NETGEAR®

Manual del usuario

Switches M4300 Intelligent Edge Series

completamente administrables apilables

Versión de software 12.0.15 y versiones anteriores

Switches de la serie M4300
Switch modular M4300-96X

Abril de 2022
202-11998-06

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

Soporte y comunidad

Visite netgear.com/support para obtener respuestas a sus preguntas y acceder a las descargas más recientes.
También puede consultar la comunidad de 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 obtener información sobre el 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 consultar la Política de privacidad de NETGEAR, visite https://www.netgear.com/about/privacy-policy.

Al usar este dispositivo, usted 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 período de devolución.

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

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
202-11998-06	Abril de 2022	Se revisaron las siguientes secciones: • Configurar usuarios SNMP V3 en la página 135 • Configurar la contraseña de un usuario en la página 506 • Configurar los ajustes de HTTPS en la página 526
202-11998-05	Noviembre de 2021	Se agregaron las siguientes secciones: • Descripción general de Auto-Trunk en la página 186. • Habilitar o deshabilitar Auto-Trunks en la página 187. • Descripción general de Auto-LAG en la página 281. • Habilitar o deshabilitar Auto-LAGs en la página 282. • Configurar el modo hash para Auto-LAGs en la página 283.
202-11998-04	Julio de 2021	Se hicieron algunos cambios menores a la potencia PoE máxima permitida por puerto (consulte Configurar puertos PoE en la página 125).
202-11998-03	Mayo de 2020	Se agregaron las siguientes secciones: • Configurar IGMP snooping automáticamente con el modo IGMP Plus en la página 239. • Configurar IGMP snooping para VLAN automáticamente con el modo IGMP Plus en la página 244. • Configurar MLD snooping automáticamente con el modo MLD Plus en la página 252. • Configurar MLD snooping para VLAN automáticamente con el modo MLD Plus en la página 256. • Configurar los ajustes de Port Link Flap en la página 278.

(Continuación) 202-11998-03	(Continuación) Mayo de 2020	(Continuación) Se revisaron las siguientes secciones: • Agregar entradas multicast estáticas Mroute en la página 424. • Configurar IGMP snooping manualmente en la página 240. • Configurar IGMP snooping para VLAN manualmente en la página 245. • Configurar MLD snooping manualmente en la página 253. • Configurar MLD snooping para VLAN manualmente en la página 258. • Configurar los ajustes del registro en memoria en la página 649.
202-11998-02	Diciembre de 2019	Se agregó información sobre la nueva tarjeta de puertos HDMI TPM404H de terceros en las siguientes secciones: • Tarjeta de puertos HDMI TPM404H de terceros para el modelo M4300-96X en la página 21. • Numeración de ranuras y puertos en las tarjetas de puertos HDMI TPM404H de terceros en la página 31. • Configurar y ver información sobre ranuras y tarjetas de puertos en la página 48. Se cambió la información sobre la contraseña necesaria para iniciar sesión en la interfaz de usuario (UI) del navegador local en el paso 3 de todas las tareas y se agregó más información en las siguientes secciones: • Descripción general de la UI del navegador local en la página 24 • Usar un navegador web para acceder al switch e iniciar sesión en la página 25 • Se eliminó la información sobre la página Initial Setup, que ya no está en la UI del navegador local. • Uso de SNMP en la página 33. • Configurar cuentas de usuario en la página 505.
202-11998-01	Septiembre de 2019	Se agregaron y cambiaron las siguientes secciones: • Se cambió Switches compatibles en la página 19 para agregar los modelos M4300-16X, M4300-24XF y M4300-48XF. • Se agregó Administrar Precision Time Protocol en la página 78. • Se cambiaron las secciones de IGMP Snooping y de MLD Snooping (consulte Administrar multicast en la página 236). Se publicó el manual en un nuevo formato.
202-11865-03	Octubre de 2018	Se hicieron los siguientes cambios importantes: • Configurar los ajustes de HTTPS en la página 526. • Configurar los ajustes de SSH en la página 531. • Administrar claves de host en la página 532. • Descargar claves de host en la página 534. • Se eliminaron las referencias al archivo de clave SSH-1 Rivest-Shamir-Adelman (RSA) en todo el manual.

202-11865-02	Junio de 2018	Se hicieron los siguientes cambios importantes: • Se revisó Numeración de puertos basada en ranuras para el modelo M4300-96X en la página 20. • Se revisó Apilamiento para el modelo M4300-96X en la página 22. • Se revisó Publicaciones disponibles y ayuda en línea en la página 22. • Se revisó Numeración de ranuras y puertos para el modelo de switch M4300-96X en la página 28. • Se revisó Configurar y mostrar la información del sistema y de las ranuras en la página 36. • Se revisó Configurar un servidor SNTP en la página 71. • Se revisó Configurar los ajustes globales de DNS en la página 80. • Se agregó Configurar y mostrar los ajustes de Bonjour en la página 95. • Se agregó Configurar los ajustes de puertos expandibles en la página 277. • Se revisó Ver estadísticas de puertos y paquetes EAP en la página 637. Se hicieron cambios menores y adiciones en otras secciones.
202-11865-01	Abril de 2018	Primera publicación.

Contenido

Capítulo 1 Introducción

Switches compatibles 19
Funciones del modelo de switch M4300-96X. 20
Numeración de puertos basada en ranuras del modelo M4300-96X. . . . . .20 Configuración de ranuras del modelo M4300-96X. . . . . .21 Funcionamiento y configuración de PoE del modelo M4300-96X . . . . . .21 Apilamiento del modelo M4300-96X . . . . . .22 Publicaciones disponibles y ayuda en línea . . . . . .22 Registrar su producto. . . . . .23 Información sobre las interfaces de usuario . . . . . .24 Descripción general de la UI del navegador local 24
Requisitos de software para usar la UI del navegador local 24
Usar un navegador web para acceder al switch e iniciar sesión 25
Acceder al switch con una dirección IP estática . . . . . .25 Acceder al switch cuando conoce la dirección IP . . . . . .26 Botones y campos definidos por el usuario de la UI del navegador local . .26 Convenciones de nomenclatura de interfaces . . . . . .27 Numeración de ranuras y puertos del modelo de switch M4300-96X. . . . .28 Ayuda en línea . . . . . .31 Vista del dispositivo en la UI del navegador local . . . . . .32 Uso de SNMP. 33

Capítulo 2 Configurar la información del sistema

Configurar y mostrar la información del sistema y de las ranuras 36
Ver o definir la información del sistema . . . . . .36 Ver el estado de los ventiladores . . . . . .38 Ver la información del sensor de temperatura . . . . . .39 Ver el estado del dispositivo . . . . . .40 Ver el estado de la CPU del sistema . . . . . .42 Configurar los umbrales de la CPU . . . . . .43 Ver y borrar las estadísticas del switch . . . . . .44 Ver la información de dispositivos USB . . . . . .47 Configurar y ver información sobre ranuras y tarjetas de puertos . . . . . .48 Configurar una interfaz de loopback. . . . . .51 Configurar las interfaces de administración 52

Configurar el puerto de servicio IPv4. 52
Configurar el puerto de servicio IPv6. 54
Descripción general de la VLAN de administración. 56
Configurar una VLAN de administración IPv4 56

Configurar una VLAN de administración IPv6 58
Configurar una interfaz de administración IPv4. 61
Configurar una interfaz de administración IPv6. 63
Administrar los ajustes de hora 66

Configurar el ajuste de hora . . . . . .66 Configurar los ajustes globales de SNTP . . . . . .67 Ver el estado global de SNTP . . . . . .69 Configurar un servidor SNTP . . . . . .71 Configurar el horario de verano . . . . . .74 Ver el estado del horario de verano . . . . . .76 Administrar Precision Time Protocol. 78
Administrar los ajustes globales de PTP 78
Administrar los ajustes de interfaz de PTP. 79
Configurar los ajustes de DNS. 80

Configurar los ajustes globales de DNS 80
Agregar una entrada estática a la tabla DNS local. 82
Configurar la preferencia de plantilla de administración de la base de datos del switch. 84
Configurar los ajustes de Green Ethernet 86

Configurar los ajustes de interfaz de Green Ethernet 87
Configurar dispositivos locales y remotos de Green Ethernet 88
Configurar los detalles de dispositivos remotos de Green Ethernet 90
Ver el resumen de estadísticas de Green Ethernet 91
Configurar el historial de EEE LPI de Green Ethernet. . . . . .93 Configurar y mostrar los ajustes de Bonjour. 95
Habilitar o deshabilitar Bonjour. 95
Mostrar la información de Bonjour 96
Configurar los ajustes del servidor DHCP 97

Configurar el servidor DHCP . . . . . 97 Configurar el pool DHCP . . . . . . 98 Configurar las opciones del pool DHCP . . . . . . 101 Ver las estadísticas del servidor DHCP . . . . . 102 Ver la información de enlaces DHCP . . . . . 104 Ver los conflictos DHCP . . . . . 105 Configurar la retransmisión DHCP . . . . . 106 Administrar un DHCP L2 Relay 107
Configurar los ajustes globales de DHCP L2 Relay . . . . . 107 Configurar una interfaz de DHCP L2 Relay . . . . . 108 Ver estadísticas de interfaz de DHCP L2 Relay . . . . . 109 Configurar los ajustes globales de UDP Relay . . . . . 110 Configurar los ajustes de interfaz de UDP Relay . . . . . 112 Administrar el servidor DHCPv6 113
Habilitar o deshabilitar el servidor DHCPv6 113
Configurar el pool DHCPv6 114
Configurar la delegación de prefijos DHCPv6 . . . . . 115 Configurar los ajustes de interfaz DHCPv6 . . . . . 116 Ver la información de enlaces DHCPv6 . . . . . 117 Ver las estadísticas del servidor DHCPv6 119

Configurar DHCPv6 Relay para una interfaz 122
Configurar Power over Ethernet 123

Configurar los ajustes básicos de PoE 123
Configurar los puertos PoE 125
Configurar los ajustes de potencia PoE 127
Configurar SNMP 130

Configurar la comunidad SNMP V1/V2 130
Configurar los ajustes de traps SNMP V1/V2 131
Configurar los indicadores de traps SNMP V1/V2 . . . . . .
133 Ver las MIB compatibles . . . . . .
134 Configurar usuarios SNMP V3 . . . . . .
. 135 Configurar LLDP . . . . . .
. . . . 137
Configurar los ajustes globales de LLDP . . . . . .
137 Configurar la interfaz LLDP . . . . . .
138 Ver las estadísticas de LLDP . . . . . .
. . . . . 139 Ver la información del dispositivo local LLDP . . . . . .
. . . . . 141 Ver la información del dispositivo remoto LLDP . . . . . .
. . . . . 143 Ver el inventario del dispositivo remoto LLDP . . . . . .
. . . . . 144 Configurar los ajustes globales de LLDP-MED . . . . . .
. . . . . 145 Configurar la interfaz LLDP-MED . . . . . .
. . . . . 146 Ver la información del dispositivo local LLDP-MED . . .
. . . . . 147 Ver la información del dispositivo remoto LLDP-MED
. . . . . 148 Ver el inventario del dispositivo remoto LLDP-MED
. . . . . 151 Configurar la dependencia de enlaces . . . . . .
. 152

Configurar un grupo de dependencia de enlaces 152
Configurar una interfaz de dependencia de enlaces 153
Configurar ISDP 155

Configurar los ajustes globales básicos de ISDP . . . . . .
155 Configurar los ajustes globales de ISDP . . . . . .
. 156 Configurar una interfaz ISDP . . . . . .
158 Ver un vecino ISDP . . . . . .
158 Ver las estadísticas de ISDP . . . . . .
. . . 160 Administrar programaciones de temporizador . . . . . .
. 161
Configurar los ajustes globales del temporizador 161
Configurar la programación de temporizador 162

Capítulo 3 Administrar el apilamiento (stacking)

Descripción general del apilamiento de switches serie M4300 . . . . . .
. . . . 165 Sincronización y actualización del firmware . . . . . .
. . . . . 165 Mantenimiento de la configuración de la pila . . . . . .
. . . . . 166 Elección del maestro de la pila . . . . . .
. . . . . 166 Restablecimiento de fábrica de la pila . . . . . .
. . . . . 167 NSF de la pila . . . . . .
. . . . . 167 Configurar una pila . . . . . .
. 168
Seleccionar un nuevo maestro de la pila . . . . . .
168 Especificar el modo de muestreo de la pila . . . . . .
. 169 Configurar un miembro de la pila . . . . . .
. 170 Cambiar los ajustes de un miembro existente 171

Configurar el modo de los puertos de pila 173
Ejecutar diagnósticos de puertos de pila . . . . . 175 Configurar la sincronización del firmware de la pila . . . . . 177 Ver el resumen de datos de NSF . . . . . 178 Ver las estadísticas de checkpoint de NSF 180

Capítulo 4 Configurar la información de switching

Configurar VLAN 182
Configurar los ajustes básicos de VLAN . . . . . 182 Restablecer la configuración de VLAN predeterminada . . . . . 184 Configurar una VLAN interna . . . . . 185 Descripción general de Auto-Trunk . . . . . 186 Habilitar o deshabilitar Auto-Trunks . . . . . 187 Configurar el trunking de VLAN . . . . . 188 Configurar la pertenencia a VLAN . . . . . 190 Ver el estado de las VLAN . . . . . 191 Configurar los ajustes de PVID de puerto . . . . . 192 Configurar una VLAN basada en MAC . . . . . 194 Configurar grupos de VLAN basadas en protocolo . . . . . 195 Configurar la pertenencia a grupos de VLAN por protocolo . . . . . 196 Configurar una VLAN basada en subred IP . . . . . 198 Configurar una DVLAN de puerto . . . . . 198 Configurar una VLAN de voz . . . . . 200 Configurar los ajustes de GARP del switch . . . . . 201 Configurar un puerto GARP . . . . . 202 Configurar Auto-VoIP 204

Configurar los ajustes de puerto basados en protocolo . . . . . 204 Configurar las propiedades de Auto-VoIP basadas en OUI . . . . . 205 Ajustes de puerto basados en OUI . . . . . 205 Agregar una entrada a la tabla OUI . . . . . 206 Eliminar entradas de la tabla OUI . . . . . 208 Ver el estado de Auto-VoIP . . . . . 208 Configurar los ajustes de iSCSI 209
Configurar los ajustes globales de iSCSI . . . . . 210 Ver las sesiones iSCSI . . . . . 211 Controlar los ajustes de destino iSCSI . . . . . 212 Ver las sesiones iSCSI . . . . . 213 Ver los detalles de las sesiones iSCSI . . . . . 214 Configurar Spanning Tree Protocol 215
Configurar los ajustes básicos de STP . . . . . 216 Configurar los ajustes avanzados de STP . . . . . 218 Configurar los ajustes de CST . . . . . 221 Configurar los ajustes de puerto de CST . . . . . 223 Ver el estado de puerto de CST . . . . . 225 Configurar los ajustes de MST . . . . . 227 Ver el estado de puerto MST de Spanning Tree . . . . . 229 Ver las estadísticas de STP 231

Configurar los ajustes de VLAN de PVST 232
Configurar los ajustes de interfaz de PVST . . . . . 233 Ver las estadísticas de PVST 235
Administrar multicast 236

Ver la tabla MFDB 236
Ver las estadísticas de MFDB 237
Administrar IGMP snooping 238
Configurar IGMP snooping automáticamente con IGMP Plus 239
Configurar IGMP snooping manualmente 240
Configurar IGMP snooping para interfaces 242
Configurar IGMP snooping para VLAN automáticamente con el

modo IGMP Plus 244
Configurar IGMP snooping para VLAN manualmente 245
Configurar un router multicast 247
Configurar una VLAN de router multicast 248
Descripción general del querier de IGMP snooping 249
Configurar el querier de IGMP snooping 249
Configurar el querier de IGMP snooping para VLAN 250
Configurar MLD snooping automáticamente con MLD Plus 252
Configurar MLD snooping manualmente 253
Configurar una interfaz de MLD snooping 255
Configurar MLD snooping para VLAN automáticamente con el

modo MLD Plus 256
Configurar MLD snooping para VLAN manualmente 258
Habilitar o deshabilitar un router multicast en una interfaz 259
Configurar los ajustes de VLAN de router multicast 260
Configurar el querier de MLD snooping 261
Configurar los ajustes de VLAN del querier de MLD snooping 262
Configurar MVR 264
Configurar los ajustes básicos de MVR . . . . . 264 Configurar los ajustes avanzados de MVR . . . . . . 265 Configurar un grupo MVR . . . . . . 266 Configurar una interfaz MVR . . . . . . 267 Configurar la pertenencia a grupos MVR . . . . . 268 Ver las estadísticas de MVR . . . . 269 Buscar y administrar la tabla de direcciones MAC 271
Buscar en la tabla de direcciones MAC 271
Establecer el intervalo de envejecimiento dinámico 272
Configurar una dirección MAC estática 273
Administrar los ajustes de puertos 274
Configurar los ajustes de puertos . . . . . 274 Configurar los ajustes de puertos expandibles . . . . . 277 Configurar los ajustes de link flap del puerto . . . . . 278 Configurar las descripciones de puertos . . . . . 279 Ver la información del transceptor del puerto . . . . . 280 Administrar grupos de agregación de enlaces 281
Descripción general de Auto-LAG . . . . . 281 Habilitar o deshabilitar Auto-LAGs 282

Configurar el modo hash para Auto-LAGs 283
Configurar los ajustes de LAG 284
Configurar la pertenencia a LAG 286
Administrar los ajustes de Multiple Registration Protocol 288

Configurar los ajustes globales de MRP 289
Configurar los ajustes de puerto de MRP . . . . . 291 Ver y borrar las estadísticas de MMRP . . . . . 292 Ver y borrar las estadísticas de MVRP . . . . . 294 Administrar la protección contra bucles 295
Acerca de la protección contra bucles 295
Protección contra bucles y transmisión de PDU 296
Protección contra bucles y Spanning Tree Protocol 296
Configurar la protección contra bucles global 296
Configurar la protección contra bucles de los puertos y ver

su estado 298

Capítulo 5 Administrar el enrutamiento

Administrar rutas 301
Configurar una ruta básica 301
Configurar rutas avanzadas 303
Especificar las preferencias de ruta 305
Configurar los ajustes IP de enrutamiento 307

Ver estadísticas 308
Configurar los parámetros de enrutamiento del switch 312

Ver las estadísticas de IP 313
Configurar la interfaz IP 317
Configurar la dirección IP secundaria 320
Administrar IPv6 321

Configurar los ajustes globales de IPv6 . . . . . 321 Ver la tabla de rutas IPv6 . . . . . 322 Configurar los ajustes de interfaz IPv6 . . . . . . 323 Configurar los ajustes de prefijo IPv6 . . . . . 326 Ver las estadísticas de IPv6 . . . . . 327 Ver la tabla de vecinos IPv6 y borrar vecinos IPv6 . . . . . 332 Configurar una ruta estática IPv6 . . . . . 334 Ver la tabla de rutas IPv6 . . . . . 335 Configurar las preferencias de ruta IPv6 . . . . . 336 Configurar túneles IPv6 . . . . . 337 Administrar VLAN 338

Usar el asistente de enrutamiento estático de VLAN 339
Configurar el enrutamiento de VLAN 340
Configurar Address Resolution Protocol 341

Mostrar las entradas de la caché ARP 342
Agregar una entrada a la tabla ARP . . . . . 343 Ver o configurar la tabla ARP . . . . . 344 Configurar RIP 346

Habilitar RIP 346

Configurar los ajustes de RIP 347
Configurar ajustes avanzados de interfaz RIP 348
Administrar la redistribución de rutas 350
Configurar el descubrimiento de routers . . . . . 353 Configurar Virtual Router Redundancy Protocol 354
Configurar los ajustes globales de VRRP . . . . . 354 Configurar ajustes avanzados de VRRP . . . . . . 355 Configurar una IP secundaria VRRP avanzada 358
Configurar una interfaz de seguimiento VRRP . . . . . 359 Ver estadísticas avanzadas de VRRP 360

Capítulo 6 Configurar OSPF y OSPFv3

Configurar OSPF 364
Configurar los ajustes básicos de OSPF . . . . . 364 Configurar el anuncio de ruta predeterminada OSPF . . . . . 365 Configurar los ajustes de OSPF . . . . . . 366 Configurar el ID de área común OSPF . . . . . 369 Configurar el área stub OSPF . . . . . 371 Configurar el área NSSA OSPF . . . . . 372 Configurar el rango de área OSPF . . . . . . 374 Configurar la interfaz OSPF . . . . . 375 Ver y borrar estadísticas OSPF de una interfaz . . . . . 380 Ver la tabla de vecinos OSPF y borrar vecinos . . . . . 382 Ver la base de datos de estado de enlace OSPF . . . . . 385 Configurar el enlace virtual OSPF . . . . . 388 Configurar la redistribución de rutas OSPF . . . . . 391 Ver el resumen de NSF OSPF . . . . . 393 Configurar OSPFv3 395

Configurar los ajustes básicos de OSPFv3 . . . . . 395 Configurar el anuncio de ruta predet. OSPFv3 . . . . . 396 Configurar ajustes avanzados de OSPFv3 . . . . . 396 Configurar el área común OSPFv3 . . . . . 399 Configurar un área stub OSPFv3 . . . . . 400 Configurar el área NSSA OSPFv3 . . . . . 402 Configurar el rango de área OSPFv3 . . . . . 404 Configurar la interfaz OSPFv3 . . . . . 405 Ver y borrar estadísticas de interfaz OSPFv3 . . . . . 409 Ver la tabla de vecinos OSPFv3 y borrar vecinos . . . . . 411 Ver la base de datos de estado de enlace OSPFv3 . . . . . 413 Configurar el enlace virtual OSPFv3 . . . . . 416 Configurar la redistribución de rutas OSPFv3 . . . . . 418 Ver el resumen de NSF OSPFv3 419

Capítulo 7 Configurar el enrutamiento multicast

Descripción general de multicast 423
Ver la tabla Mroute de multicast 423
Agregar entradas multicast estáticas Mroute 424

Configurar los ajustes globales de multicast . . . . . .
425 Configurar la interfaz multicast . . . . . .
426 Configurar los ajustes globales de DVMRP . . . . . .
427 Configurar la interfaz DVMRP . . . . . .
428 Buscar vecinos DVMRP . . . . . .
430 Ver los ajustes de siguiente salto DVMRP . . . . . .
431 Ver la poda DVMRP de multicast . . . . . .
432 Ver la ruta DVMRP . . . . . .
433 Configurar los ajustes de IGMP multicast . . . . . .
. 434
Configurar los ajustes globales de IGMP . . . . . .
434 Configurar la interfaz de enrutamiento IGMP . . . . . .
. 435 Ver estadísticas de interfaz de enrutamiento IGMP . . . . . .
. . . . . 436 Ver los grupos IGMP . . . . . .
. . . . . 438 Ver la membresía IGMP . . . . . .
. . . . 439 Configurar la interfaz proxy IGMP . . . . . .
. . . 440 Ver estadísticas de la interfaz proxy IGMP . . . . . .
. . . . 442 Ver la membresía de proxy IGMP . . . . . .
. . . . 443 Configurar los ajustes de PIM . . . . . .
. 444
Configurar los ajustes globales de PIM 444
Configurar los ajustes de PIM SSM . . . . . .
445 Configurar la interfaz PIM . . . . . .
. 446 Ver el vecino PIM . . . . . .
447 Ver el punto de encuentro candidato PIM . . . . . .
448 Ver el vecino PIM . . . . . .
449 Configurar el punto de encuentro candidato PIM . . . . . .
450 Configurar el router bootstrap candidato PIM 451
Configurar el punto de encuentro estático PIM 452
Configurar rutas estáticas multicast . . . . . .
453 Configurar el límite administrativo multicast . . . . . .
454 Configurar los ajustes de multicast IPv6 . . . . . .
. 455

Ver la tabla Mroute de multicast IPv6 . . . . . .
455 Configurar los ajustes globales de PIM IPv6 . . . . . .
. . . 456 Configurar PIM SSM IPv6 . . . . . .
. . . . . 457 Configurar la interfaz PIM IPv6 . . . . . .
. . . . . 458 Ver el vecino PIM IPv6 . . . . . .
. . . . . 459 Configurar el punto de encuentro candidato PIM IPv6 . . . .
. . . . . 460 Configurar el router bootstrap candidato PIM IPv6 . . . . . .
. . . 461 Configurar el punto de encuentro estático PIM IPv6 . . . . . .
. . . . . 462 Configurar los ajustes globales de MLD IPv6 . . . . . .
. . . . . 463 Configurar la interfaz de enrutamiento MLD IPv6 . . . . . .
. . . . . 463 Ver estadísticas de interfaz de enrutamiento MLD . . .
. . . . . 465 Ver los grupos MLD IPv6 . . . . . .
. . . . . 466 Ver y borrar el tráfico MLD IPv6 . . . . . .
. . . . . 468 Configurar la interfaz proxy MLD IPv6 . . . . . .
. . . . . 469 Ver estadísticas de la interfaz proxy MLD
IPv6 . . . . . 470 Ver la membresía de proxy MLD
IPv6 . . . . . 471 Configurar rutas estáticas
multicast IPv6 472

Capítulo 8 Configurar la calidad de servicio

Descripción general de la calidad de servicio 475
Administrar la clase de servicio 475

Configurar los ajustes globales de CoS . . . . . .
476 Asignar prioridades 802.1p a colas . . . . . .
477 Asignar valores DSCP a colas . . . . . .
478 Configurar ajustes de CoS de una interfaz . . . . . .
479 Configurar ajustes de cola CoS de una interfaz . . . . . .
480 Configurar la precedencia de descarte CoS . . . . . .
482 Administrar servicios diferenciados . . . . . .
. . . 483
Descripción general del asistente DiffServ . . . . . .
. . . 484 Usar el asistente DiffServ . . . . . .
. . . . . 484 Configurar los ajustes básicos de DiffServ . . . . . .
. . . . . 486 Configurar los ajustes globales de DiffServ . . . . . .
. . . . . 487 Configurar una clase DiffServ . . . . . .
. . . . . 489 Configurar ajustes de clase DiffServ IPv6 . . . . . .
. . . . . 494 Configurar la política DiffServ . . . . . .
. . . . . 497 Configurar la interfaz de servicio DiffServ
. . . . . 500 Ver estadísticas de servicio DiffServ . . .
. 501

Capítulo 9 Administrar la seguridad del switch

Administrar cuentas de usuario y contraseñas 505
Configurar cuentas de usuario 505
Configurar una contraseña de usuario 506
Configuración de la contraseña enable 507
Configurar una contraseña de línea 508
Administrar los ajustes del servidor RADIUS . . . . . .
509
Configurar ajustes globales del servidor RADIUS 510
Configurar un servidor RADIUS 512
Configurar servidores de contabilidad RADIUS 514
Administrar los ajustes de TACACS 516

Configurar los ajustes globales de TACACS 516
Configurar los ajustes del servidor TACACS 517
Configurar listas de autenticación 518

Configurar una lista de autenticación de inicio . . . . . .
518 Configurar una lista de autenticación enable . . . . . .
519 Configurar la lista de autenticación Dot1x . . . . . .
520 Configurar una lista de autenticación HTTP . . . . . .
522 Configurar una lista de autenticación HTTPS . . . . . .
523 Ver las sesiones iniciadas . . . . . .
. . . . . 524 Administrar el acceso HTTP, HTTPS y SSH . . . . . .
. 525
Configurar los ajustes del servidor HTTP . . . . . .
525 Configurar los ajustes de HTTPS . . . . . .
. . 526 Administrar certificados . . . . . .
. . . 528 Descargar certificados . . . . . .
. . . 529 Configurar los ajustes de SSH . . . . . .
. . . . . 531 Administrar claves de host . . . . . .
. 532

Descargar claves de host 534
Configurar el acceso Telnet 535

Configurar una lista de autenticación Telnet 535
Configurar Telnet entrante 537
Configurar Telnet saliente 538
Configurar el acceso por puerto de consola . . . . . .
540 Configurar los ajustes de denegación de servicio . . . . . .
. . . . . 541 Configurar los ajustes de control de acceso . . . . . .
. 544
Configurar un perfil de control de acceso 544
Configurar reglas de acceso del perfil de control . . . . . 546 Administrar
la autenticación de puertos 547

Configurar los ajustes globales de 802.1X 547
Configurar los ajustes de 802.1X . . . . . .
549 Configurar la autenticación de puertos . . . . . .
. 550 Ver el resumen de puertos . . . . . .
. 553 Ver el resumen de clientes . . . . . .
555 Controlar el tráfico con filtrado MAC . . . . . .
557
Configurar el filtrado MAC 557
Resumen de filtros MAC 558
Configurar seguridad de puertos y grupos privados 559

Configurar el modo global de seguridad de puertos . . . . . .
559 Configurar una interfaz de seguridad de puertos . . . . . .
. . . . 560 Convertir direcciones MAC aprendidas en estáticas . . . . . .
. 562 Configurar direcciones MAC estáticas . . . . . .
. . 563 Configurar grupos privados . . . . . .
. . . 564 Configurar la membresía de grupos privados . . . . . .
. . . . 564 Configurar puertos protegidos . . . . . .
. . . . . 566 Configurar VLAN privadas . . . . . .
. 567
Configurar un tipo de VLAN privada 567
Configurar la asociación de VLAN privadas 568
Configurar el modo de puerto de VLAN privada . . . . . .
569 Configurar una interfaz host de VLAN privada . . . . . .
570 Configurar una interfaz promiscua de VLAN privada . . . . . .
571 Administrar los ajustes de control de tormentas . . . . . .
. . . 572
Configurar el control de tormentas global 572
Configurar el control de tormentas de un puerto 573
Configurar DHCP Snooping 575

Configurar los ajustes globales de DHCP Snooping 575
Configurar una interfaz de DHCP Snooping 576
Configurar una vinculación estática DHCP Snooping . . . . . .
577 Ver las vinculaciones dinámicas DHCP Snooping . . . . . .
578 Configurar los ajustes persistentes de snooping . . . . . .
. 579 Ver y borrar estadísticas de DHCP Snooping . . . . . .
580 Configurar interfaces de IP Source Guard . . . . . .
. . . . 581
Configurar vinculaciones de IP Source Guard 583
Configurar interfaces de IPv6 Source Guard 584
Configurar una vinculación de IPv6 Source Guard 585
Configurar Dynamic ARP Inspection 586

Configurar los ajustes globales de Dynamic ARP Inspection 586
Configurar VLAN DAI . . . . . .
587 Configurar interfaces DAI . . . . . .
588 Configurar una ACL DAI . . . . . .
. . 590 Configurar una regla de ACL DAI . . . . . .
. . . . 590 Ver estadísticas DAI . . . . . .
. . . . . 591 Configurar portales cautivos . . . . . .
. 593
Configurar los ajustes globales del portal cautivo . . . . . .
593 Agregar una instancia de portal cautivo . . . . . .
. . . 595 Configurar vinculaciones de portales cautivos . . . . . .
. . . . . 597 Ver la tabla de vinculaciones del portal cautivo . . . . . .
. . . . . 598 Configurar un grupo de portal cautivo . . . . . .
. . . . . 599 Configurar los usuarios del portal cautivo . . . . . .
. . . . . 600 Configurar los indicadores de trap del portal cautivo . . . . . .
. . . . . 601 Ver y borrar clientes del portal cautivo . . . . . .
. . . 602 Configurar y administrar listas de control de acceso . . . . . .
. 604

Usar el asistente de ACL para crear una ACL simple . . . . . .
604 Configurar una ACL basada en la dirección MAC de destino . . . . . .
. 606 Usar el asistente de ACL para completar la ACL de MAC de destino . . . 608 Configurar una ACL de MAC básica . . . . . .
. . . . . 608 Configurar reglas de ACL de MAC . . . . . .
. . . . . 610 Configurar la vinculación MAC . . . . . .
. . . . . 612 Ver y eliminar vinculaciones de ACL de MAC en la tabla de vinculación MAC . . . 614 Configurar una ACL de IP .
. . . . . 615 Configurar reglas para una ACL de IP . . . . . 617 Configurar reglas para una ACL de IP extendida 619
Configurar una ACL de IPv6 . . . . . .
. 625 Configurar reglas de IPv6 . . . . . .
. . . . . 626 Configurar vinculaciones de interfaz de ACL de IP . . . . . .
. . . . . 632 Ver y eliminar vinculaciones de ACL de IP en la tabla de vinculación de ACL de IP . . . 633 Configurar vinculaciones de ACL de VLAN 634

Capítulo 10 Monitorear el switch y la red

Ver estadísticas de puertos y de paquetes EAP 637
Ver y borrar estadísticas de puertos 637
Ver y borrar las estadísticas detalladas de puertos 638
Ver estadísticas de EAP 645
Realizar una prueba de cable . . . . . .
647 Administrar los registros en búfer, de comandos y de consola . . . . . .
648
Ver y borrar los registros en búfer 648
Configurar los ajustes del registro en memoria 649
Formato del registro de mensajes . . . . . .
651 Habilitar o deshabilitar el registro de comandos . . . . . .
651 Habilitar o deshabilitar el registro de consola . . . . . .
652 Configurar los ajustes de Syslog y del host Syslog . . . . . .
653
Configurar los ajustes de Syslog 653
Configurar los ajustes del host Syslog . . . . . 654 Ver y borrar los registros de traps 656

Ver y borrar el registro de eventos 657
Configurar la duplicación de varios puertos 658

Configurar globalmente la duplicación de varios puertos 659
Configurar la interfaz de origen de la duplicación de puertos 660
Administrar una VLAN RSPAN 662

Configurar una VLAN RSPAN 662
Configurar un switch de origen RSPAN 663
Configurar una interfaz de origen RSPAN 664
Configurar el switch de destino RSPAN 666
Configurar sFlow 667
Resumen del agente sFlow . . . . . 667 Configurar la información básica del agente sFlow . . . . . 668 Configurar los ajustes avanzados del agente sFlow . . . . . 669 Configurar un receptor sFlow . . . . . 670 Configurar la interfaz sFlow 671

Capítulo 11 Mantenimiento y solución de problemas

Guardar la configuración 675
Configurar el modo de guardado automático . . . . . . 675 Restablecer el switch a sus ajustes predeterminados de fábrica . . . . . 676 Restablecer todas las contraseñas de usuario a sus valores predeterminados . . . . . 677 Cargar o exportar un archivo desde el switch 678
Cargar un archivo al servidor TFTP 678
Cargar un archivo mediante HTTP 680
Cargar un archivo desde el switch a un dispositivo USB 681
Descargar o importar un archivo al switch 682

Descargar un archivo 682
Descargar un archivo al switch mediante HTTP 684
Descargar un archivo desde un dispositivo USB 686
Administrar archivos de imagen de software 687
Copiar una imagen 687
Configurar los ajustes de imagen dual 688
Solución de problemas 689

Hacer ping a una dirección IPv4 . . . . . 689 Hacer ping a una dirección IPv6 . . . . . 691 Enviar un traceroute a una dirección IPv4 . . . . . 693 Enviar un traceroute a una dirección IPv6 . . . . . 695 Capturar paquetes . . . . . 697 Realizar un volcado completo de memoria 698

Apéndice A Ejemplos de configuración

Redes de área local virtuales (VLAN) 701
Ejemplos de configuración de VLAN 702
Listas de control de acceso (ACL) 703

Ejemplo de configuración de ACL de MAC 703
Ejemplo de configuración de ACL de IP estándar 704
Servicios diferenciados (DiffServ) 705

Clase . . . . . .
706 Clases de tráfico DiffServ . . . . . .
. . 706 Creación de políticas . . . . . .
. . . . 707 Ejemplo de configuración de DiffServ . . . . . .
. . . . . 708 802.1X . . . . . .
. . . . . 710 Ejemplo de configuración de 802.1X . . . . . .
. . . . . 711 MSTP . . . . . .
. 712
Ejemplo de configuración de MSTP 714

Apéndice B Ajustes predeterminados

Apéndice C Acrónimos y abreviaturas

1

1 Introducción

Este manual del usuario corresponde a los switches apilables totalmente administrables M4300 Intelligent Edge Series y abarca todos los modelos de switch M4300 y el modelo modular M4300-96X.

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

El capítulo contiene las siguientes secciones:

- Switches compatibles
- Funciones del modelo de switch M4300-96X
- Publicaciones disponibles y ayuda en línea
- Registrar su producto
- Descripción de las interfaces de usuario
- Descripción general de la UI del navegador local
- Usar un navegador web para acceder al switch e iniciar sesión
- Uso de 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 de errores en netgear.com/support/download/. Algunos productos pueden revisar el sitio regularmente y descargar el nuevo firmware, o usted puede buscar y descargar el nuevo firmware 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

Esta versión y este manual del usuario corresponden a los siguientes modelos de switch M4300:

- Modelos totalmente 10G:
  - M4300-16X (XSM4316PA y XSM4316PB). Modelo de switch totalmente 10G con dieciséis puertos de cobre 10G PoE+ en un chasis de medio ancho
  - M4300-8X8F (XSM4316S). Modelo de switch totalmente 10G con ocho puertos de cobre 10G y ocho puertos de fibra 10G en un chasis de medio ancho
  - M4300-12X12F (XSM4324S). Modelo de switch totalmente 10G con doce puertos de cobre 10G y doce puertos de fibra 10G en un chasis de medio ancho
  - M4300-24X24F (XSM4348S). Modelo de switch totalmente 10G con veinticuatro puertos de cobre 10G y veinticuatro puertos de fibra 10G en un chasis de ancho completo
- Modelos 1G con enlaces ascendentes 10G:
  - M4300-28G (GSM4328S). Modelo de switch con veinticuatro puertos de cobre 1G, dos puertos de cobre 10G y dos puertos de fibra 10G en un chasis de ancho completo
  - M4300-28G-POE+ (GSM4328PA y GSM4328PB). Modelo de switch con veinticuatro puertos de cobre 1G PoE+, dos puertos de cobre 10G y dos puertos de fibra 10G en un chasis de ancho completo
  - M4300-52G (GSM4352S). Modelo de switch con cuarenta y ocho puertos de cobre 1G, dos puertos de cobre 10G y dos puertos de fibra 10G en un chasis de ancho completo
  - M4300-52G-POE+ (GSM4352PA y GSM4352PB). Modelo de switch con cuarenta y ocho puertos de cobre 1G PoE+, dos puertos de cobre 10G y dos puertos de fibra 10G en un chasis de ancho completo
- Modelos 10G con puertos combo RJ45/SFP+:
  - M4300-24X (XSM4324CS). Modelo de switch con veinte puertos de cobre RJ45 y cuatro puertos combo 10G RJ45/SFP+ en un chasis de medio ancho
  - M4300-24XF (XSM4324FS). Modelo de switch con veintidós puertos de fibra 10G y dos puertos combo 10G RJ45/SFP+ en un chasis de medio ancho
  - M4300-48X (XSM4348CS). Modelo de switch con cuarenta y cuatro puertos de cobre RJ45 y cuatro puertos combo 10G RJ45/SFP+ en un chasis de ancho completo
  - M4300-48XF (XSM4348FS). Modelo de switch con cuarenta y seis puertos de fibra 10G y dos puertos combo 10G RJ45/SFP+ en un chasis de ancho completo
- Modelo de chasis modular 10G:
  - M4300-96X (XSM4396K0 y XSM4396K1). Modelo de chasis modular para hasta 12 tarjetas de puertos y numeración de puertos basada en ranuras. Para más información, consulte Funciones del modelo de switch M4300-96X en la página 20.

Funciones del modelo de switch M4300-96X

Para obtener información de hardware del modelo de switch M4300-96X, incluidas las tarjetas de puertos compatibles, las fuentes de alimentación (PSU) y los presupuestos de Power over Ethernet (PoE), consulte la Fully Managed Stackable Switch M4300-96X Hardware Installation Guide.

Esta sección describe las funciones que esta versión admite para el modelo de switch M4300-96X.

Numeración de puertos basada en ranuras para el modelo M4300-96X

Todos los puertos físicos del modelo de switch M4300-96X se basan en ranuras. Como este modelo admite 12 ranuras y cada tarjeta de puertos ofrece ocho puertos, la numeración de puertos tiene el formato número de unidad/número de ranura/número de puerto.

Tarjetas de puertos APM408C, APM408P y APM408F para el modelo M4300-96X

Para las tarjetas de puertos APM408C, APM408P y APM408F, la numeración es la siguiente:

- La unidad es el número asignado al switch, ya sea generado y asignado automáticamente por el sistema o asignado manualmente. El rango de unidades es de 1 a 8.
- La ranura es una de las 12 ranuras que admite este modelo. Por lo tanto, el número de ranura va de 1 a 12.
- Cada ranura admite una tarjeta de puertos y cada tarjeta ofrece ocho puertos. Por lo tanto, el rango de puertos es de 1 a 8.

Por ejemplo, el quinto puerto de la sexta ranura de un switch modelo M4300-96X con número de unidad 1 se designa como 1/6/5. De igual forma, el primer puerto del switch es 1/1/1 y el último puerto es 1/12/8.

Tarjeta de puertos APM402XL para el modelo M4300-96X

La numeración de los puertos de la tarjeta APM402XL es diferente de la de las otras tarjetas. Puede usar un puerto 40G con un cable de breakout, en cuyo caso el puerto 40G puede admitir hasta cuatro puertos 10G individuales, o con una conexión a otro puerto 40G individual.

- El puerto 1 (el puerto 40G izquierdo de la tarjeta) usa la siguiente numeración:
  - Si se conecta con un cable de breakout a cuatro puertos 10G individuales, los números de puerto son 1, 2, 3 y 4.
  - Si se conecta a otro puerto 40G individual, el número de puerto es 1. En ese caso, solo se usa el puerto 1 y los puertos 2, 3 y 4 no se usan en la tarjeta.
- El puerto 2 (el puerto 40G derecho de la tarjeta) usa la siguiente numeración:
  - Si se conecta con un cable de breakout a cuatro puertos 10G individuales, los números de puerto son 5, 6, 7 y 8.
  - Si se conecta a otro puerto 40G individual, el número de puerto es 5. En ese caso, solo se usa el puerto 5 y los puertos 6, 7 y 8 no se usan en la tarjeta.

Por ejemplo, si un switch con número de unidad 1 incluye una tarjeta APM402XL en la ranura 9, el puerto 1 de la tarjeta está conectado a cuatro tarjetas de puertos individuales y el puerto 2 de la tarjeta está conectado a otro puerto 40G individual, la numeración de puertos es la siguiente: 1/9/1, 1/9/2, 1/9/3, 1/9/4 y 1/9/5.

De forma predeterminada, los puertos 40G de la tarjeta APM402XL (es decir, el puerto 1 y el puerto 5) están activos, lo que significa que están en estado conectado (attached), pueden detectarse y puede usarlos. Los puertos 10G expandibles de la tarjeta APM402XL (es decir, los puertos 2–4 del primer puerto 40G y los puertos 6–8 del segundo puerto 40G) no están activos, lo que significa que están en estado desconectado (detached) y no puede usarlos. Sin embargo, puede configurarlos en estado conectado para poder usarlos (consulte Configurar los ajustes de puertos expandibles en la página 277).

Tarjeta de puertos HDMI TPM404H de terceros para el modelo M4300-96X

Para la tarjeta de puertos HDMI TPM404H de terceros, la numeración es la siguiente:

- La unidad es el número asignado al switch, ya sea generado y asignado automáticamente por el sistema o asignado manualmente. El rango de unidades es de 1 a 8.
- La ranura es una de las 6 ranuras superiores que admite este modelo. Por lo tanto, el número de ranura va de 1 a 6.

  Nota: No inserte una tarjeta TPM404H en ninguna de las ranuras inferiores (7 a 12) del switch.
- Cada ranura admite una tarjeta de puertos y cada tarjeta ofrece cuatro puertos. Por lo tanto, el rango de puertos es de 1 a 4.

Por ejemplo, el tercer puerto HDMI de la quinta ranura de un switch modelo M4300-96X con número de unidad 1 se designa como 1/5/3. De igual forma, el primer puerto HDMI del switch es 1/1/1 y el último puerto HDMI es 1/6/4.

Configuración de ranuras para el modelo M4300-96X

De forma predeterminada, las ranuras del M4300-96X están configuradas como vacías, es decir, como ranuras en las que no hay tarjetas de puertos instaladas. Ninguna ranura está preconfigurada. Para obtener información sobre cómo configurar ranuras, consulte Configurar y ver información sobre ranuras y tarjetas de puertos en la página 48.

Funcionamiento y configuración de PoE para el modelo M4300-96X

La función PoE admite tarjetas de puertos en las ranuras del modelo de switch M4300-96X:

- Cuando inicia el modelo de switch M4300-96 con tarjetas de puertos PoE APM408P ya instaladas, el switch inicializa estas tarjetas para el funcionamiento PoE. Las configuraciones existentes de las ranuras se aplican automáticamente. Por lo tanto, PoE funciona inmediatamente después de que el switch completa su proceso de inicio.

- Cuando instala una o más tarjetas de puertos PoE APM408P mientras el modelo de switch M4300-96 está en funcionamiento, el switch detecta estos módulos, los inicializa y aplica automáticamente las configuraciones existentes de las ranuras.
- Cuando retira una o más tarjetas de puertos PoE APM408P mientras el modelo de switch M4300-96 está en funcionamiento, el switch detecta la ausencia de estas tarjetas y ajusta automáticamente la configuración.

La administración de energía mejora la funcionalidad PoE mediante las siguientes funciones:

- Administración dinámica de energía basada en prioridades
- Reequilibrio automático de energía para satisfacer la demanda PoE si la energía del sistema es limitada
- Detección automática de la inserción y extracción de una fuente de alimentación (PSU) y recálculo automático de la energía disponible

Las actualizaciones de firmware PoE se realizan por ranura (es decir, para cada tarjeta APM408P).

Para más información sobre PoE, consulte Configurar Power over Ethernet en la página 123.

Apilamiento para el modelo M4300-96X

Puede configurar todos los puertos del modelo de switch M4300-96X como puertos de apilamiento. Sin embargo, se aplica un límite máximo de 16 enlaces de apilamiento activos.

La tarjeta APM402XL admite apilamiento solo por puertos 40G (es decir, solo por el puerto 1 y el puerto 5). Cuando expande los puertos, no puede usar los puertos 10G para apilamiento.

Para más información sobre el apilamiento, consulte el Capítulo 3, Administrar el apilamiento.

Publicaciones disponibles y ayuda en línea

Puede descargar las siguientes publicaciones en netgear.com/support/download/:

- La guía de instalación de su switch y de los componentes:
  - *Installation Guide M4300 Intelligent Edge Series Fully Managed Stackable Switches*
  - *Installation Guide Fully Managed Switches Model M4300-96X*
  - *Installation Guide Fully Managed Switch Port Cards APM408C, APM408P, APM408F, and APM402XL*
  - *Installation Guide NETGEAR Power Supplies Units for Managed Switches, APS150W, APS250W, APS299W, APS550W, APS1000W, APS600W, and APS1200W*
- La guía de instalación de hardware de su switch:
  - *M4300 Intelligent Edge Series Fully Managed Stackable Switches*
  - *Fully Managed Stackable Switch M4300-96X*

- Los manuales de software de los switches de la serie M4300, incluido el modelo modular M4300-96X:
  - *M4300 Intelligent Edge Series Fully Managed Stackable Switches Software Administration* Manual
  - *M4300 Intelligent Edge Series Fully Managed Stackable Switches CLI Command Reference* Manual
  - M4300 Intelligent Edge Series Fully Managed Stackable Switches User Manual (este manual)
  - *M4300 Intelligent Edge Series Fully Managed Stackable Switches Software Setup Manual*

También puede acceder a este documento en línea cuando inicia sesión en el switch. Seleccione Help > Online Help > User Guide.

Cuando inicia sesión en la UI del navegador local, hay ayuda en línea disponible. Consulte Ayuda en línea en la página 31.

Registrar su producto

Para tener derecho a actualizaciones y a 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 garantiza la exactitud de su dirección de envío. También nos gustaría incorporar sus comentarios en el desarrollo de futuros productos. Nunca vendemos ni alquilamos su dirección de correo electrónico y puede darse de baja de las comunicaciones en

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 luego registre el switch con su dirección de correo electrónico y contraseña de NETGEAR.

Descripción de las interfaces de usuario

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

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

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

Este manual describe cómo usar la UI del navegador local para administrar y supervisar el sistema.

Descripción general de la UI 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.

La UI del navegador local 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 del switch, como VLAN, QoS y ACL, mediante la UI del navegador local.

La primera vez que inicie sesión como usuario administrador en la UI del navegador local, no se requiere contraseña (es decir, la contraseña está en blanco). A partir de la versión de software 12.0.9.3, después de iniciar sesión por primera vez, deberá especificar una contraseña local del dispositivo que deberá usar cada vez que inicie sesión.

Requisitos de software para usar la UI del navegador local

Para acceder al switch con un navegador web, el navegador debe cumplir los siguientes requisitos de software:

- Microsoft Internet Explorer 10 o 11
- Microsoft Edge 25
- Google Chrome 44 o 45
- Mozilla Firefox 40 o 40.6.01
- Apple Safari en OS X 9.0

Nota: Otras versiones y versiones posteriores también podrían funcionar, pero no se probaron.

Device View se basa en HTML versión 5.

Usar un navegador web para acceder al switch e iniciar sesión

Si es la primera vez que inicia sesión en el switch y debe usar la dirección IP predeterminada de el switch, consulte la información de la guía de instalación de su switch y del manual M4200 and M4300 Series ProSAFE Managed Switches Software Setup Manual.

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.

La primera vez que inicie sesión como usuario administrador en la UI del navegador local, no se requiere contraseña (es decir, la contraseña está en blanco). A partir de la versión de software 12.0.9.3, después de iniciar sesión por primera vez, deberá especificar una contraseña local del dispositivo que deberá usar cada vez que inicie sesión.

Acceder al switch con una dirección IP estática

Para usar una dirección IP estática para acceder al switch a través de la UI del navegador local:

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. Abra un navegador web como Google Chrome, Mozilla Firefox o Microsoft Internet Explorer.
4. 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 abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

Acceder al switch cuando conoce la dirección IP

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

Para acceder al switch a través de la UI del navegador local:

1. Abra un navegador web como Google Chrome, Mozilla Firefox o Microsoft Internet Explorer.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere 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 del navegador local

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

Tabla 1. Botones de comando de la UI del navegador local

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

IMPORTANTE:

Cuando hace clic en el botón Apply, los cambios se guardan para la sesión de administración web, pero el switch no los conserva cuando se reinicia. Puede guardar manualmente la configuración de forma permanente (consulte Guardar la configuración en la página 675) o puede habilitar la función de guardado automático (consulte Configurar el modo Auto Save en la página 675), que permite que el switch guarde la configuración **de forma permanente.**

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. Las interfaces lógicas se configuran mediante el software.

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 de todos los modelos de switch M4300 excepto el modelo M4300-96X	Los puertos físicos son interfaces Gigabit Ethernet o Ethernet multivelocidad de 10G. El número de interfaz consiste en el número de unidad del switch del 1 al 8, el número de ranura (que siempre es 0) y el número de puerto, que es un número secuencial que empieza en 1.	1/0/1, 1/0/2, 1/0/3, etc. 2/0/1, 2/0/2, 2/0/3, etc. 3/0/1, 3/0/2, 3/0/3, etc.
Interfaces físicas del modelo M4300-96X	Los puertos físicos son interfaces Gigabit Ethernet, Ethernet multivelocidad de 10G o Ethernet de 40G. El número de interfaz consiste en el número de unidad del switch del 1 al 8, el número de tarjeta de puertos del 1 al 12 y el número de puerto del 1 al 8. Nota: La numeración de la tarjeta de puertos APM402XL de 40G es diferente (consulte Numeración de ranuras y puertos en la tarjeta de puertos APM402XL en la página 29).	Consulte Numeración de ranuras y puertos del modelo de switch M4300-96X en la página 28.

Tabla 3. Convenciones de nomenclatura de interfaces

Interfaz	Descripción	Ejemplo
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.
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.	0/15/1
Interfaces VLAN de enrutamiento	Esta es una interfaz que se usa para la funcionalidad de enrutamiento.	VLAN 1, VLAN 2, VLAN 3, etc.

Numeración de ranuras y puertos del modelo de switch M4300-96X

En el modelo de switch M4300-96X, las ranuras de la fila superior del chasis están numeradas del 1 al 6 de izquierda a derecha. Estas ranuras admiten PoE. Las ranuras de la fila inferior del chasis están numeradas del 7 al 12 de izquierda a derecha. Estas ranuras no admiten PoE.

La numeración de puertos depende de la tarjeta de puertos.

Numeración de ranuras y puertos en las tarjetas de puertos APM408C, APM408P y APM408F

En las tarjetas de puertos APM408C, APM408P y APM408F, los puertos de las tarjetas de las ranuras se numeran como se describe en la siguiente tabla.

Tabla 4. Numeración de puertos de las tarjetas de puertos APM408C, APM408P y APM408F

Número de ranura	Ubicación de la ranura	Número de puerto de los puertos superiores de la tarjeta	Número de puerto de los puertos inferiores de la tarjeta	Convención de interfaz
1	Fila superior	1, 3, 5, 7	2, 4, 6, 8	1/1/1, 1/1/2, 1/1/3 y así sucesivamente hasta 1/1/8
2	Fila superior	1, 3, 5, 7	2, 4, 6, 8	1/2/1, 1/2/2, 1/2/3 y así sucesivamente hasta 1/2/8
3	Fila superior	1, 3, 5, 7	2, 4, 6, 8	1/3/1, 1/3/2, 1/3/3 y así sucesivamente hasta 1/3/8
4	Fila superior	1, 3, 5, 7	2, 4, 6, 8	1/4/1, 1/4/2, 1/4/3 y así sucesivamente hasta 1/4/8
5	Fila superior	1, 3, 5, 7	2, 4, 6, 8	1/5/1, 1/5/2, 1/5/3 y así sucesivamente hasta 1/5/8
6	Fila superior	1, 3, 5, 7	2, 4, 6, 8	1/6/1, 1/6/2, 1/6/3 y así sucesivamente hasta 1/6/8
7	Fila inferior	1, 3, 5, 7	2, 4, 6, 8	1/7/1, 1/7/2, 1/7/3 y así sucesivamente hasta 1/7/8
8	Fila inferior	1, 3, 5, 7	2, 4, 6, 8	1/8/1, 1/8/2, 1/8/3 y así sucesivamente hasta 1/8/8
9	Fila inferior	1, 3, 5, 7	2, 4, 6, 8	1/9/1, 1/9/2, 1/9/3 y así sucesivamente hasta 1/9/8
10	Fila inferior	1, 3, 5, 7	2, 4, 6, 8	1/10/1, 1/10/2, 1/10/3 y así sucesivamente hasta 1/10/8

Tabla 4. Numeración de puertos de las tarjetas de puertos APM408C, APM408P y APM408F (continuación)

Número de ranura	Ubicación de la ranura	Número de puerto de los puertos superiores de la tarjeta	Número de puerto de los puertos inferiores de la tarjeta	Convención de interfaz
11	Fila inferior	1, 3, 5, 7	2, 4, 6, 8	1/11/1, 1/11/2, 1/11/3 y así sucesivamente hasta 1/11/8
12	Fila inferior	1, 3, 5, 7	2, 4, 6, 8	1/12/1, 1/12/2, 1/12/3 y así sucesivamente hasta 1/12/8

Numeración de ranuras y puertos en la tarjeta de puertos APM402XL

La numeración de los puertos de la tarjeta APM402XL es diferente de la de las otras tarjetas. Puede usar un puerto 40G con un cable de breakout, en cuyo caso el puerto 40G puede admitir hasta cuatro puertos 10G individuales, o con una conexión a otro puerto 40G individual.

El puerto 1 (el puerto de 40G izquierdo de la tarjeta de puertos) usa la siguiente numeración:

- Si se conecta con un cable divisor (break-out) a cuatro puertos individuales de 10G, los números de puerto son 1, 2, 3 y 4.
- Si se conecta a otro puerto individual de 40G, el número de puerto es 1. En esa situación, solo se usa el puerto número 1 y los números de puerto 2, 3 y 4 no se usan en la tarjeta de puertos.

El puerto 2 (el puerto de 40G derecho de la tarjeta de puertos) usa la siguiente numeración:

- Si se conecta con un cable divisor (break-out) a cuatro puertos individuales de 10G, los números de puerto son 5, 6, 7 y 8.
- Si se conecta a otro puerto individual de 40G, el número de puerto es 5. En esa situación, solo se usa el puerto número 5 y los números de puerto 6, 7 y 8 no se usan en la tarjeta de puertos.

Por ejemplo, si un switch con número de unidad 1 incluye una tarjeta APM402XL en la ranura 9, el puerto 1 de la tarjeta está conectado a cuatro tarjetas de puertos individuales y el puerto 2 de la tarjeta está conectado a otro puerto 40G individual, la numeración de puertos es la siguiente: 1/9/1, 1/9/2, 1/9/3, 1/9/4 y 1/9/5.

En la tarjeta de puertos APM402XL, los puertos de las tarjetas de las ranuras se numeran como se describe en la siguiente tabla. (En los ejemplos de convención de interfaz de la tabla, el switch se designa como unidad número 1).

En la tarjeta de puertos APM402XL, los puertos de las tarjetas de las ranuras se numeran como se describe en la siguiente tabla.

Tabla 5. Numeración de los puertos de 40G en la tarjeta de puertos APM402XL

Número de ranura	Ubicación de la ranura	Puerto	Números de puerto para 10G	Números de puerto para 40G	Convención de interfaz
1	Fila superior	1	1, 2, 3, 4	1	Para 10G: 1/1/1, 1/1/2, 1/1/3 y 1/1/4. Para 40G: 1/1/1.
		2	5, 6, 7, 8	5	Para 10G: 1/1/5, 1/1/6, 1/1/7 y 1/1/8. Para 40G: 1/1/5.
2	Fila superior	1	1, 2, 3, 4	1	Para 10G: 1/2/1, 1/2/2, 1/2/3 y 1/2/4. Para 40G: 1/2/1.
		2	5, 6, 7, 8	5	Para 10G: 1/2/5, 1/2/6, 1/2/7 y 1/2/8. Para 40G: 1/2/5.
3	Fila superior	1	1, 2, 3, 4	1	Para 10G: 1/3/1, 1/3/2, 1/3/3 y 1/3/4. Para 40G: 1/3/1.
		2	5, 6, 7, 8	5	Para 10G: 1/3/5, 1/3/6, 1/3/7 y 1/3/8. Para 40G: 1/3/5.
4	Fila superior	1	1, 2, 3, 4	1	Para 10G: 1/4/1, 1/4/2, 1/4/3 y 1/4/4. Para 40G: 1/4/1.
		2	5, 6, 7, 8	5	Para 10G: 1/4/5, 1/4/6, 1/4/7 y 1/4/8. Para 40G: 1/4/5.
5	Fila superior	1	1, 2, 3, 4	1	Para 10G: 1/5/1, 1/5/2, 1/5/3 y 1/5/4. Para 40G: 1/5/1.
		2	5, 6, 7, 8	5	Para 10G: 1/5/5, 1/5/6, 1/5/7 y 1/5/8. Para 40G: 1/5/5.
6	Fila superior	1	1, 2, 3, 4	1	Para 10G: 1/6/1, 1/6/2, 1/6/3 y 1/6/4. Para 40G: 1/6/1.
		2	5, 6, 7, 8	5	Para 10G: 1/6/5, 1/6/6, 1/6/7 y 1/6/8. Para 40G: 1/6/5.
7	Fila inferior	1	1, 2, 3, 4	1	Para 10G: 1/7/1, 1/7/2, 1/7/3 y 1/71/4. Para 40G: 1/7/1.
		2	5, 6, 7, 8	5	Para 10G: 1/7/5, 1/7/6, 1/7/7 y 1/7/8. Para 40G: 1/7/5.
8	Fila inferior	1	1, 2, 3, 4	1	Para 10G: 1/8/1, 1/8/2, 1/8/3 y 1/8/4. Para 40G: 1/8/1.
		2	5, 6, 7, 8	5	Para 10G: 1/8/5, 1/8/6, 1/8/7 y 1/8/8. Para 40G: 1/8/5.
9	Fila inferior	1	1, 2, 3, 4	1	Para 10G: 1/9/1, 1/9/2, 1/9/3 y 1/9/4. Para 40G: 1/9/1.
		2	5, 6, 7, 8	5	Para 10G: 1/9/5, 1/9/6, 1/9/7 y 1/9/8. Para 40G: 1/9/5.
10 Fila inferior 1 1, 2, 3, 4 1 Para 10G: 1/10/1, 1/10/2, 1/10/3 y 1/10/4. Para 40G: 1/10/1.					
		2 5, 6, 7, 8 5 Para 10G: 1/10/5, 1/10/6, 1/10/7 y 1/10/8. Para 40G: 1/10/5.			
11 Fila inferior 1 1, 2, 3, 4 1 Para 10G: 1/11/1, 1/11/2, 1/11/3 y 1/11/4. Para 40G: 1/11/1.					
		2 5, 6, 7, 8 5 Para 10G: 1/11/5, 1/11/6, 1/11/7 y 1/11/8. Para 40G: 1/11/5.			
12 Fila inferior 1 1, 2, 3, 4 1 Para 10G: 1/12/1, 1/12/2, 1/12/3 y 1/12/4. Para 40G: 1/12/1.					
		2 5, 6, 7, 8 5 Para 10G: 1/12/5, 1/12/6, 1/12/7 y 1/12/8. Para 40G: 1/12/5.			

Numeración de ranuras y puertos en las tarjetas de puertos HDMI TPM404H de terceros

En la tarjeta de puertos TPM404H, los puertos de las tarjetas de las ranuras se numeran como se describe en la siguiente tabla.

Tabla 6. Numeración de puertos de la tarjeta de puertos TPM404H

Número de ranura	Ubicación de la ranura	Número de puerto de los puertos de la tarjeta	Convención de interfaz
1	Fila superior	1, 2, 3, 4	1/1/1, 1/1/2, 1/1/3 y así sucesivamente hasta 1/1/4
2	Fila superior	1, 2, 3, 4	1/2/1, 1/2/2, 1/2/3 y así sucesivamente hasta 1/2/4
3	Fila superior	1, 2, 3, 4	1/3/1, 1/3/2, 1/3/3 y así sucesivamente hasta 1/3/4
4	Fila superior	1, 2, 3, 4	1/4/1, 1/4/2, 1/4/3 y así sucesivamente hasta 1/4/4
5	Fila superior	1, 2, 3, 4	1/5/1, 1/5/2, 1/5/3 y así sucesivamente hasta 1/5/4
6	Fila superior	1, 2, 3, 4	1/6/1, 1/6/2, 1/6/3 y así sucesivamente hasta 1/6/4
7	Fila inferior	No inserte una tarjeta de puertos TPM404H en ninguna de las ranuras de la fila inferior.	
8	Fila inferior		
9	Fila inferior		
10	Fila inferior		
11	Fila inferior		
12	Fila inferior		

Ayuda en línea

Cuando inicia sesión en el switch, cada página contiene un enlace a la ayuda en línea Help 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, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Help > Online Help > Support.

5. Para conectarse al sitio de soporte de NETGEAR para los switches de la serie M4300 y M4300-96X, haga clic en el botón APPLY.

Device View de la UI del navegador local

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:

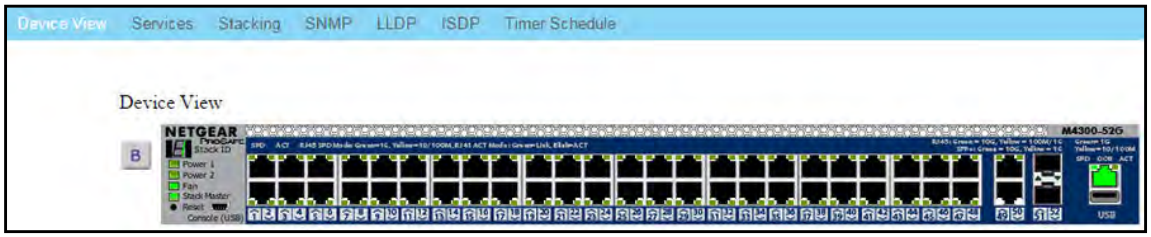
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.
3. Ingrese admin como nombre de usuario y la contraseña local del dispositivo.

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

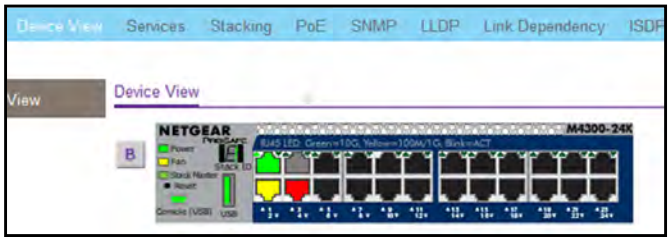
Se muestra la página System Information.

4. Seleccione System > Device View.

Como ejemplo, la siguiente figura muestra la página Device View del modelo M4300-52G.



Como otro ejemplo, la siguiente figura muestra un acercamiento de la página Device View del modelo M4300-24X.



El color del puerto indica si un puerto está activo actualmente. El verde indica que el puerto está habilitado; el rojo indica que se produjo un error en el puerto o que el enlace está deshabilitado.

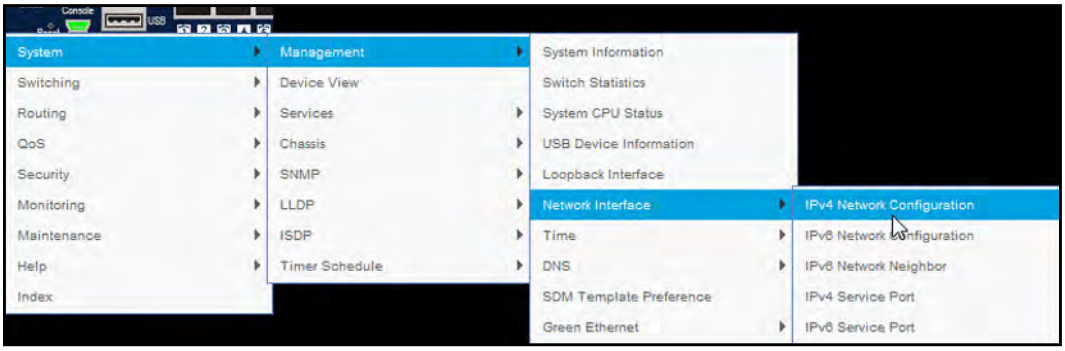
Como otro ejemplo más, la siguiente figura muestra un acercamiento de la página Device View del modelo M4300-96X. Esta figura muestra una tarjeta de puertos APM402XL en la ranura 5 y otra en la ranura 8. El puerto 1/5/6 está expandido en cuatro puertos de 10G, pero el puerto 1/5/5 está en modo de 40G. Los puertos 1/8/1 y 1/8/5 están en el modo predeterminado de 40G.



5. Haga clic en un puerto para ver un menú que muestra estadísticas y opciones de configuración.

Puede hacer clic en una opción del menú para acceder a la página que contiene las opciones de configuración o supervisión.

Si hace clic en el gráfico, pero no en un puerto específico, se muestra el menú principal. Este menú contiene las mismas opciones que las pestañas de navegación de la parte superior de la página.



Uso de 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.

A partir de la versión de software 12.0.9.3, no puede acceder al switch mediante SNMPv3 hasta que inicie sesión en el switch como admin y cambie la contraseña predeterminada (consulte Usar un navegador web para acceder al switch e iniciar sesión en la página 25). 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 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, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > SNMP > SNMP v3 > User Configuration.

   Se muestra la página User Configuration.

5. Para habilitar la autenticación, seleccione una opción de Authentication Protocol, que puede ser MD5 o SHA.
6. 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.
7. Haga clic en el botón APPLY.
La configuración se guarda.

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

2Configurar la información del sistema

Este capítulo trata los siguientes temas:

- Configurar y mostrar la información del sistema y de las ranuras
- Configurar una interfaz loopback
- Configurar las interfaces de administración
- Administrar la configuración de hora
- Administrar Precision Time Protocol
- Configurar los ajustes de DNS
- Configurar la preferencia de la plantilla de administración de la base de datos del switch
- Configurar los ajustes de Green Ethernet
- Configurar y mostrar los ajustes de Bonjour
- Configurar los ajustes del servidor DHCP
- Administrar un relay DHCP L2
- Administrar el servidor DHCPv6
- Configurar Power over Ethernet
- Configurar SNMP
- Configurar LLDP
- Configurar la dependencia de enlaces
- Configurar ISDP
- Administrar las programaciones de temporizador

Configurar y mostrar la información del sistema y de las ranuras

Puede ver y configurar la información del sistema del switch. En el modelo M4300-96X, también puede configurar la información de las ranuras y las tarjetas de puertos.

Ver o definir la información del sistema

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

Para ver o definir la información del sistema:

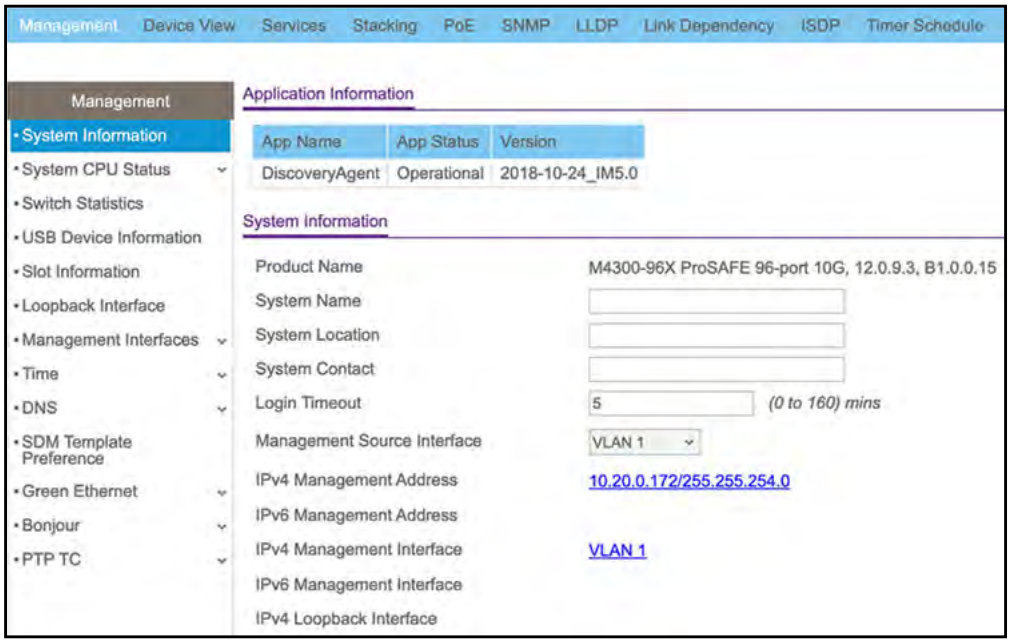
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > System Information.



5. 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.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

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

Tabla 7. 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.

Tabla 7. Información de la aplicación y del sistema (continuación)

Campo	Descripción
IPv4 Management Interface	El ID de la VLAN de administración IPv4 del switch. Haga clic en el valor Management VLAN ID mostrado para ir a la página de configuración. Consulte Configurar una VLAN de administración IPv4 en la página 56.
IPv6 Management Interface	El ID de la VLAN de administración IPv6 del switch. Haga clic en el valor Management VLAN ID mostrado para ir a la página de configuración. Consulte Configurar una VLAN de administración IPv6 en la página 58.
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.
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.
Service Port MAC Address	La dirección MAC usada para la conectividad fuera de banda.
L2 MAC Address	La dirección MAC usada para las comunicaciones en el segmento de red de capa 2.
L3 MAC Address	La dirección MAC usada para las comunicaciones en el segmento de red de capa 3.
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, la CPU y otros chipsets, y permiten que los chipsets funcionen normalmente. El estado del ventilador tiene tres valores posibles: OK, Failure y Not Present.

Para ver el estado de los ventiladores:

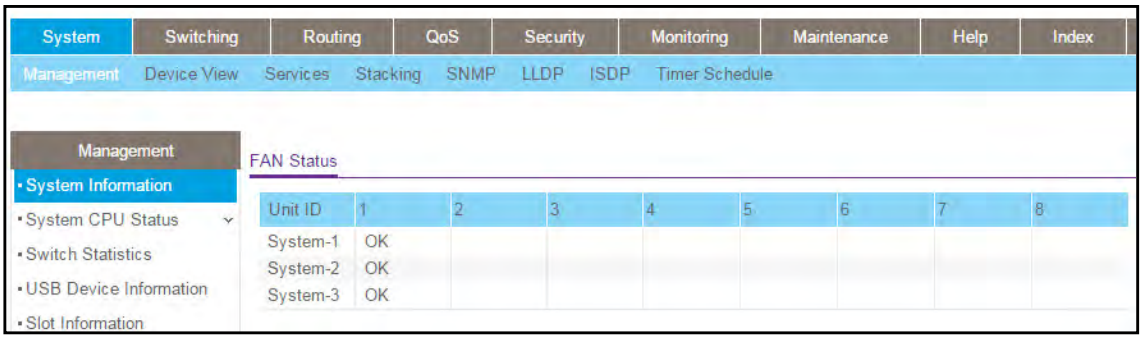
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Management > System Information > Fan Status.



5. Para actualizar la página, haga clic en el botón Actualizar (Refresh).
La siguiente tabla describe la información no configurable de Fan Status.

Tabla 8. Estado de los ventiladores

Campo	Descripción
Unit ID	El ID de unidad del switch al que pertenece el ventilador.
System-1	El estado de funcionamiento del ventilador System-1 en cada unidad.
System-2	El estado de funcionamiento del ventilador System-2 en cada unidad.
System-3	El estado de funcionamiento del ventilador System-3 en cada unidad.

Ver la información de los sensores de temperatura

Puede ver la temperatura actual de los distintos sensores del sistema en la tabla Temperature Status. La temperatura es instantánea y se puede actualizar con la información más reciente del switch al hacer clic en el botón Actualizar (Refresh). La temperatura máxima de la CPU y de las MAC depende del hardware real.

Para ver la información de temperatura:

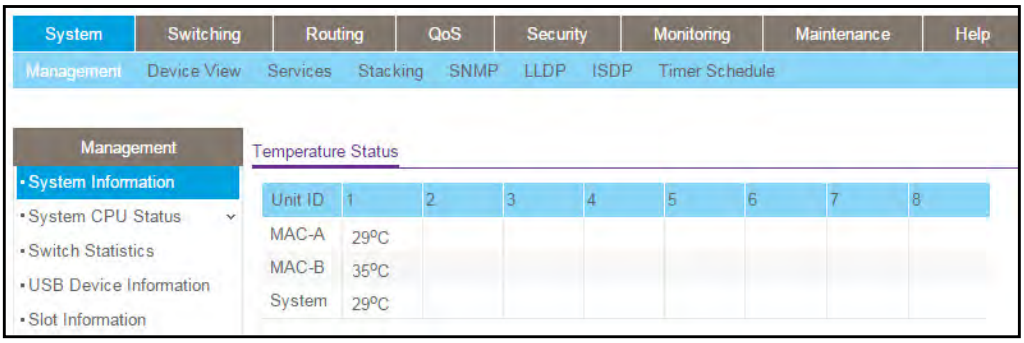
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > System Information > Temperature Sensors.



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

Tabla 9. Información del estado de temperatura

Campo	Descripción
Unit ID	El número de unidad en el switch.
MAC-A	La temperatura actual (en grados Celsius) del sensor MAC-A del switch. La máxima es 31°C.
MAC-B	La temperatura actual (en grados Celsius) del sensor MAC-B del switch. La máxima es 37°C.
System	La temperatura actual (en grados Celsius) del sensor System del switch. La máxima es 31°C.

Ver el estado del dispositivo

Esta página muestra la versión de software de cada dispositivo.

Para ver el estado del dispositivo:

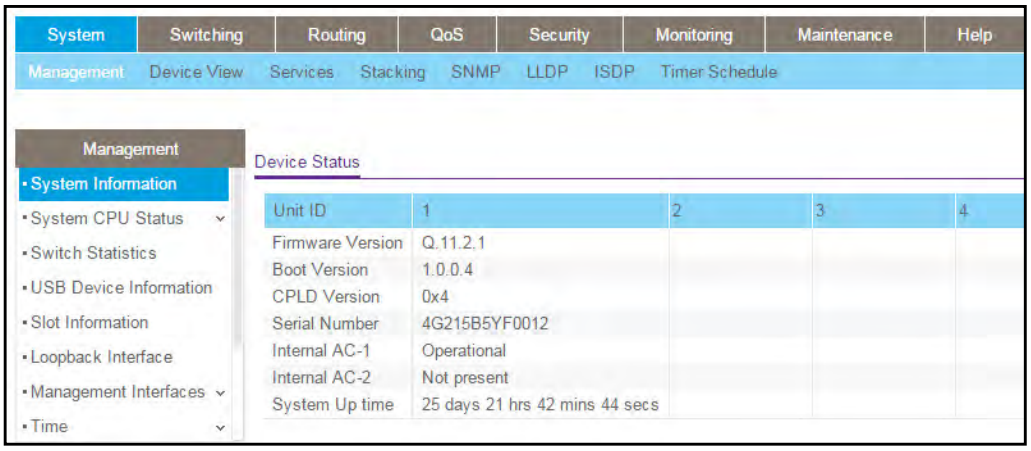
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Management > System Information > Device Status.



5. Para actualizar la página, haga clic en el botón Actualizar (Refresh).

La siguiente tabla describe la información no configurable de Device Status.

Tabla 10. Estado del dispositivo

Campo	Descripción
Unit ID	El número de unidad en el switch.
Firmware Version	El número release.version.maintenance del código que se ejecuta actualmente en el switch. Por ejemplo, si la versión mayor fuera 1, la versión 2 y el número de mantenimiento 4, el formato sería 1.2.4.
Boot Version	La versión del código de arranque en la memoria flash que carga el firmware en la memoria.
CPLD Version	La versión del software del CPLD.
Serial Number	El número de serie de este switch.
Internal AC-1, Internal AC-2, etc.	Indica el estado del módulo de alimentación correspondiente en cada unidad. El estado puede ser uno de los siguientes: • Operational. El módulo de alimentación está presente y funciona correctamente. • Powering. La alimentación principal falló o está desconectada, pero la RPS alimenta el switch. • Not Present. El módulo de alimentación no está en la ranura. • Not powered. El módulo de alimentación está presente, pero no está conectado a la fuente de energía. • Not powering. El módulo de alimentación está presente y conectado, pero el switch usa otra fuente de energía. • Incompatible. El módulo de alimentación está presente, pero no es compatible. • Failed. El módulo de alimentación está presente, pero el cable de alimentación no está conectado o hay un cable defectuoso conectado.
System Up Time	El tiempo en días, horas y minutos desde el último reinicio del switch.

Ver el estado de la CPU del sistema

Para ver el estado de la CPU del sistema:

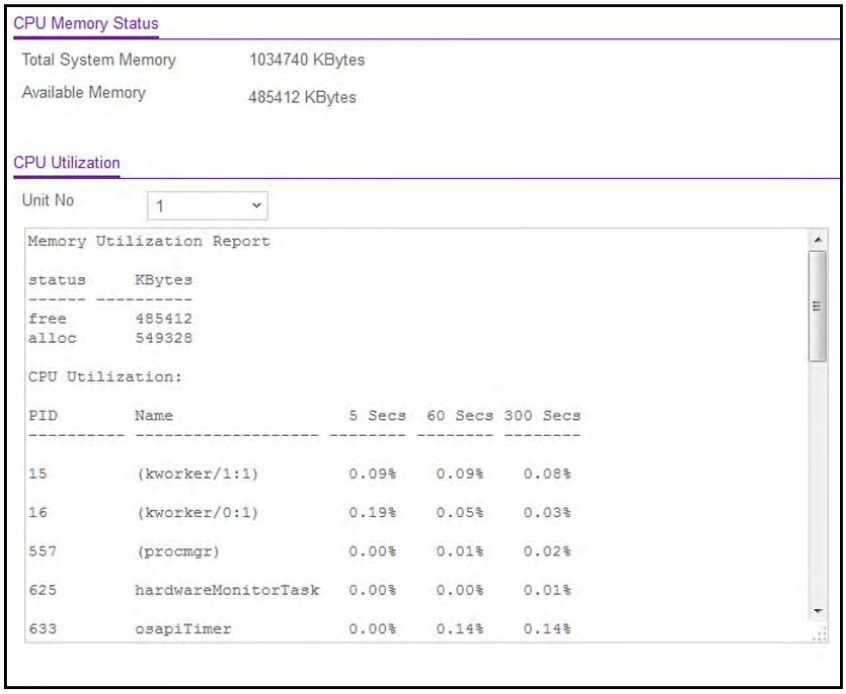
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > System CPU Status.



5. Puede ver la información de CPU Utilization, que contiene la información de memoria, la información de tareas y el porcentaje de uso de CPU por tarea.
   - Seleccione el Unit No. para mostrar la información de CPU Utilization.
   - Seleccione All para mostrar la información de CPU Utilization de todas las unidades del switch.

La siguiente tabla describe la información de CPU Memory Status.

Tabla 11. Información de CPU Memory Status

Campo	Descripción
Total System Memory	La memoria total del switch en KBytes.
Available Memory	El espacio de memoria disponible del switch en KBytes.

Configurar los umbrales de CPU

La función de notificación de umbral de uso de CPU le permite configurar umbrales que, al cruzarse, generan una notificación. La notificación se realiza mediante traps SNMP y mensajes syslog.

Para configurar los umbrales de CPU:

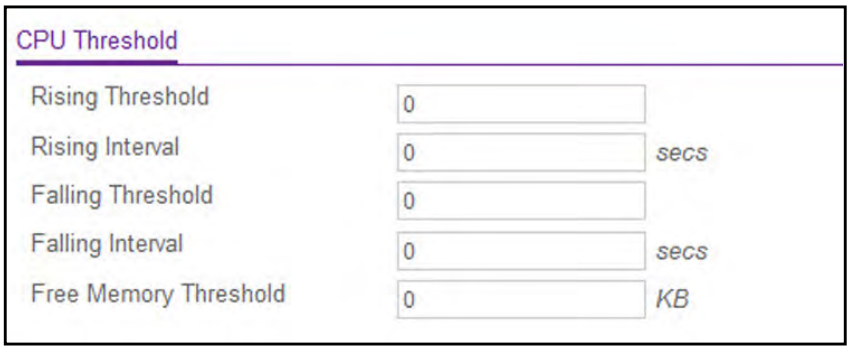
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > System CPU Status > CPU Threshold.



5. Configure el valor de Rising Threshold.

Se genera una notificación cuando el uso total de CPU supera este umbral durante el periodo configurado. El rango es de 1 a 100.

6. Configure el valor de Rising Interval.

Este periodo de supervisión del uso se puede configurar de 5 a 86400 segundos en múltiplos de 5 segundos.

7. Configure el valor de Falling Threshold.

Se genera una notificación cuando el uso total de CPU cae por debajo de este nivel durante un periodo configurado.

El umbral descendente debe ser igual o menor que el umbral ascendente. La notificación de umbral descendente solo se realiza si antes hubo una notificación de umbral ascendente. Configurar el umbral descendente y su periodo es opcional. Si no se configuran los parámetros descendentes, toman el mismo valor que los parámetros ascendentes. El rango es de 1 a 100.

8. Configure el valor de Falling Interval.

El periodo de supervisión del uso se puede configurar de 5 segundos a 86400 segundos en múltiplos de 5 segundos.

9. Configure el valor de CPU Free Memory Threshold en KB.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Ver y borrar las estadísticas del switch

Para ver y borrar las estadísticas del switch:

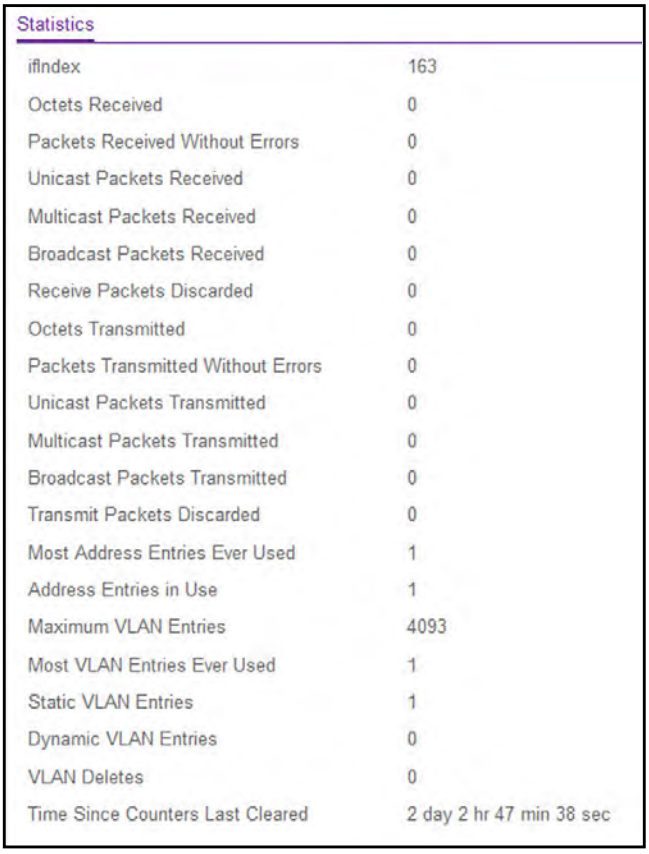
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Management > Switch Statistics.



Statistics

ifIndex	163
Octets Received	0
Packets Received Without Errors	0
Unicast Packets Received	0
Multicast Packets Received	0
Broadcast Packets Received	0
Receive Packets Discarded	0
Octets Transmitted	0
Packets Transmitted Without Errors	0
Unicast Packets Transmitted	0
Multicast Packets Transmitted	0
Broadcast Packets Transmitted	0
Transmit Packets Discarded	0
Most Address Entries Ever Used	1
Address Entries in Use	1
Maximum VLAN Entries	4093
Most VLAN Entries Ever Used	1
Static VLAN Entries	1
Dynamic VLAN Entries	0
VLAN Deletes	0
Time Since Counters Last Cleared	2 day 2 hr 47 min 38 sec

5. Para borrar todos los contadores y restablecer todas las estadísticas resumidas y detalladas a los valores predeterminados, haga clic en el botón Borrar (Clear).

El contador de paquetes descartados no se puede borrar. La siguiente tabla describe la información de Switch Statistics.

Tabla 12. Información de estadísticas del switch

Campo	Descripción
ifIndex	El ifIndex de la entrada de la tabla de interfaces asociada al procesador de este switch.
Octets Received	El número total de octetos de datos recibidos por el procesador (sin incluir bits de trama, pero incluidos los octetos FCS).
Packets Received Without Errors	El número total de paquetes (incluidos broadcast y multicast) recibidos por el procesador.
Unicast Packets Received	El número de paquetes unicast de subred entregados a un protocolo de capa superior.
Multicast Packets Received	El número total de paquetes recibidos dirigidos a una dirección multicast. No incluye los paquetes dirigidos a la dirección de broadcast.

Tabla 12. Información de estadísticas del switch (continuación)

Campo	Descripción
Broadcast Packets Received	El número total de paquetes recibidos dirigidos a la dirección de broadcast. No incluye paquetes multicast.
Receive Packets Discarded	El número de paquetes entrantes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Un posible motivo para descartar un paquete es liberar espacio en búfer.
Octets Transmitted	El número total de octetos transmitidos por la interfaz, incluidos los caracteres de trama.
Packets Transmitted Without Errors	El número total de paquetes transmitidos por la interfaz.
Unicast Packets Transmitted	El 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.
Multicast Packets Transmitted	El 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.
Broadcast Packets Transmitted	El 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.
Transmit Packets Discarded	El número de paquetes salientes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Un posible motivo para descartar un paquete es liberar espacio en búfer.
Most Address Entries Ever Used	El mayor número de entradas de la tabla de direcciones de la base de datos de reenvío que ha aprendido este switch desde el último reinicio.
Address Entries in Use	El número de entradas aprendidas y estáticas en la tabla de direcciones de la base de datos de reenvío de este switch.
Maximum VLAN Entries	El número máximo de LAN virtuales (VLAN) permitidas en este switch.
Most VLAN Entries Ever Used	El mayor número de VLAN que han estado activas en este switch desde el último reinicio.
Static VLAN Entries	El número de entradas de VLAN activas actualmente en este switch que se crearon de forma estática.
Dynamic VLAN Entries	El número de entradas de VLAN activas actualmente en este switch que se crearon por registro GVRP.
VLAN Deletes	El número de VLAN de este switch que se crearon y luego se eliminaron desde el último reinicio.
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 switch.

Ver la información del dispositivo USB

Para mostrar la información del dispositivo USB:

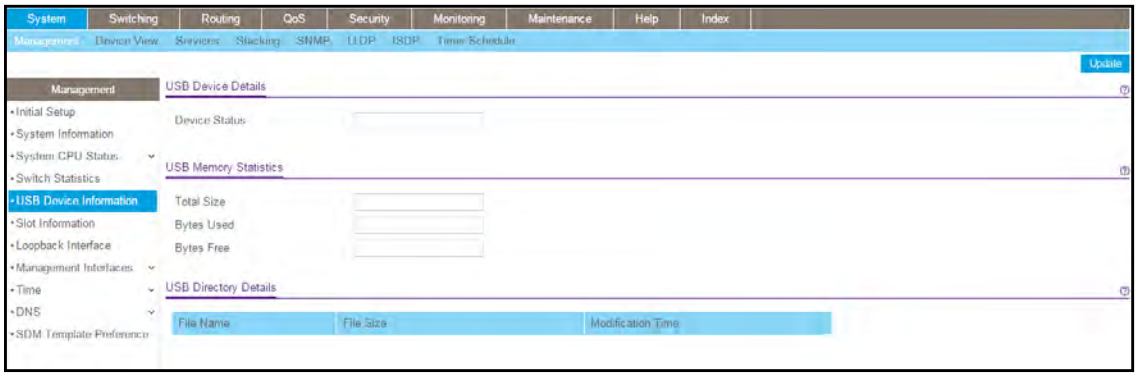
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > 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 hay un dispositivo no válido conectado.

5. Para actualizar la página, haga clic en el botón Actualizar (Refresh).

La siguiente tabla describe la información de USB Memory Statistics.

Tabla 13. Información de USB Memory Statistics

Campo	Descripción
Total Size	La capacidad de almacenamiento del dispositivo flash USB en bytes.
Bytes Used	La memoria usada en el dispositivo flash USB.
Bytes Free	La memoria libre en el dispositivo flash USB.

La siguiente tabla describe la información de USB Directory Details.

Tabla 14. Información de USB Directory Details

Campo	Descripción
File Name	El nombre del archivo almacenado en la unidad flash USB.
File Size	El tamaño en bytes del archivo almacenado en la unidad flash USB
Modification Time	La hora de la última modificación del archivo almacenado en la unidad flash USB.

Configurar y ver información de ranuras y tarjetas de puertos

Puede configurar información sobre las tarjetas de puertos instaladas en las ranuras del switch y ver información sobre las tarjetas de puertos y otros switches compatibles con el switch.

Para configurar y ver información de ranuras y tarjetas de puertos:

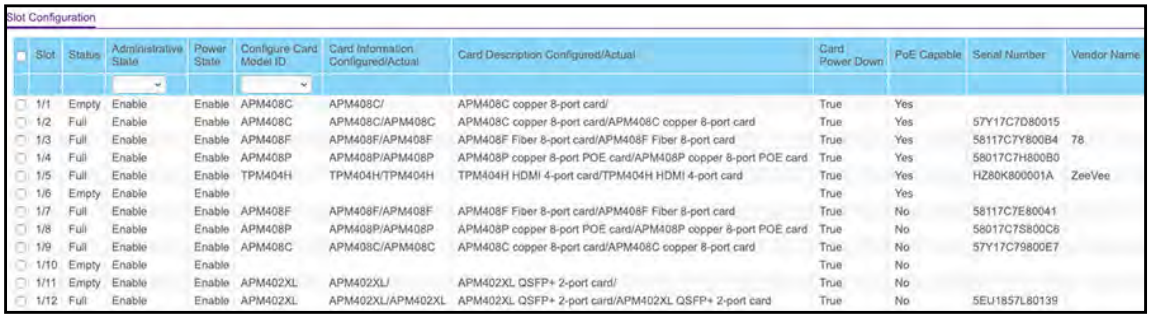
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Slot Information.


Slot Configuration

Slot	Status	Administrative State	Power State	Configure Card Model ID	Card Information Configured/Actual	Card Description Configured/Actual	Card Power Down	PoE Capable	Serial Number	Vendor Name
1/1	Empty	Enable	Enable	APM408C	APM408C/	APM408C copper 8-port card/	True	Yes		
1/2	Full	Enable	Enable	APM408C	APM408C/APM408C	APM408C copper 8-port card/APM408C copper 8-port card	True	Yes	57Y17C7D80015	
1/3	Full	Enable	Enable	APM408F	APM408F/APM408F	APM408F Fiber 8-port card/APM408F Fiber 8-port card	True	Yes	58117C7Y800B4	78
1/4	Full	Enable	Enable	APM408P	APM408P/APM408P	APM408P copper 8-port POE card/APM408P copper 8-port POE card	True	Yes	58017C7H800B0	
1/5	Full	Enable	Enable	TPM404H	TPM404H/TPM404H	TPM404H HDMI 4-port card/TPM404H HDMI 4-port card	True	Yes	HZ80K800001A	ZeeVee
1/6	Empty	Enable	Enable				True	Yes		
1/7	Full	Enable	Enable	APM408F	APM408F/APM408F	APM408F Fiber 8-port card/APM408F Fiber 8-port card	True	No	58117C7E80041	
1/8	Full	Enable	Enable	APM408P	APM408P/APM408P	APM408P copper 8-port POE card/APM408P copper 8-port POE card	True	No	58017C7S800C6	
1/9	Full	Enable	Enable	APM408C	APM408C/APM408C	APM408C copper 8-port card/APM408C copper 8-port card	True	No	57Y17C79800E7	
1/10	Empty	Enable	Enable				True	No		
1/11	Empty	Enable	Enable	APM402XL	APM402XL/	APM402XL QSFP+ 2-port card/	True	No		
1/12	Full	Enable	Enable	APM402XL	APM402XL/APM402XL	APM402XL QSFP+ 2-port card/APM402XL QSFP+ 2-port card	True	No	5EU1857L80139	

La figura anterior no muestra todas las columnas de la página.

Nota: En el ejemplo anterior del modelo M4300-96X, se muestra una tarjeta de puertos HDMI de terceros en la ranura 1/5. Puede insertar una tarjeta de puertos HDMI de terceros en cualquiera de las ranuras superiores (1–6), pero no en las inferiores.

5. Solo en el modelo M4300-96X, en el menú Administrative State, seleccione Enable o Disable.

De forma predeterminada, todas las ranuras están habilitadas, pero puede deshabilitar una ranura.

6. Solo en el modelo M4300-96X, en el menú Configured Card Model ID, seleccione la tarjeta de puertos.

Esta opción le permite preconfigurar la tarjeta de puertos antes de insertarla.
7. En el modelo M4300-96X, si cambió la configuración, haga clic en el botón Aplicar (Apply). La configuración se guarda.

La siguiente tabla describe la información no configurable de la tabla Slot Configuration.

Campo	Descripción
Slot	El número de unidad y de ranura.
Status	Indica si la ranura está vacía u ocupada.
Power State	Solo en el modelo M4300-96X, el estado de energía siempre es Enable. En otros modelos, la columna Power State no se muestra.
Card Information Configured/Actual	El modelo de la tarjeta de puertos configurada y el modelo de la tarjeta de puertos insertada en la ranura.
Card Description Configured/Actual	La descripción de la tarjeta de puertos configurada y la descripción de la tarjeta de puertos insertada en la ranura.
Card Power Down	Si el valor es True, el estado de energía se puede habilitar o deshabilitar administrativamente. Si el valor es False, el estado de energía no se puede configurar.
PoE Capable	Indica si la tarjeta de puertos admite PoE.
Serial Number	El número de serie de la tarjeta de puertos instalada.
Vendor Name	El nombre del proveedor de la tarjeta de puertos instalada.
Manufacturer Name	El nombre del fabricante de la tarjeta de puertos instalada.
FPGA Version	La versión de FPGA (Field Programmable Gate Array) de la tarjeta de puertos instalada.
Software Version	La versión de software de la tarjeta de puertos instalada.
Board Revision ID	El ID de revisión de placa de la tarjeta de puertos instalada.
Product Name	El nombre de producto de la tarjeta de puertos instalada.
Product Description	La descripción detallada del producto de la tarjeta de puertos instalada.

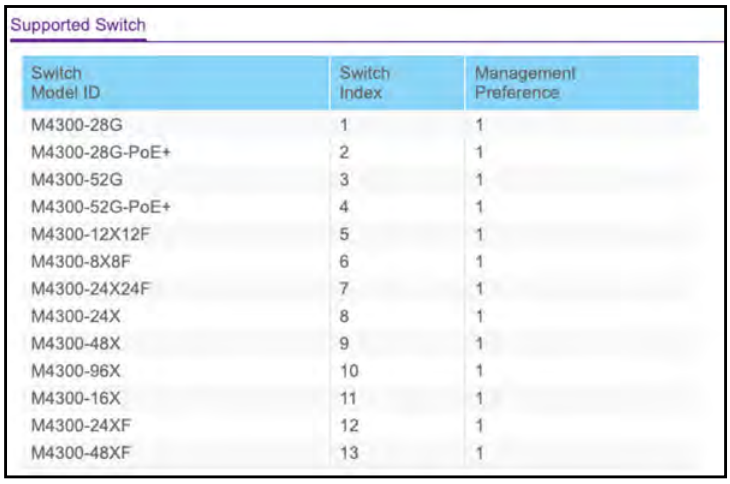


Supported Card

Card Model	Card Index	Card Type	Card Descriptor
APM408C	11	0xc6860000	APM408C copper 8-port card
APM408P	12	0xc6870000	APM408P copper 8-port POE card
APM408F	13	0xc6880000	APM408F Fiber 8-port card
APM402XL	14	0xc6890000	APM402XL QSFP+ 2-port card
TPM404H	15	0xc68a0000	TPM404H HDMI 4-port card

La siguiente tabla describe la información de la tabla Supported Card.

Campo	Descripción
Card Model	El ID de modelo de la tarjeta de puertos compatible.
Card Index	El índice asignado al tipo de tarjeta de puertos.
Card Type	El tipo de hardware de la tarjeta de puertos compatible, asignado por el fabricante.
Card Descriptor	La descripción de la tarjeta de puertos compatible, que incluye el número de producto del fabricante e información sobre el número y la velocidad de las interfaces compatibles.



Supported Switch

Switch Model ID	Switch Index	Management Preference
M4300-28G	1	1
M4300-28G-PoE+	2	1
M4300-52G	3	1
M4300-52G-PoE+	4	1
M4300-12X12F	5	1
M4300-8X8F	6	1
M4300-24X24F	7	1
M4300-24X	8	1
M4300-48X	9	1
M4300-96X	10	1
M4300-16X	11	1
M4300-24XF	12	1
M4300-48XF	13	1

La siguiente tabla describe la información de la tabla Supported Switch. Si preconfigura un nuevo miembro de pila, el índice del switch identifica el tipo de switch que se agrega a la pila.

Campo	Descripción
Switch Model ID	El número de modelo del switch compatible.
Switch Index	El índice asignado al switch compatible.
Management Preference	La preferencia de administración del switch compatible.

Configurar una interfaz loopback

Puede crear, configurar y eliminar interfaces loopback.

Para configurar una interfaz loopback:

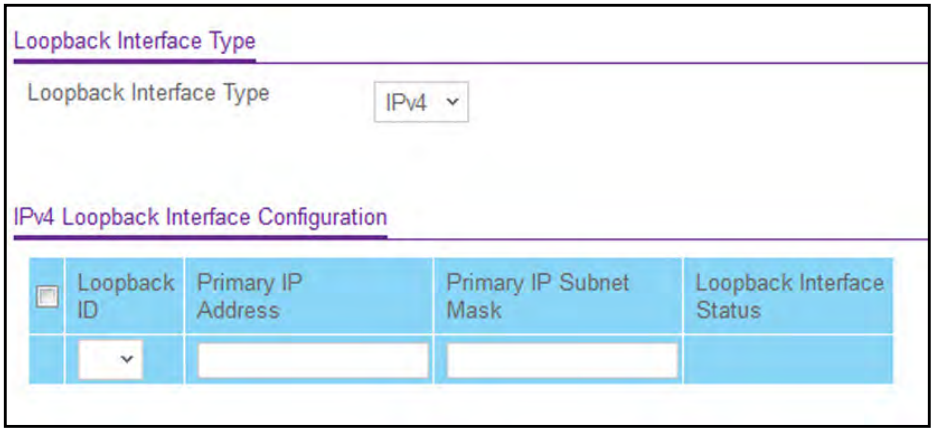
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Loopback Interface.



5. Use la lista Loopback Interface Type para seleccionar una interfaz loopback IPv4 o IPv6.

6. En la lista Loopback ID, seleccione una de las interfaces loopback configuradas actualmente.

7. En el campo Primary IP Address, introduzca la dirección principal de esta interfaz en notación decimal con puntos.

   Esta opción es visible cuando se selecciona loopback IPv4.

8. En el campo Primary IP Subnet Mask, introduzca la máscara de subred IPv4 principal en notación decimal con puntos.

   Esta opción es visible cuando se selecciona loopback IPv4.

9. En el campo Secondary IP Address, introduzca la dirección IP secundaria en notación decimal con puntos.

   Este campo solo es visible si se selecciona Add Secondary. Esta opción es visible cuando se selecciona loopback IPv4.

10. En el campo Secondary Subnet Mask, introduzca la máscara de subred secundaria de esta interfaz en notación decimal con puntos.

    Este campo solo es visible si se selecciona Add Secondary. Esta opción es visible cuando se selecciona loopback IPv4.

11. En el campo IPv6 mode, habilite IPv6 en esta interfaz usando la dirección IPv6.

    Esta opción se puede configurar antes de especificar una dirección IPv6 explícita. Esta opción es visible cuando se selecciona loopback IPv6.

12. Use el campo IPv6 Address para introducir la dirección IPv6 en formato prefijo/longitud. Esta opción es visible cuando se selecciona loopback IPv6.
13. Use el campo EUI64 para especificar opcionalmente el identificador único extendido de 64 bits (EUI-64). Esta opción es visible cuando se selecciona loopback IPv6.
14. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar las interfaces de administración

La interfaz del navegador local incluye opciones separadas para la administración IP basada en interfaz y en puerto. Al configurar la administración IP basada en puerto, se deshabilita la administración IP basada en VLAN (predeterminada/existente), y viceversa.

La interfaz de origen de las aplicaciones se establece en la VLAN 1 de forma predeterminada. Cambiar la VLAN de administración IPv4 y el puerto a un valor no predeterminado también establece automáticamente la interfaz de origen en la VLAN/puerto predeterminado VLAN 1.

Configurar el puerto de servicio IPv4

Puede configurar la información de red del puerto de servicio IPv4. El puerto de servicio es un puerto Ethernet dedicado a la administración fuera de banda del dispositivo. El tráfico de este puerto está separado del tráfico de red operativo de los puertos del switch y no se puede conmutar ni enrutar a la red operativa.

Para configurar el puerto de servicio IPv4:

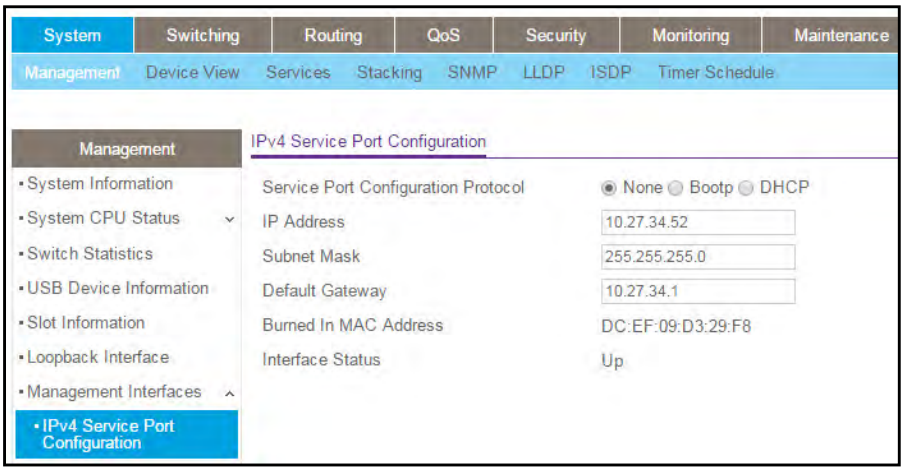
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Management > Management Interfaces > IPv4 Service Port Configuration.



5. 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 intentar obtener información de un servidor BootP de la red.
   - DHCP. En el siguiente ciclo de arranque, el cliente DHCP del dispositivo difunde una solicitud DHCP para intentar obtener información de un servidor DHCP de la red.
   - None. El dispositivo no intenta obtener información de red de forma dinámica.
   - Esto especifica cómo obtiene el dispositivo la información de red en el puerto de servicio.
6. En el campo IP Address, especifique la dirección IP de la interfaz.
   - Si el protocolo de configuración del puerto de servicio es None, puede configurar manualmente una dirección IP estática.
   - Si el protocolo de configuración del puerto de servicio es BootP o DHCP, este campo muestra la dirección IP obtenida dinámicamente (si la hay).
7. En el campo Subnet Mask, especifique la máscara de subred IP de la interfaz:
   - Si el protocolo de configuración del puerto de servicio es None, puede configurar manualmente una máscara de subred estática.
   - Si el protocolo de configuración del puerto de servicio es BootP o DHCP, este campo muestra la máscara de subred obtenida dinámicamente (si la hay).
8. En el campo Default Gateway, especifique la puerta de enlace predeterminada de la interfaz IP:
   - Si Service Port Configuration Protocol es None, puede configurar manualmente la dirección IP de la puerta de enlace predeterminada.
   - Si Service Port Configuration Protocol es BootP o DHCP, este campo muestra la dirección de la puerta de enlace predeterminada obtenida dinámicamente (si la hay).
9. Haga clic en el botón Apply.

La configuración se guarda.

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

Tabla 15. Configuración del puerto de servicio IPv4

Campo	Descripción
Burned-in MAC Address	La dirección MAC grabada de fábrica que se usa para la conectividad fuera de banda.
Interface Status	Indica si el estado del enlace es activo o inactivo.

Configurar el puerto de servicio IPv6

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

Para configurar el puerto de servicio IPv6:

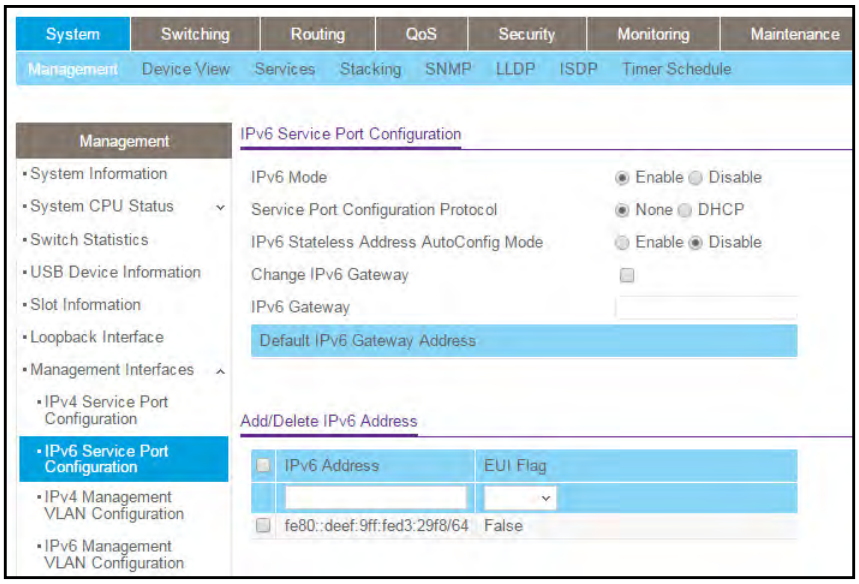
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Management Interfaces > IPv6 Service Port Configuration.



5. Seleccione el botón de opción Enable o Disable de IPv6 mode.
Esto especifica el modo administrativo IPv6 del puerto de servicio.
6. Seleccione el botón de opción None o DHCP de Service Port Configuration Protocol.

Esto especifica si el dispositivo obtiene la información de red de un servidor DHCPv6. Si selecciona None, se deshabilita el cliente DHCPv6 en el puerto de servicio.

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

- Enable. El puerto de servicio puede obtener una dirección IPv6 mediante IPv6 Neighbor Discovery Protocol (NDP) y mediante 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.

8. El campo DHCPv6 Client DUID muestra el identificador de cliente que usa el cliente DHCPv6 (si está habilitado) al enviar mensajes al servidor DHCPv6.

9. Para configurar la puerta de enlace IPv6, seleccione la casilla Change IPv6 Gateway. La puerta de enlace IPv6 es la puerta de enlace predeterminada de la interfaz del puerto de servicio IPv6.

10. Use el campo IPv6 Gateway para especificar la puerta de enlace predeterminada de la interfaz del puerto de servicio IPv6.

La tabla Add/Delete IPv6 Address muestra las direcciones IPv6 estáticas configuradas manualmente en la interfaz del puerto de servicio.

11. Especifique lo siguiente:

a. En el campo IPv6 Address, especifique la dirección IPv6 que desea agregar o quitar de la interfaz del puerto de servicio.

b. Seleccione la opción EUI Flag para habilitar el indicador Extended Universal Identifier (EUI) de la dirección IPv6, o desmárquela para omitirlo.

12. Haga clic en el botón Add.
La dirección IPv6 se agrega a la interfaz del puerto de servicio.
13. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Descripción general de la VLAN de administración

Para administrar el dispositivo con la utilidad de configuración web, la dirección IP de administración del dispositivo debe estar definida y ser conocida. De forma predeterminada se crea una interfaz VLAN de administración, que obtiene una dirección IP si hay un servidor DHCP. Si no obtiene una dirección IP, se le asigna la dirección alternativa 169.254.100.100/255.255.0.0. La VLAN de administración se usa como interfaz de origen predeterminada para syslog, el registro de mensajes, el cliente SNMP, etc. La interfaz de red está deshabilitada 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 a la VLAN de administración del switch no afectan la configuración de los puertos del panel frontal a través de los cuales se conmuta o enruta el tráfico.

Para acceder al switch a través de una red, primero debe configurarlo con información IP (dirección IP, máscara de subred). Puede configurar la información IP mediante cualquiera de los siguientes:

- 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 los siguiente:

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

Configurar una VLAN de administración IPv4

Para configurar una VLAN de administración IPv4:

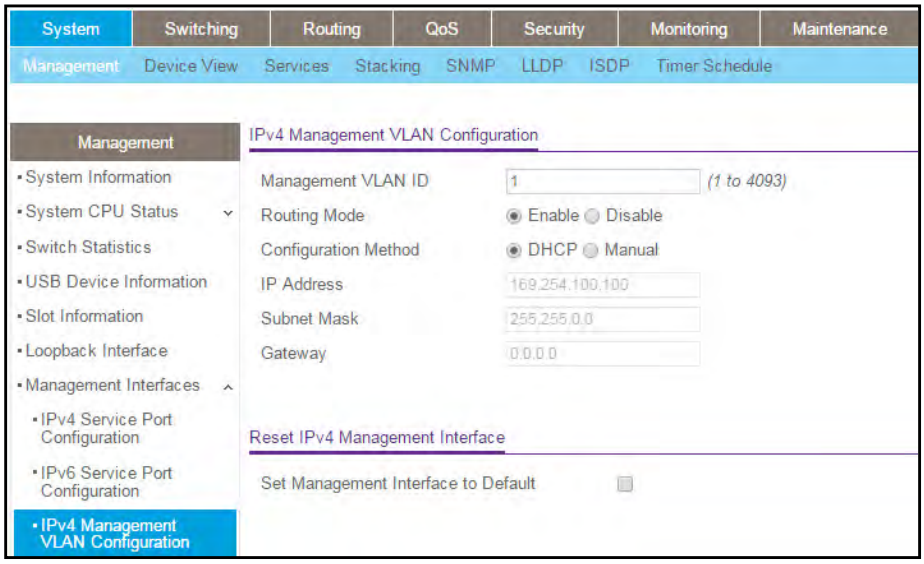
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Management > Management Interfaces > IPv4 Management VLAN Configuration.



5. En el campo Management VLAN ID, especifique el ID de la VLAN de administración del switch. La VLAN de administración se usa para administrar el switch. Puede configurarse con cualquier valor en el rango de 1–4093.

6. Seleccione el botón de opción Routing Mode para habilitar (Enable) o deshabilitar (Disable) el enrutamiento global en el dispositivo. El valor predeterminado es Enable.

7. Seleccione el botón de opción Configuration Method DHCP o Manual:

- DHCP. Transmite una solicitud DHCP.
- Manual. No hace nada.

Esto especifica lo que hace el switch al arrancar.

8. Especifique la dirección IP (IP Address) de la interfaz. El valor predeterminado de fábrica es 169.254.100.100.

9. Especifique la máscara de subred IP (IP Subnet Mask) de la interfaz. También se conoce como máscara de subred/red y define la parte de la dirección IP de la interfaz que identifica la red conectada.

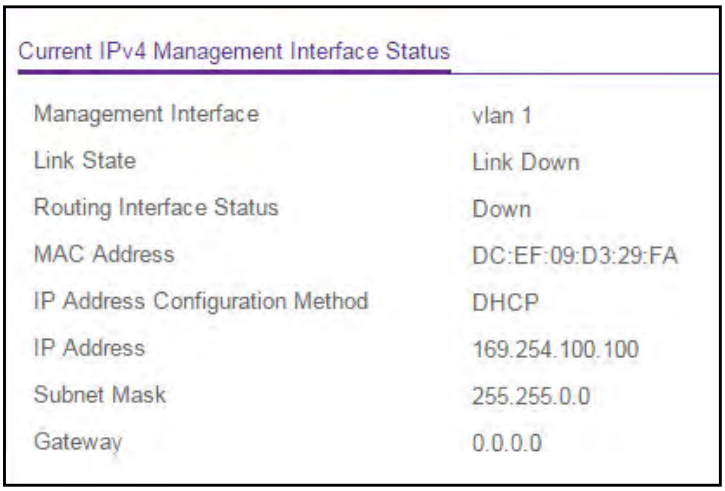
El valor predeterminado de fábrica es 255.255.0.0.

10. Especifique la puerta de enlace (Gateway) de la interfaz VLAN de administración. El valor predeterminado de fábrica es 0.0.0.0.

11. En la sección Reset IPv4 Management Interface de la página, use la opción Set Management Interface to Default para establecer la interfaz de administración IPv4 en la VLAN 1 predeterminada.

12. Haga clic en el botón Apply.

La configuración se guarda.
El estado actual de la interfaz de administración IPv4 se muestra en la parte inferior de la página.



La siguiente tabla describe los campos no configurables.

Tabla 16. Estado no configurable de la interfaz de administración IPv4

Campo	Descripción
Management Interface	Muestra la interfaz de administración IPv4 actual
Link State	Indica si el estado del enlace es activo o inactivo.
Routing Interface Status	Indica si el estado del enlace de la interfaz de administración es activo o inactivo.
MAC Address	La dirección MAC asignada a la interfaz de administración.
IP Address Configuration Method	Indica si el método de configuración de la dirección IP es DHCP o manual.
IP Address	La dirección IP de la interfaz de administración.
Subnet Mask	La máscara de subred IP de la interfaz de administración.
Gateway	La puerta de enlace predeterminada especificada para la interfaz de administración.

Configurar una VLAN de administración IPv6

Para la administración IPv6, puede usar la misma VLAN que la administración IPv4 o una VLAN distinta. La configuración de administración IPv6 no existe de forma predeterminada y debe crearla manualmente.

Para configurar una VLAN de administración IPv6:

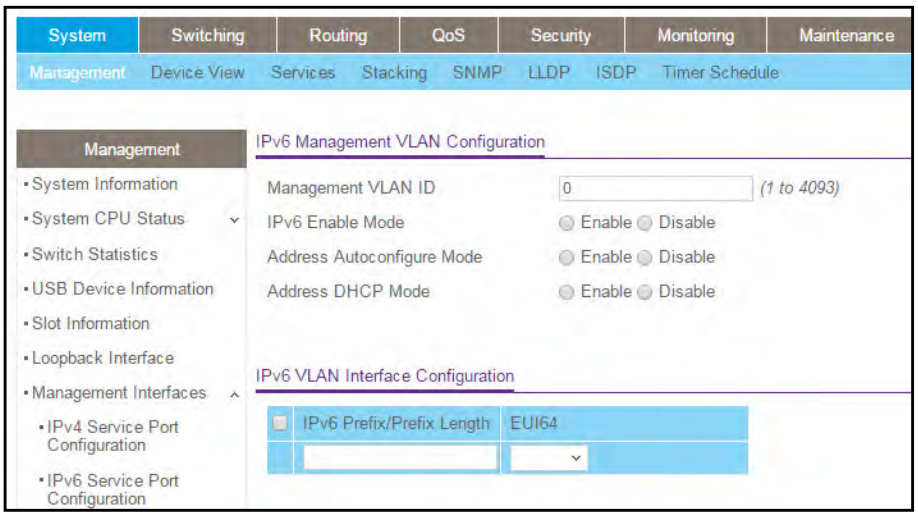
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Management Interfaces > IPv6 Management VLAN Configuration.



5. En el campo Management VLAN ID, especifique el ID de la VLAN de administración del switch. La VLAN de administración se usa para administrar el switch. El ID de VLAN puede ser cualquier valor de 1 a 4093. De forma predeterminada no hay ninguna interfaz de administración IPv6 configurada.

6. Seleccione el botón de opción IPv6 Enable Mode para habilitar o deshabilitar el modo de administración de la interfaz IPv6 de la VLAN de administración en el switch.

7. Seleccione el botón de opción para habilitar o deshabilitar Address Autoconfigure Mode. Si selecciona Enable, los parámetros de red IPv6 (prefijo IPv6 y longitud de prefijo) se configuran automáticamente para la interfaz VLAN de administración configurada. El valor predeterminado para la VLAN 1 es Auto Config.

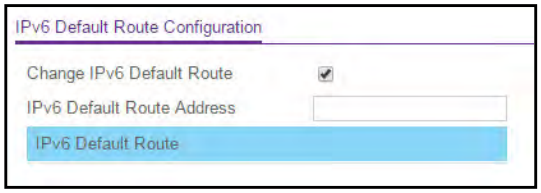
   Nota: La opción Address Autoconfigure mode solo está disponible si el enrutamiento unicast está deshabilitado globalmente.

8. Seleccione el botón de opción Address DHCP Mode Enable o Disable.

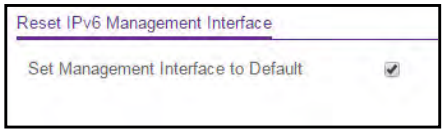
9. En la sección IPv6 VLAN Interface Configuration de la página, seleccione la opción IPv6 Prefix/Prefix Length y especifique la dirección IPv6 que desea agregar o quitar de la interfaz VLAN de administración. Si está seleccionado Address Autoconfigure Mode, este campo muestra el prefijo IPv6 y la longitud de prefijo correspondientes.

10. Establezca la opción EU164 en True para habilitar el indicador Extended Universal Identifier (EUI) de una dirección IPv6. El valor es False si no se especifica.
11. Haga clic en el botón Add.
La dirección IPv6 se agrega a la VLAN de administración.
12. Haga clic en el botón Apply.
La configuración se guarda.

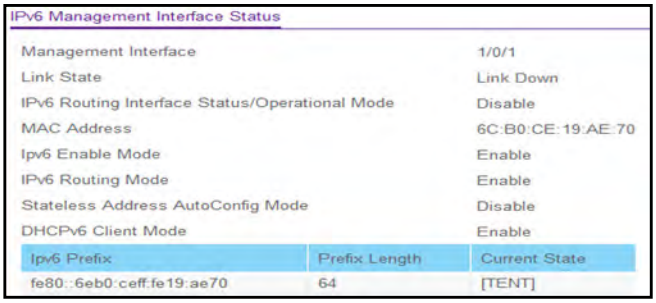
En la sección IPv6 Default Route Configuration de la página, el valor no configurable IPv6 Default Route es la ruta predeterminada de la interfaz VLAN IPv6.



13. Para hacer cambios, haga lo siguiente:
- Para agregar o quitar la ruta predeterminada IPv6, seleccione la opción Change IPv6 Default Route y especifique la dirección en el campo IPv6 Default Route Address.
- Para restablecer la interfaz de administración IPv6 a la VLAN 1 predeterminada, seleccione la opción Set Management Interface to Default.



14. Si hace algún cambio, haga clic en el botón Apply.
La configuración se guarda.
De forma predeterminada no hay ninguna interfaz de administración IPv6.
El estado actual de la interfaz de administración IPv6 se muestra en la parte inferior de la página.



La siguiente tabla describe los campos no configurables.

Tabla 17. Estado actual de la interfaz de administración IPv6

Campo	Descripción
Management Interface	Muestra la interfaz de administración IPv6 actual
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 es activo o inactivo.
MAC Address	La dirección MAC asignada a la interfaz de administración.
IPv6 Enable Mode	Indica si IPv6 Enable Mode está habilitado o deshabilitado en la interfaz de administración.
IPv6 Routing Mode	Indica si IPv6 Routing Mode está habilitado o deshabilitado en la interfaz de administración.
Stateless Address Autoconfig Mode	Indica si el modo de autoconfiguración de direcciones IP está habilitado o deshabilitado en la interfaz de administración.
DHCPv6 Client Mode	El modo Address DHCP en la interfaz de administración.
IPv6 Default Gateway	La puerta de enlace predeterminada IPv6 del switch.
IPv6 Next Hop Interface	La interfaz de siguiente salto IPv6 del switch.
Prefix Length	La longitud de prefijo en la interfaz de administración.
EU164	El indicador EUI-64 de la dirección IPv6 en la interfaz de administración.
Current State	El estado actual de la dirección IPv6 en la interfaz de administración.

Configurar una interfaz de administración IPv4

Use esta página para la administración IP basada en puertos para IPv4.

Para configurar una interfaz de administración IPv4:

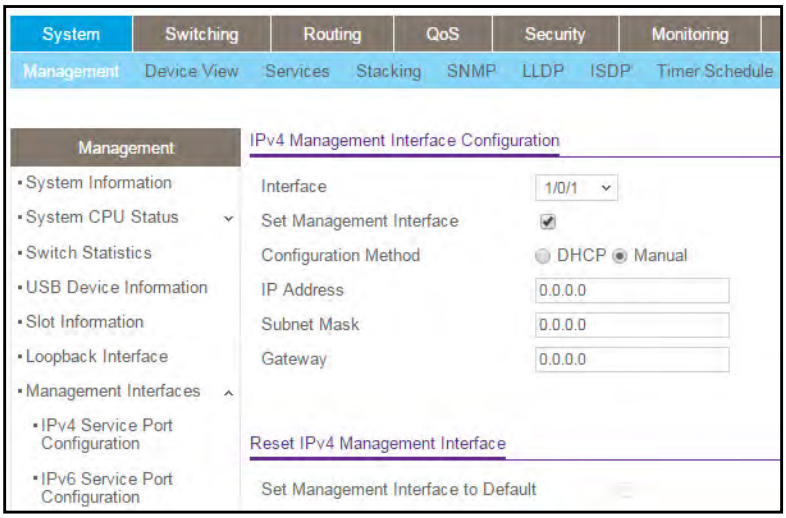
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Management Interfaces > IPv4 Management Interface Configuration.



5. Use la lista Interface para seleccionar la interfaz cuyos parámetros IPv4 o interfaz de administración desea cambiar.

6. Al seleccionar la opción Set Management Interface, la interfaz de administración se configura según la interfaz seleccionada.

De forma predeterminada, esta opción no está seleccionada.
7. Seleccione el botón de opción Configuration Method DHCP o Manual.
8. Especifique la dirección IP de la interfaz y la máscara de subred de la interfaz de administración.

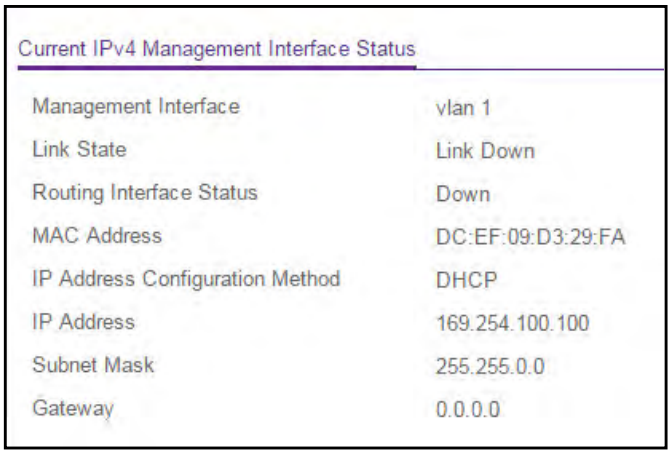
También se conoce como máscara de subred/red y define la parte de la dirección IP de la interfaz que identifica la red conectada. El valor predeterminado de fábrica es 169.254.100.100.

9. En el campo Subnet Mask, especifique la máscara de subred IP de la interfaz.
El valor predeterminado de fábrica es 255.255.0.0.
10. En el campo Gateway, especifique la puerta de enlace predeterminada de la interfaz de administración. El valor predeterminado es 0.0.0.0.

Nota: Si necesita restablecer la interfaz de administración IPv4, en la sección Reset IPv4 Management Interface de la página, use la opción Set Management Interface to Default para eliminar la configuración de la interfaz de administración IPv4 basada en puertos y restablecer la interfaz de administración IPv4 a la VLAN 1 predeterminada.

---

11. Haga clic en el botón Apply.
La configuración se guarda.
El estado actual de la interfaz de administración IPv4 se muestra en la parte inferior de la página.



La siguiente tabla describe los campos no configurables.

Tabla 18. Estado no configurable de la interfaz de administración IPv4

Campo	Descripción
Management Interface	Muestra la interfaz de administración IPv4 actual
Link State	Indica si el estado del enlace es activo o inactivo.
Routing Interface Status	Indica si el estado del enlace de la interfaz de administración es activo o inactivo.
MAC Address	La dirección MAC asignada a la interfaz de administración.
IP Address Configuration Method	Indica si el método de configuración de la dirección IP es DHCP o manual.
IP Address	La dirección IP de la interfaz de administración.
Subnet Mask	La máscara de subred IP de la interfaz de administración.
Gateway	La puerta de enlace predeterminada especificada para la interfaz de administración.

Configurar una interfaz de administración IPv6

Use esta página para la administración IP basada en puertos para IPv6.

Para configurar una interfaz de administración IPv6:

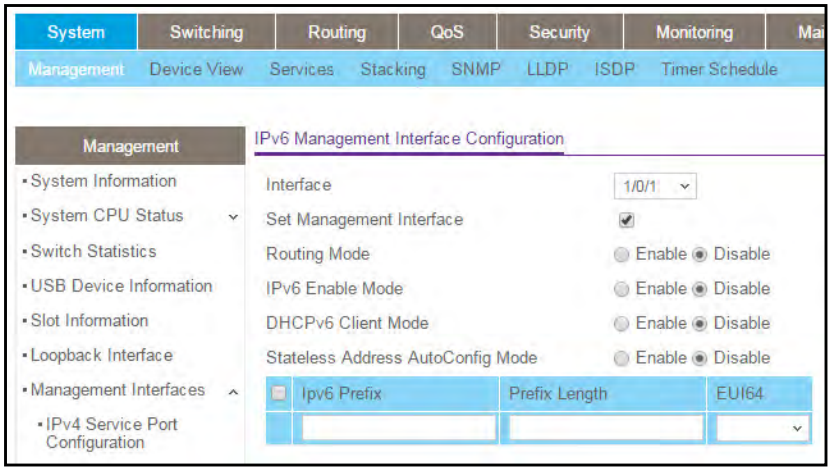
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

4. Haga clic en el botón Login.
Se muestra la página System Information.

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



6. Use la lista Interface para seleccionar la interfaz cuyos parámetros IPv6 o interfaz de administración desea cambiar.

7. Al seleccionar la opción Set Management Interface, la interfaz de administración se configura según la interfaz seleccionada. De forma predeterminada, esta opción no está seleccionada.

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

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

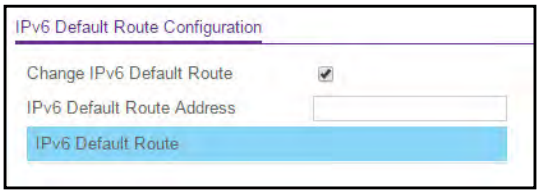
10. Seleccione el botón de opción para habilitar o deshabilitar DHCPv6 Client Mode en la interfaz de administración.

11. Seleccione el botón de opción para habilitar o deshabilitar Address Autoconfigure Mode en la interfaz de administración.

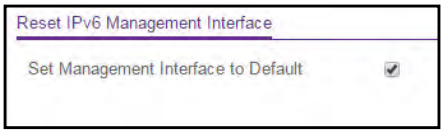
Nota: La opción Address AutoConfigure Mode solo está disponible si Unicast Routing está deshabilitado globalmente.

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

En la sección IPv6 Default Route Configuration de la página, el valor no configurable IPv6 Default Route es la ruta predeterminada de la interfaz de administración IPv6.



13. Para hacer cambios, haga lo siguiente:
    - Para agregar o quitar la ruta predeterminada IPv6, seleccione la opción Change IPv6 Default Route y especifique la dirección en el campo IPv6 Default Route Address.
    - En la sección Reset IPv6 Management Interface de la página, use la opción Set Management Interface to Default para eliminar la configuración de la interfaz de administración IPv6 basada en puertos y restablecer la interfaz de administración IPv6 a la VLAN 1 predeterminada.



14. Si hace algún cambio, haga clic en el botón Apply. La configuración se guarda.

El estado actual de la interfaz de administración IPv6 se muestra en la parte inferior de la página. La siguiente tabla describe los campos no configurables.

Tabla 19. Estado actual de la interfaz de administración IPv6

Campo	Descripción
Management Interface	Muestra la interfaz de administración IPv6 actual
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 es activo o inactivo.
MAC Address	La dirección MAC asignada a la interfaz de administración.
IP Address Configuration Method	Indica si el método de configuración de la dirección IP es DHCP o manual.
IP Address	La dirección IP de la interfaz de administración.
Subnet Mask	La máscara de subred IP de la interfaz de administración.
Gateway	La puerta de enlace predeterminada especificada para la interfaz de administración.

Administrar los ajustes de hora

El software del switch admite Simple Network Time Protocol (SNTP). Como su nombre indica, es una versión menos compleja de Network Time Protocol, un sistema para sincronizar los relojes de computadoras en red, principalmente cuando la transferencia de datos se realiza a través de Internet.

Configurar el ajuste de hora

Para configurar el ajuste de hora:

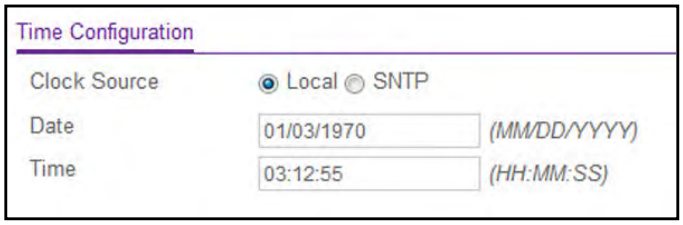
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Time > Time Configuration.



5. Seleccione el botón de opción Clock Source Local o SNTP.

   El valor predeterminado es SNTP. El reloj local solo puede establecerse en SNTP si se cumplen las dos condiciones siguientes:

   - El servidor SNTP está configurado.
   - El estado del último intento SNTP es exitoso.

6. En el campo Date, especifique la fecha actual en meses, días y años.
7. En el campo Time, especifique la hora actual en horas, minutos y segundos.
8. Haga clic en el botón Apply (Aplicar).

La configuración se guarda.

Configurar los ajustes globales de SNTP

Para configurar los ajustes globales de SNTP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

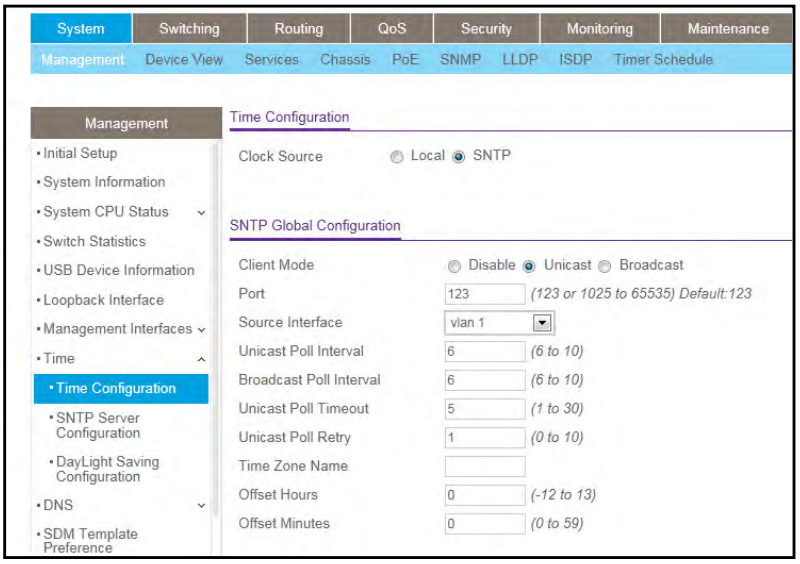
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Time > Time Configuration > SNTP Global Configuration.

   Al seleccionar la opción SNTP como Clock Source, la sección SNTP Global Configuration aparece debajo de la sección Time Configuration de la página.



5. Seleccione un botón de opción Client mode para especificar el modo de operación del cliente SNTP:
   - Disable. SNTP no está operativo. El cliente no envía solicitudes SNTP ni procesa los mensajes SNTP recibidos.
   - Unicast. SNTP opera punto a punto. Un cliente unicast envía una solicitud a un servidor designado en su dirección unicast y espera una respuesta con la que puede determinar la hora y, opcionalmente, el retardo de ida y vuelta y el desfase del reloj local respecto al servidor.
   - Broadcast. SNTP opera igual que el modo multicast, pero usa una dirección de difusión local en lugar de una dirección multicast. La dirección de difusión tiene un alcance de una sola subred, mientras que una dirección multicast tiene alcance en todo Internet.

El valor predeterminado es Unicast.
6. En el campo Port, especifique el puerto UDP local en el que el cliente SNTP recibe los paquetes del servidor.

El rango permitido es de 1025 a 65535 y el valor 123. 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.

7. Seleccione la interfaz de origen (Source Interface) para el cliente SNTP. Los valores posibles son los siguientes:

- None
- VLAN 1
- Interfaz de enrutamiento
- Routing VLAN
- Interfaz loopback de enrutamiento
- Interfaz de túnel
- Puerto de servicio

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

8. Especifique el valor de Unicast Poll Interval.

Es el número de segundos entre solicitudes de sondeo unicast, expresado como potencia de dos, en modo unicast. El rango permitido es de 6 a 10. El valor predeterminado es 6.

9. Especifique el valor de Broadcast Poll Interval.

Es el número de segundos entre solicitudes de sondeo de difusión, expresado como potencia de 2, en modo broadcast. Las difusiones recibidas antes de que venza este intervalo se descartan. El rango permitido es de 6 a 10. El valor predeterminado es 6.

10. Especifique el valor de Unicast Poll Timeout.

Es el número de segundos que se espera una respuesta SNTP en modo unicast. El rango permitido es de 1 a 30. El valor predeterminado es 5.

11. Especifique el valor de Unicast Poll Retry.

Es el número de reintentos de una solicitud a un servidor SNTP tras el primer tiempo de espera, antes de intentar usar el siguiente servidor configurado, en modo unicast. El rango permitido es de 0 a 10. El valor predeterminado es 1.

12. Use el campo Time Zone Name para configurar una zona horaria especificando el número de horas y, opcionalmente, de minutos de diferencia con UTC mediante Offset Hours y Offset Minutes.

La zona horaria puede afectar la visualización de la hora actual del sistema. El valor predeterminado es UTC. Al usar servidores de hora SNTP/NTP para actualizar el reloj del switch, los datos de hora recibidos del servidor se basan en el Tiempo Universal Coordinado (UTC), que equivale a la hora del meridiano de Greenwich (GMT). Puede no ser la zona horaria en la que se encuentra el switch.

13. Use el campo Offset Hours para especificar el número de horas de diferencia con UTC. El rango permitido es de –12 a 13. El valor predeterminado es 0.
14. Use el campo Offset Minutes para especificar el número de minutos de diferencia con UTC. El rango permitido es de 0 a 59. El valor predeterminado es 0.
15. Haga clic en el botón Apply.
La configuración se guarda.

Ver el estado global de SNTP

Al seleccionar la opción SNTP como Clock Source, el estado global de SNTP se muestra debajo de la sección SNTP Global Configuration de la página.

Para ver el estado global de SNTP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

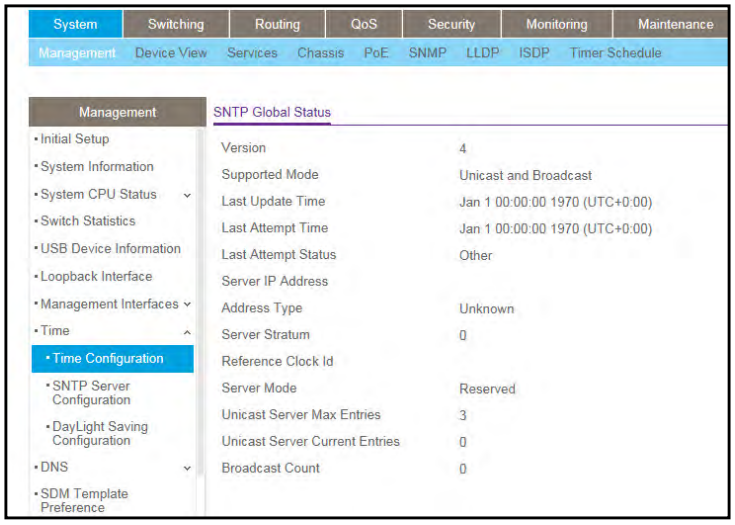
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Time > Time Configuration > SNTP Global Status

5. Seleccione la opción SNTP como Clock Source.
El estado SNTP Global Status se muestra debajo de la sección SNTP Global Configuration.



La siguiente tabla muestra la información no configurable de SNTP Global Status.

Tabla 20. 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 de la recepción de un mensaje no solicitado.
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 se aplican a todos los modos de operación. • Other. Ninguno de los siguientes valores. • Success. La operación SNTP fue exitosa 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 que admite el cliente. • Server Unsynchronized. El servidor SNTP no está sincronizado con sus pares. Esto se indica mediante el campo leap indicator del mensaje SNTP. • Server Kiss Of Death. El servidor SNTP indicó que no se deben enviar más consultas a este servidor. 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 por el 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 servidor unicast que se pueden configurar en este cliente.
Unicast Server Current Entries	El número de entradas de servidor unicast válidas configuradas actualmente para este cliente.
Broadcast Count	El número de mensajes SNTP de difusión no solicitados recibidos y procesados por el cliente SNTP desde el último reinicio.

Configurar un servidor SNTP

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

Las fuentes de hora se establecen 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 dispositivo recibe la hora del estrato 1 y superiores, ya que es un dispositivo de estrato 2.

El siguiente es un ejemplo 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 vinculado directamente a una fuente de hora de estrato 0. Los servidores de estrato 1 proporcionan los estándares primarios de hora de red.
- Estrato 2. La fuente de hora está separada del servidor de estrato 1 por una ruta de red. Por ejemplo, un servidor de estrato 2 recibe la hora a través de un enlace de red, mediante NTP, de un servidor de estrato 1.

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

Las definiciones de hora SNTP se evalúan y determinan según los siguientes niveles de hora:

- 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 dispositivo puede sondear servidores de tipo unicast para obtener la hora del servidor.

El sondeo de información unicast se usa para consultar un servidor cuya dirección IP se conoce. Solo se consultan los servidores SNTP configurados en el dispositivo para obtener información de sincronización. 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 definidos en el dispositivo mediante la página SNTP Server Configuration.

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

Puede ver y modificar la información para agregar y modificar servidores Simple Network Time Protocol (SNTP).

Para configurar los ajustes del servidor SNTP:

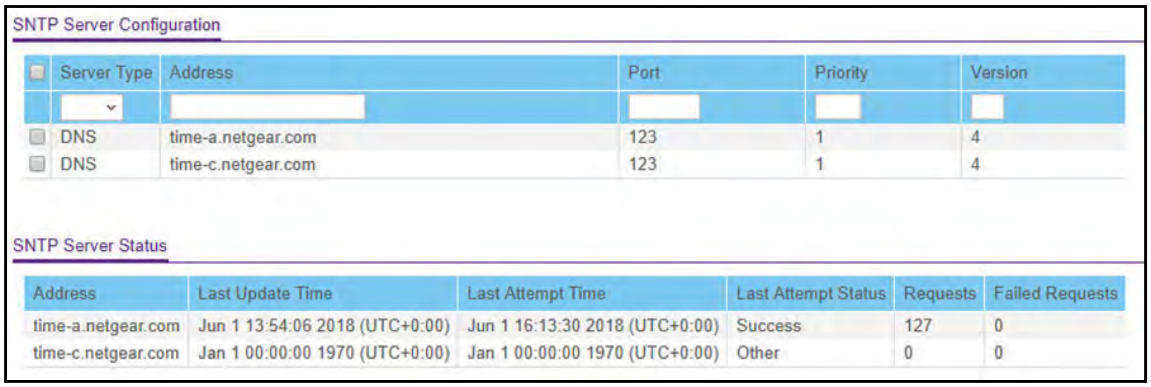
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Time > SNTP Server Configuration.



5. En la lista Server Type, seleccione el tipo de dirección del servidor SNTP configurado. Los valores posibles son los siguientes:

- IPv4
- IPv6
- DNS

El valor predeterminado es IPv4.
6. En el campo Address, especifique la dirección del servidor SNTP.

   Es 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 esta dirección es un nombre de host DNS, dicho nombre se resuelve en una dirección IP cada vez que se le envía una solicitud SNTP.

   De forma predeterminada existen dos servidores SNTP:

- time-a.netgear.com
- time-c.netgear.com

7. Introduzca en Port el número de puerto del servidor SNTP al que se envían las solicitudes SNTP. El rango válido es de 1 a 65535. El valor predeterminado es 123.

8. Especifique en Priority la prioridad de esta entrada para determinar el orden de los servidores a los que se envían las solicitudes SNTP.

   El cliente sigue enviando solicitudes a distintos servidores hasta recibir una respuesta correcta o agotar todos los servidores. La prioridad indica el orden en que se consultan los servidores. Un servidor con prioridad 1 se consulta antes que uno con prioridad 2, y así sucesivamente. Si varios servidores tienen la misma prioridad, el

orden de consulta sigue el orden lexicográfico de las entradas de esta tabla. El rango válido es de 1 a 3. El valor predeterminado es 1.

9. Especifique en NTP Version la versión de NTP que ejecuta el servidor. El rango es de 1 a 4. El valor predeterminado es 4.
10. Haga clic en el botón Add (Agregar).
Se agrega la entrada del servidor SNTP.
11. Repita los pasos anteriores para agregar más servidores SNTP. Puede configurar hasta tres servidores SNTP.
12. Haga clic en el botón Apply.
La configuración se guarda.

13. Para cambiar los ajustes, eliminar un servidor SNTP o actualizar la página, haga lo siguiente:

- Cambiar los ajustes. Para cambiar los ajustes de un servidor SNTP existente, marque la casilla junto al servidor configurado, introduzca los nuevos valores en los campos disponibles y haga clic en el botón Apply (Aplicar).

  La configuración se guarda.

- Eliminar un servidor SNTP. Para eliminar una entrada de servidor SNTP, marque la casilla junto al servidor configurado que desea eliminar y haga clic en el botón Delete (Eliminar).

  Se elimina la entrada y se actualiza el dispositivo.

- Actualizar la página. Para actualizar la página, haga clic en el botón Refresh (Actualizar).

La tabla SNTP Server Status muestra información de estado de los servidores SNTP configurados en el switch. En la siguiente tabla se muestra la información de SNTP Server Status.

Tabla 21. Estado del servidor SNTP

Campo	Descripción
Dirección	Todas las direcciones de servidor existentes. Si no hay ningún servidor configurado, aparece en la página el mensaje No SNTP server exists.
Última actualización	Fecha y hora locales (UTC) en que se usó la respuesta de este servidor para actualizar el reloj del sistema.
Último intento	Fecha y hora locales (UTC) en que se consultó por última vez este servidor SNTP.

Tabla 21. Estado del servidor SNTP (continuación)

Campo	Descripción
Estado del último intento	Estado de la última solicitud SNTP a este servidor. Si no se recibió ningún paquete de este servidor, se muestra el estado Other. • Other. Ninguno de los siguientes valores. • Success. La operación SNTP fue correcta 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 SNTP que admite el servidor no es compatible con la que admite el cliente. • Server Unsynchronized. El servidor SNTP no está sincronizado con sus pares. Esto se indica mediante 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 mediante un campo stratum igual a 0 en un mensaje recibido del servidor.
Solicitudes	Número de solicitudes SNTP hechas a este servidor desde el último reinicio del agente.
Solicitudes fallidas	Número de solicitudes SNTP fallidas hechas a este servidor desde el último reinicio.

Configurar el horario de verano

Para configurar el horario de verano:

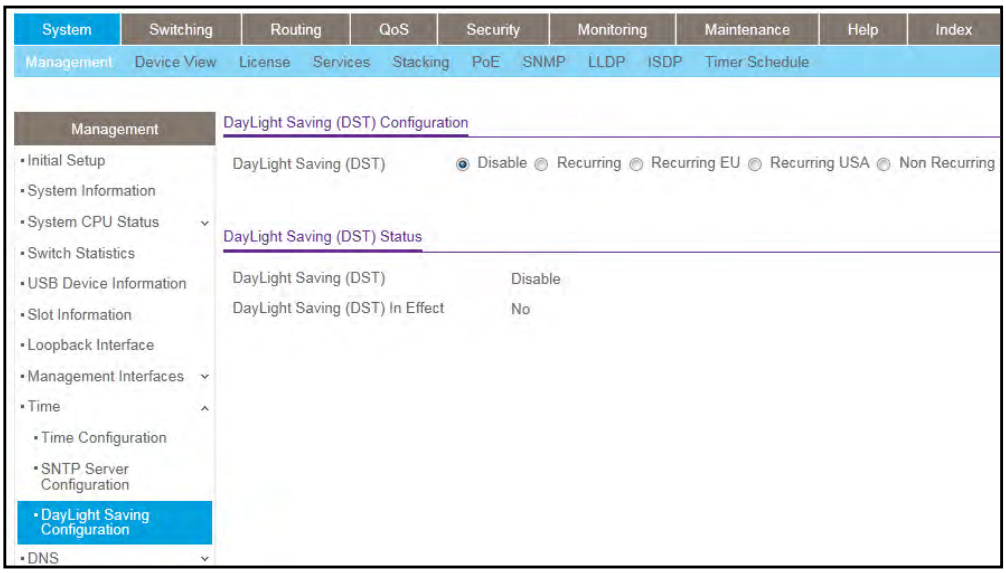
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Time > Daylight Saving Configuration.



5. Seleccione el botón de opción Daylight Saving (DST):
   - Disable. Deshabilita el horario de verano.
   - Recurring. Habilita el horario de verano recurrente.
   - Recurring EU. Habilita el horario de verano recurrente de la UE.
   - Recurring USA. Habilita el horario de verano recurrente de EE. UU.
   - Non Recurring. Configura un horario de verano no recurrente.
6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Los campos de las siguientes tablas solo están visibles cuando DayLight Saving es Recurring, Recurring EU o Recurring USA.

Tabla 22. Horario de verano - Recurrente

Campo	Descripción
Begins At	Estos campos configuran los valores de fecha y hora de inicio. • Week. Configura la semana de inicio. • Day. Configura el día de inicio. • Month. Configura el mes de inicio. • Hours. Configura la hora de inicio. • Minutes. Configura los minutos de inicio.
Ends At	Estos campos configuran los valores de fecha y hora de fin. • Week. Configura la semana de fin. • Day. Configura el día de fin. • Month. Configura el mes de fin. • Hours. Configura la hora de fin. • Minutes. Configura los minutos de fin.

Tabla 22. Horario de verano - Recurrente

Campo	Descripción
Offset	Configura el desfase recurrente en minutos. El rango válido es de 1 a 1440 minutos.
Zone	Configura la zona horaria.

Los campos de la siguiente tabla solo están visibles cuando DayLight Saving es Non Recurring.

Tabla 23. Horario de verano - No recurrente

Campo	Descripción
Begins At	Estos campos configuran los valores de fecha y hora de inicio. • Week. Configura la semana de inicio. • Day. Configura el día de inicio. • Month. Configura el mes de inicio. • Hours. Configura la hora de inicio. • Minutes. Configura los minutos de inicio.
Ends At	Estos campos configuran los valores de fecha y hora de fin. • Week. Configura la semana de fin. • Day. Configura el día de fin. • Month. Configura el mes de fin. • Hours. Configura la hora de fin. • Minutes. Configura los minutos de fin.
Offset	Configura el desfase no recurrente en minutos. El rango válido es de 1 a 1440 minutos.
Zone	Configura la zona horaria.

Ver el estado del horario de verano

Para ver el estado del horario de verano:

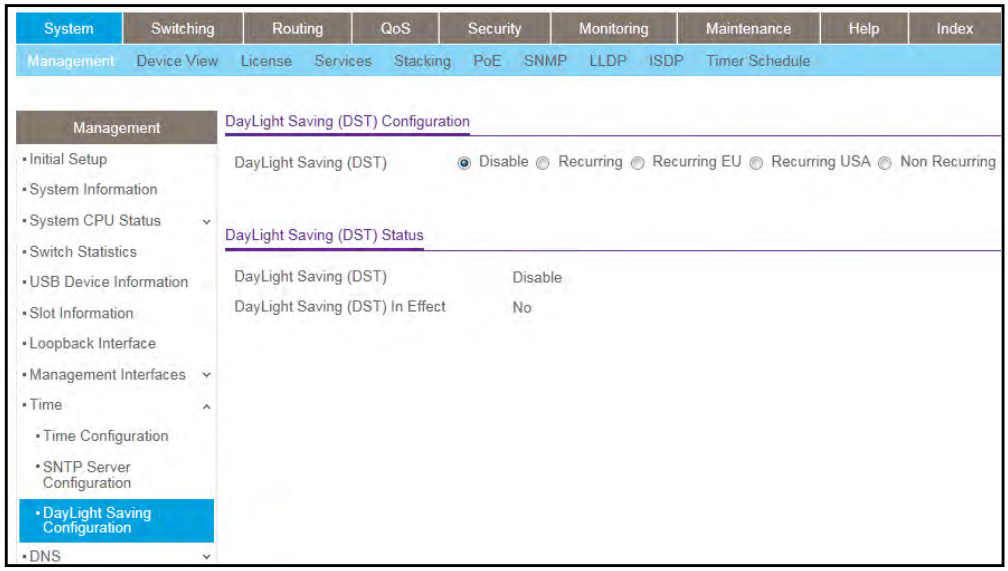
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Time > DayLight Saving Configuration.



5. Para actualizar la página, haga clic en el botón Actualizar (Refresh).
En la siguiente tabla se muestra la información de estado no configurable de Daylight Saving (DST).

Tabla 24. Estado del horario de verano

Campo	Descripción
Daylight Saving (DST)	Valor de Daylight Saving, que puede ser 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 si el horario de verano está deshabilitado.
Ends At	Muestra cuándo termina el horario de verano. Este campo no se muestra si el horario de verano está deshabilitado.
Offset (in Minutes)	Valor del desfase en minutos. Este campo no se muestra si el horario de verano está deshabilitado.
Zone	Siglas de la zona. Este campo no se muestra si el horario de verano está deshabilitado.
Daylight Saving (DST) in Effect	Muestra si el horario de verano está en vigor.

Administrar Precision Time Protocol

Precision Time Protocol (PTP, IEEE 1588) es un protocolo que permite sincronizar con precisión relojes con exactitud inferior al microsegundo en una red basada en paquetes. PTP permite que dispositivos de red de 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 deshabilitar PTP globalmente, en cuyo caso el switch no admite el paso transparente (pass-through) de PTP.

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

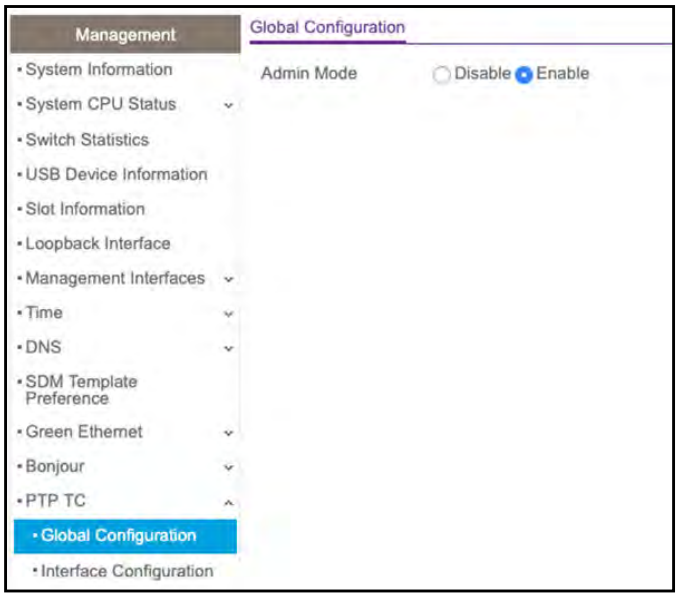
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > PTP TC > Global Configuration.



5. Seleccione el botón de opción Admin Mode Enable o Disable. El valor predeterminado es Enable.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Administrar la configuración de interfaz de PTP

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 transparente de PTP.

Para configurar los ajustes del reloj transparente PTP de extremo a extremo de una o más interfaces:

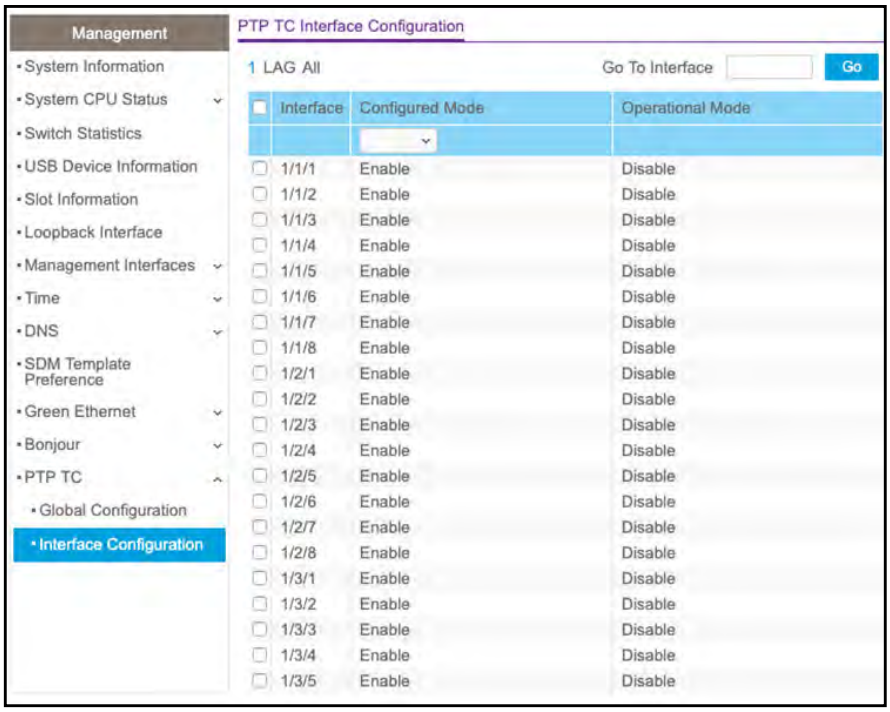
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > PTP TC > Interface Configuration.



5. 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, marque la casilla de la interfaz que desea configurar.

6. En el menú Configured Mode, seleccione Enable o Disable.

El valor predeterminado es Enable.
7. Haga clic en el botón Apply.
La configuración se guarda.
El campo Operational Mode indica si PTP está habilitado o deshabilitado en una interfaz.

Configurar los ajustes de DNS

Puede configurar la información de los servidores DNS que usa la red y cómo funciona el switch como cliente DNS.

Configurar los ajustes globales de DNS

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

Para configurar los ajustes globales de DNS:

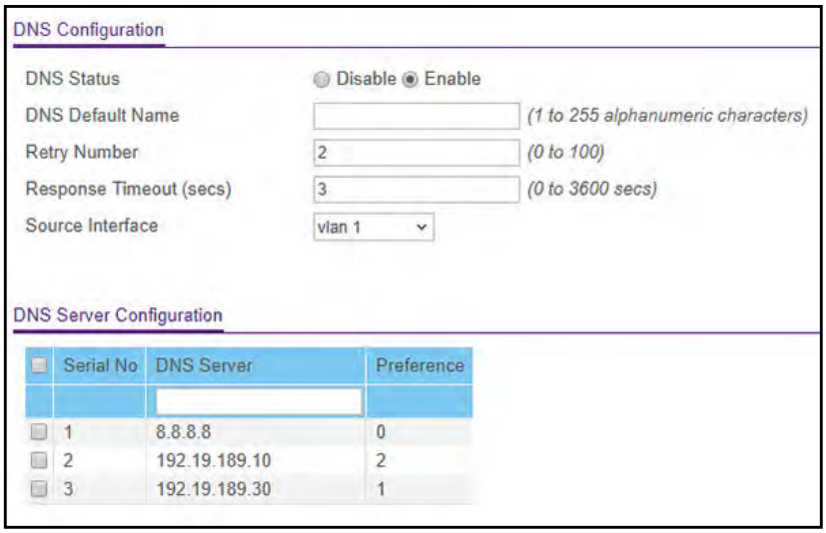
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > DNS > DNS Configuration.



La tabla DNS Server Configuration incluye un servidor DNS predeterminado con la dirección IP 8.8.8.8.

5. 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. El valor predeterminado es Enable.
   - Disable. Impide que el switch envíe consultas DNS.

6. Introduzca en DNS Default domain Name el nombre de dominio que se incluirá en las consultas DNS.

   Cuando el sistema realiza una búsqueda de 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 el usuario introduce test, test se cambia a test.netgear.com para resolver el nombre). La longitud del nombre no debe superar los 255 caracteres.

7. Use Retry Number para especificar el número de reintentos de envío de consultas DNS al servidor DNS.

   Este número va de 0 a 100. El valor predeterminado es 2.

8. Use Response Timeout (secs) para especificar el tiempo, en segundos, que se espera una respuesta a una consulta DNS.

   Este tiempo de espera va de 0 a 3600. El valor predeterminado es 3.

9. Especifique en Source Interface la interfaz de origen que se usará para DNS.

   Los valores posibles son los siguientes:

   - None
   - VLAN 1
   - Interfaz de enrutamiento
   - Routing VLAN
   - Interfaz loopback de enrutamiento

- Interfaz de túnel
- Puerto de servicio

De forma predeterminada, se usa VLAN 1 como interfaz de origen.
10. Para especificar el servidor DNS al que el switch envía las 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.

11. Para eliminar un servidor DNS de la tabla DNS Server Configuration, haga lo siguiente:

a. Marque la casilla del servidor.

b. Haga clic en el botón Eliminar (Delete).

Nota: Si hace clic en el botón Delete sin seleccionar un servidor DNS, se eliminan todos los servidores DNS de la tabla.

12. Haga clic en el botón Apply.
La configuración se guarda.
En la siguiente tabla se muestra la información de DNS Server Configuration.

Tabla 25. Configuración del servidor DNS

Campo	Descripción
N.º de serie	Número de secuencia del servidor DNS.
Preferencia	Muestra la preferencia del servidor DNS. La preferencia se determina por el orden en que se introdujeron.

Agregar una entrada estática a la tabla DNS local

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

Para agregar una entrada estática a la tabla DNS local:

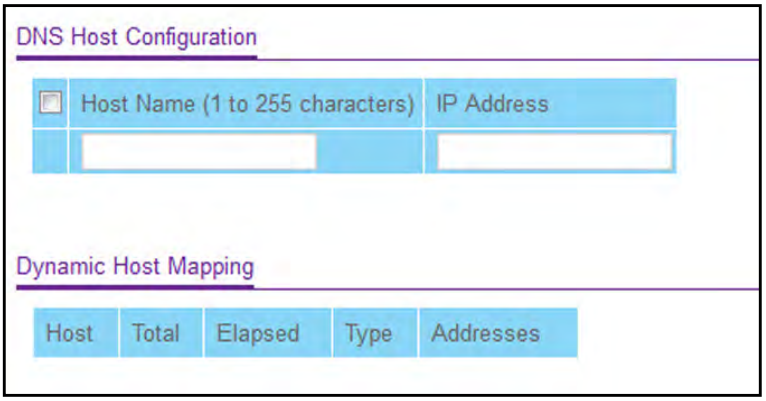
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. **Seleccione System > Management > DNS > Host Configuration.**



5. En el campo Host Name (1 to 255 characters), especifique el nombre de host estático que desea agregar. Su longitud no puede superar los 255 caracteres y es un campo obligatorio.

6. En el campo IP Address, introduzca la dirección IP en notación estándar IPv4 que se asociará con el nombre de host.

7. Haga clic en el botón Add (Agregar).
La entrada aparece en la lista de la página.

La tabla Dynamic Host Mapping muestra las entradas de nombre de host a dirección IP que el switch aprendió. En la siguiente tabla se describen los campos de host dinámico.

Tabla 26. Asignación dinámica de hosts DNS

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.
Transcurrido	Tiempo transcurrido desde la última actualización de la entrada dinámica.
Tipo	Tipo de la entrada dinámica.
Direcciones	Muestra la dirección IP asociada al nombre de host.

Configurar la preferencia de plantilla de administración de la base de datos del switch

Una plantilla Switch Database Management (SDM) es una descripción de los recursos máximos que un switch o router puede usar para diversas funciones. Distintas plantillas SDM permiten distintas combinaciones de factores de escala, lo que permite asignar los recursos de forma distinta según cómo se use el dispositivo. Es decir, las plantillas SDM le permiten reasignar los recursos del sistema para admitir una combinación distinta de funciones según los requisitos de su red.

Nota: Si conecta una unidad a una pila y su plantilla no coincide con la plantilla de la pila, la nueva unidad se reinicia automáticamente con la plantilla que usan los demás miembros de la pila. Para evitar el reinicio automático, primero establezca la plantilla SDM que usan los miembros existentes de la pila. Después, apague la nueva unidad, conéctela a la pila y enciéndala.

Puede configurar las preferencias de plantilla SDM del switch.

Para configurar los ajustes de SDM Template Preference:

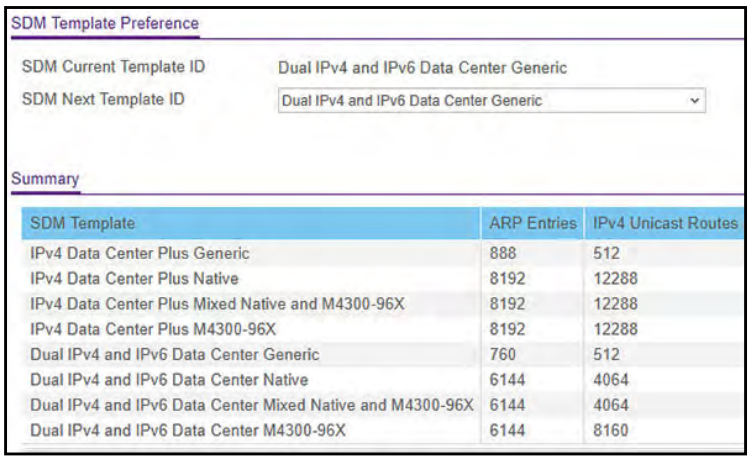
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > SDM Template Preference.



5. Use SDM Next Template ID para configurar la siguiente plantilla activa.

   Solo se activa después del siguiente reinicio. Para volver a la plantilla predeterminada después del siguiente reinicio, use la opción Default. Los valores posibles son los siguientes:

   - Default
   - IPv4 Data Center Plus Generic
   - Dual IPv4 and IPv6 Data Center Generic
   - IPv4 Data Center Plus Mixed Native and M4300-96X
   - IPv4 Data Center Plus M4300-96X
   - IPv4 Data Center Plus Native
   - Dual IPv4 and IPv6 Data Center Native
   - Dual IPv4 and IPv6 Data Center Plus Mixed Native and M4300-96X
   - Dual IPv4 and IPv6 Data Center M4300-96X

Nota: Las plantillas con la palabra clave Native solo se admiten en los switches independientes M4300-24X24F y M4300-48X y en una pila homogénea de switches M4300-24X24F y M4300-48X.

En la siguiente tabla se muestra la información de resumen.

Tabla 27. Resumen de SDM Template Preference

Campo	Descripción
SDM Current Template ID	Plantilla SDM activa actual. Los valores posibles son los siguientes: • IPv4 Data Center Plus Generic • IPv4 Data Center Plus Native • IPv4 Data Center Plus Mixed Native and M4300-96X • IPv4 Data Center Plus M4300-96X • Dual IPv4 and IPv6 Data Center Generic • Dual IPv4 and IPv6 Data Center Native • Dual IPv4 and IPv6 Data Center Plus Mixed Native and M4300-96X • Dual IPv4 and IPv6 Data Center M4300-96X
SDM Template	Identifica la plantilla. Los valores posibles son los siguientes: • IPv4 Data Center Plus Generic • IPv4 Data Center Plus Native • IPv4 Data Center Plus Mixed Native and M4300-96X • IPv4 Data Center Plus M4300-96X • Dual IPv4 and IPv6 Data Center Generic • Dual IPv4 and IPv6 Data Center Native • Dual IPv4 and IPv6 Data Center Plus Mixed Native and M4300-96X • Dual IPv4 and IPv6 Data Center M4300-96X
ARP Entries	Número máximo de entradas en la caché de Address Resolution Protocol (ARP) IPv4 para las interfaces de enrutamiento.

Tabla 27. Resumen de SDM Template Preference (continuación)

Campo	Descripción
IPv4 Unicast Routes	Número máximo de entradas de la tabla de reenvío unicast IPv4.
IPv6 NDP Entries	Número máximo de entradas de la caché de Neighbor Discovery Protocol (NDP) IPv6.
IPv6 Unicast Routes	Número máximo de entradas de la tabla de reenvío unicast IPv6.
ECMP Next Hops	Número máximo de siguientes saltos que se pueden instalar en las tablas de reenvío unicast IPv4 e IPv6.
IPv4 Multicast Routes	Número máximo de entradas de la tabla de reenvío multicast IPv4.
IPv6 Multicast Routes	Número máximo de entradas de la tabla de reenvío multicast IPv6.

Configurar los ajustes de Green Ethernet

Para configurar los ajustes de Green Ethernet:

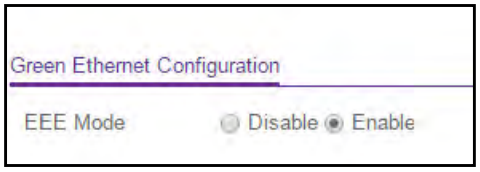
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Green Ethernet > Green Ethernet Configuration.



5. Seleccione el botón de opción EEE mode Disable o Enable. El valor de fábrica es Enable.

   Energy Efficient Ethernet (EEE) combina la MAC con una familia de PHY que admiten el funcionamiento en modo de bajo consumo. Está definido por el grupo IEEE 802.3az Energy Efficient Task Force. 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 dañan durante la transición hacia o desde el modo de bajo consumo. El tiempo de transición es transparente para los protocolos y aplicaciones de capas superiores.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar los ajustes de interfaz de Green Ethernet

Para configurar los ajustes de interfaz de Green Ethernet:

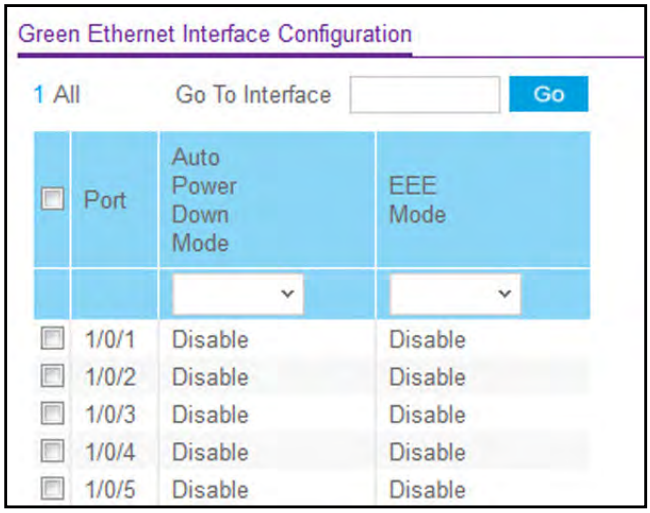
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Green Ethernet > Green Ethernet Interface Configuration.



5. 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, marque la casilla de la interfaz que desea configurar.
6. Use la opción Auto Power Down mode para habilitar o deshabilitar esta función.

   El valor de fábrica es Enable. Cuando el enlace del puerto está caído, el PHY se apaga automáticamente durante un breve periodo y luego se activa para comprobar los pulsos de enlace. Esto permite al switch realizar la autonegociación y ahorrar energía cuando no hay ningún equipo enlazado presente.

7. Use el menú EEE mode para habilitar (Enable) o deshabilitar (Disable) esta opción. El valor de fábrica es Disable. Si el modo EEE no es compatible, se muestra N/A.

