado
Puertos fan-in máximos de MSRP	12
Propagación de límite MSRP	Deshabilitado
Asignación 802.1qav, global	
Prioridad EAV	Clase A: 3 Clase B: 2
Prioridad de reasignación EAV	Clase A: 0 Clase B: 0
MRP, interfaz	
Modo MVRP	Deshabilitado
Modo MMRP	Deshabilitado
Modo MSRP	Deshabilitado
Temporizador Join	20
Temporizador Leave	100
Temporizador Leave all	1000
PVID de clase SR de MSRP	2
Parámetros Qav, interfaz	
Clase A, ancho de banda delta SRP	75
Clase B, ancho de banda delta SRP	0
Protección contra bucles L2, global	

Tabla 178. Configuración predeterminada de las funciones de conmutación (continuación)

Nombre de función/parámetro	Predeterminado
Modo administrativo	Deshabilitado
Intervalo de anuncio de TLV	5
Recepción máxima de PDU	1
Protección contra bucles L2, interfaz	
Keep alive	Deshabilitado
Acción RX	Deshabilitado

Configuración predeterminada de las funciones de enrutamiento y multicast

La siguiente tabla describe la configuración predeterminada de las funciones de enrutamiento y multicast que puede configurar.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 179. Configuración predeterminada de las funciones de enrutamiento y multicast

Nombre de función/parámetro	Predeterminado
Tabla de enrutamiento, preferencia de ruta	
Estática	1
RIP	120
IP, global	
Modo de enrutamiento	Habilitado
Respuestas de eco ICMP	64
Redirecciones ICMP	Deshabilitado
Intervalo del límite de velocidad ICMP	1000
Tamaño de ráfaga del límite de velocidad ICMP	100
Puerta de enlace predeterminada global	No configurado

Tabla 179. Configuración predeterminada de las funciones de enrutamiento y multicast (continuación)

Nombre de función/parámetro	Predeterminado
IP, interfaz	
Método de configuración de dirección IP	Ninguno
Dirección IP	Ninguno
Máscara de subred	Ninguno
Modo de enrutamiento	Deshabilitado
Modo administrativo	Habilitado
Reenviar broadcasts dirigidos a la red	Deshabilitado
Tipo de encapsulación	Ethernet
Proxy ARP	Habilitado
Proxy ARP local	Deshabilitado
Ancho de banda	1000000 para un enlace activo de 1 Gbps. (El ancho de banda se asigna automáticamente, pero puede cambiarlo).
Destino ICMP inalcanzable	Habilitado
Redirecciones ICMP	Deshabilitado
IP MTU	1500
IP, IP secundaria	
Dirección IP secundaria	Ninguno
Máscara de subred IP secundaria	Ninguno
IPv6, global	
Enrutamiento unicast IPv6	Deshabilitado
Límite de saltos	64
Intervalo de errores del límite de velocidad ICMPv6	1000
Tamaño de ráfaga del límite de velocidad ICMPv6	100
IPv6, interfaz	
Modo IPv6	Deshabilitado
Modo de cliente DHCPv6	Deshabilitado
Modo de autoconfiguración de direcciones sin estado	Deshabilitado

Tabla 179. Configuración predeterminada de las funciones de enrutamiento y multicast (continuación)

Nombre de función/parámetro	Predeterminado
Modo de enrutamiento	Deshabilitado
Modo administrativo	Habilitado
MTU	1500
Transmisiones de detección de direcciones duplicadas	1
Intervalo de vida útil	1800
Intervalo de NS anunciado	0
Intervalo de alcanzabilidad anunciado	0
Intervalo de anuncio	600
Indicador de configuración administrada anunciado	Deshabilitado
Indicador de otra configuración anunciado	Deshabilitado
Preferencia de router	Media
Indicador de supresión de anuncios	Deshabilitado
Destino inalcanzable	Habilitado
IPv6, preferencia de ruta	
Estática	1
ARP, global	
Tiempo de envejecimiento	1200
Tiempo de respuesta	1
Reintentos	4
Tamaño de caché	4096
Renovación dinámica	Habilitado
RIP, global	
Modo administrativo de RIP	Habilitado
Modo Split Horizon	Simple
Modo de resumen automático	Deshabilitado
Modo de aceptación de rutas de host	Habilitado
Originar información predeterminada	Deshabilitado

