Junos® OS

Guía de administración y monitoreo de red

Published
2024-01-24

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS Guía de administración y monitoreo de red
Copyright © 2024 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Acerca de esta guía | xxxvii

1 Descripción general

Funciones de administración de dispositivos en Junos OS | 2

Funciones de administración de dispositivos y redes | 5

Operaciones de seguimiento y registro | 11

Soporte de Junos Space para la administración de red | 13

Descripción general de las herramientas de diagnóstico | 14

2 Características de operación, administración y administración

OAM de Ethernet y administración de fallos de conectividad para enrutadores | 20

Introducción a la administración de errores de conectividad (CFM) de OAM | 20

Administración de errores de conectividad Ethernet OAM | 21

Administración de errores de conectividad OAM IEEE 802.1ag | 22

Configurar la administración de errores de conectividad (CFM) | 28

Crear un dominio de mantenimiento | 29

Crear una asociación de mantenimiento | 30

Configurar puntos intermedios de mantenimiento (MIP) | 31

Configurar puntos intermedios de la asociación de mantenimiento en la serie ACX | 33

Configurar un MEP para generar y responder a mensajes de protocolo CFM | 37

Configurar un punto de conexión de asociación de mantenimiento (MEP) | 38

Configurar un punto de conexión de asociación de mantenimiento remoto (MEP) | 40

Configurar la protección de servicio para VPWS a través de MPLS mediante la interfaz MEP | 42

Configurar el protocolo Linktrace en CFM | 47

Descripción general de los parámetros del protocolo de comprobación de continuidad | 48

Configuración de parámetros de protocolo de comprobación de continuidad para la detección de errores | 49

Configuración de la limitación de velocidad de los mensajes OAM de Ethernet | 51

Habilitación del modo de administración de errores de conectividad mejorada | 54

Configurar la administración de errores de conectividad para la interoperabilidad durante las actualizaciones de software unificadas en servicio | 55

Soporte de Junos OS para la supervisión del rendimiento que cumple con la especificación técnica MEF 36 | 56

Amortiguación del rendimiento del CFM Monitoreo de trampas y notificaciones para evitar la congestión del NMS | 57

Perfil de acción de CFM | 59

Descripción general del perfil de acción de CFM para reducir un grupo de interfaces lógicas | 59

Configurar un perfil de acción CFM para reducir un grupo de interfaces lógicas | 61

Configurar un perfil de acción de CFM para especificar acciones de CFM para eventos de CFM | 65

Interfaz de administración local Ethernet | 66

Descripción general de la interfaz de administración local Ethernet | 67

Configurar la interfaz de administración local de Ethernet | 69

Ejemplo de configuración de E-LMI | 72

Soporte CFM para paquetes encapsulados CCC | 77

Descripción general de la compatibilidad con IEEE 802.1ag CFM OAM para paquetes encapsulados CCC | 78

Funciones de CFM compatibles con circuitos VPN de capa 2 | 78

Configurar CFM para paquetes encapsulados CCC | 79

Configurar ISSU unificada para 802.1ag CFM | 80

Monitoreo CFM entre dispositivos CE y PE | 84

Notificación asincrónica del perfil de acción CFM | 85

Configuración de un perfil de acción CFM para la notificación asincrónica | 86

Descripción de la supervisión de CFM entre dispositivos CE y PE | 88

Configuración de TLV de estado de puerto y TLV de estado de interfaz | 90

Descripción general de los TLV | 90

Varios TLV para PDU CFM | 91

Compatibilidad con TLV opcionales adicionales | 93

Defectos de estado MAC | 101

Configuración de la compatibilidad con perfiles de acción MEP remotos | 104

Supervisión de un perfil de acción de MEP remoto | 105

Configuración del ID de chasis TLV | 106

Configuración del procesamiento de mensajes MAC Flush en modo CET | 107

Ejemplo: Configuración de un perfil de acción basado en TLV de protección de conexión | 110

Requisitos | 110

Descripción general y topología | 111

Configuración | 112

Configurar mensajes de comprobación de continuidad | 114

Configurar una conmutación de protección más rápida para topologías de red punto a punto | 114

Configure una convergencia más rápida para topologías de red multipunto a multipunto de base dual | 116

Configure un ID de VLAN principal para una mayor flexibilidad | 118

Configurar una asociación de mantenimiento remoto para aceptar un ID diferente | 119

Ejemplo: Configurar Ethernet CFM en interfaces físicas | 120

Requisitos | 120

Descripción general | 120

Configuración | 121

Ejemplo: Configurar Ethernet CFM en conexiones de puente | 123

Ejemplo: Configurar Ethernet CFM a través de VPLS | 128

Administración de fallos de vínculo para enrutadores | 139

Introducción a la gestión de fallos de vínculo OAM (LFM) | 139

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | 139

Descripción de la administración de fallas de vínculo OAM Ethernet para enrutadores de la serie ACX | 140

Configuración de Ethernet 802.3ah OAM | 142

Configurar la administración de errores de vínculo | 144

Configuración de la detección de vínculos | 145

Configuración del intervalo de PDU de OAM | 146

Configuración del umbral de PDU de OAM | 146

Configuración de valores de umbral para eventos de error local en una interfaz | 147

Deshabilitar el envío de TLV de eventos de vínculo | 147

Ejemplo: Configuración de la compatibilidad con OAM IEEE 802.3ah en una interfaz | 148

Ejemplo: Configuración de la compatibilidad con OAM IEEE 802.3ah para una interfaz de la serie ACX | 149

Requisitos | 149

Descripción general y topología | 149

Configuración de IEEE 802.3ah OAM en un enrutador de la serie ACX | **149**

Ejemplo: Configuración de Ethernet LFM entre el borde del proveedor y el borde del cliente | **152**

Ejemplo: Configuración de Ethernet LFM para CCC | **154**

Ejemplo: Configuración de Ethernet LFM para Ethernet agregada | **155**

Configuración de un perfil de acción de OAM | **158**

Especificación de las acciones que deben realizarse para los eventos de administración de errores de vínculo | **159**

Monitoreo de la pérdida de adyacencia del enlace | **160**

Estado del protocolo de supervisión | **161**

Configuración de valores de umbral para eventos de error en un perfil de acción | **162**

Aplicación de un perfil de acción | **162**

Detección remota de fallos para la gestión de fallos de vínculo | **163**

Detección de fallas remotas | **163**

Habilitación de la funcionalidad de jadeo moribundo | **164**

Circuito cerrado remoto para administración de fallas de vínculo | **165**

Configuración de una interfaz remota en modo de circuito cerrado | **166**

Habilitación de la compatibilidad con circuito cerrado remoto en la interfaz local | **167**

Habilitación del enrutamiento sin interrupciones para la administración de fallas de vínculo Ethernet en enrutadores de respaldo | **167**

Ejemplo: Configuración de Ethernet LFM con soporte de circuito cerrado | **171**

Administración de fallos de vínculo OAM Ethernet para conmutadores | 175

Administración de fallos de vínculo OAM de Ethernet | **175**

Configurar la administración de fallos de vínculo OAM de Ethernet | **177**

Ejemplo: Configurar la administración de fallos de vínculo OAM de Ethernet | **180**

Requisitos | **181**

Descripción general y topología | **181**

Configuración de la administración de fallas de vínculo OAM Ethernet en el conmutador 1 | **182**

Configuración de la administración de fallos de vínculo OAM Ethernet en el conmutador 2 | **184**

Verificación | **185**

Administración de errores de conectividad OAM Ethernet para conmutadores | 187

Descripción de la administración de errores de conectividad OAM Ethernet para conmutadores | **187**

Configurar la administración de errores de conectividad OAM Ethernet (procedimiento de CLI) | **190**

Creación del dominio de mantenimiento | **191**

Configuración de la mitad de la función MIP del dominio de mantenimiento | **192**

Creación de una asociación de mantenimiento | **193**

Configuración del protocolo de comprobación de continuidad | **193**

Configuración de un extremo de asociación de mantenimiento | **194**

Configuración de un perfil de acción de administración de errores de conectividad | **196**

Configuración del protocolo Linktrace | **196**

Ejemplo: Configurar la administración de errores de conectividad OAM Ethernet en conmutadores de la serie EX | **197**

Requisitos | **197**

Descripción general y topología | **198**

Configuración de la administración de errores de conectividad Ethernet OAM en el conmutador 1 | **198**

Configuración de la administración de errores de conectividad OAM Ethernet en el conmutador 2 | **200**

Verificación | **202**

Retardo de trama Ethernet | 205

Mediciones de retardo de trama Ethernet en conmutadores | **205**

Configurar interfaces MEP en conmutadores para que admitan mediciones de retardo de trama Ethernet (procedimiento de CLI) | **208**

Configuración de mediciones de retardo de trama Ethernet unidireccional en conmutadores (procedimiento de CLI) | **209**

Configurar un perfil de iterador en un conmutador (procedimiento de CLI) | **209**

Activar una sesión de medición de retardo de trama Ethernet en un conmutador | **211**

Configuración de mediciones de retardo de trama Ethernet bidireccional en conmutadores (procedimiento de CLI) | **212**

Oam del servicio Ethernet (ITU-ty.1731) para enrutadores | 213

Visión general de OAM del servicio Ethernet ITU-T Y.1731 | **213**

Descripción general de las mediciones de retardo de trama Ethernet | **214**

Descripción general de la medición de pérdida de trama Ethernet | **221**

Medición del acuerdo de nivel de servicio | **223**

Modo bajo demanda para la medición de SLA | **223**

Modo proactivo para la medición de SLA | **224**

Descripción general del protocolo de notificación de fallos de Ethernet | **226**

Descripción general de la medición de pérdidas sintéticas de Ethernet | 227

Escenarios para la configuración de ETH-SLM | 228

Formato de los mensajes ETH-SLM | 229

Transmisión de mensajes ETH-SLM | 231

Configurar sesiones de medición de retardo de trama Ethernet | 234

Directrices para configurar enrutadores que admitan una sesión de ETH-DM | 235

Pautas para iniciar una sesión de ETH-DM | 237

Directrices para administrar las estadísticas de ETH-DM y los recuentos de fotogramas de ETH-DM | 239

Configuración de enrutadores para admitir una sesión ETH-DM | 245

Configuración de interfaces MEP | 245

Asegurarse de que las ppm distribuidas no estén deshabilitadas | 247

Habilitación de la opción de marca de tiempo asistida por hardware | 249

Configuración de la opción de procesamiento del lado del servidor | 250

Activación de una sesión de mediciones de retardo de trama Ethernet | 251

Inicio de una sesión de ETH-DM | 253

Uso del comando de medición de retardo de Ethernet del monitor | 253

Inicio de una sesión unidireccional de ETH-DM | 254

Inicio de una sesión bidireccional de ETH-DM | 255

Ejemplo: Configuración de mediciones de retardo de trama Ethernet unidireccionales con interfaces de etiqueta única | 256

Ejemplo: Configuración de mediciones de retardo de trama Ethernet bidireccional con interfaces de etiqueta única | 263

Gestión de estadísticas de medición de continuidad | 269

Visualización de estadísticas de medición de continuidad | 269

Estadísticas de medición de continuidad de borrado | 270

Visualización de estadísticas de mediciones de retardo de trama Ethernet | 271

Administración de estadísticas de ETH-DM y recuentos de tramas de ETH-DM | 272

Mostrar solo estadísticas de ETH-DM | 272

Visualización de estadísticas y recuentos de fotogramas de ETH-DM | 274

Visualización de los recuentos de tramas ETH-DM para los eurodiputados adjuntando la entidad CFM | 275

Visualización de los recuentos de fotogramas ETH-DM para los eurodiputados por interfaz o nivel de dominio | 276

Borrar estadísticas y recuentos de tramas de ETH-DM | 277

Configuración de interfaces MEP para admitir mediciones de retardo de trama Ethernet | 279

Configurar la medición de pérdida de tramas Ethernet | 281

Configuración de la medición estadística de pérdida de tramas para conexiones VPLS | 281

Gestión de estadísticas de ETH-LM | 282

Visualización de estadísticas ETH-LM | 282

Borrar estadísticas de ETH-LM | 284

Ejemplo: Medición de la pérdida de tramas Ethernet para PDU LMM/LMR de etiqueta única | 285

Requisitos | 285

Descripción general y topología | 286

Configuración | 287

Verificación | 299

Ejemplo: Medición de la pérdida de tramas Ethernet para PDU LMM/LMR de doble etiqueta | 302

Requisitos | 302

Descripción general y topología | 302

Configuración | 303

Verificación | 316

Configurar un perfil de iterador | 319

Configuración de un perfil de iterador | 319

Comprobación de la configuración de un perfil de iterador | 323

Visualización de la configuración de un perfil de iterador para la medición de retardo bidireccional | 323

Visualización de la configuración de un perfil de iterador para la medición de pérdidas | 325

Visualización de la configuración de un MEP remoto con un perfil de iterador | 326

Deshabilitar un perfil de iterador | 327

Administración de estadísticas de iterador | 328

Visualización de estadísticas de iterador | 328

Borrar estadísticas de iterador | 336

Configuración de un MEP remoto con un perfil de iterador | 337

Configurar mediciones de pérdida sintética Ethernet | 338

Directrices para configurar ETH-SLM | 339

Inicio de una sesión proactiva de ETH-SLM | 340

Configuración de interfaces MEP | 341

Configuración de un perfil de iterador para ETH-SLM | 342

Asociación del perfil iterador con los eurodiputados para ETH-SLM | 344

Inicio de una sesión ETH-SLM bajo demanda | 345

Administración de estadísticas de ETH-SLM y recuentos de tramas de ETH-SLM | 346

Visualización solo de estadísticas de ETH-SLM | 347

Visualización de estadísticas y recuentos de fotogramas de ETH-SLM | 348

Visualización de los recuentos de tramas ETH-SLM para los eurodiputados adjuntando la entidad CFM | 350

Visualización de los recuentos de tramas ETH-SLM para los eurodiputados por interfaz o nivel de dominio | 351

Borrar estadísticas y recuentos de tramas de ETH-SLM | 352

Borrar estadísticas de iterador | 353

Solución de problemas de fallas con ETH-SLM | 354

Indicación de alarma Ethernet | 356

Descripción general de la función de señal de indicación de alarma Ethernet (ETH-AIS) | 356

Descripción general de la señal de indicación de alarma Ethernet | 361

Configuración de ETH-AIS en un MEP CFM | 363

Configuración de un perfil de acción | 364

Configuración de una acción que debe realizarse cuando se detecta una alarma AIS | 365

Adjuntar el perfil de acción a un eurodiputado del CFM | 366

Configuración de la señal de indicación de alarma en enrutadores de la serie ACX | 368

Modo de transmisión en línea | 371

Habilitación de la transmisión en línea de mensajes de comprobación de continuidad para obtener la máxima escala | 371

Habilitación de la transmisión en línea de keepalives de gestión de fallos de vínculo para maximizar el escalado | 373

Habilitación del modo en línea de monitoreo del rendimiento para lograr la máxima escala | 377

Valores de escala CCM y PM en línea admitidos | 379

3

Supervisión de red mediante SNMP

Descripción general de la arquitectura SNMP y las MIB SNMP | 385

Descripción de la implementación de SNMP en Junos OS | 388

Carga de archivos MIB en un sistema de administración de red | 392

Descripción de la interfaz de administración local integrada | 394

Configurar SNMP en Junos OS | 395

Configurar SNMP | 396

Configurar detalles de SNMP | 405

Configurar el temporizador de retraso de confirmación | 408

Configurar SNMP en un dispositivo que ejecute Junos OS | 408

Ejemplo: Configurar SNMP en el sistema QFabric | 411

Requisitos | 411

Descripción general | 411

Configuración | 412

Configurar opciones en dispositivos administrados para un mejor tiempo de respuesta SNMP | 416

Habilitar la opción stats-cache-lifetime | 416

Filtrar solicitudes SNMP duplicadas | 416

Excluir interfaces que tardan en responder a las consultas SNMP | 417

MIB de utilidad específica para empresas para mejorar la cobertura SNMP | 419

MIB de utilidad | 419

Optimice la configuración del sistema de administración de red para obtener los mejores resultados | 422

Interfaces para aceptar solicitudes SNMP | 424

Configurar las interfaces en las que se pueden aceptar solicitudes SNMP | 424

Configurar un agente SNMP de proxy | 425

Ejemplo: Configurar la comprobación de la lista de acceso seguro | 426

Filtrar la información de la interfaz de la salida SNMP Get y GetNext | 426

Configurar SNMP para instancias de enrutamiento | 427

Descripción de la compatibilidad de SNMP con instancias de enrutamiento | 428

Instancia de enrutamiento de administración SNMPv3 | 429

MIB SNMP admitidas para instancias de enrutamiento | 431

Clases de soporte para objetos MIB | 443

Capturas SNMP admitidas para instancias de enrutamiento | 444

Identificar una instancia de enrutamiento | 445

Habilitar el acceso SNMP a través de instancias de enrutamiento | 446

Especificar una instancia de enrutamiento en una comunidad SNMPv1 o SNMPv2c | 446

Ejemplo: Configuración de las opciones de interfaz para una instancia de enrutamiento | 447

Configuración de listas de acceso para el acceso SNMP a través de instancias de enrutamiento | 449

Configurar operaciones remotas SNMP | 450

Descripción general de las operaciones remotas de SNMP | 450

Uso de Ping MIB para dispositivos de supervisión remota que ejecutan Junos OS | 454

Iniciar una prueba de ping | 455

- Antes de empezar | 455
- Iniciar una prueba de ping | 455
- Usar múltiples PDU de conjunto | 456
- Usar una PDU de un solo conjunto | 456

Supervisar una prueba de ping en ejecución | 457

- pingResultsTable | 457
- pingProbeHistoryTable | 459
- Generar trampas | 460

Recopilar resultados de pruebas de ping | 460

Detener una prueba de ping | 462

Interpretar variables de ping | 462

Uso de la MIB de Traceroute para dispositivos de supervisión remota que ejecutan Junos OS | 463

Iniciar una prueba de Traceroute | 464

- Usar múltiples PDU de conjunto | 464
- Usar una PDU de un solo conjunto | 465

Supervisión de una prueba de Traceroute en ejecución | 465

- traceRouteResultsTable | 465
- traceRouteProbeResultsTable | 466
- traceRouteHopsTable | 468
- Generar trampas | 469

Supervisión de la finalización de la prueba de Traceroute | 469

Recopilar los resultados de las pruebas de Traceroute | 470

Detener una prueba de Traceroute | 472

Interpretar variables de traceroute | 472

Capturas SNMP | 473

Configurar capturas SNMP | 473

Configurar opciones de captura SNMP | 475

- Configuración de la dirección de origen para capturas SNMP | 476
- Configuración de la dirección del agente para capturas SNMP | 479
- Agregar identificador de objeto snmpTrapEnterprise a capturas SNMP estándar | 480

Configuración de grupos de capturas SNMP | 480

Configurar opciones y grupos de capturas SNMP en un dispositivo que ejecute Junos OS | 483

Ejemplo: Configuración de grupos de capturas SNMP | 484

Administrar trampas | 484

Capturas SNMP compatibles con Junos OS | 487

Soporte de trampas SNMP | 488

Capturas SNMP estándar compatibles con Junos OS | 509

MIB SNMP personalizadas para capturas syslog | 520

- Descripción general de las MIB SNMP personalizadas | 521
- Definir una MIB personalizada para una captura syslog | 523
- Limitaciones del uso de capturas SNMP personalizadas | 530
- Ejemplo de captura de syslog personalizada | 530

Rastrear actividad SNMP | 537

Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS | 538

- Compruebe si hay objetos MIB registrados con SNMPd | 538
- Seguimiento de la actividad SNMP | 539
- Supervisar estadísticas SNMP | 540
- Comprobar el uso de la CPU | 540
- Comprobar la respuesta del motor de reenvío de paquetes y del kernel | 540

Rastrear la actividad SNMP en un dispositivo que ejecuta Junos OS | 541

- Configurar el número y el tamaño de los archivos de registro SNMP | 543
- Configurar el acceso al archivo de registro | 543
- Configurar una expresión regular para las líneas que se van a registrar | 544

Configurar las operaciones de seguimiento | 544

Ejemplo: Seguimiento de la actividad SNMP | 546

Configurar la captura de caducidad del certificado | 546

Habilitar capturas de emparejamiento y de túnel IPsec | 547

Privilegios de acceso para un grupo SNMP | 548

Configurar los privilegios de acceso concedidos a un grupo | 549

Configurar el grupo | 550

Configurar el modelo de seguridad | 550

Configurar el nivel de seguridad | 551

Asociar vistas MIB a un grupo de usuarios SNMP | 551

Configurar la vista de notificación | 552

Configurar la vista de lectura | 552

Configurar la vista de escritura | 552

Ejemplo: Configurar los privilegios de acceso concedidos a un grupo | 553

Asignar modelo de seguridad y nombre de seguridad a un grupo | 554

Configurar el modelo de seguridad | 554

Asignar nombres de seguridad a grupos | 555

Configurar el grupo | 555

Ejemplo: Configuración del grupo de seguridad | 556

Configurar ID de motor local en SNMPv3 | 556

Configurar SNMPv3 | 558

Crear usuarios de SNMPv3 | 559

Configuración mínima de SNMPv3 en un dispositivo que ejecuta Junos OS | 559

Ejemplo: Configuración de SNMPv3 | 561

Configurar el tipo de autenticación SNMPv3 y el tipo de cifrado | 565

Configurar el tipo de autenticación SNMPv3 | 565

Configurar autenticación MD5 | 565

Configurar autenticación SHA | 565

Configurar sin autenticación | 566

Configurar el tipo de cifrado SNMPv3 | 566

Configurar el algoritmo estándar de cifrado avanzado | 567

Configurar algoritmo de cifrado de datos | 567

Configurar Triple DES | 567

No configurar cifrado | 567

Capturas SNMPv3 | 567

Configurar capturas SNMPv3 en un dispositivo que ejecute Junos OS | 568

Configurar la notificación de captura SNMPv3 | 568

Ejemplo: Configurar la notificación de captura SNMPv3 | 569

Configurar el filtro de notificación de captura | 569

Configuración de la dirección de destino de captura | 570

Configurar la dirección | 571

Configurar la máscara de dirección | 571

Configurar el puerto | 571

Configurar la instancia de enrutamiento | 571

Configuración de la dirección de destino de captura | 571

Aplicar parámetros de destino | 572

Ejemplo: Configurar la lista de etiquetas | 572

Definir y configurar los parámetros de destino de captura | 573

Aplicar el filtro de notificación de captura | 573

Configurar los parámetros de destino | 574

Configurar el modelo de procesamiento de mensajes | 574

Configurar el modelo de seguridad | 574

Configurar el nivel de seguridad | 574

Configurar el nombre de seguridad | 575

SNMPv3 informa | 575

Ejemplo: Configurar el tipo de notificación de informe y la dirección de destino | 577

Ejemplo: Configurar el ID del motor remoto y el usuario remoto | 578

Requisitos | 578

Descripción general | 578

Configuración | 580

Verificación | 581

Comunidades SNMP | 583

Configurar comunidades SNMP | **583**

Agregar un grupo de clientes a una comunidad SNMP | **587**

Configurar cadena de comunidad SNMP | **589**

Ejemplos: Configurar la cadena de comunidad SNMP | **589**

Configurar la comunidad SNMPv3 | **591**

Configuración del nombre de la comunidad | **592**

Configuración del contexto | **592**

Configuración de los nombres de seguridad | **593**

Configuración de la etiqueta | **593**

Ejemplo: Configurar la comunidad SNMPv3 | **593**

Requisitos | **593**

Descripción general | **594**

Configuración | **594**

Verificación | **597**

Vistas MIB | 598

Configurar vistas MIB | **598**

Configurar MIB de proxy de ping | **599**

MIB SNMP compatibles con Junos OS y Junos OS Evolved | 600

Compatibilidad con MIB SNMP | **601**

Objetos MIB para la serie QFX | **610**

MIB de chasis de estructura | **614**

MIB SNMP estándar compatibles con Junos OS | **621**

Las MIB específicas de la empresa para Junos OS evolucionaron | **637**

MIB SNMP específicas de la empresa compatibles con Junos OS | **650**

MIB estándar para Junos OS evolucionado | **674**

Preguntas frecuentes sobre SNMP de Junos OS | 687

4 **Monitoreo remoto de red (RMON) con alarmas y eventos SNMP**

Monitoreo remoto de redes (RMON) | 721

Descripción general de RMON | **721**

Configuración de eventos y alarmas RMON | **726**

Configurar alarmas y eventos de RMON | **727**

- Configurar SNMP | **727**
- Configurar un evento | **728**
- Configurar una alarma | **729**

Monitorear tablas MIB de RMON | **730**

Tablas de control de eventos, alarmas, registros e historial de RMON MIB | **731**

Configuración mínima de alarma RMON y entrada de eventos | **734**

Configurar una entrada de alarma RMON y sus atributos | **735**

- Configurar la entrada de alarma | **735**
- Configure la descripción | **736**
- Configurar el índice de eventos descendentes o el índice de eventos ascendentes | **736**
- Configurar el umbral descendente o ascendente | **737**
- Configurar el intervalo | **738**
- Configurar el intervalo de umbral descendente | **738**
- Configurar el tipo de solicitud | **738**
- Configurar el tipo de ejemplo | **739**
- Configurar la alarma de inicio | **739**
- Configurar la etiqueta de registro del sistema | **740**
- Configurar la variable | **740**

Configurar una entrada de evento RMON y sus atributos | **740**

Ejemplo: Configurar una alarma RMON y la entrada de eventos | **741**

Utilice alarmTable para supervisar objetos MIB | **742**

- Crear una entrada de alarma | **742**
- Configurar los objetos MIB de alarma | **743**
  - alarmInterval | **743**
  - alarmaVariable | **743**
  - alarmSampleType | **744**
  - alarmValue | **744**
  - alarmaStartupAlarm | **744**

alarmRisingThreshold | 744
alarmaFallingThreshold | 745
alarmaPropietario | 745
alarmRisingEventIndex | 745
alarmFallingEventIndex | 746
Activar una nueva fila en alarmTable | 746
Modificar una fila activa en alarmTable | 746
Desactivar una fila en alarmTable | 746
Usar eventTable para registrar alarmas | 747
Crear una entrada de evento | 747
Configurar los objetos MIB | 747
eventType | 748
eventoComunidad | 748
eventOwner | 749
descripción del evento | 749
Activar una nueva fila en eventTable | 749
Desactivar una fila en eventTable | 750
Configurar el muestreo del historial de RMON | 750
Configurar la recopilación de muestreo del historial de RMON | 750
Ver y borrar estadísticas del historial de RMON | 751
Supervisión de la calidad del servicio de red mediante RMON | 752
RMON para monitorear la calidad del servicio | 753
Descripción de los puntos de medición, los indicadores clave de rendimiento y los valores de referencia | 758
Definir y medir la disponibilidad de la red | 760
Medir la salud | 768
Mida el rendimiento | 777
Supervisión de estado con SNMP | 786
Información general sobre la supervisión de estado | 786
Configurar la supervisión de estado en dispositivos que ejecutan Junos OS | 788
Configurar la supervisión de estado | 792

5 Opciones de contabilidad

Descripción general de las opciones de contabilidad | 796

Configurar opciones de contabilidad, uso de clase de origen y opciones de uso de clase de destino | 797

Instrucciones de configuración en el nivel jerárquico [edit accounting-options] | **797**

Configuración de opciones de contabilidad | **799**

Configurar archivos de registro de datos contables | **809**

- Configurar cuánto tiempo se conservan los archivos de copia de seguridad | **810**
- Configurar el tamaño máximo del archivo | **811**
- Configurar sitios de almacenamiento para los archivos | **811**
- Configurar copia de seguridad local para archivos de contabilidad | **812**
- Configurar archivos para que se compriman | **813**
- Configurar el número máximo de archivos | **813**
- Configurar la ubicación de almacenamiento del archivo | **813**
- Configurar archivos para guardarlos después de un cambio en el rol principal | **814**
- Configurar la hora de inicio para la transferencia de archivos | **814**
- Configurar el intervalo de transferencia del archivo | **815**

Administrar archivos de contabilidad | **816**

Configurar el perfil de interfaz | **817**

- Configurar campos | **818**
- Configurar la información de archivo | **818**
- Configurar estadísticas borradas para que se notifiquen en el archivo sin formato | **818**
- Configurar el intervalo | **819**
- Ejemplo: Configurar el perfil de interfaz | **819**

Configurar el perfil de filtro | **821**

- Configurar los contadores | **821**
- Configurar la información de archivo | **822**
- Configurar el intervalo | **822**

Ejemplo: Configurar un perfil de filtro | **823**

Ejemplo: Configurar perfiles de filtro y contadores de firewall específicos de la interfaz | **824**

Configurar perfiles de uso de clase | **826**

Configurar un perfil de uso de clase | 826
Configurar la información de archivo | 827
Configurar el intervalo | 827
Crear un perfil de uso de clase para recopilar estadísticas de uso de clase de origen | 827
Crear un perfil de uso de clase para recopilar estadísticas de uso de clase de destino | 828

Configurar el perfil MIB | 829

Configurar la información de archivo | 830
Configurar el intervalo | 830
Configurar la operación MIB | 830
Configurar nombres de objetos MIB | 831
Ejemplo: Configurar un perfil MIB | 831

Configurar el perfil del motor de enrutamiento | 832

Configurar campos | 832
Configurar la información de archivo | 833
Configurar el intervalo | 833
Ejemplo: Configurar un perfil de motor de enrutamiento | 833

6

Opciones de monitoreo

Alarmas de interfaz | 836

Descripción general de alarmas | 836

Ejemplo: Configurar alarmas de interfaz | 844

Requisitos | 844
Descripción general | 844
Configuración | 845
Verificación | 847

Monitoreo de IP | 848

Descripción general de la supervisión de IP | 848

Ejemplo: Configurar la supervisión de IP en firewalls de la serie SRX | 851

Requisitos | 851
Descripción general | 851
Configuración | 852
Verificación | 854

Ejemplo: Configurar la supervisión de IP en SRX5000 línea | 855

Requisitos | 855
Descripción general | 855
Configuración | 857
Verificación | 860

Ejemplo: Configurar la supervisión de direcciones IP del grupo de redundancia del clúster de chasis | 863

Requisitos | 864
Descripción general | 864
Configuración | 865
Verificación | 867

Tecnología de monitoreo de sFlow | 869

Descripción general de la tecnología sFlow | 869

Soporte de sFlow en conmutadores | 870

Ejemplo: Configurar sFlow para redes EVPN-VXLAN | 878

Requisitos | 878
Descripción general y topología | 878
Configuración | 880
Verificación | 882
Verificar la tecnología sFlow configurada | 882

Soporte de sFlow en enrutadores | 883

Ejemplo: Configurar la tecnología sFlow para monitorear el tráfico de red | 888

Requisitos | 888
Topología | 889
Configuración | 890
Verificación | 892

Asignación de direcciones del agente de sFlow | 895

Muestreo adaptable para enrutadores y conmutadores | 897

Descripción general del muestreo adaptativo | 897

Software de diagnóstico del acelerador de flujo de paquetes | 902

Descripción general del software de diagnóstico del acelerador de flujo de paquetes y otras utilidades | 902

Puertos externos e internos y puertos de tarjeta de interfaz de red | 903

Acelerador de flujo de paquetes Pruebas y scripts de software de diagnóstico | **905**

Comando Ikondiag | **906**

Pruebas de funcionalidad básica | **907**

Pruebas y scripts de Ethernet | **911**

Pruebas de esfuerzo | **918**

Pruebas de PTP | **919**

Pruebas LED del módulo QFX-PFA-4Q | **922**

Utilidades de diagnóstico del acelerador de flujo de paquetes | **924**

Resultado de ejemplo para el software de diagnóstico del acelerador de paquetes | **930**

Instalar scripts Ethernet y PTP | **938**

Instalar scripts Ethernet y PTP | **938**

Instalar el software de diagnóstico del acelerador de flujo de paquetes | **941**

Descripción general del software de diagnóstico del acelerador de flujo de paquetes | **941**

Verifique que el módulo de expansión QFX-PFA-4Q esté instalado | **942**

Descargue el software de diagnóstico de flujo de paquetes | **943**

Copie el paquete de software de diagnóstico de flujo de paquetes en el conmutador | **943**

Instale el software de diagnóstico de flujo de paquetes en el conmutador | **944**

Configure las opciones de la máquina virtual invitada para iniciar la máquina virtual invitada en el host | **945**

Comprobar que la máquina virtual invitada funciona | **948**

Acceda a la máquina virtual invitada | **949**

Verifique que el módulo FPGA esté funcionando | **951**

Validar las conexiones entre los puertos de red del conmutador QFX5100-24Q-AA y los puertos del módulo QFX-PFA-4Q | **952**

Desinstalar la máquina virtual invitada | **955**

7

Supervisión de características de seguridad comunes

Mostrar información en tiempo real del dispositivo al host | 959

Mostrar información de monitoreo en tiempo real | **959**

Mostrar información de ruta de multidifusión | **963**

Supervisar las políticas de seguridad | 967

Supervisar las estadísticas de la política de seguridad | **967**

Interfaces de supervisión y funciones de conmutación | 968

Mostrar información de la interfaz en tiempo real | **969**

Monitor Interfaces | **972**

Monitorear PPP | **974**

8 **Gestión del rendimiento**

Análisis de red | 976

Descripción general de análisis de red | **976**

Comprender los datos de streaming de análisis de red | **987**

Descripción de la salida de archivos locales de Enhanced Analytics | **995**

Comprender la configuración y el estado de Network Analytics | **998**

Configurar la supervisión de colas y tráfico | **1000**

Configurar un archivo local para datos de análisis de red | **1003**

Configurar un recopilador remoto para datos de Streaming Analytics | **1004**

Ejemplo: Configurar estadísticas de cola y tráfico | **1006**

- Requisitos | **1007**
- Descripción general | **1007**
- Configuración | **1008**
- Verificación | **1011**

Ejemplo: Configurar la supervisión de colas y tráfico | **1015**

- Requisitos | **1016**
- Descripción general | **1016**
- Configuración | **1017**
- Verificación | **1025**

9 **Imitación de puerto**

Duplicación de puertos y analizadores | 1030

Duplicación de puertos y analizadores | **1030**

Descripción de la duplicación de puertos y los analizadores | **1031**

- Términos y definiciones del analizador y la creación de reflejo de puertos | **1033**
- Tipos de instancias | **1037**
- Duplicación de puertos y STP | **1038**
- Restricciones y limitaciones | **1039**
- Duplicación de puertos en conmutadores de la serie QFX10000 | **1044**

Duplicación de puertos en QFabric | **1044**

Duplicación de puertos en conmutadores de la serie OCX | **1046**

Duplicación de puertos en conmutadores EX2300, EX3400 y EX4300 | **1047**

Duplicación de puertos en conmutadores ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 y EX8200 | **1053**

Duplicación de puertos en firewalls de la serie SRX | **1060**

Descripción de la creación de reflejo de puertos de capa 2 | **1060**

Propiedades de duplicación de puertos de capa 2 | **1061**

Aplicación de tipos de duplicación de puertos de capa 2 | **1063**

Restricciones en la duplicación de puertos de capa 2 | **1069**

Configuración de analizadores y duplicación de puertos | **1071**

Descripción de los analizadores de duplicación de puertos | **1071**

Configuración de la creación de reflejo en conmutadores EX9200 para analizar el tráfico (procedimiento de la CLI) | **1079**

Configuración de un analizador para el análisis de tráfico local | **1080**

Configuración de un analizador para el análisis de tráfico remoto | **1081**

Configuración de un analizador estadístico para el análisis de tráfico local | **1083**

Configuración de un analizador estadístico para el análisis de tráfico remoto | **1084**

Enlazar analizadores estadísticos a puertos agrupados en el nivel de FPC | **1086**

Configurar un analizador con varios destinos mediante grupos de salto siguiente | **1087**

Definición de un grupo de salto siguiente para la creación de reflejo de capa 2 | **1088**

Configuración de la creación de reflejo en conmutadores EX4300 para analizar el tráfico (procedimiento de la CLI) | **1089**

Configuración de un analizador para el análisis de tráfico local | **1090**

Configuración de un analizador para el análisis de tráfico remoto | **1091**

Configuración de la creación de reflejo de puertos | **1093**

Configuración de la creación de reflejo de puertos para analizar el tráfico (procedimiento de la CLI) | **1094**

Configuración de la creación de reflejo de puertos para el análisis de tráfico local | **1096**

Configuración de la creación de reflejo de puertos para el análisis de tráfico remoto | **1096**

Filtrado del tráfico que entra en un analizador | **1098**

Verificación de entrada y salida para analizadores de duplicación de puertos en conmutadores de la serie EX | **1099**

Ejemplo: Configuración de analizadores de creación de reflejo de puertos para la supervisión local del uso de recursos de los empleados | **1101**

Requisitos | **1102**

Descripción general y topología | **1102**

Duplicación de todo el tráfico de empleados para análisis local | **1103**

Verificación | **1106**

Ejemplo: Configuración de la creación de reflejo de puertos para la supervisión remota del uso de los recursos de los empleados | **1107**

Requisitos | **1108**

Descripción general y topología | **1108**

Duplicación del tráfico de empleados para el análisis remoto mediante un analizador estadístico | **1110**

Verificación | **1120**

Ejemplo: Configuración de la creación de reflejo en varias interfaces para el monitoreo remoto del uso de recursos de los empleados en conmutadores EX9200 | **1121**

Requisitos | **1122**

Descripción general y topología | **1123**

Duplicación de todo el tráfico de empleados a múltiples interfaces miembro de VLAN para análisis remoto | **1125**

Verificación | **1132**

Ejemplo: Configuración de la duplicación para la supervisión remota del uso de recursos de los empleados mediante un conmutador de tránsito en conmutadores EX9200 | **1133**

Requisitos | **1135**

Descripción general y topología | **1135**

Duplicación de todo el tráfico de empleados para análisis remoto a través de un conmutador de tránsito | **1137**

Verificación | **1143**

Ejemplo: Configuración de la duplicación para el monitoreo local del uso de recursos de los empleados en conmutadores EX4300 | **1144**

Requisitos | **1145**

Descripción general y topología | **1145**

Duplicación de todo el tráfico de empleados para análisis local | **1146**

Duplicación del tráfico de empleados a la web para análisis local | **1148**

Verificación | **1152**

Ejemplo: Configuración de la duplicación para la supervisión remota del uso de recursos de los empleados en conmutadores EX4300 | **1154**

Requisitos | **1155**

Descripción general y topología | **1155**

Duplicación de todo el tráfico de empleados para análisis remoto | **1156**

Duplicación del tráfico de empleados a la web para análisis remoto | **1161**

Verificación | **1167**

Ejemplo: Configuración de la duplicación para el monitoreo remoto del uso de recursos de los empleados a través de un conmutador de tránsito en conmutadores EX4300 | **1168**

Requisitos | **1169**

Descripción general y topología | **1170**

Duplicación de todo el tráfico de empleados para análisis remoto a través de un conmutador de tránsito | **1172**

Verificación | **1178**

Configuración de instancias de creación de reflejo de puertos | **1179**

Instancia global de creación de reflejo de puertos de capa 2 | **1180**

Configuración de la instancia global de creación de reflejo de puertos de capa 2 | **1180**

Instancias con nombre de creación de reflejo de puertos de capa 2 | **1183**

Definición de una instancia con nombre de creación de reflejo de puertos de capa 2 | **1185**

Deshabilitar instancias de creación de reflejo de puertos de capa 2 | **1189**

Configuración de la duplicación de puerto en línea | **1190**

Configuración de la duplicación de puertos en interfaces físicas | **1191**

Precedencia de múltiples niveles de duplicación de puertos de capa 2 en una interfaz física | **1191**

Enlace de la creación de reflejo de puertos de capa 2 a puertos agrupados en el nivel de FPC | **1192**

Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC | **1194**

Ejemplos: Duplicación de puertos de capa 2 en varios niveles del chasis | **1196**

Configuración de la duplicación de puertos de capa 2 a través de la interfaz GRE | **1198**

Ejemplo: Configuración de la duplicación de puertos de capa 2 a través de una interfaz GRE | **1200**

Requisitos | **1200**

Descripción general | **1200**

Configuración | **1201**

Verificación | **1206**

Configuración de la creación de reflejo de puertos en interfaces lógicas | **1207**

Filtros de firewall de duplicación de puertos de capa 2 | **1208**

Definición de un filtro de firewall de duplicación de puertos de capa 2 | **1211**

Configuración del filtro de firewall independiente del protocolo para la creación de reflejo de puertos | **1214**

Ejemplo: Duplicación del tráfico web de los empleados con un filtro de firewall | **1217**

Requisitos | **1217**

Descripción general | **1217**

Configurar | **1218**

Verificación | **1222**

Duplicación de puertos de capa 2 de interfaces lógicas de enrutador PE o conmutador de PE | **1223**

Duplicación de puertos de capa 2 de interfaces Ethernet agregadas de enrutador PE o conmutador PE | **1227**

Aplicación de la creación de reflejo de puertos de capa 2 a una interfaz lógica | **1228**

Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente | **1231**

Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a una instancia de enrutamiento VPLS | **1234**

Aplicación de la duplicación de puertos de capa 2 al tráfico reenviado o inundado a una VLAN | **1236**

Ejemplo: Creación de reflejo de puertos de capa 2 en una interfaz lógica | **1238**

Ejemplo: Duplicación de puertos de capa 2 para una VPN de capa 2 | **1241**

Ejemplo: Duplicación de puertos de capa 2 para una VPN de capa 2 con vínculos LAG | **1244**

Configuración de la duplicación de puertos para varios destinos | **1248**

Descripción de la creación de reflejo de puertos de capa 2 a múltiples destinos mediante grupos de salto siguiente | **1248**

Definición de un grupo de salto siguiente en enrutadores de la serie MX para la duplicación de puertos | **1249**

Ejemplo: Configuración de duplicación de múltiples puertos con grupos de salto en enrutadores serie M, MX y T | **1251**

Ejemplo: Duplicación de puertos de capa 2 a múltiples destinos | **1256**

Configuración de la duplicación de puertos para destinos remotos | **1261**

Espejado de puerto de capa 2 a destino remoto mediante el uso de destino como VLAN | **1261**

Espejado de puertos de capa 2 de configuración a una VLAN remota | **1261**

Configuración de la duplicación de puertos en una VLAN remota | **1262**

Ejemplo: Configuración de la duplicación de puertos de capa 2 para VLAN remota | **1265**

Requisitos | **1266**

Descripción general y topología | **1266**

Duplicación del tráfico de empleados a la web para análisis remoto | **1268**

Verificación | **1273**

Configuración del análisis local y remoto de creación de reflejo de puertos | **1274**

Configuración de la creación de reflejo de puertos | **1275**

Configuración de la creación de reflejo de puertos para el análisis local | **1276**

Configuración de la creación de reflejo de puertos para el análisis remoto | **1277**

Filtrado del tráfico que entra en un analizador | **1278**

Configuración de la duplicación de puertos en firewalls de la serie SRX | **1279**

Ejemplos: Configuración de la creación de reflejo de puertos para el análisis local | **1282**

Requisitos | **1282**

Descripción general y topología | **1282**

Ejemplo: Duplicación de todo el tráfico de empleados para análisis local | **1283**

Ejemplo: Duplicación del tráfico web de los empleados con un filtro de firewall | **1285**

Requisitos | **1285**

Descripción general | **1286**

Configurar | **1286**

Verificación | **1289**

Ejemplo: Configuración de la creación de reflejo de puertos para el análisis remoto | **1291**

Requisitos | **1291**

Descripción general y topología | **1291**

Duplicación de todo el tráfico de empleados para análisis remoto | **1292**

Duplicación del tráfico de empleados a la web para análisis remoto | **1294**

Verificación | **1297**

Duplicación de puerto 1:N a múltiples destinos en conmutadores | **1298**

Duplicación de puertos 1:N: descripción y directrices de configuración | **1299**

Configurar la instancia de creación de reflejo de puertos | **1301**

Configurar el analizador nativo | **1301**

Configurar grupos de salto siguiente | **1302**

Configurar el filtro de firewall | **1302**

Configurar las interfaces | **1302**

Configurar las VLAN | **1302**

Resultados de configuración de ejemplo | **1303**

Supervisión de la duplicación de puertos | **1303**

Visualización de la configuración y el estado de la instancia de duplicación de puertos de capa 2 | **1303**

Visualización de la configuración y el estado del grupo del próximo salto | **1304**

Configurar la duplicación de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3 | **1304**

Descripción de la creación de reflejo de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3 | **1304**

Configurar un filtro con una instancia de creación de reflejo de puerto o con creación de reflejo de puerto global | **1305**

Configurar la creación de reflejo para túneles FTI | **1309**

Puntos de fijación para filtros | 1312

Sugerencias para mejorar la configuración del filtrado de paquetes | 1313

Solución de problemas de duplicación de puertos | 1313

Solución de problemas de duplicación de puertos | 1314

Egress Port Mirroring with VLAN Translation | 1314

Duplicación de puertos de salida con VLAN privadas | 1315

Mensajes de error de configuración de creación de reflejo de puerto | 1316

Una configuración del analizador devuelve el mensaje de error "No se pueden configurar varias interfaces como miembro de la VLAN de salida del analizador" | 1316