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

Configurar los dispositivos locales y remotos de Green Ethernet

Para configurar los dispositivos locales y remotos de Green Ethernet:

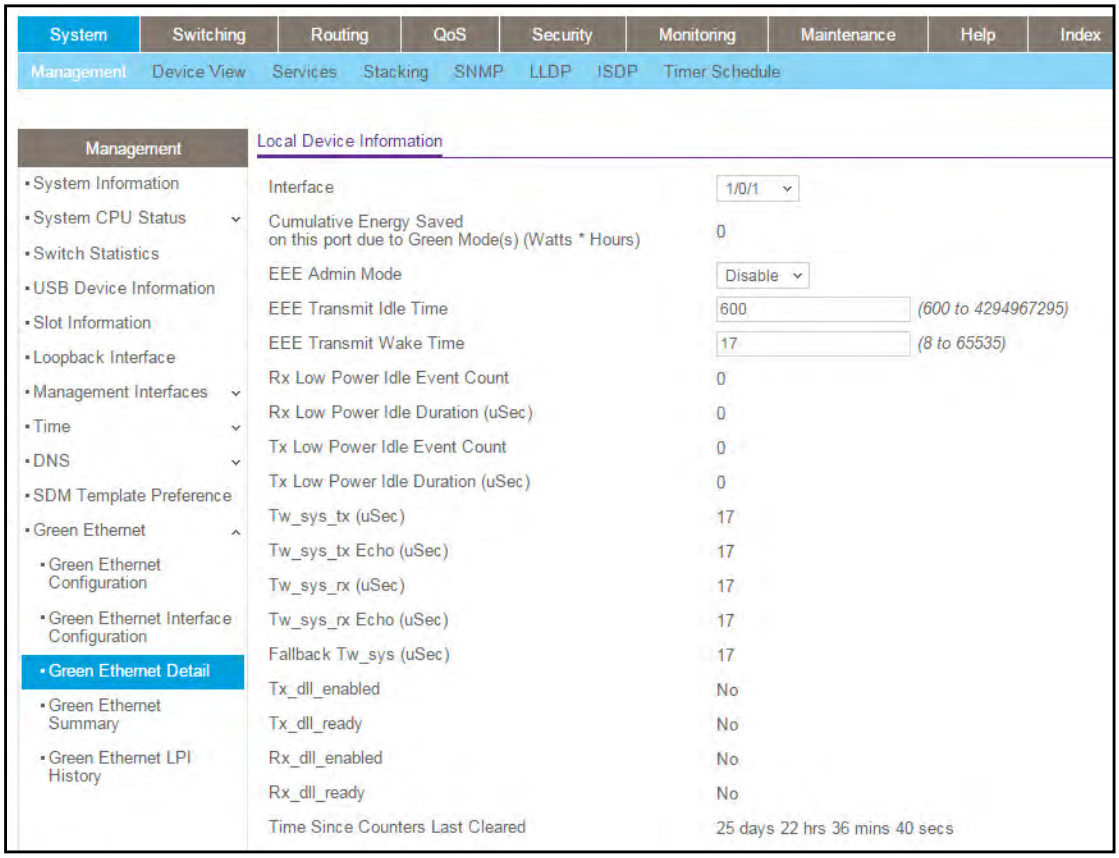
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System Management Green Ethernet Green Ethernet Details.



5. En el menú Interface, seleccione la interfaz.

6. Use la opción EEE Admin Mode para habilitar o deshabilitar el modo administrativo de Energy Efficient Ethernet en el puerto. Con el modo EEE habilitado, el puerto pasa al modo de bajo consumo cuando el enlace está inactivo. El valor predeterminado es Disabled. Si EEE Admin Mode no es compatible, se muestra N/A.

7. En el campo EEE Transmit Wake Time, introduzca el tiempo que la MAC/switch debe esperar para volver al estado activo desde el estado LPI cuando recibe un paquete para transmitir. El rango es de 8 a 65535. El valor predeterminado es 17.

8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
La siguiente tabla describe los campos no configurables.

Tabla 28. Información del dispositivo local de Green Ethernet

Campo	Descripción
Energía acumulada ahorrada en este puerto por los modos Green (vatios * horas)	Energía acumulada ahorrada por todos los modos Green habilitados en este puerto, en (vatios * horas).
Rx Low Power Idle Event Count	Este campo aumenta cada vez que la MAC RX entra en el estado de reposo de bajo consumo (LPI). Muestra el número total de eventos Rx LPI desde la última vez que se borraron los contadores EEE.
Rx Low Power Idle Duration (uSec)	Este campo indica la duración del estado Rx LPI en incrementos de 10 us. Muestra la duración total de Rx LPI desde la última vez que se borraron los contadores EEE.
Tx Low Power Idle Event Count	Este campo aumenta cada vez que la MAC TX entra en el estado LPI. Muestra el número total de eventos Tx LPI desde la última vez que se borraron los contadores EEE.
Tx Low Power Idle Duration (uSec)	Este campo indica la duración del estado Tx LPI en incrementos de 10 us. Muestra la duración total de Tx LPI desde la última vez que se borraron los contadores EEE.
Tw_sys_tx (uSec)	Entero que indica el valor de Tw_sys que el sistema local puede admitir.
Tw_sys_tx Echo (uSec)	Entero que indica el Tw_sys de transmisión del sistema remoto que usó el sistema local para calcular el Tw_sys que desea solicitar al sistema remoto.
Tw_sys_rx (uSec)	Entero que indica el valor de Tw_sys que el sistema local solicita al sistema remoto.
Tw_sys_rx Echo (uSec)	Entero que indica el Tw_sys de recepción del sistema remoto que usó el sistema local para calcular el Tw_sys que puede admitir.
Fallback Tw_sys (uSec)	Entero que indica el valor de Tw_sys de respaldo que el sistema local solicita al sistema remoto.
Tx_dll_enabled	Capa de enlace de datos habilitada: Estado de inicialización de la función de administración de la capa de enlace de datos de transmisión EEE en el sistema local.
Tx_dll_ready	Capa de enlace de datos lista: Indica que la inicialización del sistema tx ha finalizado y que está listo para actualizar/recibir LLDPDU que contengan EEE TLV.
Rx_dll_enabled	Estado de la negociación de capacidad EEE en el sistema local.

Tabla 28. Información del dispositivo local de Green Ethernet (continuación)

Campo	Descripción
Rx_dll_ready	Capa de enlace de datos lista: Indica que la inicialización del sistema rx ha finalizado y que está listo para actualizar/recibir LLDPDU que contengan EEE TLV.
Time Since Counters Last Cleared	Tiempo desde que se borraron los contadores (desde el encendido, o después de borrar los contadores EEE).

Configurar los detalles del dispositivo remoto de Green Ethernet

Para configurar la información del dispositivo remoto de Green Ethernet:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

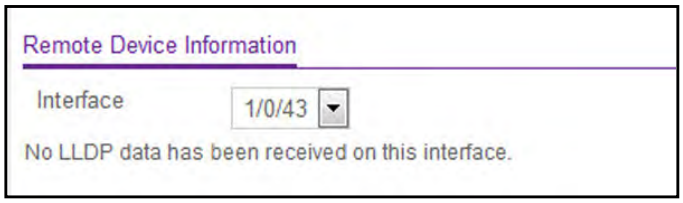
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System Management Green Ethernet Green Ethernet Details.

Se muestra la página Green Ethernet Details.
5. Desplácese hacia abajo hasta la sección Remote Device Information.



6. Seleccione la interfaz (Interface).

La siguiente tabla describe los campos no configurables.

Tabla 29. Información del dispositivo remoto de Green Ethernet

Campo	Descripción
Remote ID	El identificador de cliente remoto asignado al sistema remoto.
Remote Tw_sys_tx (uSec)	Entero que indica el valor de Tw_sys que el sistema remoto puede admitir.
Remote Tw_sys_tx Echo (uSec)	Entero que indica el valor de Tw_sys de transmisión que devuelve el sistema remoto.
Remote Tw_sys_rx (uSec)	Entero que indica el valor de Tw_sys que el sistema remoto solicita al sistema local.
Remote Tw_sys_rx Echo (uSec)	Entero que indica el valor de Tw_sys de recepción que devuelve el sistema remoto.
Remote Fallback Tw_sys (uSec)	Entero que indica el valor de Tw_sys de respaldo que anuncia el sistema remoto.

Ver el resumen de estadísticas de Green Ethernet

Para ver las estadísticas de Green Ethernet:

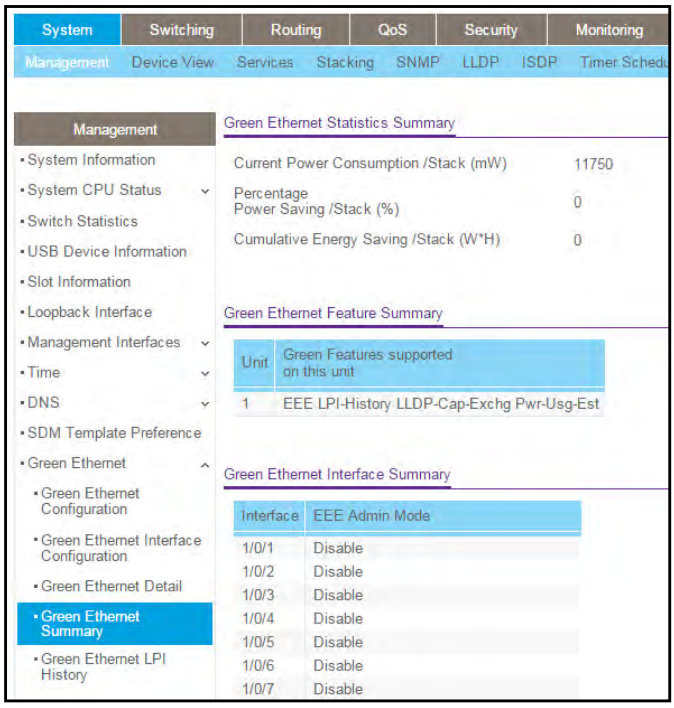
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System Management Green Ethernet Green Ethernet Summary.



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

Tabla 30. Resumen de estadísticas de Green Ethernet

Campo	Descripción
Current Power Consumption /Stack (mWatts)	Consumo de energía de todos los puertos del switch en mWatts (mW).
Percentage Power Saving /Stack (%)	Porcentaje de energía ahorrada en todos los puertos del switch con el modo Green habilitado.
Cumulative Energy Saving /Stack (Watts * Hours)	Energía acumulada ahorrada por switch en (watts * hora) con todos los modos green habilitados.

La siguiente tabla describe los campos no configurables.

Tabla 31. Resumen de funciones de Green Ethernet

Campo	Descripción
Unit	El ID de la unidad.
Green Features supported on this unit	Lista de funciones green admitidas en la unidad, que puede incluir una o varias de las siguientes: • EEE (Energy Efficient Ethernet) • LPI-History (EEE Low Power Idle History) • LLDP-Cap-Exchg (EEE LLDP Capability Exchange) • Pwr-Usg-Est (Power Usage Estimates).

Tabla 31. Resumen de funciones de Green Ethernet (continuación)

Campo	Descripción
Interface	Interfaz cuyos datos se muestran o configuran.
Energy Detect Admin mode	Habilita o deshabilita el modo Energy Detect en el puerto. Con este modo habilitado, cuando el enlace del puerto está inactivo, la PHY se desactiva automáticamente por un breve periodo y luego se reactiva para comprobar los pulsos de enlace. Esto permite al switch realizar la autonegociación y ahorrar energía cuando no hay un dispositivo enlazado.
Energy Detect Operational Status	Estado operativo actual del modo Energy Detect.
Short Reach Admin mode	Habilita o deshabilita el modo Short Reach en el puerto. Con el modo Short Reach habilitado, la PHY opera forzosamente en modo de bajo consumo sin importar la longitud del cable.
Short Reach Operational Status	Estado operativo actual del modo Short Reach.
EEE Admin mode	Habilita o deshabilita el modo Energy Efficient Ethernet en el puerto. Con el modo EEE habilitado, el puerto pasa al modo de bajo consumo cuando el enlace está inactivo.

La siguiente tabla describe los campos no configurables.

Tabla 32. Resumen de interfaces de Green Ethernet

Campo	Descripción
Interface	Interfaz cuyos datos se muestran o configuran.
EEE Admin mode	Habilita o deshabilita el modo Energy Efficient Ethernet en el puerto. Con el modo EEE habilitado, el puerto pasa al modo Low Power cuando el enlace está inactivo. Si EEE Admin Mode no es compatible, se muestra N/A.

Configurar el historial EEE LPI de Green Ethernet

Para configurar el historial EEE del modo Green del puerto:

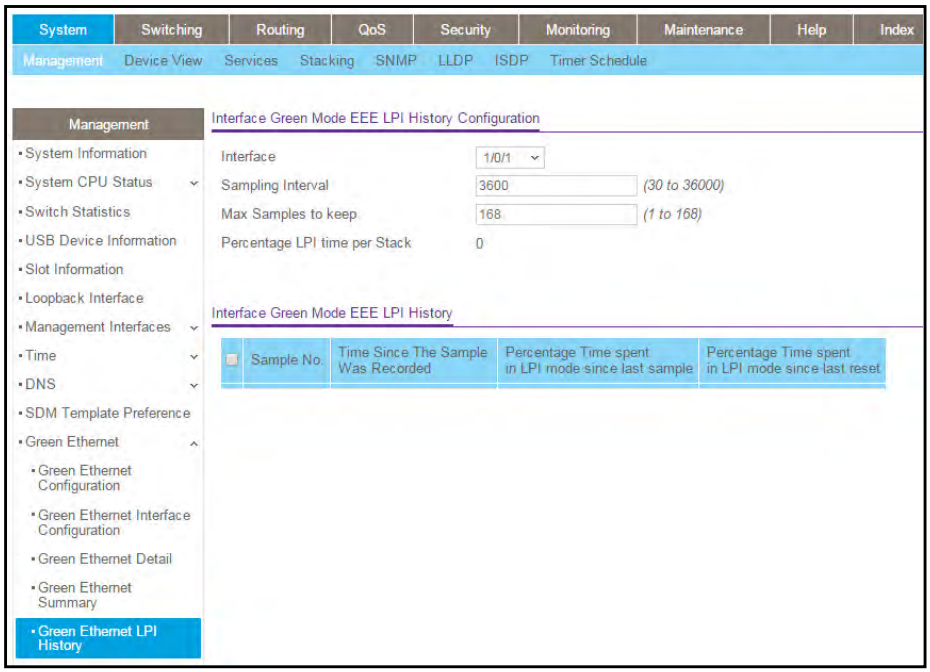
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System Management Green Ethernet Green Ethernet LPI History.



5. Seleccione la interfaz (Interface).
6. En el campo Sampling Interval, introduzca el intervalo con el que se recopilan los datos EEE LPI.

   Es un ajuste global que se aplica a todas las interfaces. El rango es de 30 a 36000. El valor predeterminado es 3600.

7. En el campo Max Samples To Keep, introduzca el número máximo de muestras que se conservarán.

   Es un ajuste global que se aplica a todas las interfaces. El rango es de 1 a 168. El valor predeterminado es 168.

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

La siguiente tabla describe los campos no configurables.

Tabla 33. Historial EEE LPI del modo Green de la interfaz

Campo	Descripción
Percentage LPI time per switch	Tiempo en modo LPI por switch desde la última vez que se borraron los contadores EEE.
Sample No.	Índice de la muestra.
Time Since The Sample Was Recorded	Cada vez que se actualiza la página, muestra un tiempo distinto, ya que refleja la diferencia entre la hora actual y la hora en que se registró la muestra.

Tabla 33. Historial EEE LPI del modo Green de la interfaz

Campo	Descripción
Percentage Time spent in LPI mode since last sample	Porcentaje de tiempo en modo LPI durante el intervalo de medición actual.
Percentage Time spent in LPI mode since last reset	Porcentaje de tiempo en modo LPI desde que se restablecieron las estadísticas EEE LPI.

Configurar y mostrar los ajustes de Bonjour

Un dispositivo Mac OS compatible con Bonjour puede detectar el switch en la red para que pueda encontrar la dirección IP del switch e iniciar sesión en su interfaz web local. Bonjour está habilitado de forma predeterminada. Puede deshabilitarlo 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, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Bonjour > Bonjour Configuration.

   Se muestra la página Bonjour Global Configuration.

5. Seleccione uno de los siguientes botones de opción:
   - Enable. Bonjour está habilitado. Este es el valor predeterminado.
   - Disable. Bonjour está deshabilitado.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Mostrar la información de Bonjour

Para mostrar la información de Bonjour:

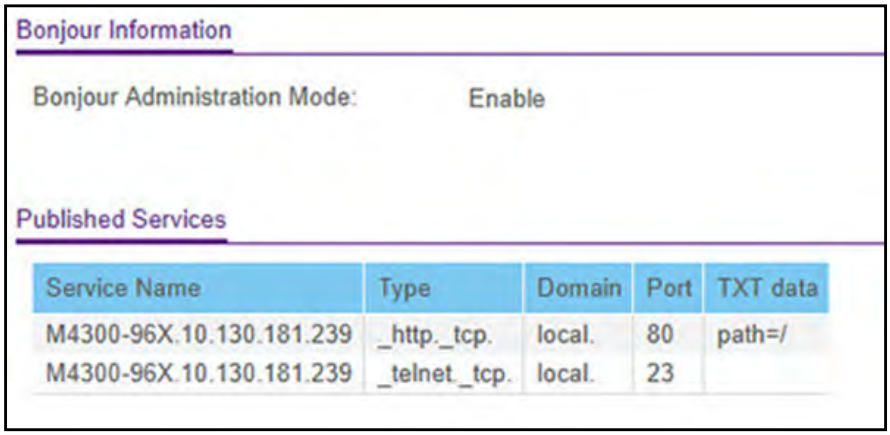
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Management > Bonjour > Bonjour Details.



El campo Bonjour Administration Mode indica si Bonjour está habilitado o deshabilitado.
5. Para actualizar la página, haga clic en el botón Actualizar (Refresh).
La siguiente tabla describe los campos no configurables que se muestran.

Tabla 34. Servicios publicados de Bonjour

Campo	Descripción
Service Name	Los nombres de servicio Bonjour del switch.
Type	Los nombres de tipo de servicio 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.

Configurar el servidor DHCP

Puede configurar el servidor DHCP, los pools DHCP, los enlaces DHCP y el relay DHCP. También puede ver las estadísticas y conflictos de DHCP.

Configurar el servidor DHCP

Para configurar un servidor DHCP:

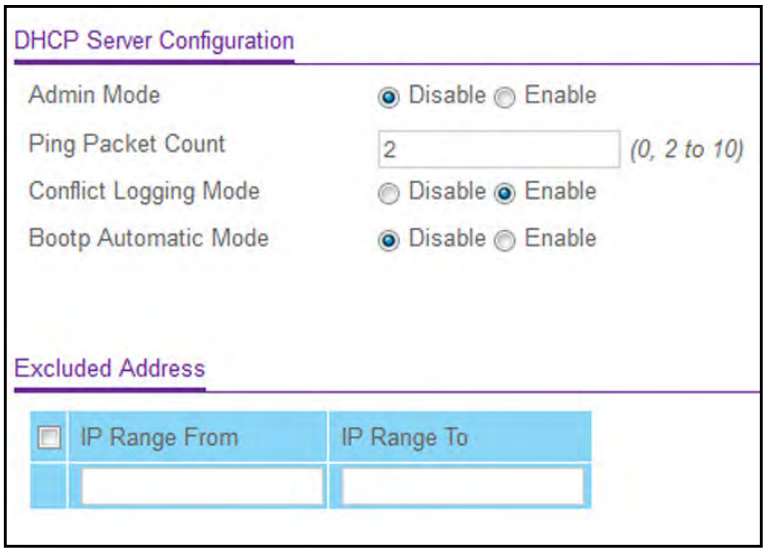
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP Server > DHCP Server Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Indica si el servicio DHCP está habilitado o deshabilitado. El valor predeterminado es Disable.

6. Use Ping Packet Count para especificar el número de paquetes que un servidor envía a una dirección del pool para comprobar si está duplicada como parte de una operación ping.

   El valor predeterminado es 2. El rango válido es 0, 2 a 10. El valor 0 deshabilita la función.

7. Seleccione el botón de opción Conflict Logging mode Disable o Enable.

Indica si se habilita o deshabilita el registro de conflictos en un servidor DHCP. El valor predeterminado es Enable.

8. Seleccione el botón de opción BootP Automatic mode Disable o Enable.

Indica si se habilita o deshabilita BootP para pools dinámicos. El valor predeterminado es Disable.

9. 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 desee excluir.

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 dirección IP especificada en el campo IP Range From, o déjelo en 0.0.0.0.

10. Haga clic en el botón Add.
Las direcciones excluidas se agregan al switch
11. Haga clic en el botón Apply.
La configuración se guarda.

Configurar el pool DHCP

Para configurar el pool DHCP:

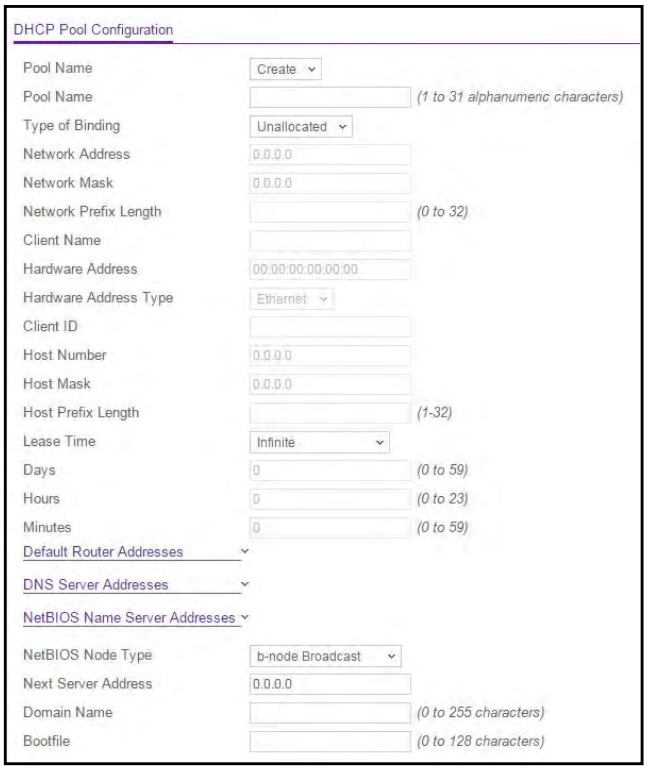
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

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



5. Haga clic en el botón Add.
Se agrega la configuración del pool.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe los campos de DHCP Pool Configuration.

Tabla 35. DHCP Pool Configuration

Campo	Descripción
Pool Name*	Para un usuario con permiso de lectura/escritura, este campo muestra los nombres de todos los pools existentes junto con la opción adicional Create. Cuando el usuario selecciona Create, aparece otro cuadro de texto, Pool Name, donde el usuario puede introducir un nombre para el pool que se creará. Para un usuario con permiso de solo lectura, este campo muestra solo los nombres de los pools existentes.
Pool Name	El nombre del pool que se creará. Este campo aparece cuando el usuario con permiso de lectura/escritura selecciona Create en la lista Pool Name*. El Pool Name puede tener hasta 31 caracteres.
Type of Binding	El tipo de enlace del pool: • Unallocated • Dynamic • Manual
Network Address	La dirección de subred para una dirección DHCP de un pool dinámico.

Tabla 35. DHCP Pool Configuration (continuación)

Campo	Descripción
Network Mask	El número de subred para una dirección DHCP de un pool dinámico. Se puede configurar Network Mask o Prefix Length para especificar la máscara de subred, pero no ambos.
Network Prefix Length	El número de subred para una dirección DHCP de un pool dinámico. Se puede configurar Network Mask o Prefix Length para especificar la máscara de subred, pero no ambos. El rango válido es de 0 a 32.
Client Name	El nombre de cliente del pool DHCP manual.
Hardware Address	La dirección MAC de la plataforma de hardware del cliente DHCP.
Hardware Address Type	El protocolo de la plataforma de hardware del cliente DHCP. Los tipos válidos son Ethernet e ieee802. El valor predeterminado es Ethernet.
Client ID	El identificador de cliente del pool DHCP manual.
Host Number	La dirección IP de un enlace manual con un cliente DHCP. El host solo se puede establecer si se especifica Client Identifier o Hardware Address. Al eliminar Host se eliminan el nombre de cliente, el ID de cliente y la dirección de hardware del pool manual, y el tipo de pool cambia a Unallocated.
Host Mask	La máscara de subred de un enlace manual con un cliente DHCP. Se puede configurar Host Mask o Prefix Length para especificar la máscara de subred, pero no ambos.
Host Prefix Length	La máscara de subred de un enlace manual con un cliente DHCP. Se puede configurar Host Mask o Prefix Length para especificar la máscara de subred, pero no ambos. El rango válido es de 0 a 32.
Lease Time	Se puede seleccionar Infinite para especificar una concesión infinita, o Specified Duration para introducir un periodo de concesión específico. En un enlace dinámico, infinito implica una concesión de 60 días; en un enlace manual, infinito implica una concesión indefinida. El valor predeterminado es Specified Duration.
Days	El número de días del periodo de concesión. Este campo solo aparece si el usuario especificó Specified Duration como Lease time. El valor predeterminado es 1. El rango válido es de 0 a 59.
Hours	El número de horas del periodo de concesión. Este campo solo aparece si el usuario especificó Specified Duration como Lease time. El rango válido es de 0 a 22.
Minutes	El número de minutos del periodo de concesión. Este campo solo aparece si especificó Specified Duration como tiempo de concesión. El rango válido es de 0 a 86399.
Default Router Addresses	La lista de direcciones de router predeterminado del pool. Haga clic en la flecha junto al nombre del campo para expandir la página y mostrar una tabla donde puede especificar hasta ocho direcciones de router predeterminado en orden de preferencia.

Tabla 35. DHCP Pool Configuration (continuación)

Campo	Descripción
DNS Server Addresses	La lista de direcciones de servidores DNS del pool. Haga clic en la flecha junto al nombre del campo para expandir la página y mostrar una tabla donde puede especificar hasta ocho direcciones de servidores DNS en orden de preferencia.
NetBIOS Name Server Addresses	La lista de direcciones de servidores de nombres NetBIOS del pool. Haga clic en la flecha junto al nombre del campo para expandir la página y mostrar una tabla donde puede especificar hasta ocho direcciones de servidores de nombres NetBIOS en orden de preferencia.
NetBIOS Node Type	El tipo de nodo NetBIOS para los clientes DHCP: • b-node Broadcast • p-node Peer-to-Peer • m-node Mixed • h-node Hybrid
Next Server Address	La dirección Next Server del pool.
Domain Name	El nombre de dominio de un cliente DHCP. Domain Name puede tener hasta 255 caracteres.
Bootfile	El nombre de la imagen de arranque predeterminada de un cliente DHCP. File Name puede tener hasta 128 caracteres.

Configurar las opciones del pool DHCP

Para configurar las opciones del pool DHCP:

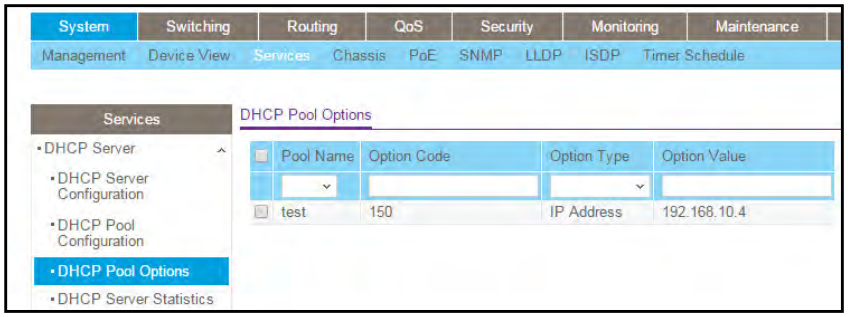
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP Server> DHCP Pool Options.



5. En la lista Pool Name, seleccione el nombre del pool.
6. Option Code especifica el código de opción configurado para el pool seleccionado.

7. Use Option Type para especificar el tipo de opción del Option Code configurado para el pool seleccionado:
   - ASCII
   - Hex
   - IP Address

8. Option Value especifica el valor del Option Code configurado para el pool seleccionado.
9. Haga clic en el botón Add.

Se agrega el Option Code al pool seleccionado.

Ver las estadísticas del servidor DHCP

Para ver las estadísticas del servidor DHCP:

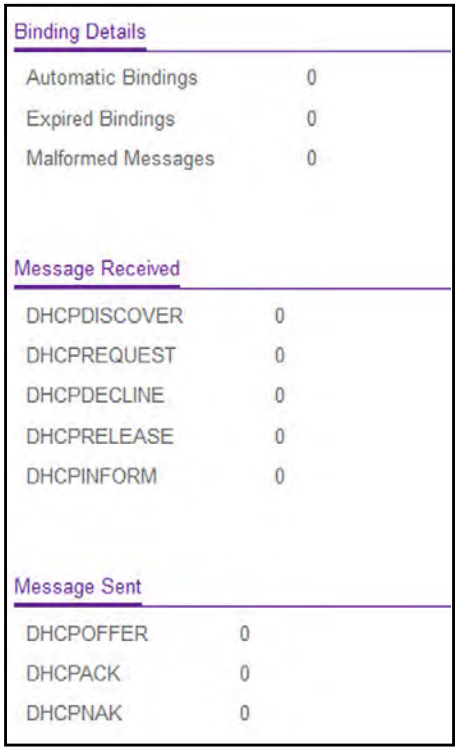
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP Server > DHCP Server Statistics.



La siguiente tabla describe los campos de DHCP Server Statistics.

Tabla 36. DHCP Server Statistics

Campo	Descripción
Automatic Bindings	El número de enlaces automáticos en el servidor DHCP.
Expired Bindings	El número de enlaces vencidos en el servidor DHCP.
Malformed Messages	El número de mensajes con formato incorrecto.
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.
DHCPOFFER	El número de mensajes DHCPOFFER enviados por el servidor DHCP.

Tabla 36. DHCP Server Statistics (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.

Ver la información de enlaces DHCP

Para ver los enlaces DHCP:

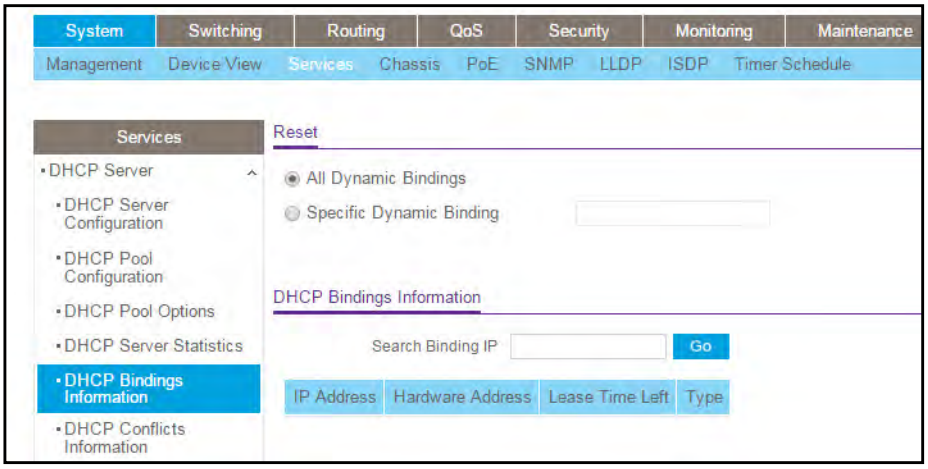
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP Server > DHCP Bindings Information.



5. Para mostrar la información de enlaces DHCP, seleccione uno de los siguientes botones de opción:

- All Dynamic Bindings. Especifica que se eliminen todos los enlaces dinámicos.
- Specific Dynamic Binding. Especifica un enlace dinámico concreto que se eliminará.

La siguiente tabla describe los campos de DHCP Bindings Information.

Tabla 37. DHCP Bindings Information

Campo	Descripción
IP Address	La dirección IP del cliente.
Hardware Address	La dirección de hardware del cliente.
Lease Time Left	El tiempo de concesión restante en días, horas y minutos, formato dd:hh:mm.
Type	El tipo de enlace: Dynamic o Manual.

Ver los conflictos de DHCP

Puede ver información sobre hosts con conflictos de direcciones, por ejemplo, cuando la misma dirección IP se asigna a dos o más dispositivos de la red.

Para ver los conflictos de DHCP:

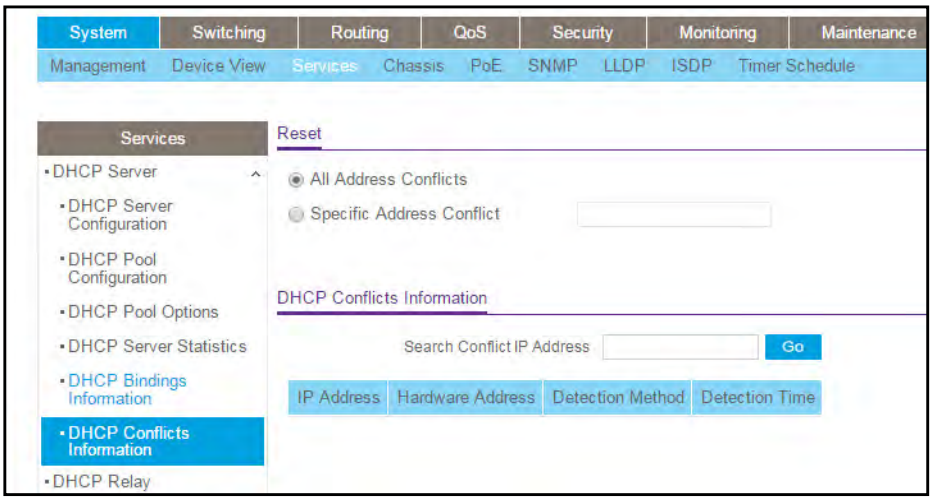
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP Server > DHCP Conflicts Information.



5. Para mostrar la información de conflictos de DHCP, seleccione uno de los siguientes botones de opción:

- All Address Conflicts. Especifica que se eliminen todos los conflictos de direcciones.
- Specific Address Conflict. Especifica un enlace dinámico concreto que se eliminará.

La siguiente tabla describe los campos de DHCP Conflicts Information.

Tabla 38. DHCP Conflicts Information

Campo	Descripción
IP Address	La dirección IP del host registrada en el servidor DHCP.
Hardware Address	La dirección de hardware del cliente.
Detection Method	La forma en que se detectaron las direcciones IP de los hosts en el servidor DHCP.
Detection Time	El momento en que se detectó el conflicto, en formato N days NNh:NNm:NNs respecto del tiempo de actividad del sistema.

Configurar el relay DHCP

Para configurar el relay DHCP:

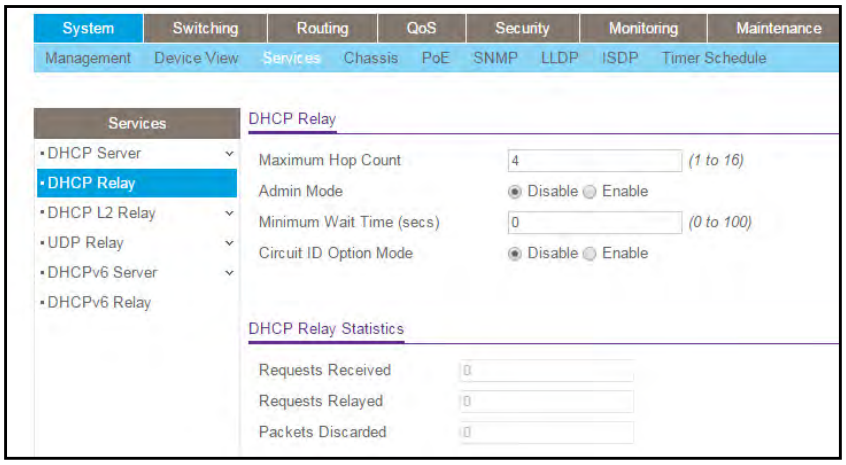
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP Relay.



5. Use Maximum Hop Count para introducir el número máximo de saltos que puede dar una solicitud de cliente antes de descartarse.

El rango es (1 a 16). El valor predeterminado es 4.
6. Seleccione el botón de opción Admin mode Disable o Enable.

Si selecciona Enable, las solicitudes DHCP se reenvían a la dirección IP introducida en el campo Server Address.

7. Use Minimum Wait Time para introducir un tiempo mínimo de espera en segundos.

Este valor se compara con la marca de tiempo de los paquetes de solicitud 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 (0 a 100).

8. Seleccione el botón de opción Circuit ID Option mode Disable o Enable.

Si selecciona Enable, las opciones de Relay Agent se agregan a las solicitudes antes de reenviarlas al servidor y se quitan de las respuestas antes de reenviarlas a los clientes.

9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe los campos de DHCP Relay Statistics.

Tabla 39. DHCP Relay Status

Campo	Descripción
Requests Received	El número total de solicitudes DHCP recibidas de todos los clientes desde el último restablecimiento del switch.
Requests Relayed	El número total de solicitudes DHCP reenviadas al servidor desde el último restablecimiento del switch.
Packets Discarded	El número total de paquetes DHCP descartados por este Relay Agent desde el último restablecimiento del switch.

Administrar un DHCP L2 Relay

Configurar los ajustes globales de DHCP L2 Relay

Para configurar los ajustes globales de DHCP L2 Relay:

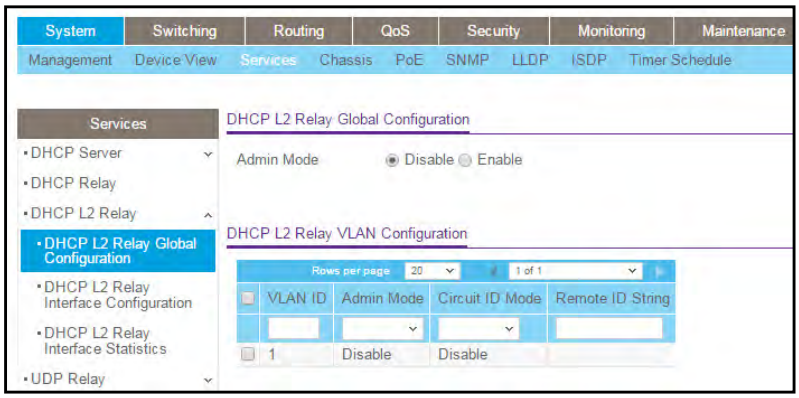
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration.



5. Seleccione el botón de opción Admin mode Disable o Enable.

En la configuración global, habilita o deshabilita DHCP L2 Relay en el switch. El valor predeterminado es Disable.

6. Para la configuración de VLAN, VLAN ID muestra el VLAN ID configurado en el switch.

a. Use Admin mode para habilitar o deshabilitar DHCP L2 Relay en la VLAN seleccionada.

b. Use Circuit ID mode para habilitar o deshabilitar la subopción Circuit ID de DHCP Option-82.

c. Use Remote ID String para especificar el Remote ID cuando Remote ID mode está habilitado.
7. Haga clic en el botón Apply.
La configuración se guarda.
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 podría 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.

Configurar una interfaz DHCP L2 Relay

Para configurar DHCP L2 Relay:

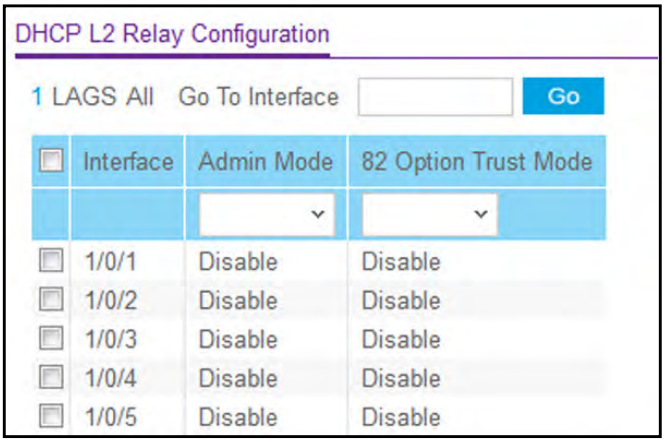
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration.



5. Use Admin mode para habilitar o deshabilitar DHCP L2 Relay en la interfaz seleccionada. El valor predeterminado es Disable.

6. Use 82 Option Trust mode para habilitar o deshabilitar que una interfaz sea de confianza para la información de DHCP L2 Relay (Option-82) recibida.

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

Ver las estadísticas de interfaces DHCP L2 Relay

Para ver las estadísticas de interfaces DHCP L2 Relay:

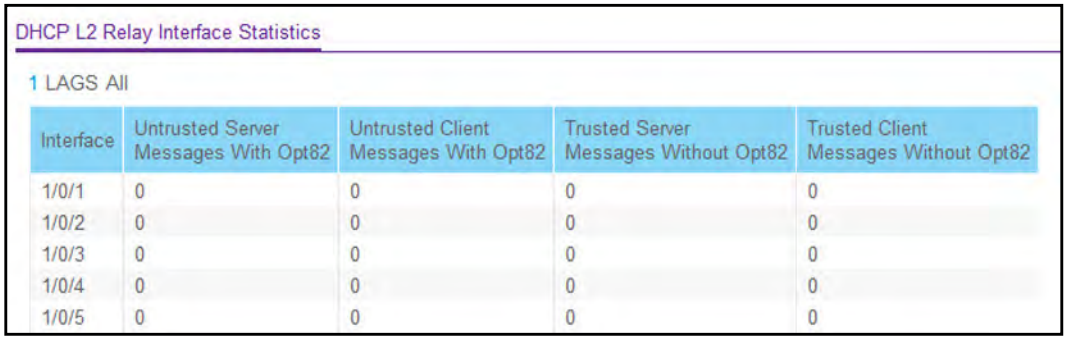
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics.



La siguiente tabla describe los campos de DHCP L2 Relay Interface Statistics.

Tabla 40. DHCP L2 Relay Interface Statistics

Campo	Descripción
Interface	Muestra la interfaz por la que se recibe el mensaje DHCP.
UntrustedServerMsgsWithOpt82	Muestra el número de mensajes DHCP con option82 recibidos de un servidor que no es de confianza.
UntrustedClientMsgsWithOpt82	Muestra el número de mensajes DHCP con option82 recibidos de un cliente que no es de confianza.
TrustedServerMsgsWithoutOpt82	Muestra el número de mensajes DHCP sin option82 recibidos de un servidor de confianza.
TrustedClientMsgsWithoutOpt82	Muestra el número de mensajes DHCP sin option82 recibidos de un cliente de confianza.

Configurar los ajustes globales de UDP Relay

Para configurar los ajustes globales de UDP Relay:

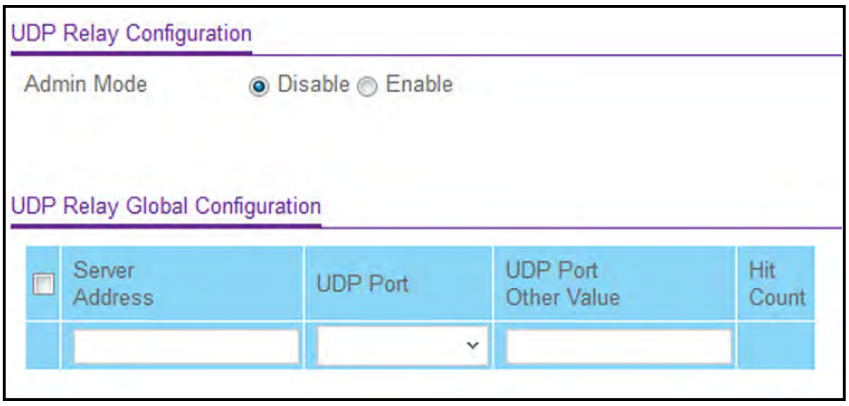
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > UDP Relay > UDP Relay Global Configuration.



5. Seleccione el botón de opción Admin mode Disable o Enable.
Habilita o deshabilita UDP Relay en el switch. El valor predeterminado es Disable.
6. Use Server Address para especificar la dirección del servidor UDP Relay en formato x.x.x.x.
7. Use UDP Port para especificar el puerto UDP de destino.
Se admiten estos puertos:

- DefaultSet. Retransmite paquetes del puerto UDP 0. Se usa si no se selecciona un puerto UDP al crear el servidor de retransmisión.
- 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 Information 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)
- Other. Si se selecciona esta opción, se habilita UDP Port Other Value. Esta opción le permite introducir su propio puerto UDP en UDP Port Other Value.

8. Use UDP Port Other Value para especificar un puerto UDP de destino entre 0 y 65535.
9. Haga clic en el botón Add.
Se crea una entrada con la configuración especificada en la tabla UDP Relay.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

El campo Hit Count muestra el número de paquetes UDP detectados en el puerto UDP.

Configurar UDP Relay en interfaces

Para configurar UDP Relay en interfaces:

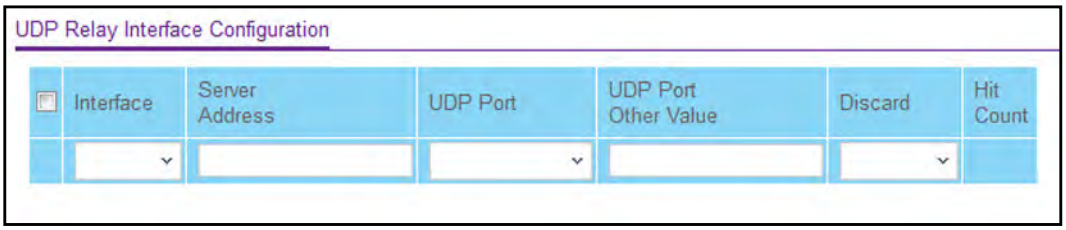
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Services > UDP Relay > UDP Relay Interface Configuration.



5. Use Interface para seleccionar la interfaz en la que se habilitará UDP Relay.
6. Use Server Address para especificar la dirección del servidor UDP Relay en formato x.x.x.x.
7. Use UDP Port para especificar el puerto UDP de destino.
Se admiten los siguientes puertos:

- DefaultSet. Retransmite paquetes del puerto UDP 0. Se usa si no se selecciona un puerto UDP al crear un servidor de retransmisión.
- 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 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)
- Other. Si se selecciona esta opción, se habilita UDP Port Other Value. Esta opción permite al usuario introducir su propio puerto UDP en UDP Port Other Value.

8. Use UDP Port Other Value para especificar un puerto UDP de destino entre 0 y 65535.
9. Use Discard para habilitar o deshabilitar el descarte de los paquetes coincidentes.

   Enable solo puede elegirse cuando el usuario introduce la dirección IP 0.0.0.0. El modo Discard puede ponerse en Disable cuando el usuario agrega una entrada nueva con una dirección IP distinta de cero.

10. Haga clic en el botón Add.

Se crea una entrada con la configuración especificada en la tabla UDP Relay.

11. Haga clic en el botón Apply.

La configuración se guarda.

El campo Hit Count muestra el número de paquetes UDP detectados en el puerto UDP.

Administrar el servidor DHCPv6

Habilitar o deshabilitar el servidor DHCPv6

Puede configurar el servidor Dynamic Host Configuration Protocol for IPv6 (DHCPv6) en el dispositivo. El dispositivo puede actuar como servidor DHCPv6 o agente de retransmisión DHCPv6 para ayudar a asignar la configuración de red a los clientes IPv6.

Para habilitar o deshabilitar el servicio DHCP:

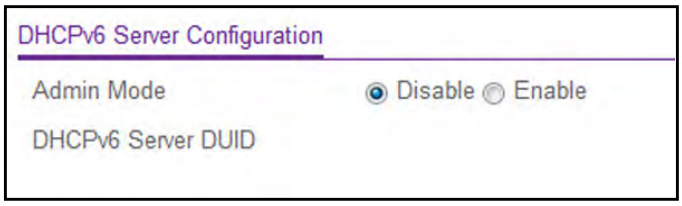
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Server > DHCPv6 Server Configuration.



5. Seleccione el botón de opción Admin mode Disable o Enable.

   Esto especifica si el modo administrativo del servicio DHCPv6 está habilitado o deshabilitado. El valor predeterminado es Disable.

6. Use el campo DHCPv6 Server DUID para especificar el DHCP Unique Identifier (DUID) del servidor DHCPv6.

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

Configurar el pool DHCPv6

Puede ver los pools del servidor DHCPv6 configurados actualmente, así como agregar y eliminar pools. Un pool del servidor DHCPv6 es un conjunto de información de configuración de red disponible para los clientes DHCPv6 que la solicitan.

Para configurar el pool DHCPv6:

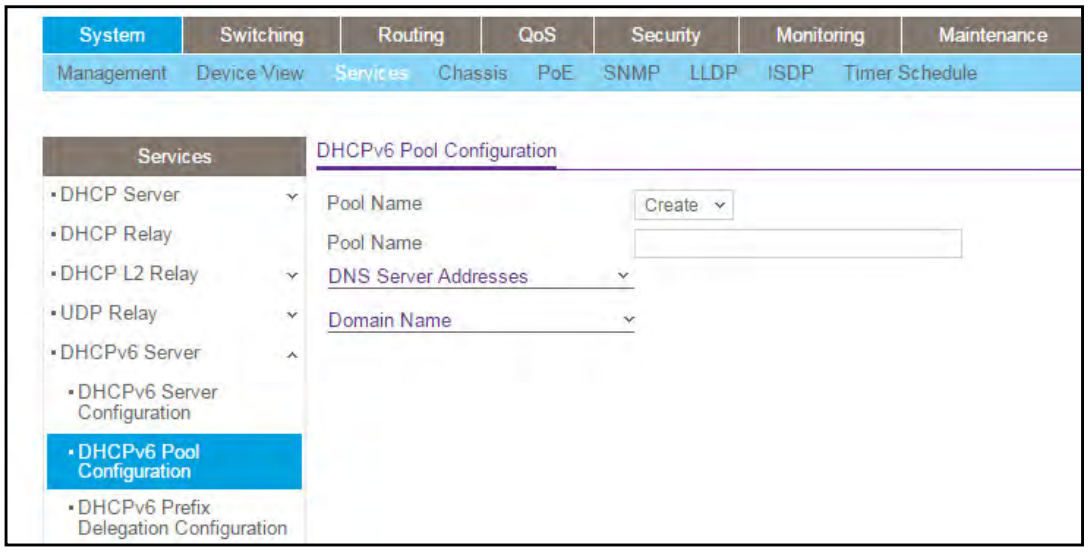
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Server > DHCPv6 Pool Configuration.



El campo Pool Name muestra los nombres de todos los pools existentes y la opción Create.

5. Para crear un pool, seleccione Create e introduzca un nombre único que identifique el pool del servidor DHCPv6 que se creará.

El nombre puede tener hasta 31 caracteres alfanuméricos.

6. Use el campo Default Router Addresses para especificar la lista de direcciones de router predeterminado del pool.

Puede especificar hasta ocho direcciones de router predeterminado en orden de preferencia.
7. Use el campo Domain Name para especificar el nombre de dominio de un cliente DHCPv6 del pool. El nombre de dominio puede tener hasta 255 caracteres alfanuméricos.
Para eliminar el pool seleccionado del switch, haga clic en el botón Delete.
8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.

Configurar la delegación de prefijos DHCPv6

Para configurar la delegación de prefijos DHCPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration.



5. Seleccione en la lista de nombres de pool configurados.
6. En los campos Prefix y Prefix Length, especifique el prefijo IPv6 delegado.
7. En el campo DUID, especifique el identificador DUID que identifica el valor DUID único del cliente.
8. Especifique Client Name, que solo es útil para registro o rastreo. El nombre puede tener hasta 31 caracteres alfanuméricos.
9. Especifique Valid Lifetime en segundos para el prefijo delegado.
Los valores válidos son de 0 a 4294967295.
10. Especifique Prefer Lifetime en segundos para el prefijo delegado.
Los valores válidos son de 0 a 4294967295.
11. Haga clic en el botón Add.
Se agrega el prefijo delegado al pool seleccionado.
12. Haga clic en el botón Apply.
La configuración se guarda.

Configurar DHCPv6 en interfaces

Puede configurar DHCPv6 por interfaz. Los modos de interfaz DHCPv6 son mutuamente excluyentes. Los campos que puede configurar en esta página dependen del modo seleccionado para la interfaz.

Para configurar DHCPv6 en interfaces:

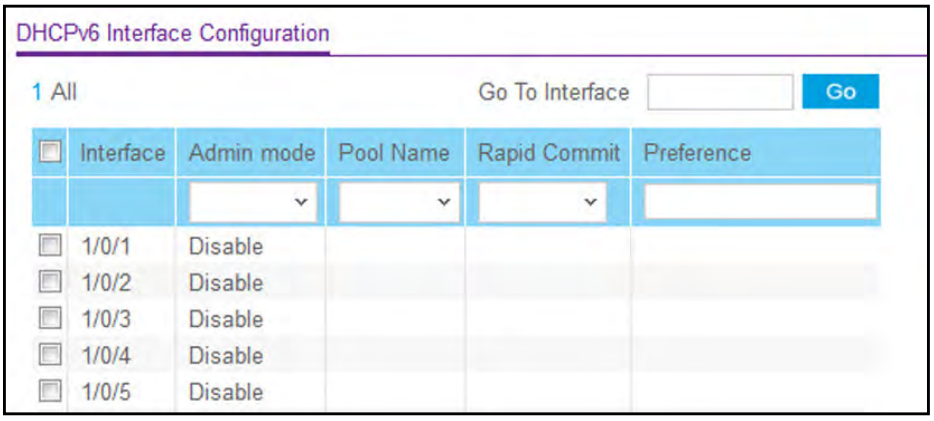
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Server > DHCPv6 Interface Configuration.



5. Seleccione la interfaz cuya información desea ver o configurar. Puede:

   a. En el campo Go To Interface, introducir la interfaz en formato unidad/ranura/puerto y hacer clic en el botón Go. Se selecciona la entrada correspondiente a la interfaz especificada.

   b. Seleccionar la casilla en la lista de interfaces configuradas con la función de servidor DHCPv6.

6. En la lista Admin mode, seleccione Enable o Disable para el modo DHCPv6 y configurar la función de servidor.

   Las funciones de servidor DHCPv6 y de retransmisión DHCPv6 son mutuamente excluyentes.

7. En el campo Pool Name, especifique el pool DHCPv6 que contiene los parámetros sin estado o de delegación de prefijos.

8. Rapid Commit es un parámetro opcional. En la lista Rapid Commit, seleccione Enable o Disable para permitir un intercambio abreviado entre el cliente y el servidor.

9. En el campo Preference, especifique el valor de preferencia que usan los clientes para elegir entre servidores DHCPv6.

   Los valores válidos son de 0 a 4294967295. El valor predeterminado es 0.

10. Haga clic en el botón Aplicar (Apply).
    La configuración se guarda.

Ver la información de enlaces DHCPv6

Puede ver las entradas de la tabla DHCP Bindings. Cuando un cliente obtiene la configuración IPv6 del servidor DHCPv6, el servidor agrega una entrada a su base de datos. La entrada se llama enlace.

Para ver la información de enlaces DHCPv6:

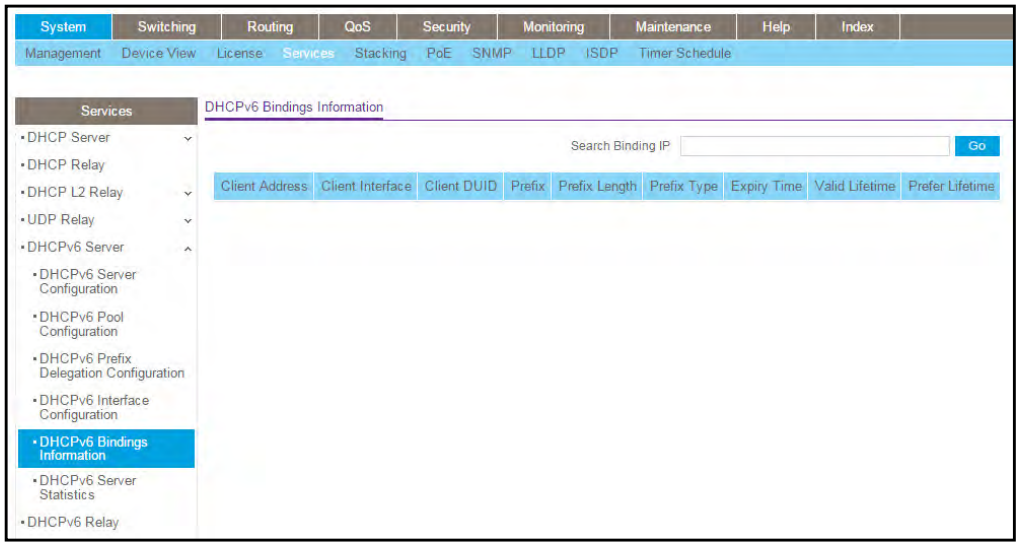
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Server > DHCPv6 Bindings Information.



5. Para actualizar la página, haga clic en el botón Actualizar (Refresh).
La siguiente tabla describe los campos no configurables que se muestran.

Tabla 41. Información de enlaces DHCPv6

Campo	Descripción
Client Address	Dirección IPv6 del cliente asociada al enlace.
Client Interface	Número de interfaz donde se produjo el enlace del cliente.
Client DUID	DHCPv6 Unique Identifier (DUID) del cliente. El DUID es una combinación de la dirección de hardware y el identificador del cliente.
Prefix	Dirección IPv6 del prefijo delegado asociado a este enlace.
Prefix Length	Longitud de máscara IPv6 del prefijo delegado asociado a este enlace.
Prefix Type	Tipo de prefijo IPv6 asociado a este enlace.
Expiry Time	Número de segundos que faltan para que venza el prefijo asociado a un enlace.

Tabla 41. Información de enlaces DHCPv6 (continuación)

Campo	Descripción
Valid Lifetime	Tiempo máximo en segundos que el cliente puede usar el prefijo.
Prefer Lifetime	Tiempo preferido en segundos que el cliente puede usar el prefijo.

Ver las estadísticas del servidor DHCPv6

Puede ver las estadísticas del servidor DHCPv6 del dispositivo, incluida la información de los mensajes DHCPv6 enviados, recibidos y descartados globalmente y en cada interfaz. Los valores de la página indican los contadores acumulados desde la última vez que se borraron.

Para ver las estadísticas del servidor DHCPv6:

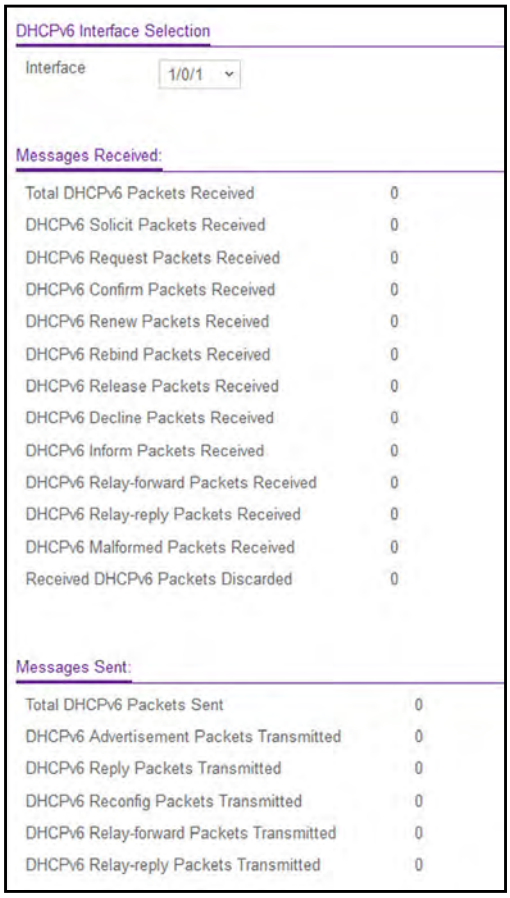
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Server > DHCPv6 Server Statistics.



5. Para ver estadísticas DHCPv6 detalladas de una interfaz, seleccione en la lista Interface la entrada cuyos datos desea mostrar.

   Si selecciona All, se muestran los datos de todas las interfaces.

6. Para restablecer los contadores DHCPv6 de una o más interfaces, seleccione cada interfaz cuyas estadísticas desea restablecer y haga clic en el botón Clear.

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

La siguiente tabla describe los campos no configurables que se muestran.

Tabla 42. Estadísticas del servidor DHCPv6

Campo	Descripción
Messages Received	Suma de todas las estadísticas de interfaz de mensajes recibidos.
Total DHCPv6 Packets Received	Número de mensajes DHCPv6 recibidos en la interfaz. 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.
DHCPv6 Solicit Packets Received	Número de mensajes DHCPv6 Solicit recibidos en la interfaz. Un cliente envía este tipo de mensaje para localizar servidores DHCPv6.

Tabla 42. Estadísticas del servidor DHCPv6 (continuación)

Campo	Descripción
DHCPv6 Request Packets Received	Número de solicitudes.
DHCPv6 Confirm Packets Received	Número de mensajes DHCPv6 Confirm recibidos en la interfaz. Un cliente envía este tipo de mensaje a todos los servidores DHCPv6 para determinar si su configuración es válida para el enlace conectado.
DHCPv6 Renew Packets Received	Número de mensajes DHCPv6 Renew recibidos en la interfaz. Un cliente envía este tipo de mensaje para extender y actualizar la configuración proporcionada por el servidor DHCPv6.
DHCPv6 Rebind Packets Received	Número de mensajes DHCPv6 Rebind recibidos en la interfaz. Un cliente envía este tipo de mensaje a cualquier servidor DHCPv6 cuando no recibe respuesta a un mensaje Renew.
DHCPv6 Release Packets Received	Número de mensajes DHCPv6 Release recibidos en la interfaz. Un cliente envía este tipo de mensaje para indicar que ya no necesita la dirección asignada.
DHCPv6 Decline Packets Received	Número de mensajes DHCPv6 Decline recibidos en la interfaz. Un cliente envía este tipo de mensaje al servidor DHCPv6 para indicar que una dirección asignada ya está en uso en el enlace.
DHCPv6 Inform Packets Received	Número de mensajes DHCP v6 information-request recibidos en la interfaz. Un cliente envía este tipo de mensaje para solicitar información de configuración distinta de la asignación de dirección IP.
DHCPv6 Relay-forward Packets Received	Número de mensajes DHCPv6 relay-forward recibidos en la interfaz. Un agente de retransmisión envía este tipo de mensaje para reenviar mensajes a los servidores.
DHCPv6 Relay-reply Packets Received	Número de mensajes DHCP v6 relay-reply recibidos en la interfaz. Un servidor envía este tipo de mensaje a un agente de retransmisión DHCP v6 y contiene el mensaje que el agente debe entregar al cliente.
DHCPv6 Malformed Packets Received	Número de mensajes DHCPv6 recibidos en la interfaz que se descartaron por estar mal formados.
Received DHCPv6 Packets Discarded	Número de paquetes descartados.
Messages Sent	Suma de todas las estadísticas de interfaz de mensajes enviados.
Total DHCPv6 Packets Sent	Número de mensajes DHCPv6 enviados por la interfaz. Los mensajes DHCPv6 enviados de un servidor DHCPv6 a un cliente DHCPv6 incluyen Advertise, Reply, Reconfigure y Relay-Reply.
DHCPv6 Advertisement Packets Transmitted	Número de mensajes DHCPv6 Advertise enviados por la interfaz. Un servidor envía este tipo de mensaje a un cliente DHCPv6 en respuesta a un mensaje Solicit e indica que está disponible para dar servicio.
DHCPv6 Reply Packets Transmitted	Número de mensajes DHCPv6 Reply enviados desde la interfaz a un cliente DHCPv6 en respuesta a un mensaje solicit, request, renew, rebind, information-request, confirm, release o decline.

Tabla 42. Estadísticas del servidor DHCPv6 (continuación)

Campo	Descripción
DHCPv6 Reconfig Packets Transmitted	Número de mensajes DHCPv6 reconfigure enviados por la interfaz. Un servidor envía este tipo de mensaje a un cliente DHCPv6 para informarle que 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.
DHCPv6 Relay-forward Packets Transmitted	Número de mensajes DHCPv6 Relay-Forward enviados por la interfaz. Un agente de retransmisión envía este tipo de mensaje para reenviar mensajes a los servidores.
DHCPv6 Relay-reply Packets Transmitted	Número de mensajes DHCPv6 Relay-Reply enviados por la interfaz. Un servidor envía este tipo de mensaje a un agente de retransmisión DHCPv6 y contiene el mensaje que el agente debe entregar al cliente.

Configurar DHCPv6 Relay en una interfaz

Para configurar DHCPv6 Relay en una interfaz:

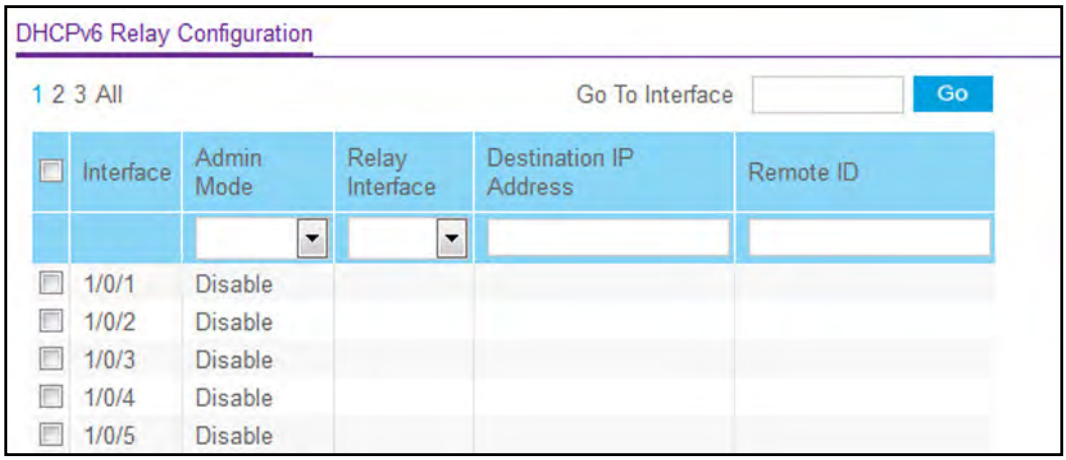
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > DHCPv6 Relay.



5. Seleccione la interfaz cuya información desea ver o configurar.

Realice una de las siguientes acciones:

- En el campo Go To Interface, introduzca la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go. Se selecciona la entrada correspondiente a la interfaz especificada.
- Seleccione la casilla en la lista de interfaces configuradas con la función DHCPv6 Relay.

6. En el campo Admin mode, especifique el modo DHCPv6, Enable o Disable, para configurar la función DHCPv6 Relay.

El valor predeterminado es Disable. Las funciones de servidor DHCPv6 y de retransmisión DHCPv6 son mutuamente excluyentes.

7. En la lista Relay Interface, seleccione una interfaz para llegar a un servidor de retransmisión.
8. En Destination IP Address, especifique una dirección IPv6 para llegar a un servidor de retransmisión.
9. 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 puede especificarse como una cadena definida por el usuario.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar Power over Ethernet

Nota: Power over Ethernet (PoE) es compatible con los modelos M4300-16X, M4300-28G-POE+, M4300-52G-POE+ y M4300-96X. Este último modelo requiere una o más tarjetas de puertos APM408.

Configurar los ajustes básicos de PoE

Para configurar los ajustes básicos de PoE:

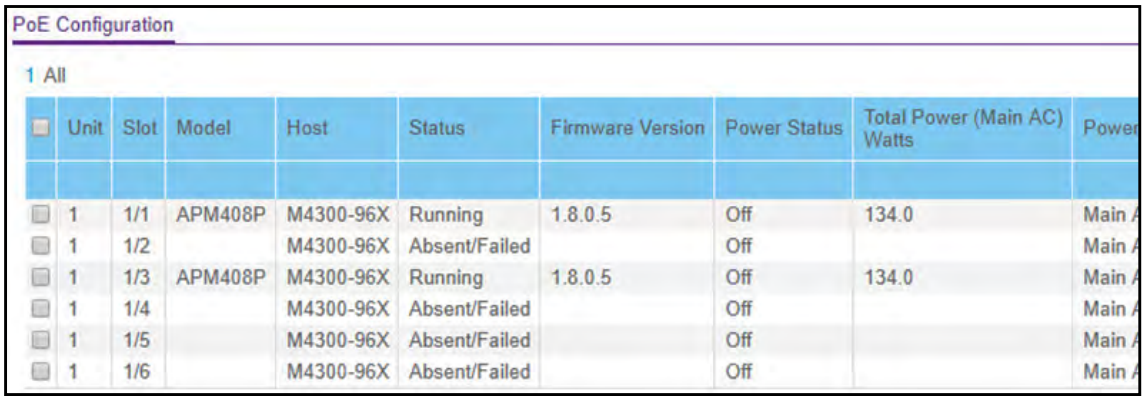
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > PoE > Basic > PoE Configuration.



El campo Unit muestra el número de unidad actual del switch PoE. El campo Slot muestra el número de ranura PoE actual del modelo M4300-96X.

5. Para configurar una unidad de switch PoE, seleccione la casilla del número de unidad del switch.
6. En el menú Power Management mode, seleccione el algoritmo de administración de energía que usa el switch para suministrar energía a los PD que la solicitan:
   - Static. Seleccione Static para que la energía asignada a cada puerto dependa del tipo de umbral de energía configurado en el puerto.
   - Dynamic. Seleccione Dynamic para que el consumo de energía de cada puerto se mida y calcule en tiempo real.
7. Para configurar los traps, en el menú PoE Trap Configuration, seleccione Enable para activar los traps de PoE o Disable para desactivarlos.

El valor predeterminado es habilitado.
8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
La siguiente tabla describe los campos no configurables de la página.

Tabla 43. Campos no configurables de la página básica PoE Configuration

Campo	Descripción
Model	Modelo de la tarjeta de puertos PoE.
Host	Switch en el que está instalada la tarjeta de puertos PoE.
Status	Estado de la tarjeta de puertos PoE.
Firmware Version	Versión de firmware del software PoE.
Power Status	Indica el estado de la energía.
Total Power (Main AC)	Potencia máxima en watts que el switch puede suministrar a todos los puertos. Si se muestra N/A, la fuente de alimentación no está presente.

Tabla 43. Campos no configurables de la página básica PoE Configuration (continuación)

Campo	Descripción
Power Source	Fuente de la energía del sistema.
Consumed Power	Potencia total en watts que se suministra a todos los puertos.

Configurar puertos PoE

Para configurar puertos PoE:

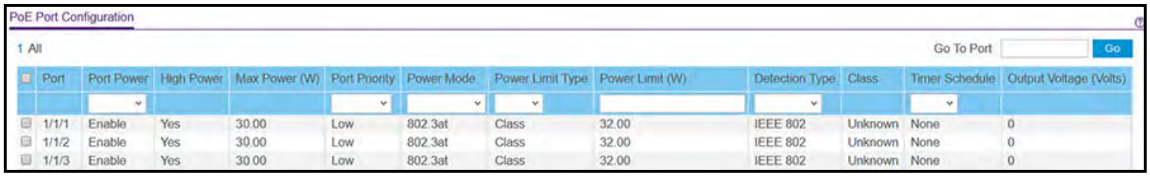
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > PoE > Advanced > PoE Port Configuration.



5. Seleccione uno o más puertos marcando sus casillas.
6. En el menú Port Power, seleccione Enable o Disable para indicar si el puerto puede suministrar energía.
7. Use el menú Port Priority para indicar qué puertos pueden seguir suministrando energía si la potencia total suministrada por el switch supera un umbral específico.

   Si el switch no puede suministrar energía a todos los dispositivos conectados, la prioridad de puerto determina qué puertos pueden seguir suministrándola. Entre puertos con la misma prioridad, los de número más bajo tienen mayor prioridad. Seleccione una de las siguientes prioridades:

   - Low. Prioridad baja
   - Medium. Prioridad media
   - High. Prioridad alta
   - Critical. Prioridad crítica

8. En el menú Power Mode, seleccione una de las siguientes opciones:
   - 802.3af. El puerto se alimenta en modo IEEE 802.3af. Por ejemplo, si la clase detectada por el switch no es la clase 4, el puerto del switch no alimenta el PD.

- Legacy. El puerto se alimenta con una corriente de arranque alta, usada por PD heredados cuyo requisito de energía de arranque supera 15W.
- Pre-802.3at. El puerto se alimenta inicialmente en modo IEEE 802.3af y luego cambia al modo de alta potencia IEEE 802.3at en un plazo de 75 ms. Este modo debe seleccionarse 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.

9. En el menú Power Limit Type, seleccione la potencia máxima que puede suministrar un puerto. Seleccione una de las siguientes opciones del menú:
   - None. El puerto consume hasta la potencia máxima de clase 0 en modo de baja potencia y hasta la potencia máxima de clase 4 en modo de alta potencia.
   - Class. El límite de potencia del puerto es igual a la clase del PD conectado.
   - User. El límite de potencia del puerto es igual al valor especificado en el campo Power Limit.
10. En el campo Power Limit (W), especifique la potencia máxima en watts que puede suministrar un puerto. La potencia máxima permitida es de 30W por puerto.
11. En el menú Detection Type, seleccione cómo detecta el puerto al PD:
    - pre-ieee. El puerto realiza la detección heredada.
    - IEEE 802. El puerto realiza una detección resistiva de 4 puntos. Es el valor predeterminado.
    - auto. El puerto realiza una detección resistiva de 4 puntos y, si es necesario, continúa con la detección heredada.
12. En el menú Timer Schedule, seleccione el programa de temporizador que se asignará al puerto.

    De forma predeterminada, la selección es None, que indica que no hay programa de temporizador asignado al puerto. Para más información sobre los programas de temporizador, consulte Administrar programas de temporizador en la página 161.
13. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
14. Para restablecer los puertos seleccionados, haga clic en el botón Reset. Se restablecen los puertos.

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

Tabla 44. Campos no configurables de la página avanzada PoE Configuration

Campo	Descripción
Port	Interfaz cuyos datos se mostrarán o configurarán.
High Power	Habilitado cuando el puerto admite el modo de alta potencia.
Max Power	Potencia máxima en watts que puede suministrar el puerto.

Tabla 44. Campos no configurables de la página Advanced PoE Configuration (continuación)

Campo	Descripción
Class	La clase define el rango de potencia que un PD consume del sistema. Definiciones de clase: 0 – 0.44-12.95 (watts) 1 – 0.44-3.83 (watts) 2 – 0.44-6.48 (watts) 3 – 0.44-12.95 (watts) 4 – 0.44-25.5 (watts)
Output Voltage	Voltaje actual suministrado al dispositivo, en volts.
Output Current	Corriente suministrada al dispositivo, en mA.
Output Power	Potencia actual suministrada al dispositivo, en watts.
Status	Estado operativo de la detección de PD del puerto. • Disabled. No se suministra energía. • DeliveringPower. El dispositivo está consumiendo energía. • Fault. Indica un problema con el puerto. • Test. El puerto está en modo de prueba. • otherFault. El puerto está inactivo por una condición de error. • Searching. El puerto no está en ninguno de los estados anteriores.
Fault Status	Describe el error cuando el puerto PSE está en estado de falla. • No Error. El puerto PSE no está en ningún estado de error. • MPS Absent. El puerto PSE detectó la ausencia de la fuente de alimentación principal. • Short. El puerto PSE detectó una condición de cortocircuito. • Overload. El PD conectado al puerto PSE intentó suministrar más energía de la que permite el hardware. • Power Denied. Se negó la energía al puerto PSE por falta de energía o por una acción administrativa.

Configurar los ajustes de energía PoE

Para configurar los ajustes de energía PoE:

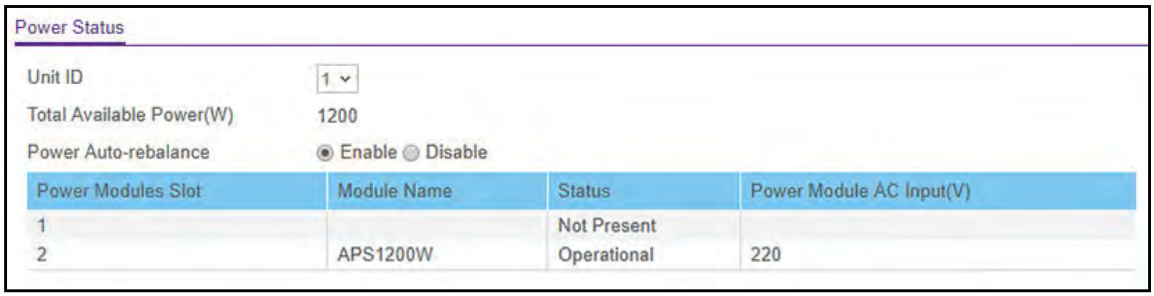
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > PoE > Advanced > Power Configuration.



5. En la sección Power Status, en el menú Unit ID, seleccione la unidad cuyo estado de energía desea mostrar.

6. Solo para el modelo de switch M4300-96X, seleccione el botón de opción Power Auto-rebalance Enable o Disable.

De forma predeterminada, está seleccionado el botón de opción Enable. Sin embargo, puede deshabilitar el reequilibrio automático de energía entre las bahías de PSU (ranuras de módulos de alimentación) del modelo de switch M4300-96X.

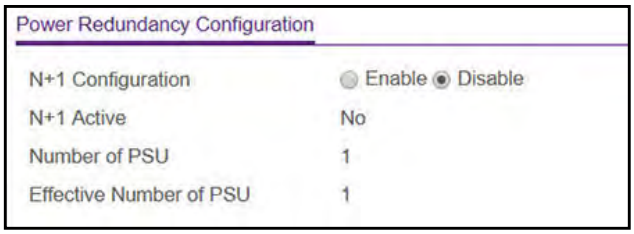
La siguiente tabla describe los campos no configurables de la sección Power Status.

Campo	Descripción
Total Available Power	La energía total disponible para la unidad, en vatios.
Power Modules Slot	El número de bahía de PSU (número de ranura del módulo de alimentación).
Module Name	El nombre del módulo de alimentación.
Status	El estado del módulo de alimentación, que puede ser uno de los siguientes: • Not Present. El módulo de alimentación no está presente. • Operational. El módulo de alimentación está conectado y funciona correctamente. • Failed. El switch no puede detectar el estado del módulo de alimentación.
Power Module AC Input	El voltaje de entrada del módulo de alimentación.



7. Solo para los modelos de switch M4300-28G-POE+ y M4300-52G-POE+, en la sección Redundancy Mode Status, seleccione el botón de opción N+1 Configuration Enable o Disable.

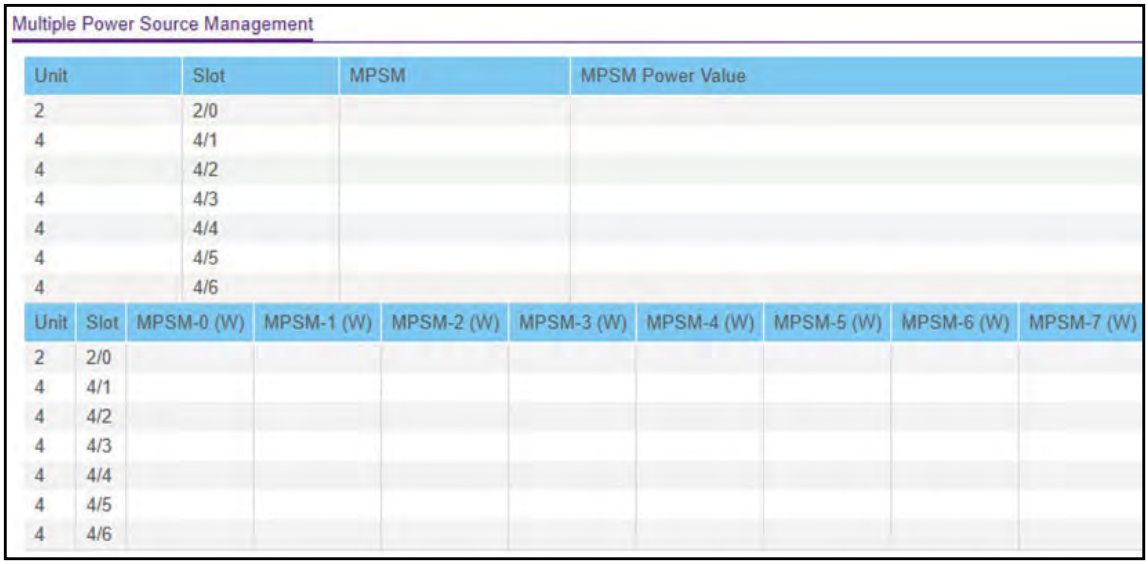
Si selecciona el botón de opción Enable, se habilita la función de redundancia de energía, lo que hace que la energía total utilizable que suministran todas las PSU disponibles sea menor que la energía que puede suministrar una sola PSU. En esta configuración, la carga se reparte por igual entre todas las PSU, que funcionan como si fueran una gran fuente de alimentación ininterrumpida. La función de redundancia de energía está deshabilitada de forma predeterminada.



La siguiente tabla describe los campos no configurables de la sección Power Redundancy Configuration.

Campo	Descripción
N+1 Active	Indica si la función de redundancia de energía N+1 está habilitada. Los valores posibles son Yes (habilitada) y No (deshabilitada).
Number of PSU	El número total de PSU.
Effective Number of PSU	El número efectivo de PSU, considerando la función de redundancia de energía N+1.

La tabla Multiple Power Source Management muestra el número de fuentes de energía activas (como tarjetas de puertos que suministran PoE) de cada unidad de switch.



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

Configurar SNMP

Puede configurar los ajustes de SNMP para SNMP V1/V2 y SNMPv3.

Configurar la comunidad SNMP V1/V2

De forma predeterminada, existen dos comunidades SNMP:

- Private, con privilegios de lectura/escritura y estado establecido en Enable.
- Public, con privilegios de solo lectura y estado establecido en Enable.

Estas son comunidades conocidas. Puede cambiar los valores predeterminados o agregar otras comunidades. Solo las comunidades que defina pueden acceder al switch mediante los protocolos SNMP V1 y SNMP V2. Solo las comunidades con acceso de lectura/escritura pueden usarse para cambiar la configuración mediante SNMP.

Nota: Si desea usar SNMP v3, use el menú User Accounts.

Para configurar la comunidad SNMP V1/V2:

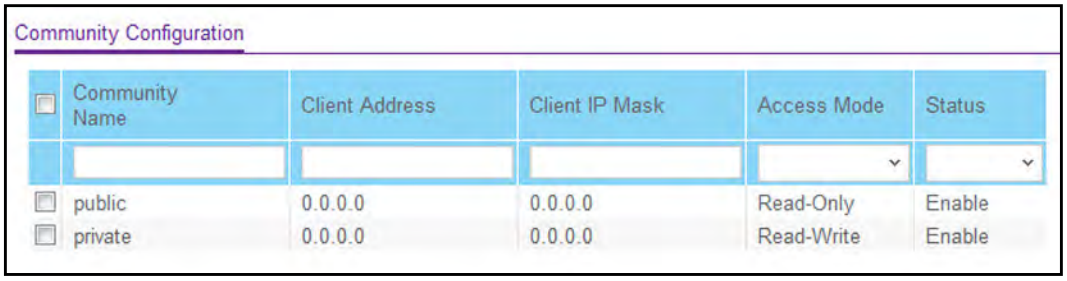
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > SNMP > SNMP V1/V2 > Community Configuration.



5. Use Community Name para reconfigurar una comunidad existente o crear una nueva.

   Use este menú para seleccionar uno de los nombres de comunidad existentes, o seleccione 'Create' para agregar uno nuevo. Una entrada válida es una cadena de hasta 16 caracteres que distingue mayúsculas y minúsculas.

6. Client Address. En conjunto, Client Address y Client IP Mask indican un rango de direcciones IP desde las que los clientes SNMP pueden usar esa comunidad para acceder a este dispositivo.

Si cualquiera de los valores (Client Address o IP Mask) es 0.0.0.0, se permite el acceso desde cualquier dirección IP. De lo contrario, se aplica un AND entre la dirección de cada cliente y la máscara, al igual que con Client Address, y, si los valores son iguales, se permite el acceso. Por ejemplo, si los parámetros Client Address y Client IP Mask son 192.168.1.0/255.255.255.0, cualquier cliente

cuya dirección esté entre 192.168.1.0 y 192.168.1.255 (inclusive) tiene acceso. Para permitir el acceso desde una sola estación, use un valor de Client IP Mask de 255.255.255.255 y use la dirección IP de ese equipo como Client Address.

7. Client IP Mask. En conjunto, Client Address y Client IP Mask indican un rango de direcciones IP desde las que los clientes SNMP pueden usar esa comunidad para acceder a este dispositivo.

Si cualquiera de los valores (Client Address o IP Mask) es 0.0.0.0, se permite el acceso desde cualquier dirección IP. De lo contrario, se aplica un AND entre la dirección de cada cliente y la máscara, al igual que con Client Address, y, si los valores son iguales, se permite el acceso. Por ejemplo, si los parámetros Client Address y Client IP Mask son 192.168.1.0/255.255.255.0, cualquier cliente

cuya dirección IP esté entre 192.168.1.0 y 192.168.1.255 (inclusive) tiene acceso. Para permitir el acceso desde una sola estación, use un valor de Client IP Mask de 255.255.255.255 y use la dirección IP de ese equipo como Client Address.

8. En el menú Access mode, seleccione Read-Write o Read-Only. Esto especifica el nivel de acceso de esta comunidad.
9. Use Status para especificar el estado de esta comunidad seleccionando Enable o Disable.

Si selecciona Enable, el Community Name debe ser único entre todos los nombres de comunidad válidos; de lo contrario, se rechaza la solicitud. Si selecciona Disable, el Community Name deja de ser válido.

10. Haga clic en el botón Add.
La comunidad seleccionada se agrega al switch.

Configurar los ajustes de traps SNMP V1/V2

Para configurar los ajustes de traps SNMP V1/V2:

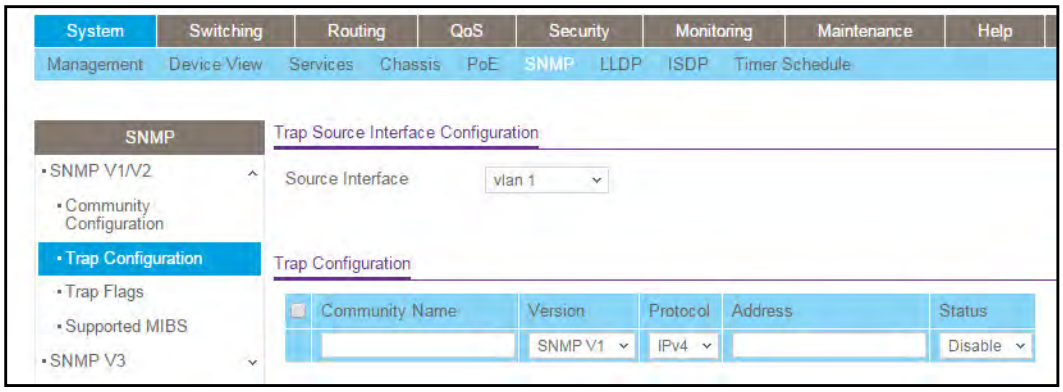
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > SNMP > SNMP V1/V2 > Trap Configuration.



5. En la lista Source Interface, seleccione la interfaz de origen que se usará para el receptor de traps SNMP. Los valores posibles son los siguientes:

- Interfaz de enrutamiento
- Routing VLAN
- Interfaz loopback de enrutamiento
- Interfaz de túnel
- Puerto de servicio

De forma predeterminada, se usa VLAN 1 como interfaz de origen.
6. Para agregar un host que reciba traps SNMP, siga estos pasos:

a. Community Name. Ingrese la cadena de comunidad del paquete de trap SNMP que se enviará al administrador de traps. Este nombre puede tener hasta 16 caracteres y distingue mayúsculas y minúsculas.

b. Version. Seleccione la versión de trap que usará el receptor:

- SNMP V1. Usa SNMP V1 para enviar traps al receptor.
- SNMP V2. Usa SNMP V2 para enviar traps al receptor.

c. Protocol. Seleccione el protocolo que usará el receptor. Seleccione IPv4 si la dirección del receptor es una dirección IPv4, o IPv6 si la dirección del receptor es IPv6. d. Address. Ingrese la dirección IPv4 en formato x.x.x.x o la dirección IPv6 en formato

xxxx:xxxx:xxxx:xxxxx:xxxx:xxxx:xxxx:xxxx para recibir traps SNMP de este dispositivo. La longitud de la dirección no puede exceder 39 caracteres.

e. Status. Seleccione el estado del receptor:

- Enable. Envía traps al receptor
- Disable. No envía traps al receptor.

f. Haga clic en el botón Add.

7. Para hacer cambios, haga lo siguiente:

- Para modificar la información de un destinatario SNMP existente, marque la casilla del destinatario y cambie los campos deseados.
- Para eliminar un destinatario, marque su casilla y haga clic en el botón Delete.

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

Configurar los indicadores de traps SNMP V1/V2

Puede habilitar o deshabilitar traps. Cuando el switch detecta la condición identificada por un trap activo, se envía un mensaje de trap a todos los receptores de traps SNMP habilitados y se escribe un mensaje en el registro de traps.

Para configurar los indicadores de trap:

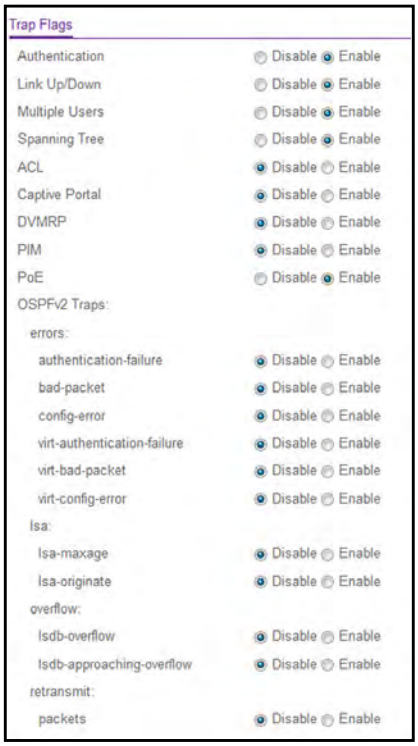
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > SNMP > SNMP V1/V2 > Trap Flags.



5. Seleccione el botón de opción Authentication Disable o Enable.

Esto habilita o deshabilita la activación de traps de falla de autenticación. El valor predeterminado de fábrica es Enable.

6. Seleccione el botón de opción Link Up/Down Disable o Enable

Esto habilita o deshabilita la activación de traps de estado de enlace. El valor predeterminado de fábrica es Enable.

7. Seleccione el botón de opción Multiple Users Disable o Enable

Esto habilita o deshabilita la activación de traps de múltiples usuarios. El valor predeterminado de fábrica es Enable. Este trap se activa cuando el mismo ID de usuario inicia sesión en el switch más de una vez al mismo tiempo (ya sea por Telnet o por el puerto serie).

8. Seleccione el botón de opción Spanning Tree Disable o Enable.

Esto habilita o deshabilita la activación de traps de spanning tree. El valor predeterminado de fábrica es Enable.
9. Seleccione el botón de opción ACL Disable o Enable.
Esto habilita o deshabilita la activación de traps de ACL. El valor predeterminado de fábrica es Disable.
10. Seleccione el botón de opción PoE Disable o Enable.

Esto habilita o deshabilita la activación de traps de PoE. El valor predeterminado de fábrica es Enable. Indica si se envían traps de PoE.

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

Ver las MIB compatibles

Para ver todas las MIB compatibles con el switch:

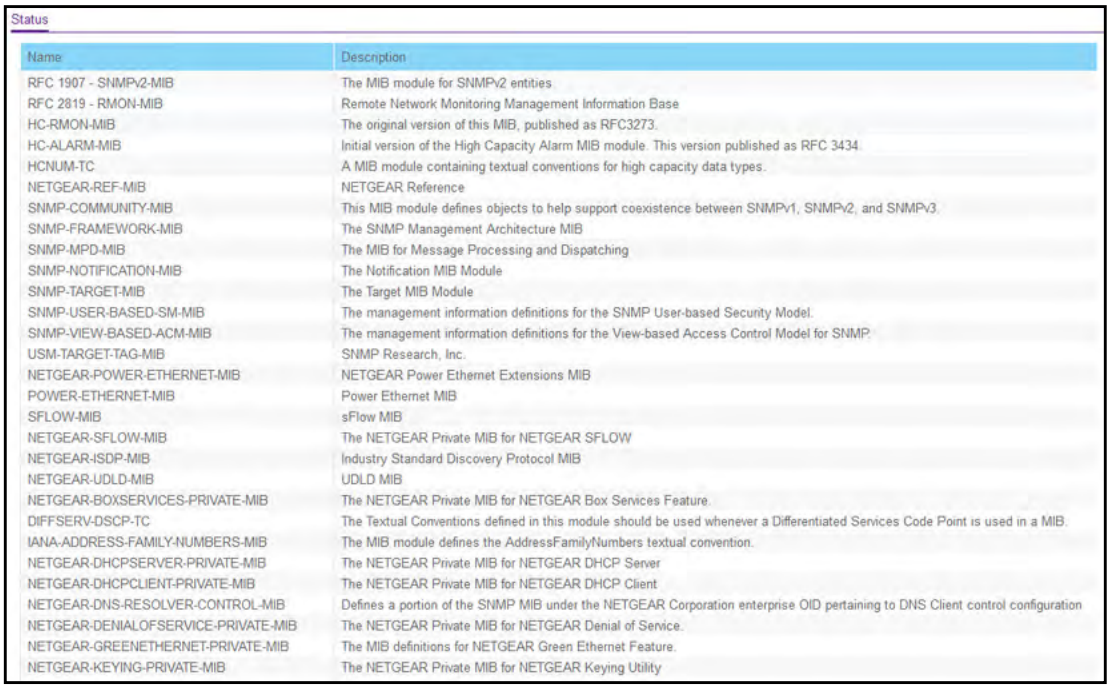
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > SNMP > SNMP V1/V2 >Supported MIBs.


Status

Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
HC-RMON-MIB	The original version of this MIB, published as RFC3273.
HC-ALARM-MIB	Initial version of the High Capacity Alarm MIB module. This version published as RFC 3434.
HCNUM-TC	A MIB module containing textual conventions for high capacity data types.
NETGEAR-REF-MIB	NETGEAR Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
NETGEAR-POWER-ETHERNET-MIB	NETGEAR Power Ethernet Extensions MIB
POWER-ETHERNET-MIB	Power Ethernet MIB
SFLOW-MIB	sFlow MIB
NETGEAR-SFLOW-MIB	The NETGEAR Private MIB for NETGEAR SFLOW
NETGEAR-ISDP-MIB	Industry Standard Discovery Protocol MIB
NETGEAR-UDLD-MIB	UDLD MIB
NETGEAR-BOXSERVICES-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Box Services Feature.
DIFFSERV-DSCP-TC	The Textual Conventions defined in this module should be used whenever a Differentiated Services Code Point is used in a MIB.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
NETGEAR-DHCPSERVER-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR DHCP Server
NETGEAR-DHCPCLIENT-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR DHCP Client
NETGEAR-DNS-RESOLVER-CONTROL-MIB	Defines a portion of the SNMP MIB under the NETGEAR Corporation enterprise OID pertaining to DNS Client control configuration
NETGEAR-DENIALOFSERVICE-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Denial of Service.
NETGEAR-GREENETHERNET-PRIVATE-MIB	The MIB definitions for NETGEAR Green Ethernet Feature.
NETGEAR-KEYING-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Keying Utility

La siguiente tabla describe los campos de SNMP Supported MIBs Status.

Tabla 45. MIB compatibles con SNMP

Campo	Descripción
Name	El número de RFC, si corresponde, y el nombre de la MIB.
Description	El título de la RFC o la descripción de la MIB.

Configurar usuarios SNMP V3

Para configurar los ajustes de SNMPv3 de una cuenta de usuario:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > SNMP > SNMP V3 > User Configuration.

   Se muestra la página User Configuration.

5. En el campo User Name, escriba un nombre para la cuenta de usuario. El nombre puede tener hasta 30 caracteres.

6. En el menú SNMP v3 Access Mode, seleccione Read-Only o Read/Write para especificar los privilegios de acceso SNMPv3 de la cuenta de usuario.

Los privilegios de acceso SNMPv3 de la cuenta admin son Read/Write.

7. Haga una selección en el menú Authentication Protocol:

- None. El usuario no puede acceder a los datos SNMP desde un navegador SNMP.
- SHA512. Se usa el protocolo SHA512 para la autenticación. Debe establecer una clave de autenticación SNMPv3 (consulte el siguiente paso).

8. Si selecciona SHA512 en el menú Authentication Protocol, establezca la contraseña (clave) en el campo Authentication Key.

La contraseña puede tener hasta 32 caracteres.

9. Haga una selección en el menú Encryption Protocol:

- None. Se omite el cifrado.
- AES128. Se usa el protocolo AES128 para el cifrado. Debe establecer una clave de cifrado (consulte el siguiente paso).

10. Si selecciona AES128 en el menú Encryption Protocol, establezca la clave de cifrado en el campo SNMPv3 Encryption Key.

La clave puede tener hasta 32 caracteres.

11. Haga clic en el botón Add.

Se agrega la cuenta de usuario.

Configurar LLDP

El estándar definido por IEEE 802.1AB, Link Layer Discovery Protocol (LLDP), permite que las estaciones de una LAN 802 anuncien sus capacidades principales y descripciones físicas. Un administrador de red consulta esta información para identificar la topología del sistema y detectar configuraciones incorrectas en la LAN.

LLDP es un protocolo unidireccional; no hay secuencias de solicitud/respuesta. La información la anuncian las estaciones que implementan la función de transmisión, y la reciben y procesan las estaciones que implementan la función de recepción. Las funciones de transmisión y recepción pueden habilitarse/deshabilitarse por separado en cada puerto. De forma predeterminada, ambas están deshabilitadas en todos los puertos. La aplicación se encarga de iniciar cada máquina de estados de transmisión y recepción correctamente, según el estado configurado y el estado operativo del puerto.

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) es una mejora de LLDP con las siguientes funciones:

- Detección automática de políticas de LAN (como ajustes de VLAN, prioridad de capa 2 y DiffServ), lo que permite redes plug and play.
- Detección de la ubicación de dispositivos para crear bases de datos de ubicación.
- Administración de energía extendida y automatizada de puntos finales Power over Ethernet.
- Administración de inventario, que permite a los administradores de red rastrear sus dispositivos de red y determinar sus características (fabricante, versiones de software y hardware, número de serie/activo).

Configurar los ajustes globales de LLDP

Puede especificar los parámetros de LLDP que se aplican al switch.

Para configurar los ajustes globales de LLDP:

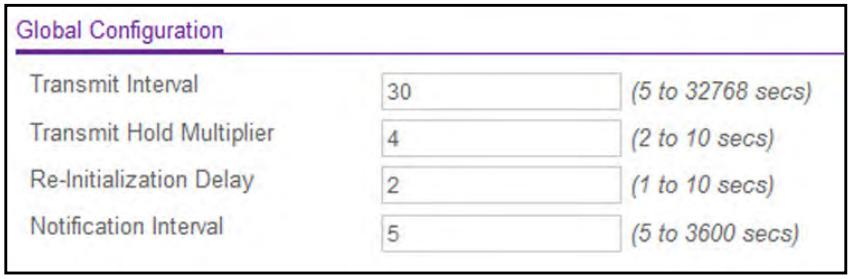
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > Global Configuration.



5. En el campo Transmit Interval, ingrese el intervalo en segundos para transmitir tramas LLDP. El rango es de 5 a 32768 s. El valor predeterminado es 30 segundos.
6. En el campo Transmit Hold Multiplier, ingrese el multiplicador de Transmit Interval para asignar el TTL. El rango es de 2 a 10 s. El valor predeterminado es 4.
7. En el campo Re-Initialization Delay, ingrese el retardo antes de la reinicialización. El rango es de 1 a 10 s. El valor predeterminado es 2 segundos.

8. En el campo Notification Interval, ingrese el intervalo en segundos para la transmisión de notificaciones.

El rango es de 5 a 3600 s. El valor predeterminado es 5 segundos.
9. Haga clic en el botón Apply.
La configuración se guarda.

Configurar la interfaz LLDP

Para configurar la interfaz LLDP:

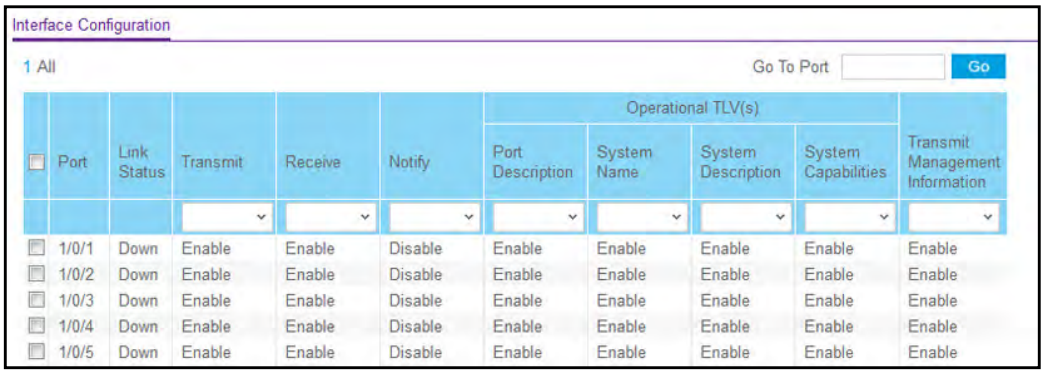
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > Interface Configuration.



5. Use Go To Port para ingresar el puerto en formato unidad/ranura/puerto y haga clic en el botón Go. Se selecciona la entrada correspondiente al puerto especificado.
6. Use Port para especificar la lista de puertos en los que se puede configurar LLDP - 802.1AB. El campo Link Status indica si el enlace está activo o inactivo.
7. Use Transmit para especificar el modo de transmisión LLDP - 802.1AB de la interfaz seleccionada.
8. Use Receive para especificar el modo de recepción LLDP - 802.1AB de la interfaz seleccionada.
9. Use Notify para especificar el modo de notificación LLDP - 802.1AB de la interfaz seleccionada.
10. TLV opcionales:

- Use Port Description para incluir el TLV de descripción de puerto en las tramas LLDP.
- Use System Name para incluir el TLV de nombre del sistema en las tramas LLDP.
- Use System Description para incluir el TLV de descripción del sistema en las tramas LLDP.
- Use System Capabilities para incluir el TLV de capacidades del sistema en las tramas LLDP.

11. Use Transmit Management Information para especificar si se transmite la dirección de administración en las tramas LLDP de la interfaz seleccionada.
12. Haga clic en el botón Apply.
Se guarda la configuración.

Ver las estadísticas de LLDP

Para ver las estadísticas de LLDP:

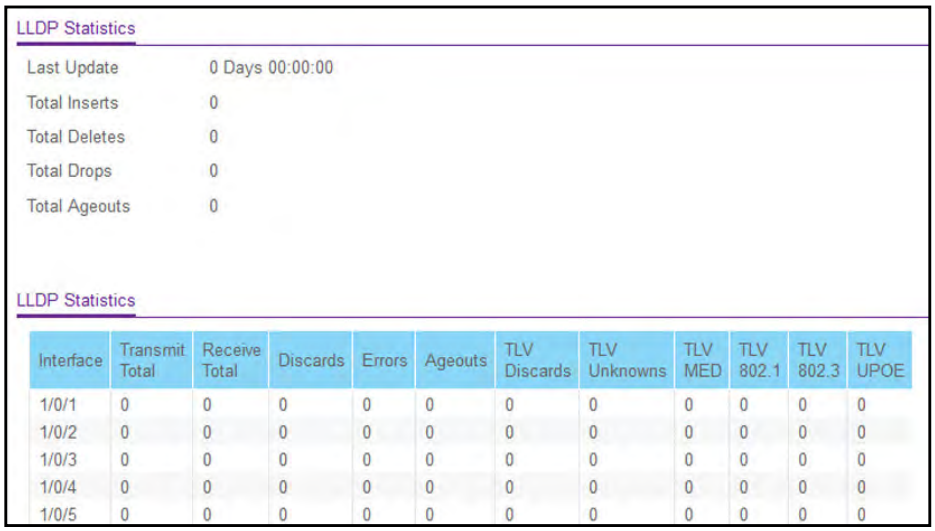
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. **Seleccione System > LLDP > Statistics.**



La siguiente tabla describe los campos de LLDP Statistics.

Tabla 46. Estadísticas de LLDP

Campo	Descripción
Last Update	La hora en que se creó, modificó o eliminó una entrada en las tablas asociadas con el sistema remoto.
Total Inserts	El número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) específico se insertó en las tablas asociadas con los sistemas remotos.
Total Deletes	El número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) específico se eliminó de las tablas asociadas con los sistemas remotos.
Total Drops	El número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) específico no pudo ingresarse en las tablas asociadas con los sistemas remotos por falta de recursos.
Total Age outs	El número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) específico se eliminó de las tablas asociadas con los sistemas remotos porque expiró el intervalo de vigencia de la información.
Interface	La unidad/ranura/puerto de las interfaces.
Transmit Total	El número de tramas LLDP transmitidas por el agente LLDP en el puerto correspondiente.
Receive Total	El número de tramas LLDP válidas recibidas por este agente LLDP en el puerto correspondiente, mientras el agente LLDP está habilitado.

Tabla 46. Estadísticas de LLDP (continuación)

Campo	Descripción
Discards	El número de TLV LLDP descartados por cualquier motivo por el agente LLDP en el puerto correspondiente.
Errors	El número de tramas LLDP no válidas recibidas por el agente LLDP en el puerto correspondiente, mientras el agente LLDP está habilitado.
Age outs	El número de expiraciones ocurridas en un puerto determinado. Una expiración es el número de veces que el conjunto completo de información anunciado por un MAC Service Access Point (MSAP) específico se eliminó de las tablas asociadas con las entradas remotas porque expiró el intervalo de vigencia de la información.
TLV Discards	El número de TLV LLDP descartados por cualquier motivo por el agente LLDP en el puerto correspondiente.
TLV Unknowns	El número de TLV LLDP recibidos en los puertos locales que no fueron reconocidos por el agente LLDP en el puerto correspondiente.
TLV MED	El número total de TLV LLDP-MED recibidos en los puertos locales.
TLV 802.1	El número total de TLV LLDP recibidos en los puertos locales que son de tipo 802.1.
TLV 802.3	El número total de TLV LLDP recibidos en los puertos locales que son de tipo 802.3.

Ver la información del dispositivo local LLDP

Para ver la información del dispositivo local LLDP:

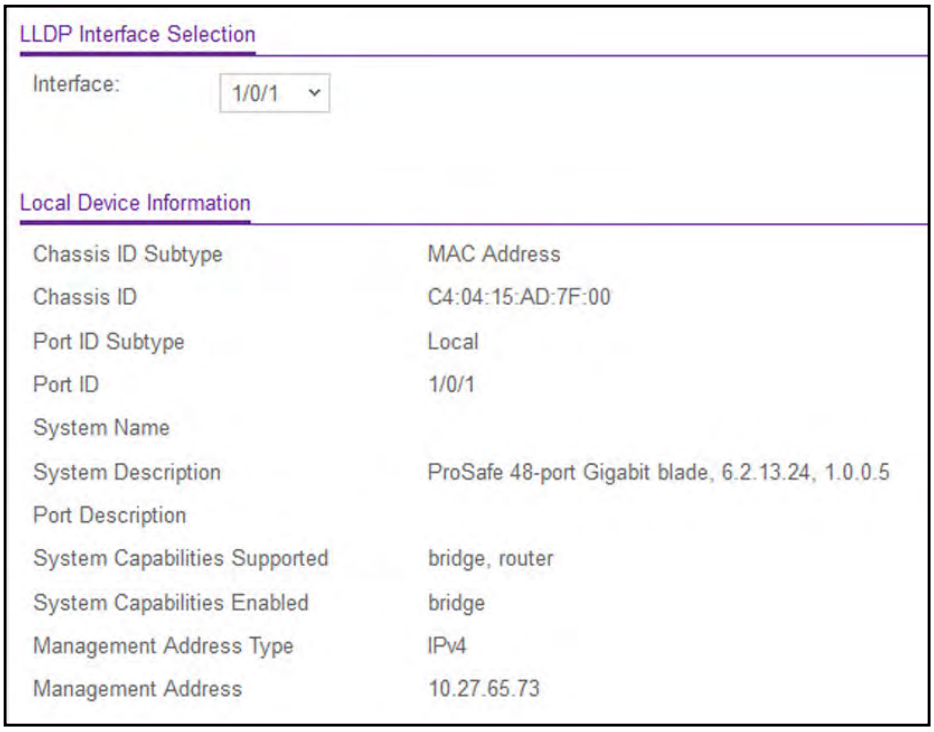
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > Local Device Information.



5. En la lista Interface, seleccione los puertos en los que se pueden transmitir tramas LLDP - 802.1AB. La siguiente tabla describe los campos de LLDP Local Device Information.

Tabla 47. Información del dispositivo local LLDP

Campo	Descripción
Chassis ID Subtype	La cadena que describe el origen del identificador del switch.
Chassis ID	El valor de cadena que identifica el componente del switch asociado con el sistema local.
Port ID Subtype	La cadena que describe el origen del identificador del puerto.
Port ID	La cadena que describe el origen del identificador del puerto.
System Name	El nombre del sistema local.
System Description	La descripción del puerto seleccionado asociado con el sistema local.
Port Description	La descripción del puerto seleccionado asociado con el sistema local.
System Capabilities Supported	Las capacidades del sistema local.
System Capabilities Enabled	Las capacidades del sistema local que son compatibles y están habilitadas.
Management Address Type	El tipo de dirección de administración.
Management Address	La dirección de administración anunciada del sistema local.

Ver la información de dispositivos remotos LLDP

Puede ver información sobre los dispositivos remotos conectados al puerto.

Para ver la información de dispositivos remotos LLDP:

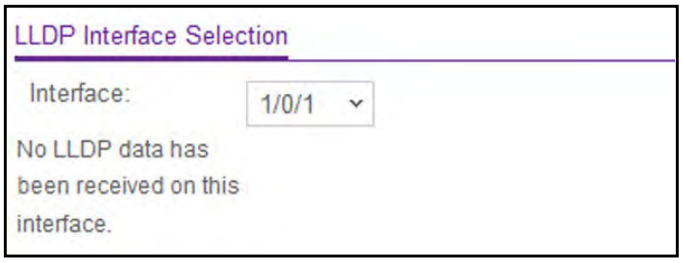
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > Remote Device Information.



5. Use Interface para seleccionar los puertos locales que pueden recibir tramas LLDP. La siguiente tabla describe los campos de LLDP Remote Device Information.

Tabla 48. Información de dispositivos remotos LLDP

Campo	Descripción
Remote ID	El ID remoto.
Switch ID	El componente del switch asociado con el sistema remoto.
Switch ID Subtype	El origen del identificador del switch.
Port ID	El componente de puerto asociado con el sistema remoto.
Port ID Subtype	El origen del identificador del puerto.
System Name	El nombre del sistema remoto.
System Description	La descripción del puerto asociado con el sistema remoto.
Port Description	La descripción del puerto asociado con el sistema remoto.
System Capabilities Supported	Las capacidades del sistema remoto.
System Capabilities Enabled	Las capacidades del sistema remoto que son compatibles y están habilitadas.

Tabla 48. Información de dispositivos remotos LLDP (continuación)

Campo	Descripción
Time to Live	El valor Time To Live, en segundos, de la entrada remota recibida.
Management Address Type	El tipo de dirección de administración.
Management Address	• Management Address. La dirección de administración anunciada del sistema remoto. • Type. El tipo de dirección de administración.

Ver el inventario de dispositivos remotos LLDP

Para ver el inventario de dispositivos remotos LLDP:

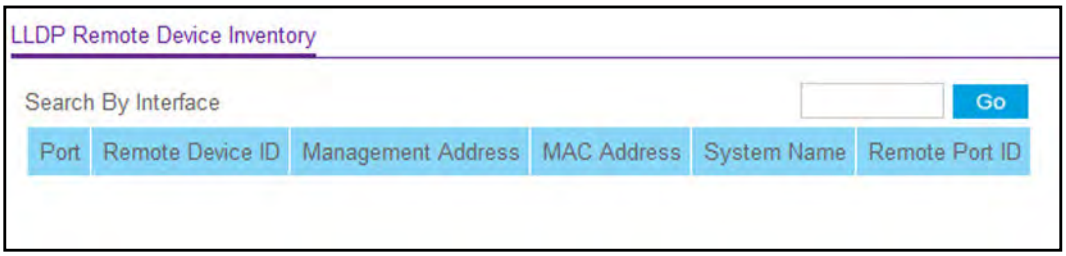
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > LLDP > Remote Device Inventory.



La siguiente tabla describe los campos de LLDP Remote Device Inventory.

Tabla 49. Inventario de dispositivos remotos LLDP

Campo	Descripción
Port	La lista de todos los puertos en los que está habilitada la trama LLDP.
Remote Device ID	El ID del dispositivo remoto.
Management Address	La dirección de administración anunciada del sistema remoto.
MAC Address	La dirección MAC asociada con el sistema remoto.

Tabla 49. Inventario de dispositivos remotos LLDP (continuación)

Campo	Descripción
Nombre del sistema	Especifica el nombre del modelo del dispositivo remoto.
ID de puerto remoto	El componente de puerto asociado con el sistema remoto.

Configurar los ajustes globales de LLDP-MED

Puede especificar los parámetros de LLDP-MED que se aplican al switch.

Para configurar los ajustes globales de LLDP-MED:

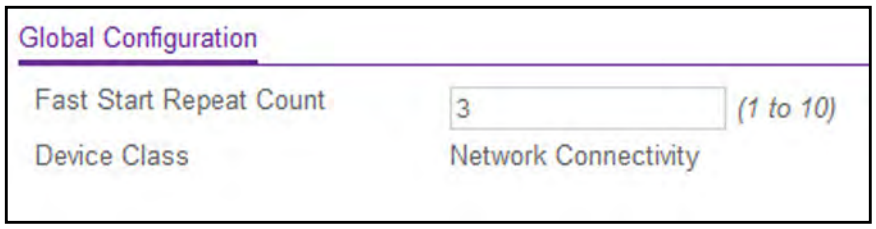
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > LLDP-MED > Global Configuration.



5. En el campo Fast Start Repeat Count, ingrese el número de PDU LLDP que se transmiten cuando se habilita el protocolo.

   El rango es de 1 a 10. El valor predeterminado de Fast Start Repeat Count es 3.

   El campo Device Class especifica la clasificación MED del dispositivo local. Hay cuatro tipos de dispositivos; tres representan los puntos finales reales (clasificados como Clase I Genéricos [controlador de comunicación IP, etc.], Clase II Multimedia [puente de conferencia, etc.], Clase III Comunicación [teléfono IP, etc.]). El cuarto tipo es el dispositivo de conectividad de red, normalmente un switch/router LAN, un puente IEEE 802.1, un punto de acceso inalámbrico IEEE 802.11, etc.

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

Configurar la interfaz LLDP-MED

Para configurar la interfaz LLDP-MED

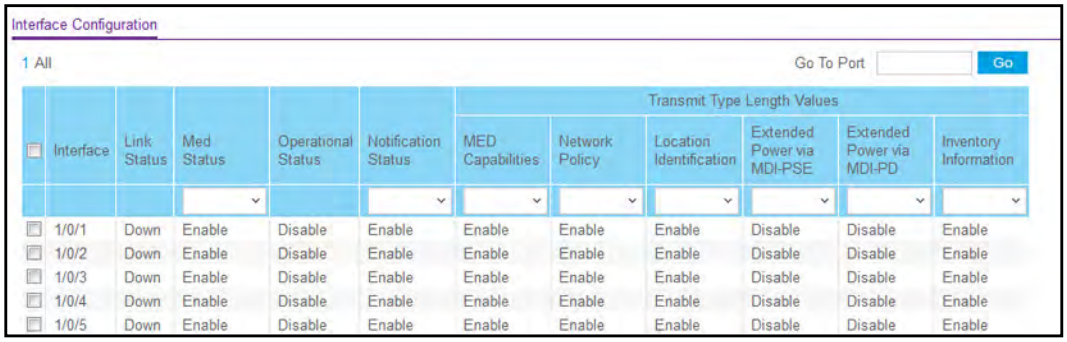
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > LLDP-MED > Interface Configuration.



   El campo Link Status muestra el estado del enlace del puerto (activo o inactivo).

   El campo Operational Status muestra si se transfieren TLV de LLDP-MED en esta interfaz.

5. Use Go To Port para ingresar el puerto en formato unidad/ranura/puerto y haga clic en el botón Go. Se selecciona la entrada correspondiente al puerto especificado.
6. Use Interface para especificar la lista de puertos en los que se puede configurar LLDP-MED - 802.1AB.
7. Use MED Status para especificar si el modo LLDP-MED está habilitado o deshabilitado en esta interfaz.
8. Use Notification Status para especificar el modo de notificación de topología LLDP-MED de la interfaz.
9. Use Transmit Type Length Values para especificar qué TLV opcionales de LLDP-MED se transmiten en las tramas PDU LLDP de la interfaz seleccionada:
   - MED Capabilities. Para transmitir el TLV de capacidades en tramas LLDP.
   - Network Policy. Para transmitir el TLV de política de red en tramas LLDP.
   - Location Identification. Para transmitir el TLV de ubicación en tramas LLDP.
   - Extended Power via MDI - PSE. Para transmitir el TLV de PSE extendido en tramas LLDP.

- Extended Power via MDI - PD. Para transmitir el TLV de PD extendido en tramas LLDP.
- Inventory Information. Para transmitir el TLV de inventario en tramas LLDP.

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

Ver la información del dispositivo local LLDP-MED

Para ver la información del dispositivo local LLDP-MED:

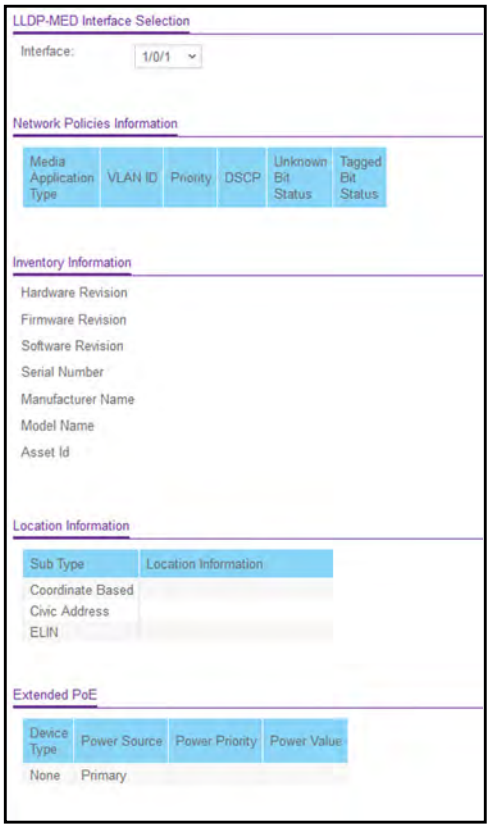
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > LLDP-MED > Local Device Information.



5. Use Interface para seleccionar los puertos en los que se pueden transmitir tramas LLDP-MED.

La siguiente tabla describe los campos de LLDP-MED Local Device Information.

Tabla 50. Información del dispositivo local LLDP-MED

Campo	Descripción
Información de política de red: Especifica si hay un TLV de política de red en las tramas LLDP.	
Tipo de aplicación multimedia	El tipo de aplicación. Los tipos son unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Cada tipo de aplicación recibido tiene ID de VLAN, prioridad, DSCP, estado del bit etiquetado y del bit desconocido. Un puerto puede recibir uno o varios de estos tipos de aplicación. Esta información solo se muestra si se transmitió un TLV de política de red
Inventario: Especifica si hay un TLV de inventario en las tramas LLDP	
Revisión de hardware	Especifica la versión de hardware.
Revisión de firmware	Especifica la versión de firmware.
Revisión de software	Especifica la versión de software.
Número de serie	Especifica el número de serie.
Nombre del fabricante	Especifica el nombre del fabricante.
Nombre del modelo	Especifica el nombre del modelo.
ID de activo	Especifica el ID de activo.
Información de ubicación: Especifica si hay un TLV de ubicación en las tramas LLDP.	
Subtipo	Especifica el tipo de información de ubicación.
Información de ubicación	La información de ubicación como cadena para el tipo de ID de ubicación.

Ver la información de dispositivos remotos LLDP-MED

Para ver la información de dispositivos remotos LLDP-MED:

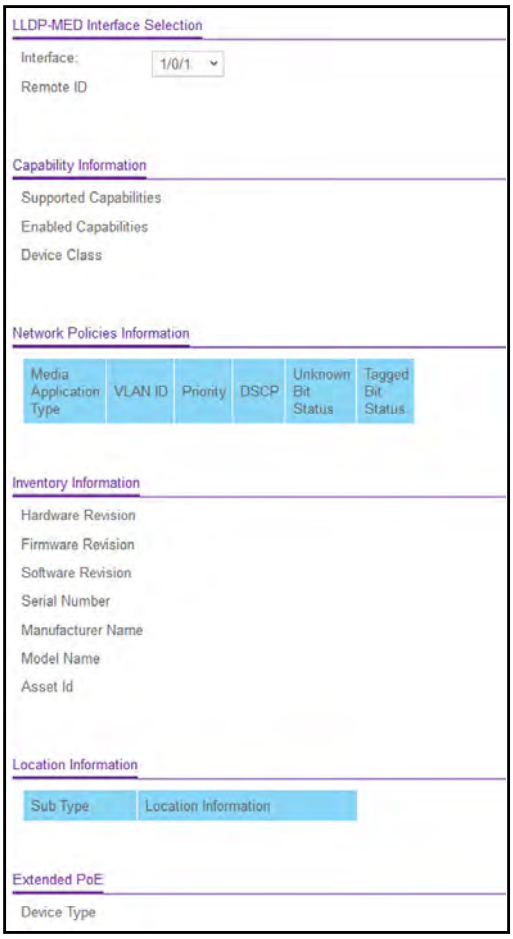
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > LLDP-MED > Remote Device Information.



5. Use Interface para seleccionar los puertos con LLDP-MED habilitado. La siguiente tabla describe los campos de LLDP-MED Remote Device Information.

Tabla 51. Información de dispositivos remotos LLDP-MED

Campo	Descripción
Información de capacidades: Las capacidades compatibles y habilitadas recibidas en el TLV MED en este puerto.	
Capacidades compatibles	Especifica las capacidades compatibles recibidas en el TLV MED en este puerto.
Capacidades habilitadas	Especifica las capacidades habilitadas recibidas en el TLV MED en este puerto.
Clase de dispositivo	Especifica la clase de dispositivo anunciada por el dispositivo remoto conectado al puerto.

Tabla 51. Información de dispositivos remotos LLDP-MED (continuación)

Campo	Descripción
Información de política de red: Especifica si se recibe un TLV de política de red en las tramas LLDP de este puerto.	
Tipo de aplicación multimedia	El tipo de aplicación. Los tipos son unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, vidoesignalling. Cada tipo de aplicación recibido tiene ID de VLAN, prioridad, DSCP, estado del bit etiquetado y del bit desconocido. Un puerto puede recibir uno o varios de estos tipos. Esta información solo se muestra si se recibió un TLV de política de red en este puerto.
ID de VLAN	El ID de VLAN asociado con un tipo de política específico.
Prioridad	La prioridad asociada con un tipo de política específico.
DSCP	El DSCP asociado con un tipo de política específico.
Estado del bit desconocido	El bit desconocido asociado con un tipo de política específico.
Estado del bit etiquetado	El bit etiquetado asociado con un tipo de política específico.
Información de inventario: Especifica si se recibe un TLV de inventario en las tramas LLDP de este puerto.	
Revisión de hardware	Especifica la versión de hardware del dispositivo remoto.
Revisión de firmware	Especifica la versión de firmware del dispositivo remoto.
Revisión de software	Especifica la versión de software del dispositivo remoto.
Número de serie	Especifica el número de serie del dispositivo remoto.
Nombre del fabricante	Especifica el nombre del fabricante del dispositivo remoto.
Nombre del modelo	Especifica el nombre del modelo del dispositivo remoto.
ID de activo	Especifica el ID de activo del dispositivo remoto.
Información de ubicación: Especifica si se recibe un TLV de ubicación en las tramas LLDP de este puerto.	
Subtipo	Especifica el tipo de información de ubicación.
Información de ubicación	La información de ubicación como cadena para el tipo de ID de ubicación.
PoE extendido: Especifica si el dispositivo remoto es un dispositivo PoE.	
Tipo de dispositivo	Especifica el tipo de dispositivo PoE remoto conectado a este puerto.
PoE PSE extendido: Especifica si se recibe un TLV de PSE extendido en la trama LLDP de este puerto	
Disponible	Valor de potencia PSE del puerto remoto en décimas de watt.
Fuente	Fuente de alimentación PSE del puerto remoto.
Prioridad	Prioridad de alimentación PSE del puerto remoto.

Tabla 51. Información de dispositivos remotos LLDP-MED (continuación)

Campo	Descripción
PoE PD extendido: Especifica si se recibe un TLV de PD extendido en la trama LLDP de este puerto.	
Requerida	Requisito de potencia PD del puerto remoto.
Fuente	Fuente de alimentación PD del puerto remoto.
Prioridad	Prioridad de alimentación PD del puerto remoto.

Ver el inventario de dispositivos remotos LLDP-MED

Para ver el inventario de dispositivos remotos LLDP-MED:

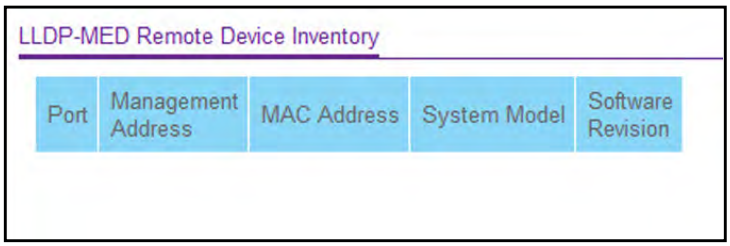
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > LLDP > LLDP-MED > Remote Device Inventory.



La siguiente tabla describe los campos de LLDP-MED Remote Device Inventory.

Tabla 52. Inventario de dispositivos remotos LLDP-MED

Campo	Definición
Puerto	Lista de todos los puertos con LLDP-MED habilitado.
Management Address	La dirección de administración anunciada del sistema remoto.
MAC Address	La dirección MAC asociada con el sistema remoto.
Modelo del sistema	Especifica el nombre del modelo del dispositivo remoto.
Revisión de software	Especifica la versión de software del dispositivo remoto.

Configurar la dependencia de enlace

La función de dependencia de enlace permite habilitar o deshabilitar uno o más puertos según el estado de enlace de otros puertos. Con la dependencia de enlace habilitada en un puerto, el estado de enlace de ese puerto depende del estado de enlace de otro puerto. Por ejemplo, si el puerto A depende del puerto B y el switch detecta una pérdida de enlace en el puerto B, el switch automáticamente desactiva el enlace del puerto A. Cuando se restablece el enlace del puerto B, el switch automáticamente restablece el enlace del puerto A.

Configurar un grupo de dependencia de enlace

Para configurar un grupo de dependencia de enlace:

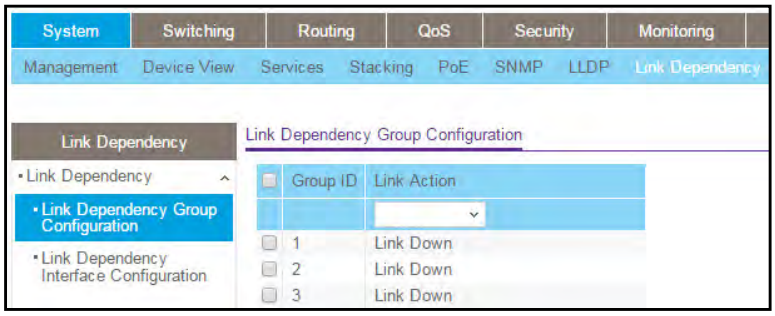
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Link Dependency > Link Dependency Group Configuration.



5. Seleccione la opción Group ID cuyos datos desea mostrar. El rango de Group ID es de 1 a 16.

6. En la lista Link Action, especifique la acción que se realizará en las interfaces descendentes cuando todas las interfaces de la lista ascendente se desactiven. El valor predeterminado es Link Down.

   a. Link Down — Cuando todas las interfaces ascendentes están inactivas, todas las descendentes se desactivan. Cuando cualquiera de las interfaces ascendentes está activa, todas las descendentes se activan.

   b. Link Up — Cuando todas las interfaces ascendentes están inactivas, todas las descendentes se activan. Cuando cualquiera de las interfaces ascendentes está activa, todas las descendentes se desactivan.

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

Configurar una interfaz de dependencia de enlace

Para configurar una interfaz de dependencia de enlace:

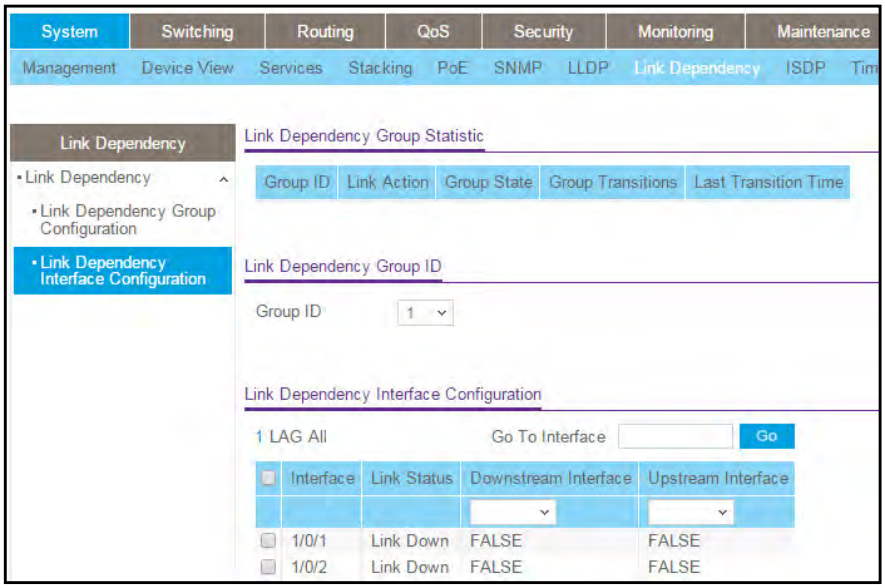
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Link Dependency > Link Dependency Interface Configuration.



5. En la sección Link Dependency Group ID de la página, use el menú Group ID para seleccionar el ID de grupo cuyos datos desea mostrar o configurar.

   El rango de Group ID es de 1 a 16.

6. Para hacer cambios, haga lo siguiente:
   - Haga clic en el botón Clear para quitar todas las interfaces del grupo especificado.
   - Haga clic en el botón Refresh para actualizar la página con la información más reciente del switch.

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

8. En la sección Link Dependency Interface Configuration de la página, seleccione qué interfaces se muestran:
   - Use LAG para mostrar solo los LAG.
   - Use All para mostrar todos los puertos físicos y LAG.
9. Use uno de los siguientes métodos para seleccionar una interfaz:
   - Use el campo Go To Interface ingresando la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go. Se selecciona la entrada de la interfaz especificada.
   - Use Interface para seleccionar la interfaz cuyos datos desea mostrar o configurar.
10. En el campo Downstream Interface, especifique si la interfaz pertenece a la lista descendente del grupo.

    Una interfaz definida como ascendente no se puede definir como descendente en el mismo grupo de estado de enlace. El valor predeterminado es False.

   - Seleccione False para quitar una interfaz de la lista descendente del grupo especificado.
   - Seleccione True para agregar una interfaz a la lista descendente del grupo especificado.
11. En el campo Upstream Interface, especifique si la interfaz pertenece a la lista ascendente del grupo.

    Una interfaz definida como ascendente no se puede definir como descendente en el mismo grupo de estado de enlace. El valor predeterminado es False.

   - Seleccione False para quitar una interfaz de la lista ascendente del grupo especificado.
   - Seleccione True para agregar una interfaz a la lista ascendente del grupo especificado.
12. Haga clic en el botón Apply.
Se guarda la configuración.
13. Haga clic en el botón Refresh para actualizar la página con la información más reciente del switch.

La siguiente tabla describe la información no configurable de Link Dependency Interface Configuration que se muestra en la página.

Tabla 53. Campo no configurable de Link Dependency Interface Configuration

Campo	Descripción
Estado del enlace	Indica si el enlace de la interfaz correspondiente está activo o inactivo.

La siguiente tabla describe la información no configurable de Link Dependency Group Statistic que se muestra en la página.

Tabla 54. Estadísticas del grupo de dependencia de enlace

Campo	Descripción
ID de grupo	ID del grupo cuyos datos se muestran. 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.

Tabla 54. Estadísticas del grupo de dependencia de enlace (continuación)

Campo	Descripción
Estado del grupo	Estado actual del grupo.
Transiciones del grupo	Indica el número de transiciones del grupo.
Hora de la última transición	Indica la hora de la última transición del grupo.

Configurar ISDP

Puede configurar los ajustes globales y de interfaz de ISDP.

Configurar los ajustes globales básicos de ISDP

Para configurar los ajustes globales básicos de ISDP:

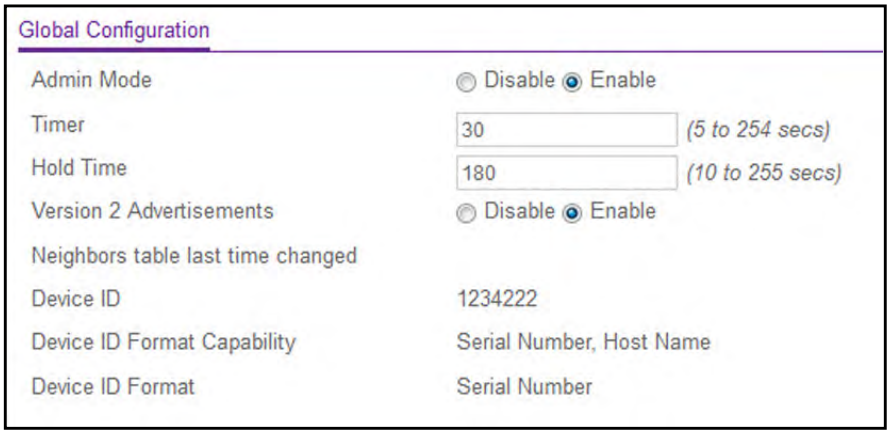
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > ISDP > Basic > Global Configuration.



5. Seleccione el botón de opción Admin mode Disable o Enable.

   Esto especifica si el servicio ISDP está habilitado o deshabilitado. El valor predeterminado es Enabled.

6. Use Timer para especificar el período entre envíos de paquetes ISDP nuevos. El rango es de 5 a 254 segundos. El valor predeterminado es 30 segundos.
7. Use Hold Time para especificar 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.

8. Seleccione el botón de opción Version 2 Advertisements Disable o Enable.

   Esto habilita o deshabilita el envío de paquetes ISDP versión 2 desde el dispositivo. El valor predeterminado es Enabled.

9. Haga clic en el botón Apply.
Se guarda la configuración.
La siguiente tabla describe los campos de ISDP Basic Global Configuration.

Tabla 55. Configuración global básica de ISDP

Campo	Descripción
Último cambio de la tabla de vecinos	Especifica si
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 globales de ISDP

Para configurar los ajustes globales de ISDP:

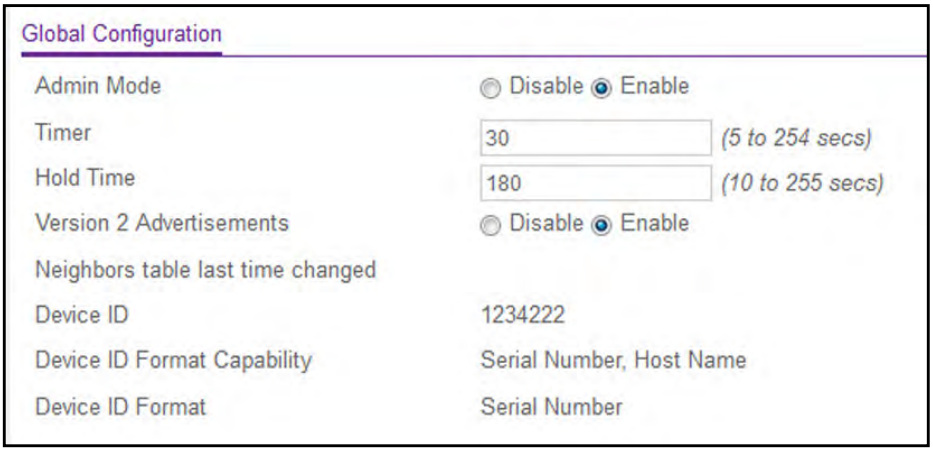
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > ISDP > Advanced > Global Configuration.



5. Seleccione el botón de opción Admin mode Disable o Enable.

   Esto especifica si el servicio ISDP está habilitado o deshabilitado. El valor predeterminado es Enable.

6. En el campo Timer, especifique el período entre envíos de paquetes ISDP nuevos. El rango es de 5 a 254 segundos. El valor predeterminado es 30 segundos.
7. 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.

8. Seleccione el botón de opción Version 2 Advertisements Disable o Enable.

   Esto habilita o deshabilita el envío de paquetes ISDP versión 2 desde el dispositivo. El valor predeterminado es Enable.

9. Haga clic en el botón Apply.
Se guarda la configuración.
La siguiente tabla describe los campos de ISDP Advanced Global Configuration.

Tabla 56. Configuración global avanzada de ISDP

Campo	Descripción
Último cambio de la tabla de vecinos	Muestra cuándo cambió por última vez 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 una interfaz ISDP

Para configurar una interfaz ISDP:

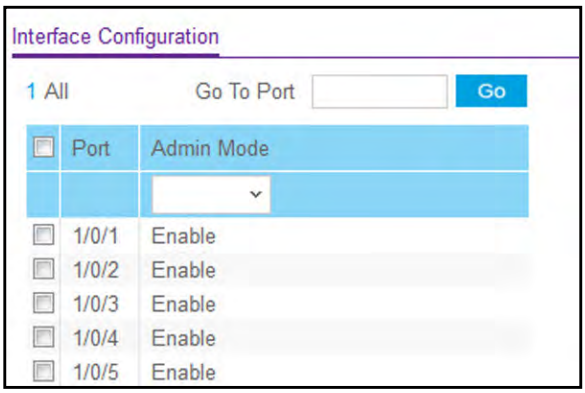
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > ISDP > Advanced > Interface Configuration.



5. Use Port para seleccionar el puerto en el que se configura el modo administrativo.
6. Use Admin mode para habilitar o deshabilitar ISDP en el puerto. El valor predeterminado es Enable.
7. Haga clic en el botón Apply.
Se guarda la configuración.

Ver un vecino ISDP

Para ver un vecino ISDP:

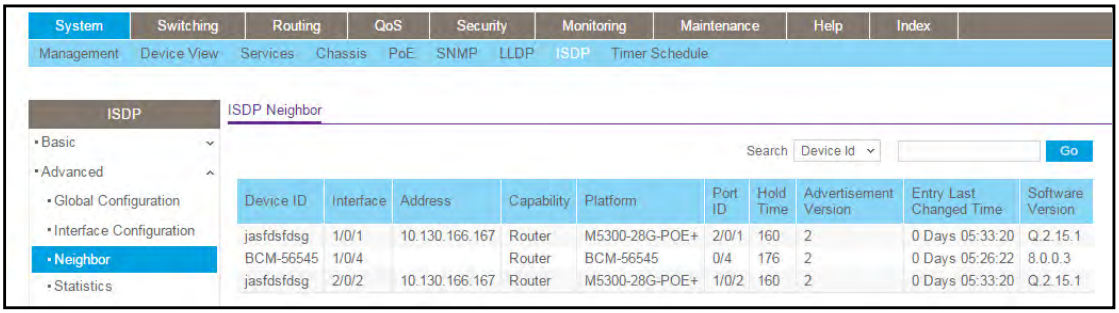
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > ISDP > Advanced > Neighbor.



La siguiente tabla describe los campos de ISDP Neighbor.

Tabla 57. Vecino ISDP

Campo	Descripción
ID de dispositivo	ID de dispositivo del vecino ISDP.
Interfaz	Interfaz en la que se detectó el vecino.
Dirección	Dirección del vecino.
Capacidad	Capacidad del vecino. Se admiten las siguientes: • Router • Trans Bridge • Source Route • Switch • Host • IGMP • Repeater
Plataforma	Tipo de modelo del vecino. (0 a 32)
ID de puerto	ID de puerto del vecino.
Tiempo de retención	Tiempo de retención de los paquetes ISDP que transmite el vecino.
Versión de anuncio	Versión de ISDP que envía el vecino.
Hora del último cambio de entrada	Tiempo transcurrido desde el último cambio de la entrada.
Versión de software	Versión de software del vecino.

Ver las estadísticas de ISDP

Para ver las estadísticas de ISDP:

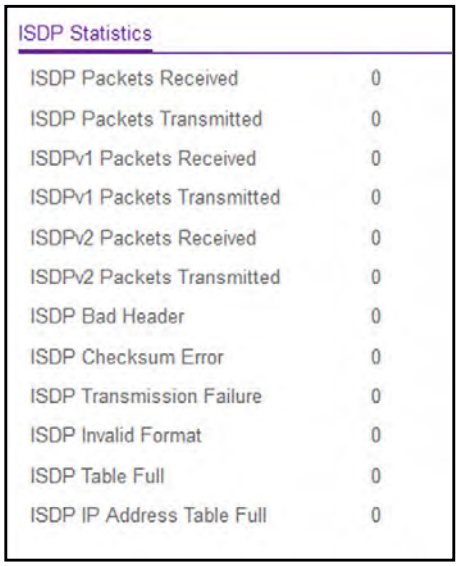
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > ISDP > Advanced > Statistics.



La siguiente tabla describe los campos de ISDP Statistics.

Tabla 58. Estadísticas de ISDP

Campo	Descripción
Paquetes ISDP recibidos	Paquetes ISDP recibidos, incluidos los paquetes ISDPv1 e ISDPv2.
Paquetes ISDP transmitidos	Paquetes ISDP transmitidos, incluidos los paquetes ISDPv1 e ISDPv2.
Paquetes ISDPv1 recibidos	Paquetes ISDPv1 recibidos.
Paquetes ISDPv1 transmitidos	Paquetes ISDPv1 transmitidos.
Paquetes ISDPv2 recibidos	Paquetes ISDPv2 recibidos.
Paquetes ISDPv2 transmitidos	Paquetes ISDPv2 transmitidos.

Tabla 58. Estadísticas de ISDP (continuación)

Campo	Descripción
Encabezado ISDP incorrecto	Paquetes ISDP incorrectos recibidos.
Error de suma de verificación ISDP	Número de errores de suma de verificación.
Falla de transmisión ISDP	Número de fallas de transmisión.
Formato ISDP no válido	Número de paquetes ISDP con formato no válido recibidos.
Tabla ISDP llena	Tamaño de la tabla ISDP.
Tabla de direcciones IP ISDP llena	Tamaño de la tabla de direcciones IP de ISDP.

Administrar programaciones de temporizador

Puede configurar los ajustes globales del temporizador y crear programaciones de temporizador.

Configurar los ajustes globales del temporizador

Para agregar o eliminar una programación de temporizador global:

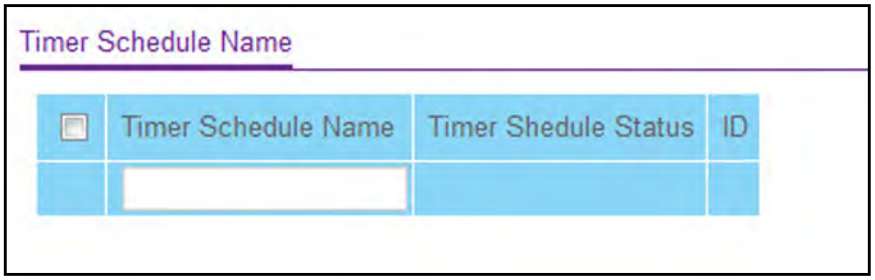
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Timer Schedule > Basic > Global Configuration.



5. Use Timer Schedule Name para especificar el nombre de una programación de temporizador.

6. Realice una de las siguientes acciones:

   - Haga clic en el botón Add.

Se agrega la programación de temporizador.

- Haga clic en el botón Delete.

  Se elimina la programación de temporizador.

Configurar la programación de temporizador

Para configurar la programación de temporizador:

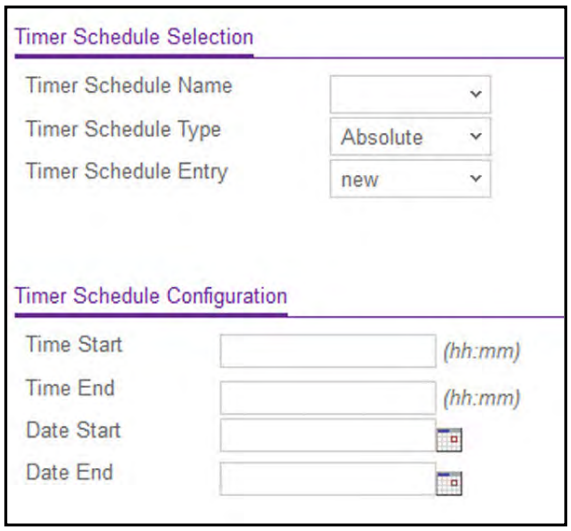
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Services > Timer Schedule > Advanced > Schedule Configuration.



5. En la lista Timer Schedule Name, seleccione la programación de temporizador.

6. En la lista Timer Schedule Type, seleccione Absolute o Periodic.

7. En la lista Timer Schedule Entry, seleccione el número de entradas de programación que desea configurar o agregar.

   Si va a agregar una entrada, seleccione new.

8. En el campo Time Start, ingrese la hora del día en formato (HH:MM) en que se inicia la operación programada.

   Este campo es obligatorio. Si no se especifica una hora, la programación no se ejecuta.

9. En el campo Time End, ingrese la hora del día en formato (HH:MM) en que termina la operación programada.

10. Use Date Start para establecer la fecha de inicio de la programación. Si no se especifica una fecha, la programación se ejecuta de inmediato.
11. Use Date Stop para establecer la fecha de terminación de la programación. Si se selecciona No End Date, la programación funciona indefinidamente.
12. Use Recurrence Pattern para indicar con qué periodicidad se repite el evento.

Si no se necesita recurrencia (la programación debe activarse una sola vez), establezca Date Stop igual a Date Start. Los valores posibles de recurrencia son los siguientes:

- Daily. La programación funciona con recurrencia diaria

  Modo diario. La opción Every WeekDay significa que la programación se activa cada día de lunes a viernes. La opción Every Day(s) significa que se activa cada número definido de días. Si no se especifica el número de días, la programación se activa todos los días.

- Weekly. La programación funciona con recurrencia semanal
  - Every Week(s). Defina cada cuántas semanas se activa la programación. Si no se especifica el número de semanas, la programación se activa cada semana.
  - WeekDay. Especifique los días de la semana en que funciona la programación.
- Monthly. La programación funciona con recurrencia mensual

  Modo mensual. Indique el día del mes en que se activa la programación. El campo Every Month(s) significa que la programación se activa cada número definido de meses.

13. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

3

3Administrar el apilamiento

Este capítulo trata los siguientes temas:

- Descripción general del apilamiento de switches de la serie M4300
- Sincronización y actualización del firmware
- Mantenimiento de la configuración de la pila
- Elección del maestro de la pila
- Comportamiento del restablecimiento a valores de fábrica de la pila
- NSF de la pila
- Configurar una pila
- Ejecutar el diagnóstico de puertos de apilamiento
- Configurar la sincronización del firmware de la pila
- Ver los datos de resumen de NSF
- Ver las estadísticas de puntos de control de NSF

Descripción general del apilamiento de switches de la serie M4300

Un switch apilable es un switch totalmente funcional como unidad independiente, pero que también se puede configurar para funcionar junto con hasta otros siete switches. Este grupo de switches se comporta como un solo switch, con la capacidad de puertos de la suma de los switches combinados.

Uno de los switches de la pila controla su funcionamiento. Este switch se llama maestro de la pila. Los demás switches de la pila son miembros de la pila. Los miembros usan tecnología de apilamiento para funcionar juntos como un sistema unificado. Los protocolos de capa 2 y superiores presentan toda la pila de switches como una sola entidad ante la red.

El maestro de la pila es el único punto de administración de toda la pila. Desde el maestro, se configura lo siguiente:

- Funciones a nivel de sistema (globales) que se aplican a todos los miembros de la pila
- Funciones a nivel de interfaz para todas las interfaces de cualquier miembro de la pila

Una pila de switches se identifica en la red por su dirección IP de red. La dirección IP de red se asigna según la dirección MAC del maestro de la pila. Cada miembro de la pila se identifica de forma única con su propio número de miembro, de 1 a 8. El maestro de la pila puede tener cualquier número dentro de ese rango.

El apilamiento admite lo siguiente:

- Hasta ocho switches por pila
- Administración con una sola dirección IP mediante navegador web, CLI o SNMP.
- Configuración maestro-esclavo:
  - El maestro conserva la configuración de toda la pila.
  - Detección automática de nuevos miembros, con sincronización del firmware (actualización o degradación según sea necesario).
- Actualizaciones de configuración en toda la pila mediante una sola operación.
- Conmutación por error automática del maestro. Pila totalmente resiliente con topología en cadena y en anillo.
- Intercambio en caliente (inserción y extracción) de miembros de la pila.

Sincronización y actualización del firmware

Todos los miembros de la pila deben ejecutar la misma versión de software para garantizar la compatibilidad dentro de la pila. De forma predeterminada, si se agrega una unidad a la pila y su versión de software no es la misma que la del maestro de la pila, no se permite que esa unidad se una a la pila. Puede habilitar la función Stack Firmware Auto Upgrade, que sincroniza automáticamente la versión de firmware de la nueva unidad con la versión que se ejecuta en el maestro de la pila. La operación de sincronización puede resultar en una actualización o en una reversión del firmware del miembro de la pila con versión distinta.

Actualizar el firmware de una pila de switches es igual que actualizar el firmware de un solo switch. Después de descargar una nueva imagen con la página File Download o SCC, la imagen descargada se distribuye a todas las unidades conectadas de la pila.

Nota: Le recomendamos establecer la imagen activa de todos los miembros de la pila igual que la imagen activa del maestro de la pila. Es decir, si image1 es la imagen activa en el maestro de la pila, todas las unidades deben usar image1 como imagen activa. Para obtener información sobre cómo configurar la imagen activa, consulte Configurar los ajustes de imagen doble en la página 688.

Mantenimiento de la configuración de la pila

El maestro de la pila almacena y mantiene los archivos de configuración guardada y en ejecución de la pila de switches. Los archivos de configuración incluyen los ajustes a nivel de sistema de la pila y los ajustes a nivel de interfaz de todos los miembros de la pila. Cada miembro conserva una copia del archivo guardado como respaldo. Si el maestro se retira de la pila o deja de estar disponible, se elige a otro miembro como maestro, que entonces funciona con esa configuración guardada.

El maestro copia su configuración en ejecución al miembro de la pila configurado como unidad de reserva cada vez que cambia (con algunas restricciones para reducir la carga). Esto permite que la unidad de reserva asuma el funcionamiento de la pila con una interrupción mínima si el maestro de la pila deja de estar disponible. La sincronización de running-config también ocurre cuando la configuración en ejecución se guarda automáticamente en el maestro de la pila o cuando cambia la unidad de reserva.

Elección del maestro de la pila

Todos los miembros de la pila pueden ser maestros. Si el maestro de la pila deja de estar disponible, los miembros restantes participan en la elección de un nuevo maestro entre ellos. Los siguientes factores determinan qué switch se elige como maestro de la pila:

- El switch que es maestro siempre tiene prioridad para conservar la función de maestro.
- Prioridad asignada.
- Dirección MAC.

Cuando la pila se enciende y completa el proceso de arranque, o cuando el maestro original de la pila deja de estar disponible, el maestro de la pila se determina mediante un proceso de elección.

Las reglas para la elección del maestro de la pila son las siguientes:

- Si una unidad se eligió anteriormente como maestro de la pila, sigue siendo el maestro y las demás unidades son miembros de la pila.

- Si ninguna unidad era maestro de la pila, o más de una unidad era maestro, se elige como maestro la unidad con la mayor preferencia de administración. El administrador puede asignar la preferencia de administración. Sin embargo, si a todas las unidades se les asigna la misma preferencia de administración, se asigna como maestro de la pila la unidad con la dirección MAC más alta.

Comportamiento del restablecimiento de fábrica de la pila

Si el maestro de la pila se restablece a la configuración predeterminada de fábrica (consulte Restablecer el switch a su configuración predeterminada de fábrica en la página 676), el maestro aplica la configuración predeterminada a todos los miembros y restablece la pila, incluidos todos los miembros participantes. Cuando la pila arranca, comienza el proceso de elección del maestro de la pila.

Un switch puede describirse en términos de tres funciones semiindependientes llamadas plano de reenvío, plano de control y plano de administración. El plano de reenvío reenvía los paquetes de datos. El plano de reenvío se implementa en hardware. El plano de control es el conjunto de protocolos que determinan cómo el plano de reenvío reenvía los paquetes, decidiendo qué paquetes de datos se pueden reenviar y hacia dónde van. El software de aplicación de la unidad de administración actúa como plano de control. El plano de administración es el software de aplicación que se ejecuta en la unidad de administración y que proporciona interfaces que permiten a un administrador de red configurar y supervisar el dispositivo.

NSF de la pila

El reenvío ininterrumpido (NSF) permite que el plano de reenvío de las unidades de la pila siga reenviando paquetes mientras los planos de control y administración se reinician a causa de una falla de energía, falla de hardware o falla de software en la unidad de administración. Una conmutación por error con reenvío ininterrumpido también puede iniciarse manualmente haciendo clic en el botón Initiate Failover de la página NSF Summary. Los flujos de tráfico que entran y salen de la pila por puertos físicos de una unidad distinta de la de administración continúan con una interrupción de menos de un segundo como máximo cuando falla la unidad de administración.

Para preparar la unidad de administración de respaldo en caso de una conmutación por error, las aplicaciones de la unidad de administración envían continuamente puntos de control de cierta información de estado a la unidad de respaldo. Los cambios en la configuración en ejecución se copian automáticamente a la unidad de respaldo. Las direcciones MAC se mantienen durante una conmutación por error con reenvío ininterrumpido, de modo que los vecinos no necesitan volver a aprenderlas.

Cuando ocurre una conmutación por error con reenvío ininterrumpido, el plano de control de la unidad de respaldo arranca desde un estado parcialmente inicializado y aplica la información de estado de los puntos de control. Mientras el plano de control se inicializa, la pila no puede reaccionar a cambios externos, como cambios en la topología de la red. Una vez que el plano de control está totalmente operativo en la nueva unidad de administración, el plano de control garantiza que el estado del hardware se actualice según sea necesario. El tiempo de conmutación del plano de control depende del tamaño de la pila, la complejidad de la configuración y la velocidad de la CPU.

El plano de administración se reinicia cuando ocurre una conmutación por error. Las conexiones de administración deben restablecerse.

Para que NSF sea eficaz, los dispositivos de red adyacentes no deben redirigir el tráfico evitando el dispositivo que se reinicia. El switch usa tres técnicas para evitar que el tráfico se redirija:

- Un protocolo puede distribuir parte de su plano de control a las unidades de la pila para que el protocolo pueda aparentar que sigue funcionando durante el reinicio. Spanning tree y los port channels usan esta técnica.
- Un protocolo puede obtener la cooperación de sus vecinos mediante una técnica conocida como reinicio ordenado (graceful restart). OSPF usa graceful restart si está habilitado.
- Un protocolo puede reiniciarse después de la conmutación por error si los vecinos reaccionan con suficiente lentitud como para no detectar normalmente la interrupción. Los protocolos de enrutamiento multicast IP son un buen ejemplo de este comportamiento.

Para aprovechar al máximo el reenvío ininterrumpido, las conexiones de capa 2 con los vecinos deben ser a través de port channels que abarquen dos o más unidades de la pila, y las rutas de capa 3 deben ser rutas ECMP con siguientes saltos a través de puertos físicos de dos o más unidades. El hardware puede mover rápidamente los flujos de tráfico de los miembros de port channel o las rutas ECMP de una unidad con falla a una unidad que sigue funcionando.

Configurar una pila

Puede mover la funcionalidad de unidad de administración principal de una unidad a otra. Al ejecutarse, toda la pila (incluidas todas las interfaces de la pila) se desconfigura y se reconfigura con la configuración de la nueva unidad de administración principal. Una vez completada la recarga, toda la administración de la pila debe realizarse en la nueva unidad de administración principal. Para conservar la configuración actual durante un traslado de la pila, guarde la configuración actual en la NVRAM antes de realizar el traslado. Un traslado de la pila hace que se pierdan todas las rutas y direcciones de capa 2. Se le pide al administrador que confirme el traslado de la administración.

Seleccionar un nuevo maestro de la pila

Para seleccionar un nuevo maestro de la pila:

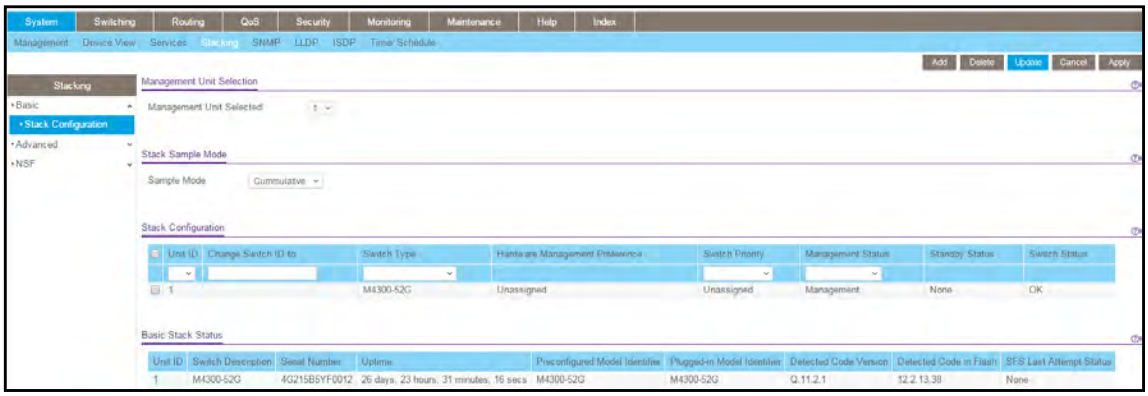
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Stacking > Basic > Stack Configuration.



El menú Management Unit Selected muestra la unidad de administración principal actual.

5. Para cambiar la unidad de administración principal, seleccione otro ID de unidad del miembro de la pila que se convertirá en maestro.

Se muestra un mensaje para notificarle que mover la administración de la pila desconfigura toda la pila, incluidas todas las interfaces.
6. Haga clic en el botón OK para confirmar la selección y recargar la pila.
La pila no está disponible hasta que se completa el proceso de arranque.

Especificar el modo de muestreo de la pila

Para especificar el modo de muestreo de la pila:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Stacking > Basic > Stack Configuration.

Use la sección Stack Sample mode de la página para configurar el modo global de administración de estado y el tamaño de muestra. Los parámetros de modo y tamaño de muestra se aplican globalmente a todas las unidades de la pila.

5. En la lista Sample mode, seleccione una de las siguientes opciones:

- Cumulative. Registra la suma acumulada de los desfases de marca de tiempo recibidos.
- History. Registra el historial de las marcas de tiempo recibidas.

6. En el campo Max Samples, configure el número máximo de muestras que se conservarán. El rango válido es de 100 a 500.
7. Haga clic en el botón Apply.
La configuración se guarda.

Configurar un miembro de la pila

Para configurar un miembro de la pila antes de agregarlo a la pila:

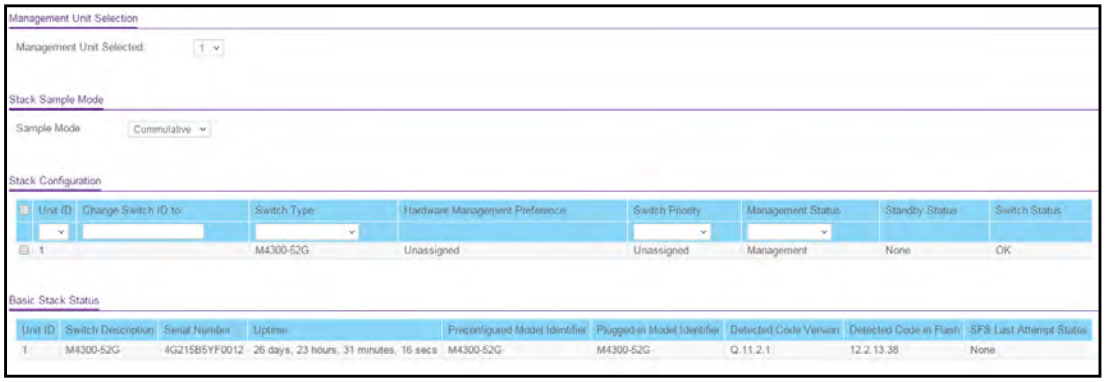
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Stacking > Stack Configuration.



5. Seleccione el Unit ID del miembro de la pila que desea agregar.
6. Seleccione el número de modelo del switch de la nueva unidad en el campo Switch Type.

7. Opcionalmente, especifique Switch Priority para seleccionar si esta unidad se convierte en unidad de administración con preferencia sobre otra unidad.

   El valor predeterminado de este ajuste es indefinido. Si el nivel de preferencia se establece en cero, el dispositivo no puede convertirse en unidad de administración. Un valor más alto indica una prioridad más alta. El valor máximo es 15.

8. Use el campo Management Status para indicar si el switch seleccionado es el maestro de la pila, un miembro normal de la pila o la unidad de reserva.

   Una unidad de reserva asume las responsabilidades del maestro de la pila si el maestro deja de estar disponible.

9. Haga clic en el botón Add.
Se agrega la unidad preconfigurada a la pila.

Cambiar la configuración de un miembro existente de la pila

Para cambiar la configuración de un miembro existente de la pila:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Stacking > Stack Configuration.

Se muestra la página Stack Configuration.
5. Marque la casilla junto al miembro de la pila que desea configurar.
6. Si lo desea, especifique un nuevo ID de unidad para el miembro de la pila en el campo Change to Switch ID. El proceso de renumeración hace que la unidad se recargue.
7. Especifique el tipo de switch, la prioridad o el estado de administración en los campos disponibles.
8. Haga clic en el botón Apply (Aplicar).
Se guardan los cambios del miembro de la pila.

Nota: Si configuró un nuevo número de unidad para un miembro existente de la pila, se le pedirá que confirme el cambio. Haga clic en el botón OK para continuar o en el botón Cancel para conservar la configuración original.

9. Para hacer otros cambios, haga lo siguiente:
   - Para quitar la unidad seleccionada de la pila, haga clic en el botón Delete.
   - Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

Nota: Si agrega o quita una unidad ficticia con PoE para preconfiguración, debe volver a iniciar sesión en una sesión web real para aplicar los cambios y ver las páginas web de PoE correspondientes.

10. Si hizo algún cambio, haga clic en el botón Apply. La configuración se guarda.

La siguiente tabla describe los campos no configurables de Stack Configuration.

Tabla 59. Stack Configuration

Campo	Descripción
Hardware Management Preference	La preferencia de administración de hardware del switch. La preferencia de administración de hardware puede estar deshabilitada o sin asignar.
Standby Status	Identifica el switch configurado como unidad de reserva. Los valores posibles son los siguientes: • Cfg Standby. Indica que la unidad está configurada como unidad de reserva. La unidad configurada como switch de reserva se convierte en administrador de la pila si falla el administrador actual. • Opr Standby. Indica que esta unidad opera como unidad de reserva y que la unidad de reserva configurada no forma parte de la pila. • None. El switch no está configurado como unidad de reserva.
Switch Status	El estado de la unidad seleccionada. Los valores posibles son los siguientes: • OK. La unidad está conectada y funciona correctamente. • Unsupported. El tipo de unidad insertada no es compatible. • Code Mismatch. La versión de firmware no es idéntica a la de la unidad maestra o de administración. • Config Mismatch. El tipo de dispositivo insertado es diferente de los dispositivos configurados. • Not Present. La unidad no está conectada. • SDM Mismatch. La plantilla SDM no coincide. • Updating Code. Hay una actualización de firmware en curso. • STM Mismatch. La plantilla STM no coincide.

La siguiente tabla describe la información no configurable de Stack Status que se muestra.

Tabla 60. Campos no configurables de Stack Status

Campo	Descripción
Hardware Management Preference	La preferencia de administración de hardware del switch, que puede estar deshabilitada o sin asignar.
Standby Status	Identifica el switch configurado como unidad de reserva: • Cfg Standby. La unidad está configurada como unidad de reserva. La unidad configurada como switch de reserva se convierte en administrador de la pila si falla el administrador actual. • Opr Standby. Esta unidad opera como unidad de reserva y la unidad de reserva configurada no forma parte de la pila. • None. El switch no está configurado como unidad de reserva.

Tabla 60. Campos no configurables de Stack Status (continuación)

Campo	Descripción
Switch Status	El estado de la unidad seleccionada. Los valores posibles son los siguientes: • OK. La unidad está conectada y funciona correctamente. • Unsupported. El tipo de unidad insertada no es compatible. • Code Mismatch. La versión del código no es idéntica a la de la unidad maestra/de administración. • Config Mismatch. El tipo de dispositivo insertado es diferente de los dispositivos configurados. • Not Present. La unidad no está conectada. • SDM Mismatch. La plantilla SDM no coincide. • Updating Code. Hay una actualización de código en curso. • STM Mismatch. La plantilla STM no coincide.
Unit ID	El ID de unidad del switch específico.
Switch Description	La descripción de la unidad configurada por el usuario.
Serial Number	El número de serie único del equipo para este switch.
Up Time	El tiempo relativo desde el último reinicio del switch.
Preconfigured Model Identifier	El tipo de modelo asignado por el fabricante del dispositivo para identificar el dispositivo.
Plugged-In Model Identifier	El tipo de modelo asignado por el fabricante del dispositivo para identificar el dispositivo conectado.
Detected Code Version	La versión de código detectada en esta unidad.
Detected Code in Flash	El número de versión principal y el número de versión del código almacenado en la memoria flash.
SFS Last Attempt Status	El estado del último intento de sincronización del firmware de la pila.

Configurar el modo de los puertos de pila

De forma predeterminada, los puertos de pila de cada switch están configurados para apilamiento. Sin embargo, puede usar estos puertos como puertos Ethernet estándar. Use la página Stack Port Configuration para configurar el modo de los puertos de pila y ver información sobre los puertos.

Para configurar el modo de los puertos de pila:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

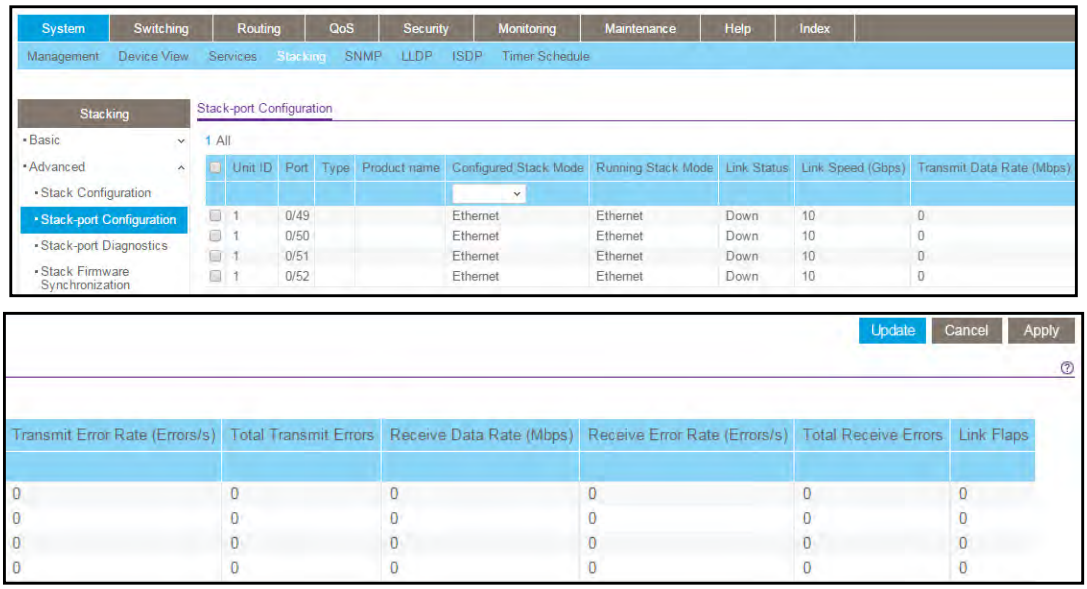
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione System > Stacking > Advanced > Stack Port Configuration.

La página se muestra en dos partes.



5. Marque la casilla asociada con la unidad y el puerto que desea configurar:

6. En el campo Configured Stack mode, seleccione el modo de funcionamiento del puerto, que puede ser:

- Stack. El puerto se conecta al puerto de pila de otro miembro de la pila. Este es el valor predeterminado para el modo de pila del panel posterior.
- Ethernet. El puerto funciona como un puerto de switch estándar que recibe y transmite tráfico de red. Este es el valor predeterminado para el modo de pila del panel frontal.

7. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe los campos de Stack Port Configuration.