Tabla 179. Configuración predeterminada de las funciones de enrutamiento y multicast (continuación)

Nombre de función/parámetro	Predeterminado
Métrica predeterminada	0
RIP, interfaz	
Versión de envío	RIP-2
Versión de recepción	Ambas
Modo RIP	Deshabilitado
Tipo de autenticación	Ninguno
Clave de autenticación	Ninguno
ID de clave de autenticación	Ninguno
RIP, redistribución de rutas	
Origen	Conectada
Modo de redistribución	Deshabilitado
Métrica	0
Lista de distribución	0
Descubrimiento de routers	
Modo de anuncio	Deshabilitado
Dirección de anuncio	224.0.0.1
Intervalo máximo de anuncio	600
Intervalo mínimo de anuncio	450
Vida útil del anuncio	1800
Nivel de preferencia	0
Multicast, global	
Modo administrativo	Deshabilitado
Multicast, interfaz	
Umbral de TTL	1
Multicast, IGMP, global	
Modo administrativo	Deshabilitado
Multicast, IGMP, interfaz de enrutamiento	

Tabla 179. Configuración predeterminada de las funciones de enrutamiento y multicast (continuación)

Nombre de función/parámetro	Predeterminado
Modo administrativo	Deshabilitado
Versión	V3
Robustez	2
Intervalo de consulta	125
Tiempo máximo de respuesta a consultas	100
Intervalo de consulta de inicio	31
Número de consultas de inicio	2
Intervalo de consulta al último miembro	10
Número de consultas al último miembro	2
Multicast, IGMP, interfaz proxy	
Modo administrativo	Deshabilitado
Intervalo de informes no solicitados	1
Multicast, PIM, global	
Modo administrativo	Deshabilitado
Multicast, PIM, global	
Modo administrativo	Deshabilitado
Intervalo de Hello	30
Intervalo Join/Prune	60
Borde BSR	Deshabilitado
Prioridad de DR	1
Multicast, PIM, candidato BSR	
Longitud de máscara de hash	30
Prioridad	0
Intervalo de anuncio	60
Multicast IPv6, PIM, global	
Modo administrativo	Deshabilitado
Multicast IPv6, PIM, global	

Tabla 179. Configuración predeterminada de las funciones de enrutamiento y multicast (continuación)

Nombre de función/parámetro	Predeterminado
Modo administrativo	Deshabilitado
Intervalo de Hello	30
Intervalo Join/Prune	60
Borde BSR	Deshabilitado
Prioridad de DR	1
Multicast IPv6, PIM, candidato BSR	
Longitud de máscara de hash	126
Prioridad	0
Intervalo de anuncio	60
Multicast IPv6, MLD, global	
Modo administrativo	Deshabilitado
Multicast IPv6, MLD, interfaz de enrutamiento	
Modo administrativo	Deshabilitado
Versión	V2
Intervalo de consulta	125
Tiempo máximo de respuesta a consultas	10000
Intervalo de consulta de inicio	31
Número de consultas de inicio	2
Intervalo de consulta al último miembro	1000
Número de consultas al último miembro	2
Multicast IPv6, MLD, interfaz proxy	
Modo administrativo	Deshabilitado
Intervalo de informes no solicitados	1

Configuración predeterminada de las funciones QoS

La siguiente tabla describe la configuración predeterminada de las funciones QoS que puede configurar.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 180. Configuración predeterminada de las funciones QoS

Nombre de función/parámetro	Predeterminado
CoS, global	
Modo de confianza global	trust IP-DSCP aplicado a todas las interfaces
CoS, asignación de colas 802.1p	
Prioridad 802.1p (802.1p -> cola)	0 -> 1 1 -> 0 2 -> 0 3 -> 1 4 -> 2 5 -> 2 6 -> 3 7 -> 3
CoS, asignación de colas IP DSCP	
Prioridad IP DSCP (IP DSCP -> cola)	0 a 7 -> 1 8 a 23 - > 0 24 a 31 -> 1 32 a 47 -> 2 48 a 63 -> 3
CoS, interfaz	
Modo de confianza de interfaz	IP DSCP
Velocidad de limitación de interfaz	0
CoS, cola de interfaz	
ID de cola	0
Ancho de banda mínimo	0
Tipo de planificador	Ponderado
Tipo de administración de colas	Taildrop
CoS, preferencia de descarte de cola	
Nivel de precedencia de descarte	1 (para todas las interfaces y colas)
Umbral mínimo WRED	40 (para todas las interfaces y colas)
Umbral máximo WRED	100 (para todas las interfaces y colas)
Escala de probabilidad de descarte WRED	10 (para todas las interfaces y colas)