10 **Mensajes de registro del sistema**

Información general sobre el registro del sistema | 1319

Descripción general del registro del sistema | 1319

Funciones de registro del sistema y niveles de gravedad de los mensajes | 1322

Configuración predeterminada del registro del sistema | 1324

Mensajes de registro del sistema predeterminados específicos de la plataforma | 1326

Interpretar mensajes generados en formato estándar | 1327

Administrar el registro del sistema operativo host y los archivos principales | 1329

Ver archivos de registro en el sistema operativo host | 1330

Copiar archivos de registro del sistema host al conmutador | 1330

Ver archivos principales en el sistema operativo host | 1330

Copie los archivos principales del sistema host al conmutador | 1331

Limpiar archivos temporales en el sistema operativo host | 1332

Registro del sistema en un sistema de chasis único | 1333

Descripción general de la configuración del registro del sistema de chasis único | 1333

Instrucciones de configuración del registro del sistema de Junos OS | 1335

Configuración mínima de registro del sistema de Junos OS | 1336

Ejemplo: Configurar mensajes de registro del sistema | 1337

Requisitos | 1338

Descripción general | 1338

Configuración | 1338

Mensajes de registro en formato de datos estructurados | **1341**

Especificar el tamaño, el número y las propiedades de archivado del archivo de registro | **1341**

Incluir información de prioridad en los mensajes de registro del sistema | **1343**

Códigos de instalación de registro del sistema y códigos numéricos consignados en la información de prioridad | **1345**

Incluir el año o milisegundo en las marcas de tiempo | **1348**

Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados | **1349**

Junos System registra operadores de expresiones regulares para la instrucción match | **1352**

Deshabilitar el registro del sistema de una instalación | **1353**

Ejemplos: Configurar el registro del sistema | **1354**

Ejemplos: Asignar una instalación alternativa | **1356**

Registro del sistema para un enrutador TX Matrix o TX Matrix Plus | 1357

Configuración del registro del sistema para un enrutador TX Matrix | **1358**

Configuración del registro del sistema para un enrutador TX Matrix Plus | **1360**

Configuración del reenvío de mensajes al enrutador de matriz de transmisión | **1362**

Configuración del reenvío de mensajes al enrutador TX Matrix Plus | **1363**

Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix | **1365**

Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix Plus | **1368**

Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix | **1371**

- Incluir información de prioridad en los mensajes reenviados | **1372**
- Agregar una cadena de texto a mensajes reenviados | **1373**
- Usar expresiones regulares para refinar el conjunto de mensajes reenviados | **1373**

Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix Plus | **1373**

- Incluir información de prioridad en los mensajes reenviados | **1374**
- Agregar una cadena de texto a mensajes reenviados | **1375**
- Usar expresiones regulares para refinar el conjunto de mensajes reenviados | **1375**

Configuración del registro del sistema de manera diferente en cada enrutador T640 en una matriz de enrutamiento | **1375**

Configuración del registro del sistema de manera diferente en cada enrutador T1600 o T4000 en una matriz de enrutamiento | **1377**

Dirija los mensajes de registro del sistema a un destino remoto | 1379

Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro | **1380**

Dirija los mensajes de registro del sistema a un archivo de registro | **1383**

Dirigir mensajes de registro del sistema a un terminal de usuario | **1384**

Dirija los mensajes de registro del sistema a la consola | **1385**

Dirija los mensajes de registro del sistema a un equipo remoto o a otro motor de enrutamiento | **1385**

Especificar una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto | **1387**

Agregar una cadena de texto a los mensajes de registro del sistema dirigidos a un destino remoto | **1387**

Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto | **1388**

Funciones predeterminadas para los mensajes de registro del sistema dirigidos a un destino remoto | **1391**

Facilidades alternativas para mensajes de registro del sistema dirigidos a un destino remoto | **1391**

Ejemplos: Asignar una función alternativa al sistema Mensajes de registro dirigidos a un destino remoto | **1393**

Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión | **1394**

Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en un enrutador TX Matrix Plus | **1395**

Mostrar archivos de registro del sistema | 1396

Mostrar un archivo de registro desde un sistema de chasis único | **1397**

Contenido de muestra del archivo de registro | **1397**

Mostrar un archivo de registro desde una matriz de enrutamiento | **1400**

Mostrar archivos de registro MD5 | **1401**

Configurar el registro del sistema para dispositivos de seguridad | 1402

Descripción general del registro del sistema para dispositivos de seguridad | **1403**

Formato binario para registros de seguridad | **1405**

Registro e informes en la caja | **1406**

Supervisar informes | **1414**

Informe de monitoreo de amenazas | **1415**

Informe de monitoreo de tráfico | **1423**

Configurar archivos de registro de seguridad binaria en caja | **1426**

Configurar archivos de registro de seguridad binaria fuera de la caja | **1428**

Configurar archivos de registro de seguridad de Protobuf en caja en modo de evento | **1430**

Configurar archivos de registro de seguridad de Protobuf en caja en modo de secuencia | **1431**

Configurar archivos de registro de seguridad de Protobuf fuera de la caja | **1433**

Enviar mensajes de registro del sistema a un archivo | **1434**

Configurar el sistema para enviar todos los mensajes de registro a través de eventd | **1435**

Configurar Syslog a través de TLS | 1436

Registros del plano de control | **1437**

Ejemplo: Configurar Syslog a través de TLS | **1437**

Requisitos | **1437**

Descripción general | **1438**

Configuración | **1438**

Registros del plano de datos | **1442**

Ejemplo: Configurar el protocolo TLS Syslog en firewalls de la serie SRX | **1442**

Requisitos | **1443**

Descripción general | **1443**

Configuración | **1443**

Verificación | **1447**

Supervisar mensajes de registro | 1447

Supervisar mensajes de registro del sistema | **1447**

11

Administración de red y solución de problemas

Monitoreo y solución de problemas | 1451

Ping Hosts | **1451**

Supervisar el tráfico a través del enrutador o conmutador | **1453**

Mostrar estadísticas en tiempo real sobre todas las interfaces del enrutador o conmutador | **1453**

Mostrar estadísticas en tiempo real sobre una interfaz en el enrutador o conmutador | **1455**

Descripción general de la memoria direccionable de contenido ternario dinámico | **1458**

Resolución de problemas de resolución de nombres DNS en directivas de seguridad del sistema lógico (solo administradores principales) | **1474**

Solución de problemas de la interfaz de servicios de vínculo | **1475**

Determinar qué componentes de CoS se aplican a los vínculos constituyentes | **1475**

Determinar qué causa la fluctuación y la latencia en el paquete multivínculo | **1479**

Determinar si LFI y equilibrio de carga funcionan correctamente | **1479**

Determinar por qué se dejan caer paquetes en un PVC entre un dispositivo de Juniper Networks y un dispositivo de terceros | **1488**

Solución de problemas de las políticas de seguridad | **1488**

Sincronización de políticas entre el motor de enrutamiento y el motor de reenvío de paquetes | **1489**

Comprobación de un error de confirmación de política de seguridad | **1490**

Comprobación de una confirmación de política de seguridad | **1491**

Depurar búsqueda de directivas | **1492**

Registrar mensajes de error utilizados para solucionar problemas relacionados con ISSU | **1493**

Errores de proceso del chasis | **1493**

Descripción del control de errores comunes para ISSU | **1494**

Errores relacionados con soporte técnico de ISSU | **1498**

Error en las comprobaciones de validación inicial | **1498**

Errores relacionados con la instalación | **1500**

Errores de conmutación por error del grupo de redundancia | **1501**

Errores de sincronización de estado del kernel | **1502**

Solución de problemas del rendimiento del sistema con la metodología de monitoreo de recursos | 1503

Descripción general del cálculo del uso de la supervisión de recursos | **1503**

Diagnóstico y depuración del rendimiento del sistema mediante la configuración de la supervisión del uso de recursos de memoria en enrutadores de la serie MX | **1506**

Solucionar problemas de la discrepancia de los valores de jnxNatObjects para MS-DPC y MS-MIC | **1510**

Objetos administrados para la memoria Ukernel para un motor de reenvío de paquetes en una ranura FPC | **1512**

Objetos administrados para datos estadísticos de memoria del motor de reenvío de paquetes | **1512**

Objetos administrados para el próximo salto, Jtree y memoria de filtro de firewall para un motor de reenvío de paquetes en una ranura FPC | **1513**

jnxPfeMemoryErrorsTable | **1513**

pfeMemoryErrors | **1514**

Configuración de las opciones de depuración y rastreo de rutas de datos | 1515

Descripción de la depuración de rutas de datos para dispositivos de la serie SRX | **1515**

Captura de paquetes desde el modo operativo | **1516**

Descripción de la depuración de seguridad mediante opciones de seguimiento | **1517**

Descripción de la depuración de flujos mediante opciones de seguimiento | **1518**

Depurar la ruta de datos (procedimiento de la CLI) | **1518**

Configuración de opciones de seguimiento de depuración de flujo (procedimiento de CLI) | **1519**

Configuración de opciones de seguimiento de seguridad (procedimiento de CLI) | **1520**

Visualización de archivos de registro y seguimiento | **1522**

Mostrar resultados para las opciones de seguimiento de seguridad | **1523**

Visualización de operaciones de seguimiento de multidifusión | **1524**

Visualización de una lista de dispositivos | **1525**

Ejemplo: Configuración de la depuración de extremo a extremo en un dispositivo de la serie SRX | **1527**

- Requisitos | **1528**
- Descripción general | **1528**
- Configuración | **1529**
- Habilitar la depuración de rutas de datos | **1531**
- Verificación | **1532**

Uso de MPLS para diagnosticar LSP, VPN y circuitos de capa 2 | 1534

Descripción general de la comprobación de conexión MPLS | **1534**

Uso de la captura de paquetes para analizar el tráfico de red | 1538

Descripción general de la captura de paquetes | **1539**

Ejemplo: Habilitar la captura de paquetes en un dispositivo | **1542**

Requisitos | **1542**

Descripción general | **1543**

Configuración | **1543**

Verificación | **1545**

Ejemplo: Configurar la captura de paquetes en una interfaz | **1547**

Requisitos | **1548**

Descripción general | **1548**

Configuración | **1548**

Verificación | **1549**

Ejemplo: Configurar un filtro de firewall para la captura de paquetes | **1550**

Requisitos | **1550**

Descripción general | **1550**

Configuración | **1551**

Verificación | **1553**

Ejemplo: Configurar la captura de paquetes para la depuración de rutas de datos | **1553**

Requisitos | **1554**

Descripción general | **1554**

Configuración | **1554**

Verificación | **1557**

Deshabilitar la captura de paquetes | **1558**

Modificar la encapsulación en interfaces con la captura de paquetes configurada | **1558**

Eliminar archivos de captura de paquetes | **1560**

Mostrar encabezados de paquetes | **1561**

Solución de problemas de dispositivos de seguridad | 1568

Resolución de problemas de resolución de nombres DNS en directivas de seguridad del sistema lógico (solo administradores principales) | **1568**

Solución de problemas de la interfaz de servicios de vínculo | **1569**

Determinar qué componentes de CoS se aplican a los vínculos constituyentes | **1570**

Determinar qué causa la fluctuación y la latencia en el paquete multivínculo | **1574**

Determinar si LFI y equilibrio de carga funcionan correctamente | **1574**

Determinar por qué se dejan caer paquetes en un PVC entre un dispositivo de Juniper Networks y un dispositivo de terceros | **1583**

Solución de problemas de las políticas de seguridad | **1583**

Sincronización de políticas entre el motor de enrutamiento y el motor de reenvío de paquetes | **1584**

Comprobación de un error de confirmación de política de seguridad | **1585**

Comprobación de una confirmación de política de seguridad | **1586**

Depurar búsqueda de directivas | **1587**

12 **Instrucciones de configuración y comandos operativos**

Descripción general de referencia de la CLI de Junos | 1589

Acerca de esta guía

Utilice esta guía para implementar y configurar las tecnologías de administración de red compatibles con Junos OS: Protocolo simple de administración de red (SNMP), supervisión remota (RMON), datos de uso de clase de destino (DCU) y uso de clase de origen (SCU) y perfiles de contabilidad. Se incluyen alarmas, eventos y funciones de seguridad, así como información sobre la administración del rendimiento, la duplicación y los analizadores de puertos, y el registro del sistema.

VÍNCULOS RELACIONADOS

- Explorador SNMP MIB

1

PART IN COVERPAGE

Descripción general

Funciones de administración de dispositivos en Junos OS | 2

Funciones de administración de dispositivos y redes | 5

Operaciones de seguimiento y registro | 11

Soporte de Junos Space para la administración de red | 13

Descripción general de las herramientas de diagnóstico | 14

Funciones de administración de dispositivos en Junos OS

summary

En esta sección se ofrece una descripción general de Junos OS (sistema operativo).

Después de instalar un dispositivo en su red, debe administrar el dispositivo dentro de su red. La administración de dispositivos se puede dividir en cinco tareas:

- Administración de fallas: supervise el dispositivo; Detectar y corregir fallos.
- Gestión de la configuración: permite configurar los atributos del dispositivo.
- Gestión contable: recopila estadísticas con fines contables.
- Administración del rendimiento: supervise y ajuste el rendimiento de los dispositivos.
- Administración de seguridad: controle el acceso a los dispositivos y autentique a los usuarios.

Las funciones de administración de red del sistema operativo Junos (Junos® OS) funcionan junto con un sistema de soporte de operaciones (OSS) para administrar los dispositivos dentro de la red. Junos OS puede ayudarle a realizar estas tareas de administración, tal y como se describe en Tabla 1 en la página 3.

Tabla 1: Funciones de administración de dispositivos en Junos OS

Tarea	Función Junos OS
Gestión de fallos	Monitoree y vea fallas mediante: • Comandos del modo operativo: para obtener más información acerca de los comandos del modo operativo, consulte el Explorador de CLI. • MIB SNMP: para obtener más información acerca de las MIB SNMP compatibles con Junos OS, consulte el archivo ."MIB SNMP compatibles con Junos OS y Junos OS Evolved" en la página 600 • Capturas SNMP estándar: para obtener más información acerca de las capturas SNMP estándar, consulte la ."MIB SNMP compatibles con Junos OS y Junos OS Evolved" en la página 600 • Capturas SNMP específicas de la empresa: para obtener más información acerca de las capturas específicas de la empresa, consulte "Capturas SNMP específicas de la empresa compatibles con Junos OS".https://www.juniper.net/documentation/en_US/junos/topics/concept/enterprise-specific-traps-overview.html • Mensajes de registro del sistema: para obtener más información acerca de cómo ver los mensajes de registro del sistema, consulte el Explorador de registros del sistema.https://apps.juniper.net/syslog-explorer/
Gestión de la configuración	• Configure los atributos del enrutador mediante la interfaz de línea de comandos (CLI), el protocolo de administración XML de Junos y el protocolo de administración XML de NETCONF. Para obtener más información acerca de cómo configurar el enrutador mediante las API, consulte la Guía del protocolo de administración XML de Junos y la Guía del protocolo de administración XML deNETCONF. • MIB de administración de configuración: para obtener más información acerca de la MIB de administración de configuración, consulte MIB de administración de configuración.https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-cfgmgmt.txt

Tabla 1: Funciones de administración de dispositivos en Junos OS *(Continued)*

Tarea	Función Junos OS
Gestión contable	Realice las siguientes tareas relacionadas con la contabilidad: • Recopile estadísticas para interfaces, filtros de firewall, clases de destino, clases de origen y el motor de enrutamiento. Para obtener más información acerca de la recopilación de estadísticas, vea Configuración de opciones de contabilidad."Configuración de opciones de contabilidad" en la página 799 • Utilice estadísticas de tráfico específicas de la interfaz y otros contadores, disponibles en la MIB de interfaces estándar, las extensiones específicas de la empresa de Juniper Networks para la MIB de interfaces y las MIB específicas de medios, como la MIB ATM específica de la empresa. • Use contadores de circuito virtual (VC) por ATM, disponibles en la MIB ATM específica de la empresa. Para obtener más información acerca de la MIB ATM, consulte MIB ATM.https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-atm.txt • Agrupe los prefijos de origen y destino en clases de origen y clases de destino y cuente los paquetes para esas clases. Recopilar estadísticas de uso de clases de destino y clases de origen. Para obtener más información acerca de las clases, consulte "MIB de uso de clase de destino" y "MIB de uso de clase de origen", Configuración de perfiles de uso de clase, la biblioteca de interfaces de red de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-dcu.txthttps://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-scu.txt"Configurar perfiles de uso de clase" en la página 826 • Cuente los paquetes como parte de un filtro de firewall. Para obtener más información acerca de las políticas de filtro de firewall, consulte MIB SNMP específicas de la empresa compatibles con Junos OS."MIB SNMP específicas de la empresa compatibles con Junos OS" en la página 650 • Muestree el tráfico, recopile los ejemplos y envíelos a un host que ejecute la utilidad cflowd de CAIDA.

Tabla 1: Funciones de administración de dispositivos en Junos OS *(Continued)*

Tarea	Función Junos OS
Gestión del rendimiento	Puede supervisar el rendimiento de las siguientes maneras: • Utilice comandos del modo operativo. Para obtener más información acerca de la supervisión del rendimiento mediante los comandos del modo operativo, consulte el Explorador de CLI.https://www.juniper.net/documentation/content-applications/cli-explorer/junos/ • Utilice el filtro de firewall. • Muestree el tráfico, recopile los ejemplos y envíelos a un host que ejecute la utilidad cflowd de CAIDA. • Use la MIB de clase de servicio específica de la empresa. Para obtener más información acerca de esta MIB, vea MIB de clase de servicio.https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-cos.txt
Gestión de la seguridad	Garantice la seguridad de su red de las siguientes maneras: • Controle el acceso al enrutador y autentique a los usuarios. • Controle el acceso al enrutador mediante SNMPv3 y SNMP a través de IPv6. Para obtener más información, consulte y Seguimiento de la actividad SNMP en un dispositivo que ejecuta Junos OS."Configurar ID de motor local en SNMPv3" en la página 556"Rastrear la actividad SNMP en un dispositivo que ejecuta Junos OS" en la página 541

Funciones de administración de dispositivos y redes

Los dispositivos Juniper admiten funciones que le permiten administrar el rendimiento del sistema, la supervisión de fallas y el acceso remoto.

Puede utilizar los comandos del modo operativo de la CLI para supervisar el estado del sistema y el rendimiento de la red. Las herramientas y comandos de supervisión muestran el estado actual del dispositivo. Puede filtrar la salida a un archivo. Las herramientas de diagnóstico y los comandos prueban la conectividad y accesibilidad de los hosts de la red.

En este tema se describen las funciones disponibles. Para utilizar las herramientas operativas de la CLI, debe tener los privilegios de acceso adecuados.

Tabla 2 en la página 6 enumera las características de administración de red.

Tabla 2: Funciones de administración de dispositivos y redes en las series QFX, OCX y EX4600

Característica	Usos típicos	Documentación
Alarmas y LED en el conmutador: muestra el estado de los componentes de hardware e indica condiciones de advertencia o error.	Gestión de fallos	*Mensajes de alarma del chasis en un dispositivo QFX3500*
Filtros de firewall: controle los paquetes que se envían hacia y desde la red, equilibre el tráfico de red y optimice el rendimiento.	Gestión del rendimiento	• Guía del usuario de políticas de enrutamiento, filtros de firewall y políticas de tráfico • *Descripción general de los filtros de firewall (serie QFX)*
Administración en banda: permite la conexión al conmutador utilizando las mismas interfaces por las que fluye el tráfico del cliente. La comunicación entre el conmutador y una consola remota se habilita mediante los servicios SSH y Telnet. SSH proporciona comunicaciones cifradas seguras, mientras que Telnet proporciona acceso sin cifrar y, por lo tanto, menos seguro, al conmutador.	Gestión de acceso remoto	• Configuración del servicio SSH para el acceso remoto al enrutador o conmutador • Configuración del servicio Telnet para el acceso remoto a un enrutador o conmutador

Tabla 2: Funciones de administración de dispositivos y redes en las series QFX, OCX y EX4600 *(Continued)*

Característica	Usos típicos	Documentación
Scripts de automatización de Junos OS de Juniper Networks: las herramientas de configuración y automatización de operaciones proporcionadas por Junos OS incluyen scripts de confirmación, scripts de operación, scripts de eventos y políticas de eventos. Los scripts de confirmación imponen reglas de configuración personalizadas, mientras que los scripts de operación, las políticas de eventos y los scripts de eventos automatizan la solución de problemas y la administración de la red.	• Gestión de la configuración • Gestión del rendimiento • Gestión de fallos	Guía del usuario de scripts de automatización
Interfaz de línea de comandos (CLI) de Junos OS: las instrucciones de configuración de CLI le permiten configurar el conmutador en función de sus requisitos de red, como la seguridad, el servicio y el rendimiento.	• Gestión de la configuración • Gestión del rendimiento • Gestión de acceso de usuarios • Gestión de acceso remoto	Guía del usuario de CLI para Junos OS
Software Junos Space: el sistema de administración de red basado en GUI multipropósito incluye una plataforma base, la plataforma de aplicaciones de red y otras aplicaciones opcionales como Diseño Ethernet, Service Now, Service Insight y Control virtual. **NOTA**: Junos Space no es compatible con la serie OCX.	• Gestión de la configuración • Gestión del rendimiento • Gestión de fallos	Soporte de Junos Space para la administración de red

Tabla 2: Funciones de administración de dispositivos y redes en las series QFX, OCX y EX4600 *(Continued)*

Característica	Usos típicos	Documentación
API XML de Junos: representación XML de instrucciones de configuración y comandos de modo operativo de Junos OS. La API XML de Junos también incluye elementos de etiqueta que son la contraparte de las instrucciones de configuración de la CLI de Junos.	• Gestión de la configuración • Gestión del rendimiento • Gestión de fallos	*Descripción general de la API XML de Junos*
Protocolo de administración XML NETCONF: protocolo de administración basado en XML que utilizan las aplicaciones cliente para solicitar y cambiar la información de configuración en plataformas de enrutamiento, conmutación y seguridad que ejecutan Junos OS. El protocolo de administración XML de NETCONF define operaciones básicas que son equivalentes a los comandos del modo de configuración de la CLI de Junos OS. Las aplicaciones cliente utilizan las operaciones de protocolo para mostrar, editar y confirmar instrucciones de configuración (entre otras operaciones), ya que los administradores utilizan comandos del modo de configuración de CLI como , y para realizar esas operaciones.`showsetcommit`	• Gestión de la configuración • Gestión del rendimiento • Gestión de fallos	Guía para desarrolladores del protocolo de administración XML de NETCONF

Tabla 2: Funciones de administración de dispositivos y redes en las series QFX, OCX y EX4600 *(Continued)*

Característica	Usos típicos	Documentación
Comandos del modo operativo: • Supervise el rendimiento del conmutador. Por ejemplo, el comando muestra el uso de CPU del motor de enrutamiento.`show chassis routing-engine` El uso elevado de la CPU del motor de enrutamiento puede afectar al rendimiento del conmutador. • Ver la actividad actual y el estado del dispositivo o la red. Por ejemplo, puede usar el comando para supervisar y diagnosticar problemas de conectividad y el comando para buscar puntos de error en la red.`ping` `traceroute`	• Gestión del rendimiento • Gestión de fallos	Explorador de CLI
Administración fuera de banda: permite la conexión al conmutador a través de una interfaz de administración. La administración fuera de banda se admite en dos interfaces Ethernet de administración dedicadas, así como en la consola y los puertos auxiliares. Las interfaces Ethernet de administración se conectan directamente al motor de enrutamiento. El tráfico de tránsito no está permitido a través de las interfaces, lo que garantiza que la congestión o los fallos en la red de tránsito no afecten la administración del conmutador.	Gestión de acceso remoto	• *Conectar un dispositivo a una red para administración fuera de banda* • *Conexión de un dispositivo de la serie QFX a una consola de administración*

Tabla 2: Funciones de administración de dispositivos y redes en las series QFX, OCX y EX4600 *(Continued)*

Característica	Usos típicos	Documentación
MIB de administración de configuración SNMP: proporciona notificaciones para los cambios de configuración en forma de capturas SNMP. Cada interrupción contiene la hora a la que se confirmó el cambio de configuración, el nombre del usuario que realizó el cambio y el método mediante el cual se realizó el cambio. El historial de los últimos 32 cambios de configuración se coloca en jnxCmChgEventTable.	Gestión de la configuración	Explorador SNMP MIB
MIB y capturas SNMP: permiten la supervisión de dispositivos de red desde una ubicación central. Utilice solicitudes SNMP como y para supervisar y ver la actividad del sistema.`getwalk` El conmutador QFX3500 admite SNMP versión 1 (v1), v2 y v3, y capturas y MIB estándar y específicas de la empresa de Juniper Networks.	Gestión de fallos	• Explorador SNMP MIB • "Descripción de la implementación de SNMP en Junos OS" en la página 388
Mensajes de registro del sistema: registra detalles de eventos del sistema y del usuario, incluidos los errores. Puede especificar la gravedad y el tipo de mensajes de registro del sistema que desea ver o guardar, y configurar la salida que se enviará a hosts locales o remotos.	• Gestión de fallos • Gestión de acceso de usuarios	• Explorador de registros del sistema • "Información general sobre el registro del sistema" en la página 1319 • "Descripción general de la configuración del registro del sistema de chasis único" en la página 1333

Operaciones de seguimiento y registro

Las operaciones de seguimiento y registro permiten realizar un seguimiento de los eventos que se producen en el conmutador (tanto las operaciones normales como las condiciones de error) y realizar un seguimiento de los paquetes generados por el conmutador o que pasan a través de él. Los resultados de las operaciones de seguimiento y registro se colocan en el directorio del conmutador.**/var/log**

Junos OS admite el rastreo remoto para los siguientes procesos:

- chassisd: proceso de control del chasis
- eventd: proceso de procesamiento de eventos
- cosd: proceso de clase de servicio

El seguimiento remoto se configura mediante la instrucción en el nivel de jerarquía.`tracing[edit system]`

> **NOTA**: La instrucción no se admite en el sistema QFX3000 QFabric.`tracing`

Puede deshabilitar el seguimiento remoto para procesos específicos del conmutador mediante la instrucción en el nivel de jerarquía.`no-remote-trace[edit` *`process-name`* `traceoptions]`

Las operaciones de registro utilizan un mecanismo de registro del sistema similar a la utilidad syslogd de UNIX para registrar operaciones de alto nivel en todo el sistema, como interfaces que suben o bajan y usuarios que inician o cierran sesión en el conmutador. Estas operaciones se configuran utilizando la instrucción en el nivel de jerarquía y utilizando la instrucción en el nivel de jerarquía.`syslog[edit system]options[edit ethernet-switching-options]`

Las operaciones de rastreo registran información más detallada sobre las operaciones del conmutador, incluida la información de enrutamiento y reenvío de paquetes. Puede configurar operaciones de seguimiento mediante la instrucción.`traceoptions`

> **NOTA**: La instrucción no se admite en el sistema QFX3000 QFabric.`traceoptions`

Puede definir operaciones de seguimiento en diferentes partes de la configuración del conmutador:

- Operaciones de seguimiento de actividad del agente SNMP: defina el seguimiento de las actividades de los agentes SNMP en el conmutador. Puede configurar operaciones de seguimiento de actividad del agente SNMP en el nivel jerárquico .`[edit snmp]`

- Operaciones globales de seguimiento de conmutación: defina el seguimiento para todas las operaciones de conmutación. Las operaciones de seguimiento de conmutación global se configuran en el nivel jerárquico .`[edit ethernet-switching-options]`

- Operaciones de seguimiento específicas del protocolo: defina el seguimiento para un protocolo de enrutamiento específico. Las operaciones de seguimiento específicas del protocolo se configuran en la jerarquía.`[edit protocols]` Las operaciones de seguimiento específicas del protocolo invalidan cualquier operación equivalente que especifique en la instrucción global .`traceoptions`

- Operaciones de seguimiento dentro de entidades de protocolo de enrutamiento individuales: algunos protocolos permiten definir operaciones de seguimiento más granulares. Por ejemplo, en el Protocolo de puerta de enlace de borde (BGP), puede configurar operaciones de seguimiento específicas del mismo nivel. Estas operaciones anulan cualquier operación equivalente de todo el BGP. Si no especifica ninguna operación de seguimiento específica del mismo nivel, los pares heredan, en primer lugar, todas las operaciones de seguimiento de todo el BGP y, en segundo lugar, las operaciones de seguimiento globales.

- Operaciones de seguimiento de interfaz: defina el seguimiento para interfaces individuales y para el propio proceso de interfaz. Las operaciones de seguimiento de interfaz se definen en el nivel jerárquico .`[edit interfaces]`

- Seguimiento remoto: para habilitar el seguimiento remoto en todo el sistema, configure la instrucción en el nivel jerárquico .`destination-override syslog host[edit system tracing]` Esto especifica el host remoto que ejecuta el proceso de registro del sistema (syslogd), que recopila los seguimientos. Las trazas se escriben en archivos del host remoto de acuerdo con la configuración syslogd de **./etc/syslog.conf** De forma predeterminada, el seguimiento remoto no está configurado.

  Para invalidar la configuración de seguimiento remoto en todo el sistema para un proceso determinado, incluya la instrucción en la jerarquía.`no-remote-trace[edit` *`process-name`* `traceoptions]` Cuando está habilitado, el proceso realiza un seguimiento local.`no-remote-trace`

  Para recopilar seguimientos, utilice la función local0 como selector del archivo en el host remoto.**/etc/syslog.conf** Para separar rastros de varios procesos en diferentes archivos, incluya el nombre del proceso o el nombre del archivo de seguimiento (si se especifica en el nivel de jerarquía [editar]) en el campo Programa del archivo.*`process-name`* `traceoptions file`**/etc/syslog.conf** Si el servidor de registro del sistema admite el análisis del nombre de host y del nombre del programa, puede separar los seguimientos de los distintos procesos.

NOTA: Durante una comprobación de confirmación, las advertencias sobre la configuración (por ejemplo, no coinciden en los tamaños de los archivos de seguimiento o el número de archivos de seguimiento) no se muestran en la consola.`traceoptions` Sin embargo, estas advertencias se registran en los mensajes de registro del sistema cuando se confirma la nueva configuración.

Soporte de Junos Space para la administración de red

in this section

- Preparación del dispositivo para Junos Space Management | 13

La aplicación Junos Space de Juniper Networks, que se ejecuta en un dispositivo virtual Junos Space, es una plataforma completa para crear e implementar aplicaciones. Esto permite la colaboración, la productividad y la gestión de la infraestructura de red y las operaciones. Junos Space proporciona un entorno de tiempo de ejecución implementado como una estructura de dispositivos virtuales y físicos.

Preparación del dispositivo para Junos Space Management

Requisitos previos

Asegúrese de que la configuración del dispositivo de la serie QFX cumple los siguientes requisitos para la detección de dispositivos en Junos Space:

- La configuración del dispositivo tiene una dirección IP de administración estática a la que se puede acceder desde el servidor de Junos Space.
- Hay un usuario con privilegios administrativos completos para la administración de Junos Space.
- SNMP está habilitado (solo si planea usar SNMP como parte de la detección de dispositivos).
- En Junos Space, configure un esquema de interfaz de administración de dispositivos (DMI) predeterminado para el dispositivo de la serie QFX.

Para preparar el dispositivo antes de usar Junos Space:

1. Realice la configuración inicial del dispositivo a través del puerto de la consola mediante la CLI de Junos OS. Esta tarea incluye la configuración de una dirección IP de administración estática y un usuario con privilegios administrativos raíz.

   Para el conmutador QFX3500, consulte Configuración de un dispositivo QFX3500 como conmutador independiente.

Para el sistema QFabric, consulte Información de configuración inicial y predeterminada del sistema QFabric y Realización de la configuración inicial del sistema QFabric en un grupo QFX3100 director.*QFabric System Initial and Default Configuration InformationPerforming the QFabric System Initial Setup on a QFX3100 Director Group*

2. (Opcional) Configure SNMP si planea usar SNMP para sondear dispositivos durante la detección de dispositivos.

3. (Opcional) Active SSH si desea utilizar la función Consola segura en Junos Space.

   Consulte Conexión a un dispositivo mediante Secure Console.https://www.juniper.net/documentation/us/en/software/junos-space22.3/junos-space-workspaces/topics/task/junos-space-devices-ssh-connecting.html

4. En Junos Space, configure un esquema DMI predeterminado. Para obtener más información acerca de la administración de esquemas DMI, consulte:

   Establecer un esquema DMI predeterminado.https://www.juniper.net/documentation/us/en/software/junos-space22.3/junos-space-workspaces/topics/task/junos-space-network-application-platform-schema-default-setting.html

VÍNCULOS RELACIONADOS

Plataforma de administración de red de Junos Space

Descripción general de las herramientas de diagnóstico

in this section

- Herramientas de diagnóstico de J-Web | **15**
- Comandos de diagnóstico de CLI | **16**

Los dispositivos Juniper Networks admiten un conjunto de herramientas J-Web y comandos de modo operativo CLI para evaluar el estado y el rendimiento del sistema. Las herramientas de diagnóstico y los comandos prueban la conectividad y accesibilidad de los hosts de la red.

- Utilice las opciones de diagnóstico de J-Web para diagnosticar un dispositivo. Los resultados de J-Web aparecen en el navegador.
- Utilice los comandos del modo operativo de la CLI para diagnosticar un dispositivo. Puede ver la salida del comando de la CLI en la consola o en el dispositivo de administración. Puede filtrar la salida a un archivo.

Para utilizar la interfaz de usuario de J-Web y las herramientas operativas de la CLI, debe tener los privilegios de acceso adecuados.

Esta sección contiene los siguientes temas:

Herramientas de diagnóstico de J-Web

Las herramientas de diagnóstico de J-Web constan de las opciones que aparecen al seleccionar y en la barra de tareas. describe las funciones de las opciones de solución de problemas. Troubleshoot**Maintain**Tabla 3 en la página 15

Tabla 3: Opciones de solución de problemas de la interfaz J-Web

La opción	Función
Opciones de solución de problemas	
Ping Host	Le permite hacer ping a un host remoto. Puede configurar opciones avanzadas para la operación de ping.
Ping MPLS	Permite hacer ping a un extremo MPLS mediante varias opciones.
Traceroute	Le permite rastrear una ruta entre el dispositivo y un host remoto. Puede configurar opciones avanzadas para la operación traceroute.
Packet Capture	Le permite capturar y analizar el tráfico de control del enrutador.
Mantener opciones	
Files	Le permite administrar archivos de registro, temporales y principales en el dispositivo.

Tabla 3: Opciones de solución de problemas de la interfaz J-Web *(Continued)*

La opción	Función
Upgrade	Le permite actualizar y administrar paquetes de Junos OS.
Licenses	Muestra el resumen de las licencias necesarias y utilizadas para cada característica que requiere una licencia. Permite añadir licencias.
Reboot	Permite reiniciar el dispositivo a una hora especificada.

Comandos de diagnóstico de CLI

Los comandos de CLI disponibles en modo operativo le permiten realizar las mismas tareas de monitoreo, solución de problemas y administración que puede realizar con la interfaz de usuario de J-Web. En lugar de invocar las herramientas a través de una interfaz gráfica, utilice comandos de modo operativo para realizar las tareas.

La salida del comando CLI aparece en la pantalla de la consola o del dispositivo de administración, o puede filtrar la salida a un archivo. En el caso de los comandos operativos que muestran resultados, como los comandos, puede redirigir el resultado a un filtro o a un archivo.`show` Cuando se muestra ayuda sobre estos comandos, una de las opciones enumeradas es , denominada canalización, que permite filtrar la salida del comando.`|`

Puede utilizar el comando para mostrar información de seguimiento de una ruta de multidifusión desde un origen a un receptor.`mtrace`

Para ver una lista de comandos del modo operativo de nivel superior, escriba un signo de interrogación (?) en el símbolo de la línea de comandos.

Puede ver los comandos de diagnóstico de CLI en el nivel superior del modo operativo enumerado en .Tabla 4 en la página 16

Tabla 4: Resumen de comandos de diagnóstico de CLI

Comando	Función
Control del entorno de CLI	

Tabla 4: Resumen de comandos de diagnóstico de CLI *(Continued)*

Comando	Función
`set` *`option`*	Configura la visualización de la CLI.
Diagnóstico y solución de problemas	
`clear`	Borra las estadísticas y la información de la base de datos de protocolos.
`mtrace`	Rastrea información sobre rutas de multidifusión desde el origen hasta el receptor.
`monitor`	Realiza la depuración en tiempo real de varios componentes de Junos OS, incluidos los protocolos de enrutamiento y las interfaces.
`ping`	Determina la accesibilidad de un host de red remoto.
`ping mpls`	Determina la accesibilidad de un extremo MPLS mediante varias opciones.
`test`	Prueba la configuración y aplicación de filtros de políticas y expresiones regulares de ruta de AS.
`traceroute`	Rastrea la ruta a un host de red remoto.
Conexión a otros sistemas de red	
`ssh`	Abre conexiones de shell seguras.
`telnet`	Abre sesiones de Telnet a otros hosts de la red.
administración	
`copy`	Copia archivos de una ubicación del dispositivo a otra, del dispositivo a un sistema remoto o de un sistema remoto al dispositivo.

Tabla 4: Resumen de comandos de diagnóstico de CLI *(Continued)*

Comando	Función
`restart` *`option`*	Reinicia los distintos procesos del sistema, incluidos el protocolo de enrutamiento, la interfaz y los procesos SNMP.
`request`	Realiza operaciones a nivel del sistema, como detener y reiniciar el dispositivo y cargar imágenes de Junos OS.
`start`	Sale de la CLI e inicia un shell de UNIX.
`configuration`	Entra en el modo de configuración.
`quit`	Sale de la CLI y vuelve al shell de UNIX.

2

PART IN COVERPAGE

Características de operación, administración y administración

OAM de Ethernet y administración de fallos de conectividad para enrutadores | 20

Administración de fallos de vínculo para enrutadores | 139

Administración de fallos de vínculo OAM Ethernet para conmutadores | 175

Administración de errores de conectividad OAM Ethernet para conmutadores | 187

Retardo de trama Ethernet | 205

Oam del servicio Ethernet (ITU-ty.1731) para enrutadores | 213

chapter label in part1

OAM de Ethernet y administración de fallos de conectividad para enrutadores

in this chapter

- Introducción a la administración de errores de conectividad (CFM) de OAM | **20**
- Configurar la administración de errores de conectividad (CFM) | **28**
- Perfil de acción de CFM | **59**
- Interfaz de administración local Ethernet | **66**
- Soporte CFM para paquetes encapsulados CCC | **77**
- Configurar ISSU unificada para 802.1ag CFM | **80**
- Monitoreo CFM entre dispositivos CE y PE | **84**
- Configurar mensajes de comprobación de continuidad | **114**
- Ejemplo: Configurar Ethernet CFM en interfaces físicas | **120**
- Ejemplo: Configurar Ethernet CFM en conexiones de puente | **123**
- Ejemplo: Configurar Ethernet CFM a través de VPLS | **128**

Introducción a la administración de errores de conectividad (CFM) de OAM

summary

En esta sección se describe la operación, administración y administración (OAM) de la administración de errores de conectividad (CFM).

in this section

- Administración de errores de conectividad Ethernet OAM | **21**
- Administración de errores de conectividad OAM IEEE 802.1ag | **22**

Administración de errores de conectividad Ethernet OAM

La administración de errores de conectividad (CFM) se define en IEEE 802.1ag. En este tema se hace hincapié en el uso de CFM en un entorno Metro Ethernet.

Las principales características de CFM son:

- Monitoreo de fallos mediante el protocolo de verificación de continuidad. Este protocolo sirve como un protocolo de detección de vecinos y comprobación de estado que identifica y mantiene adyacencias en el nivel de VLAN o vínculo.
- Descubrimiento de rutas y comprobación de errores mediante el protocolo linktrace. Similar a IP traceroute, este protocolo mapea la ruta tomada a una dirección MAC de destino a través de una o más redes puenteadas entre el origen y el destino.
- Aislamiento de errores mediante el protocolo de circuito cerrado. Similar al ping IP, este protocolo funciona con el protocolo de comprobación de continuidad durante la solución de problemas.

CFM divide la red de servicios en diferentes dominios administrativos, como operadores, proveedores y clientes. Estos dominios pueden pertenecer a dominios administrativos independientes.

Cada dominio administrativo está vinculado con un dominio de mantenimiento que contiene información suficiente para la autogestión, permite el monitoreo de extremo a extremo y evita violaciones de seguridad. Cada dominio de mantenimiento está asociado a un nivel de dominio de mantenimiento comprendido entre 0 y 7, según la jerarquía de red. A los dominios más externos se les asigna un nivel más alto que a los dominios más internos. Los puntos finales del cliente tienen el nivel de dominio de mantenimiento más alto.

Cada instancia de servicio en un dominio de mantenimiento CFM se denomina *.maintenance association* A consiste en una malla completa de puntos finales de mantenimiento (MEP) que comparten características similares.*maintenance association* Los eurodiputados son entidades CFM activas que generan y responden a mensajes de protocolo CFM.

También hay un punto intermedio de mantenimiento (MIP), que es una entidad CFM similar al MEP. Sin embargo, MIP es relativamente pasivo y solo responde a los mensajes CFM.

Los eurodiputados pueden ser o *.up MEPsdown MEPs* Un enlace puede conectar a un eurodiputado de nivel 5 con un eurodiputado de nivel 7. La interfaz en el nivel 5 es un MEP arriba (porque el otro extremo del enlace está en el nivel MEP 7), y la interfaz en el nivel 7 es un MEP abajo (porque el otro extremo del enlace está en el nivel MEP 5).

En una red Metro Ethernet, CFM se utiliza comúnmente en dos niveles:

- Por parte del proveedor de servicios para comprobar la conectividad entre los enrutadores perimetrales (PE) de su proveedor
- Por parte del cliente para comprobar la conectividad entre sus enrutadores perimetrales (CE) del cliente

> **NOTA**: El nivel de CFM del cliente configurado debe ser mayor que el nivel de CFM del proveedor de servicios.

En muchas redes Metro Ethernet, CFM se utiliza para supervisar la conectividad a través de una red VPLS y puente.

> **NOTA**: En los enrutadores de la serie ACX, OAM para VPLS solo se admite en enrutadores ACX5048, ACX5096 y ACX5448, y OAM para EVPN solo se admite en enrutadores ACX5448 y ACX710.

La compatibilidad con CFM en dispositivos PTX10001-36MR, PTX10004, PTX10008 y PTX10016 incluye las siguientes limitaciones:

- Limitaciones relacionadas con el punto final de mantenimiento (MEP) y el punto intermedio de mantenimiento (MIP): no se puede configurar:
  - Arriba MEP y abajo MEP al mismo nivel en una interfaz.
- Si el eurodiputado de arriba es más alto que el eurodiputado de abajo, el sistema no deja caer las PDU del MCP selectivamente y les permite pasar sin interrupción.
- No se admite la marca de tiempo relacionada con DM en AE con vínculos secundarios a través de varios PFE.
- Los paquetes CFM toman la cola predeterminada. No hay ninguna asignación de clase de reenvío a cola (fc a cola) en los siguientes casos:
  - Tráfico de salida, si cos-rewrite no está configurado
  - Tráfico sin etiquetar
- La configuración de los IFL habilitados para OAM puede afectar el escalado de CFM.`vlan-id-list`
- Los paquetes CFM que están enlazados al host y generados por el host no omiten los filtros de firewall configurados para la dirección de entrada y salida.

Administración de errores de conectividad OAM IEEE 802.1ag

in this section

Elementos clave de la administración de errores de conectividad | 25

Prácticas recomendadas para configurar 802.1ag Ethernet OAM para VPLS | 26

Junos OS admite la administración de errores de conectividad IEEE 802.1ag. Las interfaces Ethernet en enrutadores M7i y M10i con el CFEB-E mejorado (CFEB-E) y en enrutadores M120, M320, serie MX, serie T y serie PTX admiten el estándar IEEE 802.1ag para operación, administración y gestión (OAM). El estándar IEEE 802.1ag facilita la administración de errores de conectividad Ethernet (CFM) que ayuda a monitorear una red Ethernet que comprende una o más instancias de servicio.

En Junos OS versión 9.3 y posteriores, CFM también admite interfaces Ethernet agregadas. Las sesiones de CFM funcionan en modo distribuido en el concentrador de PIC flexible (FPC) en interfaces Ethernet agregadas. Como resultado, se admite un cambio correcto de motor de enrutamiento (GRES) en interfaces Ethernet agregadas. En versiones anteriores a Junos OS versión 13.3, las sesiones de CFM funcionan en modo centralizado en el motor de enrutamiento. Sin embargo, las sesiones CFM no se admiten en interfaces Ethernet agregadas si las interfaces que forman el paquete Ethernet agregado están en modo mixto. Además, las sesiones CFM con un intervalo de mensaje de comprobación de continuidad (CCM) de 10 milisegundos no se admiten en las interfaces Ethernet agregadas.