Tabla 61. Stack Port Configuration

Campo	Descripción
Unit ID	La unidad.
Port	Las interfaces apilables de la unidad indicada.
Slot ID	El ID de ranura con el formato unidad/ranura.
Type	El tipo de interfaces apilables de la unidad indicada.
Product Name	El nombre del adaptador XFP/SFP+.
Running Stack mode	El modo de ejecución de la interfaz apilable.
Link Status	El estado del enlace (UP/DOWN) del puerto.

Tabla 61. Stack Port Configuration (continuación)

Campo	Descripción
Link Speed (Gbps)	La velocidad máxima del puerto de apilamiento.
Transmit Data Rate (Mbps)	La tasa de transmisión aproximada en el puerto de apilamiento.
Transmit Error Rate	El número de errores en los paquetes transmitidos por segundo.
Total Transmit Errors	El número total de errores en los paquetes transmitidos desde el arranque. El contador puede reiniciarse al desbordarse.
Receive Data Rate (Mbps)	La tasa de recepción aproximada en el puerto de apilamiento.
Receive Error Rate	El número de errores en los paquetes recibidos por segundo.
Total Receive Errors	El número total de errores en los paquetes recibidos desde el arranque. El contador puede reiniciarse al desbordarse.
Link Flaps	El número total de oscilaciones del enlace.

Ejecutar el diagnóstico de los puertos de pila

Para ejecutar el diagnóstico de los puertos de pila:

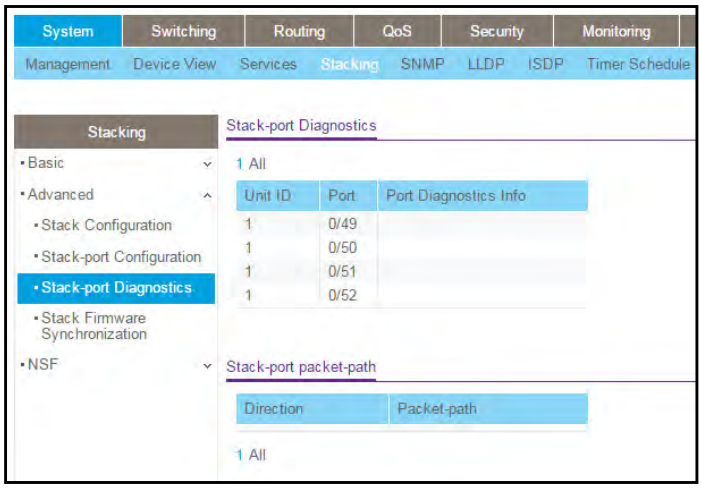
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Stacking > Advanced > Stack Port Diagnostics.



5. Seleccione Unit ID para mostrar la ruta de paquetes a partir de la unidad seleccionada.
6. Seleccione All para mostrar la ruta de paquetes de todas las unidades de la pila.
7. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe los campos de Stack Port Diagnostics.

Tabla 62. Stack Port Diagnostics

Campo	Definición
Unit ID	La unidad.
Port	La interfaz apilable de la unidad indicada.
Port Diagnostics Info	Muestra tres campos de texto (cadenas de 80 caracteres) completados por el controlador con información de depuración y estado.

La siguiente tabla describe los campos no configurables de Stack Port Packet Path.

Tabla 63. Stack Port Packed Path

Campo	Definición
Direction	La dirección de la ruta.
Packet Path	La ruta de paquetes.

Configurar la sincronización del firmware de la pila

Para configurar las funciones de sincronización del firmware de la pila:

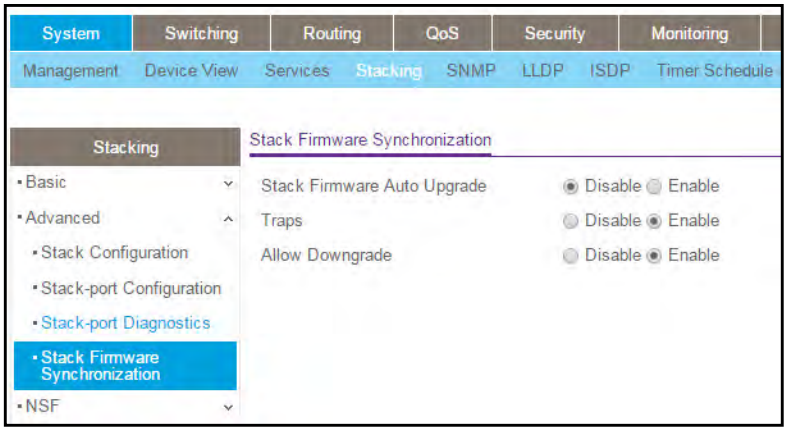
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Stacking > Advanced > Stack Firmware Synchronization.



5. Especifique si Stack Firmware Auto Upgrade está habilitado o deshabilitado.

Esta función determina qué hacer cuando un nuevo miembro intenta unirse a la pila y su firmware no coincide con la versión que se ejecuta en el maestro.

- Enable. El maestro de la pila actualiza la versión del nuevo miembro para que coincida con la versión que se ejecuta en el resto de la pila.
- Disable. No se permite que el nuevo miembro se una.

6. Use el campo Traps para habilitar o deshabilitar el envío de traps al iniciar, fallar o finalizar la sincronización del firmware de la pila.

7. Use el campo Allow Downgrade para determinar si el maestro de la pila revierte la versión de firmware de un nuevo miembro que intenta unirse a la pila si el nuevo miembro tiene una versión de firmware más reciente que la de la pila.

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

Ver los datos de NSF Summary

Para mostrar los datos de NSF Summary:

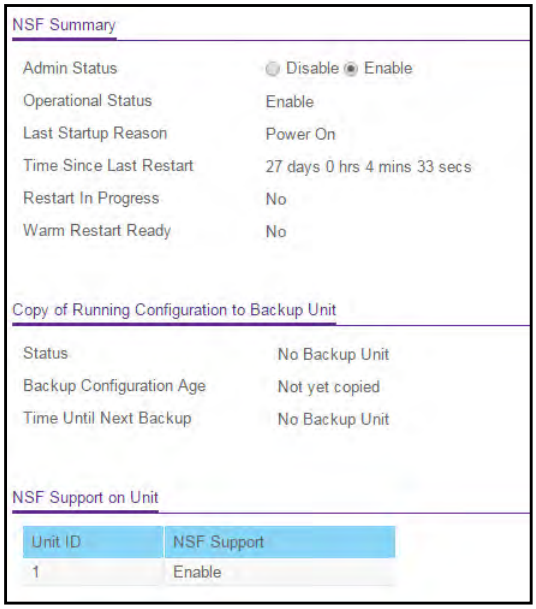
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione System > Stacking > NSF > NSF Summary



5. Use el botón de opción Admin Status para habilitar o deshabilitar la función NSF en la pila. Cuando está habilitada, la pila selecciona una unidad de respaldo. Las aplicaciones de la unidad de administración copian datos a la unidad de respaldo.
6. Para que la unidad supervisora conmute por error a la unidad de respaldo, haga clic en el botón Initiate Failover en la esquina superior derecha de la página.
7. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

La siguiente tabla describe los datos no configurables de NSF Summary que se muestran.

Tabla 64. NSF Summary

Campo	Descripción
Operational Status	Indica si NSF está habilitado en el chasis. NSF está habilitado de forma predeterminada.
Last Startup Reason	El tipo de activación que hizo que el software se iniciara la última vez. Los valores posibles son los siguientes: • Power On. El switch se reinició. Un ciclo de encendido o un comando administrativo de recarga pudo causar esto • Cold Admin Move. El sistema restablece todas las tablas de hardware sin reiniciar y la aplicación comienza desde un estado preinicializado, pero no se conservan datos de antes de la conmutación por error. • Warm Admin Move. El administrador emitió un comando para que el administrador de reserva asuma el control. • Auto Warm. La tarjeta de administración principal se reinició debido a una falla y el sistema ejecutó una conmutación por error con reenvío ininterrumpido. • Auto Cold. El sistema cambió del administrador activo al administrador de respaldo y no pudo mantener el tráfico de datos de los usuarios. Esto suele deberse a varias fallas que ocurren casi al mismo tiempo.
Time Since Last Restart	Tiempo desde que la tarjeta de administración actual se convirtió en la tarjeta de administración activa. Para el administrador de respaldo, el valor se establece en 0d:00:00:00.
Restart In Progress	Indica si hay un reinicio en curso. Un reinicio no se considera completo hasta que todas las tablas de hardware se concilian por completo.
Warm Restart Ready	Indica si terminó el punto de control completo inicial.
Copia de la configuración en ejecución a la unidad de respaldo	
Status	Estado de la copia de la configuración en ejecución a los blades de respaldo.
Backup Configuration Age	Indica el tiempo transcurrido desde la última copia de la configuración en ejecución al blade de respaldo.
Time Until Next Backup	Indica los segundos que faltan para copiar la configuración en ejecución al blade de respaldo.
Compatibilidad con NSF en la unidad	
Unit ID	El número de ranura del blade.
NSF Support	Indica si el switch admite la función de reenvío ininterrumpido (NSF).

Ver las estadísticas de puntos de control de NSF

Para ver las estadísticas de puntos de control de NSF:

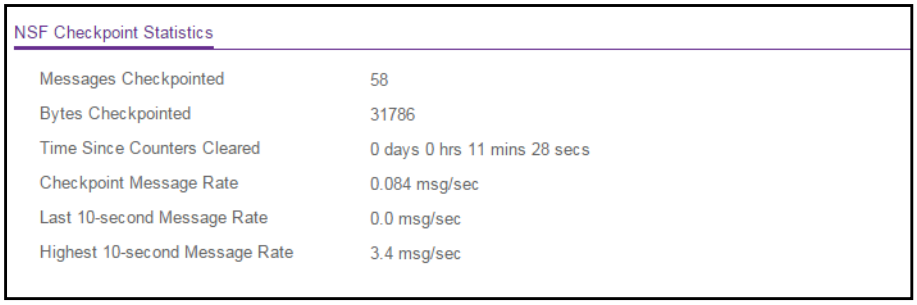
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione System > Chassis > NSF > Checkpoint Statistics.**



5. Para restablecer las estadísticas de la página, haga clic en el botón Borrar (Clear).
6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información no configurable que se muestra.

Tabla 65. Estadísticas de puntos de control de NSF

Campo	Descripción
Messages Checkpoint	El número de mensajes enviados del supervisor al blade de respaldo.
Bytes Checkpointed	La cantidad de datos enviados del supervisor al blade de respaldo.
Time Since Counters Cleared	El tiempo transcurrido desde que se restablecieron los contadores.
Checkpoint Message Rate	El número de segundos entre mediciones.
Last 10-second Message Rate	Cuántos mensajes se enviaron en el último intervalo de medición.
Highest 10-second Message Rate	El mayor número de mensajes enviados en un intervalo de medición.

4

4Configurar la información de conmutación

Este capítulo trata los siguientes temas:

- Configurar VLAN
- Configurar Auto-VoIP
- Configurar iSCSI
- Configurar Spanning Tree Protocol
- Administrar multicast
- Configurar MVR
- Buscar y administrar la tabla de direcciones MAC
- Administrar la configuración de puertos
- Administrar grupos de agregación de enlaces
- Administrar la configuración de Multiple Registration Protocol
- Administrar la protección contra bucles

Configurar VLAN

Agregar compatibilidad con LAN virtuales (VLAN) a un switch de capa 2 ofrece algunas 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 de la serie M4300 y de la familia M4300-96X 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.

Configurar los ajustes básicos de VLAN

La VLAN interna está reservada por una interfaz de enrutamiento basada en puerto y es invisible para el usuario final. Una vez que la interfaz de enrutamiento basada en puerto asigna estas VLAN internas, no se pueden asignar a una interfaz VLAN de enrutamiento.

Para configurar los ajustes de VLAN internas:

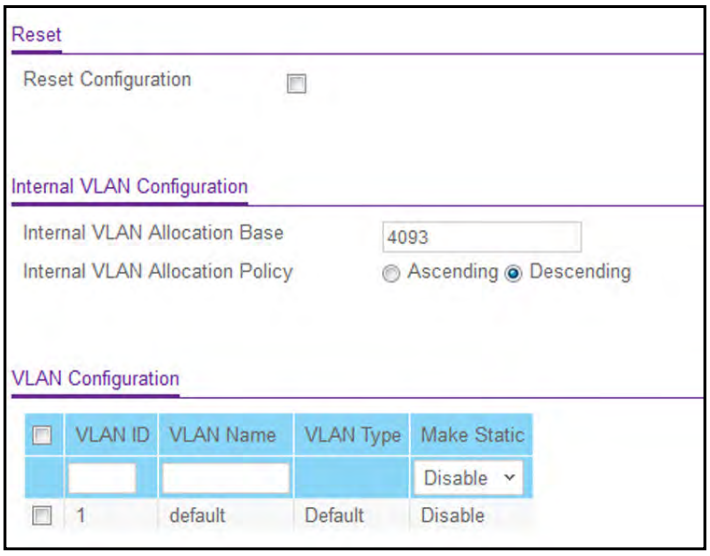
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Basic > VLAN Configuration.



5. Para restablecer la configuración de VLAN a los valores predeterminados, active la casilla Reset Configuration. 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 Ingress Filtering 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.

Se eliminan todas las VLAN, excepto la VLAN predeterminada.

6. Especifique los ajustes de VLAN internas.

La sección Internal VLAN Configuration muestra la base y el modo de asignación de las VLAN internas.

a. Use Internal VLAN Allocation Base para especificar la base de asignación de VLAN de la interfaz de enrutamiento.

El rango base predeterminado de la VLAN interna es de 1 a 4093.

b. Seleccione el botón de opción Ascending o Descending de Internal VLAN Allocation Policy.

Esto especifica una política de asignación de VLAN internas.

7. Use VLAN ID para especificar el identificador de la nueva VLAN.

El ID de VLAN va de 1 a 4093.

8. Use el campo opcional VLAN Name para especificar un nombre para la VLAN.

El nombre de la VLAN puede tener hasta 32 caracteres alfanuméricos, incluidos espacios. De forma predeterminada está en blanco. La VLAN ID 1 siempre usa el nombre Default.

El campo VLAN Type identifica el tipo de la VLAN que configura. No puede cambiar el tipo de la VLAN predeterminada (VLAN ID = 1): siempre es de tipo Default. Cuando crea una VLAN en esta página, su tipo siempre es Static. Una VLAN creada por registro GVRP usa inicialmente el tipo Dynamic. Al configurar una VLAN dinámica, puede cambiar su tipo a Static.

9. Haga clic en el botón Add.
La VLAN se agrega al switch.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Restablecer la configuración de VLAN a los valores predeterminados

Para restablecer la configuración de VLAN a los valores predeterminados:

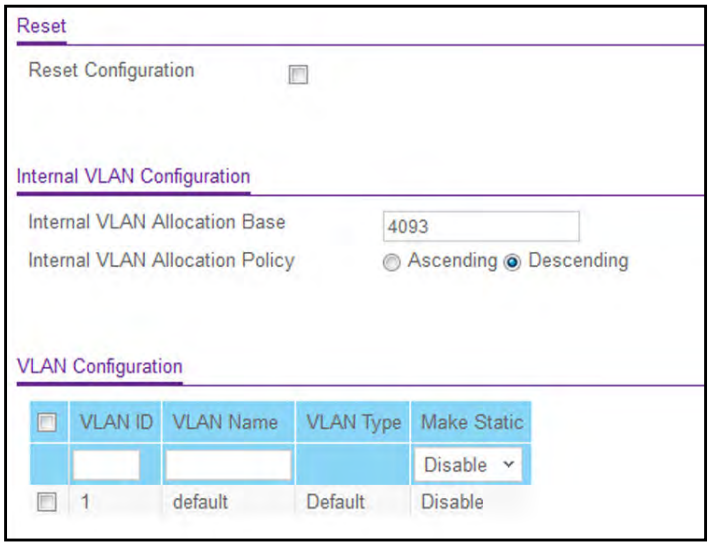
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > VLAN Configuration.



5. Active la casilla Reset Configuration.



ADVERTENCIA:

Si selecciona este botón y confirma su selección en la siguiente página, todos los parámetros de configuración de VLAN se restablecen a los valores de fábrica.

6. Confirme su selección.
Se eliminan todas las VLAN, excepto la VLAN predeterminada. 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.

Configurar una VLAN interna

La sección Internal VLAN muestra la base y el modo de asignación de las VLAN internas. La VLAN interna está reservada por una interfaz de enrutamiento basada en puerto y es invisible para el usuario final. Una vez que la interfaz de enrutamiento basada en puerto asigna estas VLAN internas, no se pueden asignar a una interfaz VLAN de enrutamiento.

Para configurar una VLAN interna:

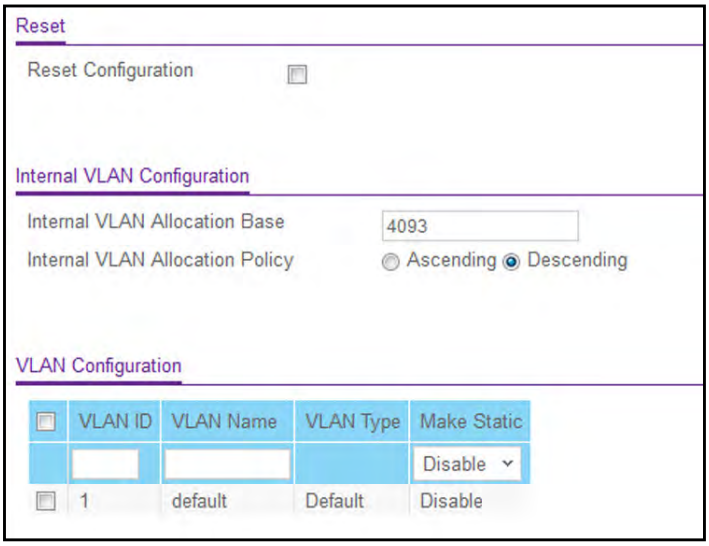
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > VLAN Configuration.



5. En el campo Internal VLAN Allocation Base, especifique la base de asignación de VLAN de la interfaz de enrutamiento.

Puede introducir un valor de 1 a 4093.
6. Seleccione el botón de opción Ascending o Descending de Internal VLAN Allocation Policy. Esto especifica una política de asignación de VLAN internas.
7. Haga clic en el botón Apply.
La configuración se guarda.

Descripción general de Auto-Trunk

Auto-Trunk es una función que permite al switch habilitar automáticamente el modo trunk en los enlaces físicos e interfaces LAG compatibles entre dispositivos asociados. Un trunk puede transportar todas las VLAN activas. De forma predeterminada, la función Auto-Trunk está deshabilitada en el switch.

Si el switch configura automáticamente un puerto como trunk (es decir, un Auto-Trunk), todas las VLAN del switch pasan a formar parte del trunk, lo que permite la configuración automática de todas las VLAN del switch y del dispositivo asociado con el que se establece el trunk.

Antes de configurar un Auto-Trunk, el switch detecta primero los enlaces físicos con el dispositivo asociado que también admite la función Auto-Trunk y luego configura automáticamente los puertos conectados y capaces de formar un trunk en ambos extremos.

Un trunk transporta varias VLAN y acepta paquetes con y sin etiqueta. Normalmente, una conexión entre el switch y un dispositivo asociado, como un router, un punto de acceso u otro switch, funciona como trunk.

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 M4300, la función Auto-Trunk está deshabilitada de forma predeterminada).
- Los puertos interconectados del switch y del dispositivo asociado deben estar habilitados. (En todos los modelos de switch M4300, 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 de switch M4300, 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 de switch 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 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 281). Si las funciones Auto-Trunk y Auto-LAG están habilitadas, 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 del trunk, y todas las VLAN del switch y del dispositivo asociado se pueden configurar automáticamente.

Habilitar o deshabilitar Auto-Trunk

De forma predeterminada, la función Auto-Trunk está deshabilitada globalmente, pero puede habilitarla globalmente.

Para habilitar o deshabilitar Auto-Trunks:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > VLAN Trunking Configuration.

   Se muestra la página VLAN Trunking Configuration.

5. 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 deshabilitada globalmente.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar el trunking de VLAN

Puede configurar el modo switchport en las interfaces. El modo switchport 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 switchport adecuado ayuda a simplificar la configuración de VLAN y a minimizar errores.

Para configurar el trunking de VLAN:

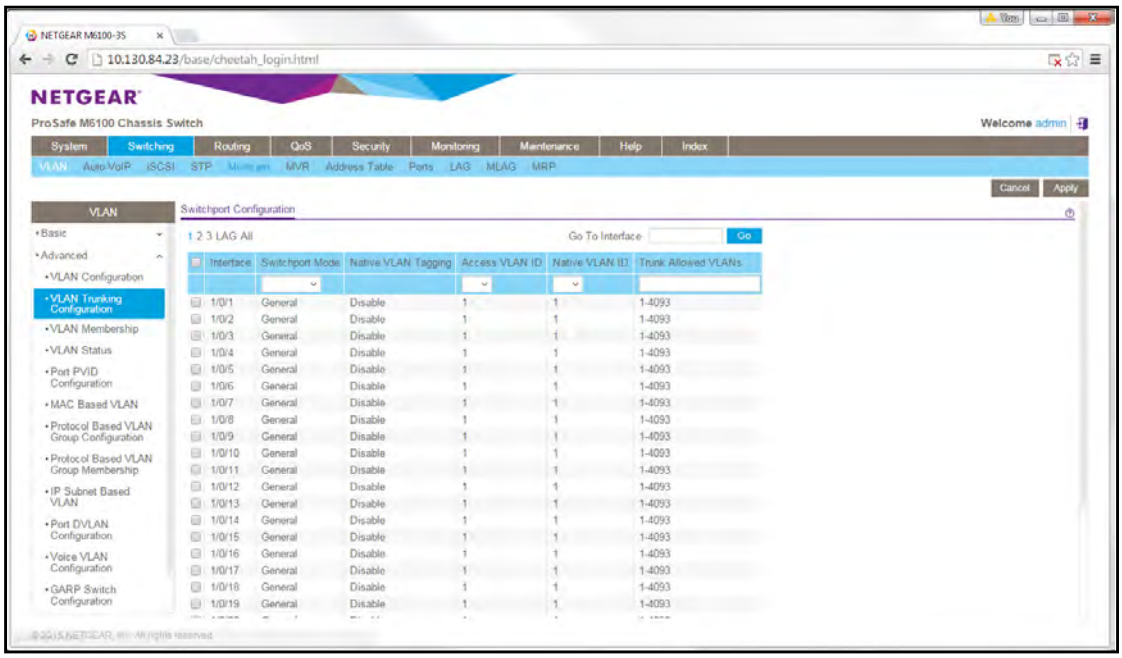
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > VLAN Trunking Configuration.



5. Para especificar qué interfaces se muestran en la página, seleccione una de las siguientes opciones:
   - Seleccione el campo Unit ID para mostrar la información de los puertos físicos de la unidad seleccionada.
   - Use LAG para mostrar solo los LAG.
   - Use All para mostrar todos los puertos físicos.
6. Use uno de los siguientes métodos para seleccionar una interfaz:
   - Use Go To Interface para seleccionar una interfaz introduciendo su número.
   - Use Interface para seleccionar la interfaz cuyos datos desea mostrar o configurar.
7. En la lista Switchport Mode, seleccione una de las siguientes opciones:
   - Access. Este modo es adecuado para puertos conectados a estaciones finales o usuarios finales. Los puertos de acceso participan en una sola VLAN. Aceptan paquetes con y sin etiqueta, pero siempre transmiten paquetes sin etiqueta.
   - Trunk. Este modo es para puertos conectados a otros switches. Los puertos trunk pueden participar en varias VLAN y aceptar paquetes con y sin etiqueta.
   - General. Este modo permite una configuración personalizada del puerto. Los atributos de VLAN del puerto general, como membresía, PVID, etiquetado, filtro de entrada, etc., se configuran en la página Port Configuration. De forma predeterminada, todos los puertos se configuran inicialmente en modo General.
   - Host. Este modo se usa para la configuración de VLAN privadas.
   - Promiscuous. Este modo se usa para la configuración de VLAN privadas.
8. Seleccione en la lista para configurar el valor de Access VLAN ID.

   Es la VLAN de acceso del puerto y solo es válida cuando el modo switchport del puerto es Access.
9. Seleccione en la lista para configurar el valor de Native VLAN ID.

   Es la VLAN nativa del puerto y solo es válida cuando el modo switchport del puerto es Trunk.
10. **Configure el valor de Trunk Allowed VLANs.**

    Es el conjunto de VLAN de las que el puerto puede ser miembro cuando está configurado en modo Trunk. De forma predeterminada, esta lista contiene todas las VLAN posibles, aunque aún no estén creadas. 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. Un valor cero borra las VLAN permitidas. El valor All establece todas las VLAN del rango (1 a 4093).

11. Haga clic en el botón Apply.

La configuración se guarda.
El campo Native VLAN Tagging muestra habilitado o deshabilitado:

- 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.
- 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

Configurar la membresía de VLAN

Para configurar la membresía de VLAN:

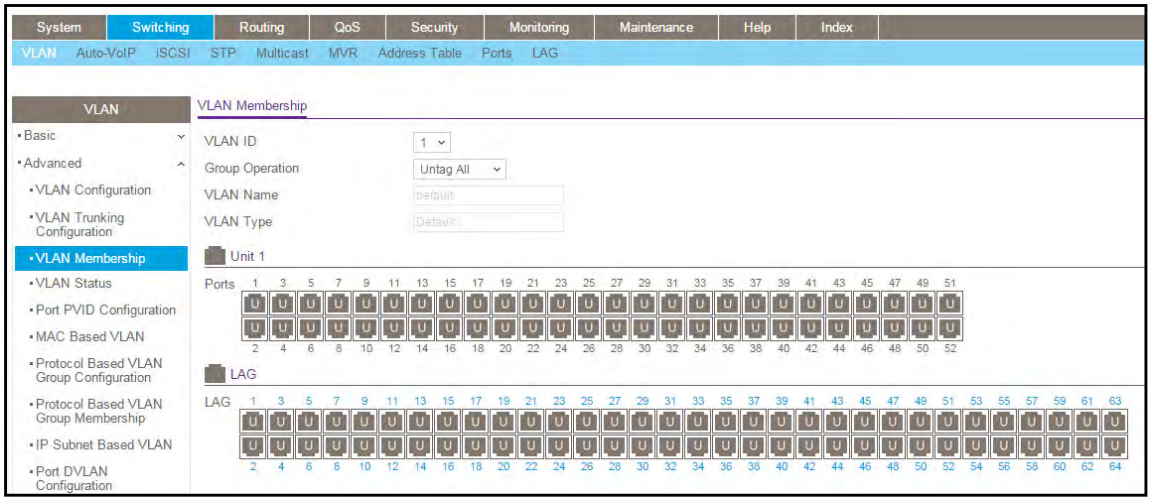
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > VLAN Membership.



5. En la lista VLAN ID, seleccione el ID de VLAN.
6. En la lista Group Operation, seleccione todos los puertos y configúrelos:
   - Untag All. Selecciona todos los puertos en los que todas las tramas transmitidas para esta VLAN van sin etiqueta. Todos los puertos se incluyen en la VLAN.
   - Tag All. Selecciona los puertos en los que todas las tramas transmitidas para esta VLAN van con etiqueta. Todos los puertos se incluyen en la VLAN.
   - Remove All. Todos los puertos que se pueden registrar dinámicamente en esta VLAN mediante GVRP. Esta selección excluye todos los puertos de la VLAN seleccionada.
7. En la representación de puertos, seleccione los números de puerto para agregarlos a esta VLAN. Cada puerto puede usar uno de tres modos:

   - T (Tagged). Seleccione los puertos en los que todas las tramas transmitidas para esta VLAN van con etiqueta. Los puertos seleccionados se incluyen en la VLAN.
   - U (Untagged). Seleccione los puertos en los que todas las tramas transmitidas para esta VLAN van sin etiqueta. Los puertos seleccionados se incluyen en la VLAN.

- EN BLANCO (detección automática). Seleccione los puertos que se pueden registrar dinámicamente en esta VLAN mediante GVRP. Esta selección excluye un puerto de la VLAN seleccionada.

8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 66. Membresía de VLAN avanzada

Campo	Definición
VLAN Name	El nombre de la VLAN seleccionada. Puede tener hasta 32 caracteres alfanuméricos, incluidos espacios. La VLAN ID 1 siempre usa el nombre Default.
VLAN Type	El tipo de la VLAN seleccionada: • Default (VLAN ID = 1). Siempre presente • Static. Una VLAN que usted configuró • Dynamic. Una VLAN creada por registro GVRP que no convirtió a estática y que, por lo tanto, GVRP puede eliminar

Ver el estado de las VLAN

Puede ver el estado de todas las VLAN configuradas actualmente.

Para ver el estado de las VLAN:

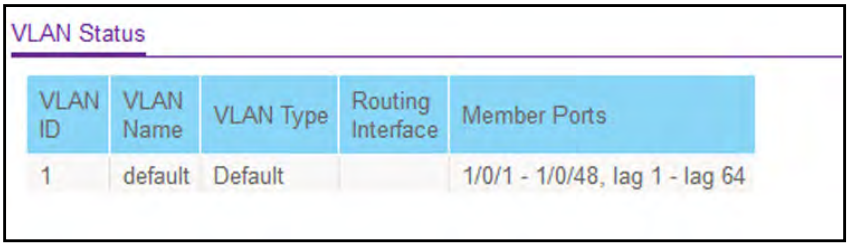
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > VLAN Status.



La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 67. 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 VLAN: • Default (VLAN ID = 1). Siempre presente • Static. Una VLAN que usted configuró • Dynamic. Una VLAN creada por registro GVRP que no convirtió a estática y que, por lo tanto, GVRP puede eliminar
Routing Interface	La interfaz asociada a la VLAN, en caso de que el enrutamiento VLAN esté configurado para esta VLAN.
Member Ports	Los puertos incluidos en la VLAN.

Configurar el PVID de los puertos

Puede asignar un ID de VLAN de puerto (PVID) a una interfaz. El PVID tiene ciertos requisitos:

- Debe definir un PVID para todos los puertos.
- Si no se especifica otro valor, se usa el PVID de la VLAN predeterminada.
- Para cambiar el PVID predeterminado del puerto, primero debe crear una VLAN que incluya el puerto como miembro.
- Use la página Port VLAN ID (PVID) Configuration para configurar una LAN virtual en un puerto.

Para configurar el PVID:

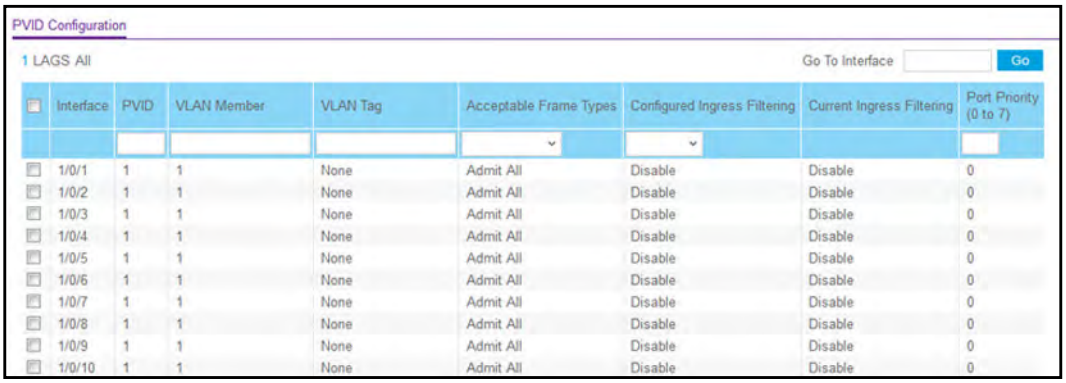
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > Port PVID Configuration.



5. Para mostrar la información de todos los puertos físicos y LAG, haga clic en el botón ALL.
6. Seleccione las interfaces.

   Active la casilla Interface junto a las interfaces. Puede seleccionar varias interfaces. Para seleccionar todas, active la casilla Interface de la fila de encabezado.

7. En el campo PVID, especifique el ID de VLAN que se asignará a las tramas sin etiqueta o con etiqueta de prioridad recibidas en este puerto.

El valor de fábrica es 1.
8. En el campo VLAN Member, especifique el ID de VLAN o la lista de VLAN de un puerto miembro.

   Los ID de VLAN van de 1 a 4093. El valor de fábrica 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.

9. En el campo VLAN Tag, especifique el ID de VLAN o la lista de VLAN de un puerto 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 el puerto es miembro de esta VLAN.

10. En la lista Acceptable Frame Types, especifique los tipos de tramas que se pueden recibir en este puerto.

    Las opciones son VLAN only y Admit All:

    - Con VLAN only, se descartan las tramas sin etiqueta o con etiqueta de prioridad recibidas en este puerto.
    - Con Admit All, se aceptan las tramas sin etiqueta o con etiqueta de prioridad recibidas en este puerto y se les asigna el ID de VLAN de puerto de este puerto. Con cualquiera de las dos opciones, las tramas con etiqueta de VLAN se reenvían de acuerdo con la especificación VLAN 802.1Q.

11. En el campo Configured Ingress Filtering, seleccione Enabled o Disabled.
    - Si está habilitado, la trama se descarta si este puerto 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 especificado para el puerto que recibió la trama.

- Si está deshabilitado, todas las tramas se reenvían de acuerdo con la especificación de puente VLAN 802.1Q. El valor de fábrica es deshabilitado.

12. 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.
13. Haga clic en el botón Aplicar
(Apply).
La configuración se guarda.

Configurar una VLAN basada en MAC

La función de VLAN basada en MAC permite asignar los paquetes entrantes sin etiqueta a una VLAN y así 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 especifica con una dirección MAC de origen y el ID de VLAN deseado. Las configuraciones MAC to VLAN se comparten en todos los puertos del dispositivo (es decir, hay una tabla para todo el sistema con asignaciones de dirección MAC a ID de VLAN).

Cuando llegan al switch paquetes sin etiqueta o con etiqueta de prioridad y existen entradas en la tabla MAC to VLAN, se busca la dirección MAC de origen del paquete. Si se encuentra una entrada, se asigna al paquete el ID de VLAN correspondiente. Si el paquete ya tiene etiqueta de prioridad, conserva ese valor; de lo contrario, la prioridad se establece en cero. El ID de VLAN asignado se verifica contra 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 el usuario puede configurar una asignación de dirección MAC a una VLAN que no se ha creado en el sistema.

Para agregar o eliminar una VLAN basada en MAC:

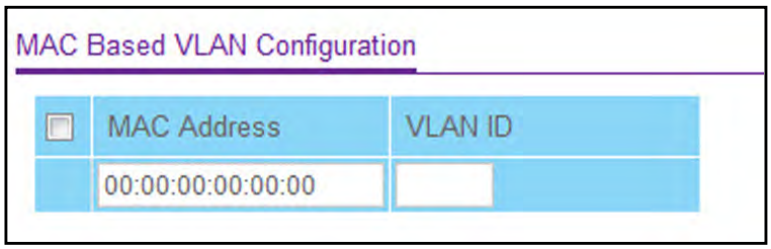
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > MAC Based VLAN.



5. En el campo MAC Address, escriba una dirección MAC válida que se vinculará a un ID de VLAN. Este campo solo se puede configurar al crear una VLAN basada en MAC.
6. En el campo VLAN ID, especifique un ID de VLAN de 1 a 4093.
7. Realice una de las siguientes acciones:
   - Para agregar una dirección MAC a la asignación de VLAN, haga clic en el botón Agregar (Add).
   - Para eliminar una dirección MAC de la asignación de VLAN, haga clic en el botón Eliminar (Delete).

Configurar grupos de VLAN basadas en protocolo

Puede usar una VLAN basada en protocolo para definir criterios de filtrado de paquetes sin etiqueta. De forma predeterminada, si no configura VLAN basadas en puerto (IEEE 802.1Q) ni basadas en protocolo, los paquetes sin etiqueta se asignan a la VLAN 1. Puede cambiar este comportamiento definiendo VLAN basadas en puerto, VLAN basadas en protocolo o ambas. Los paquetes con etiqueta siempre se manejan de acuerdo con la norma IEEE 802.1Q y no se incluyen en las VLAN basadas en protocolo.

Si asigna un puerto a una VLAN basada en protocolo para un protocolo específico, a las tramas sin etiquetar recibidas en ese puerto para ese protocolo se les asigna el ID de la VLAN basada en protocolo. A las tramas sin etiquetar recibidas en el puerto para otros protocolos se les asigna el Port VLAN ID, ya sea el PVID predeterminado (1) o un PVID que haya asignado específicamente al puerto en la página Port VLAN Configuration.

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 varios puertos. Al crear un grupo, usted especifica un nombre y se asigna un ID de grupo automáticamente.

Para configurar un grupo de VLAN basada en protocolo:

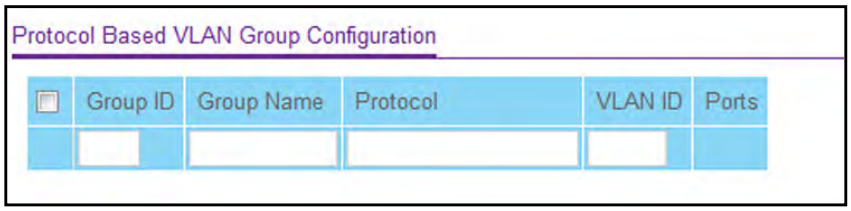
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > Protocol Based VLAN Group Configuration.



5. En el campo Group Name, escriba un nombre para el nuevo grupo.
Puede introducir hasta 16 caracteres.
6. En el campo Protocol, seleccione los protocolos que se asociarán al grupo. Hay tres protocolos configurables:

- 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 por una red.

7. En el campo VLAN ID, seleccione el ID de VLAN.

Puede ser cualquier número en el rango de 1 a 4093. Todos los puertos del grupo asignan este ID de VLAN a los paquetes sin etiquetar recibidos para los protocolos que incluyó en este grupo.

8. Haga clic en el botón Add.
El grupo de VLAN basada en protocolo se agrega al switch.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 68. Grupo de VLAN basada en protocolo

Campo	Descripción
Group ID	Número que identifica el grupo creado por el usuario. Los IDs de grupo se asignan automáticamente cuando el usuario crea un grupo.
Ports	Muestra todos los puertos miembro que pertenecen al grupo.

Configurar la membresía de grupos de VLAN basada en protocolo

Para configurar la membresía de grupos de VLAN basada en protocolo:

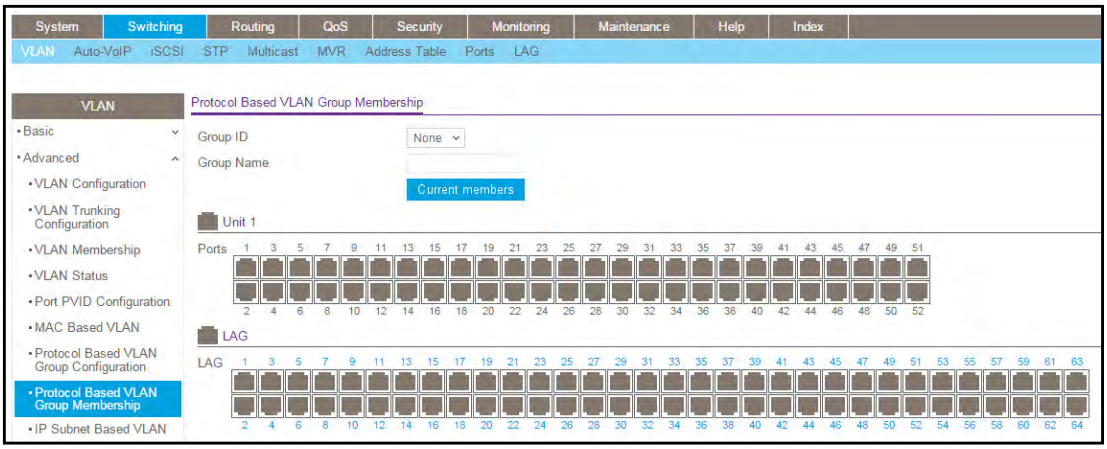
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > Protocol Based VLAN Group Membership.



5. En la lista Group ID, seleccione el ID del grupo de VLAN basada en protocolo.

6. Seleccione números de puerto (1, 2, 3, etc.) para elegir los puertos que agregará a este grupo de VLAN basada en protocolo.

   Una interfaz solo puede pertenecer a un grupo para un protocolo determinado. Si ya agregó un puerto a un grupo para IP, no puede agregarlo a otro grupo que también incluya IP, aunque puede agregarlo a un grupo nuevo para IPX.

7. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 69. Membresía de grupos de VLAN basada en protocolo

Campo	Descripción
Group Name	Este campo identifica el nombre de la VLAN basada en protocolo que seleccionó. Puede tener hasta 32 caracteres alfanuméricos, incluidos espacios.
Current Members	Haga clic en este botón para mostrar los miembros actuales del grupo de VLAN basada en protocolo seleccionado.

Configurar una VLAN basada en subred IP

La asignación de subred IP a VLAN se define configurando una entrada en la tabla IP Subnet to VLAN. Una entrada se especifica mediante una dirección IP de origen, una máscara de red y el ID de VLAN deseado. Las configuraciones de subred IP a VLAN se comparten en todos los puertos del dispositivo.

Para agregar o eliminar una VLAN basada en subred IP:

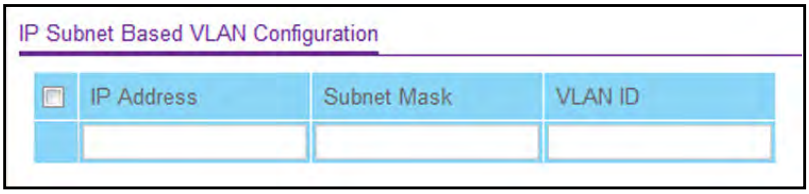
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching> VLAN > Advanced > IP Subnet Based VLAN.**



5. En el campo IP Address, especifique una dirección IP válida vinculada al ID de VLAN. Introduzca la dirección IP en notación decimal con puntos.
6. En el campo Subnet Mask, especifique una máscara de subred válida para la dirección IP. Introduzca la máscara de subred en notación decimal con puntos.
7. En el campo VLAN ID, especifique un ID de VLAN en el rango de 1 a 4093.
8. Realice una de las siguientes acciones:
   - Para agregar la VLAN basada en subred IP, haga clic en el botón Add.
   - Para eliminar la VLAN basada en subred IP, haga clic en el botón Delete.

Configurar una DVLAN de puerto

Para configurar una DVLAN de puerto:

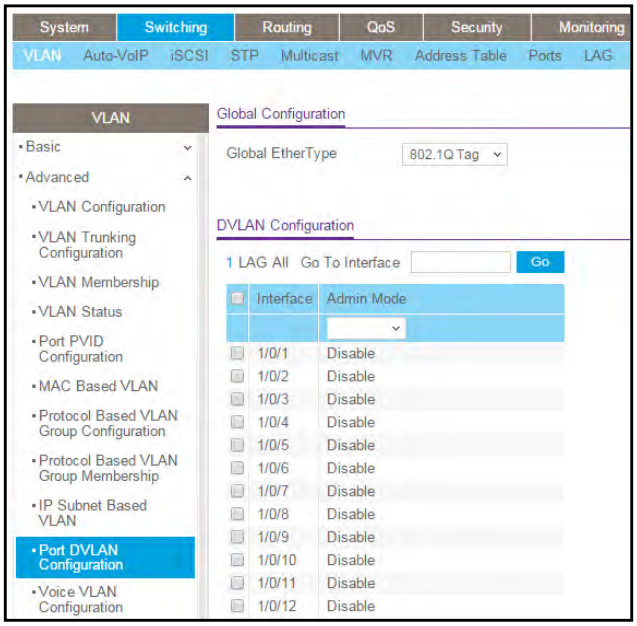
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > Port DVLAN Configuration.



5. Seleccione las casillas Interface para elegir la interfaz física. Para seleccionar todos los puertos, seleccione la casilla Interface en la parte superior de la columna.
6. En el campo Admin Mode, seleccione Enabled o Disabled.

   Esto especifica el modo administrativo con el que se habilita o deshabilita el etiquetado de doble VLAN. El valor predeterminado es Disabled.

7. En el campo Global EtherType, especifique los primeros 16 bits de la etiqueta DVLAN:

   - 802.1Q Tag. Etiqueta de uso común que representa 0x8100
   - vMAN Tag. Etiqueta de uso común que representa 0x88A8
   - Custom Tag. Configure el EtherType en cualquier valor de 0 a 65535

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

Configurar una VLAN de voz

Puede configurar los parámetros de la VLAN de voz. Solo los usuarios con privilegios de lectura/escritura pueden cambiar los datos de esta página.

Para configurar una VLAN de voz:

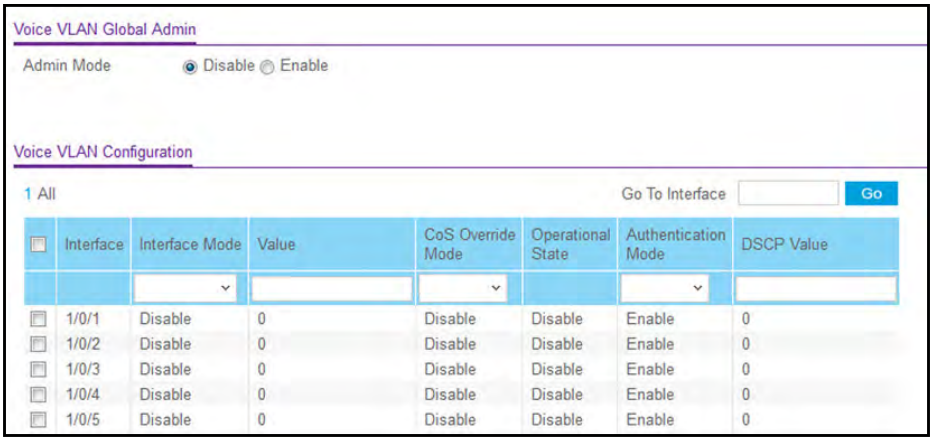
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > Voice VLAN Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Esto especifica el modo administrativo de la VLAN de voz del switch. El valor predeterminado es Disable.

6. Use Interface para seleccionar la interfaz física.
7. Use Interface Mode para seleccionar el modo de VLAN de voz de la interfaz seleccionada:
   - Disable. Es el valor predeterminado.
   - None. Permite que el teléfono IP use su propia configuración para enviar tráfico de voz sin etiquetar.
   - VLAN ID. Configura el teléfono para enviar tráfico de voz etiquetado.
   - dot1p. Configura el etiquetado de prioridad 802.1p de la VLAN de voz para el tráfico de voz. Si selecciona esta opción, introduzca el valor dot1p en el campo Value.
   - Untagged. Configura el teléfono para enviar tráfico de voz sin etiquetar.
8. Use Value para introducir el ID de VLAN o el valor dot1p.

Solo se habilita cuando se selecciona VLAN ID o dot1p como modo de interfaz.

9. En el campo CoS Override Mode, seleccione Disable o Enable.

El valor predeterminado es Disable.

10. En el campo Authentication Mode, seleccione Enable o Disable.

El valor predeterminado es Enable. Cuando el modo de autenticación está habilitado, se permite el tráfico de voz en un puerto de VLAN de voz no autorizado. Cuando está deshabilitado, los dispositivos se autorizan mediante dot1x.

Nota: La autenticación mediante dot1x solo es posible si dot1x está habilitado.

11. En el campo DSCP Value, configure el valor DSCP de la VLAN de voz para el puerto. El rango válido es de 0 a 64. El valor predeterminado es 0.

El campo Operational State muestra el estado operativo de la VLAN de voz en la interfaz.

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

Configurar los ajustes de GARP del switch

Nota: Los cambios de configuración de GARP pueden tardar hasta 10 segundos en surtir efecto.

Para configurar los ajustes de GARP del switch:

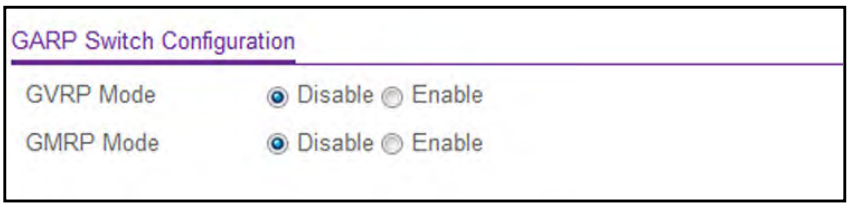
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > GARP Switch Configuration.



5. Seleccione el botón de opción GVRP Mode Disable o Enable.

   Esto selecciona el modo administrativo del protocolo de registro de VLAN GARP del switch. El valor predeterminado de fábrica es Disable.

6. Seleccione el botón de opción GMRP Mode Disable o Enable.

   Esto selecciona el modo administrativo del protocolo de registro multicast GARP del switch. El valor predeterminado de fábrica es Disable.

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

Configurar un puerto GARP

Nota: Los cambios de configuración de GARP pueden tardar hasta 10 segundos en surtir efecto.

Para configurar un puerto GARP:

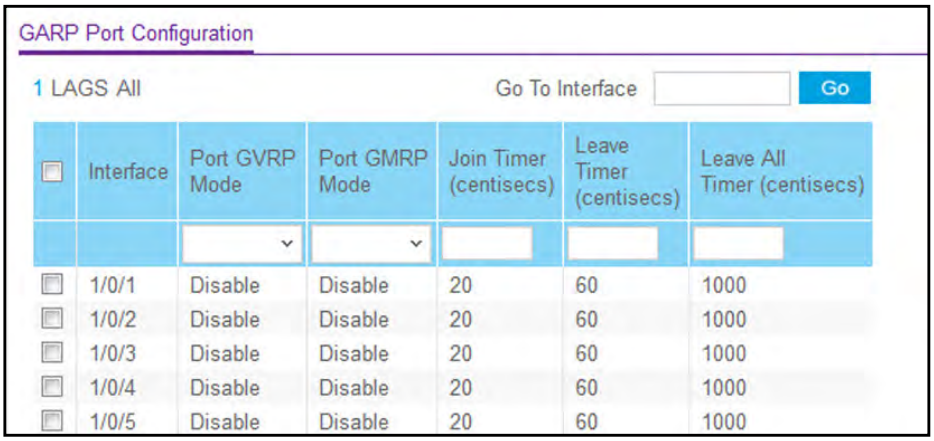
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> VLAN > Advanced > GARP Port Configuration.



5. Use Interface para seleccionar la interfaz física cuyos datos desea mostrar o configurar.

6. En el campo Port GVRP Mode, seleccione Enable o Disable.

Esto especifica el modo administrativo del protocolo de registro de VLAN GARP del puerto. Si selecciona Disable, el protocolo no está activo y los tiempos join, leave y leave all no tienen efecto. El valor predeterminado de fábrica es Disable.

7. En el campo Port GMRP Mode, seleccione Enable o Disable

Esto especifica el modo administrativo del protocolo de registro multicast GARP del puerto. Si selecciona Disable, el protocolo no está activo y los tiempos join, leave y leave all no tienen efecto. El valor predeterminado de fábrica es Disable.

8. En el campo Join Time (centiseconds), especifique el tiempo entre transmisiones de PDU GARP que registran (o vuelven a registrar) la membresía de una VLAN o grupo multicast, en centésimas de segundo.

Introduzca un número entre 10 y 100 (0.1 a 1.0 segundos). El valor predeterminado de fábrica es 20 centésimas (0.2 segundos). Existe una instancia de este temporizador para cada participante GARP en cada puerto.

9. En el campo Leave Time (centiseconds), especifique el tiempo de espera tras recibir una solicitud de baja de registro de una VLAN o grupo multicast antes de eliminar la entrada asociada, en centésimas de segundo.

Esto da tiempo a otra estación para afirmar el registro del mismo atributo y mantener el servicio sin interrupciones. Introduzca un número entre 20 y 600 (0.2 a 6.0 segundos). El valor predeterminado de fábrica es 60 centésimas (0.6 segundos). Existe una instancia de este temporizador para cada participante GARP en cada puerto.

10. Use Leave All Time (centiseconds) para controlar la frecuencia con la que se generan las PDU LeaveAll.

Una PDU LeaveAll indica que pronto se darán de baja todos los registros. Para mantener el registro, los participantes deben volver a unirse. El temporizador del período 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. Introduzca un número entre 200 y 6000 (2 a 60 segundos). El valor predeterminado de fábrica es 1000 centésimas (10 segundos). Existe una instancia de este temporizador para cada participante GARP en cada puerto.

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

Configurar Auto-VoIP

Puede configurar los ajustes de puerto basados en protocolo y los ajustes de OUI.

Configurar los ajustes de puerto basados en protocolo

Para configurar los ajustes de puerto basados en protocolo:

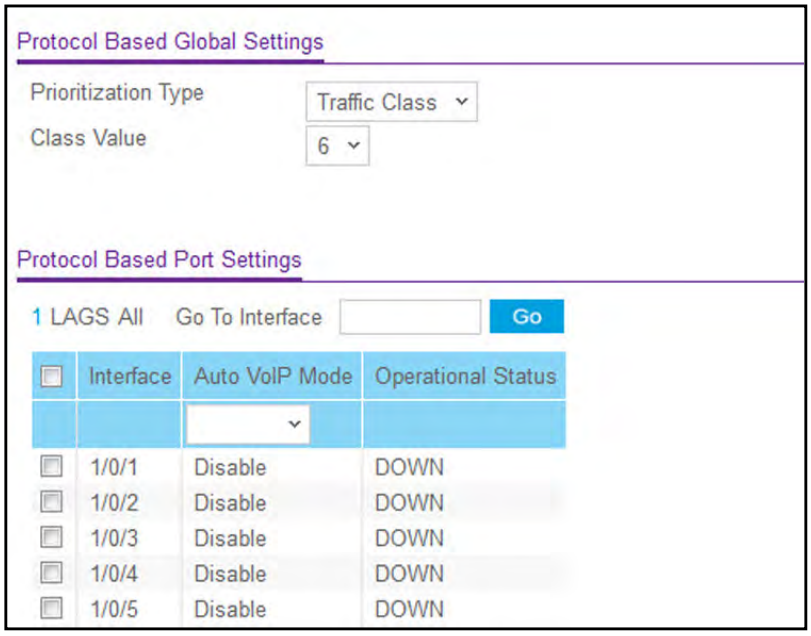
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Auto-VoIP > Protocol-based > Port Settings.



5. En el campo Prioritization Type, seleccione Traffic Class o Remark.

Esto especifica el tipo de priorización.

6. En la lista Class Value, especifique el valor de etiqueta CoS que se reasignará a los paquetes recibidos en la VLAN de voz cuando Remark CoS esté habilitado.
7. Haga clic en el botón Apply.
La configuración se guarda.

Configurar las propiedades de Auto-VoIP basadas en 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, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Auto-VoIP > OUI-based > Properties.



5. En el campo VoIP VLAN ID, escriba el ID de VLAN VoIP del switch. No hay una VLAN predeterminada para Auto-VoIP; primero debe crear una VLAN para ello.
6. En la lista OUI-based priority, seleccione la prioridad basada en OUI del switch. El valor predeterminado es 7.
7. Haga clic en el botón Apply.
La configuración se guarda.

Ajustes de puerto basados en OUI

Para configurar los ajustes de puerto de Auto-VoIP basados en OUI:

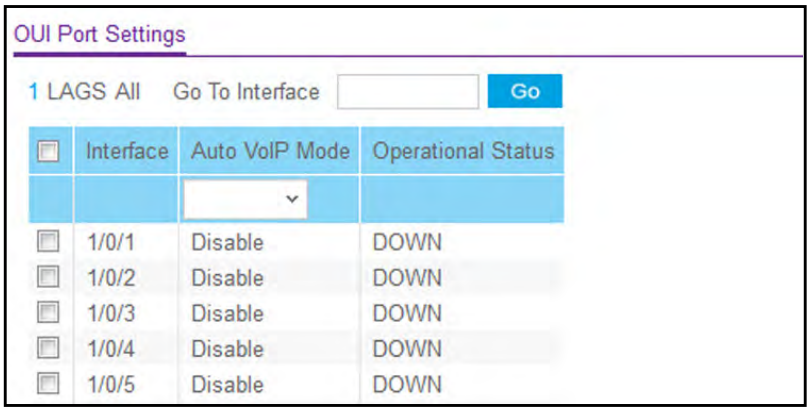
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Auto-VoIP > OUI-based > Port Settings.



El campo Operational Status muestra el estado operativo actual de cada interfaz.

5. 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, seleccione la casilla de la interfaz que desea configurar.

6. En el campo Auto VoIP Mode, seleccione Disable o Enable.

Auto-VoIP está deshabilitado de forma predeterminada.
7. Haga clic en el botón Apply.
La configuración se guarda.

Agregar una entrada nueva a la tabla OUI

Para agregar una entrada nueva a la tabla OUI:

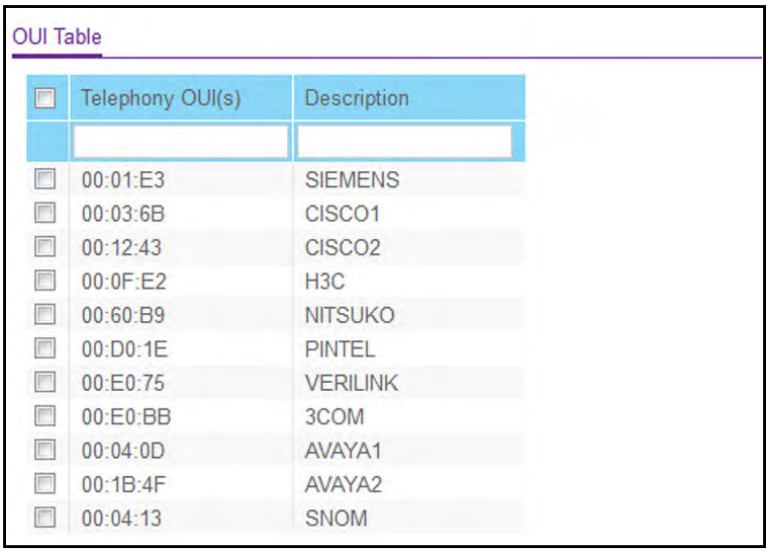
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. **Seleccione Switching > Auto-VoIP > OUI-based > OUI Table.**



5. En el campo Telephony OUI(s), especifique el prefijo OUI de VoIP que se agregará con el formato AA:BB:CC.

Se pueden configurar hasta 128 OUI.

6. En el campo Description, introduzca la descripción del OUI.

La longitud máxima de la descripción es de 32 caracteres. Los siguientes OUI están presentes en la configuración de forma predeterminada:

- 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

7. Haga clic en el botón Add.

Se agrega la entrada de OUI de telefonía.

Eliminar entradas de la tabla OUI

Para eliminar una o más entradas de la tabla OUI:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Auto-VoIP > OUI-based > OUI Table.

Se muestra la tabla OUI.
5. Seleccione una o más entradas de la tabla.
6. Haga clic en el botón Delete.
Se eliminan las entradas.

Ver el estado de Auto-VoIP

Para ver el estado de Auto-VoIP:

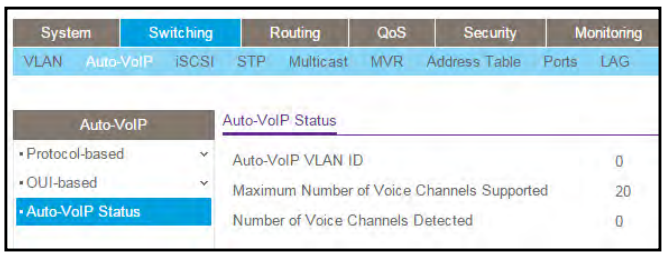
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Auto-VoIP > Auto-VoIP Status.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información de estado de Auto-VoIP no configurable.

Tabla 70. Estado de Auto-VoIP

Campo	Descripción
Auto-VoIP VLAN ID	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.

Configurar los ajustes de iSCSI

La función Internet Small Computer System Interface (iSCSI) ayuda a los administradores de red a rastrear el tráfico iSCSI entre iniciadores iSCSI y sistemas de destino. Esto se logra monitoreando o inspeccionando el tráfico para detectar los paquetes que usan las estaciones iSCSI al establecer sesiones y conexiones iSCSI. Los datos de estos intercambios se usan para crear reglas de clasificación que asignan el tráfico entre las estaciones a una clase de tráfico configurada. Los paquetes del flujo se ponen en cola y se programan para su salida por el puerto de destino según estas reglas.

En redes con iniciadores y destinos iSCSI, iSCSI ayuda a monitorear las sesiones iSCSI o a dar al tráfico iSCSI un tratamiento preferente de calidad de servicio (QoS). Las reglas de clasificación generadas dinámicamente dirigen el tráfico de datos iSCSI a colas a las que se pueden dar las características de preferencia deseadas sobre otros datos que pasan por el switch. Esto puede ayudar a evitar interrupciones de sesión en momentos de congestión que, de otro modo, harían que se descartaran paquetes iSCSI. Sin embargo, en sistemas donde gran parte del tráfico es iSCSI, también podría interferir con otro tráfico del plano de control de la red, como ARP o LACP.

El tratamiento preferente del tráfico iSCSI debe equilibrarse con las necesidades de otros datos críticos de la red.

Puede ver y administrar los ajustes de iSCSI Optimization en el dispositivo. iSCSI Optimization permite dar un tratamiento especial de calidad de servicio (QoS) al tráfico entre iniciadores y sistemas de destino iSCSI.

Además, si se configura, los paquetes pueden actualizarse con valores IEEE 802.1 o IP-DSCP. Esto se hace habilitando Remark. Remarcar los paquetes con datos de prioridad proporciona un tratamiento QoS especial a medida que los paquetes avanzan por la red.

Configurar los ajustes globales de iSCSI

Para configurar los ajustes globales de iSCSI en el switch:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > iSCSI > Basic > Global Configuration.



5. En el campo iSCSI Status, seleccione Enable o Disable.

   Esto habilita o deshabilita globalmente la función iSCSI Optimization. De forma predeterminada, iSCSI Optimization está deshabilitada.

6. Seleccione el botón de opción QoS Profile VLAN Priority Tag o DSCP.

   Esto especifica el perfil de calidad de servicio (QoS) que se aplica a los flujos iSCSI. De forma predeterminada, los flujos iSCSI se asignan a la etiqueta de prioridad VLAN (VPT)/DSCP más alta asignada a la cola más alta que no se use para la administración del switch ni para la VLAN de voz.

   Al establecer la etiqueta de prioridad VLAN/DSCP se define el perfil QoS que determina la cola de salida a la que se asigna la trama. El ajuste predeterminado del switch para la programación de colas de salida es Weighted Round Robin (WRR). Complete el ajuste de QoS configurando los puertos pertinentes para que funcionen en otros modos de programación y administración de colas mediante los ajustes de Class of Service. Según la plataforma, estas opciones pueden incluir prioridad estricta para la cola usada por el tráfico iSCSI. La desventaja de la prioridad estricta es que, en ciertas circunstancias (con mucho tráfico de alta prioridad), otro tráfico de menor prioridad podría quedar sin recursos. En WRR, la cola a la que se asigna el flujo puede configurarse para obtener el porcentaje requerido.

7. Configure la asignación global de clases de tráfico en Class of Service.

La configuración global de asignación de clases de tráfico determina la clase de tráfico usada para transmitir paquetes iSCSI. Las opciones de configuración de asignación de tráfico son las siguientes:

- IEEE 802.1P
- IP-DSCP

La configuración del componente CoS determina los cambios en la asignación de valores IEEE 802.1p o IP-DSCP a clases de tráfico. Para más información, consulte Administrar la clase de servicio en la página 475.

8. Si usa VLAN Priority como perfil QoS, en el campo VLAN Priority Tag, seleccione el valor para los paquetes de sesión iSCSI.

El rango es de 0 a 7. El valor predeterminado es 5.

9. Si usa DSCP como perfil QoS, en la lista DSCP, seleccione un valor para asignar a los paquetes de sesión iSCSI.

El rango es de 0 a 63. El valor predeterminado es 46.
10. Seleccione el botón de opción Remark Enable o Disable.

Esto habilita o deshabilita el marcado de las tramas iSCSI con la etiqueta de prioridad VLAN/DSCP configurada al salir del switch. Habilitar Remark actualiza los paquetes con valores IEEE 802.1p o IP-DSCP. Remarcar los paquetes con datos de prioridad proporciona un tratamiento QoS especial a medida que los paquetes avanzan por la red. Remark está habilitado de forma predeterminada.

11. En el campo iSCSI Aging Time, establezca el número de minutos que una sesión puede estar inactiva antes de eliminarse.

El valor de iSCSI Aging Time debe ser un número entero en el rango de 1 a 43200 minutos. El valor predeterminado es 10 minutos.

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

Ver las sesiones iSCSI

Para ver la información de las sesiones iSCSI activas:

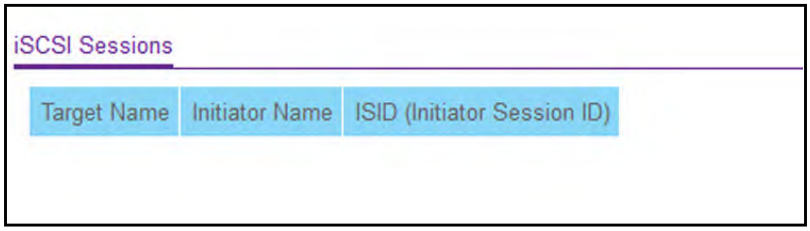
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Haga clic en Switching > iSCSI > Basic > Sessions.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable de iSCSI Sessions.

Tabla 71. Sesiones iSCSI

Campo	Descripción
Target Name	El nombre del destino.
Initiator Name	El nombre del iniciador.
Initiator Session ID (ISID)	El identificador iSCSI.

Controlar los ajustes de destinos iSCSI

Puede ver los destinos iSCSI y asignar combinaciones de puerto de destino/dirección IP de puerto para la optimización iSCSI en el switch.

Para configurar los ajustes de destinos iSCSI

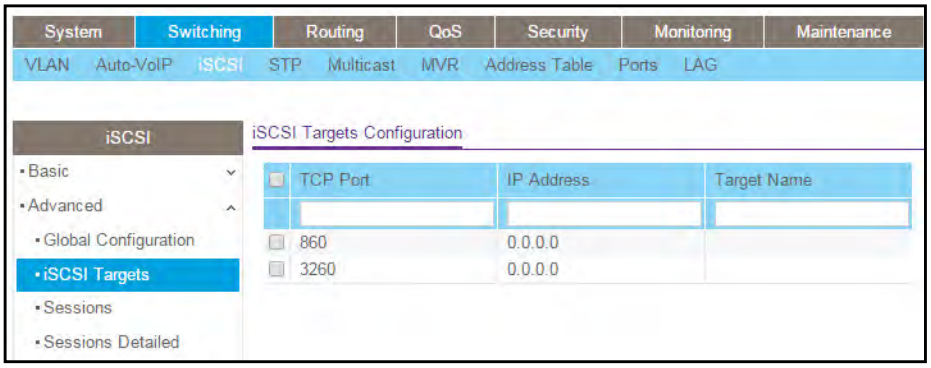
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > iSCSI > Advanced > iSCSI Targets.



5. En el campo TCP Port, especifique el puerto TCP del destino que monitorea el tráfico iSCSI.

   Se pueden definir hasta 16 puertos TCP en el sistema. Los puertos iSCSI conocidos 860 y 3260 se configuran de forma predeterminada, pero puede quitarlos como cualquier otro destino configurado.

6. En el campo IP address, especifique una dirección IP para el destino que monitorea el tráfico iSCSI. El valor predeterminado es 0.0.0.0.
7. En el campo Target Name, especifique un nombre para asignar al destino. El nombre del destino iSCSI puede tener hasta 233 caracteres.
8. Haga clic en el botón Add.

Se agrega la configuración de destinos iSCSI.

Ver las sesiones iSCSI

Para ver información sobre las sesiones iSCSI activas:

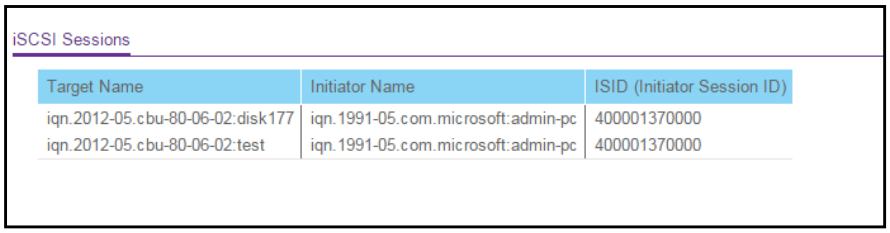
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > iSCSI > Advanced > Sessions.



A continuación se describe la información no configurable de iSCSI Sessions que se muestra.

Tabla 72. Sesiones iSCSI

Campo	Descripción
Target Name	El nombre del destino.
Initiator Name	El nombre del iniciador.
Initiator Session ID (ISID)	El identificador único que un iniciador asigna a su extremo de sesión y que, combinado con el nombre del iniciador iSCSI, proporciona un nombre único para el puerto del iniciador iSCSI.

Ver los detalles de las sesiones iSCSI

Puede ver información detallada sobre las sesiones iSCSI activas.

Para ver los detalles de las sesiones iSCSI:

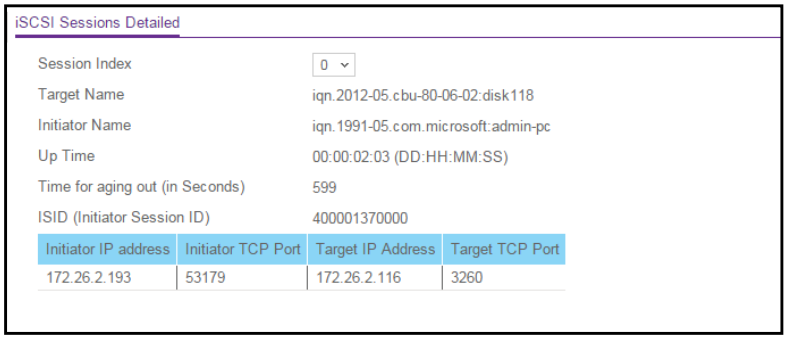
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching > iSCSI > Advanced > Sessions Detailed.**



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable de iSCSI Sessions Detailed.

Tabla 73. Detalles de sesiones iSCSI

Campo	Descripción
Session Index	La lista de índices de sesión.
El resto de los campos de esta página corresponden al Session Index seleccionado actualmente.	
Target Name	El nombre del destino.
Initiator Name	El nombre del iniciador.
Up Time	El tiempo transcurrido desde la creación de la sesión actual.
Time for Aging Out (in Seconds)	El tiempo restante, en segundos, para que expire la sesión actual.
Initiator Session ID (ISID)	El identificador único que un iniciador asigna a su extremo de sesión y que, combinado con el nombre del iniciador iSCSI, proporciona un nombre único para el puerto del iniciador iSCSI.
Initiator IP Address	La dirección IP del iniciador.
Initiator TCP Port	El número de puerto TCP del iniciador de una de las conexiones entre el destino y el iniciador.
Target IP Address	La dirección IP del destino.
Target TCP Port	El número de puerto TCP del destino de una de las conexiones entre el destino y el iniciador.

Configurar el Spanning Tree Protocol

El Spanning Tree Protocol (STP) proporciona una topología de árbol para cualquier disposición de bridges. STP también proporciona una sola ruta entre estaciones finales de una red, eliminando los bucles. Las versiones de spanning tree admitidas incluyen Common STP, Multiple STP y Rapid STP.

El STP clásico proporciona una sola ruta entre estaciones finales, evitando y eliminando bucles. Para configurar Common STP, consulte Configurar los ajustes de puerto CST en la página 223.

Multiple Spanning Tree Protocol (MSTP) admite varias instancias de Spanning Tree para canalizar eficientemente el tráfico de VLAN por distintas interfaces. Cada instancia de Spanning Tree se comporta como se especifica en IEEE 802.1w, Rapid Spanning Tree (RSTP), con ligeras modificaciones en el funcionamiento pero no en el efecto final (el principal efecto es la rápida transición del puerto a Forwarding). 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 rápida transición del puerto al estado Forwarding y la supresión de la notificación de cambio de topología. Estas funciones se representan mediante los parámetros pointtopoint y edgeport. MSTP es compatible con RSTP y STP. Se comporta adecuadamente con puentes STP y RSTP. Un puente MSTP puede configurarse para comportarse totalmente como un puente RSTP o STP.

Nota: Para que dos puentes estén en la misma región, la versión forzada debe ser 802.1s y su nombre de configuración, clave de resumen y nivel 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 básicos de STP

Para configurar los ajustes básicos de STP:

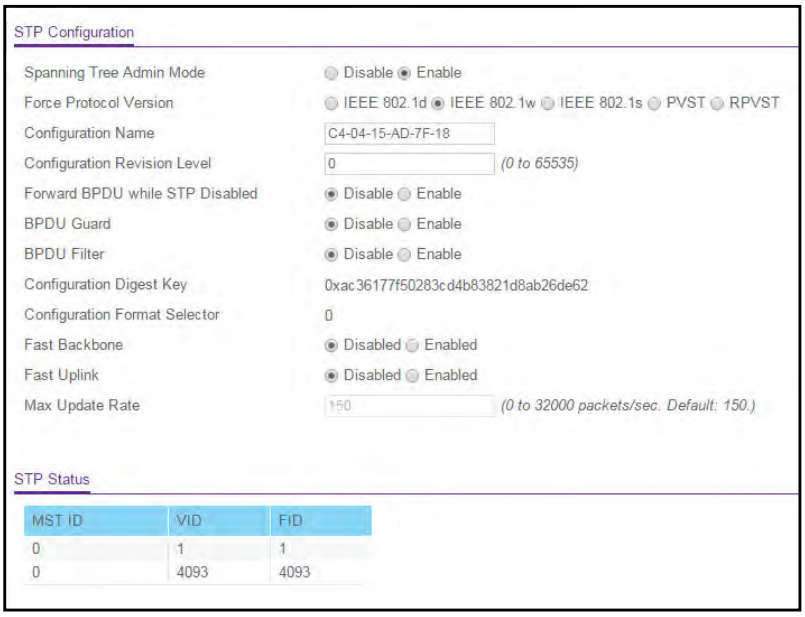
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Basic > STP Configuration.



5. Seleccione el botón de opción Spanning Tree Admin Mode Disable o Enable.

   Esto especifica si el funcionamiento de spanning tree está habilitado en el switch.

6. Use Force Protocol Version para especificar el parámetro de versión de protocolo forzada del switch.

Las opciones son IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, PVST y RPVST.

7. Use Configuration Name para especificar un identificador de la configuración que se está usando actualmente.

Puede tener hasta 32 caracteres alfanuméricos.

8. Use Configuration Revision Level para especificar un identificador de la configuración que se está usando actualmente.

Los valores permitidos son de 0 a 65535. El valor predeterminado es 0.

9. Seleccione el botón de opción Forward BPDU while STP Disabled Disable o Enable.

Esto especifica si se reenvían o no las BPDU de spanning tree mientras spanning tree está deshabilitado en el switch.

10. Seleccione el botón de opción BPDU Guard Disable o Enable.

Esto especifica si la función BPDU guard está habilitada. STP BPDU guard permite al administrador de red imponer los límites del dominio STP y mantener la topología activa coherente y predecible. Los switches detrás de puertos de borde con STP BPDU guard habilitado no influyen en la topología STP general. Al recibir BPDU, la función BPDU guard deshabilita el puerto configurado con esta opción y lo pasa al estado deshabilitado. Esto equivale a una deshabilitación administrativa del puerto.

11. Seleccione el botón de opción BPDU Filter Disable o Enable.

Esto especifica si la función BPDU Filter está habilitada. El filtrado de BPDU de STP se aplica a todos los puertos de borde operativos. Un puerto de borde operativo debe estar conectado a hosts que normalmente descartan las BPDU. Si un puerto de borde operativo recibe una BPDU, pierde de inmediato su estado operativo. En ese caso, si el filtrado de BPDU está habilitado en este puerto, se descartan las BPDU recibidas en él.

12. Seleccione el botón de opción Fast Backbone Mode Disable o Enable. (Solo PVSTP).

Use esta opción para elegir un nuevo enlace indirecto cuando falla un enlace indirecto. El sistema no ignora las BPDU inferiores, como ocurre en 802.1d. En cambio, usa las BPDU para hacer expirar la información en el puerto donde las recibió. Después, envía consultas de enlace raíz a otros puertos no designados. Según las respuestas, si al menos una es positiva, elige un nuevo enlace indirecto. El modo Fast Backbone está deshabilitado de forma predeterminada.

13. Seleccione el botón de opción Fast Uplink Mode Disable o Enable. (Solo PVSTP).

Esta opción reduce el tiempo de recuperación al seleccionar un nuevo puerto raíz cuando el puerto raíz principal deja de funcionar. El modo Fast Uplink está deshabilitado de forma predeterminada.

14. Use el campo Max Update Rate para configurar la velocidad máxima de actualización de Fast Uplink.

Este campo se puede configurar cuando el modo Fast Uplink está habilitado. Los valores permitidos son de 0 a 32000 paquetes por segundo. El valor predeterminado es 150.

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

La siguiente tabla describe los campos no configurables.

Tabla 74. Configuración de STP

Campo	Descripción
Configuration Digest Key	Identificador de la configuración que se está usando actualmente.
Configuration Format Selector	La versión del formato de configuración que se usa en el intercambio de BPDU.
MST ID	Tabla de las instancias MST (incluida la CST) y los ID de VLAN asociados a cada una.
VID ID	Tabla de los ID de VLAN y el FID asociado a cada uno.
FID ID	Tabla de los FID y los ID de VLAN asociados a cada uno.

Configurar los ajustes avanzados de STP

Para configurar los ajustes avanzados de STP:

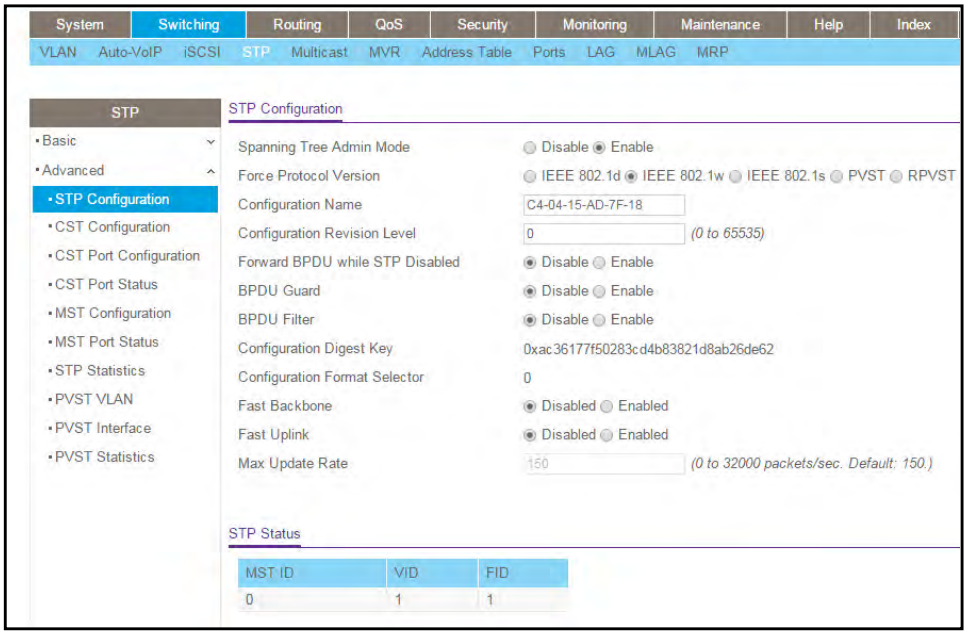
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > STP Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Esto especifica si el funcionamiento de spanning tree está habilitado en el switch. El valor predeterminado es Enable.

6. Use Force Protocol Version para especificar el parámetro de versión de protocolo forzada del switch.

   Las opciones son IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, PVST y RPVST. El valor predeterminado es IEEE 802.1w.

7. Use Configuration Name para especificar el identificador de la configuración que se está usando actualmente.

   Puede tener hasta 32 caracteres alfanuméricos.

8. Use Configuration Revision Level para especificar el identificador de la configuración que se está usando actualmente.

   Los valores permitidos son de 0 a 65535. El valor predeterminado es 0.

9. Seleccione el botón de opción Forward BPDU while STP Disabled Disable o Enable.

   Esto especifica si se reenvían las BPDU de spanning tree mientras spanning tree está deshabilitado en el switch. El valor predeterminado es Disable.

10. Seleccione el botón de opción BPDU Guard Disable o Enable.

    Esto especifica si la función BPDU guard está habilitada. STP BPDU guard permite al administrador de red imponer los límites del dominio STP y mantener la topología activa coherente y predecible. Los switches detrás de puertos de borde con STP BPDU guard habilitado no influyen en la topología STP general. Al recibir BPDU, la función BPDU guard deshabilita el puerto configurado con esta opción y lo pasa al estado deshabilitado. Esto equivale a una deshabilitación administrativa del puerto.

11. Seleccione el botón de opción BPDU Filter Disable o Enable.

    Esto especifica si la función BPDU Filter está habilitada. El filtrado de BPDU de STP se aplica a todos los puertos de borde operativos. Un puerto de borde operativo debe estar conectado a hosts que normalmente descartan las BPDU. Si un puerto de borde operativo recibe una BPDU, pierde de inmediato su estado operativo. En ese caso, si el filtrado de BPDU está habilitado en este puerto, se descartan las BPDU recibidas en él.

12. Seleccione el botón de opción Fast Backbone Mode Disable o Enable. (Solo PVSTP).

    Use esta opción para elegir un nuevo enlace indirecto cuando falla un enlace indirecto. El sistema no ignora las BPDU inferiores, como ocurre en 802.1d. En cambio, usa las BPDU para hacer expirar la información en el puerto donde las recibió. Después, envía consultas de enlace raíz a otros puertos no designados. Según las respuestas, si al menos una es positiva, elige un nuevo enlace indirecto. El modo Fast Backbone está deshabilitado de forma predeterminada.

13. Seleccione el botón de opción Fast Uplink Mode Disable o Enable. (Solo PVSTP).

    Esta opción reduce el tiempo de recuperación al seleccionar un nuevo puerto raíz cuando el puerto raíz principal deja de funcionar. El modo Fast Uplink está deshabilitado de forma predeterminada.

14. Use el campo Max Update Rate para configurar la velocidad máxima de actualización de Fast Uplink.

    Este campo se puede configurar cuando el modo Fast Uplink está habilitado. Los valores permitidos son de 0 a 32000 paquetes por segundo. El valor predeterminado es 150.

15. Haga clic en el botón Apply.

La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 75. Configuración de STP

Campo	Descripción
Configuration Digest Key	La firma de 16 bytes de tipo HMAC-MD5 creada a partir de la tabla de configuración MST (asignación de ID de VLAN a ID de MST), que se usa para identificar la configuración que se está usando actualmente.
Configuration Format Selector	La versión del formato de configuración que se usa en el intercambio de BPDU.
Estado de STP	
MST ID	Tabla de las instancias MST (incluida la CST) y los ID de VLAN asociados a cada una.
VID ID	Tabla de los ID de VLAN y el FID asociado a cada uno.
FID ID	Tabla de los FID y los ID de VLAN asociados a cada uno.

Configurar los ajustes de CST

Puede configurar Common Spanning Tree (CST) e Internal Spanning Tree en el switch.

Para configurar los ajustes de CST:

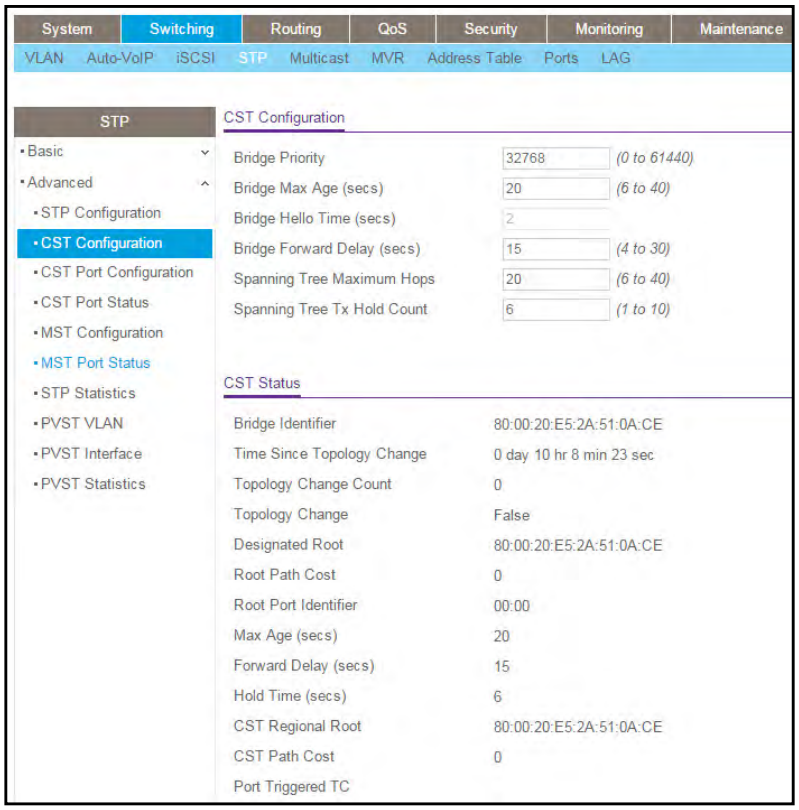
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching > STP > Advanced > CST Configuration.**



5. Especifique los valores de CST en los campos correspondientes:
   - Bridge Priority. 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. Especifica el valor de prioridad del puente para Common and Internal Spanning Tree (CST). El rango válido es 0–61440. 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 se intenta establecer cualquier valor entre 0 y 4095, se establece en 0. La prioridad predeterminada es 32768.

- Bridge Max Age (secs). La antigüedad máxima del puente para Common and Internal Spanning Tree (CST), que indica el tiempo en segundos que un puente espera antes de aplicar un cambio de topología. El rango válido es 6–40, y el valor debe ser menor o igual que (2 * Bridge Forward Delay) – 1 y mayor o igual que 2 * (Bridge Hello Time +1). El valor predeterminado es 20.
- Bridge Hello Time (secs). El tiempo de hello del puente para Common and Internal Spanning Tree (CST), que indica el tiempo en segundos que un puente raíz espera entre mensajes de configuración. El valor es fijo en 2 segundos. El valor debe ser menor o igual que (Bridge Max Age / 2) - 1. El valor predeterminado de hello time es 2.
- Bridge Forward Delay (secs). El retardo de reenvío del puente, que indica el tiempo en segundos que un puente permanece en los estados listening y learning antes de reenviar paquetes. El valor debe ser mayor o igual que (Bridge Max Age / 2) + 1. El rango es de 4 a 30 segundos. El valor predeterminado es 15 segundos.
- Spanning Tree Maximum Hops. El número máximo de saltos entre puentes que puede recorrer la información de una instancia CST antes de descartarse. El rango válido es 6–40. El valor predeterminado es 20 saltos.
- Spanning Tree Tx Hold Count. Configura el número máximo de BPDU que el puente puede enviar dentro de la ventana de hello time. El rango válido es 1–10. El valor predeterminado es 6.

6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe la información de CST Status que se muestra.

Tabla 76. Configuración avanzada de CST de STP

Campo	Descripción
Bridge identifier	El identificador de puente de la CST. Se compone de la prioridad del puente y la dirección MAC base del puente.
Time since topology change	El tiempo en segundos desde el último cambio de topología de la CST.
Topology change count	Número de veces que cambió la topología de la CST.
Topology change	El valor del parámetro de cambio de topología del switch, que indica si hay un cambio de topología en curso en algún puerto asignado a la CST. Toma el valor True o False.
Designated root	El identificador de puente del puente raíz. Se compone de la prioridad del puente y la dirección MAC base del puente.
Root Path Cost	Costo de ruta hacia la raíz designada de la CST.
Root Port Identifier	Puerto para acceder a la raíz designada de la CST.
Max Age(secs)	Costo de ruta hacia la raíz designada de la CST.

Tabla 76. Configuración avanzada de CST de STP

Campo	Descripción
Forward Delay(secs)	Valor derivado del parámetro Bridge Forward Delay del puerto raíz.
Hold Time(secs)	Tiempo mínimo entre transmisiones de BPDU de configuración.
CST Regional Root	Prioridad y dirección MAC base de la raíz regional de la CST.
CST Path Cost	Costo de ruta hacia la raíz regional del árbol CST.

Configurar los ajustes de puertos CST

Puede configurar Common Spanning Tree (CST) e Internal Spanning Tree en un puerto específico del switch.

Un puerto puede quedar deshabilitado por diagnóstico (D-Disable) cuando DOT1S sufre una condición de error grave. La causa más común es que el software DOT1S sufra una inundación de BPDU. El criterio de inundación es que DOT1S reciba más de 15 BPDU en un intervalo de 3 segundos. Las demás causas de D-Disable de DOT1S son muy poco frecuentes.

Para configurar los ajustes de puertos CST:

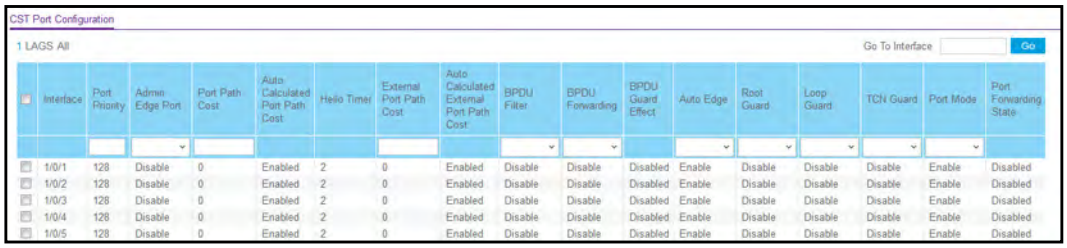
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > CST Port Configuration.



5. Seleccione una interfaz.

   Puede seleccionar una interfaz física o de port channel asociada con las VLAN asociadas con la CST.

6. Use Port Priority para especificar la prioridad de un puerto dentro de la CST.

La prioridad del puerto se establece en múltiplos de 16. Por ejemplo, si se intenta establecer cualquier valor entre 0 y 15, se establece en 0. Si se intenta establecer cualquier valor entre 16 y (2*16-1), se establece en 16, y así sucesivamente. El valor predeterminado es 128.

7. Use Admin Edge Port para especificar si el puerto es un puerto de borde dentro de la CIST. Use el menú para seleccionar Disable o Enable. El valor predeterminado es Disable.

8. Use Port Path Cost para establecer un nuevo costo de ruta para el puerto en Common and Internal Spanning Tree.

Acepta un valor en el rango de 1 a 200000000. El valor predeterminado es 0.

9. Use External Port Path Cost para establecer un nuevo costo de ruta externo para el puerto en spanning tree.

Acepta un valor en el rango de 1 a 200000000. El valor predeterminado es 0.

10. Use BPDU Filter para configurar el filtro de BPDU, que filtra el tráfico BPDU en este puerto cuando STP está habilitado en él.

Los valores posibles son Enable o Disable. El valor predeterminado es Disable.

11. Use BPDU Flood para configurar la inundación de BPDU, que inunda el tráfico BPDU que llega a este puerto cuando STP está deshabilitado en él.

Los valores posibles son Enable o Disable. El valor predeterminado es Disable.

12. Use Auto Edge para configurar el modo de borde automático de un puerto, que permite que el puerto se convierta en puerto de borde si no detecta BPDU durante cierto tiempo.

Los valores posibles son Enable o Disable. El valor predeterminado es Enable.

13. Use Root Guard para configurar el modo root guard, que hace que el puerto descarte cualquier información superior recibida y así evita que cambie la raíz del dispositivo.

El puerto pasa al estado de descarte y no reenvía ningún paquete. Los valores posibles son Enable o Disable. El valor predeterminado es Disable.

14. Use Loop Guard para habilitar o deshabilitar loop guard en el puerto y evitar bucles de reenvío de capa 2.

Si loop guard está habilitado, el puerto pasa al estado de bloqueo por inconsistencia de bucle de STP en lugar del estado listening/learning/forwarding. El valor predeterminado es Disable

15. Use TCN Guard para configurar TCN guard en un puerto, lo que impide que el puerto propague cualquier información de cambio de topología recibida por él.

Los valores posibles son Enable o Disable. El valor predeterminado es Disable.

16. Use Port Mode para habilitar o deshabilitar el modo administrativo de Spanning Tree Protocol asociado al puerto o port channel.

Los valores posibles son Enable o Disable. El valor predeterminado es Disable.
17. Haga clic en el botón Apply.
La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 77. Configuración de puertos CST

Campo	Descripción
Auto Calculated Port Path Cost	Indica si el costo de ruta se calcula automáticamente (Enabled) o no (Disabled). El costo de ruta se calcula según la velocidad de enlace del puerto si el valor configurado de Port Path Cost es cero.
Hello Timer	El valor del parámetro para la CST.
Auto Calculated External Port Path Cost	Indica si el costo de ruta externo se calcula automáticamente (Enabled) o no (Disabled). El costo de ruta externo se calcula según la velocidad de enlace del puerto si el valor configurado de External Port Path Cost es cero.
BPDU Guard Effect	Muestra el efecto de BPDU Guard, que deshabilita los puertos de borde que reciben paquetes BPDU. Los valores posibles son Enable o Disable.
Port Forwarding State	El estado de reenvío de este puerto.

Ver el estado de los puertos CST

Puede ver Common Spanning Tree (CST) e Internal Spanning Tree de un puerto específico del switch.

Para ver el estado de los puertos CST:

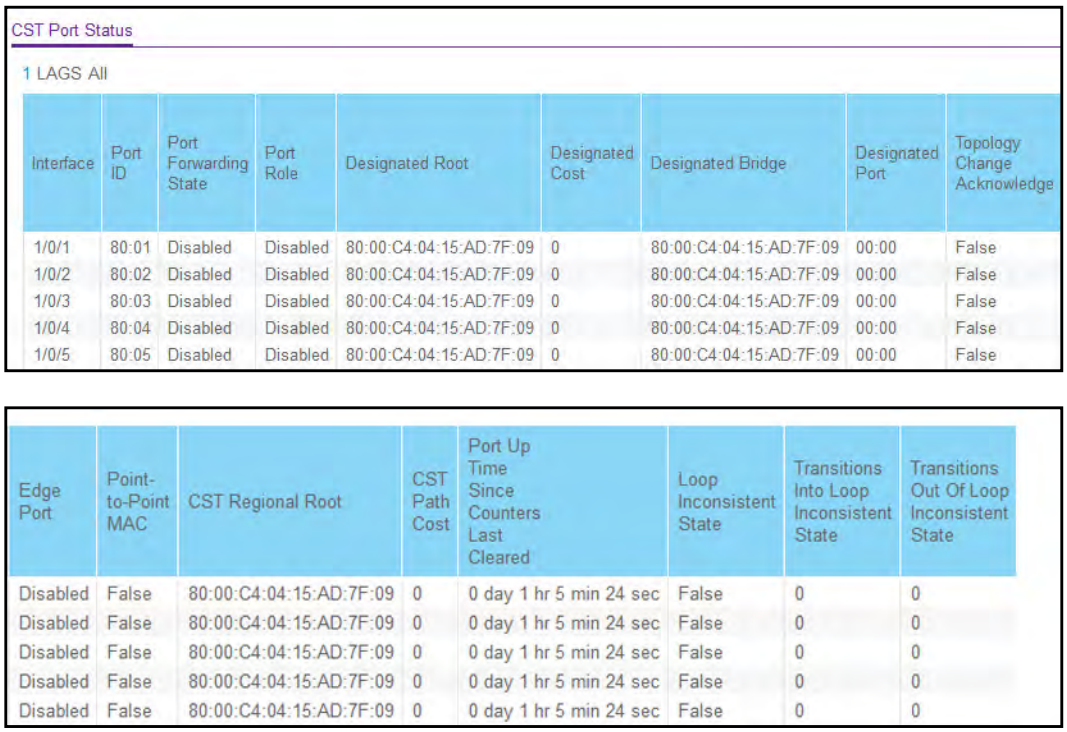
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > CST Port Status.



CST Port Status

1 LAGS All

Interface	Port ID	Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge
1/0/1	80:01	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/2	80:02	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/3	80:03	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/4	80:04	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/5	80:05	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False

Edge Port	Point-to-Point MAC	CST Regional Root	CST Path Cost	Port Up Time Since Counters Last Cleared	Loop Inconsistent State	Transitions Into Loop Inconsistent State	Transitions Out Of Loop Inconsistent State
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0

5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información de CST Status que se muestra en la página.

Tabla 78. Estado de puertos CST

Campo	Descripción
Interface	Identifica las interfaces físicas o de port channel asociadas con las VLAN asociadas con la CST.
Port ID	El identificador del puerto dentro de la CST. Se compone de la prioridad del puerto y el número de interfaz del puerto.
Port Forwarding State	El estado de reenvío de este puerto.
Port Role	A cada puerto de puente MST habilitado se le asigna un rol de puerto para cada spanning tree. El rol de puerto es uno de los siguientes valores: Root Port, Designated Port, Alternate Port, Backup Port, Master Port o Disabled Port.
Designated Root	Puente raíz de la CST. Se compone de la prioridad del puente y la dirección MAC base del puente.
Designated Cost	Costo de ruta que ofrece el puerto designado a la LAN.
Designated Bridge	Identificador del puente con el puerto designado. Se compone de la prioridad del puente y la dirección MAC base del puente.
Designated Port	Identificador del puerto en el puente designado que ofrece el menor costo a la LAN. Se compone de la prioridad del puerto y el número de interfaz del puerto.

Tabla 78. Estado de puertos CST (continuación)

Campo	Descripción
Topology Change Acknowledge	Indica si el indicador de confirmación de cambio de topología está activado en la siguiente BPDU que se transmitirá por este puerto. Es True o False.
Edge port	Indica si el puerto está habilitado como puerto de borde. Toma el valor Enabled o Disabled.
Point-to-point MAC	Valor derivado del estado punto a punto.
CST Regional Root	Identificador de puente de la raíz regional de la CST. Se compone de la prioridad del puente y la dirección MAC base del puente.
CST Path Cost	Costo de ruta hacia la raíz regional de la CST.
Port Up Time Since Counters Last Cleared	Tiempo desde que se borraron los contadores por última vez, en días, horas, minutos y segundos.
Loop Inconsistent State	Este parámetro indica si el puerto está o no en estado de inconsistencia de bucle.
Transitions Into Loop Inconsistent State	El número de veces que esta interfaz pasó al estado de inconsistencia de bucle.
Transitions Out Of Loop Inconsistent State	El número de veces que esta interfaz salió del estado de inconsistencia de bucle.

Configurar los ajustes de MST

Puede configurar Multiple Spanning Tree (MST) en el switch.

Para configurar una instancia MST:

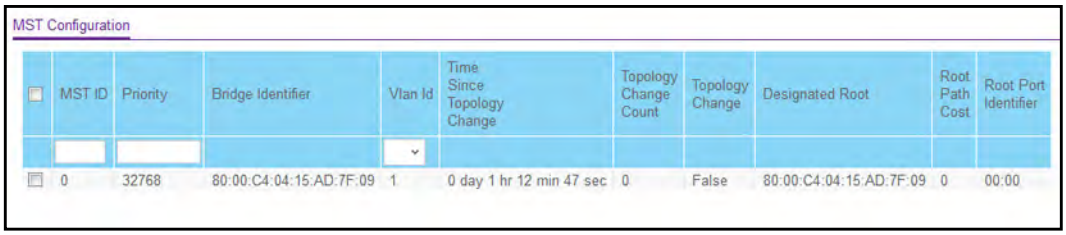
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > MST Configuration.



5. Para agregar una nueva MST, haga lo siguiente:

a. Configure los valores de MST:

- MST ID. Especifique el ID de la MST que se creará. Los valores válidos son de 1 a 4094. Solo es visible cuando se elige la opción de selección del cuadro MST ID.
- Priority. El valor de prioridad del puente para la 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 se intenta establecer cualquier valor entre 0 y 4095, se establece en 0. La prioridad predeterminada es 32768. El rango válido es 0–61440.
- VLAN ID. Muestra un cuadro combinado con cada VLAN del switch. Estas pueden seleccionarse o deseleccionarse para reconfigurar la asociación de las VLAN con las instancias MST.

b. Haga clic en el botón Add
Esto crea la nueva MST que configuró.
6. Para modificar una instancia MST, haga lo siguiente:

a. Seleccione la casilla junto a la instancia.

Puede seleccionar varias casillas para aplicar la misma configuración a todos los puertos seleccionados. b. Actualice los valores.
c. Haga clic en el botón Apply.

7. Para eliminar una instancia MST, haga lo siguiente:

a. Seleccione la casilla de la instancia.

b. Haga clic en el botón Eliminar (Delete).

Para cada instancia configurada, la página muestra la información descrita en la siguiente tabla.

Tabla 79. Configuración de MST

Campo	Descripción
Bridge Identifier	El identificador de puente de la instancia MST seleccionada. Se compone de la prioridad del puente y la dirección MAC base del puente.
Time Since Topology Change	El tiempo en segundos desde el último cambio de topología de la instancia MST seleccionada.
Topology Change Count	Número de veces que cambió la topología de la instancia MST seleccionada.
Topology Change	El valor del parámetro de cambio de topología del switch, que indica si hay un cambio de topología en curso en algún puerto asignado a la instancia MST seleccionada. Toma el valor True o False.
Designated Root	El identificador de puente del puente raíz. Se compone de la prioridad del puente y la dirección MAC base del puente

Tabla 79. Configuración de MST (continuación)

Campo	Descripción
Root Path Cost	Costo de ruta a la raíz designada para esta instancia MST.
Root PortIdentifier	Puerto para acceder a la raíz designada de esta instancia MST.

Ver el estado de puertos MST de Spanning Tree

Puede configurar y mostrar los ajustes de Multiple Spanning Tree (MST) de un puerto específico del switch.

Un puerto puede quedar deshabilitado por diagnóstico (D-Disable) cuando DOT1S sufre una condición de error grave. La causa más común es que el software DOT1S sufra una inundación de BPDU. El criterio de inundación es que DOT1S reciba más de 15 BPDU en un intervalo de 3 segundos. Las demás causas de D-Disable de DOT1S son muy poco frecuentes.

Para ver el estado de puertos MST de Spanning Tree:

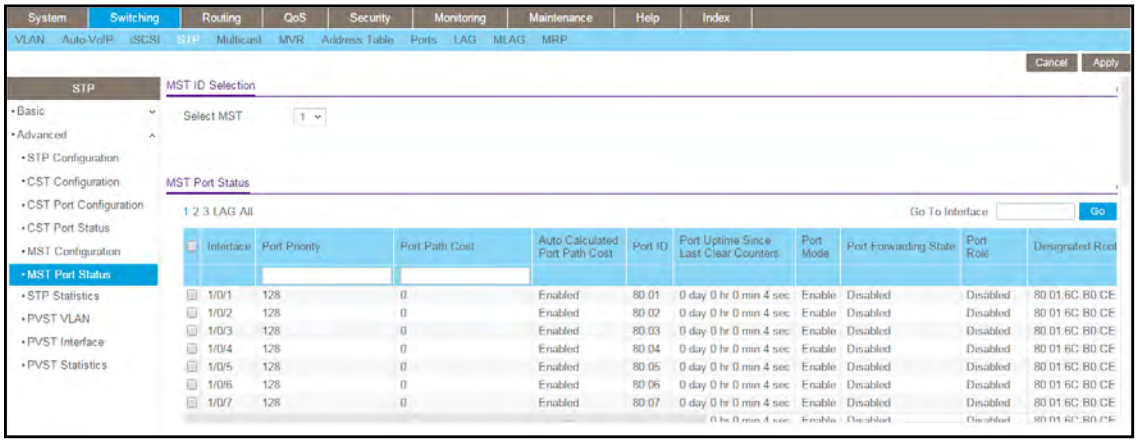
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > MST Port Status.



Nota: Si no se configuró ninguna instancia MST en el switch, la página muestra el mensaje No MSTs Available y no muestra los campos indicados en la tabla de descripción de campos siguiente.

5. Use MST ID para seleccionar una instancia MST entre las existentes.

6. Use Interface para seleccionar una de las interfaces físicas o de canal de puertos asociadas a las VLAN de la instancia MST seleccionada.

7. Use Port Priority para especificar la prioridad de un puerto dentro de la instancia MST seleccionada.

La prioridad del puerto se establece en múltiplos de 16. Por ejemplo, si intenta establecerla en cualquier valor entre 0 y 15, se establece en 0. Si intenta establecerla entre 16 y (2*16-1), se establece en 16, y así sucesivamente.

8. Use Port Path Cost para establecer un nuevo costo de ruta para el puerto especificado en la instancia MST seleccionada.

Admite un valor en el rango de 1 a 200000000.
9. Haga clic en el botón Apply.
La configuración se guarda.

La siguiente tabla describe la información de solo lectura de configuración de puertos MST que se muestra en la página Spanning Tree CST Configuration.

Tabla 80. Estado de puertos MST

Campo	Descripción
Auto Calculated Port Path Cost	Muestra si el costo de ruta se calcula automáticamente (Enable) o no (Disable). 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 especificado dentro de la instancia MST seleccionada. Se compone de la prioridad del puerto y el número de interfaz del puerto.
Port Uptime Since Last Clear Counters	Tiempo desde que se borraron los contadores por última vez, en días, horas, minutos y segundos.
Port Mode	Modo administrativo de Spanning Tree Protocol asociado al puerto o canal de puertos. Los valores posibles son Enable o Disable.
Port Forwarding State	El estado de reenvío de este puerto.
Port Role	A cada puerto de puente MST habilitado se le asigna un rol de puerto para cada spanning tree. El rol de puerto es uno de los siguientes valores: Root Port, Designated Port, Alternate Port, Backup Port, Master Port o Disabled Port.
Designated Root	Puente raíz de la instancia MST seleccionada. Se compone de la prioridad del puente y la dirección MAC base del puente.
Designated Cost	Costo de ruta que ofrece el puerto designado a la LAN.
Designated Bridge	Identificador del puente con el puerto designado. Se compone de la prioridad del puente y la dirección MAC base del puente.
Designated Port	Identificador del puerto en el puente designado que ofrece el menor costo a la LAN. Se compone de la prioridad del puerto y el número de interfaz del puerto.

Ver las estadísticas de STP

Puede ver información sobre el número y tipo de unidades de datos del protocolo de puente (BPDU) transmitidas y recibidas en cada puerto.

Para ver las estadísticas de Spanning Tree:

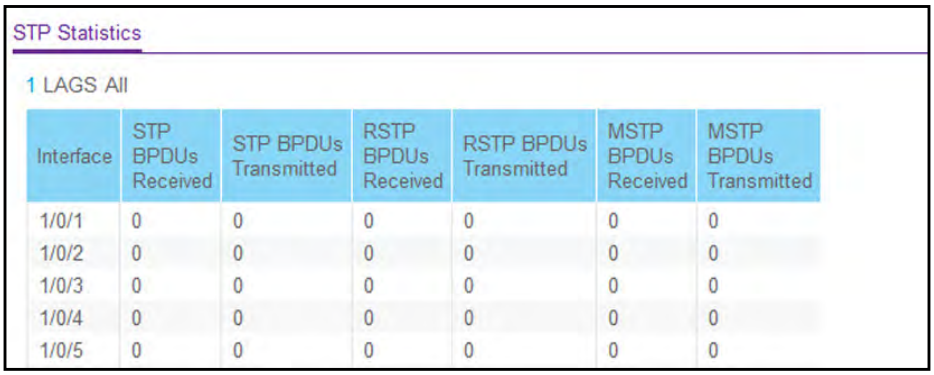
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching > STP > Advanced > STP Statistics.**



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información disponible en la página STP Statistics.

Tabla 81. Estadísticas de STP

Campo	Descripción
Interface	Selecciona una de las interfaces físicas o de canal de puertos del switch.
STP BPDUs Received	Número de BPDU STP recibidas en el puerto seleccionado.
STP BPDUs Transmitted	Número de BPDU STP transmitidas desde el puerto seleccionado.
RSTP BPDUs Received	Número de BPDU RSTP recibidas en el puerto seleccionado.
RSTP BPDUs Transmitted	Número de BPDU RSTP transmitidas desde el puerto seleccionado.
MSTP BPDUs Received	Número de BPDU MSTP recibidas en el puerto seleccionado.
MSTP BPDUs Transmitted	Número de BPDU MSTP transmitidas desde el puerto seleccionado.

Configurar los ajustes de VLAN de PVST

Puede ver y configurar los ajustes de VLAN de Per VLAN Spanning Tree Protocol (PVST)/Per VLAN Rapid Spanning Tree Protocol (RPVST) del dispositivo.

Para configurar los ajustes de VLAN de PVST/RPVST del dispositivo:

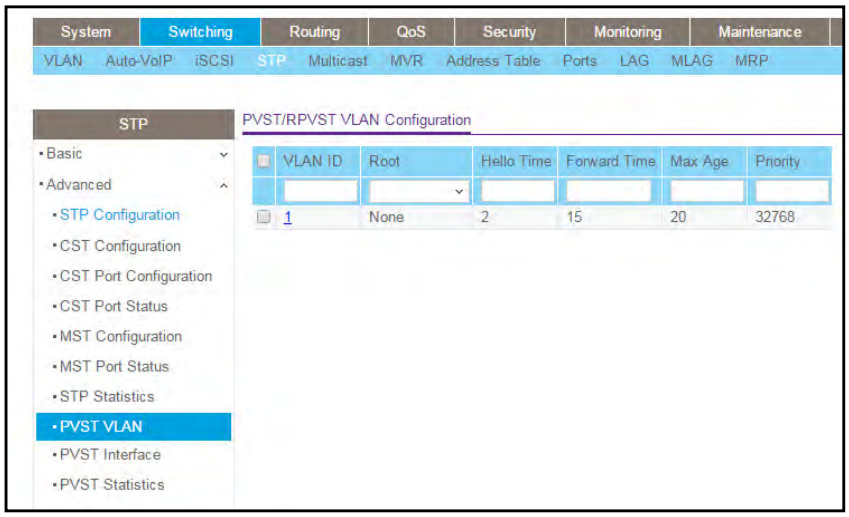
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > PVST VLAN en el menú de navegación.



5. Seleccione un VLAN ID, un identificador único de VLAN, de la lista de VLAN con STP Admin mode y PVST o RPVST habilitados.
6. En la lista Root, seleccione None, Primary o Secondary.

   El valor predeterminado es None. Este ajuste configura el switch para convertirse en puente raíz o puente raíz de reserva modificando la prioridad del puente del valor predeterminado 32768 a un valor menor calculado para asegurar que sea el puente raíz (o de reserva).

7. En el campo Hello Time, configure el intervalo hello de spanning tree para la VLAN especificada

   El tiempo hello es el intervalo entre el envío de BPDU sucesivas. Los valores permitidos van de 1 a 10 segundos. El valor predeterminado es 2 segundos.

8. En el campo Forward Time, configure el retardo de reenvío de spanning tree para la VLAN especificada.

   El rango es de 4 a 30 segundos. El valor predeterminado es 15 segundos. Es el tiempo de los estados de escucha y aprendizaje antes de que un puerto pase al estado de reenvío.

9. Use el campo Max Age para configurar la antigüedad máxima de spanning tree para la VLAN especificada.

   Max age es la antigüedad máxima antes de que un puerto de puente guarde su información de configuración. El rango es de 6 a 40 segundos. El valor predeterminado es 20 segundos.

10. Configure la prioridad (Priority) del puente de una VLAN.

    Los valores permitidos están entre 0 y 61440. Los valores válidos se indican en la siguiente tabla.

Tabla 82. Configuración de VLAN de PVST/RPVST - Prioridad de puente de VLAN

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 configurado no es uno de los especificados, se redondea al valor válido más cercano.

11. Haga clic en el botón Add.
PVST/RPVST se habilita para la VLAN seleccionada.
12. Haga clic en el botón Apply.
La configuración se guarda.

Configurar los ajustes de interfaz de PVST

Puede ver y configurar los ajustes de interfaz de Per VLAN Spanning Tree Protocol (PVST)/Per VLAN Rapid Spanning Tree Protocol (RPVST) del dispositivo.

Para configurar los ajustes de interfaz de PVST/RPVST:

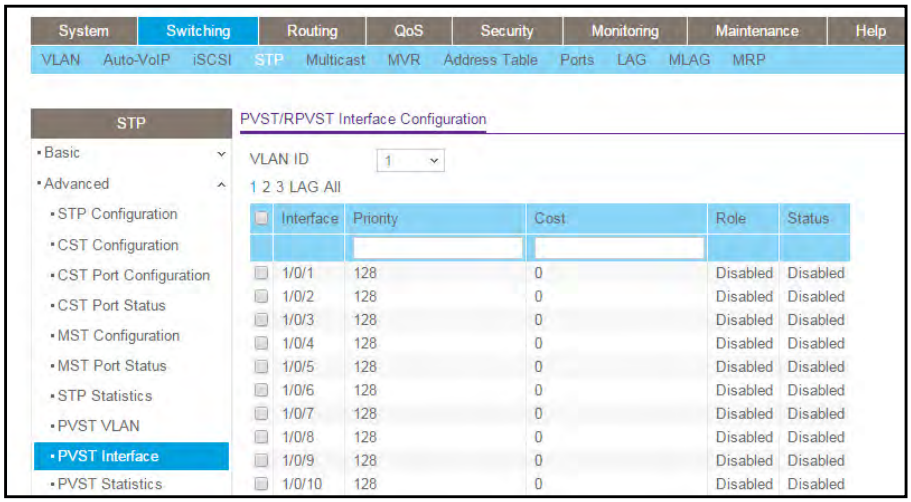
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > PVST Interface.



5. Seleccione un VLAN ID de la lista de VLAN con STP Admin mode y PVST o RPVST habilitados.

Nota: La opción Other se usa para configurar una VLAN que aún no se ha creado. Especifique el valor de VLAN ID y haga clic en el botón Apply para ver los valores reales.

6. Configure el valor de Priority, que permite al operador seleccionar la importancia relativa del puerto en el proceso de selección para el reenvío.

Establezca un número menor para dar preferencia a un puerto en el reenvío de tramas. Esta prioridad se usa cuando el puerto está configurado con tipo de enlace punto a punto. Los valores permitidos están entre 0 y 240. Los valores de prioridad se indican en la siguiente tabla. Los demás valores se redondean. El valor predeterminado es 128.

Nota: El valor debe ser múltiplo de 16.

Tabla 83. Valores de prioridad de configuración de interfaz PVST/RPVST

0	16	32
48	64	80
96	112	128 (predeterminado)
144	160	176
192	208	224
240	–	–

7. Per VLAN Cost es el costo de ruta del puerto al puente raíz.

   Los valores permitidos están entre 1 y 200,000,000. De forma predeterminada, el costo no está configurado. Use el valor 0 para quitar la configuración. Si no se configura el costo por VLAN, el costo de ruta se establece según la velocidad del enlace.

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

La siguiente tabla describe la información no configurable que muestra la página PVST/RPVST Interface Configuration.

Tabla 84. Configuración de interfaz de PVST/RPVST

Campo	Descripción
Interface	La lista de interfaces físicas y LAG.
Role	Indica el rol de la interfaz. Los valores posibles son: Disabled, Root, Designated, Alternate, Backup y Master. **Nota:** El campo aparece en blanco para la interfaz que no está incluida en la VLAN especificada.
Status	Indica el estado de la interfaz. Los valores posibles son: Discarding, Learning, Forwarding y Disabled. **Nota:** El campo aparece en blanco para la interfaz que no está incluida en la VLAN especificada.

Ver las estadísticas de PVST

Puede ver y configurar los ajustes de estadísticas de Per VLAN Spanning Tree Protocol (PVST)/Per VLAN Rapid Spanning Tree Protocol (RPVST) del dispositivo.

Para ver las estadísticas de PVST/RPVST:

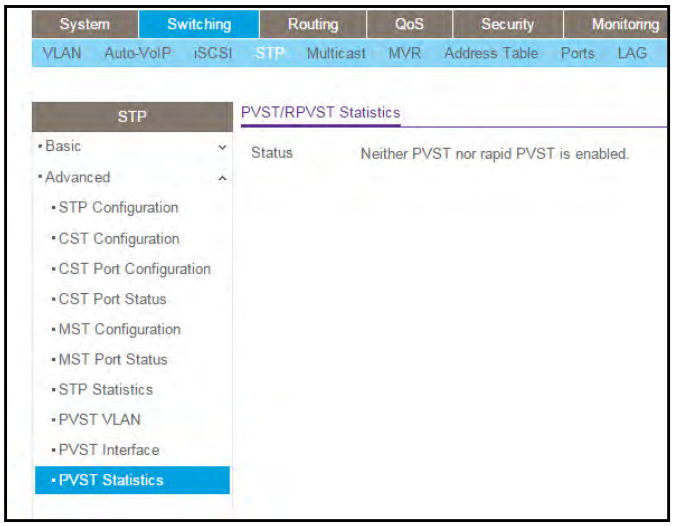
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > STP > Advanced > PVST Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

   El campo Status muestra Neither PVST nor Rapid-PVST is enabled. Si cambia el modo STP a PVST o RPVST, la página muestra información estadística.

Administrar multicast

El tráfico IP multicast es el tráfico destinado a un grupo de hosts. Los grupos de hosts se identifican por direcciones IP de clase D, que van de 224.0.0.0 a 239.255.255.255.

Ver la tabla MFDB

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 un par de VLAN ID y dirección MAC. Las entradas pueden contener datos de más de un protocolo.

Para ver la tabla MFDB:

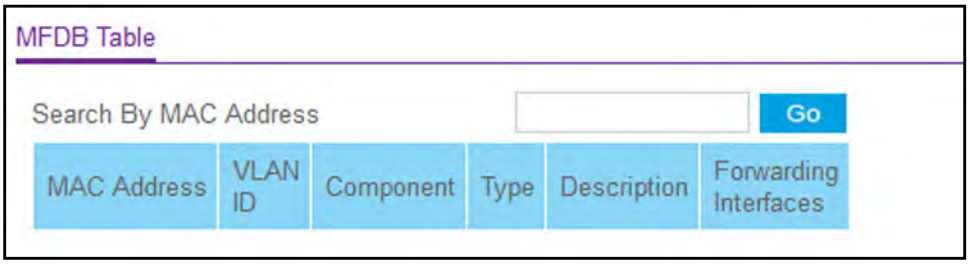
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching > Multicast > MFDB > MFDB Table.**



5. Use Search by MAC Address para escribir una dirección MAC.

   Escriba seis números hexadecimales de dos dígitos separados por dos puntos, por ejemplo 00:01:23:43:45:67.

6. Haga clic en el botón GO.
Si la dirección existe, se muestra esa entrada. Se requiere una coincidencia exacta.

Tabla 85. Tabla MFDB

Campo	Descripción
MAC Address	La dirección MAC multicast cuyos datos solicitó.
VLAN ID	El VLAN ID con el que está relacionada la dirección MAC multicast.
Type	Muestra el tipo de entrada. Las entradas estáticas son las que configura el usuario final. Las entradas dinámicas se agregan a la tabla como resultado de un proceso de aprendizaje o de un protocolo.
Component	El componente responsable de esta entrada en la base de datos de reenvío multicast. Los valores posibles son IGMP snooping, GMRP, Static Filtering y MLD snooping.
Description	La descripción de texto de esta entrada de la tabla multicast. Los valores posibles son Management Configured, Network Configured y Network Assisted.
Forwarding Interfaces	La lista de reenvío resultante se obtiene combinando todas las interfaces de reenvío y quitando las interfaces indicadas como interfaces de filtrado estático.

Ver las estadísticas de MFDB

Para ver las estadísticas de MFDB:

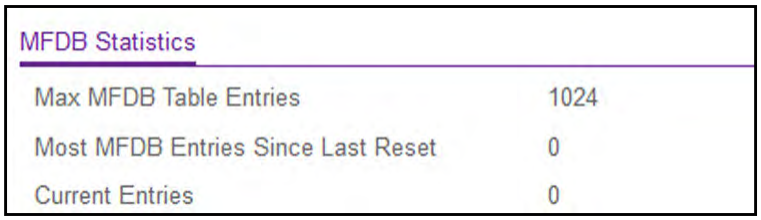
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. **Seleccione Switching > Multicast > MFDB > MFDB Statistics.**



La siguiente tabla describe los campos de MFDB Statistics.

Tabla 86. 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 marca máxima (high-water mark) de MFDB.
Current Entries	El número actual de entradas en la tabla de la base de datos de reenvío multicast.

Administrar IGMP snooping

Internet Group Management Protocol (IGMP) snooping es una función que permite al switch reenviar el tráfico multicast de forma inteligente. El tráfico IP multicast es el tráfico destinado a un grupo de hosts. Los grupos de hosts se identifican por direcciones IP de clase D; con estos mensajes, el switch reenvía el tráfico solo a los puertos que solicitan el tráfico multicast. Así se evita que el switch difunda el tráfico a todos los puertos y 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 dirección de destino de difusión o multicast, el switch reenvía una copia a cada uno de los demás segmentos de red conforme al estándar IEEE MAC Bridge. Finalmente, el paquete queda accesible para todos los nodos conectados a la red.

Este enfoque funciona bien para los paquetes de difusión que deben ser vistos o procesados por todos los nodos conectados. Sin embargo, en el caso de los paquetes multicast, puede provocar un uso menos eficiente del ancho de banda, sobre todo cuando el paquete está destinado solo a un pequeño número de nodos. Los paquetes se inundan en segmentos de red donde ningún nodo los necesita. Aunque los nodos rara vez tienen sobrecarga al filtrar paquetes dirigidos a direcciones de grupo no solicitadas, no pueden transmitir paquetes nuevos al medio compartido mientras se inunda el paquete multicast. 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 detecten (snoop) 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 del 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 del tráfico multicast. También puede configurar IGMP snooping manualmente (consulte Configurar IGMP snooping manualmente en la página 240).

Para configurar IGMP snooping automáticamente:

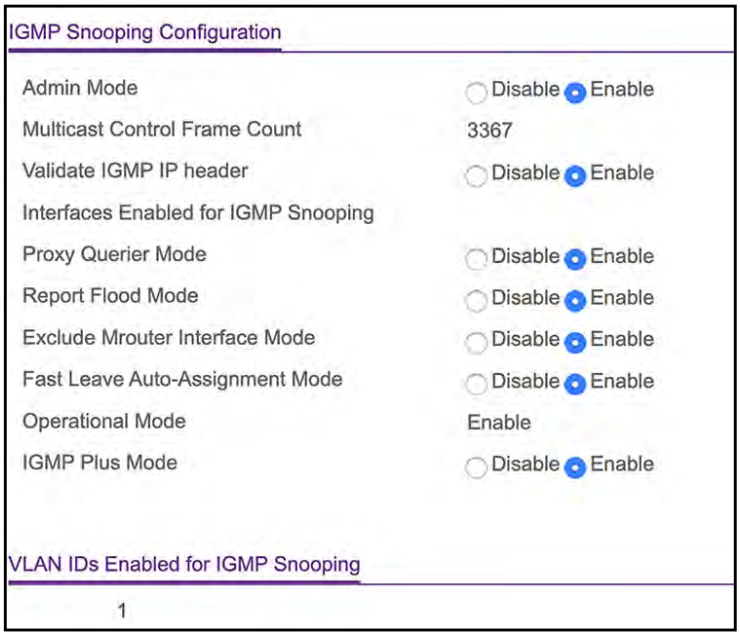
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching> Multicast > IGMP Snooping > Configuration.**



5. 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 240.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

La siguiente tabla muestra información sobre el estado global y las estadísticas de IGMP snooping en la página.

Tabla 87. Configuración de IGMP snooping

Campo	Descripción
Multicast Control Frame Count	Muestra el número de tramas de control multicast procesadas por el switch.
Interfaces Enabled for IGMP Snooping	Muestra las interfaces en las que IGMP snooping está habilitado.
Operational Mode	Muestra si IGMP snooping está habilitado o deshabilitado globalmente en el switch.
VLAN IDs Enabled For IGMP Snooping	Muestra 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 del tráfico multicast. También puede configurar IGMP snooping automáticamente (consulte Configurar IGMP snooping automáticamente con el modo IGMP Plus en la página 239).

Para configurar manualmente los ajustes de IGMP snooping:

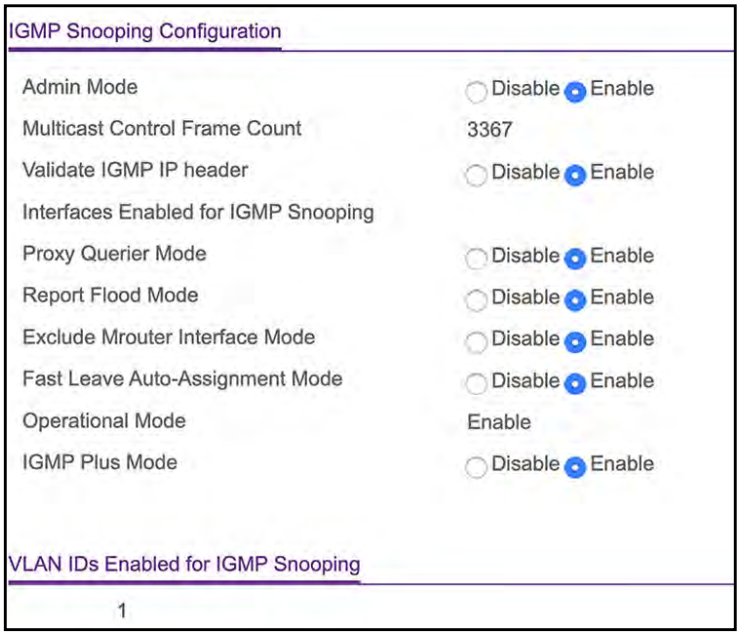
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. **Seleccione Switching> Multicast > IGMP Snooping > Configuration.**



5. Seleccione el botón de opción Admin Mode Enable o Disable.

   Esta opción habilita o deshabilita el modo administrativo de IGMP snooping en el switch. El valor predeterminado es Disable.

6. Seleccione el botón de opción Validate IGMP IP header Enable o Disable.

   Esta opción habilita o deshabilita la validación de encabezados para todas las versiones de IGMP en el switch. Si está habilitado, el encabezado IP IGMP de un paquete valida la opción Router Alert, ToS y TTL. El valor predeterminado es Enable.

7. 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.

8. 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.

9. 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 desconocidos a la interfaz mrouter ascendente.

10. 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 con el modo IGMP Plus en la página 239.

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

La siguiente tabla muestra información sobre el estado global y las estadísticas de IGMP snooping en la página.

Tabla 88. Configuración de IGMP snooping

Campo	Descripción
Multicast Control Frame Count	Muestra el número de tramas de control multicast procesadas por el switch.
Interfaces Enabled for IGMP Snooping	Muestra las interfaces en las que IGMP snooping está habilitado.
Operational Mode	Muestra si IGMP snooping está habilitado o deshabilitado globalmente en el switch.
VLAN IDs Enabled For IGMP Snooping	Muestra las VLAN en las que IGMP snooping está habilitado.

Configurar IGMP snooping para interfaces

Para configurar IGMP snooping para interfaces:

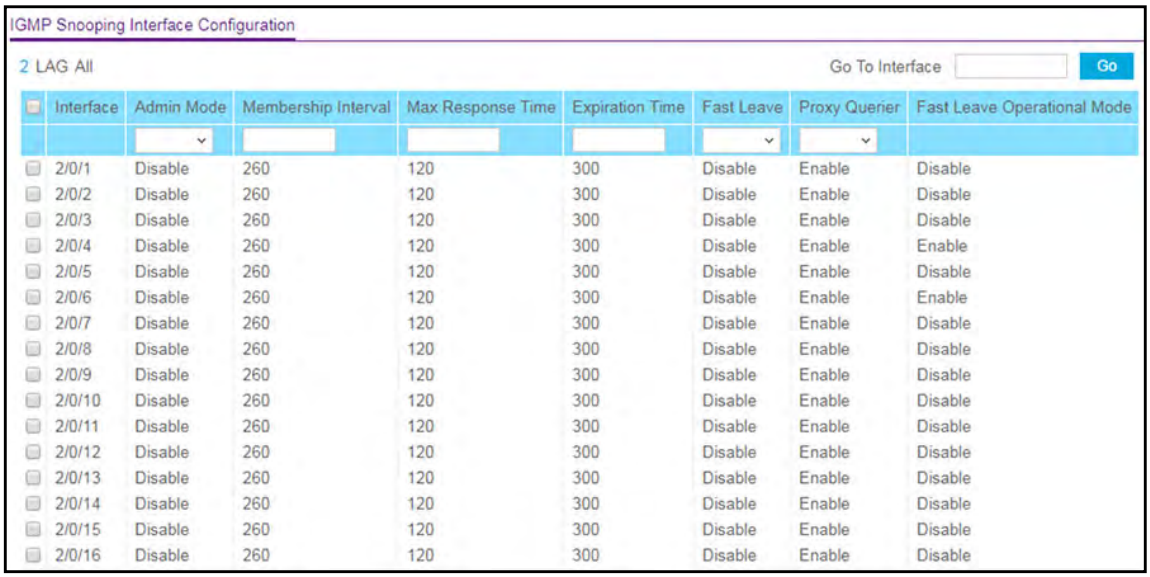
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > Interface Configuration.



Interface	Admin Mode	Membership Interval	Max Response Time	Expiration Time	Fast Leave	Proxy Querier	Fast Leave Operational Mode
2/0/1	Disable	260	120	300	Disable	Enable	Disable
2/0/2	Disable	260	120	300	Disable	Enable	Disable
2/0/3	Disable	260	120	300	Disable	Enable	Disable
2/0/4	Disable	260	120	300	Disable	Enable	Enable
2/0/5	Disable	260	120	300	Disable	Enable	Disable
2/0/6	Disable	260	120	300	Disable	Enable	Enable
2/0/7	Disable	260	120	300	Disable	Enable	Disable
2/0/8	Disable	260	120	300	Disable	Enable	Disable
2/0/9	Disable	260	120	300	Disable	Enable	Disable
2/0/10	Disable	260	120	300	Disable	Enable	Disable
2/0/11	Disable	260	120	300	Disable	Enable	Disable
2/0/12	Disable	260	120	300	Disable	Enable	Disable
2/0/13	Disable	260	120	300	Disable	Enable	Disable
2/0/14	Disable	260	120	300	Disable	Enable	Disable
2/0/15	Disable	260	120	300	Disable	Enable	Disable
2/0/16	Disable	260	120	300	Disable	Enable	Disable

La página muestra todas las interfaces físicas, VLAN y LAG.

5. 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, marque la casilla de la interfaz que desea configurar.
6. En el menú Admin Mode, seleccione Disable o Enable.

   Esta opción habilita o deshabilita el modo administrativo de IGMP snooping en la interfaz. El valor predeterminado es Disable.

7. 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.

8. 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.

9. 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 entre 0 y 3600 segundos. El valor predeterminado es 0 segundos, que indica un tiempo de espera infinito (sin expiración).

10. 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.

11. 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.

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

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 240).

Para configurar IGMP snooping para VLAN automáticamente:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > IGMP VLAN Configuration.



5. Seleccione la casilla junto al VLAN ID.

6. En el menú IGMP Plus Mode, 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:

   - Admin mode
   - Exclude Mrouter Interface Mode
   - Fast-Leave
   - Report Flood Mode

- Proxy Querier
- Querier Election 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 245.

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

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 244).

Para configurar manualmente los ajustes de IGMP snooping para VLAN:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > IGMP VLAN Configuration.



5. Para habilitar IGMP snooping en una VLAN, haga lo siguiente:

   a. Seleccione la casilla junto al VLAN ID.

   b. Configure los ajustes de IGMP snooping:

   - Admin Mode. En el menú, seleccione si desea habilitar o deshabilitar IGMP snooping en la VLAN. El valor predeterminado es Disable.
   - Fast Leave. En el menú, 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.

- Membership Interval. Especifique 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.
- Maximum Response Time. Especifique 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 de Maximum Response Time debe ser mayor que el valor del campo Group Membership Interval.
- Multicast Router Expiry Time. Especifique el tiempo de expiración del router multicast de IGMP snooping para la VLAN. El rango debe ser de 0 a 3600 segundos.
- Report Suppression. En el menú, seleccione si desea habilitar o deshabilitar el modo de supresión de informes de IGMP snooping en la VLAN. Este modo permite la supresión de 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.
- Proxy Querier. En el menú, seleccione si desea habilitar o deshabilitar el proxy querier para la VLAN. Si se deshabilita, no se envía la consulta proxy IGMP con IP de origen 0.0.0.0 en respuesta a un paquete IGMP leave. El valor predeterminado es Enable.
- Report Flood Mode. En el menú, seleccione si desea habilitar o deshabilitar el modo de inundación de informes en la VLAN. Si se habilita, 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.
- Exclude Mrouter Interface Mode. En el menú, seleccione si desea habilitar o deshabilitar Exclude Mrouter Interface Mode. Esta opción especifica el tipo de información que se reenvía a la interfaz de router multicast ascendente.

  Si se habilita, 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 pertenencia IGMPv1 o IGMPv2. La VLAN descarta los flujos multicast desconocidos. El valor predeterminado es Enable.

  Si se deshabilita, 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 244.

c. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
6. Para deshabilitar manualmente IGMP snooping en una VLAN, haga lo siguiente:

a. Seleccione la casilla junto al VLAN ID.

b. Haga clic en el botón Eliminar (Delete).
La VLAN se elimina de la lista.

7. Para modificar manualmente los ajustes de IGMP snooping de una VLAN, haga lo siguiente:

a. Marque la casilla junto al ID de VLAN.

b. Actualice los ajustes. c.
Haga clic en el botón Apply
(Aplicar). La configuración
se guarda.

Configurar un router multicast

Puede configurar la interfaz como aquella a la que está conectado el router multicast. Todos los paquetes IGMP que el switch intercepta se reenvían al router multicast accesible desde esta interfaz. Normalmente esta configuración no es necesaria, ya que el switch detecta automáticamente el router multicast y reenvía los paquetes IGMP en consecuencia. Solo es necesaria si desea asegurarse de que el router multicast reciba siempre los paquetes IGMP del switch en una red compleja.

Para configurar un router multicast:

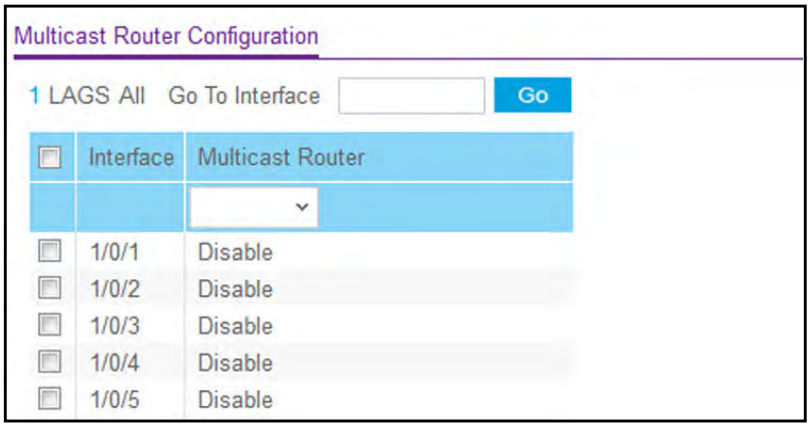
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > Multicast Router Configuration.



5. Use Interface para seleccionar la interfaz física.

6. En el campo Multicast Router, seleccione Enable o Disable.

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

Configurar una VLAN de router multicast

Puede configurar una interfaz para que reenvíe los paquetes IGMP interceptados de una VLAN específica solo al router multicast conectado a la interfaz. Normalmente esta configuración no es necesaria, ya que el switch detecta automáticamente un router multicast y reenvía los paquetes IGMP en consecuencia. Solo es necesaria si desea asegurarse de que el router multicast reciba siempre los paquetes IGMP del switch en una red compleja.

Para configurar una VLAN de router multicast:

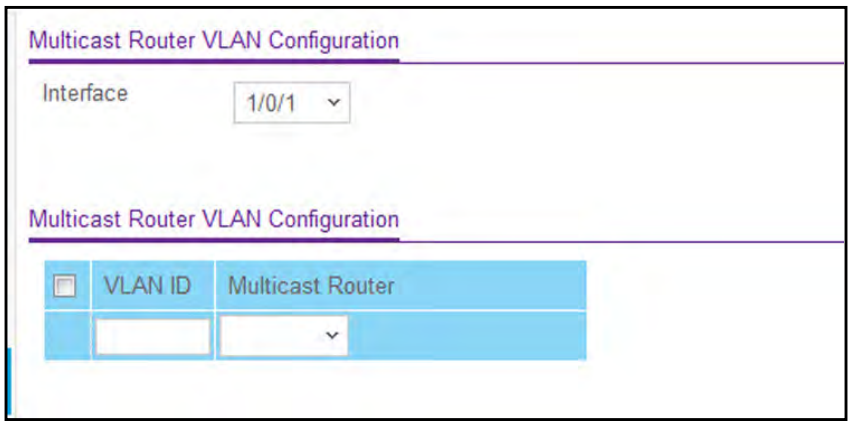
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > Multicast Router VLAN Configuration.



5. Use Interface para seleccionar la interfaz.
6. Use VLAN ID para seleccionar el ID de VLAN.

7. En el campo Multicast Router, seleccione Enable o Disable.

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

Descripción general del querier 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 pertenencias multicast. Este dispositivo central es el querier IGMP. Las respuestas a las consultas IGMP, llamadas informes IGMP, mantienen al switch actualizado sobre la pertenencia actual a grupos multicast puerto por puerto. Si el switch no recibe información de pertenencia actualizada a tiempo, deja de reenviar multicast al puerto donde se encuentra el dispositivo final.

Puede configurar y mostrar información de los queriers de IGMP snooping en la red y, por separado, en las VLAN.

Configurar el querier de IGMP snooping

Puede configurar los parámetros del querier de IGMP snooping.

Para configurar los ajustes del querier de IGMP snooping:

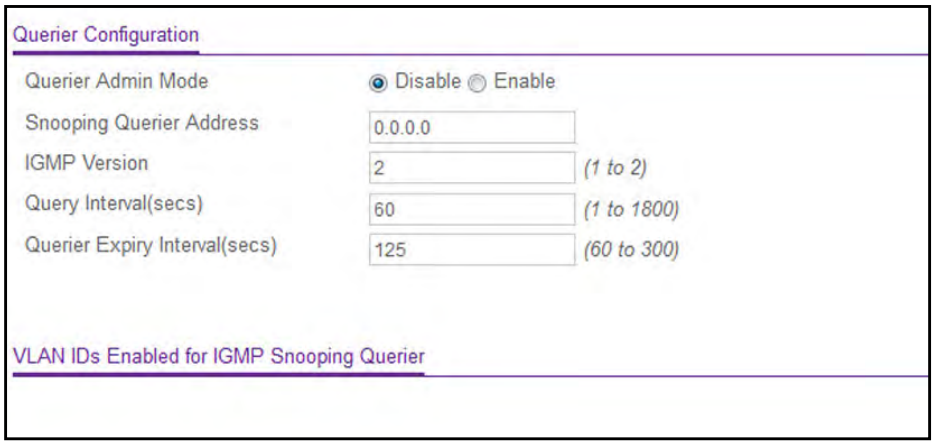
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > Querier Configuration.



5. Use Querier Admin Mode para seleccionar el modo administrativo de IGMP snooping del switch.

   El valor predeterminado es Disable.

6. En el campo Snooping Querier IP Address, escriba una dirección IP.

Especifica la dirección del snooping querier 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 envía la consulta.

7. Use IGMP Version para especificar la versión del protocolo IGMP usada en las consultas IGMP periódicas. El rango es de 1 a 2. El valor predeterminado es 2.

8. Use Query Interval(secs) para especificar el intervalo en segundos entre las consultas periódicas que envía el snooping querier.

El intervalo de consulta debe estar en el rango de 1 a 1800. El valor predeterminado es 60.

9. Use Querier Expiry Interval(secs) para especificar el intervalo en segundos tras el cual se elimina la información del último querier.

El intervalo de expiración del querier debe estar en el rango de 60 a 300. El valor predeterminado es 125.

10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La página muestra los VLAN ID habilitados para el consultor de IGMP snooping.

Configurar el querier de IGMP snooping para VLAN

Puede configurar queriers IGMP para usarlos con las VLAN de la red.

Para configurar los ajustes de VLAN del querier:

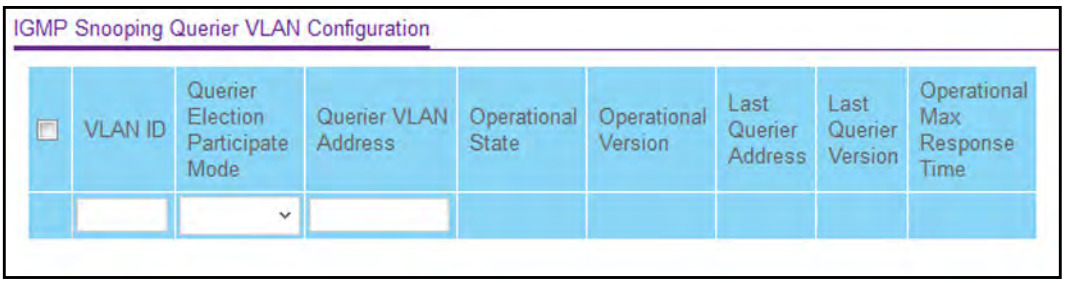
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching> Multicast > IGMP Snooping > Querier VLAN Configuration.



5. Para crear un nuevo ID de VLAN para IGMP snooping, seleccione New Entry en el campo VLAN ID y complete los siguientes campos.

También puede establecer parámetros preconfigurables del snooping querier.

- VLAN ID. ID de la VLAN en la que se habilitará el querier de IGMP snooping.
- Querier Election Participate Mode. Habilita o deshabilita el modo de participación del querier.
  - Disabled. Al detectar otro querier de la misma versión en la VLAN, el snooping querier pasa al estado non-querier.
  - Enabled. El snooping querier participa en la elección de querier, en la que la dirección IP más baja funciona como querier en esa VLAN. El otro querier pasa al estado non-querier.
- Snooping Querier VLAN Address. Especifique la dirección IP del snooping querier que se usará como dirección de origen en las consultas IGMP periódicas enviadas en la VLAN especificada.

6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 89. Configuración de VLAN del querier

Campo	Descripción
Estado operativo	Estado operativo del querier de IGMP snooping en una VLAN. Puede estar en cualquiera de los siguientes estados: • Querier: el switch de snooping es el querier en 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 snooping querier no está operativo en la VLAN. El snooping querier pasa al modo deshabilitado cuando IGMP snooping no está operativo en la VLAN o cuando no está configurada la dirección del querier ni la dirección de administración de red.
Versión operativa	Versión operativa del protocolo IGMP del querier.
Dirección del último querier	Dirección IP del último querier del que se interceptó una consulta en la VLAN.
Versión del último querier	Versión del protocolo IGMP del último querier del que se interceptó una consulta en la VLAN.
Tiempo máx. de respuesta operativo	Muestra el tiempo máximo de respuesta que se usará en las consultas que envía el snooping querier.

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 para el tráfico multicast. También puede configurar MLD snooping manualmente (consulte Configurar MLD snooping manualmente en la página 253).

Para configurar MLD snooping automáticamente:

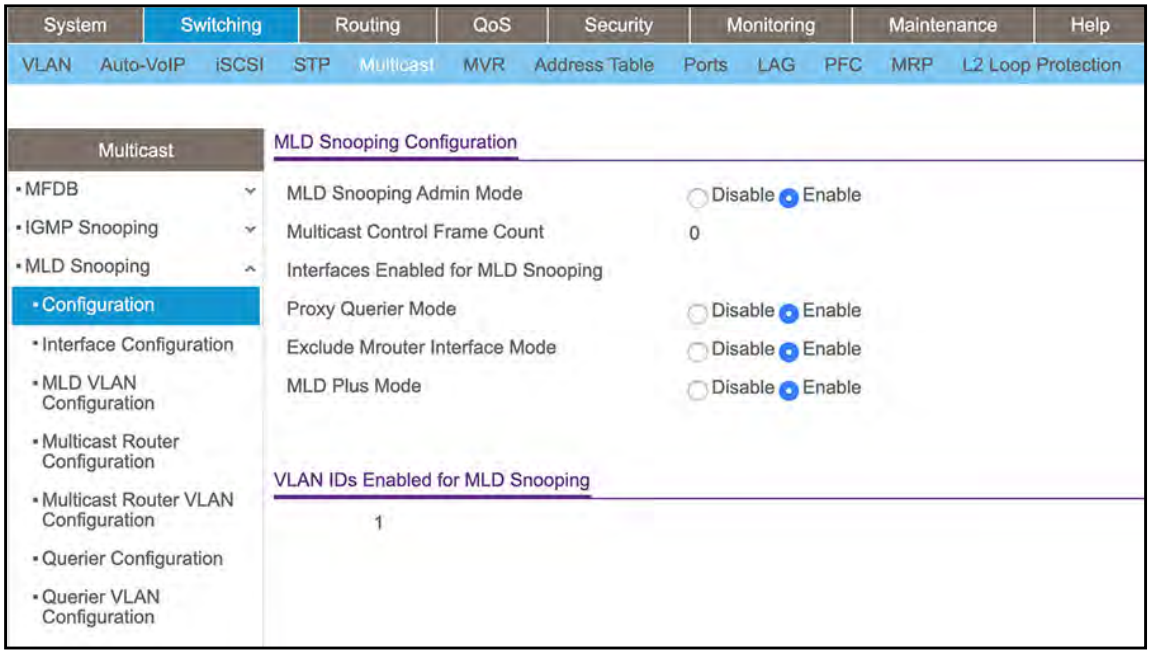
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Configuration.



5. Seleccione el botón de opción MLD Plus Mode Enable o Disable. Si se habilita, se habilitan automáticamente los siguientes modos de MLD snooping:

- 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 253.

6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
En la siguiente tabla se describen los campos no configurables de MLD Snooping Configuration.

Tabla 90. Configuración de MLD snooping

Campo	Definición
Conteo de tramas de control multicast	Número de tramas de control multicast procesadas por la CPU.
Interfaces con MLD snooping habilitado	Una o más interfaces en las que MLD snooping está habilitado administrativamente. MLD snooping debe estar habilitado globalmente y en una interfaz para que la interfaz pueda interceptar paquetes MLD y determinar qué segmentos deben recibir los paquetes multicast dirigidos a la dirección de grupo.
ID de VLAN con MLD snooping habilitado	Muestra una o más VLAN en las 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 para el tráfico multicast. También puede configurar MLD snooping automáticamente (consulte Configurar MLD snooping automáticamente con el modo MLD Plus en la página 252).

Para configurar manualmente los ajustes de MLD snooping:

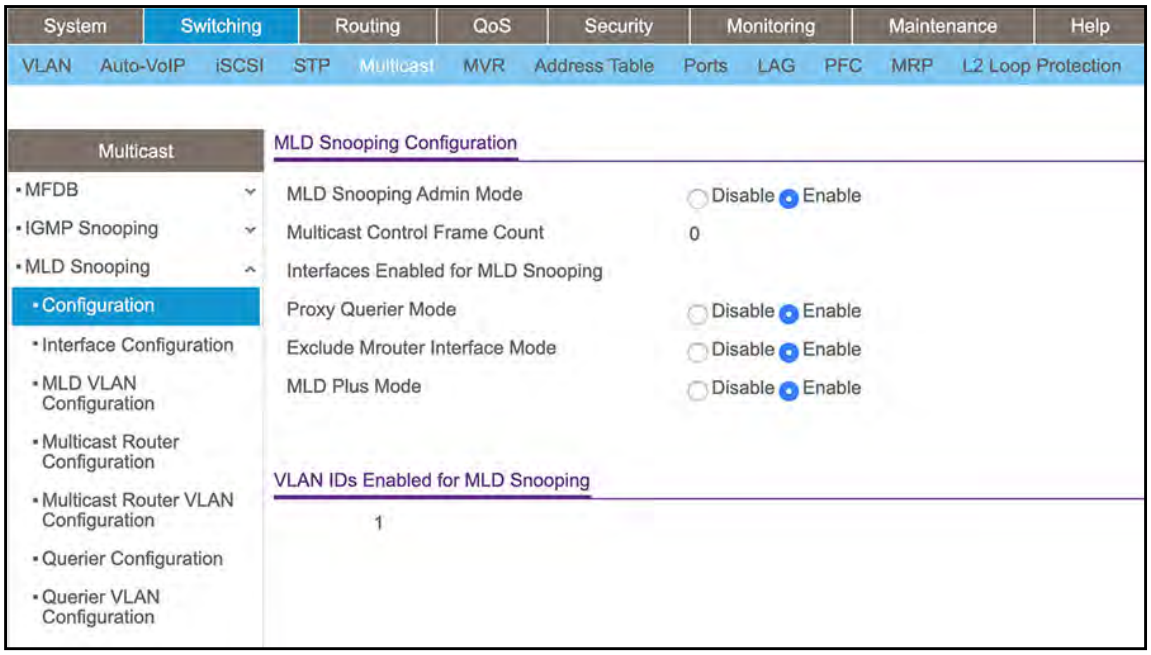
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Configuration.



5. Seleccione el botón de opción MLD Snooping Admin Mode Enable o Disable para especificar el modo administrativo de MLD snooping del switch. El valor predeterminado es Disable.

6. Seleccione el botón de opción Proxy Querier Mode Enable o Disable.

   Esto habilita o deshabilita un proxy querier MLD en el sistema. Si se deshabilita, no se envía la consulta proxy MLD con IP de origen 0::0 en respuesta a un paquete MLD leave. Si se habilita, se envían consultas proxy MLD. El valor predeterminado es Enable.

7. 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 se habilita, 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 se permite que las PDU MLD pasen por el puerto mrouter hacia la interfaz del router ascendente.

   El valor predeterminado es Enable. Si se deshabilita, 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 252.

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

En la siguiente tabla se describen los campos no configurables de MLD Snooping Configuration.

Tabla 91. Configuración de MLD snooping

Campo	Definición
Conteo de tramas de control multicast	Número de tramas de control multicast procesadas por la CPU.
Interfaces con MLD snooping habilitado	Una o más interfaces en las que MLD snooping está habilitado administrativamente. MLD snooping debe estar habilitado globalmente y en una interfaz para que la interfaz pueda interceptar paquetes MLD y determinar qué segmentos deben recibir los paquetes multicast dirigidos a la dirección de grupo.
ID de VLAN con MLD snooping habilitado	Muestra una o más VLAN en las que MLD snooping está habilitado administrativamente.

Configurar una interfaz de MLD snooping

Para configurar una interfaz de MLD snooping:

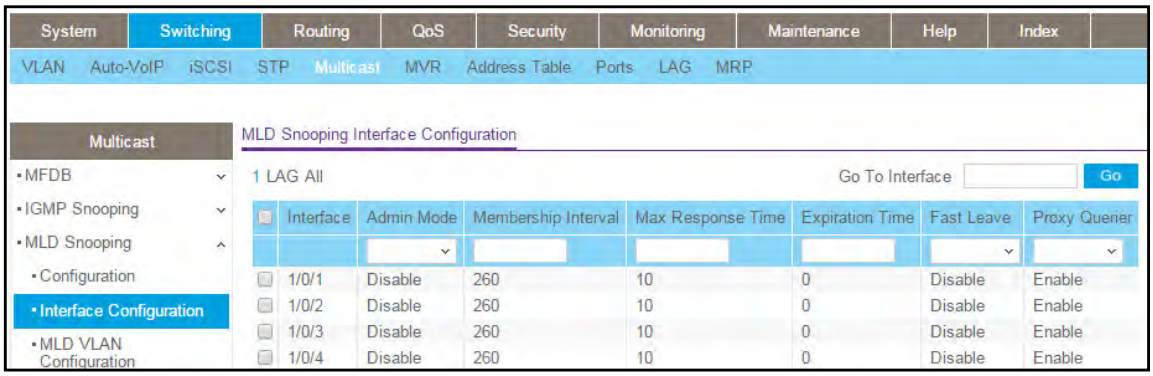
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Interface Configuration.



   Se muestran todas las interfaces físicas, VLAN y LAG.

5. 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, marque la casilla de la interfaz que desea configurar.

  Todas las interfaces físicas, VLAN y LAG se muestran en la columna Interface.

6. Use Admin Mode para seleccionar el modo de MLD snooping de la interfaz seleccionada del switch. El valor predeterminado es Disable.
7. Use Group Membership Interval(secs) para especificar el tiempo que el switch debe esperar un informe de un grupo en una interfaz antes de eliminar esa interfaz del grupo.

   El rango válido es de 2 a 3600 segundos. El valor configurado debe ser mayor que Max Response Time. El valor predeterminado es 260 segundos.

8. Use Max Response Time (secs) para especificar el tiempo que el switch debe esperar después de enviar una consulta en una interfaz porque no recibió un informe de un grupo en esa interfaz.

   Introduzca un valor mayor o igual a 1 y menor que el intervalo de pertenencia al grupo en segundos. El valor predeterminado es 10 segundos. El valor configurado debe ser menor que el intervalo de pertenencia al grupo.

9. Use Present Expiration Time para especificar 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 0 segundos. Un valor de cero indica un tiempo de espera infinito, es decir, sin expiración.

10. Fast Leave Admin Mode es el modo administrativo de Fast Leave en la interfaz.

    Si Fast Leave está habilitado, la interfaz puede eliminarse de inmediato de la entrada de la tabla de reenvío de capa 2 al recibir un mensaje MLD leave para un grupo multicast, sin enviar primero consultas generales basadas en MAC. El valor predeterminado es Disable.

11. Seleccione Enable o Disable para Proxy Querier Mode en una interfaz específica.

    Si el modo está deshabilitado, no se envía la 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.

12. Haga clic en el botón Apply.

La configuración se guarda.

Configurar MLD snooping para VLAN automáticamente con el modo MLD Plus

El modo MLD Plus le permite configurar automáticamente MLD snooping para VLAN, que se usa para crear listas de reenvío para el tráfico multicast. También puede configurar MLD snooping para VLAN manualmente (consulte Configurar IGMP snooping manualmente en la página 240).

Para configurar MLD snooping en las VLAN automáticamente:

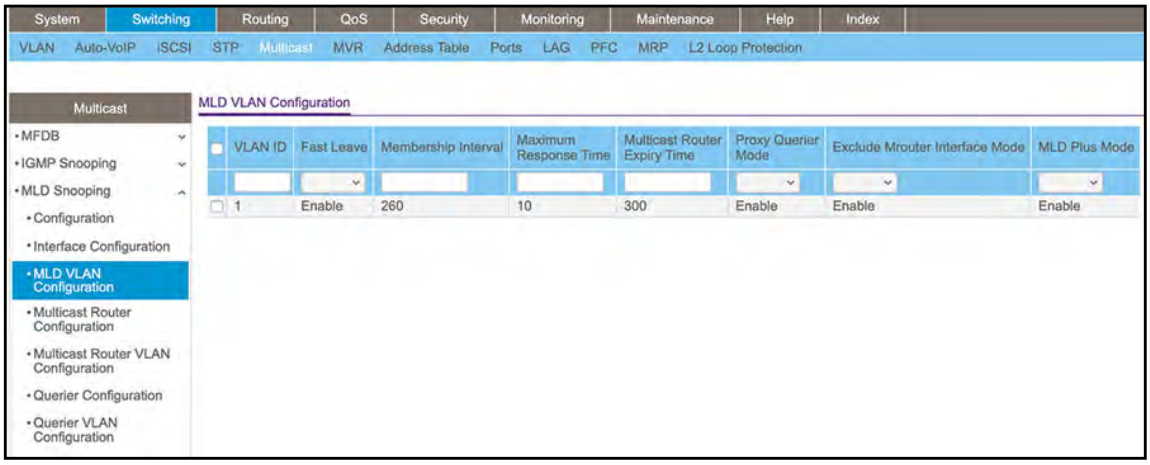
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > MLD VLAN Configuration.



5. Marque la casilla del ID de VLAN en el que se debe habilitar MLD snooping.
6. En el menú MLD Plus Mode, seleccione si desea habilitar o deshabilitar el modo MLD Plus en la VLAN.

   Si se habilita, se habilitan automáticamente los siguientes modos de MLD snooping para 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 para VLAN manualmente en la página 258.

7. Haga clic en Add para habilitar MLD snooping en la VLAN especificada.
8. Haga clic en el botón Apply (Aplicar).

La configuración se guarda.

Configurar MLD snooping para VLAN manualmente

Puede configurar manualmente los ajustes de MLD snooping para VLAN, que se usa para crear listas de reenvío para el tráfico multicast. También puede configurar MLD snooping para VLAN automáticamente (consulte Configurar MLD snooping para VLAN automáticamente con el modo MLD Plus en la página 256).

Para configurar manualmente los ajustes de MLD snooping para VLAN:

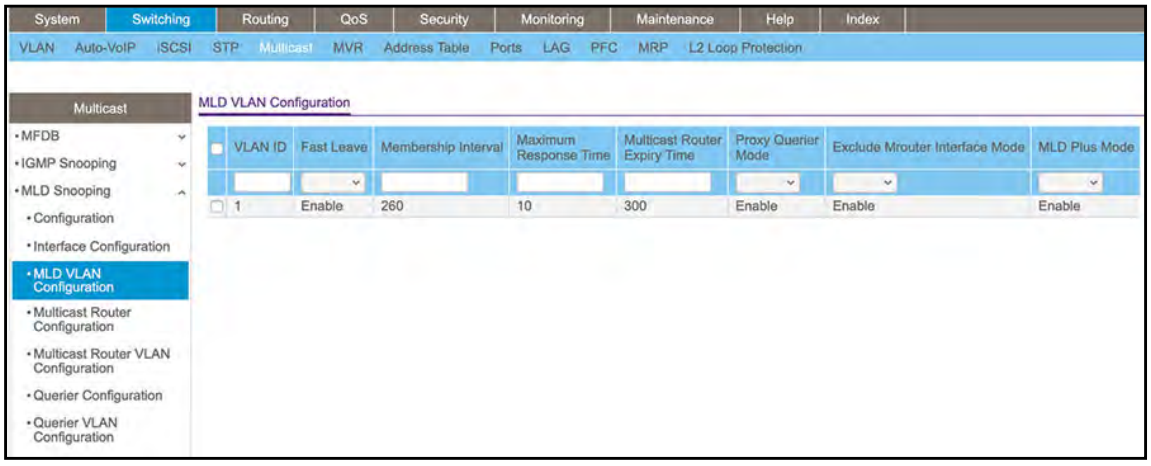
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > MLD VLAN Configuration.



5. Marque la casilla del ID de VLAN en el que se debe habilitar MLD snooping.
6. En el menú Fast Leave, seleccione si desea habilitar o deshabilitar el modo Fast Leave de MLD snooping para el ID de VLAN especificado.
7. En el campo Membership Interval, especifique el valor del intervalo de pertenencia al grupo de MLD snooping para el ID de VLAN especificado.

   El rango válido es de (Maximum Response Time + 1) a 3600.

8. En el campo Maximum Response Time, especifique el valor del tiempo máximo de respuesta de MLD snooping para el ID de VLAN especificado.

   El rango válido es de 1 a (Group Membership Interval –1). Su valor debe ser menor que el intervalo de pertenencia al grupo.

9. En el campo Multicast Router Expiry Time, especifique el valor del tiempo de expiración del router multicast de MLD snooping para el ID de VLAN especificado.

El rango válido es de 0 a 3600.

10. En el menú Proxy Querier Mode, seleccione si desea habilitar o deshabilitar el modo proxy querier para el ID de VLAN especificado.

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.

11. En el menú Exclude Mrouter Interface Mode, seleccione si desea habilitar o deshabilitar 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 se permite que las PDU MLD pasen 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 para VLAN, consulte Configurar MLD snooping para VLAN automáticamente con el modo MLD Plus en la página 256.

12. Haga clic en Add para habilitar MLD snooping en la VLAN especificada.
13. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Habilitar o deshabilitar un router multicast en una interfaz

Para habilitar o deshabilitar un router multicast en una interfaz:

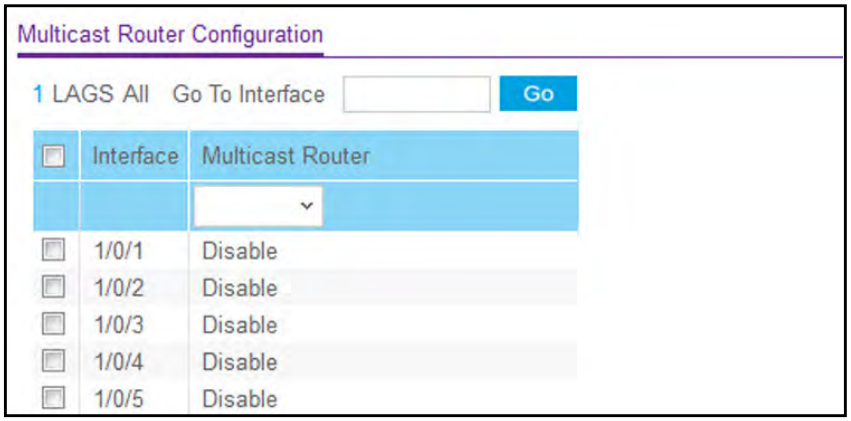
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Multicast Router Configuration.



5. En el menú Interface, seleccione la interfaz en la que desea habilitar o deshabilitar la configuración de router multicast.

6. En el menú Multicast Router, seleccione Enable o Disable.

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

Configurar los ajustes de VLAN de router multicast

Para configurar los ajustes de VLAN de router multicast:

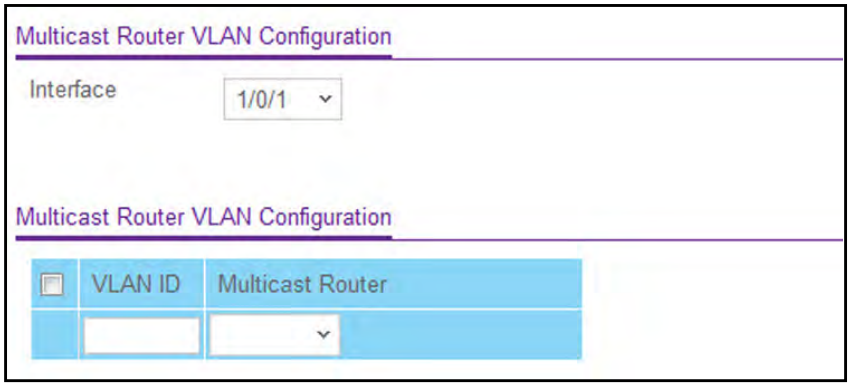
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Multicast Router VLAN Configuration.



5. En el menú Interface, seleccione la interfaz en la que desea habilitar o deshabilitar la configuración de router multicast.

6. Use el campo VLAN ID para especificar el ID de VLAN en el que desea habilitar o deshabilitar la configuración de router multicast.

7. En el menú Multicast Router, seleccione Enable o Disable.

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

Configurar el querier de MLD snooping

Puede configurar los parámetros de un querier de MLD snooping.

Para configurar un querier de MLD snooping:

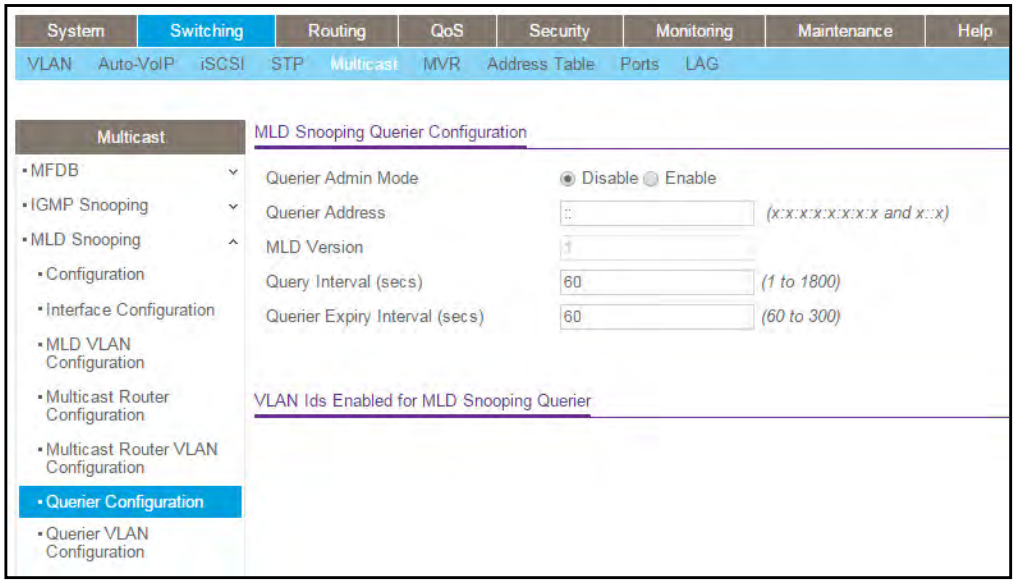
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Querier Configuration.



5. Use Querier Admin Mode para seleccionar el modo administrativo de MLD snooping del switch. El valor predeterminado es Disable.

6. Use Querier Address para especificar la dirección del snooping querier 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 envía la consulta. Los formatos IPv6 admitidos son x:x:x:x:x:x:x:x y x::x.

7. Use MLD Version para especificar la versión del protocolo MLD usada en las consultas MLD periódicas.

8. Use Query Interval(secs) para especificar el intervalo en segundos entre las consultas periódicas que envía el snooping querier.

   El intervalo de consulta debe estar en el rango de 1 a 1800. El valor predeterminado es 60.

9. Use Querier Expiry Interval(secs) para especificar el intervalo en segundos tras el cual se elimina la información del último querier.

   El intervalo de expiración del querier debe estar en el rango de 60 a 300. El valor predeterminado es 60. La página muestra los ID de VLAN habilitados para el querier de MLD snooping.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar los ajustes de VLAN del querier de MLD snooping

Para configurar los ajustes de VLAN del querier de MLD snooping:

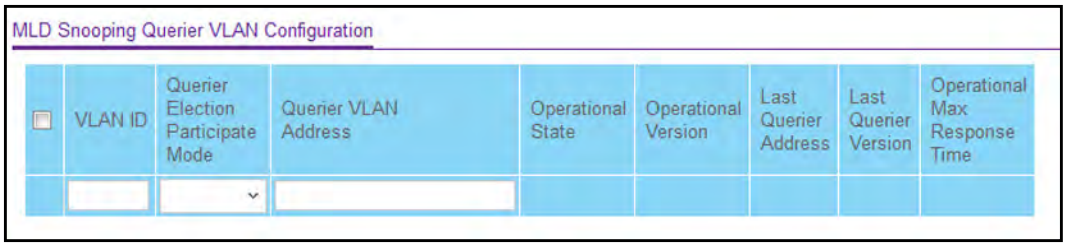
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> Multicast > MLD Snooping > Querier VLAN Configuration.



5. Use VLAN ID para seleccionar el ID de VLAN en el que el querier de MLD snooping está habilitado administrativamente y que existe en la base de datos de VLAN.
6. Use Querier Election Participate Mode para habilitar o deshabilitar la participación del querier de MLD snooping en la elección.

Si este modo está deshabilitado, al detectar otro querier de la misma versión en la VLAN, el snooping querier pasa al estado non-querier. Si este modo está habilitado, el snooping querier participa en la elección de querier, en la que gana la dirección IP más baja y funciona como querier en esa VLAN. El otro querier pasa al estado non-querier.

7. Use Querier VLAN Address para especificar la dirección del snooping querier que se usará como dirección de origen en las consultas MLD periódicas enviadas en la VLAN especificada.

8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 92. Configuración de VLAN del querier

Campo	Descripción
Estado operativo	Estado operativo del querier de MLD snooping en una VLAN. Puede estar en cualquiera de los siguientes estados: • Querier: el switch de snooping es el querier en la VLAN. El switch envía consultas periódicas con un intervalo igual al intervalo de consulta configurado. Si el switch detecta 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 snooping querier no está operativo en la VLAN. El snooping 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.
Versión operativa	Versión operativa del protocolo MLD del querier.
Dirección del último querier	Dirección IP del último querier del que se interceptó una consulta en la VLAN.
Versión del último querier	Versión del protocolo MLD del último querier del que se interceptó una consulta en la VLAN.
Tiempo máx. de respuesta operativo	Muestra el tiempo máximo de respuesta que se usará en las consultas que envía el snooping querier.

Configurar MVR

Puede configurar ajustes básicos, avanzados, de grupo, de interfaz o de pertenencia a grupos.

Configurar los ajustes básicos de MVR

Para configurar los ajustes básicos de MVR:

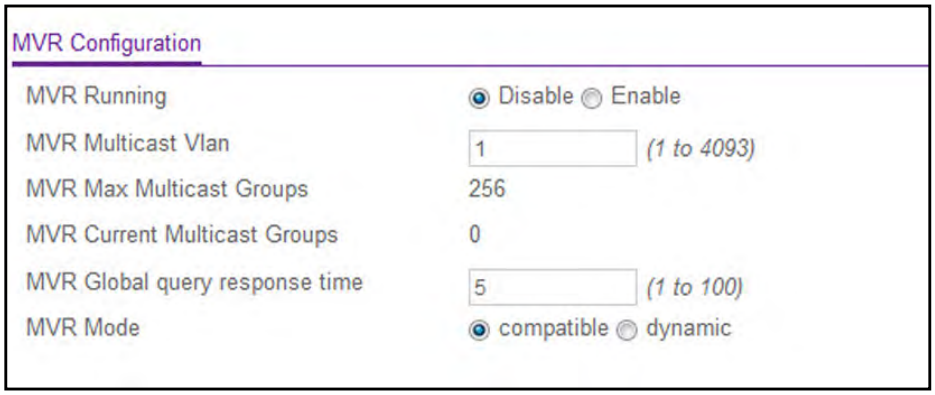
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MVR > Basic > MVR Configuration.