Tabla 180. Configuración predeterminada de las funciones QoS (continuación)

Nombre de función/parámetro	Predeterminado
DiffServ, global Sin clases, políticas ni servicios predeterminados configurados	
Modo administrativo de DiffServ	Habilitado

Configuración predeterminada de las funciones de seguridad

La siguiente tabla describe la configuración predeterminada de las funciones de seguridad que puede configurar.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 181. Configuración predeterminada de las funciones de seguridad

Nombre de función/parámetro	Predeterminado
Seguridad de administración, usuario local, contraseña	
Longitud mínima de contraseña	8
Vigencia de contraseña	0
Historial de contraseñas	0
Intentos antes del bloqueo	0
Seguridad de administración, RADIUS, global Sin servidores RADIUS configurados	
Interfaz de origen	VLAN 1
Número máximo de retransmisiones	4
Duración del tiempo de espera	5
Modo de contabilidad	Deshabilitado
Modo de atributo 4 de RADIUS	Deshabilitado
Seguridad de administración, TACACS+, global Sin servidores TACACS+ configurados	
Tiempo de espera de conexión	5
Interfaz de origen	VLAN 1

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Seguridad de administración, lista de autenticación	
defaultList	Opción 1: Local; opciones 2 a 6: N/A
networkList	Opción 1: Local; opciones 2 a 6: N/A
Seguridad de administración, lista de autenticación Enable	
enableList	Opción 1: Enabled; opción 2: None; opciones 3, 4 y 5 son N/A
enableNetList	Opción 1: Enabled; opción 2: None; opciones 3, 4 y 5 son N/A
Seguridad de administración, lista de autenticación Dot1x	
dot1xList	Deshabilitado
Seguridad de administración, lista de autenticación HTTP	
httpList	Deshabilitado
Seguridad de administración, lista de autenticación HTTPS	
httpsList	Deshabilitado
Acceso, HTTP	
Acceso HTTP	Habilitado
Puerto HTTP	80
Tiempo de espera por inactividad de sesión HTTP (minutos)	15
Tiempo de espera fijo de sesión HTTP (horas)	24
Número máximo de sesiones HTTP	16
Acceso, HTTPS	
Acceso HTTPS	Deshabilitado
Puerto HTTPS	443
Tiempo de espera por inactividad de sesión HTTPS (minutos)	15
Tiempo de espera fijo de sesión HTTPS (horas)	24
Número máximo de sesiones HTTPS	16
Acceso, SSH	
Modo administrativo de SSH	Deshabilitado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Tiempo de espera de sesión SSH	5
Número máximo de sesiones SSH	5
Lista de autenticación	networkList
Lista de autenticación Enable	enableList
Puerto SSH	22
Acceso, Telnet, lista de autenticación	
Lista de autenticación	networkList
Lista de autenticación Enable	enableList
Acceso, Telnet, Telnet entrante	
Modo administrativo del servidor Telnet	Habilitado
Permitir nuevas sesiones Telnet	Habilitado
Tiempo de espera de sesión (minutos)	5
Número máximo de sesiones	5
Acceso, Telnet, Telnet saliente	
Permitir nuevas sesiones Telnet	Habilitado
Tiempo de espera de sesión (minutos)	5
Número máximo de sesiones	5
Acceso, consola	
Tiempo de espera de inicio de sesión del puerto serie (minutos)	5
Velocidad en baudios (bps)	115200
Lista de autenticación	defaultList
Lista de autenticación Enable	enableList
Acceso, denegación de servicio	
Denegación de servicio, tamaño mínimo de encabezado TCP	20
Denegación de servicio, ICMPv4	Deshabilitado
Denegación de servicio, tamaño máximo de paquete ICMPv4	512 (si el tamaño máximo de paquete ICMPv4 está habilitado)
Denegación de servicio, ICMPv6	Deshabilitado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Denegación de servicio, tamaño máximo de paquete ICMPv6	512 (si el tamaño máximo de paquete ICMPv6 está habilitado)