Las sesiones CFM se distribuyen de forma predeterminada. Todas las sesiones de CFM deben funcionar solo en modo distribuido o solo centralizado. No se admite una operación mixta de modos distribuidos y centralizados para sesiones CFM. Para deshabilitar la distribución de sesiones CFM en interfaces Ethernet agregadas y hacer que las sesiones funcionen en modo centralizado, incluya la instrucción en el nivel de jerarquía.`no-aggregate-delegate-processing`[`edit protocols oam ethernet connectivity-fault-management`]

NOTA: Como requisito para que Ethernet OAM 802.1ag funcione, la administración periódica distribuida de paquetes (PPM) se ejecuta en el motor de enrutamiento y el motor de reenvío de paquetes. Solo puede deshabilitar PPM en el motor de reenvío de paquetes. Para deshabilitar PPM en el PFE, incluya la instrucción en el nivel de jerarquía.`ppm no-delegate-processing`[`edit routing-options ppm`]

NOTA:

- El chasis virtual de la serie MX no admite la administración de errores de conectividad distribuida en línea.
- Los enrutadores de la serie ACX admiten CFM en interfaces Ethernet agregadas con un intervalo de verificación de continuidad de 100 milisegundos o superior.

- Las sesiones CFM se admiten en interfaces Ethernet agregadas si las interfaces que forman el paquete Ethernet agregado están en modo mixto cuando el comando está habilitado.`no-aggregate-delegate-processing`
- A partir de Junos OS versión 14.2, para las sesiones de CFM en modo centralizado, se recomienda configurar un máximo de 40 sesiones de CFM con un intervalo de mensaje de comprobación de continuidad (CCM) de 100 milisegundos (100 ms) o un máximo de 400 sesiones de CFM con un intervalo de CCM de 1 segundo (1 s). Si las sesiones de CFM se configuran más allá de este límite, es posible que CFM no funcione como se esperaba. Es posible que observe problemas cuando cambia el estado de varios vínculos o cuando se reinician las tarjetas de línea.

  Tenga en cuenta que estos límites se han derivado teniendo en cuenta una carga de unidad de datos de protocolo (PDU) de 400 paquetes por segundo (pps) en el motor de enrutamiento. Este límite varía en función de la carga del motor de enrutamiento. Si el motor de enrutamiento experimenta una carga pesada, espere algunas variaciones hasta este límite.

A partir de Junos OS versión 10.3, CFM no se admite en vínculos de miembro Ethernet agregados sin etiquetar en interfaces configuradas en concentradores de puertos modulares (MPC) y tarjetas de interfaz modular (MIC) en enrutadores serie MX. Sin embargo, CFM se admite en interfaces lógicas Ethernet agregadas sin etiquetar y etiquetadas configuradas en MPC y MIC.A partir de Junos OS versión 12.3, CFM no admite la agregación de vínculos multichasis (MC-LAG). Se recomienda no configurar la instrucción al configurar CFM `.mc-ae`

A partir de Junos OS versión 11.3, en enrutadores serie T y M320, CFM no se admite en interfaces configuradas con encapsulación CCC. Si configura CFM, el sistema muestra el siguiente mensaje: "".`MEPs cannot be configured on ccc interface on this platform`

A partir de Junos OS versión 17.4, puede habilitar la compatibilidad con IEEE 802.1ag CFM en interfaces de servicio de pseudocable mediante la configuración de puntos intermedios de mantenimiento (MIP) en las interfaces de servicio de pseudocable. Las interfaces de servicio de pseudocable admiten la configuración de interfaces de suscriptor a través de la terminación de pseudocable MPLS. La terminación de las interfaces de suscriptor a través de PW permite a los operadores de red extender su dominio MPLS desde la red de acceso/agregación hasta el borde del servicio y usar un aprovisionamiento uniforme de etiquetas MPLS para una mayor parte de su red.

NOTA: La sesión MIP de CFM solo se admite en la interfaz de servicios de pseudocable y no en la interfaz de túnel de servicios de pseudocable.

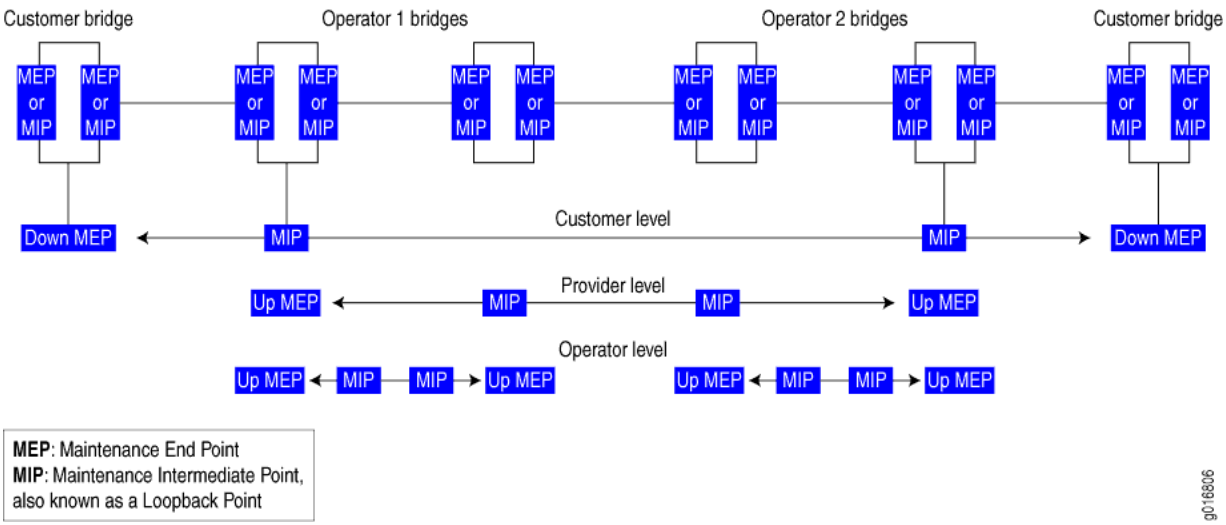
IEEE 802.1ag OAM admite un cambio de motor de enrutamiento (GRES) elegante. IEEE 802.1ag OAM es compatible con interfaces VLAN sin etiquetar, con una sola etiqueta y apiladas.

En los conmutadores de la serie EX, para utilizar la función CFM, primero debe agregar la CFM a Junos OS básico instalando una licencia de funciones mejoradas (EFL). Consulte Licencias para la serie EX para obtener más detalles.https://www.juniper.net/documentation/en_US/release-independent/licensing/topics/topic-map/understanding_software_licenses.html

Elementos clave de la administración de errores de conectividad

Figura 1 en la página 25 muestra las relaciones entre los puentes Ethernet de cliente, proveedor y operador, dominios de mantenimiento, puntos finales de asociación de mantenimiento (MEP) y puntos intermedios de mantenimiento (MIP).

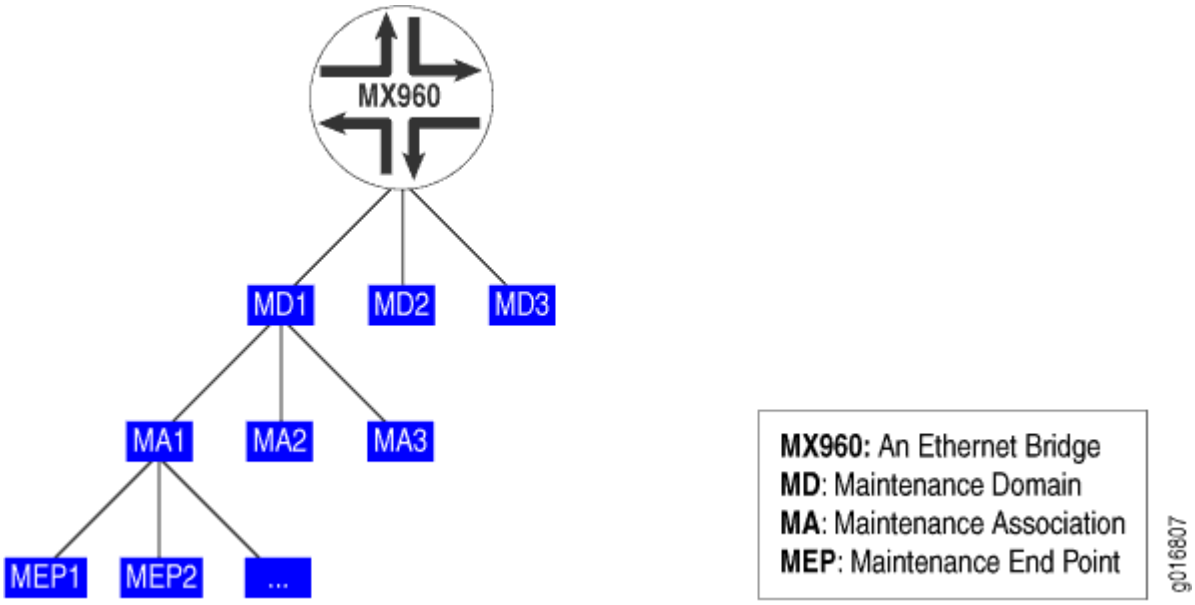
Figura 1: Relación entre los MEP, los MIP y los niveles de dominio de mantenimiento



NOTA: En los enrutadores de la serie ACX, los puntos intermedios de mantenimiento (MIP) solo se admiten en los enrutadores ACX5048 y ACX5096.

Una asociación de mantenimiento es un conjunto de MEP configurados con el mismo identificador de asociación de mantenimiento y nivel de dominio de mantenimiento. muestra las relaciones jerárquicas entre el puente Ethernet, los dominios de mantenimiento, las asociaciones de mantenimiento y los MEP.Figura 2 en la página 26

Figura 2: Relación entre puentes, dominios de mantenimiento, asociaciones de mantenimiento y MEP



Prácticas recomendadas para configurar 802.1ag Ethernet OAM para VPLS

MEJORES PRÁCTICAS: Las interfaces lógicas de una instancia de enrutamiento VPLS pueden tener la misma configuración de VLAN o configuraciones diferentes. Se requiere la normalización de VLAN para conmutar paquetes correctamente entre estas interfaces. La normalización de VLAN es efectivamente una traducción de VLAN en la que las etiquetas VLAN del paquete recibido deben traducirse si son diferentes de las etiquetas VLAN normalizadas.

Para los enrutadores de la serie MX, la VLAN normalizada se especifica mediante una de las siguientes instrucciones de configuración en la instancia de enrutamiento VPLS:

- `vlan-id` *`vlan-number`*
- `vlan-id none`
- `vlan-tags outer` *`outer-vlan-number`* `inner` *`inner-vlan-number`*

Debe configurar explícitamente en todas las interfaces que pertenecen a la instancia de enrutamiento.`vlan-maps`

Se deben tener en cuenta las siguientes consideraciones de ruta de reenvío:

- Ruta de recepción de paquetes:
  - Esta es la ruta de reenvío para los paquetes recibidos en las interfaces.
  - Ethernet OAM 802.1ag para VPLS utiliza filtros de interfaz implícitos y filtros de tabla de reenvío para inundar, aceptar y eliminar los paquetes CFM.
- Ruta de transmisión de paquetes:
  - El software JUNOS utiliza el reenvío basado en hardware del enrutador para los paquetes generados por la CPU.
  - Para los MEPs Down, los paquetes se transmiten en la interfaz en la que está configurado el MEP.
  - En los enrutadores de la serie MX, para los MEP UP, el paquete debe inundarse a otras interfaces en la instancia de enrutamiento VPLS. El enrutador crea una ruta de inundación vinculada a un próximo salto de inundación (con todas las interfaces para inundar) y luego obtiene el paquete para reenviarlo con esta ruta de inundación.
  - El enrutador también utiliza el reenvío implícito para los paquetes generados por la CPU. El resultado es que el siguiente salto de inundación vinculado a la ruta de inundación se vinculará al término de filtro. El término filtro utiliza criterios de coincidencia para identificar correctamente los paquetes generados por el host.

SEE ALSO

gestión de errores de conectividad

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.4R1	A partir de Junos OS versión 17.4, puede habilitar la compatibilidad con IEEE 802.1ag CFM en interfaces de servicio de pseudocable mediante la configuración de puntos intermedios de mantenimiento (MIP) en las interfaces de servicio de pseudocable.

14.2	A partir de Junos OS versión 14.2, para las sesiones de CFM en modo centralizado, se recomienda configurar un máximo de 40 sesiones de CFM con un intervalo de mensaje de comprobación de continuidad (CCM) de 100 milisegundos (100 ms) o un máximo de 400 sesiones de CFM con un intervalo de CCM de 1 segundo (1 s).
12.3	A partir de Junos OS versión 12.3, CFM no admite la agregación de vínculos multichasis (MC-LAG). No configure la instrucción al configurar CFM `.mc-ae`
11.3	A partir de Junos OS versión 11.3, en enrutadores serie T y M320, CFM no se admite en interfaces configuradas con encapsulación CCC.
10.3	A partir de Junos OS versión 10.3, en interfaces configuradas en concentradores de puertos modulares (MPC) y tarjetas de interfaz modular (MIC) en enrutadores serie MX, CFM no se admite en vínculos de miembro Ethernet agregados sin etiquetar. Las MPC y las MIC admiten CFM en interfaces lógicas Ethernet agregadas sin etiquetar y etiquetadas.
9.3	En Junos OS versión 9.3 y posteriores, CFM también admite interfaces Ethernet agregadas.

Configurar la administración de errores de conectividad (CFM)

in this section

- Crear un dominio de mantenimiento | **29**
- Crear una asociación de mantenimiento | **30**
- Configurar puntos intermedios de mantenimiento (MIP) | **31**
- Configurar puntos intermedios de la asociación de mantenimiento en la serie ACX | **33**
- Configurar un MEP para generar y responder a mensajes de protocolo CFM | **37**
- Configurar la protección de servicio para VPWS a través de MPLS mediante la interfaz MEP | **42**
- Configurar el protocolo Linktrace en CFM | **47**
- Descripción general de los parámetros del protocolo de comprobación de continuidad | **48**
- Configuración de parámetros de protocolo de comprobación de continuidad para la detección de errores | **49**
- Configuración de la limitación de velocidad de los mensajes OAM de Ethernet | **51**
- Habilitación del modo de administración de errores de conectividad mejorada | **54**

- Configurar la administración de errores de conectividad para la interoperabilidad durante las actualizaciones de software unificadas en servicio | **55**
- Soporte de Junos OS para la supervisión del rendimiento que cumple con la especificación técnica MEF 36 | **56**
- Amortiguación del rendimiento del CFM Monitoreo de trampas y notificaciones para evitar la congestión del NMS | **57**

Use este tema para configurar características de administración de errores de conectividad, como dominios de mantenimiento, asociaciones de mantenimiento, puntos intermedios de mantenimiento (MIP) y parámetros de comprobación de continuidad. También puede utilizar este tema para configurar un perfil de acción a fin de especificar la acción de CFM que se debe realizar cuando se produce un evento CFM específico.

A partir de la versión 22.4R2 de Junos OS Evolved, el proceso de administración de errores de conectividad (cfmd) solo se ejecuta cuando el protocolo está configurado.`ethernet connectivity-fault-management`

Crear un dominio de mantenimiento

Para habilitar la administración de errores de conectividad (CFM) en una interfaz Ethernet, primero debe configurar un dominio de mantenimiento y especificar el nombre del dominio de mantenimiento. También puede especificar el formato del nombre. Por ejemplo, si especifica que el formato de nombre sea el formato del servicio de nombres de dominio (DNS), puede especificar el nombre del dominio de mantenimiento como www.juniper.net. El formato de nombre predeterminado es la cadena de caracteres ASCII.

> **NOTA**: Para las interfaces lógicas, el nombre de dominio de mantenimiento debe ser único en todos los sistemas lógicos. Si configura el mismo nombre de dominio de mantenimiento en todos los sistemas lógicos, recibirá el siguiente mensaje de error: `error: configuration check-out failed`.

Durante la creación del dominio de mantenimiento, también puede especificar el nivel de dominio de mantenimiento. El nivel de dominio de mantenimiento indica la relación de anidamiento entre varios dominios de mantenimiento. El nivel de dominio de mantenimiento está incrustado en cada una de las tramas CFM.

NOTA: Las entradas de visualización de configuración en la lista de dominios de mantenimiento de CFM son "ordenadas por sistema" en lugar de "ordenadas por usuario".

Para crear un dominio de mantenimiento:

1. En el modo de configuración, cree un dominio de mantenimiento especificando el nombre y el formato de nombre en el nivel de jerarquía [ ].`edit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenance-domain md-name name-format option
```

NOTA: Si configura la longitud del nombre de dominio de mantenimiento mayor que 45 octetos, se muestra el siguiente mensaje de error: `error: configuration check-out failed`.

2. Especifique el nivel de dominio de mantenimiento especificando el valor en el nivel de jerarquía [ ].`edit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenace-domain md-name level number
```

SEE ALSO

gestión de errores de conectividad

maintenance-domain

name-format

Nivel

Crear una asociación de mantenimiento

Para crear una asociación de mantenimiento, incluya la instrucción en el nivel jerárquico `.maintenance-association ma-name`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name`]

Los nombres de asociación de mantenimiento pueden tener uno de los siguientes formatos:

- Como una cadena de caracteres ASCII simple

- Como identificador de VLAN de la VLAN, se asocia principalmente con la asociación de mantenimiento
- Como identificador de dos octetos en el intervalo de 0 a 65.535
- Como nombre en el formato especificado por RFC 2685

El formato de nombre corto predeterminado es una cadena de caracteres ASCII.

Para configurar el formato de nombre corto de asociación de mantenimiento, incluya la instrucción en el nivel de jerarquía.`short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id)`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`*]

> **NOTA**: Las entradas de visualización de configuración en la lista de dominios de mantenimiento de CFM son "ordenadas por sistema" en lugar de "ordenadas por usuario".

SEE ALSO

> *gestión de errores de conectividad*
>
> *name-format*
>
> *formato de nombre corto*

Configurar puntos intermedios de mantenimiento (MIP)

Los enrutadores de la serie MX admiten puntos intermedios de mantenimiento (MIP) para el protocolo CFM Ethernet OAM 802.1ag a nivel de dominio de puente. Esto le permite definir un dominio de mantenimiento para cada nivel predeterminado. Los nombres MIP se crean como en el nivel de jerarquía.`default-`*`level-number`*[`edit protocols oam ethernet connectivity-fault-management maintenance-domain`] Utilice las opciones , , y MIP para especificar la configuración de MIP.`bridge-domaininstancevirtual-switchmip-half-function`

Utilice el comando para mostrar las configuraciones de MIP.`show oam ethernet connectivity-fault-management mip (bridge-domain | instance-name | interface-name)`

Para configurar el punto intermedio de mantenimiento (MIP):

1. Configure un dominio de puente bajo un conmutador virtual definido por el usuario especificando la instrucción y el nombre del conmutador virtual definido por el usuario, en el nivel de jerarquía.`virtual-switch`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `default-`*`x`*]

NOTA: Un dominio puente debe especificarse por nombre sólo si se configura incluyendo la instrucción debajo de la instrucción.`vlan-idvirtual-switch` Si un dominio de puente está configurado con un rango de ID de VLAN, los ID de VLAN deben aparecer explícitamente después del nombre de dominio del puente.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
default-x]
user@host# set virtual-switch virtual-switch-name bridge-domain bridge-domain-name vlan-id
value
```

NOTA: También puede configurar el dominio de puente para el conmutador virtual predeterminado incluyendo la instrucción en el nivel de jerarquía.`bridge-domain`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`*]

2. Configure la instancia de enrutamiento VPLS para el dominio de mantenimiento predeterminado.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@host# set instance instance-name
```

3. Configure la función de medio punto intermedio de mantenimiento (MIP) para dividir la funcionalidad MIP en dos segmentos unidireccionales para mejorar la cobertura de la red aumentando el número de MIP que se supervisan. La función media MIP también responde a mensajes de bucle atrás y de rastreo de enlaces para identificar fallas.

NOTA: Siempre que se configure una MIP y un dominio de puente se asigne a varios dominios o asociaciones de mantenimiento, es esencial que el valor de todos los dominios y asociaciones de mantenimiento sea el mismo.`mip-half-function`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
default- x]
user@host# set mip-half-function (none | default | explicit)
```

SEE ALSO

dominio puente

gestión de errores de conectividad

Ejemplo

Función MIP-HALF

conmutador virtual

Configurar puntos intermedios de la asociación de mantenimiento en la serie ACX

in this section

- Configurar el dominio de puente de dominio de mantenimiento | 34
- Configurar la mitad de la función MIP del dominio de mantenimiento | 34
- Configurar los puntos intermedios de la asociación de mantenimiento con el dominio de puente | 35
- Configurar los puntos intermedios de la asociación de mantenimiento con conexión cruzada de circuitos | 35
- Configurar los puntos intermedios de la asociación de mantenimiento con el dominio de puente cuando se configure el extremo de la asociación de mantenimiento | 36
- Configurar los puntos intermedios de mantenimiento con conexión cruzada de circuitos cuando se configura el punto final de la asociación de mantenimiento | 36

El punto intermedio de mantenimiento (MIP) proporciona capacidad de monitoreo de puntos intermedios para servicios como puentes de capa 2, circuitos de capa 2 y VPN de capa 2. Los enrutadores ACX5048 y ACX5096 admiten MIP para el protocolo CFM Ethernet OAM 802.1ag. Utilice las opciones MIP de dominio de puente, interfaz y MIP de media función para especificar la configuración de MIP.

NOTA: ACX5048 y enrutadores ACX5096 no admiten la configuración MIP en los servicios VPLS.

NOTA: ACX5448 enrutador no admite MIP.

> **NOTA**: Siempre que se configure una MIP y un dominio de puente se asigne a varios dominios o asociaciones de mantenimiento, es esencial que el valor de todos los dominios y asociaciones de mantenimiento sea el mismo.`mip-half-function`

Para mostrar las configuraciones de MIP, utilice el comando.`show oam ethernet connectivity-fault-management mip (bridge-domain | instance-name | interface-name)`

Las siguientes configuraciones de MIP son compatibles con los enrutadores ACX5048 y ACX5096:

- MIP con dominio con puente
- MIP con conexión cruzada de circuito (CCC)
- MIP con dominio de puente cuando se configura el extremo de asociación de mantenimiento
- MIP con CCC cuando se configura el punto final de la asociación de mantenimiento

En las secciones siguientes se describe la configuración de MIP:

Configurar el dominio de puente de dominio de mantenimiento

Para configurar el dominio de puente, incluya la instrucción en el nivel de jerarquía.`vlans[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`maintenance-domain-name`*`]`

> **NOTA**: Las configuraciones de la CLI de capa 2 y los comandos show para los enrutadores ACX5048 y ACX5096 difieren en comparación con otros enrutadores de la serie ACX. Para obtener más información, consulte Modo de próxima generación de capa 2 para la serie ACX.

Configurar la mitad de la función MIP del dominio de mantenimiento

La función media MIP (MHF) divide la funcionalidad MIP en dos segmentos unidireccionales, mejora la visibilidad con una configuración mínima y mejora la cobertura de red al aumentar el número de puntos que se pueden monitorear. MHF amplía la capacidad de monitoreo al responder a los mensajes de circuito cerrado y linktrace para ayudar a aislar las fallas.

Siempre que se configure un MIP y un dominio de puente se asigne a varios dominios o asociaciones de mantenimiento, es esencial que el valor de media función MIP para todos los dominios y asociaciones de mantenimiento sea el mismo. Para configurar la función MIP half, incluya la instrucción en el nivel de jerarquía.`mip-half-function[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`maintenance-domain-name`*`]`

Configurar los puntos intermedios de la asociación de mantenimiento con el dominio de puente

En enrutadores ACX5048 y ACX5096, puede configurar el MIP con dominio de puente. A continuación se muestra un ejemplo para configurar el MIP con dominio de puente:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain default-6 {
                vlan bd1;
                mip-half-function default;
            }
        }
    }
}
```

Configurar los puntos intermedios de la asociación de mantenimiento con conexión cruzada de circuitos

En enrutadores ACX5048 y ACX5096, puede configurar el MIP con conexión cruzada de circuitos (CCC). A continuación se muestra un ejemplo para configurar el MIP con CCC:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain default-6 {
                interface xe-0/0/42.0;
                mip-half-function default;
            }
        }
    }
}
```

Configurar los puntos intermedios de la asociación de mantenimiento con el dominio de puente cuando se configure el extremo de la asociación de mantenimiento

En enrutadores ACX5048 y ACX5096, puede configurar el MIP con dominio de puente cuando se configura un punto final de asociación de mantenimiento (MEP). A continuación se muestra un ejemplo para configurar la MIP con dominio de puente cuando se configura MEP:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md2 {
                level 5;
                mip-half-function default;
                maintenance-association ma2 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 222 {
                        interface xe-0/0/42.0;
                        direction up;
                    }
                }
            }
        }
    }
}
```

Configurar los puntos intermedios de mantenimiento con conexión cruzada de circuitos cuando se configura el punto final de la asociación de mantenimiento

En enrutadores ACX5048 y ACX5096, puede configurar el MIP con conexión cruzada de circuito (CCC) cuando se configura un punto final de asociación de mantenimiento (MEP). A continuación se muestra un ejemplo para configurar la MIP con CCC cuando se configura MEP:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md2 {
                level 5;
```

```
                mip-half-function default;
                maintenance-association ma2 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 222 {
                        interface xe-0/0/42.0;
                        direction up;
                    }
                }
            }
        }
    }
}
```

SEE ALSO

dominio puente

gestión de errores de conectividad

Ejemplo

Función MIP-HALF

Configurar un MEP para generar y responder a mensajes de protocolo CFM

in this section

- Configurar un punto de conexión de asociación de mantenimiento (MEP) | **38**
- Configurar un punto de conexión de asociación de mantenimiento remoto (MEP) | **40**

Un punto de conexión de asociación de mantenimiento (MEP) hace referencia al límite de un dominio. Un MEP genera y responde a mensajes de protocolo de administración de errores de conectividad (CFM). Puede configurar varios MEP up para una sola combinación de ID de asociación de mantenimiento e ID de dominio de mantenimiento para interfaces que pertenecen a un servicio VPLS determinado o a un dominio de puente. Puede configurar varios MEP inactivos para una sola instancia de identificador de dominio de mantenimiento y nombre de asociación de mantenimiento para supervisar los servicios proporcionados por el servicio de LAN privada virtual (VPLS), dominio de puente, conexión cruzada de circuitos (CCC) o dominios IPv4.

Para las instancias de enrutamiento de VPN de capa 2 (conmutación local) y las instancias de enrutamiento EVPN, también puede configurar varios MEP up para una sola combinación de ID de asociación de mantenimiento e ID de dominio de mantenimiento en interfaces lógicas. La interfaz lógica se puede configurar en diferentes dispositivos o en el mismo dispositivo. Para admitir varios MEP en dos IFL, se deben configurar servicios de red IP mejorados para el chasis.

Puede habilitar el descubrimiento automático de un MEP. Con la detección automática, un MEP puede aceptar mensajes de verificación de continuidad (CCM) de todos los MEP remotos de la misma asociación de mantenimiento. Si la detección automática no está habilitada, se deben configurar los MEP remotos. Si el MEP remoto no está configurado, los MCPs del MEP remoto se tratan como errores.

La medición de continuidad es proporcionada por un protocolo de verificación de continuidad existente. La continuidad de cada eurodiputado remoto se mide como el porcentaje de tiempo que el eurodiputado remoto estuvo operativo durante el tiempo total habilitado administrativamente. Aquí, el tiempo de actividad operacional es el tiempo total durante el cual la adyacencia del MCP está activa para un MEP remoto en particular y el tiempo administrativo habilitado es el tiempo total durante el cual el MEP local está activo. También puede reiniciar la medición de continuidad borrando el tiempo de actividad operativo medido actualmente y el tiempo habilitado administrativamente.

Configurar un punto de conexión de asociación de mantenimiento (MEP)

Para configurar un punto de conexión de asociación de mantenimiento:

1. Especifique un ID para el MEP en el [`.edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`*] Puede especificar cualquier valor del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name]
user@host# set mep mep-id
```

2. Habilite el descubrimiento automático del punto final de mantenimiento para que el MEP pueda aceptar mensajes de verificación de continuidad (CCM) de todos los MEP remotos de la misma asociación de mantenimiento.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

3. Especifique la dirección en la que se transmiten los paquetes CCM para el MEP. Puede especificar arriba o abajo. Si especifica la dirección como hacia arriba, los MCPs se transmiten desde todas las interfaces lógicas que forman parte de la misma instancia de puente o VPLS, excepto la interfaz

configurada en el MEP. Si especifica que la dirección es hacia abajo, los MCPs sólo se transmiten desde la interfaz configurada en el MEP.

> **NOTA**: Los puertos en el estado de bloqueo del Protocolo de árbol de expansión (STP) no bloquean los paquetes CFM destinados a un MEP inactivo. Los puertos en un estado de bloqueo STP sin el protocolo de verificación de continuidad configurado bloquean los paquetes CFM.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set direction down
```

> **NOTA**: A partir de Junos OS versión 12.3, para todas las interfaces configuradas en concentradores de puertos modulares (MPC) en plataformas de enrutamiento universal 5G serie MX, ya no es necesario configurar la instrucción para todas las VPN de capa 2 y circuitos de capa 2 sobre los que se ejecutan MEP CFM.`no-control-word` Para todas las demás interfaces de los enrutadores serie MX y de todos los demás enrutadores y conmutadores, debe seguir configurando la instrucción en el nivel de jerarquía o al configurar los MEP de CFM.`no-control-word`[`edit routing-instances` *`routing-instance-name`* `protocols l2vpn`][`edit protocols l2circuit neighbor` *`neighbor-id`* `interface` *`interface-name`*] De lo contrario, los paquetes CFM no se transmiten y el comando no muestra ningún MEP remoto.`show oam ethernet connectivity-fault-management mep-database`

4. Especifique la interfaz a la que está conectado el MEP. Puede ser una interfaz física, una interfaz lógica o una interfaz troncal. En los enrutadores de la serie MX, el MEP se puede conectar a una VLAN específica de una interfaz troncal.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set interface interface-name
```

5. Especifique los bits de prioridad IEEE 802.1 que utilizan los mensajes de seguimiento de vínculos y comprobación de continuidad. Puede especificar un valor de hasta 7 como prioridad.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set priority number
```

6. Especifique el defecto de prioridad más baja que genera una alarma de fallo cada vez que CFM detecta un defecto. Los valores posibles incluyen: Todos los defectos, err-xcon, mac-rem-err-xcon, sin defectos, rem-err-xcon y xcon.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set lowest-priority-defect mac-rem-err-xcon
```

7. Especifique el ID del MEP remoto en el nivel [.`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`* `mep` *`mep-id`*] Puede especificar cualquier valor del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-namemep mep-id]
user@host# set remote-mep mep-id
```

SEE ALSO

Prioridad

Configurar un punto de conexión de asociación de mantenimiento remoto (MEP)

Para configurar un punto de conexión de asociación de mantenimiento remoto:

1. Configure el MEP remoto especificando el ID del MEP en el nivel [.`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`* `mep` *`mep-id`*] Puede especificar cualquier valor del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-namemep mep-id]
user@host# edit remote-mep mep-id
```

2. Especifique el nombre del perfil de acción que se utilizará para el MEP remoto incluyendo la instrucción en el [.`action-profile` *`profile-name`*`edit protocols oam ethernet connectivity-fault-management`

`maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`* `mep` *`mep-id`* `remote-mep` *`remote-mep-id`*] El perfil debe definirse en el nivel jerárquico [].`edit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-namemep mep-id remote-mep remote-mep-id]
user@host# set action-profile profile-name
```

3. Configure el MEP remoto para detectar la pérdida inicial de conectividad. De forma predeterminada, el MEP no genera mensajes de defectos de pérdida de continuidad (LOC). Al configurar la instrucción, se detecta un defecto de pérdida de continuidad (LOC) si no se recibe ningún mensaje de comprobación de continuidad del MEP remoto en un período igual a 3,5 veces el intervalo de comprobación de continuidad configurado para la asociación de mantenimiento.`detect-loc` Si se detecta un defecto de LOC, se genera un mensaje de error syslog.

> **NOTA**: Cuando se configura la administración de errores de conectividad (CFM) junto con , cualquier dispositivo configurado para desactivar la interfaz se ejecuta si no se recibe el mensaje de comprobación de continuidad.`detect-locaction-profile` Sin embargo, el no se ejecuta si no ha configurado y no se recibe el mensaje de comprobación de continuidad.`action-profile detect-loc`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-namemep mep-id remote-mep remote-mep-id]
user@host# set detect-loc
```

SEE ALSO

- MEP remoto

VÍNCULOS RELACIONADOS

- perfil de acción
- Descubrimiento automático
- gestión de errores de conectividad
- detect-loc
- Dirección
- defecto de prioridad más baja

Configurar la protección de servicio para VPWS a través de MPLS mediante la interfaz MEP

Puede habilitar la protección de servicio para un servicio de cable privado virtual (VPWS) a través de MPLS especificando una ruta de trabajo o una ruta de protección en el MEP. La protección de servicio proporciona una protección de conexión de extremo a extremo de la ruta de trabajo en caso de fallo.

Para configurar la protección del servicio, debe crear dos rutas de transporte independientes: una ruta de trabajo y una ruta de protección. Puede especificar la ruta de trabajo y la ruta de protección creando dos asociaciones de mantenimiento. Para asociar la asociación de mantenimiento con una ruta de acceso, debe configurar la instrucción para el MEP dentro de la asociación de mantenimiento y especificar la ruta como funcional o proteger.`interface`

> **NOTA**: Si no se especifica la ruta, la sesión supervisa la ruta activa.

Tabla 5 en la página 42 Describe las opciones de protección de servicio disponibles.

Tabla 5: Opciones de protección de servicio

La opción	Description
`working`	Especifica la ruta de trabajo.
`protect`	Especifica la ruta de protección.

En esta configuración, habilitamos la protección de servicio para el servicio VPWS. La sesión del MCP está configurada para la ruta de trabajo y hace referencia a la sesión del MCP configurada para la ruta de protección utilizando la instrucción.`protect-maintenance-association` El nombre de la ruta de transporte de protección para la asociación de mantenimiento está configurado y asociado a la asociación de mantenimiento para la ruta de trabajo.

Para configurar la protección de servicio para VPWS a través de MPLS:

1. En el modo de configuración, cree un dominio de mantenimiento especificando el nombre y el formato de nombre en el nivel de jerarquía [ ].`edit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenance-domain md-name name-format option
```

> **NOTA**: Si configura la longitud del nombre de dominio de mantenimiento mayor que 45 octetos, se muestra el siguiente mensaje de error: `error: configuration check-out failed`.

2. Especifique el nivel de dominio de mantenimiento especificando el valor en el nivel de jerarquía [ ].`edit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenace-domain md-name level number
```

3. Cree una asociación de mantenimiento para la ruta de trabajo especificando el nombre y el formato de nombre corto en el nivel de jerarquía [].`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`*

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# set maintenance-association test-ma short-name-format option
```

4. Especifique el nombre de la asociación de mantenimiento utilizada para la protección de la conexión y el nombre del perfil de conmutación de protección automática (perfil aps) en el nivel jerárquico [].`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`*

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name]
user@host# set protect-maintenance-association ma-name aps-profile aps-profile-name
```

5. Especifique el tiempo de espera entre las transmisiones de mensajes de comprobación de continuidad en el nivel jerárquico [ ].`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `continuity-check` La duración puede ser uno de los siguientes valores: 10 minutos (10 m), 1 minuto (1 m), 10 segundos (10 segundos), 1 segundo (1s), 100 milisegundos (100 ms) o 10 milisegundos (10 ms). El valor predeterminado es 1 minuto.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name continuity-check]
user@host# set interval option
```

6. Especifique un ID para el MEP en el [.`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`*] Puede especificar cualquier valor del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name]
user@host# set mep mep-id
```

7. Habilite el descubrimiento automático del punto final de mantenimiento para que el MEP pueda aceptar mensajes de verificación de continuidad (CCM) de todos los MEP remotos de la misma asociación de mantenimiento.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

8. Especifique la dirección en la que se transmiten los paquetes CCM para el MEP. Puede especificar arriba o abajo. Si especifica la dirección como hacia arriba, los MCPs se transmiten desde todas las interfaces lógicas que forman parte de la misma instancia de puente o VPLS, excepto la interfaz configurada en el MEP. Si especifica que la dirección es hacia abajo, los MCPs sólo se transmiten desde la interfaz configurada en el MEP.

> **NOTA**: Los puertos en el estado de bloqueo del Protocolo de árbol de expansión (STP) no bloquean los paquetes CFM destinados a un MEP inactivo. Los puertos en un estado de bloqueo STP sin el protocolo de verificación de continuidad configurado bloquean los paquetes CFM.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set direction down
```

> **NOTA**: A partir de Junos OS versión 12.3, para todas las interfaces configuradas en concentradores de puertos modulares (MPC) en plataformas de enrutamiento universal 5G serie MX, ya no es necesario configurar la instrucción para todas las VPN de capa 2 y circuitos de capa 2 sobre los que se ejecutan MEP CFM.`no-control-word` Para todas las demás interfaces de los enrutadores serie MX y de todos los demás enrutadores y conmutadores, debe seguir configurando la instrucción en el nivel de jerarquía o al configurar los MEP de

CFM.`no-control-word`[`edit routing-instances` *`routing-instance-name`* `protocols l2vpn`][`edit protocols l2circuit neighbor` *`neighbor-id`* `interface` *`interface-name`*] De lo contrario, los paquetes CFM no se transmiten y el comando no muestra ningún MEP remoto.`show oam ethernet connectivity-fault-management mep-database`

9. Especifique la interfaz a la que está conectado el MEP. Puede ser una interfaz física, una interfaz lógica o una interfaz troncal. En los enrutadores de la serie MX, el MEP se puede conectar a una VLAN específica de una interfaz troncal. Además, especifique la ruta de transporte como funcionando.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set interface interface-name working
```

10. Cree una asociación de mantenimiento para la ruta de protección especificando el nombre y el formato de nombre corto en el nivel de jerarquía [].`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`*

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# set maintenance-association ma-name short-name-format option
```

11. Especifique el tiempo de espera entre las transmisiones de mensajes de comprobación de continuidad en el nivel jerárquico [ ].`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `continuity-check` La duración puede ser uno de los siguientes valores: 10 minutos (10 m), 1 minuto (1 m), 10 segundos (10 segundos), 1 segundo (1s), 100 milisegundos (100 ms) o 10 milisegundos (10 ms). El valor predeterminado es 1 minuto.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name continuity-check]
user@host# set interval option
```

12. Especifique un ID para el MEP en el [.`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`*] Puede especificar cualquier valor del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name]
user@host# set mep mep-id
```

13. Habilite el descubrimiento automático del punto final de mantenimiento para que el MEP pueda aceptar mensajes de verificación de continuidad (CCM) de todos los MEP remotos de la misma asociación de mantenimiento.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set auto-discovery
```

14. Especifique la dirección en la que se transmiten los paquetes CCM para el MEP. Puede especificar arriba o abajo. Si especifica la dirección como hacia arriba, los MCPs se transmiten desde todas las interfaces lógicas que forman parte de la misma instancia de puente o VPLS, excepto la interfaz configurada en el MEP. Si especifica que la dirección es hacia abajo, los MCPs sólo se transmiten desde la interfaz configurada en el MEP.

> **NOTA**: Los puertos en el estado de bloqueo del Protocolo de árbol de expansión (STP) no bloquean los paquetes CFM destinados a un MEP inactivo. Los puertos en un estado de bloqueo STP sin el protocolo de verificación de continuidad configurado bloquean los paquetes CFM.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set direction down
```

> **NOTA**: A partir de Junos OS versión 12.3, para todas las interfaces configuradas en concentradores de puertos modulares (MPC) en plataformas de enrutamiento universal 5G serie MX, ya no es necesario configurar la instrucción para todas las VPN de capa 2 y circuitos de capa 2 sobre los que se ejecutan MEP CFM.`no-control-word` Para todas las demás interfaces de los enrutadores serie MX y de todos los demás enrutadores y conmutadores, debe seguir configurando la instrucción en el nivel de jerarquía o al configurar los MEP de CFM.`no-control-word`[`edit routing-instances` *`routing-instance-name`* `protocols l2vpn`][`edit protocols l2circuit neighbor` *`neighbor-id`* `interface` *`interface-name`*] De lo contrario, los paquetes CFM no se transmiten y el comando no muestra ningún MEP remoto.`show oam ethernet connectivity-fault-management mep-database`

15. Especifique la interfaz a la que está conectado el MEP. Puede ser una interfaz física, una interfaz lógica o una interfaz troncal. En los enrutadores de la serie MX, el MEP se puede conectar a una

VLAN específica de una interfaz troncal. Además, especifique la ruta de transporte como funcionando.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@host# set interface interface-name protect
```

SEE ALSO

> *Descubrimiento automático*
>
> *Intervalo*
>
> *name-format*
>
> *protect-maintenance-association*
>
> *formato de nombre corto*

Configurar el protocolo Linktrace en CFM

El protocolo linktrace se utiliza para el descubrimiento de rutas entre un par de puntos de mantenimiento. Los mensajes de Linktrace son activados por un administrador utilizando el comando para verificar la ruta entre un par de MEP bajo la misma asociación de mantenimiento.`traceroute` Los mensajes de seguimiento de enlaces también se pueden usar para verificar la ruta entre un MEP y un MIP en el mismo dominio de mantenimiento. El protocolo linktrace le permite configurar el tiempo de espera de una respuesta. Si no se recibe respuesta para un mensaje de solicitud de seguimiento de vínculos, las entradas de solicitud y respuesta se eliminan después de que expire el intervalo. También puede configurar el número de entradas de respuesta de linktrace que se almacenarán para la solicitud de linktrace correspondiente.

La operación de los mensajes de solicitud y respuesta de linktrace IEEE 802.1ag es similar a la operación de los comandos de capa 3 .`traceroute` Para obtener más información sobre el comando, consulte la Biblioteca de administración de Junos OS para dispositivos de enrutamiento.`traceroute`https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/index.html

Para configurar el protocolo linktrace:

1. Configure el tiempo de espera de una respuesta de linktrace en el nivel de jerarquía [].`edit protocols oam ethernet connectivity-fault-management` Puede especificar el valor en minutos o segundos. El valor predeterminado es 10 minutos.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set linktrace age time
```

2. Configure el número de entradas de respuesta de linktrace que se almacenarán por solicitud de linktrace. Puede especificar un valor del 1 al 500. El valor predeterminado es 100.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set linktrace path-database-sizepath-database-size
```

SEE ALSO

> *Edad*
>
> *path-database-size*
>
> *gestión de errores de conectividad*

Descripción general de los parámetros del protocolo de comprobación de continuidad

El protocolo de comprobación de continuidad se utiliza para la detección de fallos por parte de los puntos finales de mantenimiento (MEP) dentro de una asociación de mantenimiento. El MEP envía periódicamente mensajes de multidifusión de verificación de continuidad. Los paquetes del protocolo de comprobación de continuidad utilizan el valor ethertype 0x8902 y la dirección MAC de destino de multidifusión 01:80:c2:00:00:32.

En la lista siguiente se describen los parámetros del protocolo de comprobación de continuidad que puede configurar:

- `interval`—Frecuencia de los mensajes de verificación de continuidad (MCP), es decir, el tiempo transcurrido entre la transmisión de los mensajes MCP. Puede especificar 10 minutos (), 1 minuto (), 10 segundos (), 1 segundo (), 100 milisegundos () o 10 milisegundos ().`10m1m10s1s100ms10ms` El valor predeterminado es 1 minuto. Por ejemplo, si especifica el intervalo como 1 minuto, el MEP envía los mensajes de verificación de continuidad cada minuto al MEP receptor.

> **NOTA**: Para que el intervalo del mensaje de comprobación de continuidad se configure para 10 milisegundos, la administración periódica de paquetes (PPM) se ejecuta en el motor de enrutamiento y en el motor de reenvío de paquetes de forma predeterminada. Solo puede

deshabilitar PPM en el motor de reenvío de paquetes. Para deshabilitar PPM en el motor de reenvío de paquetes, utilice la instrucción en el nivel de jerarquía.`no-delegate-processing[edit routing-options ppm]`

El intervalo de comprobación de continuidad de 10 milisegundos no se admite para sesiones CFM a través de una interfaz de conmutación de etiquetas (LSI).

- `hold-interval`—Frecuencia con la que se puede vaciar la base de datos MEP, si no se producen actualizaciones. Los eurodiputados receptores utilizan los mensajes de verificación de continuidad para crear una base de datos de eurodiputados de todos los diputados de la asociación de mantenimiento. La frecuencia es el número de minutos que se deben esperar antes de vaciar la base de datos MEP si no se producen actualizaciones. El valor predeterminado es 10 minutos.

  NOTA: El vaciado basado en temporizador de retención solo se aplica a los MEP remotos descubiertos automáticamente y no a los MEP remotos configurados estáticamente.