5. Use MVR Running para habilitar (Enable) o deshabilitar (Disable) la función MVR. El valor de fábrica es Disable.
6. Use MVR Multicast VLAN para especificar la VLAN en la que se reciben los datos multicast de MVR. Todos los puertos de origen pertenecen a esta VLAN. El valor puede estar en el rango de 1 a 4093. El valor predeterminado es 1.

7. Use MVR Global Query Response Time para establecer el tiempo máximo de espera de los informes de pertenencia IGMP en un puerto receptor.

   Este tiempo solo se aplica al procesamiento de salida de puertos receptores. 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 de grupo IGMP antes de quitar el puerto de la membresía del grupo

multicast. El valor se expresa en décimas de segundo. El rango es de 1 a 100 décimas. El valor de fábrica es 5 décimas, o medio segundo.

8. Use MVR Mode para especificar el modo de funcionamiento de MVR.
Los valores posibles son compatible o dynamic. El valor de fábrica es compatible.
9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 93. Configuración de MVR

Campo	Definición
MVR Max Multicast Groups	El número máximo de grupos multicast que admite MVR.
MVR Current Multicast Groups	Muestra el número actual de grupos MVR asignados.

Configurar los ajustes avanzados de MVR

Para configurar los ajustes avanzados de MVR:

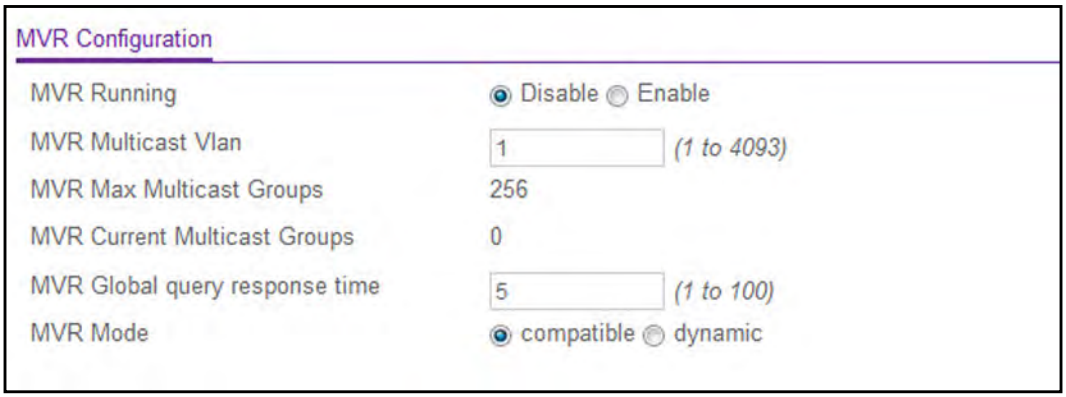
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MVR > Advanced > MVR Configuration.



5. Seleccione el botón de opción MVR Running Enable o Disable.

El valor de fábrica es Disable.

6. Use MVR Multicast VLAN para especificar la VLAN en la que se reciben los datos multicast de MVR.

   Todos los puertos de origen pertenecen a esta VLAN. El valor puede estar en un rango de 1 a 4094. El valor predeterminado es 1.

7. Use MVR Global query response time para establecer el tiempo máximo de espera de los informes de membresía IGMP en un puerto receptor. Este tiempo solo se aplica al procesamiento de salida de puertos receptores. 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 de grupo IGMP antes de quitar el puerto de la membresía del grupo multicast. El valor se expresa en décimas de segundo. El rango es de 1 a 100 décimas. El valor de fábrica es 5 décimas, o medio segundo.

8. Seleccione un botón de opción MVR Mode para especificar el modo de funcionamiento de MVR. El valor de fábrica es compatible.
9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 94. Configuración avanzada de MVR

Campo	Definición
MVR Max Multicast Groups	El número máximo de grupos multicast que admite MVR.
MVR Current Multicast Groups	Muestra el número actual de grupos MVR asignados.

Configurar un grupo MVR

Para configurar un grupo MVR:

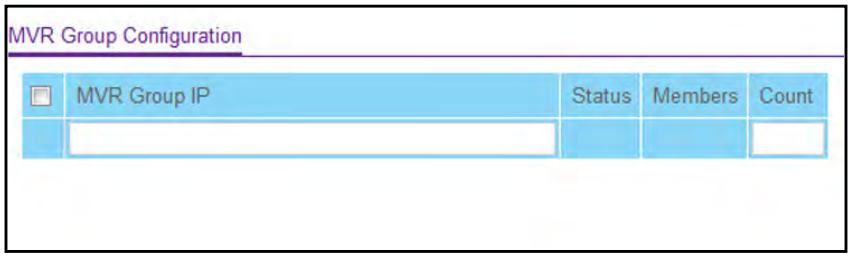
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MVR > Advanced > MVR Group Configuration.



5. Use MVR Group IP para especificar la dirección IP del nuevo grupo MVR.
6. Use Count para especificar el número de grupos MVR contiguos.

   Esto 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.

7. Haga clic en el botón Add.
Se agrega el grupo MVR.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 95. Configuración de grupos MVR

Campo	Definición
Status	El estado del grupo MVR específico.
Members	La lista de puertos que participan en el grupo MVR específico.

Configurar una interfaz MVR

Para configurar una interfaz MVR:

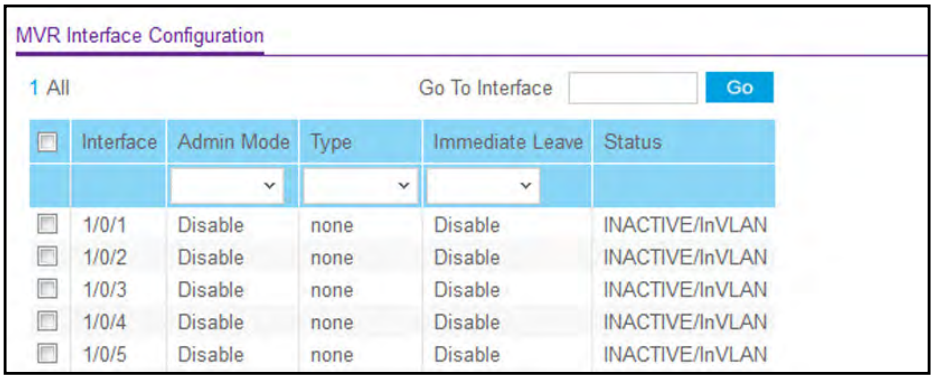
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MVR > Advanced > MVR Interface Configuration.



Se muestra el estado de cada puerto.
5. Use Interface para seleccionar la interfaz.
6. Use Admin Mode para habilitar (Enable) o deshabilitar (Disable) MVR en un puerto. El valor de fábrica es Disable.
7. Use Type para configurar el puerto como puerto receptor MVR o puerto de origen. El tipo de puerto predeterminado es none.

8. Use Immediate Leave para habilitar o deshabilitar la función Immediate Leave de MVR en un puerto.

El valor de fábrica es Disable.
9. Haga clic en el botón Apply. La configuración se guarda.

Configurar la membresía de grupos MVR

Para configurar la membresía de grupos MVR:

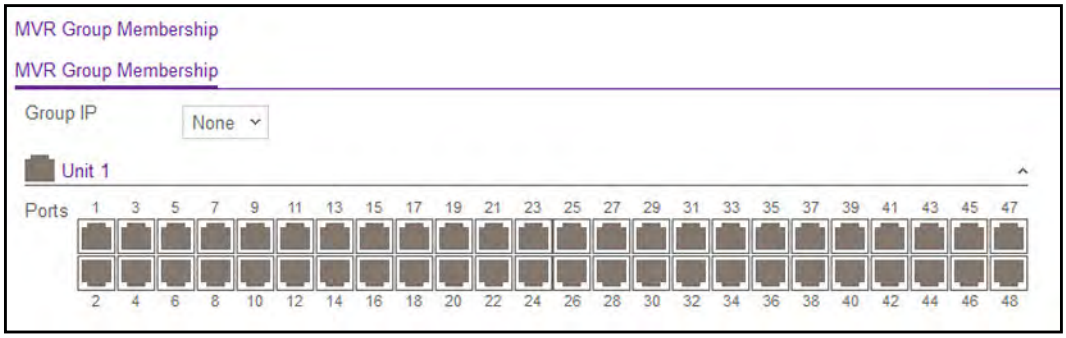
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MVR > Advanced > MVR Group Membership.



5. Use Group IP para especificar la dirección IP multicast del grupo MVR.
6. Use Port List para ver la lista configurada de miembros del grupo MVR seleccionado. Puede usar esta lista de puertos para agregar los puertos seleccionados a este grupo MVR.
7. Haga clic en el botón Apply.
Se guarda la configuración.

Ver las estadísticas de MVR

Para ver las estadísticas de MVR:

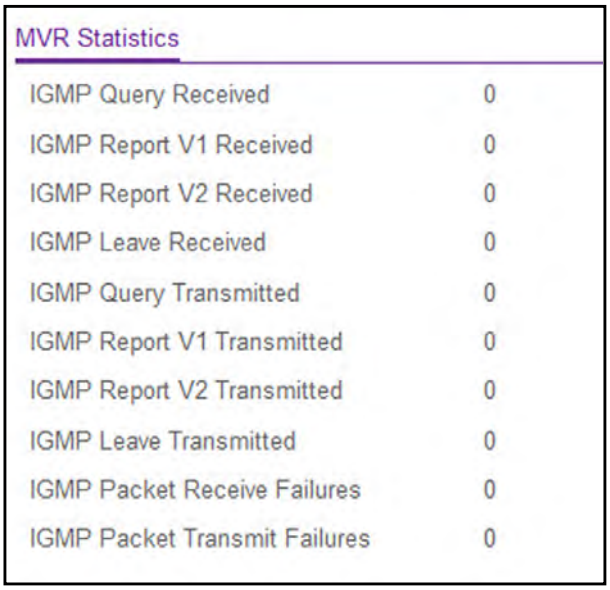
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MVR > Advanced > MVR Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 96. 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.

Buscar y administrar la 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 tiene información de reenvío o filtrado. La función de puenteo transparente usa esta información para determinar cómo propagar una trama recibida.

Buscar en la tabla de direcciones MAC

Para buscar en la tabla de direcciones MAC:

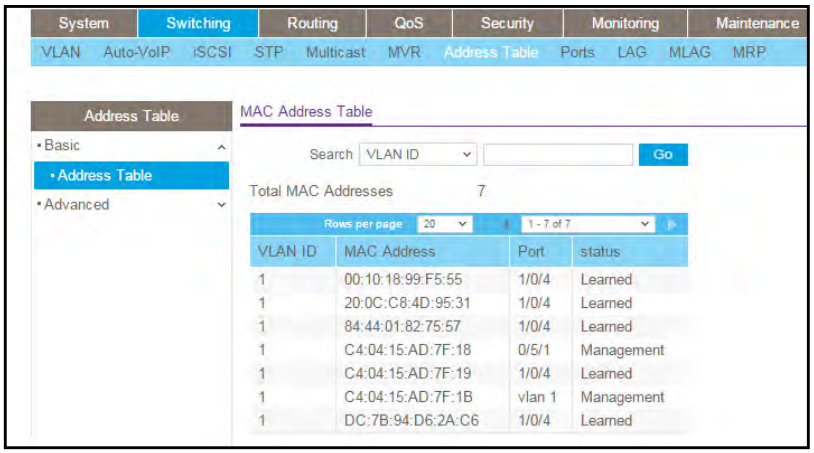
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching > Address Table> Basic > Address Table.**



5. Use Search By para buscar direcciones MAC por dirección MAC, VLAN ID o puerto:
   - Searched by MAC Address. 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.

- Searched by VLAN ID. Seleccione VLAN ID e introduzca el VLAN ID, por ejemplo, 100. Luego haga clic en el botón Go. Si la dirección existe, la entrada se muestra primero, seguida de las demás direcciones MAC (mayores).
- Searched by Port. Seleccione Port e introduzca el ID de puerto en formato Unit/Slot/Port, por ejemplo, 2/1/1. Luego haga clic en el botón Go. Si la dirección existe, la entrada se muestra primero, seguida de las demás direcciones MAC (mayores).

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 97. Tabla de direcciones básica

Campo	Descripción
Total MAC Address	Muestra el número total de direcciones MAC aprendidas o configuradas.
MAC Address	Una dirección MAC unicast para la que el switch tiene información de reenvío y/o filtrado. 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.
Port	El puerto en el que se aprendió esta dirección.
Status	El estado de esta entrada. Los valores significan lo siguiente: • Static. El sistema o un usuario agregó el valor de la instancia correspondiente y no se puede volver a aprender. • Learned. El valor de la instancia correspondiente se aprendió y está en uso. • Management. El valor de la instancia correspondiente también es el valor de una instancia existente de dot1dStaticAddress.

Establecer el intervalo de envejecimiento de direcciones dinámicas

Puede establecer el intervalo de envejecimiento de direcciones de la base de datos de reenvío especificada.

Para establecer el intervalo de envejecimiento de direcciones:

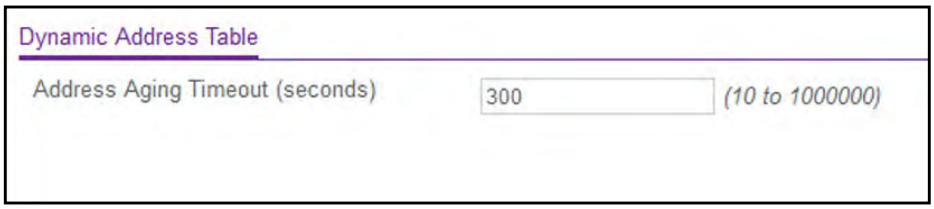
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Address Table> Advanced > Dynamic Addresses.



5. Use Address Aging Timeout (seconds) para especificar el tiempo de espera en segundos para que caduque la información de reenvío aprendida dinámicamente.

   IEEE 802.1D-1990 recomienda un valor predeterminado de 300 segundos. El valor puede ser cualquier número entre 10 y 1000000 segundos. El valor de fábrica es 300.

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

Configurar una dirección MAC estática

Para configurar una dirección MAC estática:

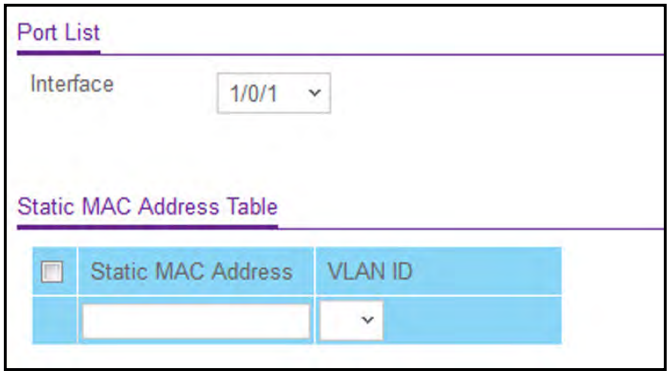
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Address Table> Advanced > Static MAC Address.



5. Use Interface para seleccionar la interfaz física o los LAG.
6. En el campo Static MAC Address, escriba la dirección MAC.
7. Seleccione el VLAN ID asociado a la dirección MAC.

8. Realice una de las siguientes acciones:

- Haga clic en el botón Add.

  La dirección MAC estática se agrega al switch.

- Haga clic en el botón Delete.

  La dirección MAC estática se elimina del switch.

Administrar la configuración de puertos

Puede ver y supervisar la información de los puertos físicos disponibles en el switch.

Configurar los ajustes de puertos

Puede configurar las interfaces físicas del switch.

Para configurar los ajustes de puertos:

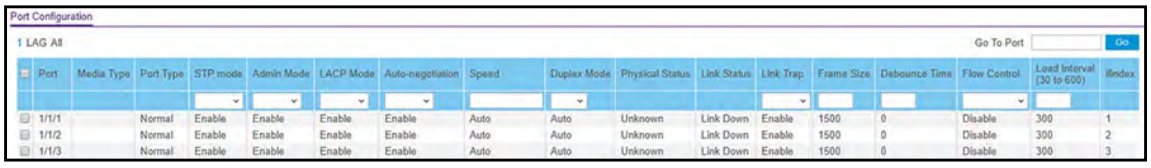
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Ports > Port Configuration.



5. En la columna Port, marque la casilla de uno o más puertos o LAG.

6. En el menú STP Mode, seleccione el modo administrativo de Spanning Tree Protocol del puerto o LAG.

   Los valores posibles son:

   - Enable. Habilita Spanning Tree Protocol en este puerto.
   - Disable. Deshabilita Spanning Tree Protocol en este puerto.

   El valor predeterminado es Enable.

7. En el menú Admin Mode, seleccione Enable o Disable.

   Establece el modo administrativo de control del puerto. Para que el puerto participe en la red, debe seleccionar Enable. El valor de fábrica es Enable.

8. En el menú LACP Mode, seleccione Enable o Disable.

   Selecciona el modo administrativo de Link Aggregation Control Protocol. El modo debe estar habilitado para que el puerto participe en la agregación de enlaces. El valor de fábrica es Enable.

9. En el menú Auto-negotiation, seleccione Enable o Disable.

Especifica el modo de autonegociación de este puerto. El valor predeterminado es Enable.

Nota: Después de cambiar el modo de autonegociación, es posible que el switch no esté accesible durante algunos segundos mientras se aplica la nueva configuración.

10. En el menú Speed, seleccione una de las siguientes velocidades:

- Auto. La velocidad se establece mediante la autonegociación.
- 100. 100 Mbits/segundo
- 10G. 10 Gbits/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. El valor predeterminado es Auto.

Nota: Después de cambiar la velocidad, es posible que el switch no esté accesible durante algunos segundos mientras se aplica la nueva configuración.

11. En el menú Duplex Mode, seleccione uno de los siguientes valores:

- Auto. El modo dúplex se establece mediante la autonegociación.
- Full. La transmisión entre los dispositivos ocurre en ambas direcciones simultáneamente.
- Half. La transmisión entre los dispositivos ocurre en una sola dirección a la vez.

El valor predeterminado es Auto.

Nota: Después de cambiar el modo dúplex, es posible que el switch no esté accesible durante algunos segundos mientras se aplica la nueva configuración.

12. En el menú Link Trap, seleccione si se envía un trap cuando cambia el estado del enlace. El valor de fábrica es Enable.

13. En el campo Frame Size, especifique el tamaño máximo de trama Ethernet que el puerto admite o está configurado para usar, incluidos el encabezado Ethernet, el CRC y la carga útil.

El rango es de 1518 a 9398. El tamaño máximo de trama predeterminado es 1518.

14. En el campo Debounce Time, especifique el valor del temporizador de debounce del puerto en múltiplos de 100 milisegundos (ms), en el rango de 100 a 5000.

El valor predeterminado del temporizador de debounce es 0, lo que significa que el debounce está deshabilitado.

15. En el menú Flow Control, habilite o deshabilite el control de flujo IEEE 802.3.

    El valor predeterminado es Disable. El switch no envía tramas de pausa si los búferes del puerto se llenan. El control de flujo ayuda a evitar la pérdida de datos cuando el puerto no puede procesar la cantidad de tramas que se conmutan. Si está habilitado, el switch puede enviar una trama de pausa para detener el tráfico en un puerto si la memoria usada por los paquetes del puerto supera un umbral preconfigurado, y responde a 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 la utilización vuelve a un umbral bajo especificado, el switch permite que el puerto vuelva a transmitir tramas. En las interfaces LAG, el modo de control de flujo se muestra en blanco porque el control de flujo no se aplica.

16. En el campo Load Interval, especifique el periodo de intervalo de carga cuyos datos se usan para calcular las estadísticas de carga.

    Introduzca el intervalo en múltiplos de 30 segundos. El rango permitido es de 30 a 600. El intervalo de carga predeterminado es de 300 segundos. Cuanto menor sea el intervalo, más precisa será la tasa instantánea de las estadísticas de carga.

17. Haga clic en el botón Apply.

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 98. Configuración de puertos

Campo	Descripción
Media Type	El tipo de medio.
Port Type	En los puertos normales, este campo es Normal. De lo contrario, los valores posibles son los siguientes: • Mirrored. El puerto es un puerto reflejado cuyo tráfico se copia al puerto de sondeo. • Probe. Use este puerto para supervisar un puerto reflejado. • Trunk Member. El puerto es miembro de un trunk de agregación de enlaces. Consulte las páginas de LAG para obtener más información.
Admin Status	Cuando el modo administrativo del puerto es D-Disable, este campo indica el motivo. Los motivos posibles son: • STP. Infracción de Spanning Tree Protocol. • UDLD. Infracción del protocolo UDLD. • XCEIVER. Se insertó un SFP/SFP+ no compatible.
Physical Status	Indica la velocidad y el modo dúplex del puerto.
Link Status	Indica si el enlace está activo o inactivo.
ifIndex	El ifIndex de la entrada de la tabla de interfaces asociada a este puerto.

Configurar los puertos expandibles

Puede ver y configurar los puertos expandibles.

Para ver y configurar la información de los puertos expandibles:

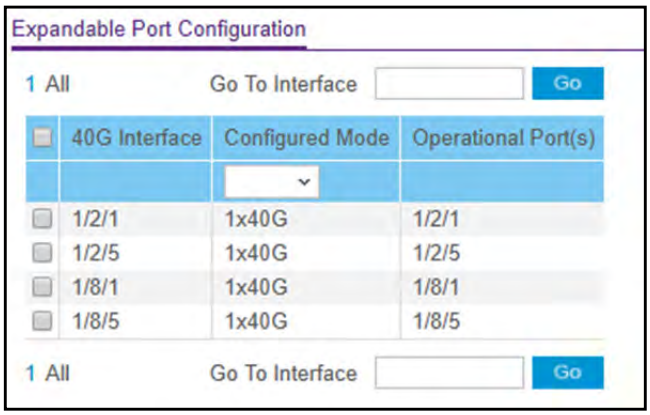
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Ports > Expandable Port Configuration.



La columna no configurable Operational Port(s) muestra los puertos que están operativos.
5. En la columna 40G Interface, marque la casilla de la interfaz.

6. En el menú Configured Mode, seleccione el modo del puerto expandible:
   - 1x40G. La interfaz no se expande y funciona en modo 40. Este es el valor predeterminado.
   - 4x10G. La interfaz se expande a cuatro puertos de 10G.

7. Haga clic en el botón Apply.
La configuración se guarda.
8. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

Configurar los ajustes de link flap de los puertos

Puede configurar los ajustes de link flap (oscilación del enlace), 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:

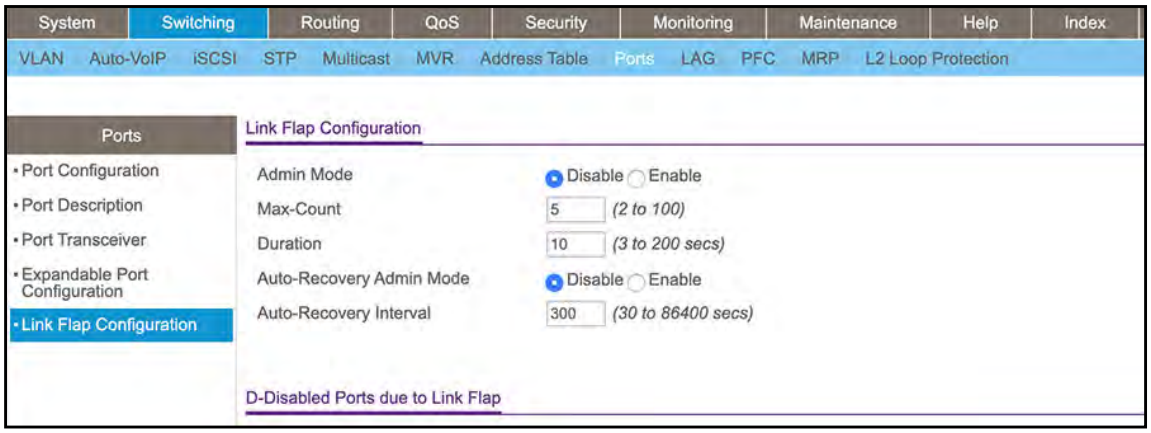
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching > Ports > Link Flap Configuration.**



5. Configure los siguientes ajustes:

   - Admin Mode. Seleccione el botón de opción Enable o Disable.

     Este ajuste determina el modo administrativo de link flap. Para poder configurar los ajustes de link flap, debe seleccionar Enable. El valor predeterminado es Disable.

   - Max-Count. Introduzca el número máximo de oscilaciones permitidas antes de que el puerto pase al estado deshabilitado. De forma predeterminada, el número es 5. Puede introducir un número de 2 a 10. Este ajuste solo se aplica si está seleccionado el botón de opción Admin Mode Enable.
   - Duration. Introduzca el periodo máximo en segundos durante el cual se cuentan las oscilaciones del enlace. Si el número de oscilaciones del puerto es mayor o igual que el número introducido 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. Este ajuste solo se aplica si está seleccionado el botón de opción Admin Mode Enable.

- Auto-Recovery Admin Mode. Seleccione el botón de opción Enable o Disable.

  Este ajuste determina el modo administrativo de recuperación automática. Para habilitar la recuperación automática, debe seleccionar Enable. El valor predeterminado es Disable.

  Si está habilitado, el puerto sale automáticamente del estado deshabilitado al cumplirse el intervalo.

- Auto-Recovery Interval. Introduzca el periodo en segundos tras el cual el puerto sale automáticamente del estado deshabilitado. El periodo predeterminado es de 300 segundos. Puede introducir un periodo de 30 a 8640 segundos. Este ajuste solo se aplica si está seleccionado el botón de opción Auto-Recovery Admin Mode.

6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La sección D-Disabled Ports due to Link Flap muestra los puertos que están en estado deshabilitado.

Configurar las descripciones de los puertos

Para configurar y mostrar la descripción de todos los puertos del dispositivo:

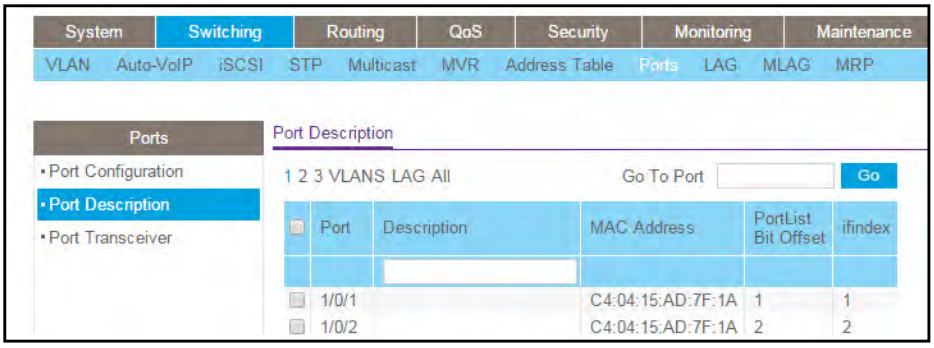
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Ports > Port Description.



5. Use Port Description para introducir la cadena de descripción que se asociará a un puerto. Puede tener hasta 64 caracteres.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 99. Descripción de puertos

Campo	Descripción
Port	Selecciona la interfaz cuyos datos se mostrarán o configurarán.
MAC Address	La dirección física de la interfaz especificada.
PortList Bit Offset	El valor de desplazamiento de bits correspondiente al puerto cuando se usa el tipo de objeto MIB PortList para administrar en SNMP.
ifIndex	El índice de interfaz asociado al puerto.

Ver la información de los transceptores de los puertos

Puede ver la información de los transceptores de todos los puertos de fibra del switch

Para ver la información de los transceptores de los puertos:

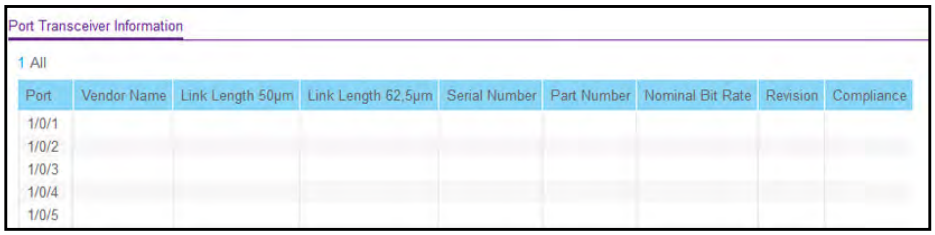
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > Ports > Port Transceiver.



5. Seleccione Unit ID para mostrar los puertos físicos de la unidad seleccionada, o seleccione All para mostrar los puertos físicos de todas las unidades.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh).

A continuación se describe la información no configurable que se muestra.

Tabla 100. Transceptor de puerto

Campo	Descripción
Port	La interfaz cuyos datos se mostrarán.
Vendor Name	Nombre del fabricante del SFP.
Link Length 50 µm	Longitud de enlace admitida para fibra de 50 µm.
Link Length 62, 5 µm	Longitud de enlace admitida para fibra de 62, 5 µm.
Serial Number	Número de serie del SFP.
Part Number	Número de parte del SFP.
Nominal Bit Rate	Tasa de señalización nominal del SFP.
Revision	Revisión del fabricante del SFP.
Compliance	Cumplimiento del SFP.

Administrar los grupos de agregación de enlaces

Los grupos de agregación de enlaces (LAG), también llamados port-channels, 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 repartir la carga. La membresía VLAN del LAG se asigna después de crear el LAG. De forma predeterminada, el LAG se convierte en 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.

Se admiten LAG estáticos. Cuando se agrega un puerto a un LAG como miembro estático, no transmite ni recibe LACPDU.

Descripción general de Auto-LAG

Un Auto-LAG es un LAG que se forma automáticamente entre dos dispositivos compatibles con la función Auto-LAG. Un Auto-LAG es un LAG dinámico de capa 2 basado en 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 los puertos interconectados y compatibles de ambos extremos. El switch solo puede formar un Auto-LAG con cada dispositivo asociado.

La función Auto-LAG puede funcionar junto con la función Auto-Trunk (consulte Descripción general de Auto-Trunk en la página 186). Si la función Auto-Trunk está habilitada en el switch y en el dispositivo asociado con el que se forma 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 del modo de puerto de switch predeterminado al modo de puerto trunk.

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 M4300, las funciones Auto-LAG y Auto-Trunk están deshabilitadas de forma predeterminada).
- Debe haber al menos dos enlaces establecidos entre el switch y el dispositivo asociado, y estos enlaces deben admitir la misma velocidad y 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 M4300, 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 de switch 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 trunk 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 puede admitir un Auto-LAG.

Habilitar o deshabilitar Auto-LAGs

De forma predeterminada, la función Auto-LAG está deshabilitada globalmente, pero puede habilitarla globalmente.

Para habilitar o deshabilitar Auto-LAGs:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> LAG > LAG Configuration.

   Se muestra la página LAG Configuration.

5. 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 deshabilitada globalmente.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar el modo de hash de Auto-LAGs

Al habilitar Auto-LAG, de forma predeterminada usa un modo 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 hash llamado 2 Dest MAC, VLAN, EType, incoming port). Puede cambiar el modo hash (es decir, el modo de balanceo de carga) de la función Auto-LAG.

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. 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, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> LAG > LAG Configuration.

   Se muestra la página LAG Configuration.

5. En la sección LAG Global Configuration, en el menú Auto-LAG Global Hash Mode, seleccione el modo hash para los Auto-LAG:
   - 1 Src MAC, VLAN, EType, incoming port: dirección MAC de origen, VLAN, EtherType y puerto de entrada asociados con el paquete.

- 2 Dest MAC, VLAN, EType, incoming port: dirección MAC de destino, VLAN, EtherType y puerto de entrada asociados con el 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 con el 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.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar los ajustes de LAG

Puede agrupar uno o más enlaces Ethernet full-duplex para 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:

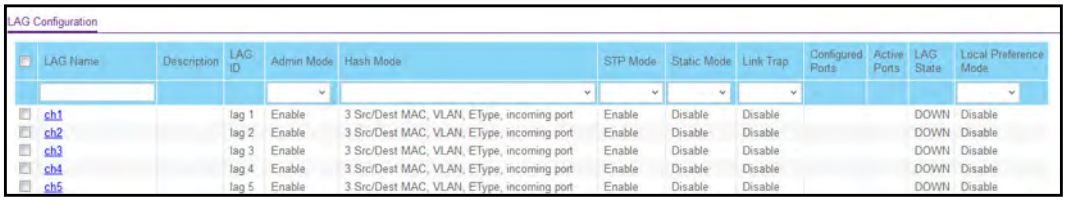
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> LAG > LAG Configuration.



5. Use LAG Name para introducir el nombre que se asignará al LAG.

   Puede introducir cualquier cadena de hasta 15 caracteres alfanuméricos. Debe especificar un nombre válido para crear el LAG.

6. Use Admin Mode para seleccionar Enable o Disable.

Con el LAG deshabilitado, no fluye tráfico y se descartan las LACPDU, pero los enlaces que forman el LAG no se liberan. El valor de fábrica es Enable.

7. Use Hash Mode para seleccionar el modo de balanceo de carga de un port-channel (LAG).

El tráfico se balancea en un port-channel (LAG) seleccionando uno de los enlaces del canal por el que se transmiten paquetes específicos. El enlace se selecciona creando un patrón binario a partir de campos seleccionados del paquete y asociando ese patrón a un enlace determinado:

- Src MAC, VLAN, EType, incoming port. MAC de origen, VLAN, EtherType y puerto de entrada asociados con el paquete.
- Dest MAC, VLAN, EType, incoming port. MAC de destino, VLAN, EtherType y puerto de entrada asociados con el paquete.
- Src/Dest MAC, VLAN, EType, incoming port. MAC de origen/destino, VLAN, EtherType y puerto de entrada asociados con el paquete. Src/Dest MAC, VLAN, EType, incoming port es el valor predeterminado.
- Src IP and Src TCP/UDP Port fields. Campos de IP de origen y TCP/UDP de origen del paquete.
- Dest IP and Dest TCP/UDP Port fields. Campos de IP de destino y puerto TCP/UDP de destino del paquete.
- Src/Dest IP and TCP/UDP Port Fields. Campos de IP de origen/destino y de puertos TCP/UDP de origen/destino del paquete.
- Enhanced hashing Mode. Ofrece operación MODULO-N según el número de puertos del LAG, hash de tráfico unicast y no unicast con un algoritmo hash común, excelente balanceo de carga y selección de atributos del paquete según su tipo:
  - Para paquetes L2, se usan las direcciones MAC de origen y destino para el cálculo del hash.
  - Para paquetes L3, se usan la IP de origen, la IP de destino y los puertos TCP/UDP.

8. Use STP Mode para habilitar o deshabilitar el modo administrativo de Spanning Tree Protocol asociado al LAG.

Los valores posibles son:

- Disable. Spanning tree está deshabilitado para este LAG.
- Enable. Spanning tree está habilitado para este LAG. Enable es el valor predeterminado.

9. Use Static Mode para seleccionar Enable o Disable.

Si está habilitado, el LAG no transmite ni procesa las LACPDU recibidas; es decir, los puertos miembros no transmiten LACPDU y todas las LACPDU que reciben se descartan. El valor de fábrica es Disable.

10. Use Link Trap para especificar si se envía un trap cuando cambia el estado del enlace. El valor de fábrica es Enable, con el que se envía el trap.

11. Use Local Preference Mode para habilitar o deshabilitar el modo de preferencia local de la interfaz LAG.

El valor predeterminado es Disable.

12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 101. LAG Configuration

Campo	Descripción
LAG Description	Introduzca la cadena de descripción del LAG. Puede tener hasta 64 caracteres.
LAG ID	Identificación del LAG.
LAG State	Indica si el enlace está activo o inactivo.
Configured Ports	Indica los puertos miembros de este port-channel
Active Ports	Indica los puertos que participan activamente en el port-channel.

Configurar la pertenencia a LAG

Puede seleccionar dos o más enlaces Ethernet full-duplex para formar un grupo de agregación de enlaces (LAG), también llamado port-channel. El switch puede tratar el port-channel como si fuera un solo enlace.

Para configurar la pertenencia a LAG:

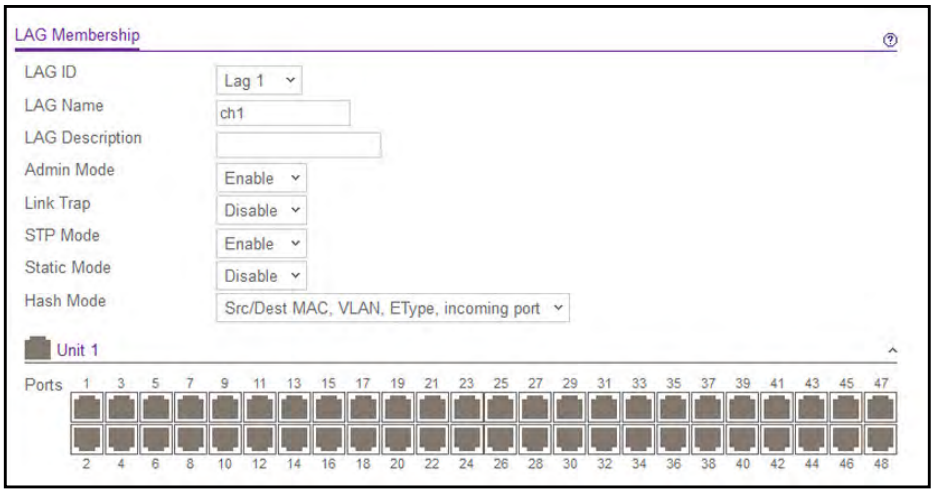
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> LAG > LAG Membership.



5. Use LAG ID para seleccionar la identificación del LAG.
6. Use LAG Name para introducir el nombre que se asignará al LAG.

   Puede introducir cualquier cadena de hasta 15 caracteres alfanuméricos. Debe especificar un nombre válido para crear el LAG.

7. Use LAG Description para introducir la cadena de descripción del LAG. Puede tener hasta 64 caracteres.

8. Use Admin Mode para seleccionar Enable o Disable.

   Con el LAG deshabilitado, no fluye tráfico y se descartan las LACPDU, pero los enlaces que forman el LAG no se liberan. El valor de fábrica es Enable.

9. Use Link Trap para especificar si se envía un trap cuando cambia el estado del enlace. El valor de fábrica es Enable, con el que se envía el trap.

10. Use STP Mode para habilitar o deshabilitar el modo administrativo de Spanning Tree Protocol asociado al LAG.

    Los valores posibles son:

- Disable. Spanning tree está deshabilitado para este LAG.
- Enable. Spanning tree está habilitado para este LAG. Enable es el valor predeterminado.

11. Use Static Mode para seleccionar Enable o Disable.

    Si está habilitado, el LAG no transmite ni procesa las LACPDU recibidas; es decir, los puertos miembros no transmiten LACPDU y todas las LACPDU que reciben se descartan. El valor de fábrica es Disable.

12. Use Hash Mode para seleccionar el modo de balanceo de carga de un port-channel (LAG).

    El tráfico se balancea en un port-channel (LAG) seleccionando uno de los enlaces del canal por el que se transmiten paquetes específicos.

El enlace se selecciona creando un patrón binario a partir de campos seleccionados del paquete y asociando ese patrón a un enlace determinado:

- Src MAC,VLAN,EType,incoming port. MAC de origen, VLAN, EtherType y puerto de entrada asociados con el paquete.
- Dest MAC,VLAN,EType,incoming port. MAC de destino, VLAN, EtherType y puerto de entrada asociados con el paquete.
- Src/Dest MAC,VLAN,EType,incoming port. MAC de origen/destino, VLAN, EtherType y puerto de entrada asociados con el paquete. Es la opción predeterminada.
- Src IP and Src TCP/UDP Port fields. Campos de IP de origen y TCP/UDP de origen del paquete.
- Dest IP and Dest TCP/UDP Port fields. Campos de IP de destino y puerto TCP/UDP de destino del paquete.
- Src/Dest IP and TCP/UDP Port fields. Campos de IP de origen/destino y de puertos TCP/UDP de origen/destino del paquete.
- Enhanced Hashing Mode. Ofrece operación MODULO-N según el número de puertos del LAG, hash de tráfico unicast y no unicast con un algoritmo hash común, excelente balanceo de carga y selección de atributos del paquete según su tipo:
  - Para paquetes L2, se usan las direcciones MAC de origen y destino para el cálculo del hash.
  - Para paquetes L3, se usan la IP de origen, la IP de destino y los puertos TCP/UDP.

13. Use Port Selection Table para seleccionar los puertos miembros del LAG.
14. Haga clic en el botón Aplicar (Apply).

La configuración se guarda.

Administrar la configuración de Multiple Registration Protocol

Al igual que 802.1AS, Multiple Registration Protocol (MRP) es una función de audio video bridging (AVB) disponible en algunas plataformas FASTPATH. MRP es un protocolo de registro base que permite a los dispositivos con una aplicación MRP registrar atributos en otros dispositivos de una red. MRP ofrece una aplicación para registrar atributos como el ancho de banda de un stream AV y la información de direcciones MAC. Diversas aplicaciones lo usan para propagar el registro. Los switches blade admiten 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.

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.

Con MRP, los atributos de red se declaran, registran, retiran y eliminan de forma totalmente dinámica 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 del 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:

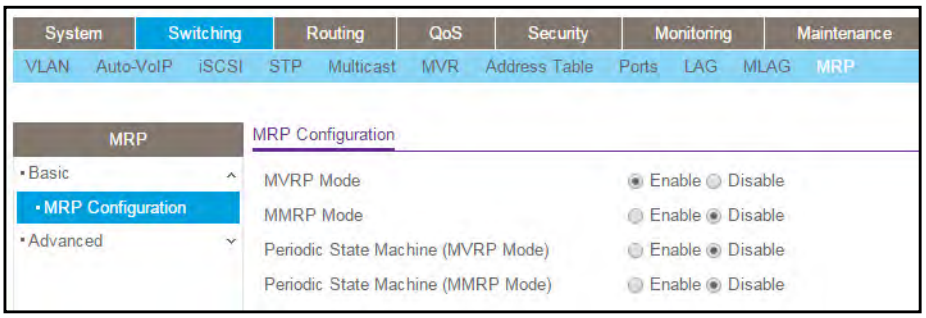
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MRP > Basic > MRP Configuration.



Nota: Los campos disponibles en la página MRP Configuration varían según la plataforma y las funciones que admite.

5. Seleccione el botón de opción MVRP Mode Enable o Disable.

   Esto especifica el modo administrativo global de MVRP en el dispositivo. El valor predeterminado es Disable.

   Multiple VLAN Registration Protocol (MVRP) registra las VLAN en la red, lo que permite la configuración automática de VLAN en el dispositivo. 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.

6. Seleccione el botón de opción MMRP Enable o Disable.

   Esto especifica el modo administrativo global de MMRP en el dispositivo. El valor predeterminado es Disable.

   Multiple MAC Registration Protocol (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 dispositivo.

7. Seleccione el botón de opción Periodic State Machine (MVRP) Enable o Disable.

   Si está habilitada, la máquina de estados puede ayudar a limitar el efecto de los cambios de topología y reducir el número de unidades de datos de protocolo (PDU) transmitidas entre dispositivos. El valor predeterminado es Disable.

8. Seleccione el botón de opción Periodic State Machine (MMRP) Enable o Disable.

   Si está habilitada, la máquina de estados puede ayudar a limitar el efecto de los cambios de topología y reducir el número de unidades de datos de protocolo (PDU) transmitidas entre dispositivos. El valor predeterminado es Disable.

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

Configurar MRP en puertos

Puede configurar el modo MRP y los temporizadores por puerto. Los temporizadores controlan cuándo y con qué frecuencia se transmiten los mensajes en cada interfaz.

Para configurar MRP en puertos:

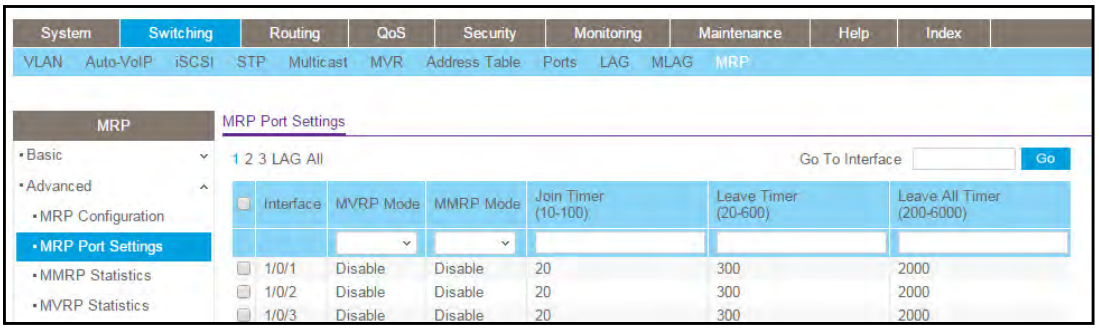
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> MRP > Advanced > Port Settings.



5. Para configurar uno o más puertos o LAG, seleccione la casilla junto a cada puerto o LAG que desea configurar.

Puede seleccionar varios puertos para aplicar la misma configuración a las interfaces seleccionadas.

6. En el campo MVRP Mode, seleccione Enable o Disable.

   Esto especifica el modo administrativo de Multiple VLAN Registration Protocol (MVRP) en la interfaz. MVRP registra las VLAN en la red, lo que permite la configuración automática de VLAN en el dispositivo.

7. En el campo MMRP Mode, seleccione Enable o Disable.

   Esto especifica el modo administrativo de Multiple MAC Registration Protocol (MMRP) en la interfaz. MMRP permite propagar la información de direcciones MAC en la red y registrar y anular el registro de direcciones MAC individuales y de la pertenencia a grupos de direcciones MAC.

8. Use el campo MRP Join Timer para configurar el tiempo en centisegundos que se esperan mensajes JoinIn de otros participantes MRP después de que la interfaz envía 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.

9. Use el campo MRP Leave Timer para configurar el tiempo en centisegundos que se espera antes de que la interfaz anule el registro de atributos de otros participantes MRP.

Si la interfaz recibe mensajes Join de otros participantes antes de que expire el temporizador Leave, los atributos no se anulan. El rango es de 20 a 600 centisegundos. El valor predeterminado es 300.

10. Use el campo MRP Leave All Timer para configurar el tiempo de espera, después de que la interfaz inicia 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.
11. Haga clic en el botón Apply.
La configuración se guarda.

Ver y 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:

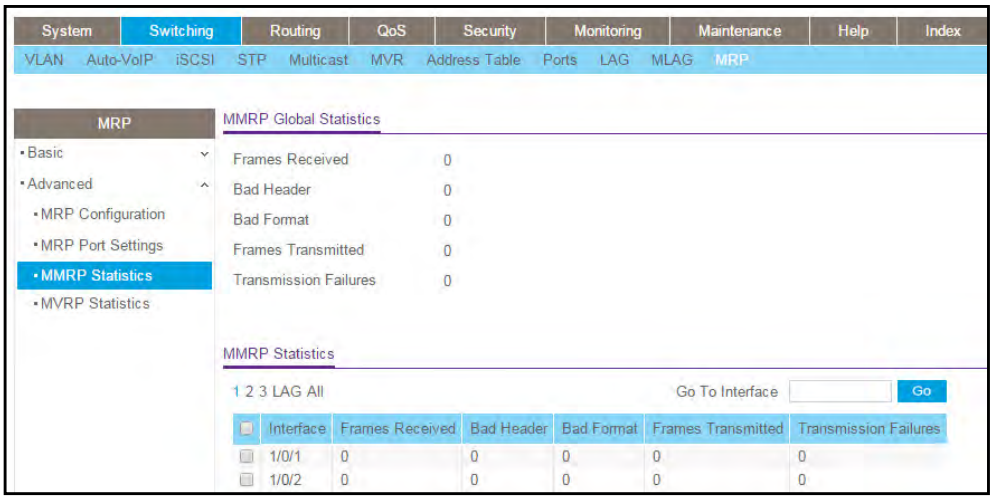
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Switching > MRP > Advanced > MMRP Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar las estadísticas de uno o más puertos, haga lo siguiente:

   a. Seleccione la casilla junto a la interfaz o interfaces.

   b. Haga clic en el botón Clear.
   Se borran las estadísticas.

La siguiente tabla describe la información no configurable que muestra la página MMRP Global Statistics.

Tabla 102. MMRP Global Statistics

Campo	Descripción
Interface	En la tabla MMRP Statistics, este campo identifica la interfaz asociada al resto de los datos de la fila.
Frames Received	Número de tramas MMRP recibidas en el dispositivo o en la interfaz específica.
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.
Transmission Failures	Número de tramas MMRP que el switch no pudo transmitir.

Ver y borrar estadísticas de MVRP

Puede ver y borrar la información sobre las tramas MVRP transmitidas y recibidas por el switch y por cada interfaz.

Para ver y borrar las estadísticas de MVRP:

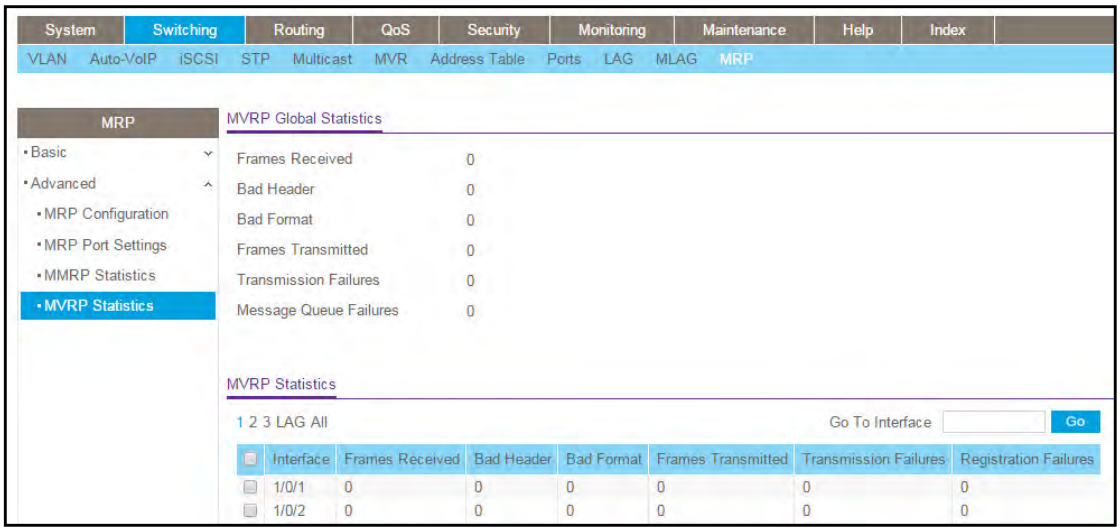
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching > MRP > MVRP Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar las estadísticas de uno o más puertos, haga lo siguiente:

   a. Seleccione la casilla junto a la interfaz o interfaces.

   b. Haga clic en el botón Clear.
   Se borran las estadísticas.

La siguiente tabla describe la información no configurable que muestra la página MVRP Global Statistics.

Tabla 103. MVRP Statistics

Campo	Descripción
Interface	En la tabla MVRP Statistics, este campo identifica la interfaz asociada al resto de los datos de la fila.
Frames Received	Número de tramas MVRP recibidas en el switch.
Bad Header	Número de tramas MVRP con encabezado incorrecto recibidas en el switch.
Bad Format	Número de tramas MVRP con formato de cuerpo de PDU incorrecto recibidas en el switch.
Frames Transmitted	Número de tramas MVRP transmitidas en el switch.
Transmission Failures	Número de tramas MVRP que el switch no pudo transmitir.
Message Queue Failures	Número de mensajes que no pudieron agregarse a la cola.
Registration Failures	Número de tramas MVRP que no se pudieron registrar en un dispositivo o interfaz específica.

Administrar la protección contra bucles

La protección contra bucles puede detectar bucles físicos y lógicos entre 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. Detectarlos manualmente puede ser complicado.

El switch puede identificar automáticamente los bucles en la red. Puede habilitar la protección contra bucles por puerto o globalmente.

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 con la función habilitada. Puede deshabilitar selectivamente la transmisión de paquetes PDU en puertos específicos aunque la protección contra bucles esté habilitada en ellos. Si el switch recibe un paquete con esa dirección de destino multicast, compara la dirección MAC de origen del paquete 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 del switch, el switch 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 sirven de enlace ascendente entre switches compatibles con spanning tree. Está diseñada para switches no administrados que descartan las unidades de datos de protocolo de bridge (BPDU) de spanning tree.

Debe habilitar la función globalmente antes de habilitarla por puerto para que se pueda instalar el filtro de política del sistema.

Protección contra bucles y transmisión de paquetes PDU

La protección contra bucles envía paquetes del protocolo de bucles desde todos los puertos donde está habilitada. Puede configurar el intervalo (de 1 a 5 segundos) entre dos paquetes PDU sucesivos. El intervalo predeterminado es de 5 segundos. Si el switch recibe un paquete del protocolo de bucles en un puerto cuya acción es apagar el puerto, este ya no puede recibir ni enviar tramas.

La protección contra bucles opera por puerto, independientemente de la asignación y pertenencia a VLAN, detectando 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 sirven de enlace ascendente entre switches compatibles con spanning tree. Puede coexistir con Spanning Tree Protocol (STP). Puede habilitar la protección contra bucles y STP en un puerto porque estas funciones operan de forma independiente. STP no apaga un puerto cuando detecta un bucle, sino que lo mantiene en estado de bloqueo. Como las PDU se permiten en estado de bloqueo, se reciben los paquetes de protección y esta apaga 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 por puerto (consulte Configurar la protección contra bucles en puertos y ver su estado en la página 298), debe habilitarla y configurarla globalmente.

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, escriba la dirección IP del switch.

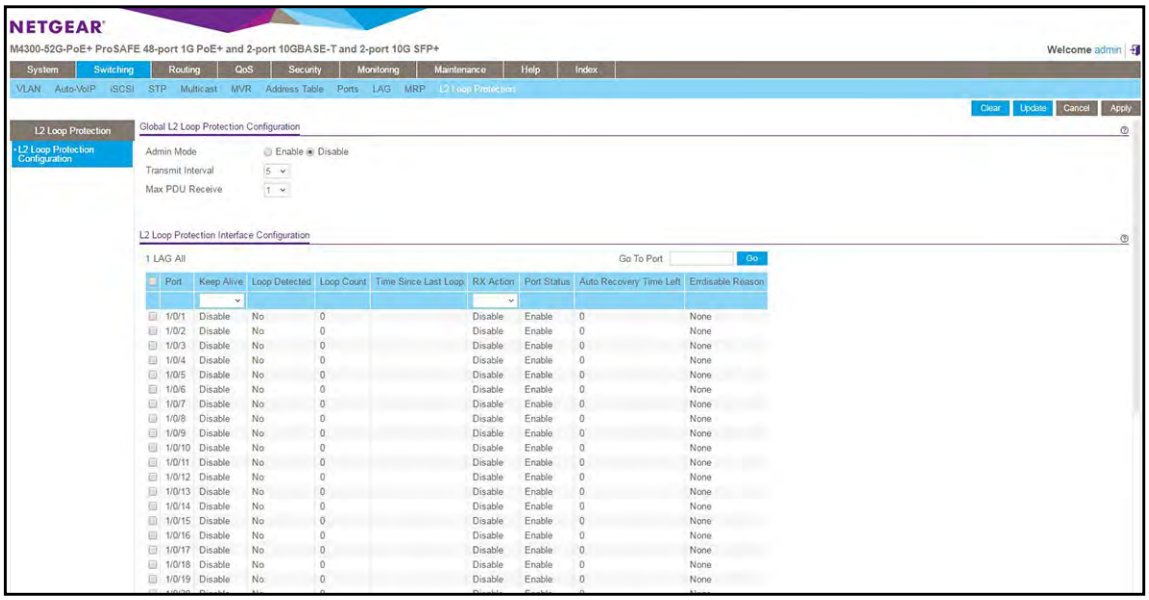
Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Switching> L2 Loop Protection > L2 Loop Protection Configuration.



5. 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 Transmit Interval, seleccione el intervalo entre las transmisiones de paquetes de bucle en un puerto.

     El rango es de 1 a 5 segundos. El ajuste predeterminado es 5 segundos. El intervalo seleccionado se aplica a todos los puertos en los que habilite la protección contra bucles.

   - 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 ajuste predeterminado es 1 paquete. El número de paquetes seleccionado se aplica a todos los puertos en los que habilite la protección contra bucles.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar la protección contra bucles de los puertos y ver el estado de la protección contra bucles

Antes de configurar la protección contra bucles en puertos individuales, debe habilitar globalmente la protección contra bucles (consulte Configurar los ajustes globales de protección contra bucles en la página 296).

Para habilitar y configurar la protección contra bucles de un puerto y ver su estado en el switch:

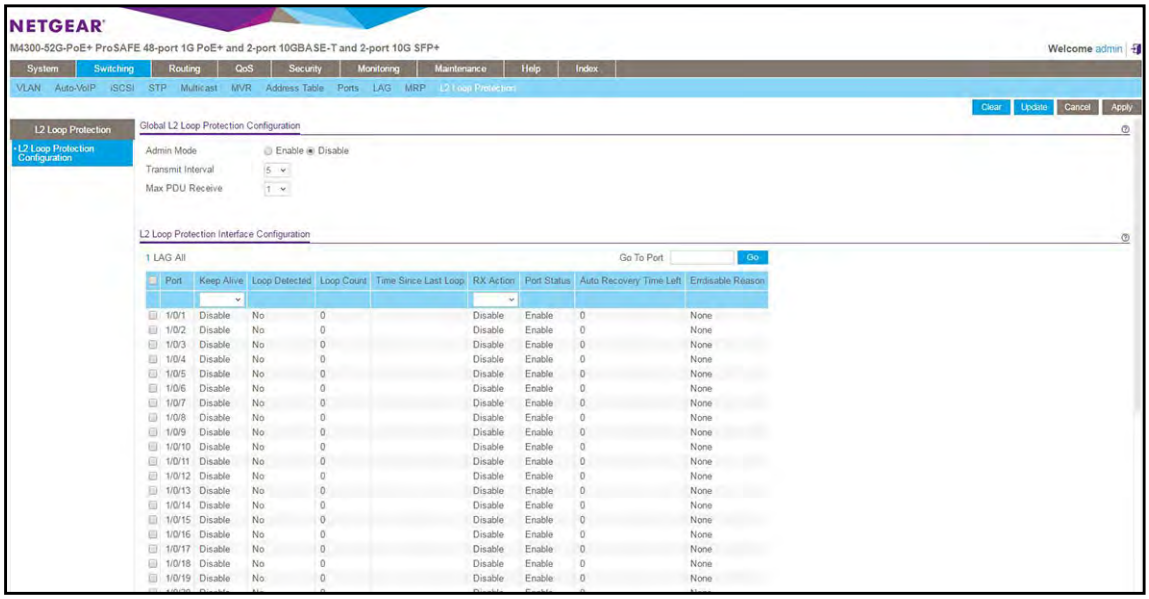
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Switching> L2 Loop Protection > L2 Loop Protection Configuration.**



5. Seleccione una de las siguientes opciones para especificar qué puertos se muestran en la página:
   - Haga clic en LAG para mostrar la lista de todas las interfaces LAG.
   - Haga clic en All para mostrar la lista de todos los puertos físicos y las interfaces LAG.
6. Use uno de los siguientes métodos para seleccionar un puerto:
   - En el campo Go To Port, ingrese el puerto en formato unidad/ranura/puerto y haga clic en el botón Go.
   - Junto a la columna Port, marque la casilla del puerto que desea configurar.

Nota: Puede seleccionar varios puertos. Para seleccionar todos, marque la casilla del encabezado de la tabla.

7. En el menú Keep Alive, seleccione Enable para especificar que se habilite la protección contra bucles en el puerto.

De forma predeterminada, la protección contra bucles está deshabilitada en un puerto.

8. En el menú RX Action, seleccione la acción que toma 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. Este es el ajuste predeterminado.
   - Both. Registra el mensaje y deshabilita el puerto cuando se detecta un bucle.

9. Haga clic en el botón Apply.
La configuración se guarda.
10. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 104. Información de configuración de protección contra bucles de interfaces

Campo	Descripción
Loop Detected	Indica (Yes o No) si se detectó un bucle en el puerto.
Loop Count	El número de paquetes recibidos en el puerto después de detectar el bucle.
Time Since Last Loop	El tiempo transcurrido desde que se detectó el bucle.
Port Status	El estado del puerto (Enabled o Disabled).
Auto Recovery Time Left	El tiempo restante antes de que el puerto se vuelva a habilitar mediante el proceso de recuperación automática. El tiempo está en el rango de 30 a 604800 segundos.
Errdisable Reason	El motivo por el que se deshabilitó el puerto. Además de deshabilitarse por la protección contra bucles, el puerto puede deshabilitarse por Unidirectional Link Detection (UDLD), una tormenta de broadcast, una tormenta de unicast, etc.

5

5Administrar el enrutamiento

Este capítulo trata los siguientes temas:

- Administrar rutas
- Configurar los ajustes de IP de enrutamiento
- Configurar los parámetros de enrutamiento del switch
- Administrar IPv6
- Administrar VLAN
- Configurar Address Resolution Protocol
- Configurar RIP
- Configurar Router Discovery
- Configurar Virtual Router Redundancy Protocol

Administrar rutas

La tabla de enrutamiento recopila rutas de varios orígenes: rutas estáticas y rutas locales. La tabla de enrutamiento puede aprender varias rutas al mismo destino desde varios orígenes. La tabla de enrutamiento enumera todas las rutas.

Configurar una ruta básica

Para configurar una ruta básica:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Routing Table > Basic > Route Configuration.



5. En la lista Route Type, seleccione uno de los siguientes tipos de ruta.
   - Default. Para crear una ruta predeterminada, solo debe especificar la dirección del siguiente salto y la preferencia.
   - Static. Para crear una ruta estática, especifique la dirección de red, la máscara de subred, la dirección del siguiente salto y la preferencia.
   - Static Reject. Para crear una ruta estática de rechazo, especifique la dirección de red, la máscara de subred y la preferencia.
6. Network Address muestra el prefijo de ruta IP del destino.
7. Subnet Mask indica la parte de la dirección de la interfaz IP que identifica la red conectada.

   También se conoce como máscara de subred/red.

8. Next Hop IP Address muestra la dirección IP del router de salida que se usa al reenviar tráfico al siguiente router (si lo hay) en la ruta hacia el destino.

   El siguiente router siempre es uno de los vecinos adyacentes o la dirección IP de la interfaz local para una red conectada directamente.

9. Preference muestra un valor entero 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 ingresa en la base de datos de reenvío. Al especificar la preferencia de una ruta estática, el usuario controla si una ruta estática tiene más o menos prioridad que las rutas de los protocolos de enrutamiento dinámico. La preferencia también controla si una ruta estática tiene más o menos prioridad que otras rutas estáticas al mismo destino.

10. Use Description para especificar una descripción que identifique esta ruta.

    La descripción debe constar de caracteres alfanuméricos, guiones o guiones bajos y puede tener hasta 31 caracteres.

11. Haga clic en el botón Add.
Se agrega la ruta estática al switch.
12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 105. Configuración de rutas básicas de la tabla de enrutamiento

Campo	Descripción
Network Address	El prefijo de ruta IP del destino.
Subnet Mask	También conocida como máscara de subred/red, indica la parte de la dirección de la interfaz IP que identifica la red conectada.
Protocol	Este campo indica qué protocolo creó la ruta especificada. Las posibilidades son las siguientes: • Local • Static
Route Type	Este campo puede ser Connected, Static o Dynamic, según el protocolo.
Next Hop Interface	La interfaz de salida del router que se usa al reenviar tráfico al destino.
Next Hop Address	La dirección IP del router de salida que se usa al reenviar tráfico al siguiente router (si lo hay) en la ruta hacia el destino. El siguiente router siempre es uno de los vecinos adyacentes o la dirección IP de la interfaz local para una red conectada directamente.

Tabla 105. Configuración de rutas básicas de la tabla de enrutamiento (continuación)

Campo	Descripción
Preference	La preferencia es un valor entero de 0 a 255. El usuario 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 ingresa en la base de datos de reenvío. Al especificar la preferencia de una ruta estática, el usuario controla si una ruta estática tiene más o menos prioridad que las rutas de los protocolos de enrutamiento dinámico. La preferencia también controla si una ruta estática tiene más o menos prioridad que otras rutas estáticas al mismo destino.
Metric	Costo administrativo de la ruta al destino. Si no se ingresa un valor, el predeterminado es 1. El rango es 0–255.

Configurar rutas avanzadas

Para configurar rutas avanzadas:

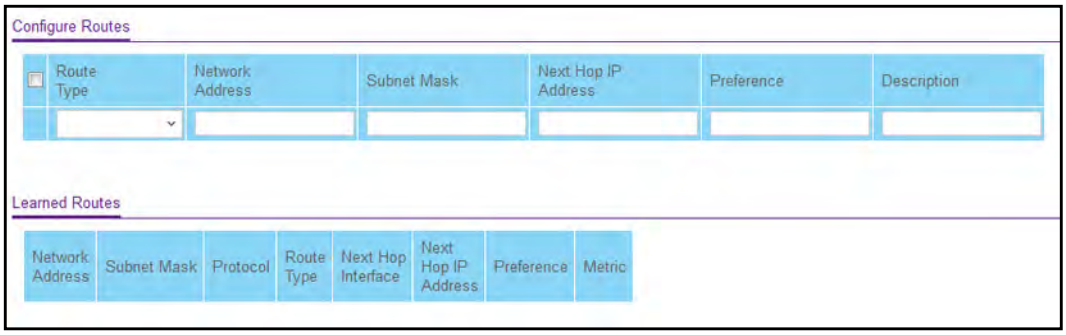
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Routing Table> Advanced > Route Configuration.



5. Use el campo Route Type para especificar Default o una ruta estática de rechazo.

   Si crea una ruta predeterminada, solo debe especificar la dirección IP del siguiente salto; de lo contrario, debe completar todos los campos.

6. Network Address muestra el prefijo de ruta IP del destino.
7. Subnet Mask indica la parte de la dirección de la interfaz IP que identifica la red conectada.

También se conoce como máscara de subred/red.

8. Next Hop IP Address muestra la dirección IP del router de salida que se usa al reenviar tráfico al siguiente router (si lo hay) en la ruta hacia el destino.

   El siguiente router siempre es uno de los vecinos adyacentes o la dirección IP de la interfaz local para una red conectada directamente.

9. Preference muestra un valor entero 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 ingresa en la base de datos de reenvío. Al especificar la preferencia de una ruta estática, el usuario controla si una ruta estática tiene más o menos prioridad que las rutas de los protocolos de enrutamiento dinámico. La preferencia también controla si una ruta estática tiene más o menos prioridad que otras rutas estáticas al mismo destino.

10. Use Description para especificar una descripción que identifique esta ruta.

    La descripción debe constar de caracteres alfanuméricos, guiones o guiones bajos y puede tener hasta 31 caracteres.

11. Haga clic en el botón Add.

Se agrega la ruta estática al switch.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 106. Configuración de rutas - Rutas aprendidas

Campo	Descripción
Network Address	El prefijo de ruta IP del destino.
Subnet Mask	También conocida como máscara de subred/red, indica la parte de la dirección de la interfaz IP que identifica la red conectada.
Protocol	Este campo indica qué protocolo creó la ruta especificada. Las posibilidades son las siguientes: • Local • Static
Route Type	Este campo puede ser default o static.
Next Hop Interface	La interfaz de salida del router que se usa al reenviar tráfico al destino.
Next Hop IP Address	La dirección IP del router de salida que se usa al reenviar tráfico al siguiente router (si lo hay) en la ruta hacia el destino. El siguiente router siempre es uno de los vecinos adyacentes o la dirección IP de la interfaz local para una red conectada directamente.

Tabla 106. Configuración de rutas - Rutas aprendidas (continuación)

Campo	Descripción
Preference	La preferencia es un valor entero de 0 a 255. El usuario 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 ingresa en la base de datos de reenvío. Al especificar la preferencia de una ruta estática, el usuario controla si una ruta estática tiene más o menos prioridad que las rutas de los protocolos de enrutamiento dinámico. La preferencia también controla si una ruta estática tiene más o menos prioridad que otras rutas estáticas al mismo destino.
Metric	Costo administrativo de la ruta al destino. Si no se ingresa un valor, el predeterminado es 1. El rango es 0–255.

Especificar las preferencias de rutas

Puede configurar la preferencia predeterminada de cada protocolo, por ejemplo, 60 para rutas estáticas, 120 para RIP. Estos valores son arbitrarios en el rango de 1 a 255 y son independientes 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 elige seleccionando la ruta con el valor de preferencia más bajo. Cuando hay varias rutas a un destino, se usan los valores de preferencia para determinar la ruta preferida. Si aún hay empate, se elige la ruta con la mejor métrica de ruta. Para evitar problemas con métricas no coincidentes (como las métricas de RIP y de Open Shortest Path First [OSPF], que no son directamente comparables), debe configurar valores de preferencia distintos para cada protocolo.

Para especificar las preferencias de ruta

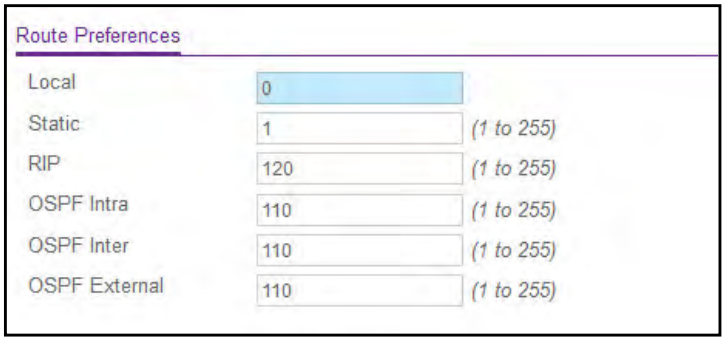
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Routing Table > Advanced > Route Preferences.



5. Use Static para especificar el valor de preferencia de las rutas estáticas en el router. El valor predeterminado es 1. El rango es de 1 a 255.
6. Especifique el valor de preferencia de las rutas RIP en el router. El valor predeterminado es 120. El rango es de 1 a 255.
7. Especifique el valor de preferencia de las rutas OSPF Intra en el router.

El valor predeterminado es 110. El rango es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que se den preferencias a las rutas aprendidas mediante OSPF en el siguiente orden: intra < inter < type-1 < type-2.

8. Especifique el valor de preferencia de las rutas OSPF Inter en el router.

El valor predeterminado es 110. El rango es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que se den preferencias a las rutas aprendidas mediante OSPF en el siguiente orden: intra < inter < type-1 < type-2.

9. Especifique el valor de preferencia de las rutas OSPF External en el router.

El valor predeterminado es 110. El rango es de 1 a 255. La especificación de OSPF (RFC 2328) requiere que el valor de preferencia sea el mismo para todos los tipos de rutas OSPF externas, como type1/type2/nssa1/nssa2.

10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
El campo Local muestra el valor de preferencia de rutas locales.

Configurar los ajustes de IP de enrutamiento

Puede configurar los ajustes de IP de enrutamiento del switch, a diferencia de los ajustes de IP de una interfaz.

Para configurar los ajustes de IP de enrutamiento:

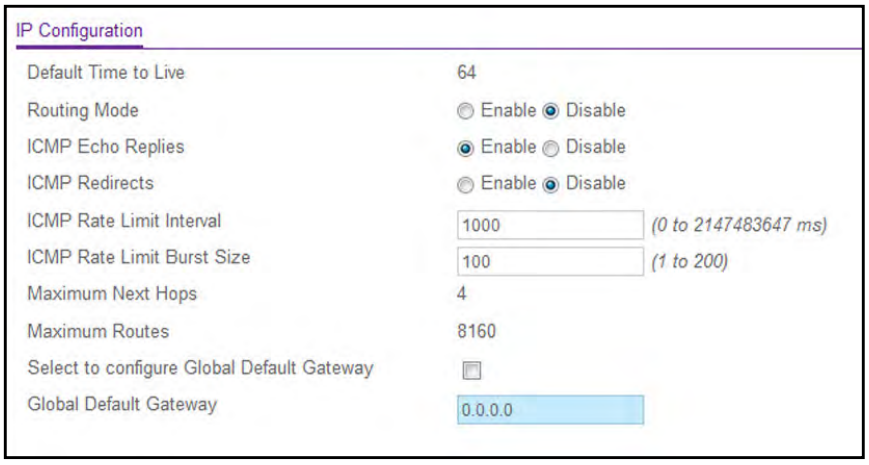
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IP > Basic > IP Configuration.



5. Use Routing Mode para seleccionar Enable o Disable.

Debe habilitar el enrutamiento en el switch antes de poder enrutar a través de cualquiera de las interfaces. El valor predeterminado es Disable.

6. Use ICMP Echo Replies para seleccionar Enable o Disable.

Si selecciona Enable, solo el router puede enviar respuestas ECHO. De forma predeterminada, se envían respuestas ICMP Echo a las solicitudes de eco.

7. Use ICMP Redirects para seleccionar Enable o Disable.

Si se habilita globalmente y a nivel de interfaz, solo el router puede enviar ICMP Redirects.

8. Use ICMP Rate Limit Interval para controlar los paquetes de error ICMP especificando el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

De forma predeterminada, el límite de tasa es de 100 paquetes/s (el intervalo de ráfaga es de 1000 ms). Para deshabilitar el límite de tasa ICMP, establezca este campo en 0. El intervalo válido es de 0 a 2147483647.

9. Use ICMP Rate Limit Burst Size para controlar los paquetes de error ICMP especificando el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

De forma predeterminada, el tamaño de ráfaga es de 100 paquetes. Cuando el intervalo de ráfaga es 0, configurar este campo no es una operación válida. El rango válido del tamaño de ráfaga es de 1 a 200.

10. Use Select para configurar Global Default Gateway y editar el campo Global Default Gateway.

11. Use Global Default Gateway para establecer la puerta de enlace predeterminada global en el valor configurado manualmente. Una puerta de enlace predeterminada configurada con este comando tiene prioridad sobre una puerta de enlace predeterminada aprendida de un servidor DHCP. Solo se puede configurar una puerta de enlace predeterminada. Si ejecuta este comando varias veces, cada comando reemplaza el valor anterior.

12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 107. Configuración de IP de enrutamiento

Campo	Descripción
Default Time to Live	El 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 la capa de transporte no proporciona un valor TTL.
Maximum Next Hops	El número máximo de saltos que admite el switch. Es una constante definida en tiempo de compilación.
Maximum Routes	El número máximo de rutas (tamaño de la tabla de enrutamiento) que admite el switch. Es una constante definida en tiempo de compilación.

Ver estadísticas

Las estadísticas que se informan en esta página son las especificadas en RFC 1213.

Para ver estadísticas:

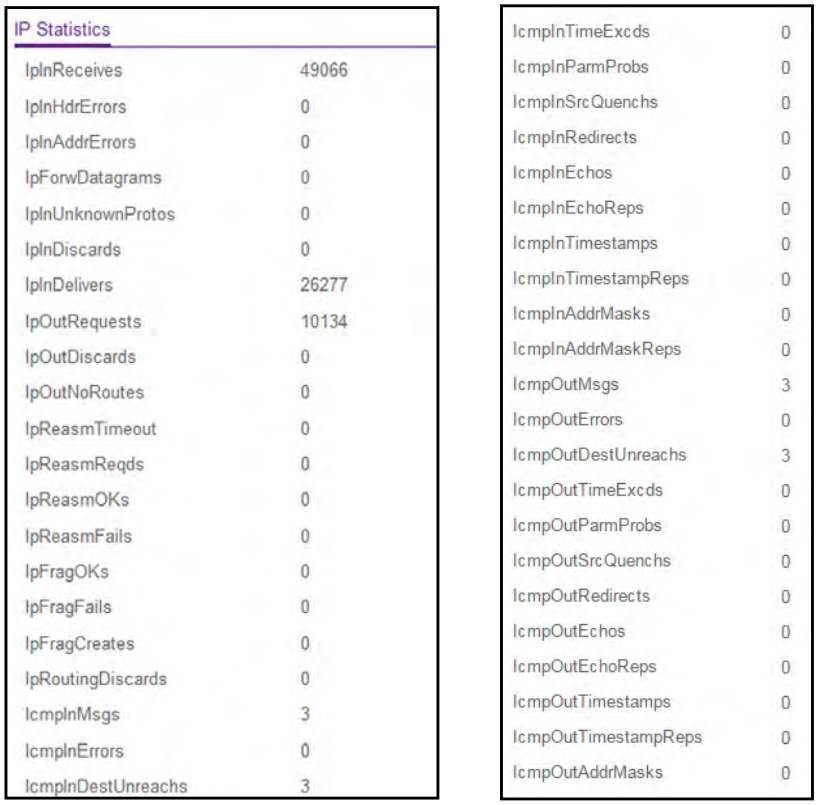
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> IP > Basic > Statistics.



IP Statistics	
IpInReceives	49066
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	26277
IpOutRequests	10134
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	3
IcmpInErrors	0
IcmpInDestUnreachs	3
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenchs	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoReps	0
IcmpInTimestamps	0
IcmpInTimestampReps	0
IcmpInAddrMasks	0
IcmpInAddrMaskReps	0
IcmpOutMsgs	3
IcmpOutErrors	0
IcmpOutDestUnreachs	3
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenchs	0
IcmpOutRedirects	0
IcmpOutEchos	0
IcmpOutEchoReps	0
IcmpOutTimestamps	0
IcmpOutTimestampReps	0
IcmpOutAddrMasks	0

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 108. Estadísticas básicas de IP

Campo	Descripción
IpInReceives	El número total de datagramas de entrada recibidos de las interfaces, incluidos los recibidos con errores.
IpInHdrErrors	El número de datagramas de entrada descartados por errores en sus encabezados IP, como sumas de comprobación incorrectas, versiones no coincidentes, otros errores de formato, tiempo de vida excedido, errores detectados al procesar sus opciones IP, etc.
IpInAddrErrors	El número de datagramas de entrada descartados porque la dirección IP del campo de destino de su encabezado IP no era una dirección válida para recibirse en esta entidad. Este recuento incluye direcciones no válidas (por ejemplo, 0.0.0.0) y direcciones de clases no compatibles (clase E). Para las entidades que no son puertas de enlace IP y por lo tanto no reenvían datagramas, este contador incluye los datagramas descartados porque la dirección de destino no era una dirección local.
IpForwDatagrams	El 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 las entidades que no actúan como puertas de enlace IP, este contador incluye solo los paquetes que se enrutaron desde el origen a través de esta entidad y cuyo procesamiento de la opción source-route fue exitoso.

Tabla 108. Estadísticas básicas de IP (continuación)

Campo	Descripción
IpInUnknownProtos	El número de datagramas con dirección local recibidos correctamente pero descartados por un protocolo desconocido o no compatible.
IpInDiscards	El número de datagramas IP de entrada que no presentaron problemas que impidieran su procesamiento, pero que se descartaron (por falta de espacio en búfer). Este contador no incluye los datagramas descartados mientras esperaban el reensamblado.
IpInDelivers	El número total de datagramas de entrada entregados correctamente a los protocolos de usuario IP (incluido ICMP).
IpOutRequests	El número total de datagramas IP que los protocolos de usuario IP locales (incluido ICMP) entregaron a IP en solicitudes de transmisión. Este contador no incluye los datagramas contados en ipForwDatagrams.
IpOutDiscards	El número de datagramas IP de salida que no presentaron problemas que impidieran su transmisión a su destino, pero que se descartaron por motivos como falta de espacio en búfer. Este contador incluiría los datagramas contados en ipForwDatagrams si alguno de esos paquetes cumpliera este criterio (discrecional) de descarte.
IpOutNoRoutes	El número de datagramas IP descartados porque no se pudo encontrar una ruta para transmitirlos a su destino. Este contador 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.
IpReasmTimeout	El número máximo de segundos que se retienen los fragmentos recibidos mientras esperan el reensamblado en esta entidad.
IpReasmReqds	El número de fragmentos IP recibidos que se reensamblaron en esta entidad.
IpReasmOKs	El número de datagramas IP reensamblados correctamente.
IpReasmFails	El número de fallas detectadas por el algoritmo de reensamblado IP (por cualquier motivo: tiempo de espera agotado, errores, etc.). No es necesariamente un recuento de fragmentos IP descartados, ya que algunos algoritmos pueden perder la cuenta del número de fragmentos al combinarlos a medida que se reciben.
IpFragOKs	El número de datagramas IP que se fragmentaron en esta entidad.
IpFragFails	El número de datagramas IP descartados porque debían fragmentarse en esta entidad pero no fue posible, por motivos como tener activado el indicador Don't Fragment.
IpFragCreates	El número de fragmentos de datagramas IP generados como resultado de la fragmentación en esta entidad.
IpRoutingDiscards	El número de entradas de enrutamiento descartadas aunque eran válidas. Un posible motivo para descartar una entrada así podría ser liberar espacio en búfer para otras entradas de enrutamiento.
IcmpInMsgs	El número total de mensajes ICMP que recibió la entidad. Este contador incluye todos los contados por icmpInErrors.

Tabla 108. Estadísticas básicas de IP (continuación)

Campo	Descripción
IcmpInErrors	El número de mensajes ICMP que la entidad recibió pero determinó que tenían errores específicos de ICMP (sumas de comprobación ICMP incorrectas, longitud incorrecta, etc.).
IcmpInDestUnreachs	El número de mensajes ICMP de destino inalcanzable recibidos.
IcmpInTimeExcds	El número de mensajes ICMP de tiempo excedido recibidos.
IcmpInParmProbs	El número de mensajes ICMP de problema de parámetros recibidos.
IcmpInSrcQuenchs	El número de mensajes ICMP de source quench recibidos.
IcmpInRedirects	El número de mensajes ICMP de redirección recibidos.
IcmpInEchos	El número de mensajes ICMP de eco (solicitud) recibidos.
IcmpInEchoReps	El número de mensajes ICMP de respuesta de eco recibidos.
IcmpInTimestamps	El número de mensajes ICMP de marca de tiempo (solicitud) recibidos.
IcmpInTimestampReps	El número de mensajes ICMP de respuesta de marca de tiempo recibidos.
IcmpInAddrMasks	El número de mensajes ICMP de solicitud de máscara de dirección recibidos.
IcmpInAddrMaskReps	El número de mensajes ICMP de respuesta de máscara de dirección recibidos.
IcmpOutMsgs	El número total de mensajes ICMP que esta entidad intentó enviar. Este contador incluye todos los contados por icmpOutErrors.
IcmpOutErrors	El número de mensajes ICMP que esta entidad no envió debido a problemas detectados en ICMP, como la falta de búferes. Este valor no incluye los errores detectados fuera de la capa ICMP, como la imposibilidad de IP de enrutar el datagrama resultante. En algunas implementaciones puede que ningún tipo de error contribuya al valor de este contador.
IcmpOutDestUnreachs	El número de mensajes ICMP de destino inalcanzable enviados.
IcmpOutTimeExcds	El número de mensajes ICMP de tiempo excedido enviados.
IcmpOutParmProbs	El número de mensajes ICMP de problema de parámetros enviados.
IcmpOutSrcQuenchs	El número de mensajes ICMP de source quench enviados.
IcmpOutRedirects	El número de mensajes ICMP de redirección enviados. Para un host, siempre es cero, ya que los hosts no envían redirecciones.
IcmpOutEchos	El número de mensajes ICMP de eco (solicitud) enviados.
IcmpOutEchoReps	El número de mensajes ICMP de respuesta de eco enviados.
IcmpOutTimestamps	El número de mensajes ICMP de marca de tiempo (solicitud).
IcmpOutTimestampReps	El número de mensajes ICMP de respuesta de marca de tiempo enviados.
IcmpOutAddrMasks	El número de mensajes ICMP de solicitud de máscara de dirección enviados.

Configurar los parámetros de enrutamiento del switch

Puede configurar los parámetros de enrutamiento del switch, a diferencia de los de una interfaz.

Para configurar los parámetros de enrutamiento del switch:

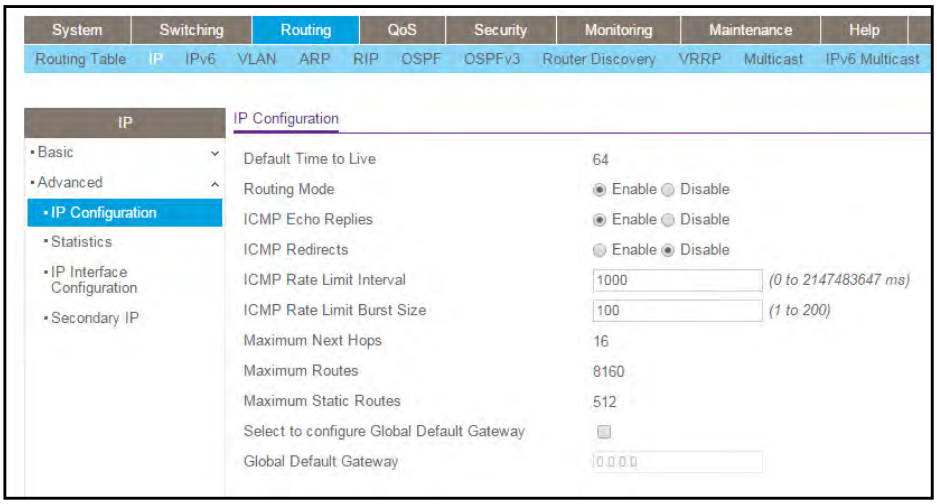
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IP > Advanced > IP Configuration.



5. Use Routing Mode para seleccionar Enable o Disable.

Debe habilitar el enrutamiento en el switch antes de poder enrutar a través de cualquiera de las interfaces. El valor predeterminado es Disable.

6. Use ICMP Echo Replies para seleccionar Enable o Disable.

Si selecciona Enable, solo el router puede enviar respuestas ECHO. De forma predeterminada, se envían respuestas ICMP Echo a las solicitudes de eco.

7. Use ICMP Redirects para seleccionar Enable o Disable.

El router solo puede enviar redirecciones ICMP si esta opción está habilitada globalmente y en la interfaz.

8. Use ICMP Rate Limit Interval para controlar los paquetes de error ICMP especificando el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

   De forma predeterminada, el límite es de 100 paquetes/s (el intervalo de ráfaga es de 1000 ms). Para deshabilitar la limitación de velocidad ICMP, establezca este campo en 0. El intervalo válido va de 0 a 2147483647.

9. Use ICMP Rate Limit Burst Size para controlar los paquetes de error ICMP especificando el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

   De forma predeterminada, el tamaño de ráfaga es de 100 paquetes. Cuando el intervalo de ráfaga es 0, no es válido configurar este campo. El tamaño de ráfaga válido es de 1 a 200.

10. Use Select to Configure Global Default Gateway para editar el campo Global Default Gateway.

11. Use Global Default Gateway para establecer la puerta de enlace predeterminada global con el valor configurado manualmente.

   Una puerta de enlace predeterminada configurada con este comando tiene preferencia sobre una aprendida de un servidor DHCP. Solo se puede configurar una puerta de enlace predeterminada. Si ejecuta este comando varias veces, cada comando reemplaza el valor anterior.

12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 109. Configuración IP de enrutamiento

Campo	Descripción
Default Time to Live	El 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 la capa de transporte no proporciona un valor TTL.
Maximum Next Hops	El número máximo de saltos que admite el switch. Es una constante definida en tiempo de compilación.
Maximum Routes	El número máximo de rutas (tamaño de la tabla de enrutamiento) que admite el switch. Es una constante definida en tiempo de compilación.
Máximo de rutas estáticas	Número máximo de rutas estáticas admitidas por el switch.

Ver las estadísticas IP

Las estadísticas que se informan en esta página son las especificadas en RFC 1213.

Para ver las estadísticas IP:

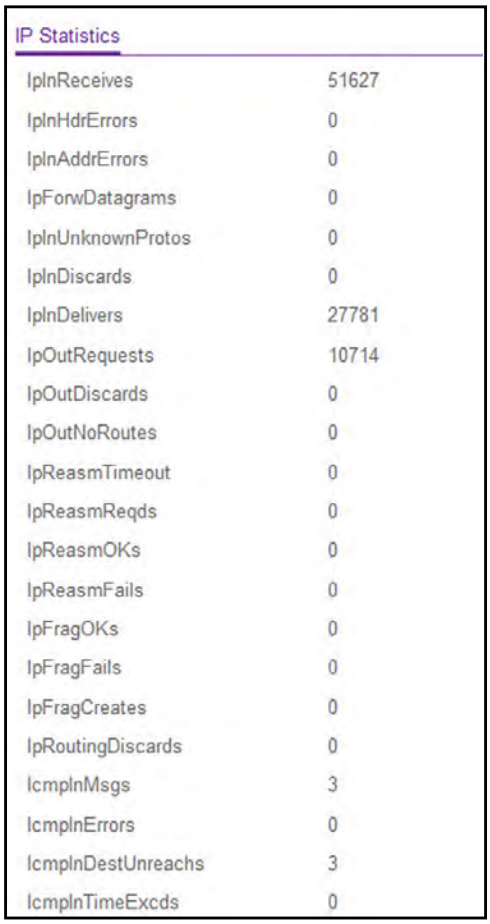
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. **Seleccione Routing> IP > Advanced > Statistics.**



La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 110. Estadísticas IP

Campo	Descripción
IpInReceives	El 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, incluidas sumas de verificación incorrectas, versión no coincidente, otros errores de formato, tiempo de vida excedido, errores al procesar sus opciones IP, etc.

Tabla 110. 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 (como la Clase E). En entidades que no son gateways IP y que por lo tanto no reenvían datagramas, este contador 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 razones como 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. Incluye los datagramas que un host no puede enrutar porque todas sus puertas de enlace predeterminadas están inactivas.
IpReasmTimeout	Número máximo de segundos que se retienen los fragmentos recibidos mientras esperan reensamblaje en esta entidad.
IpReasmReqds	Número de fragmentos IP recibidos que debían reensamblarse 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 del número de fragmentos al combinarlos conforme se reciben.
IpFragOKs	El número de datagramas IP que se fragmentaron en esta entidad.

Tabla 110. Estadísticas IP (continuación)

Campo	Descripción
IpFragFails	Número de datagramas IP descartados porque debían fragmentarse en esta entidad pero no fue posible; por ejemplo, esto ocurre si tienen 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 son 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	El número de mensajes ICMP de destino inalcanzable recibidos.
IcmpInTimeExcds	El número de mensajes ICMP de tiempo excedido recibidos.
IcmpInParmProbs	El número de mensajes ICMP de problema de parámetros recibidos.
IcmpInSrcQuenchs	El número de mensajes ICMP de source quench recibidos.
IcmpInRedirects	El número de mensajes ICMP de redirección recibidos.
IcmpInEchos	El número de mensajes ICMP de eco (solicitud) recibidos.
IcmpInEchoReps	El número de mensajes ICMP de respuesta de eco recibidos.
IcmpInTimestamps	El número de mensajes ICMP de marca de tiempo (solicitud) recibidos.
IcmpInTimestampReps	Número de mensajes ICMP de respuesta de marca de tiempo recibidos.
IcmpInAddrMasks	El número de mensajes ICMP de solicitud de máscara de dirección recibidos.
IcmpInAddrMaskReps	El número de mensajes ICMP de respuesta de máscara de dirección recibidos.
IcmpOutMsgs	El 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	El número de mensajes ICMP de destino inalcanzable enviados.
IcmpOutTimeExcds	El número de mensajes ICMP de tiempo excedido enviados.
IcmpOutParmProbs	El número de mensajes ICMP de problema de parámetros enviados.
IcmpOutSrcQuenchs	Número de mensajes ICMP de source quench enviados.

Tabla 110. Estadísticas IP (continuación)

Campo	Descripción
IcmpOutRedirects	Número de mensajes ICMP de redirección enviados. En un host es cero, ya que los hosts no envían redirecciones.
IcmpOutEchos	El número de mensajes ICMP de eco (solicitud) enviados.
IcmpOutEchoReps	El número de mensajes ICMP de respuesta de eco enviados.
IcmpOutTimestamps	El número de mensajes ICMP de marca de tiempo (solicitud).
IcmpOutTimestampReps	El número de mensajes ICMP de respuesta de marca de tiempo enviados.
IcmpOutAddrMasks	El número de mensajes ICMP de solicitud de máscara de dirección enviados.
IcmpOutAddrMaskReps	Número de mensajes ICMP de respuesta de máscara de dirección enviados.

Configurar la interfaz IP

Puede actualizar los datos de la interfaz IP de este switch.

Para configurar la interfaz IP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

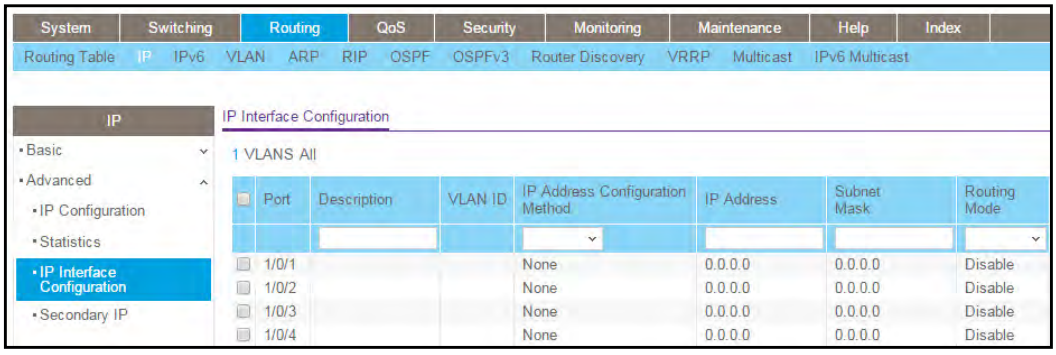
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

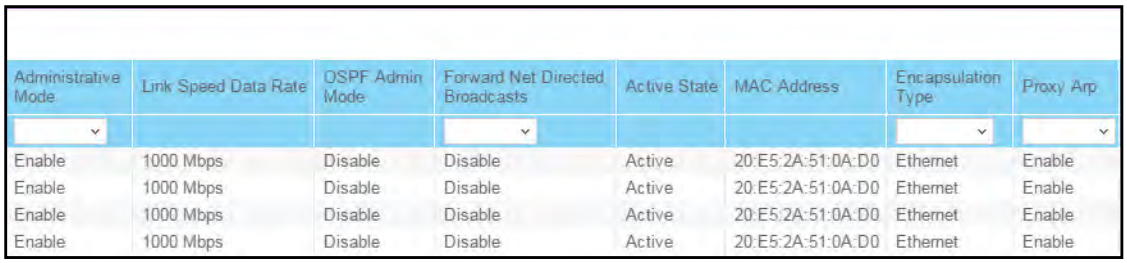
   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

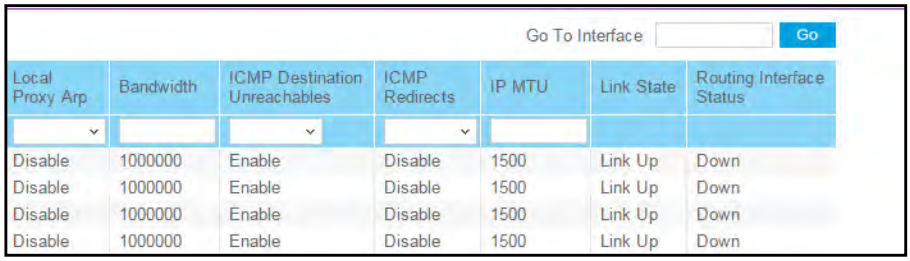
4. Seleccione Routing> IP > Advanced > IP Interface Configuration.

   La página se muestra en tres partes.





Administrative Mode	Link Speed Data Rate	OSPF Admin Mode	Forward Net Directed Broadcasts	Active State	MAC Address	Encapsulation Type	Proxy Arp
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable



Local Proxy Arp	Bandwidth	ICMP Destination Unreachables	ICMP Redirects	IP MTU	Link State	Routing Interface Status
Disable	1000000	Enable	Disable	1500	Link Up	Down
Disable	1000000	Enable	Disable	1500	Link Up	Down
Disable	1000000	Enable	Disable	1500	Link Up	Down
Disable	1000000	Enable	Disable	1500	Link Up	Down

5. 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 Port, marque la casilla de la interfaz que desea configurar.
6. Use Description para ingresar la descripción de la interfaz.
7. Use IP Address Configuration Method para indicar el método con el que se configura la dirección IP en la interfaz.

   Hay tres métodos: None, Manual y 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.

8. Use IP Address para ingresar la dirección IP de la interfaz.
9. Use Subnet Mask para ingresar 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.

10. En la lista Routing Mode, seleccione Enable o Disable.

El valor predeterminado es Enable.
11. Use Administrative Mode para habilitar o deshabilitar el modo administrativo de la interfaz. El valor predeterminado es Enable. Este modo no se admite en interfaces VLAN lógicas.

12. Use Forward Net Directed Broadcasts para seleccionar cómo se manejan los paquetes broadcast dirigidos a la red.

    Si selecciona Enable, los broadcasts dirigidos a la red se reenvían.

Si selecciona Disable, se descartan. El valor predeterminado es Disable.

13. Use Encapsulation Type para seleccionar el tipo de encapsulamiento de capa de enlace de los paquetes transmitidos desde la interfaz especificada.

Los valores posibles son Ethernet y SNAP. El valor predeterminado es Ethernet.
14. Use Proxy Arp para deshabilitar o habilitar el proxy ARP en la interfaz especificada.
15. Use Local Proxy Arp para deshabilitar o habilitar el proxy ARP local en la interfaz especificada.
16. Use Bandwidth (kbps) para especificar el ancho de banda configurado en esta interfaz.

Este parámetro comunica la velocidad de la interfaz a los protocolos de nivel superior. OSPF usa el ancho de banda para calcular el costo del enlace. El rango válido es de 1 a 10000000.

17. Use ICMP Destination Unreachables para especificar el modo de envío de mensajes ICMP de destino inalcanzable en esta interfaz.

Si está en Disabled, esta interfaz no envía mensajes ICMP de destino inalcanzable. Este modo está habilitado de forma predeterminada.

18. Use ICMP Redirects para habilitar o deshabilitar el modo de redirecciones ICMP.

El router envía una redirección ICMP en una interfaz solo si las redirecciones están habilitadas tanto globalmente como en la interfaz. Este modo está habilitado de forma predeterminada.

19. Use IP MTU para especificar el tamaño máximo de los paquetes IP enviados por una interfaz.

El rango válido va de 68 bytes a la MTU del enlace. El valor predeterminado es 0. Un valor de 0 indica que la MTU IP no está configurada. En ese caso, el router usa la MTU del enlace como MTU IP. La MTU IP es el tamaño máximo de trama menos la longitud del encabezado de capa 2.

20. Para eliminar la dirección IP de la interfaz seleccionada, haga clic en el botón Delete.
21. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 111. IP Interface Configuration

Campo	Descripción
ID de VLAN	ID de VLAN de la interfaz.
Modo administrativo OSPF	Muestra el modo administrativo OSPF de la interfaz. El valor predeterminado es Disable.
Estado del enlace	El estado de la interfaz especificada es Active o Inactive. Una interfaz se considera activa si el enlace está activo y está en estado de reenvío.
Estado de la interfaz de enrutamiento	Indica si el estado del enlace está activo o inactivo.

Configurar la dirección IP secundaria

Para configurar la dirección IP secundaria:

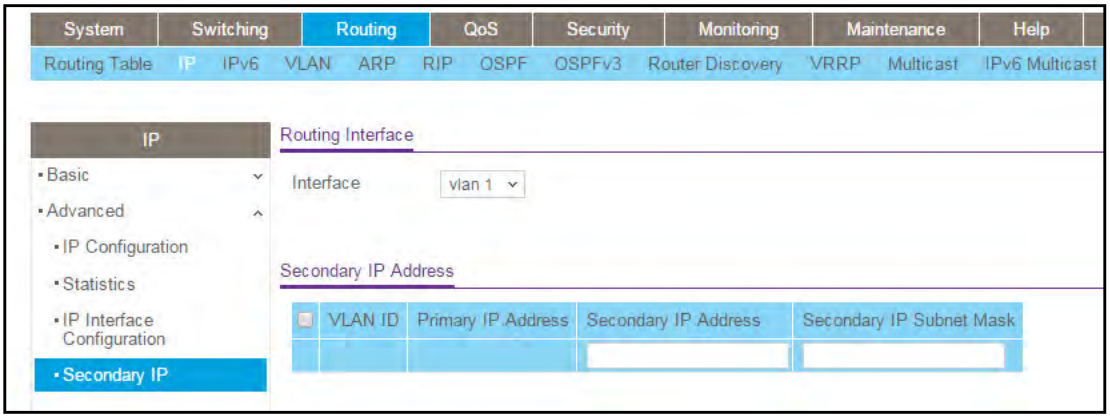
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IP > Advanced > Secondary IP.



5. En la lista Routing Interface, seleccione la interfaz.
6. En el campo Secondary IP Address, agregue una dirección IP secundaria a la interfaz seleccionada.

7. En el campo Secondary IP Subnet Mask, ingrese la máscara de subred asociada con la dirección IP secundaria.

   También se llama máscara de subred/red y define la parte de la dirección IP de la interfaz que identifica la red conectada. Este valor es de solo lectura una vez configurado.

8. Haga clic en el botón Add.

Se agrega la dirección IP secundaria de la interfaz seleccionada.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 112. IP secundaria

Campo	Descripción
ID de VLAN	ID de VLAN asociado con la interfaz mostrada o configurada.
Dirección IP principal	Dirección IP principal de la interfaz.

Administrar IPv6

Configurar los ajustes globales de IPv6

Puede configurar parámetros de enrutamiento IPv6 del switch, a diferencia de los de una interfaz.

Para configurar los ajustes globales de IPv6:

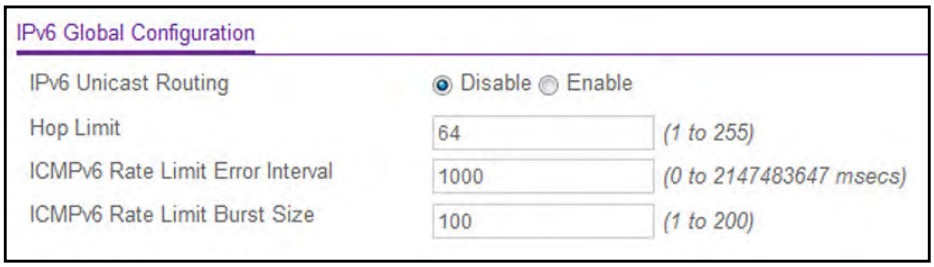
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Basic > Global Configuration.



5. En el campo IPv6 Unicast Routing, seleccione la opción para habilitar (Enable) o deshabilitar (Disable) globalmente el enrutamiento unicast IPv6.
6. En el campo Hop Limit, ingrese el número de saltos unicast usado en los paquetes IPv6 originados por el nodo.

   El valor también se incluye en los anuncios de router. Los valores válidos van de 1 a 255, inclusive. El valor predeterminado es Not Configured, lo que significa que se envía cero en los anuncios de router.

7. En el campo ICMPv6 Rate Limit Error Interval, especifique el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

   Este valor controla los paquetes de error ICMPv6. El límite predeterminado es de 100 paquetes por segundo, es decir, un intervalo de ráfaga de 1000 ms. Para deshabilitar la limitación ICMP, establezca este campo en 0. El intervalo válido va de 0 a 2147483647 ms.

8. En el campo ICMPv6 Rate Limit Burst Size, especifique el número de paquetes de error ICMP permitidos por intervalo de ráfaga.

   Este valor controla los paquetes de error ICMP. El tamaño de ráfaga predeterminado es de 100 paquetes. Cuando el intervalo de ráfaga es 0, no es válido configurar este campo. El tamaño de ráfaga válido es de 1 a 200.

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

Ver la tabla de rutas IPv6

Para ver la tabla de rutas IPv6:

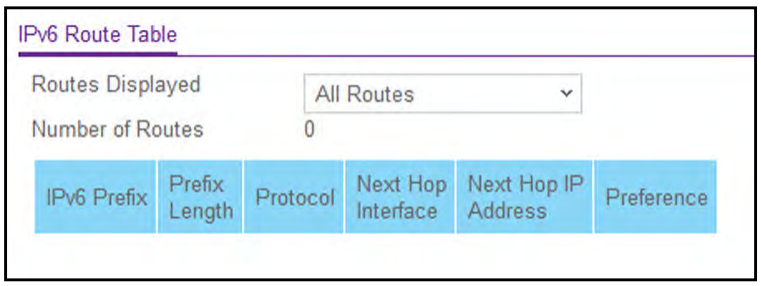
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Basic > Route Table.



5. En la lista Routes Displayed, seleccione una de las siguientes opciones:

- All Routes. Muestra todas las rutas IPv6 activas.
- Best Routes Only. Muestra solo las mejores rutas activas.
- Configured Routes Only. Muestra las rutas configuradas por el usuario.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh).

La siguiente tabla describe la información no configurable que se muestra.

Tabla 113. Tabla de rutas IPv6

Campo	Descripción
Número de rutas	Número total de rutas activas en la tabla de rutas.
Prefijo IPv6	Prefijo de red de la ruta activa.
Longitud del prefijo	Longitud del prefijo de la ruta activa.
Protocolo	Tipo de protocolo de la ruta activa.
Interfaz del siguiente salto	Interfaz por la que la ruta está activa. Para una ruta de rechazo, el siguiente salto es una interfaz Null0.
Dirección IP del siguiente salto	Dirección IPv6 del siguiente salto de la ruta activa.
Preferencia	Preferencia de la ruta configurada.

Configurar los ajustes de interfaz IPv6

Para configurar los ajustes de interfaz IPv6:

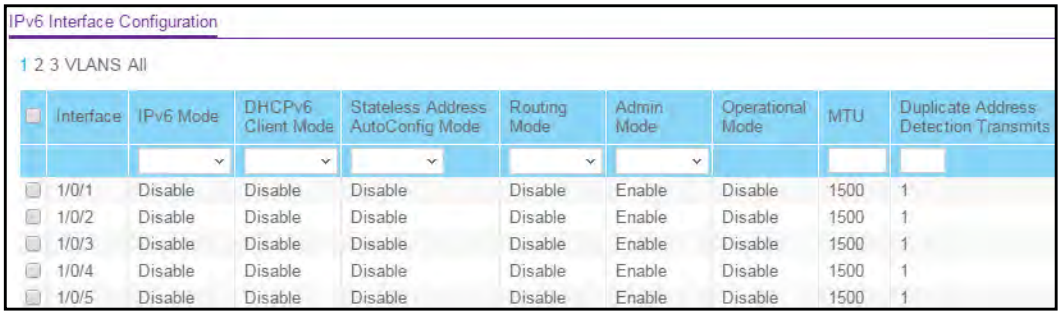
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

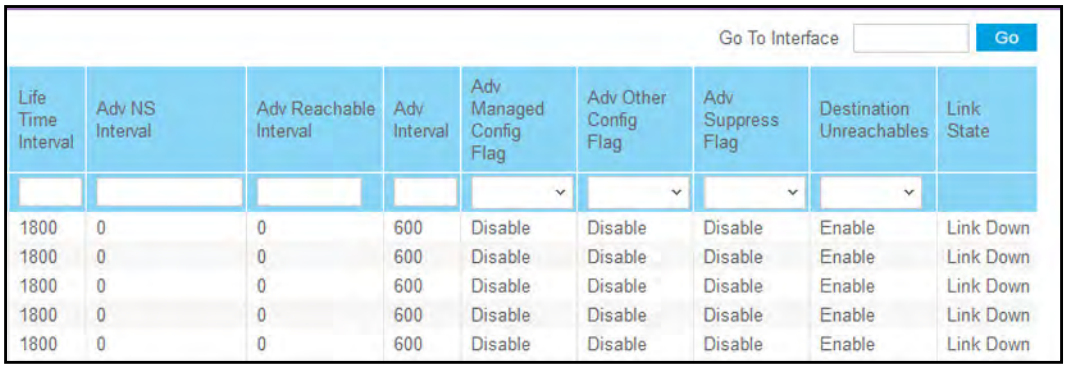
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Interface Configuration.





5. 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, seleccione la casilla de la interfaz que desea configurar.

     Todas las interfaces físicas son válidas.

6. Seleccione Enable o Disable en la lista IPv6 Mode.

Con el modo IPv6 habilitado, la interfaz puede operar con IPv6 sin una dirección global. En ese caso, se usa una dirección link-local basada en EUI-64. El valor predeterminado es Disable.

7. En la lista DHCPv6 Client Mode, seleccione Enable o Disable para el modo cliente DHCPv6 en una interfaz.

En un momento dado, solo una interfaz puede actuar como cliente. El valor predeterminado es Disable.

8. En la lista Stateless Address AutoConfig Mode, seleccione Enable o Disable para el modo de autoconfiguración de direcciones sin estado en una interfaz.

El valor predeterminado es Disable.
9. En la lista Routing Mode, seleccione Enable o Disable para el modo de enrutamiento de una interfaz. El valor predeterminado es Disable.
10. En la lista Admin Mode, seleccione Enable o Disable para el modo IPv6.

El valor predeterminado es Disable. Con el modo IPv6 habilitado, la interfaz puede operar con IPv6 sin una dirección global. En ese caso, se usa una dirección link-local basada en EUI-64.

11. En el campo MTU, especifique la unidad máxima de transmisión de una interfaz.

Si el valor es 0, la interfaz no está habilitada para enrutamiento. No es válido establecer 0 si el enrutamiento está habilitado. El rango de MTU es de 1280 a 1500. El valor predeterminado es 1500.

12. En el campo Duplicate Address Detection Transmits, especifique el número de transmisiones de detección de direcciones duplicadas (DAD) en una interfaz.

Los valores de transmisiones DAD deben estar entre 0 y 600. El valor predeterminado es 1.

13. Especifique el Life Time Interval de los anuncios de router enviados desde la interfaz.

    Este valor debe ser mayor o igual que el intervalo máximo de anuncio. 0 significa no usar el router como router predeterminado. El rango es de 0 a 9000. El valor predeterminado es 1800.

14. En el campo Adv NS Interval, especifique el campo de tiempo de retransmisión de los anuncios de router enviados desde la interfaz.

Un valor de 0 significa que no se especifica el intervalo para el router. El rango del intervalo de solicitud de vecinos es de 1000 a 4294967295. El valor predeterminado es 0.

15. En el campo Adv Reachable Interval, especifique el tiempo de anuncio de router.

    Es el tiempo durante el que se considera alcanzables a los vecinos después de la confirmación ND. El rango es de 0 a 3600000. El valor predeterminado es 0.

16. Use el campo Adv Interval para especificar el tiempo máximo permitido entre envíos de anuncios de router desde la interfaz.

    El rango del intervalo máximo de anuncio es de 4 a 1800. El valor predeterminado es 600.

17. En la lista Adv Other Config Flag, seleccione Enable o Disable para especificar el indicador de otra configuración con estado de los anuncios de router.

    El valor predeterminado de este indicador es Disable.

18. En la lista Adv Suppress Flag, seleccione Enable o Disable para la supresión de anuncios de router en una interfaz.

    El valor predeterminado del indicador de supresión es Disable.

19. En la lista Destination Unreachables, seleccione Enable o Disable para el modo de envío de mensajes ICMPv6 de destino inalcanzable en esta interfaz.

    Si se deshabilita, esta interfaz no envía mensajes ICMPv6 de destino inalcanzable. De forma predeterminada, este modo está habilitado.

20. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 114. Configuración avanzada de interfaz IPv6

Campo	Descripción
Modo operativo	Especifica el estado operativo de una interfaz. El valor predeterminado es Disable.
Estado del enlace	Indica si el enlace está activo o inactivo.

Configurar los ajustes de prefijos IPv6

Para configurar los ajustes de prefijos IPv6:

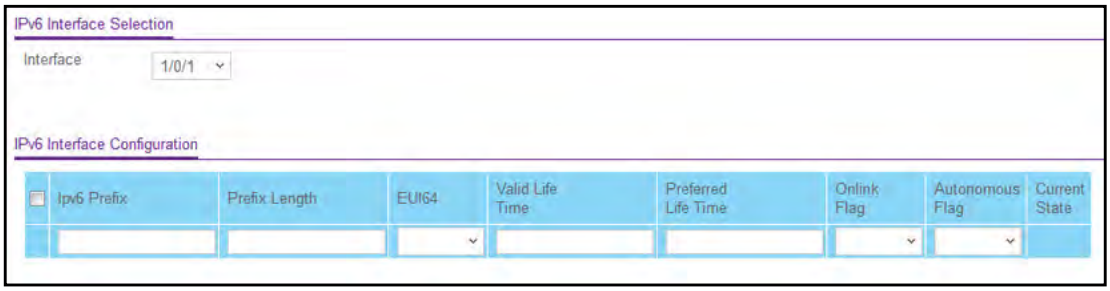
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing> IPv6 > Advanced > Prefix Configuration.**



5. En la lista Interface, seleccione la interfaz.

   Al cambiar la selección, la página se actualiza y todos los campos se actualizan para el puerto recién seleccionado. Todas las interfaces físicas son válidas.

6. En el campo IPv6 Prefix, especifique el prefijo IPv6 de una interfaz.
7. En el campo Prefix Length, especifique la longitud del prefijo IPv6 de una interfaz.
8. En la lista EUI64, seleccione Enable o Disable para el prefijo unicast de 64 bits especificado.
9. En el campo Valid Life Time, especifique el tiempo por prefijo del anuncio de router.

   Es el tiempo durante el que el prefijo se considera válido para la determinación on-link. El rango es de 0 a 4294967295.

10. En el campo Preferred Life Time, especifique el tiempo por prefijo del anuncio de router. Una dirección autoconfigurada generada a partir de este prefijo es preferida. El tiempo preferido debe estar en el rango de 0 a 4294967295.
11. En la lista Onlink Flag, seleccione Enable o Disable.

    Esto especifica si el prefijo seleccionado se puede usar para la determinación on-link. El valor predeterminado es Enable.

12. En la lista Autonomous Flag, seleccione Enable o Disable.

Esto especifica si el prefijo seleccionado se puede usar para la configuración autónoma de direcciones. El valor predeterminado es Enable.

13. Haga clic en el botón Add.
Se agrega la dirección IPv6 a la interfaz.
14. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

El campo Current State muestra el estado de la dirección IPv6. El estado es TENT si el enrutamiento está deshabilitado o falla DAD. El estado es Active si la interfaz está activa y DAD se completó correctamente.

Ver las estadísticas IPv6

Para ver las estadísticas de interfaz IPv6:

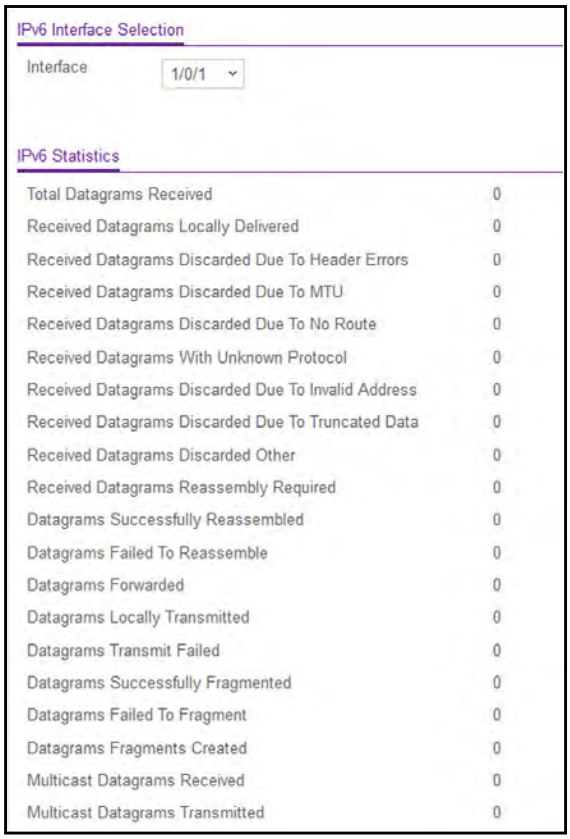
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Statistics.



5. En la lista Interface, seleccione la interfaz.

   Al cambiar la selección, la página se actualiza y todos los campos se actualizan para el puerto recién seleccionado.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información no configurable que se muestra.

Tabla 115. Estadísticas avanzadas de interfaz IPv6

Campo	Descripción
Total de datagramas recibidos	Número total de datagramas de entrada recibidos por la interfaz, incluidos los recibidos con errores.
Datagramas recibidos entregados localmente	Número total de datagramas entregados correctamente a protocolos de usuario IPv6 (incluido ICMP). Este contador aumenta en la interfaz a la que se dirigieron estos datagramas, que puede no ser la interfaz de entrada de algunos de ellos.
Datagramas recibidos descartados por errores de encabezado	Número de datagramas de entrada descartados por errores en sus encabezados IPv6, como versión no coincidente, otros errores de formato, número de saltos excedido, errores al procesar sus opciones IPv6, etc.
Datagramas recibidos descartados por MTU	Número de datagramas de entrada que no se pudieron reenviar porque su tamaño superaba la MTU del enlace de la interfaz de salida.

Tabla 115. IPv6 Advanced Interface Statistics (continuación)

Campo	Descripción
Datagramas recibidos descartados por falta de ruta	Número de datagramas de entrada descartados porque no se encontró ninguna ruta para transmitirlos a su destino
Datagramas recibidos con protocolo desconocido	Número de datagramas dirigidos localmente recibidos correctamente pero descartados por un protocolo desconocido o no admitido. Este contador aumenta en la interfaz a la que se dirigieron estos datagramas, que puede no ser la interfaz de entrada de algunos de ellos.
Datagramas recibidos descartados por dirección no válida	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 recibirse en esta entidad. Este recuento incluye direcciones no válidas (por ejemplo, ::0) y direcciones no admitidas (como direcciones con prefijos no asignados). Para las entidades que no son routers IPv6 y que, 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 que no presentaron problemas que impidieran continuar su procesamiento, pero que se descartaron por motivos como falta de espacio en el búfer. Este contador no incluye los datagramas descartados mientras esperaban el reensamblado.
Received Datagrams Reassembly Required	El número de fragmentos IPv6 recibidos que debían reensamblarse en esta interfaz. Este contador aumenta en la interfaz a la que se dirigieron estos fragmentos, que podría no ser la interfaz de entrada de algunos de los fragmentos.
Datagrams Successfully Reassembled	El número de datagramas IPv6 reensamblados correctamente. Este contador aumenta en la interfaz a la que se dirigieron estos datagramas, que podría no ser necesariamente la interfaz de entrada de algunos de los fragmentos.
Datagrams Failed To Reassemble	El número de fallas detectadas por el algoritmo de reensamblado IPv6 (por cualquier motivo: tiempo de espera agotado, errores, etc.). No es necesariamente un recuento de fragmentos IPv6 descartados, ya que algunos algoritmos (en particular el algoritmo de RFC 815) pueden perder la cuenta del número de fragmentos al combinarlos a medida que se reciben. Este contador aumenta en la interfaz a la que se dirigieron estos fragmentos, que podría no ser la interfaz de entrada de algunos de los fragmentos.
Datagrams Forwarded	El número de datagramas de salida que esta entidad recibió y reenvió a sus destinos finales. En las entidades que no actúan como routers IPv6, este contador incluye solo los paquetes enrutados en origen a través de esta entidad cuyo procesamiento de ruta de origen fue correcto. Para un datagrama reenviado correctamente, aumenta 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 Successfully Fragmented	El número de datagramas IPv6 que se fragmentaron en esta interfaz de salida.

Tabla 115. IPv6 Advanced Interface Statistics (continuación)

Campo	Descripción
Datagrams Failed To Fragment	El número de datagramas de salida que no se pudieron fragmentar en esta interfaz.
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 116. ICMPv6 Statistics

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 podría no ser la interfaz de entrada de los mensajes.
ICMPv6 Messages With Errors Received	El número de mensajes ICMP que la interfaz recibió pero determinó que tenían errores específicos de ICMP (sumas de verificación ICMP incorrectas, longitud incorrecta, etc.).
ICMPv6 Destination Unreachable Messages Received	El número de mensajes ICMP Destination Unreachable recibidos por la interfaz.
ICMPv6 Messages Prohibited Administratively Received	El número de mensajes ICMP destination unreachable/ communication administratively prohibited recibidos por la interfaz.
ICMPv6 Time Exceeded Messages Received	El número de mensajes ICMP Time Exceeded recibidos por la interfaz.
ICMPv6 Parameter Problem Messages Received	El número de mensajes ICMP Parameter Problem recibidos por la interfaz.
ICMPv6 Packet Too Big Messages Received	El número de mensajes ICMP Packet Too Big recibidos por la interfaz.
ICMPv6 Echo Request Messages Received	El número de mensajes ICMP Echo (request) recibidos por la interfaz.
ICMPv6 Echo Reply Messages Received	El número de mensajes ICMP Echo Reply recibidos por la interfaz.
ICMPv6 Router Solicit Messages Received	El número de mensajes ICMP Router Solicit recibidos por la interfaz.
ICMPv6 Router Advertisement Messages Received	El número de mensajes ICMP Router Advertisement recibidos por la interfaz.
ICMPv6 Neighbor Solicit Messages Received	El número de mensajes ICMP Neighbor Solicit recibidos por la interfaz.

Tabla 116. ICMPv6 Statistics (continuación)

Campo	Descripción
ICMPv6 Neighbor Advertisement Messages Received	El número de mensajes ICMP Neighbor Advertisement recibidos por la interfaz.
ICMPv6 Redirect Messages Received	El número de mensajes ICMPv6 Redirect recibidos por la interfaz.
ICMPv6 Group Membership Query Messages Received	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 Transmitted	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 debido a problemas detectados dentro de ICMP, como falta de búferes. Este valor no incluye los errores detectados fuera de la capa ICMP, como la imposibilidad de IPv6 de 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 interfaz.
ICMPv6 Messages Prohibited Administratively Transmitted	Número de mensajes ICMP Destination Unreachable/ Communication Administratively Prohibited enviados.
ICMPv6 Time Exceeded Messages Transmitted	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 Transmitted	El número de mensajes ICMP Packet Too Big enviados por la interfaz.
ICMPv6 Echo Request Messages Transmitted	El número de mensajes ICMP Echo (request) enviados por la interfaz.
ICMPv6 Echo Reply Messages Transmitted	El número de mensajes ICMP Echo Reply enviados por la interfaz.
ICMPv6 Router Solicit Messages Transmitted	El número de mensajes ICMP Neighbor Solicitation enviados por la interfaz.
ICMPv6 Router Advertisement Messages Transmitted	El número de mensajes ICMP Router Advertisement enviados por la interfaz.
ICMPv6 Neighbor Solicit Messages Transmitted	El número de mensajes ICMP Neighbor Solicitation enviados por la interfaz.
ICMPv6 Neighbor Advertisement Messages Transmitted	El número de mensajes ICMP Neighbor Advertisement enviados por la interfaz.

Tabla 116. ICMPv6 Statistics (continuación)

Campo	Descripción
ICMPv6 Redirect Messages Transmitted	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.

Ver la tabla de vecinos IPv6 y borrar los vecinos IPv6

Para ver la tabla de vecinos IPv6 y borrar los vecinos IPv6:

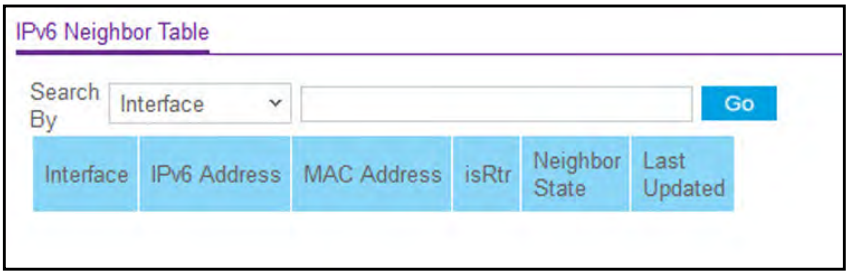
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Neighbor Table.



5. Use el campo Search By para buscar rutas IPv6 por IPv6 Address o Interface.
   - Para buscar por dirección IPv6, seleccione IPv6 Address en la lista Search By. Ingrese la dirección IPv6 hexadecimal de 128 bytes en grupos de cuatro dígitos separados por dos puntos, por ejemplo, 2001:231F:::1. Después, haga clic en el botón Go. Si la dirección existe, se muestra esa entrada. Se requiere una coincidencia exacta.

- Para buscar por interfaz, seleccione Interface en la lista Search By e ingrese el ID de interfaz con el formato unidad/ranura/puerto, por ejemplo, 2/1/1. Después, haga clic en el botón Go. Si la dirección existe, se muestra esa entrada.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh).

7. Para borrar los vecinos IPv6 de una interfaz seleccionada o de todas las interfaces, haga clic en el botón Clear.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 117. IPv6 Advanced Neighbor Table

Campo	Descripción
Interface	La interfaz cuya configuración se muestra en la fila actual de la tabla.
IPv6 Address	La dirección IPv6 del vecino o de la interfaz.
MAC Address	Especifica la dirección MAC asociada con una interfaz.
isRtr	Indica si el vecino es un router. Si el vecino es un router, el valor es True. Si el vecino no es un router, el valor es False.
Neighbor State	El estado de la entrada de la caché de vecinos. Los siguientes son los estados de las entradas dinámicas en la caché de descubrimiento de vecinos IPv6: • Incmp. Se está realizando la resolución de direcciones en 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 una confirmación positiva dentro de los últimos Reachable Time milisegundos de que la ruta de reenvío al vecino funcionaba correctamente. En el estado REACH, el dispositivo no realiza ninguna acción especial al enviar paquetes. • Stale. Transcurrieron más de ReachableTime milisegundos desde que se recibió la última confirmación positiva de que la ruta de reenvío funcionaba correctamente. En el estado STALE, el dispositivo no realiza ninguna acción hasta que se envía un paquete. • Delay. Transcurrieron más de ReachableTime milisegundos desde que se recibió la última confirmación positiva de que la ruta de reenvío funcionaba correctamente. Se envió un paquete dentro de los últimos DELAY_FIRST_PROBE_TIME segundos. Si no se recibe ninguna confirmación de accesibilidad dentro de DELAY_FIRST_PROBE_TIME segundos después de 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 accesibilidad reenviando mensajes de solicitud de vecino cada RetransTimer milisegundos hasta que se recibe una confirmación de accesibilidad.
Last Updated	Tiempo desde que se confirmó que la dirección es accesible.

Configurar una ruta estática IPv6

Configurar una ruta estática IPv6:

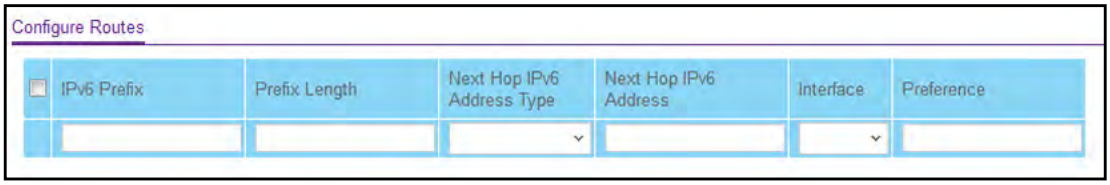
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Static Route Configuration.



5. En el campo IPv6 Prefix, especifique el prefijo IPv6 de la ruta configurada.
6. En el campo Prefix Length, especifique la longitud del prefijo IPv6 de la ruta configurada.

7. En la lista Next Hop IPv6 Address Type, seleccione una de las siguientes opciones:

   - Global IPv6 Address.
   - Link-Local IPv6 address. Si la dirección IPv6 del siguiente salto especificada es una dirección IPv6 link-local, especifique la interfaz para la dirección de siguiente salto IPv6 link-local.
   - Static-Reject. Seleccione Static-Reject para crear una ruta static-reject para un prefijo de destino. En ese caso, no se especifica ninguna dirección de siguiente salto.

8. Ingrese la Next Hop IPv6 Address para la ruta configurada.
9. Seleccione en la lista Interface, con el formato unidad/ranura/puerto, la dirección de siguiente salto IPv6 link-local.

Este campo solo está habilitado si se selecciona Link-Local.

10. Especifique la Preference de la ruta configurada.
11. Haga clic en el botón Add.

Se agrega la ruta.

Ver la tabla de rutas IPv6

Para ver la tabla de rutas IPv6:

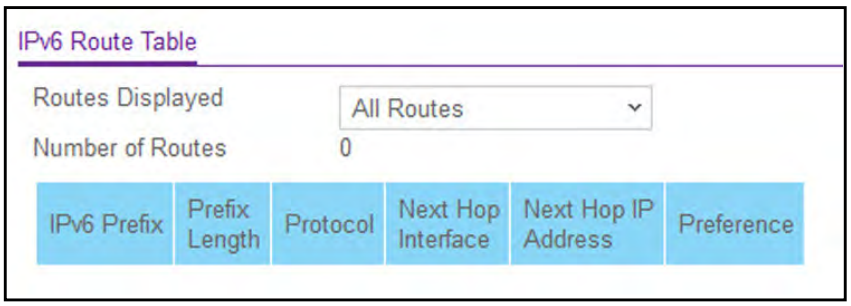
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Route Table.



5. En el campo Routes Displayed, seleccione qué rutas desea mostrar en la siguiente lista:
   - All Routes. Muestra todas las rutas IPv6 activas.
   - Best Routes Only. Muestra solo las mejores rutas activas.
   - Configured Routes Only. Muestra las rutas configuradas por el usuario.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información no configurable que se muestra.

Tabla 118. IPv6 Advanced Route Table

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.
Longitud del prefijo	Longitud del prefijo de la ruta activa.
Protocol	El tipo de protocolo de la ruta activa.
Interfaz del siguiente salto	Interfaz por la que la ruta está activa. Para una ruta de rechazo, el siguiente salto es una interfaz Null0.
Next Hop IP Address	La dirección IPv6 del siguiente salto de la ruta activa.
Preference	La preferencia de la ruta configurada.

Configurar las preferencias de rutas IPv6

Use esta página para configurar la preferencia predeterminada de cada protocolo. Estos valores son valores arbitrarios en el rango de 1 a 255 y son independientes 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 elige seleccionando la ruta con el valor de preferencia más bajo. Cuando hay varias rutas a un destino, los valores de preferencia se usan para determinar la ruta preferida. Si aún hay un empate, se elige la ruta con la mejor métrica. Para evitar problemas con métricas no coincidentes, debe configurar valores de preferencia diferentes para cada protocolo.

Configurar las preferencias de rutas IPv6:

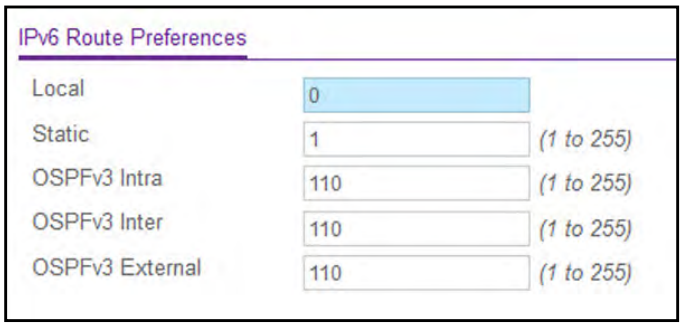
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Route Preference.



5. En el campo Static, especifique el valor de preferencia de rutas estáticas del router. El rango es de 1 a 255. El valor predeterminado es 1.
6. En el campo OSPFv3 Intra, especifique el valor de preferencia de rutas OSPFv3 intra del router. El rango es de 1 a 255. El valor predeterminado es 110.
7. En el campo OSPFv3 Inter, especifique el valor de preferencia de rutas OSPFv3 inter del router. El rango es de 1 a 255. El valor predeterminado es 110.

8. En el campo OSPFv3 External, especifique el valor de preferencia de rutas OSPFv3 externas del router.

   El rango es de 1 a 255. El valor predeterminado es 110.

9. Haga clic en el botón Apply.
La configuración se guarda.
El campo Local muestra la preferencia local.

Configurar túneles IPv6

Puede crear, configurar y eliminar túneles.

Para configurar un túnel IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 > Advanced > Tunnel Configuration.



5. En el campo Tunnel ID, seleccione un ID de la lista de ID de túnel disponibles.

6. En la lista Mode, seleccione un modo admitido:

- 6-in-4-configured
- 6-to-4

7. Seleccione el IPv6 Mode en la lista.
8. Habilite IPv6 en esta interfaz con la dirección IPv6.
Esta opción solo se puede configurar hasta que especifique una dirección IPv6 explícita.

9. En la lista IPv6 Unreachables, seleccione Enable o Disable.

Esto especifica el modo de envío de mensajes ICMPv6 Destination Unreachable en esta interfaz. Si selecciona Disable, esta interfaz no envía mensajes ICMPv6 de destino inalcanzable. De forma predeterminada, el modo de mensajes IPv6 de destino inalcanzable está habilitado.

10. En el campo IPv6 Address/Prefix Length, ingrese una dirección IPv6 configurada para la interfaz seleccionada.

La dirección debe ingresarse con el formato prefijo/longitud.

11. En la lista EUI64, seleccione Enable o Disable para el identificador único extendido de 64 bits (EUI-64).

    Para túneles 6to4, configure la dirección IPv6 con los primeros 48 bits con el formato 2002:tunnel-source-IPv4-address::/48.

12. Especifique la Source Address deseada para este túnel.
Este valor debe ingresarse en notación decimal con puntos.

13. Seleccione la Source Interface para este túnel.

La dirección asociada con la interfaz seleccionada se usa como dirección de origen.
14. Ingrese la Destination Address para este túnel en notación decimal con puntos.
15. Haga clic en el botón Add.
Se agrega el túnel.
16. 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.

Administrar VLAN

Puede configurar el software del switch para que algunos puertos admitan VLAN y otros puertos admitan enrutamiento. También puede configurar el software para que el tráfico de una VLAN se trate como si la VLAN fuera un puerto de router.

Cuando un puerto está habilitado para puenteo (predeterminado) 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 un puerto puede configurarse para pertenecer a más de una VLAN, el enrutamiento de VLAN puede estar habilitado para todas las VLAN del puerto 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. Esta sección muestra cómo configurar el switch NETGEAR para admitir el enrutamiento de VLAN. 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 es un puerto de router.

Usar el asistente de enrutamiento estático de VLAN

El asistente VLAN Static Routing Wizard crea una VLAN y le agrega los puertos seleccionados. El asistente le da la opción de agregar los puertos seleccionados como una agregación de enlaces (LAG). El asistente hace lo siguiente:

- Crea una VLAN y genera un nombre único para la VLAN.
- Agrega los puertos seleccionados a la VLAN recién creada y quita los puertos seleccionados de la VLAN predeterminada.
- Crea un LAG, agrega los puertos seleccionados a un LAG y, después, agrega el LAG a la VLAN recién creada.
- Habilita el etiquetado en los puertos seleccionados si el puerto está en otra VLAN. Deshabilita el etiquetado si un puerto seleccionado NO existe en otra VLAN.
- Excluye de la VLAN los puertos NO seleccionados.
- Habilita el enrutamiento en la VLAN con la dirección IP y la máscara de subred ingresadas.

Para usar el asistente VLAN Static Routing Wizard:

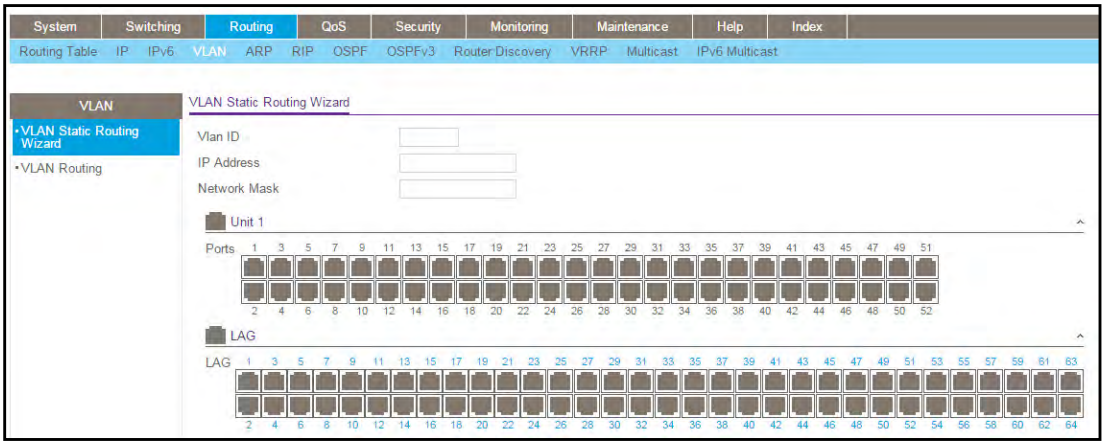
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> VLAN > VLAN Static Routing Wizard.



5. Use VLAN ID para especificar el identificador de VLAN (VID) asociado con esta VLAN. El ID de VLAN va de 1 a 4093.
6. Use Ports para mostrar los puertos físicos y LAG seleccionables (si los hay).

Los puertos seleccionados se agregan a la VLAN de enrutamiento. Cada puerto tiene tres modos:

- T (Tagged). Seleccione los puertos en los que todas las tramas transmitidas para esta VLAN van con etiqueta. Los puertos seleccionados se incluyen en la VLAN.
- U (Untagged). Seleccione los puertos en los que todas las tramas transmitidas para esta VLAN van sin etiqueta. Los puertos seleccionados se incluyen en la VLAN.
- BLANK(Autodetect). Seleccione los puertos que pueden registrarse dinámicamente en esta VLAN mediante GVRP. Esta opción tiene el efecto de excluir un puerto de la VLAN seleccionada.

7. Use la opción LAG Enabled para agregar los puertos seleccionados a la VLAN como un LAG. El valor predeterminado es No.
8. Use IP Address para definir la dirección IP de la interfaz VLAN.
9. Use Network Mask para definir la máscara de subred de la interfaz VLAN.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar el enrutamiento de VLAN

Para configurar el enrutamiento de VLAN:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> VLAN > VLAN Routing.



5. Seleccione el VLAN ID.
Este campo muestra los ID de todas las VLAN configuradas en este switch.
6. Use IP Address para ingresar la dirección IP que se configurará para la interfaz de enrutamiento de la VLAN.
7. Use Subnet Mask para ingresar la máscara de subred que se configurará para la interfaz de enrutamiento de la VLAN.

8. Haga clic en el botón Add.
Se agrega la interfaz de enrutamiento de VLAN para el ID de VLAN seleccionado.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 119. Configuración de enrutamiento VLAN

Campo	Descripción
Port	La interfaz asignada a la VLAN para el enrutamiento.
MAC Address	La dirección MAC asignada a la interfaz de enrutamiento VLAN

Configurar Address Resolution Protocol

Address Resolution Protocol (ARP) asocia una dirección MAC de capa 2 con una dirección IPv4 de capa 3. El software del switch ofrece configuración de ARP dinámica y manual. Con la configuración manual de ARP, puede agregar entradas estáticas a la tabla ARP.

ARP es una parte necesaria del Internet Protocol (IP) y se usa para traducir una dirección IP a una dirección de medio (MAC), definida por una red de área local (LAN) como Ethernet. Una estación que necesita enviar un paquete 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 cada estación de una red mantiene localmente. Las entradas de la caché ARP se aprenden examinando la información de origen de los campos de carga útil del paquete ARP, ya sea una solicitud o una respuesta ARP. Así, cuando se difunde una solicitud ARP a todas las estaciones de un segmento LAN o LAN virtual (VLAN), cada destinatario tiene la oportunidad de guardar la dirección IP y MAC del remitente en su caché ARP. La respuesta ARP, al ser unicast, normalmente solo la ve el solicitante, que guarda la información del remitente en su caché ARP. La información más reciente siempre reemplaza el contenido existente en la caché ARP.

El número de entradas ARP admitidas depende de la plataforma.

Los dispositivos pueden cambiar de lugar en una red, por lo que una dirección IP que en un momento estaba asociada a cierta dirección MAC ahora se encuentra con otra MAC, o desaparece de la red por completo (por ejemplo, porque se reconfiguró, se desconectó o se apagó). Esto genera información obsoleta en la caché ARP, a menos que las entradas se actualicen según la nueva información vista en la red, se refresquen periódicamente para comprobar si la dirección aún existe, o se eliminen de la caché si la entrada se identificó como remitente de un paquete ARP durante un intervalo de caducidad, que normalmente se especifica en la configuración.

Mostrar las entradas de la caché ARP

Use esta página para mostrar las entradas de la caché ARP. La tabla muestra las conexiones remotas que este switch ha visto más recientemente.

Para mostrar las entradas de la caché ARP:

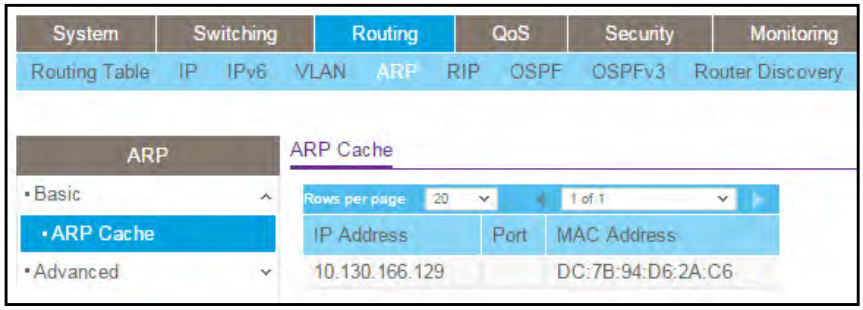
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> ARP > Basic > ARP Cache.



La página muestra la siguiente información:

- IP Address. Muestra la dirección IP asociada a 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 a la conexión.
- MAC Address. Muestra la dirección MAC unicast del dispositivo. La dirección consta de seis números hexadecimales de 2 dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40.

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 podría 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.

5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

Agregar una entrada a la tabla ARP

Puede agregar una entrada a la tabla de Address Resolution Protocol (ARP).

Para agregar una entrada a la tabla ARP:

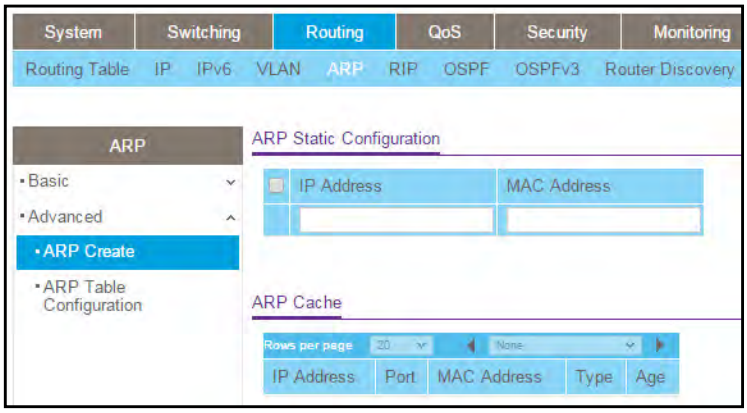
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> ARP > Advanced > ARP Create.



5. Use IP Address para introducir la dirección IP que desea agregar.

   Debe ser la dirección IP de un dispositivo en una subred conectada a una de las interfaces de enrutamiento existentes del switch.

6. Use MAC Address para especificar la dirección MAC unicast del dispositivo.

   Introduzca la dirección como seis números hexadecimales de 2 dígitos separados por dos puntos, por ejemplo, 00:06:29:32:81:40.

7. Haga clic en el botón Add.
La entrada ARP estática se agrega al switch.
8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
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 podría 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 la información no configurable que se muestra en la página.

Tabla 120. Caché ARP

Campo	Descripción
IP Address	La dirección IP. Debe ser la dirección IP de un dispositivo en una subred conectada a una de las interfaces de enrutamiento existentes del switch.
Port	La unidad/ranura/puerto asociado a la conexión.
MAC Address	La dirección MAC unicast del dispositivo. La dirección consta de seis números hexadecimales de dos dígitos separados por dos puntos, por ejemplo 00:06:29:32:81:40.
Type	El tipo de entrada ARP. Los valores posibles son los siguientes: • Local. Una entrada ARP asociada a 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 configurada por el usuario. • Dynamic. Una entrada ARP que aprendió el router.
Age	Tiempo transcurrido desde la última actualización de la entrada en la tabla ARP (en segundos).

Ver o configurar la tabla ARP

Puede cambiar los parámetros de configuración de la tabla de Address Resolution Protocol (ARP). También puede usar esta página para mostrar el contenido de la tabla.

Para configurar la tabla ARP:

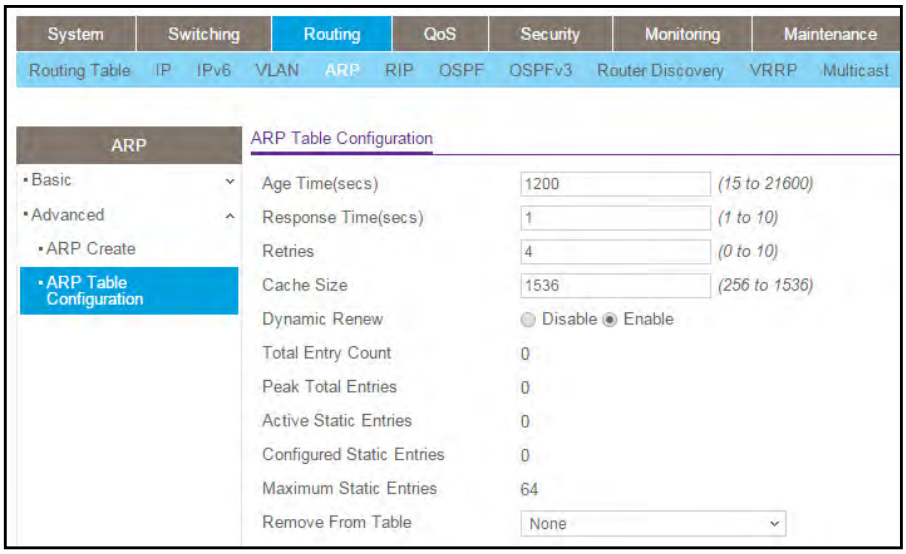
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> ARP > Advanced > ARP Table Configuration.



5. Use Age Time para introducir el tiempo, 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 de Age Time es 1200 segundos.

6. Use Response Time para introducir el tiempo, en segundos, que el dispositivo espera una respuesta ARP a una solicitud ARP que envía.

   El rango de este campo es de 1 a 10 segundos. El valor predeterminado es 1 segundo.

7. Use Retries para introducir el número máximo de reintentos de una solicitud ARP cuando no se recibe una respuesta ARP.

   El número incluye la solicitud ARP inicial. El rango de este campo es de 0 a 10. El valor predeterminado de Retries es 4.

8. Use Cache Size para especificar el número máximo de entradas permitidas en la tabla ARP.

   Este número incluye todas las entradas ARP estáticas y dinámicas. El rango de este campo es de 256 a 1536. El valor predeterminado de Cache Size es 1536.

9. Si se selecciona, la opción Dynamic Renew permite que el componente ARP intente renovar automáticamente las entradas ARP dinámicas cuando caducan.

La configuración predeterminada es Enable.
10. Use Remove from Table para eliminar ciertas entradas de la tabla ARP. Las opciones indican el tipo de entrada ARP que se eliminará:

- **All Dynamic Entries**
- **All Dynamic and Gateway Entries**
- Specific Dynamic/Gateway Entry. Esta opción permite al usuario especificar la dirección IP requerida.
- Specific Static Entry. Esta opción permite al usuario especificar la dirección IP requerida.
- None. Se selecciona si el usuario no desea eliminar ninguna entrada de la tabla ARP.

- Remove IP Address. Este campo solo se muestra si selecciona Specific Dynamic/Gateway Entry o Specific Static Entry en la lista Remove from Table. El campo Remove IP Address le permite introducir la dirección IP de la entrada que se eliminará de la tabla ARP.

11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 121. Configuración de la tabla ARP

Campo	Descripción
Total Entry Count	Número total de entradas en la tabla ARP.
Peak Total Entries	Valor más alto alcanzado por Total Entry Count. Este contador se reinicia cada vez que cambia el valor de Cache Size de la tabla ARP.
Active Static Entries	Número total de entradas estáticas activas en la tabla ARP.
Configured Static Entries	Número total de entradas estáticas configuradas en la tabla ARP.
Maximum Static Entries	Número máximo de entradas estáticas que se pueden definir.

Configurar RIP

Habilitar RIP

Para habilitar RIP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > RIP > Basic > RIP Configuration.



5. En el campo RIP Admin Mode, seleccione la opción Enable o Disable. Si selecciona Enable, RIP se activa en el switch. El valor predeterminado es Enable.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar los ajustes de RIP

Para configurar los ajustes avanzados de RIP:

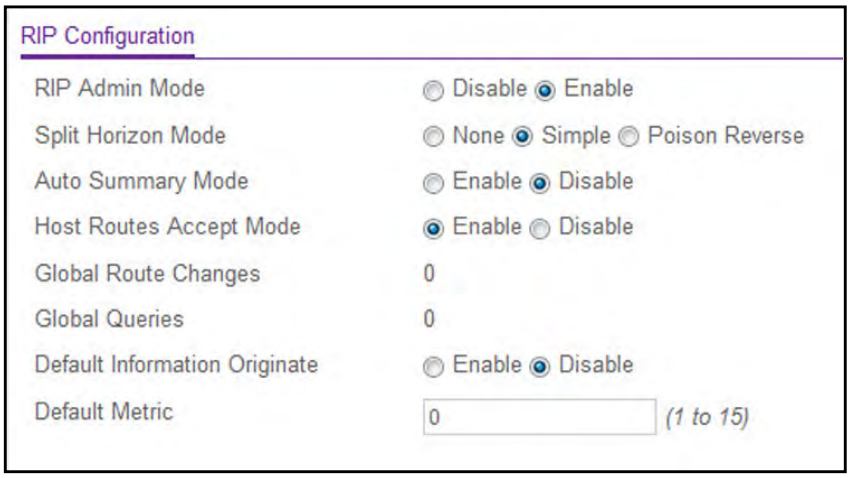
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > RIP > Advanced > RIP Configuration.



5. Seleccione el botón de opción Disable o Enable de RIP Admin Mode. Si selecciona Enable, RIP se activa en el switch. De forma predeterminada, RIP está habilitado.

6. Seleccione un botón de opción de Split Horizon Mode:

- None. No se realiza ningún procesamiento especial en este caso.
- Simple. Una ruta no se incluye en las actualizaciones enviadas al router del que se aprendió. El valor predeterminado es Simple.
- Poison Reverse. Una ruta se incluye en las actualizaciones enviadas al router del que se aprendió, pero la métrica se establece en infinito.

El horizonte dividido (split horizon) es una técnica para evitar problemas causados por incluir rutas en actualizaciones enviadas al router del que se aprendió originalmente la ruta

7. En el campo Auto Summary Mode, seleccione la opción Enable o Disable.

Si selecciona Enable, los grupos de rutas adyacentes se resumen en entradas únicas para reducir el número total de entradas. El valor predeterminado es Disable.

8. En el campo Host Routes Accept Mode, seleccione la opción Enable o Disable.

Si selecciona Enable, el router acepta rutas de host. El valor predeterminado es Enable.

9. En el campo Default Information Originate, habilite o deshabilite el anuncio de la ruta predeterminada.

10. En el campo Default Metric, especifique un valor predeterminado para la métrica de las rutas redistribuidas.

Este campo muestra la métrica predeterminada si ya se estableció, o 0 si no se configuró antes. Los valores válidos son de 1 a 15.

11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 122. Configuración avanzada de RIP

Campo	Descripción
Global Route Changes	El número de cambios de ruta que RIP realizó en la base de datos de rutas IP. No incluye la actualización de la antigüedad de una ruta.
Global Queries	El número de respuestas enviadas a consultas RIP de otros sistemas.

Configurar los ajustes avanzados de interfaces RIP

Para configurar los ajustes avanzados de interfaces RIP:

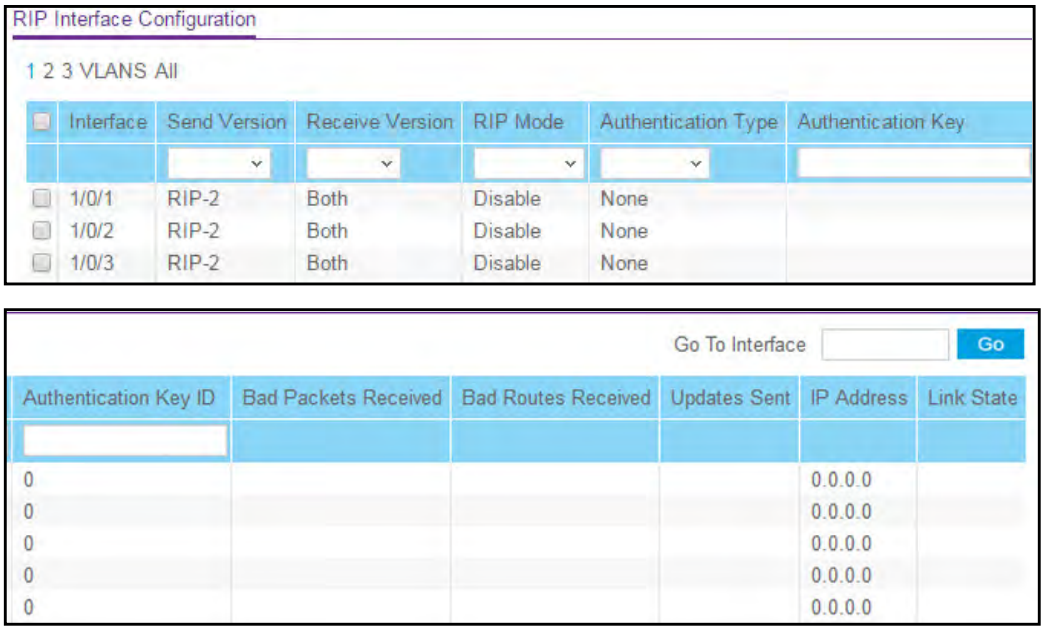
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > RIP > Advanced > Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.
6. En la lista Send Version, seleccione la versión de los paquetes de control RIP que enviará la interfaz.

   El valor es uno de los siguientes:
   - None. No se envían paquetes de control RIP.
   - RIP-1. Envía paquetes con formato RIP versión 1 mediante broadcast.
   - RIP-1c. Modo de compatibilidad con RIP versión 1. Envía paquetes con formato RIP versión 2 mediante broadcast.
   - RIP-2. Envía paquetes RIP versión 2 mediante multicast. El valor predeterminado es RIP-2.
7. En la lista Receive Version, seleccione qué paquetes de control RIP acepta la interfaz. El valor es uno de los siguientes:
   - RIP-1. Acepta solo paquetes con formato RIP versión 1.
   - RIP-2. Acepta solo paquetes con formato RIP versión 2.
   - Both. Acepta paquetes en cualquiera de los dos formatos. El valor predeterminado es Both.
   - None. No se aceptan paquetes de control RIP.
8. Seleccione Enable o Disable en la lista RIP Mode.

   Antes de habilitar RIP versión 1 o versión 1c en una interfaz, primero debe habilitar el modo de broadcast dirigido a la red en la interfaz correspondiente. El valor predeterminado es Disable.

9. Seleccione el tipo de autenticación en la lista Authentication Type.

Los tipos son los siguientes:

- None. Es el estado inicial de la interfaz. Si selecciona esta opción, no se ejecuta ningún protocolo de autenticación.
- Simple. Si selecciona Simple, se le pide introducir una clave de autenticación. Esta clave se incluye, sin cifrar, en el encabezado RIP de todos los paquetes enviados a la red. Todos los routers de la red deben configurarse con la misma clave.
- Encrypt. Si selecciona Encrypt, se le pide introducir una clave y un ID de autenticación. El cifrado usa el algoritmo MD5 Message-Digest. Todos los routers de la red deben configurarse con la misma clave e ID.

10. Introduzca la RIP Authentication Key de la interfaz especificada.

Si seleccionó el tipo de autenticación None, no se le pide una clave. Si seleccionó Simple o Encrypt, la clave puede tener hasta 16 octetos. El valor de la clave solo se muestra si inició sesión con privilegios de lectura/escritura.

11. Haga clic en el botón Apply.

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 123. Configuración avanzada de interfaces 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 realmente en esta interfaz. No incluye explícitamente las actualizaciones completas enviadas con información nueva.
IP Address	La dirección IP de la interfaz del router.
Link State	Indica si la interfaz RIP está activa o inactiva.

Administrar la redistribución de rutas

Use esta página para configurar los parámetros de redistribución de rutas RIP. Los valores permitidos de cada campo se muestran junto al campo. Si se introduce un valor no válido, se muestra un mensaje de alerta con la lista de todos los valores válidos.

Para configurar los ajustes avanzados de redistribución de rutas RIP:

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

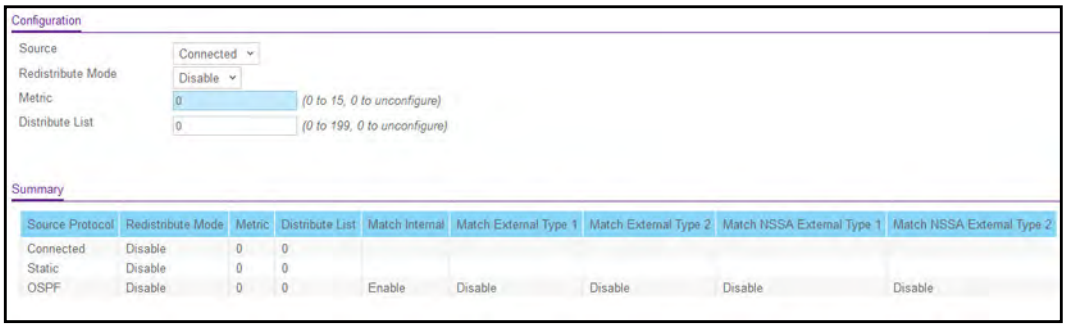
Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > RIP > Advanced > Route Redistribution.



La lista Source solo contiene 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.

5. En la lista Source, seleccione un valor. Los valores válidos son los siguientes:

- Connected
- Static
- OSPF

6. En la lista Redistribute Mode, habilite o deshabilite el modo de redistribución de RIP. El valor predeterminado es Disable.
7. Introduzca la métrica (Metric) de las rutas redistribuidas para la ruta de origen indicada. Los valores válidos son de 0 a 15; 0 significa sin configurar.

8. Use el campo Distribute List para establecer la lista de acceso que filtra las rutas que redistribuirá el protocolo de destino.

Solo se redistribuyen las rutas permitidas. Si este comando hace referencia a una lista de acceso inexistente, se permiten todas las rutas. Los valores válidos de los ID de lista de acceso son de 0 a 199. Cuando se usa para filtrar rutas, los únicos campos de una lista de acceso que se usan son los siguientes:

- Dirección IP de origen y máscara de red
- Dirección IP de destino y máscara de red
- Acción (permitir o denegar)

Todos los demás campos (como Source y Destination Port, Precedence, 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, que 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 y máscara de red de destino (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, que indica qué bits de la máscara de destino de la ruta son significativos para el filtrado.

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

La siguiente tabla describe los datos no configurables de RIP Route Redistribution que se muestran.

Tabla 124. Resumen de redistribución de rutas RIP

Campo	Descripción
Source Protocol	La ruta de origen que redistribuirá RIP. Los valores válidos son los siguientes: • Connected • Static • OSPF
Redistribute Mode	El modo de redistribución de rutas de un protocolo de origen específico. De forma predeterminada está deshabilitado.
Metric	La métrica de las rutas redistribuidas para la ruta de origen indicada. El campo muestra 0 cuando 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 cuando no está configurada.
La siguiente lista de rutas redistribuidas es válida cuando se selecciona OSPF como origen. La lista puede incluir uno o más de los siguientes:	
Match Internal	Establece que se redistribuyan las rutas OSPF internas.
Match External Type 1	Establece que se redistribuyan las rutas OSPF externas de tipo 1.
Match External Type 2	Establece que se redistribuyan las rutas OSPF externas de tipo 2.
Match NSSA External Type 1	Establece que se redistribuyan las rutas OSPF NSSA externas de tipo 1.
Match NSSA External Type 2	Establece que se redistribuyan las rutas OSPF NSSA externas de tipo 2.

Configurar el descubrimiento de routers

Para configurar el descubrimiento de routers:

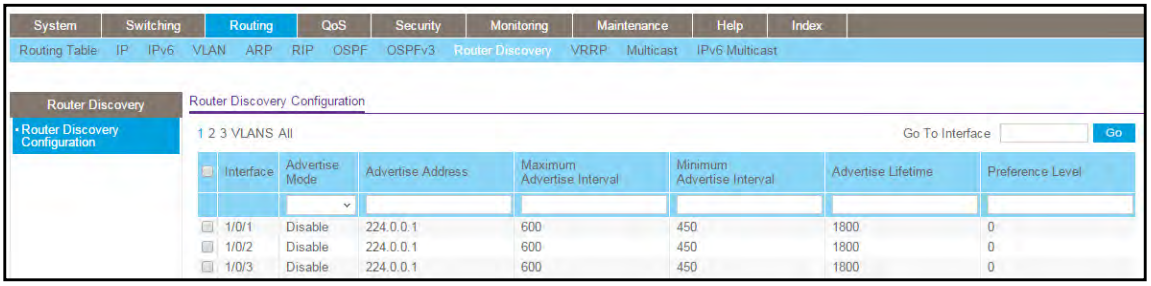
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Router Discovery > Router Discovery Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.

6. Use Advertise Mode para seleccionar Enable o Disable.

   Si selecciona Enable, se transmiten anuncios de router desde la interfaz seleccionada.

7. Use Advertise Address para seleccionar Enable o Disable.

   Si selecciona Enable, se transmiten anuncios de router desde la interfaz seleccionada.

8. Use Maximum Advertise Interval para introducir el tiempo máximo (en segundos) permitido entre anuncios de router enviados desde la interfaz.
9. Use Minimum Advertise Interval para introducir el tiempo mínimo (en segundos) permitido entre anuncios de router enviados desde la interfaz.

   El valor debe estar en el rango de 3 a 1800. El valor predeterminado es 450.000000.

10. Use Advertise Lifetime para introducir el valor (en segundos) del campo de vida útil en los anuncios de router enviados desde la interfaz.

Es el tiempo máximo durante el cual los hosts consideran las direcciones anunciadas como direcciones de router válidas.

11. Use Preference Level para especificar el nivel de preferencia del router como router predeterminado respecto a otros routers de la misma subred.

Se prefieren las direcciones con número más alto. Debe introducir un número entero.
12. Haga clic en el botón Apply.
La configuración se guarda.

Configurar Virtual Router Redundancy Protocol

Configurar los ajustes globales de VRRP

Para configurar los ajustes globales de VRRP:

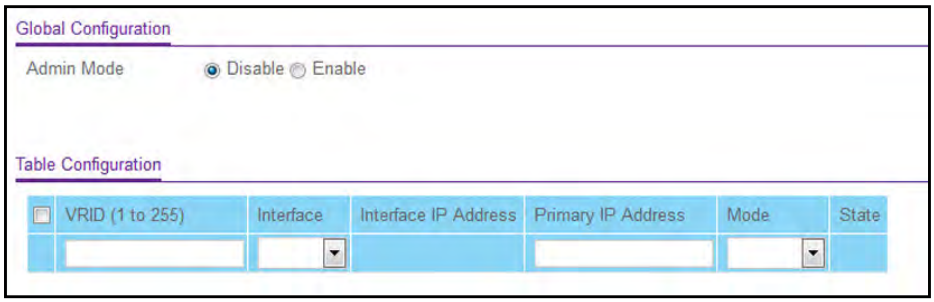
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > VRRP > Basic > VRRP Configuration.



5. En el campo Global Configuration Admin Mode, establezca el estado administrativo de VRRP en el router seleccionando el botón de opción Enable o Disable.

De forma predeterminada, VRRP está deshabilitado.
6. Seleccione el VRID.

El campo VRID solo se puede configurar si está creando un router virtual nuevo. Los valores válidos son de 1 a 255.
7. Seleccione la unidad/ranura/puerto del nuevo router virtual en el menú Interface.
8. En el campo Primary IP Address, introduzca la dirección IP principal del router virtual.
9. En el menú Mode, seleccione el modo Active o Inactive del nuevo router virtual.
10. Haga clic en el botón Add.
El router virtual se agrega a la configuración del switch.
11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 125. Configuración global de VRRP

Campo	Descripción
Interface IP Address	Indica la dirección IP asociada a la interfaz seleccionada.
State	El estado actual del router virtual. Los valores posibles son los siguientes: • Initialize • Master • Backup

Configurar los ajustes avanzados de VRRP

Para configurar los ajustes globales avanzados de VRRP.

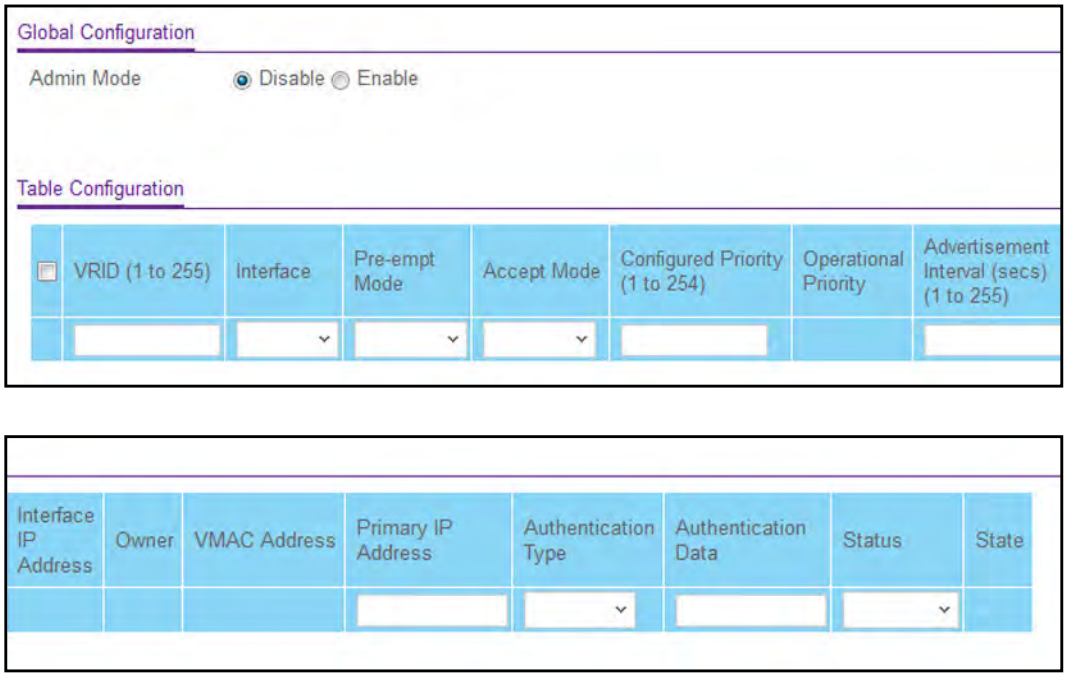
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > VRRP > Advanced > VRRP Configuration.



5. En el campo Global Configuration Admin Mode, establezca el estado administrativo de VRRP en el router seleccionando el botón de opción Enable o Disable.

De forma predeterminada, VRRP está deshabilitado.
6. Seleccione el VRID.
El campo VRID solo se puede configurar si está creando un router virtual nuevo. Los valores válidos son de 1 a 255.
7. Seleccione la unidad/ranura/puerto del nuevo router virtual en el menú Interface.
8. En el campo Pre-empt Mode, seleccione la opción Enable o Disable.

Si selecciona Enable, un router de respaldo reemplaza al router maestro si tiene una prioridad mayor que la del router virtual maestro, siempre que el maestro no sea el propietario de la dirección IP del router virtual. El valor predeterminado es Enable.

9. En el campo Accept Mode, seleccione la opción Enable o Disable.

Si selecciona Enable, el maestro VRRP acepta todo tipo de paquetes de datos dirigidos a las direcciones IP asociadas al router virtual. Si selecciona Disable, el maestro VRRP descarta todo tipo de paquetes de datos dirigidos a las direcciones IP asociadas al router virtual, si no es el propietario de la dirección IP. El valor predeterminado es Disable.

10. En el campo Configured Priority, introduzca la prioridad que usará el router VRRP en la elección del router virtual maestro.

Los valores válidos son de 1 a 254. Si la dirección IP virtual es igual a la dirección IP de la interfaz, la prioridad se establece en 254, sin importar lo que introduzca.

11. En el campo Advertisement Interval, introduzca el tiempo, en segundos, entre las transmisiones de paquetes de anuncio de este router virtual.

Introduzca un número de 1 a 255. El valor predeterminado es 1 segundo.

12. En el campo Primary IP Address, introduzca la dirección IP asociada al router virtual.

El valor predeterminado es 0.0.0.0.
13. En el menú Authentication Type, seleccione el tipo de autenticación del router virtual. Las opciones son las siguientes:

- 0-None. No se realiza autenticación. El valor predeterminado es None.
- 1-Simple. La autenticación se realiza con una contraseña de texto.

14. En el menú Status, seleccione la opción Active o Inactive para iniciar o detener el funcionamiento del router virtual.