Denegación de servicio, primer fragmento	Deshabilitado
Denegación de servicio, fragmento ICMP	Deshabilitado
Denegación de servicio, SIP=DIP	Deshabilitado
Denegación de servicio, SMAC=DMAC	Deshabilitado
Denegación de servicio, TCP FIN & URG & PSH	Deshabilitado
Denegación de servicio, indicador y secuencia TCP	Deshabilitado
Denegación de servicio, fragmento TCP	Deshabilitado
Denegación de servicio, desplazamiento TCP	Deshabilitado
Denegación de servicio, puerto TCP	Deshabilitado
Denegación de servicio, TCP SYN	Deshabilitado
Denegación de servicio, TCP SYN & FIN	Deshabilitado
Denegación de servicio, puerto UDP	Deshabilitado
Acceso, control de acceso, perfil de acceso Sin perfil de acceso configurado	
Autenticación de puertos, 802.1X, global	
Modo administrativo de Dot1x	Deshabilitado
Modo administrativo de autenticación	Deshabilitado
Modo de asignación de VLAN	Deshabilitado
Modo de inundación EAPOL	Deshabilitado
Modo de creación dinámica de VLAN	Deshabilitado
Modo de supervisión	Deshabilitado
Usuarios	admin
Inicio de sesión	defaultList
Autenticación de puertos, 802.1X, interfaz	
Modo de control	Auto
Modo de host	Multi-Domain-Multi-Host
MAB	Deshabilitado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Tipo de autenticación MAB	N/A
Periodo de silencio	60
Periodo de transmisión	30
ID de VLAN de invitados	0
ID de VLAN no autenticada	0
Máximo de solicitudes de reautenticación	2
Tiempo de espera del suplicante	30
Tiempo de espera del servidor	30
Máximo de solicitudes	2
Capacidades PAE	Authenticator
Reautenticación periódica	Deshabilitado
Tipo de periodo de reautenticación	Servidor
Periodo de reautenticación	0
Privilegios de usuario	admin, guest
Máximo de usuarios	48
Orden de autenticación, método 1	DOT1X
Orden de autenticación, método 2	MAB
Orden de autenticación, método 3	CAPTIVE-PORTAL
Control de tráfico, filtro MAC **Sin filtros MAC configurados**	
Control de tráfico, seguridad de puertos, administración de puertos	
Modo de seguridad de puertos	Deshabilitado
Control de tráfico, seguridad de puertos, interfaz	
Modo de seguridad	Deshabilitado
Máximo de direcciones MAC aprendidas	4096
Máximo de direcciones MAC estáticas	48
Apagado por infracción	Deshabilitado
Trap por infracción	Deshabilitado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Control de tráfico, grupo privado	
Grupos privados	Ninguno configurado
Control de tráfico, puerto protegido	
Puertos protegidos	Ninguno configurado
Control de tráfico, VLAN privada	
VLAN privadas	Ninguno configurado
Control de tráfico, control de tormentas, global	
Control de tormentas broadcast (todas)	Habilitado
Control de tormentas multicast (todas)	Deshabilitado
Control de tormentas unicast desconocido (todas)	Deshabilitado
Control de tráfico, control de tormentas, interfaz	
Tormenta broadcast, modo de recuperación	Habilitado
Tormenta broadcast, tipo de nivel de recuperación	Porcentaje
Tormenta broadcast, nivel de recuperación	5
Tormenta broadcast, acción de control	Ninguno
Tormenta multicast, modo de recuperación	Deshabilitado
Tormenta multicast, tipo de nivel de recuperación	Porcentaje
Tormenta multicast, nivel de recuperación	5
Tormenta multicast, acción de control	Ninguno
Tormenta unicast, modo de recuperación	Deshabilitado
Tormenta unicast, tipo de nivel de recuperación	Porcentaje
Tormenta unicast, nivel de recuperación	5
Tormenta unicast, acción de control	Ninguno
Control, DHCP Snooping, global	
Modo DHCP Snooping	Deshabilitado
Validación de dirección MAC	Habilitado
Control, DHCP Snooping, interfaz	