  La lógica del intervalo de espera ejecuta un temporizador de sondeo por nivel de sesión CFM (no por nivel de MEP remoto) donde la duración del temporizador de sondeo es igual al tiempo de espera configurado. Cuando el temporizador de sondeo expira, elimina todas las entradas MEP remotas detectadas automáticamente que hayan estado en el estado de error durante un período de tiempo igual o mayor que el tiempo de espera configurado. Si el MEP remoto completa la duración del tiempo de espera en el estado de error, el vaciado no se producirá hasta que caduque el siguiente temporizador de sondeo. Por lo tanto, es posible que el vaciado remoto de MEP no se realice exactamente en el tiempo de espera configurado.

- `loss-threshold`—Número de mensajes de comprobación de continuidad que se pueden perder antes de que el enrutador marque el MEP como inactivo. El valor puede ser de 3 a 256 unidades de datos de protocolo (PDU). El valor predeterminado es 3 PDU.

SEE ALSO

intervalo de espera

Intervalo

umbral de pérdida

Configuración de parámetros de protocolo de comprobación de continuidad para la detección de errores

El protocolo de comprobación de continuidad se utiliza para la detección de errores por un punto final de asociación de mantenimiento (MEP) dentro de una asociación de mantenimiento. Un eurodiputado

genera y responde periódicamente mensajes de multidifusión de verificación de continuidad. Los paquetes del protocolo de comprobación de continuidad utilizan el valor ethertype 0x8902 y la dirección MAC de destino de multidifusión 01:80:c2:00:00:32. Los eurodiputados receptores utilizan los mensajes de verificación de continuidad (MCP) para construir una base de datos de eurodiputados de todos los eurodiputados de la asociación de mantenimiento.

Para configurar parámetros de protocolo de comprobación de continuidad:

1. Especifique el tiempo que debe esperar en minutos antes de vaciar la base de datos MEP, si no se producen actualizaciones, con un valor comprendido entre 1 minuto y 30.240 minutos. El valor predeterminado es 10 minutos.

   NOTA: El vaciado basado en el temporizador de espera solo se aplica a los MEP remotos descubiertos automáticamente y no a los MEP remotos configurados estáticamente.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name  continuity-check]
   user@host# set hold-interval minutes
   ```

2. Especifique el tiempo de espera (duración) entre las transmisiones de los MCPs. La duración puede ser uno de los siguientes valores: 10 minutos (10 m), 1 minuto (1 m), 10 segundos (10 segundos), 1 segundo (1s), 100 milisegundos (100 ms) o 10 milisegundos (10 ms). El valor predeterminado es 1 minuto.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name continuity-check]
   user@host# set interval duration
   ```

3. Especifique el número de mensajes de comprobación de continuidad que se pueden perder antes de que el enrutador marque el MEP como inactivo. El valor puede ser de 3 a 256 unidades de datos de protocolo (PDU). El valor predeterminado es 3 PDU.

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
   maintenance-association ma-name continuity-check]
   user@host# set loss-threshold number
   ```

SEE ALSO

> *control de continuidad*
>
> *intervalo de espera*
>
> *Intervalo*
>
> *umbral de pérdida*

Configuración de la limitación de velocidad de los mensajes OAM de Ethernet

El M320 con enrutadores Enhanced III FPC, M120, M7i, M10 con CFEB y MX Series admiten la limitación de velocidad de los mensajes OAM de Ethernet. Según la configuración de administración de errores de conectividad (CFM), los paquetes CFM se descartan, se envían a la CPU para su procesamiento o se inundan a otras interfaces de puente. Esta característica permite que el enrutador intercepte los paquetes CFM entrantes para prevenir ataques DoS.

Puede aplicar la limitación de velocidad de los mensajes OAM de Ethernet en cualquiera de los dos niveles de vigilancia de CFM, como se indica a continuación:

- Vigilancia de CFM a nivel global: utiliza un aplicador de políticas a nivel global para vigilar el tráfico de CFM que pertenece a todas las sesiones.
- Vigilancia de CFM a nivel de sesión: utiliza un aplicador de policía creado para vigilar el tráfico de CFM que pertenece a una sesión.

Para configurar la vigilancia de CFM a nivel global, incluya la instrucción y sus opciones en el nivel jerárquico .`policer[edit protocols oam ethernet connectivity-fault-management]`

Para configurar la vigilancia de CFM a nivel de sesión, incluya la instrucción en el nivel de jerarquía.`policer[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `level` *`number`* `maintenance-association` *`ma-name`*`]`

En el ejemplo siguiente se muestra un aplicador de control de CFM utilizado para limitar la velocidad de CFM:

```
[edit]
firewall {
    policer cfm-policer {
        if-exceeding {
            bandwidth-limit 8k;
            burst-size-limit 2k;
        }
        then discard;
    }
}
```

Caso 1: Vigilancia de CFM a nivel mundial

En este ejemplo se muestra un aplicador de políticas a nivel global, a nivel de CFM, para limitar la tasa de CFM. La instrucción en el nivel de jerarquía global especifica el aplicador que se utilizará para vigilar todos los paquetes de comprobación de continuidad del tráfico CFM que pertenecen a todas las sesiones.`continuity-check` *`cfm-policer`*`[edit protocols oam ethernet connectivity-fault-management policer]` La instrucción en el nivel de jerarquía especifica el aplicador que se utilizará para vigilar todos los paquetes de comprobación de no continuidad del tráfico CFM que pertenecen a todas las sesiones.`other` *`cfm-policer1`*`[edit protocols oam ethernet connectivity-fault-management policer]` La instrucción especifica que se deben vigilar todos los paquetes CFM con el aplicador de control especificado.`all` *`cfm-policer2`*`cfm-policer2` Si se utiliza la opción, el usuario no puede especificar las opciones anteriores y .`all` *`policer-name`*`continuity-checkother`

```
[edit protocols oam ethernet]
connectivity-fault-management {
    policer {
        continuity-check cfm-policer;
        other cfm-policer1 ;
        all cfm-policer2;
        }
    }
```

Caso 2: Vigilancia CFM a nivel de sesión

En este ejemplo se muestra un aplicador de CFM a nivel de sesión que se usa para limitar la velocidad de CFM. La instrucción en el nivel de jerarquía de sesión especifica el aplicador que se utilizará para vigilar solo los paquetes de comprobación de continuidad del tráfico CFM que pertenecen a la sesión especificada.`policer[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`*`]` La instrucción en el nivel de jerarquía especifica el aplicador que se utilizará para vigilar todos los paquetes de comprobación de no continuidad del tráfico CFM que pertenezcan únicamente a esta sesión.`other` *`cfm-policer1`*`[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`*`]` La instrucción especifica que se deben vigilar todos los paquetes CFM con el aplicador de control especificado.`all` *`cfm-policer2`*`cfm-policer2` Si se utiliza la opción, el usuario no puede especificar las opciones anteriores y .`all` *`policer-name`*`continuity-checkother`

```
[edit protocols oam ethernet]
connectivity-fault-management {
    maintenance-domain md {
        level number;
        maintenance-association ma {
            continuity-check {
```

```
                interval 1s;
            }
            policer {
                continuity-check cfm-policer;
                other cfm-policer1;
                all cfm-policer2;
                }
            }
            mep 1 {
                interface ge-3/3/0.0;
                direction up;
                auto-discovery;
            }
        }
    }
```

En el caso de la vigilancia global de CFM, el mismo policía se comparte en varias sesiones de CFM. En la vigilancia de CFM por sesión, se debe crear un controlador independiente para limitar la velocidad de los paquetes específicos de esa sesión.

NOTA: La configuración del aplicador de políticas de nivel de servicio para dos sesiones CFM cualesquiera en la misma interfaz en diferentes niveles debe satisfacer las siguientes restricciones si la dirección de las sesiones es la misma:

- Si una sesión está configurada con , la otra sesión no puede tener una configuración o `.policer allpolicer allpolicer other`
- Si una sesión está configurada con , la otra sesión no puede tener una configuración o `.policer otherpolicer allpolicer other`

Se producirá un error de confirmación si se confirma dicha configuración.

NOTA: No se admiten aplicadores de políticas con PBB y MIP.

SEE ALSO

policer (sesión CFM)

policer (CFM Global)

Mostrar políticas de administración de fallas de conectividad Ethernet de OAM

Clear OAM Ethernet connectivity-fault-management policer

Habilitación del modo de administración de errores de conectividad mejorada

Puede habilitar el modo de administración de errores de conectividad mejorada (CFM) para habilitar una implementación eficaz de OAM de Ethernet en redes de escalado. Al habilitar el modo CFM mejorado, Junos OS admite 32.000 puntos finales de asociación de mantenimiento (MEP) y puntos intermedios de mantenimiento (MIP) por chasis para dominios puente, VPLS, L2VPN y CCC. En versiones anteriores, Junos OS admite 8.000 MEP y 8000 MIPS por chasis. Si no habilita CFM mejorado, Junos OS seguirá admitiendo el número existente de MIP y MEP por chasis.

NOTA: Para admitir el modo CFM mejorado, configure el modo de servicios de red en el enrutador como `.enhanced-ip` Si el modo de servicios de red no es y ha habilitado CFM mejorado, se muestra el siguiente mensaje de advertencia:`enhanced-ip`

```
[edit protocols oam ethernet] 'connectivity-fault-management' enhanced ip is not effective please
configure enhanced ip and give router reboot
```

Para habilitar el modo CFM mejorado, realice los pasos siguientes:

1. En el modo de configuración, vaya al nivel de jerarquía.`[edit protocols oam ethernet connectivity-fault-management]`

   ```
   [edit]
   user@host# edit protocols oam ethernet connectivity-fault-management
   ```

2. Habilite una implementación eficaz de OAM de Ethernet habilitando el modo CFM mejorado.

   ```
   [edit protocols oam ethernet connectivity-fault-management ]
   user@host# set enhanced-cfm-mode
   ```

3. Confirme el cambio de modo. Aparecerá un mensaje de advertencia pidiéndole que reinicie CFM. Si no reinicia CFM, Junos OS reiniciará CFM automáticamente.

   ```
   [edit protocols oam ethernet connectivity-fault-management ]
   user@host # commit
   [edit protocols oam ethernet]
   'connectivity fault management’
   CFM mode change is catastrophic. cfmd will be restarted
   commit complete
   ```

4. Para comprobar si se ha configurado el modo CFM mejorado, utilice el comando.`show oam ethernet connectivity-fault-management state`

```
[edit protocols oam ethernet connectivity-fault-management ]
user@host# show oam ethernet connectivity-fault-management
enhanced-cfm-mode;
traceoptions {
    file cfmd.log size 1g;
}
maintenance-domain md6 {
    level 6;
    maintenance-association ma6 {
        continuity-check {
            interval 1s;
        }
        mep 102 {
            interface ge-0/0/0.0;
            direction up;
        }
    }
}
```

SEE ALSO

> *modo CFM mejorado*

Configurar la administración de errores de conectividad para la interoperabilidad durante las actualizaciones de software unificadas en servicio

A partir de la versión 17.1, la administración de errores de conectividad (CFM) de Junos OS durante una actualización de software en servicio unificada (ISSU), funciona cuando el dispositivo del mismo nivel no es un enrutador de Juniper Networks. Al interoperar con el enrutador de otro proveedor, el enrutador de Juniper Networks conserva la información de sesión y continúa transmitiendo PDU de mensajes de comprobación de continuidad (CCM) durante la ISSU unificada. La administración de errores de conectividad sigue funcionando.

Esta característica requiere que se cumplan las siguientes condiciones:

- Los keepalives del motor de reenvío de paquetes deben estar habilitados para proporcionar transmisión en línea de MCPs. La función no funciona cuando los MCPs son transmitidos por la CPU de una tarjeta de línea, que es el método de transmisión predeterminado.

- El intervalo entre los MCPs debe ser de 1 segundo.

La interoperabilidad de CFM durante una ISSU unificada se admite en los siguientes MPC: MPC1, MPC2, MPC2-NG, MPC3-NG, MPC5 y MPC6.

Para habilitar la interoperabilidad de CFM con dispositivos de terceros en una ISSU unificada:

1. Habilite keepalives en línea.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-keepalives enable
```

2. Establezca el intervalo CCM en 1 segundo.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name continuity-check]
user@host# set interval 1s
```

SEE ALSO

Habilitación de la transmisión en línea de mensajes de comprobación de continuidad para obtener la máxima escala | 371

Soporte de Junos OS para la supervisión del rendimiento que cumple con la especificación técnica MEF 36

Junos OS versión 16.1R1 y posteriores admiten la supervisión del rendimiento que cumple con la especificación técnica MEF 36. La especificación técnica MEF 36 especifica la MIB de supervisión del rendimiento. La MIB de supervisión del rendimiento es necesaria para gestionar las implementaciones de operaciones, administración y mantenimiento de servicios (OAM) que satisfagan los requisitos y el marco de OAM de servicio especificados en MEF 17 y MEF 35, los objetos de administración especificados en MEF 7.1 y las funciones de supervisión del rendimiento definidas en ITU-T Y.1731 y IEEE 802.1ag.

Puede habilitar la supervisión del rendimiento conforme a MEF-36 configurando la instrucción en el nivel de jerarquía.`measurement-interval`[`edit protocols oam ethernet cfm performance-monitoring`]

Cuando la supervisión del rendimiento conforme a MEF-36 está habilitada:

- Es posible que una solicitud SNMP get next para una variable no obtenga el valor actual a menos que se realice una caminata SNMP antes de realizar la solicitud get next. Esta limitación se aplica únicamente a las estadísticas actuales para la medición de retardo, la medición de pérdidas y la medición de pérdidas sintéticas.

- El resultado del campo puede mostrar un intervalo de medición de 0 (cero) y una marca de tiempo incorrecta hasta que expire el tiempo del primer ciclo.`Current delay measurement statistics`
- El tamaño de TLV de datos admitido para las unidades de datos del protocolo de supervisión del rendimiento (PDU) es de 1386 bytes cuando la supervisión del rendimiento compatible con MEF-36 está habilitada. El tamaño del TLV es de 1400 bytes en modo heredado.
- El valor máximo configurable para la bandeja de umbral inferior es 4.294.967.294.
- El índice de pérdida de trama (FLR) se excluye en las mediciones de pérdida durante el período de indisponibilidad solo para la medición de pérdida sintética. En caso de medición de pérdidas, se incluye FLR incluso durante el período de indisponibilidad.
- Durante un período de pérdida de continuidad (adyacencia hacia abajo), aunque no se envían PDU SOAM, no se detienen los cálculos de FLR y disponibilidad. Estos cálculos se realizan con el supuesto de una pérdida del 100%.
- Es posible que el número de PDU SOAM que se envían durante el primer intervalo de medición sea inferior al esperado. Esto se debe a un retraso en la detección del estado de adyacencia en el nivel de la sesión de supervisión del rendimiento.
- El número de PDU SOAM transmitidas durante un intervalo de medición para un tiempo de ciclo de 100 ms podría no ser exacto. Por ejemplo, en un intervalo de medición de dos minutos con un tiempo de ciclo de 100 ms, las PDU SOAM transmitidas podrían estar en el rango de 1198-2000.

SEE ALSO

> *intervalo de medición*

Amortiguación del rendimiento del CFM Monitoreo de trampas y notificaciones para evitar la congestión del NMS

Puede amortiguar la supervisión del rendimiento, las capturas de cruce de umbrales y las notificaciones que se generan cada vez que se produce un evento de cruce de umbral para evitar la congestión del sistema de administración de red (NMS).

La amortiguación limita el número de capturas jnxSoamPmThresholdCrossingAlarm enviadas al NMS al resumir las ocurrencias de solapas durante un período de tiempo, conocido como temporizador de trampa de solapa, y envía una única notificación jnxSoamPmThresholdFlapAlarm al NMS. Puede configurar la duración del temporizador de captura de aletas en cualquier valor de 1 a 360 segundos.

La notificación jnxSoamPmThresholdFlapAlarm se genera y envía cuando se cumplen las siguientes condiciones:

- Se ha producido al menos un colgajo cuando el temporizador de colgajo ha caducado.
- Ha cambiado el valor del temporizador de captura de solapas, lo que provocó que el temporizador se detuviera.

Puede habilitar la amortiguación a nivel global para el iterador o puede habilitar la amortiguación en el tipo de umbral individual del iterador. Por ejemplo, para habilitar la amortiguación a nivel global, para el iterador, use el siguiente comando: `set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles` *`profile-name`* `flap-trap-monitor`. Para habilitar la amortiguación en un tipo de umbral específico, para el comando , utilice el siguiente comando:`avg-fd-twoway-threshold` `set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles` *`profile-name`* `avg-fdv-twoway-threshold flap-trap-monitor`.

También puede desactivar la amortiguación.

SEE ALSO

> *flap-trap-monitor*
>
> Descripción general de la amortiguación de la interfaz física

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.1	A partir de la versión 17.1, la administración de errores de conectividad (CFM) de Junos OS durante una actualización de software en servicio unificada (ISSU), funciona cuando el dispositivo del mismo nivel no es un enrutador de Juniper Networks.
12.3	A partir de Junos OS versión 12.3, para todas las interfaces configuradas en concentradores de puertos modulares (MPC) en plataformas de enrutamiento universal 5G serie MX, ya no es necesario configurar la instrucción para todas las VPN de capa 2 y circuitos de capa 2 sobre los que se ejecutan MEP CFM.`no-control-word`
12.3	A partir de Junos OS versión 12.3, para todas las interfaces configuradas en concentradores de puertos modulares (MPC) en plataformas de enrutamiento universal 5G serie MX, ya no es necesario configurar la instrucción para todas las VPN de capa 2 y circuitos de capa 2 sobre los que se ejecutan MEP CFM.`no-control-word`

12.3	A partir de Junos OS versión 12.3, para todas las interfaces configuradas en concentradores de puertos modulares (MPC) en plataformas de enrutamiento universal 5G serie MX, ya no es necesario configurar la instrucción para todas las VPN de capa 2 y circuitos de capa 2 sobre los que se ejecutan MEP CFM.`no-control-word`

Perfil de acción de CFM

summary

in this section

- Descripción general del perfil de acción de CFM para reducir un grupo de interfaces lógicas | **59**
- Configurar un perfil de acción CFM para reducir un grupo de interfaces lógicas | **61**
- Configurar un perfil de acción de CFM para especificar acciones de CFM para eventos de CFM | **65**

Descripción general del perfil de acción de CFM para reducir un grupo de interfaces lógicas

in this section

- Ventajas de crear un perfil de acción CFM para reducir un grupo de interfaces lógicas | **60**

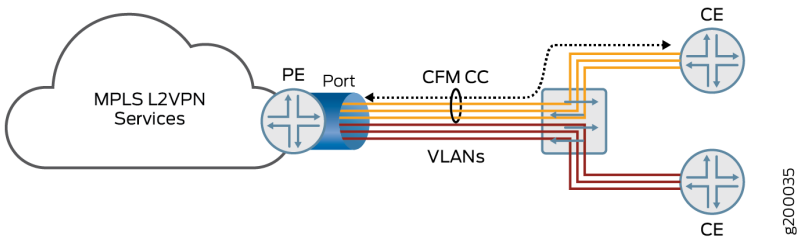
Con el crecimiento de las redes, existe el requisito de monitorear una gran cantidad de servicios que usan CFM. Para supervisar cada servicio, se requiere una sesión por interfaz lógica de servicio. Si los servicios son grandes, este método no escala ya que el número de sesiones es limitado. En lugar de una sesión de CFM por servicio, una sola sesión de CFM puede supervisar varios servicios.

Además, hay escenarios en los que el dispositivo de interfaz de usuario a red (UNI) debe desconectarse en función de las sesiones en la interfaz lógica de interfaz de red a red (NNI). Aquí, la interfaz lógica NNI se refiere a la interfaz principal y la interfaz física UNI se refiere a la interfaz de acceso que aloja

múltiples interfaces lógicas de servicio. En función de la supervisión de la interfaz principal, puede desactivar las interfaces lógicas de servicio asociadas con la interfaz de acceso.

Figura 3 en la página 60 ilustra una topología en la que varios servicios destinados a enrutadores perimetrales del cliente (CE) comparten un único puerto en un enrutador perimetral de proveedor (PE). Cada servicio utiliza una interfaz lógica. Un conjunto de servicios o interfaces lógicas (con color amarillo) están destinados a un enrutador CE y un conjunto de servicios o interfaces lógicas coloreadas en rojo están destinados a otro enrutador CE. Para supervisar cada servicio, necesita sesiones de punto final de asociación de mantenimiento (MEP) dedicadas para cada servicio. Puede desactivar el servicio desactivando la interfaz lógica del servicio cada vez que se interrumpa la sesión. Sin embargo, este enfoque no es escalable si tenemos un gran número de servicios. Tampoco es factible supervisar la sesión CFM en la interfaz física, ya que es posible que se conecten varios enrutadores CE y que se interrumpan los servicios a otros enrutadores CE. Para abordar este problema de supervisión de varios servicios con una sola sesión, puede crear un perfil de acción de CCM para reducir un grupo de interfaces lógicas mediante una sesión de CFM configurada en una sola interfaz lógica.

Figura 3: Topología de múltiples servicios VLAN que comparten un único puerto en un enrutador PE destinado a múltiples enrutadores CE



Puede configurar los perfiles de acción del MCP para los siguientes escenarios:

- Para desactivar un grupo de interfaces lógicas que tienen el mismo puerto primario cuando la sesión de monitoreo de CCM se ejecuta en una de las interfaces lógicas pero en un puerto primario diferente.
- Para desactivar un grupo de interfaces lógicas cuando la sesión de monitoreo de CCM se ejecuta en una de las interfaces lógicas, todas pertenecientes al mismo puerto principal.
- Para desactivar el puerto, cuando la sesión de monitoreo del MCP se está ejecutando en una de las interfaces lógicas de un puerto padre diferente.

Ventajas de crear un perfil de acción CFM para reducir un grupo de interfaces lógicas

- Reduce los requerimientos de recursos en redes escaladas donde es necesario monitorear múltiples servicios.

- Evita la necesidad de crear sesiones MEP individuales para cada servicio en una topología que incluye múltiples servicios para ser monitoreados, mejorando así el rendimiento y la escalabilidad de la red.

SEE ALSO

> *perfil de acción*

Configurar un perfil de acción CFM para reducir un grupo de interfaces lógicas

Para supervisar varios servicios o IFL utilizando la sesión CFM configurada en una única interfaz lógica, puede crear un perfil de acción de CCM para reducir un grupo de interfaces lógicas. Debe definir una acción para reducir el grupo de interfaces en el perfil de acción. A continuación, definirá el nombre del dispositivo de interfaz y el número de interfaces lógicas que deben desplegarse. Una interfaz lógica se representa mediante una combinación de `.interface-device-nameunit-list` Los pasos siguientes explican el procedimiento para desactivar un grupo de interfaces lógicas cuando se especifican y /o `.interface-device-nameunit-list`

1. En el modo de configuración, en el nivel de jerarquía [], especifique el nombre del perfil de acción y los eventos de CFM.`edit protocols oam ethernet connectivity-fault-management` Puede configurar más de un evento en el perfil de acción.

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set action-profile profile-name event [event1, event2, event3..]
   ```

   Suponga, por ejemplo,

   ```
   user@host# set action-profile AP_test event adjacency-loss rdi
   ```

   > **NOTA**: La acción no se apoyará con eventos que no sean pérdida de adyacencia y RDI.`interface-group-down` Cualquier otro evento configurado dará como resultado un error de confirmación.

2. En el modo de configuración, en el nivel de jerarquía [], defina la acción para reducir el grupo de interfaces.`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`*

   ```
   [edit protocols oam ethernet connectivity-fault-management action-profile  AP-test ]
   user@host# set action interface-group-down
   ```

> **NOTA**: La acción no se admitirá con otras acciones relacionadas con la interfaz.`interface-group-down` Cualquier otra acción configurada dará como resultado un error de confirmación.

3. En el nivel de jerarquía [], defina el dominio de mantenimiento.`edit protocols oam ethernet connectivity-fault-management` Especifique los parámetros de mantenimiento-asociación.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenance-domain domain-name  level number maintenance-association ma-name
continuity-check interval 1s
```

Suponga, por ejemplo,

```
user@host# set maintenance-domain md6 level 6 maintenance-association ma6 continuity-check
interval 1s
```

4. En el , defina el extremo de la asociación de mantenimiento y los parámetros asociados.`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`*

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name]
user@host# set mep mep-id interface interface-name direction down remote -mep mep-id
```

Suponga, por ejemplo,

```
user@host# set mep 101 interface ge-0/0/0.0 direction down remote -mep 102
```

5. Si el perfil de acción tiene una acción configurada, es obligatorio configurarla en el nivel RMEP.`interface-group-downinterface-group` En el modo de configuración, en el incluir la instrucción para bajar el grupo de interfaces marcado con el perfil de acción como .`[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `mep` *`mep-id`* `remote-mep` *`mep-id`* `action-profile` *`profile-name`*`interface-groupinterface-group-down`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep mep-id action-profile profile-name]
user@host# set interface-group
```

Suponga, por ejemplo,

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md6 maintenance-association ma6 mep 101 remote-mep 102 action-profile AP_test]
user@host# set interface-group
```

NOTA: Si la configuración no está incluida en la configuración de RMEP.`interface-group` La configuración da como resultado un error de confirmación.

6. Una interfaz lógica se representa mediante una combinación de .`interface-device-nameunit-list` Configure el nombre de la interfaz del dispositivo y el número de interfaces lógicas en el .`[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `mep` *`mep-id`* `remote-mep` *`mep-id`* `action-profile` *`profile-name`* `interface-group`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep mep-id action-profile profile-name
interface-group]
user@host# set interface interface-name
user@host# set unit-list logical-interface-unit-number
```

Suponga, por ejemplo,

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md6 maintenance-association ma6 mep 101 remote-mep 102 action-profile AP_test interface-group]
user@host# set interface ge-0/0/0.0
user@host# set unit-list 1223-3344
```

En este ejemplo de configuración, la interfaz ge-0/0/0.0 está inactiva.

NOTA:

- Al menos uno de los parámetros, o debe estar configurado.`interface-groupinterface-device-nameunit-list` Si el nombre del dispositivo de interfaz no está configurado, la interfaz MEP se considera como el nombre del dispositivo y la interfaz lógica de ese dispositivo se desactiva.

- Si el parámetro supera el límite recomendado, se produce un error de confirmación.`unit-list`
- Si no se especifica el en el , se desactivan los números de interfaz lógica mencionados en para la interfaz física.*interface-device-name*`interface-groupunit-list`
- Si no se especifica en el , los IFL se desactivan para la interfaz configurada.*unit-list*`interface-group`

7. Compruebe la configuración mediante el comando.`show protocols oam`

```
[edit]
user@host# show protocols oam
ethernet {
    connectivity-fault-management {
        action-profile AP_TEST {
            event {
                adjacency-loss;
                rdi;
            }
            action {
                interface-group-down;
            }
        }
        maintenance-domain md6 {
            level 6;
            maintenance-association ma6 {
                continuity-check {
                    interval 1s;
                }
                mep 102 {
                    interface ge-0/0/0.0;
                    direction down;
                    remote-mep 103 {
                        action-profile AP_TEST;
                        interface-group {
                          ge-0/0/1;
                           unit-list [12 23-33 44];
                        }
                    }
                }
            }
```

```
        }
    }
}
```

SEE ALSO

> *grupo de interfaz*
>
> *interfaz-grupo-abajo*

Configurar un perfil de acción de CFM para especificar acciones de CFM para eventos de CFM

Puede crear un perfil de acción de administración de errores de conectividad (CFM) para definir los indicadores de eventos y los umbrales que se van a supervisar. También puede especificar la acción que debe realizarse cuando se produzca alguno de los eventos configurados. Cuando se producen los eventos CFM, el enrutador realiza la acción correspondiente en función de su especificación. Puede configurar uno o más eventos en el perfil de acción. Como alternativa, puede configurar un perfil de acción y especificar acciones predeterminadas cuando falle la conectividad con un extremo de asociación de mantenimiento remoto (MEP).

> **NOTA**: No puede configurar varias acciones en este momento. Solo se puede configurar una acción. Esta limitación afecta tanto a las instrucciones y `.actionclear-action`

Para configurar el perfil de acción de CFM:

1. En el modo de configuración, en el nivel de jerarquía [], especifique el nombre del perfil de acción y los eventos de CFM.`edit protocols oam ethernet connectivity-fault-management` Puede configurar más de un evento en el perfil de acción. Los posibles eventos incluyen: interface-status-tlv, port-status-tlv, adyacencia-pérdida, RDI.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set action-profile profile-name event [event1, event2, event3..]
```

2. Especifique la acción que debe realizar el enrutador cuando ocurra el evento. La acción se desencadena cuando se produce el evento. Si ha configurado más de un evento en el perfil de acción, no es necesario que se produzcan todos los eventos para desencadenar la acción.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set action-profile profile-name action action
```

3. Especifique la acción predeterminada que debe realizar el enrutador cuando falle la conectividad con un MEP remoto. Si no se configura ninguna acción, no se realiza ninguna acción.

> **NOTA**: No es aconsejable asociar un perfil de acción con la acción en una sesión CFM MEP que se ejecuta sobre una interfaz de conexión cruzada de circuito (CCC) (l2circuit/l2vpn) y puede dar lugar a una situación de interbloqueo.`interface-down`

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set action-profile profile-name default-actions action
```

SEE ALSO

evento (CFM)

acciones predeterminadas

gestión de errores de conectividad

Interfaz de administración local Ethernet

in this section

- Descripción general de la interfaz de administración local Ethernet | **67**
- Configurar la interfaz de administración local de Ethernet | **69**
- Ejemplo de configuración de E-LMI | **72**

Descripción general de la interfaz de administración local Ethernet

Las interfaces Gigabit Ethernet (), 10 Gigabit Ethernet () y Ethernet agregada () admiten la interfaz de administración local Ethernet (E-LMI).gexeae

> **NOTA**: En los enrutadores de la serie MX, E-LMI es compatible con interfaces Gigabit Ethernet (), 10 Gigabit Ethernet () y Ethernet agregada () configuradas en enrutadores serie MX solo con DPC.gexeae

La especificación E-LMI está disponible en el Foro Metro Ethernet. Los procedimientos y protocolos de E-LMI se utilizan para habilitar la configuración automática del borde del cliente (CE) para admitir los servicios de Metro Ethernet. El protocolo E-LMI también proporciona información de estado de interfaz de usuario a red (UNI) y conexión virtual Ethernet (EVC) al CE. La información UNI y EVC permite la configuración automática del funcionamiento CE basado en la configuración Metro Ethernet.

El protocolo E-LMI funciona entre el dispositivo CE y el dispositivo perimetral del proveedor (PE). Solo se ejecuta en el vínculo PE-CE y notifica al CE el estado de conectividad y los parámetros de configuración de los servicios Ethernet disponibles en el puerto CE. El alcance del protocolo E-LMI se muestra en .Figura 4 en la página 67

Figura 4: Ámbito de aplicación del protocolo E-LMI

La implementación de E-LMI en enrutadores de las series ACX y MX incluye solo el lado PE del protocolo E-LMI.

E-LMI interopera con un protocolo OAM, como Connectivity Fault Management (CFM), que se ejecuta dentro de la red del proveedor para recopilar el estado de OAM. CFM se ejecuta en el nivel de mantenimiento del proveedor (UNI-N a UNI-N con hasta MEPs en la UNI). E-LMI se basa en el CFM para el estado de extremo a extremo de los EVC en todos los dominios CFM (dominio SVLAN o VPLS).

El protocolo E-LMI transmite la siguiente información:

- Notificación al CE de la adición/eliminación de un EVC (activo, no activo o parcialmente activo)

- Notificación al CE del estado de disponibilidad de un EVC configurado
- Comunicación de los atributos UNI y EVC al CE:
  - Atributos de UNI:
    - Identificador UNI (un nombre configurado por el usuario para UNI)
    - Tipo de mapa CE-VLAN ID/EVC (agrupación todo a uno, multiplexación de servicios con agrupación o sin agrupación)
    - No se admite el perfil de ancho de banda (incluidas las siguientes características):
      - CM (modo de acoplamiento)
      - CF (bandera de color)
      - CIR (tasa de información comprometida)
      - CBR (tamaño de ráfaga comprometida)
      - EIR (tasa de exceso de información)
      - EBS (tamaño de ráfaga excesiva)
  - Atributos de EVC:
    - ID de referencia de EVC
    - Tipo de estado de EVC (activo, no activo o parcialmente activo)
    - Tipo de EVC (punto a punto o multipunto a multipunto)
    - ID de EVC (un nombre configurado por el usuario para EVC)
    - Perfil de ancho de banda (no compatible)
  - Mapa CE-VLAN ID/EVC

E-LMI en enrutadores de la serie MX admite los siguientes tipos de EVC:

- SVLAN Q-in-Q (punto a punto o multipunto a multipunto): requiere una sesión de CFM de extremo a extremo entre UNI-N para supervisar el estado del SVE.
- VPLS (BGP o LDP) (punto a punto o multipunto a multipunto): el estado del pseudocable VPLS o las sesiones CFM de extremo a extremo entre UNI-N se pueden utilizar para supervisar el estado de EVC.
- Circuito L2/L2VPN (punto a punto): se puede utilizar el estado del pseudocable VPLS o las sesiones CFM de extremo a extremo entre UNI-N para supervisar el estado de EVC.

NOTA: y no son compatibles.`l2-circuitl2vpn`

El protocolo E-LMI de los enrutadores de la serie ACX admite los tipos de circuito de capa 2 y EVC de VPN de capa 2, y permite el reenvío de pérdida de vínculos para servicios de pseudocable (circuito de capa 2 y VPN de capa 2) de la siguiente manera:

- Interfuncionamiento entre el protocolo de gestión de errores de conectividad (CFM) y el protocolo E-LMI para circuitos de capa 2 y VPN de capa 2.
  - Sesión de CFM de extremo a extremo entre UNI para supervisar el estado de EVC.
  - En el caso de la redundancia de pseudocable, CFM se puede utilizar para monitorear sesiones de pseudocable activas y de respaldo. El estado de EVC se declara como inferior a los dispositivos CE solo cuando las sesiones de pseudocable activas y de respaldo dejan de funcionar.
- Interfuncionamiento entre la indicación remota de defectos (RDI) y E-LMI para circuito de capa 2 y VPN de capa 2.
  - Si un punto final de asociación de mantenimiento (MEP) recibe un bit RDI establecido en una trama de mensaje de comprobación de continuidad (CCM) y si la detección de errores de RDI está habilitada en la configuración de EVC en , entonces el pseudocable se declara como hasta enrutadores CE a través de E-LMI.`[edit protocols oam ethernet evcs evc-id evc-protocol cfm management-domain name management-association name faults rdi]`
- Si no existe una sesión CFM de extremo a extremo entre UNI, el estado ascendente y descendente del pseudocable (circuito de capa 2 o VPN de capa 2) activa un mensaje asíncrono de cambio de estado de EVC a los enrutadores CE a través de E-LMI.

NOTA: Los enrutadores serie ACX no admiten E-LMI para servicios de capa 2 (puente).

Configurar la interfaz de administración local de Ethernet

in this section

- Configuración de un protocolo OAM (CFM) | **70**
- Asignación del protocolo OAM a un EVC | **70**
- Habilitación de e-LMI en una interfaz y asignación de ID de VLAN CE a un EVC | **70**

Para configurar E-LMI, realice los pasos siguientes:

Configuración de un protocolo OAM (CFM)

Para obtener información sobre la configuración del protocolo OAM (CFM), consulte Descripción general de la administración de errores de conectividad OAM IEEE 802.1ag."Administración de errores de conectividad OAM IEEE 802.1ag" en la página 22

Asignación del protocolo OAM a un EVC

Para configurar un EVC, debe especificar un nombre para el EVC utilizando la instrucción en el nivel de jerarquía.`evcs`*`evc-id`*`[edit protocols oam ethernet]` Puede establecer el protocolo EVC para supervisar las estadísticas de EVC en o utilizar la instrucción y sus opciones en el nivel jerárquico `.cfmvplsevc-protocol[edit protocols oam ethernet evcs]`

Puede establecer el número de UNI remotas en el EVC mediante la instrucción en el nivel de jerarquía.`remote-uni-count` *`number`*`[edit protocols oam ethernet evcs evcs-protocol]` El valor predeterminado es 1. La configuración de un valor mayor que 1 hace que la EVC sea multipunto a multipunto.`remote-uni-count` Si ingresa un valor mayor que el número real de puntos de conexión, el estado de EVC se mostrará como parcialmente activo incluso si todos los puntos de conexión están activos. Si ingresa un número de puntos de conexión inferior al real, el estado se mostrará como activo, incluso si todos los puntos de conexión no están activos.`remote-uni-count`

Puede configurar un EVC incluyendo la instrucción en el nivel de jerarquía:`evcs[edit protocols oam ethernet]`

```
[edit protocols oam ethernet]
evcs evc-id {
    evc-protocol (cfm (management-domain name management-association name ) | vpls (routing-
instance name)) {
        remote-uni-count <number>;      # Optional, defaults to 1
        multipoint-to-multipoint;
 # Optional, defaults to point-to-point if remote-uni-count is 1
    }
}
```

Habilitación de e-LMI en una interfaz y asignación de ID de VLAN CE a un EVC

Para configurar E-LMI, incluya la instrucción en el nivel jerárquico :`lmi[edit protocols oam ethernet]`

```
[edit protocols oam ethernet]
lmi {
```

```
    polling-verification-timer value;
# Polling verification timer (T392), defaults to 15 seconds
    status-counter count; # Status counter (N393), defaults to 4
    interface name {
        evc evc-id {
            default-evc;
            vlan-list [ vlan-ids ];
        }
        evc-map-type (all-to-one-bundling | bundling | service-multiplexing);
        polling-verification-time value; # Optional, defaults to global value
        status-counter count; # Optional, defaults to global value
        uni-id value; # Optional, defaults to interface-name
    }
}
```

Puede establecer el contador de estado para contar errores consecutivos mediante la instrucción en el nivel de jerarquía.`status-counter` *`count`*`[edit protocols oam ethernet lmi]` El contador de estado se utiliza para determinar si E-LMI está operativo o no. El valor predeterminado es 4.

Puede establecer la instrucción en el nivel jerárquico `.polling-verification-timer` *`value`*`[edit protocols oam ethernet lmi]` El valor predeterminado es 15 segundos.

Puede habilitar una interfaz y establecer sus opciones para su uso con E-LMI utilizando la instrucción en el nivel de jerarquía.`interface` *`name`*`[edit protocols oam ethernet lmi]` Solo se admiten , , y las interfaces.`gexeae` Puede utilizar la opción de interfaz para especificar un nombre para la UNI.`uni-id` Si no está configurado, el valor predeterminado es la variable de nombre de `.uni-idinterface` *`name`*

Puede especificar el tipo de mapa CE-VLAN ID/EVC mediante la opción de interfaz.`evc-map-type type` Las opciones son , , o `.all-to-one-bundlingbundlingservice-multiplexing` La multiplexación de servicios es sin agrupación. El tipo predeterminado es `.all-to-one-bundling`

Para especificar el EVC que utiliza una interfaz, utilice la instrucción en el nivel de jerarquía.`evc` *`evc-id`*`[edit protocols oam ethernet lmi interface` *`name`*`]` Puede especificar una interfaz como interfaz EVC predeterminada mediante la instrucción en el nivel de jerarquía.`default-evc[edit protocols oam ethernet lmi interface` *`name`* `evc` *`evc-id`*`]` Todos los VID que no están asignados a ningún otro EVC se asignan a este EVC. Solo se puede configurar un EVC como predeterminado.

Puede asignar una lista de VLAN a un EVC mediante la instrucción en el nivel de jerarquía.`vlan-list` *`vlan-id-list`*`[edit protocols oam ethernet lmi interface` *`name`* `evc` *`evc-id`*`]`

Ejemplo de configuración de E-LMI

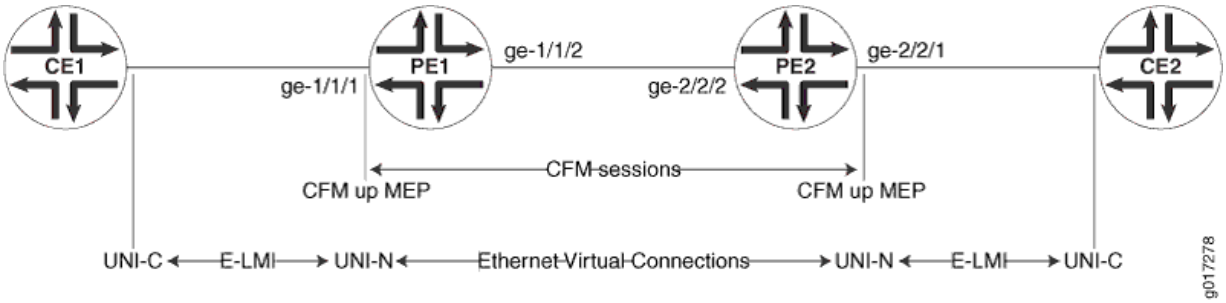
in this section

- Ejemplo de topología | 72
- Configuración de PE1 | 72
- Configuración de PE2 | 74
- Configuración de dos UNI que comparten el mismo EVC | 76

Ejemplo de topología

Figura 5 en la página 72 ilustra la configuración de E-LMI para un EVC punto a punto (SVLAN) supervisado por CFM. En este ejemplo, las VLAN del 1 al 2048 se asignan a (SVLAN 100) y del 2049 al 4096 se asignan a (SVLAN 200).evc1evc2 Se crean dos sesiones de CFM para supervisar estos EVC.

Figura 5: Configuración de E-LMI para un EVC punto a punto (SVLAN) monitoreado por CFM



Configuración de PE1

```
[edit]
interfaces {
    ge-1/1/1 {
        unit 0 {
            family bridge {
                interface-mode trunk;
                vlan-id-list 1-2048;
            }
        }
```

```
        unit 1 {
            family bridge {
                interface-mode trunk;
                vlan-id-list 2049-4096;
            }
        }
    }
    ge-1/1/2 {
        unit 0 {
            vlan-id 100;
            family bridge {
                interface-mode trunk;
                inner-vlan-id-list 1-2048;
            }
        }
        unit 1 {
            vlan-id 200;
            family bridge {
                interface-mode trunk;
                inner-vlan-id-list 2049-4096;
            }
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 0;
                    maintenance-association 1 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-1/1/1.0 vlan 1;
                        }
                    }
                    maintenance-association 2049 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-1/1/1.1 vlan 2049;
                        }
```

```
                    }
                }
            }
            evcs {
                evc1 {
                    evc-protocol cfm management-domain md management-association 1;
                    remote-uni-count 1;
                }
                evc2 {
                    evc-protocol cfm management-domain md management-association 2049;
                    remote-uni-count 1;
                }
            }
            lmi {
                interface ge-1/1/1 {
                    evc evc1 {
                        vlan-list 1-2048;
                    }
                    evc evc2 {
                        vlan-list 2049-4096;
                    }
                    evc-map-type bundling;
                    uni-id uni-ce1;
                }
            }
        }
    }
}
```

Configuración de PE2

```
[edit]
interfaces {
    ge-2/2/1 {
        unit 0 {
            family bridge {
                interface-mode trunk;
                vlan-id-list 1-2048;
            }
        }
        unit 1 {
```

```
            family bridge {
                interface-mode trunk;
                vlan-id-list 2049-4096;
            }
        }
    }
    ge-2/2/2 {
        unit 0 {
            vlan-id 100;
            family bridge {
                interface-mode trunk;
                inner-vlan-id-list 1-2048;
            }
        }
        unit 1 {
            vlan-id 200;
            family bridge {
                interface-mode trunk;
                inner-vlan-id-list 2049-4095;
            }
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 0;
                    maintenance-association 1 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-2/2/1.0 vlan 1;
                        }
                    }
                    maintenance-association 2049 {
                        name-format vlan;
                        mep 1 {
                            direction up;
                            interface ge-2/2/1.1 vlan 2049;
                        }
                    }
```

```
                }
            }
            evcs {
                evc1 {
                    evc-protocol cfm management-domain md management-association 1;
                    remote-uni-count 1;
                }
                evc2 {
                    evc-protocol cfm management-domain md management-association 2049;
                    uni-count 2;
                }
            }
            lmi {
                interface ge-2/2/1 {
                    evc evc1 {
                        vlan-list 1-2048;
                    }
                    evc evc2 {
                        vlan-list 2049-4095;
                    }
                    evc-map-type bundling;
                    uni-id uni-ce2;
                }
            }
        }
    }
}
```

Configuración de dos UNI que comparten el mismo EVC

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management { ...}
        evcs {
            evc1 {
                evc-protocol cfm management-domain md management-association 1;
                remote-uni-count 1;
            }
        }
        lmi {
```

```
            interface ge-2/2/1 {
                evc evc1 {
                    vlan-list 0-4095;
                }
                evc-map-type all-to-one-bundling;
                uni-id uni-ce1;
            }
            interface ge-2/3/1 {
                evc evc1 {
                    vlan-list 0-4095;
                }
                evc-map-type all-to-one-bundling;
                uni-id uni-ce2;
            }
        }
    }
}
```

VÍNCULOS RELACIONADOS

gestión de errores de conectividad

Soporte CFM para paquetes encapsulados CCC

in this section

- Descripción general de la compatibilidad con IEEE 802.1ag CFM OAM para paquetes encapsulados CCC | **78**
- Funciones de CFM compatibles con circuitos VPN de capa 2 | **78**
- Configurar CFM para paquetes encapsulados CCC | **79**

Descripción general de la compatibilidad con IEEE 802.1ag CFM OAM para paquetes encapsulados CCC

La red privada virtual de capa 2 (L2VPN) es un tipo de servicio de red privada virtual que se utiliza para transportar el tráfico privado de capa 2 del cliente (por ejemplo, Ethernet, ATM o Frame Relay) a través de la infraestructura IP/MPLS compartida del proveedor de servicios. El enrutador perimetral del proveedor de servicios (PE) debe tener una interfaz con encapsulación de conexión cruzada de circuitos (CCC) para conmutar el tráfico perimetral del cliente (CE) a la red pública.