El valor predeterminado es inactive.
15. Haga clic en el botón Add.
El router virtual se agrega a la configuración del switch.
16. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 126. Configuración global avanzada de VRRP

Campo	Descripción
Operational Priority	Indica la prioridad que se usará en el proceso de elección del router virtual maestro. Los valores más altos implican mayor prioridad. • El router maestro envía una prioridad de 0 para indicar que este router dejó de participar en VRRP y que un router virtual de respaldo pasa a ser el nuevo maestro. • La prioridad 255 se usa para el router propietario de las direcciones IP asociadas.
Interface IP Address	Indica la dirección IP asociada a la interfaz seleccionada.
Owner	Se establece en True si la dirección IP virtual y la dirección IP de la interfaz son iguales; de lo contrario, se establece en False. Si este parámetro es True, el router virtual es el propietario de la dirección IP virtual y siempre gana la elección de router maestro cuando está activo.
VMAC Address	La dirección MAC virtual asociada al router virtual, compuesta por un identificador único de organización de 24 bits, la constante de 16 bits que identifica el bloque de direcciones VRRP y el VRID de 8 bits.
State	El estado actual del router virtual. Los valores posibles son los siguientes: • Initialize • Master • Backup

Configurar una dirección IP secundaria de VRRP avanzada

Para configurar la dirección IP secundaria de VRRP avanzada:

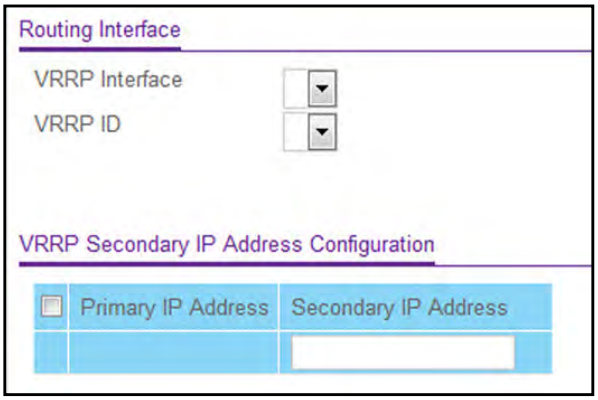
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > VRRP > Advanced > VRRP Secondary IP Address Configuration.



5. En los menús VRRP Interface y VRRP ID, seleccione un router virtual.
Los routers virtuales se muestran por número de interfaz e ID de VRRP.
6. En el campo Secondary IP Address, introduzca la dirección IP de la interfaz.

   Esta dirección debe pertenecer a una de las subredes configuradas actualmente en la interfaz. Este valor es de solo lectura una vez configurado.

7. Haga clic en el botón Add.
La dirección IP secundaria se agrega a la interfaz VRRP seleccionada.
8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
El campo Primary IP Address muestra la dirección IP principal del router virtual.

Configurar una interfaz de seguimiento VRRP avanzada

Para configurar una interfaz de seguimiento VRRP avanzada:

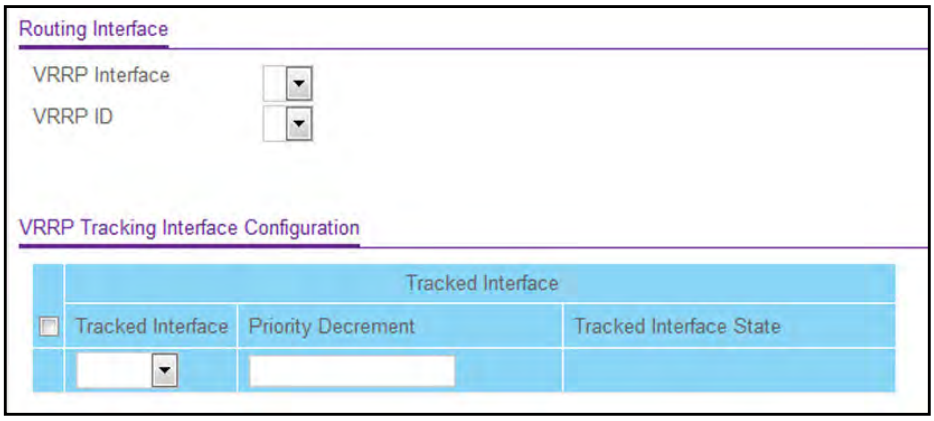
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > VRRP > Advanced > VRRP Tracking Configuration.

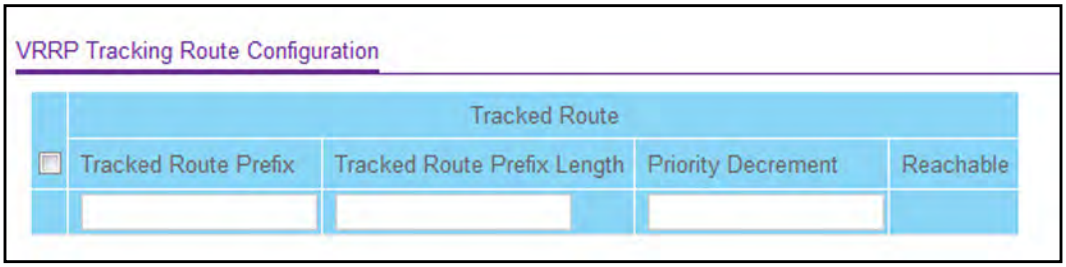


5. En los menús VRRP Interface y VRRP ID, seleccione un router virtual. Los routers virtuales se muestran por número de interfaz e ID de VRRP.
6. En el menú Tracked Interface, seleccione una interfaz de enrutamiento.

   El menú muestra todas las interfaces de enrutamiento que aún no tienen seguimiento para el ID de VRRP y la configuración de interfaz. El menú no muestra las interfaces loopback ni los túneles, que no pueden tener seguimiento.

7. En el campo Priority Decrement, introduzca el valor de reducción de prioridad para la interfaz con seguimiento. El rango válido es de 1 a 254. El valor predeterminado es 10.

   El campo no configurable Tracked Interface State muestra el estado de la interfaz con seguimiento.



8. En el campo Tracked Route Prefix, introduzca el prefijo de la ruta.
9. En el campo Tracked Route Prefix Length, introduzca la longitud del prefijo de la ruta.
10. En el campo Priority Decrement, introduzca el valor de reducción de prioridad para la ruta. El rango válido es de 1 a 254. El valor predeterminado es 10.
El campo no configurable Reachable muestra la accesibilidad de la ruta con seguimiento.
11. Haga clic en el botón Add.
La interfaz o ruta con seguimiento se agrega al VRRP.
12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 127. Configuración avanzada de seguimiento VRRP

Campo	Descripción
Tracked Interface State	El estado de la interfaz con seguimiento.
Reachable	La accesibilidad de la ruta con seguimiento.

Ver estadísticas avanzadas de VRRP

Para ver las estadísticas avanzadas de VRRP:

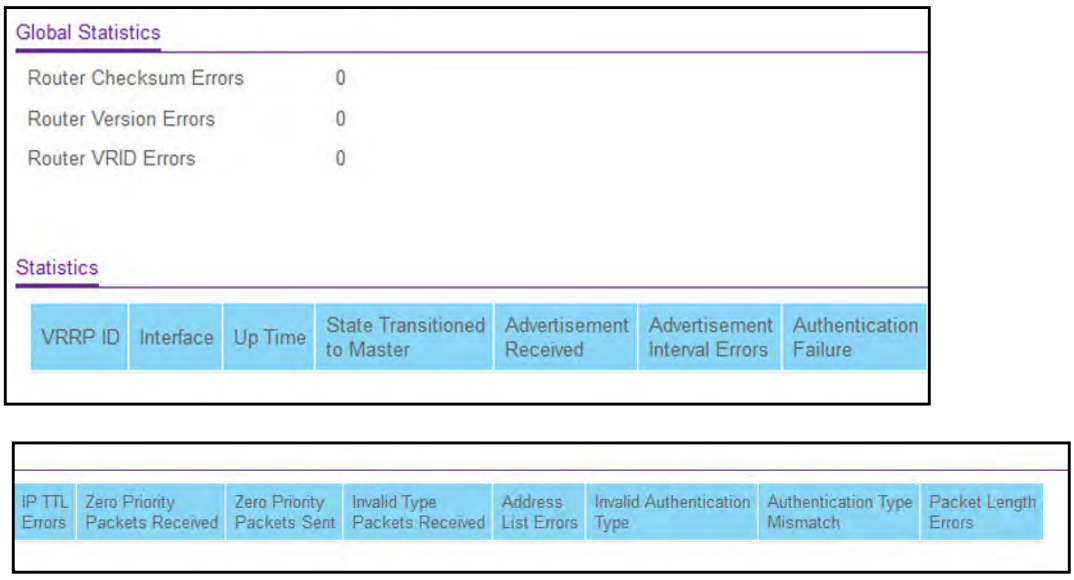
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > VRRP > Advanced > VRRP Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 128. Estadísticas avanzadas de VRRP

Campo	Descripción
Estadísticas globales	
Router Checksum Errors	El número total de paquetes VRRP recibidos con un valor de checksum VRRP no válido.
Router Version Errors	El número total de paquetes VRRP recibidos con un número de versión desconocido o no admitido.
Router VRID Errors	El número total de paquetes VRRP recibidos con un VRID no válido para este router virtual.
Estadísticas	
VRRP ID	El VRID del router virtual seleccionado.
Interface	La unidad/ranura/puerto del router virtual seleccionado.
Up Time	El tiempo, en días, horas, minutos y segundos, transcurrido desde que el router virtual pasó al estado inicializado.
State Transitioned to Master	El número total de veces que el estado de este router virtual pasó a Master.
Advertisement Received	El número total de anuncios VRRP recibidos por este router virtual.
Advertisement Interval Errors	El número total de paquetes de anuncio VRRP recibidos cuyo intervalo de anuncio era distinto del configurado para el router virtual local.

Tabla 128. Estadísticas avanzadas de VRRP (continuación)

Campo	Descripción
Authentication Failure	El número total de paquetes VRRP recibidos que no superaron la verificación de autenticación.
IP TTL Errors	El número total de paquetes VRRP recibidos por el router virtual con un IP Time-To-Live (TTL) distinto de 255.
Zero Priority Packets Received	El número total de paquetes VRRP recibidos por el router virtual con prioridad 0.
Zero Priority Packets Sent	El número total de paquetes VRRP enviados por el router virtual con prioridad 0.
Invalid Type Packets Received	El número de paquetes VRRP recibidos por el router virtual con un valor no válido en el campo Type.
Address List Errors	El número total de paquetes recibidos cuya lista de direcciones no coincide con la lista configurada localmente para el router virtual.
Invalid Authentication Type	El número total de paquetes recibidos con un tipo de autenticación desconocido.
Authentication Type Mismatch	El número total de paquetes recibidos con un tipo de autenticación distinto del método de autenticación configurado localmente.
Packet Length Errors	El número total de paquetes recibidos con una longitud menor que la longitud del encabezado VRRP.

6

6Configurar OSPF y OSPFv3

Este capítulo trata los siguientes temas:

- Configurar OSPF
- Configurar OSPFv3

Configurar OSPF

Configurar los ajustes básicos de OSPF

Para configurar los ajustes básicos de OSPF:

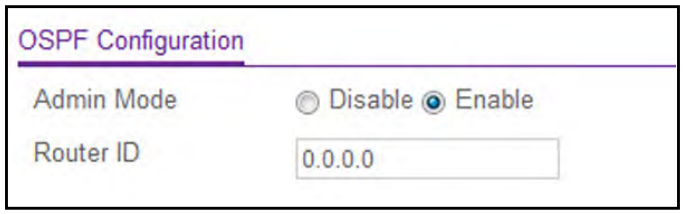
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Basic > OSPF Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Si selecciona Enable, OSPF se activa en el switch. De forma predeterminada, OSPF está habilitado. Debe configurar un ID de router antes de que OSPF pueda funcionar. Use la página IP Configuration para configurar un ID de router o ejecute el comando de CLI config router id. Para más información, consulte Configurar los ajustes IP de enrutamiento en la página 307.

   El campo Router ID muestra el entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS).

   Para cambiar el ID de router, primero debe deshabilitar OSPF. Después de establecer el nuevo ID de router, debe volver a habilitar OSPF para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar los ajustes de anuncio de ruta predeterminada de OSPF

Para configurar los ajustes de anuncio de ruta predeterminada:

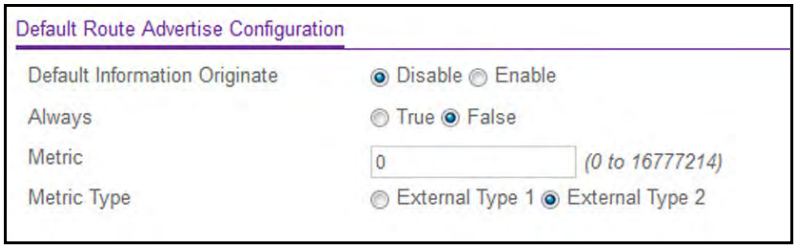
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

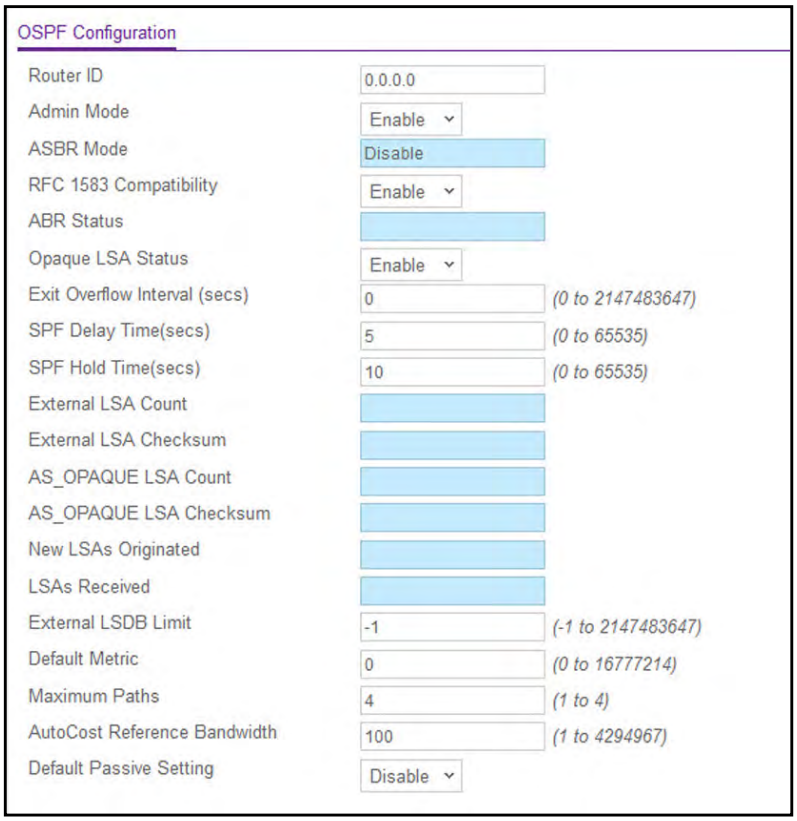
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing > OSPF > Advanced > OSPF Configuration.**





5. En el campo Default Information Originate, seleccione la opción Enable o Disable.

Si selecciona Enable, OSPF origina un LSA externo que anuncia una ruta predeterminada (0.0.0.0/0.0.0.0). Default Information Originate está deshabilitado de forma predeterminada.

6. En el campo Always, seleccione True o False.

Si Default Information Originate está habilitado pero la opción Always es False, OSPF origina una ruta predeterminada solo si ya existe una ruta predeterminada en la tabla de enrutamiento del router.

Establezca Always en True para forzar que OSPF origine una ruta predeterminada aunque ya exista o no una ruta predeterminada. El valor predeterminado es False.

7. En el campo Metric, especifique la métrica de la ruta predeterminada.
Los valores válidos van de 0 a 16777214. El valor predeterminado es 0.
8. En el campo Metric Type, seleccione el tipo de métrica OSPF de la ruta predeterminada.

Se admiten dos tipos: External Type 1 y External Type 2. El valor predeterminado es External Type 2.

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

Configurar los ajustes de OSPF

Para configurar los ajustes de OSPF:

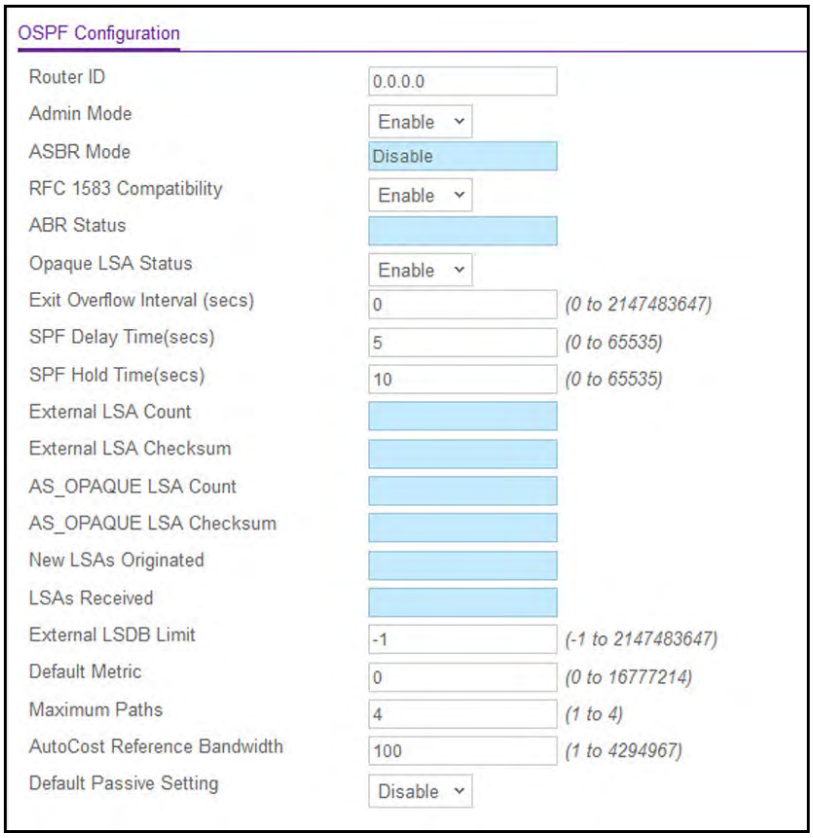
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > OSPF Configuration.



5. En el campo Router ID, introduzca el entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS).

   Para cambiar el ID de router, primero debe deshabilitar OSPF. Después de establecer el nuevo ID de router, debe volver a habilitar OSPF para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.

6. En el campo Admin Mode, seleccione Enable o Disable.

   Si selecciona Enable, OSPF se activa en el switch. El valor predeterminado es Enable. Debe configurar un ID de router antes de que OSPF pueda funcionar. Para más información, consulte Configurar los ajustes IP de enrutamiento en la página 307.

7. En el campo RFC 1583 Compatibility, seleccione Enable o Disable.

   Esto especifica las reglas de preferencia que se usan al elegir entre varios AS-external-LSA que anuncian el mismo destino. Si selecciona Enable, las reglas de preferencia son las definidas en la sección 16.4.1 del estándar OSPF-2 (RFC 2328), que evita bucles de enrutamiento cuando los AS-external-LSA del mismo destino se originan en áreas distintas. El valor predeterminado es Enable. Todos los routers del dominio OSPF deben configurarse igual. Si todos los routers OSPF pueden funcionar según RFC 2328, RFC 1583 Compatibility debe estar deshabilitado.

8. Establezca Opaque LSA Status en Enable si OSPF almacenará e inundará LSA opacos. Un LSA opaco se usa para inundar información definida por el usuario dentro de un dominio de routers OSPF.

9. Cuando el número de LSA externos no predeterminados supera un límite configurado, el router entra en estado de desbordamiento según lo definido en RFC 1765.

   Use el campo Exit Overflow Interval para especificar cuántos segundos debe esperar OSPF antes de intentar salir del estado de desbordamiento. En este estado, OSPF no puede originar LSA externos no predeterminados. Si Exit Overflow Interval es 0, OSPF no sale del estado de desbordamiento hasta que se deshabilita y se vuelve a habilitar. El rango es de 0 a 2,147,483,647 segundos. El valor predeterminado es 0.

10. Configure SPF Delay Time.

   Es el número de segundos desde que OSPF recibe un cambio de topología hasta el inicio del siguiente cálculo SPF. Delay Time es un entero de 0 a 65535 segundos. El valor predeterminado es 5 segundos. Un valor de 0 significa que no hay retraso; es decir, el cálculo SPF se inicia al producirse un cambio de topología.

11. Configure SPF Hold Time.

   Es el tiempo mínimo en segundos entre dos cálculos SPF consecutivos. El rango es de 0 a 65,535 segundos. El valor predeterminado es 10 segundos. Un valor de 0 significa que no hay retraso; es decir, pueden realizarse dos cálculos SPF, uno inmediatamente después del otro.

12. Use el campo External LSDB Limit para establecer el límite de LSDB externa de OSPF.

   Si el valor es –1, no hay límite. Cuando el número de AS-external-LSA no predeterminados en la base de datos de estado de enlace de un router alcanza el límite de LSDB externa, el router entra en estado de desbordamiento. El router nunca mantiene más AS-external-LSA no predeterminados que el límite de LSDB externa en la base de datos. El límite de LSDB externa debe establecerse de forma idéntica en todos los
   routers conectados al backbone OSPF y/o a cualquier área OSPF normal. El rango del campo External LSDB Limit es de –1 a 2147483647. El valor predeterminado es –1.

13. Use el campo Default Metric para establecer una métrica predeterminada para las rutas redistribuidas.

   Este campo está en blanco si no se configuró una métrica predeterminada. El rango de valores válidos es de 1 a 16777214. El valor predeterminado es 0.

14. Use el campo Maximum Paths para establecer el número de rutas que OSPF puede informar para un destino determinado.

El rango de valores válidos es de 1 a 16. El valor predeterminado es 4.
15. Configure AutoCost Reference Bandwidth para controlar cómo calcula OSPF el costo del enlace.

   Especifique el ancho de banda de referencia en megabits por segundo. Salvo que se configure un costo de enlace, este se calcula dividiendo el ancho de banda de referencia entre el ancho de banda de la interfaz. El rango es de 1 a 4294967. El valor predeterminado es 100.

16. En el campo Default Passive Setting, seleccione Enable o Disable en la lista para configurar el ajuste global de modo pasivo de todas las interfaces OSPF.

   Configurar este campo sobrescribe cualquier ajuste de modo pasivo a nivel de interfaz. OSPF no forma adyacencias en interfaces pasivas, pero sí anuncia las redes conectadas como redes stub. El valor predeterminado es Disabled.

17. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 129. Configuración de OSPF

Campo	Descripción
ASBR Mode	El router es un router de borde de sistema autónomo si está configurado para redistribuir rutas de otro protocolo, o si está configurado para originar un LSA externo que anuncia la ruta predeterminada.
ABR Status	El router es un router de borde de sistema autónomo si está configurado para redistribuir rutas de otro protocolo, o si está configurado para originar un LSA externo que anuncia la ruta predeterminada.
External LSA Count	El número de LSA (anuncios de estado de enlace) externos (LS tipo 5) en la base de datos de estado de enlace.
External LSA Checksum	La suma de los checksums LS de los LSA externos (anuncios de estado de enlace) contenidos en la base de datos de estado de enlace. Esta suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar las bases de datos de estado de enlace de dos routers. Este valor está en hexadecimal.
AS_OPAQUE LSA Count	El número de LSA opacos con alcance de inundación en todo el dominio.
AS_OPAQUE LSA Checksum	La suma de los checksums LS de los LSA opacos con alcance de inundación en todo el dominio. Esta suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar las bases de datos de estado de enlace de dos routers. Este valor está en hexadecimal.
New LSAs Originated	En cualquier área OSPF, un router origina varios LSA. Cada router origina un router-LSA. Si el router también es el router designado de alguna de las redes del área, origina LSA de red para esas redes. Este valor representa el número de LSA originados por este router.
LSAs Received	El número de LSA (anuncios de estado de enlace) recibidos que se determinó que eran instancias nuevas. Este número no incluye instancias más nuevas de LSA autooriginados.

Configurar el ID de área común de OSPF

Para agregar o eliminar un ID de área:

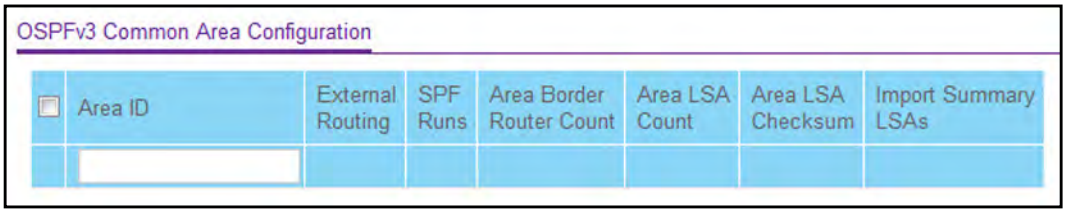
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Common Area Configuration.



5. Introduzca el OSPF Area ID.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

6. Realice una de las siguientes acciones:

- Haga clic en el botón Add.

  Se agrega el ID de área.

- Haga clic en el botón Delete.

  Se elimina el ID de área.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 130. Configuración de área común de OSPF

Campo	Descripción
External Routing	Definición de las capacidades del router para el área, incluido si los AS-external-LSA se inundan hacia/a través del área. Si el área es un área stub, estas son las opciones con las que puede configurar la capacidad de enrutamiento externo; de lo contrario, la única opción es Import External LSAs. • Import External LSAs. Importa y propaga los LSA externos. • Import No LSAs. No importa ni propaga los LSA externos.
SPF Runs	El número de veces que se calculó la tabla de rutas intraárea usando la base de datos de estado de enlace de esta área. Normalmente se hace con el algoritmo de Dijkstra.
Area Border Router Count	El número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	El número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
Area LSA Checksum	La suma sin signo de 32 bits de los checksums LSA de los anuncios de estado de enlace contenidos en la base de datos de estado de enlace de esta área. Esta suma excluye los anuncios de estado de enlace externos (LSA tipo 5). La suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar la base de datos de estado de enlace de dos routers.

Tabla 130. Configuración de área común de OSPF (continuación)

Campo	Descripción
Flood List Length	Es el número de LSA en la lista de inundación de esta área.
Import Summary LSAs	Los LSA de resumen se importan a esta área.

Configurar el área stub de OSPF

Para configurar el área stub de OSPF:

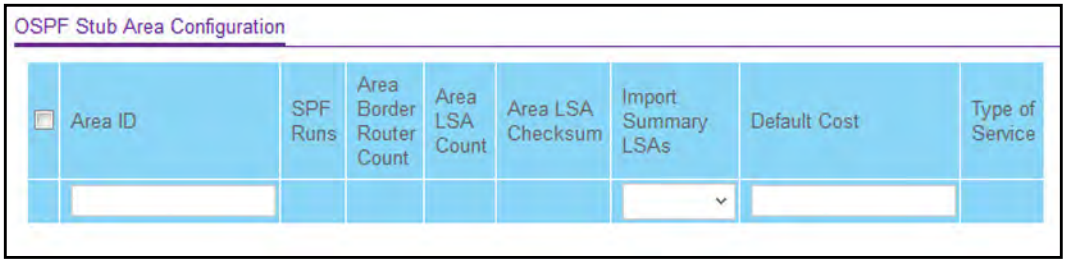
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Stub Area Configuration.



5. Introduzca el OSPF Area ID.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

6. Configure Import Summary LSAs seleccionando Enable o Disable en la lista.

Si selecciona Enable, los LSA de resumen se importan a las áreas stub.

7. Configure Default Cost introduciendo el valor de métrica que se aplicará a la ruta predeterminada anunciada al área stub.

Los valores válidos van de 1 a 16,777,215.
8. Haga clic en el botón Add.
El área se configura como área stub.
9. Haga clic en el botón Apply.
La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 131. Configuración de área stub de OSPF

Campo	Descripción
SPF Runs	El número de veces que se calculó la tabla de rutas intraárea usando la base de datos de estado de enlace de esta área. Normalmente se hace con el algoritmo de Dijkstra.
Area Border Router Count	El número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	El número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
Area LSA Checksum	La suma sin signo de 32 bits de los checksums LSA de los anuncios de estado de enlace contenidos en la base de datos de estado de enlace de esta área. Esta suma excluye los anuncios de estado de enlace externos (LSA tipo 5). La suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar la base de datos de estado de enlace de dos routers.
Type of Service	Este campo es el ToS normal asociado a la métrica stub.

Configurar el área NSSA de OSPF

Para configurar el área NSSA:

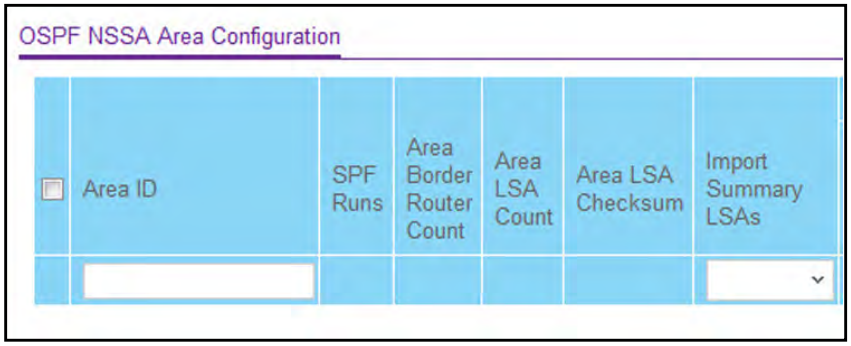
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > NSSA Area Configuration.





5. Introduzca el OSPF Area ID.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

6. Configure Import Summary LSAs seleccionando Enable o Disable en la lista.

Si selecciona Enable, los LSA de resumen se importan a las áreas NSSA.

7. Configure Default Information Originate.

Esta opción le permite anunciar una ruta predeterminada en la NSSA cuando la importación de LSA de resumen está deshabilitada.

a. En la lista Admin Mode, seleccione Enable o Disable para Default Information Originate.

b. En el campo Metric Value, establezca el valor de métrica predeterminado para Default Information Originate. El rango de valores es de 1 a 16777214.
c. En el campo Metric Type, seleccione el tipo de la métrica especificada en el campo Metric Value.

Las opciones son las siguientes:

- Comparable Cost. Métricas externas tipo 1 comparables con la métrica OSPF.
- Non-comparable Cost. Métricas externas tipo 2 que se consideran mayores que el costo de la métrica OSPF.

8. Seleccione el Translator Role de la NSSA.

Las opciones son las siguientes:
a. Always. Hace que el router asuma el rol de traductor en cuanto se convierte en router de borde.
b. Candidate. Hace que el router participe en el proceso de elección del traductor cuando alcanza el estado de router de borde.

9. En el campo Translator Stability Interval, configure el traductor de la NSSA.

El valor es el período durante el cual un traductor elegido sigue realizando sus funciones después de determinar que otro router lo destituyó como traductor. El rango válido es de 0 a 3600.

10. En el campo Redistribute Mode, seleccione Enable o Disable en la lista.

Esto configura el ABR de la NSSA para que las rutas externas aprendidas se redistribuyan a la NSSA.

11. Haga clic en el botón Add.
El área se configura como área NSSA.

12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 132. Configuración de área NSSA de OSPF

Campo	Descripción
SPF Runs	El número de veces que se calculó la tabla de rutas intraárea usando la base de datos de estado de enlace de esta área. Normalmente se hace con el algoritmo de Dijkstra.
Area Border Router Count	El número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	El número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
Area LSA Checksum	La suma sin signo de 32 bits de los checksums LSA de los anuncios de estado de enlace contenidos en la base de datos de estado de enlace de esta área. Esta suma excluye los anuncios de estado de enlace externos (LSA tipo 5). La suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar la base de datos de estado de enlace de dos routers.
Translator State	Este campo muestra si el router de borde NSSA traduce el Tipo 7 a Tipo 5 y cómo lo hace. Las opciones posibles son las siguientes: • Enabled. El rol de traductor del router de borde NSSA está establecido en Always. • Elected. El router de borde NSSA candidato está traduciendo LSA de Tipo 7 a Tipo 5. • Disabled. El router de borde NSSA candidato no está traduciendo LSA de Tipo 7 a Tipo 5.

Configurar el rango de área de OSPF

Para configurar el rango de área de OSPF:

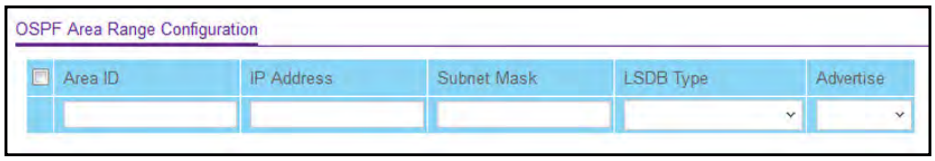
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Area Range Configuration.



5. Introduzca el OSPF Area ID.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.
6. Introduzca la dirección IP del rango de direcciones del área seleccionada.
7. Introduzca la máscara de subred del rango de direcciones del área seleccionada.

8. En la lista del campo LSDB Type, seleccione el tipo de anuncio de enlace asociado con el área y el rango de direcciones especificados.

Las opciones son: Network Summary o NSSA External. El tipo predeterminado es Network Summary.

9. En la lista Advertise, seleccione Enable o Disable.

Si selecciona Enable, el rango de direcciones se anuncia fuera del área mediante un LSA de resumen de red. El valor predeterminado es Enable.

10. Haga clic en el botón Add.
Se agrega el nuevo rango de direcciones.
11. Haga clic en el botón Apply.
La configuración se guarda.

Configurar la interfaz OSPF

Para configurar la interfaz OSPF:

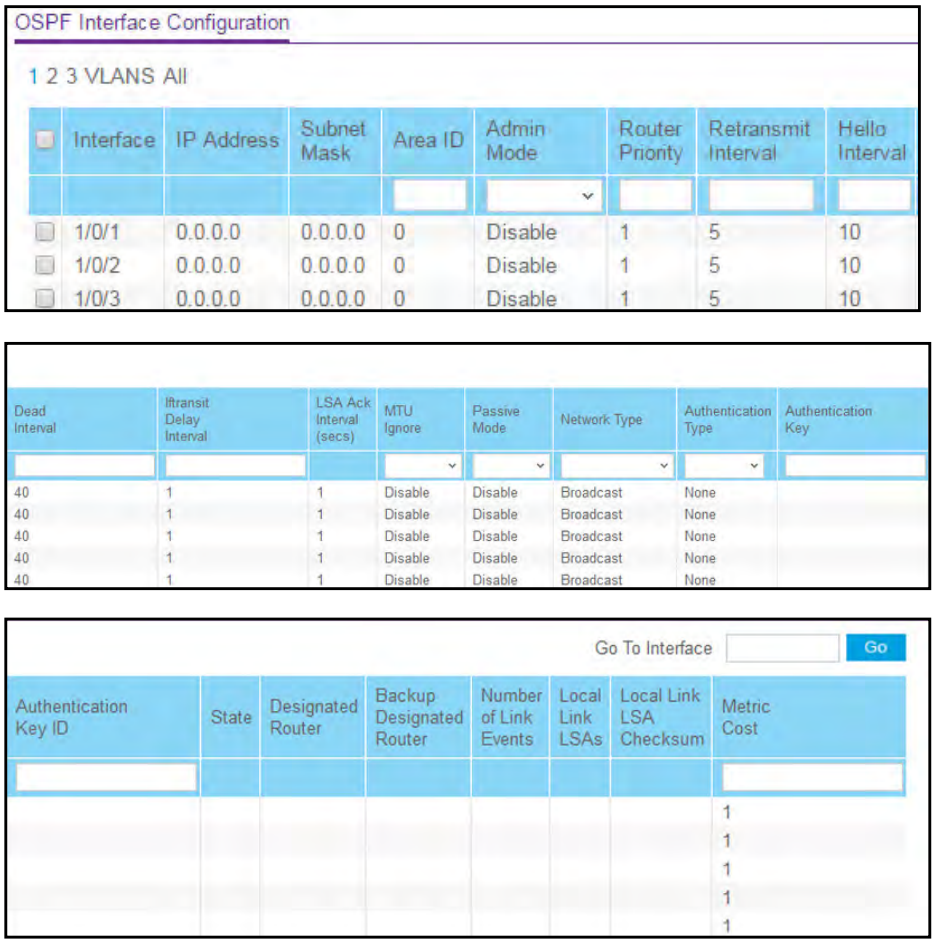
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.
6. En el campo OSPF Area ID, introduzca el entero de 32 bits en formato decimal con puntos.

   Este ID identifica de forma única el área OSPF a la que se conecta la interfaz de router seleccionada. Si asigna un ID de área que no existe, el área se crea con valores predeterminados.

7. En la lista Admin Mode, seleccione Enable o Disable.

   El valor predeterminado es Disable. Puede configurar parámetros de OSPF sin habilitar el modo administrativo de OSPF, pero el cambio no surte efecto hasta que lo habilite. La siguiente información se muestra solo si el modo administrativo está habilitado:

   - Estado
   - Router designado
   - Router designado de respaldo

- Número de eventos de enlace
- Intervalo de LSA Ack
- Costo de métrica

Para que OSPF funcione por completo, debe introducir una dirección IP y una máscara de subred válidas. Para más información, consulte Configurar la interfaz IP en la página 317.

Nota: Una vez que OSPF se inicializa en el router, permanece inicializado hasta que el router se restablece.

8. En el campo Router Priority, introduzca la prioridad OSPF de la interfaz seleccionada.

La prioridad de una interfaz se especifica como un entero de 0 a 255. El valor predeterminado es 1, que es la prioridad de router más alta. Un valor de 0 indica que el router no puede convertirse en el router designado de esta red.

9. Configure Retransmit Interval introduciendo el intervalo de retransmisión OSPF de la interfaz especificada.

Es el número de segundos entre anuncios de estado de enlace para las adyacencias de esta interfaz de router. Este valor también se usa al retransmitir descripciones de base de datos y paquetes de solicitud de estado de enlace. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

10. Configure Hello Interval introduciendo el intervalo hello OSPF de la interfaz especificada, en segundos.

Este parámetro debe ser igual en todos los routers conectados a una red. Los valores van de 1 a 65,535. El valor predeterminado es 10 segundos.

11. Introduzca OSPF Dead Interval de la interfaz especificada, en segundos.

Esto especifica cuánto tiempo espera un router los paquetes hello de un router vecino antes de declararlo inactivo. Este parámetro debe ser igual en todos los routers conectados a una red. Este valor debe ser un múltiplo del intervalo hello (por ejemplo, 4). Los valores válidos van de 1 a 65,535. El valor predeterminado es 40 segundos.

12. En el campo Iftransit Delay Interval, escriba el retardo de tránsito OSPF de la interfaz especificada.

Especifica el número estimado de segundos que tarda en transmitirse un paquete de actualización de estado de enlace por la interfaz seleccionada. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

13. Configure MTU Ignore seleccionando Enable o Disable en la lista.

MTU Ignore deshabilita la detección de discrepancias de MTU de OSPF en los paquetes de descripción de base de datos recibidos. El valor predeterminado es Disable (la detección está habilitada).

14. Configure Passive Mode seleccionando Enable o Disable en la lista.

Haga pasiva una interfaz para evitar que OSPF forme una adyacencia en ella. OSPF anuncia las redes conectadas a interfaces pasivas como redes stub. De forma predeterminada, las interfaces no son pasivas, es decir, el modo pasivo predeterminado es Disable.

15. En la lista OSPF Network Type, seleccione Broadcast o Point-to-Point.

OSPF selecciona un router designado y origina LSA de red solo en redes de difusión. En un enlace punto a punto no puede haber más de dos routers OSPF. El tipo de red predeterminado para interfaces Ethernet es broadcast.

16. Seleccione en la lista un tipo de autenticación (Authentication Type) distinto de None. Las opciones son las siguientes:

- None. Es el estado inicial de la interfaz. Si selecciona esta opción, no se ejecuta ningún protocolo de autenticación. El valor predeterminado es None.
- Simple. Se le pide escribir una clave de autenticación. Esta clave se incluye, en texto claro, en el encabezado OSPF de todos los paquetes enviados en la red. Todos los routers de la red deben configurarse con la misma clave.
- Encrypt. Se le pide escribir una clave y un ID de autenticación. El cifrado usa el algoritmo MD5 Message-Digest. Todos los routers de la red deben configurarse con la misma clave e ID.

17. Escriba el valor de Authentication Key ID que se usará para la autenticación.

Solo se le pide un ID si selecciona Encrypt como tipo de autenticación. El ID es un número entre 0 y 255, inclusive.

18. En el campo Metric Cost, escriba el costo del enlace.

OSPF usa este valor para calcular las rutas más cortas. El rango es de 1 a 65,535. El valor predeterminado es 1.

19. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 133. Configuración de interfaz OSPF

Campo	Descripción
IP Address	La dirección IP de la interfaz.
Subnet Mask	La máscara de red, que indica la parte de la dirección IP que identifica la red conectada.
LSA Ack Interval (secs)	El número de segundos que se espera antes de enviar un acuse de recibo diferido.

Tabla 133. Configuración de interfaz OSPF (continuación)

Campo	Descripción
State	El estado de la interfaz del router seleccionada. Puede ser uno de los siguientes: • Down. Es el estado inicial de la interfaz. Los protocolos de nivel inferior indicaron que la interfaz no se puede usar. Los parámetros de la interfaz se establecen en sus valores iniciales. Todos los temporizadores de la interfaz están deshabilitados y no hay adyacencias asociadas a la interfaz. • Loopback. La interfaz del router hacia la red está en bucle, ya sea por hardware o por software. La interfaz no está disponible para el tráfico de datos normal. Puede obtener información sobre la calidad de esta interfaz enviándole pings ICMP o mediante una prueba de errores de bits. Por ello, todavía se pueden dirigir paquetes IP a una interfaz en estado loopback. Para facilitarlo, estas interfaces se anuncian en las LSA de router como rutas de host único, cuyo destino es la dirección IP de la interfaz. • Waiting. El router intenta determinar la identidad del router designado de respaldo de la red supervisando los paquetes hello recibidos. El router no puede elegir un router designado de respaldo ni un router designado hasta salir del estado de espera. Esto evita cambios innecesarios del router designado de respaldo. • Designated Router. Este router es el router designado en la red conectada. Se establecen adyacencias con todos los demás routers conectados a la red. El router también debe originar una LSA de red para el nodo de red. La LSA de red contiene enlaces a todos los routers (incluido el router designado) conectados a la red.
State (continuación)	• Backup Designated Router. Este router es el router designado de respaldo en la red conectada. Se convierte en router designado si falla el router designado actual. El router establece adyacencias con todos los demás routers conectados a la red. El router designado de respaldo realiza funciones ligeramente distintas durante la inundación de LSA, en comparación con el router designado. • Other Designated Router. La interfaz está conectada a una red de difusión en la que otros routers son el router designado y el router designado de respaldo. El router intenta formar adyacencias con el router designado y con el router designado de respaldo.
Designated Router	La identidad del router designado de esta red, desde el punto de vista del router anunciante. El router designado se identifica aquí por su ID de router. El valor 0.0.0.0 significa que no hay router designado. Este campo solo aparece si el modo administrativo de OSPF está habilitado.
Backup Designated Router	La identidad del router designado de respaldo de esta red, desde el punto de vista del router anunciante. El router designado de respaldo se identifica aquí por su ID de router. Es 0.0.0.0 si no hay router designado de respaldo.
Number of Link Events	El número de veces que la interfaz OSPF especificada cambió de estado.
Local Link LSAs	El número de LSA opacas cuyo alcance de inundación es el enlace de esta interfaz.
Local Link LSA Checksum	La suma de las sumas de verificación de las LSA de enlace local de este enlace.

Ver y borrar las estadísticas OSPF de una interfaz

Si OSPF está habilitado, puede ver y borrar las estadísticas de la interfaz seleccionada.

Para ver y borrar las estadísticas OSPF de una interfaz:

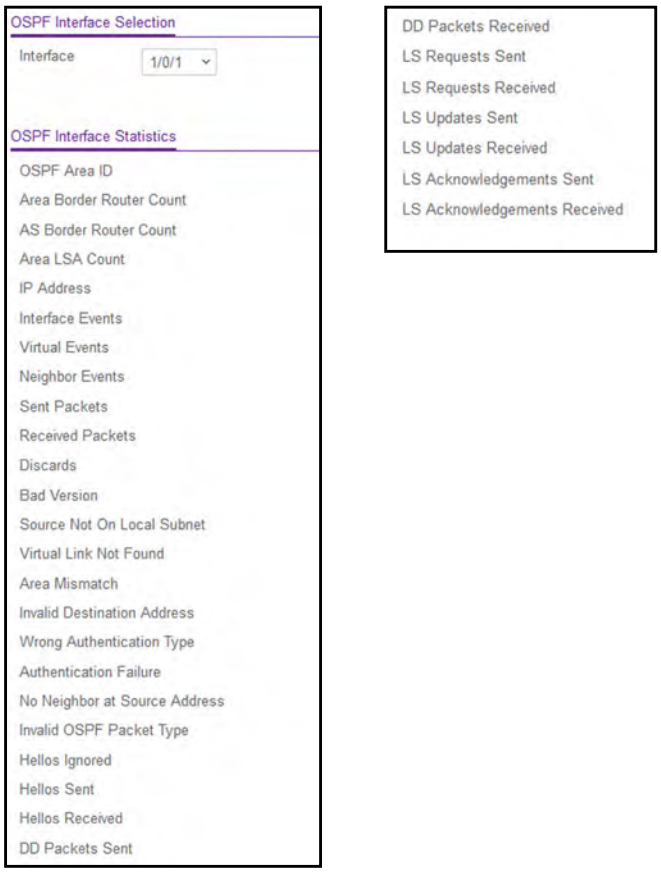
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Interface Statistics.



5. En el área OSPF Interface Selection de la página, en la lista del campo Interface, seleccione la interfaz cuyas estadísticas desea mostrar.
6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh).
7. Para borrar todas las estadísticas de la interfaz OSPF, haga clic en el botón Clear.

La siguiente tabla describe los datos no configurables de OSPF Interface Statistics que se muestran.

Tabla 134. Estadísticas de interfaz OSPF

Campo	Descripción
OSPF Area ID	El área OSPF a la que pertenece la interfaz del router seleccionada. Un ID de área OSPF es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta la interfaz.
Area Border Router Count	El número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
AS Border Router Count	El número total de routers de borde de sistema autónomo accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	El número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
IP Address	La dirección IP de la interfaz.
Interface Events	El número de veces que la interfaz OSPF especificada cambió de estado o ocurrió un error.
Virtual Events	El número de cambios de estado o errores ocurridos en este enlace virtual.
Neighbor Events	El número de veces que esta relación de vecindad cambió de estado u ocurrió un error.
Sent Packets	El número de paquetes OSPF transmitidos en la interfaz.
Received Packets	El número de paquetes OSPF válidos recibidos en la interfaz.
Discards	El número de paquetes OSPF recibidos que se descartaron por un error en el paquete o en su procesamiento.
Bad Version	El número de paquetes OSPF recibidos cuyo campo de versión en el encabezado OSPF no coincide con la versión del proceso OSPF que maneja el paquete.
Source Not on Local Subnet	El número de paquetes recibidos que se descartaron porque la dirección IP de origen no está dentro de una subred configurada en una interfaz local.
Virtual Link Not Found	El número de paquetes OSPF recibidos que se descartaron porque la interfaz de entrada está en un área que no es backbone y el encabezado OSPF identifica el paquete como perteneciente al backbone, pero OSPF no tiene un enlace virtual hacia el remitente del paquete.
Area Mismatch	El número de paquetes OSPF descartados porque el ID de área del encabezado OSPF no es el ID de área configurado en la interfaz de entrada.
Invalid Destination Address	El número de paquetes OSPF descartados porque la dirección IP de destino del paquete no es la dirección de la interfaz de entrada ni las direcciones multicast AllDrRouters o AllSpfRouters.
Wrong Authentication Type	El número de paquetes descartados porque el tipo de autenticación especificado en el encabezado OSPF no coincide con el tipo de autenticación configurado en la interfaz de entrada.

Tabla 134. Estadísticas de interfaz OSPF (continuación)

Campo	Descripción
Authentication Failure	El número de paquetes OSPF descartados porque el remitente no es un vecino existente o su dirección IP no coincide con la dirección IP registrada previamente para ese vecino.
No Neighbor at Source Address	El número de paquetes OSPF descartados porque el remitente no es un vecino existente o su dirección IP no coincide con la dirección IP registrada previamente para ese vecino.
Invalid OSPF Packet Type	El número de paquetes OSPF descartados porque el campo de tipo de paquete en el encabezado OSPF no es un tipo conocido.
Hellos Ignored	El número de paquetes hello recibidos de vecinos nuevos que este router ignoró al alcanzarse el límite de vecinos en una interfaz o en el sistema en general.
Hellos Sent	El número de paquetes hello enviados por este router en esta interfaz.
Hellos Received	El número de paquetes hello recibidos por este router en esta interfaz.
DD Packets Sent	El número de paquetes de descripción de base de datos enviados por este router en esta interfaz.
DD Packets Received	El número de paquetes de descripción de base de datos recibidos por este router en esta interfaz.
LS Requests Sent	El número de solicitudes LS enviadas por este router en esta interfaz.
LS Requests Received	El número de solicitudes LS recibidas por este router en esta interfaz.
LS Updates Sent	El número de actualizaciones LS enviadas por este router en esta interfaz.
LS Updates Received	El número de actualizaciones LS recibidas por este router en esta interfaz.
LS Acknowledgements Sent	El número de acuses de recibo LS enviados por este router en esta interfaz.
LS Acknowledgements Received	El número de acuses de recibo LS recibidos por este router en esta interfaz.

Ver la tabla de vecinos OSPF y borrar los vecinos OSPF

Puede ver la lista de la tabla de vecinos OSPF. Al especificar un ID de vecino, se muestra información detallada de ese vecino. La información solo se muestra si OSPF está habilitado. También puede borrar los vecinos OSPF.

Para ver la tabla de vecinos OSPF y borrar los vecinos OSPF:

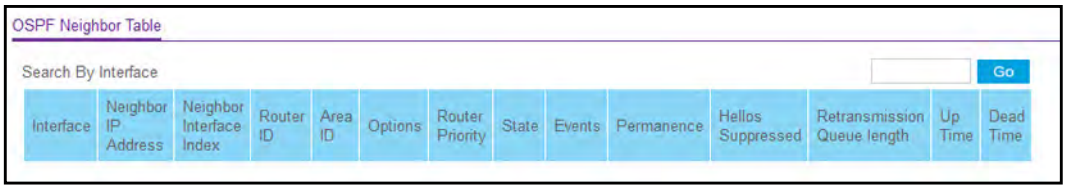
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Neighbor Table.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar todos los vecinos de la tabla, haga clic en el botón Clear.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 135. Tabla de vecinos OSPF

Campo	Descripción
Interface	La interfaz cuyos datos se mostrarán o configurarán. La ranura 0 es la unidad base.
Neighbor IP Address	La dirección IP de la interfaz del router vecino hacia la red conectada. Se usa como dirección IP de destino cuando se envían paquetes del protocolo como unicast por esta adyacencia. También se usa en las LSA de router como ID de enlace de la red conectada si el router vecino es seleccionado como router designado. La dirección IP del vecino se aprende al recibir paquetes hello del vecino. En los enlaces virtuales, se aprende durante el proceso de creación de la tabla de enrutamiento.
Neighbor Interface Index	Un valor unidad/ranura/puerto que identifica el índice de interfaz del vecino.
Router ID	Un entero de 32 bits en formato decimal con puntos que representa la interfaz del vecino.
Area ID	El ID del área OSPF asociada a la interfaz.
Options	Un valor entero que indica las capacidades opcionales de OSPF que admite el vecino. Las capacidades opcionales de OSPF del vecino también se indican en sus paquetes hello. Esto permite rechazar los paquetes hello recibidos (por ejemplo, ni siquiera se empiezan a formar relaciones de vecindad) si hay discrepancias en ciertas capacidades OSPF esenciales.
Router Priority	La prioridad OSPF de la interfaz especificada. La prioridad de una interfaz es un entero de 0 a 255. Un valor de 0 indica que el router no puede convertirse en router designado en esta red.

Tabla 135. Tabla de vecinos OSPF (continuación)

Campo	Descripción
State	El estado de un vecino puede ser el siguiente: • Down. Es el estado inicial de una conversación con un vecino. Indica que no se ha recibido información reciente del vecino. En redes NBMA, aún se pueden enviar paquetes hello a vecinos en estado Down, aunque con menor frecuencia. • Attempt. Este estado solo es válido para vecinos conectados a redes NBMA. Indica que no se ha recibido información reciente del vecino, pero que se debe hacer un esfuerzo mayor para contactarlo. Esto se hace enviándole paquetes hello en los intervalos hello. • Init. Se vio recientemente un paquete hello del vecino. Sin embargo, aún no se estableció comunicación bidireccional con el vecino (por ejemplo, el router no apareció en el paquete hello del vecino). Todos los vecinos en este estado (o superior) se indican en los paquetes hello enviados desde la interfaz asociada. • 2-Way. La comunicación entre los dos routers es bidireccional. Esto lo garantiza el funcionamiento del protocolo hello. Es el estado más avanzado antes de empezar a establecer la adyacencia. El router designado de respaldo se selecciona entre los vecinos en estado 2-way o superior. • Exchange Start. Es el primer paso para crear una adyacencia entre los dos routers vecinos. El objetivo es decidir qué router es el maestro y el número de secuencia DD inicial. Las conversaciones con vecinos en este estado o superior se llaman adyacencias.
State (continuación)	• Exchange. El router describe toda su base de datos de estado de enlace enviando paquetes de descripción de base de datos al vecino. También se pueden enviar paquetes de solicitud de estado de enlace pidiendo las LSA más recientes del vecino. Todas las adyacencias en estado exchange o superior se usan en el procedimiento de inundación. Estas adyacencias pueden transmitir y recibir todos los tipos de paquetes del protocolo de enrutamiento OSPF. • Loading. Se envían al vecino paquetes de solicitud de estado de enlace pidiendo las LSA más recientes descubiertas (pero aún no recibidas) en el estado exchange. • Full. Los routers vecinos son totalmente adyacentes. Estas adyacencias ahora aparecen en las LSA de router y de red.
Events	El número de veces que esta relación de vecindad cambió de estado u ocurrió un error.
Permanence	Muestra el estado de la entrada. Dynamic y Permanent indican cómo se conoció al vecino.
Hellos Suppressed	Indica si se suprimen los hello hacia el vecino.
Retransmission Queue Length	Un entero que representa la longitud actual de la cola de retransmisión del ID de router vecino especificado de la interfaz especificada.
Up Time	Tiempo activo del vecino; tiempo desde que la adyacencia alcanzó por última vez el estado Full.
Dead Time	El tiempo, en segundos, que se espera antes de que el router considere que el vecino es inaccesible.

Ver la base de datos de estado de enlace OSPF

Para ver la base de datos de estado de enlace OSPF:

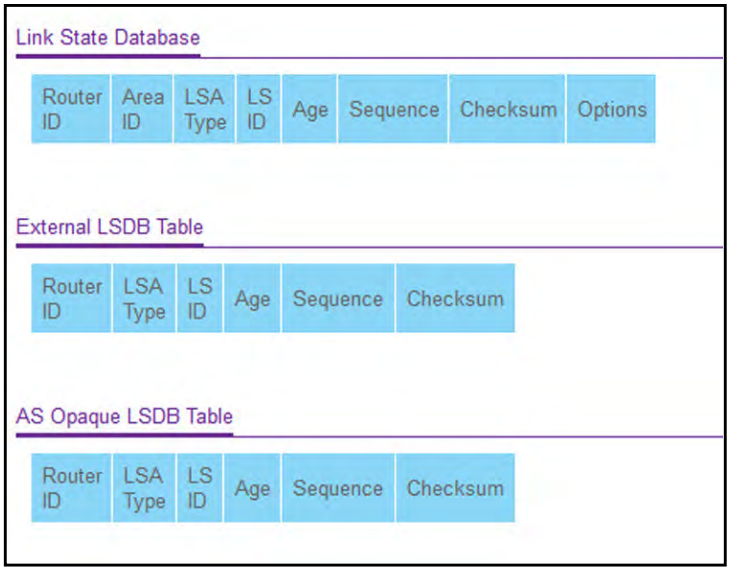
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing > OSPF > Advanced > Link State Database.**



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 136. Base de datos de estado de enlace OSPF

Campo	Descripción
Router ID	El entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS). El ID de router se establece en la página IP Configuration. Para cambiarlo, primero debe deshabilitar OSPF. Después de establecer el nuevo ID de router, debe volver a habilitar OSPF para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.
Area ID	El ID de un área OSPF a la que está conectada una de las interfaces del router. Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que está conectada una interfaz.

Tabla 136. Base de datos de estado de enlace OSPF (continuación)

Campo	Descripción
LSA Type	El formato y la función del anuncio de estado de enlace. LSA Type es uno de los siguientes: • Illegal • Router Links • Network Links • Network Summary • ASBR Summary • AS-external • Group Member • NSSA • TMP2 • Link Opaque • Area Opaque • AS Opaque • Unknown
LS ID	El ID de estado de enlace identifica la parte del dominio de enrutamiento que describe el anuncio. El valor de LS ID depende del tipo LS del anuncio.
Age	El tiempo, en segundos, desde que se originó el anuncio de estado de enlace.
Sequence	El campo de número de secuencia es un entero de 32 bits con signo. Se usa para detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.
Checksum	La suma de verificación se usa para detectar datos dañados en un anuncio. Este daño puede ocurrir mientras el anuncio se inunda o mientras está almacenado en la memoria de un router. Este campo es la suma de verificación de todo el contenido del anuncio, excepto el campo LS age.
Options	El campo Options del encabezado del anuncio de estado de enlace indica qué capacidades opcionales están asociadas al anuncio. Las opciones son las siguientes: • Q. Habilita la compatibilidad con ingeniería de tráfico QoS. • E. Describe la forma en que se inundan las LSA externas al AS. • MC. Describe la forma en que se reenvían los datagramas IP multicast según las especificaciones del estándar. • O. Describe si se admiten LSA opacas. • V. Describe si se admiten las extensiones OSPF++ para VPN/COS.

La siguiente tabla describe la información no configurable que se muestra en la tabla External Link State Database (LSDB).

Tabla 137. Tabla de base de datos de estado de enlace externo OSPF

Campo	Descripción
Router ID	El entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS). El ID de router se establece en la página IP Configuration. Para cambiarlo, primero debe deshabilitar OSPF. Después de establecer el nuevo ID de router, debe volver a habilitar OSPF para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.
LSA Type	El formato y la función del anuncio de estado de enlace. LSA Type es uno de los siguientes: • ASBR Summary • AS-external • NSSA • TMP2
LS ID	El ID de estado de enlace identifica la parte del dominio de enrutamiento que describe el anuncio. El valor de LS ID depende del tipo LS del anuncio.
Age	El tiempo, en segundos, desde que se originó el anuncio de estado de enlace.
Sequence	El campo de número de secuencia es un entero de 32 bits con signo. Se usa para detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.
Checksum	La suma de verificación se usa para detectar datos dañados en un anuncio. Este daño puede ocurrir mientras el anuncio se inunda o mientras está almacenado en la memoria de un router. Este campo es la suma de verificación de todo el contenido del anuncio, excepto el campo LS age.

La siguiente tabla describe la información no configurable que se muestra en la tabla AS Opaque Link State Database (LSDB).

Tabla 138. Tabla de base de datos de estado de enlace opaco AS OSPF

Campo	Descripción
Router ID	El entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS). El ID de router se establece en la página IP Configuration. Para cambiarlo, primero debe deshabilitar OSPF. Después de establecer el nuevo ID de router, debe volver a habilitar OSPF para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.
LSA Type	El formato y la función del anuncio de estado de enlace. LSA Type es uno de los siguientes: • Area Opaque • AS Opaque • Link Opaque

Tabla 138. Tabla de base de datos de estado de enlace opaco AS OSPF (continuación)

Campo	Descripción
LS ID	El ID de estado de enlace identifica la parte del dominio de enrutamiento que describe el anuncio. El valor de LS ID depende del tipo LS del anuncio.
Age	El tiempo, en segundos, desde que se originó el anuncio de estado de enlace.
Sequence	El campo de número de secuencia es un entero de 32 bits con signo. Se usa para detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.
Checksum	La suma de verificación se usa para detectar datos dañados en un anuncio. Este daño puede ocurrir mientras el anuncio se inunda o mientras está almacenado en la memoria de un router. Este campo es la suma de verificación de todo el contenido del anuncio, excepto el campo LS age.

Configurar el enlace virtual OSPF

Para configurar el enlace virtual OSPF:

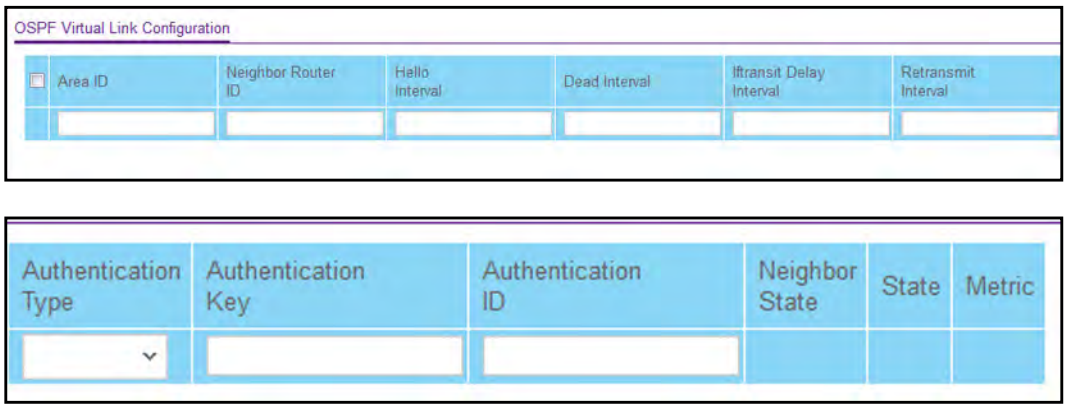
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Virtual Link Configuration.



5. En el campo Area ID, escriba el ID de área OSPF.

Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

Se pueden configurar enlaces virtuales entre cualquier par de routers de borde de área con interfaces en un área común (que no sea backbone).

6. Configure el valor de Neighbor Router ID escribiendo la parte del vecino de la especificación del enlace virtual.

Se pueden configurar enlaces virtuales entre cualquier par de routers de borde de área con interfaces en un área común (que no sea backbone).

7. En el campo Hello Interval, escriba el intervalo hello de OSPF de la interfaz especificada en segundos.

Este parámetro debe ser igual en todos los routers conectados a una red. Los valores válidos van de 1 a 65,535. El valor predeterminado es 10 segundos.

8. En el campo Dead Interval, escriba el intervalo dead de OSPF de la interfaz especificada en segundos.

Esto especifica cuánto tiempo espera un router los paquetes hello de un router vecino antes de declararlo inactivo. Este parámetro debe ser igual en todos los routers conectados a una red. Este valor debe ser un múltiplo del intervalo hello (por ejemplo, 4). Los valores válidos van de 1 a 65,535. El valor predeterminado es 40.

9. En el campo Iftransit Delay Interval, introduzca el retardo de tránsito OSPF de la interfaz especificada.

Especifica el número estimado de segundos que tarda en transmitirse un paquete de actualización de estado de enlace por la interfaz seleccionada. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

10. En el campo Retransmit Interval, introduzca el intervalo de retransmisión OSPF de la interfaz especificada.

Es el número de segundos entre anuncios de estado de enlace para las adyacencias de esta interfaz de router. Este valor también se usa al retransmitir descripciones de base de datos y paquetes de solicitud de estado de enlace. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

11. En el menú Authentication Type, seleccione uno de los siguientes tipos de autenticación:

- None. Es el estado inicial de la interfaz.
- Simple. Si selecciona Simple, se le pide introducir una clave de autenticación. Esta clave se incluye, sin cifrar, en el encabezado OSPF de todos los paquetes enviados en la red. Todos los routers de la red deben configurarse con la misma clave.
- Encrypt. Si selecciona Encrypt, se le pide introducir una clave de autenticación y un ID de autenticación. El cifrado usa el algoritmo MD5 Message-Digest. Todos los routers de la red deben configurarse con la misma clave e ID.

12. En el campo Authentication Key, introduzca la clave de autenticación OSPF de la interfaz especificada.

Si no selecciona autenticación, no se le pide introducir una clave.

- Si selecciona la autenticación Simple, no puede usar una clave de más de 8 octetos.
- Si selecciona Encrypt, la clave puede tener hasta 16 octetos.

El valor de la clave solo se muestra si inició sesión con privilegios de lectura/escritura; de lo contrario, se muestra con asteriscos.

13. En el campo Authentication ID, introduzca el ID que se usará para la autenticación.

Solo se le pide introducir un ID cuando selecciona Encrypt como tipo de autenticación. El ID es un número entre 0 y 255, inclusive.

14. Haga clic en el botón Add (Agregar).
Se agrega el nuevo enlace virtual.
15. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 139. Configuración de enlace virtual OSPF

Campo	Descripción
Estado del vecino	El estado de la interfaz OSPF puede ser uno de estos valores: • Down. Es el estado inicial de la interfaz. Los protocolos de nivel inferior indicaron que la interfaz no se puede usar. Los parámetros de la interfaz tienen sus valores iniciales. Todos los temporizadores de la interfaz están deshabilitados y no hay adyacencias asociadas a la interfaz. • Waiting. El router intenta determinar la identidad del router designado de respaldo supervisando los paquetes hello recibidos. El router no puede elegir un router designado de respaldo ni un router designado hasta que salga del estado Waiting. Esto evita cambios innecesarios del router designado de respaldo. • Point-to-Point. La interfaz está operativa y conectada al enlace virtual. Al entrar en este estado, el router intenta formar una adyacencia con el router vecino. Se envían paquetes hello al vecino cada intervalo hello en segundos. • Designated Router. Este router es el router designado en la red conectada. Se establecen adyacencias con todos los demás routers conectados a la red. El router también debe originar un network-LSA para el nodo de red. El network-LSA contiene enlaces a todos los routers (incluido el router designado) conectados a la red. • Backup Designated Router. Este router es el router designado de respaldo en la red conectada. Se convierte en router designado si el router designado actual falla. El router establece adyacencias con todos los demás routers conectados a la red. El router designado de respaldo realiza funciones ligeramente distintas durante el procedimiento de inundación, en comparación con el router designado. • Other Designated Router. La interfaz está conectada a una red broadcast o NBMA en la que se eligieron otros routers como router designado y router designado de respaldo. El router intenta formar adyacencias tanto con el router designado como con el router designado de respaldo.

Tabla 139. Configuración de enlace virtual OSPF (continuación)

Campo	Descripción
Estado	Estado de la interfaz. Puede tener uno de los siguientes valores: • Down. Es el estado inicial de la interfaz. Los protocolos de nivel inferior indicaron que la interfaz no se puede usar. Los parámetros de la interfaz tienen sus valores iniciales. Todos los temporizadores de la interfaz están deshabilitados y no hay adyacencias asociadas a la interfaz. • Waiting. El router intenta determinar la identidad del router designado de respaldo supervisando los paquetes hello recibidos. El router no puede elegir un router designado de respaldo ni un router designado hasta que salga del estado Waiting. Esto evita cambios innecesarios del router designado de respaldo. • Point-to-Point. La interfaz está operativa y conectada al enlace virtual. Al entrar en este estado, el router intenta formar una adyacencia con el router vecino. Se envían paquetes hello al vecino cada intervalo hello en segundos. • Designated Router. Este router es el router designado en la red conectada. Se establecen adyacencias con todos los demás routers conectados a la red. El router también debe originar un network-LSA para el nodo de red. El network-LSA contiene enlaces a todos los routers (incluido el router designado) conectados a la red. • Backup Designated Router. Este router es el router designado de respaldo en la red conectada. Se convierte en router designado si el router designado actual falla. El router establece adyacencias con todos los demás routers conectados a la red. El router designado de respaldo realiza funciones ligeramente distintas durante el procedimiento de inundación, en comparación con el router designado. • Other Designated Router. La interfaz está conectada a una red broadcast o NBMA en la que se eligieron otros routers como router designado y router designado de respaldo. El router intenta formar adyacencias tanto con el router designado como con el router designado de respaldo.
Métrica	Valor de métrica que usa el enlace virtual.

Configurar la redistribución de rutas OSPF

Puede configurar los parámetros de redistribución de rutas OSPF. Los valores permitidos para cada campo se muestran junto al campo. Si se introducen valores no válidos, aparece un mensaje de alerta con la lista de todos los valores válidos.

Configurar la redistribución de rutas OSPF:

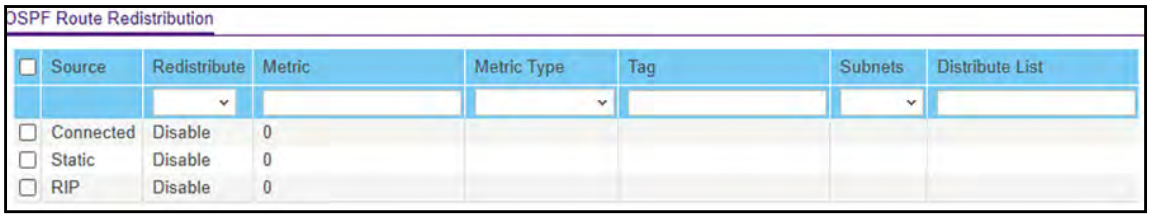
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > Route Redistribution.



5. En el menú Source, seleccione una de las rutas de origen disponibles que no se hayan configurado previamente para redistribución por OSPF.

Los valores válidos son los siguientes:

- Connected
- OSPF
- RIP
- Static

6. En la lista Redistribute, seleccione Enable o Disable para la redistribución del protocolo de origen seleccionado.

7. Establezca en Metric el valor que se usará como métrica de las rutas redistribuidas.

Este campo muestra la métrica si el origen estaba preconfigurado y puede modificarse. Los valores válidos son de 0 a 16777214.

8. En la lista Metric Type, seleccione el tipo de métrica OSPF de las rutas redistribuidas.

9. Establezca el campo Tag de las rutas redistribuidas.

Este campo muestra la etiqueta si el origen estaba preconfigurado; de lo contrario, la etiqueta es 0 y puede modificarse. Los valores válidos son de 0 a 4294967295.

10. En la lista Subnets, seleccione si las rutas con subredes se redistribuirán (Enable) o no (Disable).

11. En el campo Distribute List, establezca la lista de acceso que filtra las rutas que redistribuirá el protocolo de destino.

Solo se redistribuyen las rutas permitidas. Si este comando hace referencia a una lista de acceso inexistente, se permiten todas las rutas. Los valores válidos para los ID de lista de acceso son de 1 a 199.

Cuando se usa para filtrar rutas, los únicos campos de una lista de acceso que se usan son los siguientes:

- Dirección IP de origen y máscara de red
- Dirección IP de destino y máscara de red
- Acción (permitir o denegar)

Todos los demás campos (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 wildcard, que 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 y máscara de red de destino (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, que indica qué bits de la máscara de destino de la ruta son significativos para el filtrado.

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

Ver el resumen de NSF OSPF

Puede ver el resumen de NSF OSPF. Los valores permitidos para cada campo se muestran junto al campo. Si se introducen valores no válidos, aparece un mensaje de alerta con la lista de todos los valores válidos.

Para configurar el resumen de NSF OSPF:

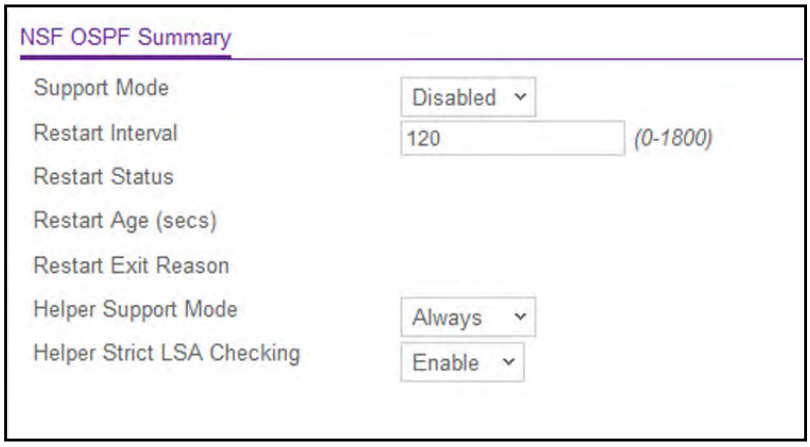
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPF > Advanced > NSF OSPF Summary.



5. En la lista Support Mode, configure cómo realiza la unidad los reinicios ordenados (graceful restart) seleccionando uno de los siguientes valores posibles:

- Always. Indica que OSPF realiza un reinicio ordenado en todos los eventos de reinicio en caliente planificados y no planificados.
- Disabled. Deshabilita los reinicios ordenados de OSPF.
- Planned. Indica que OSPF realiza un reinicio ordenado solo cuando el reinicio está planificado (por ejemplo, debido a un comando initiate failover).

El valor predeterminado es Disabled.
6. Configure Restart Interval. Los valores válidos son de 0 a 1800 segundos. El valor predeterminado es 120 segundos.

7. Use el campo Helper Support Mode para configurar cómo actúa la unidad cuando un vecino realiza un reinicio en caliente.

Los valores posibles son:

- Always. Indica que OSPF ayuda a un vecino que se reinicia durante todos los eventos de reinicio en caliente planificados y no planificados.
- Disabled. Impide que OSPF actúe como vecino auxiliar.
- Planned. Indica que OSPF ayuda a un vecino que se reinicia solo durante eventos planificados.

El valor predeterminado es Always.

8. Configure Helper Strict LSA Checking seleccionando Enable o Disable.

Si se habilita, la unidad sale del modo auxiliar cada vez que cambia la topología.
9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 140. Resumen de NSF OSPF

Campo	Descripción
Estado de reinicio	Estado de reinicio de la función OSPF Helper. Los valores posibles son los siguientes: • Not Restarting • Planned Restart • Unplanned Restart
Antigüedad del reinicio (segundos)	Tiempo transcurrido desde el último reinicio.
Motivo de salida del reinicio	Muestra cómo se inició por última vez la unidad maestra del switch. Los valores posibles son los siguientes: • Not Attempted. No se intentó el reinicio ordenado. • In Progress. El reinicio está en curso. • Completed. El reinicio ordenado anterior se completó correctamente. • Timed Out. El reinicio ordenado anterior agotó el tiempo de espera. • Topology Changed. El reinicio ordenado anterior terminó prematuramente debido a un cambio de topología.

Configurar OSPFv3

Configurar los ajustes básicos de OSPFv3

Para configurar los ajustes básicos de OSPFv3:

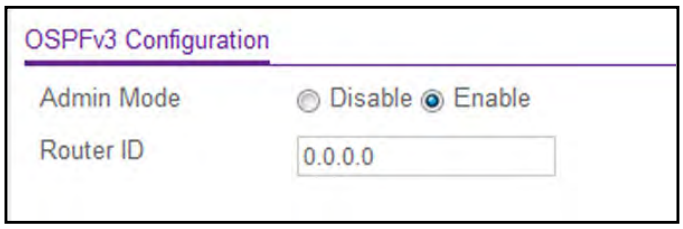
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Basic > OSPFv3 Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Si selecciona Enable, OSPFv3 se activa en el switch. De forma predeterminada, OSPFv3 está habilitado. Debe configurar un ID de router antes de que OSPFv3 pueda estar operativo. Para obtener más información, consulte Configurar los ajustes IP de enrutamiento en la página 307.

   Nota: Una vez que OSPFv3 se inicializa en el router, permanece inicializado hasta que router se restablece.

6. Introduzca en Router ID un entero de 32 bits en formato decimal con puntos que identifique de forma única al router dentro del sistema autónomo (AS).

   Para cambiar el ID de router, primero debe deshabilitar OSPFv3. Después de establecer el nuevo ID, debe volver a habilitar OSPFv3 para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.

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

Configurar los ajustes de anuncio de ruta predeterminada de OSPFv3

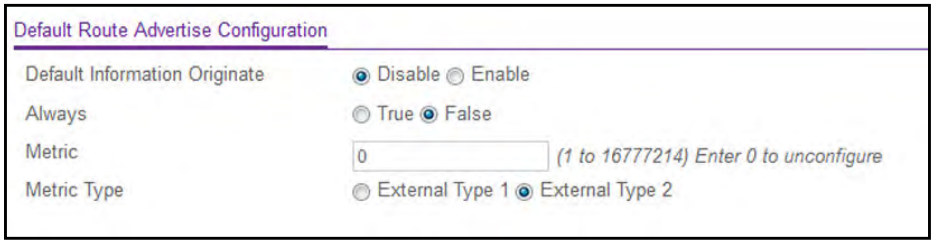
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > OSPFv3 Configuration.



5. Seleccione el botón de opción Default Information Originate Enable.

   Al seleccionar Enable, puede especificar los demás ajustes de esta página. Al seleccionar Disable, los demás campos de esta página vuelven a sus valores predeterminados.

6. Seleccione el botón de opción Always True o False.
Si se establece en True, este campo activa el anuncio del router. El valor predeterminado es False.
7. En el campo Metric, especifique la métrica de la ruta predeterminada. Los valores válidos van de 0 a 16777214. El valor predeterminado es 0.

8. Seleccione el botón de opción Metric Type External Type 1 o External Type 2.

Establece el tipo de métrica OSPFv3 de la ruta predeterminada. El valor predeterminado es External Type 2.
9. Haga clic en el botón Apply.
La configuración se guarda.

Configurar los ajustes avanzados de OSPFv3

Para configurar los ajustes avanzados de OSPFv3:

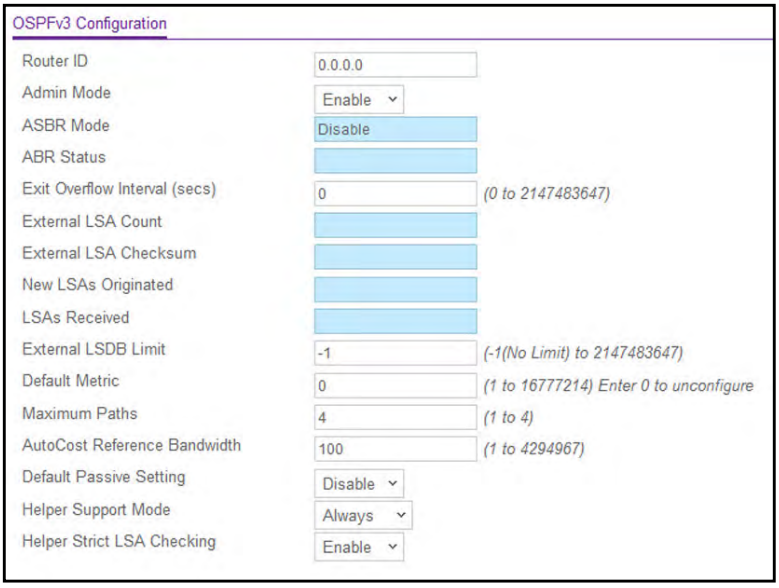
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > OSPFv3 Configuration.



5. Introduzca en Router ID un entero de 32 bits en formato decimal con puntos que identifique de forma única al router dentro del sistema autónomo (AS).

   Para cambiar el ID de router, primero debe deshabilitar OSPFv3. Después de establecer el nuevo ID, debe volver a habilitar OSPFv3 para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.

6. En el campo Admin Mode, seleccione Enable o Disable.

   Si selecciona Enable, OSPFv3 se activa en el switch. El valor predeterminado es Enable. Debe configurar un ID de router antes de que OSPFv3 pueda estar operativo. Para obtener más información, consulte Configurar los ajustes IP de enrutamiento en la página 307.

   Nota: Una vez que OSPFv3 se inicializa en el router, permanece inicializado hasta que router se restablece.

7. En el campo Exit Overflow Interval, especifique el número de segundos que, después de entrar en estado de desbordamiento, el router debe esperar antes de intentar salir de ese estado.

   Como OSPFv3 no puede originar LSA externos no predeterminados en estado de desbordamiento, esto permite que el router vuelva a originar AS-external-LSA no predeterminados. Si introduce un intervalo de salida de 0, el router no sale del estado de desbordamiento hasta que se reinicia. El rango es de 0 a 2,147,483,647 segundos. El valor predeterminado es 0.

Cuando el número de LSA externos no predeterminados supera un límite configurado, el router entra en estado de desbordamiento según se define en RFC 1765.

8. Introduzca External LSDB Limit. Es el número máximo de AS-external-LSA que se pueden almacenar en la base de datos.

Un valor de –1 indica que no hay límite en el número que se puede guardar. El rango válido es de –1 a 2147483647. El valor predeterminado es –1 (sin límite).

9. Use el campo Default Metric para establecer un valor predeterminado para la métrica de las rutas redistribuidas.

Este campo muestra la métrica predeterminada si ya se estableció, o queda vacío si no se configuró. Los valores válidos son de 1 a 16777214. El valor predeterminado es 0 (sin configurar).

10. Use el campo Maximum Paths para configurar el número máximo de rutas que OSPFv3 puede informar para un destino determinado.

Los valores válidos son de 1 a 4.

11. Configure AutoCost Reference Bandwidth para controlar cómo calcula OSPF las métricas predeterminadas de la interfaz.

Los valores válidos son de 1 a 4294967. El valor predeterminado es 100.

12. En Default Passive Setting, seleccione Enable o Disable para configurar el modo pasivo global de todas las interfaces OSPF.

Configurar este campo sobrescribe cualquier ajuste de modo pasivo a nivel de interfaz. OSPF no forma adyacencias en interfaces pasivas, pero sí anuncia las redes conectadas como redes stub.

13. Use Helper Support Mode para configurar cómo actúa la unidad cuando un vecino realiza un reinicio en caliente.

Los valores posibles son:

- Planned. OSPF ayuda a un vecino que se reinicia solo durante eventos planificados.
- Always. OSPF ayuda a un vecino que se reinicia durante todos los eventos de reinicio en caliente planificados y no planificados.
- Disabled. OSPF no actúa como vecino auxiliar.

14. Configure Helper Strict LSA Checking seleccionando Enable o Disable.

Si se habilita, la unidad sale del modo auxiliar cada vez que cambia la topología.

15. Haga clic en el botón Apply.

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 141. Configuración avanzada de OSPFv3

Campo	Descripción
ASBR Mode	Indica si el modo ASBR está habilitado o deshabilitado. Enable indica que el router es un router de borde de sistema autónomo. El router se convierte automáticamente en ASBR cuando se configura para redistribuir rutas aprendidas de otro protocolo.
ABR Status	Sus valores son Enabled o Disabled. Enabled indica que el router es un router de borde de área. Disabled indica que no es un router de borde de área.
External LSA Count	Número de anuncios de estado de enlace (LSA) externos (LS tipo 5) en la base de datos de estado de enlace.
External LSA Checksum	Suma de las sumas de verificación LS de los LSA externos contenidos en la base de datos de estado de enlace. Esta suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar las bases de datos de estado de enlace de dos routers.
New LSAs Originated	En cualquier área OSPFv3, un router origina varios LSA. Cada router origina un router-LSA. Si el router también es el router designado de alguna de las redes del área, origina network-LSA para esas redes. Este valor representa el número de LSA originados por este router.
LSAs Received	Número de LSA recibidos que se determinó que eran nuevas instancias. Este número no incluye las instancias más recientes de LSA autooriginados.

Configurar el área común de OSPFv3

Para configurar un área común de OSPFv3 o devolver un área común de OSPFv3 al estado normal:

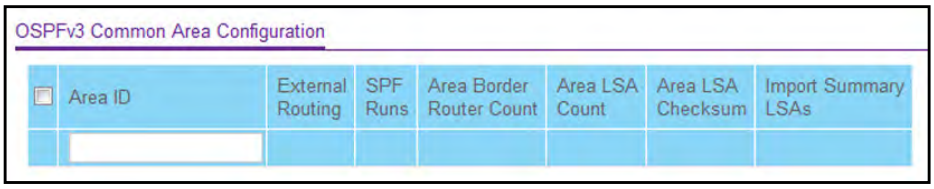
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Common Area Configuration.



5. En el campo Area ID, introduzca el ID de área OSPF.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

6. Realice una de las siguientes acciones:

- Haga clic en el botón Add.

  El área se configura como área común.

- Haga clic en el botón Delete.

  El área vuelve al estado normal.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 142. Configuración avanzada de área común de OSPFv3

Campo	Descripción
External Routing	Definición de las capacidades del router para el área, incluido si los AS-external-LSA se inundan o no hacia el área o a través de ella.
SPF Runs	Número de veces que se calculó la tabla de rutas intraárea con la base de datos de estado de enlace de esta área. Se hace con el algoritmo de Dijkstra.
Area Border Router Count	Número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	Número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
Area LSA Checksum	Suma sin signo de 32 bits de las sumas de verificación LSA de los anuncios de estado de enlace contenidos en la base de datos de estado de enlace de esta área. Esta suma excluye los anuncios de estado de enlace externos (LSA tipo 5). La suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar las bases de datos de estado de enlace de dos routers.
Import Summary LSAs	Indica si la importación de LSA de resumen a esta área está habilitada o deshabilitada.

Configurar un área stub de OSPFv3

Para configurar el área stub de OSPFv3:

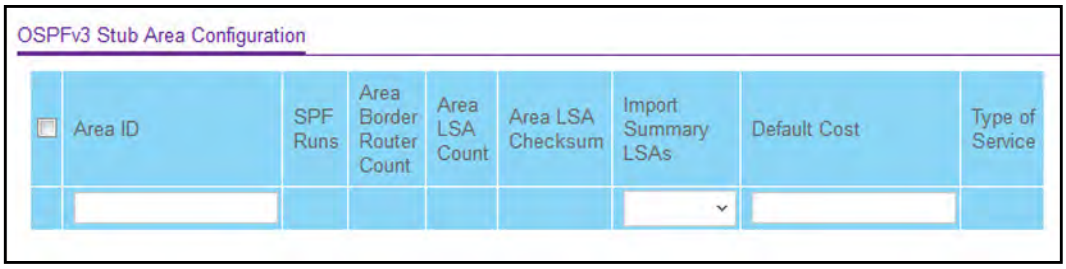
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Stub Area Configuration.



5. En el campo Area ID, introduzca el ID de área OSPF.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

6. En la lista Import Summary LSAs, seleccione Enable o Disable.

Si selecciona Enable, los LSA de resumen se importan a las áreas. El valor predeterminado es Enable.

7. En el campo Default Cost, introduzca el valor de métrica que se aplicará a la ruta predeterminada anunciada en el área stub.

Los valores válidos van de 1 a 16,777,215. Este valor solo se aplica a las áreas stub.
8. Haga clic en el botón Add.
El área se configura como área stub.
9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 143. Configuración avanzada de área stub de OSPFv3

Campo	Descripción
SPF Runs	Número de veces que se calculó la tabla de rutas intraárea con la base de datos de estado de enlace de esta área. Se hace con el algoritmo de Dijkstra.
Area Border Router Count	Número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	Número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.

Tabla 143. Configuración avanzada de área stub de OSPFv3 (continuación)

Campo	Descripción
Area LSA Checksum	Suma sin signo de 32 bits de las sumas de verificación LSA de los anuncios de estado de enlace contenidos en la base de datos de estado de enlace de esta área. Esta suma excluye los anuncios de estado de enlace externos (LSA tipo 5). La suma puede usarse para determinar si hubo un cambio en la base de datos de estado de enlace de un router y para comparar las bases de datos de estado de enlace de dos routers.
Type of Service	Este campo es el ToS normal asociado con la métrica stub.

Configurar el área NSSA de OSPFv3

Para configurar el área NSSA de OSPFv3:

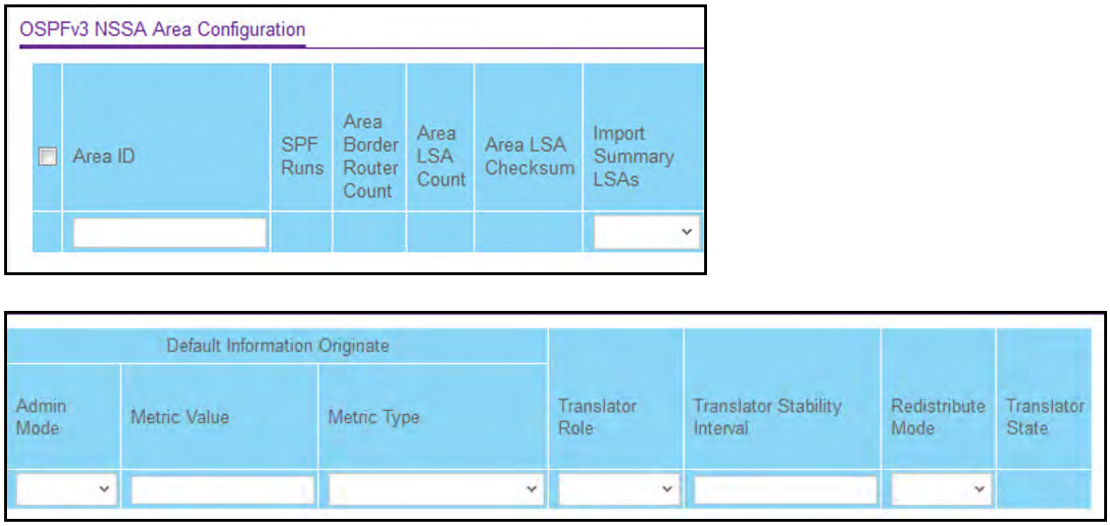
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > NSSA Area Configuration.



5. En el campo Area ID, introduzca el ID de área OSPF.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.

6. Configure Import Summary LSAs seleccionando Enable o Disable en la lista.

Si selecciona Enable, los LSA de resumen se importan a las áreas stub.

7. Configure Default Information Originate.

Esta opción le permite anunciar una ruta predeterminada en la NSSA cuando la importación de LSA de resumen está deshabilitada.

a. En la lista Admin Mode, seleccione Enable o Disable para Default Information Originate.

b. En el campo Metric Value, establezca el valor de métrica predeterminado para Default Information Originate. El rango de valores es de 1 a 16777214.
c. En el campo Metric Type, seleccione el tipo de la métrica especificada en el campo Metric Value.

Las opciones son las siguientes:

- Comparable Cost. Métricas externas tipo 1 comparables con la métrica OSPF.
- Non-comparable Cost. Métricas externas tipo 2 que se consideran mayores que el costo de la métrica OSPF.

8. Seleccione el rol de traductor (Translator Role) de la NSSA.

Las opciones son las siguientes:
a. Always. Hace que el router asuma el rol de traductor en cuanto se convierte en router de borde.
b. Candidate. Hace que el router participe en el proceso de elección del traductor cuando alcanza el estado de router de borde.

9. En el campo Translator Stability Interval, configure el traductor de la NSSA.

El valor es el período durante el cual un traductor elegido sigue realizando sus funciones después de determinar que otro router lo destituyó como traductor. El rango válido es de 0 a 3600.

10. En el campo Redistribute Mode, seleccione Enable o Disable.

Esto configura el ABR de la NSSA para que las rutas externas aprendidas se redistribuyan a la NSSA.

11. Haga clic en el botón Add.
El área se configura como área NSSA.
12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 144. Configuración avanzada de área NSSA de OSPFv3

Campo	Descripción
SPF Runs	Número de veces que se calculó la tabla de rutas intraárea con la base de datos de estado de enlace de esta área. Normalmente se hace con el algoritmo de Dijkstra.
Area Border Router Count	El número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.

Tabla 144. Configuración avanzada de área NSSA de OSPFv3 (continuación)

Campo	Descripción
Area LSA Count	El número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
Area LSA Checksum	La suma sin signo de 32 bits de las sumas de verificación de los LSA contenidos en la base de datos de estado de enlace de esta área. Esta suma excluye los anuncios de estado de enlace externos (LSA tipo 5). La suma permite determinar si hubo un cambio en la base de datos de estado de enlace de un router y comparar la base de datos de estado de enlace de dos routers.
Translator State	Indica si el router de borde NSSA traduce el tipo 7 al tipo 5 y cómo lo hace. Los valores posibles son los siguientes: • Enabled. El rol de traductor del router de borde NSSA se estableció en always. • Elected. El router de borde NSSA candidato está traduciendo LSA de tipo 7 a tipo 5. • Disabled. El router de borde NSSA candidato NO está traduciendo LSA de tipo 7 a tipo 5.

Configurar el rango de área de OSPFv3

Para configurar el rango de área de OSPFv3:

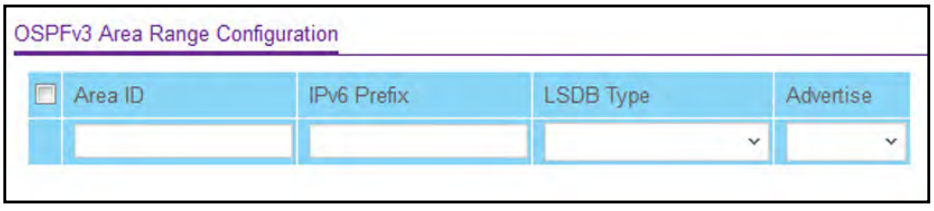
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Area Range Configuration.



5. Introduzca el ID de área de OSPFv3 (Area ID).
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta una interfaz de router.
6. Introduzca en IPv6 Prefix el prefijo IPv6 del rango de direcciones del área seleccionada.

7. En la lista del campo LSDB Type, seleccione el tipo de anuncio de enlace asociado con el área y el rango de direcciones especificados.

   Las opciones son Network Summary o NSSA External. El tipo predeterminado es Network Summary.

8. En el campo Advertise, seleccione la opción Enable o Disable.

   Si selecciona Enable, el rango de direcciones se anuncia fuera del área mediante un LSA de resumen de red. El valor predeterminado es Enable.

9. Haga clic en el botón Add.
El nuevo rango de direcciones se agrega al switch.

Configurar la interfaz OSPFv3

Para configurar la interfaz OSPFv3:

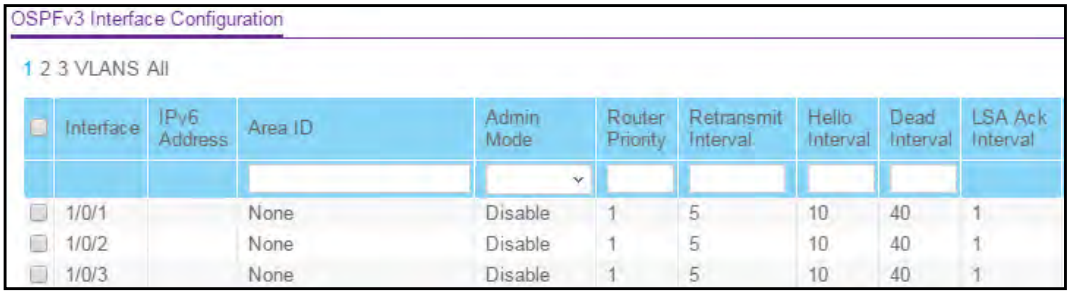
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

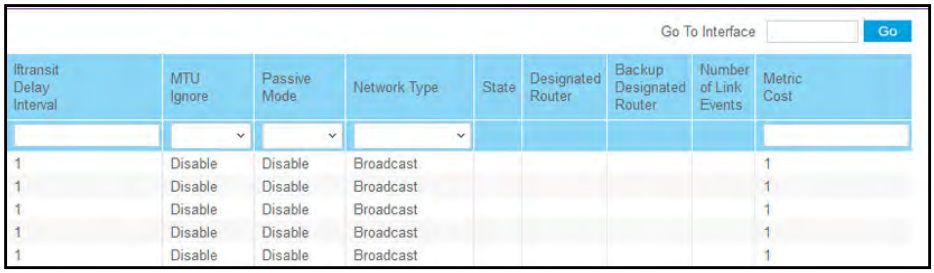
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Interface Configuration.





5. 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, seleccione la casilla de la interfaz que desea configurar.

6. En el campo Area ID, introduzca el entero de 32 bits en formato decimal con puntos que identifica de forma única el área OSPFv3 a la que se conecta la interfaz de router seleccionada.

Si asigna un ID de área que no existe, el área se crea con los valores predeterminados.

7. Configure Admin Mode seleccionando la opción Enable o Disable de la lista.

   El valor predeterminado es Disable. Puede configurar los parámetros de OSPFv3 sin habilitar el modo administrativo de OSPFv3, pero la configuración no surte efecto hasta que lo habilite. La siguiente información solo se muestra si el modo administrativo está habilitado:

   - Estado
   - Router designado
   - Router designado de respaldo
   - Número de eventos de enlace
   - Intervalo de LSA Ack
   - Costo de métrica

   Para que OSPFv3 funcione completamente, debe introducir un prefijo/longitud de prefijo IPv6 válido. Esto puede hacerse con el comando CLI IPv6 address.

   Nota: Una vez que OSPFv3 se inicializa en el router, permanece inicializado hasta que router se restablece.

8. Configure Router Priority introduciendo la prioridad OSPFv3 de la interfaz seleccionada.

   La prioridad de una interfaz se especifica como un entero de 0 a 255. El valor predeterminado es 1, que es la prioridad de router más alta. Un valor de 0 indica que el router no puede convertirse en el router designado de esta red.

9. Configure Retransmit Interval introduciendo el intervalo de retransmisión OSPFv3 de la interfaz especificada.

   Es el número de segundos entre anuncios de estado de enlace para las adyacencias de esta interfaz de router. Este valor también se usa al retransmitir descripciones de base de datos y paquetes de solicitud de estado de enlace. Los valores válidos van de 0 a 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

10. Configure Hello Interval introduciendo el intervalo de hello OSPFv3 de la interfaz especificada en segundos.

    Este parámetro debe ser igual en todos los routers conectados a una red. Los valores válidos van de 1 a 65,535. El valor predeterminado es 10 segundos.

11. Introduzca el OSPFv3 Dead Interval de la interfaz especificada en segundos.

Especifica cuánto tiempo espera un router a recibir los paquetes hello de un router vecino antes de declarar que ese router está inactivo. Este parámetro debe ser igual en todos los routers conectados a una red. Este valor es un múltiplo del intervalo de hello (por ejemplo, 4). Los valores válidos van de 1 a 65,535. El valor predeterminado es 40 segundos.

12. En el campo Iftransit Delay Interval, introduzca el retardo de tránsito OSPFv3 de la interfaz especificada.

    Especifica el número estimado de segundos que tarda en transmitirse un paquete de actualización de estado de enlace por la interfaz seleccionada. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

13. Configure MTU Ignore seleccionando Enable o Disable en la lista.

    MTU Ignore deshabilita la detección de discrepancias de MTU de OSPF al recibir paquetes de descripción de base de datos. El valor predeterminado es Disable (la detección de discrepancias de MTU está habilitada).

14. Configure Passive Mode seleccionando Enable o Disable en la lista.

    Haga pasiva una interfaz para evitar que OSPF forme una adyacencia en ella. OSPF anuncia las redes conectadas a interfaces pasivas como redes stub. De forma predeterminada, las interfaces no son pasivas, es decir, el modo pasivo predeterminado es Disable.

15. Establezca el OSPFv3 Network Type de la interfaz seleccionando Broadcast o Point-to-Point Mode en la lista.

    OSPFv3 selecciona un router designado y origina LSA de red solo para redes broadcast. En un enlace punto a punto no puede haber más de dos routers OSPFv3. El tipo de red predeterminado para interfaces Ethernet es Broadcast.

16. En el campo Metric Cost, introduzca el valor del costo de tipo de servicio (TOS).

    OSPF usa este valor para calcular las rutas más cortas. El rango es de 1 a 65,535. El valor predeterminado es 1. Metric Cost solo se puede configurar si OSPFv3 está inicializado en la interfaz.

17. Haga clic en el botón Apply.

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 145. Configuración avanzada de interfaz OSPFv3

Campo	Descripción
IPv6 Address	La dirección IPv6 de la interfaz.
LSA Ack Interval (secs)	El número de segundos entre transmisiones de paquetes de confirmación de LSA, que debe ser menor que el intervalo de retransmisión.

Tabla 145. Configuración avanzada de interfaz OSPFv3 (continuación)

Campo	Descripción
State	El estado actual de la interfaz de router seleccionada. Puede ser uno de los siguientes: • Down. Es el estado inicial de la interfaz. Los protocolos de nivel inferior indican que la interfaz no se puede usar. Los parámetros de la interfaz tienen sus valores iniciales. Todos los temporizadores de la interfaz están deshabilitados y no hay adyacencias asociadas a la interfaz. • Loopback. La interfaz del router con la red está en loopback, ya sea en el hardware o en el software. La interfaz no está disponible para el tráfico de datos normal. Sin embargo, es posible que desee obtener información sobre la calidad de esta interfaz, ya sea enviándole pings ICMP o mediante algo como una prueba de errores de bits. Por ello, los paquetes IP aún pueden dirigirse a una interfaz en estado loopback. Para facilitarlo, estas interfaces se anuncian en los LSA de router como rutas de host únicas, cuyo destino es la dirección IP de la interfaz. • Waiting. El router intenta determinar la identidad del router designado de respaldo de la red supervisando los paquetes hello recibidos. El router no puede elegir un router designado de respaldo ni un router designado hasta que salga del estado waiting. Esto evita cambios innecesarios del router designado de respaldo. • Designated Router. Este router es el router designado de la red conectada. Se establecen adyacencias con todos los demás routers conectados a la red. El router también debe originar un LSA de red para el nodo de red. El LSA de red contiene enlaces a todos los routers (incluido el router designado) conectados a la red. • Backup Designated Router. Este router es el router designado de respaldo de la red conectada. Se promueve a router designado si falla el router designado actual. El router establece adyacencias con todos los demás routers conectados a la red. El router designado de respaldo realiza funciones ligeramente distintas durante el procedimiento de inundación de LSA, en comparación con el router designado. • Other Designated Router. La interfaz está conectada a una red broadcast o NBMA en la que se seleccionaron otros routers como router designado o router designado de respaldo. El router intenta formar adyacencias tanto con el router designado como con el router designado de respaldo. Nota: El estado solo se muestra si el modo administrativo de OSPFv3 está habilitado.
Designated Router	La identidad del router designado de esta red, desde el punto de vista del router anunciante. El router designado se identifica aquí por su ID de router. El valor 0.0.0.0 significa que no hay router designado. Nota: Este campo solo se muestra si el modo administrativo de OSPFv3 está habilitado.
Backup Designated Router	La identidad del router designado de respaldo de esta red, desde el punto de vista del router anunciante. El router designado de respaldo se identifica aquí por su ID de router. Se establece en 0.0.0.0 si no hay router designado de respaldo. Nota: Este campo solo se muestra si el modo administrativo de OSPFv3 está habilitado.
Number of Link Events	Es el número de veces que la interfaz OSPF especificada cambió de estado. Nota: Este campo solo se muestra si el modo administrativo de OSPFv3 está habilitado.

Ver y borrar las estadísticas de interfaz OSPFv3

Puede ver y borrar las estadísticas de la interfaz seleccionada. La información solo se muestra si OSPFv3 está habilitado.

Para ver y borrar las estadísticas de interfaz OSPFv3:

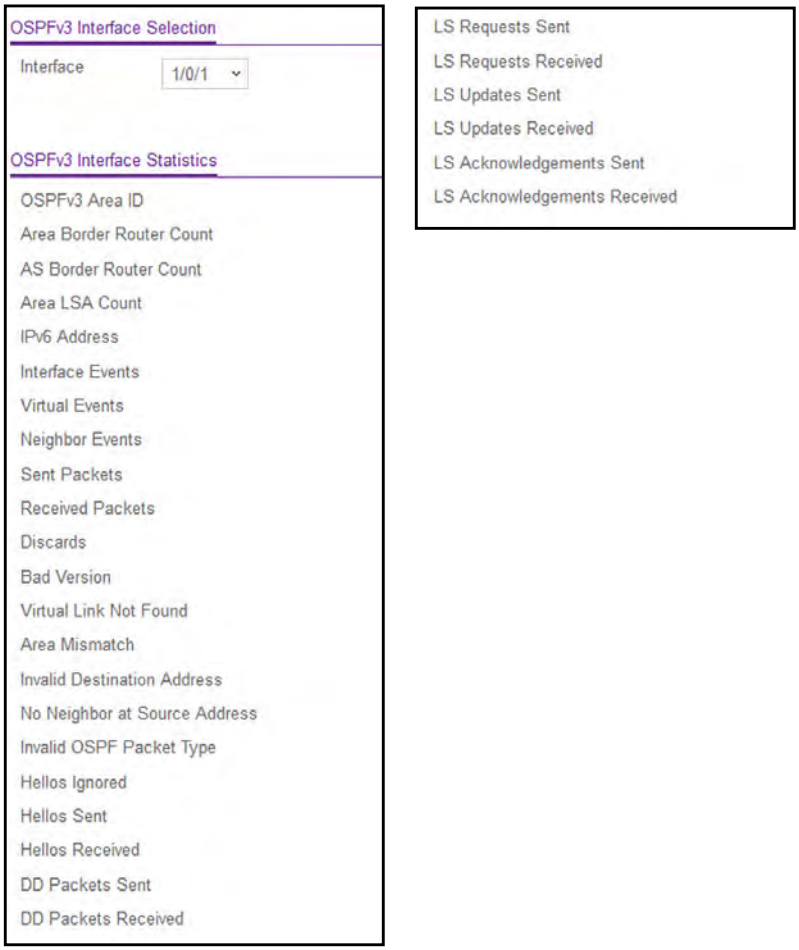
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing > OSPFv3 > Advanced > Interface Statistics.**



5. En el área OSPFv3 Interface Selection de la página, en la lista Interface, seleccione la interfaz.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh).
7. Para borrar todas las estadísticas de la interfaz OSPFv3, haga clic en el botón Clear.

La siguiente tabla describe los datos no configurables de OSPF Interface Statistics que se muestran.

Tabla 146. Estadísticas avanzadas de interfaz OSPFv3

Campo	Descripción
OSPFv3 Area ID	El área OSPFv3 a la que pertenece la interfaz de router seleccionada. Un ID de área OSPFv3 es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que se conecta la interfaz.
Area Border Router Count	El número total de routers de borde de área accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
AS Border Router Count	El número total de routers de borde de sistema autónomo accesibles dentro de esta área. Inicialmente es cero y se calcula en cada pasada SPF.
Area LSA Count	Número total de anuncios de estado de enlace en la base de datos de estado de enlace de esta área, excluidos los LSA externos de AS.
IPv6 Address	La dirección IPv6 de la interfaz.
Interface Events	El número de veces que la interfaz OSPFv3 especificada cambió de estado o se produjo un error.
Virtual Events	El número de cambios de estado o errores ocurridos en este enlace virtual.
Neighbor Events	El número de veces que esta relación de vecindad cambió de estado u ocurrió un error.
Sent Packets	El número de paquetes OSPFv3 transmitidos en la interfaz.
Received Packets	El número de paquetes OSPFv3 válidos recibidos en la interfaz.
Discards	El número de paquetes OSPFv3 recibidos que se descartaron por un error en el paquete o un error al procesarlo.
Bad Version	El número de paquetes OSPFv3 recibidos cuyo campo de versión en el encabezado OSPFv3 no coincide con la versión del proceso OSPFv3 que maneja el paquete.
Virtual Link Not Found	El número de paquetes OSPFv3 recibidos descartados cuando la interfaz de entrada está en un área que no es backbone y el encabezado OSPFv3 identifica el paquete como perteneciente al backbone, pero OSPFv3 no tiene un enlace virtual con el remitente del paquete.
Area Mismatch	El número de paquetes OSPFv3 descartados porque el ID de área del encabezado OSPFv3 no es el ID de área configurado en la interfaz de entrada.
Invalid Destination Address	El número de paquetes OSPFv3 descartados porque la dirección IP de destino del paquete no es la dirección de la interfaz de entrada ni la dirección multicast AllDrRouters o AllSpfRouters.
No Neighbor at Source Address	El número de paquetes OSPFv3 descartados porque el remitente no es un vecino existente o su dirección IP no coincide con la dirección IP registrada previamente para ese vecino.

Tabla 146. Estadísticas avanzadas de interfaz OSPFv3 (continuación)

Campo	Descripción
Invalid OSPF Packet Type	El número de paquetes OSPFv3 descartados porque el campo de tipo de paquete del encabezado OSPFv3 no es un tipo conocido.
Hellos Ignored	El número de paquetes hello recibidos de vecinos nuevos que este router ignoró al alcanzarse el límite de vecinos en una interfaz o en el sistema en general.
Hellos Sent	El número de paquetes hello enviados por este router en esta interfaz.
Hellos Received	El número de paquetes hello recibidos por este router en esta interfaz.
DD Packets Sent	El número de paquetes de descripción de base de datos enviados por este router en esta interfaz.
DD Packets Received	El número de paquetes de descripción de base de datos recibidos por este router en esta interfaz.
LS Requests Sent	El número de solicitudes LS enviadas por este router en esta interfaz.
LS Requests Received	El número de solicitudes LS recibidas por este router en esta interfaz.
LS Updates Sent	El número de actualizaciones LS enviadas por este router en esta interfaz.
LS Updates Received	El número de actualizaciones LS recibidas por este router en esta interfaz.
LS Acknowledgements Sent	El número de acuses de recibo LS enviados por este router en esta interfaz.
LS Acknowledgements Received	El número de acuses de recibo LS recibidos por este router en esta interfaz.

Ver la tabla de vecinos OSPFv3 y borrar los vecinos OSPFv3

Esta página muestra la tabla de vecinos OSPFv3. Esta información solo se muestra si OSPFv3 está habilitado y existe al menos una interfaz con OSPFv3 habilitado que tenga un vecino válido. También puede borrar los vecinos OSPFv3.

Para ver la tabla de vecinos OSPFv3 y borrar los vecinos OSPFv3:

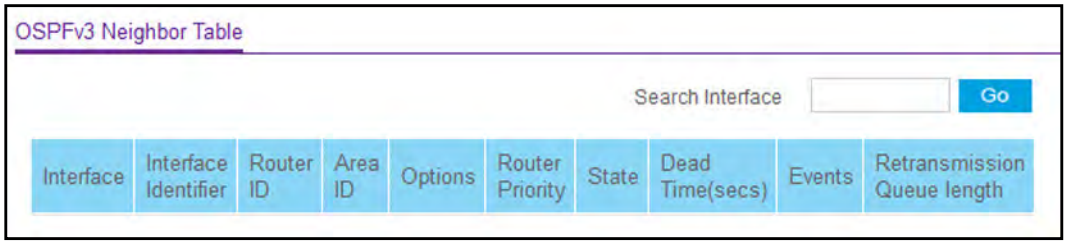
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Neighbor Table.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar todos los vecinos de la tabla, haga clic en el botón Clear.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 147. Tabla avanzada de vecinos OSPFv3

Campo	Descripción
Interface	La interfaz cuyos datos se mostrarán o configurarán. La ranura 0 es la unidad base.
Interface Identifier	El ID de interfaz que el vecino anuncia en sus paquetes hello en este enlace.
Router ID	Un entero de 32 bits en formato decimal con puntos que representa el ID de router del vecino en la interfaz seleccionada.
Area ID	Un entero de 32 bits en formato decimal con puntos que representa el área común con el vecino seleccionado.
Options	Una máscara de bits correspondiente al campo de opciones del vecino.
Router Priority	La prioridad de este vecino en el algoritmo de elección del router designado. Un valor de 0 significa que el vecino no puede convertirse en el router designado en esta red.
State	El estado de la relación con este vecino.
Dead Time	El tiempo, en segundos, desde que se recibió el último hello de los vecinos adyacentes. Se establece en 0 para vecinos en un estado menor o igual a Init.
Events	El número de veces que esta relación de vecindad cambió de estado u ocurrió un error.
Retransmission Queue Length	Un entero que representa la longitud actual de la cola de retransmisión del vecino seleccionado.

Ver la base de datos de estado de enlace de OSPFv3

Para ver la base de datos de estado de enlace OSPF:

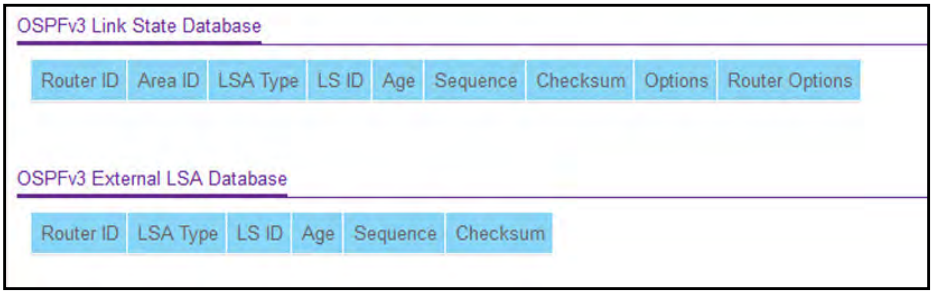
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing > OSPFv3 > Advanced > Link State Database.**



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 148. Base de datos avanzada de estado de enlace de OSPFv3

Campo	Descripción
Router ID	El entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS). El ID de router se establece en la página OSPFv3 Configuration. Para cambiar el ID de router, primero debe deshabilitar OSPFv3. Después de establecer el nuevo ID, debe volver a habilitar OSPFv3 para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.
Area ID	El ID de un área OSPFv3 a la que está conectada una de las interfaces del router. Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a la que está conectada una interfaz.

Tabla 148. Base de datos avanzada de estado de enlace de OSPFv3 (continuación)

Campo	Descripción
LSA Type	El formato y la función del anuncio de estado de enlace. LSA Type es uno de los siguientes: • Router LSA. Un router puede originar uno o más LSA de router para un área determinada. Cada LSA de router originado en un área describe los estados de todas las interfaces del router hacia el área. • Network LSA. El router designado origina un LSA de red para cada enlace con dos o más routers conectados. Enumera todos los routers conectados al enlace. • Inter-Area Router LSA. Este tipo describe un prefijo externo al área, pero interno al sistema autónomo. Lo origina un router de borde de área. • AS-External LSA. Este tipo de LSA describe una ruta a un prefijo externo al sistema autónomo y lo origina un router de borde del sistema autónomo. • Link LSA. Un router origina un Link LSA distinto para cada enlace conectado. Proporciona la dirección link local del router a los routers conectados al enlace y les informa de una lista de prefijos IPv6 que se asocian con el enlace. • Intra-Area-Prefix LSA. El router designado de un enlace origina uno o más LSA intra-area-prefix para anunciar los prefijos del enlace en toda el área. Un router puede originar varios LSA intra-area-prefix para un área determinada para anunciar sus propios prefijos y los de sus enlaces stub conectados.
LS ID	El ID de estado de enlace identifica la parte del dominio de enrutamiento que describe el anuncio. El valor de LS ID depende del tipo LS del anuncio.
Age	El tiempo, en segundos, desde que se originó el anuncio de estado de enlace.
Sequence	El campo de número de secuencia es un entero de 32 bits con signo. Se usa para detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.
Checksum	La suma de verificación se usa para detectar datos dañados en un anuncio. Este daño puede ocurrir mientras el anuncio se inunda o mientras está almacenado en la memoria de un router. Este campo es la suma de verificación de todo el contenido del anuncio, excepto el campo LS age.
Options	El campo Options del encabezado del anuncio de estado de enlace indica qué capacidades opcionales están asociadas con el anuncio. Las opciones son las siguientes: • Q. Habilita la compatibilidad con ingeniería de tráfico QoS. • E. Describe la forma en que se inundan los LSA AS-external. • MC. Describe la forma en que se reenvían los datagramas IP multicast según las especificaciones estándar. • O. Describe si se admiten LSA opacos. • V. Describe si las extensiones OSPF++ para VPN/COS son compatibles.
Router Options	Las opciones específicas del router.

La siguiente tabla describe la información no configurable que se muestra en la tabla External Link State Database (LSDB).

Tabla 149. Tabla avanzada de base de datos de estado de enlace externo de OSPFv3

Campo	Descripción
Router ID	El entero de 32 bits en formato decimal con puntos que identifica de forma única al router dentro del sistema autónomo (AS). El ID de router se establece en la página OSPFv3 Configuration. Para cambiar el ID de router, primero debe deshabilitar OSPFv3. Después de establecer el nuevo ID, debe volver a habilitar OSPFv3 para que el cambio surta efecto. El valor predeterminado es 0.0.0.0, aunque no es un ID de router válido.
LSA Type	El formato y la función del anuncio de estado de enlace. LSA Type es uno de los siguientes: • Router LSA. Un router puede originar uno o más LSA de router para un área determinada. Cada LSA de router originado en un área describe los estados de todas las interfaces del router hacia el área. • Network LSA. El router designado origina un LSA de red para cada enlace con dos o más routers conectados. Enumera todos los routers conectados al enlace. • Inter-Area Router LSA. Este tipo describe un prefijo externo al área, pero interno al sistema autónomo. Lo origina un router de borde de área. • AS-External LSA. Este tipo de LSA describe una ruta a un prefijo externo al sistema autónomo y lo origina un router de borde del sistema autónomo. • Link LSA. Un router origina un link LSA distinto para cada enlace conectado. Proporciona la dirección link local del router a los routers conectados al enlace y les informa de una lista de prefijos IPv6 que se asocian con el enlace. • Intra-Area-Prefix LSA. El router designado de un enlace origina uno o más LSA intraarea-prefix para anunciar los prefijos del enlace en toda el área. Un router puede originar varios LSA intra-area-prefix para un área determinada para anunciar sus propios prefijos y los de sus enlaces stub conectados.
LS ID	El ID de estado de enlace identifica la parte del dominio de enrutamiento que describe el anuncio. El valor de LS ID depende del tipo LS del anuncio.
Age	El tiempo, en segundos, desde que se originó el anuncio de estado de enlace.
Sequence	El campo de número de secuencia es un entero de 32 bits con signo. Se usa para detectar anuncios de estado de enlace antiguos y duplicados. Cuanto mayor es el número de secuencia, más reciente es el anuncio.
Checksum	La suma de verificación se usa para detectar datos dañados en un anuncio. Este daño puede ocurrir mientras el anuncio se inunda o mientras está almacenado en la memoria de un router. Este campo es la suma de verificación de todo el contenido del anuncio, excepto el campo LS age.

Configurar el enlace virtual OSPFv3

Para configurar el enlace virtual OSPFv3:

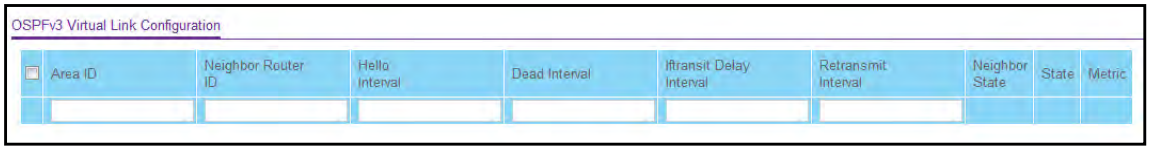
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Virtual Link Configuration.



5. Introduzca el Area ID del área OSPF.
Un ID de área es un entero de 32 bits en formato decimal con puntos que identifica de forma única el área a

   a la que se conecta una interfaz de router. Los enlaces virtuales pueden configurarse entre cualquier par de routers de borde de área con interfaces hacia un área común (que no sea backbone).

6. Configure el valor de Neighbor Router ID escribiendo la parte del vecino de la especificación del enlace virtual.

   Se pueden configurar enlaces virtuales entre cualquier par de routers de borde de área con interfaces en un área común (que no sea backbone).

7. En el campo Hello Interval, introduzca el intervalo de hello OSPFv3 de la interfaz especificada en segundos.

   Este parámetro debe ser igual en todos los routers conectados a una red. Los valores válidos van de 1 a 65,535. El valor predeterminado es 10 segundos.

8. En el campo Dead Interval, introduzca el intervalo dead OSPFv3 de la interfaz especificada en segundos.

   Especifica cuánto tiempo espera un router a recibir los paquetes hello de un router vecino antes de declarar que ese router está inactivo. Este parámetro debe ser igual en todos los routers conectados a una red. Este valor es un múltiplo del intervalo de hello (por ejemplo, 4). Los valores válidos van de 1 a 65,535. El valor predeterminado es 40.

9. En el campo Iftransit Delay Interval, introduzca el retardo de tránsito OSPFv3 de la interfaz especificada.

   Especifica el número estimado de segundos que tarda en transmitirse un paquete de actualización de estado de enlace por la interfaz seleccionada. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 1 segundo.

10. En el campo Retransmit Interval, introduzca el intervalo de retransmisión OSPFv3 de la interfaz especificada.

    Es el número de segundos entre anuncios de estado de enlace para las adyacencias de esta interfaz de router. Este valor también se usa al retransmitir descripciones de base de datos y paquetes de solicitud de estado de enlace. Los valores válidos van de 1 a 3600 segundos (1 hora). El valor predeterminado es 5 segundos.

11. Haga clic en el botón Add
El nuevo enlace virtual se agrega al switch.
12. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 150. Configuración avanzada de enlace virtual OSPFv3

Campo	Descripción
Neighbor State	El estado de la relación con el vecino virtual. El estado de la interfaz OSPFv3 puede ser cualquiera de estos valores: • Down. Es el estado inicial de la interfaz. Los protocolos de nivel inferior indicaron que la interfaz no se puede usar. Los parámetros de la interfaz tienen sus valores iniciales. Todos los temporizadores de la interfaz están deshabilitados y no hay adyacencias asociadas a la interfaz. • Waiting. El router intenta determinar la identidad del router designado (de respaldo) supervisando los paquetes hello recibidos. El router no puede elegir un router designado de respaldo ni un router designado hasta que salga del estado waiting. Esto evita cambios innecesarios del router designado (de respaldo). • Point-to-Point. La interfaz está operativa y conectada al enlace virtual. Al entrar en este estado, el router intenta formar una adyacencia con el router vecino. La interfaz envía paquetes hello al vecino cada intervalo de hello en segundos. • Designated Router. Este router es el router designado de la red conectada. Se establecen adyacencias con todos los demás routers conectados a la red. El router también debe originar un LSA de red para el nodo de red. El LSA de red contiene enlaces a todos los routers (incluido el router designado) conectados a la red. • Backup Designated Router. Este router es el router designado de respaldo de la red conectada. Se promueve a router designado si falla el router designado actual. El router establece adyacencias con todos los demás routers conectados a la red. El router designado de respaldo realiza funciones ligeramente distintas durante el procedimiento de inundación, en comparación con el router designado. • Other Designated Router. La interfaz está conectada a una red broadcast o NBMA en la que se seleccionaron otros routers como router designado y router designado de respaldo. El router intenta formar adyacencias tanto con el router designado como con el router designado de respaldo.

Tabla 150. Configuración avanzada de enlaces virtuales OSPFv3 (continuación)

Campo	Descripción
State	El estado de la interfaz. Toma uno de los siguientes valores: • Down. Es el estado inicial de la interfaz. Los protocolos de nivel inferior indicaron que la interfaz no se puede usar. Los parámetros de la interfaz tienen sus valores iniciales. Todos los temporizadores de la interfaz están deshabilitados y no hay adyacencias asociadas a la interfaz. • Waiting. El router intenta determinar la identidad del router designado de respaldo supervisando los paquetes hello recibidos. El router no puede elegir un router designado de respaldo ni un router designado hasta salir del estado de espera. Esto evita cambios innecesarios del router designado de respaldo. • Point-to-Point. La interfaz está operativa y conectada al enlace virtual. Al entrar en este estado, el router intenta formar una adyacencia con el router vecino. Se envían paquetes hello al vecino cada hello interval segundos. • Designated Router. Este router es el router designado de la red conectada. Se establecen adyacencias con todos los demás routers conectados a la red. El router también debe originar un network-LSA para el nodo de red. El network-LSA contiene enlaces a todos los routers (incluido el router designado) conectados a la red. • Backup Designated Router. Este router es el router designado de respaldo de la red conectada. Se convierte en router designado si falla el router designado actual. El router establece adyacencias con todos los demás routers conectados a la red. El router designado de respaldo realiza funciones ligeramente distintas durante el procedimiento de inundación, en comparación con el router designado. • Other Designated Router. La interfaz está conectada a una red de difusión o NBMA en la que se seleccionaron otros routers como router designado y router designado de respaldo. El router intenta formar adyacencias con el router designado y con el router designado de respaldo.
Metric	El valor de métrica que usa el enlace virtual.

Configurar la redistribución de rutas OSPFv3

Puede configurar los parámetros de redistribución de rutas OSPFv3. Los valores permitidos para cada campo se muestran junto al campo. Si se introducen valores no válidos, aparece un mensaje de alerta con la lista de todos los valores válidos.

Para configurar la redistribución de rutas OSPFv3:

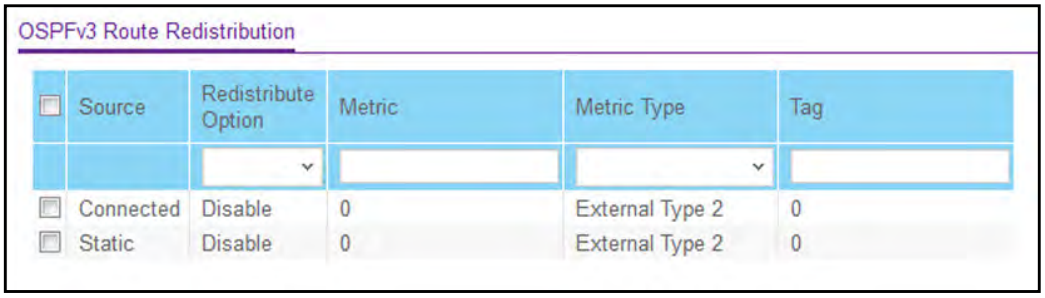
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > Route Redistribution.



5. En el menú Source, seleccione entre las rutas de origen disponibles que no se hayan configurado previamente para redistribución por OSPFv3. Los valores válidos son:
   - Connected
   - Static
6. En la lista Redistribute Option, seleccione Enable o Disable para la redistribución del protocolo de origen seleccionado.
7. Establezca en Metric el valor que se usará como métrica de las rutas redistribuidas.

   Este campo muestra la métrica si el origen se configuró previamente; de lo contrario, la etiqueta es 0 y se puede modificar. Los valores válidos son de 0 a 16777214.

8. En la lista Metric Type, seleccione el tipo de métrica OSPFv3 de las rutas redistribuidas.
9. Establezca el campo Tag de las rutas redistribuidas.

   Este campo muestra la etiqueta si el origen estaba preconfigurado; de lo contrario, la etiqueta es 0 y puede modificarse. Los valores válidos son de 0 a 4294967295.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Ver el resumen de NSF OSPFv3

Puede ver el resumen de NSF OSPFv3. Los valores permitidos de cada campo se muestran junto al campo. Si introduce un valor no válido, aparece un mensaje de alerta con la lista de todos los valores válidos.

Para ver el resumen de NSF OSPF:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > OSPFv3 > Advanced > NSF OSPFv3 Summary.



5. En la lista Support mode, seleccione uno de los siguientes valores:
   - Always. OSPF realiza un reinicio ordenado en todos los eventos de reinicio en caliente planificados y no planificados.
   - Disabled. Impide que OSPF realice reinicios ordenados.
   - Planned. OSPF realiza un reinicio ordenado solo cuando el reinicio está planificado (por ejemplo, debido a un comando initiate failover).

   El valor predeterminado es Disabled. Este ajuste configura cómo realiza la unidad los reinicios ordenados.

6. Configure el Restart Interval.

Los valores válidos son de 0 a 1800 segundos. El valor predeterminado es 120 segundos.
7. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 151. Resumen avanzado de NSF OSPFv3

Campo	Descripción
Restart Status	El estado de reinicio de la función auxiliar de OSPF. Los valores posibles son los siguientes: • Not Restarting • Planned Restart • Unplanned Restart
Antigüedad del reinicio (segundos)	Tiempo transcurrido desde el último reinicio.

Tabla 151. Resumen avanzado de NSF OSPFv3 (continuación)

Campo	Descripción
Restart Exit Reason	Muestra cómo se inició por última vez la unidad maestra del switch. Los valores posibles son: • Not Attempted. No se intentó un reinicio ordenado. • In Progress. El reinicio está en curso. • Completed. El reinicio ordenado anterior se completó correctamente. • Timed Out. El reinicio ordenado anterior agotó el tiempo de espera. • Topology Changed. El reinicio ordenado anterior terminó prematuramente debido a un cambio de topología.

7

7Configurar el enrutamiento multicast

Este capítulo trata los siguientes temas:

- Descripción general de multicast
- Configurar los ajustes de IGMP multicast
- Configurar los ajustes de PIM
- Configurar rutas multicast estáticas
- Configurar el límite administrativo multicast
- Configurar los ajustes de multicast IPv6

Descripción general de multicast

Multicast es ideal para tráfico de video y audio que requiere control de paquetes multicast para un funcionamiento óptimo. Multicast incluye compatibilidad con IGMPv2 e IGMPv3. 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 IP de destino. Aunque esto puede lograrse enviando mensajes unicast (punto a punto) a cada uno

de los hosts de destino, la multidifusión es el método más conveniente 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 IP 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.

Ver la tabla Mroute multicast

Para ver la tabla de rutas multicast (Mroute):

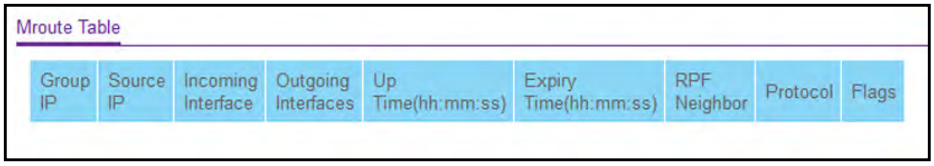
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > Multicast > Mroute Table.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 152. Tabla Mroute multicast

Campo	Descripción
Group IP	La dirección IP del grupo de destino.
Source IP	La dirección IP del origen del paquete multicast, que se combina con la IP del grupo para identificar por completo una ruta de la tabla Mroute.

Tabla 152. Tabla Mroute multicast (continuación)

Campo	Descripción
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 IP del vecino de reenvío por ruta inversa (RPF).
Protocol	El protocolo de enrutamiento multicast que creó esta entrada. Los valores posibles son: • PIM-DM • PIM-SM • DVMRP
Flags	El valor de este campo es válido si el protocolo de enrutamiento multicast en ejecución es PIM-SM. Los valores posibles son RPT o SPT. Para otros protocolos se muestra “------”.

Agregar entradas multicast estáticas a Mroute

Puede agregar entradas de rutas multicast (Mroute) estáticas a la tabla Mroute.

Para agregar entradas multicast estáticas a la tabla Mroute:

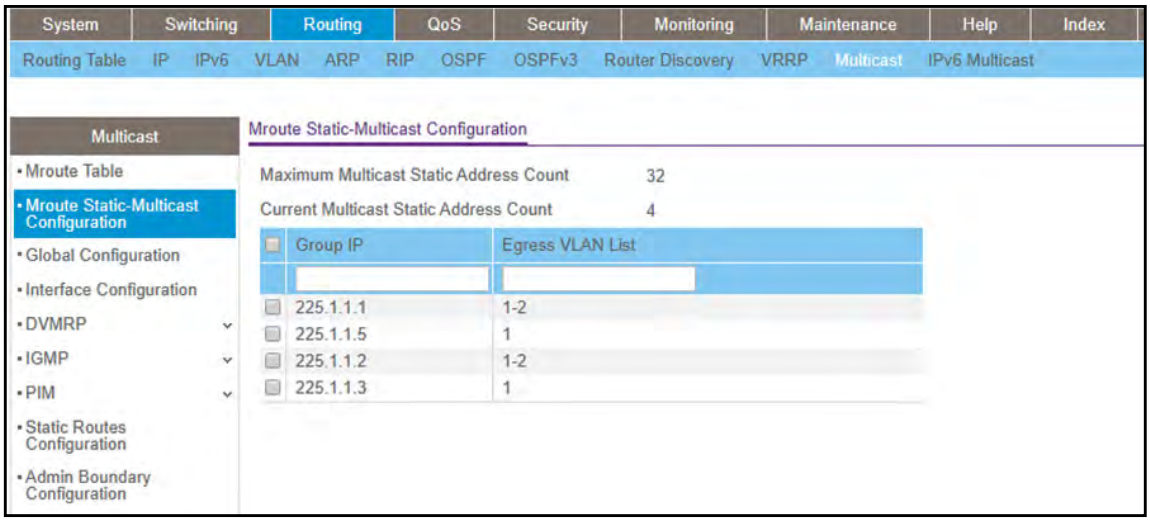
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > Multicast > Mroute Static-Multicast Configuration.



5. En el campo Group IP, introduzca la dirección IP del grupo multicast.

6. En el campo Egress VLAN List, introduzca la VLAN o las VLAN a las que pertenece la dirección IP del grupo multicast.

7. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 153. Mroute Static-Multicast Configuration

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 agregadas a la tabla Mroute.

Configurar los ajustes globales de multicast

Para configurar los ajustes globales de multicast:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > Multicast > Global Configuration.



5. En el campo Admin Mode, seleccione la opción Enable o Disable para establecer el estado administrativo del reenvío multicast en el router.

El valor predeterminado es Disable.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
A continuación se describe la información no configurable que se muestra.

Tabla 154. Configuración global de multicast

Campo	Descripción
Protocol State	El estado operativo del módulo de reenvío multicast.
Table Maximum Entry Count	El número máximo de entradas en la tabla de enrutamiento multicast IP.
Protocol	El protocolo de enrutamiento multicast activado actualmente en el router, si lo hay.
Table Entry Count	El número de entradas de rutas multicast presentes actualmente en la tabla de rutas multicast.

Configurar la interfaz multicast

Para configurar la interfaz multicast:

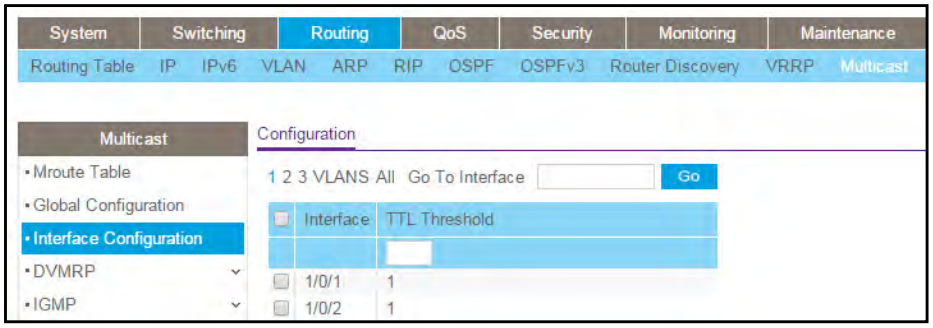
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > Multicast > Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.
6. Introduzca el TTL Threshold por debajo del cual un paquete de datos multicast no se reenvía desde la interfaz seleccionada.

   Introduzca un número entre 0 y 255. El valor predeterminado es 1. Si introduce 0, se reenvían todos los paquetes multicast de la interfaz seleccionada. Debe configurar al menos una interfaz de router para ver este campo.

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

Configurar los ajustes globales de DVMRP multicast

Para configurar los ajustes globales de DVMRP multicast:

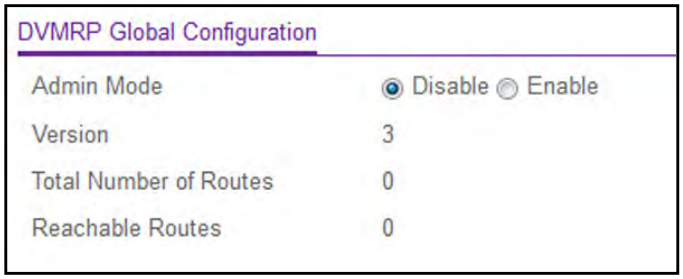
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > DVMRP > Global Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.
Establece el estado administrativo de DVMRP en activo o inactivo. El valor predeterminado es Disable.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 155. Configuración global de DVMRP

Campo	Descripción
Version	El valor actual de la cadena de versión de DVMRP.
Total Number of Routes	El número de rutas en la tabla de enrutamiento DVMRP.
Reachable Routes	El número de rutas de la tabla de enrutamiento DVMRP que usan una métrica no infinita.

Configurar la interfaz DVMRP

Para configurar la interfaz DVMRP multicast:

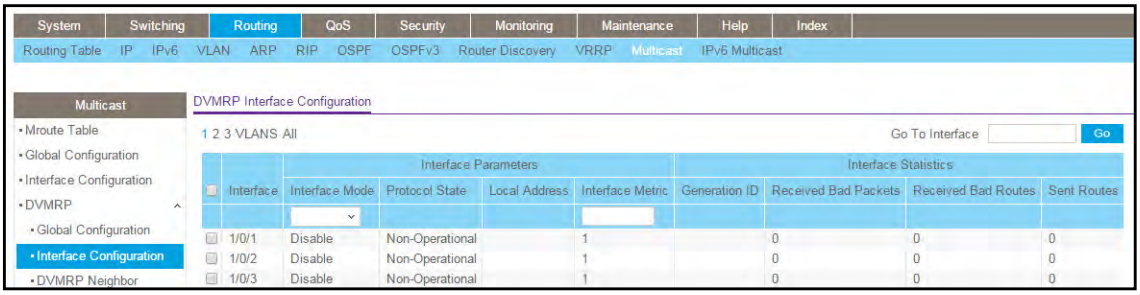
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > DVMRP > Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.
6. En el campo Interface Mode, seleccione la opción Enable o Disable para establecer el modo administrativo de la interfaz de enrutamiento DVMRP seleccionada.

El valor predeterminado es Disable.

7. En el campo Interface Metric, introduzca la métrica DVMRP de la interfaz seleccionada.

   Este valor se envía en los mensajes DVMRP como el costo para llegar a esta red. Los valores válidos son de 1 a 31. El valor predeterminado es 1.

8. Haga clic en el botón Apply (Aplicar).

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 156. Configuración de interfaces DVMRP

Campo	Descripción
Protocol State	El estado operativo del protocolo DVMRP en la interfaz seleccionada, Operational o Non-Operational.
Local Address	La dirección IP que se usa como dirección de origen en los paquetes enviados desde la interfaz seleccionada.
Generation ID	El ID de generación DVMRP que usa el router para la interfaz seleccionada. Este valor se restablece cada vez que se inicia una interfaz y se incluye en los mensajes prune. Un cambio en el ID de generación indica a los routers vecinos que descarten toda la información anterior sobre este router.
Received Bad Packets	El número de paquetes no válidos recibidos en la interfaz seleccionada.
Received Bad Routes	El número de rutas no válidas recibidas en la interfaz seleccionada.
Sent Routes	El número de rutas enviadas en la interfaz seleccionada.

Buscar vecinos DVMRP

Para buscar vecinos DVMRP:

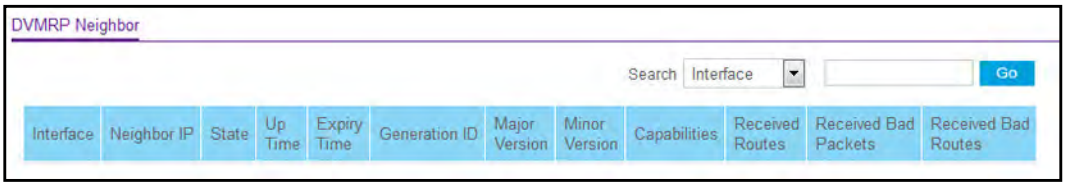
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > DVMRP > DVMRP Neighbor.



5. Use el menú Search para buscar entradas de vecinos por interfaz MAC o por dirección IP del vecino:
   - Seleccione Interface en el menú, introduzca la interfaz en formato unidad/ranura/puerto (por ejemplo, 1/0/13) y haga clic en el botón Go.

     Si la entrada del vecino existe, se muestra primero, seguida de las demás entradas.
   - Seleccione Neighbor IP en el menú, introduzca la dirección IP del vecino y haga clic en el botón Go.

     Si existe la entrada con la IP de vecino coincidente, se muestra primero, seguida de las demás entradas. Se requiere una coincidencia exacta.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 157. Vecinos DVMRP

Campo	Descripción
Interface	Seleccione la interfaz cuyos datos se mostrarán; de lo contrario, se muestran todas las interfaces.
Neighbor IP	La dirección IP del vecino cuya información se muestra
State	El estado del router vecino especificado en la interfaz seleccionada, activo o inactivo.
Up Time	El tiempo de actividad DVMRP del vecino especificado en la interfaz seleccionada. Es el tiempo transcurrido desde que se aprendió la entrada del vecino.

Tabla 157. Vecinos DVMRP (continuación)

Campo	Descripción
Expiry Time	El tiempo de expiración DVMRP del vecino especificado en la interfaz seleccionada. Es el tiempo restante antes de que caduque la entrada del vecino, y no se aplica si el estado del router vecino es inactivo.
Generation ID	El ID de generación DVMRP del vecino especificado en la interfaz seleccionada.
Major Version	La versión principal de DVMRP del vecino especificado en la interfaz seleccionada.
Minor Version	La versión secundaria de DVMRP del vecino especificado en la interfaz seleccionada.
Capabilities	Las capacidades DVMRP del vecino especificado en la interfaz seleccionada.
Received Routes	El número de rutas recibidas del vecino especificado en la interfaz seleccionada.
Received Bad Packets	El número de paquetes no válidos recibidos del vecino especificado en la interfaz seleccionada.
Received Bad Routes	El número de rutas no válidas recibidas del vecino especificado en la interfaz seleccionada.

Ver los ajustes de Next Hop de DVMRP

Para ver los ajustes de Next Hop de DVMRP multicast:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > DVMRP > DVMRP Next Hop.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 158. DVMRP Next Hop

Campo	Descripción
Source IP	La dirección IP que se usa con la máscara de origen para identificar la red de origen de esta entrada de la tabla.
Source Mask	La máscara de red que se usa con la dirección IP de origen.
Next Hop Interface	La interfaz de salida de este salto siguiente.
Type	El tipo de salto siguiente. Leaf significa que no hay vecinos dependientes posteriores en la interfaz de salida. De lo contrario, el tipo es branch.

Ver DVMRP Prune multicast

Para ver DVMRP Prune multicast:

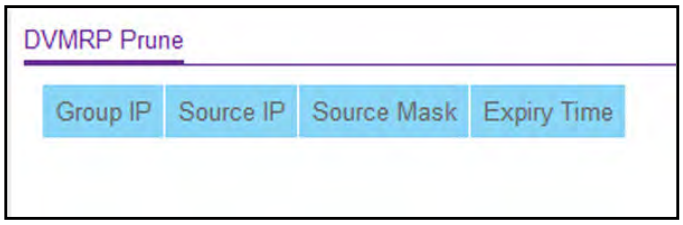
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > DVMRP > DVMRP Prune.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 159. DVMRP Prune

Campo	Descripción
Group IP	La dirección de grupo que se podó.
Source IP	La dirección IP que se usa con la máscara de origen para identificar la red de origen de esta entrada de la tabla.

Tabla 159. DVMRP Prune (continuación)

Campo	Descripción
Source Mask	La máscara de red que se usa con la dirección IP de origen.
Expiry Time	El tiempo restante antes de que esta poda expire en el vecino ascendente. Si no se recibieron mensajes prune de los vecinos descendentes, se establece en el valor del temporizador predeterminado de vida de la poda; de lo contrario, se establece en el menor valor recibido o en el temporizador predeterminado, el que sea menor.

Ver la ruta DVMRP

Para ver la ruta DVMRP multicast:

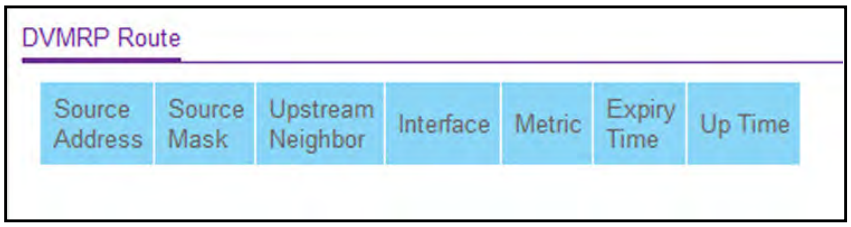
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > DVMRP > DVMRP Route.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 160. Ruta DVMRP

Campo	Descripción
Source Address	La dirección de red que se combina con la máscara de origen para identificar los orígenes de esta entrada.
Source Mask	La máscara de subred que se usa con la dirección IP de origen para identificar los orígenes de esta entrada.
Upstream Neighbor	La dirección del vecino ascendente (por ejemplo, el vecino RPF) del que se reciben los datagramas IP de estos orígenes.

Tabla 160. Ruta DVMRP (continuación)

Campo	Descripción
Interface	La interfaz en la que se reciben los datagramas IP enviados por estos orígenes. Un valor de 0 normalmente significa que la ruta es un agregado para el que no existe interfaz de salto siguiente.
Metric	La distancia en saltos a la subred de origen.
Expiry Time	El tiempo restante antes de que esta poda expire en el vecino ascendente. Si no se recibieron mensajes prune de los vecinos descendentes, se establece en el valor del temporizador predeterminado de vida de la poda; de lo contrario, se establece en el menor valor recibido o en el temporizador predeterminado, el que sea menor.
Up Time	El tiempo transcurrido desde que el router aprendió la ruta representada por esta entrada.

Configurar los ajustes de IGMP multicast

Puede configurar los ajustes de IGMP y ver las estadísticas de IGMP.

Configurar los ajustes globales de IGMP

Para configurar los ajustes globales de IGMP:

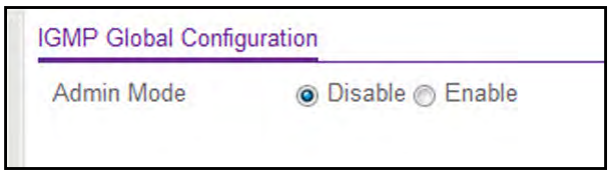
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > Global Configuration.



5. En el campo Admin Mode, seleccione la opción Enable o Disable.

   Establece el estado administrativo de IGMP en el router en activo o inactivo. El valor predeterminado es Disable.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar la interfaz de enrutamiento IGMP

Para configurar la interfaz de enrutamiento IGMP:

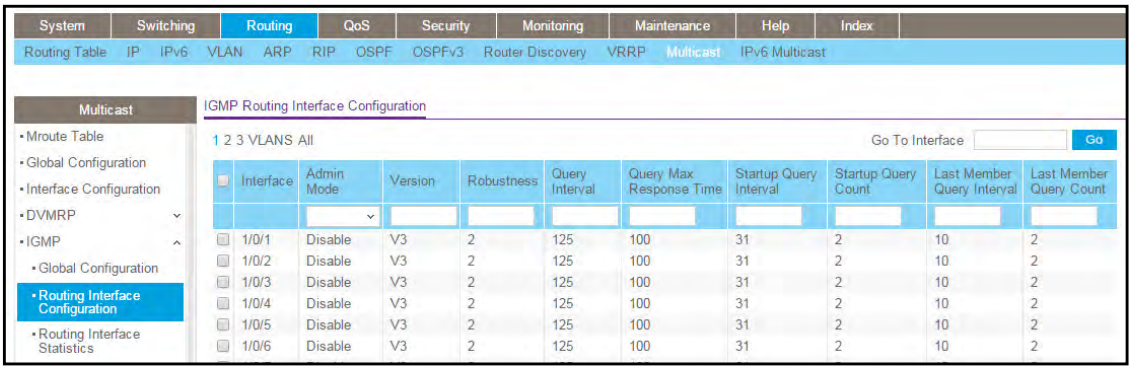
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > Routing Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.

6. En el campo Admin Mode, seleccione la opción Enable o Disable para establecer el estado administrativo de IGMP en la interfaz de enrutamiento seleccionada.

El valor predeterminado es Disable.
7. En el campo Version, introduzca la versión de IGMP que se configurará en la interfaz seleccionada.

   Los valores válidos son de 1 a 3. El valor predeterminado es 3. Este campo solo se puede configurar si el modo de interfaz IGMP está habilitado.

8. En el campo Robustness, introduzca el valor de robustez.

Esta variable permite ajustar la pérdida de paquetes esperada en una subred. Si espera que la subred tenga pérdidas, introduzca un número más alto. IGMP tolera hasta (variable de robustez – 1) pérdidas de paquetes. Los valores válidos son de 1 a 255. El valor predeterminado es 2.

9. En el campo Query Interval, introduzca la frecuencia en segundos con la que se transmiten los paquetes IGMP host-query en esta interfaz.

Los valores válidos son de 1 a 3600. El valor predeterminado es 125.

10. En el campo Query Max Response Time, introduzca el tiempo máximo de respuesta a consultas, en décimas de segundo, que se anuncia en las consultas IGMPv2 de esta interfaz.

El valor predeterminado es 100. Los valores válidos son de 0 a 255.

11. En el campo Startup Query Interval, introduzca el número de segundos entre la transmisión de consultas de inicio en la interfaz seleccionada.

Los valores válidos son de 1 a 300. El valor predeterminado es 31.
12. En el campo Startup Query Count, introduzca el número de consultas que se envían al inicio. Los valores válidos son de 1 a 20. El valor predeterminado es 2.

13. En el campo Last Member Query Interval, introduzca el intervalo de consulta del último miembro en décimas de segundo.

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. Los valores válidos son de 0 a 255. El valor predeterminado es 10. Este valor no se usa en IGMP versión 1.

14. En el campo Last Member Query Count, introduzca el número de consultas que se envían al recibir un informe leave group.

Los valores válidos son de 1 a 20. El valor predeterminado es 2.
15. Haga clic en el botón Apply.
La configuración se guarda.

Ver las estadísticas de las interfaces de enrutamiento IGMP

Para ver las estadísticas de las interfaces de enrutamiento IGMP:

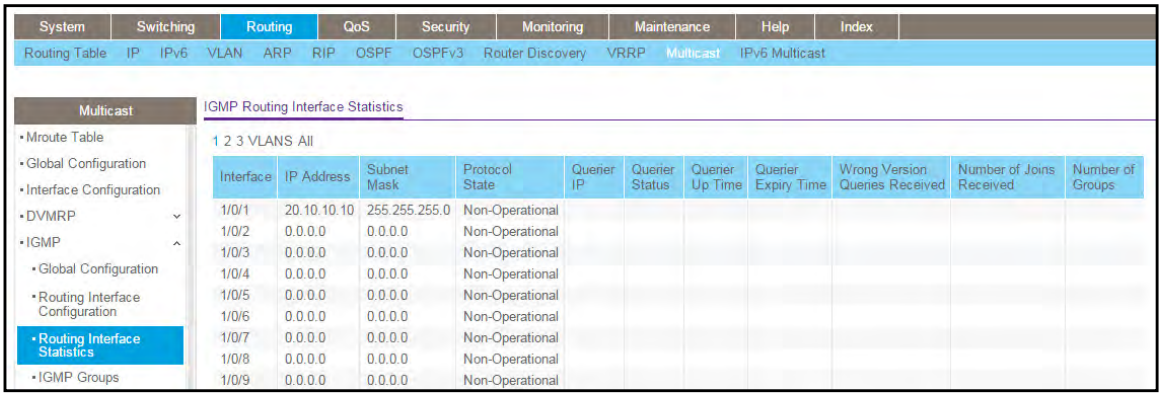
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > Routing Interface Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 161. Estadísticas de interfaces de enrutamiento IGMP multicast

Campo	Descripción
Interface	La interfaz en la que está habilitado IGMP.
IP Address	La dirección IP de la interfaz seleccionada.
Subnet Mask	La máscara de subred de la dirección IP de la interfaz seleccionada.
Protocol State	El estado operativo de IGMP en la interfaz seleccionada, Operational o Non-Operational.
Querier IP	La dirección del querier IGMP en la subred IP a la que está conectada la interfaz seleccionada.
Querier Status	Indica si la interfaz seleccionada está en modo querier o non-querier.
Querier Up Time	El tiempo en segundos desde el último cambio del querier de la interfaz IGMP.
Querier Expiry Time	El tiempo en segundos que falta para que venza el temporizador other querier present. Si el sistema local es el querier, es cero.
Wrong Version Queries Received	El número de consultas recibidas en la interfaz seleccionada con una versión de IGMP que no coincide con la versión de IGMP configurada para la interfaz, durante la vida de la entrada. IGMP requiere que todos los routers de una LAN estén configurados con la misma versión de IGMP. Por lo tanto, si se reciben consultas con un número de versión incorrecto, indica un error de configuración.
Number of Joins Received	El número de veces que se agregó una membresía de grupo en la interfaz seleccionada; es decir, el número de veces que se agregó una entrada de esta interfaz a la tabla de caché. Esto da una idea de la cantidad de actividad IGMP en la interfaz.
Number of Groups	El número actual de entradas de la interfaz seleccionada en la tabla de caché.

Ver los grupos IGMP

Para ver los grupos IGMP:

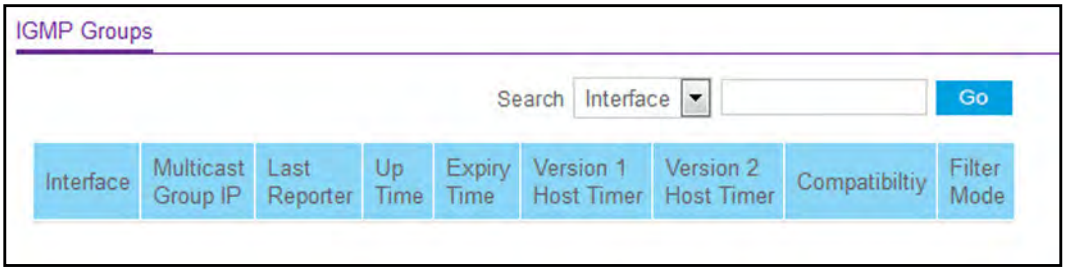
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > IGMP Groups.



5. Use el menú Search para buscar entradas multicast por interfaz o grupo:
   - Seleccione Interface en el menú, 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 primero, seguida de las demás entradas.

   - Seleccione Group en el menú, introduzca la dirección IP del grupo multicast y haga clic en el botón Go.

     Si la entrada existe, la entrada con el grupo coincidente se muestra como la primera, seguida del resto. Se requiere una coincidencia exacta.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información no configurable que se muestra.

Tabla 162. Grupos IGMP multicast

Campo	Descripción
Interface	Interfaz cuyos datos se mostrarán.
Multicast Group IP	Dirección del grupo multicast IP cuyos datos se mostrarán.
Last Reporter	Dirección IP del origen del último informe de pertenencia recibido para la dirección del grupo multicast IP en la interfaz seleccionada.

Tabla 162. Grupos IGMP multicast (continuación)

Campo	Descripción
Up Time	Tiempo transcurrido desde que se creó esta entrada.
Expiry Time	Tiempo mínimo restante antes de que esta entrada expire.
Version 1 Host Timer	Tiempo restante hasta que el router local asume que no hay miembros de IGMP versión 1 en la subred IP conectada a esta interfaz. Al recibir un informe de pertenencia IGMPv1, este temporizador se restablece al temporizador de pertenencia al grupo. Mientras no sea cero, el router local ignora los mensajes leave IGMPv2 de este grupo que recibe en la interfaz seleccionada. Este campo solo se muestra si la interfaz está configurada para IGMP versión 1.
Version 2 Host Timer	Tiempo restante hasta que el router local asume que no hay miembros de IGMP versión 2 en la subred IP conectada a esta interfaz. Al recibir un informe de pertenencia IGMPv2, este temporizador se restablece al temporizador de pertenencia al grupo. Mientras no sea cero, el router local ignora los mensajes leave IGMPv1 e IGMPv3 de este grupo que recibe en la interfaz seleccionada. Este campo solo se muestra si la interfaz está configurada para IGMP versión 2.
Compatibility	Muestra el modo de compatibilidad (v1, v2 y v3) de este grupo en la interfaz especificada.
Filter Mode	Modo de filtro de origen (Include, Exclude o NA) del grupo especificado en esta interfaz. Con el modo NA activo, el campo está en blanco.

Ver la pertenencia IGMP

Para ver la pertenencia IGMP:

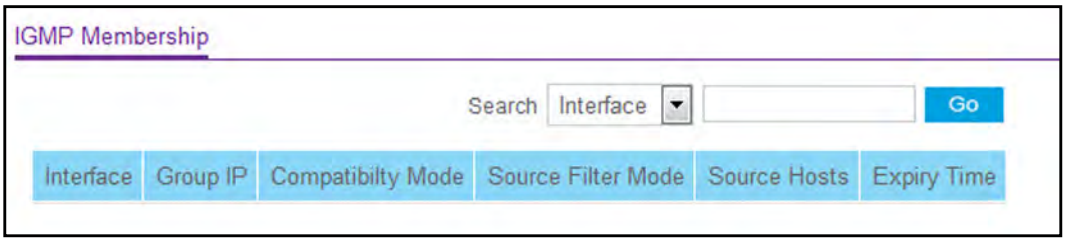
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > IGMP Membership.



5. Use el menú Search para buscar entradas multicast por interfaz o dirección IP de grupo.
   - Seleccione Interface en el menú, 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 primero, seguida de las demás entradas.

   - Seleccione Group IP en el menú, introduzca la 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 del resto. Se requiere una coincidencia exacta.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información no configurable que se muestra.

Tabla 163. Pertenencia IGMP multicast

Campo	Descripción
Interface	Interfaz por la que se reenvían los paquetes multicast.
Group IP	Dirección del grupo multicast IP cuyos datos se mostrarán.
Compatibility Mode	Muestra el modo de compatibilidad (v1, v2 y v3) de este grupo en la interfaz especificada.
Source Filter Mode	Modo de filtro de origen (Include, Exclude o NA) del grupo especificado en esta interfaz. Con el modo NA activo, el campo está en blanco.
Source Hosts	Muestra las direcciones de origen que son miembros de esta dirección multicast.
Expiry Time	Muestra el intervalo de expiración de cada dirección de origen miembro de este grupo multicast. Es el tiempo tras el cual expira la entrada de origen especificada.

Configurar la interfaz proxy IGMP

Para configurar la interfaz proxy IGMP:

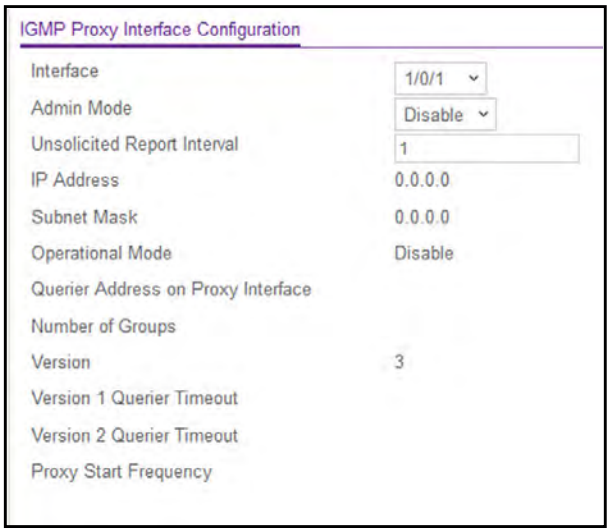
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > Proxy Interface Configuration.



5. Use la lista Interface para seleccionar el puerto.
Debe configurar al menos una interfaz de router antes de configurar o ver datos de una interfaz proxy IGMP, y no debe ser una interfaz de enrutamiento IGMP.
6. Seleccione Enable o Disable en la lista Admin Mode.

   Esto define el estado administrativo del proxy IGMP en la interfaz seleccionada. El valor predeterminado es Disable. Los modos administrativos globales de Routing, IGMP y Multicast deben estar habilitados para habilitar el modo de interfaz proxy IGMP.

7. En el campo Unsolicited Report Interval, introduzca el intervalo no solicitado en segundos.

   El intervalo de informes no solicitados es el tiempo entre repeticiones del informe inicial de pertenencia de un host a un grupo. Los valores válidos son de 1 a 260. El valor predeterminado es 1.

8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 164. Configuración de la interfaz proxy IGMP multicast

Campo	Descripción
IP Address	Dirección IP de la interfaz proxy IGMP.
Subnet Mask	Máscara de subred de la dirección IP de la interfaz proxy IGMP.

Tabla 164. Configuración de la interfaz proxy IGMP multicast (continuación)

Campo	Descripción
Operational Mode	Estado operativo de la interfaz proxy IGMP.
Querier Address on Proxy Interface	Dirección del consultor (querier) en la interfaz proxy.
Number of Groups	Número actual de entradas de grupos multicast de la interfaz proxy IGMP en la tabla de caché.
Version	Introduzca la versión de IGMP que se configurará en la interfaz seleccionada. Los valores válidos son de 1 a 3; el predeterminado es 3. Este campo solo es configurable cuando el modo de interfaz proxy IGMP está habilitado.
Version 1 Querier Timeout	Valor de tiempo de espera del consultor IGMP versión 1 anterior, en segundos. El intervalo del consultor de versión anterior es el tiempo de espera para que un host vuelva al modo IGMPv3 tras recibir una consulta de versión anterior. Al recibir una consulta de versión anterior, los hosts ajustan su temporizador de consultor de versión anterior presente al intervalo del consultor de versión anterior.
Version 2 Querier Timeout	Valor de tiempo de espera del consultor IGMP versión 2 anterior, en segundos.
Proxy Start Frequency	Número de veces que se activó el proxy.

Ver las estadísticas de la interfaz proxy IGMP

Para ver las estadísticas de la interfaz proxy IGMP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > Proxy Interface Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

A continuación se describe la información no configurable que se muestra.

Tabla 165. Estadísticas de la interfaz proxy IGMP multicast

Campo	Descripción
Proxy Interface	Interfaz por la que se reciben los paquetes IGMP.
Version	Versión de los paquetes IGMP recibidos.
Queries Received	Número de consultas IGMP recibidas.
Report Received	Número de informes IGMP recibidos.
Reports Sent	Número de informes IGMP enviados.
Leaves Received	Número de mensajes leave IGMP recibidos.
Leaves Sent	Número de mensajes leave IGMP enviados.

Ver la pertenencia proxy IGMP

Para ver la pertenencia proxy IGMP:

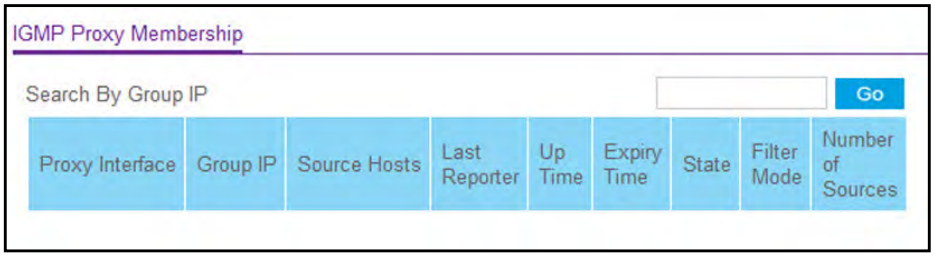
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > IGMP > Proxy Membership.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 166. Pertenencia proxy IGMP multicast

Campo	Descripción
Proxy Interface	Interfaz en la que está habilitado el proxy IGMP.
Group IP	Dirección del grupo multicast IP.
Source Hosts	Muestra las direcciones de origen que son miembros de esta dirección multicast.
Last Reporter	Dirección IP del origen del último informe de pertenencia recibido para la dirección del grupo multicast IP en la interfaz proxy IGMP.
Up Time	Tiempo transcurrido desde que se creó esta entrada.
Expiry Time	Muestra el intervalo de expiración de cada dirección de origen miembro de este grupo multicast. Es el tiempo tras el cual expira la entrada de origen especificada.
State	Estado de la entrada del host. Un host puede estar en uno de estos estados. Non-member (no miembro): no pertenece al grupo en la interfaz. Delaying member (miembro en espera): pertenece al grupo en la interfaz y el temporizador de informes está activo. Este temporizador se usa para enviar los informes. Idle member (miembro inactivo): el host pertenece al grupo en la interfaz y no hay temporizador de informes activo.
Filter Mode	Modo de filtro del grupo (Include/Exclude/None) para el grupo especificado en la interfaz proxy IGMP.
Number of Sources	Número de hosts de origen presentes en el grupo multicast seleccionado.

Configurar los ajustes de PIM

Puede configurar PIM y ver sus estadísticas.

Configurar los ajustes globales de PIM multicast

Protocol-Independent Multicast (PIM) es un protocolo estándar de enrutamiento multicast que ofrece enrutamiento multicast interdominio escalable a través de Internet, independiente de los mecanismos de cualquier protocolo de enrutamiento unicast.

Para configurar los ajustes globales de PIM:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > Global Configuration.



5. En el campo Admin Mode, seleccione el protocolo PIM del router. Los valores posibles son Disable, PIM-SM o PIM-DM. El valor predeterminado es Disable.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar PIM SSM

Mientras que PIM emplea un router de punto de encuentro (RP) configurado especialmente como punto de reunión entre emisores y receptores multicast, Protocol-Independent Multicast Single-Source Multicast (PIM-SSM) no usa un RP. Solo admite árboles de distribución por ruta de origen. Se usa entre routers para que sepan qué paquetes multicast reenviarse entre sí y a sus LAN conectadas directamente. El modelo de servicio SSM puede implementarse con un subconjunto estricto de los mecanismos del protocolo PIM. La semántica de IP multicast normal y la de SSM pueden coexistir en un mismo router, y ambas pueden implementarse con el protocolo PIM. Un rango de direcciones multicast, actualmente 232.0.0.0/8 en IPv4 y FF3x::/32 en IPv6, está reservado para SSM.

Para configurar PIM SSM:

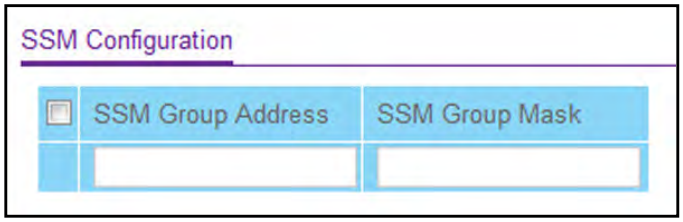
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > SSM Configuration.



5. En el campo SSM Group Address, introduzca la dirección IP del grupo multicast de origen específico.

6. En el campo SSM Group Mask, introduzca la máscara de la dirección IP del grupo multicast de origen específico.

7. Haga clic en el botón Add.
Se agrega el grupo de origen específico.

Configurar la interfaz PIM

Para configurar la interfaz PIM multicast:

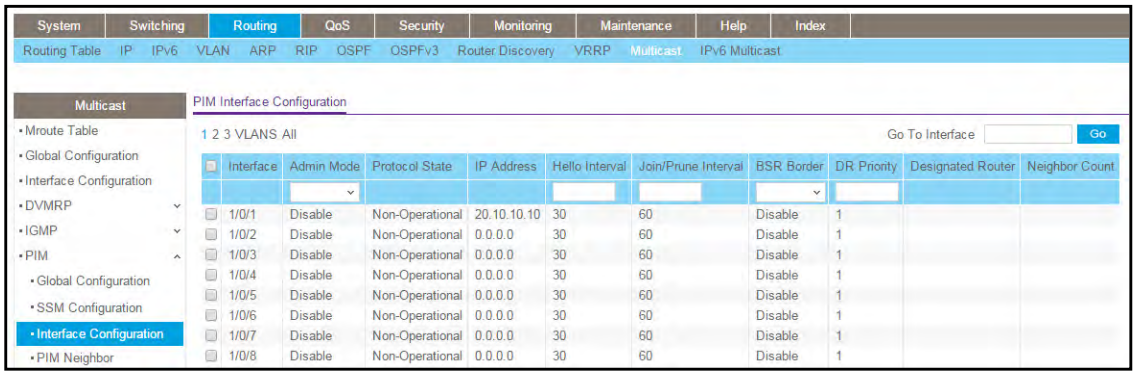
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.

6. En el campo Admin Mode, seleccione Enable o Disable para definir el estado administrativo de PIM en el router.

El valor predeterminado es Disable.

7. En el campo Hello Interval, introduzca el tiempo en segundos entre transmisiones de mensajes PIM hello en esta interfaz.

Los valores válidos son de 0 a 18000. El valor predeterminado es 30.

8. En Join/Prune Interval, introduzca el tiempo en segundos con que se transmiten los mensajes PIM Join/Prune en esta interfaz PIM. Los valores válidos son de 0 a 18000. El valor predeterminado es 60.

9. En el campo BSR Border, seleccione Enable o Disable para definir el estado de límite del bootstrap router (BSR) en la interfaz seleccionada.

10. Introduzca DR Priority para la interfaz seleccionada.
Los valores válidos son de 0 a 2147483647. El valor predeterminado es 1.
11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 167. Configuración de la interfaz PIM multicast

Campo	Descripción
Protocol State	Estado de PIM en el router: Operational o Non-Operational.
IP Address	Dirección IP de la interfaz PIM seleccionada. Si introduce una dirección IPv6, el formato es prefijo/longitud de prefijo.
Designated Router	Router designado en la interfaz PIM seleccionada.
Neighbor Count	Número de vecinos PIM en la interfaz seleccionada.

Ver los vecinos PIM

Para ver los vecinos PIM:

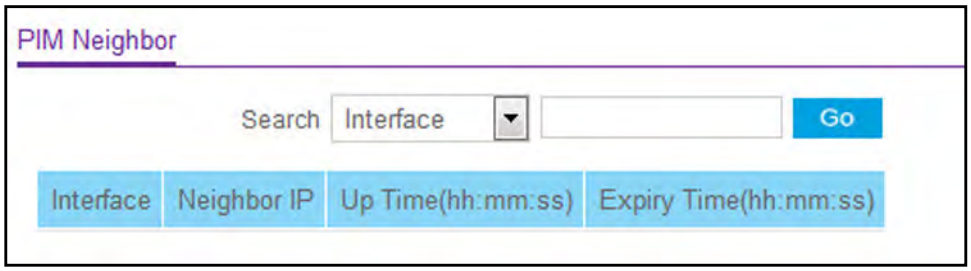
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > PIM Neighbor.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 168. Vecinos PIM multicast

Campo	Descripción
Interface	Interfaz en la que se muestra el vecino.
Neighbor IP	Dirección IP del vecino PIM de esta entrada.
Up Time (hh:mm:ss)	Tiempo desde que este vecino PIM se convirtió (por última vez) en vecino del router local.
Expiry Time (hh:mm:ss)	Tiempo mínimo restante antes de que expire este vecino PIM.