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Modo de confianza	Deshabilitado
Paquetes no válidos	Deshabilitado
Límite de velocidad (pps)	Ninguno
Intervalo de ráfaga (s)	N/A
Control, DHCP Snooping, persistente	
Almacenamiento	Local
Retardo de escritura	300
Control, DHCPv6 Snooping, global	
Modo DHCPv6 Snooping	Deshabilitado
Validación de dirección MAC	Habilitado
Control, DHCPv6 Snooping, interfaz	
Modo de confianza	Deshabilitado
Paquetes no válidos	Deshabilitado
Límite de velocidad (pps)	Ninguno
Intervalo de ráfaga (s)	N/A
Control, DHCPv6 Snooping, persistente	
Almacenamiento	Local
Retardo de escritura	300
Control, IP Source Guard, interfaz	
Modo IPSG	Deshabilitado
Seguridad de puerto IPSG	Deshabilitado
Control, IPv6 Source Guard, interfaz	
Modo IPv6SG	Deshabilitado
Seguridad de puerto IPv6SG	Deshabilitado
Control, inspección dinámica de ARP, global	
Validar MAC de origen	Deshabilitado
Validar MAC de destino	Deshabilitado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
Validar IP	Deshabilitado
Control, inspección dinámica de ARP, VLAN	
VLAN ID	1
Modo administrativo	Deshabilitado
Paquetes no válidos	Habilitado
Indicador estático	Deshabilitado
Control, inspección dinámica de ARP, interfaz	
Modo de confianza	Deshabilitado
Límite de velocidad (pps)	15
Intervalo de ráfaga (s)	1
Control, portal cautivo, global	
Modo administrativo	Habilitado
Puerto HTTP adicional	8888
Puerto HTTP seguro adicional	0
Tiempo de espera de autenticación	300
Control, portal cautivo, configuración de CP	
CP ID	1
Nombre de CP	Predeterminado
Modo administrativo	Habilitado
Protocolo	HTTP
Verificación	Invitado
Bloqueo	No bloqueado
Grupo	0
Tiempo de espera por inactividad	0
Cierre de sesión del usuario	Deshabilitado
Servidor de autenticación RADIUS	Ninguno
Modo de redirección	Deshabilitado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
URL de redirección	/v1/security/captive_portal/cp_welcome.html
Color de fondo	#BFBFBF
Color de primer plano	#999999
Color del separador	#B70024
Ancho de banda máximo de bajada	0
Ancho de banda máximo de bajada	0
Entrada máxima	0
Salida máxima	0
Total máximo	0
Control, portal cautivo, grupo de CP	
ID de grupo	1
Nombre de grupo	Predeterminado
Control, portal cautivo, indicadores de trap de CP	
Modo de trap de CP	Deshabilitado
Falla de autenticación de cliente	Ninguno
Conexión de cliente	Deshabilitado
Base de datos de clientes llena	Ninguno
Desconexión de cliente	Deshabilitado
ACL Sin ACL predeterminadas configuradas	
Número total de ACL admitidas	100. Este total aplica a todas las ACL MAC, ACL IPv4 y ACL IPv6 en conjunto.
ACL MAC	Ninguno configurado

Tabla 181. Configuración predeterminada de las funciones de seguridad (continuación)

Nombre de función/parámetro	Predeterminado
ACL IP	Ninguno configurado
ACL IPv6	Ninguno configurado

Configuración predeterminada de las funciones de supervisión

La siguiente tabla describe la configuración predeterminada de las funciones de supervisión que puede configurar.

(Los parámetros no configurables no se incluyen en la tabla, pero pueden aparecer en la hoja de datos, que puede descargar en netgear.com/support/download/).