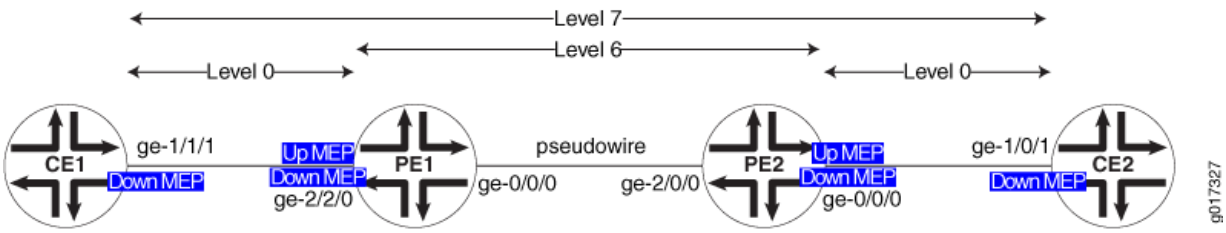
IEEE 802.1ag Ethernet Connectivity Fault Management (CFM) es un estándar OAM que se utiliza para realizar la detección, el aislamiento y la verificación de fallas en LAN de puente virtual. Los enrutadores de las series M120 y MX ofrecen compatibilidad CFM con interfaces puente/VPLS/enrutadas y admiten Ethernet OAM 802.1ag para paquetes encapsulados CCC.

Funciones de CFM compatibles con circuitos VPN de capa 2

Las funciones de CFM compatibles con los circuitos L2VPN son las siguientes:

- Creación de eurodiputados arriba/abajo a cualquier nivel en las interfaces lógicas orientadas a CE.
- Creación de MIPs a cualquier nivel en las interfaces lógicas orientadas a CE.
- Soporte para comprobación de continuidad, circuito cerrado y protocolo linkrace.
- Soporte para el protocolo de medición de retardo Ethernet Y1731.
- Compatibilidad con perfiles de acción para desactivar las interfaces lógicas orientadas hacia CE cuando se detecta pérdida de conectividad.

Figura 6: Topología VPN de capa 2



Para supervisar el circuito L2VPN, se puede configurar un CFM up MEP (Level 6 in Figura 6 en la página 78) en las interfaces lógicas orientadas hacia CE de los enrutadores perimetrales del proveedor PE1 y PE2. Para supervisar el circuito de fijación CE-PE, se puede configurar un MEP CFM down en las interfaces lógicas del cliente de CE1-PE1 y CE2-PE2 (nivel 0 en).Figura 6 en la página 78

Configurar CFM para paquetes encapsulados CCC

El único cambio con respecto a la configuración de CLI existente es la introducción de un nuevo comando para crear un MIP en la interfaz orientada a CE del enrutador PE.

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {

                # Define a maintenance domains for each default level.
                #; These names are specified as DEFAULT_level_number
                maintenance-domain DEFAULT_x {
                    # L2VPN CE interface
                    interface (ge | xe)-fpc/pic/port.domain;
                }
                {
                level number;
                maintenance-association identifier {
                    mep mep-id {
                        direction (up | down);
                        # L2 VPN CE interface on which encapsulation family CCC is configured.
                        interface  (ge | xe)-fpc/pic/port.domain;
                        auto-discovery;
                        priority number;
                    }
                }
            }
        }
    }
    }
}
```

SEE ALSO

gestión de errores de conectividad

Configurar ISSU unificada para 802.1ag CFM

Una actualización de software en servicio unificada (ISSU) le permite actualizar entre dos versiones diferentes de Junos OS sin interrupciones en el plano de control y con una interrupción mínima del tráfico. La ISSU unificada se habilita automáticamente para los protocolos de administración de errores de conectividad (CFM) e interopera entre los extremos de mantenimiento local y remoto (MEP).

Junos OS proporciona compatibilidad con ISSU unificada mediante el valor de longitud de tipo de umbral de pérdida (TLV), que se habilita automáticamente para CFM. Los TLV se describen en el estándar IEEE 802.1ag para CFM como un método de codificación de longitud variable e información opcional en una unidad de datos de protocolo (PDU). El TLV de umbral de pérdida indica el valor de umbral de pérdida de un MEP remoto. El TLV de umbral de pérdida se transmite como parte de los mensajes de comprobación de continuidad del CFM.

NOTA: A partir de Junos OS versión 15.1, la configuración de ISSU con CFM (802.1ag) solo se admite en enrutadores MX y PTX compatibles con TLV. No se admite la interoperabilidad con otros proveedores.

Durante una ISSU unificada, el plano de control puede caer durante varios segundos y provocar la caída de los paquetes de comprobación de continuidad del CFM. Esto puede hacer que el MEP remoto detecte una pérdida de conectividad y marque el MEP como inactivo. Para mantener el MEP activo durante una ISSU unificada, el TLV de umbral de pérdida comunica el valor de umbral mínimo que el MEP receptor requiere para mantener activo al MEP. El MEP receptor analiza el TLV y actualiza el valor del umbral de pérdida, pero solo si el nuevo valor de umbral es mayor que el valor de umbral configurado localmente.

Se describe una descripción general de CFM a partir de "IEEE 802.1ag OAM Connectivity Fault Management Overview" en la página 22, y debe observar con más detalle los requisitos adicionales descritos en este tema.

Tabla 6 en la página 80 muestra el formato TLV de umbral de pérdida.

Tabla 6: Formato TLV de umbral de pérdida

Parámetro	Octeto (secuencia)	Description
Tipo=31	1	Obligatorio. Obligatorio. Si es 0, no le seguirán los campos Length o Value. Si no es 0, al menos el campo Longitud sigue al campo Tipo.

Tabla 6: Formato TLV de umbral de pérdida *(Continued)*

Parámetro	Octeto (secuencia)	Description
Longitud=12	2	Obligatorio si el campo Tipo no es 0. No está presente si el campo Tipo es 0. Los 16 bits del campo Longitud indican el tamaño, en octetos, del campo Valor. 0 en el campo Longitud indica que no hay ningún campo Valor.
OUI	3	Opcional. Identificador único de la organización (OUI), que es controlado por el IEEE y suelen ser los tres primeros bytes de una dirección MAC (Juniper OUI 0x009069).
Subtipo	1	Opcional. Subtipo definido organizativamente.
valor	4	Opcional. Valor umbral de pérdida.
Bandera	4	Opcional. Bit0 (identifica que una ISSU está en curso) Bit1-31 (reservado)

Junos OS proporciona compatibilidad de configuración para la instrucción, lo que permite controlar la transmisión del umbral de pérdida TLV en las PDU de mensajes de comprobación de continuidad.`convey-loss-threshold` La instrucción especifica que el TLV de umbral de pérdida debe transmitirse como parte de los mensajes de comprobación de continuidad.`convey-loss-threshold` Si no se especifica la instrucción, los mensajes de comprobación de continuidad transmiten este TLV sólo cuando hay una ISSU unificada en curso.`convey-loss-threshold` Junos OS proporciona esta configuración en el nivel de comprobación de continuidad. De forma predeterminada, los mensajes de comprobación de continuidad no incluyen el TLV de umbral de pérdida.

Para configurar el umbral de pérdida de transmisión, utilice la instrucción en el nivel de jerarquía.`convey-loss-threshold[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `continuity-check]`

Para el MEP remoto, el TLV de umbral de pérdida solo se transmite durante la ISSU unificada si la instrucción no está configurada.`convey-loss-threshold` El MEP remoto vuelve al umbral de pérdida predeterminado si no se recibe ningún TLV de umbral de pérdida o si el TLV tiene un valor de umbral predeterminado de 3.

A continuación se muestra un ejemplo de las instrucciones de configuración de ISSU:

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain identifier {
                level number;
                    maintenance-association identifier {
                        continuity-check {
                            convey-loss-threshold;
                            interval number;
                            loss-threshold number;
                            hold-interval number;
                        }
                    }
                }
            }
        }
    }
}
```

Junos OS guarda el último TLV de umbral de pérdida recibido del MEP remoto. Puede mostrar el último TLV de umbral de pérdida guardado que recibe el MEP remoto mediante el comando, como en el ejemplo siguiente:`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `local-mep` *`identifier`* `remote-mep` *`identifier`*

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md3
maintenance-association ma5 local-mep 2 remote-mep 1
Maintenance domain name: md3, Format: string, Level: 3
  Maintenance association name: ma3, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 2, Direction: up, MAC address: 00:19:e2:b0:76:be
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: yes
    Prefer me: no, Protection in use: no, FRR Flag: no
  Interface name: xe-4/1/1.0, Interface status: Active, Link status: Up
    Loss Threshold TLV:
      Loss Threshold: 3  , Flag:    0x0
```

```
 Remote MEP identifier: 1, State: ok
    MAC address: 00:1f:12:b7:ce:79, Type: Learned
    Interface: xe-4/1/1.0
    Last flapped: Never
    Continuity: 100%, Admin-enable duration: 45sec, Oper-down duration: 0sec
    Effective loss threshold: 3 frames
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
    Connection Protection TLV:
      Prefer me: no, Protection in use: no, FRR Flag: no
    Loss Threshold TLV:   #Displays last received value
      Loss Threshold: 3  , Flag:    0x0
```

Junos OS guarda el último TLV de umbral de pérdida transmitido de un MEP local. Puede mostrar el último TLV de umbral de pérdida transmitida y el umbral de pérdida efectiva (operativo) para el MEP remoto, utilizando el comando, como en el ejemplo siguiente:`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `local-mep` *`identifier`* `remote-mep` *`identifier`*

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md3
maintenance-association ma5 local-mep 2 remote-mep 1
Maintenance domain name: md3, Format: string, Level: 3
  Maintenance association name: ma3, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 2, Direction: up, MAC address: 00:19:e2:b0:76:be
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none
  Connection Protection TLV: yes
    Prefer me: no, Protection in use: no, FRR Flag: no
  Interface name: xe-4/1/1.0, Interface status: Active, Link status: Up
    Loss Threshold TLV:   #Displays last transmitted value
      Loss Threshold: 3  , Flag:    0x0

   Remote MEP identifier: 1, State: ok
    MAC address: 00:1f:12:b7:ce:79, Type: Learned
    Interface: xe-4/1/1.0
    Last flapped: Never
    Continuity: 100%, Admin-enable duration: 45sec, Oper-down duration: 0sec
    Effective loss threshold: 3 frames   #Displays operational threshold
    Remote defect indication: falsePort status TLV: none
```

```
    Interface status TLV: none
    Connection Protection TLV:
      Prefer me: no, Protection in use: no, FRR Flag: no
    Loss Threshold TLV:
      Loss Threshold: 3  , Flag:    0x0
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
15.1	A partir de Junos OS versión 15.1, la configuración de ISSU con CFM (802.1ag) solo se admite en enrutadores MX y PTX compatibles con TLV.

VÍNCULOS RELACIONADOS

- Antes de comenzar una ISSU unificada
- Requisitos del sistema de ISSU unificada

Monitoreo CFM entre dispositivos CE y PE

in this section

- Notificación asincrónica del perfil de acción CFM | **85**
- Configuración de un perfil de acción CFM para la notificación asincrónica | **86**
- Descripción de la supervisión de CFM entre dispositivos CE y PE | **88**
- Configuración de TLV de estado de puerto y TLV de estado de interfaz | **90**
- Configuración del ID de chasis TLV | **106**
- Configuración del procesamiento de mensajes MAC Flush en modo CET | **107**
- Ejemplo: Configuración de un perfil de acción basado en TLV de protección de conexión | **110**

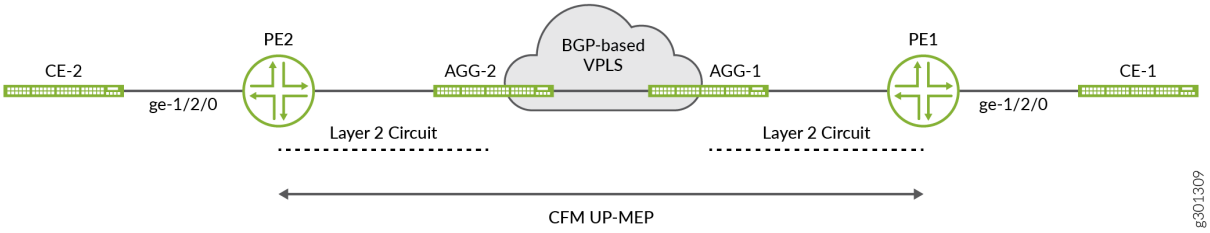
Utilice este tema para obtener más información sobre la supervisión de CFM entre dispositivos perimetrales de proveedor y dispositivos perimetrales de cliente cuando el dispositivo perimetral de cliente no es un dispositivo de Juniper. Además, puede obtener más información acerca de cómo los TLV de estado de interfaz, los TLV de estado de puerto, el TLV de ID de chasis y el TLV de protección de conexión ayudan a monitorear su red.

Notificación asincrónica del perfil de acción CFM

summary

La notificación asíncrona basada en CFM permite la sincronización del estado del vínculo entre dos dispositivos CE conectados entre sí a través de un pseudocable que se origina en sus respectivos dispositivos PE Emula el escenario como si dos dispositivos CE estuvieran conectados directamente. CFM proporciona señalización de extremo a extremo incluso si PE1 y PE2 no están conectados a través de una sola red, sino a través de un conjunto de redes.

Conectividad de capa 2 entre PE1 y PE2



La figura 1 es un ejemplo de escenario de despliegue en el que se puede usar la notificación asincrónica basada en CFM para sincronizar el estado del vínculo entre CE1 y CE2. Los siguientes dos requisitos se pueden cumplir con la configuración de notificación asíncrona.

- Cuando el vínculo entre PE2 y CE2 disminuye, el vínculo entre PE1 y CE1 también se reduce. Cuando se restaura el enlace, también debe restaurar el estado del enlace PE1 a CE1. El cambio de estado del vínculo entre PE1 y CE1 debería funcionar de la misma manera.
- Cuando hay un problema de conectividad entre PE1 y PE2, se activa un vínculo entre PE1 y CE1 y PE2 a CE2. Si se restaura el estado de la conexión, debería restaurar el estado del vínculo en ambos extremos

SEE ALSO

connectivity-fault-management

Configuración de un perfil de acción CFM para la notificación asincrónica

summary

CFM UP-MEP en PE1 a PE2, monitorea la conectividad entre PE1 y PE2. El uso de en estos puntos finales UP-MEP transmite el estado del enlace entre PE1 a CE1 a PE2 y el estado del enlace entre PE2 a CE2 a PE1.`interface-status-tlv` El perfil de acción debe configurarse en PE1 a PE2 para dirigir la notificación asíncrona hacia los respectivos dispositivos CE. Se activa cuando se detecta pérdida de adyacencia o se detecta un vínculo caído en el archivo .`interface-status-tlv`

1. Habilitar en el nivel de interfaz`asynchronous-notification`

   Por ejemplo

   ```
   user@host# set interface interface-name gigether-option asynchronous-notification
   ```

2. Configure el perfil de acción y los eventos de CFM para activar este perfil de acción en el nivel jerárquico [].`edit protocols oam ethernet connectivity-fault-management` Puede configurar más de un evento en el perfil de acción

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@host# set action-profile profile-name event [event1, event2, event3]
   ```

   Por ejemplo

   ```
   user@host# set action-profile AP_test event adjacency-loss
   ```

   La acción no se admite con eventos que no sean , y .`asynchronous-notificationinterface-status-tlv down interface-status-tlv lower-layer-down adjacency-loss` Cualquier otro evento configurado da como resultado un error de confirmación

   .

3. Defina la acción como notificación asíncrona en el nivel jerárquico [action-profile profile-name].`edit protocols oam ethernet connectivity-fault-management`

   ```
   [edit protocols oam ethernet connectivity-fault-management action-profile AP_test]
   user@host# set action asynchronous-notification
   ```

4. Defina el dominio de mantenimiento en el nivel de jerarquía [] y especifique los parámetros de asociación de mantenimiento`edit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# set maintenance-domain domain-name level number maintenance-association ma-name
continuity-check interval 1s
```

Por ejemplo

```
user@host# set maintenance-domain md6 level 6 maintenance-association ma6 continuity-check
interval 1s
```

5. Configure la generación de .it si se configura en base a `.interface-status-tlvasynchronous-notificationinterface-status-tlv`

```
[edit protocols oam ethernet connectivity-fault-management] user@host# set maintenance-domain
domain-name level number maintenance-association ma-name
continuity-check interface-status-tlv
```

Por ejemplo

```
user@host# set maintenance-domain md6 level 6 maintenance-association ma6 continuity-check
interface-status-tlv
```

6. Defina el extremo de la asociación de mantenimiento en el nivel de jerarquía [] y especifique los parámetros asociados.`edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name] user@host# set mep mep-id direction up interface interface-
name
```

Por ejemplo

```
user@host# set mep 101 direction up interface ge-0/0/0.0
```

7. Establezca un perfil de acción de notificación asíncrono en el nivel RMEP.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep mep-id ] user@host# set action profile
action profile-name
```

Suponga, por ejemplo,

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md6 maintenance-
association ma6 mep 101 remote-mep 102] user@host# set action-profile AP_test
```

SEE ALSO

No Link Title

Descripción de la supervisión de CFM entre dispositivos CE y PE

in this section

- Caso de uso de multi-homing activo único con bit RDI | **89**
- Multihoming activo/activo Caso de uso con bit RDI | **89**

Puede habilitar la supervisión de la administración de errores de conectividad (CFM) entre los dispositivos perimetrales del proveedor y los dispositivos perimetrales del cliente cuando el dispositivo perimetral del cliente no es un dispositivo de Juniper. Cuando la interfaz no funciona, CFM propaga el estado de la interfaz en los mensajes CC. El mensaje CC informa al dispositivo perimetral del cliente de que el dispositivo perimetral del proveedor no funciona.

Puede configurar la supervisión de CFM mediante cualquiera de las dos opciones siguientes:

- TLV de estado de la interfaz (tipo, longitud y valor): puede habilitar la supervisión de la administración de errores de conectividad (CFM) entre los dispositivos perimetrales del proveedor y los dispositivos perimetrales del cliente cuando el dispositivo perimetral del cliente no es un dispositivo Juniper mediante el TLV de estado de la interfaz. Cuando la interfaz está inactiva, CFM propaga el estado de la interfaz utilizando el TLV de estado de la interfaz. El TLV Estado de la interfaz indica el estado de la interfaz en la que está configurado el MEP que transmite el MCP, o la interfaz siguiente inferior en el IETF RFC 2863 IF-MIB. Por lo tanto, el dispositivo perimetral del cliente es consciente de que el

dispositivo perimetral del proveedor está inactivo. Para configurar la supervisión de CFM mediante el TLV de estado de interfaz, utilice la instrucción en el nivel de jerarquía.`interface-status-tlv`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`maintenance-domain`*`maintenance-association` *`maintenance-association`* `continuity-check` Esta es la opción estándar.

- RDI (indicación remota de defectos): a partir de Junos OS versión 17.3R1, puede habilitar la supervisión de la administración de errores de conectividad (CFM) entre los dispositivos perimetrales del proveedor y los dispositivos perimetrales del cliente cuando el dispositivo perimetral del cliente no es un dispositivo Juniper mediante el bit de indicación remota de defectos (RDI). Cuando se habilita la supervisión de CFM, CFM propaga el estado del dispositivo perimetral del proveedor a través del bit de indicación remota de defectos (RDI) en los mensajes CC. Por lo tanto, el dispositivo perimetral del cliente es consciente de que el dispositivo perimetral del proveedor está inactivo. El bit RDI se borra cuando se realiza una copia de seguridad del servicio. Para configurar la supervisión de CFM mediante el bit RDI, utilice la instrucción en el nivel de jerarquía.`interface-status-send-rdi`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`maintenance-domain`*`maintenance-association` *`maintenance-association`* `continuity-check` Esta opción es necesaria si el dispositivo perimetral del cliente no admite el TLV de estado de interfaz.

> **NOTA**: Cuando la interfaz está establecida en CCC y ha configurado RDI, se envía el bit RDI. CFM no supervisa el estado de la interfaz. Si CCC abajo se establece cuando la interfaz no está en espera, el bit RDI se envía con los mensajes CC si ha configurado RDI.

Caso de uso de multi-homing activo único con bit RDI

Considere la siguiente topología donde hay dos dispositivos perimetrales de proveedor (PE1 y PE2), así como dos dispositivos perimetrales de cliente (CE1 y CE2). PE1 está en estado activo mientras que PE2 está en estado de espera. CFM abajo MEP se configura entre el PE y CE. CFM detecta que el CCC está abajo y debido a que CFM abajo MEP está configurado, los mensajes CC generados tienen el bit RDI. Los mensajes CC de PE2 a CE2 tienen el bit RDI configurado para indicar el estado bloqueado. Cuando PE2 se activa, CCM hacia abajo se borra y el bit RDI se borra de los mensajes CC posteriores.

Multihoming activo/activo Caso de uso con bit RDI

Considere la topología en la que hay dos dispositivos perimetrales de proveedor (PE1 y PE2) y dos dispositivos perimetrales de cliente (CE1 y CE2). PE1 está en estado activo mientras que PE2 está en estado de espera. Si CFM abajo MEP no está configurado entre PE y CE para monitorear la conectividad del vínculo, los mensajes CC generados no tienen el bit RDI. CFM abajo MEP se configura entre el PE y CE. CFM detecta que el CCC está abajo y debido a que CFM abajo MEP está configurado, los mensajes CC generados tienen el bit RDI. Los mensajes CC de PE2 a CE2 tienen el bit RDI configurado para indicar el estado bloqueado. Cuando PE2 se activa, CCM hacia abajo se borra y el bit RDI se borra de los mensajes CC posteriores.

SEE ALSO

interface-status-tlv

interface-status-send-rdi

Configuración de TLV de estado de puerto y TLV de estado de interfaz

in this section

- Descripción general de los TLV | **90**
- Varios TLV para PDU CFM | **91**
- Compatibilidad con TLV opcionales adicionales | **93**
- Defectos de estado MAC | **101**
- Configuración de la compatibilidad con perfiles de acción MEP remotos | **104**
- Supervisión de un perfil de acción de MEP remoto | **105**

Descripción general de los TLV

El tipo, la longitud y el valor (TLV) se describen en el estándar IEEE 802.1ag para CFM como un método de codificación de longitud variable y/o información opcional en una PDU. Los TLV no están alineados con ninguna palabra o límite de octeto en particular. Los TLV se suceden sin relleno entre ellos.

Tabla 1 muestra el formato TLV e indica si es obligatorio u opcional.

Tabla 7: Formato de los TLV

Parámetro	Octeto (secuencia)	Description
Tipo	1	Obligatorio. Si es 0, no le seguirán los campos Length o Value. Si no es 0, al menos el campo Longitud sigue al campo Tipo.
Longitud	2–3	Obligatorio si el campo Tipo no es 0. No está presente si el campo Tipo es 0. Los 16 bits del campo Longitud indican el tamaño, en octetos, del campo Valor. 0 en el campo Longitud indica que no hay ningún campo Valor.

Tabla 7: Formato de los TLV *(Continued)*

Parámetro	Octeto (secuencia)	Description
valor	4	Longitud especificada por el campo Longitud. Opcional. No está presente si el campo Tipo es 0 o si el campo Longitud es 0.

Varios TLV para PDU CFM

Tabla 8 en la página 91 muestra un conjunto de TLV definidos por IEEE 802.1ag para varios tipos de PDU CFM. Cada TLV se puede identificar por el valor único asignado a su campo de tipo. Algunos valores de campo de tipo están reservados.

Tabla 8: Escriba valores de campo para varios TLV para PDU CFM

TLV u organización	Tipo de campo
Finalizar TLV	0
ID de remitente TLV	1
TLV de estado del puerto	2
TLV de datos	3
Estado de la interfaz TLV	4
Respuesta TLV de entrada	5
Respuesta salida TLV	6
Identificador de salida LTM TLV	7
Identificador de salida LTR TLV	8
Reservado para IEEE 802.1	9 a 30

Tabla 8: Escriba valores de campo para varios TLV para PDU CFM *(Continued)*

TLV u organización	Tipo de campo
TLV específico de la organización	31
Definido por el UIT-T Y.1731	32 a 63
Reservado para IEEE 802.1	64 a 255

No todos los TLV son aplicables a todos los tipos de PDU CFM.

- TLV aplicables al mensaje de verificación de continuidad (CCM):
  - Finalizar TLV
  - ID de remitente TLV
  - TLV de estado del puerto
  - Estado de la interfaz TLV
  - TLV específico de la organización
- TLV aplicables para mensajes de circuito cerrado (LBM):
  - Finalizar TLV
  - ID de remitente TLV
  - TLV de datos
  - TLV específico de la organización
- TLV aplicables para la respuesta de circuito cerrado (LBR):
  - Finalizar TLV
  - ID de remitente TLV
  - TLV de datos
  - TLV específico de la organización
- TLV aplicables para mensajes de rastreo de enlaces (LTM):
  - Finalizar TLV

  - Identificador de salida LTM TLV
  - ID de remitente TLV
  - TLV específico de la organización
- TLV aplicables para la respuesta de rastreo de enlaces (LTR):
  - Finalizar TLV
  - Identificador de salida LTR TLV
  - Respuesta TLV de entrada
  - Respuesta salida TLV
  - ID de remitente TLV
  - TLV específico de la organización

Los siguientes TLV son actualmente compatibles con las PDU de CFM aplicables:

- Finalizar TLV
- Respuesta TLV de entrada
- Respuesta salida TLV
- Identificador de salida LTR TLV
- Identificador de salida LTM TLV
- TLV de datos

Compatibilidad con TLV opcionales adicionales

in this section

TLV de estado del puerto | **94**
Estado de la interfaz TLV | **97**

Se admiten los siguientes TLV opcionales adicionales:

- TLV de estado del puerto

- Estado de la interfaz TLV

Los enrutadores de la serie MX admiten la configuración de TLV de estado de puerto y TLV de estado de interfaz. La configuración de la TLV de estado de puerto permite al operador controlar la transmisión de la TLV de estado de puerto en PDU CFM.

> **NOTA**: Aunque las instrucciones de configuración de TLV de estado de puerto están visibles en la CLI en los enrutadores M120 y M320, el TLV de estado de puerto no se puede configurar en estos sistemas. El TLV de estado de puerto solo se puede habilitar en una interfaz MEP si es una interfaz lógica de puente, lo que no es posible en estos sistemas.

Para obtener información de configuración, consulte las secciones siguientes:

TLV de estado del puerto

El TLV de estado del puerto indica la capacidad del puerto puente en el que reside el MEP transmisor para pasar datos ordinarios, independientemente del estado del MAC. El valor de este TLV está controlado por la variable MEP , como se muestra en .`enableRmepDefect`Tabla 10 en la página 94 El formato de este TLV se muestra en .Tabla 9 en la página 94

Cualquier cambio en el valor de los TLV de estado del puerto desencadena una transmisión adicional de los MCPs MEP de los puertos de puente.

Tabla 9: Estado del puerto Formato TLV

Parámetro	Octeto (secuencia)
Tipo = 2	1
Longitud	2–3
Valor (Ver)Tabla 10 en la página 94	4

Tabla 10: Valores TLV de estado del puerto

Mnemónica	Datos ordinarios que pasan libremente por el puerto	valor
psBloqueado	No: `enableRmepDefect` = falso	1

Tabla 10: Valores TLV de estado del puerto *(Continued)*

Mnemónica	Datos ordinarios que pasan libremente por el puerto	valor
psUp	Sí: `enableRmepDefect` = verdadero	2

La variable MEP es una variable booleana que indica si las tramas de la instancia de servicio supervisada por las asociaciones de mantenimiento si esta MEP están habilitadas para pasar a través de este puerto de puente mediante el protocolo de árbol de expansión y la administración de topología de VLAN.`enableRmepDefect` Se establece en TRUE si:

- El puerto del puente se establece en un estado en el que el tráfico puede pasar a través de él.
- El puerto de puente ejecuta varias instancias del árbol de expansión.
- La interfaz MEP no está asociada a un dominio puente.

Configuración de TLV de estado de puerto

Junos OS proporciona compatibilidad de configuración para el TLV de estado del puerto, lo que permite controlar la transmisión de este TLV en PDU CCM. Junos OS proporciona esta configuración en el nivel de comprobación de continuidad. De forma predeterminada, el MCP no incluye el TLV de estado del puerto. Para configurar la TLV de estado del puerto, utilice la instrucción en el nivel de jerarquía.`port-status-tlv`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `continuity-check`]

> **NOTA**: IEEE 802.1ag no exige la configuración del TLV de estado del puerto. Junos OS lo proporciona para dar más flexibilidad al operador; sin embargo, recibe y procesa MCPs con un TLV de estado de puerto, independientemente de esta configuración.

A continuación se muestra un ejemplo de las instrucciones de configuración:

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain identifier {
                level number;
                    maintenance-association identifier {
                        continuity-check {
                            interval number,
```

```
                            loss-threshold number;
                            hold-interval number;
                            port-status-tlv; # Sets Port Status TLV
                        }
                    }
                }
            }
        }
    }
}
```

No puede habilitar la transmisión TLV de estado de puerto en los dos casos siguientes:

- Si la interfaz MEP bajo la asociación de mantenimiento no es de tipo puente.
- Si el MEP está configurado en una interfaz física.

Visualización del TLV de estado del puerto recibido

Junos OS guarda el último TLV de estado de puerto recibido de un MEP remoto. Si el valor Estado de puerto recibido no corresponde a uno de los valores estándar enumerados en , el comando lo muestra como "desconocido".Tabla 10 en la página 94`show` Puede mostrar la última TLV de estado del puerto recibida guardada mediante el comando, como en el siguiente ejemplo:`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `local-mep` *`identifier`* `remote-mep` *`identifier`*

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md5
maintenance-association ma5 local-mep 2001 remote-mep 1001
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
```

```
    Port status TLV: none # RX PORT STATUS
    Interface status TLV: none
```

Visualización del TLV de estado del puerto transmitido

Junos OS guarda el último TLV de estado de puerto transmitido de un MEP local. Si no se ha habilitado la transmisión de la TLV de estado del puerto, el comando muestra "none".`show` Puede mostrar el último TLV de estado del puerto transmitido guardado utilizando el comando, como en el siguiente ejemplo:`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `local-mep` *`identifier`* `remote-mep` *`identifier`*

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md5
maintenance-association ma5 local-mep 2001 remote-mep 1001
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up # TX PORT STATUS
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
```

Estado de la interfaz TLV

El TLV Estado de la interfaz indica el estado de la interfaz en la que está configurado el MEP que transmite el MCP, o la interfaz siguiente inferior en el IETF RFC 2863 IF-MIB. El formato de este TLV se muestra en .Tabla 11 en la página 98 Los valores enumerados se muestran en .Tabla 12 en la página 98

Tabla 11: Estado de la interfaz Formato TLV

Parámetro	Octeto (secuencia)
Tipo = 4	1
Longitud	2–3
Valor (Ver)Tabla 12 en la página 98	4

Tabla 12: Estado de la interfaz Valores TLV

Mnemónica	Estado de la interfaz	valor
Isup	hacia arriba	1
isDown	abajo	2
isTesting	Pruebas	3
esDesconocido	Desconocido	4
isDormant	Inactivo	5
isNotPresent	notPresent	6
isLowerLayerDown	lowerLayerDown	7

NOTA: Cuando el estado operativo de una interfaz lógica cambia del estado abajo (valor de estado de 2) al estado de capa inferior (valor de estado de 7) y viceversa, no se genera la captura SNMP de LinkDown. Por ejemplo, si configura un paquete de interfaz Ethernet agregado con una etiqueta VLAN y agrega al paquete una interfaz física que está en estado operativamente inactivo, el estado operativo del paquete de interfaz lógica Ethernet agregado en ese punto es capa inferior (7). Si desconecta el MIC asociado a la interfaz, la captura LinkDown no se genera cuando la interfaz lógica cambia del estado inferior de capa descendente al estado descendente.

Del mismo modo, considere otro escenario de ejemplo en el que se agrega una interfaz física a un paquete de Ethernet agregado que tiene etiquetado VLAN y la interfaz lógica Ethernet agregada está deshabilitada. Cuando la interfaz lógica está deshabilitada, el estado operativo de la interfaz lógica cambia a inactivo. Si deshabilita la interfaz física que forma parte del paquete Ethernet agregado, el estado operativo de la interfaz lógica Ethernet agregada permanece inactivo. Si vuelve a habilitar la interfaz lógica Ethernet agregada, el estado operativo de la misma cambia de capa inferior a capa inferior. La captura SNMP de LinkDown no se genera en este momento.

Configuración de TLV de estado de interfaz

Junos OS proporciona soporte de configuración para el TLV de estado de interfaz, lo que permite a los operadores controlar la transmisión de este TLV en PDU CCM a través de la configuración a nivel de verificación de continuidad.

NOTA: IEEE 802.1ag no exige esta configuración; más bien se proporciona para dar más flexibilidad al operador. Junos OS recibe y procesa MCPs con el TLV Estado de interfaz, independientemente de esta configuración.

La configuración del TLV de estado de la interfaz se muestra a continuación:

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain identifier {
                    level number;
                    maintenance-association identifier {
                        continuity-check {
                            interval number;
                            loss-threshold number;
                            hold-interval number;
                            interface-status-tlv; # Sets the interface status TLV
                        }
                    }
                }
            }
        }
```

```
    }
}
```

NOTA: Junos OS admite la transmisión de solo tres de los siete valores posibles para el TLV de estado de la interfaz. Los valores admitidos son 1, 2 y 7. Sin embargo, Junos OS es capaz de recibir cualquier valor para el TLV de estado de la interfaz.

Visualización del TLV de estado de interfaz recibido

Junos OS guarda el último TLV de estado de interfaz recibido del MEP remoto. Si el valor de Estado de interfaz recibido no corresponde a uno de los valores estándar enumerados en , el comando muestra "desconocido".Tabla 11 en la página 98`show`

Puede mostrar este último TLV de estado de interfaz guardado usando el comando, como en el siguiente ejemplo:`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `local-mep` *`identifier`* `remote-mep` *`identifier`*

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md5 maintenance-association ma5 local-mep 2001 remote-mep 1001

Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none # displays the Interface Status TLV state
```

Visualización del TLV de estado de la interfaz transmitida

Junos OS guarda el último TLV de estado de interfaz transmitido desde un MEP local. Si no se ha habilitado la transmisión del TLV de estado de la interfaz, el comando muestra "none".`show`

Puede mostrar el último TLV de estado de interfaz transmitido mediante el comando, como en el ejemplo siguiente:`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`identifier`* `maintenance-association` *`identifier`* `local-mep` *`identifier`* `remote-mep` *`identifier`*

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md5
maintenance-association ma5 local-mep 2001 remote-mep 1001

Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 2001, Direction: down, MAC address: 00:19:e2:b2:81:4a
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: ge-2/0/0.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 1001, State: ok
    MAC address: 00:19:e2:b0:74:00, Type: Learned
    Interface: ge-2/0/0.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: none
```

Defectos de estado MAC

Junos OS proporciona información sobre defectos de estado de MAC, lo que indica que uno o más de los MEP remotos informa de un error en su TLV de estado de puerto o TLV de estado de interfaz. Indica "sí" si algún eurodiputado remoto informa que su interfaz no es isUp (por ejemplo, al menos una interfaz de eurodiputados remotos no está disponible), o si todos los eurodiputados remotos informan de un TLV de estado de puerto que contiene algún valor distinto de psUp (por ejemplo, todos los puertos puente de eurodiputados remotos no están reenviando datos). Hay dos comandos que puede utilizar para ver la indicación de defectos de estado de MAC.`show`

Utilice el comando para mostrar los defectos de estado de MAC:`mep-database`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md6
maintenance-association ma6
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 500, Direction: down, MAC address: 00:05:85:73:7b:39
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: up, Port status TLV: up
  Interface name: xe-5/0/0.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM            : no
    Erroneous CCM received                  : no
    Cross-connect CCM received              : no
    RDI sent by some MEP                    : no
    Some remote MEP's MAC in error state    : yes # MAC Status Defects yes/no
  Statistics:
    CCMs sent                               : 1658
    CCMs received out of sequence           : 0
    LBMs sent                               : 0
    Valid in-order LBRs received            : 0
    Valid out-of-order LBRs received        : 0
    LBRs received with corrupted data       : 0
    LBRs sent                               : 0
    LTMs sent                               : 0
    LTMs received                           : 0
    LTRs sent                               : 0
    LTRs received                           : 0
    Sequence number of next LTM request     : 0
    1DMs sent                               : 0
    Valid 1DMs received                     : 0
    Invalid 1DMs received                   : 0
    DMMs sent                               : 0
    DMRs sent                               : 0
    Valid DMRs received                     : 0
    Invalid DMRs received                   : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      200     00:05:85:73:39:4a       ok    xe-5/0/0.0
```

Utilice el comando para mostrar los defectos de estado de MAC:`interfaces`

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
Interface name: xe-5/0/0.0, Interface status: Active, Link status: Up
  Maintenance domain name: md6, Format: string, Level: 6
    Maintenance association name: ma6, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: up, Port status TLV: up
    MEP identifier: 500, Direction: down, MAC address: 00:05:85:73:7b:39
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                  : no
      Erroneous CCM received                        : no
      Cross-connect CCM received                    : no
      RDI sent by some MEP                          : no
      Some remote MEP's MAC in error state          : yes # MAC Status Defects yes/no
    Statistics:
      CCMs sent                                     : 1328
      CCMs received out of sequence                 : 0
      LBMs sent                                     : 0
      Valid in-order LBRs received                  : 0
      Valid out-of-order LBRs received              : 0
      LBRs received with corrupted data             : 0
      LBRs sent                                     : 0
      LTMs sent                                     : 0
      LTMs received                                 : 0
      LTRs sent                                     : 0
      LTRs received                                 : 0
      Sequence number of next LTM request           : 0
      1DMs sent                                     : 0
      Valid 1DMs received                           : 0
      Invalid 1DMs received                         : 0
      DMMs sent                                     : 0
      DMRs sent                                     : 0
      Valid DMRs received                           : 0
      Invalid DMRs received                         : 0
    Remote MEP count: 1
      Identifier    MAC address        State    Interface
        200     00:05:85:73:39:4a       ok    xe-5/0/0.0
```

Configuración de la compatibilidad con perfiles de acción MEP remotos

Según los valores de y en los paquetes CCM recibidos, se puede realizar una acción específica, como , mediante las opciones.`interface-status-tlvport-status-tlvinterface-downaction-profile` Se pueden configurar varios perfiles de acción en el enrutador, pero solo se puede asignar un perfil de acción a un MEP remoto.

El perfil de acción se puede configurar con al menos un evento para desencadenar la acción; Pero la acción se activará si se produce alguno de estos eventos. No es necesario que se produzcan todos los eventos configurados para desencadenar .`action`

Un perfil de acción solo se puede aplicar a nivel de MEP remoto.

En el ejemplo siguiente se muestra una configuración de perfil de acción con comentarios explicativos agregados:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile tlv-action {
    event {
        # If interface status tlv with value specified in the config is received
        interface-status-tlv down|lower-layer-down;

        # If port status tlv with value specified in the config is received
        port-status-tlv blocked;

        # If connectivity is lost to the peer */
        adjacency-loss;
    }
    action {
        # Bring the interface down */
        interface-down;
    }
    default-actions interface-down;
    }

# domains
    maintenance-domain identifier {
        # maintenance domain level (0-7)
        level number;

        # association
        maintenance-association identifier {
            mep identifier {
```

```
                interface ge-x/y/z.w;

                remote-mep identifier {
                    # Apply the action-profile for the remote MEP
                    action-profile tlv-action;
                }
            }
        }
    }
```

Supervisión de un perfil de acción de MEP remoto

Puede utilizar el comando para ver el estado del perfil de acción de un MEP remoto, como en el ejemplo siguiente:`show oam ethernet connectivity-fault-management mep-database`

mostrar conectividad Ethernet OAM gestión de fallos MEP-base de datos remote-mep (evento de perfil de acción)

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain md5
maintenance-association ma5 remote-mep 200
Maintenance domain name: md5, Format: string, Level: 5
  Maintenance association name: ma5, Format: string
  Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
  MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
  Auto-discovery: enabled, Priority: 0
  Interface status TLV: none, Port status TLV: none  # last status TLVs transmitted by the router
  Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up

  Remote MEP identifier: 200, State: ok # displays the remote MEP name and state
    MAC address: 00:05:85:73:96:1f, Type: Configured
    Interface: ge-1/0/8.0
    Last flapped: Never
    Remote defect indication: false
    Port status TLV: none
    Interface status TLV: lower-layer-down
    Action profile: juniper  # displays remote MEP's action profile identifier
      Last event: Interface-status-tlv lower-layer-down  # last remote MEP event
                                                         # to trigger action
      Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)
                              # action occurrence time
```

VÍNCULOS RELACIONADOS

gestión de errores de conectividad

Administración de errores de conectividad OAM IEEE 802.1ag | 22

Configuración del ID de chasis TLV

En la versión 16.1R2 y posteriores, puede configurar Junos OS para enviar el ID de remitente TLV junto con los paquetes. El TLV de ID de remitente es un TLV opcional que se envía en mensajes de comprobación de continuidad (CCM), mensajes de circuito cerrado y mensajes de seguimiento de vínculos (LTM), como se especifica en el estándar IEEE 802.1ag. El TLV del ID de remitente contiene el ID del chasis, que es la dirección MAC única basada en CFM del dispositivo, y la dirección IP de administración, que es una dirección IPv4 o IPv6.

El valor del campo en el TLV indica si el TLV contiene o no la información del ID del chasis.`length` Los valores posibles para el campo son cero () o cualquier número válido, lo que indica la ausencia o presencia de información de ID de chasis en el TLV, respectivamente.`length0`

Puede habilitar Junos OS para que envíe el ID de remitente TLV al nivel global mediante el comando.`set protocols oam ethernet connectivity-fault-management sendid-tlv send-chassis-tlv` Si el TLV del ID de remitente está configurado en el nivel global, el dominio de mantenimiento predeterminado, la asociación de mantenimiento y la mitad de la función de punto intermedio de asociación de mantenimiento (MIP) heredan esta configuración.

También puede configurar el TLV de ID de remitente en los siguientes niveles jerárquicos:

- `[edit protocols oam ethernet connectivity-fault-management]`.
- `[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`maintenance-domain-name`* `maintenance-association` *`maintenance-association-name`* `continuity-check]`.

La configuración de TLV del ID de remitente en el nivel de asociación de mantenimiento tiene prioridad sobre la configuración de nivel global.

NOTA: El TLV de ID de remitente solo es compatible con PDU 802.1ag y no es compatible con unidades de datos de protocolo de supervisión de rendimiento (PDU).

SEE ALSO

Administración de errores de conectividad OAM IEEE 802.1ag | 22

Configuración del procesamiento de mensajes MAC Flush en modo CET

in this section

- Configuración de un perfil de acción TLV de protección de conexión | **109**

En el modo de transporte Ethernet de operadora (CET), los enrutadores de la serie MX se utilizan como enrutadores de borde de proveedor (PE) y, en el lado de acceso, se utilizan conmutadores Ethernet de operadora A2200 de Nokia Siemens Networks (denominados dispositivos de dominio electrónico) que ejecutan protocolos basados en estándares. En los enrutadores de la serie MX, los pseudocables VPLS se configuran dinámicamente mediante el protocolo de distribución de etiquetas (LDP). En los dispositivos de dominio electrónico, los cambios en la topología se detectan mediante sesiones de administración de errores de conectividad (CFM) que se ejecutan entre los dispositivos de dominio electrónico y los enrutadores PE de la serie MX. Los enrutadores PE de la serie MX pueden desactivar la interfaz Ethernet del operador si se produce una pérdida de conectividad CFM. Esto activa un vaciado de MAC local, así como una notificación de vaciado de MAC de protocolo de distribución de etiquetas dirigido (T-LDP) que se envía a los PE remotos de la serie MX para activar el vaciado de MAC en ellos.