Ver el punto de encuentro candidato de PIM

Para ver el punto de encuentro (RP) candidato de PIM multicast:

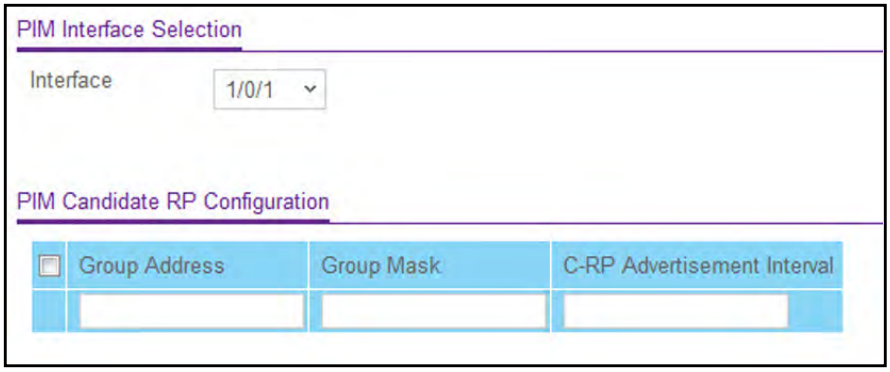
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > Candidate RP Configuration.



La siguiente tabla describe la información no configurable que se muestra.

Tabla 169. Vecinos PIM multicast

Campo	Descripción
Campo	**Descripción**
Interface	Interfaz en la que se muestra el vecino.
Neighbor IP	Dirección IP del vecino PIM de esta entrada.
Up Time (hh:mm:ss)	Tiempo desde que este vecino PIM se convirtió (por última vez) en vecino del router local.
Expiry Time (hh:mm:ss)	Tiempo mínimo restante antes de que expire este vecino PIM.

Ver los vecinos PIM

Para ver los vecinos PIM multicast:

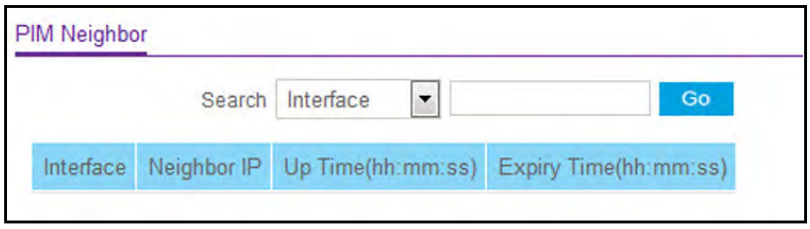
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > PIM Neighbor.



Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

Tabla 170. Vecinos PIM multicast

Campo	Descripción
Interface	Interfaz en la que se muestra el vecino.
Neighbor IP	Dirección IP del vecino PIM de esta entrada.
Up Time (hh:mm:ss)	Tiempo desde que este vecino PIM se convirtió (por última vez) en vecino del router local.
Expiry Time (hh:mm:ss)	Tiempo mínimo restante antes de que expire este vecino PIM.

Configurar el punto de encuentro candidato de PIM

Para configurar el punto de encuentro (RP) candidato de PIM:

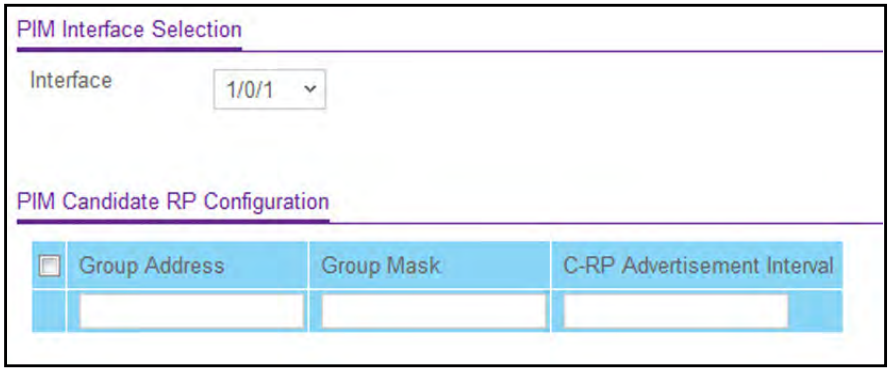
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > Candidate RP Configuration.



5. En la lista de interfaces, seleccione la interfaz.
6. Introduzca Group Address que se transmite en los anuncios de RP candidato. Si introduce una dirección IPv6, el formato es prefijo/longitud de prefijo.
7. En el campo Group Mask, introduzca la máscara de la dirección de grupo transmitida en los anuncios de RP candidato
8. En el campo C-RP Advertisement Interval, especifique el intervalo en segundos con que se envían los mensajes C-RP por unicast al bootstrap router (BSR).

   El rango es de 1 a 16383 segundos. El valor predeterminado es 60 segundos. Si este campo se envía sin valor, se usa el predeterminado.

9. Haga clic en el botón Add.

Se agrega la dirección de RP candidato para el router PIM.

Configurar el bootstrap router candidato de PIM

Para configurar el bootstrap router (BSR) candidato de PIM multicast:

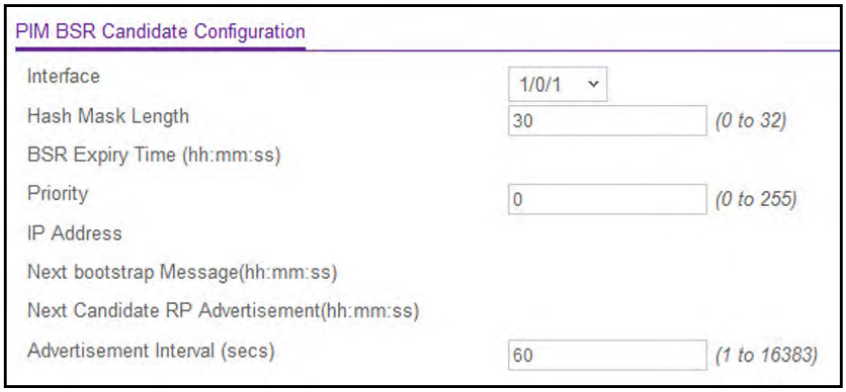
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > BSR Candidate Configuration.



5. En la lista de interfaces, seleccione la interfaz.
6. Introduzca C-BSR Hash Mask Length que se anunciará en los mensajes bootstrap.

   Esta longitud de máscara hash se usa en el algoritmo hash para seleccionar el RP de un grupo determinado. Los valores válidos son de 0 a 32. El valor predeterminado es 30.

7. En el campo Priority, introduzca la prioridad del C-BSR.
8. Introduzca el valor de Advertisement Interval del C-BSR en segundos. El valor predeterminado es 60.
9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 171. Configuración de BSR candidato multicast

Campo	Descripción
BSR Expiry Time (hh:mm:ss)	Tiempo (en horas, minutos y segundos) en el que expira el bootstrap router (BSR) elegido aprendido.
IP Address	Dirección IP del BSR elegido.
Next bootstrap Message (hh:mm:ss)	Tiempo (en horas, minutos y segundos) en el que se espera el siguiente mensaje bootstrap de este BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Tiempo (en horas, minutos y segundos) en el que se envía el siguiente anuncio de RP candidato.

Configurar el punto de encuentro estático de PIM

Puede configurar estáticamente la dirección del punto de encuentro (RP) para uno o más grupos multicast.

Para configurar el RP estático de PIM:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > PIM > Static RP Configuration.



5. En el campo RP Address, introduzca la dirección IP para uno o más grupos multicast.
6. En el campo Group Address, introduzca la dirección de grupo del RP.
7. Introduzca Group Mask del RP que se creará o eliminará.
8. En el campo Override, seleccione Enable o Disable.

   Enable indica que, en caso de conflicto, el RP configurado con esta opción prevalece sobre el RP aprendido por BSR.

9. Haga clic en el botón Add.
Se agrega la dirección de RP estático para uno o más grupos multicast
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar rutas estáticas multicast

Para configurar rutas estáticas multicast:

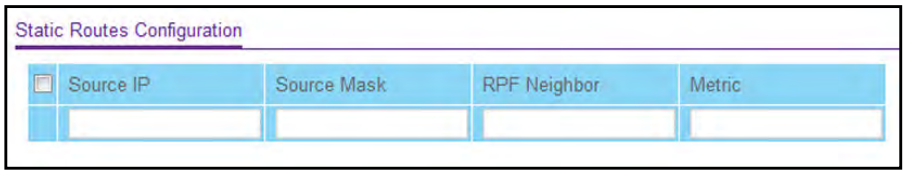
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > Static Routes Configuration.



5. En el campo Source IP, introduzca la dirección IP que identifica el origen de los paquetes multicast de la entrada que está creando.
6. En el campo Source Mask, introduzca la máscara de subred que se aplicará a la dirección IP de origen.
7. En el campo RPF Neighbor, introduzca la dirección IP del router vecino en la ruta hacia el origen.
8. En el campo Metric, introduzca el costo de estado de enlace de la ruta hacia el origen multicast.

   El rango es de 0 a 255; el valor predeterminado es 1. Puede cambiar la métrica de una ruta configurada seleccionando la ruta estática y editando este campo.

9. Haga clic en el botón Add.
Se agrega la ruta estática al switch.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar el límite administrativo multicast

Un límite de alcance administrativo es un mecanismo para detener la entrada y salida de tráfico multicast de un rango determinado de direcciones multicast en una interfaz de enrutamiento determinada.

Para configurar el límite administrativo multicast:

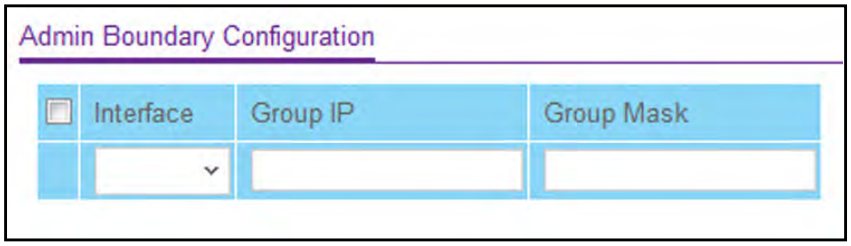
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> Multicast > Admin Boundary Configuration.



5. En la lista Interface, seleccione la interfaz de router en la que se configurará el límite de alcance administrativo.
6. En el campo Group IP, introduzca la dirección del grupo multicast que inicia el rango de direcciones que se excluirán.

La dirección debe estar en el rango de 239.0.0.0 a 239.255.255.255.
7. En el campo Group Mask, introduzca la máscara que se aplicará a la dirección del grupo multicast.

   La combinación de la máscara y la IP del grupo da el rango de direcciones de alcance administrativo para la interfaz seleccionada.

8. Haga clic en el botón Add.
Se agrega el límite de alcance administrativo.

Configurar los ajustes de multicast IPv6

Ver la tabla Mroute de multicast IPv6

Puede ver el contenido de la tabla Mroute en formato tabular.

Para ver la tabla Mroute:

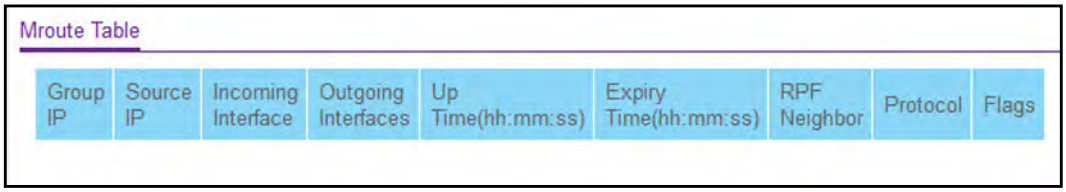
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing > IPv6 Multicast > Mroute Table.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 172. Tabla Mroute multicast

Campo	Descripción
Group IP	La dirección IP del grupo de destino.
Source IP	La dirección IP del origen del paquete multicast, que se combina con la IP del grupo para identificar por completo una ruta de la tabla Mroute.
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 IP del vecino de reenvío por ruta inversa (RPF).

Tabla 172. Tabla Mroute multicast (continuación)

Campo	Descripción
Protocol	Protocolo de enrutamiento multicast que creó esta entrada. Los valores posibles son: • PIM-DM • PIM-SM
Flags	El valor de este campo es válido si el protocolo de enrutamiento multicast en ejecución es PIM-SM. Los valores posibles son RPT o SPT. Para otros protocolos se muestra un – (guion).

Configurar los ajustes globales de PIM IPv6

Para configurar los ajustes globales de PIM IPv6:

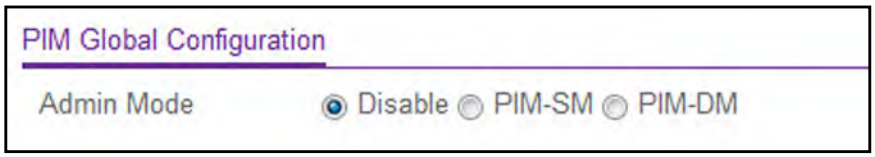
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > IPv6 PIM > Global Configuration.



5. Seleccione un botón de opción de Admin Mode.

   Las opciones son Disable o la variante del protocolo PIM: modo denso (PIM-DM) o modo disperso (PIM-SM).

   De forma predeterminada, este ajuste está deshabilitado. La opción Disable define el estado administrativo de PIM en el router como activo o inactivo.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar PIM SSM para IPv6

Mientras que PIM emplea un router de punto de encuentro (RP) configurado especialmente como punto de reunión entre emisores y receptores multicast, Protocol-Independent Multicast Single-Source Multicast (PIM-SSM) no usa un RP. Solo admite árboles de distribución por ruta de origen. Se usa entre routers para que sepan qué paquetes multicast reenviarse entre sí y a sus LAN conectadas directamente. El modelo de servicio SSM puede implementarse con un subconjunto estricto de los mecanismos del protocolo PIM. La semántica de IP multicast normal y la de SSM pueden coexistir en un mismo router, y ambas pueden implementarse con el protocolo PIM. Un rango de direcciones multicast, actualmente 232.0.0.0/8 en IPv4 y FF3x::/32 en IPv6, está reservado para SSM.

Para configurar PIM SSM para IPv6:

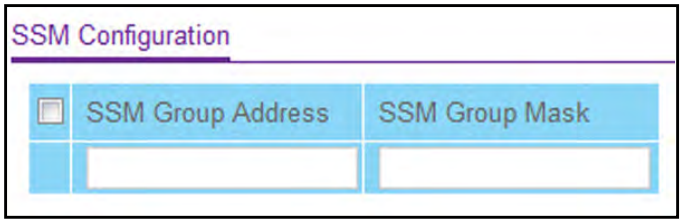
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > IPv6 PIM > SSM Configuration.



5. En el campo SSM Group Address, introduzca la dirección IP del grupo multicast de origen específico.
6. En el campo SSM Group Mask, introduzca la máscara de la dirección IP del grupo multicast de origen específico.
7. Haga clic en el botón Add.
Se agrega el grupo de origen específico.

Configurar la interfaz PIM IPv6

Para configurar la interfaz PIM IPv6:

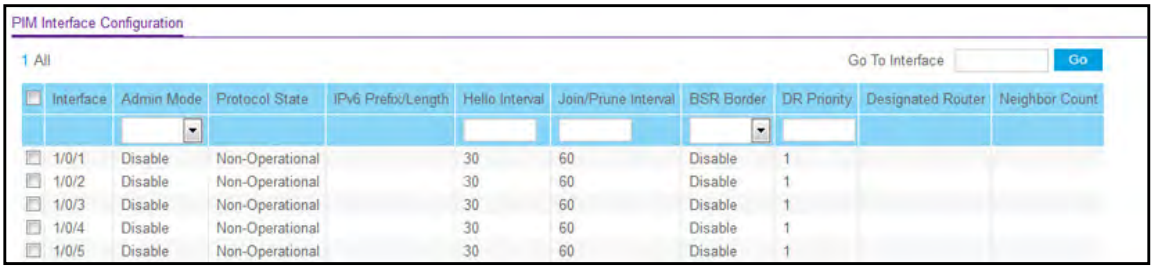
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > IPv6 PIM > Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.

6. En el campo Admin Mode, seleccione Enable o Disable.
Esto define el estado administrativo de PIM-SM en el router. El valor predeterminado es Disable.

7. En el campo Hello Interval, introduzca el tiempo en segundos entre transmisiones de mensajes PIM hello en esta interfaz.

   Los valores válidos son de 0 a 18000. El valor predeterminado es 30.

8. En el campo Join/Prune Interval, introduzca la frecuencia con que se transmiten los mensajes PIM Join/Prune en esta interfaz PIM.

   Los valores válidos son de 0 a 18000. El valor predeterminado es 60.

9. En el campo BSR Border, seleccione Enable o Disable para definir el estado de límite del bootstrap router (BSR) en la interfaz seleccionada.

10. Introduzca DR Priority para la interfaz seleccionada.
Los valores válidos son de 0 a 2147483647. El valor predeterminado es 1.

11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 173. Configuración de la interfaz PIM IPv6

Campo	Descripción
Protocol State	Estado de PIM en el router: Operational o Non-Operational.
IPv6 Prefix/Length	Prefijo de dirección IPv6 y longitud de la interfaz seleccionada.
Designated Router	Router designado en la interfaz PIM seleccionada.
Neighbor Count	Número de vecinos PIM en la interfaz seleccionada.

Ver los vecinos PIM IPv6

Para ver los vecinos PIM IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > IPv6 PIM > PIM Neighbor.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 174. Vecinos PIM IPv6

Campo	Descripción
Interface	Interfaz en la que se muestra el vecino.
Neighbor IP	Dirección IP del vecino PIM de esta entrada.

Tabla 174. Vecinos PIM IPv6

Campo	Descripción
Up Time (hh:mm:ss)	Tiempo desde que este vecino PIM se convirtió (por última vez) en vecino del router local.
Expiry Time (hh:mm:ss)	Tiempo mínimo restante antes de que expire este vecino PIM.

Configurar el punto de encuentro candidato de PIM IPv6

Para configurar el punto de encuentro candidato de PIM IPv6:

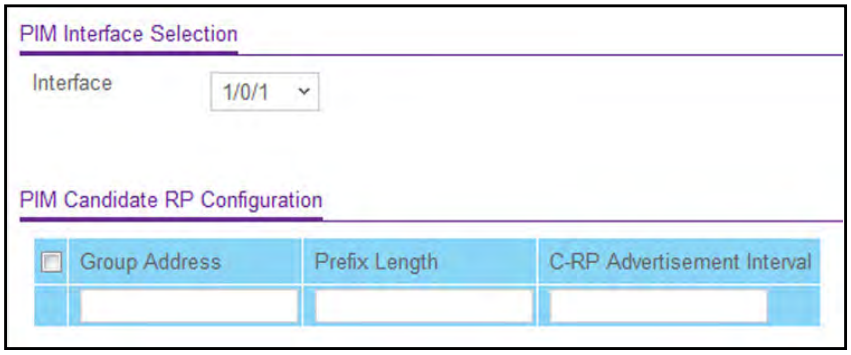
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > IPv6 PIM > Candidate RP Configuration.



5. En la lista de interfaces, seleccione la interfaz.
6. En el campo Group Address, introduzca el prefijo de dirección IPv6 del grupo transmitido en los anuncios de RP candidato.
7. En el campo Prefix Length, introduzca la longitud del prefijo IPv6 del grupo transmitida en los anuncios de RP candidato
8. En C-RP Advertisement Interval, especifique el intervalo en segundos con que se envían los mensajes C-RP por unicast al bootstrap router (BSR).

   El rango es de 1 a 16383 segundos. El valor predeterminado es 60 segundos. Si este campo se envía sin valor, se usa el predeterminado.

9. Haga clic en el botón Add.
Se agrega la dirección de RP candidato para el router PIM.

Configurar el bootstrap router candidato de PIM IPv6

Para configurar el BSR candidato de PIM IPv6:

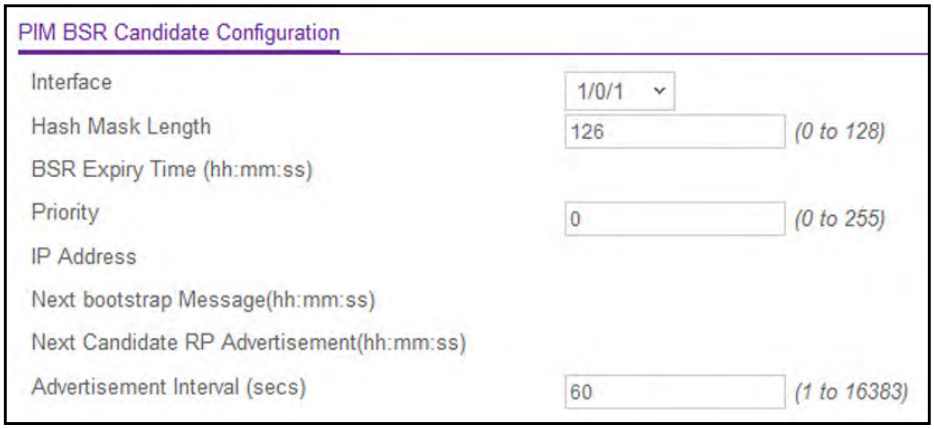
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing> IPv6 Multicast > IPv6 PIM > BSR Candidate Configuration.**



5. En la lista de interfaces, seleccione la interfaz.
6. Introduzca C-BSR Hash Mask Length que se anunciará en los mensajes bootstrap.

   Esta longitud de máscara hash se usa en el algoritmo hash para seleccionar el RP de un grupo determinado. Los valores válidos son de 0 a 128. El valor predeterminado es 126.

7. En el campo Priority, introduzca la prioridad del C-BSR.
8. Introduzca el valor de Advertisement Interval del C-BSR en segundos. El valor predeterminado es 60.

   Para quitar los valores configurados de Hash Mask Length y Priority y restaurar los valores predeterminados, haga clic en el botón Delete.

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

La siguiente tabla describe la información no configurable que se muestra.

Tabla 175. Configuración de candidatos BSR de PIM IPv6

Campo	Descripción
BSR Expiry Time (hh:mm:ss)	Tiempo (en horas, minutos y segundos) en el que expira el bootstrap router (BSR) elegido aprendido.
IP Address	Dirección IP del BSR elegido.
Next bootstrap Message (hh:mm:ss)	Tiempo (en horas, minutos y segundos) en el que se espera el siguiente mensaje bootstrap de este BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Tiempo (en horas, minutos y segundos) en el que se envía el siguiente anuncio de RP candidato.

Configurar el punto de encuentro estático de PIM IPv6

Puede configurar estáticamente la dirección del punto de encuentro (RP) para uno o más grupos multicast.

Para configurar el RP estático de PIM IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > IPv6 PIM > Static RP Configuration.



5. En el campo RP Address, ingrese la dirección IP del RP.
6. En el campo Group Address, ingrese la dirección del RP.
7. En el campo Prefix Length, ingrese la longitud del prefijo de la dirección de grupo.
8. En el campo Override, seleccione Enable o Disable.

   Enable indica que, si hay un conflicto, el RP configurado con esta opción prevalece sobre el RP aprendido por BSR.

9. Haga clic en el botón Add.
Se agrega la dirección de RP estático para uno o más grupos multicast.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar los ajustes globales de MLD IPv6

Para configurar los ajustes globales de PIM IPv6:

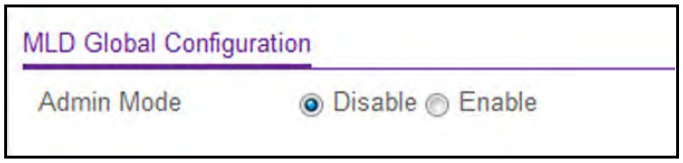
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > Global Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Esto establece el estado administrativo de MLD en el router como activo o inactivo. El valor predeterminado es Disable.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar la interfaz de enrutamiento MLD IPv6

Para configurar la interfaz de enrutamiento MLD IPv6:

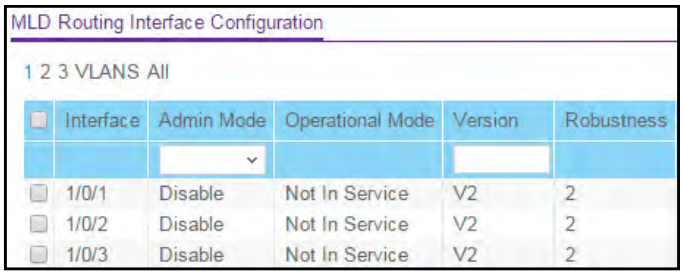
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

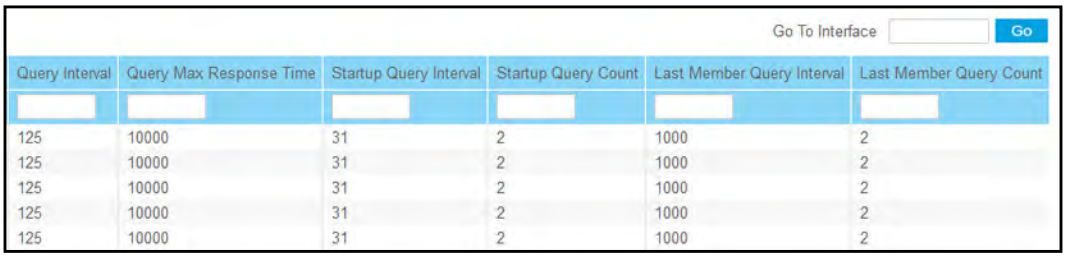
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > Routing Interface Configuration.





5. 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, seleccione la casilla de la interfaz que desea configurar.
6. En el campo Admin Mode, seleccione Enable o Disable.

   Esto establece el estado administrativo de MLD en la interfaz de enrutamiento seleccionada. El valor predeterminado es Disable.

7. En el campo Version, ingrese la versión que desea configurar en la interfaz seleccionada. Los valores válidos son de 1 a 2. El valor predeterminado es 2.

8. En el campo Query Interval, ingrese la frecuencia en segundos con la que se transmiten los paquetes de consulta de host MLD en esta interfaz.

   Los valores válidos son de 1 a 3600. El valor predeterminado es 125.

9. En el campo Query Max Response Time, ingrese el tiempo máximo de respuesta a consultas, en milisegundos, que se anuncia en las consultas MLDv2 de esta interfaz.

   Los valores válidos son de 0 a 65535. El valor predeterminado es 10000 milisegundos.

10. En el campo Startup Query Interval, ingrese el intervalo configurado en segundos entre las consultas generales que envía un querier al iniciar.

    El valor predeterminado es 31.

11. Ingrese el valor de Startup Query Count para indicar el número configurado de consultas enviadas al iniciar, separadas por el intervalo de consulta de inicio.

El valor predeterminado es 2.

12. En el campo Last Member Query Interval, ingrese el intervalo de consulta del último miembro en milisegundos.

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 tiempo entre mensajes de consulta específicos de grupo. Los valores válidos son de 0 a 655355. El valor predeterminado es 1000 milisegundos.

13. En el campo Last Member Query Count, ingrese el número de consultas que se envían al recibir un reporte de abandono de grupo.

Los valores válidos son de 1 a 20. El valor predeterminado es 2.
14. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 176. Configuración de la interfaz de enrutamiento MLD IPv6

Campo	Descripción
Operational Mode	El estado operativo de MLD en la interfaz.
Robustness	El parámetro de robustez de la interfaz seleccionada. Esta variable permite ajustar la pérdida de paquetes esperada en una subred. Si se espera que una subred tenga pérdidas, se puede aumentar la variable de robustez. MLD tolera hasta (variable de robustez –1) pérdidas de paquetes. El valor predeterminado es 2.

Ver las estadísticas de la interfaz de enrutamiento MLD IPv6

Para ver las estadísticas de la interfaz de enrutamiento MLD multicast IPv6:

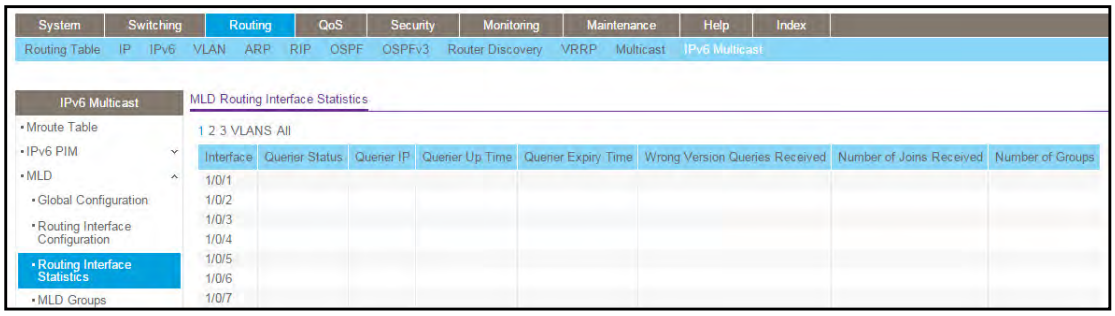
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > Routing Interface Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 177. Estadísticas de la interfaz de enrutamiento MLD IPv6

Campo	Descripción
Interface	Interfaz cuyos datos se mostrarán.
Querier Status	Indica si la interfaz seleccionada es un querier MLD o no querier en la subred con la que está asociada.
Querier IP	La dirección del querier MLD en la subred IP a la que está conectada la interfaz seleccionada.
Querier Up Time	El tiempo en segundos desde el último cambio del querier de la interfaz MLD.
Querier Expiry Time	El tiempo en segundos que falta para que venza el temporizador other querier present. Si el sistema local es el querier, es cero.
Wrong Version Queries Received	El número de consultas recibidas cuya versión de MLD no coincide con la versión de MLD de la interfaz.
Number of Joins Received	El número de veces que se agregó una membresía de grupo en la interfaz seleccionada.
Number of Groups	El número actual de entradas de membresía de la interfaz seleccionada en la tabla de caché.

Ver los grupos MLD IPv6

Para ver los grupos MLD IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > MLD Groups.



5. Use el menú Search para buscar entradas multicast por interfaz o grupo:

- Seleccione Interface en el menú, ingrese 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 de las demás entradas.

- Seleccione Group en el menú, ingrese la dirección IP del grupo MLD y haga clic en el botón Go.

  Si la entrada existe, se muestra como la primera entrada, seguida de las demás entradas. Se requiere una coincidencia exacta.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información no configurable que se muestra.

Tabla 178. Grupos MLD multicast IPv6

Campo	Descripción
Interface	Interfaz cuyos datos se mostrarán.
Group IP	La dirección de los miembros MLD.
Last Reporter	La dirección IP del origen del último reporte de membresía recibido para esta dirección de grupo multicast en la interfaz seleccionada.
Up Time	El tiempo transcurrido en segundos desde que se conoce el grupo multicast.
Expiry Time	El tiempo restante en segundos antes de que la entrada se elimine de la tabla de membresía MLD de esta interfaz.
Filter Mode	El modo de filtro del grupo multicast en esta interfaz. Los valores posibles son Include y Exclude.
Version 1 Host Timer	El tiempo restante hasta que el router asume que ya no hay hosts MLD versión 1 en la interfaz especificada.
Group Compat Mode	El modo de compatibilidad del grupo multicast en la interfaz. Los valores posibles son MLDv1 y MLDv2.
Source Hosts	Muestra las direcciones de origen que son miembros de esta dirección multicast.
Source Address (Expiry Time)	Este parámetro muestra el intervalo de expiración de cada dirección de origen que es miembro de este grupo multicast. Es el tiempo después del cual expira la entrada de origen especificada.

Ver y borrar el tráfico MLD IPv6

Para ver y borrar el tráfico MLD IPv6:

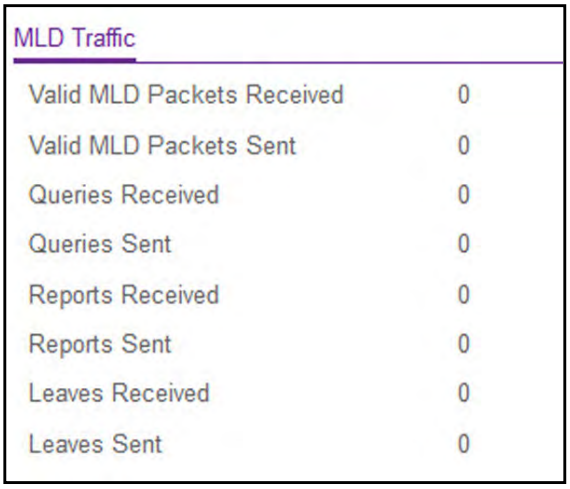
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Routing> IPv6 Multicast > MLD > MLD Traffic.**



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar todo el tráfico MLD IPv6, haga clic en el botón Clear.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 179. Tráfico MLD multicast IPv6

Campo	Descripción
Valid MLD Packets Received	El número de paquetes MLD válidos recibidos por el router.
Valid MLD Packets Sent	El número de paquetes MLD válidos enviados por el router.
Queries Received	El número de consultas MLD válidas recibidas por el router.
Queries Sent	El número de consultas MLD válidas enviadas por el router.
Reports Received	El número de reportes MLD válidos recibidos por el router.
Reports Sent	El número de reportes MLD válidos enviados por el router.

Tabla 179. Tráfico MLD multicast IPv6 (continuación)

Campo	Descripción
Leaves Received	El número de mensajes de abandono MLD válidos recibidos por el router.
Leaves Sent	El número de mensajes de abandono MLD válidos enviados por el router.

Configurar la interfaz proxy MLD IPv6

Para configurar la interfaz proxy MLD multicast IPv6:

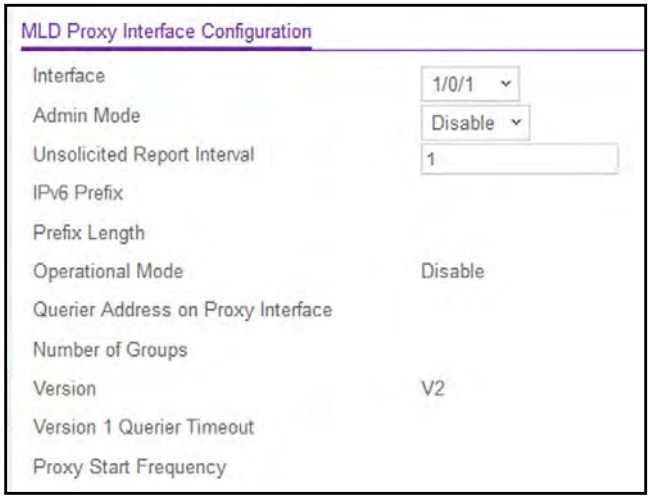
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > Proxy Interface Configuration.



5. En la lista Interface, seleccione la interfaz.
6. En la lista Admin Mode, seleccione Enable o Disable.

   Esto establece el estado administrativo del proxy MLD en la interfaz seleccionada. El valor predeterminado es Disable. Los modos administrativos globales de Routing, MLD y Multicast deben estar habilitados para habilitar el modo de interfaz proxy MLD.

7. En el campo Unsolicited Report Interval, introduzca el intervalo no solicitado en segundos.

El intervalo de reporte no solicitado es el tiempo entre repeticiones del reporte inicial de un host de membresía en un grupo. Los valores válidos son de 1 a 260. El valor predeterminado es 1.

8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 180. Configuración de la interfaz proxy MLD multicast IPv6

Campo	Descripción
IPv6 Prefix	La dirección IPv6 de la interfaz proxy MLD.
Prefix Length	La longitud del prefijo de la dirección IPv6 de la interfaz proxy MLD.
Operational Mode	El estado operativo de la interfaz proxy MLD.
Querier Address on Proxy Interface	Dirección del consultor (querier) en la interfaz proxy.
Number of Groups	El número actual de entradas de grupos multicast de la interfaz proxy MLD en la tabla de caché.
Version	Este campo solo se puede configurar cuando el modo de interfaz proxy MLD está habilitado. Ingrese la versión de MLD que desea configurar en la interfaz seleccionada. Los valores válidos son de 1 a 2. La versión predeterminada es 3.
Version 1 Querier Timeout	El valor de tiempo de espera, en segundos, del querier de MLD versión 1 anterior. El intervalo del querier de versión anterior es el tiempo de espera para que un host vuelva al modo MLDv2 después de recibir una consulta de versión anterior. Cuando se recibe una consulta de versión anterior, los hosts establecen su temporizador de querier de versión anterior en Older Version querier Interval.
Proxy Start Frequency	El número de veces que se activó el proxy.

Ver las estadísticas de la interfaz proxy MLD IPv6

Para ver las estadísticas de la interfaz proxy MLD multicast IPv6:

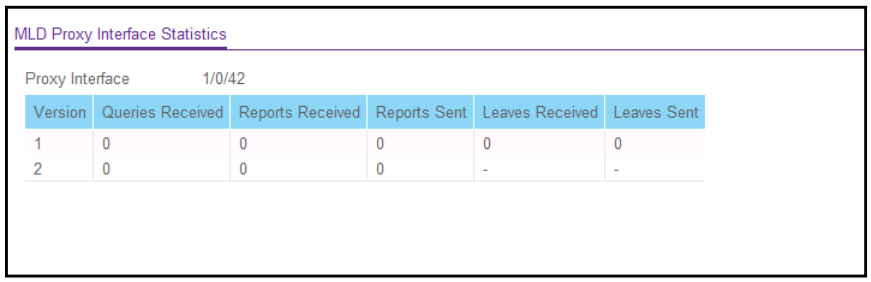
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > Proxy Interface Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 181. Estadísticas de la interfaz proxy MLD multicast IPv6

Campo	Descripción
Proxy Interface	La interfaz en la que se recibieron 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 reportes proxy MLD recibidos.
Reports Sent	El número de reportes proxy MLD enviados.
Leaves Received	El número de mensajes de abandono proxy MLD recibidos.
Leaves Sent	El número de mensajes de abandono proxy MLD enviados.

Ver la membresía del proxy MLD IPv6

Para ver la membresía del proxy MLD multicast IPv6:

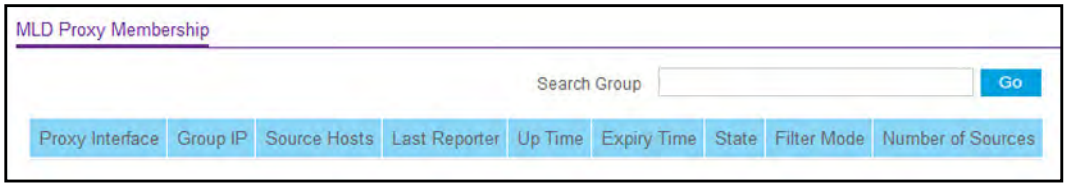
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > MLD > Proxy Membership.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 182. Membresía del proxy MLD multicast IPv6

Campo	Descripción
Proxy Interface	La interfaz en la que está habilitado el proxy MLD.
Group IP	La dirección del grupo multicast IPv6.
Source Hosts	Las direcciones de origen que son miembros de esta dirección multicast.
Last Reporter	La dirección IPv6 del origen del último reporte de membresía recibido para la dirección de grupo multicast IPv6 en la interfaz proxy MLD.
Up Time	Tiempo transcurrido desde que se creó esta entrada.
Expiry Time	El intervalo de expiración de cada dirección de origen que es miembro de este grupo multicast. Es el tiempo después del cual expira la entrada de origen especificada.
State	El estado de la entrada de host. Un host puede estar en uno de los siguientes estados: • Non-member state. No pertenece al grupo en la interfaz. • Delaying member state. El host pertenece al grupo en la interfaz y el temporizador de reportes está en marcha. Este temporizador se usa para enviar los reportes. • Idle member state. El host pertenece al grupo en la interfaz y no hay ningún temporizador de reportes en marcha.
Filter Mode	El modo de filtro de grupo (Include/Exclude/None) del grupo especificado en la interfaz proxy MLD. Los modos posibles son los siguientes: • Include • Exclude • None
Number of Sources	El número de hosts de origen presentes en el grupo multicast seleccionado.

Configurar rutas estáticas multicast IPv6

Para configurar los ajustes de rutas estáticas multicast IPv6:

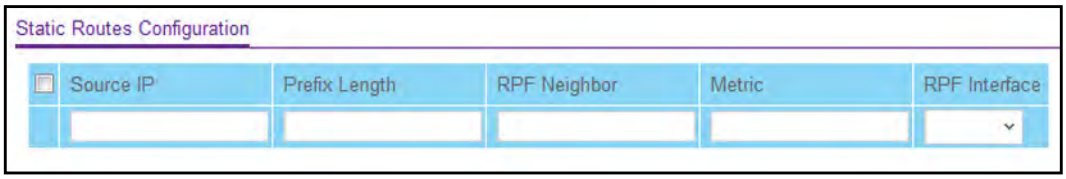
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Routing> IPv6 Multicast > Static Routes Configuration.



5. En el campo Source IP, ingrese la dirección IP que identifica el origen de los paquetes multicast de la entrada que está creando.
6. En el campo Prefix Length, ingrese la longitud de prefijo que se aplica a la dirección IPv6 de origen.
7. En el campo RPF Neighbor, ingrese la dirección IP del router vecino en la ruta hacia el origen.
8. En el campo Metric, ingrese el costo de estado de enlace de la ruta al origen multicast.

   El rango es de 0 a 255; el valor predeterminado es 1. Puede cambiar la métrica de una ruta configurada seleccionando la ruta estática y editando este campo.

9. Seleccione el número de interfaz en la lista RPF Interface.
Es la interfaz que se conecta al router vecino para la dirección IP de origen indicada.
10. Haga clic en el botón Add.
Se agrega la ruta estática al switch.
11. Haga clic en el botón Apply.
La configuración se guarda.

8

8Configurar la calidad de servicio

Este capítulo trata los siguientes temas:

- Descripción general de la calidad de servicio
- Administrar la clase de servicio
- Administrar los servicios diferenciados

Descripción general de la calidad de servicio

En un switch típico, cada puerto físico tiene una o más colas para transmitir paquetes en la red conectada. A menudo se proporcionan varias colas por puerto para dar preferencia a ciertos paquetes sobre otros según criterios definidos por el usuario. Cuando un paquete se pone en cola 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 es necesario un retardo, los paquetes se retienen en la cola hasta que el programador autoriza la cola para la transmisión. Cuando las colas se llenan, los paquetes no pueden retenerse para su transmisión y el switch los descarta.

QoS es un medio para proporcionar una entrega de datos uniforme y predecible al distinguir entre paquetes con requisitos de tiempo estrictos y los que toleran más el retardo. Los paquetes con requisitos de tiempo estrictos reciben un tratamiento especial en una red compatible con QoS. Por ello, todos los elementos de la red deben ser compatibles con QoS. La presencia de al menos un nodo no compatible con QoS crea una deficiencia en la ruta de red y se compromete el rendimiento de todo el flujo de paquetes.

Administrar la clase de servicio

La función de colas Class of Service (CoS) le permite configurar directamente ciertos aspectos de las colas del switch. Esto proporciona el comportamiento de 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 tasa de transmisión, son configurables por el usuario a nivel de cola (o puerto).

Se admiten ocho colas por puerto.

Use CoS para establecer el modo de confianza de Class of Service 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 se establece en un modo confiable, usa una tabla de asignación adecuada para el campo confiable que se usa. Esta tabla de asignación indica la cola CoS a la que se reenvía el paquete en los puertos de salida correspondientes. Por supuesto, el campo confiable debe existir en el paquete para que la tabla de asignación sea útil, por lo que hay acciones predeterminadas cuando no es así. Estas acciones consisten en dirigir el paquete a un nivel CoS específico configurado para el puerto de entrada en 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 la designación de prioridad de ningún paquete entrante y usa en su lugar el valor de prioridad predeterminado del puerto. Todos los paquetes que llegan a la entrada de un puerto no confiable se dirigen a una cola CoS específica en los puertos de salida correspondientes, de acuerdo con la prioridad predeterminada configurada del puerto de entrada. Este proceso también se usa cuando no se puede respetar la asignación de un puerto confiable, por ejemplo, cuando llega un paquete no IP a un puerto configurado para confiar en el valor IP DSCP.

Configurar los ajustes globales de CoS

Para configurar los ajustes globales de CoS:

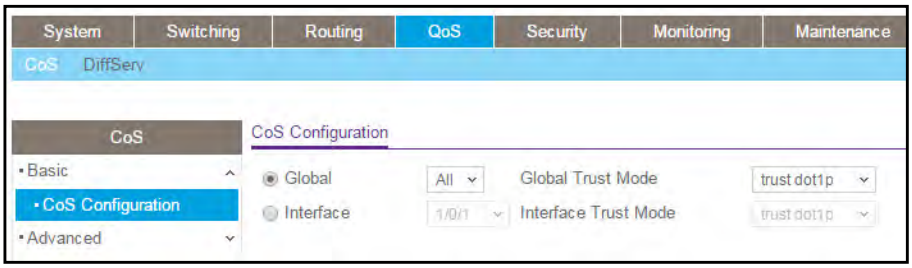
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione QoS> CoS > Basic > CoS Configuration.**



   Nota: También puede ir a esta página seleccionando QoS > CoS > **Advanced > CoS Configuration**.

5. Use Global para especificar todas las interfaces configurables de CoS.
La opción Global representa los ajustes de configuración global más recientes.
6. Use Interface para especificar los ajustes de configuración de CoS por interfaz.
7. Use Global Trust Mode para especificar si se confía en una marca de paquete específica en la entrada. Global Trust Mode puede ser uno de los siguientes:

   - untrusted
   - trust dot1p
   - trust ip-dscp

El valor predeterminado es trust dot1p.
8. Use Interface Trust Mode para especificar si se confía en una marca de paquete específica en la entrada. Interface Trust Mode puede ser uno de los siguientes:

   - untrusted
   - trust dot1p
   - trust ip-dscp

El valor predeterminado es
untrusted.
9. Haga clic en el botón Apply. La
configuración se guarda.

Asignar prioridades 802.1p a colas

La página 802.1p to Queue Mapping también muestra la tabla Current 802.1p Priority Mapping.

Para asignar prioridades 802.1p a colas:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP
del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > CoS > Advanced > 802.1p to Queue Mapping.



5. Use Interface para seleccionar interfaces.

   Puede especificar los ajustes de configuración de CoS por interfaz o para todas las interfaces configurables de CoS.

6. Especifique a qué clase de tráfico interna se asigna el valor 802.1p correspondiente.

   El número de cola depende del hardware específico. La fila 802.1p Priority contiene selectores de clase de tráfico para cada una de las ocho prioridades 802.1p que se asignarán. La prioridad va de baja (0) a alta (3). 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 3, podría ser tráfico sensible al tiempo, como voz o video.

   Los valores de cada lista representan la clase de tráfico. La clase de tráfico es la cola de hardware de un puerto. Los valores más altos de clase de tráfico 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.

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

Asignar valores DSCP a colas

Puede especificar a qué clase de tráfico interna se asigna el valor DSCP correspondiente.

Para asignar valores DSCP a colas:

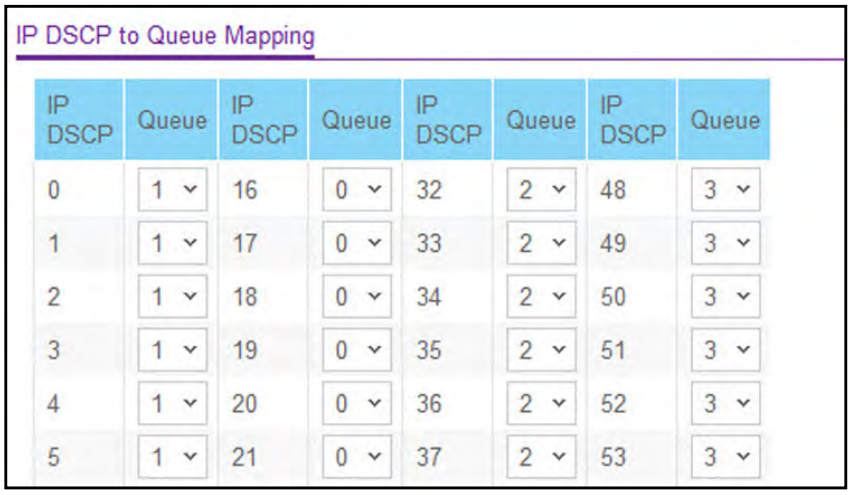
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > CoS > Advanced > IP DSCP to Queue Mapping.



El campo IP DSCP muestra un valor IP DSCP de 0 a 63.

5. 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.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar los ajustes de interfaz CoS de una interfaz

Puede aplicar una tasa de limitación de interfaz a todas las interfaces o a una interfaz específica.

Para configurar CoS en una interfaz:

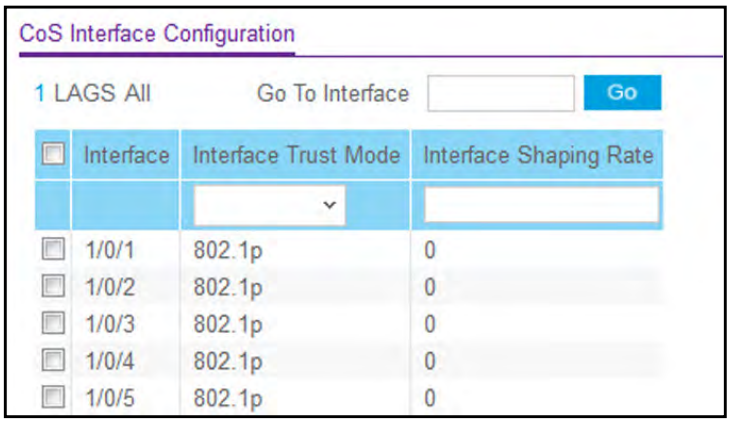
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > CoS> Advanced > CoS Interface Configuration.



5. Seleccione una de las siguientes opciones para especificar qué interfaces se muestran en la página:
   - Seleccione LAG para mostrar la lista de todas las interfaces LAG.
   - Seleccione All para mostrar la lista de todas las interfaces físicas y LAG.
6. Use uno de los siguientes métodos para seleccionar una interfaz:
   - Use el campo Go To Interface para ingresar la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.

     Se selecciona la entrada correspondiente a la interfaz especificada.

   - Seleccione una interfaz de la lista Interface de todas las interfaces configurables de CoS.
7. Use Interface Trust Mode para especificar si se confía o no en una marca de paquete específica en la entrada.

   Interface Trust Mode puede ser uno de los siguientes:

   - Untrusted
   - 802.1p
   - IP DSCP

El valor predeterminado es 802.1p.
8. Use Interface Shaping Rate para especificar el ancho de banda máximo permitido.

Normalmente se usa para limitar la tasa de transmisión de salida. Este valor se controla independientemente 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 rango válido es de 0 a 100 en incrementos de 1. El valor 0 significa que el máximo es ilimitado.

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

Configurar los ajustes de colas CoS de una interfaz

Puede definir lo que hace una cola específica configurando las colas de salida del switch. Los parámetros configurables por el usuario controlan el ancho de banda que usa la cola, la profundidad de la cola en momentos de congestión y la programación de la transmisión de paquetes del conjunto de todas las colas de un puerto. Cada puerto tiene su propia configuración relacionada con colas CoS.

El proceso de configuración se simplifica al permitir que cada parámetro de cola CoS se configure globalmente o por puerto. Un cambio de configuración global se aplica automáticamente a todos los puertos del sistema.

Para configurar los ajustes de colas CoS de una interfaz:

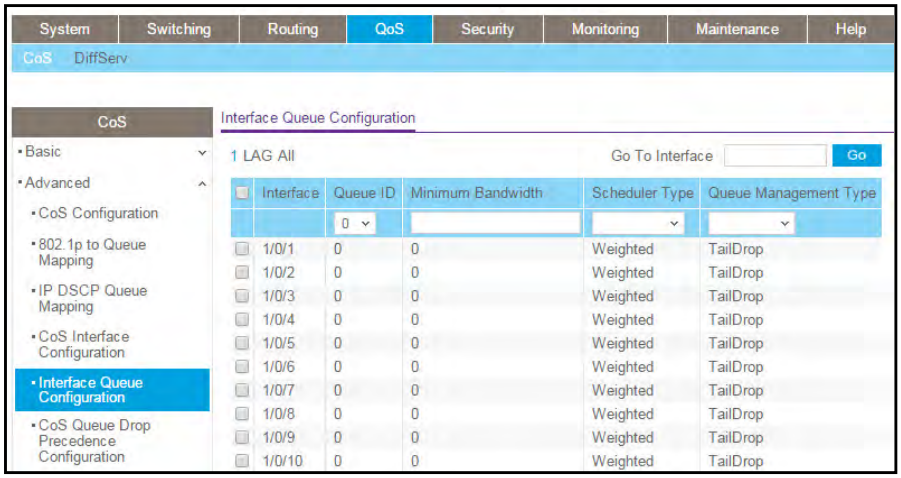
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione QoS > CoS >Advanced > Interface Queue Configuration.



5. Marque la casilla junto al puerto o LAG que desea configurar.

   Puede seleccionar varios puertos y LAG para aplicar el mismo ajuste a las interfaces seleccionadas. Marque la casilla de la fila de encabezado para aplicar un modo de confianza o una tasa a todas las interfaces.

6. Use el menú Queue ID para seleccionar la cola que desea configurar (según la plataforma).

7. Use Minimum Bandwidth para especificar el ancho de banda mínimo garantizado asignado a esta cola.

   Si establece este valor por encima de su ancho de banda máximo correspondiente, el máximo aumenta automáticamente al mismo valor. El valor predeterminado es 0. El rango válido es de 0 a 100 en incrementos de 1. El valor 0 significa que no hay mínimo garantizado. La suma de los valores de Minimum Bandwidth de todas las colas de la interfaz seleccionada no puede exceder el máximo definido (100).

8. Queue Management Type muestra la técnica de administración de profundidad de cola que se usa para las colas de esta interfaz.

   Solo se usa si el dispositivo admite ajustes independientes por cola. En el menú Queue Management Type, seleccione TailDrop o WRED. El valor predeterminado es TailDrop.

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

Configurar los ajustes de precedencia de descarte de CoS

Para configurar los ajustes de precedencia de descarte de CoS:

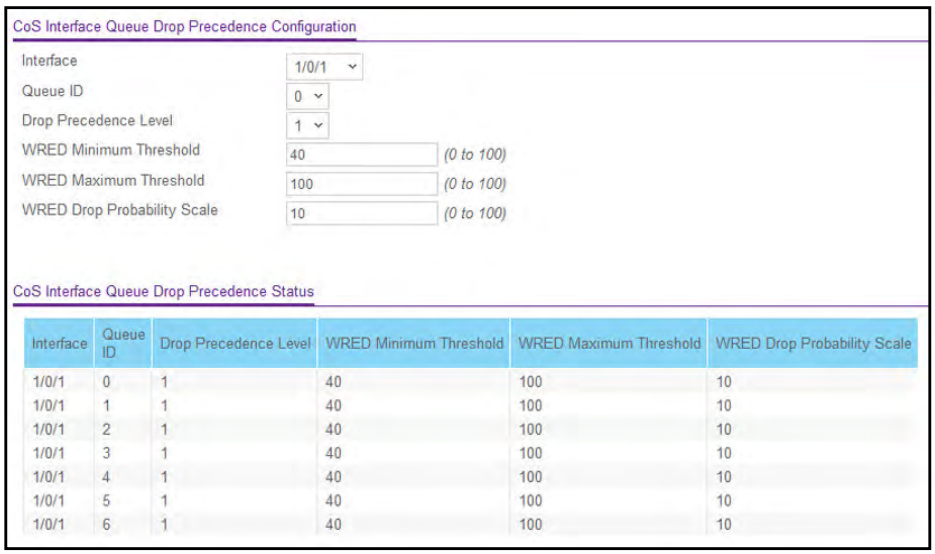
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione QoS > CoS> Advanced > CoS Queue Drop Precedence Configuration.**



5. Use Interface para especificar todas las interfaces configurables de CoS.
6. Use Queue ID para especificar todas las colas disponibles.
Los valores válidos son de 0 a 6. El valor predeterminado es 0.
7. Use Drop Precedence Level para especificar todos los niveles de precedencia de descarte disponibles. Los valores válidos son de 1 a 4. El valor predeterminado es 1.

8. Use WRED Minimum Threshold para especificar el umbral mínimo de cola de RED ponderado por debajo del cual no se descartan paquetes para el nivel de precedencia actual.

   El rango es de 0 a 100. El valor predeterminado es 40.

9. Use WRED Maximum Threshold para especificar 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. El valor predeterminado es 100.

10. Use WRED Drop Probability Scale para determinar la probabilidad de descarte de paquetes del nivel de precedencia de descarte actual.

El rango es de 0 a 100. El valor predeterminado es 10.
11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 183. Estado de precedencia de descarte de colas de interfaz CoS

Campo	Descripción
Interfaz	La interfaz configurable de CoS.
ID de cola	El ID de la cola.
Nivel de precedencia de descarte	El nivel de precedencia de descarte.
Umbral mínimo WRED	Valor del umbral mínimo de cola de RED ponderado.
Umbral máximo WRED	Valor del umbral máximo de cola de RED ponderado.
Escala de probabilidad de descarte WRED	Valor de probabilidad de descarte de paquetes.

Administrar servicios diferenciados

La función QoS incluye compatibilidad con servicios diferenciados (DiffServ), que permite clasificar el tráfico en flujos y darle cierto tratamiento de QoS según comportamientos por salto definidos.

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 sin garantía. En momentos de congestión, los paquetes pueden retrasarse, enviarse esporádicamente o descartarse. Para 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. En cambio, cualquier degradación tiene efectos indeseables en aplicaciones con requisitos de tiempo estrictos, como voz o multimedia.

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 con políticas y defina las instrucciones de la política.
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 política se pueden definir 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 que se realizan dependen de la clase que coincide con el paquete.

El procesamiento de paquetes comienza evaluando los criterios de coincidencia de clase de un paquete. Una política se aplica a un paquete cuando se encuentra una coincidencia de clase dentro de 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 se usan como 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 el protocolo UDP.
  - HTTP. Establece el criterio de coincidencia en el puerto de destino HTTP.
  - FTP. Establece el criterio de coincidencia en el puerto de destino FTP.
  - Telnet. Establece el criterio de coincidencia en el 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.
- Si la vigilancia (policing) está habilitada (es decir, en YES), el estilo de política DiffServ es 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 vigilancia en markdscp ef.
  - Med. Establece la acción de vigilancia en markdscp af31.
  - Low. Establece la acción de vigilancia en send.
- Si la vigilancia está deshabilitada (es decir, en NO), todo el tráfico se marca así:
  - High. Establece la marca de política en ipdscp ef.
  - Med. Establece la marca de política en ipdscp af31.
  - Low. Establece la marca de política en ipdscp be.
- Cada puerto seleccionado se agrega a la política creada.

Usar el asistente DiffServ

Para usar el asistente DiffServ:

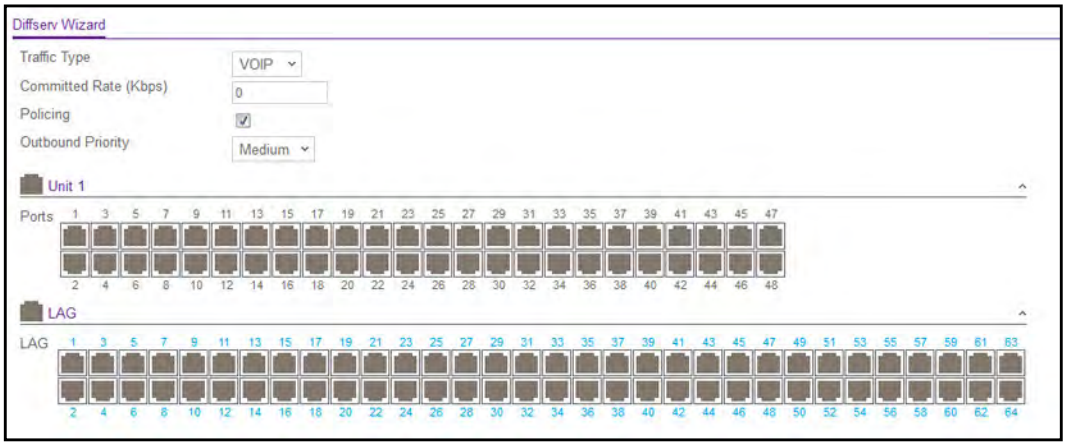
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione QoS> DiffServ > DiffServ Wizard.



5. Use Traffic Type para definir la clase DiffServ.

Las opciones de tipo de tráfico son: VOIP, HTTP, FTP, Telnet y Every.
6. Ports muestra los puertos que se pueden configurar para admitir una política DiffServ. La política DiffServ se agrega a los puertos seleccionados.
7. Use Enable Policing para agregar vigilancia a la política DiffServ. La tasa de vigilancia que se aplicará.

8. Especifique Committed Rate:

- Cuando la vigilancia está habilitada, la tasa comprometida se aplica a la política y la acción de vigilancia se establece en conform.
- Cuando la vigilancia está deshabilitada, la tasa comprometida no se aplica y la política se establece en markdscp.

9. Especifique Outbound Priority:

- Cuando la vigilancia está habilitada, Outbound Priority define el tipo de acción de vigilancia conforme, donde: High establece la acción en markdscp ef, Med la establece en markdscp af31 y Low la establece en send.
- Cuando la vigilancia está deshabilitada, Outbound Priority define la política, donde: High establece la política en mark ipdscp ef, Med la establece en mark ipdscp af31 y Low la establece en mark ipdscp be.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar los ajustes básicos de 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 política se pueden definir 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. Después, se agregan una o más clases a una política. Luego, las políticas se agregan a interfaces.

El procesamiento de paquetes comienza evaluando los criterios de coincidencia de un paquete. La opción de tipo de clase all especifica que cada criterio de una clase debe ser verdadero para que un paquete coincida con esa clase. La opción any especifica que al menos un criterio debe ser verdadero 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 dentro de ella.

Para configurar los ajustes básicos de DiffServ:

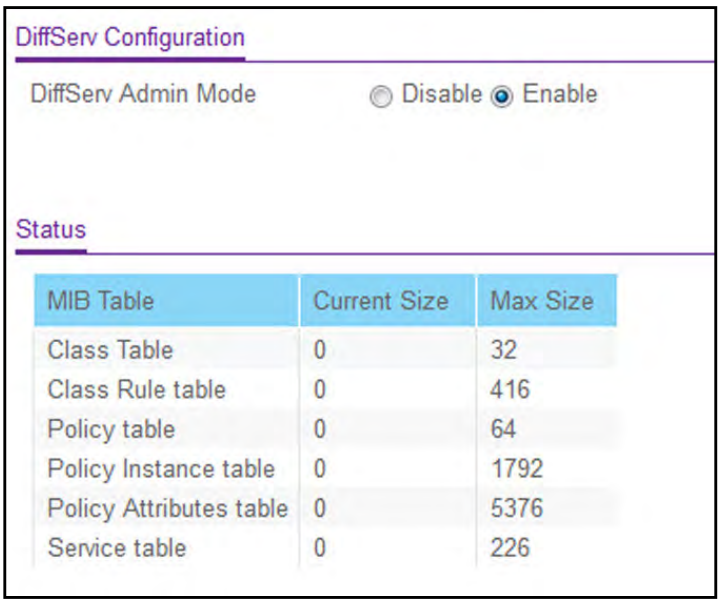
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione QoS> DiffServ > Basic > DiffServ Configuration.**



5. Seleccione el modo administrativo de DiffServ:
   - Enable. Los servicios diferenciados están activos. Es el modo predeterminado.
   - Disable. La configuración de DiffServ se conserva y se puede cambiar, pero no está activa.
6. Haga clic en el botón Aplicar (Apply).

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra.

Tabla 184. Configuración de DiffServ

Campo	Descripción
Tabla de clases	Número actual y máximo de entradas de clasificadores en la tabla. Los clasificadores DiffServ diferencian entre tipos de tráfico.
Tabla de reglas de clase	Número actual y máximo de entradas de reglas de clase en la tabla. Las reglas de clase especifican los criterios de coincidencia de una definición de clase.
Tabla de políticas	Número actual y máximo de entradas de políticas en la tabla. La política determina las acciones de acondicionamiento de tráfico o de aprovisionamiento de servicio aplicadas a una clase de tráfico.
Tabla de instancias de política	Número actual y máximo de entradas de instancias de política-clase en la tabla. Una instancia de política-clase es una política asociada con una clase DiffServ existente.
Tabla de atributos de política	Número actual y máximo de entradas de atributos de política en la tabla. Una entrada de atributo de política vincula varios atributos de política a una instancia de política-clase.
Tabla de servicios	Número actual y máximo de entradas de servicio en la tabla. Una entrada de servicio asocia una política DiffServ con una interfaz y una dirección de entrada o salida.

Configurar los ajustes globales de 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 política se pueden definir 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. Después, se agregan una o más clases a una política. Luego, las políticas se agregan a interfaces.

El procesamiento de paquetes comienza evaluando los criterios de coincidencia de un paquete. La opción de tipo de clase all especifica que cada criterio de una clase debe ser verdadero para que un paquete coincida con esa clase. La opción any especifica que al menos un criterio debe ser verdadero 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 dentro de ella.

Para configurar el modo global de DiffServ:

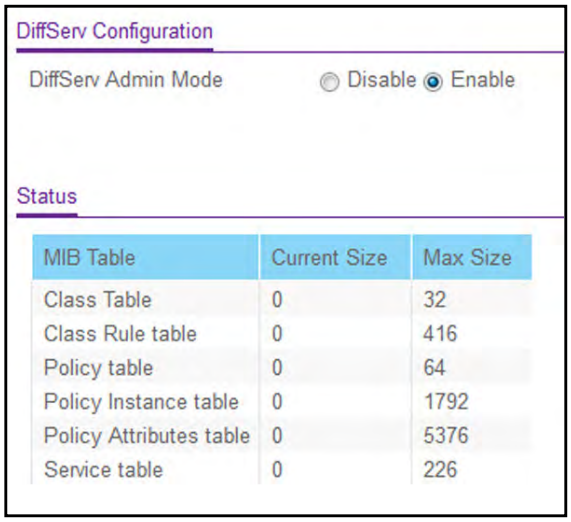
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > DiffServ > Advanced > Diffserv Configuration.



5. Seleccione el modo administrativo de DiffServ:
   - Enable. Los servicios diferenciados están activos.
   - Disable. La configuración de DiffServ se conserva y se puede cambiar, pero no está activa.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

La siguiente tabla describe la información que se muestra en la tabla Status de la página DiffServ Configuration.

Tabla 185. Estado de DiffServ

Campo	Descripción
Tabla de clases	Número de clases DiffServ configuradas respecto al total permitido en el switch.
Tabla de reglas de clase	Número de reglas de clase configuradas respecto al total permitido en el switch.

Tabla 185. Estado de DiffServ (continuación)

Campo	Descripción
Tabla de políticas	Número de políticas configuradas respecto al total permitido en el switch.
Tabla de instancias de política	Número de instancias de política-clase configuradas respecto al total permitido en el switch.
Tabla de atributos de política	Número de atributos de política configurados (vinculados a las instancias de política-clase) respecto al total permitido en el switch.
Tabla de servicios	Número de servicios configurados (vinculados a las políticas en interfaces especificadas) respecto al total permitido en el switch.

Configurar una clase DiffServ

Puede agregar un nombre de clase DiffServ nuevo o cambiar el nombre de una clase existente o eliminarla. También puede definir los criterios que se asocian con una clase DiffServ. Al recibir 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. Después de crear una clase, haga clic en su vínculo para ir a la página Class.

Para configurar una clase DiffServ:

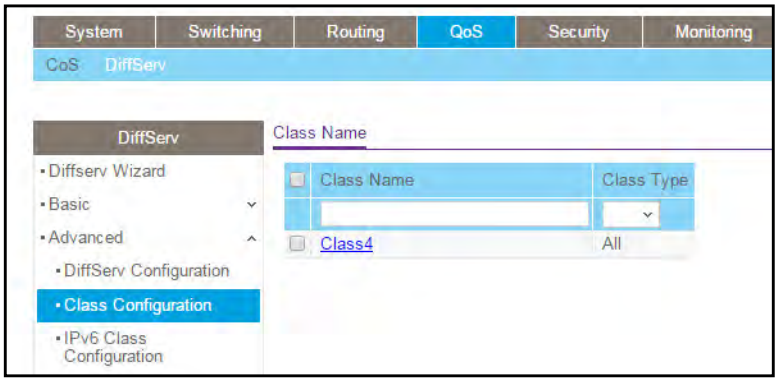
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > DiffServ > Advanced > Class Configuration.



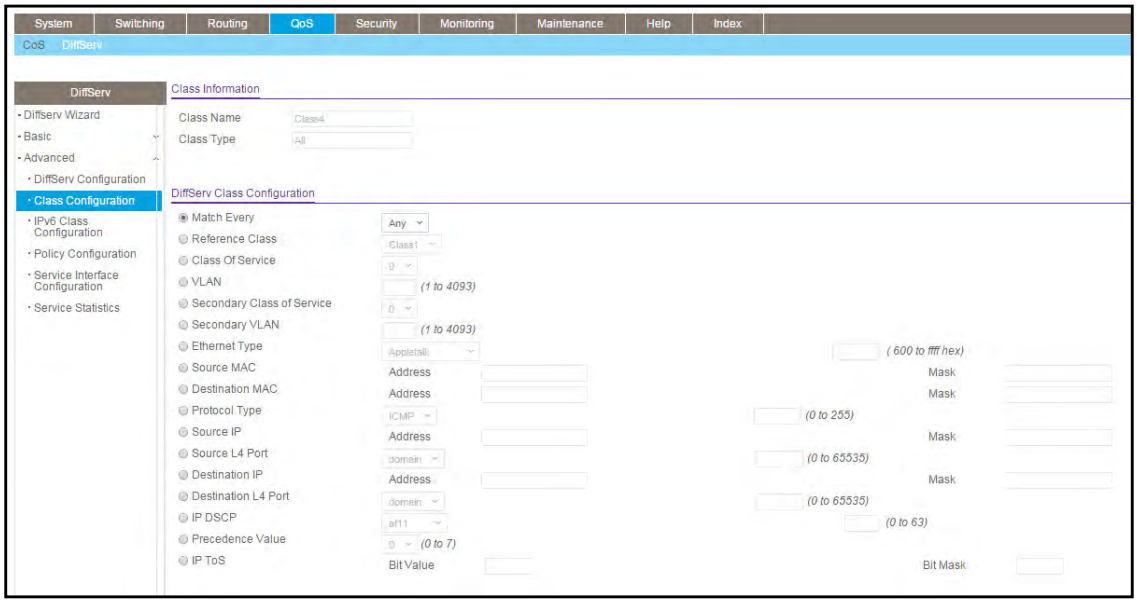
5. Para crear una clase nueva, ingrese un nombre de clase, seleccione el tipo de clase y haga clic en el botón Add.

   Este campo también enumera todos los nombres de clases DiffServ existentes, de los cuales puede seleccionar uno. El switch solo admite el valor de Class Type All, que significa que deben cumplirse todos los criterios de coincidencia definidos para la clase para que un paquete coincida. All indica el AND lógico de todos los criterios. Solo puede seleccionar el tipo de clase al crear una clase nueva. Después de crearla, el campo Class Type deja de ser configurable.

6. Para cambiar el nombre de una clase existente, marque la casilla junto a la clase configurada y actualice el nombre.
7. Haga clic en el botón Apply.
La configuración se guarda.
8. Después de crear una clase, haga clic en el nombre de una clase existente. El nombre de la clase es un hipervínculo.



   Se muestra la página Class Configuration con los campos de configuración de la clase.



9. Para configurar los detalles de la clase, complete los campos:
   - Class Name. El nombre de la clase DiffServ configurada.
   - Class Type. El tipo de clase DiffServ.

Solo puede seleccionar el tipo de clase al crear una clase nueva. Después de crearla, este campo muestra el tipo de clase, pero no puede cambiarlo.

10. Defina los criterios que se asocian con una clase DiffServ:
    - Match Every. Agrega a la definición de la clase una condición según la cual todos los paquetes se consideran parte de la clase.
    - Reference Class. Seleccione esta opción para hacer referencia a otra clase para los criterios. Los criterios definidos en la clase de referencia se usan además de los criterios que defina para la clase seleccionada. Al 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 lo sumo a otra clase del mismo tipo.
    - Class of Service. Seleccione esta opción para exigir que el valor de Class of Service (CoS) del encabezado de la trama Ethernet coincida con el valor de CoS especificado. Esta opción enumera todos los valores del criterio Class of Service en el rango de 0 a 7, de los cuales puede seleccionar uno.
    - VLAN. Seleccione esta opción para exigir que el ID de VLAN de un paquete coincida con un ID de VLAN o con un ID dentro de un rango continuo. Si configura un rango, hay coincidencia si el ID de VLAN del paquete es igual a cualquier ID de VLAN del rango. El valor de VLAN está en el rango de 0 a 4093.
    - Secondary Class of Service. Seleccione esta opción para exigir que el valor secundario de Class of Service (CoS) del encabezado de la trama Ethernet coincida con el valor secundario de CoS especificado.
    - Secondary VLAN. Seleccione esta opción para exigir que el ID de VLAN de un paquete coincida con un ID de VLAN secundario o con uno dentro de un rango continuo. Si configura un rango, hay coincidencia si el ID de VLAN secundario del paquete es igual a cualquier ID de VLAN secundario del rango. Después de seleccionar esta opción, use los siguientes campos para configurar los criterios de VLAN secundaria:
        - Secondary VLAN ID Start. El ID de VLAN secundario que debe coincidir o el ID de VLAN secundario con el valor más bajo del rango de VLAN.
        - Secondary VLAN ID End. El ID de VLAN secundario con el valor más alto del rango de VLAN. Este campo no es necesario si el criterio es un solo ID de VLAN.
    - Ethernet Type. Seleccione esta opción para exigir que el valor EtherType del encabezado de la trama Ethernet coincida con el valor EtherType especificado. Después de seleccionar esta opción, especifique EtherType Keyword en la lista de protocolos comunes asignados a su valor EtherType.
    - Source MAC Address. Seleccione esta opción para exigir que la dirección MAC de origen de un paquete coincida con la dirección MAC especificada. Después de seleccionar esta opción, use los siguientes campos para configurar los criterios de dirección MAC de origen:
        - MAC Address. La dirección MAC de origen que debe coincidir.
        - MAC 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 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 aa:bb:xx:xx:xx:xx generan

una coincidencia (donde x es cualquier número hexadecimal). Tenga en cuenta que no es una máscara comodín como la que usan las ACL.

- Source MAC Mask. Máscara de bits con el mismo formato que una dirección MAC que indica qué partes de la dirección MAC de origen se usan para comparar con el contenido del paquete.
- Destination MAC Address. Seleccione esta opción para exigir que la dirección MAC de destino de un paquete coincida con la dirección MAC especificada. Después de seleccionar esta opción, use los siguientes campos para configurar los criterios de dirección MAC de destino:
  - MAC Address. La dirección MAC de destino que debe coincidir.
  - MAC 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 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 aa:bb:xx:xx:xx:xx generan una coincidencia (donde x es cualquier número hexadecimal). Tenga en cuenta que no es una máscara comodín como la que usan las ACL.
- Destination MAC Mask. Máscara de bits con el mismo formato que una dirección MAC que indica qué partes de la dirección MAC de destino se usan para comparar con el contenido del paquete.
- Protocol Type. Enumera las palabras clave de los protocolos de capa 4, de las cuales puede seleccionar una. La lista incluye 'other' como opción para los demás valores.
- Source IP Address. Una dirección IP de origen válida en formato decimal con puntos.
- Source Mask. 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 esta opción para exigir que el puerto de origen TCP/UDP de un paquete coincida con el puerto especificado o con un número dentro de un rango de puertos. Si configura un rango, hay coincidencia si el puerto de origen del paquete es igual a cualquier puerto de origen del rango. Después de seleccionar esta opción, use los siguientes campos para configurar una palabra clave, un número o un rango de puertos de origen para los criterios de coincidencia:
  - Protocol. Seleccione en la lista la palabra clave L4 en la que se basa la coincidencia. Si selecciona una palabra clave, los demás campos de puerto de origen no están disponibles.
  - Port End. Número de puerto de origen L4 definido por el usuario que debe coincidir o el número de puerto de origen con el valor más bajo del rango de puertos.
  - Port Start. El puerto de origen con el valor más alto del rango de puertos. Este campo no es necesario si el criterio es un solo puerto.
- Destination IP Address. Una dirección IP de destino válida en formato decimal con puntos.
- DestinationMask. 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 esta opción para exigir que el puerto de destino TCP/UDP de un paquete coincida con el puerto especificado o con un número dentro de un rango de puertos. Si

configura un rango, hay coincidencia si el puerto de destino del paquete es igual a cualquier puerto de destino del rango. Después de seleccionar esta opción, use los siguientes campos para configurar una palabra clave, un número o un rango de puertos de destino para los criterios de coincidencia:

  - Protocol. Seleccione en la lista la palabra clave L4 en la que se basa la coincidencia. Si selecciona una palabra clave, los demás campos de puerto de destino no están disponibles.
  - Port End. Número de puerto de destino L4 definido por el usuario que debe coincidir o el número de puerto de destino con el valor más bajo del rango de puertos.
  - Port Start. El puerto de destino con el valor más alto del rango de puertos. Este campo no es necesario si el criterio es un solo puerto.

- IP DSCP. Seleccione esta opción para exigir que el valor IP DiffServ Code Point (DSCP) del paquete coincida con el valor especificado. El valor DSCP se define como los seis bits de orden superior del octeto Service Type del encabezado IP. Después de seleccionar esta opción, use uno de los siguientes campos para configurar los criterios de IP DSCP.
  - IP DSCP Keyword. La palabra clave IP DSCP que corresponde al valor IP DSCP que debe coincidir. Si selecciona una palabra clave, no puede configurar un valor IP DSCP.
  - IP DSCP Value. El valor IP DSCP que debe coincidir.
- Precedence Value. Seleccione esta opción para exigir que el valor IP Precedence del paquete coincida con el número configurado en el campo IP Precedence Value. El campo IP Precedence de un paquete se define como los tres bits de orden superior del octeto Service Type del encabezado IP.
- IP ToS. Seleccione esta opción para exigir que los bits Type of Service (ToS) del encabezado IP del paquete coincidan con el valor especificado. El campo IP ToS de un paquete se define como los ocho bits del octeto Service Type del encabezado IP. Después de seleccionar esta opción, use los siguientes campos para configurar los criterios de ToS:
  - ToS Bits. Ingrese un valor de octeto hexadecimal de dos dígitos en el rango de 00 a ff para comparar con los bits del campo ToS del paquete.
  - ToS 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.
La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra en Class Summary, en la parte inferior de la página DiffServ Advanced Class Configuration.

Tabla 186. Configuración de clases DiffServ - Resumen de clases

Campo	Descripción
Match Criteria	Los criterios de coincidencia configurados para la clase especificada.
Values	Los valores de los criterios de coincidencia configurados.

Configurar los ajustes de clases DiffServ IPv6

Puede agregar un nuevo nombre de clase DiffServ IPv6, o cambiar el nombre de una clase existente o eliminarla. También puede definir los criterios que se asociarán a 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. Después de crear una clase, haga clic en el enlace de la clase para ir a la página Class.

Para configurar los ajustes de clases DiffServ IPv6:

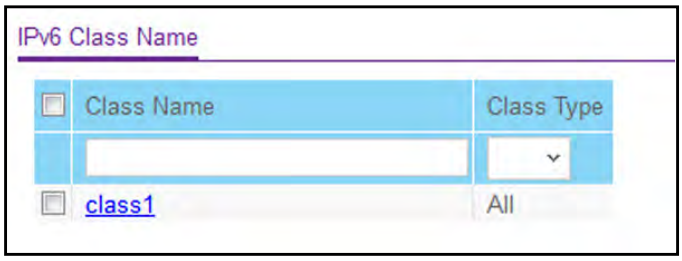
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > DiffServ > Advanced > IPv6 Class Configuration.



5. Para crear una clase nueva, ingrese un nombre de clase, seleccione el tipo de clase y haga clic en el botón Add.

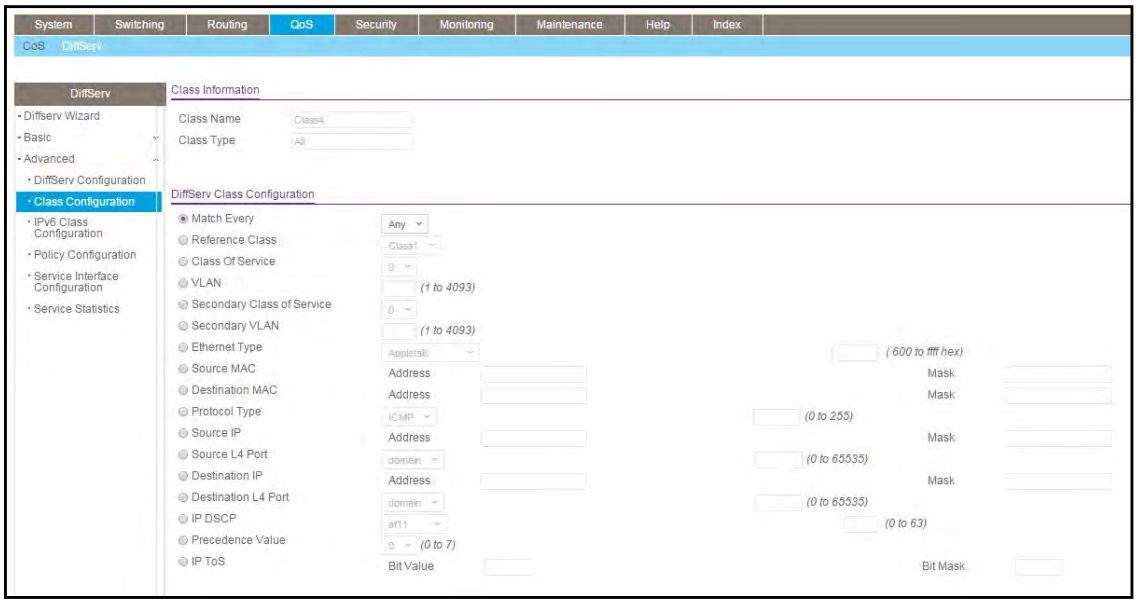
   Este campo también muestra todos los nombres de clases DiffServ existentes, entre los que puede seleccionar uno. El switch solo admite el valor de Class Type All, que significa que todos los criterios de coincidencia definidos para la clase deben cumplirse para que un paquete coincida. All significa el AND lógico de todos los criterios de coincidencia. Este campo es un selector solo al crear una clase nueva. Después de crear la clase, se convierte en un campo no configurable que muestra el tipo de clase configurado.

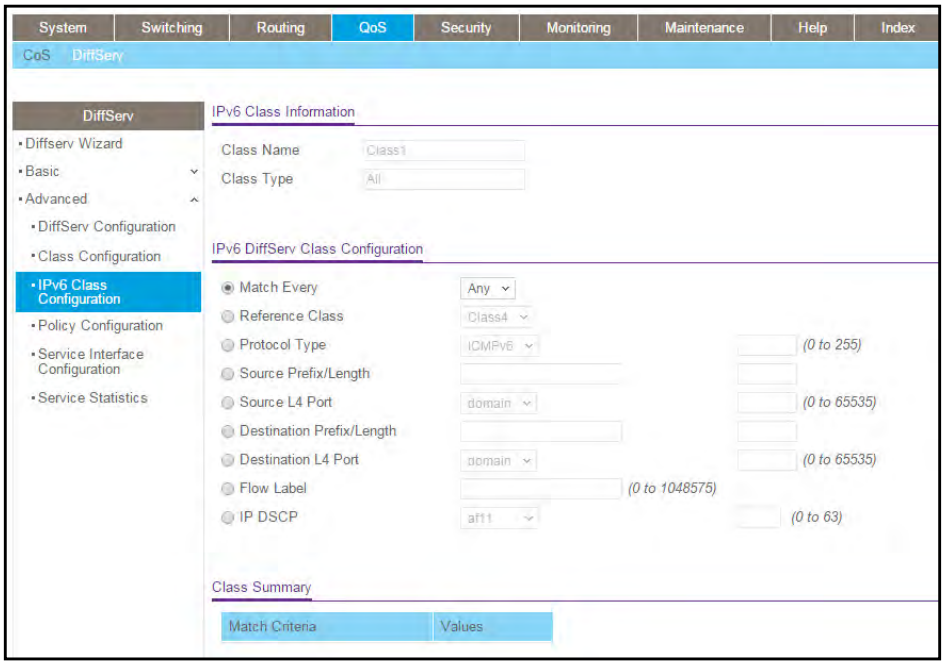
6. Para cambiar el nombre de una clase existente, seleccione la casilla junto a la clase configurada y actualice el nombre

7. Haga clic en el botón Apply.
La configuración se guarda.
8. Después de crear una clase, haga clic en el nombre de una clase existente. El nombre de la clase es un hipervínculo.



Se muestra la página Class Configuration con los campos de configuración de la clase.





9. Para configurar la clase IPv6, complete los campos:

- Class Name. El nombre de la clase DiffServ configurada.
- Class Type. El tipo de clase DiffServ.

  Solo puede especificar el tipo de clase al crear una clase nueva. Después de crear la clase, este campo muestra el tipo de clase, pero no puede cambiarlo.

10. Defina los criterios que se asocian con una clase DiffServ:
    - Match Every. Agrega a la definición de la clase una condición según la cual todos los paquetes se consideran parte de la clase.
    - Reference Class. Muestra las clases que pueden asignarse como clases de referencia a la clase actual.
    - Protocol Type. Enumera las palabras clave de los protocolos de capa 4, de las cuales puede seleccionar una. La lista incluye 'other' como opción para los demás valores.
    - Source Prefix Length. Es un prefijo IPv6 de origen válido para comparar con un paquete IPv6. El prefijo siempre se especifica con su longitud. El prefijo puede introducirse en el rango de 0 a FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF y la longitud del prefijo en el rango de 0 a 128.
    - Source L4 Port. Muestra las palabras clave de los puertos de capa 4 de origen conocidos, entre las que puede seleccionar una. La lista incluye 'other' como opción para los puertos sin nombre.
    - Destination Prefix/Length. Es un prefijo IPv6 de destino válido para comparar con un paquete IPv6. El prefijo siempre se especifica con su longitud. El prefijo puede introducirse en el rango de 0 a FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF y la longitud del prefijo en el rango de 0 a 128.
    - Destination L4 Port. Muestra las palabras clave de los puertos de capa 4 de destino conocidos, entre las que puede seleccionar una. La lista incluye 'other' como opción para los puertos sin nombre.
    - Flow Label. Es un número de 20 bits único de un paquete IPv6, que usan las estaciones finales para indicar el tratamiento de calidad de servicio en los routers. La etiqueta de flujo puede especificarse en el rango de 0 a 1048575.
    - IP DSCP. Puede seleccionar una palabra clave para los valores DSCP conocidos. La lista incluye Other como opción para los valores restantes.

11. Match Criteria. Muestra los criterios de coincidencia configurados para la clase especificada.
12. Values. Muestra los valores de los criterios de coincidencia configurados.
13. Haga clic en el botón Aplicar (Apply).

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra en Class Summary, en la parte inferior de la página DiffServ Advanced IPv6 Class Configuration.

Tabla 187. Configuración de clases DiffServ IPv6 - Resumen de clases

Campo	Descripción
Match Criteria	Los criterios de coincidencia configurados para la clase especificada.
Values	Los valores de los criterios de coincidencia configurados.

Configurar una política DiffServ

Puede asociar un conjunto de clases con una o más instrucciones de política. Después de crear una política, haga clic en el enlace de la política para ir a la página Policy.

Para configurar una política DiffServ:

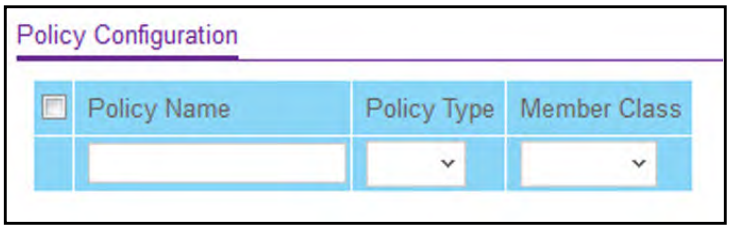
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > DiffServ > Advanced > Policy Configuration.

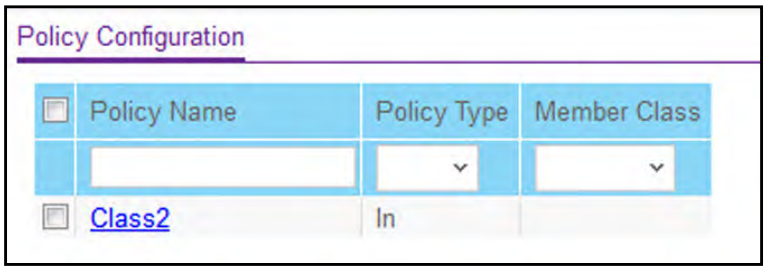


5. Use Policy Name para identificar de forma única una política DiffServ con una cadena alfanumérica de 1 a 31 caracteres que distingue mayúsculas y minúsculas.
6. En la lista Member Class, seleccione una clase DiffServ.

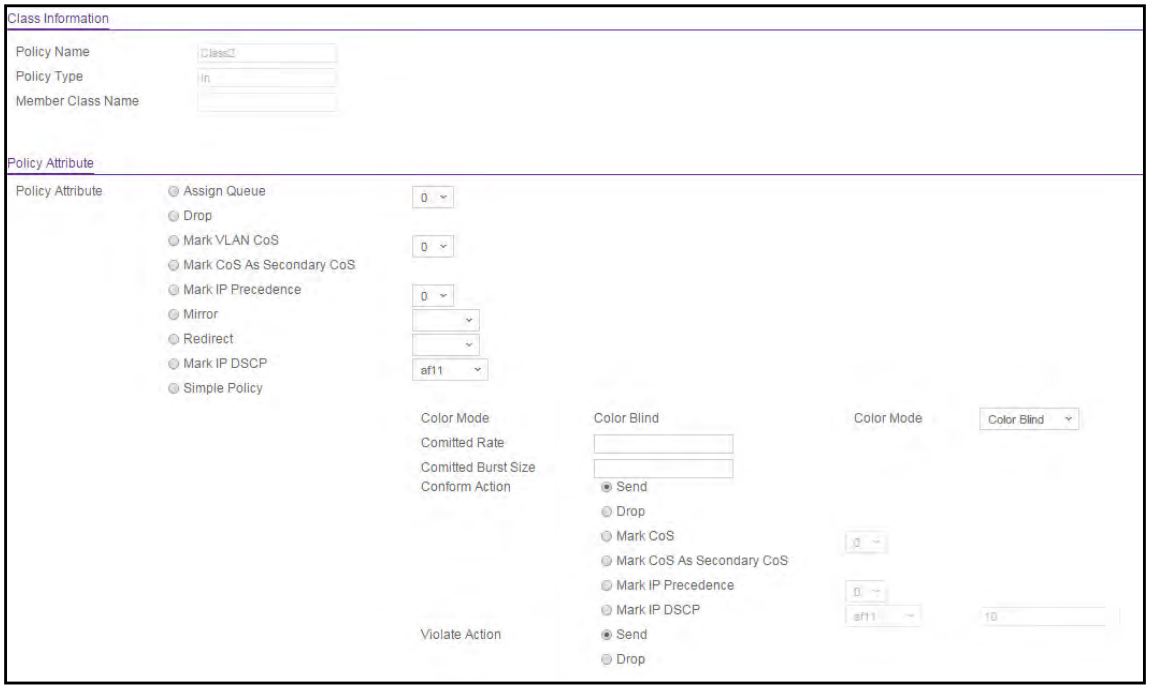
   Muestra todas las clases DiffServ existentes definidas actualmente como miembros de la política especificada. Esta lista se actualiza automáticamente al agregar o quitar una clase de la política. Este campo es un selector solo cuando se va a quitar una instancia de clase de política existente. Después de quitarla, se convierte en un campo no configurable.

7. Policy Type. La dirección del flujo de tráfico a la que se aplica la política.
   - In indica que el tipo es específico para la dirección de tráfico entrante.
   - Out indica que el tipo es específico para la dirección de tráfico saliente.

8. Haga clic en el botón Add.
La nueva política se agrega al switch.
9. Para configurar los atributos de la política, haga clic en el nombre de la política. El nombre de la política es un hipervínculo.



Se muestra la página Policy Configuration con los campos de configuración de la política.



10. Seleccione Assign Queue, la cola a la que se asignan los paquetes de esta clase de política. Es un valor entero en el rango de 0 a 6.

11. Configure los atributos de la política:

- Drop. Seleccione el botón de opción drop. Este indicador señala que el atributo de la política está definido para descartar todos los paquetes entrantes.
- Mark VLAN CoS. Es un valor entero en el rango de 0 a 7 para establecer la prioridad de la VLAN.
- Mark CoS as Secondary Cos. Esta opción marca los bits de prioridad de la etiqueta VLAN externa de todos los paquetes con la prioridad de la etiqueta VLAN interna. En esencia, el CoS de la etiqueta VLAN interna se copia en el CoS de la etiqueta VLAN externa.

- Mark IP Precedence. Es un valor de precedencia IP en el rango de 0 a 7.
- **Mirror**
- **Redirect**
- Two Rate Policy. Con el policer de dos tasas, puede aplicar la vigilancia del tráfico según dos tasas independientes: Committed Rate y Peak Rate.
- Mark IP DSCP. Muestra las palabras clave de los valores DSCP conocidos, entre las que puede seleccionar una. La lista incluye 'other' como opción para los valores restantes.
- Simple Policy. Use este atributo para establecer el estilo de vigilancia del tráfico de la clase especificada. Este comando usa una sola tasa de datos y un tamaño de ráfaga, con dos resultados (conform y violate).

12. Si selecciona el atributo Simple Policy, puede configurar los siguientes campos:
    - Color Mode. Muestra el modo de color. El valor predeterminado es Color Blind.
      - **Color Blind**
      - **Color Aware**

        El modo Color Aware requiere que existan una o más clases de color válidas para usarse con esta instancia de política. Una clase de color válida contiene un solo criterio de coincidencia no excluido para uno de los siguientes campos (siempre que el campo no entre en conflicto con el clasificador de la propia instancia de política):

      - **CoS**
      - **IP DSCP**
      - **IP Precedence**
    - Committed Rate. Este valor se especifica en el rango de 1 a 4294967295 kilobits por segundo (Kbps).
    - Committed Burst Size. Este valor se especifica en el rango de 1 a 128 KBytes. El tamaño de ráfaga comprometido determina la cantidad de tráfico conforme permitida.
    - Conform Action. Muestra las acciones que se aplicarán a los paquetes conformes según las métricas de vigilancia, entre las que puede seleccionar una. El valor predeterminado es send.
    - Violate Action. Muestra las acciones que se aplicarán a los paquetes infractores según las métricas de vigilancia, entre las que puede seleccionar una. El valor predeterminado es send.
    - Para cada selector de acción puede elegirse una de las siguientes acciones:
      - Drop. Estos paquetes se descartan inmediatamente.
      - Mark IP DSCP. DiffServ marca estos paquetes con el valor DSCP especificado antes de presentarlos al elemento de reenvío del sistema. Esta opción requiere que se establezca el campo DSCP.
      - Mark CoS. DiffServ marca estos paquetes con el valor CoS especificado antes de presentarlos al elemento de reenvío del sistema. Esta opción requiere que se establezca el campo Mark CoS.
      - Mark CoS As Secondary CoS. Seleccione esta opción para marcar todos los paquetes de un flujo de tráfico con el número de cola CoS secundaria especificado. Use el campo Class of Service para seleccionar el valor CoS que se marcará en el campo de prioridad del encabezado 802.1p de la

etiqueta 802.1Q secundaria (interna) de un paquete con doble etiqueta VLAN. Si el paquete no contiene ya este encabezado, se inserta uno.

- Send. DiffServ presenta estos paquetes sin modificar al elemento de reenvío del sistema.
- Mark IP Precedence. DiffServ marca estos paquetes con el valor de IP Precedence especificado antes de presentarlos al elemento de reenvío del sistema. Esta opción requiere que se establezca el campo Mark IP Precedence.

13. Si selecciona Two Rate, puede configurar campos adicionales (los mismos que para una política simple).

14. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 188. Configuración de políticas DiffServ - Atributo de política

Campo	Descripción
Policy Name	Muestra el nombre de la política DiffServ.
Policy Type	Muestra el tipo de la política como In.
Member Class Name	Muestra el nombre de cada instancia de clase dentro de la política.

Configurar la interfaz de servicio DiffServ

Para configurar la interfaz de servicio DiffServ:

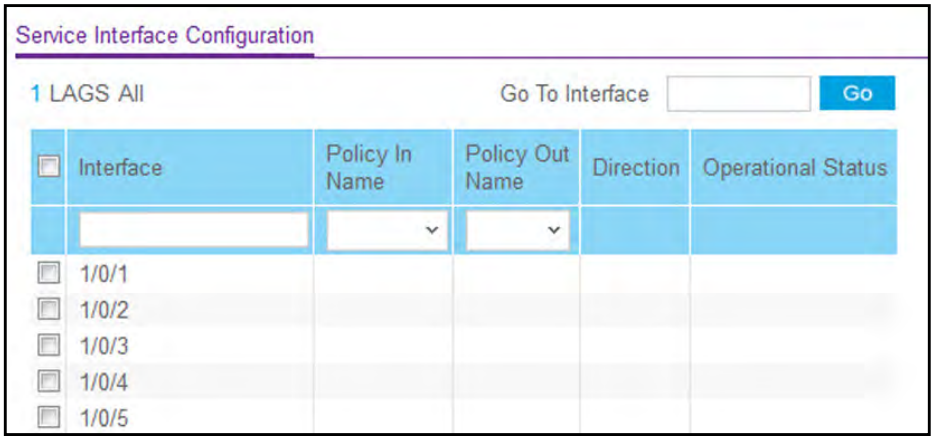
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > DiffServ > Advanced > Service Interface Configuration.



5. 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, seleccione la casilla de la interfaz que desea configurar.
6. Policy Name. Muestra todos los nombres de políticas, entre los que puede seleccionar uno.

   Este campo no se muestra a los usuarios de lectura/escritura cuando la plataforma no admite la asociación de políticas de servicio entrantes.

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

Tabla 189. Configuración de la interfaz de servicio

Campo	Descripción
Direction	Indica que la dirección del tráfico de esta interfaz de servicio es In.
Operational Status	Muestra el estado operativo de esta interfaz de servicio, Up o Down.

Ver las estadísticas de servicio DiffServ

Esta página muestra información estadística orientada a clases de la política, especificada por la interfaz y la dirección. La lista Member Class se completa según la interfaz y la dirección especificadas y, por lo tanto, según la política asociada (si la hay). Al resaltar un nombre de clase miembro se muestra la información estadística de la instancia de clase de política para la interfaz y dirección especificadas.

Para ver las estadísticas de servicio DiffServ:

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

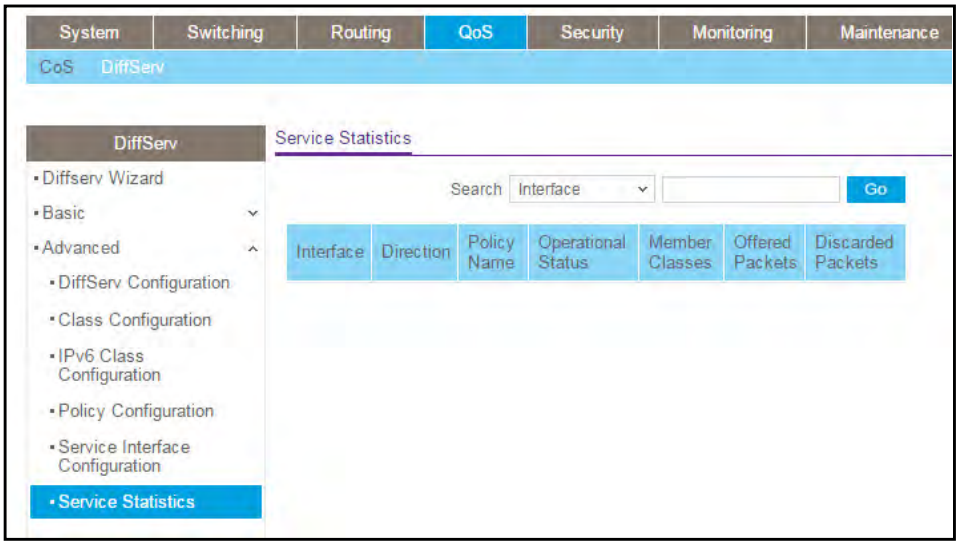
Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione QoS > DiffServ > Advanced > Service Statistics.



5. Use el menú Search para buscar estadísticas DiffServ por interfaz o clase miembro:

- Para buscar por interfaz, seleccione Interface, introduzca la interfaz con el formato unidad/ranura/puerto (por ejemplo, 1/0/13) y haga clic en el botón Go.

  Si la entrada existe, se muestra primero, seguida de las demás 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 una clase miembro coincidente, se muestra como la primera entrada, seguida de las demás. Se requiere una coincidencia exacta.

6. Para actualizar la página con la información más reciente del switch, haga clic en el botón Actualizar (Refresh). La siguiente tabla describe la información disponible en la página Service Statistics.

Tabla 190. Estadísticas de servicio DiffServ

Campo	Descripción
Interface	Lista de todas las combinaciones válidas de número de ranura y puerto del sistema con una política DiffServ asociada actualmente en dirección In.
Direction	Lista de la dirección del tráfico de la interfaz como In. Muestra solo las direcciones para las que hay una política DiffServ asociada actualmente.

Tabla 190. Estadísticas de servicio DiffServ (continuación)

Campo	Descripción
Policy Name	Nombre de la política asociada actualmente a la interfaz y la dirección especificadas.
Operational Status	Estado operativo de la política asociada actualmente a la interfaz y la dirección especificadas. El valor es Up o Down.
Member Classes	Lista de todas las clases DiffServ definidas actualmente 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 queda vacía.
Offered Packets	Recuento del número total de paquetes ofrecidos a todas las instancias de clase de esta política de servicio antes de aplicar su tratamiento DiffServ definido. Es el recuento total por interfaz y por dirección.
Discarded Packets	Recuento del número total de paquetes descartados para todas las instancias de clase de esta política de servicio por cualquier motivo debido al tratamiento DiffServ. Es el recuento total por interfaz y por dirección. Los paquetes descartados se admiten en la dirección entrante, pero no en la saliente.

9

9Administrar la seguridad del switch

Puede configurar la contraseña de inicio de sesión, los ajustes de Remote Authorization Dial-In User Service (RADIUS), los ajustes de Terminal Access Controller Access Control System (TACACS) y las listas de autenticación.

Este capítulo trata los siguientes temas:

- Administrar cuentas de usuario y contraseñas
- Administrar los ajustes del servidor RADIUS
- Administrar los ajustes de TACACS
- Configurar listas de autenticación
- Ver sesiones de inicio de sesión
- Administrar el acceso HTTP, HTTPS y SSH
- Configurar el acceso Telnet
- Configurar el acceso por el puerto de consola
- Configurar los ajustes de denegación de servicio
- Configurar los ajustes de control de acceso
- Administrar la autenticación de puertos
- Controlar el tráfico con filtrado MAC
- Configurar la seguridad de puertos y los grupos privados
- Configurar puertos protegidos
- Configurar VLAN privadas
- Administrar los ajustes de control de tormentas
- Configurar DHCP snooping
- Configurar interfaces IP Source Guard
- Configurar Dynamic ARP Inspection
- Configurar portales cautivos
- Configurar y administrar listas de control de acceso

Administrar cuentas de usuario y contraseñas

Puede configurar cuentas de usuario y contraseñas de inicio de sesión.

Configurar cuentas de usuario

De forma predeterminada, existen dos cuentas de usuario:

- admin, con privilegios de lectura/escritura
- guest, con privilegios de solo lectura

Los nombres de cuenta no distinguen mayúsculas y minúsculas.

La primera vez que inicie sesión como usuario administrador en la UI del navegador local, no se requiere contraseña (es decir, la contraseña está en blanco). A partir de la versión de software 12.0.9.3, después de iniciar sesión por primera vez, deberá especificar una contraseña local del dispositivo que deberá usar cada vez que inicie sesión.

Un usuario guest no puede iniciar sesión hasta que el usuario admin especifique una contraseña para él.

Si inicia sesión como usuario admin con privilegios de lectura/escritura, puede asignar contraseñas y establecer parámetros de seguridad para las cuentas predeterminadas, y agregar y eliminar cuentas (excepto la cuenta admin), hasta un máximo de seis cuentas. Como usuario admin con privilegios de lectura/escritura puede modificar datos en las páginas de la UI del navegador local.

Para agregar una cuenta de usuario:

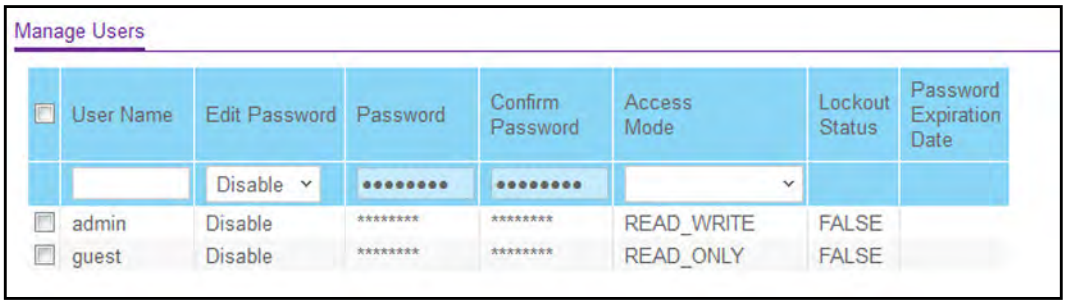
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Security> Management Security > Local User > User Management.**



5. En el campo User Name, introduzca el nombre de la nueva cuenta.

   Solo puede introducir un nombre de usuario nuevo al crear una cuenta. Los nombres de usuario tienen hasta 64 caracteres y no distinguen mayúsculas y minúsculas. Los caracteres válidos incluyen 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.

6. Establezca el campo Edit Password en Enable solo cuando vaya a cambiar la contraseña. El valor predeterminado es Disable.
7. 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.

8. En el campo Confirm Password, introduzca de nuevo la contraseña para confirmar que la escribió correctamente.

   Este campo no muestra la contraseña al escribirla, sino asteriscos (*).

   El campo Access Mode muestra el modo de acceso del usuario. La cuenta admin siempre tiene acceso de lectura/escritura y a todas las demás cuentas se les asigna acceso de solo lectura. El valor predeterminado es de solo lectura.

   El campo Lockout Status indica si la cuenta de usuario está bloqueada (TRUE o FALSE).

El campo Password Expiration Date indica la fecha de vencimiento actual de la contraseña.
9. Haga clic en el botón Add.
Se agrega la cuenta de usuario.

Configurar una contraseña de usuario

Para configurar una contraseña de usuario:

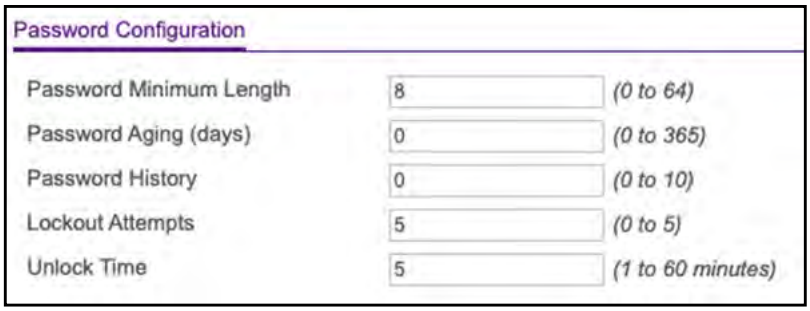
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security> Management Security > Local User > User Password Configuration.



5. En el campo Password Minimum Length, escriba la longitud mínima en caracteres de todas las contraseñas nuevas de usuarios locales.

6. En el campo Password Aging (days), escriba el tiempo máximo en días durante el cual las contraseñas de usuario son válidas desde que se establecen.

Cuando una contraseña vence, el usuario debe introducir una nueva contraseña en el primer inicio de sesión después del vencimiento. Un valor de 0 indica que las contraseñas nunca vencen.

7. En el campo Password History, escriba el número de contraseñas anteriores que se almacenarán para evitar su reutilización.

Esto garantiza que los usuarios no reutilicen contraseñas con frecuencia. Un valor de 0 indica que no se almacenan contraseñas anteriores.

8. En el campo Lockout Attempts, especifique el número de intentos fallidos de autenticación local permitidos antes de que se bloquee la cuenta de usuario.

El valor predeterminado es 5 veces. Si introduce 0, un intento fallido de autenticación local no provoca el bloqueo de la cuenta de usuario. El rango es de 0 a 5 veces.

9. En el campo Unlock Time, especifique el tiempo en minutos tras el cual se desbloquea una cuenta de usuario bloqueada.

El valor predeterminado es 5 minutos. El rango es de 0 a 60 minutos.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configuración de la contraseña enable

Puede cambiar la contraseña de EXEC privilegiado. Las contraseñas tienen un máximo de 64 caracteres alfanuméricos. La contraseña distingue mayúsculas y minúsculas.

Para configurar la contraseña enable:

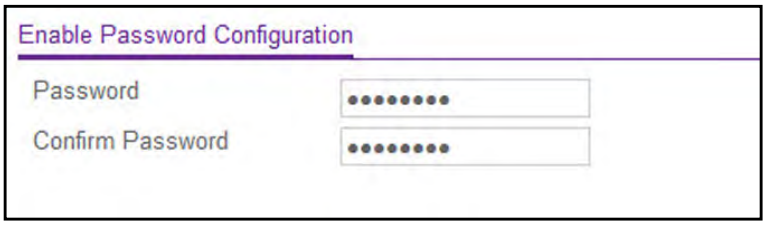
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security> Management Security > Enable Password.



5. En el campo Password, escriba la contraseña.
Las contraseñas tienen un máximo de 64 caracteres alfanuméricos.

6. En el campo Confirm Password, escriba de nuevo la contraseña para confirmar que la introdujo correctamente.

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

Configurar una contraseña de línea

Para configurar una contraseña de línea:

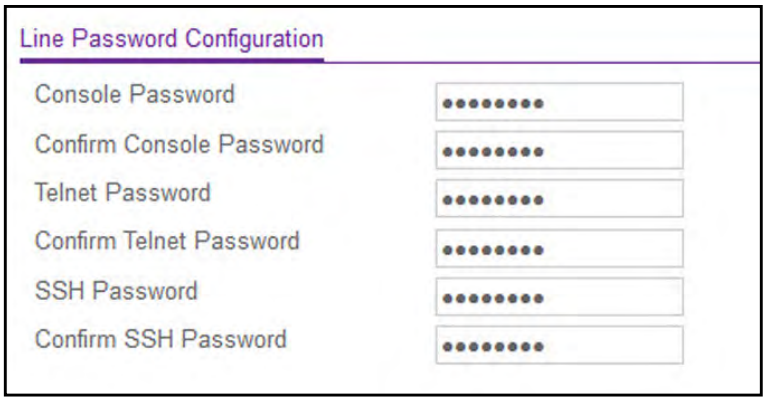
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security> Management Security > Line Password.



5. En el campo Console Password, introduzca la contraseña de consola.
Las contraseñas tienen un máximo de 64 caracteres alfanuméricos.

6. En el campo Confirm Console Password, escriba de nuevo la contraseña para confirmar que la escribió correctamente.

7. En el campo Telnet Password, escriba la contraseña de Telnet.
Las contraseñas tienen un máximo de 64 caracteres alfanuméricos.

8. En el campo Confirm Telnet Password, escriba de nuevo la contraseña para confirmar que la introdujo correctamente.

9. En el campo SSH Password, escriba la contraseña de SSH. Las contraseñas tienen un máximo de 64 caracteres alfanuméricos.

10. En el campo Confirm SSH Password, escriba de nuevo la contraseña para confirmar que la introdujo correctamente.

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

Administrar los ajustes del servidor RADIUS

Los servidores RADIUS proporcionan 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 una contraseña antes de autorizar el uso de la red. Los servidores RADIUS proporcionan un método de autenticación centralizado para lo siguiente:

- Acceso web
- Puerto de control de acceso (802.1X)

Configurar los ajustes globales del servidor RADIUS

Puede agregar información sobre uno o más servidores RADIUS de la red.

Para configurar los ajustes globales del servidor RADIUS:

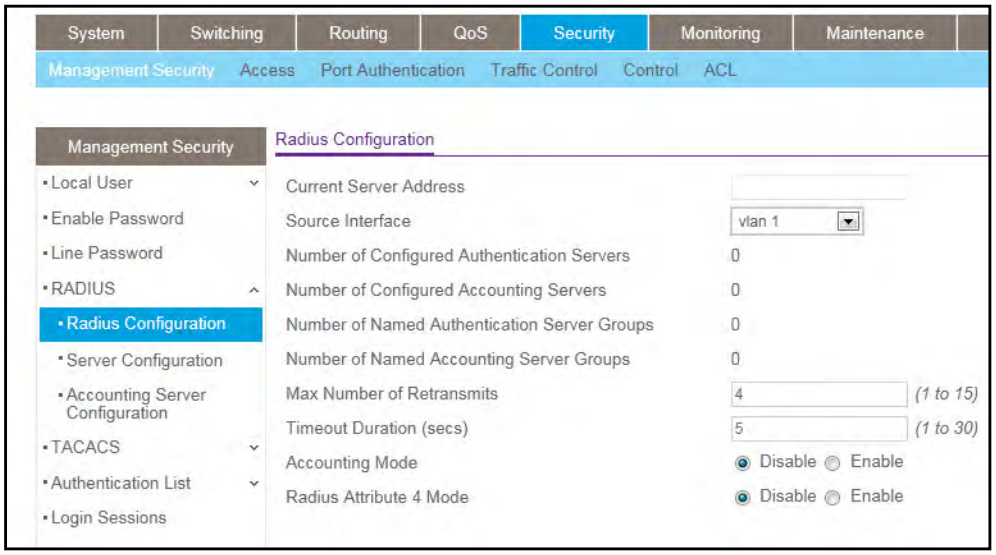
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > RADIUS > Radius Configuration.



El campo Current Server IP Address está en blanco si no hay servidores configurados (consulte Configurar un servidor RADIUS en la página 512). El switch admite hasta tres servidores RADIUS configurados. Si hay más de un servidor RADIUS configurado, el servidor actual es el servidor principal. Si ningún servidor está configurado como principal, el servidor actual es el servidor RADIUS agregado más recientemente.

5. En la lista Source Interface, seleccione la interfaz que se usará para RADIUS. Los valores posibles son los siguientes:

- None
- Interfaz de enrutamiento
- Routing VLAN

- Interfaz loopback de enrutamiento
- Service Port

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

6. En el campo Max Number of Retransmits, especifique el número máximo de veces que un paquete de solicitud se retransmite al servidor RADIUS.

El rango válido es 1– 15. El valor predeterminado es 4.

Tenga en cuenta el tiempo de retraso máximo al configurar las retransmisiones máximas y el tiempo de espera de RADIUS. Si hay varios servidores RADIUS configurados, se agota el valor máximo de retransmisiones de cada uno antes de intentar con el siguiente servidor. Una retransmisión no ocurre hasta que transcurre el tiempo de espera configurado en ese servidor sin una respuesta del servidor RADIUS. Por lo tanto, el retraso máximo para recibir una respuesta de la aplicación RADIUS es igual a las retransmisiones por el tiempo de espera de todos los servidores configurados. Si la solicitud RADIUS se generó por un intento de inicio de sesión, todas las interfaces de usuario se bloquean hasta que la aplicación RADIUS devuelve una respuesta.

7. En el campo Timeout Duration, especifique el tiempo de espera, en segundos, para las retransmisiones de solicitudes.

El rango válido es 1–30. El valor predeterminado es 5.

Tenga en cuenta el tiempo máximo de retardo al configurar las retransmisiones máximas y el tiempo de espera de RADIUS. Si hay varios servidores RADIUS configurados, se agota el número máximo de retransmisiones de cada uno antes de intentar con el siguiente servidor. No se produce una retransmisión hasta que transcurre el tiempo de espera configurado en ese servidor sin respuesta del servidor RADIUS. Por lo tanto, el retardo máximo para recibir una respuesta de la aplicación RADIUS es igual a las retransmisiones por el tiempo de espera de todos los servidores configurados. Si la solicitud RADIUS se generó por un intento de inicio de sesión de un usuario, todas las interfaces de usuario quedan bloqueadas hasta que la aplicación RADIUS devuelva una respuesta.

8. Seleccione el botón de opción Disable o Enable de Accounting Mode.

Esto especifica si el modo de contabilidad RADIUS está habilitado o deshabilitado en el servidor actual.

9. Seleccione el botón de opción Disable o Enable de RADIUS Attribute 4.

Esto habilita o deshabilita el atributo RADIUS 4. El valor predeterminado es Disable. El campo Radius Attribute 4 Value es opcional y solo se ve cuando el modo del atributo RADIUS 4 está habilitado. Acepta una dirección IP con el formato xx.xx.xx.xx.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

La siguiente tabla describe los campos RADIUS no configurables que se muestran en la página.

Tabla 191. Configuración de RADIUS

Campo	Descripción
Current Server Address	La dirección del servidor actual. Este campo está en blanco si no hay servidores configurados.
Number of Configured Authentication Servers	El número de servidores RADIUS de autenticación configurados. El valor puede ir de 0 a 32.
Number of Configured Accounting Servers	El número de servidores RADIUS de contabilidad configurados. El valor puede ir de 0 a 32.
Number of Named Authentication Server Groups	El número de grupos de autenticación de servidores RADIUS con nombre configurados.
Number of Named Accounting Server Groups	El número de grupos de contabilidad de servidores RADIUS con nombre configurados.

Configurar un servidor RADIUS

Para configurar un servidor RADIUS:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security> RADIUS > Server Configuration.



5. Para agregar un servidor RADIUS, especifique lo siguiente:
   - En el campo Radius Server IP Address, especifique la dirección IP del servidor RADIUS.
   - En el campo Radius Server Name, especifique el nombre del servidor.

- Use Port para especificar el puerto UDP que usa este servidor. El rango válido es 0–65535.
- Secret Configured. El secreto solo se aplica si esta opción es Yes. Si la opción es No, lo que se introduzca en el campo del secreto no tiene efecto y no se conserva.
- Use Secret para especificar el secreto compartido de este servidor.
- Use Primary Server para establecer el servidor seleccionado como principal o secundario.
- Use Message Authenticator para habilitar o deshabilitar el atributo de autenticador de mensajes del servidor seleccionado.

6. Haga clic en el botón Agregar (Add).
El servidor se agrega al switch.
El campo Current indica si el servidor está en uso actualmente como servidor de autenticación. La siguiente tabla describe las estadísticas del servidor RADIUS que se muestran en la página.

Tabla 192. Estadísticas de RADIUS

Campo	Descripción
Radius Server	La dirección o el nombre del servidor RADIUS cuyas estadísticas se muestran.
Round Trip Time	El 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.
Access Requests	El número de paquetes RADIUS access-request enviados a este servidor. Este número no incluye retransmisiones.
Access Retransmissions	El número de paquetes RADIUS access-request retransmitidos a este servidor.
Access Accepts	El número de paquetes RADIUS access-accept, tanto válidos como no válidos, recibidos de este servidor.
Access Rejects	El número de paquetes RADIUS access-reject, tanto válidos como no válidos, recibidos de este servidor.
Access Challenges	El número de paquetes RADIUS access-challenge, tanto válidos como no válidos, recibidos de este servidor.
Malformed Access Responses	El número de paquetes RADIUS access-response mal formados recibidos de este servidor. Los paquetes mal formados incluyen paquetes con una longitud no válida. Los autenticadores o atributos de firma incorrectos y los tipos desconocidos no se incluyen en las respuestas de acceso mal formadas.
Bad Authenticators	El número de paquetes RADIUS access-response con autenticadores o atributos de firma no válidos recibidos de este servidor.
Pending Requests	El número de paquetes RADIUS access-request destinados a este servidor que aún no han agotado el tiempo de espera ni recibido respuesta.
Timeouts	El número de tiempos de espera de autenticación agotados con este servidor.

Tabla 192. Estadísticas de RADIUS

Campo	Descripción
Unknown Types	El número de paquetes RADIUS de tipo desconocido recibidos de este servidor en el puerto de autenticación.
Packets Dropped	El número de paquetes RADIUS recibidos de este servidor en el puerto de autenticación y descartados por algún otro motivo.

Configurar servidores de contabilidad RADIUS

Para configurar un servidor de contabilidad RADIUS:

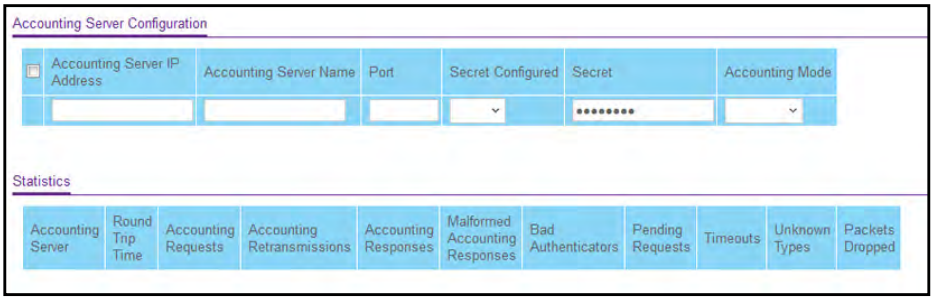
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > RADIUS > Accounting Server Configuration.



5. En el campo Accounting Server IP Address, especifique la dirección IP del servidor de contabilidad RADIUS.
6. En el campo Accounting Server Name, introduzca el nombre del servidor de contabilidad.
7. En el campo Port, especifique el número de puerto UDP que usa el servidor para verificar el servidor de contabilidad RADIUS.

   El rango válido es 0–65535. Si el usuario tiene acceso de solo lectura, el valor se muestra pero no se puede cambiar.

8. En la lista Secret Configured, seleccione Yes para agregar un secreto RADIUS en el campo siguiente. Después de agregar el servidor de contabilidad RADIUS, este campo indica si el secreto compartido de este servidor está configurado.

9. En el campo Secret, escriba el secreto compartido que se usará con el servidor de contabilidad especificado.
10. En la lista Accounting Mode, habilite o deshabilite el modo de contabilidad RADIUS.
11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe las estadísticas del servidor de contabilidad RADIUS disponibles en la página.

Tabla 193. Estadísticas del servidor de contabilidad RADIUS

Campo	Descripción
Accounting Server Address	El servidor de contabilidad asociado a las estadísticas.
Round Trip Time(secs)	El intervalo de tiempo, en centésimas de segundo, entre el accounting-response más reciente y el accounting-request correspondiente de este servidor de contabilidad RADIUS.
Accounting Requests	El número de paquetes RADIUS accounting-request enviados, sin incluir retransmisiones.
Accounting Retransmissions	El número de paquetes RADIUS accounting-request retransmitidos a este servidor de contabilidad RADIUS.
Accounting Responses	El número de paquetes RADIUS recibidos en el puerto de contabilidad desde este servidor.
Malformed Accounting Responses	El número de paquetes RADIUS accounting-response mal formados recibidos de este servidor. Los paquetes mal formados incluyen paquetes con una longitud no válida. Los autenticadores incorrectos y los tipos desconocidos no se incluyen como respuestas de contabilidad mal formadas.
Bad Authenticators	El número de paquetes RADIUS accounting-response con autenticadores no válidos recibidos de este servidor de contabilidad.
Pending Requests	El número de paquetes RADIUS accounting-request enviados a este servidor que aún no han agotado el tiempo de espera ni recibido respuesta.
Timeouts	El número de tiempos de espera de contabilidad agotados con este servidor.
Unknown Types	El número de paquetes RADIUS de tipo desconocido recibidos de este servidor en el puerto de contabilidad.
Packets Dropped	El número de paquetes RADIUS recibidos de este servidor en el puerto de contabilidad y descartados por algún otro motivo.

Administrar la configuración de 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 al iniciar sesión mediante nombres de usuario y contraseñas definidas por el usuario.
- Autorización. Se realiza al iniciar sesión. Cuando termina la sesión de autenticación, se inicia una sesión de autorización con el nombre de usuario autenticado. El servidor TACACS comprueba los privilegios del usuario.

El protocolo TACACS garantiza la seguridad de la red mediante intercambios de protocolo cifrados entre el dispositivo y el servidor TACACS.

Configurar los ajustes globales de TACACS

Puede configurar los ajustes de TACACS para la comunicación entre el switch y el servidor TACACS que configure a través del puerto de administración en banda.

Para configurar los ajustes globales de TACACS:

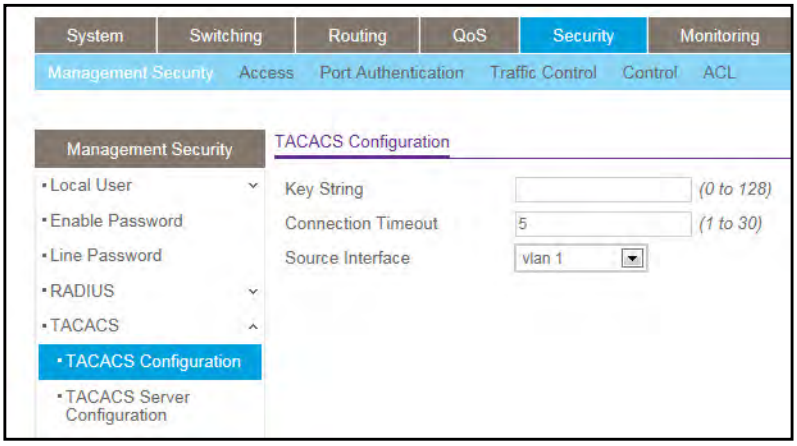
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > TACACS > TACACS Configuration.



5. 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 válido es 0–128. La clave debe coincidir con la configurada en el servidor TACACS.

6. En el campo Connection Timeout, especifique el número máximo de segundos permitido para establecer una conexión TCP entre el switch y el servidor TACACS.

7. En la lista Source Interface, seleccione la interfaz de origen que se usará para TACACS. Los valores posibles son los siguientes:

   - None. Se usa como dirección de origen la dirección IP principal de la interfaz de salida (originadora).
   - 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 del puerto de administración.

   De forma predeterminada, se usa la VLAN 1 como interfaz de origen. Cuando se muestra el valor None, significa que la interfaz de enrutamiento configurada dejó de enrutar.

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

Configurar los servidores TACACS

Puede configurar hasta cinco servidores TACACS con los que el switch puede comunicarse.

Para configurar los servidores TACACS:

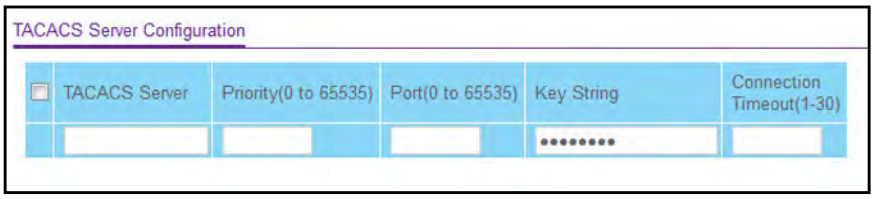
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security> TACACS > TACACS Server Configuration.



5. Use TACACS Server para configurar la dirección IP del servidor TACACS.
6. Use Priority para especificar el orden en que se usan los servidores TACACS. El rango válido es 0–65535.
7. Use Port para especificar el puerto de autenticación. Debe estar en el rango 0–65535.
8. Use Key String para especificar la clave de autenticación y cifrado para las comunicaciones TACACS entre el dispositivo y el servidor TACACS.

   El rango válido es 0–128. La clave debe coincidir con la usada en el servidor TACACS.

9. Use Connection Timeout para especificar el tiempo que transcurre antes de que la conexión entre el dispositivo y el servidor TACACS agote el tiempo de espera.

   El rango es 1–30.
10. Haga clic en el botón Add.

El servidor se agrega al switch.

Configurar listas de autenticación

El switch admite varias listas de autenticación.

Configurar una lista de autenticación de inicio de sesión

Una lista de inicio de sesión especifica los métodos de autenticación para validar el acceso al switch o al puerto de los usuarios asociados a la lista. Los usuarios preconfigurados, admin y guest, están asignados a una lista preconfigurada llamada defaultList, que no se puede eliminar. Todos los usuarios nuevos también se asignan a defaultList hasta que los asigne específicamente a una lista distinta.

Hay dos listas predeterminadas: DefaultList y networkList.

Para configurar una lista de autenticación de inicio de sesión:

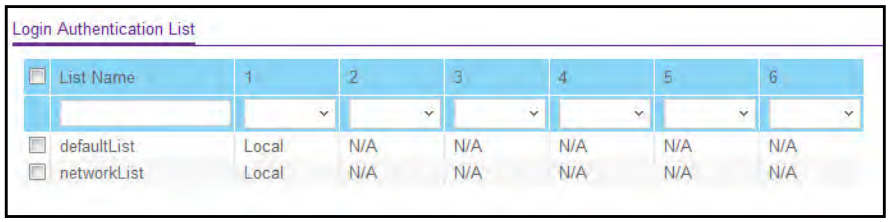
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > Authentication List > Login Authentication List.



5. Para crear una lista de inicio de sesión nueva, introduzca el nombre en el campo List Name. El nombre puede tener hasta 15 caracteres alfanuméricos y no distingue mayúsculas de minúsculas.

6. En las columnas del encabezado de la tabla (1, 2, 3, 4, 5, 6), seleccione el método que aparecerá primero en la lista de autenticación seleccionada.

   Las opciones son las siguientes:

   - Enable. Se usa la contraseña de EXEC privilegiado para la autenticación.
   - Line. Se usa la contraseña de línea para la autenticación.
   - None. El usuario no se puede autenticar.
   - 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.
   - Deny. La autenticación siempre falla.

7. Haga clic en el botón Add.
La lista de inicio de sesión se agrega al switch.

Configurar una lista de autenticación Enable

Una lista Enable especifica los métodos de autenticación para validar el acceso a EXEC privilegiado de los usuarios asociados a la lista. Los usuarios preconfigurados, admin y guest, están asignados a una lista preconfigurada llamada defaultList, que no se puede eliminar. Todos los usuarios nuevos también se asignan a defaultList hasta que los asigne específicamente a una lista distinta. Hay dos listas predeterminadas: enableList y enableNetList.

Para configurar una lista de autenticación Enable:

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

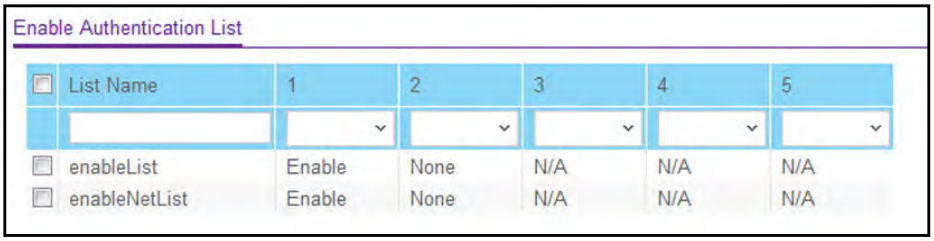
Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > Authentication List > Enable Authentication List.



5. Para crear una lista Enable nueva, introduzca el nombre en el campo List Name. Puede tener hasta 15 caracteres alfanuméricos y no distingue mayúsculas de minúsculas.

6. En las columnas del encabezado de la tabla (1, 2, 3, 4, 5, 6), seleccione el método que aparecerá primero en la lista de autenticación seleccionada.

   Las opciones son las siguientes:

   - Enable. Se usa la contraseña de EXEC privilegiado para la autenticación.
   - Line. Se usa la contraseña de línea para la autenticación.
   - None. El usuario no se puede autenticar.
   - 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.
   - Deny. La autenticación siempre falla.

7. Haga clic en el botón Add.
La lista de inicio de sesión se agrega al switch.

Configurar la lista de autenticación Dot1x

Puede configurar una lista dot1x. Una lista dot1x especifica los métodos de autenticación para validar el acceso al puerto de los usuarios asociados a la lista. Solo se admite un método dot1x.

La lista predeterminada es dot1xList.

Para configurar la lista de autenticación dot1x:

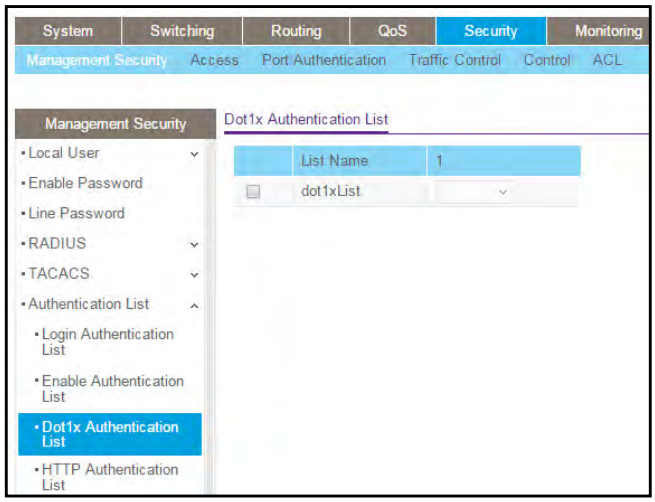
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > Authentication List > Dot1x Authentication List.



5. Active la casilla del nombre de la lista dot1x.
6. Seleccione el método que aparecerá primero en la lista de autenticación de inicio de sesión seleccionada. Las opciones son las siguientes:

- IAS. Se usan para la autenticación el ID y la contraseña del usuario en la base de datos del servidor de autenticación interno.
- Local. Se usan para la autenticación el ID y la contraseña del usuario almacenados localmente.
- RADIUS. El ID y la contraseña del usuario se autentican con el servidor RADIUS en lugar de localmente.
- None. El usuario se autentica sin nombre de usuario ni contraseña.

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

Configurar una lista de autenticación HTTP

Puede configurar una lista HTTP. Una lista HTTP especifica los métodos de autenticación para validar el acceso al switch o al puerto mediante HTTP.

Para configurar una lista de autenticación HTTP:

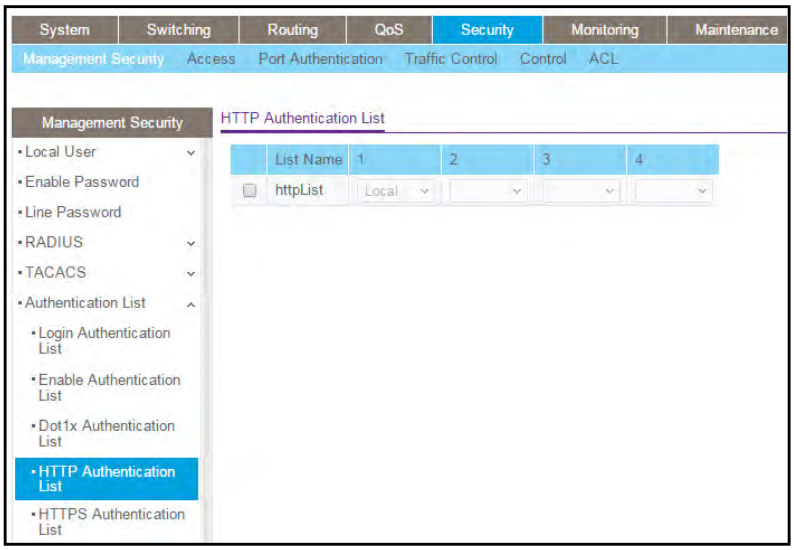
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > Authentication List > HTTP Authentication List.



5. Active la casilla del nombre de la lista HTTP.

6. En las columnas del encabezado de la tabla (1, 2, 3, 4, 5, 6), seleccione el método que aparecerá primero en la lista de autenticación seleccionada.

   Las opciones son las siguientes:

   - Enable. Se usa la contraseña de EXEC privilegiado para la autenticación.
   - None. El usuario no se puede autenticar.
   - 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.

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

Configurar una lista de autenticación HTTPS

Puede configurar una lista HTTPS. Una lista de inicio de sesión especifica los métodos de autenticación para validar el acceso al switch o al puerto mediante HTTPS de los usuarios asociados a la lista. La lista predeterminada es httpsList.

Para configurar una lista de autenticación HTTPS:

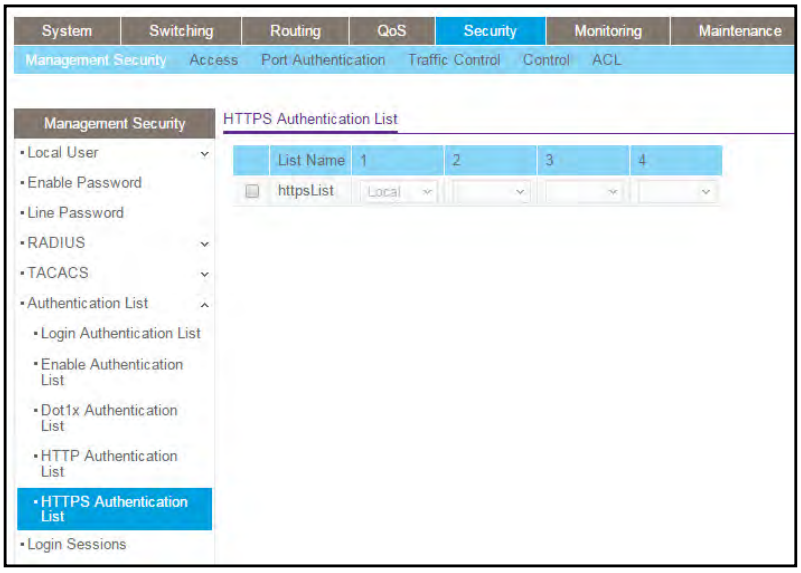
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > Authentication List > HTTPS Authentication List.



5. Active la casilla del nombre de la lista HTTPS.

6. En las columnas del encabezado de la tabla (1, 2, 3, 4, 5, 6), seleccione el método que aparecerá primero en la lista de autenticación seleccionada.

Las opciones son las siguientes:

- Enable. Se usa la contraseña de EXEC privilegiado para la autenticación.
- None. El usuario no se puede autenticar.
- 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.

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

Ver las sesiones iniciadas

Para ver las sesiones iniciadas:

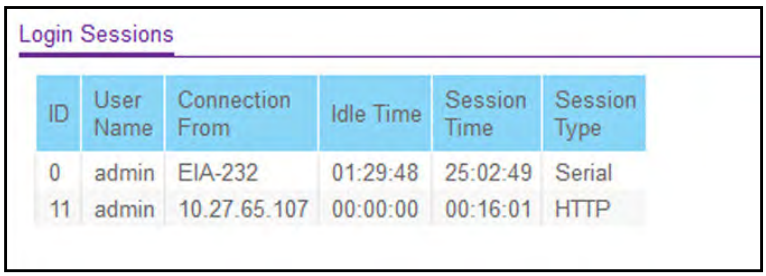
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Management Security > Login Sessions.



La siguiente tabla describe los campos que se muestran en la tabla.

Tabla 194. Sesiones iniciadas

Campo	Descripción
ID	Identifica el ID de esta fila.
User Name	El nombre del usuario cuya sesión está abierta.
Connection From	El equipo desde el que está conectado el usuario.

Tabla 194. Sesiones iniciadas

Campo	Descripción
Idle Time	El tiempo de inactividad de la sesión.
Session Time	El tiempo total de la sesión.
Session Type	El tipo de sesión: Telnet, Serial o SSH

Administrar el acceso HHTP, HTTPS y SSH

Puede configurar el acceso HTTP y HTTP seguro a la interfaz de administración del switch.

Configurar el servidor HTTP

Para acceder al switch con un navegador web, primero debe configurarlo con información IP (dirección IP, máscara de subred y puerta de enlace predeterminada). Puede configurar la información IP con cualquiera de los siguientes métodos:

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

Una vez establecida la conectividad en banda, puede cambiar la información IP mediante la administración web.

Para configurar el servidor HTTP:

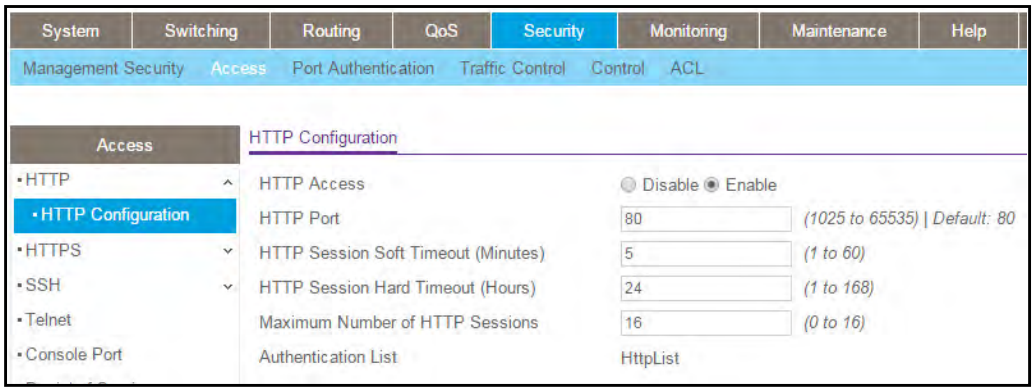
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access> HTTP > HTTP Configuration.



5. Seleccione el botón de opción Disable o Enable de HTTP Access.

   Esto especifica si se puede acceder al switch desde un navegador web. Si habilita el modo web, puede administrar el switch desde un navegador web. El valor de fábrica es Enable.

6. En el campo HTTP Port, introduzca el número de puerto HTTP. El rango válido es 80 y de 1025 a 65535. El valor predeterminado es 80.

7. En el campo HTTP Session Soft Timeout (Minutes), establezca el tiempo de inactividad de las sesiones HTTP.

   El valor debe estar en el rango de 1 a 60 minutos. El valor predeterminado es 5 minutos. Se muestra el valor configurado actualmente.

8. En el campo HTTP Session Hard Timeout (Hours), establezca el tiempo de espera absoluto de las sesiones HTTP.

   Este tiempo de espera no depende del nivel de actividad de la sesión. El valor debe estar en el rango de 1 a 168 horas. El valor predeterminado es 24 horas. Se muestra el valor configurado actualmente.

9. En el campo Maximum Number of HTTP Sessions, establezca el número máximo permitido de sesiones HTTP.

   El valor debe estar en el rango de 0 a 16. El valor predeterminado es 16. Se muestra el valor configurado actualmente.

10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
El campo Authentication List muestra la lista que usa HTTP.

Configurar HTTPS

HTTP seguro (HTTPS) permite transmitir HTTP a través de una conexión cifrada Secure Sockets Layer (SSL) o Transport Layer Security (TLS). Cuando administra el switch con la interfaz del navegador local, HTTPS ayuda a garantizar que la comunicación entre el sistema de administración y el switch esté protegida contra espionaje y ataques de intermediario (man-in-the-middle).

Puede configurar los ajustes de la comunicación HTTPS entre la estación de administración y el switch.

Para configurar HTTPS:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > HTTPS > HTTPS Configuration.



5. Seleccione el botón de opción Admin Mode Disable o Enable.

   Esto habilita o deshabilita el modo administrativo de HTTPS seguro. Se muestra el valor configurado actualmente. El valor predeterminado es Disable. Solo puede descargar certificados SSL cuando el modo de administración HTTPS está deshabilitado. El modo de administración HTTPS solo se puede habilitar si hay un certificado en el dispositivo.

   Nota: La versión de Transport Layer Security (TLS) es 1.2. No puede cambiar esta versión.

6. En el campo HTTPS Port, escriba el número de puerto HTTPS.

   El valor debe estar en el rango de 1025 a 65535. El puerto 443 es el valor predeterminado. Se muestra el valor configurado actualmente.

7. En el campo HTTPS Session Soft Timeout (Minutes), introduzca el tiempo de inactividad de las sesiones HTTPS.

   El valor debe estar en el rango de 1 a 60 minutos. El valor predeterminado es 5 minutos. Se muestra el valor configurado actualmente.

8. En el campo HTTPS Session Hard Timeout (Hours), establezca el tiempo de espera absoluto de las sesiones HTTPS.

Este tiempo de espera no depende del nivel de actividad de la sesión. El valor debe estar en el rango de 1 a 168 horas. El valor predeterminado es 24 horas. Se muestra el valor configurado actualmente.

9. En el campo Maximum Number of HTTPS Sessions, introduzca el número máximo permitido de sesiones HTTPS.

El valor debe estar en el rango de 0 a 16. El valor predeterminado es 16. Se muestra el valor configurado actualmente.

Nota: El campo Authentication List muestra la lista de autenticación de HTTPS.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Administrar certificados

Puede generar o eliminar certificados.

Para administrar certificados:

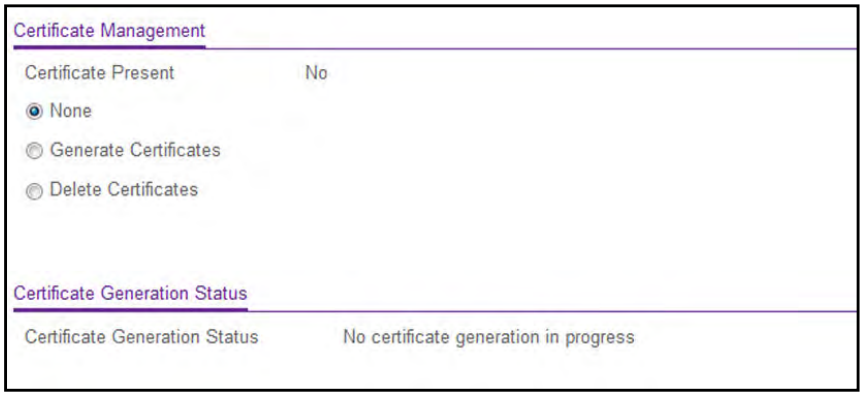
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Access > HTTPS > Certificate Management.



El campo Certificate Present muestra si hay un certificado en el dispositivo.

5. Seleccione uno de los siguientes botones de opción:
   - None. No se realiza ninguna acción de administración de certificados. Esta es la selección predeterminada.
   - Generate Certificates. Comienza a generar los archivos de certificado.
   - Delete Certificates. Elimina los archivos de certificado correspondientes, si existen.

6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
El campo Certificate Generation Status muestra el estado de generación del certificado SSL.

Descargar certificados

Puede transferir un archivo de certificado al switch.

Para que el servidor web del switch acepte conexiones HTTPS de una estación de administración, el servidor web necesita un certificado de clave pública. Puede generar un certificado externamente (por ejemplo, sin conexión) y descargarlo al switch.

Antes de descargar un archivo al switch, deben cumplirse las siguientes condiciones:

- El archivo que se descargará del servidor TFTP está en el directorio correspondiente del servidor.
- El archivo tiene el formato correcto.
- El switch tiene una ruta al servidor TFTP.

Para descargar certificados:

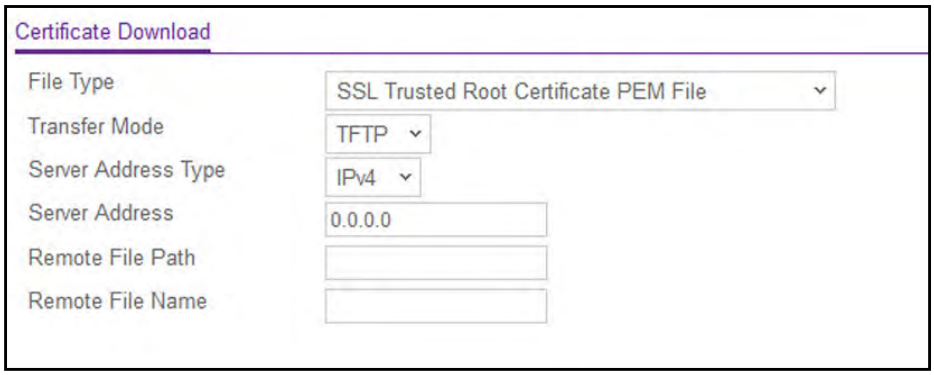
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > HTTPS > Certificate Download.



5. En la lista File Type, especifique el tipo de archivo que desea transferir:
   - SSL Trusted Root Certificate PEM File. Archivo de certificado raíz de confianza SSL (codificado en PEM)
   - SSL Server Certificate PEM File. Archivo de certificado de servidor SSL (codificado en PEM)
   - SSL DH Weak Encryption Parameter PEM File. Archivo de parámetros de cifrado débil Diffie-Hellman de SSL (codificado en PEM)
   - SSL DH Strong Encryption Parameter PEM File. Archivo de parámetros de cifrado fuerte Diffie-Hellman de SSL (codificado en PEM)

6. En la lista Transfer Mode, especifique el protocolo que se usará para transferir el archivo:
   - TFTP. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol

7. En la lista Server Address Type, especifique IPv4, IPv6 o DNS para indicar el formato del campo TFTP/SFTP/SCP Server Address.

   El valor predeterminado de fábrica es IPv4.

8. En el campo Server Address, escriba la dirección IP o el nombre de host DNS del servidor de acuerdo con el formato indicado por el tipo de dirección del servidor.

   El valor predeterminado de fábrica es la dirección IPv4 0.0.0.0.
9. En el campo Remote File Path, ingrese la ruta del archivo que desea descargar. Puede ingresar hasta 96 caracteres. El valor predeterminado de fábrica es en blanco.
10. 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 de fábrica es en blanco.
11. Haga clic en el botón Apply.
La configuración se guarda.

Configurar los ajustes de SSH

Puede ver y modificar la configuración del servidor Secure Shell (SSH) del dispositivo. SSH es un protocolo de red que permite acceder a la interfaz de administración CLI con un cliente SSH en un sistema administrativo remoto. SSH es un método de acceso más seguro que Telnet porque cifra la comunicación entre el sistema administrativo y el dispositivo. Puede descargar o generar claves de host SSH para la administración segura basada en CLI.

Para configurar los ajustes de SSH:

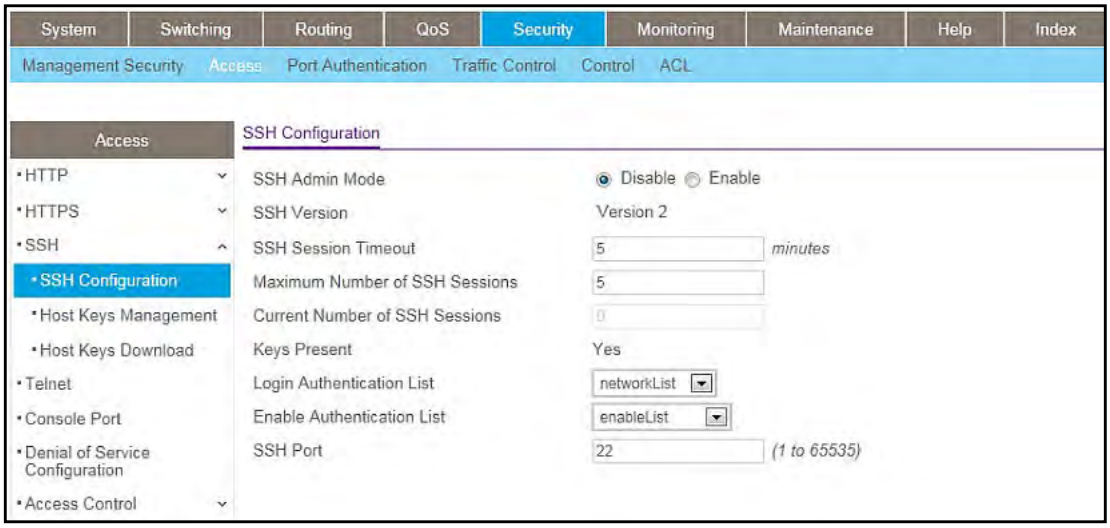
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > SSH > SSH Configuration.



5. Seleccione el botón de opción SSH Admin Mode Disable o Enable.

Esto habilita o deshabilita el modo administrativo del servidor SSH. Cuando este modo está habilitado, se puede acceder al dispositivo con un cliente SSH en un sistema remoto. Se muestra el valor configurado actualmente. El valor predeterminado es Disable.

6. Use SSH Session Timeout para configurar el tiempo de espera por inactividad de las sesiones SSH entrantes al switch.

Un usuario conectado que no presenta actividad SSH durante este tiempo se desconecta automáticamente del dispositivo. El rango aceptable para este campo es de 1 a 5 minutos.

7. Use Maximum Number of SSH Sessions para configurar el número máximo de sesiones SSH entrantes que pueden conectarse al dispositivo simultáneamente.

Se muestra el valor configurado actualmente. El rango aceptable para este campo es de 0 a 5.
8. Use Login Authentication List para seleccionar una lista de autenticación.
Esta lista se usa para autenticar a los usuarios que intentan iniciar sesión en el switch.
9. Use Enable Authentication List para seleccionar una lista de autenticación.
Esta lista se usa para autenticar a los usuarios que intentan obtener privilegios de nivel enable.
10. Use SSH Port para ingresar el puerto, en el rango de 1 a 65535.
El valor predeterminado es 22.
11. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe los campos no configurables que se muestran en la página.

Tabla 195. SSH Configuration

Campo	Descripción
SSH Version	El servidor SSH del dispositivo 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 servidor SSH del dispositivo.
Keys Present	Muestra Yes o No según 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)

Administrar las claves de host

Puede generar o eliminar claves RSA y DSA.

Para administrar las claves de host:

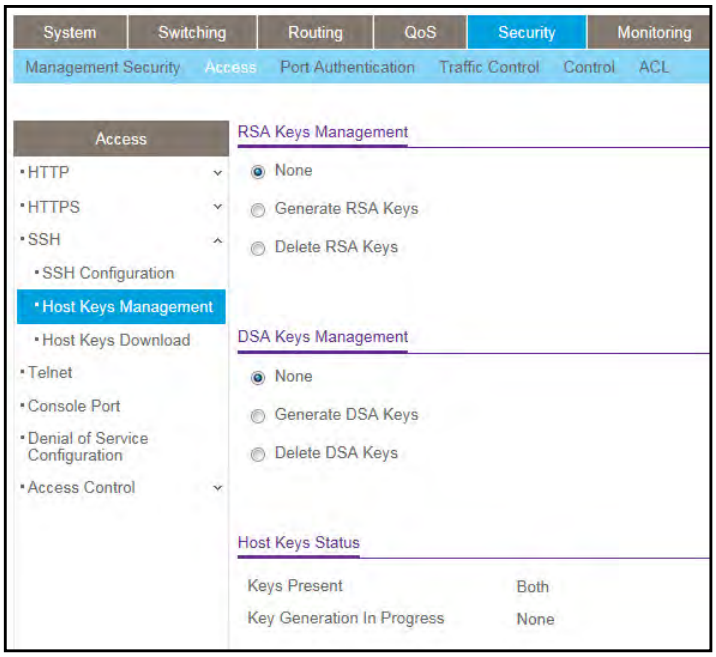
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > SSH > Host Keys Management.



5. Seleccione un botón de opción de RSA Keys Management:

- None. Esta es la opción predeterminada.
- Generate RSA Keys. Comienza a generar las claves de host RSA. Para generar archivos de clave SSH, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.
- Delete RSA Keys. Elimina el archivo de clave RSA correspondiente, si existe.

6. Seleccione un botón de opción de DSA Keys Management:

- None. Esta es la opción predeterminada.
- Generate DSA Keys. Comienza a generar las claves de host DSA.

  Para generar archivos de clave SSH, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.
- Delete DSA Keys. Elimina el archivo de clave DSA correspondiente, si existe.

7. Haga clic en el botón Apply.
Comienza la descarga del archivo de clave de host.

Nota: Para descargar archivos de clave SSH, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.

La siguiente tabla describe los campos no configurables que se muestran en la página.

Tabla 196. RSA Key Management

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.

Descargar las claves de host

Puede descargar un archivo de clave SSH-2 RSA o SSH-2 DSA de un sistema remoto al dispositivo.

Para descargar las claves de host:

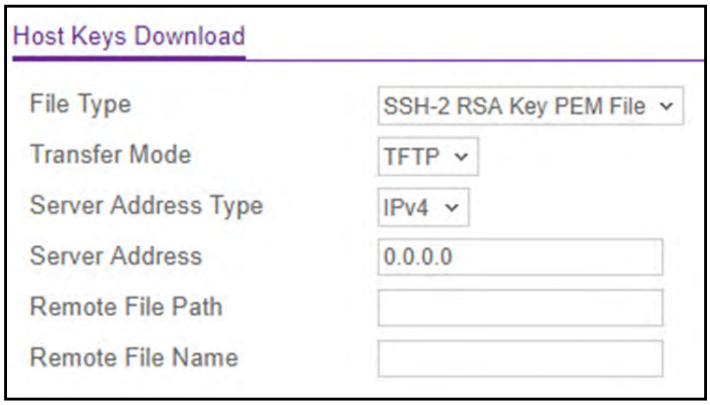
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > SSH > Host Keys Download.



5. En la lista File Type, seleccione el tipo de archivo que desea transferir:
   - 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)

6. En la lista Transfer Mode, seleccione el protocolo que se usará para transferir el archivo:
   - TFTP. Trivial File Transfer Protocol
   - **SFTP**. Secure File Transfer Protocol
   - **SCP**. Secure Copy Protocol
7. En el campo Server Address Type, especifique IPv4, IPv6 o DNS.

   Esto especifica el formato del campo TFTP/SFTP/SCP Server Address. El valor predeterminado de fábrica es IPv4.

8. En el campo Server Address, ingrese la dirección IP o el nombre de host DNS del servidor de acuerdo con el formato indicado por el tipo de dirección del servidor.

El valor predeterminado de fábrica es la dirección IPv4 0.0.0.0.
9. En el campo Remote File Path, ingrese la ruta del archivo que desea descargar. Puede ingresar hasta 96 caracteres. El valor predeterminado de fábrica es en blanco.
10. 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 de fábrica es en blanco.
11. Haga clic en el botón Apply.
Comienza la descarga del archivo de clave de host.

Nota: Para descargar archivos de clave SSH, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.

Configurar el acceso por Telnet

Puede configurar una lista de autenticación de Telnet y administrar Telnet de salida y de entrada.

Configurar una lista de autenticación de Telnet

Puede seleccionar Login Authentication List y Enable Authentication List:

- Login Authentication List. 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 información sobre cómo crear una lista de autenticación de inicio de sesión, consulte Configurar una lista de autenticación de inicio de sesión en la página 518.
- Enable Authentication List. 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 información sobre cómo crear una lista de autenticación enable, consulte Configurar una lista de autenticación de inicio de sesión en la página 518.

Para configurar la lista de autenticación de Telnet:

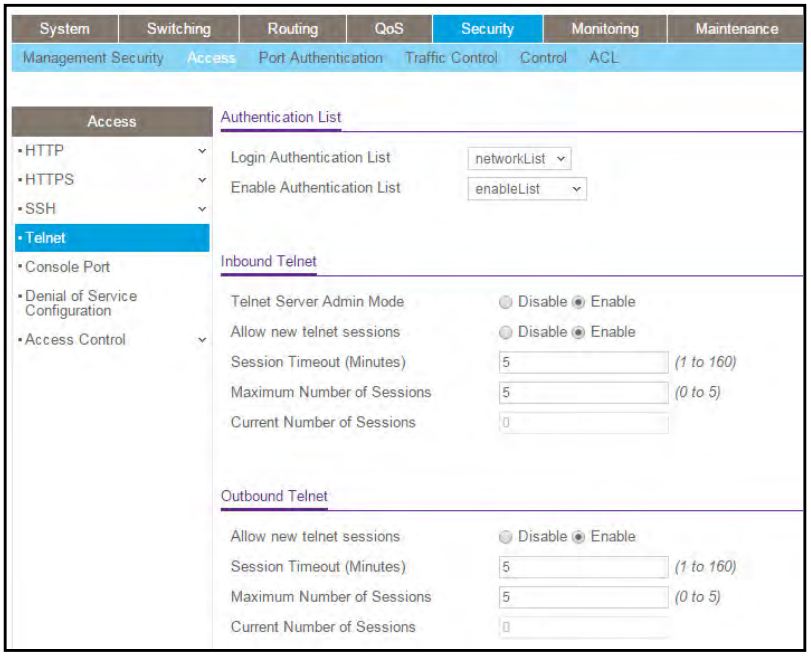
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > Telnet.



5. En el menú Login Authentication List, seleccione qué lista de autenticación debe usarse para iniciar sesión por Telnet.

   El valor predeterminado es networkList.

6. En el menú Enable Authentication List, seleccione qué lista de autenticación debe usarse para iniciar sesión por Telnet en el modo EXEC privilegiado.

El valor predeterminado es enableList.
7. Haga clic en el botón Apply. La configuración se guarda.

Configurar Telnet de entrada

Puede regular las nuevas sesiones Telnet de entrada. Si Allow New Telnet Sessions está habilitado, se pueden establecer nuevas sesiones Telnet de entrada hasta que no haya más sesiones disponibles. Si Allow New Telnet Sessions está deshabilitado, no se establecen nuevas sesiones Telnet de entrada. Una sesión establecida permanece activa hasta que se termina o hasta que un error anormal

de la red termina la sesión.

Para configurar Telnet de entrada:

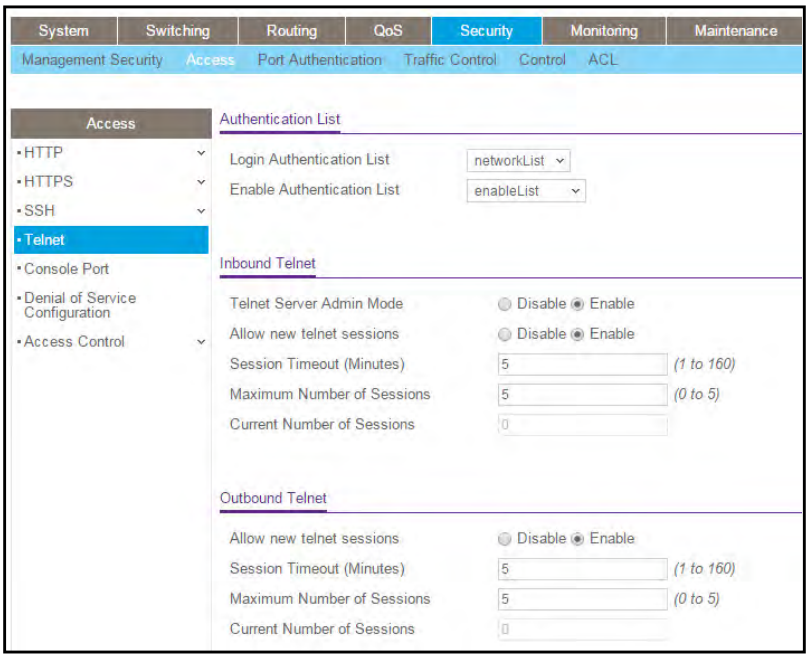
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > Telnet.



5. Junto a Allow new telnet sessions, seleccione el botón de opción Disable o Enable.

   Esto especifica si la nueva sesión Telnet de entrada está habilitada o deshabilitada. El valor predeterminado es Enabled, de modo que se pueden establecer nuevas sesiones Telnet de entrada hasta que no haya más sesiones disponibles. Si está deshabilitado, no se establecen nuevas sesiones Telnet de entrada. Una sesión establecida permanece activa hasta que se termina o hasta que un error anormal de la red termina la sesión.

6. En el campo Session Timeout, especifique cuántos minutos de inactividad pueden transcurrir en una sesión Telnet de entrada antes de que se cierre la sesión.

Puede ingresar cualquier número del 1 al 160. El valor predeterminado de fábrica es 5 minutos.

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

El campo Current Number of Sessions muestra el número de sesiones Telnet de entrada actuales.

Configurar Telnet de salida

Puede regular las nuevas sesiones Telnet de salida. Si Allow New Telnet Sessions está habilitado, se pueden establecer nuevas sesiones Telnet de salida hasta que no haya más sesiones disponibles. Si Allow New Telnet Sessions está deshabilitado, no se establecen nuevas sesiones Telnet de salida. Una sesión establecida permanece activa hasta que se termina o hasta que un error anormal de la red termina la sesión.

Para configurar Telnet de salida:

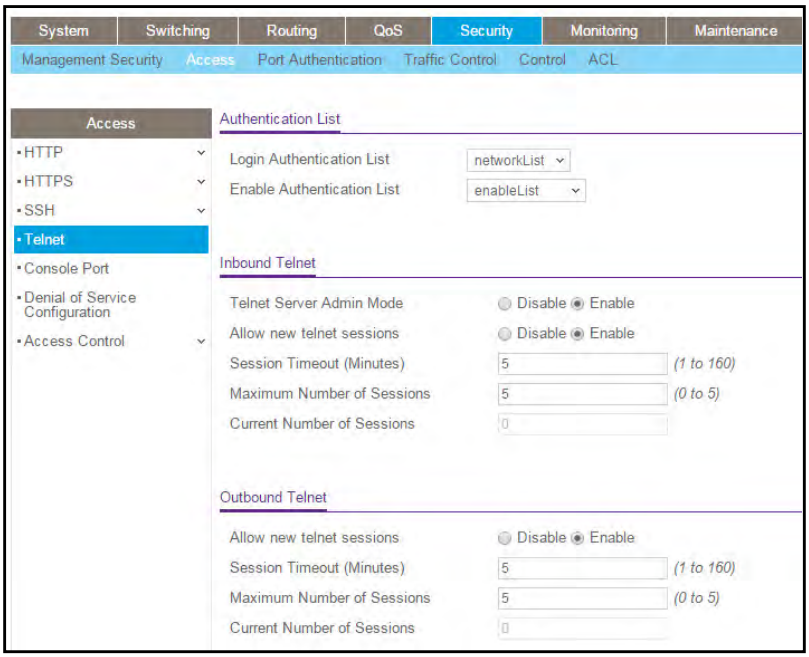
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Access > Telnet.



5. Junto a Allow new telnet sessions, seleccione el botón de opción Disable o Enable.

   Esto especifica si la nueva sesión Telnet de salida está habilitada o deshabilitada. El valor predeterminado es Enabled, de modo que se pueden establecer nuevas sesiones Telnet de salida hasta que no haya más sesiones disponibles. Si está deshabilitado, no se establecen nuevas sesiones Telnet de salida. Una sesión establecida permanece activa hasta que se termina o hasta que un error anormal de la red termina la sesión.

6. En el campo Session Timeout, especifique cuántos minutos de inactividad pueden transcurrir en una sesión Telnet de entrada antes de que se cierre la sesión.

   Puede ingresar cualquier número del 1 al 160. El valor predeterminado de fábrica es 5 minutos.

7. 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 de fábrica.

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

   El campo Current Number of Sessions muestra el número de sesiones Telnet de salida actuales.

Configurar el acceso por el puerto de consola

Para configurar el puerto de consola:

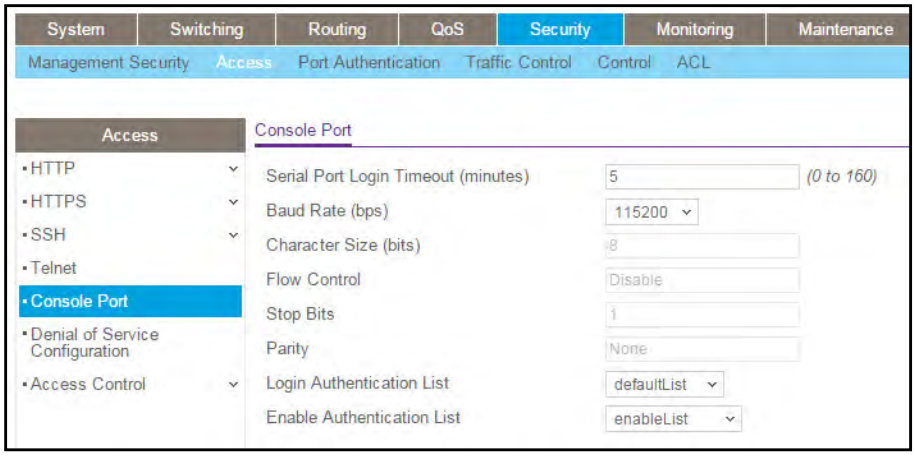
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > Console Port.



5. En el campo Serial Port Login Timeout (minutes), 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. El valor predeterminado de fábrica es 5. Ingresar 0 deshabilita el tiempo de espera.

6. En la lista Baud Rate (bps), seleccione la velocidad en baudios predeterminada para la conexión del puerto serie.

   Puede elegir entre 1200, 2400, 4800, 9600, 19200, 38400, 57600 y 115200 baudios. El valor predeterminado de fábrica es 115200 baudios.

7. En la lista Login Authentication List, seleccione qué lista de autenticación usar al iniciar sesión por Telnet.

   El valor predeterminado es defaultList.

8. En la lista Enable Authentication List, seleccione qué lista de autenticación usar al entrar en el modo EXEC privilegiado.

   El valor predeterminado es enableList.

9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 197. Console Port

Campo	Descripción
Character Size (bits)	El número de bits de un carácter. Siempre es 8.
Flow Control	Si el control de flujo por hardware está habilitado o deshabilitado. Siempre está deshabilitado.
Stop Bits	El número de bits de parada por carácter. Siempre es 1.
Parity	El método de paridad que se usa en el puerto serie. Siempre es None.

Configurar los ajustes de denegación de servicio

Para configurar los ajustes de denegación de servicio:

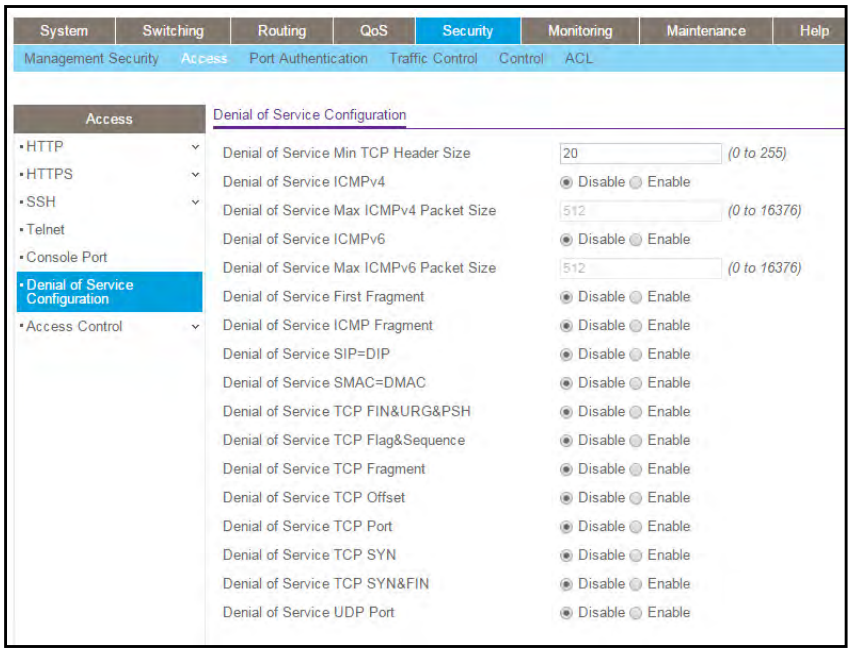
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > Denial of Service Configuration.