Tabla 182. Configuración predeterminada de las funciones de supervisión

Función	Predeterminado
Registros, registro en memoria	
Estado administrativo	Habilitado
Comportamiento	Wrap (sobrescribir)
Filtro de gravedad	Notice
Umbral	80
Registros, registro de comandos	
Estado administrativo	Deshabilitado
Registros, registro de consola	
Estado administrativo	Deshabilitado
Filtro de gravedad	Error
Registros, registro de servidor	
Estado administrativo	Deshabilitado
Puerto UDP local	514
Interfaz de origen	VLAN 1s
Duplicación, duplicación de múltiples puertos, global	
ID de sesión	1

Tabla 182. Configuración predeterminada de las funciones de supervisión (continuación)

Función	Predeterminado
Modo administrativo	False
Puerto de destino	Ninguno
Tipo de filtro	Ninguno
Duplicación, duplicación de varios puertos, interfaz	
Dirección	Ninguno
Duplicación, VLAN RSPAN	
VLAN ID	1
Modo administrativo	False
Duplicación, switch de origen RSPAN, global	
ID de sesión	1
Modo administrativo	False
VLAN de destino RSPAN	Ninguno
Tipo de filtro	Ninguno
Duplicación, switch de origen RSPAN, interfaz	
Dirección	Ninguno
Duplicación, switch de destino RSPAN, global	
ID de sesión	1
Modo administrativo	False
VLAN de origen RSPAN	Ninguno
Puerto de destino RSPAN	Ninguno
Tipo de filtro	Ninguno
Agente sFlow	
Interfaz de origen	VLAN 1
Receptor sFlow	
Tiempo de espera del receptor	0
Sin tiempo de espera	False
Tamaño máximo de datagrama	1400

Tabla 182. Configuración predeterminada de las funciones de supervisión (continuación)

Función	Predeterminado
Propietario del receptor	0.0.0.0
Puerto del receptor	6343
Interfaz sFlow	
Poller, índice de receptor	0
Poller, intervalo de sondeo	0
Sampler, índice de receptor	0
Sampler, tasa de muestreo	0
Sampler, tamaño máximo de encabezado	128

Especificaciones técnicas de hardware por modelo

Las tablas de las siguientes secciones describen las especificaciones técnicas de hardware principales y exclusivas de cada modelo.

Para obtener más información de hardware, consulte la hoja de datos, que puede descargar en netgear.com/support/download/.

Modelo M4250-10G2F-PoE+ (SKU GSM4212P)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-10G2F-PoE+.

Tabla 183. Especificaciones técnicas de hardware del modelo M4250-10G2F-PoE+

Característica		Descripción
Interfaces de red		Ocho puertos RJ-45 1GBASE-T PoE+ (802.3at) Dos puertos RJ-45 1GBASE-T Dos puertos de enlace ascendente de fibra SFP de 1G.
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 3.5–2.25A
Consumo de energía	PoE máx. Sin PoE En espera	163.9W - 559.55 BTU/hr 17.32W - 59.13 BTU/hr 8.53W - 29.12BTU/hr

Tabla 183. Especificaciones técnicas de hardware del modelo M4250-10G2F-PoE+ (continuación)

Característica		Descripción
Presupuesto de energía PoE		125W
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 7.87 in (200 mm)
Peso		6.28 lb (2.850 kg)

Modelo M4250-10G2XF-PoE+ (SKU GSM4212PX)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-10G2XF-PoE+.

Tabla 184. Especificaciones técnicas de hardware del modelo M4250-10G2XF-PoE+

Característica		Descripción
Interfaces de red		Ocho puertos RJ-45 1GBASE-T PoE+ (802.3at) Dos puertos RJ-45 1GBASE-T Dos puertos de enlace ascendente de fibra SFP+ de 10G.
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 5A
Consumo de energía	PoE máx. Sin PoE En espera	306.4W - 1046.05 BTU/hr 25W - 85.35 BTU/hr 12.96W - 44.24BTU/hr
Presupuesto de energía PoE		240W
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 7.87 in (200 mm)
Peso		6.39 lb (2.900 kg)

M4250-10G2XF-PoE++ (SKU GSM4212UX)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-10G2XF-PoE++.

Tabla 185. Especificaciones técnicas de hardware del modelo M4250-10G2XF-PoE++

Característica		Descripción
Interfaces de red		Ocho puertos RJ-45 1GBASE-T PoE++ (802.3bt) Dos puertos RJ-45 1GBASE-T Dos puertos de enlace ascendente de fibra SFP+ de 10G.
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 10A
Consumo de energía	PoE máx. Sin PoE En espera	837.7W - 2859.91 BTU/hr 26.3W - 89.79 BTU/hr 18W - 61.45BTU/hr
Presupuesto de energía PoE		720W
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 10.12 in (257 mm)
Peso		8.44 lb (3.830 kg)

M4250-26G4F-PoE+ (SKU GSM4230P)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-26G4F-PoE+.