En el modo interoperativo CET, los enrutadores de la serie MX deben interoperar con los dispositivos de acceso Ax100 Carrier Ethernet de Nokia Siemens Networks (denominados dispositivos de dominio A) que ejecutan protocolos heredados. Los dispositivos Nokia Siemens Networks A4100 y A8100 actúan como un intermediario entre los enrutadores PE de la serie MX y los dispositivos de dominio A. Estos dispositivos intermedios realizan procedimientos de función de intertrabajo (IWF) para que las sesiones de administración de operaciones (OAM) se puedan ejecutar entre enrutadores de la serie MX y dispositivos de dominio A. No hay pseudocables VPLS entre los enrutadores PE de la serie MX y los dispositivos intermedios A4100 y A8100 de Nokia Siemens Networks, por lo que no hay ningún protocolo LDP ejecutándose entre los enrutadores PE para enviar notificaciones de cambio de topología. Para comunicar los cambios de topología, los enrutadores de la serie MX pueden activar un vaciado de MAC y propagarlo en el núcleo. Los enrutadores de la serie MX pueden usar perfiles de acción basados en el evento de valor de longitud de tipo de protección de conexión (TLV). El perfil de acción desactiva la *interfaz lógica* del borde de la operadora en los enrutadores PE de la serie MX, lo que activará un vaciado de MAC local y también propagará el cambio de topología al núcleo mediante la notificación LDP.

Para VPLS no hay conectividad de extremo a extremo monitoreada. Los anillos de acceso se supervisan de forma independiente mediante la ejecución de CFM en múltiples puntos finales (MEP) en las rutas de trabajo y protección para cada uno de los servicios entre los dispositivos de dominio electrónico y los enrutadores PE de la serie MX, y entre los dispositivos de dominio A y los enrutadores PE de la serie MX, el IWF alojado por los dispositivos A-4100 de Nokia Siemens Networks. Cuando hay un fallo de conectividad en la ruta de trabajo, los dispositivos Nokia Siemens Networks Ax200 realizan un cambio a

la ruta de protección, activando una notificación de cambio de topología (en forma de TLV transportados en CCM) que se enviará en la ruta activa.

Figura 7: Topología de base dual interoperacional CET

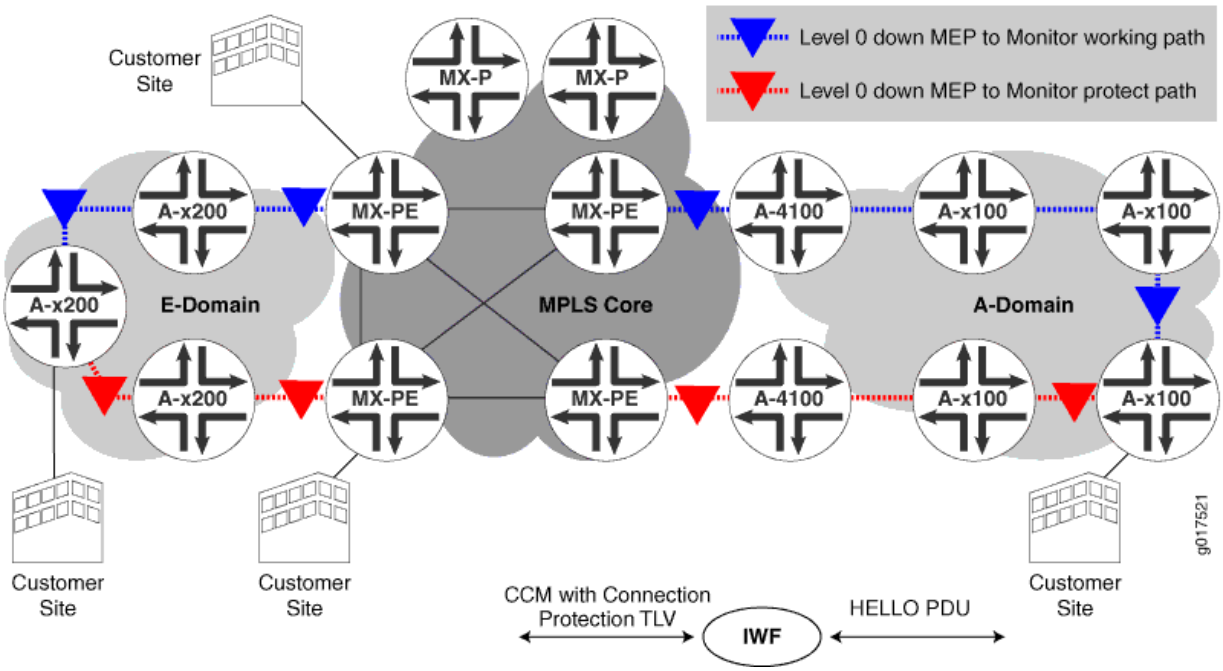


Figura 7 en la página 108 describe la topología de base dual en los enrutadores PE de la serie MX conectados al dominio A. Cuando un dispositivo de dominio A activa un cambio, comienza a cambiar el tráfico de servicio a la nueva ruta activa. Este cambio se comunica en las unidades de datos del protocolo HELLO (PDU) enviadas por ese dispositivo de dominio A en las rutas de trabajo y protección. Cuando el IWF en el A4100 recibe estas PDU HELLO, las convierte en mensajes CCM estándar y también inserta un TLV de protección de conexión. El campo "Protección en uso" de la TLV de protección de conexión está codificado con la ruta actualmente activa y se incluye en el mensaje del MCP. Los mensajes CCM son recibidos por los enrutadores PE de la serie MX a través del radio VLAN en A4100. En el escenario de base dual anterior, un enrutador de PE de la serie MX supervisa la ruta de trabajo y el otro enrutador de PE de la serie MX supervisa la ruta de protección.

Un vaciado de MAC se produce cuando la sesión de CFM que supervisa la ruta de trabajo detecta que el tráfico de servicio se ha movido a la ruta de protección o cuando la sesión de CFM que supervisa la ruta de protección detecta que el tráfico de servicio se ha movido a la ruta de trabajo.

Figura 8: Topología de conexión dual interoperacional CET

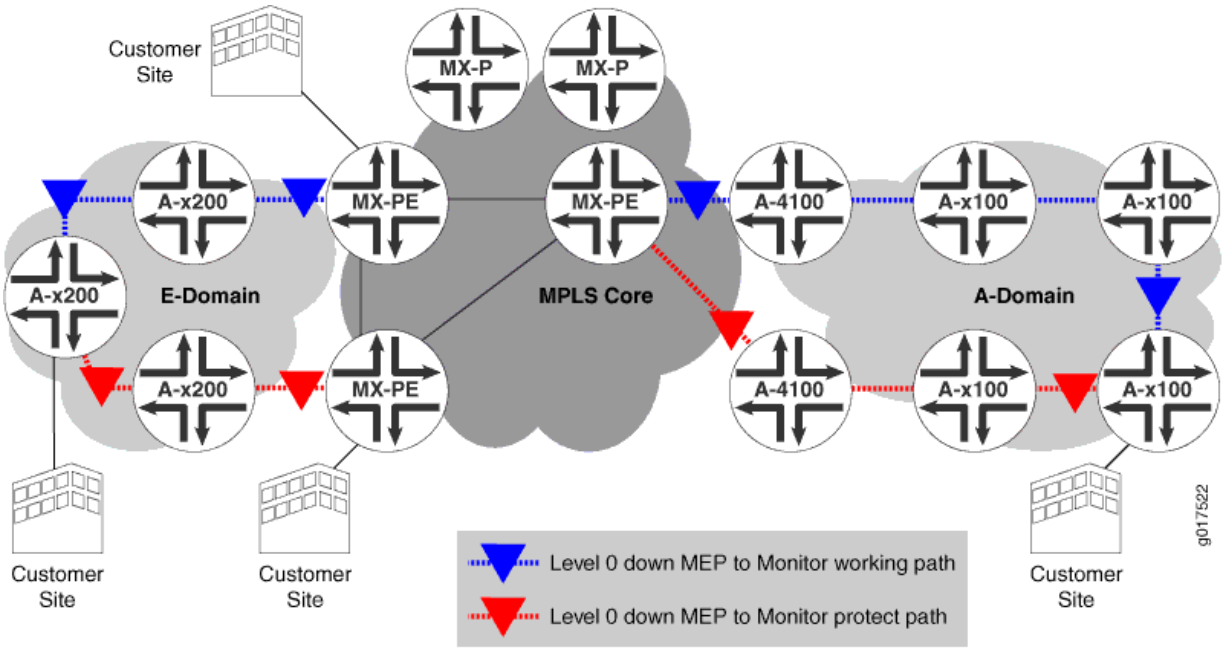


Figura 8 en la página 109 describe la topología de conexión dual en los enrutadores PE de la serie MX conectados al dominio A. El mecanismo de vaciado de MAC utilizado en este caso también es el mismo que el utilizado para el dominio A en el escenario de base dual (Figura 1). Sin embargo, en este caso, ambas sesiones de CFM están alojadas por un solo enrutador PE de la serie MX. Cuando el Ax100 en el dominio A detecta cambios en la topología, el enrutador PE de la serie MX recibe el TLV de protección de conexión en el mensaje CCM para las rutas de trabajo y protección con el valor de "Protección en uso" que indica qué ruta es la activa. Según el evento que se genere para la sesión CFM, el enrutador PE de la serie MX desplegará la interfaz adecuada que activará un vaciado de MAC local.

Configuración de un perfil de acción TLV de protección de conexión

Se puede configurar un perfil de acción para realizar la acción en función de los valores de los paquetes CCM recibidos.`interface-downconnection-protection-tlv`

En el ejemplo siguiente se muestra una configuración de perfil de acción con comentarios explicativos agregados:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
    event {
        # If a connection protection TLV with a “Protection-in-use” value of SET is received */
        connection-protection-tlv <using-protection-path>;
        # If a connection protection TLV with a “Protection-in-use” value of RESET is received */
```

```
        connection-protection-tlv <using-working-path>;
    }
    action {
        # Bring the interface down */
        interface-down;
    }
}
```

SEE ALSO

> *conexión-protección-tlv*
>
> Administración de errores de conectividad OAM IEEE 802.1ag | **22**

Ejemplo: Configuración de un perfil de acción basado en TLV de protección de conexión

in this section

- Requisitos | **110**
- Descripción general y topología | **111**
- Configuración | **112**

En este ejemplo se muestra cómo configurar un perfil de acción basado en la TLV de protección de conexión con el fin de desencadenar vaciados de MAC basados en cambios de topología en una red CET.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 11.2 o posterior
- Un enrutador PE serie MX

Descripción general y topología

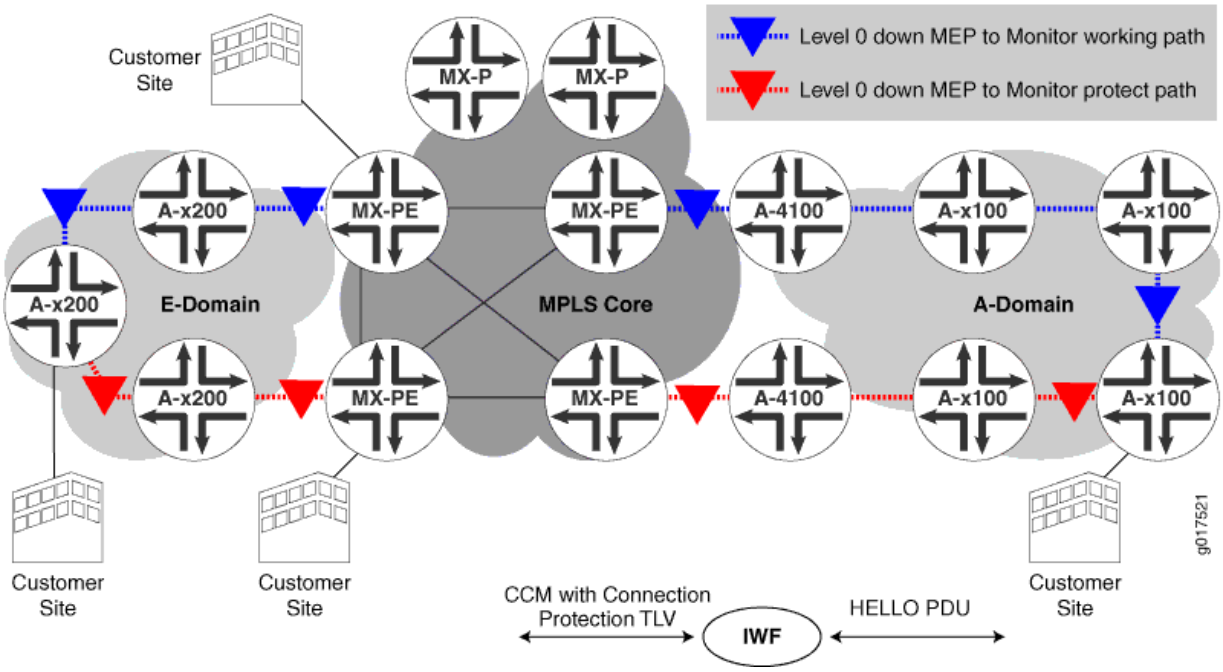
in this section

- Topología | 111

La topología física de una red CET que utiliza enrutadores PE de la serie MX se muestra en Figura 9 en la página 111

Topología

Figura 9: Topología de la red CET



Las siguientes definiciones describen el significado de la abreviatura del dispositivo y los términos utilizados en .Figura 9 en la página 111

- Dispositivo perimetral del proveedor (PE): dispositivo o conjunto de dispositivos en el borde de la red del proveedor que presenta la vista del proveedor del sitio del cliente.
- E-domain—Nokia Siemens Networks Carrier Ethernet Switches que ejecutan protocolos basados en estándares y se utilizan en el lado de acceso.

- Dominio A: conmutadores Ethernet de operadora de Nokia Siemens Networks que ejecutan protocolos heredados.

Configuración

in this section

- Procedimiento | **112**

Procedimiento

Procedimiento paso a paso

Para configurar un perfil de acción basado en el TLV de protección de conexión, realice estas tareas:

1. Configurar un perfil de acción

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
    event {
```

2. Si el TLV de protección de conexión se recibe con un valor de "Protección en uso" de SET, entonces el TLV de protección de conexión debe usar la ruta de protección

```
connection-protection-tlv <using-protection-path>;
```

3. Si el TLV de protección de conexión se recibe con un valor de "Protección en uso" de RESET, entonces el TLV de protección de conexión debe usar la ruta de trabajo

```
connection-protection-tlv <using-working-path>;
}
```

4. Configure el perfil de acción para desactivar la interfaz

```
action {
    /* Bring the interface down */
```

```
    interface-down;
}
}
```

Resultados

Comprobar los resultados de la configuración

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile <tlv-action> {
    event {
        connection-protection-tlv <using-protection-path>;
        connection-protection-tlv <using-working-path>;
    }
    action {
        interface-down;
    }
}
```

SEE ALSO

conexión-protección-tlv

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.3R1	A partir de Junos OS versión 17.3R1, puede habilitar la supervisión de la administración de errores de conectividad (CFM) entre los dispositivos perimetrales del proveedor y los dispositivos perimetrales del cliente cuando el dispositivo perimetral del cliente no es un dispositivo Juniper mediante el bit de indicación remota de defectos (RDI).
16.1	En la versión 16.1R2 y posteriores, puede configurar Junos OS para enviar el ID de remitente TLV junto con los paquetes.

VÍNCULOS RELACIONADOS

Introducción a la administración de errores de conectividad (CFM) de OAM | 20

Visión general de OAM del servicio Ethernet ITU-T Y.1731 | 213

Configurar mensajes de comprobación de continuidad

in this section

- Configurar una conmutación de protección más rápida para topologías de red punto a punto | 114
- Configure una convergencia más rápida para topologías de red multipunto a multipunto de base dual | 116
- Configure un ID de VLAN principal para una mayor flexibilidad | 118
- Configurar una asociación de mantenimiento remoto para aceptar un ID diferente | 119

Junos OS proporciona mejoras para activar una conmutación de protección y convergencia más rápidas en caso de fallos en los dominios de Ethernet para los servicios de Ethernet de operadora. Estas mejoras se pueden utilizar cuando los dispositivos CE del dominio Ethernet detectan fallos de servicio más rápidos y propagan la información en el TLV de estado de interfaz de los mensajes de comprobación de continuidad (CCM). Cuando se reciben MCP, los dispositivos de PE pueden realizar ciertas acciones, lo que facilita una conmutación de protección y convergencia más rápidas. Puede configurar CCM para una mejor escalabilidad mediante la información proporcionada en este tema.

Configurar una conmutación de protección más rápida para topologías de red punto a punto

Puede aplicar un perfil de acción para proporcionar una conmutación de protección más rápida para topologías de red punto a punto con la conmutación local configurada. En un estado normal, las sesiones de CCM se configuran en las interfaces de trabajo y protección. Los paquetes CCM transmitidos contienen un TLV de estado de interfaz con el valor hacia arriba en la interfaz de trabajo y el valor hacia abajo en la interfaz de protección. Cuando se produce un error en un vínculo en la interfaz de trabajo, la interfaz de protección comienza a recibir el TLV de estado de la interfaz como activo. Con la configuración del perfil, si el TLV de estado de interfaz recibido en la interfaz de protección está activo, la interfaz de trabajo se marca automáticamente como .`interface-down`

Para configurar el evento down, incluya la instrucción en el nivel de jerarquía.`interface-status-tlvinterface-status-tlv down`[`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`* `event`]

Para configurarlo como acción del perfil de acción, incluya la instrucción en el nivel jerárquico .`interface-downinterface-down`[`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`* `action`]

Para configurar como acción clara, incluya en el nivel de jerarquía.*peer-interfacepeer-interface*[`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`* `clear-action`]

```
[edit protocols oam]
ethernet  {
    connectivity-fault-management   {
        action-profile p1 {
            event {
                interface-status-tlv down;
            }
            action {
                interface-down;
            }
            clear-action {
                interface-down peer-interface;
            }
        }
    }
}
```

En esta configuración de perfil de acción, cuando el TLV de estado de la interfaz se recibe como arriba, el se marca como inactivo.*peer-interface*

El se configura en la instrucción.*peer-interface*`protect-maintenance-association` Considere el siguiente ejemplo usando la instrucción en la configuración:`protect-maintenance-association`

```
[edit protocols oam]
ethernet  {
    connectivity-fault-management   {
        action-profile p1 {
            event {
                adjacency-loss;
            }
            action {
                interface-down;
            }
            clear-action {
                interface-down peer-interface;
            }
```

```
        }
        maintenance-domain nsn {
            level 5;
            maintenance-association ma1 {
                protect-maintenance-association ma2;
                continuity-check {
                    interval 100ms;
                    connection-protection-tlv;
                }
                mep 100 {
                    interface ge-1/1/0.0;
                    direction down;
                    auto-discovery;
                }
            }
            maintenance-association ma2 {
                continuity-check {
                    interval 100ms;
                    connection-protection-tlv;
            }
            mep 101 {
                    interface ge-1/2/0.0;
                    direction down;
                    auto-discovery;
            }
            remote-mep 100
                action-profile p1;
            }
        }
    }
}
```

SEE ALSO

> *gestión de errores de conectividad*

Configure una convergencia más rápida para topologías de red multipunto a multipunto de base dual

Puede aplicar un perfil de acción para proporcionar una convergencia más rápida para topologías de red multipunto a multipunto de base dual. Si un servicio Ethernet multipunto a multipunto utiliza reenvío

basado en MAC y existen direcciones MAC obsoletas en las tablas de aprendizaje, esto puede dar lugar a agujeros negros de tráfico en la red donde el tráfico entrante se descarta silenciosamente, sin informar a la fuente de que los datos no llegaron a su destinatario. Con la configuración del perfil, si la TLV de estado de la interfaz recibida en la interfaz de protección está activa, la TLV de estado de la interfaz en la interfaz de trabajo se marca como inactiva y el dispositivo PE de la interfaz de protección propaga un mensaje de vaciado de MAC remoto a los dispositivos PE en el servicio de LAN privada virtual (VPLS) mediante TLDP-MAC-FLUSH. El vaciado de MAC evita el filtrado de ruta nula debido a entradas mac-db obsoletas.

Para configurar el evento down, incluya la instrucción en el nivel de jerarquía.`interface-status-tlvinterface-status-tlv down`[`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`* `event`]

Para configurarlo como acción del perfil de acción, incluya la instrucción en el nivel jerárquico .`propagate-remote-flushpropagate-remote-flush`[`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`* `action`]

Para configurar como acción clara, incluya la instrucción en el nivel de jerarquía.`propagate-remote-flushpropagate-remote-flush`[`edit protocols oam ethernet connectivity-fault-management action-profile` *`profile-name`* `clear-action`]

```
[edit protocols oam]
ethernet  {
    connectivity-fault-management   {
        action-profile test {
            event {
                interface-status-tlv down;
            }
            action {
                propagate-remote-mac-flush;
            }
            clear-action {
                propagate-remote-mac-flush;
            }
        }
    }
}
```

En esta configuración de perfil de acción, cuando el paquete CCM entrante contiene el TLV de estado de interfaz con valor abajo, la acción se activa para el perfil de acción.`propagate-remote-mac-flush`

SEE ALSO

> Administración de errores de conectividad OAM IEEE 802.1ag | 22
>
> *gestión de errores de conectividad*

Configure un ID de VLAN principal para una mayor flexibilidad

Puede asignar un ID de LAN virtual (VLAN) principal en la asociación de mantenimiento para una mayor flexibilidad en el número de etiquetas. Cuando se configura un o en una interfaz, el OAM de servicio debe ejecutarse en una de las VLAN.`vlan-rangevlan-id-list` La VLAN asignada para la supervisión del servicio se considera la VLAN principal. Si no se configura a, Junos OS asigna la primera VLAN desde o .`primary-vidvlan-rangevlan-id-list` En versiones anteriores, Junos OS asignaba VLAN 4095.

Para configurar un ID de VLAN principal, puede especificar la instrucción en el nivel de jerarquía:`primary-vid`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`*]

```
[edit protocols oam ethernet connectivity-fault-management]
maintenance domain md3 {
    level 3;
    maintenance-association ma3 {
        primary-vid 2000;
        continuity-check {
            interval 10ms;
            connection-protection-tlv;
        }
        mep 2 {
            interface ge-2/2/0.0;
            direction up;
            auto-discovery;
        }
    }
}
```

SEE ALSO

> Administración de errores de conectividad OAM IEEE 802.1ag | 22
>
> *conexión-protección-tlv*
>
> *gestión de errores de conectividad*

Configurar una asociación de mantenimiento remoto para aceptar un ID diferente

Puede configurar una asociación de mantenimiento para que acepte un identificador de asociación de mantenimiento (ID) diferente de un vecino mediante la inclusión de una instrucción.`remote-maintenance-association` Las sesiones del MCP 802.1ag esperan el mismo identificador de asociación de mantenimiento de sus vecinos. Si hay una discrepancia en el identificador de asociación de mantenimiento, las PDU se marcan como PDU de error. Si se configura una instrucción, se acepta un identificador de asociación de mantenimiento diferente y las sesiones del MCC 802.1ag no marcan las PDU del MCP como PDU de error cuando el nombre de la asociación de mantenimiento es el mismo que el nombre especificado en la instrucción.`remote-maintenance-associationremote-maintenance-association`

Para configurar una asociación de mantenimiento remoto, incluya la instrucción en el nivel de jerarquía:`remote-maintenance-association`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`*]

```
[edit protocols oam ethernet connectivity-fault-management]
maintenance domain md3 {
    level 1;
    maintenance-association ma3 {
        remote-maintenance-association fix-ma;
        continuity-check {
            interval 10ms;
            connection-protection-tlv;
        }
        mep 2 {
            interface ge-2/2/0.0;
            direction up;
            auto-discovery;
        }
    }
}
```

Con esta configuración, se mejora la interoperabilidad de los MCPs con dispositivos CE de gama baja que admiten configuraciones de identificadores de asociación de mantenimiento fijo.

SEE ALSO

Administración de errores de conectividad OAM IEEE 802.1ag | **22**

gestión de errores de conectividad

conexión-protección-tlv

VÍNCULOS RELACIONADOS

Introducción a la administración de errores de conectividad (CFM) de OAM | 20

Configurar la administración de errores de conectividad (CFM) | 28

Ejemplo: Configurar Ethernet CFM en interfaces físicas

in this section

- Requisitos | 120
- Descripción general | 120
- Configuración | 121

En este ejemplo se muestra la configuración de la administración de errores de conectividad Ethernet (CFM) en interfaces físicas.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 9.3 o posterior.

Descripción general

CFM se puede utilizar para supervisar el vínculo físico entre dos enrutadores. Esta funcionalidad es similar a la admitida por el protocolo IEEE 802.3ah LFM.

En Junos OS versión 9.3 y posteriores, CFM también admite interfaces Ethernet agregadas. En las interfaces configuradas en concentradores de puertos modulares (MPC) y tarjetas de interfaz modular (MIC) en enrutadores de la serie MX, CFM no se admite en vínculos de miembro Ethernet agregados sin etiquetar. Las MPC y las MIC admiten CFM en interfaces lógicas Ethernet agregadas sin etiquetar y etiquetadas.

NOTA: Las configuraciones de este ejemplo son solo ejemplos parciales de configuraciones de enrutador completas y funcionales. No copie estas configuraciones y utilícelas directamente en un sistema real.

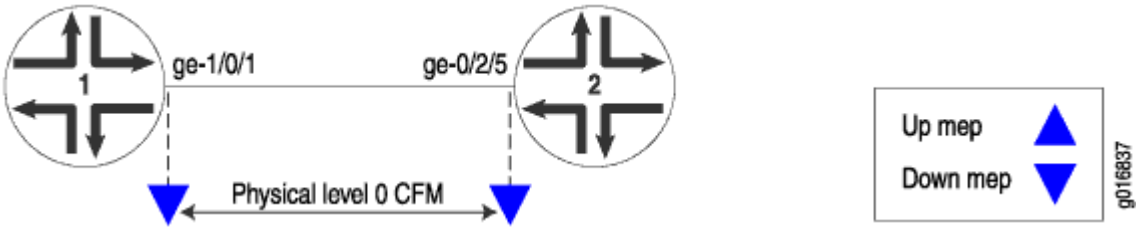
Configuración

in this section

- Configuración rápida de CLI | 121

En el ejemplo siguiente, dos enrutadores (enrutador 1 y enrutador 2) están conectados por un vínculo Gigabit Ethernet punto a punto. El vínculo entre estos dos enrutadores se supervisa mediante CFM. Esto se muestra en Figura 10 en la página 121. El límite único es un "MEP abajo" en la terminología de CFM.

Figura 10: CFM de Ethernet en interfaces físicas



Para configurar Ethernet CFM en interfaces físicas, realice estas tareas:

Configuración rápida de CLI

Enrutador 1

Configure la interfaz y CFM:

```
[edit]
interfaces ge-1/0/1 {
    unit 0 {
        family inet;
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
```

```
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 100 {
                            interface ge-1/0/1;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

La configuración del enrutador 2 refleja la del enrutador 1, con la excepción del archivo *.mep-id*

Enrutador 2

Configure la interfaz y CFM:

```
[edit]
interfaces ge-0/2/5 {
    unit 0 {
        family inet;
    }
}

protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 200 {
                            interface ge-0/2/5;
                            direction down;
```

```
                        auto-discovery;
                    }
                }
            }
        }
    }
    }
}
```

Para comprobar que la interfaz física está configurada correctamente para CFM, utilice el comando.`show interface` Para verificar la configuración de CFM, utilice uno o varios de los comandos enumerados en el Explorador de CLI.`show oam ethernet connectivity-fault-management`https://www.juniper.net/documentation/content-applications/cli-explorer/junos/

VÍNCULOS RELACIONADOS

Mostrar interfaces de administración de fallos de conectividad Ethernet de OAM

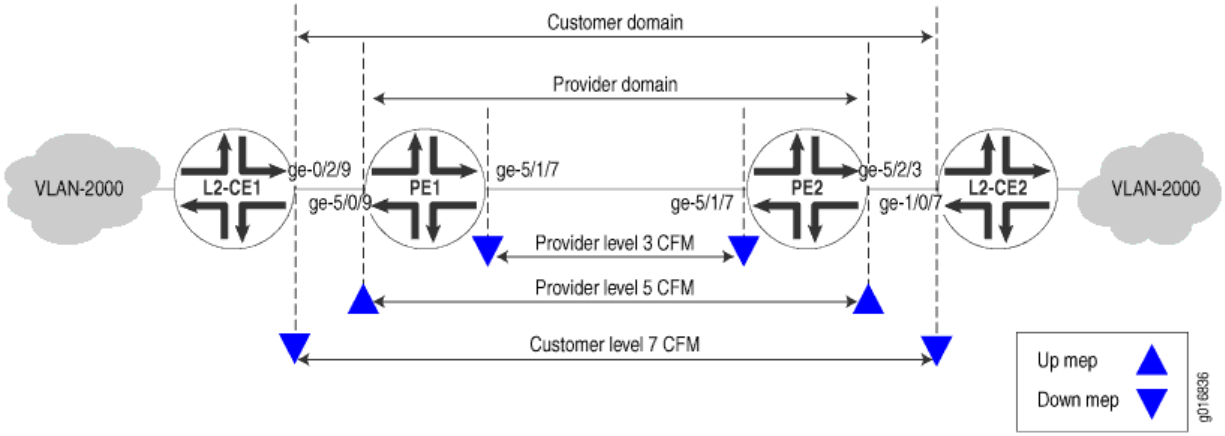
Ejemplo: Configurar Ethernet CFM en conexiones de puente

En este ejemplo, tanto el cliente como el proveedor de servicios ejecutan Ethernet CFM a través de una red de puente simple. La red se muestra en Figura 11 en la página 124. El cliente ha configurado Ethernet CFM en los enrutadores de la serie MX L2-CE1 y L2-CE2. El proveedor de servicios ha configurado Ethernet CFM en los enrutadores de la serie MX PE1 y PE2.

NOTA: Las configuraciones de este ejemplo son solo ejemplos parciales de configuraciones de enrutador completas y funcionales. No copie estas configuraciones y utilícelas directamente en un sistema real.

El proveedor de servicios utiliza CFM nivel 3 para el vínculo entre PE1 y PE2 y el nivel 5 de un puerto orientado hacia CE al otro. El cliente está utilizando CFM nivel 7. Los límites están marcados con la terminología CFM "up mep" y "down mep" en la figura.

Figura 11: CFM de Ethernet a través de una red de puente



Estas son las configuraciones de CFM en los enrutadores del cliente.

CFM en L2-CE1

```
[edit interfaces]
ge-0/2/9 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}

[edit protocols oam ethernet]
connectivity-fault-management {
    maintenance-domain customer {
        level 7;
        maintenance-association customer-site1 {
            continuity-check {
                interval 1s;
            }
            mep 700 {
                interface ge-0/2/9.0;
                direction down;
                auto-discovery;
            }
        }
    }
}
```

CFM en L2-CE2

```
[edit interfaces]
ge-1/0/7 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}

[edit protocols oam ethernet]
connectivity-fault-management {
    maintenance-domain customer {
        level 7;
        maintenance-association customer-site2 {
            continuity-check {
                interval 1s;
            }
            mep 800 {
                interface ge-1/0/7.0;
                direction down;
                auto-discovery;
            }
        }
    }
}
```

Estas son las configuraciones de CFM en los enrutadores del proveedor.

CFM en PE1

```
[edit interfaces]
ge-5/0/9 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}
ge-5/1/7 {
    vlan-tagging;
```

```
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}

[edit bridge-domains]
bridge-vlan2000 {
    domain-type bridge;
    vlan-id 2000;
    interface ge-5/0/9.0;
    interface ge-5/1/7.0;
}

[edit protocols oam ethernet connectivity-fault-management]
maintenance-domain provider-outer {
    level 5;
    maintenance-association provider-outer-site1 {
        continuity-check {
            interval 1s;
        }
        mep 200 {
            interface ge-5/0/9.0;
            direction up;
            auto-discovery;
        }
    }
}
maintenance-domain provider-inner {
    level 3;
    maintenance-association provider-inner-site1 {
        continuity-check {
            interval 1s;
        }
        mep 200 {
            interface ge-5/1/7.0;
            direction down;
            auto-discovery;
        }
    }
}
```

CFM en PE2

```
[edit interfaces]
ge-5/1/7 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}
ge-5/2/3 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 2000;
    }
}

[edit bridge-domains]
bridge-vlan2000 {
    domain-type bridge;
    interface ge-5/2/3.0;
    interface ge-5/1/7.0;
}

[edit protocols oam ethernet connectivity-fault-management]
maintenance-domain provider-outer {
    level 5;
    maintenance-association provider-outer-site1 {
        continuity-check {
            interval 1s;
        }
        mep 100 {
            interface ge-5/2/3.0;
            direction up;
            auto-discovery;
        }
    }
}
maintenance-domain provider-inner {
```

```
    level 3;
    maintenance-association provider-inner-site1 {
        continuity-check {
            interval 1s;
        }
        mep 100 {
            interface ge-5/1/7.0;
            direction down;
            auto-discovery;
        }
    }
}
```

VÍNCULOS RELACIONADOS

Configurar mensajes de comprobación de continuidad | 114

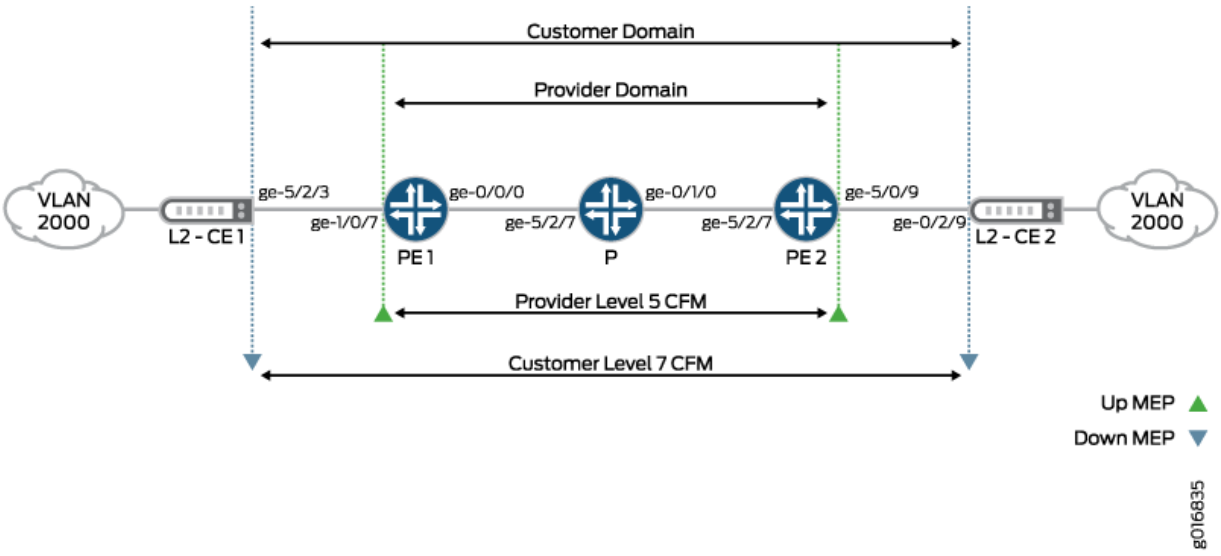
Ejemplo: Configurar Ethernet CFM a través de VPLS

En este ejemplo, tanto el cliente como el proveedor de servicios ejecutan CFM Ethernet a través de una red VPLS y de conmutación de etiquetas multiprotocolo (MPLS). La red se muestra en Figura 12 en la página 129. El cliente ha configurado Ethernet CFM en los enrutadores de la serie MX L2-CE1 y L2-CE2. El proveedor de servicios ha configurado Ethernet CFM en los enrutadores de la serie MX PE1, P y PE2.

> **NOTA**: Las configuraciones de este ejemplo son solo ejemplos parciales de configuraciones de enrutador completas y funcionales. No copie estas configuraciones y utilícelas directamente en un sistema real.

El proveedor de servicios utiliza CFM nivel 5 y el cliente está utilizando CFM nivel 7. Los límites están marcados con la terminología CFM "up mep" y "down mep" en la figura.

Figura 12: Ethernet OAM con VPLS



NOTA: Las interfaces lógicas de una instancia de enrutamiento VPLS pueden tener la misma configuración de VLAN o diferentes. Se requiere la normalización de VLAN para conmutar paquetes correctamente entre estas interfaces. La normalización admite la asignación automática de VLAN y realiza operaciones en etiquetas VLAN para lograr la traducción deseada. Consulte Configuración de una VLAN normalizada para traducción o etiquetado.

NOTA: Se deben tener en cuenta las siguientes consideraciones de ruta de reenvío:

- Ruta de recepción de paquetes:
  - Esta es la ruta de reenvío para los paquetes recibidos en las interfaces.
  - Ethernet OAM 802.1ag para VPLS utiliza filtros de interfaz implícitos y filtros de tabla de reenvío para inundar, aceptar y eliminar los paquetes CFM.
- Ruta de transmisión de paquetes:
  - Junos OS utiliza el reenvío basado en hardware del enrutador para los paquetes generados por la CPU.

- En el caso de los MEPs inactivos, los paquetes se transmiten en la interfaz en la que está configurado el MEP.
- En los enrutadores de la serie MX, para los MEPs, los paquetes deben inundarse a otras interfaces en la instancia de enrutamiento VPLS. El enrutador crea una ruta de inundación vinculada a un próximo salto de inundación (con todas las interfaces para inundar) y luego obtiene los paquetes que se reenviarán con esta ruta de inundación.

A continuación, se muestran las configuraciones de VPLS y CFM en los enrutadores del proveedor de servicios.

Configuración de PE1

```
[edit chassis]
fpc 5 {
    pic 0 {
        tunnel-services {
            bandwidth 1g;
        }
    }
}

[edit interfaces]
ge-1/0/7 {
    encapsulation flexible-ethernet-services;
    vlan-tagging;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 2000;
    }
}
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.200.1.1/24;
        }
        family mpls;
    }
}
lo0 {
    unit 0 {
```

```
        family inet {
            address 10.255.168.231/32 {
                primary;
            }
            address 127.0.0.1/32;
        }
    }
}

[edit routing-instances]
vpls-vlan2000 {
    instance-type vpls;
    vlan-id 2000;
    interface ge-1/0/7.1;
    route-distinguisher 10.255.168.231:2000;
    vrf-target target:1000:1;
    protocols {
        vpls {
            site-range 10;
            site vlan2000-PE1 {
                site-identifier 2;
            }
        }
    }
}

[edit protocols]
rsvp {
    interface ge-0/0/0.0;
}
mpls {
    label-switched-path PE1-to-PE2 {
        to 10.100.1.1;
    }
    interface ge-0/0/0.0;
}
bgp {
    group PE1-to-PE2 {
        type internal;
        local-address 10.200.1.1;
        family l2vpn {
            signaling;
        }
```

```
        local-as 65000;
        neighbor 10.100.1.1;
    }
}
ospf {
    traffic-engineering;
    reference-bandwidth 4g;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
        interface ge-0/0/0.0;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain customer-site1 {
                level 5;
                maintenance-association customer-site1 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 100 {
                        interface ge-1/0/7.1;
                        direction up;
                        auto-discovery;
                    }
                }
            }
        }
    }
}
```

Configuración de PE2

```
[edit chassis]
fpc 5 {
    pic 0 {
        tunnel-services {
            bandwidth 1g;
```

```
        }
    }
}

[edit interfaces]
ge-5/0/9 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
        encapsulation vlan-vpls;
        vlan-id 2000;
    }
}
ge-5/2/7 {
    unit 0 {
        family inet {
            address 10.100.1.1/24;
        }
        family mpls;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.255.168.230/32 {
                primary;
            }
            address 127.0.0.1/32;
        }
    }
}

[edit routing-instances]
vpls-vlan2000 {
    instance-type vpls;
    vlan-id 2000;
    interface ge-5/0/9.1;
    route-distinguisher 10.255.168.230:2000;
    vrf-target target:1000:1;
    protocols {
        vpls {
            site-range 10;
            site vlan2000-PE2 {
```

```
                site-identifier 1;
            }
        }
    }
}

[edit protocols]
rsvp {
    interface ge-5/2/7.0;
}
mpls {
    label-switched-path PE2-to-PE1 {
        to 10.200.1.1;
    }
    interface ge-5/2/7.0;
}
bgp {
    group PE2-to-PE1 {
        type internal;
        local-address 10.100.1.1;
        family l2vpn {
            signaling;
        }
        local-as 65000;
        neighbor 10.200.1.1;
    }
}
ospf {
    traffic-engineering;
    reference-bandwidth 4g;
    area 0.0.0.0 {
        interface all;
        interface fxp0.0 {
            disable;
        }
        interface ge-5/2/7.0;
    }
}
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain customer-site1 {
                level 5;
```

```
                maintenance-association customer-site1 {
                    continuity-check {
                        interval 1s;
                    }
                    mep 200 {
                        interface ge-5/0/9.1;
                        direction up;
                        auto-discovery;
                    }
                }
            }
        }
    }
}
```

Configuración del enrutador P

Solo MPLS, no se necesita CFM:

```
[edit]
interfaces {
    ge-5/2/7 {
        # Connected to PE1
        unit 0 {
            family inet {
                address 10.200.1.10/24;
            }
            family mpls;
        }
    }
    ge-0/1/0 {
        # Connected to PE2
        unit 0 {
            family inet {
                address 10.100.1.10/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0{
            family inet {
```

```
                address 10.255.168.240/32;
            }
        }
    }
}

[edit]
protocols {
    rsvp {
        interface ge-0/1/0.0;
        interface ge-5/2/7.0;
    }
    mpls {
        interface ge-0/1/0.0;
        interface ge-5/2/7.0;
    }
    ospf {
        traffic-engineering;
        reference-bandwidth 4g;
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
            interface ge-0/1/0.0;
            interface ge-5/2/7.0;
        }
    }
}
```

CFM en L2-CE1

Esta es la configuración de CFM en L2-E1:

```
[edit interfaces]
ge-5/2/3 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}
```

```
[edit protocols oam]
ethernet {
    connectivity-fault-management {
        maintenance-domain customer {
            level 7;
            maintenance-association customer-site1 {
                continuity-check {
                    interval 1s;
                }
                mep 800 {
                    interface ge-5/2/3.0;
                    direction down;
                    auto-discovery;
                }
            }
        }
    }
}
```

CFM en L2-CE2

Esta es la configuración de CFM L2-CE2:

```
[edit interfaces]
ge-0/2/9 {
    vlan-tagging;
    unit 0 {
        vlan-id 2000;
    }
}

[edit protocols oam]
ethernet {
    connectivity-fault-management {
        maintenance-domain customer {
            level 7;
            maintenance-association customer-site1 {
                continuity-check {
                    interval 1s;
                }
                mep 700 {
                    interface ge-0/2/9.0;
```

```
                    direction down;
                    auto-discovery;
                }
            }
        }
    }
}
```

VÍNCULOS RELACIONADOS

Configurar mensajes de comprobación de continuidad | 114

chapter label in part2

Administración de fallos de vínculo para enrutadores

in this chapter

- Introducción a la gestión de fallos de vínculo OAM (LFM) | 139
- Configurar la administración de errores de vínculo | 144
- Detección remota de fallos para la gestión de fallos de vínculo | 163
- Circuito cerrado remoto para administración de fallas de vínculo | 165

Introducción a la gestión de fallos de vínculo OAM (LFM)

summary

En esta sección se describe la operación, administración y administración (OAM) de la administración de errores de vínculo (LFM).

in this section

- Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | 139
- Descripción de la administración de fallas de vínculo OAM Ethernet para enrutadores de la serie ACX | 140
- Configuración de Ethernet 802.3ah OAM | 142

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah

Las interfaces Ethernet capaces de ejecutarse a 100 Mbps o más rápido en conmutadores serie EX, PTX, MX, M (excepto enrutadores M5 y M10) y enrutadores serie T admiten el estándar IEEE 802.3ah para operación, administración y gestión (OAM). Puede configurar IEEE 802.3ah OAM en vínculos directos punto a punto Ethernet o vínculos a través de repetidores Ethernet. El estándar IEEE 802.3ah cumple con los requisitos de capacidades OAM a medida que Ethernet pasa de ser únicamente una tecnología empresarial a ser una WAN y una tecnología de acceso, además de ser compatible con la tecnología Ethernet existente. Junos OS admite la administración de errores de vínculo IEEE 802.3ah.

Las características de la administración de fallas de vínculo son:

- Discovery
- Monitoreo de enlaces
- Detección remota de fallos
- Circuito cerrado remoto

A partir de Junos OS versión 17.3R1, el demonio de administración de errores de vínculo Ethernet (lfmd) se ejecuta en el motor de enrutamiento de reserva también cuando se configura un cambio correcto del motor de enrutamiento (GRES).

No se admiten las siguientes características:

- Ethernet que se ejecuta sobre un protocolo de capa 2, como Ethernet a través de ATM, no se admite en las configuraciones de OAM.
- El circuito cerrado remoto no es compatible con la PIC de LAN/WAN de 10 Gigabit Ethernet con SFP +.
- La función de circuito cerrado remoto mencionada en la sección 57.2.11 de IEEE 802.3ah no es compatible con los enrutadores T4000.