5. En el campo Denial of Service Min TCP Header Size, especifique el tamaño mínimo de encabezado TCP permitido.

Si DoS TCP Fragment está habilitado, el switch descarta estos paquetes:

- Primeros fragmentos TCP con carga útil TCP: IP_Payload_Length - IP_Header_Size < Min_TCP_Header_Size.
- Su rango es de 0 a 255. El valor predeterminado es 20.

6. Seleccione el botón de opción Denial of Service ICMPv4 Disable o Enable.

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. El valor predeterminado de fábrica es Disable.

7. Especifique Denial of Service Max ICMPv4 Packet Size.

Este es el tamaño máximo de paquete ICMPv4 permitido. Si la prevención de DoS ICMPv4 está habilitada, el switch descarta los paquetes ping ICMP IPv4 con un tamaño mayor que el tamaño máximo de paquete ICMPv4 configurado. Su rango es de 0 a 16376. El valor predeterminado es 512.

8. Use Denial of Service ICMPv6 para habilitar la prevención de DoS ICMPv6.

Esto hace que el switch descarte los paquetes ICMPv6 con el tipo ECHO_REQ (ping) y un tamaño mayor que el tamaño de paquete ICMPv6 configurado. El valor predeterminado de fábrica es Disable.

9. Use Denial of Service Max ICMPv6 Packet Size para especificar el tamaño máximo de paquete ICMP IPv6 permitido.

Si la prevención de DoS ICMPv6 está habilitada, el switch descarta los paquetes ping ICMP IPv6 con un tamaño mayor que el tamaño máximo de paquete ICMPv6 configurado. Su rango es de 0 a 16376. El valor predeterminado es 512.

10. Seleccione el botón de opción Denial of Service First Fragment Disable o Enable.

Esto habilita la prevención de DoS del primer fragmento, que hace que el switch verifique las opciones de DoS en los paquetes IP del primer fragmento cuando recibe paquetes IP fragmentados. De lo contrario, el switch ignora los paquetes IP del primer fragmento. El valor predeterminado de fábrica es Disable.

11. Seleccione el botón de opción Denial of Service ICMP Fragment Disable o Enable.

Al habilitar la prevención de DoS de fragmentos ICMP, el switch descarta los paquetes ICMP fragmentados. El valor predeterminado de fábrica es Disable.

12. Seleccione el botón de opción Denial of Service SIP=DIP Disable o Enable.

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. El valor predeterminado de fábrica es Disable.

13. Seleccione el botón de opción Denial of Service SMAC=DMAC Disable o Enable.

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. El valor predeterminado de fábrica es Disable.

14. Seleccione el botón de opción Denial of Service TCP FIN&URG&PSH Disable o Enable.

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 TCP Sequence Number=0. El valor predeterminado de fábrica es Disable.

15. Seleccione el botón de opción Denial of Service TCP Flag&Sequence Disable o Enable.

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. El valor predeterminado de fábrica es Disable.

16. Seleccione el botón de opción Denial of Service TCP Fragment Disable o Enable.

Al habilitar la prevención de DoS de fragmentos TCP, el switch descarta los siguientes paquetes:

Primeros fragmentos TCP con carga útil TCP: IP_Payload_Length - IP_Header_Size < Min_TCP_Header_Size.

El valor de fábrica es Disable.

17. Seleccione el botón de opción Denial of Service TCP Offset Disable o Enable.

Al habilitar la prevención de DoS TCP Offset, el switch descarta los paquetes con un encabezado TCP con Offset=1. El valor predeterminado de fábrica es Disable.

18. Seleccione el botón de opción Denial of Service TCP Port Disable o Enable.

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. El valor predeterminado de fábrica es Disable.

19. Seleccione el botón de opción Denial of Service TCP SYN Disable o Enable.

Al habilitar la prevención de DoS TCP SYN, el switch descarta los paquetes con el indicador TCP SYN activado. El valor predeterminado de fábrica es Disable.

20. Seleccione el botón de opción Denial of Service TCP SYN & FIN Disable o Enable.

Al habilitar la prevención de DoS TCP SYN & FIN, el switch descarta los paquetes con los indicadores TCP SYN y FIN activados. El valor predeterminado de fábrica es Disable.

21. Seleccione el botón de opción Denial of Service UDP Port Disable o Enable.

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. El valor predeterminado de fábrica es Disable.

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

Configurar los ajustes de control de acceso

Puede configurar un perfil de control de acceso y asociar una regla de control de acceso con el perfil. El switch admite solo un perfil de control de acceso.

Para terminar de configurar un perfil con una regla, siga los procedimientos que se describen en las siguientes secciones:

1. Configurar un perfil de control de acceso en la página 544
2. Configurar los ajustes de reglas de acceso del perfil de control de acceso en la página 546

Configurar un perfil de control de acceso

Para configurar los ajustes del perfil de acceso:

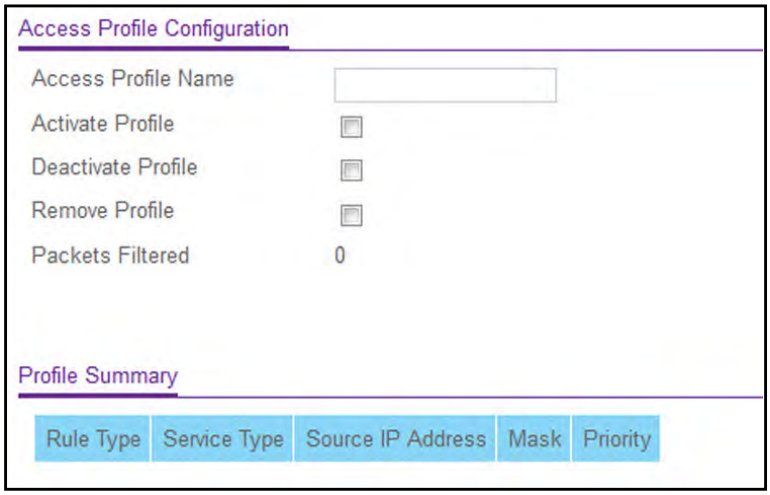
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Access > Access Control > Access Profile Configuration.



5. En el campo Access Profile Name, ingrese el nombre del perfil de acceso que desea agregar. La longitud máxima es de 32 caracteres.

6. Realice una de las siguientes acciones:
   - Para activar un perfil de acceso, marque la casilla Activate Profile.
   - Para desactivar un perfil de acceso, marque la casilla Deactivate Profile.
   - Para eliminar un perfil de acceso, marque la casilla Remove Profile.

     Le recomendamos desactivar el perfil de acceso antes de eliminarlo.

7. Haga clic en el botón Apply.
La configuración se guarda.
El campo Packets Filtered muestra el número de paquetes filtrados. La siguiente tabla describe la información no configurable que se muestra.

Tabla 198. Access Profile Configuration Profile Summary

Campo	Descripción
Rule Type	La acción que se realiza cuando se cumplen las reglas.
Service Type	El tipo de servicio elegido. La política se restringe al tipo de servicio elegido.
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.

Configurar los ajustes de reglas de acceso del perfil de control de acceso

Después de configurar un perfil de control de acceso, puede configurar y aplicar reglas de control de acceso. Sin embargo, para hacerlo, el perfil de control de acceso debe estar desactivado. Después de agregar la regla de control de acceso, puede volver a activar el perfil de control de acceso.

Para configurar los ajustes de reglas de acceso:

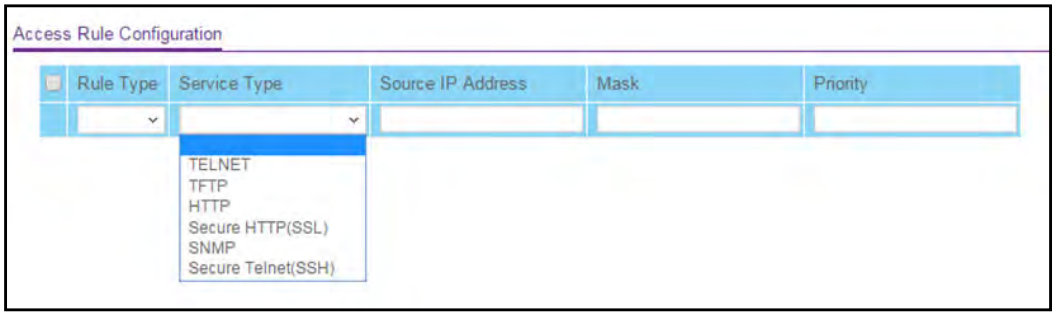
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Access > Access Control > Access Rule Configuration.



5. En el menú Rule Type, seleccione si el tráfico se permite (Permit) o se deniega (Deny) cuando una regla coincide.
6. En el menú Service Type, seleccione el método de administración al que se restringe la política:
   - TELNET
   - TFTP
   - HTTP
   - Secure HTTP (SSL)
   - SNMP
   - Secure Telnet (SSH)
7. En el campo Source IP Address, ingrese la dirección IP de origen, es decir, la dirección IP desde la que se origina el tráfico de administración.
8. En el campo Mask, ingrese la máscara de la dirección IP de origen.
9. En el menú Priority, seleccione la prioridad de 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 IP de origen 10.10.10.10 se configura con prioridad 1 para permitir, y la IP de origen 10.10.10.10 se configura con prioridad 2 para denegar, el acceso se permite si el perfil está activo, y la segunda regla se ignora.

10. Haga clic en el botón Add.
Se agrega la regla de acceso.

11. Para agregar otra regla, repita los pasos del Paso 5 al Paso 10.

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

Administrar la autenticación de puertos

En la autenticación basada en puertos, 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 un momento dado, solo un solicitante puede intentar la autenticación en un puerto en este modo. Los puertos en este modo están bajo control bidireccional. Este es el modo de autenticación predeterminado.

La red 802.1X tiene tres componentes:

- Autenticadores. El puerto que se autentica antes de permitir el acceso al sistema.
- Solicitantes. El host conectado al puerto autenticado que solicita acceso a los servicios del sistema.
- Servidor de autenticación. El servidor externo, por ejemplo, el
- servidor que realiza la autenticación en nombre del autenticador e indica si el usuario está autorizado para acceder a los servicios del sistema.

Configurar los ajustes globales de 802.1X

Para configurar los ajustes globales de 802.1X:

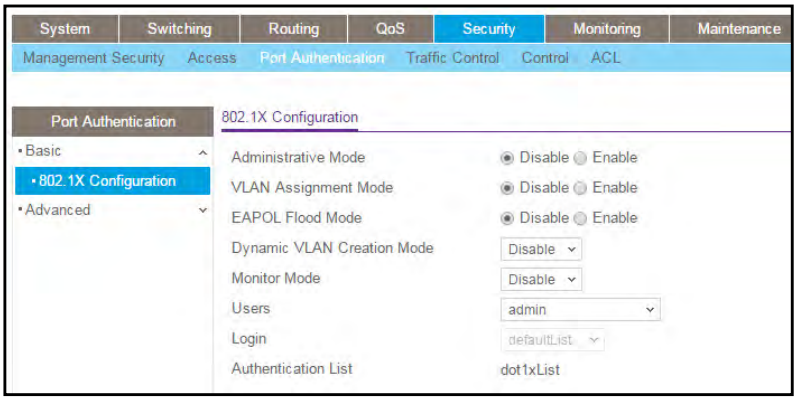
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Port Authentication > Basic > 802.1X Configuration.



5. Seleccione el botón de opción Administrative Mode Disable o Enable.
Esto habilita o deshabilita el modo administrativo de 802.1X en el switch.

- Enable. Se permite la autenticación basada en puertos en el switch.

  Si 802.1X está habilitado, la autenticación la realiza un servidor RADIUS. Esto significa que el método de autenticación principal debe ser RADIUS. Para establecer el método, seleccione Security > Management Security > Authentication List y seleccione RADIUS como método 1 para defaultList. Para obtener más información, consulte Configurar una lista de autenticación de inicio de sesión en la página 518.

- Disable. El switch no verifica la autenticación 802.1X antes de permitir tráfico en ningún puerto, aunque los puertos estén configurados para permitir solo usuarios autenticados. Valor predeterminado.

6. Seleccione el botón de opción VLAN Assignment Mode Disable o Enable.

El valor predeterminado es Disable.

7. Seleccione el botón de opción EAPOL Flood Mode Disable o Enable.

El valor predeterminado es Disable.

8. Use Dynamic VLAN Creation Mode para seleccionar Disable o Enable.

El valor predeterminado es Disable.

9. Use Monitor Mode para seleccionar Disable o Enable.

El valor predeterminado es Disable. Esta función supervisa el proceso de autenticación dot1x y ayuda a diagnosticar los casos de fallas de autenticación.

10. Use Users para seleccionar el nombre de usuario de la lista de inicio de sesión seleccionada para la seguridad de puertos 802.1x.
11. Use Login para seleccionar la lista de inicio de sesión que se aplicará al usuario especificado. Se muestran todas las listas de inicio de sesión configuradas. El campo Authentication List muestra la lista de autenticación que usa 802.1X.
12. Haga clic en el botón Apply.
La configuración se guarda.

Configurar los ajustes de 802.1X

Puede habilitar o deshabilitar el control de acceso 802.1X en el sistema.

Para configurar los ajustes de 802.1X:

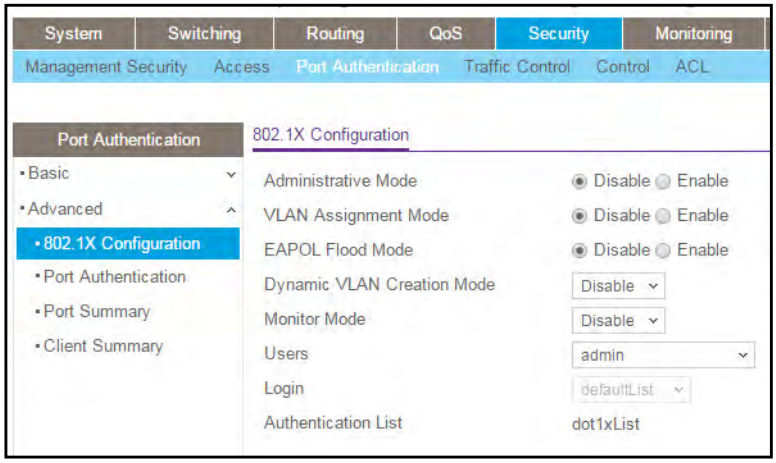
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Port Authentication > Advanced > 802.1X Configuration.



5. Seleccione el botón de opción Administrative Mode Disable o Enable. El valor predeterminado es Disable.

6. Seleccione el botón de opción VLAN Assignment Mode Disable o Enable.

El valor predeterminado es Disable.

7. Seleccione el botón de opción EAPOL Flood Mode Disable o Enable.

El valor predeterminado es Disable.

8. Use Dynamic VLAN Creation Mode para seleccionar Disable o Enable.

El valor predeterminado es Disable.

9. Use Monitor Mode para seleccionar Disable o Enable.

El valor predeterminado es Disable. Esta función supervisa el proceso de autenticación dot1x y ayuda a diagnosticar los casos de fallas de autenticación.

10. Use Users para seleccionar el nombre de usuario de la lista de inicio de sesión seleccionada para la seguridad de puertos 802.1x.
11. Use Login para seleccionar la lista de inicio de sesión que se aplicará al usuario especificado.
Se muestran todas las listas de inicio de sesión configuradas. El campo Authentication List muestra la lista que usa 802.1X.
12. Haga clic en el botón Apply.
La configuración se guarda.

Configurar la autenticación de puertos

Puede habilitar y configurar el control de acceso en uno o más puertos.

Para configurar los ajustes de 802.1X del puerto:

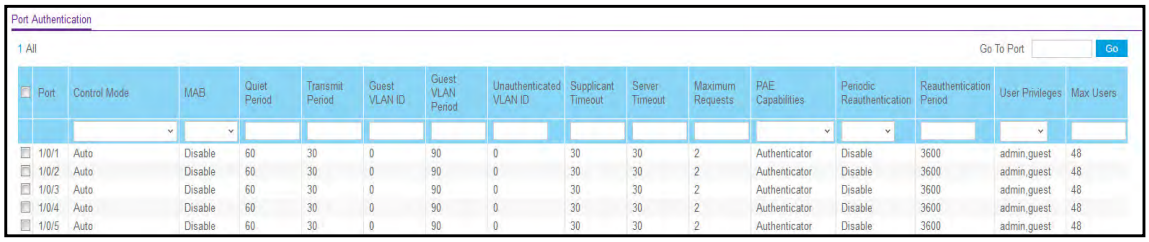
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Port Authentication > Advanced > Port Authentication.



Nota: Mueva la barra de desplazamiento horizontal de la parte inferior de la página para ver más campos.

5. Seleccione la casilla junto al puerto que desea configurar.

   También puede seleccionar varias casillas para aplicar los mismos ajustes a los puertos seleccionados, o la casilla de la fila de encabezado para aplicarlos a todos los puertos.

6. Para los puertos seleccionados, especifique los siguientes ajustes:
   - Control Mode. Seleccione una opción de modo de control. El modo de control solo se establece si el estado del enlace del puerto es Link Up. Las opciones son las siguientes:
     - Force unauthorized. La entidad de acceso al 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.
  - MAC Based. 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, por cada solicitante.
  - N/A. El modo de control no aplica.
- Use MAB para habilitar o deshabilitar el modo basado en MAC. La opción predeterminada es Disable. 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, por cada solicitante.
- Quiet Period. Este campo le permite configurar el periodo de silencio del puerto seleccionado. Establece el valor en segundos del temporizador que usa la máquina de estados del autenticador en este puerto para definir los periodos en los que no intenta adquirir un solicitante. El periodo de silencio es el tiempo durante el cual el autenticador no intenta adquirir un solicitante tras un intercambio de autenticación fallido con el solicitante. Debe ser un número en el rango de 0 a 65535. Un valor de periodo de silencio de 0 significa que la máquina de estados del autenticador nunca adquiere un solicitante. El valor predeterminado es 60. Cambiar el valor no modifica la configuración hasta que hace clic en el botón Apply.
- Transmit Period. Este campo le permite configurar el periodo de transmisión del puerto seleccionado. Es el valor, en segundos, del temporizador que usa la máquina de estados del autenticador en el puerto especificado para determinar cuándo enviar una trama EAPOL EAP request/identity al solicitante. Debe ser un número en el rango de 1 a 65535. El valor predeterminado es 30. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply.
- GuestVLAN ID. Este campo le permite configurar el ID de VLAN de invitados en la interfaz. El rango válido es 0–4093. El valor predeterminado es 0. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply. Escriba 0 para borrar el ID de VLAN de invitados en la interfaz.
- Guest VLAN Period. Este campo permite al usuario escribir el periodo de VLAN de invitados del puerto seleccionado. Es el valor, en segundos, del temporizador de la autenticación de VLAN de invitados. Debe ser un valor de 1 a 300. El valor predeterminado es 90. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply.
- Unauthenticated VLAN ID. Escriba el ID de VLAN no autenticada del puerto seleccionado. El rango válido es 0–4093. El valor predeterminado es 0. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply. Escriba 0 para borrar el ID de VLAN no autenticada en la interfaz.
- Supplicant Timeout. Escriba el tiempo de espera del solicitante para el puerto seleccionado. Es el valor, en segundos, del temporizador que usa la máquina de estados del autenticador en este puerto para agotar el tiempo de espera del solicitante. Debe estar

en el rango de 1 a 65535. El valor predeterminado es 30. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply.

- Server Timeout. Escriba el tiempo de espera del servidor para el puerto seleccionado. Es el valor, en segundos, del temporizador que usa el autenticador en este puerto para agotar el tiempo de espera del servidor de autenticación. Debe estar en el rango de 1 a 65535. El valor predeterminado es 30. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply.
- Maximum Requests. Escriba el máximo de solicitudes del puerto seleccionado. Es el número máximo de veces que la máquina de estados del autenticador en este puerto retransmite una EAPOL EAP request/identity antes de agotar el tiempo de espera del solicitante. Debe estar en el rango de 1 a 10. El valor predeterminado es 2. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply.
- PAE Capabilities. Seleccione la funcionalidad de entidad de acceso al puerto (PAE) del puerto seleccionado. Los valores posibles son Authenticator o Supplicant.
- Periodic Reauthentication. Habilita o deshabilita la reautenticación del solicitante en el puerto especificado. Los valores son Enable o Disable. Si el valor es Enable, se produce la reautenticación. De lo contrario, no se permite. El valor predeterminado es Disable. Cambiar la selección no modifica la configuración hasta que se hace clic en el botón Apply.
- Reauthentication Period. Escriba el periodo de reautenticación del puerto seleccionado. Es el valor, en segundos, del temporizador de la máquina de estados del autenticador en este puerto para determinar cuándo se reautentica el solicitante. Debe ser un valor en el rango de 1 a 65535. El valor predeterminado es 3600. Cambiar el valor no modifica la configuración hasta que se hace clic en el botón Apply.
- User Privileges. Agrega el usuario especificado a la lista de usuarios con acceso al puerto especificado o a todos los puertos.
- Max Users. Escriba el límite de solicitantes en la interfaz especificada.

7. Para iniciar la secuencia de inicialización en el puerto seleccionado, haga clic en el botón Initialize. Comienza la secuencia de inicialización.

   Solo puede hacer clic en este botón si el modo de control es auto. Si el botón no está disponible, aparece atenuado. Al hacer clic en este botón, la acción es inmediata. No necesita hacer clic en el botón Apply para que se realice la acción.

8. Haga clic en el botón Reauthentication.

Comienza la secuencia de reautenticación en el puerto seleccionado.

Solo puede hacer clic en este botón si el modo de control es auto. Si el botón no está disponible, aparece atenuado. Al hacer clic en este botón, la acción es inmediata. No necesita hacer clic en el botón Apply para que se realice la acción.

Ver el resumen de puertos

Puede ver información sobre los ajustes de control de acceso de un puerto específico.

Para ver el resumen de puertos:

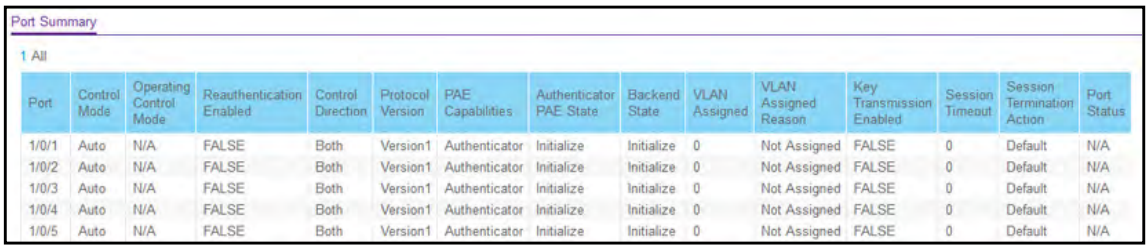
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Port Authentication > Advanced > Port Summary.



La siguiente tabla describe los campos de la página Port Summary.

Tabla 199. Resumen de puertos

Campo	Descripción
Port	El puerto cuyos ajustes se muestran en la fila actual de la tabla.
Control Mode	Indica el modo de control configurado para el puerto. Los valores posibles son los siguientes: • Force Unauthorized. La entidad de acceso al 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. • MAC Based. La PAE del autenticador establece el modo del puerto controlado según el resultado de los intercambios de autenticación entre un solicitante, un autenticador y un servidor de autenticación, por cada solicitante.

Tabla 199. Resumen de puertos (continuación)

Campo	Descripción
Operating Control Mode	El modo de control con el que opera realmente el puerto. Los valores posibles son los siguientes: • ForceUnauthorized • ForceAuthorized • Auto • MAC Based • N/A: Si el puerto está en estado desconectado, no puede participar en el control de acceso de puertos.
Reauthentication Enabled	Indica si se permite la reautenticación del solicitante en el puerto especificado. Los valores posibles son True y False. Si el valor es True, se produce la reautenticación. De lo contrario, no se permite.
Control Direction	La dirección de control del puerto especificado. La dirección de control determina el grado en que se producen intercambios de protocolo entre el solicitante y el autenticador. Esto afecta si el puerto controlado no autorizado ejerce control sobre la comunicación en ambas direcciones (deshabilitando tramas entrantes y salientes) o solo en la dirección entrante (deshabilitando solo la recepción de tramas entrantes). Este campo no es configurable en algunas plataformas.
Protocol Version	La versión de protocolo asociada al puerto seleccionado. El único valor posible es 1, correspondiente a la primera versión de la especificación 802.1x. Este campo no es configurable.
PAE Capabilities	La funcionalidad de entidad de acceso al puerto (PAE) del puerto seleccionado. Los valores posibles son Authenticator o Supplicant. Este campo no es configurable.
Authenticator PAE State	El estado actual de la máquina de estados PAE del autenticador. Los valores posibles son los siguientes: • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend State	El estado actual de la máquina de estados de autenticación de backend. Los valores posibles son los siguientes: • Request • Response • Success • Fail • Timeout • Initialize • Idle

Tabla 199. Resumen de puertos (continuación)

Campo	Descripción
VLAN Assigned	El VLAN ID asignado por el autenticador a la interfaz seleccionada. Este campo solo aparece cuando el modo de control de puerto de la interfaz seleccionada no es MAC-based. Este campo no es configurable.
VLAN Assigned Reason	El motivo del VLAN ID asignado por el autenticador a la interfaz seleccionada. Este campo solo aparece cuando el modo de control de puerto de la interfaz seleccionada no es MAC-based. Este campo no es configurable. Los valores posibles son los siguientes: • Radius • Unauth • Default • Not Assigned
Key Transmission Enabled	Indica si la transmisión de claves está habilitada en el puerto seleccionado. Este campo no es configurable. Los valores posibles son True y False. Si el valor es False, no se transmiten claves. De lo contrario, se admite la transmisión de claves en el puerto seleccionado.
Session Timeout	El tiempo de espera de sesión establecido por el servidor RADIUS para el puerto seleccionado. Este campo solo aparece cuando el modo de control del puerto seleccionado no es MAC-based.
Session Termination Action	La acción de terminación establecida por el servidor RADIUS para el puerto seleccionado. Este campo solo aparece cuando el modo de control del puerto seleccionado no es MAC-based. Los valores posibles son los siguientes: • Default • Reauthenticate Si la acción de terminación es default, al final de la sesión se inicializan los datos del cliente. De lo contrario, se intenta la reautenticación.
Port Status	El estado de autorización del puerto especificado. Los valores posibles son Authorized, Unauthorized y N/A. Si el puerto está en estado desconectado, el valor es N/A porque el puerto no puede participar en el control de acceso de puertos.

Ver el resumen de clientes

Para ver el resumen de clientes:

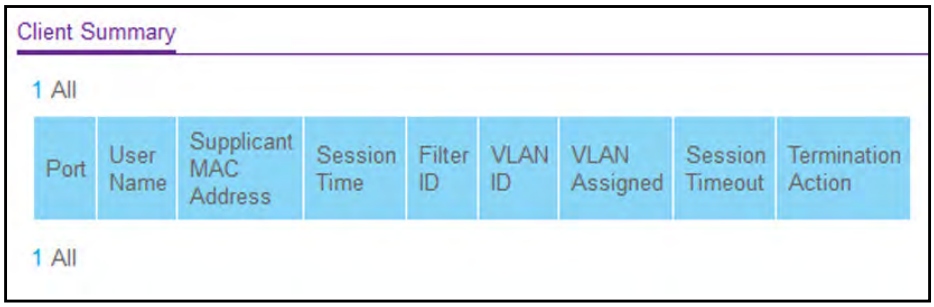
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Port Authentication > Advanced > Client Summary.



La siguiente tabla describe los campos de la página Client Summary.

Tabla 200. Resumen de clientes

Campo	Descripción
Port	El puerto que se mostrará.
User Name	El nombre de usuario 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 políticas asignado por el autenticador al dispositivo solicitante.
VLAN ID	El VLAN ID asignado por el autenticador al dispositivo solicitante.
VLAN Assigned	El motivo del VLAN ID asignado por el autenticador al dispositivo solicitante.
Session Timeout	El tiempo de espera de sesión establecido por el servidor RADIUS para el dispositivo solicitante.
Termination Action	La acción de terminación establecida por el servidor RADIUS para el dispositivo solicitante.

Controlar el tráfico con filtrado MAC

Puede configurar filtros MAC

Configurar el filtrado MAC

Puede crear filtros MAC que limiten el tráfico permitido de entrada y salida en puertos específicos del sistema.

Para configurar los ajustes de filtros MAC:

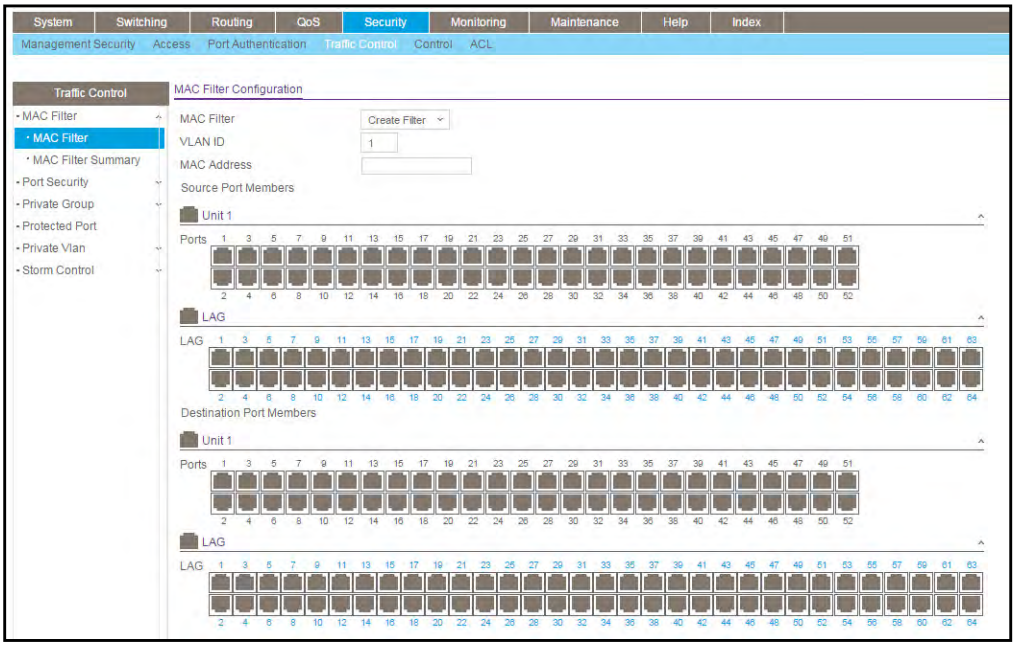
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > MAC Filter.



Esta es la lista de pares de dirección MAC y VLAN ID de todos los filtros configurados.
5. Para cambiar las máscaras de puertos de un filtro existente, seleccione la entrada.
6. Para agregar un filtro nuevo, seleccione Create Filter en la lista MAC Filter.

7. En la lista VLAN ID, seleccione la VLAN que se usará con la dirección MAC para identificar por completo los paquetes que se filtrarán.

   Solo puede cambiar este campo cuando está seleccionado Create Filter en la lista MAC Filter.

8. En el campo MAC Address, especifique la dirección MAC del filtro en el formato 00:01:1A:B2:53:4D.

   Puede cambiar este campo cuando selecciona la opción Create Filter. 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. Use Source Port Members para indicar los puertos que se incluirán en el filtro de entrada.

   Si se recibe un paquete con la dirección MAC y el VLAN ID seleccionados en un puerto que no está en la lista, se descarta.

10. Use Destination Port Members para indicar los puertos que se incluirán en el filtro de salida.

    Los paquetes con la dirección MAC y el VLAN ID seleccionados solo se transmiten desde puertos que están en la lista. Los puertos de destino solo pueden incluirse en el filtro multicast.

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

Resumen de filtros MAC

Para ver el resumen de filtros MAC:

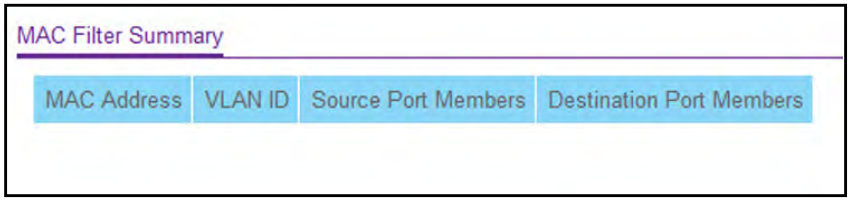
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > MAC Filter > MAC Filter Summary.



La siguiente tabla describe la información que se muestra en la página.

Tabla 201. Resumen de filtros MAC

Campo	Descripción
MAC Address	La dirección MAC del filtro en el formato 00:01:1A:B2:53:4D.
VLAN ID	El VLAN ID asociado al filtro.
Source Port Members	Una lista de puertos que se usan para filtrar los paquetes entrantes.
Destination Port Members	Una lista de puertos que se usan para filtrar los paquetes salientes.

Configurar la seguridad de puertos y los grupos privados

Puede configurar los ajustes de seguridad de puertos y crear grupos privados de puertos.

Configurar el modo global de seguridad de puertos

Puede bloquear uno o más puertos del sistema. Cuando un puerto está bloqueado, solo se pueden reenviar los paquetes con una dirección MAC de origen permitida. Todos los demás paquetes se descartan.

Para configurar el modo global de seguridad de puertos:

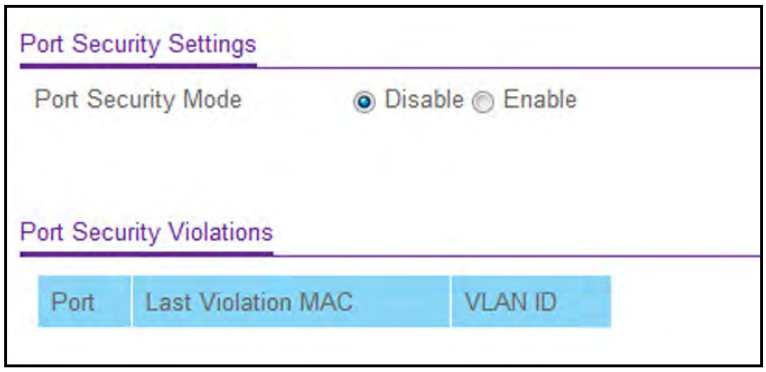
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Port Security > Port Administration.



5. Seleccione el botón de opción Port Security Mode Disable o Enable.

La tabla Port Security Violations muestra información sobre las infracciones ocurridas en los puertos con seguridad de puertos habilitada. La siguiente tabla describe los campos de la tabla Port Security Violations.

Tabla 202. Infracciones de seguridad de puertos

Campo	Descripción
Port	La interfaz física.
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 dirección MAC infractora.

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 alcanzó el límite, un paquete con una dirección MAC de origen desconocida se aprende y se reenvía normalmente. Al alcanzar 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:

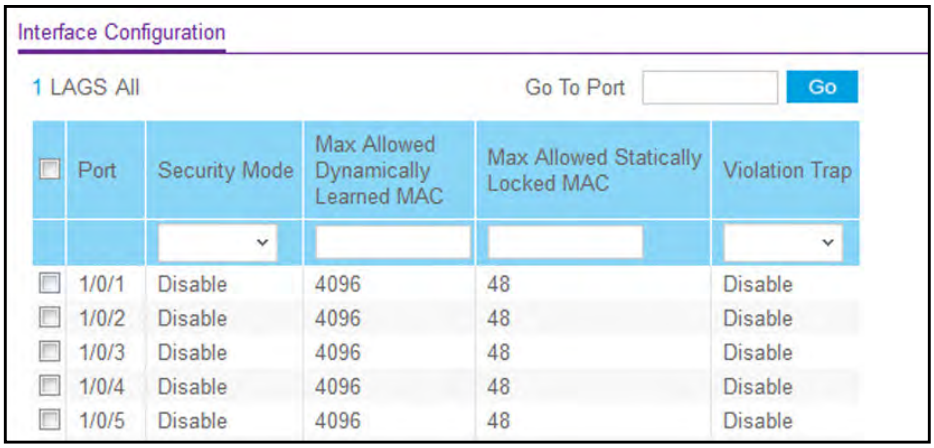
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Port Security > Interface Configuration.



5. Use uno de los siguientes métodos para seleccionar un puerto:
   - En el campo Go To Port, escriba la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.
   - Junto a la columna Port, seleccione la casilla del puerto que desea configurar, seleccione varias casillas para aplicar el mismo ajuste a los puertos seleccionados, o seleccione la casilla del encabezado de la tabla para aplicar los mismos ajustes a todos los puertos.
6. Especifique los siguientes ajustes:
   - Security Mode. Habilita o deshabilita la seguridad de puertos en la interfaz seleccionada.
   - Max Allowed Dynamically Learned MAC. Establece el número máximo de direcciones MAC aprendidas dinámicamente en la interfaz seleccionada.
   - Max Allowed Statically Locked MAC. Establece el número máximo de direcciones MAC bloqueadas estáticamente en la interfaz seleccionada.
   - Violation Traps. Habilita o deshabilita el envío de traps de infracción que indican cuándo se recibe un paquete con una dirección MAC no permitida en un puerto bloqueado.
7. Haga clic en el botón Apply.
La configuración se guarda.

Convertir direcciones MAC aprendidas en direcciones estáticas

Puede convertir una dirección MAC aprendida dinámicamente en una dirección bloqueada estáticamente.

Para convertir las direcciones MAC aprendidas y ver las direcciones MAC aprendidas de una interfaz:

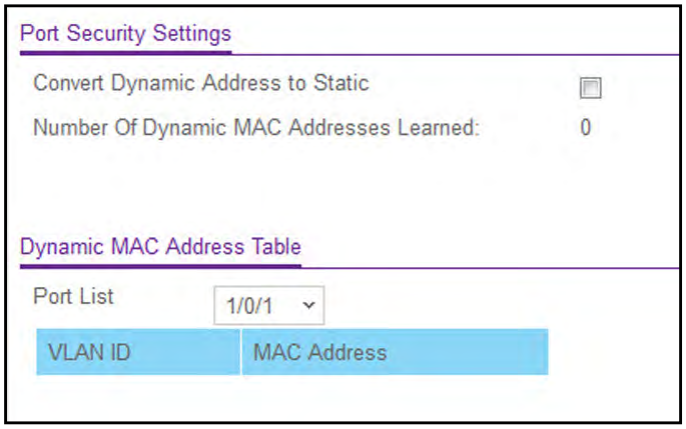
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Port Security > Dynamic MAC Address.



5. Seleccione la casilla Convert Dynamic Address to Static para convertir una dirección MAC aprendida dinámicamente en una dirección bloqueada estáticamente.

   Las entradas de direcciones MAC dinámicas se convierten en entradas estáticas en orden numérico ascendente hasta alcanzar el límite estático.

6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
7. En el menú Port List, seleccione la interfaz física.

En la siguiente tabla se muestran las direcciones MAC y sus VLAN asociadas aprendidas en la interfaz seleccionada.

Tabla 203. Dirección MAC dinámica

Campo	Descripción
Número de direcciones MAC dinámicas aprendidas	Número de direcciones MAC aprendidas dinámicamente en la interfaz.
ID de VLAN	ID de VLAN que corresponde a la dirección MAC.
Dirección MAC	Direcciones MAC aprendidas en un puerto específico.

Configurar direcciones MAC estáticas

Para configurar una dirección MAC estática:

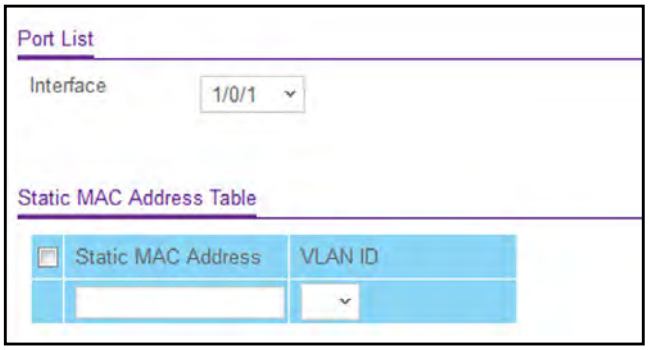
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Security > Traffic Control > Port Security > Static MAC Address.**



5. En el menú Interface, seleccione la interfaz física.
6. En el campo Static MAC Address, introduzca la dirección MAC que desea agregar.

7. En el campo VLAN ID, seleccione el ID de VLAN que corresponde a la dirección MAC que se agrega.
8. Haga clic en el botón Add.

La dirección MAC estática se agrega al switch.

Configurar grupos privados

Para configurar un grupo privado de control de tráfico:

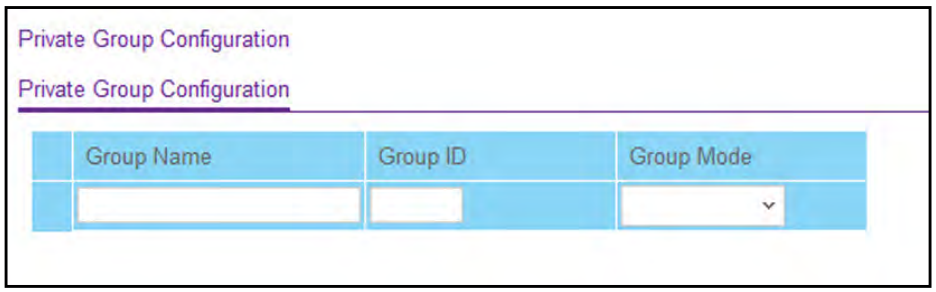
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private Group > Private Group Configuration.



5. En el campo Group Name, introduzca el nombre del grupo privado. El nombre puede tener hasta 24 bytes de caracteres sin espacios.
6. En el campo opcional Group ID, especifique el identificador del grupo privado. El rango del ID de grupo es de 1 a 192.
7. En la lista Group Mode, seleccione el modo del grupo privado.

   El modo de grupo puede ser isolated o community. En modo isolated, el puerto miembro del grupo no puede reenviar su tráfico de salida a ningún otro miembro del mismo grupo. De forma predeterminada, el modo es community, en el que cada puerto miembro puede reenviar tráfico a otros miembros del mismo grupo, pero no a miembros de otros grupos.

8. Haga clic en el botón Add.
El grupo privado se crea en el switch.

Configurar la pertenencia a grupos privados

Para configurar la pertenencia a grupos privados:

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

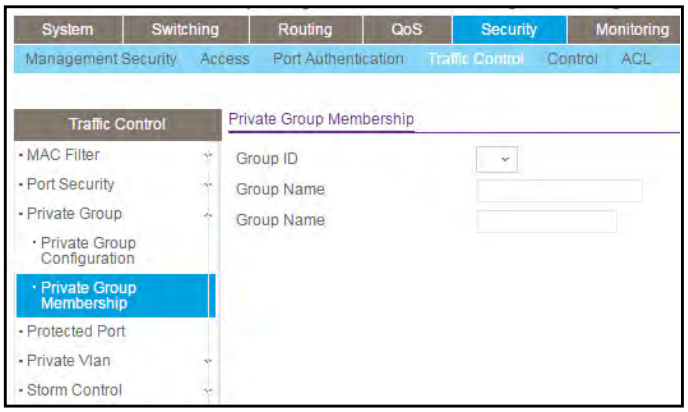
Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private Group > Private Group Membership.



5. En la lista Group ID, seleccione el ID de grupo.
6. Use Port List para agregar los puertos seleccionados a este grupo privado. La lista de puertos se muestra cuando hay al menos un grupo configurado.
7. Haga clic en el botón Apply.

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 204. Pertenencia a grupos privados

Campo	Descripción
Nombre del grupo	Nombre del grupo privado seleccionado. Puede tener hasta 24 caracteres sin espacios.
Modo del grupo	Modo del grupo privado seleccionado. Los modos son los siguientes: • community • isolated En modo isolated, el puerto miembro del grupo no puede reenviar su tráfico de salida a ningún otro miembro del mismo grupo. De forma predeterminada, el modo es community. Cada puerto miembro puede reenviar tráfico a otros miembros del mismo grupo, pero no a miembros de otros grupos.

Configurar puertos protegidos

Si un puerto se configura como protegido, no reenvía tráfico a ningún otro puerto protegido del switch, pero sí a los puertos no protegidos. Puede configurar los puertos como protegidos o no protegidos. Necesita privilegios de lectura y escritura para modificar la configuración.

Para configurar puertos protegidos:

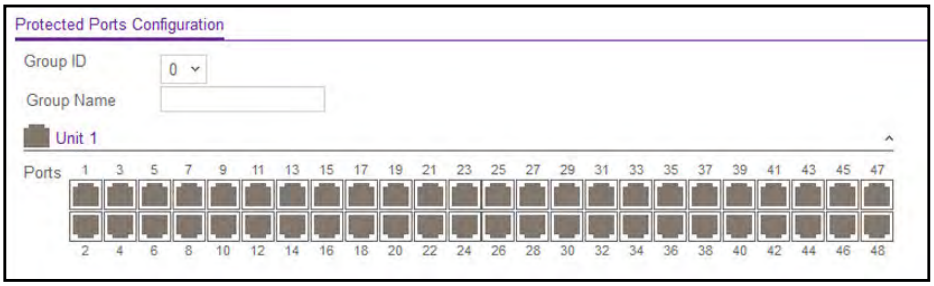
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Protected Ports.



5. En la lista Group ID, seleccione un grupo de puertos protegidos que se pueden combinar en un grupo lógico.

   El tráfico puede fluir entre puertos protegidos de distintos grupos, pero no dentro del mismo grupo. La lista incluye todos los ID de grupo de puertos protegidos admitidos en la plataforma actual. El rango válido del ID de grupo es de 0 a 2.

6. Use el campo opcional Group Name para asociar un nombre al grupo de puertos protegidos (con fines de identificación).

   Puede tener hasta 32 caracteres alfanuméricos, incluidos espacios. El valor predeterminado es vacío. Este campo es opcional.

7. Haga clic en la barra naranja para mostrar los puertos disponibles.
8. Marque la casilla debajo de cada puerto que desee configurar como protegido.

   La lista de selección incluye los puertos físicos, protegidos y no protegidos. Los puertos protegidos aparecen marcados para diferenciarlos. No es posible reenviar tráfico entre dos puertos protegidos. Si no se configura, el estado predeterminado es no protegido.

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

Configurar 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 tráfico de capa 2, sino también tráfico como FTP, HTTP y Telnet.

Configurar un tipo de VLAN privada

Para configurar un tipo de VLAN privada:

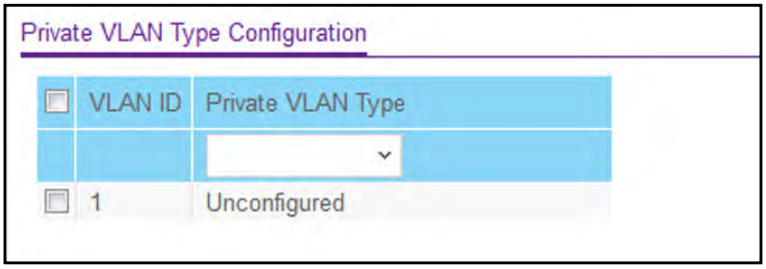
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Type Configuration.



5. Use Private VLAN Type para seleccionar el tipo de VLAN privada. El valor de fábrica es Unconfigured.
6. Haga clic en el botón Aplicar (Apply).
Se guarda la configuración.

El campo VLAN ID especifica el ID de VLAN para el que se establece el tipo de VLAN privada. El valor de fábrica es Unconfigured.

Configurar los ajustes de asociación de VLAN privada

Para configurar la asociación de VLAN privada:

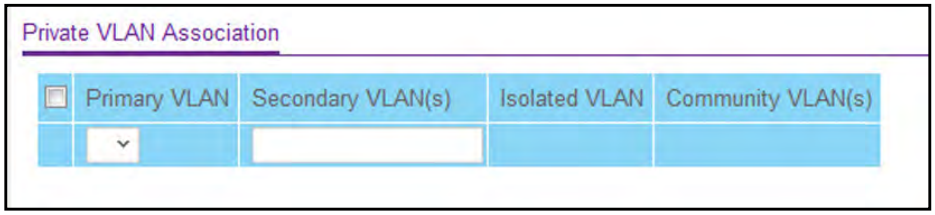
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Association Configuration.



5. Use Primary VLAN para seleccionar el ID de VLAN principal del dominio. Se usa para asociar VLAN secundarias al dominio.

6. Use Secondary VLAN(s) para mostrar todas las VLAN creadas estáticamente (excepto la principal y las VLAN predeterminadas).

Este control se usa para asociar VLAN a la VLAN principal seleccionada.
7. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 205. Asociación de VLAN privada

Campo	Descripción
VLAN aislada	VLAN aislada asociada a la VLAN principal seleccionada.
VLAN de comunidad	Lista de VLAN de comunidad asociadas a la VLAN principal seleccionada.

Configurar el modo de puerto de VLAN privada

Para configurar el modo de puerto de VLAN privada:

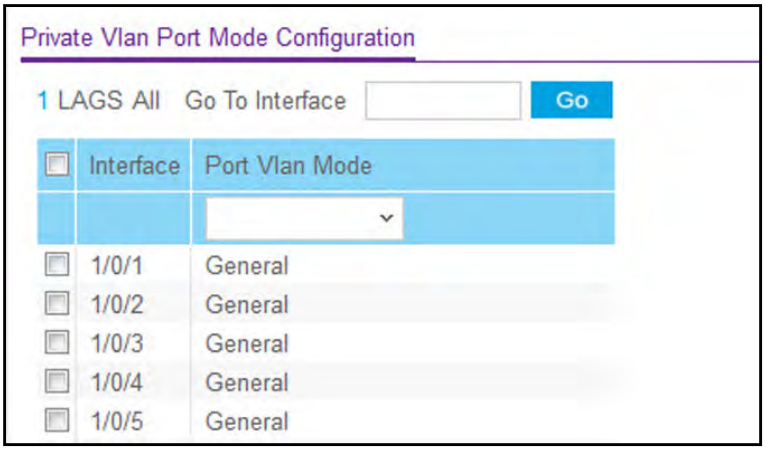
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Port Mode Configuration.



5. En el menú Port Vlan Mode, seleccione el modo de puerto de VLAN privada:

   - General. Establece el puerto en modo General.
   - Host. Establece el puerto en modo Host. Se usa para configurar VLAN privadas.
   - Promiscuous. Establece el puerto en modo Promiscuous. Se usa para configurar VLAN privadas.

El valor de fábrica es General.
6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar una interfaz host de VLAN privada

Para configurar una interfaz host de VLAN privada:

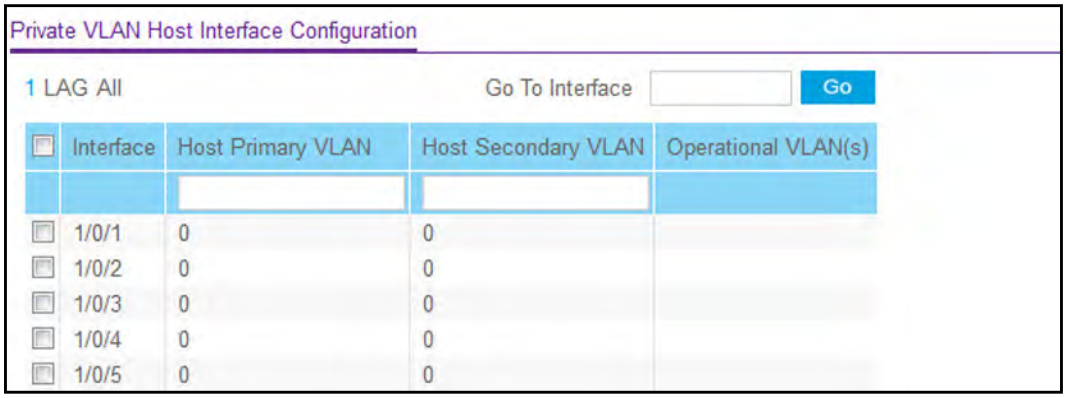
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration.



5. En el campo Host Primary VLAN, establezca el ID de VLAN principal para el modo Host Association. El rango del ID de VLAN es 2–4093.
6. Use Host Secondary VLAN para establecer el ID de VLAN secundaria para el modo Host Association. El rango del ID de VLAN es 2–4093.
7. Haga clic en el botón Apply.

La configuración se guarda.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 206. Configuración de interfaz host de VLAN privada

Campo	Descripción
Interfaz	Seleccione la interfaz física o LAG.
VLAN operativas	VLAN operativas.

Configurar una interfaz promiscua de VLAN privada

Para configurar una interfaz promiscua de VLAN privada:

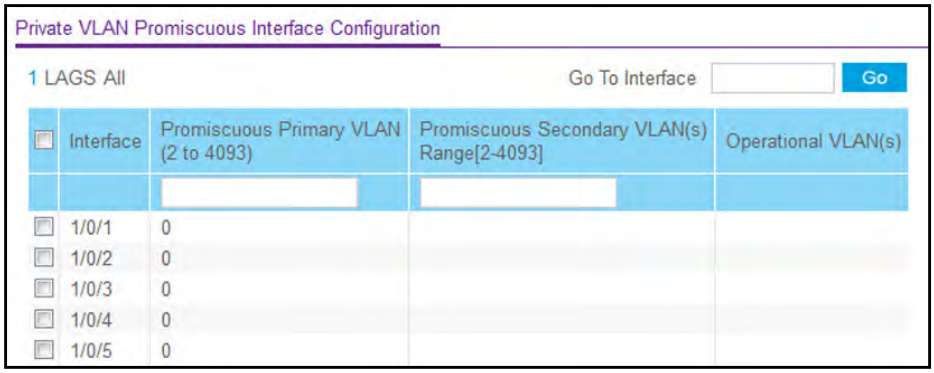
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration.



5. Use Promiscuous Primary VLAN para establecer el ID de VLAN principal para el modo Promiscuous Association.

   El rango del ID de VLAN es 2–4093.

6. Use Promiscuous Secondary VLAN ID(s) para establecer la lista de ID de VLAN secundarias para el modo Promiscuous Association.

   Este campo acepta un solo ID de VLAN, un rango de ID de VLAN o una combinación de ambos en secuencia separados por ','. Puede especificar un ID de VLAN individual, como 10. Puede especificar rangos de VLAN separados por un guion, por ejemplo, 10-13. Puede especificar una combinación de ambos separada por comas, por ejemplo: 12,15,40–43,1000–1005, 2000. El rango del ID de VLAN es 2–4093.

   Nota: La lista de ID de VLAN indicada en este control reemplaza la lista de VLAN secundarias configurada en la asociación.

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

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 207. Configuración de interfaz promiscua de VLAN privada

Campo	Descripción
Interfaz	Seleccione la interfaz física o LAG.
VLAN operativas	VLAN operativas.

Administrar los ajustes de control de tormentas

Una tormenta de broadcast es el resultado de un número excesivo de mensajes broadcast transmitidos simultáneamente a través de una red por un solo puerto. Las respuestas reenviadas pueden sobrecargar los recursos de la red o hacer que la red agote el tiempo de espera.

El switch mide por puerto la tasa de paquetes broadcast/multicast/unicast desconocidos entrantes y descarta paquetes cuando la tasa supera el valor definido. El control de tormentas se habilita 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

Para configurar los ajustes globales de control de tormentas:

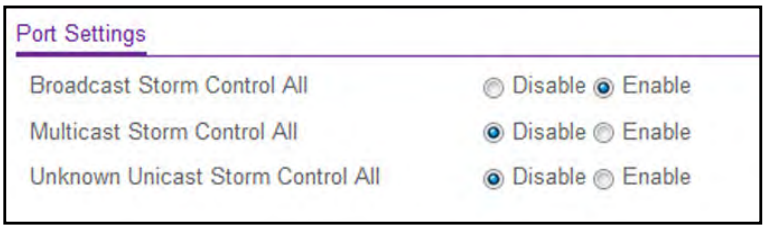
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Storm Control > Storm Control Global Configuration.



Los tres controles siguientes permiten habilitar o deshabilitar fácilmente, de forma global, cada tipo de paquete cuya tasa se limita en todos los puertos. El estado efectivo del control de tormentas de cada puerto se puede ver en la página de configuración de puertos.

5. Seleccione los ajustes de control de tormentas:
   - Seleccione el botón de opción Broadcast Storm Control All Disable o Enable.

     Esto habilita o deshabilita el modo Broadcast Storm Recovery en todos los puertos. Si selecciona Enable y el tráfico broadcast en cualquier puerto Ethernet supera el umbral configurado, el switch bloquea (descarta) el tráfico broadcast. El valor de fábrica es Enable.
   - Seleccione el botón de opción Multicast Storm Control All Disable o Enable.

     Esto habilita o deshabilita el modo Multicast Storm Recovery en todos los puertos. Si selecciona Enable y el tráfico multicast en cualquier puerto Ethernet supera el umbral configurado, el switch bloquea (descarta) el tráfico multicast. El valor de fábrica es Disable.
   - Seleccione el botón de opción Unknown Unicast Storm Control All Disable o Enable.

     Esto habilita o deshabilita el modo Unicast Storm Recovery en todos los puertos. Si selecciona Enable y el tráfico unicast en cualquier puerto Ethernet supera el umbral configurado, el switch bloquea (descarta) el tráfico unicast. El valor de fábrica es Disable.

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar el control de tormentas de un puerto

Para configurar el control de tormentas de un puerto:

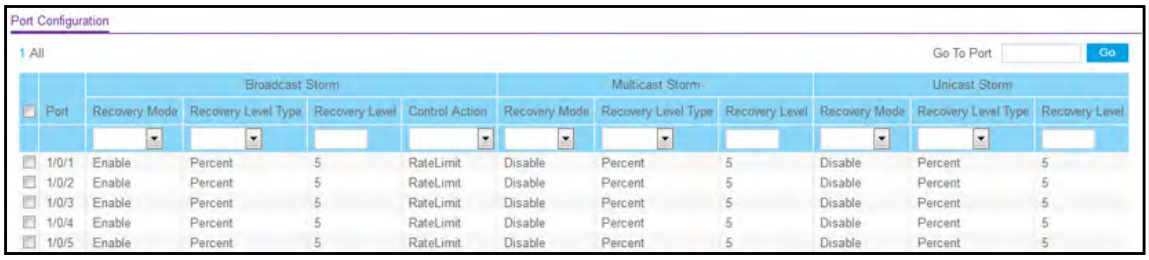
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Traffic Control > Storm Control > Storm Control Interface Configuration.



5. Use uno de los siguientes métodos para seleccionar un puerto:
   - En el campo Go To Port, escriba la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.
   - Junto a la columna Port, seleccione la casilla del puerto que desea configurar, seleccione varias casillas para aplicar el mismo ajuste a los puertos seleccionados, o seleccione la casilla del encabezado de la tabla para aplicar los mismos ajustes a todos los puertos.
6. Configure el control de tormentas de broadcast:
   - Recovery Mode. Habilite o deshabilite esta opción. Si selecciona Enable y el tráfico broadcast en el puerto especificado supera el umbral configurado, el switch bloquea (descarta) el tráfico broadcast. El valor de fábrica es Enable.
   - Recovery Level Type. Especifique el nivel de recuperación como porcentaje de la velocidad del enlace o en paquetes por segundo.
   - Recovery Level. Especifique el umbral a partir del cual se activa el control de tormentas. El valor de fábrica es el 5 por ciento de la velocidad del puerto para el tipo pps.
   - Control Action. Especifique la acción que se realiza cuando se supera el umbral configurado de la tormenta de broadcast. Puede seleccionar que se apague el puerto o que se limite la tasa del tráfico del puerto. El valor predeterminado es RateLimit.
7. Configure el control de tormentas de broadcast:
   - Recovery Mode. Habilite o deshabilite esta opción. Si selecciona Enable y el tráfico multicast en el puerto especificado supera el umbral configurado, el switch bloquea (descarta) el tráfico multicast. El valor de fábrica es Enable.
   - Recovery Level Type. Especifique el nivel de recuperación como porcentaje de la velocidad del enlace o en paquetes por segundo.
   - Recovery Level. Especifique el umbral a partir del cual se activa el control de tormentas. El valor de fábrica es el 5 por ciento de la velocidad del puerto para el tipo pps.
8. Configure el control de tormentas de broadcast:
   - Recovery Mode. Habilite o deshabilite esta opción. Si selecciona Enable y el tráfico unicast en el puerto especificado supera el umbral configurado, el switch bloquea (descarta) el tráfico unicast. El valor de fábrica es Enable.
   - Recovery Level Type. Especifique el nivel de recuperación como porcentaje de la velocidad del enlace o en paquetes por segundo.
   - Recovery Level. Especifique el umbral a partir del cual se activa el control de tormentas. El valor de fábrica es el 5 por ciento de la velocidad del puerto para el tipo pps.

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

Configurar DHCP snooping

Puede configurar los ajustes globales y de interfaz de DHCP snooping.

Configurar los ajustes globales de DHCP snooping

Para configurar los ajustes globales de DHCP snooping:

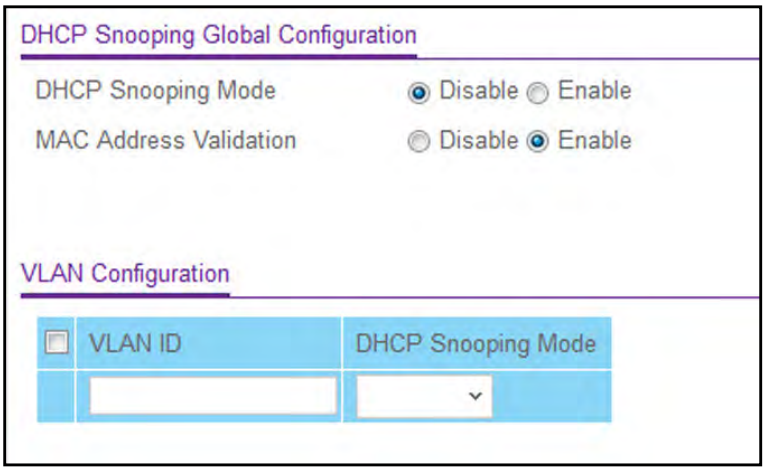
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > DHCP Snooping > Global Configuration.



5. Seleccione el botón de opción DHCP Snooping Mode Disable o Enable.

El valor de fábrica es Disable.

6. Seleccione el botón de opción MAC Address Validation Disable o Enable.

Esto habilita o deshabilita la validación de la dirección MAC del remitente para DHCP snooping. El valor de fábrica es Enable.

7. Use VLAN ID para introducir la VLAN en la que se habilitará el modo DHCP snooping.
8. Use DHCP Snooping Mode para habilitar o deshabilitar la función DHCP snooping en la VLAN introducida.

El valor de fábrica es Disable.
9. Haga clic en el botón Apply.
La configuración se guarda.

Configurar una interfaz de DHCP snooping

Para configurar una interfaz de DHCP snooping:

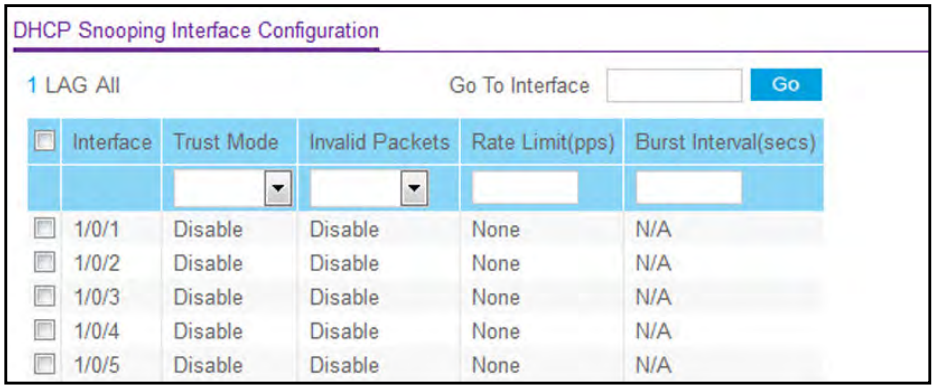
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > DHCP Snooping > Interface Configuration.



5. 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, marque la casilla del puerto que desea configurar, marque varias casillas para aplicar la misma configuración a todas las interfaces seleccionadas o marque la casilla del encabezado de la tabla para aplicar la misma configuración a todas las interfaces.
6. Si Trust Mode está habilitado, la aplicación DHCP snooping considera el puerto como de confianza. El valor de fábrica es Disable.

7. Si Invalid Packets está habilitado, la aplicación DHCP snooping registra los paquetes no válidos en esta interfaz.

El valor de fábrica es Disable.

8. Use Rate Limit (pps) para especificar el valor de límite de tasa para DHCP snooping.

Si la tasa entrante de paquetes DHCP supera este valor durante el intervalo de ráfaga consecutivo en segundos, el puerto se apaga. Si este valor es N/A, el intervalo de ráfaga no tiene sentido y se deshabilita. El valor predeterminado es N/A. Puede establecerse en –1, que significa N/A. El rango del límite de tasa es de 0 a 300.

9. Use Burst Interval (secs) para especificar el intervalo de ráfaga para limitar la tasa en esta interfaz.

Si el límite de tasa es N/A, el intervalo de ráfaga no tiene sentido y es N/A. El valor predeterminado es N/A. Puede establecerse en –1, que significa N/A. El rango de Burst Interval es de 1 a 15.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar un enlace estático de DHCP snooping

Para configurar un enlace estático de snooping:

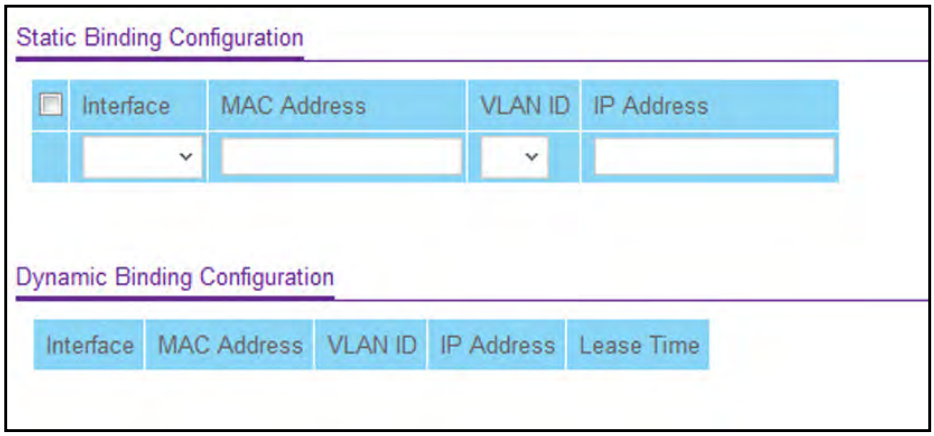
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > DHCP Snooping > Binding Configuration.



5. Para configurar un enlace estático, especifique lo siguiente:

a. En el menú Interface, seleccione la interfaz.

b. En el campo MAC Address, especifique la dirección MAC que debe agregarse a la entrada de enlace.
Es la clave de la base de datos de enlaces.
c. En el menú VLAN ID, seleccione la VLAN de la regla de enlace. El ID de VLAN va de 1 a 4093.
d. En el campo IP Address, especifique una dirección IP válida para la regla de enlace. e. Haga clic en el botón Agregar (Add).
La entrada de enlace de DHCP snooping se agrega a la base de datos.

Ver los enlaces dinámicos de DHCP snooping

Para ver los enlaces dinámicos de DHCP snooping:

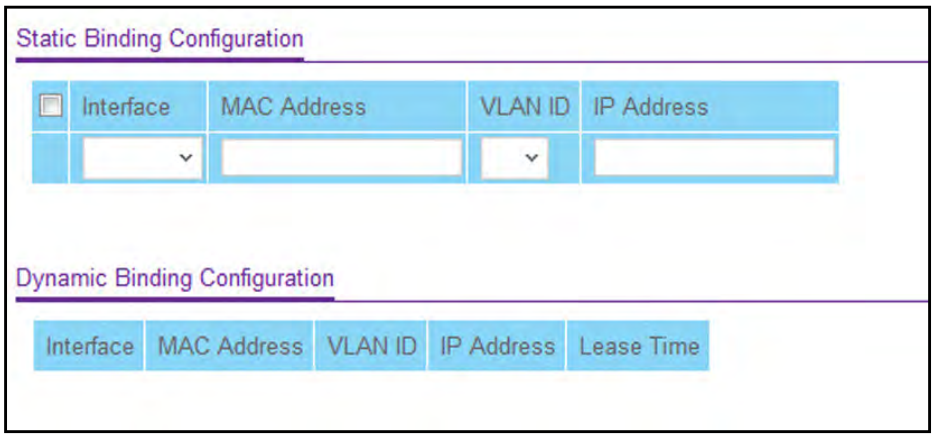
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > DHCP Snooping > Binding Configuration.



En la siguiente tabla se describen los campos de la tabla Dynamic Binding Configuration.

Tabla 208. Enlaces DHCP dinámicos

Campo	Descripción
Interfaz	Interfaz en la que se aprendió el enlace dinámico.
Dirección MAC	Dirección MAC aprendida para el enlace.
ID de VLAN	ID de VLAN que corresponde al enlace.
Dirección IP	Dirección IP que corresponde al enlace.
Tiempo de concesión	Tiempo de concesión restante del enlace.

Configurar los ajustes de persistencia de snooping

Para configurar los ajustes de persistencia de snooping:

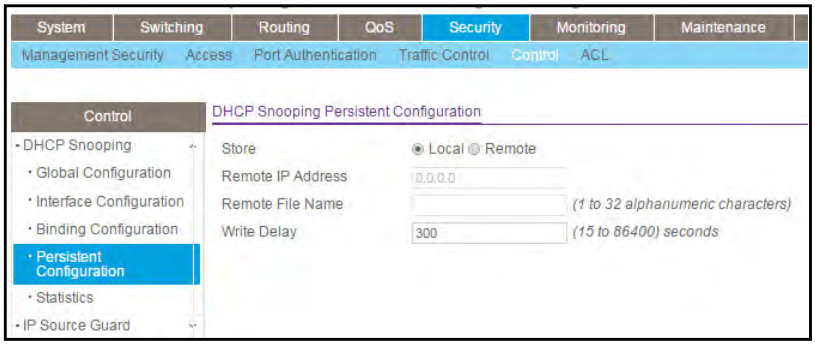
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > DHCP Snooping > Persistent Configuration.



5. Seleccione el botón de opción Store Local o Remote.
Al seleccionar Local se deshabilitan los campos remotos Remote File Name y Remote IP Address.
6. Si selecciona el botón de opción Remote, haga lo siguiente:

   a. En el campo Remote IP Address, escriba la dirección IP remota en la que se almacena la base de datos de snooping.

   b. En el campo Remote File Name, introduzca el nombre del archivo remoto donde se almacenará la base de datos.

7. En el campo Write Delay, introduzca el tiempo máximo para escribir la base de datos en el almacenamiento local o remoto.

El rango es de 15 a 86400.
8. Haga clic en el botón Apply (Aplicar). La configuración se guarda.

Ver y borrar las estadísticas de DHCP snooping

Para ver y borrar las estadísticas de DHCP snooping:

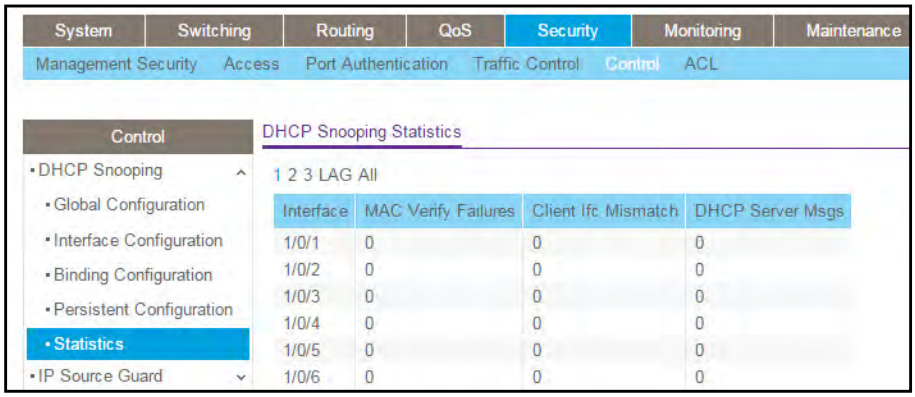
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > DHCP Snooping > Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar las estadísticas de todas las interfaces, haga clic en el botón Clear (Borrar).
La siguiente tabla describe las estadísticas de DHCP snooping.

Tabla 209. Estadísticas de DHCP snooping

Campo	Descripción
Interfaz	Interfaz no confiable y con snooping habilitado cuyas estadísticas se mostrarán.
Fallas de verificación MAC	Número de paquetes descartados por DHCP snooping porque no se encontró ninguna entrada de enlace de DHCP snooping coincidente.

Tabla 209. Estadísticas de DHCP snooping (continuación)

Campo	Descripción
Discrepancia de Ifc de cliente	Número de mensajes DHCP descartados según la verificación de la dirección MAC de origen y la dirección HW del cliente.
Mensajes del servidor DHCP	Número de mensajes del servidor descartados en un puerto no confiable.

Configurar interfaces de IP Source Guard

Puede configurar IP source guard (IPSG) en cada interfaz. IPSG es una función de seguridad que filtra 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 un par de dirección IP de origen y dirección MAC de origen. 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 donde DHCP snooping está deshabilitado o donde DHCP snooping está habilitado pero el puerto es de confianza, todo el tráfico IP recibido en ese puerto se descarta según las entradas IPSG configuradas por el administrador. Además, IPSG interactúa con la seguridad de puertos, también llamada bloqueo MAC de puertos, para hacer cumplir la dirección MAC de origen en los paquetes recibidos. La seguridad de puertos controla el aprendizaje de direcciones MAC de origen en la base de datos de reenvío de capa 2 (la tabla de direcciones MAC). Cuando se recibe una trama con una dirección MAC de origen no aprendida previamente, la seguridad de puertos consulta a la función IPSG para determinar si la dirección MAC pertenece a un enlace válido.

Para configurar los ajustes de interfaz de IP Source Guard:

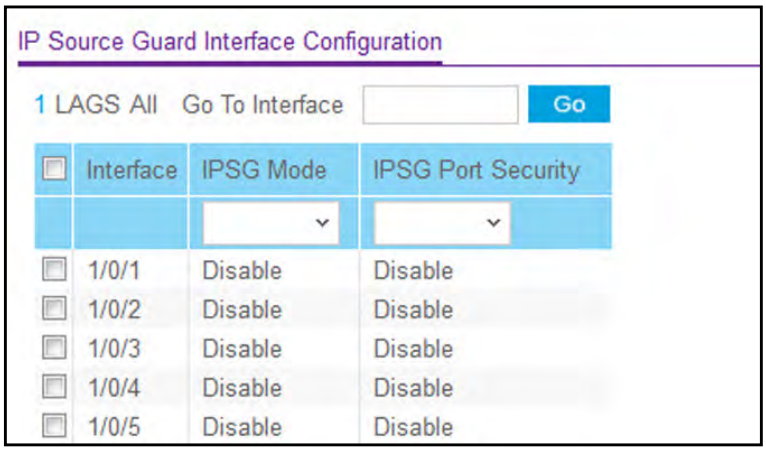
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > IP Source Guard > Interface Configuration.



5. 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, marque la casilla del puerto que desea configurar, marque varias casillas para aplicar la misma configuración a todas las interfaces seleccionadas o marque la casilla del encabezado de la tabla para aplicar la misma configuración a todas las interfaces.
6. En la lista IPSG Mode, seleccione Disable o Enable.

   Establece el modo administrativo de IPSG en la interfaz. Cuando el modo IPSG está habilitado, la dirección IP del remitente en esta interfaz se valida con la base de datos de enlaces de DHCP snooping. Si IPSG está habilitado, los paquetes no se reenvían si la dirección IP del remitente no está en la base de datos de enlaces de DHCP snooping. El valor de fábrica es Disable.

7. En la lista IPSG Port Security, seleccione Disable o Enable.

   Esto habilita o deshabilita el modo administrativo de la seguridad de puertos IPSG en la interfaz seleccionada. Si se habilita, los paquetes no se reenvían si la dirección MAC del remitente no está en la tabla de la base de datos de reenvío (FDB) ni en la base de datos de enlaces de DHCP snooping. Para aplicar el filtrado por dirección MAC, se requieren además las siguientes configuraciones:

   - Habilitar port-security globalmente.
   - Habilitar port-security a nivel de interfaz.

   La seguridad de puertos IPSG no se puede habilitar si IPSG está deshabilitado. El valor de fábrica es Disable. Además, no puede desactivar la seguridad de puertos IPv6SG mientras IPv6SG esté habilitado.

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

Configurar los ajustes de enlace de IP Source Guard

Para configurar los ajustes de enlace estático de IP Source Guard:

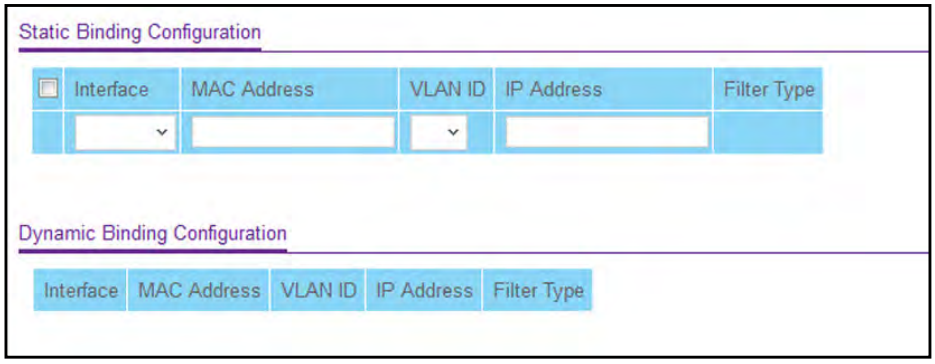
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > IP Source Guard > Binding Configuration.



5. En el menú Interface, seleccione la interfaz.
6. En el campo MAC Address, escriba la dirección MAC del enlace.
7. En el menú VLAN ID, seleccione la VLAN de la regla de enlace.
8. En el campo IP Address, especifique una dirección IP válida para la regla de enlace.
9. Haga clic en el botón Add.

La entrada de enlace estático de IPSG se agrega a la base de datos.

En la siguiente tabla se describe la información no configurable de enlaces dinámicos de IP Source Guard que se muestra.

Tabla 210. Configuración de enlaces dinámicos de IP Source Guard

Campo	Descripción
Interfaz	Interfaz para la que se agrega un enlace a la base de datos IPSG.
Dirección MAC	Dirección MAC de la entrada de enlace.
ID de VLAN	VLAN de la entrada de enlace.

Tabla 210. Configuración de enlaces dinámicos de IP Source Guard (continuación)

Campo	Descripción
Dirección IP	Muestra la dirección IP válida de la entrada de enlace.
Tipo de filtro	Tipo de filtro usado en la interfaz. Uno es el filtro por dirección IP de origen y el otro es el filtro por dirección IP y dirección MAC de origen.

Configurar los ajustes de interfaz de IPv6 Source Guard

Para configurar los ajustes de interfaz de IPv6 Source Guard:

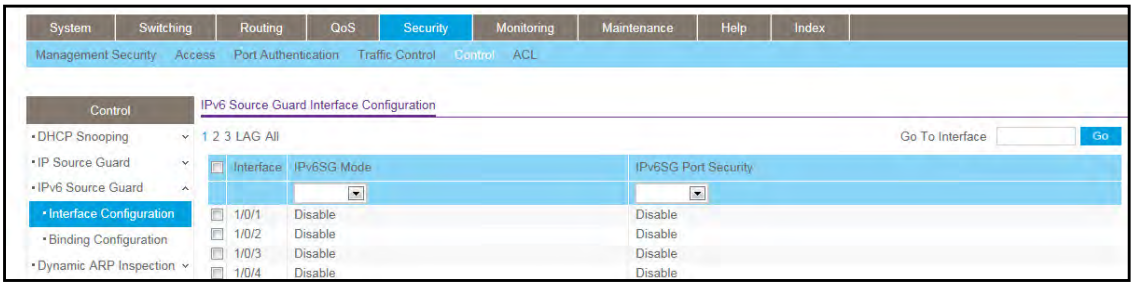
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > IPv6 Source Guard > Interface Configuration.



5. 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, marque la casilla del puerto que desea configurar, marque varias casillas para aplicar la misma configuración a todas las interfaces seleccionadas o marque la casilla del encabezado de la tabla para aplicar la misma configuración a todas las interfaces.
6. Use el menú IPv6SG Mode para habilitar o deshabilitar la validación de la dirección IPv6 del remitente en esta interfaz.

   Si IPv6SG está habilitado, los paquetes no se reenvían si la dirección IPv6 del remitente no está en la base de datos de enlaces de DHCP snooping. El valor de fábrica es Disable.

7. Use el menú IPv6SG Port Security para habilitar o deshabilitar la seguridad de puertos IPv6SG en la interfaz seleccionada.

   Si la seguridad de puerto IPv6SG está habilitada, los paquetes no se reenvían si la dirección MAC del remitente no está en la tabla FDB ni en la base de datos de enlaces de DHCP snooping. Para aplicar el filtrado por dirección MAC, se requieren las siguientes configuraciones adicionales:

   - Habilitar port-security globalmente.
   - Habilitar port-security a nivel de interfaz.

   La seguridad de puerto IPv6SG no se puede habilitar si IPv6SG está deshabilitado. El valor de fábrica es Disable. Además, no se puede desactivar la seguridad de puerto IPv6SG mientras IPv6SG esté habilitado.

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

Configurar un enlace de IPv6 Source Guard

Para configurar un enlace estático de IPv6 Source Guard:

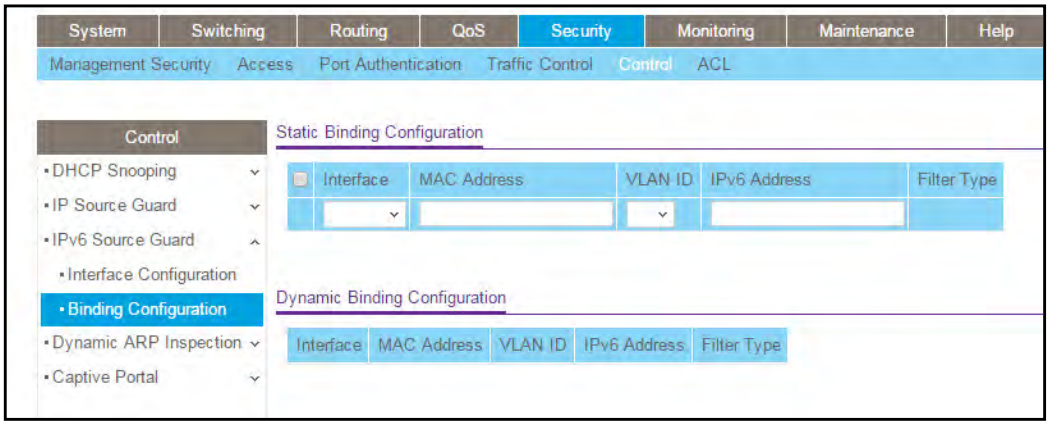
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > IPv6 Source Guard > Binding Configuration.



5. En el menú Interface, seleccione la interfaz para agregar un enlace a la base de datos IPv6SG.
6. En el campo MAC Address, especifique la dirección MAC del enlace.

7. En el menú VLAN ID, seleccione la VLAN de la lista para la regla de enlace.
8. En el campo IPv6 Address, especifique una dirección IP válida para la regla de enlace.
9. Haga clic en el botón Add.
La entrada de enlace estático IPv6SG se agrega a la base de datos.

La siguiente tabla describe la información no configurable de los enlaces dinámicos de IPv6 Source Guard que se muestra.

Tabla 211. Configuración de enlaces dinámicos de IPv6 Source Guard

Campo	Descripción
Interface	La interfaz para agregar un enlace a la base de datos IPSG.
Dirección MAC	Dirección MAC de la entrada de enlace.
ID de VLAN	VLAN de la entrada de enlace.
IPv6 Address	Muestra la dirección IPv6 válida de la entrada de enlace.
Filter Type	Tipo de filtro usado en la interfaz. Uno es el filtro por dirección IPv6 de origen y el otro es el filtro por dirección IPv6 de origen y dirección MAC.

Configurar la inspección dinámica de ARP

Puede configurar las VLAN, interfaces y ACL de inspección dinámica de ARP (DAI) con sus reglas asociadas.

Configurar los ajustes globales de inspección dinámica de ARP

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, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > Dynamic ARP Inspection > DAI Configuration.



5. Seleccione el botón de opción Validate Source MAC Disable o Enable.

Esto especifica el modo de validación de MAC de origen de DAI del switch. Si selecciona Enable, se habilita la validación de MAC del remitente de los paquetes ARP. El valor de fábrica es Disable.

6. Seleccione el botón de opción Validate Destination MAC Disable o Enable

Esto especifica el modo de validación de MAC de destino de DAI del switch. Si selecciona Enable, se habilita la validación de MAC de destino de los paquetes de respuesta ARP. El valor de fábrica es Disable.

7. Seleccione el botón de opción Validate IP Disable o Enable.

Esto especifica el modo de validación de IP de DAI del switch. Si selecciona Enable, se habilita la validación de direcciones IP de los paquetes ARP. El valor de fábrica es Disable.

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

Configurar VLAN de DAI

Puede configurar una o más VLAN de inspección dinámica de ARP (DAI).

Para configurar una o más VLAN de DAI:

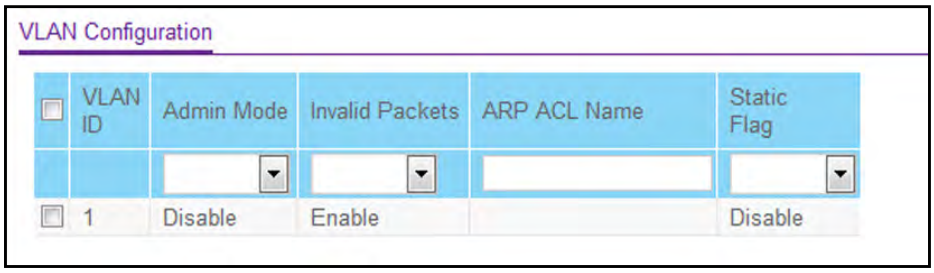
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration.



5. Use las casillas VLAN ID para seleccionar una o más VLAN compatibles con DAI.
6. En la lista Admin Mode, seleccione Enable o Disable.

   Esto indica si la inspección dinámica de ARP está habilitada en esta VLAN. Si se establece en Enable, la inspección dinámica de ARP está habilitada. Si se establece en Disable, la inspección dinámica de ARP está deshabilitada. El valor predeterminado es Disable.

7. Use Invalid Packets para indicar si el registro de inspección dinámica de ARP está habilitado en esta VLAN.

   Si se establece en Enable, se registra la información de los paquetes ARP no válidos. Si se establece en Disable, el registro de inspección dinámica de ARP está deshabilitado. El valor predeterminado es Enable.

8. Use ARP ACL Name para especificar un nombre para la lista de acceso ARP. Una VLAN puede configurarse para usar esta ACL ARP, que contiene reglas, como filtro para la validación

   de paquetes ARP. El nombre puede tener hasta 31 caracteres alfanuméricos. El nombre de la ACL ARP se elimina si especifica N/A.

9. Use Static Flag para determinar si el paquete ARP debe validarse con la base de datos de DHCP snooping en caso de que no coincidan las reglas de la ACL ARP.

   Si el indicador está habilitado, el paquete ARP se valida solo con las reglas de la ACL ARP. Si el indicador está deshabilitado, el paquete ARP requiere una validación adicional con las entradas de DHCP snooping. El valor de fábrica es Disable.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Configurar las interfaces DAI

Puede configurar una o más interfaces de inspección dinámica de ARP (DAI).

Para configurar una o más interfaces DAI:

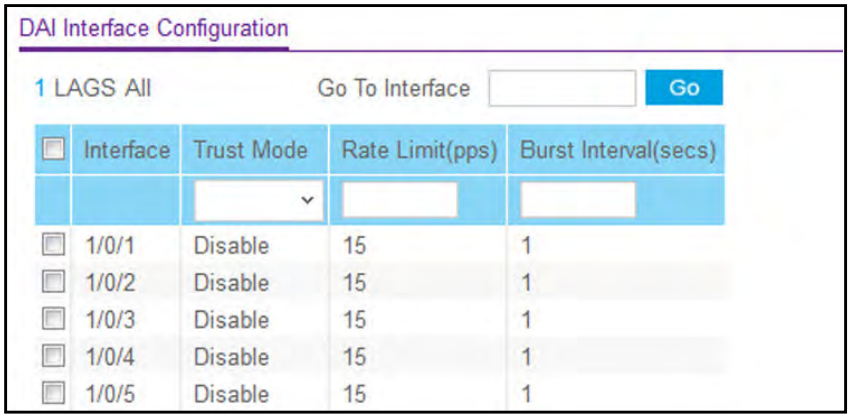
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Dynamic ARP Inspection > DAI Interface Configuration.



5. 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, marque la casilla del puerto que desea configurar, marque varias casillas para aplicar la misma configuración a todas las interfaces seleccionadas o marque la casilla del encabezado de la tabla para aplicar la misma configuración a todas las interfaces.

6. Use Trust Mode para indicar si la interfaz es de confianza para la inspección dinámica de ARP.

   Si se establece en Enable, la interfaz es de confianza. Los paquetes ARP que llegan a esta interfaz se reenvían sin verificación. Si se establece en Disable, la interfaz no es de confianza. Los paquetes ARP que llegan a esta interfaz se someten a inspección ARP. El valor de fábrica es Disable.

7. Use Rate Limit (pps) para especificar el límite de velocidad para la inspección dinámica de ARP.

   Si la velocidad de entrada de paquetes ARP supera este valor durante el intervalo de ráfaga consecutivo en segundos, los paquetes ARP se descartan. Si el valor es N/A, no hay límite. El valor puede establecerse en –1, que significa N/A. El rango es 0– 300. El valor de fábrica es 15 pps (paquetes por segundo).

8. Use Burst Interval (secs) para especificar el intervalo de ráfaga para la limitación de velocidad en esta interfaz. Si el límite de velocidad es None, el intervalo de ráfaga no tiene efecto y se muestra como N/A. El rango es de 1 a 15. El valor de fábrica es 1 segundo.

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

Configurar una ACL DAI

Puede configurar una ACL de inspección dinámica de ARP (DAI).

Para configurar una ACL DAI:

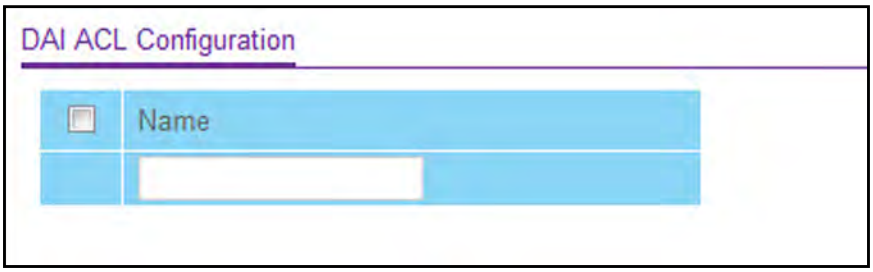
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > Dynamic ARP Inspection > DAI ACL Configuration.



5. Use Name para crear una ACL ARP para DAI.
6. Haga clic en el botón Agregar (Add).
La ACL DAI se agrega a la configuración del switch.

7. Para eliminar la ACL DAI seleccionada de la configuración del switch, haga clic en el botón Delete.

Configurar una regla de ACL DAI

Puede configurar una regla de ACL de inspección dinámica de ARP (DAI).

Para configurar una regla de ACL DAI:

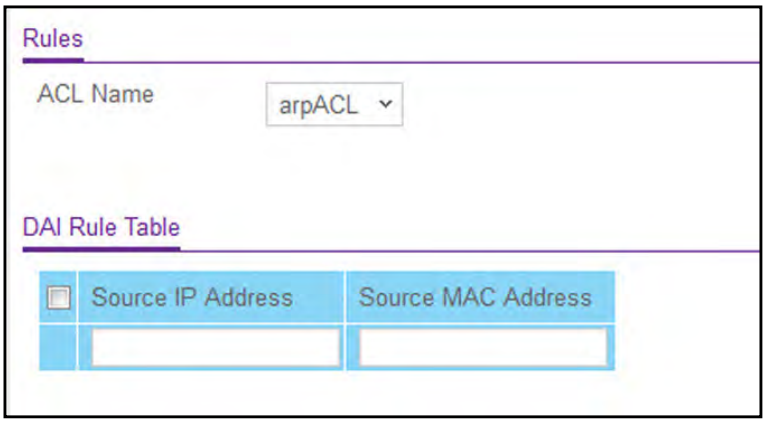
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration.



5. En el menú ACL Name, seleccione la ACL ARP de DAI para la que desea configurar la regla.

6. En el campo Source IP Address, introduzca la dirección IP de origen que se usará como coincidencia de la regla.

7. En el campo Source MAC Address, introduzca la dirección MAC de origen que se usará como coincidencia de la regla.

8. Haga clic en el botón Add.
La regla se agrega a la ACL seleccionada.

Ver las estadísticas de DAI

Para ver las estadísticas de DAI:

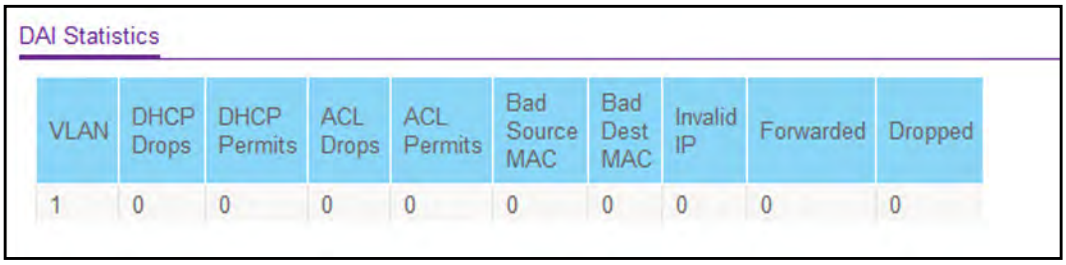
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Dynamic ARP Inspection > DAI Statistics.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar las estadísticas de DAI, haga clic en el botón Clear.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 212. Estadísticas de DAI

Campo	Descripción
VLAN	El ID de VLAN habilitada cuyas estadísticas se mostrarán.
DHCP Drops	Número de paquetes ARP que DAI descartó porque no se encontró ninguna entrada de enlace de DHCP snooping coincidente.
DHCP Permits	Número de paquetes ARP que DAI reenvió porque se encontró una entrada de enlace de DHCP snooping coincidente.
ACL Drops	Número de paquetes ARP que DAI descartó porque no se encontró ninguna regla de ACL ARP coincidente para esta VLAN y el indicador estático está activado en esta VLAN.
ACL Permits	Número de paquetes ARP que DAI permitió porque se encontró una regla de ACL ARP coincidente para esta VLAN.
Bad Source MAC	Número de paquetes ARP que DAI descartó porque la dirección MAC del remitente en los paquetes ARP no coincidía con la MAC de origen del encabezado Ethernet.
Bad Dest MAC	Número de paquetes ARP que DAI descartó porque la dirección MAC de destino en los paquetes de respuesta ARP no coincidía con la MAC de destino del encabezado Ethernet.
Invalid IP	Número de paquetes ARP que DAI descartó porque la dirección IP del remitente en los paquetes ARP o la dirección IP de destino en los paquetes de respuesta 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 de 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.

Configurar 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 tanto a invitados como a usuarios 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 dispositivo o en un servidor RADIUS.

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 configurados en el switch.

Para configurar los ajustes globales del portal cautivo:

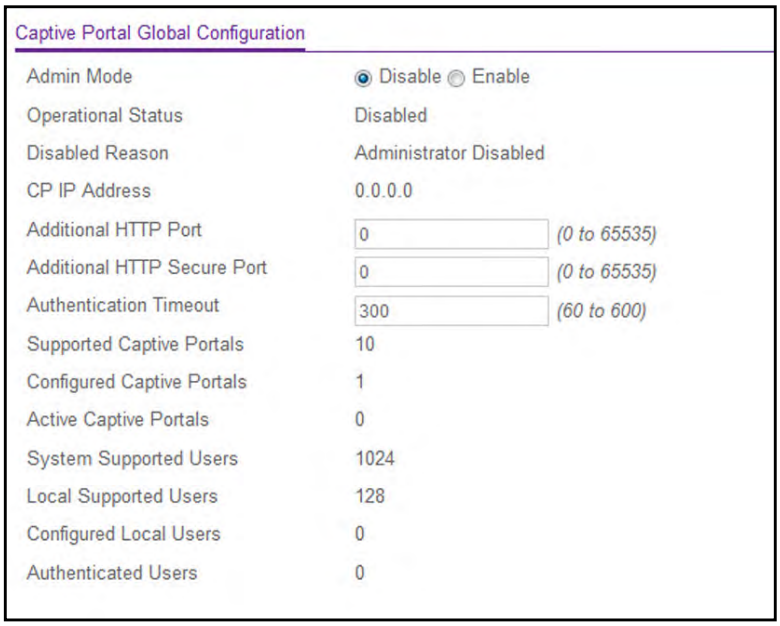
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Security > Control > Captive Portal > CP Global Configuration.**



5. Seleccione el botón de opción Admin Mode Disable o Enable.

Esto establece el modo administrativo de la función de portal cautivo. De forma predeterminada, CP está deshabilitado.

6. En el campo Additional HTTP Port, introduzca un número de puerto entre 0–65535 (excepto el puerto 80).

   El tráfico HTTP usa el puerto estándar 80, pero puede usar el campo Additional HTTP Port para configurar un puerto adicional para el tráfico HTTP. Introduzca 0 para quitar el puerto HTTP adicional. El valor predeterminado es 0.

7. En el campo Additional HTTP Secure Port, introduzca un número de puerto entre 0–65535 (excepto el puerto 443).

   El tráfico HTTP seguro usa el puerto estándar 443, pero puede configurar un puerto adicional para el tráfico HTTP seguro con el campo Additional HTTP Secure Port. Introduzca 0 para quitar el puerto HTTP seguro adicional. El valor predeterminado es 0.

8. Use el campo Authentication Timeout para introducir el número de segundos que el portal cautivo mantiene abierta la sesión de autenticación con un cliente que intenta acceder a la red a través de un portal.

   Para acceder a la red a través de un portal, el cliente primero debe introducir la información de autenticación en una página web de autenticación. Al vencer el tiempo de espera, el switch desconecta cualquier conexión TCP o SSL activa con el cliente. El rango válido es de 60 a 600 segundos. El tiempo de espera de autenticación predeterminado es de 300 segundos.

9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra.

Tabla 213. Configuración global del portal cautivo

Campo	Descripción
Operational Status	El estado operativo de la función de portal cautivo, que puede ser Enabled o Disabled. El valor predeterminado es Disabled.
Disabled Reason	Si CP está deshabilitado, este campo muestra el motivo, que puede ser uno de los siguientes: • Deshabilitado administrativamente • Dirección IP no configurada • Sin interfaz de enrutamiento IP • Enrutamiento deshabilitado
CP IP Address	La dirección IP que usa el portal cautivo.
Supported Captive Portals	El número de portales cautivos admitidos en el sistema.
Configured Captive Portals	Muestra el número de portales cautivos configurados en el switch.
Active Captive Portals	Muestra el número de instancias de portal cautivo habilitadas operativamente.
System Supported Users	Muestra el número de usuarios autenticados que admite el sistema.
Local Supported Users	Muestra el número de entradas que admite la base de datos de usuarios locales.

Tabla 213. Configuración global del portal cautivo (continuación)

Campo	Descripción
Configured Local Users	El número de usuarios locales configurados.
Authenticated Users	Muestra el número de usuarios autenticados actualmente en todas las instancias de portal cautivo de este switch.

Agregar una instancia de portal cautivo

De forma predeterminada, el switch tiene un portal cautivo. Puede cambiar su configuración y también puede crear y configurar hasta nueve portales adicionales.

Para agregar una instancia de portal cautivo:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP Configuration.



5. En el campo CP Name, introduzca el nombre de la configuración. El nombre puede tener de 1 a 31 caracteres alfanuméricos.
6. En la lista Admin Mode, seleccione Enable o Disable.

   Esto establece el modo administrativo de la función de portal cautivo. De forma predeterminada, el portal cautivo está deshabilitado.

7. En el campo Protocol, seleccione HTTP o HTTPS como protocolo que usan las instancias de portal cautivo para comunicarse con los clientes durante la verificación:
   - HTTP no usa cifrado durante la verificación.
   - HTTPS usa Secure Sockets Layer (SSL), que requiere un certificado para proporcionar cifrado. El certificado se presenta al usuario al conectarse.
8. Seleccione el tipo de verificación de usuario (Verification) que realiza la instancia de portal cautivo con los clientes que intentan conectarse:
   - Guest. No es necesario que una base de datos autentique al usuario.
   - Local. El dispositivo usa una base de datos local para autenticar a los usuarios.
   - RADIUS. El dispositivo usa una base de datos en un servidor RADIUS remoto para autenticar a los usuarios.
9. Seleccione el estado de bloqueo (Block).

   Si el CP está bloqueado, los usuarios no pueden acceder a la red a través del CP. Use esta función para proteger temporalmente la red ante eventos inesperados, como ataques de denegación de servicio.

10. Si el modo de verificación es Local o RADIUS, use el campo Group para asignar un grupo de usuarios existente al portal cautivo.

    Todos los usuarios del grupo pueden acceder a la red a través de este portal. La lista User Group es la misma para todas las configuraciones de CP del switch.

11. En el campo Idle Timeout, introduzca el número de segundos de espera antes de terminar una sesión. La sesión del usuario se cierra al alcanzar el tiempo de espera por inactividad. Si establece el valor en 0, no se aplica el tiempo de espera. El rango válido es de 0 a 900 segundos. El valor predeterminado es 0.

12. En la lista User Logout, seleccione Enable o Disable para permitir que un cliente autenticado se desautentique de la red.

    Si esta opción está desactivada o el usuario no solicita expresamente cerrar sesión, el estado de conexión del cliente permanece autenticado hasta que el portal cautivo desautentica al usuario, por ejemplo, al alcanzar el tiempo de espera por inactividad o de sesión.

13. Si el modo de verificación es RADIUS, use el campo Radius Auth Server para introducir la dirección IP del servidor RADIUS que se usará para autenticar a los clientes.

    El dispositivo actúa como cliente RADIUS y realiza todas las transacciones RADIUS en nombre de los clientes.

14. Seleccione Redirect Mode para especificar si el CP redirige al cliente recién autenticado a la URL configurada (habilitado).

Si este modo está deshabilitado, se usa la página de bienvenida predeterminada según la configuración regional.
15. Especifique la Redirect URL a la que se redirige al cliente recién autenticado. La longitud máxima de la URL es de 512 caracteres alfanuméricos.
16. En el campo Background Color, especifique el valor del color de fondo. Por ejemplo, #BFBFBF.

17. En el campo Foreground Color, especifique el valor del color de primer plano. Por ejemplo, #999999.
18. En el campo Separator Color, especifique el valor del color del separador. Por ejemplo, #46008F.

19. En el campo Max Bandwidth Down, especifique la velocidad máxima a la que un cliente puede recibir datos de la red.

    La velocidad se expresa en bytes por segundo. 0 indica que no se aplica el límite. El rango es de 0 a 536870911.

20. En el campo Max Bandwidth Up, especifique la velocidad máxima en bytes por segundo a la que un cliente puede enviar datos a la red.

    Un valor de 0 indica que no se aplica el límite. El rango es de 0 a 536870911.

21. En el campo Max Input, especifique el número máximo de octetos que el usuario puede transmitir.

    Al alcanzar este límite, el usuario se desconecta. 0 indica que el límite no se aplica. El rango es de 0 a 4294967295.

22. En el campo Max Output, especifique el número máximo de octetos que el usuario puede recibir.

    Al alcanzar este límite, el usuario se desconecta. 0 indica que no se aplica el límite. El rango es de 0 a 4294967295.

23. En el campo Max Total, especifique el número máximo de octetos que el usuario puede transferir, es decir, la suma de los octetos transmitidos y recibidos.

    Al alcanzar este límite, el usuario se desconecta. 0 indica que no se aplica el límite. El rango es de 0 a 4294967295.

24. Haga clic en el botón Add.
Se agrega la instancia de portal cautivo.

Configurar los enlaces de portales cautivos

Puede asociar un portal cautivo configurado con una red específica (SSID). La función CP solo se ejecuta en las interfaces que especifique. Se pueden asociar varias interfaces a un CP, pero una interfaz solo puede asociarse a un CP a la vez.

Para configurar los enlaces de portales cautivos:

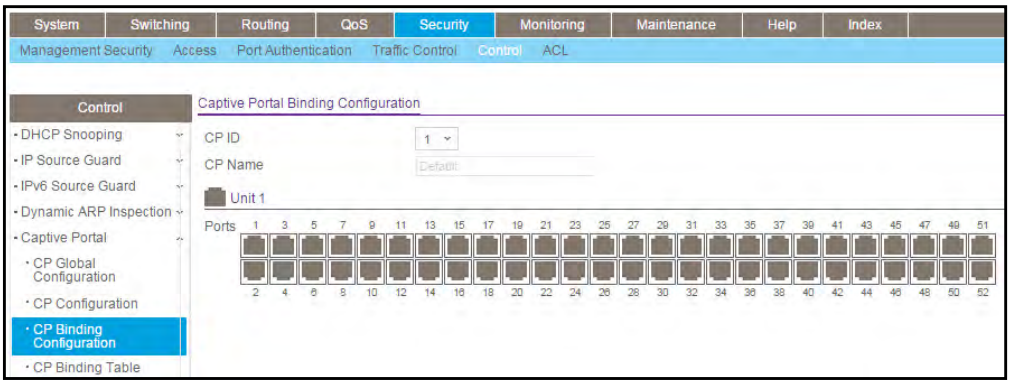
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP Binding Configuration.



5. Seleccione el CP ID de la lista.

El ID es un valor único que identifica la instancia de portal cautivo. Este valor se asigna automáticamente a la instancia al crearla y no se puede cambiar.

6. En el campo CP Name, especifique el nombre de la configuración. El nombre puede tener de 1 a 31 caracteres alfanuméricos.
7. Haga clic en una o más interfaces.
Las interfaces quedan seleccionadas.
8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.

Ver la tabla de enlaces de portales cautivos

Para ver la tabla de enlaces de portales cautivos:

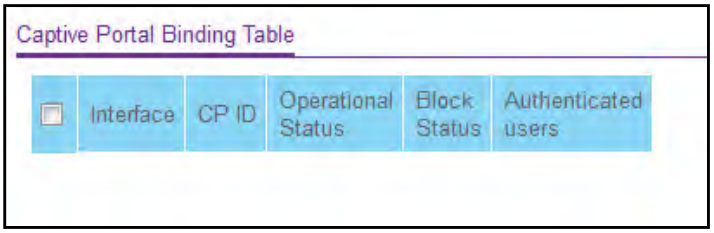
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP Binding Table.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh. La siguiente tabla describe la información no configurable que se muestra.

Tabla 214. Tabla de enlaces de portales cautivos

Campo	Descripción
Interface	La interfaz.
CP ID	El ID de la instancia de portal cautivo.
Operational Status	Indica si el portal está activo en la interfaz especificada.
Block Status	Indica si el portal cautivo está bloqueado temporalmente para la autenticación.
Authenticated Users	Muestra el número de usuarios autenticados que usan la instancia de portal cautivo en esta interfaz.

Configurar un grupo de portal cautivo

Para configurar un grupo de portal cautivo:

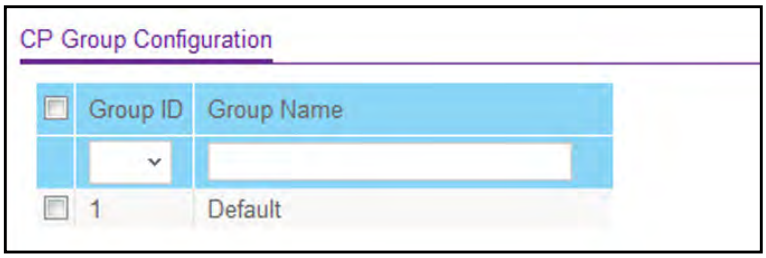
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP Group Configuration.



5. Seleccione el Group ID de la lista.
6. En el campo Group Name, especifique el nombre del grupo de usuarios. El nombre puede tener de 1 a 31 caracteres alfanuméricos.
7. Haga clic en el botón Add.
Se agrega el grupo.

Configurar los ajustes de usuario del portal cautivo

Para configurar los ajustes de usuario del portal cautivo:

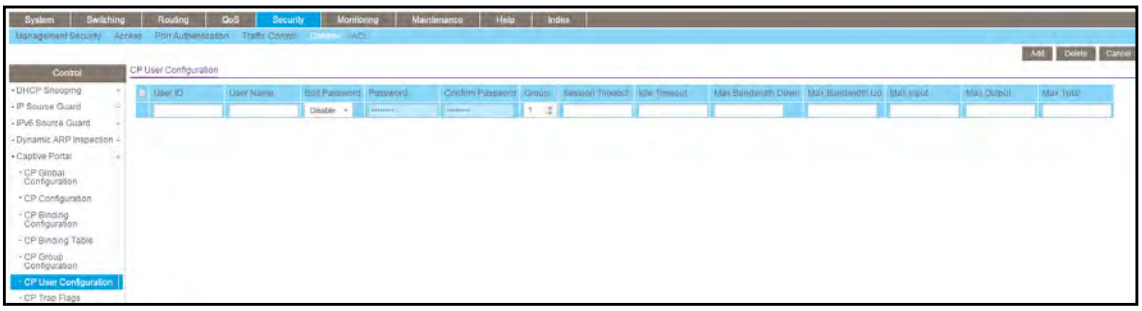
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP User Configuration.



5. Introduzca el User ID local para identificar el nombre del usuario.
6. En el campo User Name, introduzca el nombre del usuario.

   El nombre puede tener de 1 a 31 caracteres alfanuméricos. Una vez creados, los nombres de usuario no se pueden cambiar ni modificar.

7. En la lista Edit Password, seleccione Enable solo cuando vaya a cambiar la contraseña. El valor predeterminado es Disable.
8. En el campo Password, introduzca una contraseña para el usuario.
La contraseña puede tener de 8 a 64 caracteres.
9. En el campo Confirm Password, vuelva a introducir la contraseña del usuario.
10. Use el campo Group para asignar el usuario al menos a un grupo de usuarios.

Para asignar un usuario a más de un grupo, presione la tecla Ctrl y haga clic en cada grupo. Los usuarios nuevos se asignan al grupo de usuarios 1-Default de forma predeterminada.

11. En el campo Session Timeout, introduzca el número de segundos que un usuario puede permanecer conectado a la red.

Al alcanzar el valor de Session Timeout, la sesión del usuario se cierra automáticamente.
12. En el campo Idle Timeout, introduzca el número de segundos de espera antes de terminar una sesión. La sesión del usuario se cierra al alcanzar el tiempo de espera por inactividad. Si el atributo es 0 o no está presente, se usa el valor configurado para el portal cautivo.

13. En el campo Max Bandwidth Down, introduzca la velocidad máxima, en bits por segundo, a la que un cliente puede recibir datos de la red.

Un valor de 0 indica que se usa la configuración global. El rango es de 0 a 536870911 bps.

14. En el campo Max Bandwidth Up, introduzca la velocidad máxima, en bits por segundo, a la que un cliente puede enviar datos a la red.

Un valor de 0 indica que se usa el límite global. El rango es de 0 a 536870911 bps.
15. En el campo Max Input, introduzca el número de octetos que el usuario puede recibir. Al alcanzar este límite, el usuario se desconecta. 0 significa que se usa el límite global. El rango es de 0 a 4294967295.
16. En el campo Max Output, introduzca el número de octetos que el usuario puede transmitir. Al alcanzar este límite, el usuario se desconecta. 0 significa que se usa el límite global. El rango es de 0 a 4294967295.
17. En el campo Max Total, introduzca 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. 0 significa que se usa el límite global. El rango es de 0 a 4294967295.

18. Haga clic en el botón Add.
El usuario se agrega a la base de datos de usuarios locales.

Configurar los indicadores de trap del portal cautivo

Puede especificar si el portal cautivo envía traps SNMP y qué eventos del portal cautivo generan un trap. Todos los traps SNMP de CP están deshabilitados de forma predeterminada.

Para configurar los indicadores de trap del portal cautivo:

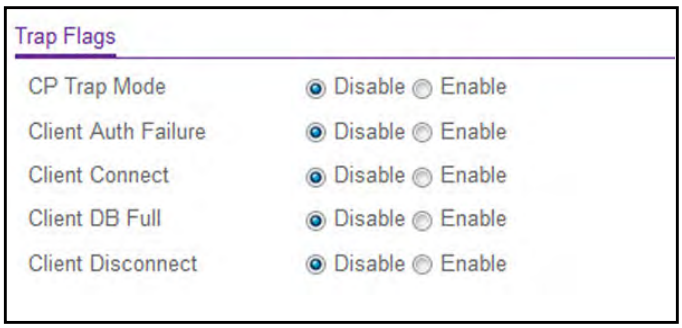
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP Trap Flags.



5. Seleccione el botón de opción CP Trap Mode Disable o Enable. Esto habilita o deshabilita el modo de trap del portal cautivo.
6. Seleccione el botón de opción Client Authentication Failure Disable o Enable.

Si lo habilita, el agente SNMP envía un trap cuando un cliente intenta autenticarse con un portal cautivo pero no lo logra.

7. Seleccione el botón de opción Client Connect Disable o Enable.

Si lo habilita, el agente SNMP envía un trap cuando un cliente se autentica en un portal cautivo y se conecta a él.

8. Seleccione el botón de opción Client Database Full Disable o Enable.

Si lo habilita, el agente SNMP envía un trap cada vez que no se puede agregar una entrada a la base de datos de clientes porque está llena.

9. Seleccione el botón de opción Client Disconnect Disable o Enable.

Si lo habilita, el agente SNMP envía un trap cuando un cliente se desconecta de un portal cautivo.

10. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Ver y borrar los clientes del portal cautivo

Puede ver y borrar la información sobre el tráfico que un cliente envió o recibió.

Para ver y borrar los clientes del portal cautivo:

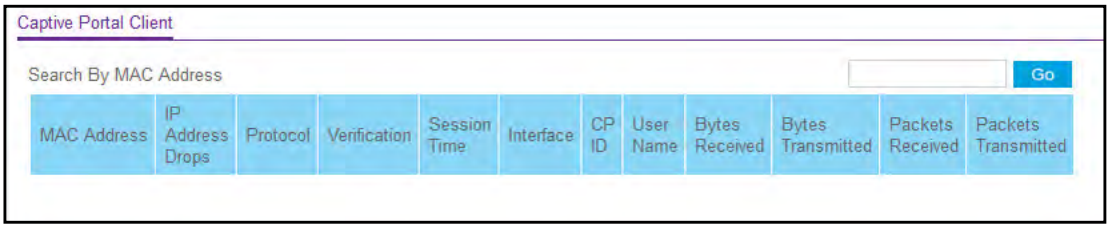
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > Control > Captive Portal > CP Client.



5. Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.
6. Para borrar la información de la tabla de clientes, haga clic en el botón Clear. La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 215. Cliente del portal cautivo

Campo	Descripción
MAC Address	Muestra la dirección MAC del cliente.
IP Address Drops	Identifica la dirección IP del cliente (si corresponde).
Protocol	Muestra el protocolo de conexión actual, HTTP o HTTPS.
Verification	Muestra el tipo de cuenta actual: Guest, Local o RADIUS.
Session Time	Muestra el tiempo transcurrido desde que se autorizó al cliente.
Interface	Identifica la interfaz que usa el cliente.
CP ID	El ID de la instancia de portal cautivo.
User Name	El nombre de usuario (o ID de invitado) del cliente conectado.
Bytes Received	Total de bytes que recibió el cliente.
Bytes Transmitted	Total de bytes que transmitió el cliente.
Packets Received	Total de paquetes que recibió el cliente.
Packets Transmitted	Total de paquetes que transmitió el cliente.

Configurar y administrar 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 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, sobre todo, proporcionar seguridad a la red. El software de los switches ProSafe Managed admite ACL IPv4, IPv6 y MAC.

Primero se crea un ID de ACL basada en IPv4, IPv6 o MAC. Luego se crea una regla y se asigna a un ID de ACL único. A continuación, se definen las reglas, que pueden identificar protocolos, direcciones IP y MAC de origen y destino, y otros criterios de coincidencia de paquetes. Por último, se usa el número de ID para asignar la ACL a un puerto o a un LAG.

Usar el asistente de ACL para crear una ACL simple

El asistente de ACL (ACL Wizard) le ayuda a crear una ACL simple y aplicarla a los puertos seleccionados de forma fácil y rápida. Debe seleccionar un tipo de ACL al crear una ACL. Luego agregue una regla a esta ACL y aplíquela a los puertos seleccionados. El asistente permite crear la ACL, pero no modificarla. Para modificar la ACL, vaya a la página ACL Configuration. Consulte Configurar una ACL IP en la página 615.

Para usar el asistente de ACL para crear una ACL simple:

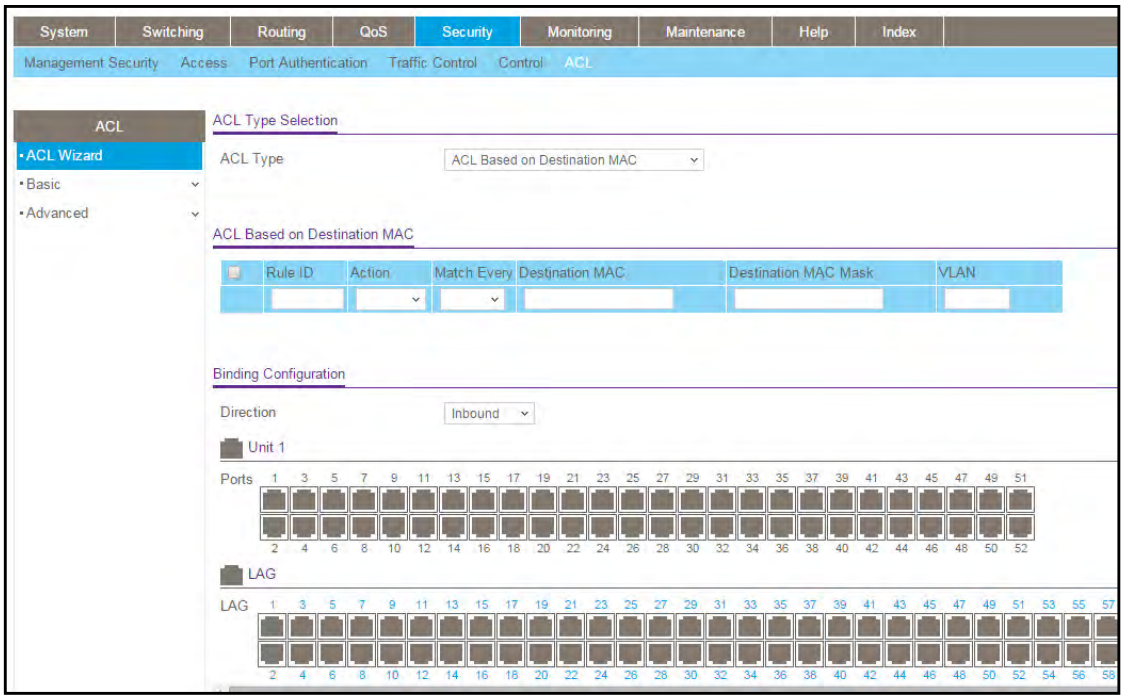
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > ACL Wizard.



Nota: Los pasos de este 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 IPv4 de origen, lo que se muestra en esta página varía según el paso actual del proceso de configuración de la regla.

5. Use ACL Type para especificar el tipo de ACL que usará para crear la ACL. Puede seleccionar uno de 10 tipos opcionales:

- 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 de prefijo IPv6.
- ACL Based on Source IPv6. Crea una ACL basada en el prefijo IPv6 de origen y la longitud de 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.

6. En el menú Direction, seleccione Inbound o Outbound. La regla de tráfico se aplica solo al tráfico de entrada o solo al tráfico de salida.

7. En las figuras del switch Unit 1 y LAG que aparecen en pantalla, seleccione los puertos y LAG a los que se debe aplicar la regla.

Si un puerto o LAG no está seleccionado, haga clic en él para seleccionarlo. Si está seleccionado, haga clic en él para quitar la selección.

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

Configurar una ACL basada en la dirección MAC de destino

Nota: La vinculación de ACL a una interfaz falla si el sistema no tiene recursos para vincular una nueva ACL.

Para configurar una regla basada en la dirección MAC de destino:

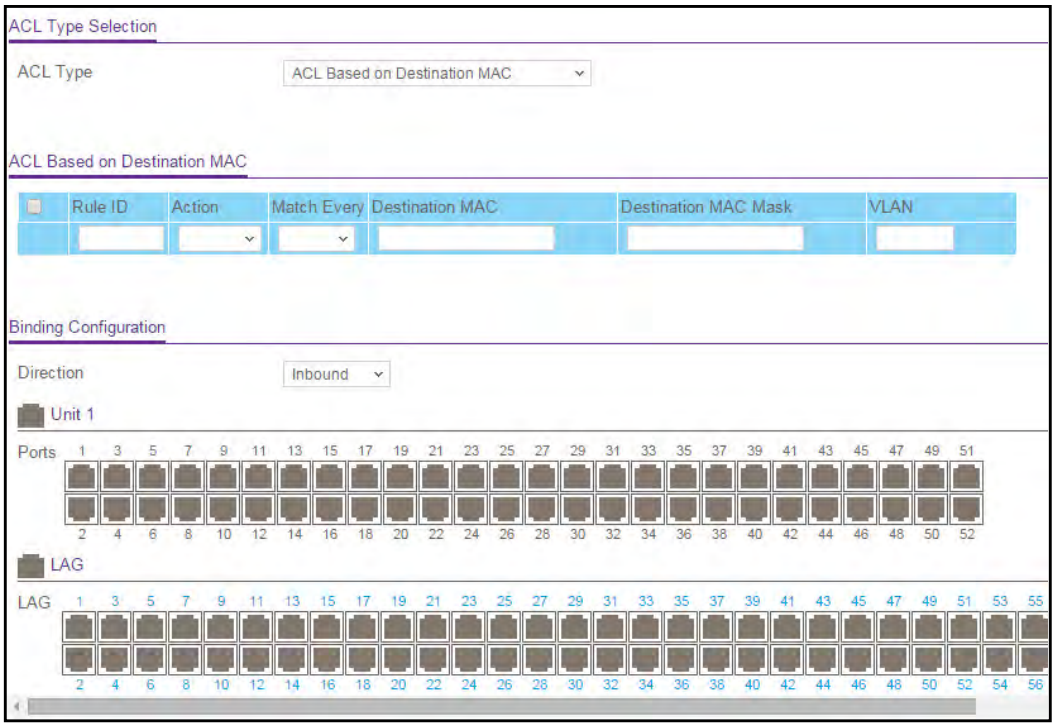
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > ACL > ACL Wizard.



5. Use Rule ID para introducir un número entero de 1 a 1023 que identifica la regla.

6. Use Action para especificar qué acción se toma si un paquete cumple el criterio de la regla. Las opciones son Permit o Deny.

7. En la lista Match Every, seleccione True o False:

- True significa que todos los paquetes deben coincidir con la ACL y la regla seleccionadas y se permiten o deniegan. En este caso, como todos los paquetes coinciden con la regla, no se ofrece la opción de configurar otros criterios de coincidencia.
- Para configurar criterios de coincidencia específicos para la regla, elimínela y vuelva a crearla, o vuelva a configurar Match Every en False para que se muestren los demás criterios.

8. Use Destination MAC para especificar la dirección MAC de destino que se comparará con una trama Ethernet.

   El formato válido es xx:xx:xx:xx:xx:xx. La palabra clave BPDU se puede especificar con una dirección MAC de destino 01:80:C2:xx:xx:xx.

9. Use Destination MAC Mask para especificar la máscara de dirección MAC de destino que indica qué bits de la MAC de destino se comparan con una trama Ethernet.

   El formato válido es xx:xx:xx:xx:xx:xx. La palabra clave BPDU se puede especificar con una máscara MAC de destino 00:00:00:ff:ff:ff.

10. Especifique el VLAN ID que se comparará con una trama Ethernet.
El rango válido es de 1 a 4093. Se puede configurar un rango de VLAN o una VLAN.
11. En el menú Direction, seleccione Inbound o Outbound.

La regla de tráfico se aplica solo al tráfico de entrada o solo al tráfico de salida.

12. En las figuras del switch Unit 1 y LAG que aparecen en pantalla, seleccione los puertos y LAG a los que se debe aplicar la regla.

    Si un puerto o LAG no está seleccionado, haga clic en él para seleccionarlo. Si está seleccionado, haga clic en él para quitar la selección.

13. Haga clic en el botón Add.
La regla se agrega a la ACL basada en la dirección MAC de destino.
14. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Usar el asistente de ACL para completar la ACL de MAC de destino

Para obtener información sobre el asistente de ACL, consulte Usar el asistente de ACL para crear una ACL simple en la página 604.

Para completar la ACL de MAC de destino con el asistente de ACL, haga lo siguiente:
1. Seleccione la ACL de MAC de destino como tipo de ACL.
2. Introduzca la DMAC VLAN como regla de ACL.
3. Para seleccionar la dirección y los puertos a los que se vinculará la ACL, en el campo Directions, seleccione la dirección de filtrado de paquetes de la ACL.

   Las opciones son Inbound o Outbound.

   La tabla Port Selection Table especifica la lista de todas las interfaces válidas disponibles para la asignación de ACL.

   Se muestran todas las interfaces físicas sin enrutamiento y las interfaces que participan en LAG.

Configurar una ACL MAC básica

Una ACL MAC consta de un conjunto de reglas que se comparan secuencialmente con un paquete. Cuando un paquete cumple el criterio de una regla, se aplica la acción especificada (Permit/Deny) y no se comprueban las demás reglas. Las reglas de la ACL MAC se especifican/crean en la página MAC ACL Rule Configuration.

Definir una ACL MAC y aplicarla al switch implica varios pasos:
1. Cree el nombre de la ACL.
2. Cree reglas para la ACL.
3. Asigne la ACL por su nombre a un puerto.

Para obtener información sobre cómo ver la configuración, consulte Ver y eliminar vínculos de ACL MAC en la tabla MAC Binding Table en la página 614.

Para configurar una ACL MAC:

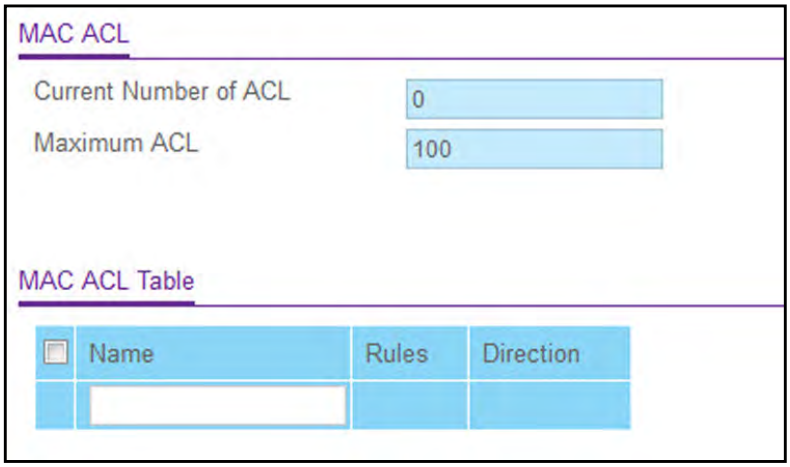
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > Basic > MAC ACL.



   La página MAC ACL muestra el número de ACL configuradas actualmente en el switch y el número máximo de ACL que se pueden configurar. El número actual es igual al número de ACL IPv4 e IPv6 configuradas más el número de ACL MAC configuradas.

5. En el campo Name, especifique un nombre para la ACL MAC.

   La cadena del nombre solo puede incluir caracteres alfabéticos, numéricos, guiones, guiones bajos o espacios. 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 MAC.
   - Direction. La dirección del tráfico de paquetes afectada por la ACL MAC, que puede ser Inbound o en blanco.

6. Haga clic en el botón Agregar (Add).
La ACL MAC se agrega a la configuración del switch.

Configurar reglas de ACL MAC

Puede definir reglas para las ACL basadas en MAC. La definición de la lista de acceso incluye reglas que especifican si el tráfico que cumple el criterio se reenvía normalmente o se descarta. Una regla predeterminada de denegar todo es la última regla de cada lista.

Para configurar reglas de ACL MAC:

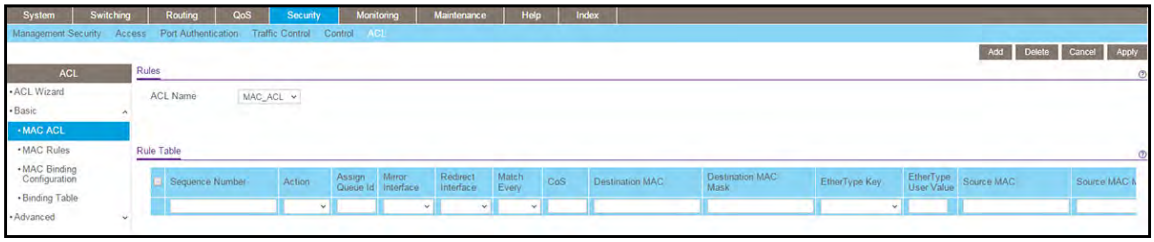
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > Basic > MAC Rules.



5. En el menú ACL Name, seleccione la ACL MAC a la que desea agregar o cambiar una regla.
6. Use Sequence Number para introducir un número entero de 1 a 2147483647. Este número identifica la regla. Una ACL MAC puede contener hasta 1023 reglas.
7. Use Action para especificar qué acción se toma si un paquete cumple el criterio de la regla. Las opciones son Permit o Deny.

8. Use Assign Queue ID para especificar el identificador de la cola de salida de hardware que maneja todos los paquetes que coinciden con esta regla de ACL.

   El rango válido de ID de cola es de 0 a 7.

9. Use Mirror Interface para especificar la interfaz de salida a la que se copia el flujo de tráfico coincidente además de reenviarse normalmente por el dispositivo.

   Este campo no se puede establecer si ya hay una interfaz de redirección configurada para la regla de ACL. Este campo se muestra para la acción Permit.

10. Use Redirect Interface para especificar la interfaz de salida a la que se fuerza el flujo de tráfico coincidente, omitiendo cualquier decisión de reenvío que normalmente tomaría el dispositivo.

Este campo no se puede establecer si ya hay una interfaz espejo configurada para la regla de ACL.
11. Use Match Every para indicar que se compare cada paquete MAC de capa 2. Los valores válidos son:

- True. Indica que se considera que todos los paquetes coinciden con la regla de ACL seleccionada.
- False. Indica que no es obligatorio que todos los paquetes coincidan con la regla de ACL seleccionada.

12. Use CoS para especificar la prioridad de usuario 802.1p que se comparará con una trama Ethernet. El rango válido es de 0 a 7.

13. Use Destination MAC para especificar la dirección MAC de destino que se comparará con una trama Ethernet. El formato válido es xx:xx:xx:xx:xx:xx.

La palabra clave BPDU se puede especificar con una dirección MAC de destino 01:80:C2:xx:xx:xx.

14. Use Destination MAC Mask para especificar la máscara de dirección MAC de destino que indica qué bits de la MAC de destino se comparan con una trama Ethernet.

El formato válido es xx:xx:xx:xx:xx:xx. La palabra clave BPDU se puede especificar con una máscara MAC de destino 00:00:00:ff:ff:ff.

15. Use EtherType Key para especificar el valor EtherType que se comparará con una trama Ethernet. Los valores válidos son:

- Appletalk
- ARP
- IBM SNA
- IPv4
- IPv6
- IPX
- MPLS multicast
- MPLS unicast
- NetBIOS
- Novell
- PPPoE
- Reverse ARP
- User Value

16. Use EtherType User Value para especificar el valor EtherType personalizado definido por el usuario que se usa al seleccionar User Value como EtherType key, para compararlo con una trama Ethernet.

El rango válido es de 0x0600 a 0xFFFF.

17. Use Source MAC para especificar la dirección MAC de origen que se comparará con una trama Ethernet.

El formato válido es xx:xx:xx:xx:xx:xx.

18. Use Source MAC Mask para especificar la máscara de dirección MAC de origen que indica qué bits de la MAC de origen se comparan con una trama Ethernet.

El formato válido es xx:xx:xx:xx:xx:xx.
19. Use VLAN para especificar el VLAN ID que se comparará con una trama Ethernet. El rango válido es de 1 a 4095. Se puede configurar un rango de VLAN o una VLAN.
20. Use Logging para habilitar o deshabilitar el registro.

Si se establece en Enable, el registro se habilita para esta regla de ACL (según la disponibilidad de recursos del dispositivo). Si el indicador de trap de la lista de acceso también está habilitado, se generan traps periódicos que indican cuántas veces se activó esta regla durante el intervalo de informe actual. Se usa un intervalo de informe fijo de 5 minutos para todo el sistema. No se emite un trap si el número de coincidencias de la regla de ACL es cero en el intervalo actual. Este campo solo se admite para la acción Deny.

21. Use Rate Limit Conform Data Rate para especificar el valor de la tasa de datos conforme de la regla de ACL MAC.

Los valores válidos son de 1 a 4294967295 en Kbps.
22. Use Rate Limit Burst Size para especificar el tamaño de ráfaga de la regla de ACL MAC. Los valores válidos son de 1 a 128 en Kbytes.
23. Use Time Range para introducir el nombre del rango de tiempo asociado a la regla de ACL MAC.

Rule Status indica si la regla de ACL está activa o inactiva. Si este campo está vacío, no hay programaciones de temporizador asignadas a la regla.

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

Configurar el vínculo MAC

Cuando una ACL se vincula a una interfaz, todas las reglas definidas se aplican a la interfaz seleccionada. Use la página MAC Binding Configuration para asignar listas de ACL MAC a prioridades de ACL e interfaces.

Para configurar el enlace MAC:

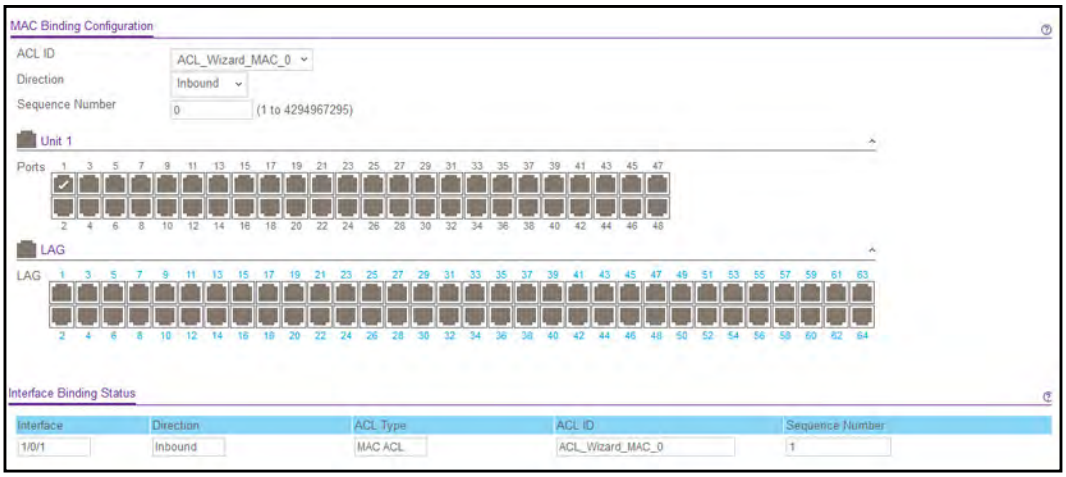
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > ACL > Basic > MAC Binding Configuration.



5. Seleccione una ACL MAC en la lista ACL ID.
Puede seleccionar una y vincularla a las interfaces.

La dirección de filtrado de paquetes (Direction) de la ACL es Inbound, lo que significa que las reglas de ACL MAC se aplican al tráfico que entra en el puerto.

6. Especifique un Sequence Number opcional para indicar el orden de esta lista de acceso respecto de otras listas de acceso ya asignadas a esta interfaz y dirección.

Un número bajo indica mayor precedencia. Si un número de secuencia ya está en uso para esta interfaz y dirección, la lista de acceso especificada reemplaza a la lista de acceso vinculada actualmente con ese número de secuencia. Si no especifica el número de secuencia, se usa un número de secuencia una unidad mayor que el número de secuencia más alto en uso para esta interfaz y dirección. El rango válido es 1–4294967295.

7. La tabla Port Selection Table muestra todas las interfaces válidas disponibles para vincular ACL. Se muestran todas las interfaces físicas sin enrutamiento, la interfaz VLAN y las interfaces que participan en LAG.

- Para agregar la ACL seleccionada a un puerto o LAG, haga clic en la casilla debajo del número de puerto o LAG para que aparezca una X en la casilla.
- Para quitar la ACL seleccionada de un puerto o LAG, haga clic en la casilla debajo del número de puerto o LAG para quitar la selección. Una X en la casilla indica que la ACL está aplicada a la interfaz.

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

La siguiente tabla describe la información que se muestra en la sección Interface Binding Status.

Tabla 216. Interface Binding Status

Campo	Descripción
Interface	La interfaz de la ACL asignada.
Direction	Muestra la dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignada a la interfaz y dirección seleccionadas.
ACL ID	El número de ACL (en el caso de ACL IP) o el nombre de ACL (en el caso de ACL MAC) que identifica la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL especificada respecto de otras ACL asignadas a la interfaz y dirección seleccionadas.

Ver y eliminar vínculos de ACL MAC en la tabla MAC Binding Table

Puede ver y eliminar los vínculos de ACL MAC en la tabla MAC Binding Table.

Para ver y eliminar vínculos de ACL MAC:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > Basic > MAC Binding Table.



5. Para eliminar un vínculo de ACL MAC con una interfaz, marque la casilla junto a la interfaz y haga clic en el botón Delete.

La siguiente tabla describe la información que se muestra en la tabla MAC Binding Table.

Tabla 217. 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 asignada a la interfaz y dirección seleccionadas.
ACL ID	El nombre de ACL que identifica la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL especificada respecto de otras ACL asignadas a la interfaz y dirección seleccionadas.

Configurar una ACL IP

Una ACL IP o IPv6 consta de un conjunto de reglas que se comparan secuencialmente con un paquete. Cuando un paquete cumple el criterio de una regla, se aplica la acción especificada (Permit/Deny) y no se comprueban las demás reglas. Debe especificar las interfaces a las que se aplica una ACL IP, así como si se aplica al tráfico de entrada o de salida. Las reglas de la ACL IP se especifican o crean en la página IPv6 ACL Rule Configuration.

Para configurar una ACL IP:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > Advanced > IP ACL.



La página IP ACL muestra el tamaño actual de la tabla de ACL y el tamaño máximo de la tabla de ACL. El tamaño actual es igual al número de ACL IPv4 e IPv6 configuradas más el número de ACL MAC configuradas. El tamaño máximo es 100.

El campo Current Number of ACL muestra el número actual de todas las ACL configuradas en el switch.

El campo Maximum ACL muestra el número máximo de ACL IP que se pueden configurar en el switch, según el hardware.

5. En el campo IP ACL, especifique el ID de ACL o el nombre de ACL IP, según el tipo de ACL IP.
   El IP ACL ID es un entero en el siguiente rango:
   - 1–99: Crea una ACL IP básica, que permite permitir o denegar el tráfico de una dirección IP de origen.
   - 100–199: Crea una ACL IP extendida, que permite permitir o denegar tipos específicos de tráfico de capa 3 o capa 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: Cree una cadena de nombre de ACL IPv4 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 IP.
   - Type. Identifica la ACL como ACL IP básica (con ID de 1 a 99), ACL IP extendida (con ID de 100 a 199) o ACL IP con nombre.
6. Haga clic en el botón Agregar (Add).

La ACL IP se agrega a la configuración del switch.

Configurar reglas para una ACL IP

Puede mostrar las reglas de las listas de control de acceso (ACL) IP que creó.

Nota: Existe una regla predeterminada implícita de denegar todo como última regla de una lista de ACL.

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.

Para configurar reglas para una ACL IP:

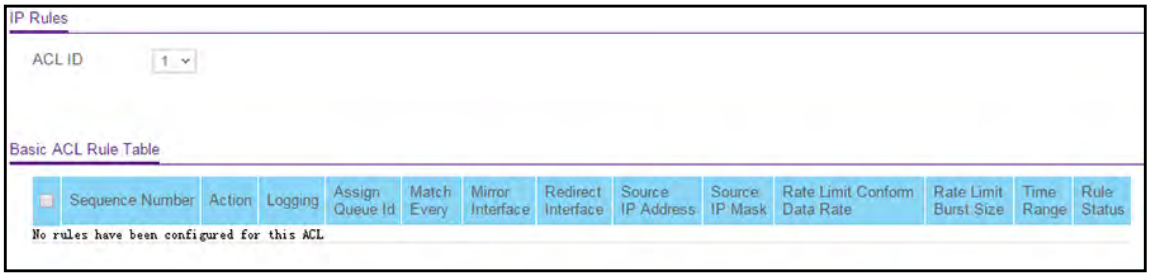
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

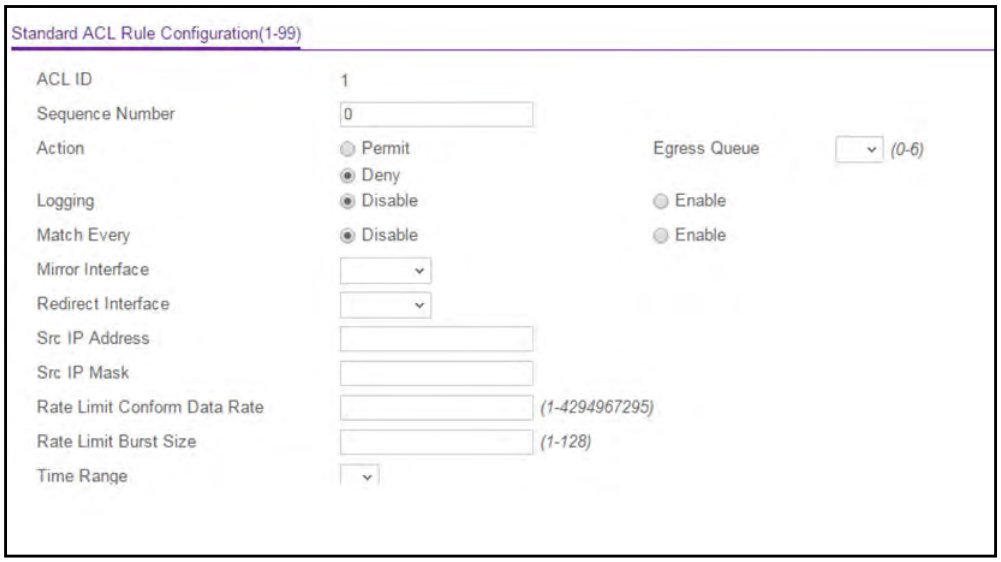
4. Seleccione Security > ACL > Advanced > IP Rules.



Si no existen 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.

5. En el menú ACL ID, seleccione la ACL IP a la que desea agregar o cambiar una regla. Para las ACL IP básicas, debe ser un ID en el rango de 1 a 99.

6. Realice una de las siguientes acciones:
   - Para agregar una regla de ACL IP, haga clic en el botón Add.
   - Para cambiar una regla existente, haga clic en el hipervínculo de la regla en la columna Sequence Number de la tabla Basic ACL Rule Table.



7. Configure las siguientes opciones de la regla:
   - Sequence Number. Introduzca un número entero de 1 a 2147483647. Este número identifica la regla. Una ACL IP puede contener hasta 1023 reglas.
   - Action. Especifique qué acción se toma si un paquete cumple el criterio de la regla. Las opciones son Permit o Deny.
   - Logging. Si se establece en Enable, el registro se habilita para esta regla de ACL (sujeto a los recursos disponibles en el dispositivo). Si también está habilitado el indicador de trap de la lista de acceso, se generan traps periódicos que indican cuántas veces se aplicó esta regla durante el intervalo de informe actual. Se usa un intervalo fijo de 5 minutos para todo el sistema. No se emite un trap si el conteo de la regla de ACL es cero en el intervalo actual. Este campo es visible para la acción Deny.
   - Egress Queue. Identificador de la cola de salida de hardware que maneja todos los paquetes que coinciden con esta regla de ACL IP. El rango válido de ID de cola es de 0 a 6. Este campo es visible cuando se elige Permit como acción.
   - Match Every. Seleccione True o False. True significa que todos los paquetes deben coincidir con la ACL IP y la regla seleccionadas y se permiten o se niegan. En este caso, como todos los paquetes coinciden con la regla, no se ofrece la opción de configurar otros criterios. Para configurar criterios específicos para la regla, elimínela y vuelva a crearla, o cambie Match Every a False para que se muestren los demás criterios.
   - Mirror Interface. Interfaz de salida específica a la que se copia el flujo de tráfico coincidente, además de reenviarse normalmente por el dispositivo. Este campo no se puede establecer si ya hay una interfaz de redirección configurada para la regla de ACL. Este campo es visible para la acción Permit.
   - Redirect Interface. Interfaz de salida específica a la que se fuerza el flujo de tráfico coincidente, omitiendo cualquier decisión de reenvío que el dispositivo tome normalmente. Este campo no se puede establecer si ya hay una interfaz de duplicación configurada para la regla de ACL. Este campo está habilitado para la acción Permit.

- Src IP Address. Ingrese una dirección IP en notación decimal con puntos para compararla 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. Especifica la velocidad de datos conforme de la regla de ACL IP. Los valores válidos son de 1 a 4294967295 Kbps.
- Rate Limit Burst Size. Especifica el tamaño de ráfaga de la regla de ACL IP. Los valores válidos son de 1 a 128 KB.
- Time Range. Nombre del rango de tiempo asociado con la regla de ACL IP.

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

El campo Rule Status de la página IP Rules indica si la regla de ACL está activa o inactiva. En blanco significa que no hay programaciones de temporizador asignadas a la regla.

Configurar reglas para una ACL IP extendida

Puede ver las reglas de las listas de control de acceso IP que creó. Lo que se muestra en esta página varía según el paso del proceso de configuración de reglas.

Nota: Existe una regla predeterminada implícita de denegar todo como última regla de una lista de ACL.

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.

Para configurar reglas para una ACL IP extendida:

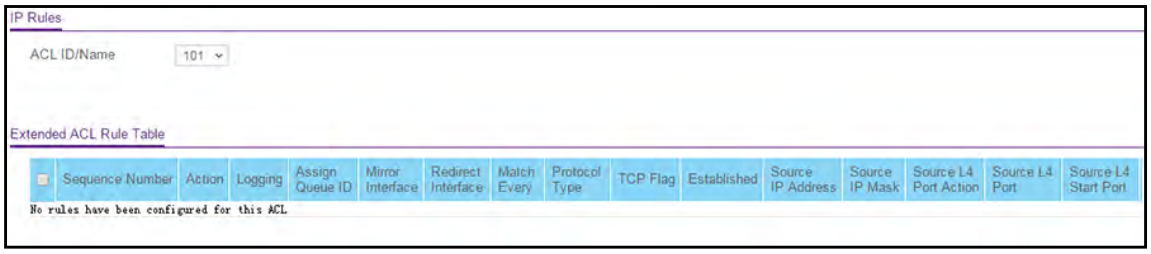
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > ACL > Advanced > IP Extended Rules.

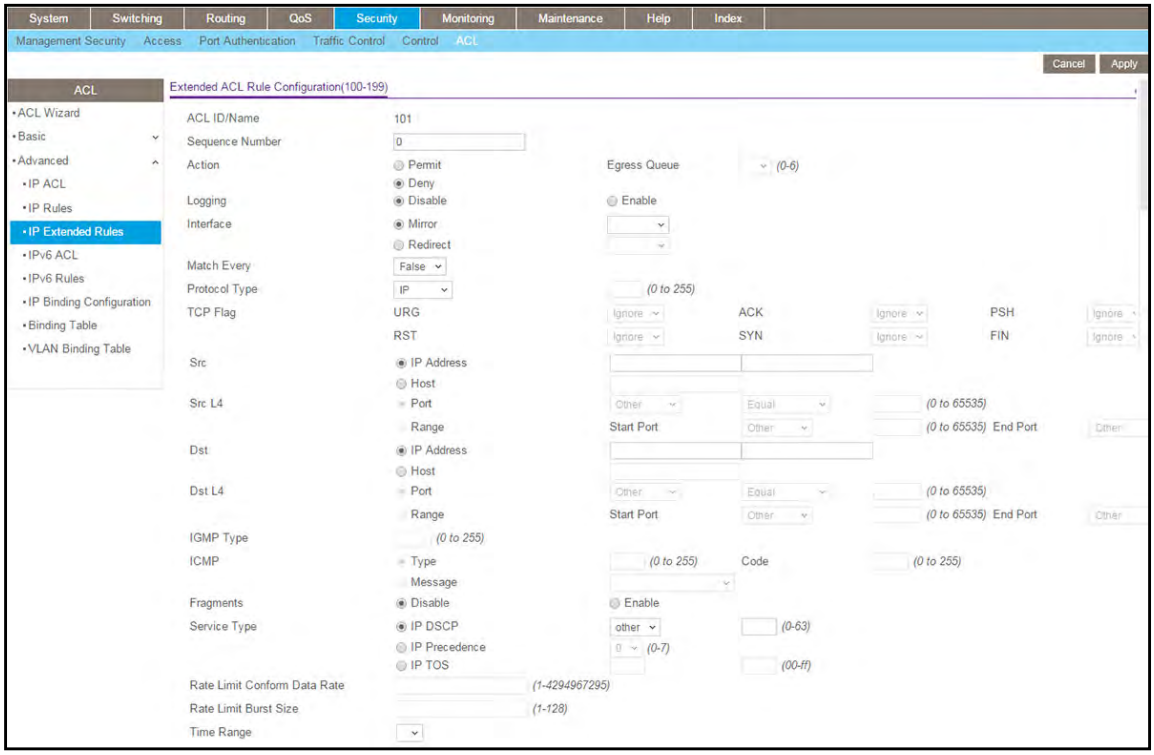


Si no existen reglas, la tabla Extended ACL Rule Table muestra el mensaje No rules have been configured for this ACL. Si existen una o más reglas para la ACL, se muestran en la tabla Extended ACL Rule Table.

5. En el menú ACL ID/Name, seleccione la ACL IP a la que desea agregar o cambiar una regla.

   Para ACL IP extendidas, debe ser un ID en el rango de 101 a 199 o un nombre.

6. Realice una de las siguientes acciones:
   - Para agregar una regla de ACL IP, haga clic en el botón Add.
   - Para cambiar una regla existente, haga clic en el hipervínculo de la regla en la columna Sequence Number de la tabla Extended ACL Rule Table.



7. Configure las siguientes opciones de la regla:
   - Sequence Number. Ingrese un número entero en el rango de 1 a 2147483647. Este número identifica la regla. Una ACL IP extendida puede contener hasta 1023 reglas.

- Action. Especifique qué acción se toma si un paquete cumple el criterio de la regla. Las opciones son Permit o Deny.
- Logging. Si se establece en Enable, el registro se habilita para esta regla de ACL (sujeto a los recursos disponibles en el dispositivo). Si también está habilitado el indicador de trap de la lista de acceso, se generan traps periódicos que indican cuántas veces se aplicó esta regla durante el intervalo de informe actual. Se usa un intervalo fijo de 5 minutos para todo el sistema. No se emite un trap si el conteo de la regla de ACL es cero en el intervalo actual. Este campo es visible para la acción Deny.
- Egress Queue. Identificador de la cola de salida de hardware que maneja todos los paquetes que coinciden con esta regla de ACL IP. El rango válido de ID de cola es de 0 a 6. Este campo es visible cuando se elige Permit como acción.
- Interface. Para la acción Permit, use una interfaz de duplicación o una 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 el dispositivo tome normalmente.
- Match Every. En el menú, seleccione True o False.

  True significa que todos los paquetes deben coincidir con la ACL IP y la regla seleccionadas y se permiten o se niegan. En este caso, como todos los paquetes coinciden con la regla, la opción de configurar otros criterios no está disponible. Para configurar criterios específicos para la regla, elimínela y vuelva a crearla, o seleccione False en el menú Match Every.
- Protocol Type. En el menú, seleccione el protocolo con el que se debe comparar el protocolo IP del paquete: ICMP, IGMP, IP, TCP, UDP, EIGRP, GRE, IPINIP, OSPF o PIM.
- TCP Flag. Para cada indicador TCP, especifique si el indicador TCP del paquete debe coincidir. Los valores 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 de ACL si el indicador TCP del paquete está activado.
  - Clear (-). Un paquete coincide con esta regla de ACL 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, ingrese una dirección IP de origen en notación decimal con puntos para compararla 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, ingrese una dirección IP con su 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 comodín de 255.255.255.255 indica que todos los bits son importantes.

- Src L4. Las opciones solo están disponibles cuando el protocolo es TCP o UDP. Use la opción de puerto L4 de origen para especificar condiciones de coincidencia para números de puerto L4 en la regla de ACL extendida.

  Puede seleccionar el botón de opción Port o el botón de opción Range:

  - Si selecciona el botón de opción Port, puede seleccionar una clave de puerto en el menú o ingresar usted mismo el número de puerto.
    - Los nombres de puertos TCP IP de origen son bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, www, pop2, pop3.
    - Los nombres de puertos UDP IP de origen son domain, echo, ntp, rip, snmp, tftp, time, who.

    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 ingresar un número de puerto. Si selecciona Other en el menú pero deja el campo en blanco, significa cualquiera.

    Las condiciones de coincidencia para números de puerto L4 son las siguientes:

    - Equal. La regla de ACL IP coincide solo si el número de puerto de origen de capa 4 es igual al número 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 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 o clave de puerto especificado.
    - Not Equal. La regla de ACL IP coincide solo si el número de puerto de origen de capa 4 no es igual al número o clave de puerto especificado.
  - 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 puerto 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. Sus valores pueden ir de 0 a 65535.

    Seleccione Other en el menú para ingresar números de puerto. Si selecciona Other en el menú pero deja los campos en blanco, 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 comodín de 255.255.255.255 indica que todos los bits son importantes.

- Dst. En el campo Dst, ingrese una dirección IP de destino en notación decimal con puntos para compararla con la dirección IP de destino del paquete como criterio de la regla de ACL IP seleccionada:
  - Si selecciona el botón de opción IP Address, ingrese una dirección IP con su 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 comodín de 255.255.255.255 indica que todos los bits son importantes.
- Dst L4. Las opciones solo están disponibles cuando el protocolo es TCP o UDP. Use la opción de puerto L4 de destino para especificar condiciones de coincidencia para números de puerto L4 en la regla de ACL extendida.

  Puede seleccionar el botón de opción Port o el botón de opción Range:
  - Si selecciona el botón de opción Port, puede seleccionar una clave de puerto en el menú o ingresar usted mismo el número de puerto.
    - Los nombres de puertos TCP IP de destino son bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, www, pop2, pop3.
    - Los nombres de puertos UDP IP de destino son domain, echo, ntp, rip, snmp, tftp, time, who.

    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 ingresar un número de puerto. Si selecciona Other en el menú pero deja el campo en blanco, significa cualquiera.

    Las condiciones de coincidencia para números de puerto L4 son las siguientes:
    - Equal. La regla de ACL IP coincide solo si el número de puerto de destino de capa 4 es igual al número o clave de puerto especificado.
    - Less Than. La regla de ACL IP coincide si el número de puerto de destino de capa 4 es menor que el número o clave de puerto especificado.
    - Greater Than. La regla de ACL IP coincide si el número de puerto de destino de capa 4 es mayor que el número o clave de puerto especificado.
    - Not Equal. La regla de ACL IP coincide solo si el número de puerto de destino de capa 4 no es igual al número o clave de puerto especificado.
  - 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 puerto 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. Sus valores pueden ir de 0 a 65535.

    Seleccione Other en el menú para ingresar números de puerto. Si selecciona Other en el menú pero deja los campos en blanco, 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 comodín de 255.255.255.255 indica que todos los bits son importantes.

- IGMP Type. Si especifica el tipo IGMP, la regla de ACL IP coincide con el tipo de mensaje IGMP especificado. Los valores posibles están en el rango de 0 a 255. Si este campo se deja vacío, significa cualquiera.
- ICMP. Seleccione el botón de opción ICMP Type o ICMP Message:
  - Si selecciona el botón de opción ICMP Type, tenga en cuenta lo siguiente:
    - Los campos ICMP Type e ICMP Code solo están habilitados si el protocolo es ICMP. Use estos campos para especificar una condición de coincidencia para paquetes ICMP:
    - La regla de ACL IP coincide con el tipo de mensaje ICMP especificado. Los números de tipo posibles están en el rango de 0 a 255.
    - Si especifica información en el campo ICMP Code, la regla de ACL IP coincide con el código de mensaje ICMP especificado. Los valores posibles del código están en el rango de 0 a 255.
    - Si estos campos se dejan vacíos, significa cualquiera.
  - Si selecciona el botón de opción ICMP Message, seleccione el tipo de mensaje ICMP que coincidirá 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 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, time-exceeded, ttl-exceeded y unreachable.
- Fragments. Seleccione Enable para permitir fragmentos iniciales (es decir, con el bit de fragmento activado) o deje el valor predeterminado Disable para impedir el uso de fragmentos iniciales.

  Esta opción no es válida para reglas que coinciden con información L4, como el número de puerto TCP, porque esa información viaja 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 adecuados.
  - 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. Ingrese un entero de 0 a 63. Para seleccionar el IP DSCP, elija una de las palabras clave DSCP del menú. Para especificar un valor numérico, seleccione Other y aparece un campo donde puede ingresar 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. Ingrese 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 comparar con el campo IP ToS del paquete.

  Por ejemplo, para verificar 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 de la regla de ACL IP. Los valores válidos son de 1 a 4294967295 Kbps.
- Rate Limit Burst Size. Especifique el tamaño de ráfaga de la regla de ACL IP. Los valores válidos son de 1 a 128 KB.
- Time Range. Especifique el nombre del rango de tiempo que desea asociar con la regla de ACL IP.

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

El campo Rule Status indica si la regla de ACL está activa o inactiva. En blanco significa que no hay programaciones de temporizador asignadas a la regla.

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 realiza la acción especificada (permitir o negar) y no se evalúan las reglas adicionales.

Debe especificar las interfaces a las que se aplica una ACL IP y seleccionar si la ACL IP se aplica al tráfico de entrada o de salida.

Para configurar una ACL IPv6:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > Advanced > IPv6 ACL.



5. En el campo IPv6 ACL de la tabla IPv6 ACL Table, especifique el nombre de la ACL IPv6.

   Es la cadena del nombre de la ACL IPv6, que incluye hasta 31 caracteres alfanuméricos. El nombre debe comenzar con una letra.

6. Haga clic en el botón Agregar (Add).
La ACL IPv6 se agrega a la configuración del switch.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 218. ACL IPv6

Campo	Descripción
Número actual de ACL	Número actual de ACL IP configuradas en el switch.
Máximo de ACL	Número máximo de ACL IP que se pueden configurar en el switch, según el hardware.
Reglas	Número de reglas asociadas con la ACL IP.
Tipo	El tipo es ACL IPv6.

Configurar reglas IPv6

Use estas páginas para mostrar las reglas de las listas de control de acceso IPv6, que se crean con la página IPv6 Access Control List Configuration. De forma predeterminada, no hay ningún valor específico vigente para ninguna de las reglas de ACL IPv6.

Para configurar reglas de ACL IPv6:

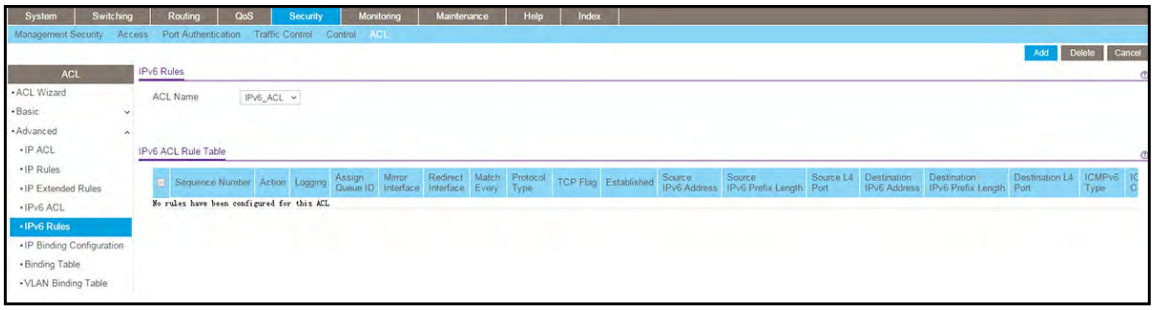
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

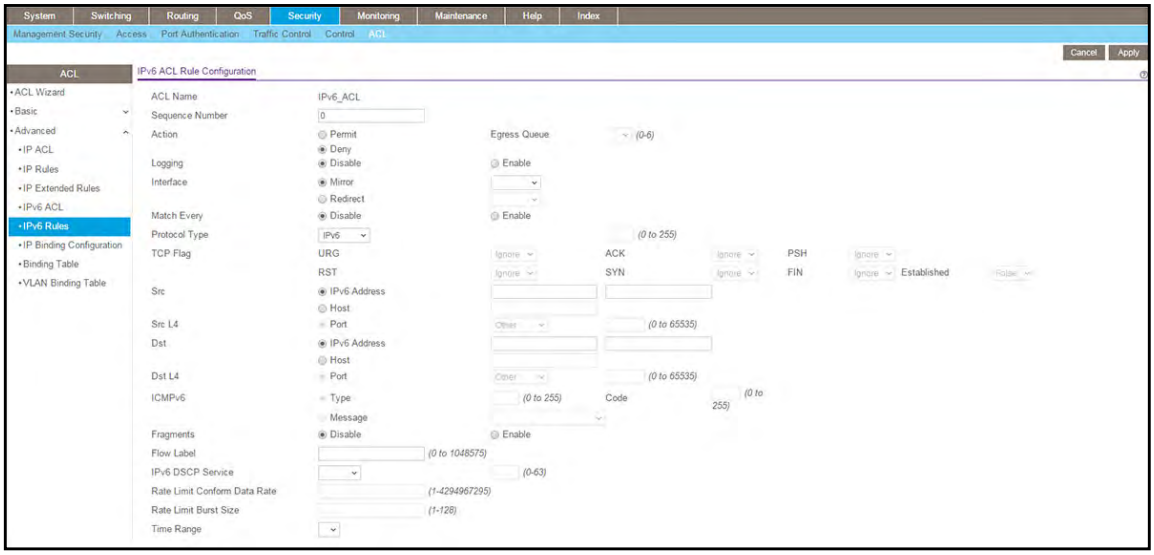
   Se muestra la página System Information.

4. 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.

5. En el menú ACL Name, seleccione la ACL IPv6 a la que desea agregar o cambiar una regla.
6. Realice una de las siguientes acciones:
   - Para agregar una regla de ACL IPv6, haga clic en el botón Add.
   - Para cambiar una regla existente, haga clic en el hipervínculo de la regla en la columna Sequence Number de la tabla IPv6 ACL Rule Table.



7. Configure las siguientes opciones de la regla:
   - Sequence Number. Ingrese un número entero en el rango de 1 a 2147483647. Este número identifica la regla. Una ACL IPv6 puede contener hasta 1023 reglas.

- Action. Especifique qué acción se toma si un paquete cumple el criterio de la regla. Las opciones son Permit o Deny.
- Logging. Si se establece en Enable, el registro se habilita para esta regla de ACL (sujeto a los recursos disponibles en el dispositivo). Si también está habilitado el indicador de trap de la lista de acceso, se generan traps periódicos que indican cuántas veces se aplicó esta regla durante el intervalo de informe actual. Se usa un intervalo fijo de 5 minutos para todo el sistema. No se emite un trap si el conteo de la regla de ACL es cero en el intervalo actual. Este campo es visible para la acción Deny.
- Egress Queue. Identificador de la cola de salida de hardware que maneja todos los paquetes que coinciden con esta regla de ACL IPv6. El rango válido de ID de cola es de 0 a 7. Este campo es visible cuando se elige Permit como acción.
- Interface. Para la acción Permit, use una interfaz de duplicación o una 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 el dispositivo tome normalmente.
- Match Every. En el menú, seleccione True o False.

  True significa que todos los paquetes deben coincidir con la ACL IPv6 y la regla seleccionadas y se permiten o se niegan. En este caso, como todos los paquetes coinciden con la regla, la opción de configurar otros criterios no está disponible. Para configurar criterios específicos para la regla, elimínela y vuelva a crearla, o seleccione False en el menú Match Every.
- Protocol Type. Especifique el tipo de protocolo IPv6 de una de las siguientes formas:
  - En el menú Protocol Type, seleccione IPv6, TCP, UDP o ICMPv6.
  - En el menú Protocol Type, seleccione Other y, en el campo asociado, especifique un entero de 1 a 255. Este número representa el protocolo IPv6.
- TCP Flag. Para cada indicador TCP, especifique si el indicador TCP del paquete debe coincidir. Los valores 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 de ACL si el indicador TCP del paquete está activado.
  - Clear (-). Un paquete coincide con esta regla de ACL 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, ingrese una dirección IPv6 de origen para compararla con la dirección IPv6 de origen del paquete como criterio de la regla de ACL IPv6 seleccionada:
  - Si selecciona el botón de opción IPv6 Address, ingrese una dirección IPv6 para aplicar este criterio. Si este campo se deja vacío, significa cualquiera.

- Si selecciona el botón de opción Host, ingrese una dirección IPv6 de host de origen que coincida con la dirección IPv6 especificada. Si este campo se deja vacío, significa cualquiera.

El argumento de dirección IPv6 de origen debe tener el formato documentado en RFC 2373, donde la dirección se especifica en hexadecimal con valores de 16 bits separados por dos puntos.

- Src L4. Las opciones solo están disponibles cuando el protocolo es TCP o UDP. Use la opción de puerto L4 de origen para especificar condiciones de coincidencia para números de puerto L4 en la regla de ACL extendida.

  Puede seleccionar el botón de opción Port o el botón de opción Range:

  - Si selecciona el botón de opción Port, puede seleccionar una clave de puerto en el menú o ingresar usted mismo el número de puerto.
    - Los nombres de puertos TCP IP de origen son bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, www, pop2, pop3.
    - Los nombres de puertos UDP IP de origen son domain, echo, ntp, rip, snmp, tftp, time, who.

    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 ingresar un número de puerto. Si selecciona Other en el menú pero deja el campo en blanco, significa cualquiera.

    Las condiciones de coincidencia para números de puerto L4 son las siguientes:

    - Equal. La regla de ACL IPv6 coincide solo si el número de puerto de origen de capa 4 es igual al número o clave de puerto especificado.
    - Less Than. La regla de ACL IPv6 coincide si el número de puerto de origen de capa 4 es menor que el número o clave de puerto especificado.
    - Greater Than. La regla de ACL IPv6 coincide si el número de puerto de origen de capa 4 es mayor que el número o clave de puerto especificado.
    - Not Equal. La regla de ACL IPv6 coincide solo si el número de puerto de origen de capa 4 no es igual al número o clave de puerto especificado.
  - Si selecciona el botón de opción Range, la regla de ACL IPv6 coincide solo si el número de puerto de capa 4 de origen está dentro del rango especificado. El puerto inicial, el puerto 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. Sus valores pueden ir de 0 a 65535.

    Seleccione Other en el menú para ingresar números de puerto. Si selecciona Other en el menú pero deja los campos en blanco, significa cualquiera.

- Dst. En el campo Dst, ingrese una dirección IPv6 de destino para compararla con la dirección IPv6 de destino del paquete como criterio de la regla de ACL IPv6 seleccionada:
  - Si selecciona el botón de opción IPv6 Address, ingrese una dirección IPv6 para aplicar este criterio. Si este campo se deja vacío, significa cualquiera.
  - Si selecciona el botón de opción Host, ingrese una dirección IPv6 de host de origen que coincida con la dirección IPv6 especificada. Si este campo se deja vacío, significa cualquiera.

El argumento de dirección IPv6 de origen debe tener el formato documentado en RFC 2373, donde la dirección se especifica en hexadecimal con valores de 16 bits separados por dos puntos.

- Dst L4. Las opciones solo están disponibles cuando el protocolo es TCP o UDP. Use la opción de puerto L4 de destino para especificar condiciones de coincidencia para números de puerto L4 en la regla de ACL extendida.

  Puede seleccionar el botón de opción Port o el botón de opción Range:

  - Si selecciona el botón de opción Port, puede seleccionar una clave de puerto en el menú o ingresar usted mismo el número de puerto.
    - Los nombres de puertos TCP IP de destino son bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, www, pop2, pop3.
    - Los nombres de puertos UDP IP de destino son domain, echo, ntp, rip, snmp, tftp, time, who.