Tabla 186. Especificaciones técnicas de hardware del modelo M4250-26G4F-PoE+

Característica		Descripción
Interfaces de red		24 puertos RJ-45 1GBASE-T PoE+ (802.3at) Dos puertos RJ-45 1GBASE-T Cuatro puertos de enlace ascendente de fibra SFP de 1G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 4.4A
Consumo de energía	PoE máx. Sin PoE En espera	401W - 1369.01 BTU/hr 35.8W - 122.22 BTU/hr 23.4W - 79.89 BTU/hr
Presupuesto de energía PoE		300W

Tabla 186. Especificaciones técnicas de hardware del modelo M4250-26G4F-PoE+ (continuación)

Característica		Descripción
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 10.12 in (257 mm)
Peso		9.47 lb (4.300 kg)

M4250-26G4XF-PoE+ (SKU GSM4230PX)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-26G4XF-PoE+.

Tabla 187. Especificaciones técnicas de hardware del modelo M4250-26G4XF-PoE+

Característica		Descripción
Interfaces de red		24 puertos RJ-45 1GBASE-T PoE+ (802.3at) Dos puertos RJ-45 1GBASE-T Cuatro puertos de enlace ascendente de fibra SFP+ de 10G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 6.4–2.5A
Consumo de energía	PoE máx. Sin PoE En espera	614W - 2096.2 BTU/hr 46.8W - 159.78 BTU/hr 33.9W - 115.73 BTU/hr
Presupuesto de energía PoE		480W
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 15.75 in (400 mm)
Peso		12.02 lb (5.453 kg)

M4250-26G4F-PoE++ (SKU GSM4230UP)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-26G4F-PoE++.

Tabla 188. Especificaciones técnicas de hardware del modelo M4250-26G4F-PoE++

Característica		Descripción
Interfaces de red		24 puertos RJ-45 1GBASE-T PoE++ (802.3bt) Dos puertos RJ-45 1GBASE-T Cuatro puertos de enlace ascendente de fibra SFP de 1G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 10A por cada PSU
Consumo de energía	PoE máx. Sin PoE En espera	1 PSU: 889W - 3035.05 BTU/hr 2 PSU: 1734W - 5919.88 BTU/hr 48.8W - 166.6 BTU/hr 36.9W - 125.98 BTU/hr
Presupuesto de energía PoE		1440W con 2 PSU
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 15.75 in (400 mm)
Peso		14.87 lb (6.746 kg)

M4250-40G8F-PoE+ (SKU GSM4248P)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-40G8F-PoE+.

Tabla 189. Especificaciones técnicas de hardware del modelo M4250-40G8F-PoE+

Característica		Descripción
Interfaces de red		40 puertos RJ-45 1GBASE-T PoE+ (802.3at) Ocho puertos de enlace ascendente de fibra SFP de 1G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 6.7–2.6A
Consumo de energía	PoE máx. Sin PoE En espera	624.8W - 2133.07 BTU/hr 59.5W - 203.13 BTU/hr 46.4W - 158.41 BTU/hr
Presupuesto de energía PoE		480W

Tabla 189. Especificaciones técnicas de hardware del modelo M4250-40G8F-PoE+ (continuación)

Característica		Descripción
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 15.75 in (400 mm)
Peso		12.90 lb (5.852 kg)

M4250-40G8XF-PoE+ (SKU GSM4248PX)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-40G8XF-PoE+.

Tabla 190. Especificaciones técnicas de hardware del modelo M4250-40G8XF-PoE+

Característica		Descripción
Interfaces de red		40 puertos RJ-45 1GBASE-T PoE+ (802.3at) Ocho puertos de enlace ascendente de fibra SFP+ de 10G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 12A
Consumo de energía	PoE máx. Sin PoE En espera	1197W - 4086.56 BTU/hr 89.2W - 304.53 BTU/hr 74.5W - 254.34 BTU/hr
Presupuesto de energía PoE		960W
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 15.75 in (400 mm)
Peso		13.91 lb (6.312 kg)

M4250-40G8XF-PoE++ (SKU GSM4248UX)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-40G8XF-PoE++.