NOTA: Los vínculos de miembro de Ethernet agregados ahora usarán la dirección MAC física como dirección MAC de origen en los paquetes OAM de 802.3ah.

Descripción de la administración de fallas de vínculo OAM Ethernet para enrutadores de la serie ACX

El sistema operativo Junos de Juniper Networks (Junos OS) para enrutadores de la serie ACX de Juniper Networks permite que las interfaces Ethernet de estos enrutadores admitan el estándar IEEE 802.3ah para la operación, administración y mantenimiento (OAM) de Ethernet en redes de acceso. El estándar define la administración de fallas de vínculo OAM (LFM). Puede configurar IEEE 802.3ah OAM LFM en vínculos Ethernet punto a punto que estén conectados directamente o a través de repetidores Ethernet. El estándar IEEE 802.3ah cumple con los requisitos de capacidades OAM, incluso cuando Ethernet pasa de ser únicamente una tecnología empresarial a una WAN y tecnología de acceso, y el estándar sigue siendo compatible con la tecnología Ethernet existente.

Ethernet OAM proporciona herramientas que el software de administración de red y los administradores de red pueden utilizar para determinar cómo funciona una red de vínculos Ethernet. Ethernet OAM debe:

- Confíe únicamente en la dirección MAC (Media Access Control) o en el identificador de LAN virtual para la solución de problemas.
- Trabaje independientemente del transporte y función Ethernet real a través de puertos Ethernet físicos o un servicio virtual como un pseudocable.
- Aísle los fallos en una arquitectura de red plana (o de un solo operador) o en redes anidadas, jerárquicas (o de múltiples proveedores).

Las siguientes funciones de LFM de OAM son compatibles con los enrutadores de la serie ACX:

- Descubrimiento y monitoreo de enlaces

  El proceso de descubrimiento se activa automáticamente cuando OAM está habilitado en la interfaz. El proceso de descubrimiento permite que las interfaces Ethernet descubran y supervisen el par en el vínculo si también es compatible con el estándar IEEE 802.3ah. Puede especificar el modo de detección utilizado para la compatibilidad con IEEE 802.3ah OAM. En el modo activo, la interfaz descubre y supervisa el par en el vínculo si el par también admite la funcionalidad OAM IEEE 802.3ah. En el modo pasivo, el par inicia el proceso de detección. Después de que se ha iniciado el proceso de descubrimiento, ambas partes participan en el proceso. El enrutador realiza la supervisión de vínculos mediante el envío periódico de unidades de datos de protocolo OAM (PDU) para anunciar el modo, la configuración y las capacidades de OAM.

  Puede especificar el número de PDU de OAM que una interfaz puede omitir antes de que el vínculo entre pares se considere inactivo.

- Detección remota de fallos

  La detección remota de fallos utiliza indicadores y eventos. Las banderas se utilizan para transmitir lo siguiente:

  - **Link Fault** significa una pérdida de señal
  - **Dying Gasp** significa una condición irrecuperable, como un corte de energía. En esta condición, el par local informa al par remoto sobre el estado de error. Cuando el par remoto recibe una PDU que muere, realiza una acción correspondiente al perfil de acción configurado con el evento.**link-adjacency-loss**

    > **NOTA**: ACX5096 y ACX5048 enrutadores no admiten morir sin aliento.

    Cuando LFM se configura en una interfaz, se genera una PDU de muerte para la interfaz en las siguientes condiciones de error:

    - Falla de energía
    - Pánico o bloqueo del motor de reenvío de paquetes

- **Critical Event** significa un evento crítico específico del proveedor no especificado.

Puede especificar el intervalo en el que se envían las PDU OAM para la detección de errores.

> **NOTA**: Los enrutadores de la serie ACX admiten la recepción de paquetes que mueren, pero no pueden generarlos.

- Modo de circuito cerrado remoto

  El modo de circuito cerrado remoto garantiza la calidad del vínculo entre el enrutador y un par remoto durante la instalación o la solución de problemas. En este modo, cuando la interfaz recibe una trama que no es una PDU OAM o una trama de pausa, lo envía de vuelta a la misma interfaz en la que se recibió. El vínculo parece estar en el estado activo. Puede usar la confirmación de circuito cerrado devuelta para probar el retraso, la fluctuación y el rendimiento.

  Si un equipo terminal de datos remoto (DTE) admite el modo de circuito cerrado remoto, Junos OS puede colocar el DTE remoto en modo de circuito cerrado. Cuando coloca un DTE remoto en modo de circuito cerrado, la interfaz recibe la solicitud de bucle cerrado remoto y pone la interfaz en modo de circuito cerrado remoto. Cuando la interfaz está en modo de circuito cerrado remoto, todas las tramas, excepto las PDU OAM y las tramas de pausa, se vuelven a bucle. No se realizan cambios en los marcos. Las PDU OAM se siguen enviando y procesando.

Configuración de Ethernet 802.3ah OAM

El estándar IEEE 802.3ah para operación, administración y gestión (OAM) proporciona una especificación para *la conectividad Ethernet en la primera milla (EFM).* EFM define cómo se puede transmitir Ethernet a través de nuevos tipos de medios mediante nuevas interfaces de capa física Ethernet (PHY). Puede configurar IEEE 802.3ah OAM en vínculos directos punto a punto Ethernet o vínculos a través de repetidores Ethernet. El estándar OAM IEEE 802.3ah cumple con los requisitos de capacidades OAM a medida que Ethernet pasa de ser únicamente una tecnología empresarial a ser una WAN y una tecnología de acceso, además de ser compatible con la tecnología Ethernet existente.

Para las interfaces Ethernet capaces de funcionar a 100 Mbps o más, el estándar IEEE 802.3ah OAM es compatible con numerosos enrutadores y conmutadores de Juniper Networks. En este tema se describe la compatibilidad con la configuración de las funciones OAM de IEEE 802.3ah en enrutadores.

A partir de Junos OS versión 12.1, los enrutadores serie PTX admiten las siguientes características de OAM IEEE 802.3ah en el nivel de interfaz física:

- Descubrimiento y monitoreo de enlaces
- Señalización y detección de fallos
- Procesamiento de administración periódica de paquetes (PPM)

- Compatibilidad con perfiles de acción
- Conmutación del motor de enrutamiento elegante (GRES)

Para configurar la compatibilidad con OAM 802.3ah para interfaces Ethernet, incluya la instrucción en el nivel de jerarquía:`oam[edit protocols]`

```
oam {
    ethernet {
        link-fault-management {
            interfaces {
                interface-name {
                    pdu-interval interval;
                    link-discovery (active | passive);
                    pdu-threshold count;
                }
            }
        }
    }
}
```

Puede configurar valores de umbral para eventos de error que desencadenan el envío de TLV de eventos de vínculo cuando los valores superan el umbral. Para establecer valores de umbral para eventos de error en una interfaz, incluya la instrucción en el nivel de jerarquía.`event-thresholds[edit protocols oam ethernet link-fault-management interface]`

También puede configurar valores de umbral de OAM dentro de un perfil de acción y aplicar el perfil de acción a varias interfaces. Para crear un perfil de acción, incluya la instrucción en el nivel jerárquico .`action-profile[edit protocols oam ethernet link-fault-management]`

Puede configurar Ethernet OAM en una interfaz agregada o en cada uno de sus vínculos miembro. Sin embargo, se recomienda configurar Ethernet OAM en la interfaz agregada, lo que habilitará internamente Ethernet OAM en los vínculos de miembro.

Para ver estadísticas de OAM, utilice el comando del modo operativo.`show oam ethernet link-fault-management` Para borrar las estadísticas de OAM, utilice el comando de modo operativo.`clear oam ethernet link-fault-management statistics` Para borrar la información del estado de administración de errores de vínculo y reiniciar el proceso de descubrimiento de vínculos en interfaces Ethernet, utilice el comando de modo operativo.`clear oam ethernet link-fault-management state` Para obtener más información acerca de estos comandos, consulte el Explorador de CLI.https://www.juniper.net/documentation/content-applications/cli-explorer/junos/

Para habilitar la compatibilidad con OAM IEEE 802.3ah, incluya la instrucción en el nivel jerárquico :`interface[edit protocols oam ethernet link-fault-management]`

```
[edit protocols oam ethernet link-fault-management interface interface-name]
```

Cuando habilita IEEE 802.3ah OAM en una interfaz física, el proceso de descubrimiento se activa automáticamente.

SEE ALSO

> *Umbrales de eventos*
>
> *perfil de acción*

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.3R1	A partir de Junos OS versión 17.3R1, el demonio de administración de errores de vínculo Ethernet (lfmd) se ejecuta en el motor de enrutamiento de reserva también cuando se configura un cambio correcto del motor de enrutamiento (GRES).

Configurar la administración de errores de vínculo

in this section

- Configuración de la detección de vínculos | **145**
- Configuración del intervalo de PDU de OAM | **146**
- Configuración del umbral de PDU de OAM | **146**
- Configuración de valores de umbral para eventos de error local en una interfaz | **147**
- Deshabilitar el envío de TLV de eventos de vínculo | **147**
- Ejemplo: Configuración de la compatibilidad con OAM IEEE 802.3ah en una interfaz | **148**
- Ejemplo: Configuración de la compatibilidad con OAM IEEE 802.3ah para una interfaz de la serie ACX | **149**

- Ejemplo: Configuración de Ethernet LFM entre el borde del proveedor y el borde del cliente | 152
- Ejemplo: Configuración de Ethernet LFM para CCC | 154
- Ejemplo: Configuración de Ethernet LFM para Ethernet agregada | 155
- Configuración de un perfil de acción de OAM | 158
- Especificación de las acciones que deben realizarse para los eventos de administración de errores de vínculo | 159
- Monitoreo de la pérdida de adyacencia del enlace | 160
- Estado del protocolo de supervisión | 161
- Configuración de valores de umbral para eventos de error en un perfil de acción | 162
- Aplicación de un perfil de acción | 162

Use este tema para comprender cómo configurar las funciones de administración de errores de vínculo en su dispositivo. También puede utilizar este tema para configurar un perfil de acción a fin de especificar la acción LFM que debe realizarse cuando se produce un evento LFM específico y aplicar el perfil de acción.

A partir de la versión 22.4R1 de Junos OS Evolved, el proceso de administración de errores de vínculo Ethernet (lfmd) solo se ejecuta cuando el protocolo está configurado.`link-fault-management`

Configuración de la detección de vínculos

Cuando el protocolo OAM IEEE 802.3ah está habilitado en una interfaz física, el proceso de descubrimiento se activa automáticamente. El proceso de descubrimiento permite que las interfaces Ethernet descubran y supervisen el par en el vínculo si también es compatible con el estándar IEEE 802.3ah.

Puede especificar el modo de detección utilizado para la compatibilidad con IEEE 802.3ah OAM. El proceso de descubrimiento se activa automáticamente cuando la funcionalidad OAM IEEE 802.3ah está habilitada en un puerto. La supervisión de vínculos se realiza cuando la interfaz envía PDU OAM periódicas.

Para configurar el modo de detección, incluya la instrucción en el nivel de jerarquía:`link-discovery`[`edit protocol oam ethernet link-fault-management interface` *`interface-name`*]

```
[edit protocol oam ethernet link-fault-management interface interface-name]
link-discovery (active | passive);
```

En el modo activo, la interfaz descubre y supervisa el par en el vínculo si el par también admite la funcionalidad OAM IEEE 802.3ah. En el modo pasivo, el par inicia el proceso de detección. Después de que se ha iniciado el proceso de descubrimiento, ambas partes participan en el descubrimiento.

SEE ALSO

> *descubrimiento de enlaces*

Configuración del intervalo de PDU de OAM

Se envían PDU OAM periódicas para realizar el monitoreo de vínculos.

Puede especificar el intervalo de envío periódico de la PDU OAM para la detección de errores.

Para configurar el intervalo de envío, incluya la instrucción en el nivel de jerarquía:`pdu-interval`[`edit protocol oam ethernet link-fault-management interface` *`interface-name`*]

```
[edit protocol oam ethernet link-fault-management interface interface-name]
pdu-interval interval;
```

El intervalo periódico de OAM PDU es de 100 a 1000 milisegundos. El intervalo de envío predeterminado es de 1000 milisegundos.

SEE ALSO

> *Intervalo PDU*

Configuración del umbral de PDU de OAM

Puede especificar el número de PDU de OAM que una interfaz puede pasar por alto antes de que el vínculo entre pares se considere inactivo.

Para configurar el número de PDU que se pueden omitir del par, incluya la instrucción en el nivel de jerarquía:`pdu-threshold`[`edit protocol oam ethernet link-fault-management interface` *`interface-name`*]

```
[edit protocol oam ethernet link-fault-management interface interface-name]
pdu-threshold threshold-value;
```

El intervalo de valores de umbral es de 3 a 10. El valor predeterminado es tres PDU.

SEE ALSO

> *Umbral de PDU*

Configuración de valores de umbral para eventos de error local en una interfaz

Puede configurar valores de umbral en una interfaz para los errores locales que desencadenan el envío de TLV de eventos de vínculo.

Para establecer los valores de umbral de error para enviar TLV de eventos, incluya las instrucciones, , y en el nivel de jerarquía:`frame-errorframe-periodframe-period-summarysymbol-period`[`edit protocols oam ethernet link-fault-management interface` *`interface-name`* `event-thresholds`]

```
[edit protocol oam ethernet link-fault-management interface interface-name]
event-thresholds {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

SEE ALSO

> *Umbrales de eventos*
>
> *frame-error*
>
> *período de marco*
>
> *frame-period-summary*
>
> *símbolo-punto*

Deshabilitar el envío de TLV de eventos de vínculo

Puede deshabilitar el envío de TLV de eventos de vínculo.

Para deshabilitar la supervisión y el envío de PDU que contengan TLV de eventos de vínculo en PDU periódicas, incluya la instrucción en el nivel de jerarquía:`no-allow-link-events`[`edit protocols oam ethernet link-fault-management interface` *`interface-name`* `negotiation-options`]

```
[edit protocol oam ethernet link-fault-management interface interface-name negotiation-options]
no-allow-link-events;
```

SEE ALSO

> *no-allow-link-events*

Ejemplo: Configuración de la compatibilidad con OAM IEEE 802.3ah en una interfaz

Configure la compatibilidad con OAM 802.3ah en una interfaz de 10 Gigabit Ethernet:

```
[edit]
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface xe-0/0/0 {
                    link-discovery active;
                    pdu-interval 800;
                    pdu-threshold 4;
                    remote-loopback;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                    event-thresholds {
                        frame-error 30;
                        frame-period 50;
                        frame-period summary 40;
                        symbol-period 20;
                    }
                }
            }
        }
    }
}
```

SEE ALSO

> *administración de fallas de enlace*

Ejemplo: Configuración de la compatibilidad con OAM IEEE 802.3ah para una interfaz de la serie ACX

in this section

- Requisitos | 149
- Descripción general y topología | 149
- Configuración de IEEE 802.3ah OAM en un enrutador de la serie ACX | 149

Junos OS para enrutadores de la serie ACX permite que las interfaces Ethernet de estos enrutadores admitan el estándar IEEE 802.3ah para la operación, administración y mantenimiento (OAM) de Ethernet en redes de acceso. El estándar define la administración de fallas de vínculo OAM (LFM). Puede configurar IEEE 802.3ah OAM LFM en vínculos Ethernet punto a punto que estén conectados directamente o a través de repetidores Ethernet.

En este ejemplo se describe cómo habilitar y configurar OAM en una interfaz Gigabit Ethernet.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 12.2 o posterior para enrutadores de la serie ACX.
- Un enrutador ACX1000 o ACX2000.

Descripción general y topología

En este ejemplo, se configura una interfaz de 10 Gigabit Ethernet en un enrutador de la serie ACX compatible con OAM de 802,3 ah, que incluye: descubrimiento de vínculos, unidades de datos de protocolo (PDU), circuito cerrado remoto, negociación y umbrales de eventos.

Configuración de IEEE 802.3ah OAM en un enrutador de la serie ACX

in this section

- Configuración rápida de CLI | 150
- Procedimiento | 150

Configuración rápida de CLI

Para configurar rápidamente IEEE 802.3ah Ethernet OAM, copie los siguientes comandos y péguelos en la CLI:

```
edit
edit protocols oam ethernet link-fault-management
set interface xe-0/0/0 link-discovery active pdu-interval 800 pdu-threshold 4 remote-loopback
negotiation-options allow-remote-loopback
set interface xe-0/0/0 event-thresholds frame-error 30 frame-period 50 frame-period-summary 40
symbol-period 20
```

Procedimiento

Procedimiento paso a paso

Para configurar la compatibilidad con OAM IEEE 802.3ah en una interfaz:

1. Habilite la compatibilidad con IEEE 802.3ah OAM en una interfaz:

   ```
   [edit protocols oam ethernet link-fault-management]
   ```

   user@router1# **set interface (OAM Link-Fault Management) xe-0/0/0**

2. Especifique que la interfaz inicia el proceso de descubrimiento estableciendo el modo de detección de vínculos en :**active**

   user@router# **set interface xe-0/0/0 link-discovery active**

3. Establezca el intervalo de envío periódico de PDU OAM (en milisegundos) en 800:

   user@router# **set interface xe-0/0/0 pdu-interval 800**

4. Defina el número de PDU de OAM que se perderán antes de que se registre un error como 4:

   user@router# **set interface xe-0/0/0 pdu-threshold 4**

5. Configure la interfaz remota en modo de circuito cerrado para que todas las tramas, excepto las PDU OAM, se vuelvan a reproducir sin ningún cambio:

   user@router# **set interface xe-0/0/0 remote-loopback**

6. Configure la compatibilidad con circuito cerrado remoto para la interfaz local:

user@router# **set interface xe-0/0/0 negotiation-options allow-remote-loopback**

7. Establezca el recuento de umbrales para enviar eventos de error de trama en 30:

   user@router# **set interface xe-0/0/0 event-thresholds frame-error 30**

8. Establezca el recuento de umbrales para enviar eventos de error de período de trama en 50:

   user@router# **set interface xe-0/0/0 event-thresholds frame-period 50**

9. Configure el recuento de umbrales para enviar eventos de error de resumen de período de fotogramas a 40:

   user@router# **set interface xe-0/0/0 event-thresholds frame-period-summary 40**

10. Establezca el recuento de umbrales para enviar eventos de período de símbolos en 20:

    user@router# **set interface xe-0/0/0 event-thresholds symbol-period 20**

Resultados

Compruebe los resultados de la configuración:

```
[edit]

user@router# show
```

```
[edit]
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface xe-0/0/0 {
                    link-discovery active;
                    pdu-interval 800;
                    pdu-threshold 4;
                    remote-loopback;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                    event-thresholds {
                        frame-error 30;
                        frame-period 50;
```

```
                        frame-period-summary 40;
                        symbol-period 20;
                    }
                }
            }
        }
    }
}
```

SEE ALSO

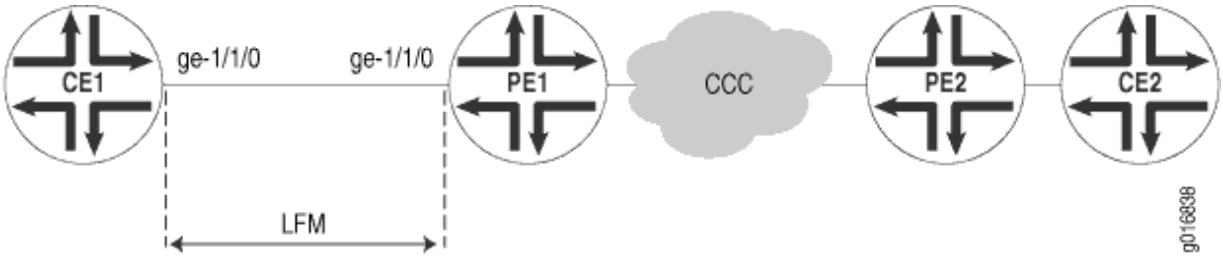
administración de fallas de enlace

Ejemplo: Configuración de Ethernet LFM entre el borde del proveedor y el borde del cliente

En este ejemplo, LFM se habilita en un vínculo IP entre las interfaces de borde del proveedor (PE) y borde del cliente (CE). Si el enlace se cae, el fallo será detectado por LFM y las interfaces en ambos lados se marcarán .**Link-Layer-Down** Esto da lugar a notificaciones a varios subsistemas (por ejemplo, enrutamiento) que tomarán las medidas adecuadas.

El vínculo que ejecuta LFM se muestra en .Figura 13 en la página 152

Figura 13: LFM de Ethernet entre el borde del proveedor y el borde del cliente



Para configurar Ethernet LFM en un vínculo IP entre interfaces PE y CE:

1. Configure LFM en el enrutador PE:

```
[edit]
interfaces ge-1/1/0 {
    unit 0 {
        family inet {
```

```
            address 11.11.11.1/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

2. Configure LFM en el enrutador CE:

```
[edit]
interfaces ge-1/1/0 {
    unit 0 {
        family inet {
            address 11.11.11.2/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

SEE ALSO

Guía del usuario de interfaces Ethernet para dispositivos de enrutamiento

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | 139

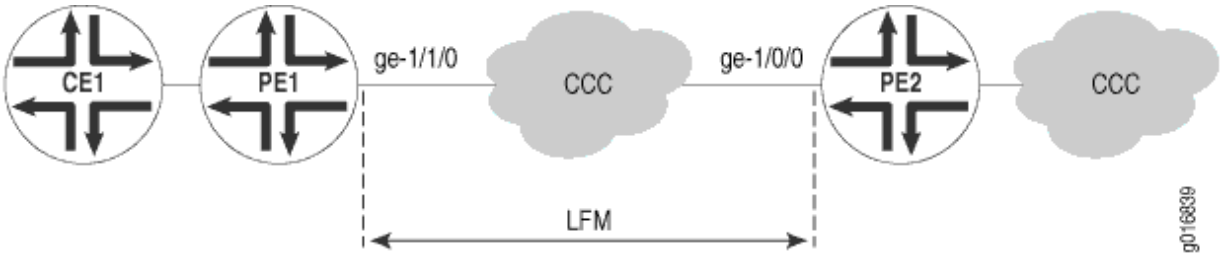
Ejemplo: Configuración de Ethernet LFM con soporte de circuito cerrado | 171

Ejemplo: Configuración de Ethernet LFM para CCC

En este ejemplo, LFM se configura entre dos PE (PE1 y PE2) conectados mediante CCC. Con LFM en su lugar, se detectará una falla de enlace de inmediato, en lugar de depender de los protocolos de enrutamiento para encontrar la falla en la conexión CCC de extremo a extremo. Esto también ayuda a detectar el enlace fallido exacto en lugar de solo encontrar que la conectividad CCC de extremo a extremo ha fallado. Además, debido a que LFM se ejecuta en el nivel de capa de enlace, no necesita una dirección IP para funcionar y, por lo tanto, se puede usar donde la detección de fallas bidireccional (BFD) no puede.

Los vínculos que ejecutan LFM se muestran en Figura 14 en la página 154

Figura 14: Ethernet LFM para CCC



Para configurar Ethernet LFM entre dos PE conectados mediante CCC:

1. Configure LFM en el enrutador PE1 con CCC:

```
[edit]
interfaces ge-1/1/0 {
    encapsulation ethernet-ccc;
    unit 0;
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
```

```
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

2. Configure LFM en el enrutador PE2 con CCC:

```
[edit]
interfaces ge-1/0/0 {
    encapsulation ethernet-ccc;
    unit 0;
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/0/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                }
            }
        }
    }
}
```

SEE ALSO

Guía del usuario de interfaces Ethernet para dispositivos de enrutamiento

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | **139**

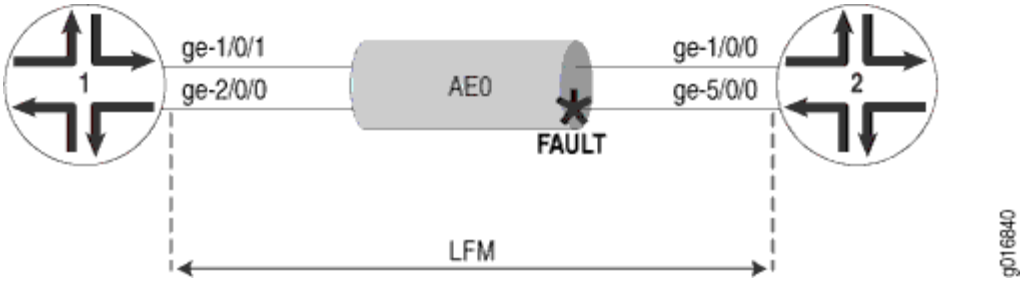
Ejemplo: Configuración de Ethernet LFM con soporte de circuito cerrado | **171**

Ejemplo: Configuración de Ethernet LFM para Ethernet agregada

En este ejemplo, LFM se configura en una interfaz Ethernet agregada (AE0) entre el enrutador 1 y el enrutador 2. Cuando se configura en Ethernet agregada, LFM se ejecuta en todos los vínculos de miembros individuales. LFM se habilita o deshabilita en los enlaces de miembro a medida que se agregan o eliminan del grupo de agregación. El estado de los vínculos individuales se utiliza para determinar el estado de la interfaz agregada.

El uso de LFM con Ethernet agregada se muestra en Figura 15 en la página 156.

Figura 15: LFM de Ethernet para Ethernet agregada



Para configurar LFM en una interfaz Ethernet agregada entre dos enrutadores:

1. Configure LFM en el enrutador 1 para AE0:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 1;
        }
    }
}
interfaces ge-1/0/1 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ge-2/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ae0 {
    unit 0 {
        family inet {
            address 11.11.11.2/24;
        }
    }
}
protocols {
```

```
    oam {
        ethernet {
            link-fault-management {
                interface ae0;
            }
        }
    }
}
```

2. Configure LFM en el enrutador 2 para AE0:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 1;
        }
    }
}
interfaces ge-1/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ge-5/0/0 {
    gigether-options {
        802.3ad ae0;
    }
}
interfaces ae0 {
    unit 0 {
        family inet {
            address 11.11.11.1/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ae0;
            }
```

```
        }
    }
}
```

SEE ALSO

Guía del usuario de interfaces Ethernet para dispositivos de enrutamiento

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | 139

Ejemplo: Configuración de Ethernet LFM con soporte de circuito cerrado | 171

Configuración de un perfil de acción de OAM

Puede crear un perfil de acción para definir indicadores y umbrales de error de evento, así como la acción que debe realizarse. A continuación, puede aplicar el perfil de acción a una o más interfaces.

Para configurar un perfil de acción, incluya la instrucción en el nivel de jerarquía:`action-profile[edit protocols oam ethernet link-fault-management]`

```
action-profile profile-name {
    action {
        syslog;
        link-down;
        send-critical-event;
    }
    event {
        link-adjacency-loss;
        link-event-rate {
            frame-error count;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
        protocol-down;
    }
}
```

NOTA: A partir de Junos OS versión 14.2, siempre que la administración de errores de vínculo (LFM) con un perfil de acción esté configurada para marcar la interfaz como inactiva (mediante la

inclusión de la instrucción link-down en el nivel jerárquico [edit protocols oam ethernet link-fault-management]), el puerto se coloca en estado bloqueado (estado STP). En tal estado de la interfaz, el tráfico de datos no se transmite en esa interfaz. Debido a que los MEP de mantenimiento descendente de gestión de fallos de conectividad (CFM) aparecen en puertos bloqueados, las sesiones de CFM aparecen correctamente. Sin embargo, la interfaz está inactiva y el TLV de estado de la interfaz no contiene el estado correcto. Solo si configura el TLV de estado del puerto, se reflejará el estado real del puerto. El TLV de estado de la interfaz no lleva el estado real del puerto.

SEE ALSO

Configuración de una interfaz remota en modo de circuito cerrado | **166**

Habilitación de la compatibilidad con circuito cerrado remoto en la interfaz local | **167**

Especificación de las acciones que deben realizarse para los eventos de administración de errores de vínculo

Puede especificar la acción que debe realizar el sistema cuando se produzca el evento de error de vínculo configurado. Se pueden aplicar varios perfiles de acción a una sola interfaz. Para cada perfil de acción, se debe especificar al menos un evento y una acción. Las acciones solo se realizan cuando todos los eventos del perfil de acción son verdaderos. Si se especifica más de una acción, se ejecutarán todas las acciones.

Es posible que desee establecer un umbral más bajo para una acción específica, como registrar el error, y establecer un umbral más alto para otra acción, como enviar un TLV de evento crítico.

Para especificar la acción, incluya la instrucción en el nivel de jerarquía:`action`[`edit protocols oam ethernet link-fault-management action-profile` *`profile-name`*]

```
[edit protocol oam ethernet link-fault-management action-profile profile-name]
event {
    link-adjacency-loss;
    protocol-down;
}
action {
    syslog;
    link-down;
    send-critical-event;
}
```

Para crear una entrada de registro del sistema cuando se produzca el evento de error de vínculo, incluya la instrucción.`syslog`

Para deshabilitar administrativamente el vínculo cuando se produzca el evento link-fault, incluya la instrucción.`link-down`

Para enviar TLV de eventos de vínculo IEEE 802.3ah en la PDU de OAM cuando se produce un evento de error de vínculo, incluya la instrucción.`send-critical-event`

> **NOTA**: Si se especifican varias acciones en el perfil de acciones, todas las acciones se ejecutan sin ningún orden en particular.

SEE ALSO

- *Acción*
- *Syslog*
- *Enlace hacia abajo*
- *send-critical-event*

Monitoreo de la pérdida de adyacencia del enlace

Puede especificar las acciones que se tomen cuando se pierda la adyacencia del vínculo. Cuando se pierde la adyacencia del vínculo, el sistema realiza la acción definida en la instrucción del perfil de acción.`action`

Para configurar el sistema para que realice acciones cuando se pierda la adyacencia del vínculo, incluya la instrucción en el nivel de jerarquía:`link-adjacency-loss`[`edit protocols oam ethernet link-fault-management action-profile` *`profile-name`* `event`]

```
[edit protocol oam ethernet link-fault-management action-profile profile-name]
link-adjacency-loss;
```

SEE ALSO

- *link-adyacencia-pérdida*
- Habilitación de la compatibilidad con circuito cerrado remoto en la interfaz local | 167

Estado del protocolo de supervisión

El indicador CCC-DOWN está asociado con una conexión de conexión cruzada de circuito (CCC), un circuito de capa 2 y una VPN de capa 2, que envían el estado CCC-DOWN al kernel. El indicador CCC-DOWN indica que el CCC está inactivo. El estado CCC-DOWN se envía al kernel cuando la conexión CCC, el circuito de capa 2 o la VPN de capa 2 están inactivos. Esto, a su vez, derriba la interfaz PE orientada hacia CE asociada con la conexión CCC, el circuito de capa 2 o la VPN de capa 2.

Cuando se señala el indicador CCC-DOWN al protocolo IEEE 802.3ah, el sistema realiza la acción definida en la instrucción del perfil de acción.`action` Para obtener más información acerca de los circuitos de capa 2, consulte la Guía del usuario de circuitos de capa 2 de Junos OS, Guía de configuración de VPN de Junos OS.

Para supervisar el protocolo IEEE 802.3ah en la interfaz PE orientada a CE, incluya la instrucción en el nivel de jerarquía:protocol-down[`edit protocols oam ethernet link-fault-management action-profile` *`profile-name`* `event`]

1. En el modo de configuración, vaya al nivel de jerarquía.[`edit protocols oam ethernet link-fault-management action-profile profile-name event`]

```
[edit]
user@host# edit protocols oam ethernet link-fault-management action-profile profile-name event
```

2. Incluya la instrucción.`protocol-down`

```
[edit protocols oam ethernet link-fault-management action-profile profile-name event]
user@host# set protocol-down
```

NOTA: Si se especifican varios eventos en el perfil de acción, todos los eventos deben producirse antes de que se realice la acción especificada.

SEE ALSO

protocolo inactivo

Configuración de una interfaz remota en modo de circuito cerrado | 166

Habilitación de la compatibilidad con circuito cerrado remoto en la interfaz local | 167

Configuración de valores de umbral para eventos de error en un perfil de acción

Puede configurar umbrales de eventos de vínculo para eventos de error recibidos que desencadenen la acción especificada en la instrucción.`action` A continuación, puede aplicar el perfil de acción a una o más interfaces.

Para configurar umbrales de eventos de vínculo, incluya la instrucción en el nivel de jerarquía:`link-event-rate`[`edit protocols oam ethernet link-fault-management action-profile` *`profile-name`* `event`]

```
link-event-rate {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
}
```

SEE ALSO

> *link-event-rate*

Aplicación de un perfil de acción

Puede aplicar un perfil de acción a una o varias interfaces.

Para aplicar un perfil de acción a una interfaz, incluya la instrucción en el nivel de jerarquía:`apply-action-profile`[`edit protocols oam ethernet link-fault-management action-profile interface` *`interface-name`*]

```
[edit protocol oam ethernet link-fault-management interface interface-name]
apply-action-profile profile-name;
```

SEE ALSO

> *perfil de aplicación-acción*

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
14.2	A partir de Junos OS versión 14.2

VÍNCULOS RELACIONADOS

Circuito cerrado remoto para administración de fallas de vínculo | 165

Detección remota de fallos para la gestión de fallos de vínculo

in this section

Detección de fallas remotas | 163
Habilitación de la funcionalidad de jadeo moribundo | 164

Use este tema para obtener más información acerca de las fallas remotas y cómo se detectan, y también cómo habilitar la característica de jadeo moribundo para evitar daños en el sistema de archivos para LFM.

Detección de fallas remotas

La detección de errores se basa en indicadores o en el tipo, longitud y valores de eventos de error (TLV) recibidos en las unidades de datos de protocolo (PDU) de OAM. Las marcas que desencadenan un error de vínculo son:

- Evento crítico
- Jadeo moribundo
- Error de vínculo

Los TLV de eventos de vínculo son enviados por el DTE remoto por medio de PDU de notificación de eventos. Los TLV de eventos de vínculo son:

- Evento de período de símbolo erróneo

- Evento de trama con errores
- Evento de período de trama con errores
- Evento de resumen de segundos de trama con errores

SEE ALSO

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | **139**

Configuración de la administración de errores de vínculo OAM IEEE 802.3ah

Habilitación de la funcionalidad de jadeo moribundo

Morir jadeando significa una condición irrecuperable, como un corte de energía. En esta condición, el par local informa al par remoto sobre el estado de error. Cuando el par remoto recibe una PDU que muere, realiza una acción correspondiente al perfil de acción configurado con el evento.**link-adjacency-loss** Morir jadeante ayuda a evitar la corrupción del sistema de archivos.

> **NOTA**: ACX5096 y ACX5048 enrutadores no admiten morir sin aliento.

Los enrutadores de la serie ACX pueden generar y recibir paquetes de muerte y muerte. Cuando LFM se configura en una interfaz, se genera una PDU de muerte para la interfaz en las siguientes condiciones de error:

- Falla de energía
- Pánico o bloqueo del motor de reenvío de paquetes

Los enrutadores de la serie ACX admiten las siguientes instrucciones CLI para habilitar la funcionalidad de morir-jadear:

- `dgasp-int`—Permite la funcionalidad morir-jadear.
- `dgasp-usb`—Restablece el puerto USB durante un evento de muerte sin aliento.

Las instrucciones y CLI se agregan bajo la jerarquía para habilitar la funcionalidad de morir-jadear.`dgasp-intdgasp-usb[edit system]`

Para habilitar la funcionalidad dying-gasp, debe configurar las instrucciones y CLI como se muestra a continuación:`dgasp-intdgasp-usb`

```
root@host% cli
root@host> configure
```

```
Entering configuration mode

[edit]
root@host# set system dgasp-int

[edit]
root@host# set system dgasp-usb

[edit]
root@host# commit

commit complete

[edit]
root@host# show system
dgasp-int;
dgasp-usb;
```

La funcionalidad de morir-jadeo está deshabilitada de forma predeterminada.

SEE ALSO

Descripción de la administración de fallas de vínculo OAM Ethernet para enrutadores de la serie ACX | 140

VÍNCULOS RELACIONADOS

Introducción a la gestión de fallos de vínculo OAM (LFM) | 139

Circuito cerrado remoto para administración de fallas de vínculo

in this section

- Configuración de una interfaz remota en modo de circuito cerrado | 166
- Habilitación de la compatibilidad con circuito cerrado remoto en la interfaz local | 167

Habilitación del enrutamiento sin interrupciones para la administración de fallas de vínculo Ethernet en enrutadores de respaldo | 167

Ejemplo: Configuración de Ethernet LFM con soporte de circuito cerrado | 171

Use este tema para comprender qué sucede cuando establece una interfaz remota en modo de circuito cerrado y cómo habilitar el circuito cerrado remoto. También puede obtener información sobre cómo habilitar el enrutamiento sin interrupciones para LFM.

Configuración de una interfaz remota en modo de circuito cerrado

Puede configurar el software para establecer el DTE remoto en modo de circuito cerrado en las siguientes interfaces:

- Interfaces IQ2 e IQ2-E Gigabit Ethernet
- Interfaces Ethernet en los enrutadores serie MX o conmutadores serie EX

Junos OS puede colocar un DTE remoto en modo de circuito cerrado (si el modo de circuito cerrado remoto es compatible con la DTE remota). Cuando coloca un DTE remoto en modo de circuito cerrado, la interfaz recibe la solicitud de circuito cerrado remoto y pone la interfaz en modo de circuito cerrado remoto. Cuando la interfaz está en modo de circuito cerrado remoto, todas las tramas, excepto las PDU OAM, se vuelven a reproducir sin que se realicen cambios en las tramas. Las PDU de OAM se siguen enviando al plano de administración y procesándose.

Para configurar el circuito cerrado remoto, incluya la instrucción en el nivel de jerarquía:`remote-loopback`[`edit protocol oam ethernet link-fault-management interface` *`interface-name`*]

```
[edit protocol oam ethernet link-fault-management interface interface-name]
remote-loopback;
```

Para sacar el DTE remoto del modo de circuito cerrado, quite la instrucción de la configuración.`remote-loopback`

SEE ALSO

circuito cerrado remoto

Habilitación de la compatibilidad con circuito cerrado remoto en la interfaz local

Puede permitir que un DTE remoto establezca una interfaz local en modo de circuito cerrado remoto en las interfaces IQ2 e IQ2-E Gigabit Ethernet y en todas las interfaces Ethernet de los enrutadores serie MX y conmutadores de la serie EX. Cuando una DTE remota envía una solicitud de circuito cerrado remoto, Junos OS pone la interfaz local en modo de circuito cerrado. Cuando una interfaz está en modo de circuito cerrado, todas las tramas, excepto las PDU OAM, se vuelven a bucle sin ningún cambio en las tramas. Las PDU de OAM se siguen enviando al plano de administración y procesándose. De forma predeterminada, la característica de circuito cerrado remoto no está habilitada.

Para habilitar el circuito cerrado remoto, incluya la instrucción en el nivel de jerarquía:`allow-remote-loopback`[`edit protocol oam ethernet link-fault-management interface` *`interface-name`* `negotiation-options`]

```
[edit protocol oam ethernet link-fault-management interface interface-name negotiation-options]
allow-remote-loopback;
```

> **NOTA**: La activación del circuito cerrado remoto de OAM puede provocar la pérdida de tramas de datos.

SEE ALSO

> *allow-remote-loopback*

Habilitación del enrutamiento sin interrupciones para la administración de fallas de vínculo Ethernet en enrutadores de respaldo

A partir de Junos OS versión 17.3R1, el demonio de administración de errores de vínculo Ethernet (lfmd) se ejecuta en el motor de enrutamiento de reserva también cuando se configura un cambio correcto del motor de enrutamiento (GRES). Cuando el demonio lfmd también se ejecuta en el motor de enrutamiento de reserva, los estados de administración de errores de vínculo se mantienen sincronizados y, por lo tanto, el demonio lfmd requiere un esfuerzo mínimo.

Para habilitar el enrutamiento sin interrupciones para Ethernet LFM en enrutadores de respaldo:

1. Habilite el cambio correcto del motor de enrutamiento. De forma predeterminada, GRES está deshabilitado. Para habilitar GRES, incluya la instrucción en el nivel de jerarquía [].`graceful-`

`switchoveredit chassis redundancy` De forma predeterminada, el enrutamiento sin interrupción está deshabilitado. Cuando se habilita GRES, se habilita NSR.

```
[edit chassis redundancy]
user@host# set graceful-switchover
```

2. Sincronice la configuración del motor de enrutamiento. Para sincronizar la configuración principal del motor de enrutamiento con la copia de seguridad, incluya la instrucción en el nivel de jerarquía [].`synchronizeedit system`

```
[edit system]
user@host# set commit synchronize
```

3. Después de habilitar el enrutamiento sin interrupciones, confirme la configuración.

```
[edit routing options]
user@host# commit
```

4. Para comprobar si el enrutamiento sin interrupción está habilitado en el enrutador de reserva, en el modo operativo, utilice el comando en el enrutador principal y, a continuación, en el enrutador de reserva.`show oam ethernet link-fault-management` Dado que ha habilitado la sincronización, la salida del enrutador principal y del enrutador de reserva son idénticos. Sin embargo, las estadísticas mantenidas por el enrutador principal no se sincronizan con el enrutador de respaldo.

```
{master}
user@host# show oam ethernet link-fault-management ge-0/2/0 detail
```

```
Interface: ge-0/2/0
    Status: Running, Discovery state: Send Any
    Transmit interval: 100ms, PDU threshold: 3 frames, Hold time: 300ms
    Peer address: ac:4b:c8:81:90:a4
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
```

```
      Loopback control: 786, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Enabled, Loop status: Not Found
    Detect LOC: Enabled, LOC status: Not Found
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: unsupported, Link events: supported
      Variable requests: unsupported
Application profile statistics:
  Profile Name                   Invoked     Executed
  LK_ADJ_LOSS100_1                         1        1
  LK_ADJ_LOSS100_2                         1        0
  LK_ADJ_LOSS100_3                         1        0
  LK_ADJ_LOSS101_1                         1        1
  LK_ADJ_LOSS101_2                         1        0
  LK_ADJ_LOSS101_3                         1        0
  LK_ADJ_LOSS106_1                         0        0
  LK_ADJ_LOSS106_2                         0        0
  LK_ADJ_LOSS106_3                         0        0
```

```
  LK_ADJ_LOSS107_1                          0        0
  LK_ADJ_LOSS107_2                          0        0
  LK_ADJ_LOSS107_3                          0        0
```

```
{backup}
user@host# show oam ethernet link-fault-management ge-0/2/0 detail
```

```
Interface: ge-0/2/0
    Status: Running, Discovery state: Send Any
    Transmit interval: 100ms, PDU threshold: 3 frames, Hold time: 300ms
    Peer address: ac:4b:c8:81:90:a4
    Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 786, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
```

```
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Enabled, Loop status: Not Found
    Detect LOC: Enabled, LOC status: Not Found
    Remote entity information:
      Remote MUX action: forwarding, Remote parser action: forwarding
      Discovery mode: active, Unidirectional mode: unsupported
      Remote loopback mode: unsupported, Link events: supported
      Variable requests: unsupported
Application profile statistics:
  Profile Name                    Invoked     Executed
  LK_ADJ_LOSS100_1                          0        0
  LK_ADJ_LOSS100_2                          0        0
  LK_ADJ_LOSS100_3                          0        0
  LK_ADJ_LOSS101_1                          0        0
  LK_ADJ_LOSS101_2                          0        0
  LK_ADJ_LOSS101_3                          0        0
  LK_ADJ_LOSS106_1                          0        0
  LK_ADJ_LOSS106_2                          0        0
  LK_ADJ_LOSS106_3                          0        0
  LK_ADJ_LOSS107_1                          0        0
  LK_ADJ_LOSS107_2                          0        0
  LK_ADJ_LOSS107_3                          0        0
```

NOTA: Después del cambio, si se observan problemas, use el comando para sesiones específicas.`clear oam ethernet link-fault-management state` Si el problema no se resuelve, reinicie el demonio lfmd.

SEE ALSO

Descripción general de la administración de fallas de vínculo OAM IEEE 802.3ah | **139**

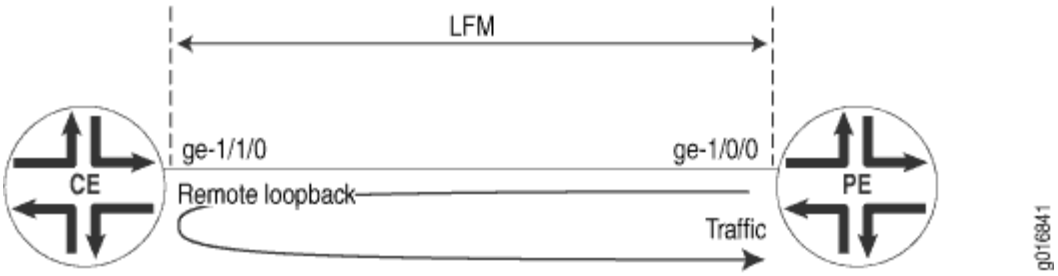
Mostrar administración de fallas de vínculo Ethernet de OAM

Ejemplo: Configuración de Ethernet LFM con soporte de circuito cerrado

En este ejemplo, LFM se configura entre el enrutador perimetral del proveedor (PE) y el enrutador perimetral del cliente (CE). El enrutador PE puede poner al enrutador CE en modo de circuito cerrado

remoto. Esto permite que el PE tenga todo el tráfico enviado al enrutador CE en bucle hacia atrás con fines de diagnóstico, como se muestra en Figura 16 en la página 172.