    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 ingresar un número de puerto. Si selecciona Other en el menú pero deja el campo en blanco, significa cualquiera.

    Las condiciones de coincidencia para números de puerto L4 son las siguientes:

    - Equal. La regla de ACL IPv6 coincide solo si el número de puerto de destino de capa 4 es igual al número o clave de puerto especificado.
    - Less Than. La regla de ACL IPv6 coincide si el número de puerto de destino de capa 4 es menor que el número o clave de puerto especificado.
    - Greater Than. La regla de ACL IPv6 coincide si el número de puerto de destino de capa 4 es mayor que el número o clave de puerto especificado.
    - Not Equal. La regla de ACL IPv6 coincide solo si el número de puerto de destino de capa 4 no es igual al número o clave de puerto especificado.
  - Si selecciona el botón de opción Range, la regla de ACL IPv6 coincide solo si el número de puerto de capa 4 de destino está dentro del rango especificado. El puerto inicial, el puerto 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. Sus valores pueden ir de 0 a 65535.

    Seleccione Other en el menú para ingresar números de puerto. Si selecciona Other en el menú pero deja los campos en blanco, significa cualquiera.

- IGMPv6 Type. Si especifica el tipo IGMPv6, la regla de ACL IPv6 coincide con el tipo de mensaje IGMPv6 especificado. Los valores posibles están en el rango de 0 a 255. Si este campo se deja vacío, significa cualquiera.
- ICMPv6. Seleccione el botón de opción ICMP Type o ICMP Message:
  - Si selecciona el botón de opción ICMP Type, tenga en cuenta lo siguiente:
    - Los campos ICMP Type e ICMP Code solo están habilitados si el protocolo es ICMPv6. Use estos campos para especificar una condición de coincidencia para paquetes ICMPv6:

- La regla de ACL IPv6 coincide con el tipo de mensaje ICMPv6 especificado. Los números de tipo posibles están en el rango de 0 a 255.
- Si especifica información en el campo ICMP Code, la regla de ACL IPv6 coincide con el código de mensaje ICMPv6 especificado. Los valores posibles del código están en el rango de 0 a 255.
- Si estos campos se dejan vacíos, significa cualquiera.

- Si selecciona el botón de opción ICMP Message, seleccione el tipo de mensaje ICMPv6 que coincidirá 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 ICMPv6 son: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded y unreachable.

- Fragments. Seleccione Enable para permitir fragmentos iniciales (es decir, con el bit de fragmento activado) o deje el valor predeterminado Disable para impedir el uso de fragmentos iniciales.

  Esta opción no es válida para reglas que coinciden con información L4, como el número de puerto TCP, porque esa información viaja en el paquete inicial.

- Flow Label. El campo Flow Label solo se habilita si se selecciona ICMPv6 en el menú Protocol Type. 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 calidad de servicio en los routers. La etiqueta de flujo puede especificarse en el rango de 0 a 1048575.
- IPv6 DSCP Service. Especifique el campo IP DiffServ Code Point (DSCP). Es una configuración opcional.

  El DSCP se define como los seis bits de orden superior del octeto de tipo de servicio en el encabezado IPv6. Ingrese un entero de 0 a 63. Para seleccionar el IPv6 DSCP, seleccione 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 tasa de datos conforme de la regla de ACL IPv6. Los valores válidos son de 1 a 4294967295 en Kbps.
- Rate Limit Burst Size. Especifique el tamaño de ráfaga de la regla de ACL IPv6. Los valores válidos son de 1 a 128 en Kbytes.
- Time Range. Especifique el nombre del rango de tiempo que desea asociar con la regla de ACL IPv6.

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

El campo Rule Status indica si la regla de ACL está activa o inactiva. En blanco significa que no hay programaciones de temporizador asignadas a la regla.

Configurar las vinculaciones de interfaz de ACL IP

Cuando una ACL se vincula a una interfaz, todas las reglas definidas se aplican a la interfaz seleccionada. Puede asignar listas de ACL a prioridades de ACL y a interfaces.

Para configurar las vinculaciones de interfaz de ACL IP:

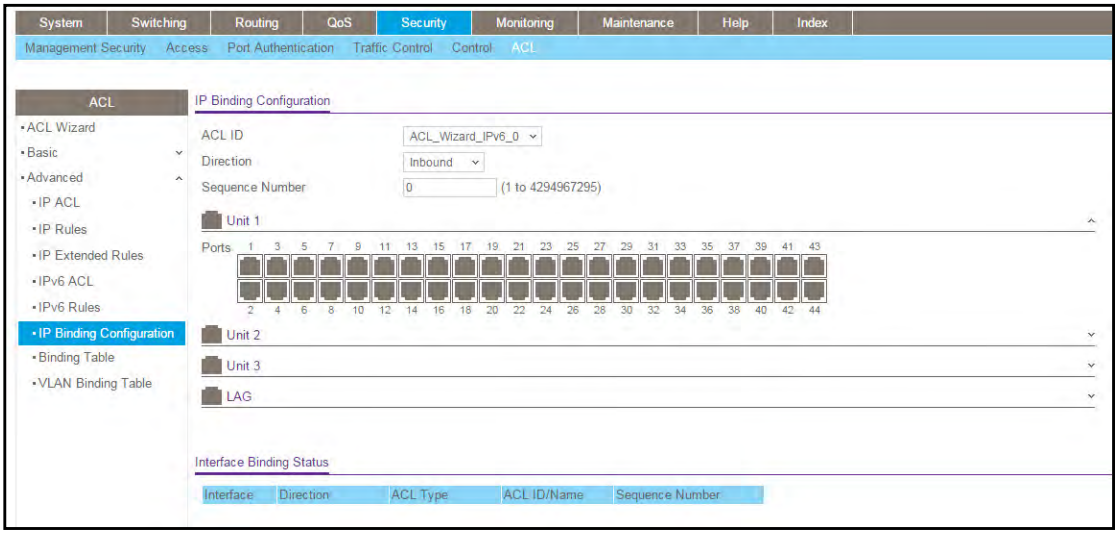
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL > Advanced > IP Binding Configuration.



5. En el menú ACL ID, seleccione una ACL IP.

Nota: La vinculación de ACL a una interfaz falla cuando el sistema no tiene recursos para vincular una nueva ACL. Las ACL IPv4 y las ACL IPv6 no pueden vincularse al mismo tiempo a una interfaz.

---

6. Seleccione la dirección de filtrado de paquetes (Direction) de la ACL.

   Las direcciones válidas son Inbound u Outbound. La dirección de filtrado de paquetes de la ACL es Inbound, lo que significa que las reglas de ACL IP se aplican al tráfico que entra al puerto.

7. Especifique un Sequence Number opcional para indicar el orden de esta lista de acceso respecto a otras listas de acceso ya asignadas a esta interfaz y dirección.

   Un número bajo indica mayor precedencia. Si un número de secuencia ya está en uso para esta interfaz y dirección, la lista de acceso especificada reemplaza a la lista de acceso vinculada actualmente con ese número de secuencia. Si no especifica el número de secuencia (es decir, el valor es 0), se usa un número de secuencia una unidad mayor que el número de secuencia más alto en uso para esta interfaz y dirección. El rango válido es 1–4294967295.

8. En las figuras del switch Unit 1, Unit 2, Unit 3 y LAG en pantalla, seleccione los puertos y LAG a los que debe aplicarse la regla.

   Si un puerto o LAG no está seleccionado, haga clic en él para seleccionarlo. Si está seleccionado, haga clic en él para quitar la selección.

9. Haga clic en el botón Apply.
La configuración se guarda.
La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 219. Configuración de vinculaciones IP

Campo	Descripción
Interface	Muestra la interfaz seleccionada.
Direction	Muestra la dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignada a la interfaz y dirección seleccionadas.
ACL ID/Name	El número de ACL (en el caso de ACL IP) o el nombre de ACL (en el caso de ACL IP con nombre y ACL IPv6) que identifica la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL especificada respecto a otras ACL asignadas a la interfaz y dirección seleccionadas.

Ver y eliminar vinculaciones de ACL IP en la tabla de vinculaciones de ACL IP

Para ver y eliminar vinculaciones de ACL IP:

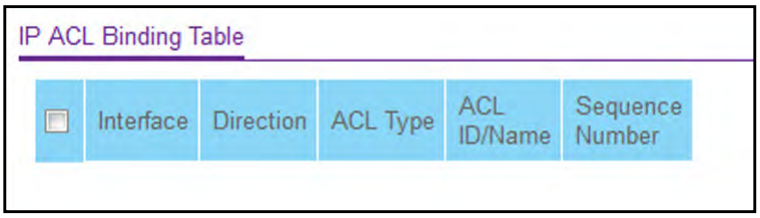
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Security > ACL > Advanced > Binding Table.



5. Para eliminar una vinculación de ACL IP a interfaz, marque la casilla junto a la interfaz y haga clic en el botón Delete.

La siguiente tabla describe la información que se muestra en la tabla IP ACL Binding Table.

Tabla 220. Tabla de vinculaciones de ACL IP

Campo	Descripción
Interface	Muestra la interfaz seleccionada.
Direction	Muestra la dirección de filtrado de paquetes seleccionada para la ACL.
ACL Type	El tipo de ACL asignada a la interfaz y dirección seleccionadas.
ACL ID/Name	El número de ACL (en el caso de ACL IP) o el nombre de ACL (en el caso de ACL IP con nombre y ACL IPv6) que identifica la ACL asignada a la interfaz y dirección seleccionadas.
Sequence Number	El número de secuencia que indica el orden de la ACL especificada respecto de otras ACL asignadas a la interfaz y dirección seleccionadas.

Configurar las vinculaciones de ACL de VLAN

Para configurar las vinculaciones de ACL de VLAN:

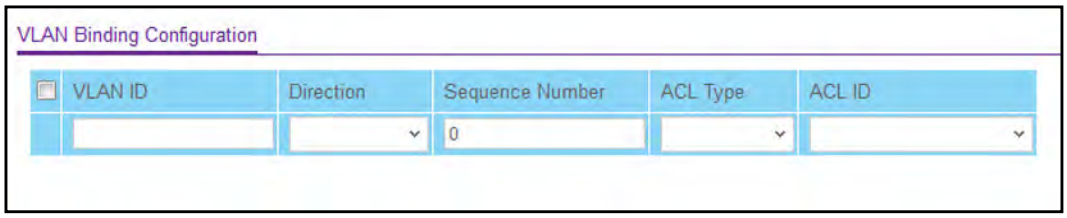
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Security > ACL> Advanced > VLAN Binding Table.



5. En el campo VLAN ID, ingrese el ID de VLAN al que debe aplicarse la vinculación.
6. En el menú Direction, seleccione la dirección de filtrado de paquetes.
7. En el campo Sequence Number, ingrese un número de secuencia opcional.

   Puede especificar un número de secuencia opcional para indicar el orden de esta lista de acceso respecto a otras listas de acceso ya asignadas al ID de VLAN y a la dirección seleccionada. Un número menor indica mayor precedencia. Si un número de secuencia ya está en uso para el ID de VLAN y la dirección seleccionada, la lista de acceso especificada reemplaza a la ACL vinculada actualmente con ese número de secuencia. Si no especifica un número de secuencia (el valor es 0), se usa un número de secuencia una unidad mayor que el número de secuencia más alto en uso para el ID de VLAN y la dirección seleccionada. El rango válido es de 1 a 4294967295.

8. En el menú ACL Type, seleccione el tipo de ACL. Los tipos de ACL válidos incluyen IP ACL, MAC ACL e IPv6 ACL.

9. En el menú ACL ID, seleccione para mostrar todas las ACL configuradas, según el tipo de ACL seleccionado.
10. Haga clic en el botón Add.

Se agrega la vinculación de ACL de VLAN a la tabla ACL VLAN Binding Table.

10

10Supervisar el switch y la red

Este capítulo trata los siguientes temas:

- Ver estadísticas de puertos y paquetes EAP
- Administrar los registros en búfer, de comandos y de consola
- Configurar los ajustes de Syslog y de host Syslog
- Ver y borrar los registros de traps
- Ver y borrar el registro de eventos
- Configurar la duplicación de varios puertos
- Administrar una VLAN RSPAN
- Configurar sFlow

Ver estadísticas de puertos y paquetes EAP

Puede ver estadísticas de puertos, incluidas estadísticas detalladas, y estadísticas de paquetes Extensible Authentication Protocol (EAP).

Ver y borrar estadísticas de puertos

Puede ver un resumen de las estadísticas de tráfico por puerto del switch y borrarlas.

Para ver y borrar estadísticas de puertos:

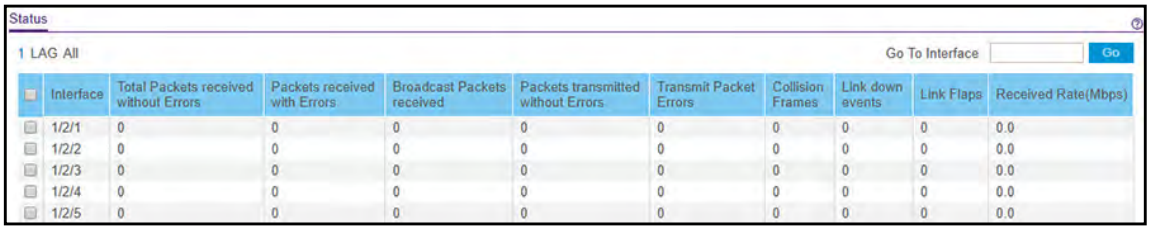
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring Ports > Port Statistics.



La figura anterior no muestra todas las columnas.

5. Use un botón en la parte inferior de la página para realizar una de las siguientes acciones:
   - Para borrar todos los contadores de todos los puertos del switch, marque la casilla de la fila de 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.
   - Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

La siguiente tabla describe las estadísticas por puerto que se muestran en la página.

Tabla 221. Estadísticas de puertos

Campo	Descripción
Interface	Este objeto indica la interfaz de la entrada de la tabla de interfaces asociada con este puerto en un adaptador.
Total Packets Received Without Errors	El número total de paquetes recibidos sin errores.
Packets Received With Error	El número de paquetes entrantes que contenían errores que impedían entregarlos a un protocolo de capa superior.
Broadcast Packets Received	El número total de paquetes correctos recibidos dirigidos a la dirección de broadcast. No incluye paquetes multicast.
Packets Transmitted Without Errors	El número de tramas transmitidas por este puerto a su segmento.
Transmit Packet Errors	El número de paquetes salientes que no se pudieron transmitir debido a errores.
Collision Frames	La mejor estimación del número total de colisiones en este segmento Ethernet.
Number of Link Down Events	El número total de eventos de enlace inactivo en un puerto físico.
Link Flaps	El número total de ocurrencias de eventos de enlace inactivo a enlace activo (cada una es una oscilación de enlace) durante el tiempo de debouncing.
Received Rate (Mbps)	La tasa de datos recibidos en Mbps.
Transmitted Rate (Mbps)	La tasa de datos transmitidos en Mbps.
Received Error Rate	La tasa de datos recibidos con errores en Mbps.
Transmitted Error Rate	La tasa 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.
Time Since Counters Last Cleared	El tiempo transcurrido en días, horas, minutos y segundos desde la última vez que se borraron las estadísticas de este puerto.

Ver y borrar las estadísticas detalladas de puertos

Puede ver diversas estadísticas de tráfico por puerto y borrarlas.

Para ver y borrar las estadísticas detalladas de puertos:

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

Se abre la ventana de inicio de sesión.

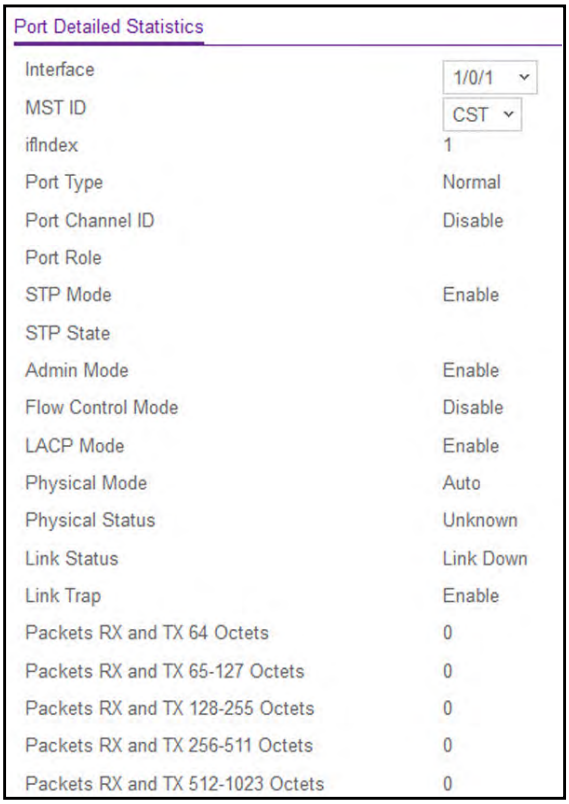
3. Ingrese admin como nombre de usuario, ingrese la contraseña local del dispositivo y haga clic en el botón Login.

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Ports > Port Detailed Statistics.

   La siguiente figura muestra algunos de los campos de la página Port Detailed Statistics, pero no todos.



5. Use un botón en la parte inferior de la página para realizar una de las siguientes acciones:
   - Para borrar todos los contadores, haga clic en el botón Clear. Esto restablece todas las estadísticas de este puerto a los valores predeterminados.
   - Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

La siguiente tabla describe la información detallada de puerto que se muestra en la página. Para ver información de otro puerto, seleccione el número de puerto en el menú Interface.

Tabla 222. Estadísticas detalladas de puertos

Campo	Descripción
MST ID	Muestra las instancias MST asociadas con la interfaz.
ifIndex	Este objeto indica el ifIndex de la entrada de la tabla de interfaces asociada con este puerto en un adaptador.
Port Type	Para los puertos normales, este campo es normal. De lo contrario, los valores posibles son los siguientes: • Mirrored. Este puerto participa en la duplicación de puertos como puerto duplicado. Consulte las páginas de Port Mirroring para obtener más información. • Probe. Este puerto participa en la duplicación de puertos como puerto de sondeo. Consulte las páginas de Port Mirroring para obtener más información. • Trunk Member. El puerto es miembro de un trunk de agregación de enlaces. Consulte las páginas de Port Channel para obtener más información.
Port Channel ID	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.
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 valores: Root, Designated, Alternate, Backup, Master o Disabled.
STP Mode	El modo administrativo de Spanning Tree Protocol asociado con el puerto o port channel. Los valores posibles son los siguientes: • Enable. Spanning tree está habilitado para este puerto. • Disable. Spanning tree está deshabilitado para este puerto.
STP State	El estado actual de Spanning Tree del puerto. Este estado controla qué acción toma un puerto al recibir una trama. Si el puente detecta un puerto con mal funcionamiento, coloca ese puerto en el estado broken. Los estados se definen en IEEE 802.1D: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Admin Mode	El estado administrativo del control del puerto. El puerto debe estar habilitado para que se le permita entrar a la red. El valor predeterminado de fábrica es habilitado.
Flow Control Mode	Indica si el control de flujo está habilitado o deshabilitado para el puerto. Este campo no es válido para interfaces LAG.
LACP Mode	Indica el estado administrativo de Link Aggregation Control Protocol. El modo debe estar habilitado para que el puerto participe en la agregación de enlaces.
Physical Mode	Indica la velocidad del puerto y el modo dúplex. En modo de autonegociación, el modo dúplex y la velocidad se establecen mediante el proceso de autonegociación.
Physical Status	Indica la velocidad y el modo dúplex del puerto.

Tabla 222. Estadísticas detalladas de puertos (continuación)

Campo	Descripción
Link Status	Indica si el enlace está activo o inactivo.
Link Trap	Indica si el puerto envía o no un trap cuando cambia el estado del enlace.
Packets RX and TX 64 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían 64 octetos de longitud (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 65-127 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 65 y 127 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 128-255 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 128 y 255 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 256-511 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 256 y 511 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 512-1023 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 512 y 1023 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 1024-1518 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 1024 y 1518 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 1519-2047 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 1519 y 2047 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 2048-4095 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 2048 y 4095 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets RX and TX 4096-9216 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos o transmitidos que tenían entre 4096 y 9216 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Octets Received	El número total de octetos de datos (incluidos los de paquetes erróneos) recibidos en la red (sin contar los bits de trama pero incluyendo los octetos FCS). Este objeto puede usarse como una estimación razonable del uso de Ethernet. Si se desea mayor precisión, los objetos etherStatsPkts y etherStatsOctets deben muestrearse antes y después de un intervalo común.
Packets Received 64 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían 64 octetos de longitud (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Received 65-127 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 65 y 127 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Received 128-255 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 128 y 255 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).

Tabla 222. Estadísticas detalladas de puertos (continuación)

Campo	Descripción
Packets Received 256-511 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 256 y 511 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Received 512-1023 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 512 y 1023 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Received 1024-1518 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 1024 y 1518 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Received > 1518 Octets	El número total de paquetes recibidos de más de 1518 octetos (sin contar los bits de trama, pero incluyendo los octetos FCS) y que por lo demás estaban bien formados.
Total Packets Received Without Errors	El número total de paquetes recibidos sin errores.
Unicast Packets Received	El número de paquetes unicast de subred entregados a un protocolo de capa superior.
Multicast Packets Received	El número total de paquetes correctos recibidos dirigidos a una dirección multicast. Este número no incluye los paquetes dirigidos a la dirección de broadcast.
Broadcast Packets Received	El número total de paquetes correctos recibidos dirigidos a la dirección de broadcast. No incluye paquetes multicast.
Transmit Packets Discarded	El número total de paquetes salientes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Un posible motivo para descartar un paquete podría ser liberar espacio en búfer.
Receive Packets Discarded	El número de paquetes entrantes descartados aunque no se detectaron errores que impidieran entregarlos a un protocolo de capa superior. Un posible motivo para descartar un paquete podría ser liberar espacio en búfer.
Total Packets Received with MAC Errors	El número total de paquetes entrantes que contenían errores que impedían entregarlos a un protocolo de capa superior.
Jabbers Received	El número total de paquetes recibidos de más de 1518 octetos (sin contar los bits de trama, pero incluyendo los 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 definición 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 cualquier paquete excede 20 ms. El rango permitido para detectar jabber es de 20 ms a 150 ms.
Fragments Received	El número total de paquetes recibidos de menos de 64 octetos de longitud con ERROR CRC (sin contar los bits de trama pero incluyendo los octetos FCS).
Undersize Received	El número total de paquetes recibidos de menos de 64 octetos de longitud con GOOD CRC (sin contar los bits de trama pero incluyendo los octetos FCS).

Tabla 222. Estadísticas detalladas de puertos (continuación)

Campo	Descripción
Alignment Errors	El número total de paquetes recibidos con una longitud (sin contar los bits de trama, pero incluyendo los octetos FCS) de entre 64 y 1518 octetos, inclusive, pero con una secuencia de verificación de trama (FCS) incorrecta con un número no entero de octetos.
Rx FCS Errors	El número total de paquetes recibidos con una longitud (sin contar los bits de trama, pero incluyendo los octetos FCS) de entre 64 y 1518 octetos, inclusive, pero con una secuencia de verificación de trama (FCS) incorrecta con un número entero de octetos
Overruns	El número total de tramas descartadas porque este puerto estaba sobrecargado de paquetes entrantes y no pudo procesar el flujo de entrada.
Total Received Packets Not Forwarded	Un recuento de las tramas válidas recibidas que fueron descartadas (es decir, filtradas) por el proceso de reenvío.
802.3x Pause Frames Received	Un recuento de las 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 funciona en modo half-duplex.
Unacceptable Frame Type	El número de tramas descartadas de este puerto por ser de un tipo de trama no aceptable.
Total Packets Transmitted (Octets)	El número total de octetos de datos (incluidos los de paquetes erróneos) transmitidos en la red (sin contar los bits de trama pero incluyendo los octetos FCS). Este objeto puede usarse como una estimación razonable del uso de Ethernet. Si se desea mayor precisión, los objetos etherStatsPkts y etherStatsOctets deben muestrearse antes y después de un intervalo común.
Packets Transmitted 64 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían 64 octetos de longitud (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Transmitted 65-127 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 65 y 127 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Transmitted 128-255 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 128 y 255 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Transmitted 256-511 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 256 y 511 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Transmitted 512-1023 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 512 y 1023 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Transmitted 1024-1518 Octets	El número total de paquetes (incluidos los paquetes erróneos) recibidos que tenían entre 1024 y 1518 octetos de longitud, inclusive (sin contar los bits de trama pero incluyendo los octetos FCS).
Packets Transmitted > 1518 Octets	El número total de paquetes transmitidos de más de 1518 octetos (sin contar los bits de trama, pero incluyendo los octetos FCS) y que por lo demás estaban bien formados. Este contador tiene una tasa máxima de incremento de 815 conteos por segundo a 10 Mb/s.

Tabla 222. Estadísticas detalladas de puertos (continuación)

Campo	Descripción
Maximum Frame Size	El tamaño máximo de trama Ethernet que la interfaz admite o está configurada para usar, incluidos el encabezado Ethernet, el CRC y la carga útil (1518 a 9216). El tamaño máximo de trama predeterminado es 1518.
Total Packets Transmitted Successfully	El número de tramas transmitidas por este puerto a su segmento.
Unicast Packets Transmitted	El 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.
Multicast Packets Transmitted	El 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.
Broadcast Packets Transmitted	El 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.
Total Transmit Errors	La suma de colisiones simples, múltiples y excesivas.
Total Transmit Packets Discarded	La suma de las tramas de colisión única descartadas, las tramas de colisión múltiple descartadas y las tramas excesivas descartadas.
Single Collision Frames	Recuento de tramas transmitidas correctamente en una interfaz determinada cuya transmisión se vio impedida por exactamente una colisión.
Multiple Collision Frames	Recuento de tramas transmitidas correctamente en una interfaz determinada cuya transmisión se vio impedida por más de una colisión.
Excessive Collision Frames	Recuento de tramas cuya transmisión en una interfaz determinada falla por colisiones excesivas.
STP BPDUs Received	Número de BPDU STP recibidas en el puerto seleccionado.
STP BPDUs Transmitted	Número de BPDU STP transmitidas desde el puerto seleccionado.
RSTP BPDUs Received	Número de BPDU RSTP recibidas en el puerto seleccionado.
RSTP BPDUs Transmitted	Número de BPDU RSTP transmitidas desde el puerto seleccionado.
MSTP BPDUs Received	Número de BPDU MSTP recibidas en el puerto seleccionado.
MSTP BPDUs Transmitted	Número de BPDU MSTP transmitidas desde el puerto seleccionado.
802.3x Pause Frames Transmitted	Recuento 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 funciona en modo half-duplex.
GVRP PDUs Received	Recuento de PDU GVRP recibidas en la capa GARP.
GVRP PDUs Transmitted	Recuento de PDU GVRP transmitidas desde la capa GARP.
GVRP Failed Registrations	Número de veces que no pudieron completarse los intentos de registro GVRP.
GMRP PDUs Received	Recuento de PDU GMRP recibidas desde la capa GARP.
GMRP PDUs Transmitted	Recuento de PDU GMRP transmitidas desde la capa GARP.

Tabla 222. Estadísticas detalladas de puertos (continuación)

Campo	Descripción
GMRP Failed Registrations	Número de veces que no pudieron completarse los intentos de registro GMRP.
EAPOL Frames Received	Número de tramas EAPOL válidas de cualquier tipo recibidas por este autenticador.
EAPOL Frames Transmitted	Número de tramas EAPOL de cualquier tipo transmitidas por este autenticador.
Load Interval	Período en segundos cuyos datos se usan para calcular las estadísticas de carga.
Received Rate (Mbps)	La tasa de datos recibidos en Mbps.
Transmitted Rate (Mbps)	La tasa de datos transmitidos en Mbps.
Received Error Rate	La tasa de datos recibidos con errores en Mbps.
Transmitted Error Rate	La tasa 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.
Time Since Counters Last Cleared	El tiempo transcurrido en días, horas, minutos y segundos desde la última vez que se borraron las estadísticas de este puerto.

Ver estadísticas de EAP

Puede mostrar información sobre los paquetes EAP recibidos en un puerto específico.

Para ver las estadísticas de EAP:

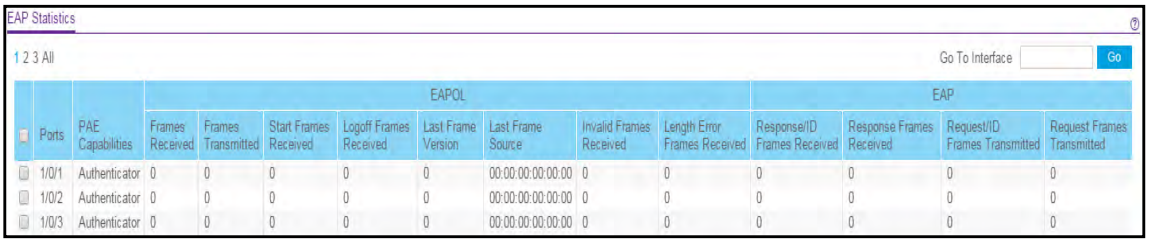
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Ports > EAP Statistics.



5. Use un botón de la parte inferior de la página para realizar una de las siguientes acciones:
   - Para borrar todos los contadores EAP de todos los puertos del switch, seleccione la casilla del encabezado de fila y haga clic en el botón Clear. Al hacer clic en el botón se restablecen todas las estadísticas de todos los puertos a los valores predeterminados.
   - Para borrar los contadores de un puerto específico, seleccione la casilla asociada al puerto y haga clic en el botón Clear.
   - Para actualizar la página con la información más reciente del switch, haga clic en el botón Refresh.

La siguiente tabla describe las estadísticas de EAP que se muestran en la página.

Tabla 223. Estadísticas de EAP

Campo	Descripción
Port	Selecciona el puerto que se mostrará. Al cambiar la selección, la página se actualiza y todos los campos se actualizan para el puerto recién seleccionado. Todas las interfaces físicas son válidas.
PAE Capabilities	Muestra las capacidades PAE del puerto seleccionado.
EAPOL Frames Received	Muestra el número de tramas EAPOL válidas de cualquier tipo recibidas por este autenticador.
EAPOL Frames Transmitted	Muestra el número de tramas EAPOL de cualquier tipo transmitidas por este autenticador.
EAPOL Start Frames Received	Muestra el número de tramas EAPOL start recibidas por este autenticador.
EAPOL Logoff Frames Received	Muestra el número de tramas EAPOL logoff recibidas por este autenticador.
EAPOL Last Frame Version	Muestra el número de versión del protocolo incluido en la trama EAPOL recibida más recientemente.
EAPOL Last Frame Source	Muestra la dirección MAC de origen incluida en la trama EAPOL recibida más recientemente.
EAPOL Invalid Frames Received	Muestra el número de tramas EAPOL recibidas por este autenticador cuyo tipo de trama no se reconoce.
EAPOL Length Error Frames Received	Muestra el número de tramas EAPOL recibidas por este autenticador cuyo tipo de trama no se reconoce.
EAP Response/ID Frames Received	Muestra el número de tramas EAP response/identity recibidas por este autenticador.

Tabla 223. Estadísticas de EAP

Campo	Descripción
EAP Response Frames Received	Muestra el número de tramas EAP response válidas (distintas de las tramas resp/ID) recibidas por este autenticador.
EAP Request/ID Frames Transmitted	Muestra el número de tramas EAP request/identity transmitidas por este autenticador.
EAP Request Frames Transmitted	Muestra el número de tramas EAP request (distintas de las tramas request/identity) transmitidas por este autenticador.

Realizar una prueba de cable

Para realizar una prueba de cable:

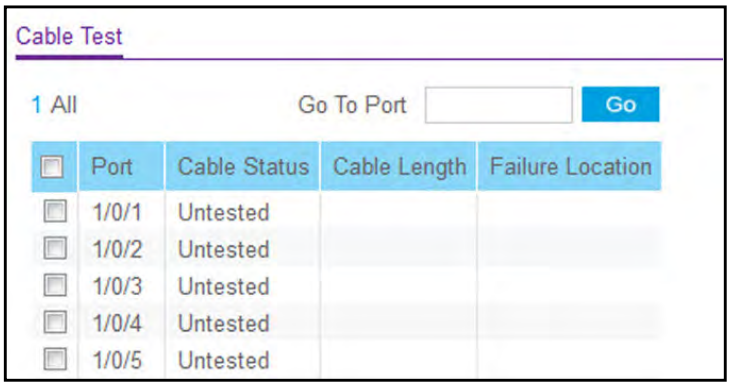
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Ports > Cable Test.



5. Use uno de los siguientes métodos para seleccionar un puerto:
   - En el campo Go To Port, escriba la interfaz en formato unidad/ranura/puerto y haga clic en el botón Go.
   - Junto a la columna Port, seleccione la casilla del puerto que desea probar.

6. Haga clic en el botón Aplicar (Apply).
Se realiza una prueba de cable en la interfaz seleccionada. La prueba 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 terminación o conectados a tierra.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 224. Prueba de cable

Campo	Descripción
Cable Status	Muestra el estado del cable como Normal, Open o Short. • Normal: el cable funciona correctamente. • Open: el cable está desconectado o hay un conector defectuoso. • Short: hay un cortocircuito eléctrico en el cable. • Cable Test Failed: No se pudo determinar el estado del cable. Es posible que el cable funcione. • 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. Cable Length solo se muestra si el estado del cable es Normal.
Failure Location	La distancia estimada en metros desde el extremo del cable hasta el punto de falla. Solo se muestra si el estado del cable es Open o Short.

Administrar los registros en búfer, de comandos y de consola

El switch genera mensajes en respuesta a eventos, fallas o errores que ocurren en la plataforma, así como a cambios de configuración u otros sucesos. Estos mensajes se almacenan localmente y pueden reenviarse a uno o más puntos centralizados de recopilación para monitoreo o archivo a largo plazo (consulte Configurar los ajustes de Syslog y del host Syslog en la página 653). La configuración local y remota del registro incluye el filtrado de los mensajes registrados o reenviados según la gravedad y el componente que los genera.

Ver y borrar los registros en búfer

Para ver y borrar los registros en búfer:

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

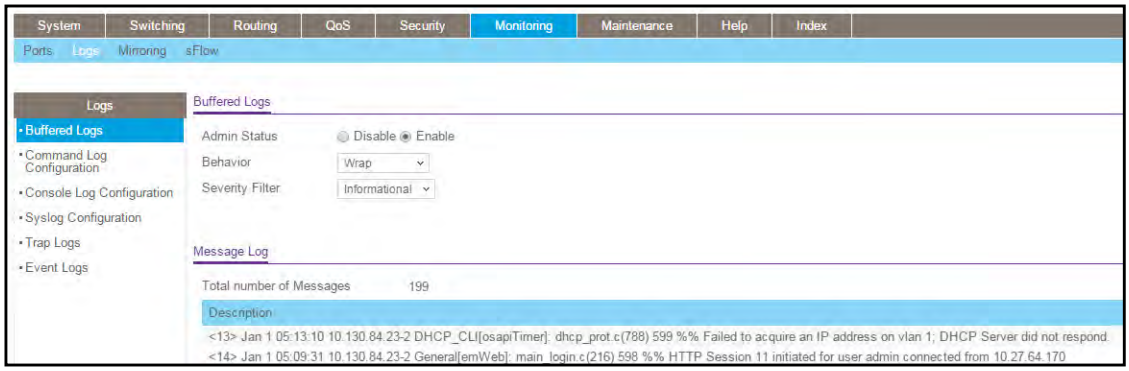
Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Logs > Buffered Logs.



5. Para borrar el registro en búfer de la memoria, haga clic en el botón Clear.

Configurar los ajustes del registro en memoria

Este registro almacena mensajes en la memoria según los ajustes de componente y gravedad de los mensajes.

Para configurar los ajustes del registro en memoria:

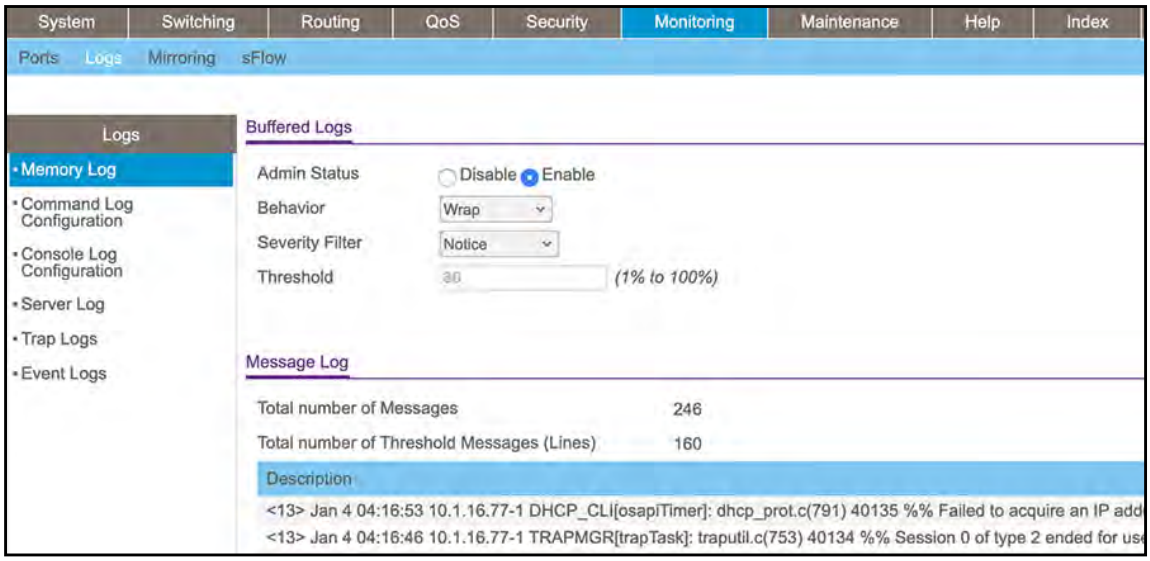
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Logs > Memory Log.



5. Seleccione el botón de opción Admin Status Enable o Disable. Un registro deshabilitado no registra mensajes.
6. En el menú Behavior, seleccione la acción que se realiza cuando el registro está lleno.

   El registro puede sobrescribirse de forma circular (Wrap, la acción predeterminada) o detenerse cuando está lleno (Stop-on-Full).

7. En el menú Severity Filter, seleccione el nivel de gravedad:
Un registro guarda los mensajes de gravedad igual o superior al nivel configurado. Los niveles de gravedad son los siguientes:

- Emergency (0). El sistema no se puede usar.
- Alert (1). Debe actuarse de inmediato.
- Critical (2). Condiciones críticas.
- Error (3). Condiciones de error.
- Warning (4). Condiciones de advertencia.
- Notice (5). Condiciones normales pero significativas.
- Informational (6). Mensajes informativos.
- Debug (7). Mensajes de nivel de depuración.

8. En el campo Threshold, introduzca el porcentaje (de 1 a 100 por ciento) del espacio del registro que, al superarse, detiene el registro.

   El umbral solo se aplica si la opción del menú Behavior es Stop-on-Full.

   De forma predeterminada, la opción del menú Behavior es Wrap y el umbral no se aplica.

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

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. Es el mensaje número 237 registrado con IP del sistema 0.0.0.0 e 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. 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: En el registro de mensajes, solo se muestran en la página las 200 entradas más recientes.

Habilitar o deshabilitar el registro de comandos

Para habilitar o deshabilitar el registro de comandos:

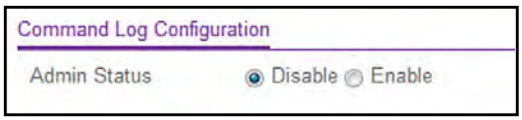
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Monitoring > Logs > Command Log Configuration.**



5. Use Admin Mode para habilitar o deshabilitar el registro de comandos de CLI seleccionando el botón de opción correspondiente.
6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

Habilitar o deshabilitar el registro de consola

Permite registrar en cualquier dispositivo serie conectado al host.

Para habilitar o deshabilitar el registro de consola:

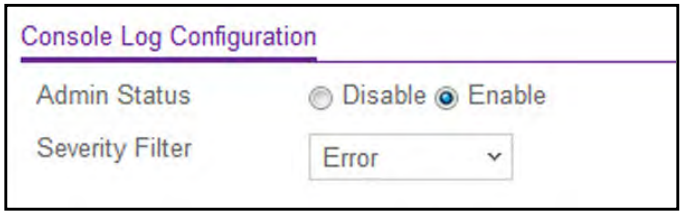
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Logs > Console Log Configuration.



5. Seleccione el botón de opción Admin Status Disable o Enable. Un registro deshabilitado no registra mensajes.

6. Severity Filter. Un registro guarda los mensajes de gravedad igual o superior al umbral configurado.
   Seleccione la opción de gravedad eligiendo la línea correspondiente en la lista desplegable. Están disponibles estos niveles de gravedad:
   - Emergency (0). El sistema no se puede usar.
   - Alert (1). Debe actuarse de inmediato.
   - Critical (2). Condiciones críticas.
   - Error (3). Condiciones de error.
   - Warning (4). Condiciones de advertencia.
   - Notice (5). Condiciones normales pero significativas.
   - Informational (6). Mensajes informativos.
   - Debug (7). Mensajes de nivel de depuración.

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

Configurar los ajustes de Syslog y del host Syslog

Puede hacer que el switch filtre los mensajes que se reenvían según la gravedad y el componente que los genera. También puede configurar los ajustes del host syslog.

Configurar los ajustes de Syslog

Para configurar los ajustes de syslog:

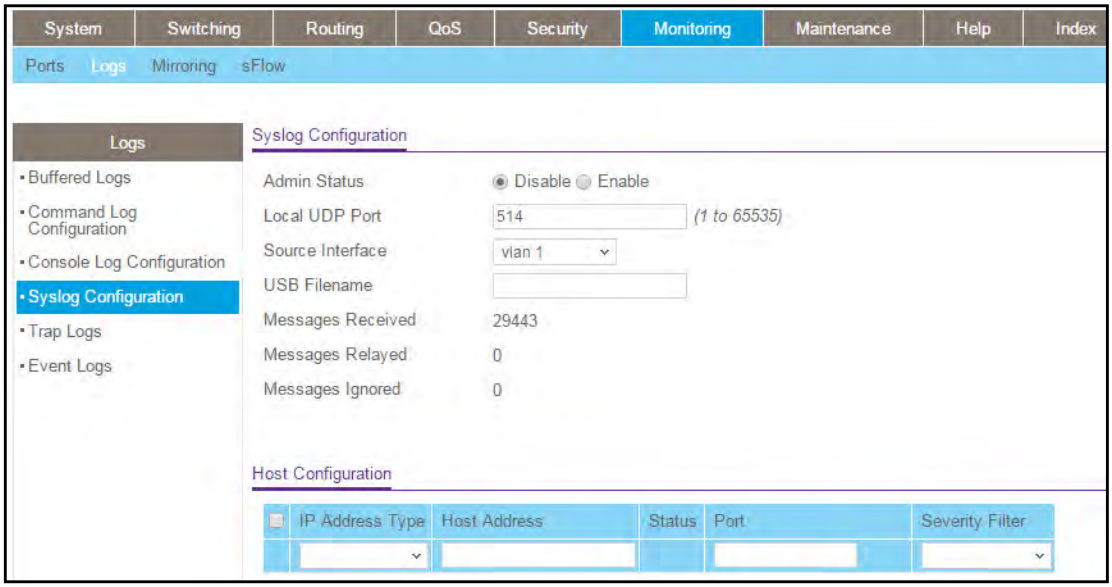
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Monitoring > Logs > Syslog Configuration.**



El campo Status indica si el host se configuró para registrar activamente o no.

5. Seleccione el botón de opción Admin Status Disable o Enable.

   Esto habilita o deshabilita el registro en los hosts syslog configurados. Cuando Admin Status está deshabilitado, el dispositivo no retransmite registros a los hosts syslog y no se envían mensajes a

ningún recopilador ni relay. Cuando Admin Status de syslog está habilitado, los mensajes se envían a los recopiladores o relays configurados con los valores configurados para cada uno.

6. Use Local UDP Port para especificar el puerto del host local desde el que se envían los mensajes syslog. El rango es de 1 a 65535. El puerto predeterminado es 514.

7. Especifique la Source Interface que se usará
para syslog. Los valores posibles son los siguientes:

- None. Cuando se muestra el valor None, significa que la interfaz de enrutamiento configurada dejó de enrutar.
- Interfaz de enrutamiento
- Routing VLAN
- Interfaz loopback de enrutamiento
- Interfaz de túnel
- Puerto de servicio

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

8. Use el campo USB Filename para especificar el nombre del archivo USB. El nombre no puede incluir los siguientes símbolos: V:*?”<>!. Puede introducir hasta 64 caracteres. Los 64 caracteres corresponden solo al nombre; la extensión se agrega automáticamente. El valor predeterminado está en blanco.

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

Nota: Syslog puede escribir los mensajes de registro simultáneamente en un servidor remoto y en el dispositivo de almacenamiento USB.

Configurar los ajustes del host Syslog

Para configurar los ajustes del host syslog:

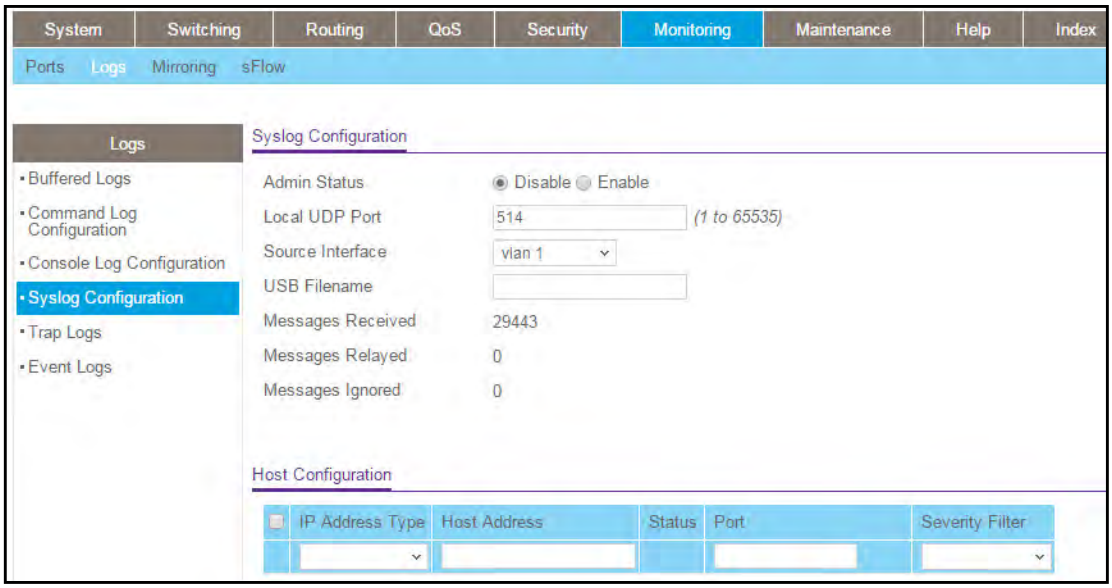
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP
del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Monitoring > Logs > Syslog Configuration.



5. En la sección Host Configuration, configure los siguientes ajustes:
   - En el menú IP Address Type, seleccione el tipo de dirección del host.
     - IPv4
     - IPv6
     - DNS
   - En el campo Host Address, especifique la dirección del host configurado para syslog.
   - En el campo Port, especifique el puerto del host al que se envían los mensajes syslog.

     El puerto predeterminado es 514.

   - Seleccione la opción de gravedad en la lista Severity Filter.

     Un registro guarda los mensajes de gravedad igual o superior al umbral configurado. Están disponibles estos niveles de gravedad:

     - Emergency (0). El sistema no se puede usar
     - Alert (1). Debe actuarse de inmediato
     - Critical (2). Condiciones críticas
     - Error (3). Condiciones de error
     - Warning (4). Condiciones de advertencia
     - Notice (5). Condiciones normales pero significativas
     - Informational (6). Mensajes informativos
     - Debug (7). Mensajes de nivel de depuración

6. Haga clic en el botón Aplicar (Apply). La configuración se guarda.

La siguiente tabla describe la información no configurable.

Tabla 225. Configuración de Syslog

Campo	Descripción
Messages Received	Número de mensajes recibidos por el proceso de registro. Incluye los mensajes descartados o ignorados.
Messages Relayed	Recuento de mensajes syslog retransmitidos.
Messages Ignored	Recuento de mensajes syslog ignorados.

Ver y borrar los registros de traps

Puede ver y borrar las entradas del registro de traps. La información puede obtenerse como archivo.

Para ver y borrar los registros de traps:

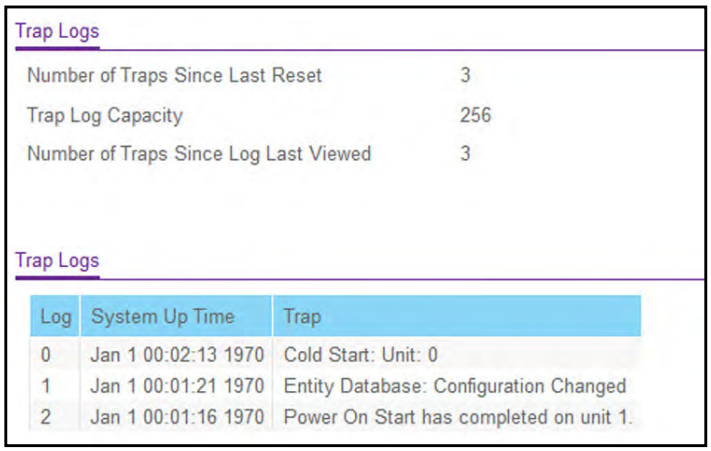
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Monitoring > Logs > Trap Logs.**



La página también muestra información sobre los traps enviados.
5. Para borrar todos los contadores, haga clic en el botón Clear.

Esto restablece todas las estadísticas de los registros de traps a los valores predeterminados. La siguiente tabla describe la información de Trap Log que se muestra en la página.

Tabla 226. Registros de traps

Campo	Descripción
Number of Traps Since Last Reset	El número de traps ocurridos desde el último reinicio del switch.
Trap Log Capacity	El número máximo de traps almacenados en el registro. Si el número de traps supera la capacidad, las entradas nuevas sobrescriben las más antiguas.
Number of Traps since log last viewed	El número de traps ocurridos desde la última vez que se mostraron. Mostrar los traps por cualquier método (interfaz de terminal, web, carga de archivo desde el switch, etc.) hace que este contador se ponga en 0.
Log	El número de secuencia de este trap.
System Up Time	El momento en que ocurrió este trap, expresado en días, horas, minutos y segundos desde el último reinicio del switch.
Trap	Información que identifica el trap.

Ver y borrar el registro de eventos

Puede ver y borrar el registro de eventos, que contiene los mensajes de error del sistema. El registro de eventos no se borra al restablecer el sistema.

Para ver y borrar el registro de eventos:

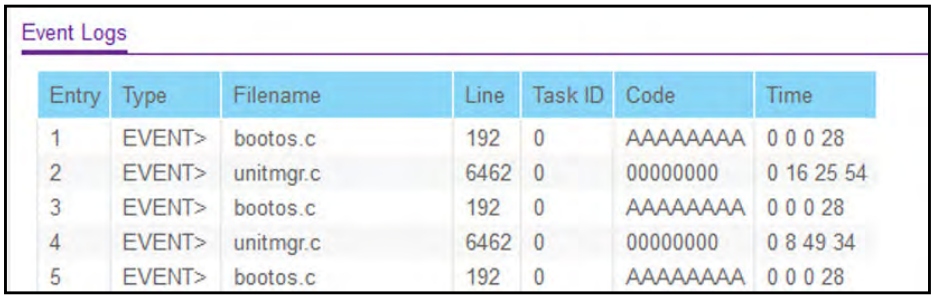
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Logs > Event Logs.



5. Para borrar los mensajes del registro de eventos, haga clic en el botón Clear. La siguiente tabla describe la información del registro de eventos que se muestra en la página.

Tabla 227. 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	El momento en que ocurrió este evento.

Configurar la duplicación de varios puertos

La duplicación de puertos selecciona el tráfico de red para que lo analice un analizador de red. Esto se hace para puertos específicos del switch. Así, varios puertos del switch se configuran como puertos de origen y un puerto del switch se configura como puerto de destino. Puede configurar cómo se duplica el tráfico en un puerto de origen. Los paquetes recibidos en el puerto de origen, transmitidos por un puerto, o tanto recibidos como transmitidos, pueden duplicarse en el puerto de destino.

El paquete que se copia en el puerto de destino tiene el mismo formato que el paquete original en el cable. Esto significa que, si la duplicación copia un paquete recibido, el paquete copiado está con o sin etiqueta VLAN tal como se recibió en el puerto de origen. Si la duplicación copia un paquete transmitido, el paquete copiado está con o sin etiqueta VLAN tal como se transmite en el puerto de origen.

Configurar globalmente la duplicación de varios puertos

Para configurar globalmente la duplicación de varios puertos:

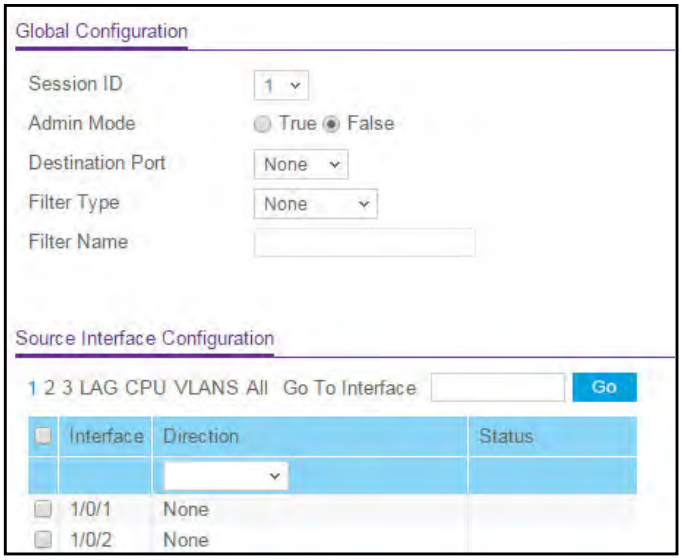
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. **Seleccione Monitoring > Mirroring > Multiple Port Mirroring.**



5. Seleccione el número de ID de sesión de duplicación de puertos en la lista Session ID. El número de sesiones permitidas depende de la plataforma.
6. Seleccione el modo administrativo de la sesión de duplicación seleccionada con el botón de opción True (habilitado) o False (deshabilitado).

   Seleccione la opción True para habilitar el modo Admin de la sesión seleccionada. Cuando una sesión está habilitada, todo el tráfico que entra o sale de los puertos de origen de la sesión se copia (duplica) en el puerto de destino correspondiente o en una VLAN de analizador de puertos conmutados remoto (RSPAN). De forma predeterminada, el modo Admin está deshabilitado (False). Si el modo es False (deshabilitado), el origen configurado no duplica el tráfico al destino.

7. En la lista Destination Port, seleccione la interfaz de destino a la que se copiará el tráfico del puerto.

   Solo puede configurar un puerto de destino en el sistema. Actúa como puerto de sonda y recibe el tráfico de todos los puertos de origen configurados. Si el valor no está configurado, se muestra como None. El valor predeterminado es None.

8. En la lista Filter Type, seleccione la ACL de IP o MAC que puede duplicar el tráfico que coincide con una regla permit.

Los valores posibles son los siguientes:

- None. No hay ningún filtro configurado para la sesión.
- IP ACL. Configure el ID o nombre de la lista de acceso IP. El ID de la ACL de IP que se aplicará al tráfico del origen. Solo el tráfico que coincide con las reglas de la ACL se duplica en el destino.
- MAC ACL. Configure la ACL de MAC. El ID de la ACL de MAC que se aplicará al tráfico del origen. Solo el tráfico que coincide con las reglas de la ACL se duplica en el destino.

El valor predeterminado es None.
9. En el campo Filter Name, introduzca el nombre del filtro, si está configurado para la sesión.
10. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar la interfaz de origen de la duplicación de puertos

Nota: Si una interfaz participa en una VLAN y es miembro de un LAG, la VLAN no puede asignarse como VLAN de origen de una sesión de monitoreo. Al mismo tiempo, si una interfaz participa en una VLAN y esta VLAN está asignada como VLAN de origen de una sesión de monitoreo, la interfaz puede asignarse como miembro de un LAG.

Para configurar la interfaz de origen de la duplicación de puertos:

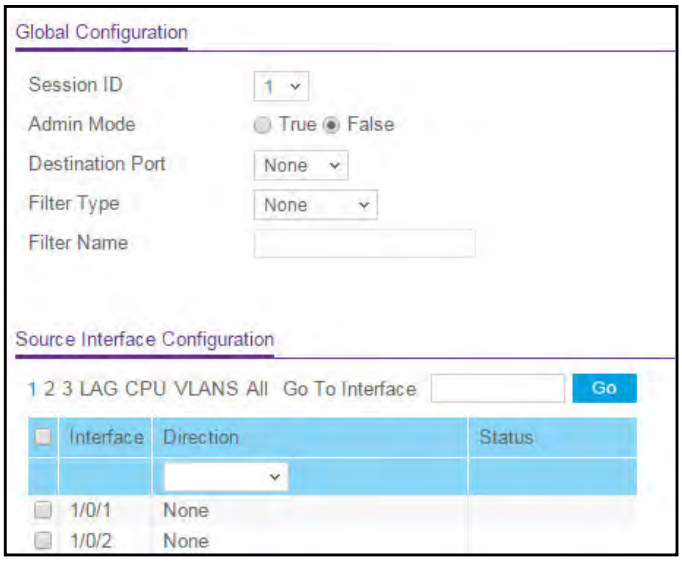
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Monitoring > Mirroring > Multiple Port Mirroring.



5. En la sección Source Interface Configuration, seleccione qué interfaces se muestran en la página:
   - Seleccione Unit ID para mostrar los puertos físicos de la unidad seleccionada.
   - Seleccione LAG para mostrar solo una lista de LAG.
   - Seleccione CPU para mostrar solo una lista de CPU.
   - Seleccione VLANs para mostrar una lista de las VLAN disponibles.
   - Seleccione All para mostrar una lista de todos los puertos físicos, LAG, CPU y VLAN.
6. Use uno de los siguientes métodos para seleccionar una interfaz:
   - En el campo Go To Interface, introduzca la interfaz con el formato unidad/ranura/puerto y haga clic en el botón Go.
   - Junto a la columna Interface, seleccione la casilla de la interfaz o interfaces que desea incluir.
7. En el campo Direction, especifique la dirección del tráfico que se duplicará desde los puertos duplicados configurados.

   Si el valor no está configurado, se muestra como None. El valor predeterminado es None. Las opciones de dirección son las siguientes:

   - None. El valor no está configurado.
   - Tx and Rx. Monitorea los paquetes transmitidos y recibidos.
   - Rx. Monitorea solo los paquetes recibidos (de entrada).
   - Tx. Monitorea solo los paquetes transmitidos (de salida).

   Nota: Para las VLAN, solo se aplican las opciones Tx and Rx y None.

   - Tx and Rx. Especifica la VLAN como VLAN de origen.
   - None. Quita la VLAN de origen especificada.

Si la VLAN está configurada como VLAN de origen, su dirección se muestra como un campo en blanco.

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

Los ajustes se aplican al sistema. Si el puerto está configurado como puerto de origen, el valor del campo Mirroring Port es Mirrored.

El campo Status indica el estado de la interfaz.

Nota: Si un cuadro de diálogo de error incluye varios mensajes de error, resuelva los primeros mensajes de error para poder ver los mensajes de error restantes.

Administrar una VLAN RSPAN

Puede configurar la VLAN para usar la VLAN de analizador de puertos conmutados remoto (RSPAN). RSPAN le permite duplicar el tráfico de varios puertos de origen (o de todos los puertos que son miembros de una VLAN) de distintos dispositivos de red y enviar el tráfico duplicado a un puerto de destino (un puerto de sonda 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.

Configurar una VLAN RSPAN

Para configurar una VLAN RSPAN:

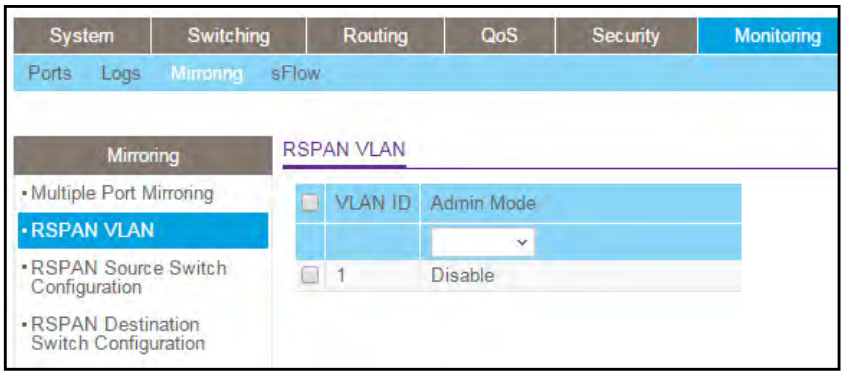
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Monitoring > Mirroring > RSPAN VLAN.



La columna VLAN ID muestra todas las VLAN del dispositivo.
5. Seleccione la VLAN que se usará como VLAN RSPAN.

6. En la lista Admin Mode, seleccione Enable o Disable para la compatibilidad con RSPAN en la VLAN correspondiente.

El valor predeterminado es
Disable.
7. Haga clic en el botón Apply.
La configuración se guarda.

Configurar un switch de origen RSPAN

Para configurar un switch de origen RSPAN:

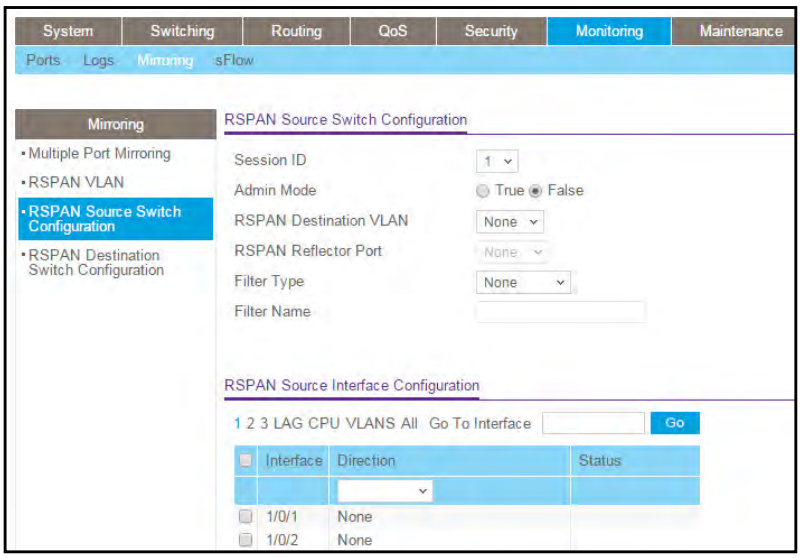
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Mirroring > RSPAN Source Switch Configuration.



5. Seleccione el número de Session ID de la lista.

6. Seleccione el botón de opción Admin Mode True (habilitado) o False (deshabilitado) para la sesión seleccionada.

   Cuando una sesión está habilitada, todo el tráfico que entra o sale de los puertos de origen de la sesión se copia (duplica) al puerto de destino correspondiente o a una VLAN de analizador de puertos conmutados remoto (RSPAN). De forma predeterminada, Admin mode es False (deshabilitado).

7. Seleccione la RSPAN Destination VLAN de la lista de ID de VLAN disponibles.
8. Seleccione el RSPAN Reflector Port de la lista de interfaces de puerto reflector.

9. Seleccione en la lista Filter Type para configurar ACL IP o MAC que puedan duplicar el tráfico que coincida con una regla de permiso.

   Los valores posibles son los siguientes:

   - **None**.
   - IP ACL. Configurar ACL IP.
   - MAC ACL. Configurar ACL MAC.

10. Introduzca el Filter Name, si hay un filtro configurado para la sesión.
11. Haga clic en el botón Apply.
La configuración se guarda.

Configurar una interfaz de origen RSPAN

Para configurar una interfaz de origen RSPAN:

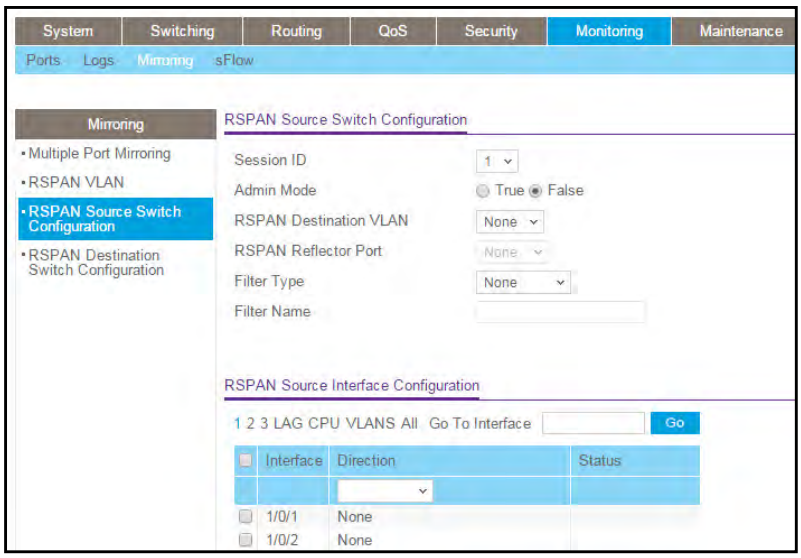
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Mirroring > RSPAN Source Switch Configuration.



5. Use uno de los siguientes métodos para mostrar las interfaces disponibles en la página:

   - Seleccione un Unit ID (1, 2, 3) para mostrar una lista de puertos físicos de la unidad seleccionada.
   - Seleccione LAG para mostrar solo los LAG.
   - Seleccione CPU para mostrar solo las CPU.
   - Seleccione VLAN para mostrar una lista de los ID de VLAN disponibles.
   - Seleccione All para mostrar todos los puertos físicos, LAG, CPU y VLAN.

6. Use uno de los siguientes métodos para seleccionar una interfaz:

   - En el campo Go To Interface, introduzca la interfaz con el formato unidad/ranura/puerto y haga clic en el botón Go.
   - Junto a la columna Interface, seleccione la casilla de la interfaz que desea usar como origen, o seleccione varias casillas para usar todas las interfaces seleccionadas como orígenes.

7. Seleccione en la lista Direction la dirección del tráfico que se duplicará desde los puertos duplicados configurados.

   Si el valor no está configurado, se muestra None. El valor predeterminado es None.

   - None. El valor no está configurado.
   - Tx and Rx. Supervisa los paquetes transmitidos y recibidos.
   - Tx. Supervisa solo los paquetes transmitidos.
   - Rx. Supervisa solo los paquetes recibidos.

8. Haga clic en el botón Apply (Aplicar).
La configuración se guarda.
El tráfico de las interfaces seleccionadas se envía al puerto de sondeo. El campo Status indica el estado de la interfaz.

Configurar el switch de destino RSPAN

Para configurar el switch de destino RSPAN:

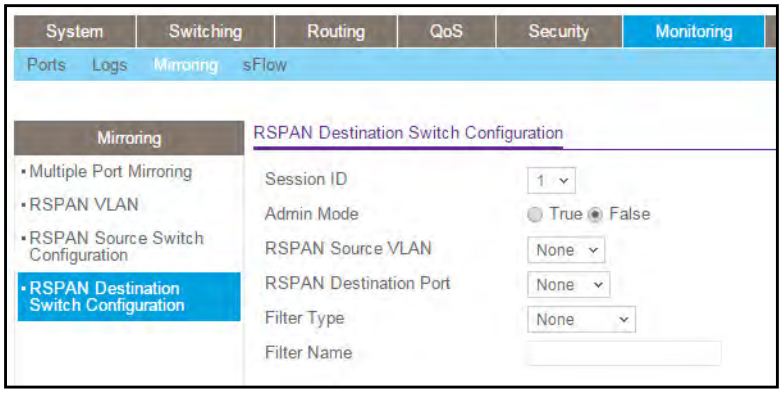
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring > Mirroring > RSPAN Destination Switch Configuration.



5. En la lista Session ID, seleccione el ID de sesión.
6. Seleccione el botón de opción Admin Mode True (habilitado) o False (deshabilitado) para la sesión seleccionada.

   Cuando una sesión está habilitada, todo el tráfico que entra o sale de los puertos de origen de la sesión se copia (duplica) al puerto de destino correspondiente o a una VLAN de analizador de puertos conmutados remoto (RSPAN). De forma predeterminada, Admin mode está deshabilitado.

7. Seleccione la RSPAN Source VLAN de la lista de ID de VLAN disponibles.
8. Seleccione la RSPAN Destination VLAN de la lista de interfaces de destino.
9. Configure el Filter Type.

Las ACL IP o MAC pueden duplicar el tráfico que coincida con una regla de permiso. Los valores posibles son los siguientes:

- None. No hay ningún filtro configurado para la sesión.
- IP ACL. Configurar ACL IP.
- MAC ACL. Configurar ACL MAC.

10. Introduzca el Filter Name, si está configurado para la sesión.
11. Haga clic en el botón Apply.
La configuración se guarda.

Configurar sFlow

sFlow es el estándar para supervisar redes conmutadas y enrutadas de alta velocidad. La tecnología sFlow está integrada en los equipos de red y ofrece visibilidad completa de la actividad de la red, lo que permite administrar y controlar eficazmente sus recursos.

El sistema de supervisión sFlow consta de un sFlow Agent (integrado en un switch, router o sonda independiente) y un sFlow Collector central. El sFlow Agent usa tecnología de muestreo para capturar estadísticas de tráfico del dispositivo que supervisa. Los datagramas sFlow se usan para reenviar de inmediato las estadísticas muestreadas a un sFlow Collector para su análisis.

El sFlow Agent usa dos formas de muestreo: muestreo estadístico basado en paquetes de los flujos conmutados o enrutados, y muestreo de contadores basado en tiempo.

Resumen del sFlow Agent

El muestreo de flujos de paquetes y el muestreo de contadores los realizan instancias sFlow asociadas a fuentes de datos individuales dentro del sFlow Agent. Ambos tipos de muestreo están diseñados como parte de un sistema integrado. Ambos tipos de muestras se combinan en datagramas sFlow. El muestreo de flujos de paquetes genera un flujo constante, pero aleatorio, de datagramas sFlow que se envían al sFlow Collector. Las muestras de contadores pueden tomarse de forma oportunista para completar estos datagramas.

Para realizar el muestreo de flujos de paquetes, se configura una instancia sFlow Sampler con una tasa de muestreo. Este proceso genera registros de flujos de paquetes. Para realizar el muestreo de contadores, la instancia sFlow Poller se configura con un intervalo de sondeo. Este proceso genera registros de contadores. El sFlow Agent recopila ambos tipos de registros y los envía en forma de datagramas sFlow a los sFlow Collectors.

Puede configurar los ajustes básicos o avanzados de sFlow.

Configurar la información básica del sFlow Agent

Para configurar la información básica del sFlow Agent:

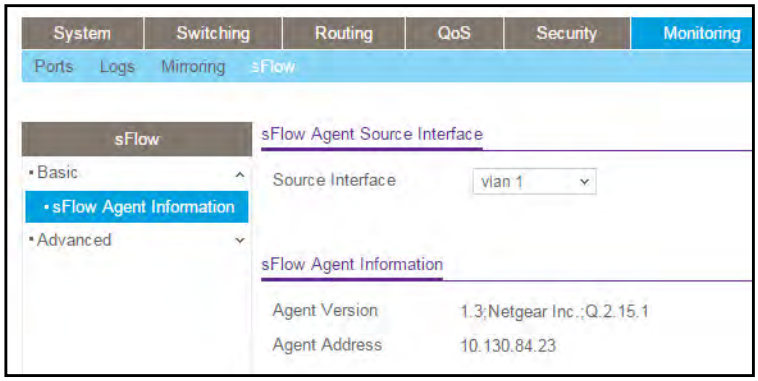
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring> sFlow > Basic > sFlow Agent Information.



5. En la lista Source Interface, seleccione la interfaz de administración que usa el sFlow Agent. Los valores posibles son los siguientes:

- None
- Interfaz de enrutamiento
- Routing VLAN
- Interfaz loopback de enrutamiento
- Interfaz de túnel
- Puerto de servicio

De forma predeterminada, se usa VLAN 1 como interfaz de origen.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

La siguiente tabla describe la información no configurable.

Tabla 228. Información básica del sFlow Agent

Campo	Descripción
Agent Version	Identifica de forma única la versión e implementación de esta MIB. La cadena de versión debe tener la siguiente estructura: MIB Version;Organization;Software Revision, donde: • MIB Version: Por ejemplo, 1.3, la versión de esta MIB • Organization: NETGEAR, Inc. • Revision: 1.0
Agent Address	La dirección IP asociada a este agente.

Configurar los ajustes avanzados del sFlow Agent

Para configurar los ajustes avanzados del sFlow Agent:

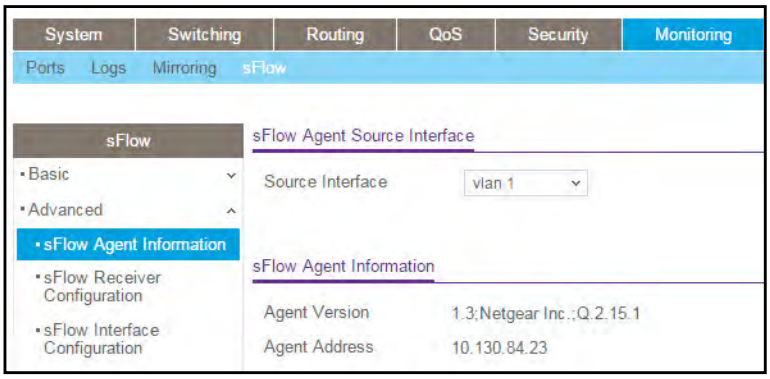
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring> sFlow > Advanced > sFlow Agent Information.



5. En la lista Source Interface, seleccione la interfaz de administración que usará el sFlow Agent. Los valores posibles son los siguientes:

- None
- Interfaz de enrutamiento
- Routing VLAN

- Interfaz loopback de enrutamiento
- Interfaz de túnel
- Puerto de servicio

De forma predeterminada, se usa VLAN 1 como interfaz de origen.
6. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.
La siguiente tabla describe la información no configurable.

Tabla 229. Información avanzada del sFlow Agent

Campo	Descripción
Agent Version	Identifica de forma única la versión e implementación de esta MIB. La cadena de versión debe tener la siguiente estructura: MIB Version;Organization;Software Revision, donde: • MIB Version: '1.3', la versión de esta MIB • Organization: NETGEAR, Inc. • Revision: 1.0
Agent Address	La dirección IP asociada a este agente.

Configurar un receptor sFlow

Use la página sFlow Receiver Configuration para configurar el receptor sFlow.

Para configurar un receptor sFlow:

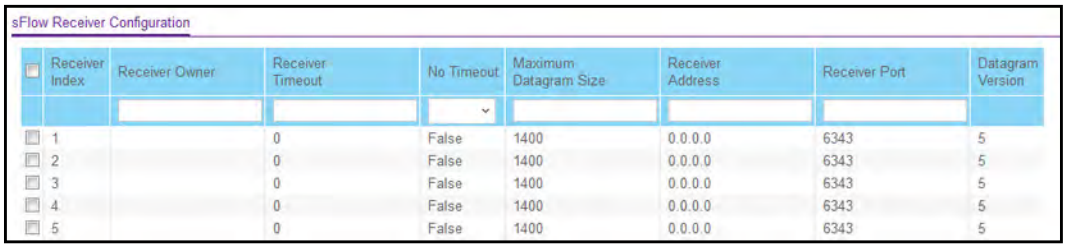
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring> sFlow > Advanced > sFlow Receiver Configuration.



5. Junto a la columna Receiver Index, seleccione la casilla del receptor cuyos datos se mostrarán o configurarán.

El rango permitido es de 1 a 8.
6. En el campo Receiver Owner, especifique el propietario del receptor.

Es la entidad que usa esta entrada de sFlowRcvrTable. Una cadena vacía indica que la entrada no está reclamada y la configuración del receptor se restablece a los valores predeterminados. Una entidad que desee reclamar una entrada de sFlowRcvrTable debe asegurarse de que no esté reclamada antes de intentarlo. La entrada se reclama estableciendo la cadena de propietario. La entrada debe reclamarse antes de poder modificar otros objetos del sampler.

7. En el campo Receiver Timeout, especifique el tiempo (en segundos) restante antes de que el sampler se libere y deje de muestrear.

Una entidad de administración que desee mantener el control del sampler debe establecer un nuevo valor antes de que venza el anterior. El rango válido es de 0 a 2147483647. Un valor de cero significa básicamente que el receptor no está configurado y restablece la configuración del receptor seleccionado a sus valores predeterminados. Al configurar los ajustes del receptor sFlow, debe seleccionar la opción Timeout Mode antes de configurar un Timeout Value.

8. En el menú No Timeout, seleccione True o False para establecer el muestreo sin tiempo de espera del receptor.

El muestreo no se detiene mientras la entrada seleccionada de No Timeout sea True. El valor predeterminado es False.

9. En el campo Maximum Datagram Size, especifique el número máximo de bytes de datos que pueden enviarse en un solo datagrama de muestra.

Establezca este valor para evitar la fragmentación de los datagramas sFlow. El valor predeterminado es 1400. El rango permitido es de 200 a 12188.

10. En el campo Receiver Address, especifique la dirección IP del colector sFlow. Si se establece en 0.0.0.0, no se envían datagramas sFlow.
11. En el campo Receiver Port, especifique el puerto de destino de los datagramas sFlow. El rango permitido es de 1 a 65535.
12. El campo Receiver Datagram Version muestra la versión de los datagramas sFlow que se enviarán.
13. Haga clic en el botón Aplicar (Apply).
La configuración se guarda.

Configurar la interfaz sFlow

El agente sFlow recopila muestras estadísticas basadas en paquetes de los flujos conmutados y las envía a los receptores configurados. Una fuente de datos configurada para recopilar muestras de flujo se llama sampler. El agente sFlow también recopila muestras basadas en tiempo de las estadísticas de las interfaces de red y las envía a los receptores sFlow configurados. Una fuente de datos configurada para recopilar muestras de contadores se llama poller.

Para configurar la interfaz sFlow:

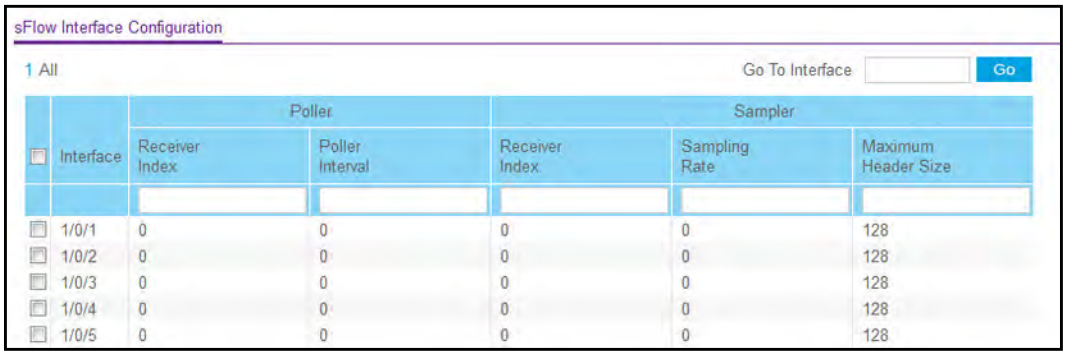
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Monitoring> sFlow > Advanced > sFlow Interface Configuration.



5. Use uno de los siguientes métodos para seleccionar una interfaz para el poller y el sampler de flujo:
   - 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, seleccione la casilla de la interfaz que desea usar.

Este agente solo admite puertos físicos.
6. Poller Receiver Index es el receptor sFlow asociado a este poller de contadores.

   Use Poller Receiver Index para especificar el receptor sFlow. El rango permitido es de 1 a 8. Si se establece en 0, la configuración del poller se restablece a la predeterminada y el poller se elimina.

7. Use Poller Interval para especificar el número máximo de segundos entre muestras sucesivas de los contadores asociados a esta fuente de datos.

Un intervalo de 0 deshabilita el muestreo de contadores. El rango permitido es de 0 a 86400 segundos.
8. Use Sampler Receiver Index para especificar el receptor sFlow de este sampler de flujo.

   Si se establece en 0, la configuración del sampler se restablece a la predeterminada y el sampler se elimina. Solo se pueden establecer receptores activos. Si un receptor vence, también vencen todos los samplers asociados al receptor. El rango permitido es de 1 a 8.

9. Use Sampling Rate para especificar la tasa de muestreo estadístico de paquetes de esta fuente.

   Una tasa de muestreo de 1 cuenta todos los paquetes. Una tasa de 0 deshabilita el muestreo. El rango permitido es de 1024 a 65536.

10. Use Maximum Header Size para especificar el número máximo de bytes que se copiarán de un paquete muestreado.

El rango permitido es de 20 a 256.
11. Haga clic en el botón Apply.
La configuración se guarda.

11

11Mantenimiento y solución de problemas

Este capítulo trata los siguientes temas:

- Guardar la configuración
- Configurar el modo de guardado automático
- Restablecer el switch a la configuración de fábrica
- Restablecer todas las contraseñas de usuario a sus valores predeterminados
- Cargar o exportar un archivo desde el switch
- Descargar o importar un archivo al switch
- Administrar los archivos de imagen de software
- Solución de problemas

Guardar la configuración

Al guardar la configuración, el switch conserva los cambios que realizó cuando se reinicia. Puede guardar la configuración manualmente o configurar el guardado automático.

Para guardar la configuración:

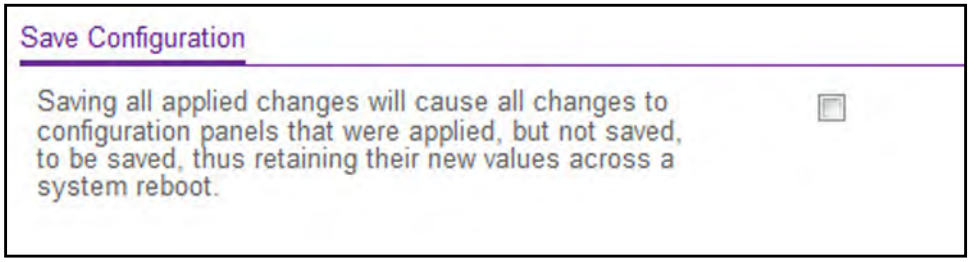
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Save Config > Save Configuration.



5. Seleccione la casilla.
6. Haga clic en el botón Aplicar (Apply).

La configuración se guarda.
Si reinicia el switch, la configuración guardada se conserva.

Configurar el modo de guardado automático

Para configurar el modo de guardado automático:

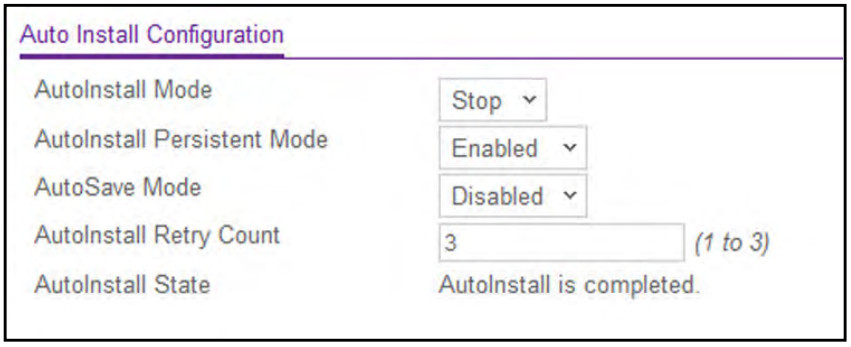
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > Save Config > Auto Install Configuration.



El campo Autoinstall State muestra el estado actual del proceso de Autoinstall.
5. En el menú AutoInstall Mode, seleccione iniciar/detener el modo de instalación automática en el switch.

6. En el menú AutoInstall Persistent Mode, habilite o deshabilite el modo persistente de AutoInstall.

7. En el menú AutoSave Mode, seleccione Enabled o Disabled.

8. En el menú AutoInstall Retry Count, especifique el número de intentos TFTP unicast que se realizan para el archivo especificado por DHCP antes de pasar a intentos TFTP broadcast.

9. Haga clic en el botón Apply.
La configuración se guarda.
Si reinicia el switch, la configuración guardada se conserva.

Restablecer el switch a la configuración de fábrica

Nota: Si restablece el switch a la configuración predeterminada, la dirección IP se restablece a 169.254.100.100 y el cliente DHCP se habilita. La dirección IP del puerto OOB se establece en 192.168.0.239.

Para restablecer el switch a los ajustes predeterminados de fábrica:

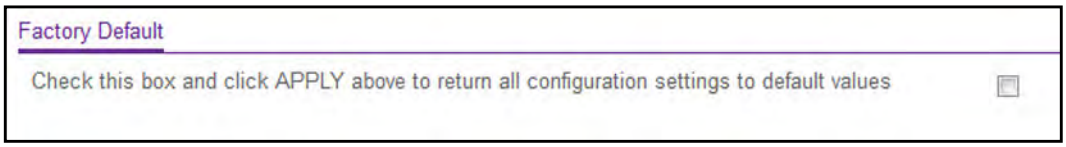
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Reset > Factory Default.



5. Seleccione la casilla.
6. Haga clic en el botón Aplicar (Apply).
Se abre una ventana emergente de confirmación.
7. Haga clic en Yes para confirmar.
Todos los parámetros de configuración se restablecen a sus valores de fábrica. Todos los cambios que realizó se pierden, aunque los haya guardado.

Restablecer todas las contraseñas de usuario a sus valores predeterminados

Para restablecer todas las contraseñas de usuario a sus valores predeterminados:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Reset > Password Reset.



5. Seleccione la casilla.

6. Haga clic en el botón Aplicar (Apply).
Todas las contraseñas de usuario se restablecen a sus valores de fábrica.

Cargar o exportar un archivo desde el switch

Puede cargar archivos de configuración (ASCII), de registro (ASCII) y de imagen (binarios) desde el switch al servidor TFTP.

Cargar un archivo al servidor TFTP

Para cargar un archivo desde el switch al servidor TFTP:

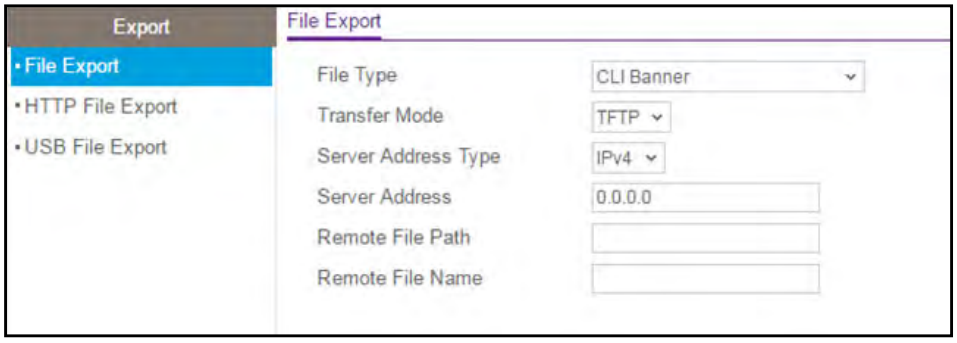
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Export > File Export.



5. Use File Type para especificar el tipo de archivo que se cargará:
   - CLI Banner. Especifique CLI Banner para obtener el archivo de banner de la CLI.
   - Text Configuration. Especifique la configuración en modo texto para obtener la configuración almacenada.
   - Script File. Especifique Script file para obtener la configuración almacenada.
   - Error Log. Especifique Error log para obtener el registro de errores del sistema (persistente), también llamado registro de eventos.
   - Trap Log. Especifique Trap log para obtener los registros de traps del sistema.

- Buffered Log. Especifique Buffered Log para obtener el registro en búfer (en memoria) del sistema.
- Tech Support. Especifique Tech Support para obtener la información del switch necesaria para la solución de problemas.
- Crash Logs. Especifique Crash Log para obtener los registros de fallos.
- Backup Configuration. Especifique Backup Configuration en modo texto para obtener la configuración de respaldo almacenada.
- CPU Packets Capture File. Especifique CPU Packets Capture File para obtener los paquetes de CPU capturados almacenados.
- Factory Default Configuration. Especifique Factory Default Configuration en modo texto para obtener la configuración de fábrica almacenada.

El valor de fábrica es CLI Banner.

6. Use Transfer Mode para especificar el protocolo que se usará para transferir el archivo:

- TFTP. Trivial File Transfer Protocol
- **SFTP**. Secure File Transfer Protocol
- **SCP**. Secure Copy Protocol
- **FTP**. File Transfer Protocol

7. Use Server Address Type para especificar IPv4, IPv6 o DNS e indicar el formato del campo Server Address. El valor de fábrica es IPv4.

8. Use Server Address para introducir la dirección IP del servidor según el formato indicado por el tipo de dirección del servidor.

El valor predeterminado de fábrica es la dirección IPv4 0.0.0.0.
9. Use Remote File Path para introducir la ruta para cargar el archivo.

La ruta solo puede incluir letras, números, barras diagonales, puntos o guiones bajos. Puede introducir hasta 160 caracteres. El valor de fábrica es vacío.

10. Use Remote File Name para introducir el nombre del archivo que se descargará del servidor. Puede introducir hasta 32 caracteres.

El valor de fábrica es vacío.
11. Use Local File Name para especificar el nombre del archivo de script local que se cargará.

Nota: Este campo solo es visible cuando File Type es Script File.

12. Use User Name para introducir el nombre de usuario para el inicio de sesión remoto en el servidor SFTP/SCP al que se envía el archivo.

Nota: Este campo solo es visible cuando se selecciona el modo de transferencia SFTP o SCP.

13. Use Password para introducir la contraseña para el inicio de sesión remoto en el servidor SFTP/SCP al que se envía el archivo.

Nota: Este campo solo es visible cuando se selecciona el modo de transferencia SFTP o SCP.

14. Haga clic en el botón Aplicar (Apply).

Se carga el archivo. La última fila de la tabla muestra información sobre el progreso de la transferencia.

Cargar un archivo mediante HTTP

Para usar la carga de archivos por HTTP:

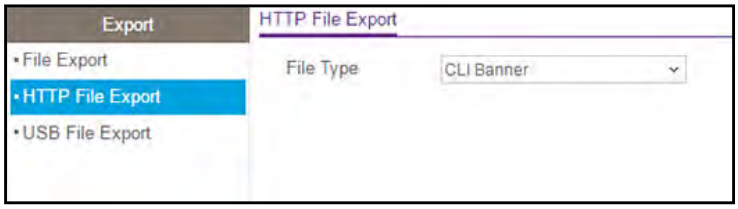
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > Export > HTTP File Export.



5. Use File Type para especificar el tipo de archivo que se cargará:
   - CLI Banner. Especifique CLI Banner para obtener el archivo de banner de la CLI.
   - Text Configuration. Especifique la configuración en modo texto para obtener la configuración almacenada.
   - Script File. Especifique Script file para obtener la configuración almacenada.
   - Error Log. Especifique Error log para obtener el registro de errores del sistema (persistente), también llamado registro de eventos.
   - Trap Log. Especifique Trap log para obtener los registros de traps del sistema.
   - Buffered Log. Especifique buffered log para obtener el registro en búfer (en memoria) del sistema.
   - Tech Support. Especifique Tech Support para obtener la información del switch necesaria para la solución de problemas.
   - Crash Logs. Especifique Crash Logs para obtener los registros de fallos del sistema.
   - Backup Configuration. Especifique Backup Configuration en modo texto para obtener la configuración de respaldo almacenada.

- CPU Packets Capture File. Especifique CPU Packets Capture File para obtener los paquetes de CPU capturados almacenados.
- Factory Default Configuration. Especifique Factory Default Configuration en modo texto para obtener la configuración de fábrica almacenada.

El valor de fábrica es CLI Banner.
6. Haga clic en el botón Aplicar
(Apply).
Se carga el archivo.

Cargar un archivo desde el switch a un dispositivo USB

Para cargar un archivo desde el switch a un dispositivo USB:

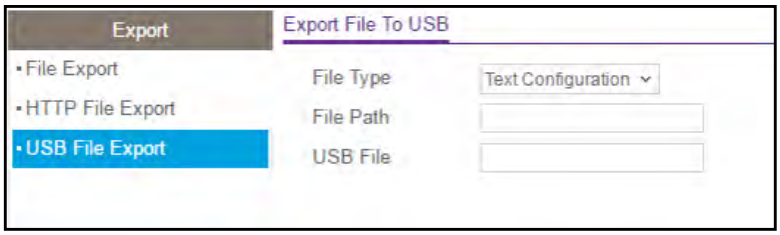
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Export > USB File Export.



De forma predeterminada, la selección del menú File Type es Text Configuration. La configuración almacenada que se obtendrá está en modo texto.

5. En el campo File Path, introduzca la ruta del archivo que se cargará. Puede usar hasta 146 caracteres. El valor predeterminado es vacío.
6. Use USB File para asignar un nombre y una ruta al archivo que se cargará. Puede ingresar hasta 32 caracteres. El valor predeterminado de fábrica es en blanco.
7. Haga clic en el botón Apply.
Se carga el archivo.

Descargar o importar un archivo al switch

El switch admite la descarga de archivos del sistema desde un sistema remoto al switch mediante TFTP o HTTP.

Descargar un archivo

Para poder descargar archivos de claves SSH, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.

Para poder descargar archivos relacionados con SSL, HTTPS debe estar deshabilitado administrativamente.

Para descargar un archivo:

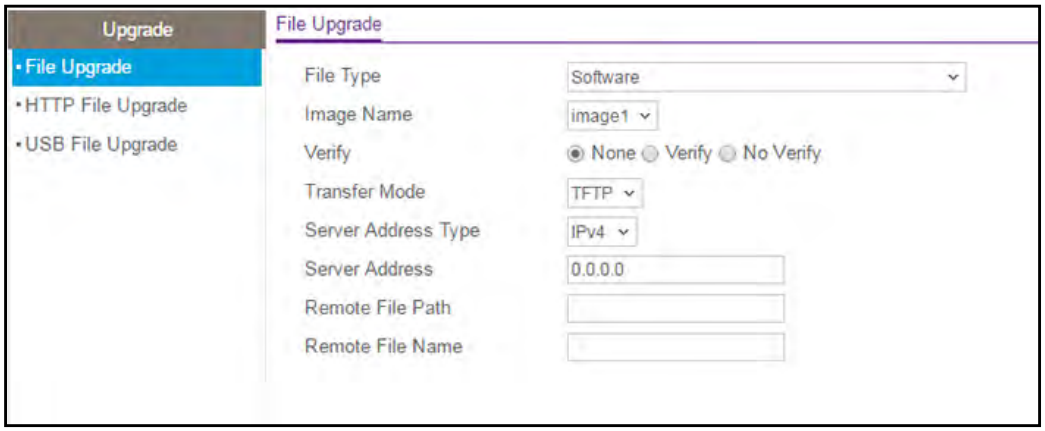
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Upgrade > File Upgrade.



5. Use File Type para especificar el tipo de archivo que se transferirá al dispositivo.
   - Software. Seleccione esta opción para transferir el código de software del dispositivo y actualizar la memoria flash operativa.
   - Text Configuration. Seleccione esta opción para transferir al dispositivo la configuración en modo texto y actualizar la configuración del switch. Si el archivo tiene errores, la actualización se detiene.

- SSH-2 RSA Key PEM File. Seleccione esta opción para transferir al dispositivo un archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (codificado en PEM).
- SSH-2 DSA Key PEM File. Seleccione esta opción para transferir al dispositivo un archivo de clave SSH-2 Digital Signature Algorithm (DSA) (codificado en PEM).
- SSL Trusted Root Certificate PEM File. Seleccione esta opción para transferir al dispositivo un archivo de certificado raíz de confianza SSL (codificado en PEM). Los archivos SSL contienen información para cifrar, autenticar y validar las sesiones HTTPS.
- Use SSL Server Certificate PEM File. Seleccione esta opción para transferir al dispositivo un archivo de certificado de servidor SSL (codificado en PEM).
- Use SSL DH Weak Encryption Parameter PEM File. Seleccione esta opción para transferir al dispositivo un archivo de parámetros de cifrado débil Diffie-Hellman SSL (codificado en PEM).
- Use SSL DH Strong Encryption Parameter PEM File. Seleccione esta opción para transferir al dispositivo un archivo de parámetros de cifrado fuerte Diffie-Hellman SSL (codificado en PEM).
- Script File. Seleccione esta opción para transferir al dispositivo un archivo de script de configuración basado en texto. Debe usar la interfaz de línea de comandos (CLI) para validar y activar el script.
- CLI Banner. Seleccione esta opción para transferir el banner de la CLI al dispositivo. Este archivo contiene el texto que se muestra en la CLI antes del indicador de inicio de sesión.
- IAS Users. Seleccione esta opción para transferir al dispositivo un 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. Seleccione esta opción para transferir el archivo de configuración de fábrica a un sistema remoto.
- Public Key Configuration. Seleccione esta opción para transferir al dispositivo el archivo de clave pública usado para validar los scripts de configuración.
- Public Key Image. Seleccione esta opción para transferir al dispositivo el archivo de clave pública usado para validar la imagen de código.
- Application. Seleccione esta opción para transferir una aplicación al dispositivo.
- Tech Support Commands File. Seleccione esta opción para transferir un archivo de comandos de soporte técnico al dispositivo.

El valor de fábrica es Software.

6. El campo Image Name solo es visible cuando se selecciona File Type Software. Use Image Name para seleccionar una de las imágenes de la lista:
   - Image1. Especifique la imagen de código image1 que se obtendrá.
   - Image2. Especifique la imagen de código image2 que se obtendrá.

7. El campo Verify está visible cuando se selecciona File Type Software y Script File. Seleccione una de las opciones de Verify: None, Verify, No Verify respecto a la transferencia en el código de software del dispositivo.

8. El campo Application File Name está visible cuando se selecciona File Type Application. Ingrese el nombre del archivo de aplicación que se descargará al dispositivo.

9. Use Transfer Mode para especificar el protocolo de transferencia del archivo:

- TFTP. Trivial File Transfer Protocol
- **SFTP**. Secure File Transfer Protocol
- **SCP**. Secure Copy Protocol
- **FTP**. File Transfer Protocol

10. Use Server Address Type para especificar IPv4, IPv6 o DNS e indicar el formato del campo TFTP/SFTP/SCP Server Address.

El valor predeterminado de fábrica es IPv4.

11. Use Server Address para ingresar la dirección IP del servidor TFTP según el formato indicado por el tipo de dirección del servidor, por ejemplo, una dirección IP en formato x.x.x.x.

El valor predeterminado de fábrica es la dirección IPv4 0.0.0.0.
12. Use Remote File Path para ingresar la ruta del archivo que se descargará.

La ruta del archivo no puede incluir los siguientes símbolos: ' \:*?”<>| '. Se pueden ingresar hasta 160 caracteres. El valor predeterminado de fábrica es en blanco.

13. Use Remote File Name para ingresar el nombre del archivo que se descargará del servidor.

La ruta del archivo no puede incluir los siguientes símbolos: ' \:*?”<>| '. Puede ingresar hasta 32 caracteres. El valor predeterminado de fábrica es en blanco.

14. Use User Name para ingresar el nombre de usuario para el inicio de sesión remoto en el servidor SFTP/SCP donde se encuentra el archivo.

Nota: Este campo solo es visible cuando se selecciona el modo de transferencia SFTP o SCP.

15. Use Password para ingresar la contraseña para el inicio de sesión remoto en el servidor SFTP/SCP donde se encuentra el archivo.

Nota: Este campo solo está visible cuando el modo de transferencia\ SFTP o SCP está SFTP o SCP.

16. Haga clic en el botón Apply.

El archivo se descarga. La última fila de la tabla muestra información sobre el progreso de la transferencia. Solo se muestra después de que inicia el proceso. La página se actualiza automáticamente hasta que finaliza la transferencia del archivo.

Descargar un archivo al switch mediante HTTP

Puede descargar archivos de varios tipos al switch mediante una sesión HTTP (por ejemplo, a través de su navegador web).

Para poder descargar archivos de claves SSH, SSH debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.

Para poder descargar archivos PEM de SSL, SSL debe estar deshabilitado administrativamente y no debe haber sesiones SSH activas.

Para descargar un archivo al switch mediante HTTP:

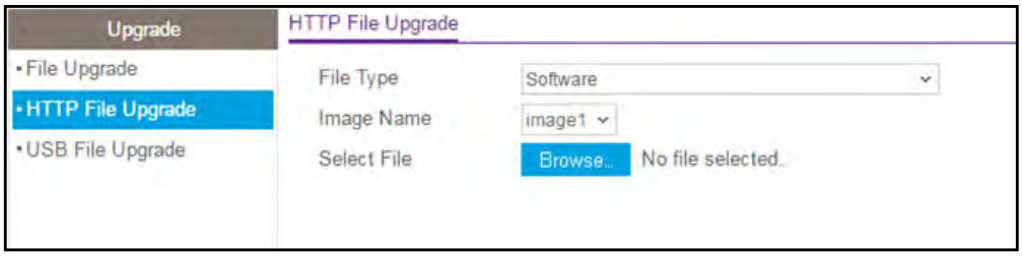
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Upgrade > HTTP File Upgrade.



5. Use File Type para especificar el tipo de archivo que se transferirá:
   - Software. Código de software para actualizar la memoria flash operativa.
   - Text Configuration. Configuración en modo de texto para actualizar la configuración del switch. Si el archivo tiene errores, la actualización se detiene.
   - Use SSH-2 RSA Key PEM File para especificar el archivo de clave SSH-2 Rivest-Shamir-Adelman (RSA) (codificado en PEM).
   - Use SSH-2 DSA Key PEM File para especificar el archivo de clave SSH-2 Digital Signature Algorithm (DSA) (codificado en PEM).
   - Use SSL Trusted Root Certificate PEM File para especificar el archivo de certificado raíz de confianza SSL (codificado en PEM).
   - Use SSL Server Certificate PEM File para especificar el archivo de certificado de servidor SSL (codificado en PEM).
   - Use SSL DH Weak Encryption Parameter PEM File para especificar el archivo de parámetros de cifrado débil Diffie-Hellman de SSL (codificado en PEM).
   - Use SSL DH Strong Encryption Parameter PEM File para especificar el archivo de parámetros de cifrado fuerte Diffie-Hellman de SSL (codificado en PEM).
   - Use Config Script para especificar el archivo de configuración de script.
   - CLI Banner. Especifique CLI Banner si se mostrará un banner antes del indicador de inicio de sesión.
   - Use IAS Users para especificar el archivo de base de datos de usuarios del servidor de autenticación interno.

   El valor de fábrica es Software.

6. El campo Image Name solo está visible cuando se selecciona File Type Software. Use Image Name para seleccionar una de las imágenes de la lista:
   - Image1. Especifica la imagen de código image1 que se descargará.
   - Image2. Especifica la imagen de código image2 que se descargará.

7. Junto a Select File, haga clic en el botón Browse y navegue hasta el archivo que se descargará. Puede seleccionar un archivo de hasta 80 caracteres.
8. Haga clic en el botón Apply (Aplicar).
La descarga comienza.
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 queda en blanco. Esto indica que la transferencia del archivo terminó.

Descargar un archivo desde un dispositivo USB

Para descargar un archivo desde un dispositivo USB:

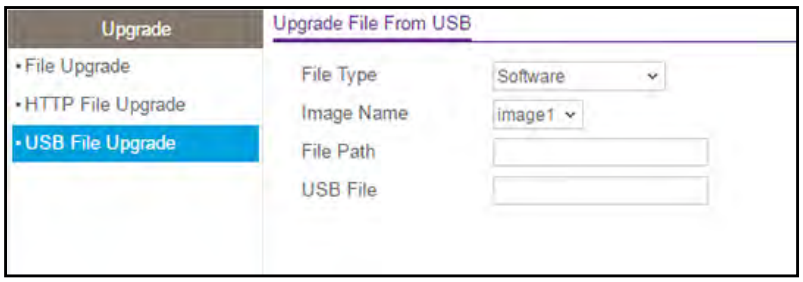
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Upgrade> USB File Upgrade.



5. Use File Type para especificar el tipo de archivo que se descargará:
   - Software. Código de software que se descargará a la memoria flash operativa.
   - Text Configuration. Configuración en modo de texto para actualizar la configuración del switch (Startup-config).

Si el archivo tiene errores, la actualización se detiene. El valor predeterminado de fábrica es Software.

6. Use Image Name para seleccionar una de las imágenes de la lista:

- Image1. Seleccione image1 para descargar a image1.
- Image2. Seleccione image2 para descargar a image2.

El campo Image Name solo está visible cuando se selecciona File Type Software.
7. Use el campo File Path para indicar la ruta del archivo que se descargará. Puede ingresar hasta 146 caracteres. El valor predeterminado es en blanco.
8. Use USB File para indicar el nombre y la ruta del archivo que se descargará. Puede ingresar hasta 32 caracteres. El valor predeterminado de fábrica es en blanco.
9. Haga clic en el botón Apply.

La descarga comienza. El campo Download Status muestra el estado de la transferencia del archivo al switch. La última fila de la tabla muestra información sobre el progreso de la transferencia. Solo se muestra después de que inicia el proceso. La página se actualiza automáticamente hasta que finaliza la transferencia del archivo.

Administrar archivos de imagen de software

El sistema mantiene dos versiones de la imagen de software del switch en almacenamiento permanente. Una es la imagen activa y la otra es la imagen de respaldo. La imagen activa se carga en los reinicios posteriores del switch. Esta función reduce el tiempo de inactividad del switch al actualizar o revertir el software del switch.

Copiar una imagen

Para copiar una imagen:

1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > File Management > Copy.



5. Use Source Image para seleccionar image1 o image2 como imagen de origen (la imagen que se copiará).
6. Use Switch Member para seleccionar la unidad de destino a la que copiará desde el supervisor.
7. Use Destination Image para seleccionar image1 o image2 como imagen de destino.
8. Haga clic en el botón Apply (Aplicar).
La imagen se copia.

Configurar los ajustes de imagen dual

La función Dual Image permite que el switch conserve dos imágenes en almacenamiento permanente. El administrador puede designar image1 o image2 como la imagen activa que se cargará en los reinicios posteriores del switch. Esta función reduce el tiempo de inactividad del switch al actualizar o revertir la imagen de software.

Para configurar los ajustes de imagen dual:

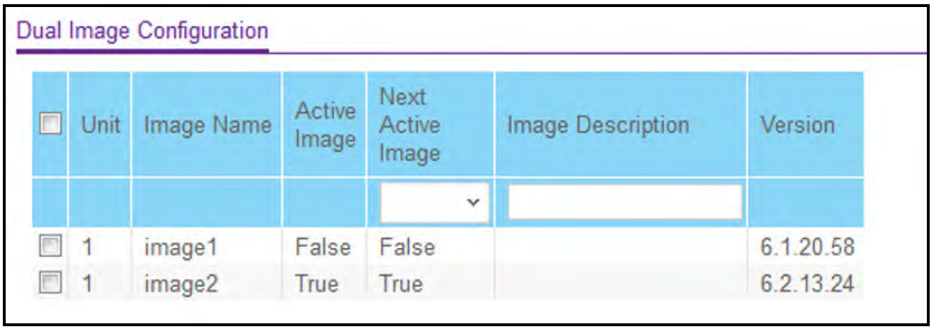
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > File Management > Dual Image Configuration.



5. Use Unit para seleccionar el ID de la unidad cuya imagen de código desea activar, actualizar o eliminar.
6. Use Next Active Image para que la imagen seleccionada sea la próxima imagen activa en los reinicios posteriores de esta unidad.
7. Use Image Description para especificar la descripción de la imagen seleccionada.
8. Haga clic en el botón Apply (Aplicar).

La configuración se guarda.

Nota: Después de activar una imagen, debe realizar un restablecimiento del sistema del switch para ejecutar la nueva imagen.

La siguiente tabla describe la información no configurable que se muestra en la página.

Tabla 230. Dual Image Configuration

Campo	Descripción
Image Name	Muestra el nombre de la imagen de la unidad seleccionada.
Active Image	La imagen activa actual de la unidad seleccionada.
Version	La versión del archivo de código image1.

Solución de problemas

Puede enviar un ping, rastrear una ruta y realizar un volcado de memoria.

Hacer ping a una dirección IPv4

Puede indicar al switch que envíe una solicitud de ping a una dirección IP especificada para comprobar si el switch puede comunicarse con una estación IP en particular. Al hacer clic en el botón Apply, el switch envía el número especificado de solicitudes de ping y se muestran los resultados.

Si no se recibe respuesta al ping, aparece el siguiente mensaje:

```
Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec
```

Si se recibe una respuesta al ping, aparece el siguiente mensaje:

```
Reply From a.b.c.d: icmp_seq = 0. time= xyz usec.
Reply From a.b.c.d: icmp_seq = 1. time= abc usec.
Reply From a.b.c.d: icmp_seq = 2. time= def usec.
Tx = count, Rx = count Min/Max/Avg RTT = xyz/abc/def msec
```

Para configurar los ajustes y hacer ping a un host de la red:

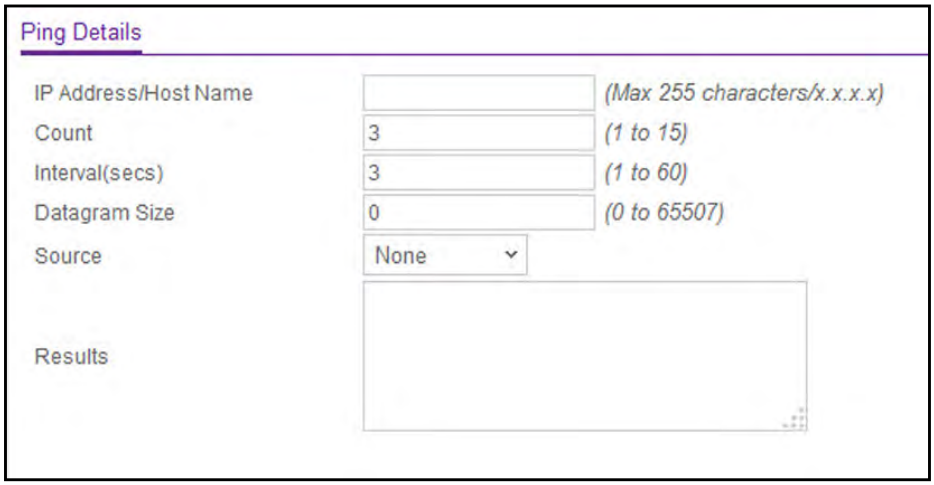
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Troubleshooting > Ping IPv4.



5. Use IP Address/Host Name para ingresar la dirección IP o el nombre de host de la estación a la que el switch hará ping.

El valor inicial es en blanco.
6. En el campo Count, ingrese el número de solicitudes de eco que se enviarán. El valor predeterminado es 3. El rango es de 1 a 15.
7. Ingrese el Interval entre paquetes de ping en segundos. El valor predeterminado es 3 segundos. El rango es de 1 a 60.

8. Ingrese el Datagram Size del paquete de ping.
El valor predeterminado es 0 bytes. El rango es de 0 a 65507.
9. Ingrese la dirección IP o interfaz Source que se usará al enviar los paquetes de solicitud de eco.

Si no se requiere un origen, seleccione None como opción de origen. Los valores posibles son los siguientes:

- None. La dirección de origen del paquete de ping será la dirección de la interfaz de salida predeterminada.
- IP Address. La dirección IP de origen que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona IP Address como opción de origen.
- Interface. La interfaz que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona Interface como opción de origen.

Nota: Los valores configurados en los campos de esta página no se guardan en el switch. Por lo tanto, al actualizar la página, estos campos vuelven a sus valores predeterminados.

10. Haga clic en el botón Aplicar (Apply).

Los pings se envían a la dirección especificada. El switch envía el número de pings especificado en el campo Count y los resultados se muestran debajo de los datos configurables, en el área Results.

Hacer ping a una dirección IPv6

Esta página se usa para enviar una solicitud de ping a un nombre de host o dirección IPv6 especificados. Puede usarla para comprobar si el switch puede comunicarse con una estación IPv6 en particular. Al hacer clic en el botón Apply, el switch envía el número especificado de solicitudes de ping y los resultados se muestran debajo de los datos configurables. La salida muestra lo siguiente:

```
Send count=n, Receive count=n from (IPv6 Address). Average round trip
time = n ms.
```

Para usar Ping IPv6:

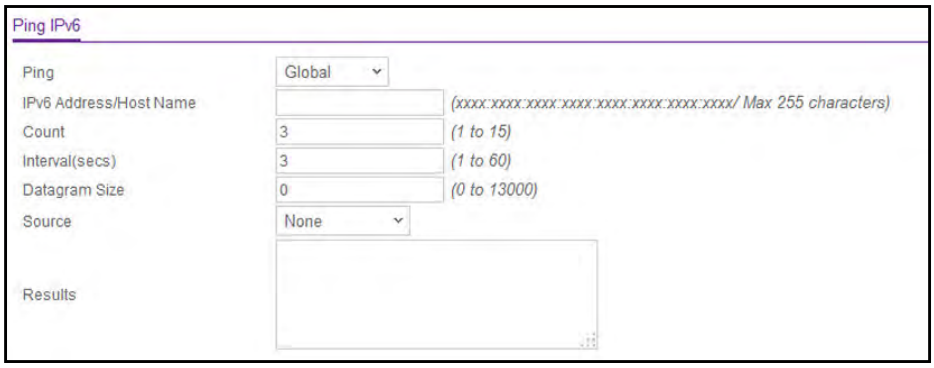
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > Troubleshooting > Ping IPv6.



5. Seleccione el tipo de Ping en la lista.
Los valores posibles son los siguientes:

- Global. Hace ping a una dirección IPv6 global.
- Link Local. Hace ping a una dirección IPv6 link-local a través de la interfaz especificada. Este campo se muestra cuando se selecciona Interface como opción de ping.

6. Use IPv6 Address/Hostname para ingresar la dirección IPv6 o el nombre de host de la estación a la que el switch hará ping.

El valor inicial es en blanco. El formato es xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. El número máximo de caracteres es 255.

7. Use Count para ingresar el número de solicitudes de eco que se enviarán.
El rango es de 1 a 15. El valor predeterminado es 3.
8. Ingrese el Interval en segundos entre paquetes de ping.
El rango es de 1 a 60. El valor predeterminado es 3.
9. Use Datagram Size para ingresar el tamaño del datagrama.
El rango válido es de 0 a 13000. El valor predeterminado es 0 bytes.
10. Ingrese la dirección IP o interfaz Source que se usará al enviar los paquetes de solicitud de eco.

Si no se requiere un origen, seleccione None como opción de origen. Los valores posibles son los siguientes:

- None. La dirección de origen del paquete de ping será la dirección de la interfaz de salida predeterminada.
- IPv6 Address. La dirección IPv6 de origen que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona IPv6 Address como opción de origen.
- Interface. La interfaz que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona Interface como opción de origen.

Nota: Los valores configurados en los campos de esta página no se guardan en el switch. Por lo tanto, al actualizar la página, estos campos vuelven a sus valores predeterminados.

11. Haga clic en el botón Apply.

Los pings se envían a la dirección IPv6 o al nombre de host especificados. El switch envía el número de pings especificado en el campo Count y los resultados se muestran debajo de los datos configurables, en el área Results.

Enviar un traceroute a una dirección IPv4

Use esta página para indicar al switch que envíe una solicitud de traceroute a una dirección IP o nombre de host especificados. Puede usarla para descubrir las rutas que siguen los paquetes hacia un destino remoto. Al hacer clic en el botón Apply, el switch envía el traceroute y los resultados se muestran debajo de los datos configurables.

Si se recibe una respuesta al traceroute, aparece el siguiente mensaje:

```
1 e.f.g.h 9869 usec 9775 usec 10584 usec
2 0.0.0.0 0 usec * 0 usec * 0 usec *
3 0.0.0.0 0 usec * 0 usec * 0 usec *
Hop Count = j Last TTL = k Test attempt = m Test Success = n.
```

Para configurar los ajustes de traceroute y enviar paquetes de sondeo para descubrir la ruta a un host de la red:

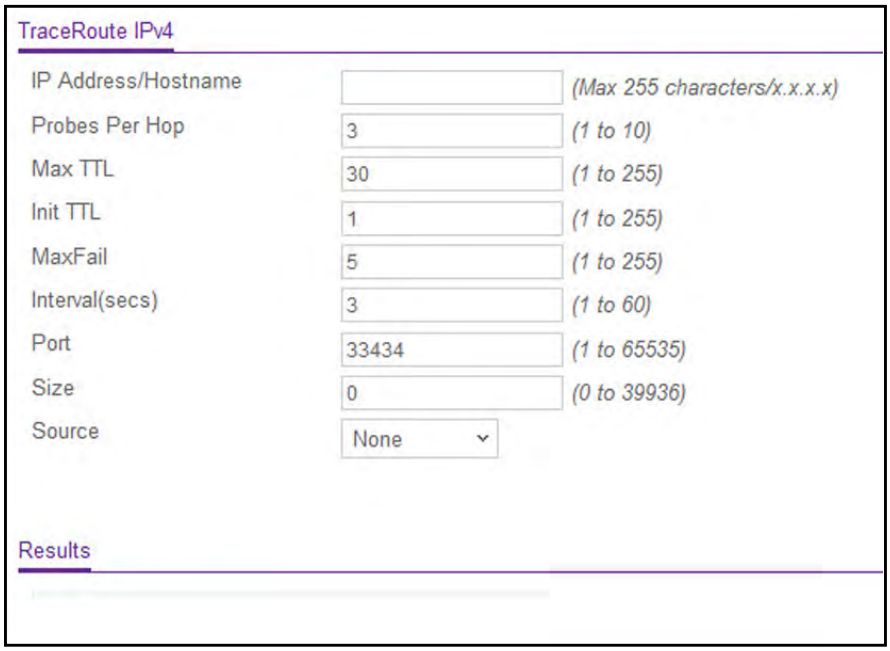
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

   Se muestra la página System Information.

4. Seleccione Maintenance > Troubleshooting > Traceroute IPv4.



5. Use IP Address/Hostname para ingresar la dirección IP o el nombre de host de la estación hacia la que desea descubrir una ruta.

El valor predeterminado es en blanco.
6. Ingrese el número de Probes Per Hop. El valor predeterminado es 3. El rango es de 1 a 10.
7. Ingrese el Maximum TTL para el destino. El valor predeterminado es 30. El rango es de 1 a 255.

8. Ingrese el Initial TTL que se usará.

El valor predeterminado es 1. El rango es de 1 a 255.
9. Ingrese el Maximum Failures permitido en la sesión.
El valor predeterminado es 5. El rango es de 1 a 255.
10. Interval (secs). Ingrese el tiempo entre sondeos en segundos.
El valor predeterminado es 3. El rango es de 1 a 60.
11. Ingrese el UDP Destination Port en los paquetes de sondeo.
El valor predeterminado es 33434. El rango es de 1 a 65535.
12. Ingrese el Size de los paquetes de sondeo.
El valor predeterminado es 0. El rango es de 0 a 39936.
13. Ingrese la dirección IP o interfaz Source que se usará al enviar los paquetes de solicitud de eco.

Si no se requiere un origen, seleccione None como opción de origen. Los valores posibles son los siguientes:

- None. La dirección de origen del paquete de ping será la dirección de la interfaz de salida predeterminada.
- IP Address. La dirección IP de origen que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona IP Address como opción de origen.
- Interface. La interfaz que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona Interface como opción de origen.

Nota: Los valores configurados en los campos de esta página no se guardan en el switch. Por lo tanto, al actualizar la página, estos campos vuelven a sus valores predeterminados.

14. Haga clic en el botón Aplicar (Apply).
Se envía una solicitud de traceroute a la dirección IP o nombre de host especificados. Los resultados se muestran debajo de los datos configurables, en el área TraceRoute Results.

El campo Results muestra el resultado del traceroute IPv4 después de que el switch envía una solicitud de traceroute a la dirección IP o nombre de host especificados.

Enviar un traceroute a una dirección IPv6

Use esta página para indicar al switch que envíe una solicitud de traceroute a una dirección IPv6 o nombre de host especificados. Puede usarla para descubrir las rutas que siguen los paquetes hacia un destino remoto. Al hacer clic en el botón Apply, el switch envía un traceroute y los resultados se muestran debajo de los datos configurables.

Si se recibe una respuesta al traceroute, aparece el siguiente mensaje:

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = p Last TTL = q Test attempt = r Test Success = s.
```

Para usar traceroute IPv6:

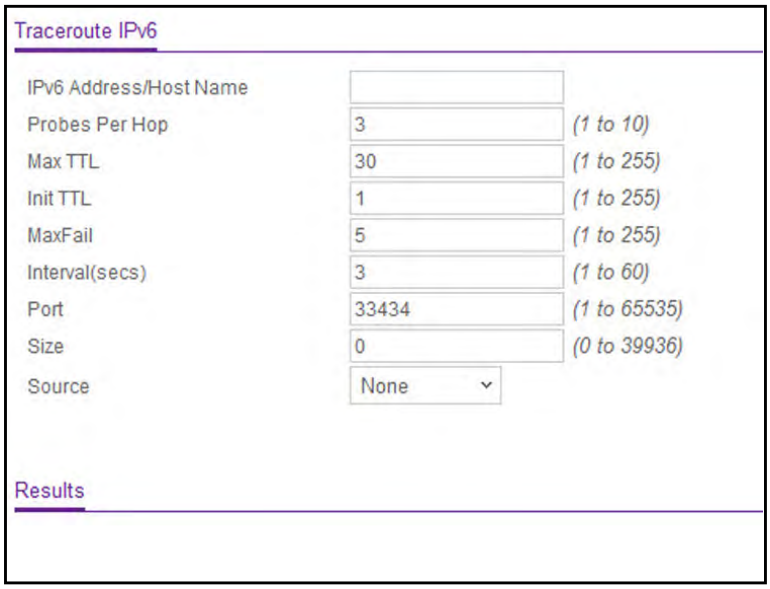
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > Troubleshooting > Traceroute IPv6.



5. En el campo IPv6 Address/Hostname, ingrese la dirección IPv6 o el nombre de host de la estación hacia la que desea que el switch descubra una ruta.

   El valor inicial es en blanco. La dirección IPv6 o el nombre de host que ingrese no se conserva tras un ciclo de encendido.

6. Ingrese el valor de Probes Per Hop.

El valor predeterminado es 3. El rango es de 1 a 10.
7. Ingrese el Maximum TTL para el destino.

   El valor predeterminado es 30. El rango es de 1 a 255. El MaxTTL que ingrese no se conserva tras un ciclo de encendido.

8. Ingrese el Initial TTL que se usará.

   El valor predeterminado es 1. El rango es de 1 a 255. El InitTTL que ingrese no se conserva tras un ciclo de encendido.

9. Ingrese el Maximum Failures permitido en la sesión.

   El valor predeterminado es 5. El rango es de 1 a 255. El MaxFail que ingrese no se conserva tras un ciclo de encendido.

10. Interval (secs): ingrese el tiempo entre sondeos en segundos.

    El valor predeterminado es 3. El rango es de 1 a 60. El intervalo que ingrese no se conserva tras un ciclo de encendido.

11. Ingrese el UDP Destination Port en los paquetes de sondeo.

    El valor predeterminado es 33434. El rango es de 1 a 65535. El puerto que ingrese no se conserva tras un ciclo de encendido.

12. Ingrese el Size de los paquetes de sondeo.

El valor predeterminado es 0. El rango es de 0 a 39936. El tamaño que ingrese no se conserva tras un ciclo de encendido.

13. Ingrese la dirección IP o interfaz Source que se usará al enviar los paquetes de solicitud de eco.

Si no se requiere un origen, seleccione None como opción de origen. Los valores posibles son los siguientes:

- None. La dirección de origen del paquete de ping será la dirección de la interfaz de salida predeterminada.
- IP Address. La dirección IP de origen que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona IP Address como opción de origen.
- Interface. La interfaz que se usará al enviar los paquetes de solicitud de eco. Este campo se muestra cuando se selecciona Interface como opción de origen.

Nota: Los valores configurados en los campos de esta página no se guardan en el switch. Por lo tanto, al actualizar la página, estos campos vuelven a sus valores predeterminados.

14. Haga clic en el botón Aplicar (Apply).
El traceroute comienza. Los resultados se muestran en el área TraceRoute.

El campo Results muestra el resultado del traceroute IPv6 después de que el switch envía una solicitud de traceroute a la dirección IP o nombre de host especificados.

Capturar paquetes

Puede capturar y almacenar paquetes en un dispositivo de almacenamiento flash USB.

Para iniciar la captura de paquetes:

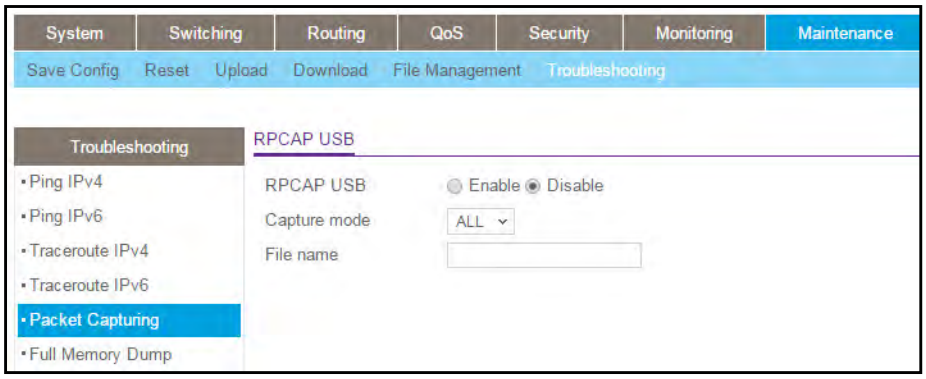
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > Troubleshooting > Packet Capturing.



5. Junto a RPCAP USB, seleccione el botón de opción Enable.
6. En el menú Capture Mode, seleccione el tipo de tráfico de CPU:
   - All. Captura todo el tráfico. Esta opción es la configuración predeterminada.
   - TX. Captura solo el tráfico transmitido.
   - RX. Captura solo el tráfico recibido.
7. En el campo File Name, ingrese el nombre del archivo USB.

   El nombre del archivo no puede incluir los siguientes símbolos: '\/:*?”<>|'. Puede ingresar hasta 64 caracteres, lo que se refiere solo a la longitud del nombre de archivo; es decir, la extensión se agrega automáticamente. El valor predeterminado de fábrica es en blanco.

8. Para iniciar el proceso de captura de paquetes, haga clic en el botón Apply. Los paquetes se capturan hasta que detenga el proceso.
9. Para detener el proceso de 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:

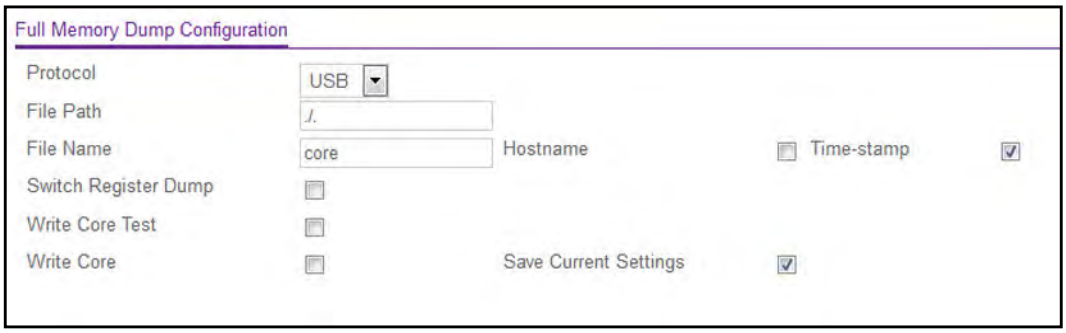
1. Abra un navegador web.
2. En el campo de dirección de su navegador web, escriba la dirección IP del switch. Se abre la ventana de inicio de sesión.

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

   La primera vez que inicie sesión, no se requiere contraseña. Sin embargo, después deberá especificar una contraseña local del dispositivo para usarla cada vez que inicie sesión.

Se muestra la página System Information.

4. Seleccione Maintenance > Troubleshooting > Full Memory Dump.



5. En el menú Protocol, seleccione el protocolo usado para almacenar el archivo de volcado de núcleo. Los valores posibles son los siguientes:

- None. Deshabilita el volcado de núcleo.
- TFTP. Establece el protocolo TFTP.
- NFS. Establece el protocolo NFS.
- USB. Establece el protocolo USB.

6. En el campo File Path, ingrese la ruta de la ubicación donde se almacenará el archivo de volcado de núcleo.
7. En el campo File Name, ingrese el nombre del archivo de volcado de núcleo.
8. Seleccione la opción Hostname para agregar el nombre de host al nombre del archivo de volcado de núcleo.
9. Seleccione la opción Time-stamp para agregar una marca de tiempo al nombre del archivo de volcado de núcleo.

10. Seleccione la opción Switch Register Dump para volcar los registros del chip del switch en caso de una excepción.

11. Seleccione la opción Write Core Test para probar la configuración del volcado de núcleo.

12. Seleccione la opción Write Core para crear un volcado de núcleo y almacenarlo en el servidor externo configurado previamente.

Al ejecutar este procedimiento, el dispositivo se recarga.
13. Seleccione la opción Save Current Settings para guardar la configuración actual del sistema.
14. Haga clic en el botón Aplicar (Apply).
El volcado de memoria se envía a la ubicación especificada.

A

AEjemplos de configuración

Este apéndice contiene información sobre cómo configurar las siguientes funciones:

- Redes de área local virtuales (VLAN)
- Listas de control de acceso (ACL)
- Servicios diferenciados (DiffServ)
- 802.1X
- MSTP

Redes de área local virtuales (VLAN)

Una red de área local (LAN) generalmente se puede definir como un dominio de broadcast. Hubs, bridges 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 con una definición que asigna estaciones de trabajo con un criterio distinto a 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 PC, 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, todo el personal de marketing podría estar repartido por un edificio. Sin embargo, si todos se asignan 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 accesibles 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 mayor frecuencia entre sí pueden agruparse en VLAN comunes, sin importar su ubicación física. El tráfico de cada grupo queda contenido 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 armario de cableado.
- Ofrecen mayor rendimiento. Las VLAN liberan ancho de banda al limitar el tráfico de nodo a nodo y de broadcast en toda la red.
- Garantizan una mayor seguridad de la red. Las VLAN crean límites virtuales que solo se pueden cruzar a través de un router. Así, se pueden usar las 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 a un puerto, se etiqueta automáticamente con el número de VLAN ID predeterminado del puerto. Cada puerto tiene un VLAN ID predeterminado configurable por el usuario (el valor predeterminado es 1). El VLAN ID predeterminado de cada puerto se puede cambiar en la página Port PVID Configuration. Consulte Configure Port PVID Settings en la página 192.
- Cuando un paquete etiquetado entra a un puerto, su etiqueta no se ve afectada por el VLAN ID predeterminado. El paquete continúa hacia la VLAN especificada por su número de VLAN ID.
- Si el puerto por el que entró 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, este puede enviarse a otros puertos con el mismo VLAN ID.

- Los paquetes que salen del switch van etiquetados o sin etiquetar, según la configuración de las propiedades de membresía de VLAN de ese puerto. Una U en un puerto significa que los paquetes que salen del switch por ese puerto van sin etiquetar. A la inversa, una T en un puerto significa que los paquetes que salen del switch por ese puerto van etiquetados con el VLAN ID asociado con el puerto.

El ejemplo de esta sección incluye numerosos pasos para ilustrar una amplia gama de configuraciones y 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 etiquetar.

En este ejemplo, se crean dos VLAN nuevas, se cambia la membresía de puertos de la VLAN predeterminada 1 y se asignan puertos miembro a las dos VLAN nuevas:

1. En la página Basic VLAN Configuration (consulte Configure VLANs en la página 182), cree las siguientes VLAN:
   - Una VLAN con VLAN ID 10.
   - Una VLAN con VLAN ID 20.
2. En la página VLAN Membership (consulte Configure VLAN Membership en la página 190), especifique la membresía de 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 Configure Port PVID Settings en la página 192), especifique el PVID de los puertos g1 y g4 para que los paquetes que entren por ellos se etiqueten con el VLAN ID del puerto:
   - Puerto g1: PVID 10
   - Puerto g4: PVID 20
4. Con la configuración de VLAN establecida, las siguientes situaciones producen los resultados descritos:
   - Si un paquete sin etiquetar entra por el puerto 1, el switch lo etiqueta con VLAN ID 10. El paquete tiene acceso al puerto 2 y al puerto 3. Al paquete saliente se le quita la etiqueta para salir por el puerto 2 como paquete sin etiquetar. En 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, tiene acceso al puerto 1 y al puerto 2. Si el paquete sale por el puerto 1 o 2, se le quita la etiqueta y sale del switch como paquete sin etiquetar.
   - Si un paquete sin etiquetar entra por el puerto 4, el switch lo etiqueta con VLAN ID 20. El paquete tiene acceso al puerto 5 y al puerto 6. Al paquete saliente se le quita la etiqueta y se convierte en

un paquete sin etiquetar al salir por el puerto 6. En 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 llegar 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. Las ACL 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 se realiza a velocidad de línea.

Las listas de acceso son una colección secuencial de condiciones de permiso y denegación. Esta colección de condiciones, conocida como criterios 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 coincide o no con los criterios especificados.

El filtrado de tráfico requiere los dos pasos básicos siguientes:

1. Cree una definición de lista de acceso.

   La definición de lista de acceso incluye reglas que especifican si el tráfico que coincide con los criterios se reenvía normalmente o se descarta. Además, puede asignar el tráfico que coincide con los criterios a una cola específica o redirigirlo a un puerto específico. Una regla predeterminada de denegar todo es la última regla de cada lista.

2. Aplique la lista de acceso a una interfaz en dirección de entrada.

El software del switch permite vincular ACL a puertos físicos y LAG. El software del 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 todo el demás 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 Configure a Basic MAC ACL en la página 608).

   De forma predeterminada, esta ACL se vincula en la dirección de entrada, lo que significa que el switch examinará el tráfico al entrar al puerto.

2. En la página MAC Rules, cree una regla para Sales_ACL con la siguiente configuración:
   - ID: 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 Configure MAC ACL Rules en la página 610.

3. En la página MAC Binding Configuration, asigne Sales_ACL a los puertos gigabit de interfaz 6, 7 y 8, y luego haga clic en el botón Apply. (Consulte Configure MAC Binding en la página 612).

   Puede asignar un número de secuencia opcional para indicar el orden de esta lista de acceso en relación con otras listas de acceso, si ya hay alguna asignada a esta interfaz y dirección.

4. La tabla MAC Binding Table muestra la información de vinculación de interfaz y ACL MAC (consulte View and Delete MAC ACL Bindings in the MAC Binding Table en la página 614).

La ACL llamada 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 para tramas Ethernet. Las tramas que cumplen estos criterios 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 de permiso con los criterios de coincidencia deseados y vincularla a las interfaces 6, 7 y 8.

Ejemplo de configuración de ACL IP estándar

El siguiente ejemplo muestra cómo crear una ACL basada en IP que impide que cualquier tráfico IP del departamento de finanzas se permita en los puertos asociados con 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 un IP ACL ID de 1 (consulte Configure an IP ACL en la página 615).
2. En la página IP Rules, cree una regla para la ACL IP 1 con la siguiente configuración:
   - Rule ID: 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: 255.255.255.0

Para obtener más información sobre las reglas de ACL IP, consulte Configure Rules for an IP ACL en la página 617.

3. Haga clic en el botón Add.
4. En la página IP Rules, cree una segunda regla para la ACL IP 1 con la siguiente configuración:
   - Rule ID: 2
   - Action: Permit
   - Match Every: True
5. Haga clic en el botón Add.
6. En la página IP Binding Configuration, asigne ACL ID 1 a los puertos gigabit de interfaz 2, 3 y 4, y asigne el número de secuencia 1 (consulte Configure IP ACL Interface Bindings en la página 632).

   De forma predeterminada, esta ACL IP se vincula en la dirección de entrada, por lo que examina el tráfico al entrar al switch.
7. Haga clic en el botón Apply.
8. Use la página IP Binding Table para ver las interfaces y la información de vinculación de ACL IP (consulte View and Delete IP ACL Bindings in the IP ACL Binding Table en la página 633).

La ACL IP de este ejemplo coincide con 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 Ethernet 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 entregue 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. Para 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 del servicio tiene efectos indeseables en aplicaciones con requisitos de tiempo estrictos, como voz o multimedia.

La calidad de servicio (QoS) puede proporcionar una entrega de datos constante y predecible al distinguir los paquetes con requisitos de tiempo estrictos de los que toleran más el retardo. Los paquetes con requisitos de tiempo estrictos reciben un trato 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 tiempo necesarios, se crea una deficiencia en la ruta de red y se compromete el rendimiento de todo el flujo de paquetes.

Existen dos tipos básicos de QoS:

- Servicios integrados: los recursos de red se reparten según la solicitud y se reservan (reserva de recursos) de acuerdo con la política de administración de la red (RSVP, por ejemplo).
- Servicios diferenciados: los recursos de red se reparten según la clasificación del tráfico y la prioridad, dando trato preferente a los datos con requisitos de tiempo estrictos.

La función DiffServ contiene varios bloques conceptuales de QoS que puede usar para construir una red de servicios diferenciados. Use estos mismos bloques de diferentes maneras para construir otros tipos de arquitecturas de QoS.

Se necesitan 3 bloques clave de QoS para configurar 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 construir 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 de exclusión) de la clase referenciada.

Para configurar DiffServ, debe definir niveles de servicio, es decir, las clases de reenvío/PHB identificadas por un valor DSCP determinado, en la interfaz de salida. Estos niveles de servicio se definen configurando clases BA para cada uno.

Creación de 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:

- Traffic Conditioning Policy: política que se aplica a una clase de tráfico DiffServ
- Service Provisioning Policy: política que se aplica a un nivel de servicio DiffServ

Debe configurar manualmente las distintas instrucciones y reglas usadas en las políticas de acondicionamiento de tráfico y de aprovisionamiento de servicio para lograr la operación deseada 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. Hay varias acciones de QoS distintas asociadas con el acondicionamiento de tráfico:

- Descarte. Descarta un paquete al llegar. Es útil para emular el funcionamiento de una lista 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 punto de código DiffServ en un paquete con el valor DSCP que representa el nivel de servicio asociado con una clase de tráfico DiffServ específica. 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 a un valor especificado al transmitir paquetes de la clase de tráfico. Se inserta un encabezado 802.1p si aún no existe. Es útil para asignar un nivel de prioridad de capa 2 basado en la definición de una clase de reenvío DiffServ (como el valor DSCP o IP Precedence) para transmitir características de QoS a switches posteriores que no revisan habitualmente el valor DSCP del encabezado IP.
- Policing. Método para restringir el tráfico entrante asociado con una clase específica de modo que cumpla con los términos de la TCS. Se puede aplicar un trato especial a los paquetes fuera de perfil que exceden la especificación de conformidad o que no son conformes.

La función DiffServ admite los siguientes tipos de tratamiento de policing de tráfico (acciones):

- drop. El paquete se descarta
- mark cos. Los bits de prioridad de usuario 802.1p se (re)marcan y se reenvían
- mark dscp. El DSCP del paquete se (re)marca y se reenvía
- mark prec. El IP Precedence del paquete se (re)marca y se reenvía
- send: el paquete se reenvía sin modificación de DiffServ

Reconocimiento del modo de color. El policing de la función DiffServ usa el modo color blind o color aware. El modo color blind ignora la coloración (marcado) del paquete entrante. El modo color aware toma en cuenta el marcado actual del paquete al determinar el resultado del policing. Se usa una clase de tráfico auxiliar junto con la definición de policing 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 se puede especificar el color del tráfico excedente.

- Conteo. Actualiza las estadísticas de octetos y paquetes para rastrear el manejo de datos a lo largo de las rutas de tráfico dentro de DiffServ. En esta función DiffServ, el usuario no configura explícitamente los contadores, sino que se integran en el sistema según la política DiffServ que se crea. Consulte la sección Estadísticas de este documento para obtener más detalles.
- Asignación de cola de QoS. Dirige el 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 que pertenecen a la clase.
- Redirección. Fuerza el flujo de tráfico clasificado a un puerto de salida especificado (físico o LAG). Puede ocurrir además de cualquier acción de marcado o policing. 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 la siguiente configuración:
   - Class Name: Class1
   - Class Type: All

   Para obtener más información sobre esta página, consulte Configure a DiffServ Class en la página 489.
2. Haga clic en el hipervínculo Class1 para ver 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 ingrese 4567 como valor del puerto de origen
   - Destination IP Address: 192.12.2.0

- Destination Mask: 255.255.255.0
- Destination L4 Port: Other, e ingrese 4568 como valor del puerto de destino

Para obtener más información sobre esta página, consulte Configure a DiffServ Class en la página 489.

4. Haga clic en el botón Apply.
5. En la página Policy Configuration, cree una nueva política con la siguiente configuración:
   - Policy Selector: Policy1
   - Member Class: Class1

   Para obtener más información sobre esta página, consulte Configure DiffServ Policy en la página 497.

6. Haga clic en el botón Agregar (Add).
La política se agrega.
7. Haga clic en el hipervínculo Policy1 para ver 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 Configure DiffServ Policy en la página 497.

9. En la página Service Configuration, seleccione la casilla junto a las interfaces g7 y g8 para asociarles la política y luego haga clic en el botón Apply. (Consulte Configure the DiffServ Service Interface en la página 500).

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 de 4567 y un puerto de destino de 4568 desde 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 confirmada para este flujo es enviar los paquetes con una velocidad comprometida de 1000000 Kbps y un tamaño de ráfaga de 128 KB. Los paquetes que exceden la velocidad comprometida y el tamaño de ráfaga se descartan.

802.1X

Las redes de área local (LAN) suelen implementarse en entornos que permiten que dispositivos no autorizados se conecten físicamente a la infraestructura LAN, o que usuarios no autorizados intenten acceder a la LAN a través de equipos ya conectados. En esos entornos, quizá desee restringir el acceso a los servicios que ofrece 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 las infraestructuras LAN para autenticar y autorizar dispositivos conectados a un puerto LAN con características de conexión punto a punto, y para impedir el acceso a ese puerto cuando falla el proceso de autenticación y autorización. En este contexto, un puerto es un único punto de conexión a la LAN, como los puertos de bridges MAC y las asociaciones entre estaciones o puntos de acceso en LAN inalámbricas IEEE 802.11.

El estándar IEEE 802.11 describe un marco arquitectónico en el que se llevan a cabo 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 permite a los usuarios no autenticados un acceso limitado a los recursos de la red.

Nota: Puede usar funciones de QoS para limitar la velocidad en la VLAN de invitados y así limitar los recursos de red que proporciona la VLAN de invitados.

Otra función de 802.1X es la posibilidad de configurar un puerto para habilitar/deshabilitar la compatibilidad con 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 este puede ofrecer 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 de un switch para garantizar que solo los sistemas autorizados puedan acceder a sus servicios.

El control de acceso por puerto ofrece un medio para impedir el acceso no autorizado de suplicantes a los servicios que ofrece 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 de acceso público o a LAN departamentales.

El control de acceso se logra exigiendo la autenticación de los suplicantes conectados a los puertos controlados de un autenticador. El resultado del proceso de autenticación determina si el suplicante está autorizado para 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 ese puerto.
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 del autenticador también se encarga de enviar la información recibida del suplicante al servidor de autenticación para que se verifiquen las credenciales, lo que determinará el estado de autorización del puerto. La PAE del autenticador controla el estado autorizado/no autorizado del puerto controlado
según el resultado del proceso de autenticación basado en RADIUS.

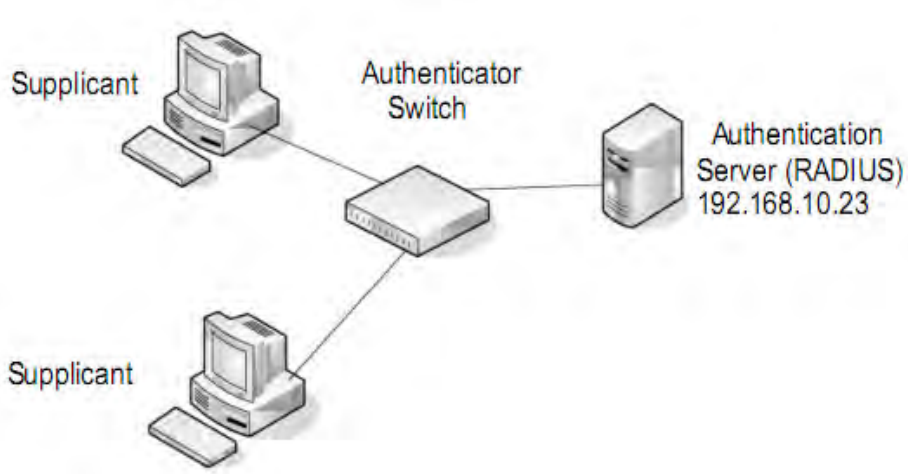


Figura 1. Roles de autenticación 802.1X

Ejemplo de configuración de 802.1X

Este ejemplo muestra cómo configurar el switch para exigir autenticación basada en 802.1X en los puertos de una sala de conferencias corporativa (1/0/5– 1/0/8). Estos puertos están disponibles para visitantes, quienes deben autenticarse antes de obtener acceso a la red. La autenticación la gestiona 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 VLAN ID 150 y VLAN Name Guest.

1. En la página Port Authentication, seleccione los puertos 1/0/5, 1/0/6, 1/0/7 y 1/0/8.
2. En el menú Port Control, seleccione Unauthorized.

El ajuste Port Control de todos los demás puertos donde no se necesita autenticación debe ser Authorized. Cuando Port Control es Authorized, el puerto se coloca incondicionalmente en un estado force-Authorized y no requiere autenticación. Cuando Port Control es Auto, la PAE del autenticador establece el modo del puerto controlado

3. En el campo Guest VLAN de los puertos 1/0/5– 1/0/8, ingrese 150 para asignarlos a la VLAN de invitados.

   Puede configurar ajustes adicionales para controlar el acceso a la red a través de los puertos. Consulte Configure a Port Security Interface en la página 560 para obtener información sobre los ajustes.

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 Configure the Global Port Security Mode en la página 559).

   Este ejemplo usa los valores predeterminados de autenticación de puertos, pero hay varios ajustes adicionales que puede configurar. 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 ajustes:
   - Server Address: 192.168.10.23
   - Secret Configured: Yes
   - Secret: secret123
   - Active: Primary

   Para obtener más información, consulte Manage the RADIUS Server Settings en la página 509.

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 Configure a Login Authentication List en la página 518).

Este ejemplo habilita la seguridad de puertos basada en 802.1X en el switch y solicita a los hosts conectados en los puertos g5-g8 una autenticación basada en 802.1X. El switch pasa la información de autenticación al servidor RADIUS configurado.

MSTP

Spanning Tree Protocol (STP) se ejecuta en redes con bridges para ayudar a eliminar bucles. Si ocurre un bucle de bridge, la red puede inundarse de tráfico. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) admite varias instancias de Spanning Tree para canalizar eficientemente el tráfico de VLAN por distintas interfaces. Cada instancia de Spanning Tree se comporta de la manera especificada en IEEE 802.1w, Rapid Spanning Tree, con ligeras modificaciones en el funcionamiento pero no en el efecto final (el principal es la transición rápida del puerto al estado Forwarding).

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 Forwarding y la supresión de la Topology Change Notification. Estas funciones se representan con los parámetros pointtopoint y edgeport. MSTP es compatible con RSTP y STP, y se comporta adecuadamente con bridges STP y RSTP.

Un bridge MSTP puede configurarse para comportarse totalmente como un bridge RSTP o STP. Así, un bridge IEEE 802.1s inherentemente también admite IEEE 802.1w e IEEE 802.1D.

El algoritmo y protocolo MSTP proporciona conectividad simple y completa para las tramas asignadas a cualquier VLAN en una LAN con bridges compuesta 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) compuestas por LAN y/o bridges MSTP. Estas regiones y los demás bridges y LAN se conectan en un solo Common Spanning Tree (CST). [IEEE DRAFT P802.1s/D13]

MSTP conecta todos los bridges y LAN con un solo Common and Internal Spanning Tree (CIST). El CIST admite la determinación automática de cada región MST y elige 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 VLAN ID determinado se asignen a una y solo una de las MSTI o al IST dentro de la región, que la asignación sea coherente entre 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 como pertenecientes a una VLAN, conecta de forma simple y completa todas las LAN y dispositivos de red en toda la red, aunque las tramas de distintas VLAN pueden tomar rutas diferentes dentro de cualquier región, según IEEE DRAFT P802.1s/D13.

Todos los bridges, ya sea que 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 diferente para cada uno de estos protocolos. Un bridge MSTP transmite la BPDU adecuada según el tipo de BPDU recibida en un puerto específico.

Una región MST consta de uno o más bridges MSTP con el mismo MST Configuration Identifier, que usan las mismas MSTI y sin bridges conectados que no puedan recibir y transmitir BPDU MSTP. El MST Configuration Identifier tiene los siguientes componentes:

1. Configuration Identifier Format Selector
2. Configuration Name
3. Configuration Revision Level

4. Configuration Digest: firma de 16 bytes de tipo HMAC-MD5 creada a partir de la tabla MST Configuration Table (asignación de VLAN ID a MSTID)

Como hay varias instancias de Spanning Tree, se mantiene un estado MSTP por puerto y por instancia (o por puerto y por VLAN, ya que cualquier VLAN puede estar en una

y solo una MSTI o CIST). Por ejemplo, el puerto A puede estar en forwarding para la instancia 1 y en discarding para la instancia 2. Los estados de puerto cambiaron desde la especificación IEEE 802.1D.

Para admitir varios spanning trees, un bridge MSTP debe configurarse con una asignación inequívoca de VLAN ID (VID) a spanning trees. Esto se logra:

1. Garantizando que la asignación de VID a FID sea inequívoca.

2. Garantizando que cada FID admitido por el bridge se asigne exactamente a una instancia de Spanning Tree.

La combinación de la asignación de VID a FID y luego de FID a MSTI define una correspondencia de VID con instancias de spanning tree, representada por la tabla MST Configuration Table.

Con esta asignación se garantiza que cada VLAN se asigne a una y solo una MSTI. El CIST también es una instancia de spanning tree con MSTID 0.

Puede existir una instancia sin VID asignados, pero cada VLAN debe asignarse a una de las otras instancias de spanning tree.

La parte de la topología activa de la red que conecta dos bridges de la misma región MST atraviesa solo bridges MST y LAN de esa región, y nunca bridges de ningún tipo fuera de la región; es decir, la conectividad dentro de la región es independiente de la conectividad externa.

Ejemplo de configuración de MSTP

Este ejemplo muestra cómo crear una instancia MSTP en el switch. La red de ejemplo incluye tres switches que atienden distintas ubicaciones de la red. En este ejemplo, 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.

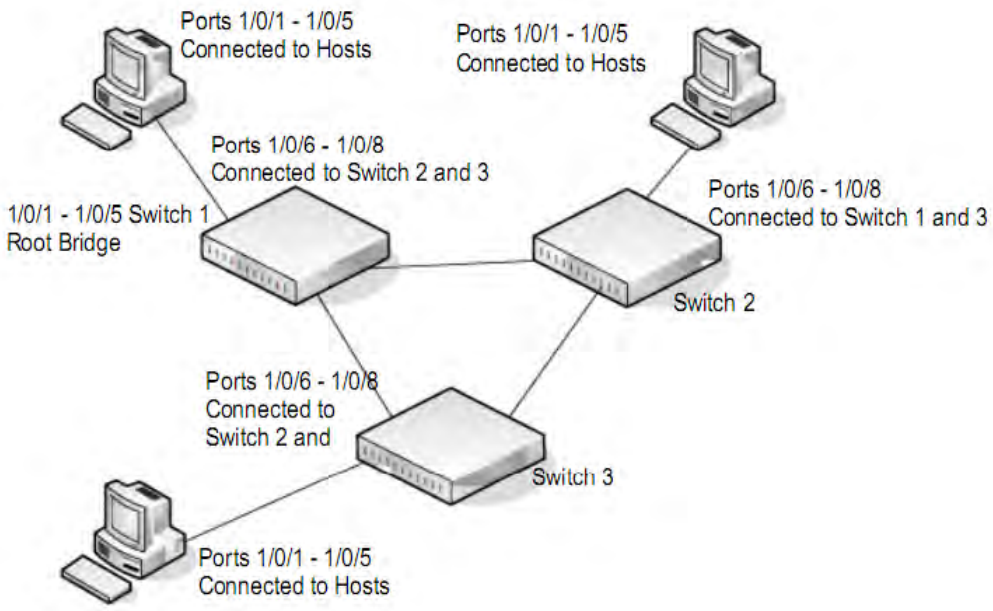


Figura 2. Configuración de ejemplo de MSTP

Realice los siguientes procedimientos en cada switch para configurar MSTP:

1. Use la página VLAN Configuration para crear las VLAN 300 y 500 (consulte Configure Basic VLAN Settings en la página 182).
2. Use la página VLAN Membership para incluir los puertos 1/0/1–1/0/8 como miembros etiquetados (T) o sin etiquetar (U) de VLAN 300 y VLAN 500 (consulte Configure Basic VLAN Settings en la página 182).
3. En la página STP Configuration, habilite la opción Spanning Tree State (consulte Configure Advanced STP Settings en la página 218).

   Use los valores predeterminados para el resto de los ajustes de STP. De forma predeterminada, STP Operation mode es MSTP y Configuration Name es la dirección MAC del switch.

4. En la página CST Configuration, establezca el valor de Bridge Priority de cada uno de los tres switches para forzar que el switch 1 sea el root bridge:
   - Switch 1: 4096
   - Switch 2: 12288
   - Switch 3: 20480

   Nota: Los valores de prioridad de bridge son múltiplos de 4096.

   Si no especifica un root bridge y a todos los switches se les asigna el mismo valor de prioridad de bridge, se elige como root bridge el switch con la dirección MAC más baja (consulte Configure CST Settings en la página 221).

5. En la página CST Port Configuration, seleccione los puertos 1/0/1–1/0/8 y seleccione Enable en el menú STP Status (consulte Configure CST Port Settings en la página 223).
6. Haga clic en el botón Aplicar (Apply).
7. Seleccione los puertos 1/0/1–1/0/5 (puertos edge) y seleccione Enable en el menú Fast Link.

   Como los puertos edge no corren riesgo de bucles de red, los puertos con Fast Link habilitado pasan directamente al estado Forwarding.

8. Haga clic en el botón Apply (Aplicar).

   Puede usar la página CST Port Status para ver la información de spanning tree de cada puerto.

9. En la página MST Configuration, cree una instancia MST con la siguiente configuración:
   - MST ID: 1
   - Priority: use el valor predeterminado (32768)
   - VLAN ID: 300

   Para obtener más información, consulte Configure MST Settings en la página 227.

10. Haga clic en el botón Add.

11. Cree una segunda instancia MST con la siguiente configuración
    - MST ID: 2
    - Priority: 49152
    - VLAN ID: 500
12. Haga clic en el botón Add.

En este ejemplo, suponga que el switch 1 se convirtió en el root bridge de la instancia MST 1, y el switch 2 en el root bridge de la instancia MST 2. El switch 3 tiene hosts del departamento de ventas (puertos 1/0/1, 1/0/2 y 1/0/3) y del departamento de RR. HH. (puertos 1/0/4 y 1/0/5). Los switches 1 y 2 también incluyen hosts de los departamentos de ventas y recursos humanos. Los hosts conectados desde el switch 2 usan VLAN 500, instancia MST 2, para comunicarse directamente con los hosts del switch 3. Del mismo modo, los hosts del switch 1 usan VLAN 300, instancia MST 1, para comunicarse directamente con los hosts del 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 a más instancias de MSTP.

B

BConfiguración predeterminada

Este apéndice describe la configuración predeterminada de muchas de las funciones del software de los switches NETGEAR.

Tabla 231. Configuración predeterminada

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
Puerta de enlace predeterminada	0.0.0.0
Protocolo	DHCP
ID de VLAN de administración	1
Longitud mínima de contraseña	Ocho caracteres
Modo de administración IPv6	Ninguno
Cliente SNTP	Habilitado
Servidor SNTP	No configurado
Registro global	Habilitado
Registro de comandos CLI	Deshabilitado
Registro en consola	Habilitado (nivel de gravedad: debug y superior)
Registro en RAM	Habilitado (nivel de gravedad: debug y superior)
Registro persistente (FLASH)	Deshabilitado
DNS	Habilitado (sin servidores configurados)
SNMP	Habilitado (SNMPv1/SNMPv2, SNMPv3)
Traps SNMP	Habilitado

Tabla 231. Configuración predeterminada (continuación)

Función	Predeterminado
Auto Install	Habilitado
Auto Save	Deshabilitado
sFlow	Habilitado
ISDP	Habilitado (versiones 1 y 2)
RMON	Habilitado
TACACS	No configurado
RADIUS	No configurado
SSH/SSL	Deshabilitado
Telnet	Habilitado
Protección contra denegación de servicio	Deshabilitado
Captive Portal	Deshabilitado
Autenticación Dot1x (IEEE 802.1X)	Deshabilitado
Seguridad de puertos basada en MAC	Todos los puertos desbloqueados
Listas de control de acceso (ACL)	Ninguna configurada
IP source guard (IPSG)	Deshabilitado
DHCP snooping	Deshabilitado
Inspección dinámica de ARP	Deshabilitado
Puertos protegidos	Ninguno
Grupos privados	Ninguno
Compatibilidad con control de flujo (IEEE 802.3x)	Deshabilitado
Prevención de bloqueo head-of-line	Deshabilitado
Tamaño máximo de trama	1518 bytes
Compatibilidad con Auto-MDI/MDIX	Habilitado
Autonegociación	Habilitado
Velocidad de puerto anunciada	Capacidad máxima
Control de tormentas de broadcast	Habilitado
Duplicación de puertos	Deshabilitado
LLDP	Habilitado

Tabla 231. Configuración predeterminada (continuación)

Función	Predeterminado
LLDP-MED	Habilitado
Envejecimiento de direcciones de la tabla MAC	300 segundos (direcciones dinámicas)
Relay DHCP de capa 2	Deshabilitado
VLAN ID predeterminado	1
Nombre de VLAN predeterminado	Default
Modo de administración Auto-Trunk	Deshabilitado
GVRP	Deshabilitado
Temporizadores GARP Leave: 60 centisegundos Leave All: 1000 centisegundos Join: 20 centisegundos	
Voice VLAN	Deshabilitado
Guest VLAN	Deshabilitado
VLAN asignadas por RADIUS	Deshabilitado
Double VLAN	Deshabilitado
Spanning Tree Protocol (STP)	Habilitado
Modo de operación de STP	IEEE 802.1s RSTP
Funciones opcionales de STP	Deshabilitado
Prioridad de bridge STP	32768
Multiple Spanning Tree	Deshabilitado
Modo de administración Auto-LAG	Deshabilitado
Modo hash global de Auto-LAG	2 Dest MAC, VLAN, EType, puerto de entrada
Agregación de enlaces	No hay grupos de agregación de enlaces (LAG) configurados
Prioridad del sistema LACP	1
Modo de enrutamiento	Deshabilitado
IP helper y relay UDP	Deshabilitado
Interfaces de túnel y loopback	Ninguna
DiffServ	Habilitado
Auto VoIP	Deshabilitado
Clase de tráfico Auto VoIP	6
MLD snooping	Deshabilitado

Tabla 231. Configuración predeterminada (continuación)

Función	Predeterminado
IGMP snooping	Habilitado
Consultor de IGMP snooping	Habilitado
GMRP	Deshabilitado

C

CAcrónimos y abreviaturas

En la mayoría de los casos, los acrónimos y abreviaturas se definen la primera vez que se usan en este documento. Los acrónimos y abreviaturas también se definen en la siguiente tabla.

Tabla 232. Acrónimos y abreviaturas

Acrónimo	Definición
100BASE-TX	Fast Ethernet a 100 Mbps (12.5 MBps) con autonegociación
1000BASE-T	Ethernet Gbps sobre par trenzado a 1 Gbps (125 Mbps)
10GBASE-T	O IEEE 802.3an. Estándar del comité IEEE 802.3 para ofrecer conexiones Ethernet de 10 gigabits por segundo (Gbps) (1,250 megabits por segundo (Mbps)) sobre cables convencionales de par trenzado blindado o sin blindar (UTP).
802.1x	Estándar de protocolo de autenticación IEEE 802.1x
ACE	Access Control Entry (entrada de control de acceso)
ACL	Access Control List (lista de control de acceso)
API	Application Programming Interface (interfaz de programación de aplicaciones)
ARP	Address Resolution Protocol (protocolo de resolución de direcciones)
AVB	Audio Video Broadcast, Audio Video Bridging
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
Archivo de arranque	La imagen de software (normalmente un archivo .stk) destinada a descargarse y ejecutarse en el dispositivo administrado NETGEAR ProSafe de destino.
BSP	Board Support Package
CDP	Cisco Discovery Protocol
CE	Control Element (elemento de control)
CLI	Command Line Interface (interfaz de línea de comandos)

Tabla 232. Acrónimos y abreviaturas (continuación)

Acrónimo	Definición
CoS	Class of Service (clase de servicio). Indica cómo un protocolo de capa superior requiere que un protocolo de capa inferior trate sus mensajes. Una definición de CoS consta de un número de ruta virtual y un campo de prioridad de transmisión (ToS)
DAPI	Destination Access Point Identifier
DCVPN	Data Center Virtual Private Network
Puerta de enlace predeterminada	Dirección IP de un router que un host puede usar como primer salto cuando el host no conoce una ruta más específica hacia un destino determinado.
Ruta predeterminada	Ruta configurada manualmente (estática) cuyo destino es 0.0.0.0/0.0.0.0 y que, por lo tanto, coincide con el destino de todos los paquetes. Un router usa una ruta predeterminada para reenviar paquetes que no coinciden con una ruta más específica.
DHCP	Dynamic Host Configuration Protocol (RFC 2131, RFC3315). Mecanismo para asignar direcciones IP dinámicamente, de modo que puedan reutilizarse cuando los hosts ya no las necesitan.
Servidor DHCP	Los servidores Dynamic Host Configuration Protocol otorgan la dirección y asignan parámetros a los clientes que lo solicitan en la red. Actualmente interesa que estos servidores proporcionen información del servidor TFTP y del archivo de arranque.
DLL	Data Link Layer (capa de enlace de datos)
Servidor DNS	Servidores Domain Name System que proporcionan la correspondencia entre direcciones IP y nombres de host.
DSCP	Differentiated Services Code Point
DTL	Device Transformation Layer
DTP	Dynamic Trunking Protocol
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
ECMP	Equal Cost Multiple Paths
EEE	Energy Efficient Ethernet (del IEEE 802.3az Energy Efficient Ethernet Task Force y del IEEE 802.3az Energy Efficient Ethernet Study Group).
EFP	Egress Filter Processor
FDB	Forwarding Database (base de datos de reenvío)
HAPI	Hardware Application Programming Interface
Interfaz de host	Interfaz IP que no es una interfaz de enrutamiento. Solo los paquetes originados localmente se envían por una interfaz de host. Solo se reciben paquetes con destino local. Las interfaces de host no participan en protocolos de enrutamiento dinámico.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Tabla 232. Acrónimos y abreviaturas (continuación)

Acrónimo	Definición
IAS	Internal Authentication Server (servidor de autenticación interno)
IFP	Ingress Filter Processor
IGMP	Internet Group Management Protocol
Interfaz en banda	Interfaz IP que puede usarse para la administración en banda. Cualquier interfaz IP distinta del puerto fuera de banda.
IP	Internet Protocol
Propietario de dirección IP	Router VRRP que tiene las direcciones IP del router virtual como direcciones de interfaz reales. Es el router que, cuando está activo, responde a los paquetes dirigidos a una de estas direcciones IP para pings ICMP, conexiones TCP, etc.
Interfaz IP	Interfaz configurada como interfaz IP en lugar de interfaz de switching de capa 2. A una interfaz IP se le deben asignar una o más direcciones IP. También se denomina interfaz de capa 3.
IP MAP	Componente de NETGEAR ProSafe Managed que administra la configuración IPv4 global y por interfaz. IP MAP administra la configuración de rutas estáticas y predeterminadas. IP MAP agrega y elimina rutas locales, estáticas y predeterminadas de RTO.
IP6MAP	El equivalente IPv6 de IP MAP.
IPv4	Internet Protocol versión 4
IPv6	Internet Protocol versión 6
ISDP	Industry Standard Discovery Protocol
ISID	Identificador de sesión definido por el iniciador
L2	Capa 2 (redes)
L3	Capa 3 (redes)
LAG	Link Aggregation Group (estándar IEEE)
LLDP	Link Layer Discovery Protocol
LLPF	Link Local Protocol Filtering
Ruta local	Ruta hacia una subred conectada. Un router crea una ruta local para cada dirección IP activa configurada localmente y usa la ruta local para llegar a otras estaciones de la subred conectada.
LPI	Low-power Idle (inactividad de bajo consumo)
MAB	MAC Authentication Bypass
MAC	Media Access Control
Interfaz de administración	Interfaz IP externa usada para enviar y recibir paquetes IP para configurar y supervisar el dispositivo.
VLAN de administración	VLAN configurada para usarse en la administración en lugar del tráfico de control o de datos.

Tabla 232. Acrónimos y abreviaturas (continuación)

Acrónimo	Definición
MFDB	Multicast Forwarding Database
MIB	Management Information Base
MLAG	Multi-switch Link Aggregation
MMU	Memory Management Unit
MPLS	Multiprotocol Label Switching: estándar relacionado con la calidad de IP.
MUA	Message User Agent
MVR	Multicast VLAN Registration
N/A	no aplica
N_IDLE	Normal IDLE
NAS	Network Access Server, Network Application Support
NMS	Network Management System (sistema de administración de red)
NSF	Nonstop Forwarding
OTP	One-Time Password (contraseña de un solo uso)
PA	Policy Assisted
PAE	Port Access Entity
PD	Powered Device (dispositivo alimentado)
PDU	Protocol Data Unit (unidad de datos de protocolo)
PIM-DM	Protocol-Independent Multicast Dense mode
PIM-SM	Protocol-Independent Multicast Sparse mode
Dirección IP principal	Dirección IP seleccionada del conjunto de direcciones de interfaz reales. Una posible selección consiste en seleccionar siempre la primera dirección. Los anuncios VRRP siempre se envían usando la dirección IP principal como origen del paquete IP.
PoE	Power over Ethernet. Corresponde al estándar IEEE 802.3AF, que admite el suministro de energía de hasta 15.4W por puerto.
PoE+	Power over Ethernet Plus. Corresponde al estándar IEEE 802.3AT, que admite el suministro de energía de hasta 30.0W por puerto.
PSE	Power Sourcing Equipment (equipo de suministro de energía)
PVST+	Per VLAN Spanning Tree Plus
PVSTP	Per VLAN Rapid Spanning Tree Protocol
QoS	Quality of Service (calidad de servicio)
RADIUS	Remote Authentication Dial-in User Service

Tabla 232. Acrónimos y abreviaturas (continuación)

Acrónimo	Definición
RED	Random Early Discard
Interfaz de enrutamiento	Interfaz IP cuyos puertos físicos son puertos del panel frontal y están asociados con una VLAN. Los paquetes recibidos en una interfaz de enrutamiento pueden transmitirse en una VLAN distinta de aquella en la que se recibieron.
RTC	Real-time Clock (reloj en tiempo real)
RTO	Administrador de tablas de enrutamiento de NETGEAR ProSafe Managed
SDM	Switch Database Management
Puerto de servicio	Interfaz IP en una interfaz Ethernet independiente de los puertos del panel frontal. El puerto de servicio está dedicado a la administración. Tiene su propia interfaz independiente con la pila IP. El puerto de servicio es una interfaz de host.
SM	máquina de estados
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority (prioridad estricta)
SSTP	Shared Spanning Tree Protocol
TFTP	Trivial File Transfer Protocol
Servidor TFTP	Los servidores Trivial File Transfer Protocol almacenan los archivos de configuración y/o de imagen que solicitan los clientes.
TLV	Type-Length-Value (tipo-longitud-valor)
UDLD	Uni-Directional Link Detection
UI	User Interface (interfaz de usuario)
UPoE	Universal Power over Ethernet. Aún no existe un estándar IEEE para UPoE. UPoE de NETGEAR admite el suministro de energía de hasta 60W por puerto.
USB	Universal Serial Bus
Router virtual	Objeto abstracto administrado por VRRP que actúa como router predeterminado para los hosts de una LAN compartida. Consta de un identificador de router virtual y un conjunto de direcciones IP asociadas en una LAN común. Un router VRRP puede respaldar uno o más routers virtuales
Respaldo de router virtual	Conjunto de routers VRRP disponibles para asumir la responsabilidad de reenvío de un router virtual si falla el Master actual.
Master de router virtual	Router VRRP que asume la responsabilidad de reenviar los paquetes enviados a las direcciones IP asociadas con el router virtual y de responder a las solicitudes ARP de esas direcciones IP. Tenga en cuenta que, si el propietario de la dirección IP está disponible, siempre se convertirá en el Master.
VLAN	Virtual Local Area Network (red de área local virtual)

Tabla 232. Acrónimos y abreviaturas (continuación)

Acrónimo	Definición
Router VRRP	Router que ejecuta Virtual Router Redundancy Protocol. Puede participar en uno o más routers virtuales.
VTP	VLAN Trunking Protocol