Tabla 191. Especificaciones técnicas de hardware del modelo M4250-40G8XF-PoE++

Característica		Descripción
Interfaces de red		40 puertos RJ-45 1GBASE-T PoE++ (802.3bt) Ocho puertos de enlace ascendente de fibra SFP+ de 10G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 12A por cada PSU
Consumo de energía	PoE máx. Sin PoE En espera	1 PSU: 912W - 3113.57 BTU/hr 2 PSU: 1998W - 6821.17 BTU/hr, 3 PSU: 3523W - 12027.52 BTU/hr 82.6W - 282 BTU/hr 68.5W - 233.86 BTU/hr
Presupuesto de energía PoE		2880W con 3 PSU
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 3.40 in (86.4 mm), 2U 13.78 in (350 mm)
Peso		22.72 lb (10.280 kg)

M4250-12M2XF (SKU MSM4214X)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-12M2XF.

Tabla 192. Especificaciones técnicas de hardware del modelo M4250-12M2XF

Característica		Descripción
Interfaces de red		Doce puertos RJ-45 2.5GBASE-T Dos puertos de enlace ascendente de fibra SFP+ de 10G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 1.2–0.6A
Consumo de energía	Carga máx. En espera	37.9W - 129.39 BTU/hr 14.1W - 48.14 BTU/hr
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 3.94 in (100 mm)
Peso		3.85 lb (1.745 kg)

M4250-16XF (SKU XSM4216F)

La siguiente tabla muestra las especificaciones exclusivas del modelo M4250-16XF.

Tabla 193. Especificaciones técnicas de hardware del modelo M4250-16XF

Característica		Descripción
Interfaces de red		Dieciséis puertos de fibra SFP+ de 1G/10G
Entrada de alimentación de CA		100–240V ~ 50–60Hz, 2.5–1.25A
Consumo de energía	Carga máx. En espera	47.84W - 163.33 BTU/hr 19.27W - 65.78 BTU/hr
Dimensiones	Ancho Alto Profundidad	17.32 in (440 mm) 1.70 in (43.2 mm), 1U 7.87 in (200 mm)
Peso		6.17 lb (2.800 kg)

Especificaciones técnicas generales de hardware

Las siguientes especificaciones técnicas de hardware se aplican a todos los modelos de switch de la serie M4250:

Tabla 194. Especificaciones técnicas generales de hardware de los modelos de switch de la serie M4250

Característica	Descripción
Temperatura de funcionamiento	Modelos PoE+ y PoE++: 32º a 122ºF (0° a 50°C)
	Modelos sin PoE: 32º a 113ºF (0° a 45°C)
Humedad de funcionamiento	Humedad relativa máxima de 90%, sin condensación
Altitud de funcionamiento	10,000 ft (3,000 m) máximo
Temperatura de almacenamiento	–4° a 158°F (–20º a 70ºC)
Humedad de almacenamiento	Humedad relativa máxima de 95%, sin condensación
Altitud de almacenamiento	10,000 ft (3,000 m) máximo

Tabla 194. Especificaciones técnicas generales de hardware de los modelos de switch de la serie M4250 (continuación)

Característica	Descripción
Certificaciones de emisiones e inmunidad electromagnéticas	CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014, Clase A, EN 61000-3-3:2013, EN 55024:2010
	VCCI: VCCI-CISPR 32:2016, Clase A
	RCM: AS/NZS CISPR 32:2013 Clase A
	CCC: GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Clase A)
	FCC: 47 CFR FCC Parte 15, Clase A, ANSI C63.4:2014
	ISED: ICES-003:2016 Edición 6, Clase A, ANSI C63.4:2014
	BSMI: CNS 13438 Clase A
Certificaciones de seguridad	Informe / certificado CB IEC 60950-1:2005 (ed.2)+A1:2009+A2:2013
	Listado UL (UL 1950)/cUL IEC 950/EN 60950
	CE LVD: EN 60950-1: 2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
	RCM (AS/NZS) 60950.1:2015
	CCC (China Compulsory Certificate): GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Clase A)
	BSMI: CNS 14336-1