Figura 16: Ethernet LFM con soporte de circuito cerrado



Para configurar LFM entre un enrutador PE y un enrutador CE:

1. Configure el circuito cerrado LFM en el enrutador PE:

```
[edit]
interfaces ge-1/0/0 {
    unit 0 {
        family inet {
            address 11.11.11.1/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/0/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                    remote-loopback;
                }
            }
        }
    }
}
```

2. Configure el circuito cerrado LFM en el enrutador CE:

```
[edit]
interfaces ge-1/1/0 {
    unit 0 {
        family inet {
            address 11.11.11.2/24;
        }
    }
}
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-1/1/0 {
                    pdu-interval 1000;
                    pdu-threshold 5;
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
        }
    }
}
```

NOTA: Si se elimina la instrucción en el enrutador CE antes de quitar el enrutador CE del modo de circuito cerrado remoto, el flujo de tráfico entre el enrutador PE y el enrutador CE se verá afectado.`negotiation options allow-remote-loopback` Por lo tanto, elimine la instrucción en el enrutador PE antes de eliminar la instrucción en el enrutador CE.`remote-loopbacknegotiation-options allow-remote-loopback`

SEE ALSO

Ejemplo: Configuración de Ethernet LFM entre el borde del proveedor y el borde del cliente | 152

Ejemplo: Configuración de Ethernet LFM para CCC | 154

Ejemplo: Configuración de Ethernet LFM para Ethernet agregada | 155

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.3R1	A partir de Junos OS versión 17.3R1, el demonio de administración de errores de vínculo Ethernet (lfmd) se ejecuta en el motor de enrutamiento de reserva también cuando se configura un cambio correcto del motor de enrutamiento (GRES).

VÍNCULOS RELACIONADOS

Introducción a la gestión de fallos de vínculo OAM (LFM) | 139

Configurar la administración de errores de vínculo | 144

chapter label in part3

Administración de fallos de vínculo OAM Ethernet para conmutadores

in this chapter

- Administración de fallos de vínculo OAM de Ethernet | 175
- Configurar la administración de fallos de vínculo OAM de Ethernet | 177
- Ejemplo: Configurar la administración de fallos de vínculo OAM de Ethernet | 180

Administración de fallos de vínculo OAM de Ethernet

El sistema operativo Junos de Juniper Networks (Junos OS) para Juniper Networks permite que las interfaces Ethernet de estos conmutadores admitan el estándar IEEE 802.3ah para la operación, administración y mantenimiento (OAM) de Ethernet en redes de acceso. El estándar define la administración de fallas de vínculo OAM (LFM). Puede configurar IEEE 802.3ah OAM LFM en vínculos Ethernet punto a punto que estén conectados directamente o a través de repetidores Ethernet. El estándar IEEE 802.3ah cumple con los requisitos de capacidades OAM, incluso cuando Ethernet pasa de ser únicamente una tecnología empresarial a una WAN y tecnología de acceso, y el estándar sigue siendo compatible con la tecnología Ethernet existente.

Ethernet OAM proporciona las herramientas que el software de administración de red y los administradores de red pueden utilizar para determinar cómo funciona una red de vínculos Ethernet. Ethernet OAM debe:

- Confíe únicamente en la dirección MAC (Media Access Control) o en el identificador de LAN virtual para la solución de problemas.
- Trabaje independientemente del transporte y función Ethernet real a través de puertos Ethernet físicos o un servicio virtual como pseudocable.
- Aísle los fallos en una arquitectura de red plana (o de un solo operador) o en redes anidadas, jerárquicas (o de múltiples proveedores).

Se admiten las siguientes características de LFM de OAM:

- Descubrimiento y monitoreo de enlaces

  El proceso de descubrimiento se activa automáticamente cuando OAM está habilitado en la interfaz. El proceso de descubrimiento permite que las interfaces Ethernet descubran y supervisen el par en el vínculo si también es compatible con el estándar IEEE 802.3ah. Puede especificar el modo de detección utilizado para la compatibilidad con IEEE 802.3ah OAM. En el modo activo, la interfaz descubre y supervisa el par en el vínculo si el par también admite la funcionalidad OAM IEEE 802.3ah. En el modo pasivo, el par inicia el proceso de detección. Después de que se ha iniciado el proceso de descubrimiento, ambas partes participan en el descubrimiento. El conmutador realiza la supervisión de vínculos mediante el envío periódico de unidades de datos de protocolo OAM (PDU) para anunciar el modo, la configuración y las capacidades de OAM.

  Puede especificar el número de PDU de OAM que una interfaz puede pasar por alto antes de que el vínculo entre pares se considere inactivo.

- Detección remota de fallos

  La detección remota de fallos utiliza indicadores y eventos. Las banderas se utilizan para transmitir lo siguiente: Falla de vínculo significa una pérdida de señal, Dying Gasp significa una condición irrecuperable, como una falla de energía, y Evento crítico significa un evento crítico no especificado específico del proveedor. Puede especificar el intervalo de envío periódico de la PDU OAM para la detección de errores. El conmutador utiliza la PDU OAM de notificación de eventos para notificar al dispositivo OAM remoto cuando se detecta un problema. Puede especificar la acción que debe realizar el sistema cuando se produzca el evento de error de vínculo configurado.

- Modo de circuito cerrado remoto

  El modo de circuito cerrado remoto garantiza la calidad del vínculo entre el conmutador y un par remoto durante la instalación o la solución de problemas. En este modo, cuando la interfaz recibe una trama que no es una PDU OAM o una trama de pausa, lo envía de vuelta a la misma interfaz en la que se recibió. El vínculo parece estar en el estado activo. Puede usar la confirmación de circuito cerrado devuelta para probar el retraso, la *fluctuación* y el rendimiento.

  Junos OS puede colocar un DTE remoto en modo de circuito cerrado (si la DTE remota admite el modo de circuito cerrado remoto). Cuando coloca un DTE remoto en modo de circuito cerrado, la interfaz recibe la solicitud de bucle cerrado remoto y pone la interfaz en modo de circuito cerrado remoto. Cuando la interfaz está en modo de circuito cerrado remoto, todas las tramas, excepto las PDU OAM, se vuelven a bucle sin que se realicen cambios en las tramas. Las PDU OAM se siguen enviando y procesando.

Configurar la administración de fallos de vínculo OAM de Ethernet

La administración de fallos de vínculo (LFM) de Ethernet OAM se puede utilizar para la detección y administración de fallas a nivel de vínculo físico. El IEEE 802.3ah LFM funciona a través de enlaces Ethernet punto a punto, ya sea directamente o a través de repetidores.

Para configurar Ethernet OAM LFM mediante la CLI:

1. Habilite la compatibilidad con IEEE 802.3ah OAM en una interfaz:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface                          interface-
name
```

> **NOTA**: Puede configurar Ethernet OAM LFM en interfaces agregadas.

> **NOTA**: Los pasos restantes son opcionales. Puede elegir cuál de estas funciones desea configurar para Ethernet OAM LFM en el conmutador.

2. Especifique si la interfaz o el par inicia el proceso de descubrimiento configurando el modo de descubrimiento de vínculos en o (= interfaz inicia; = inicia par):`activepassiveactivepassive`

```
[edit protocols oam ethernet link-fault-management]
 user@switch# set interface interface-namelink-discovery active
```

3. Configure un intervalo periódico de envío de PDU OAM (en milisegundos) para la detección de errores:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface pdu-intervalinterval
```

4. Especifique el número de PDU de OAM que una interfaz puede pasar por alto antes de que el vínculo entre pares se considere inactivo:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name                    pdu-
threshold                    threshold-value
```

5. Configure valores de umbral de eventos en una interfaz para los errores locales que desencadenan el envío de TLV de eventos de vínculo:

   - Establezca el valor de umbral (en segundos) para enviar eventos de error de trama o realizar la acción especificada en el perfil de acción:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name                    event-
thresholds                    frame-error
count
```

   - Establezca el valor de umbral (en segundos) para enviar eventos de período de fotogramas o realizar la acción especificada en el perfil de acción:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-
period
count
```

   - Establezca el valor de umbral (en segundos) para enviar eventos frame-period-summary o realizar la acción especificada en el perfil de acción:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-period-
summary
count
```

   - Establezca el valor de umbral (en segundos) para enviar eventos de período de símbolos o realizar la acción especificada en el perfil de acción:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds symbol-
```

```
period
count
```

NOTA: Puede deshabilitar el envío de TLV de eventos de vínculo.

Para deshabilitar el envío de TLV de eventos de vínculo:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name                    negotiation-
options                    no-allow-link-events
```

6. Cree un perfil de acción para definir los indicadores de error de evento y los umbrales que deben tomarse cuando se produce el evento de error de vínculo. A continuación, aplique el perfil de acción a una o más interfaces. (También puede aplicar varios perfiles de acción a una sola interfaz).

   a) Asigne un nombre al perfil de acción:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set action-profile                    profile-
name
```

   b) Especifique las acciones que debe realizar el sistema cuando se produzca el evento de error de vínculo:

```
[edit protocols oam ethernet link-fault-management]
 user@switch# set action-profile profile-name
action
syslog
```

```
user@switch# set action-profile profile-name action link-
down
```

c) Especifique eventos para el perfil de acción:

```
[edit protocols oam ethernet link-fault-management]
 user@switch# set action-profile profile-name event link-adjacency-
loss
```

NOTA: Para cada perfil de acción, debe especificar al menos un evento de vínculo y una acción. Las acciones solo se realizan cuando todos los eventos del perfil de acción son verdaderos. Si se especifica más de una acción, se ejecutan todas las acciones. Puede establecer un umbral bajo para una acción específica, como registrar el error, y establecer un umbral alto para otra acción, como el registro del sistema.

7. Establezca una interfaz remota en modo de circuito cerrado para que todas las tramas, excepto las PDU OAM, se vuelvan a reproducir sin que se realicen cambios en las tramas. Establezca el DTE remoto en modo de circuito cerrado (el DTE remoto debe admitir el modo de circuito cerrado remoto) y, a continuación, habilite la compatibilidad con circuito cerrado remoto para la interfaz local.

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name                          remote-
loopback
```

```
user@switch# set interface interface-name negotiation-options allow-remote-
loopback
```

Ejemplo: Configurar la administración de fallos de vínculo OAM de Ethernet

in this section

- Requisitos | **181**
- Descripción general y topología | **181**
- Configuración de la administración de fallas de vínculo OAM Ethernet en el conmutador 1 | **182**

Configuración de la administración de fallos de vínculo OAM Ethernet en el conmutador 2 | 184
Verificación | 185

Junos OS permite que las interfaces Ethernet de estos conmutadores admitan el estándar IEEE 802.3ah para la operación, administración y mantenimiento (OAM) de Ethernet en redes de acceso. El estándar define la administración de fallas de vínculo OAM (LFM). Puede configurar IEEE 802.3ah OAM LFM en vínculos Ethernet punto a punto que estén conectados directamente o a través de repetidores Ethernet.

En este ejemplo se describe cómo habilitar y configurar OAM LFM en una interfaz Gigabit Ethernet:

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 9.4 o posterior para conmutadores serie EX
- Dos conmutadores EX3200 o EX4200 conectados directamente

Descripción general y topología

in this section

Topología | 181

Los conmutadores Junos OS permiten que las interfaces Ethernet de estos conmutadores admitan el estándar IEEE 802.3ah para la operación, administración y mantenimiento (OAM) de Ethernet en redes de acceso. El estándar define la administración de fallas de vínculo OAM (LFM). Puede configurar IEEE 802.3ah OAM LFM en vínculos Ethernet punto a punto que estén conectados directamente o a través de repetidores Ethernet.

Topología

En este ejemplo se utilizan dos conmutadores EX4200 conectados directamente. Antes de empezar a configurar Ethernet OAM LFM en dos conmutadores, conecte los dos conmutadores directamente a través de una interfaz troncal.

Configuración de la administración de fallas de vínculo OAM Ethernet en el conmutador 1

in this section

- Configuración rápida de CLI | 182
- Procedimiento | 182
- Resultados | 183

Configuración rápida de CLI

Para configurar rápidamente Ethernet OAM LFM, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

```
[edit protocols oam ethernet link-fault-management]
                    set interface ge-0/0/0
                    set interface ge-0/0/0 link-discovery active
                    set interface ge-0/0/0 pdu-interval 800
                    set interface ge-0/0/0 remote-loopback
```

Procedimiento

Procedimiento paso a paso

Para configurar Ethernet OAM LFM en el conmutador 1:

1. Habilite la compatibilidad con IEEE 802.3ah OAM en una interfaz:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0
```

2. Especifique que la interfaz inicia el proceso de descubrimiento configurando el modo de detección de vínculos para :`active`

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0 link-discovery active
```

3. Establezca el intervalo de envío periódico de PDU OAM (en milisegundos) en 800 en el conmutador 1:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface pdu-interval 800
```

4. Establezca una interfaz remota en modo de circuito cerrado para que todas las tramas, excepto las PDU OAM, se vuelvan a reproducir sin que se realicen cambios en las tramas. Asegúrese de que el DTE remoto admite el modo de circuito cerrado remoto. Para establecer el DTE remoto en modo de circuito cerrado

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0.0 remote-
loopback
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]

user@switch1# show
```

```
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-0/0/0 {
                    pdu-interval 800;
                    link-discovery active;
                    remote-loopback;
```

```
                }
            }
        }
    }
```

Configuración de la administración de fallos de vínculo OAM Ethernet en el conmutador 2

in this section

- Configuración rápida de CLI | 184
- Procedimiento | 184

Configuración rápida de CLI

Para configurar rápidamente Ethernet OAM LFM en el conmutador 2, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

```
[edit protocols oam ethernet link-fault-management ]
                    set interface ge-0/0/1
                    set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

Procedimiento

Procedimiento paso a paso

Para configurar Ethernet OAM LFM en el conmutador 2:

1. Habilite OAM en la interfaz par del conmutador 2:

```
[edit protocols oam ethernet link-fault-management]
user@switch2# set interface ge-0/0/1
```

2. Habilite la compatibilidad con circuito cerrado remoto para la interfaz local:

```
[edit protocols oam ethernet link-fault-management]
user@switch2# set interface ge-0/0/1 negotiation-options allow-remote-
loopback
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch2# show
```

```
protocols {
    oam {
        ethernet {
            link-fault-management {
                interface ge-0/0/1 {
                    negotiation-options {
                        allow-remote-loopback;
                    }
                }
            }
        }
    }
```

Verificación

in this section

- Comprobar que OAM LFM se ha configurado correctamente | **186**

Comprobar que OAM LFM se ha configurado correctamente

Propósito

Compruebe que OAM LFM se haya configurado correctamente.

Acción

Utilice el comando: `show oam ethernet link-fault-management`

```
user@switch1#
```

Salida de muestra

nombre-comando

```
Interface: ge-0/0/0.0
Status: Running, Discovery state: Send Any
Peer address: 00:19:e2:50:3b:e1
Flags:Remote-Stable Remote-State-Valid Local-Stable 0x50
Remote entity information:
Remote MUX action: forwarding, Remote parser action: forwarding
Discovery mode: active, Unidirectional mode: unsupported
Remote loopback mode: supported, Link events: supported
Variable requests: unsupported
```

Significado

Cuando el resultado muestra la dirección MAC y el estado de detección es , significa que OAM LFM se ha configurado correctamente.`Send Any`

chapter label in part4

Administración de errores de conectividad OAM Ethernet para conmutadores

in this chapter

- Descripción de la administración de errores de conectividad OAM Ethernet para conmutadores | 187
- Configurar la administración de errores de conectividad OAM Ethernet (procedimiento de CLI) | 190
- Ejemplo: Configurar la administración de errores de conectividad OAM Ethernet en conmutadores de la serie EX | 197

Descripción de la administración de errores de conectividad OAM Ethernet para conmutadores

in this section

- Limitaciones de CFM en conmutadores EX4600 | 189
- Limitaciones de CFM en conmutadores de las series QFX5120, QFX5200 y QFX5210 | 190

La especificación IEEE 802.1ag proporciona administración de errores de conectividad Ethernet (CFM). CFM supervisa las redes Ethernet que pueden comprender una o más instancias de servicio para detectar errores de conectividad que comprometan la red.

Las principales características de CFM son:

- Monitoreo de fallos mediante el protocolo de verificación de continuidad. Este es un protocolo de detección de vecinos y comprobación de estado que descubre y mantiene adyacencias en el nivel de VLAN.
- Descubrimiento de rutas y comprobación de errores mediante el protocolo linktrace.

- Aislamiento de errores mediante el protocolo de circuito cerrado.

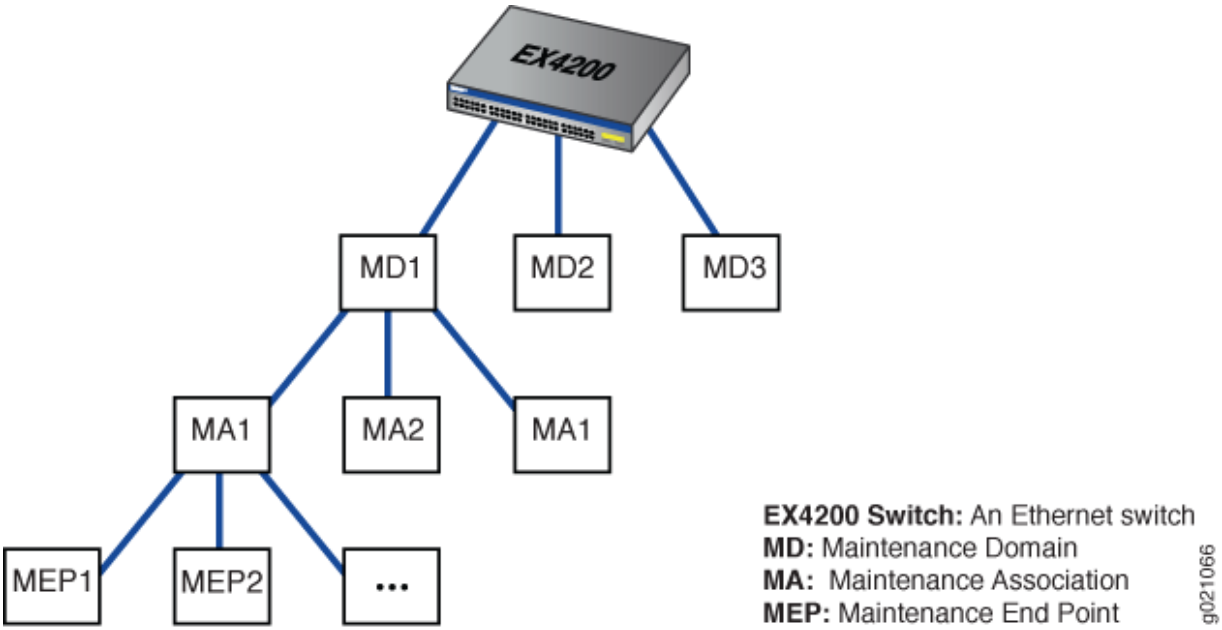
CFM divide la red de servicio en varios dominios administrativos. Por ejemplo, los operadores, proveedores y clientes pueden formar parte de diferentes dominios administrativos. Cada dominio administrativo se mapea en un dominio de mantenimiento que proporciona suficiente información para realizar su propia gestión, evitando así brechas de seguridad y haciendo posible el monitoreo de extremo a extremo.

En un dominio de mantenimiento CFM, cada instancia de servicio se denomina asociación de mantenimiento. Una asociación de mantenimiento puede considerarse como una malla completa de puntos finales de asociación de mantenimiento (MEP) que tienen características similares. Los eurodiputados son entidades activas de CFM que generan y responden a los mensajes de protocolo CFM. También hay un punto intermedio de mantenimiento (MIP), que es una entidad CFM similar al MEP, pero más pasiva (los MIP solo responden a los mensajes CFM).

Cada dominio de mantenimiento está asociado a un nivel de dominio de mantenimiento del 0 al 7. La asignación de niveles se basa en la jerarquía de la red, donde a los dominios externos se les asigna un nivel superior al de los dominios internos. Configure los puntos finales del cliente para que tengan el nivel de dominio de mantenimiento más alto. El nivel de dominio de mantenimiento es un parámetro obligatorio que indica las relaciones de anidamiento entre varios dominios de mantenimiento. El nivel está incrustado en cada trama CFM. Los mensajes del CFM dentro de un nivel determinado son procesados por los eurodiputados en ese mismo nivel.

Para habilitar CFM en una interfaz Ethernet, debe configurar dominios de mantenimiento, asociaciones de mantenimiento y puntos finales de asociación de mantenimiento (MEP). Figura 17 en la página 189 muestra las relaciones entre los dominios de mantenimiento, los puntos finales de asociación de mantenimiento (MEP) y los puntos intermedios de mantenimiento (MIP) configurados en un conmutador.

Figura 17: Relación entre los MEP, los MIP y los niveles de dominio de mantenimiento



Limitaciones de CFM en conmutadores EX4600

A partir de Junos OS versión 18.3R1, Junos OS proporciona compatibilidad con CFM en EX4600. La compatibilidad con CFM en EX4600 tiene las siguientes limitaciones:

- El soporte CFM se proporciona a través de software que utiliza filtros. Esto puede afectar la escalabilidad.
- No se admite el modo Motor de reenvío de paquetes en línea (PFE). En el modo PFE en línea, puede delegar el procesamiento de administración periódica de paquetes (PPM) al motor de reenvío de paquetes (PFE), lo que da como resultado un manejo de paquetes más rápido y el intervalo CCM admitido es de 10 milisegundos.
- No se admite la supervisión del rendimiento (OAM del servicio Ethernet ITU-T Y.1731).
- No se admite un intervalo CCM inferior a 1 segundo.
- CFM no se admite en interfaces enrutadas ni en interfaces Ethernet agregadas (lag).
- No se admite la función media MIP, para dividir la funcionalidad MIP en dos segmentos unidireccionales para mejorar la cobertura de red.
- No se apoya al eurodiputado UP.
- El número total de sesiones de CFM admitidas es 20.

Limitaciones de CFM en conmutadores de las series QFX5120, QFX5200 y QFX5210

A partir de Junos OS versión 18.4R1, Junos OS ofrece compatibilidad CFM en conmutadores QFX5200 y conmutadores QFX5210. A partir de Junos OS versión 19.4R1, Junos OS proporciona compatibilidad CFM en conmutadores QFX5120. La compatibilidad con CFM en conmutadores de las series QFX5120, QFX5200 y QFX5210 tiene las siguientes limitaciones:

- El soporte CFM se proporciona a través de software que utiliza filtros. Esto puede afectar la escalabilidad.
- No se admite el modo Motor de reenvío de paquetes en línea (PFE). En el modo PFE en línea, puede delegar el procesamiento de administración periódica de paquetes (PPM) al motor de reenvío de paquetes (PFE), lo que da como resultado un manejo de paquetes más rápido y el intervalo CCM admitido es de 10 milisegundos.
- No se admite la supervisión del rendimiento (OAM del servicio Ethernet ITU-T Y.1731).
- No se admite un intervalo CCM inferior a 1 segundo.
- CFM no se admite en interfaces enrutadas ni en interfaces Ethernet agregadas (lag).
- No se admite la función media MIP, para dividir la funcionalidad MIP en dos segmentos unidireccionales para mejorar la cobertura de red.
- No se apoya al eurodiputado UP.
- El número total de sesiones de CFM admitidas es 20.

VÍNCULOS RELACIONADOS

Guía de configuración de interfaces de red de Junos OS

Configurar la administración de errores de conectividad OAM Ethernet (procedimiento de CLI)

in this section

- Creación del dominio de mantenimiento | **191**
- Configuración de la mitad de la función MIP del dominio de mantenimiento | **192**

- Creación de una asociación de mantenimiento | 193
- Configuración del protocolo de comprobación de continuidad | 193
- Configuración de un extremo de asociación de mantenimiento | 194
- Configuración de un perfil de acción de administración de errores de conectividad | 196
- Configuración del protocolo Linktrace | 196

Las interfaces Ethernet en los conmutadores Ethernet de la serie EX de Juniper Networks y Junos OS de Juniper Networks para los conmutadores de la serie EX admiten el estándar IEEE 802.1ag para la operación, administración y gestión (OAM). La especificación IEEE 802.1ag proporciona administración de errores de conectividad Ethernet (CFM).

NOTA: Esta función no se admite en conmutadores EX4300 en interfaces Ethernet agregadas (LAG).

En este tema se describen estas tareas:

Creación del dominio de mantenimiento

Un dominio de mantenimiento comprende entidades de red como operadores, proveedores y clientes. Para habilitar la administración de errores de conectividad (CFM) en una interfaz Ethernet, debe crear dominios de mantenimiento, asociaciones de mantenimiento y MEP.

Para crear un dominio de mantenimiento:

1. Especifique un nombre para el dominio de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set maintenance-domain domain-name
```

2. Especifique un formato para el nombre de dominio de mantenimiento. Si especifica , no se configura ningún nombre:`none`
   - Una cadena de caracteres ASCII simple
   - Un formato de servicio de nombres de dominio (DNS)
   - Una dirección MAC (Media Access Control) más un identificador de dos octetos en el intervalo del 0 al 65.535

- none

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@switch# set name-format format
```

Por ejemplo, para especificar el formato de nombre como dirección MAC más un identificador de dos octetos:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@switch# set name-format mac+2oct
```

3. Configure el nivel de dominio de mantenimiento, que se utiliza para indicar la relación de anidamiento entre este dominio y otros dominios. Utilice un valor del 0 al 7:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@switch# set level level
```

> **NOTA**: Las entradas de visualización de configuración en la lista de dominios de mantenimiento de CFM son "ordenadas por sistema" en lugar de "ordenadas por usuario".

Configuración de la mitad de la función MIP del dominio de mantenimiento

> **NOTA**: La función media MIP (MHF) no se admite en conmutadores EX4600, QFX5200 y QFX5210.

La media función MIP (MHF) divide la funcionalidad del punto intermedio de asociación de mantenimiento (MIP) en dos segmentos unidireccionales, mejora la visibilidad con una configuración mínima y mejora la cobertura de red al aumentar el número de puntos que se pueden monitorear. MHF amplía la capacidad de monitoreo al responder a mensajes de circuito cerrado y rastreo de vínculos para ayudar a aislar las fallas. Siempre que se configure un MIP, el valor de la mitad de la función MIP para todos los dominios y asociaciones de mantenimiento debe ser el mismo.

Para configurar la función media MIP:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@switch# set mip-half-function  (none | default | explicit)
```

Creación de una asociación de mantenimiento

En un dominio de mantenimiento CFM, cada instancia de servicio se denomina asociación de mantenimiento.

Para crear una asociación de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@switch# set maintenance-association ma-name
```

NOTA: Las entradas de visualización de configuración en la lista de dominios de mantenimiento de CFM son "ordenadas por sistema" en lugar de "ordenadas por usuario".

Configuración del protocolo de comprobación de continuidad

El protocolo de comprobación de continuidad se utiliza para la detección de errores por un punto final de asociación de mantenimiento (MEP) dentro de una asociación de mantenimiento. El MEP envía periódicamente mensajes de multidifusión de verificación de continuidad. Los eurodiputados receptores utilizan los mensajes de verificación de continuidad (MCP) para construir una base de datos de eurodiputados de todos los eurodiputados de la asociación de mantenimiento.

Para configurar el protocolo de comprobación de continuidad:

1. Habilite el protocolo de comprobación de continuidad:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name]
user@switch# set continuity-check
```

2. Especifique el intervalo de retención de comprobación de continuidad. El intervalo de espera es el número de minutos que se deben esperar antes de vaciar la base de datos MEP si no se producen actualizaciones. El valor predeterminado es 10 minutos.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name continuity-check]
user@switch# set hold-interval number
```

3. Especifique el intervalo CCM. El intervalo es el tiempo entre la transmisión de los MCPs. Puede especificar 10 minutos (10 m), 1 minuto (1 m), 10 segundos (10 segundos), 1 segundo (1s), 100 milisegundos (100 ms) o 10 milisegundos (10 ms).

> **NOTA**: En los conmutadores EX4600, QFX5200 y QFX5210, no se admite un intervalo CCM inferior a 1 segundo.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name continuity-check]
user@switch# set interval number
```

4. Especifique el número de MCPs (es decir, unidades de datos de protocolo) que se pueden perder antes de que el MEP se marque como inactivo. El número predeterminado de unidades de datos de protocolo (PDU) es 3.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name continuity-check]
user@switch# set loss-threshold number
```

Configuración de un extremo de asociación de mantenimiento

Para configurar un punto de conexión de asociación de mantenimiento:

1. Especifique un ID para el MEP. El valor puede ser del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name]
user@switch# set mep mep-id]
```

2. Habilite la detección automática del extremo de mantenimiento si desea que el MEP acepte mensajes de comprobación de continuidad (CCM) de todos los MEP remotos de la misma asociación de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id
user@switch# set auto-discovery
```

3. Puede especificar que los paquetes CFM (MCP) se transmitan sólo en una dirección para el MEP, es decir, que la dirección se establezca de modo que los MCPs se transmitan únicamente desde (no hacia) la interfaz configurada en este MEP.`down`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@switch# set direction down
```

4. Especifique la interfaz lógica a la que está conectado el MEP. Puede ser una interfaz de acceso o una interfaz troncal. Si especifica una interfaz troncal, la VLAN asociada a esa interfaz debe tener un ID de VLAN.

> **NOTA**: No puede asociar una interfaz de acceso que pertenezca a varias VLAN con el MEP.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@switch# set interface interface-name
```

5. Puede configurar un MEP remoto del cual se esperan los MCPs. Si la detección automática no está habilitada, el MEP remoto debe configurarse con la instrucción.`mep` Si el MEP remoto no está configurado bajo la instrucción, los MCPs del MEP remoto se tratan como errores.`mep`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name
maintenance-association ma-name mep mep-id]
user@switch# set remote-mep mep-id
```

Configuración de un perfil de acción de administración de errores de conectividad

Puede configurar un perfil de acción y especificar la acción que debe realizarse cuando se produzca alguno de los eventos configurados. Como alternativa, puede configurar un perfil de acción y especificar acciones predeterminadas cuando falle la conectividad con un MEP remoto.

Para configurar un perfil de acción:

1. Especifique un nombre para un perfil de acción:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set action-profile profile-name
```

2. Configure la acción del perfil de acción:

```
[edit protocols oam ethernet connectivity-fault-management action-profile profile-name]
user@switch# set action interface-down
```

3. Configure uno o más eventos en el perfil de acción, cuya ocurrencia desencadenará la acción correspondiente a realizar:

```
[edit protocols oam ethernet connectivity-fault-management action-profile profile-name]
user@switch# set event event
```

   Consulte Guía de configuración de interfaces de red de Junos OS.

Configuración del protocolo Linktrace

El protocolo linktrace se utiliza para el descubrimiento de rutas entre un par de puntos de mantenimiento. Los mensajes de Linktrace son activados por un administrador utilizando el comando para verificar la ruta entre un par de MEP bajo la misma asociación de mantenimiento.`traceroute` Los mensajes de seguimiento de enlaces también se pueden utilizar para comprobar la ruta entre un MEP y un MIP en el mismo dominio de mantenimiento.

Para configurar el protocolo linktrace:

1. Configure el temporizador de antigüedad de la ruta de seguimiento de enlaces. Si no se recibe respuesta a una solicitud de seguimiento de enlaces, las entradas de solicitud y respuesta se eliminan después de que caduque el temporizador de antigüedad:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set linktrace age time
```

2. Configure el número de entradas de respuesta de linktrace que se almacenarán por solicitud de linktrace:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set linktrace path-database-size path-database-size
```

VÍNCULOS RELACIONADOS

Guía de configuración de interfaces de red de Junos OS

Ejemplo: Configurar la administración de errores de conectividad OAM Ethernet en conmutadores de la serie EX

in this section

- Requisitos | 197
- Descripción general y topología | 198
- Configuración de la administración de errores de conectividad Ethernet OAM en el conmutador 1 | 198
- Configuración de la administración de errores de conectividad OAM Ethernet en el conmutador 2 | 200
- Verificación | 202

Las interfaces Ethernet de los conmutadores de la serie EX y Junos OS para los conmutadores de la serie EX admiten el estándar IEEE 802.1ag para la operación, administración y gestión (OAM). La especificación IEEE 802.1ag proporciona administración de errores de conectividad Ethernet (CFM).

En este ejemplo se describe cómo habilitar y configurar OAM CFM en una interfaz Gigabit Ethernet:

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 10.2 o posterior para conmutadores serie EX
- Dos conmutadores de la serie EX conectados por un vínculo Gigabit Ethernet punto a punto

Descripción general y topología

CFM se puede utilizar para monitorear el vínculo físico entre dos conmutadores. En el ejemplo siguiente, dos conmutadores están conectados por un vínculo punto a punto de Gigabit Ethernet. El vínculo entre estos dos conmutadores se supervisa mediante CFM.

Configuración de la administración de errores de conectividad Ethernet OAM en el conmutador 1

in this section

- Configuración rápida de CLI | **198**
- Procedimiento | **198**
- Resultados | **199**

Configuración rápida de CLI

Para configurar rápidamente Ethernet OAM CFM, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
set name-format character-string
set maintenance-domain private level 0
set maintenance-association private-ma
set continuity-check hold-interval 1s
```

Procedimiento

Procedimiento paso a paso

Para habilitar y configurar CFM de OAM en el conmutador 1:

1. Especifique el formato de nombre de dominio de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
user@switch1# set name-format character-string
```

2. Especifique el nombre de dominio de mantenimiento y el nivel de dominio de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch1# set maintenance-domain private level 0
```

3. Cree una asociación de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain private]
user@switch1# set maintenance-association private-ma
```

4. Habilite el protocolo de comprobación de continuidad y especifique el intervalo de retención de comprobación de continuidad:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain private
maintenance-association private-ma]
user@switch1# set continuity-check hold-interval 1s
```

5. Configure el punto de conexión de la asociación de mantenimiento (MEP):

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain private
maintenance-association private-ma]
user@switch1# set mep 100 interface ge-1/0/1 auto-discovery direction down
```

Resultados

Compruebe los resultados de la configuración.

```
[edit]
user@switch1 > show
```

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
```

```
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 100 {
                            interface ge-1/0/1;
                            auto-discovery;
                            direction down;
                        }
                }
            }
        }
    }
```

Configuración de la administración de errores de conectividad OAM Ethernet en el conmutador 2

in this section

- Configuración rápida de CLI | 200
- Procedimiento | 201
- Resultados | 202

Configuración rápida de CLI

Para configurar rápidamente Ethernet OAM CFM, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
set name-format character-string
set maintenance-domain private level 0
set maintenance-association private-ma
set continuity-check hold-interval 1s
```

Procedimiento

Procedimiento paso a paso

La configuración del conmutador 2 refleja la del conmutador 2.

1. Especifique el formato de nombre de dominio de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch2# set name-format character-string
```

2. Especifique el nombre de dominio de mantenimiento y el nivel de dominio de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch2# set maintenance-domain private level 0
```

3. Cree una asociación de mantenimiento:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain private]
user@switch2# set maintenance-association private-ma
```

4. Habilite el protocolo de comprobación de continuidad y especifique el intervalo de retención de comprobación de continuidad:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain private
maintenance-association private-ma]
user@switch2# set continuity-check hold-interval 1s
```

5. Configurar el punto de conexión de la asociación de mantenimiento (MEP)

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain private
maintenance-association private-ma]
user@switch2# set mep 200 interface ge-0/2/5 auto-discovery direction down
```

Resultados

Compruebe los resultados de la configuración.

```
[edit]
user@switch2 > show
```

```
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain private {
                    level 0;
                    maintenance-association private-ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 200 {
                            interface ge-0/2/5;
                            auto-discovery;
                            direction down;
                        }
                }
            }
        }
    }
```

Verificación

in this section

- Comprobación de que OAM CFM se ha configurado correctamente | **203**

Para confirmar que la configuración funcione correctamente, realice las siguientes tareas:

Comprobación de que OAM CFM se ha configurado correctamente

Propósito

Compruebe que OAM CFM se haya configurado correctamente.

Acción

Utilice el comando:`show oam ethernet connectivity-fault-management interfaces detail`

```
user@switch1# show oam ethernet connectivity-fault-management interfaces detail
```

Salida de muestra

nombre-comando

```
Interface name: ge-1/0/1.0, Interface status: Active, Link status: Up
  Maintenance domain name: private, Format: string, Level: 0
    Maintenance association name: private-ma, Format: string
    Continuity-check status: enabled, Interval: 1ms, Loss-threshold: 3 frames
    MEP identifier: 100, Direction: down, MAC address: 00:90:69:0b:4b:94
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : yes
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : yes
    Statistics:
      CCMs sent                                    : 76
      CCMs received out of sequence                : 0
      LBMs sent                                    : 0
      Valid in-order LBRs received                 : 0
      Valid out-of-order LBRs received             : 0
      LBRs received with corrupted data            : 0
      LBRs sent                                    : 0
      LTMs sent                                    : 0
      LTMs received                                : 0
      LTRs sent                                    : 0
      LTRs received                                : 0
      Sequence number of next LTM request          : 0
```

```
Remote MEP count: 2
  Identifier    MAC address        State    Interface
   2001     00:90:69:0b:7f:71       ok    ge-0/2/5.0
```

Significado

Cuando el resultado muestra que el estado de la comprobación de continuidad es y muestra detalles del MEP remoto, significa que la administración de errores de conectividad (CFM) se ha configurado correctamente.`enabled`

VÍNCULOS RELACIONADOS

- Guía de configuración de interfaces de red de Junos OS

chapter label in part5

Retardo de trama Ethernet

in this chapter

- Mediciones de retardo de trama Ethernet en conmutadores | 205
- Configurar interfaces MEP en conmutadores para que admitan mediciones de retardo de trama Ethernet (procedimiento de CLI) | 208
- Configuración de mediciones de retardo de trama Ethernet unidireccional en conmutadores (procedimiento de CLI) | 209
- Configurar un perfil de iterador en un conmutador (procedimiento de CLI) | 209
- Activar una sesión de medición de retardo de trama Ethernet en un conmutador | 211
- Configuración de mediciones de retardo de trama Ethernet bidireccional en conmutadores (procedimiento de CLI) | 212

Mediciones de retardo de trama Ethernet en conmutadores

in this section

- Mediciones de retardo de trama Ethernet | 206
- Tipos de mediciones de retardo de trama Ethernet | 206
- Limitaciones | 207

En muchos casos, un proveedor de servicios podría estar sujeto a sanciones impuestas por regulación, estatuto o contrato si el rendimiento de la red no está dentro de los límites establecidos para el servicio. Un objetivo clave de rendimiento es el retraso, junto con su pariente cercano, la variación del retraso (a menudo llamada *fluctuación*). Algunas aplicaciones (como la transferencia masiva de archivos) funcionarán igual de bien con retrasos altos en toda la red y variaciones de retardo alto, mientras que otras aplicaciones (como voz) solo pueden funcionar con retrasos bajos y estables. Muchas redes invocan protocolos o funciones disponibles en la capa 3 (la capa de paquetes) o superior para medir los retrasos de la red y la fluctuación vínculo por enlace. Sin embargo, cuando la red consta de muchos

vínculos Ethernet, hay pocos protocolos y funciones disponibles en la capa 2 (la capa de trama) que permitan a los enrutadores y conmutadores medir el retraso y la fluctuación de tramas. Aquí es donde la capacidad de configurar y monitorear el retardo de trama Ethernet es útil.

Este tema incluye:

Mediciones de retardo de trama Ethernet

Puede realizar mediciones de retardo de trama Ethernet (denominadas ETH-DM en las especificaciones de Ethernet) en conmutadores Ethernet de la serie EX de Juniper Networks. Esta función permite configurar instrucciones de operación, administración y mantenimiento (OAM) bajo demanda para la medición del retardo de trama y la variación de retardo de trama (jitter). Puede configurar la medición del retardo de trama Ethernet en modo unidireccional o bidireccional (ida y vuelta) para recopilar estadísticas de retardo de trama simultáneamente de varias sesiones. La medición de retardo de trama Ethernet proporciona un control preciso a los operadores para activar la medición de retardo en un servicio determinado y se puede utilizar para monitorear SLA.

La medición del retardo de trama Ethernet también recopila otra información útil, como los retrasos del peor y mejor de los casos, el retraso promedio y la variación del retraso promedio. Admite la marca de tiempo asistida por software en la dirección de recepción para mediciones de retraso. También proporciona una visualización en tiempo de ejecución de las estadísticas de retraso cuando se activa la medición de retraso bidireccional. La medición de retardo de trama Ethernet registra las últimas 100 muestras recogidas por punto final de asociación de mantenimiento remoto (MEP) o por sesión de gestión de fallos de conectividad (CFM). Puede recuperar el historial en cualquier momento utilizando comandos simples. Puede borrar todas las estadísticas de medición de retardo de trama Ethernet y los contadores de PDU. La medición del retardo de trama Ethernet es totalmente compatible con la especificación ITU-T Y.1731 ().*OAM Functions and Mechanisms for Ethernet-based Networks*

La medición del retardo de trama Ethernet utiliza la infraestructura IEEE 802.1ag CFM.

Generalmente, las mediciones de retardo de trama Ethernet se realizan de manera similar de una sesión MEP o CFM a otra. Sin embargo, estas mediciones no se realizan a los puntos intermedios de asociación de mantenimiento (MIP).

Para obtener una descripción completa de la medición del retardo de trama Ethernet, consulte los temas OAM del servicio Ethernet ITU-T Y.1731 en la Biblioteca de interfaces de red de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces.html

Tipos de mediciones de retardo de trama Ethernet

Hay dos tipos de mediciones de retardo de trama Ethernet:

- Unidireccional

- Bidireccional (ida y vuelta)

Para la medición de retardo de trama Ethernet unidireccional, cualquiera de los MEP puede enviar una solicitud para comenzar una medición de retardo unidireccional a su MEP par. Sin embargo, las estadísticas se recopilan solo en el MEP receptor. Esta función requiere que los relojes de los MEP transmisores y receptores estén sincronizados. Si estos relojes no están sincronizados, solo se calculan correctamente los valores de variación de retardo unidireccional y variación de retardo promedio (y, por lo tanto, serán válidos). Utilice los comandos del MEP del receptor para mostrar estadísticas de retraso unidireccional.`show`

Para la medición de retardo de trama Ethernet bidireccional (ida y vuelta), cualquiera de los MEP puede enviar una solicitud para comenzar una medición de retardo bidireccional a su MEP par, que responde con información de marca de tiempo. Las estadísticas en tiempo de ejecución se recopilan y muestran en el MEP iniciador. No es necesario sincronizar los relojes en los diputados transmisores y receptores. Junos OS admite marcas de tiempo en tramas de respuesta a medición de retardo (DMR) para aumentar la precisión de los cálculos de retardo.

Utilice los comandos del MEP del iniciador para mostrar estadísticas de retraso bidireccional y del MEP del receptor para mostrar estadísticas de retraso unidireccional.`show`

Puede crear un perfil de iterador para transmitir periódicamente paquetes de medición de SLA en forma de tramas compatibles con ITU-Y.1731 para la medición de retardo o pérdida.

Limitaciones

A continuación se presentan algunas limitaciones con respecto al uso de la medición de retardo de trama Ethernet:

- Las mediciones de retardo de trama Ethernet solo están disponibles cuando la administración periódica distribuida de paquetes (PPM) está habilitada.
- Las estadísticas recopiladas se pierden después de un cambio elegante del motor de enrutamiento (GRES).
- Solo puede supervisar una sesión en la misma dirección MEP o MAC remota.
- La precisión se ve comprometida cuando cambia la configuración del sistema (por ejemplo, debido a la reconfiguración). Recomendamos realizar mediciones de retardo de trama Ethernet en un sistema estable.

Configurar interfaces MEP en conmutadores para que admitan mediciones de retardo de trama Ethernet (procedimiento de CLI)

La medición del retardo de trama Ethernet es una herramienta útil para proporcionar estadísticas de rendimiento o respaldar o desafiar los acuerdos de nivel de servicio (SLA). De forma predeterminada, la medición de retardo de trama Ethernet utiliza software para el sellado de tiempo y los cálculos de retardo. Puede configurar un conmutador de la serie EX para realizar y mostrar mediciones de retardo de trama Ethernet en interfaces Ethernet. Los conmutadores admiten marcas de tiempo asistidas por software.

Antes de empezar a configurar interfaces MEP para admitir mediciones de retardo de trama Ethernet en conmutadores, asegúrese de tener:

- Administración de errores de conectividad (CFM) de operación, administración y mantenimiento (OAM) configurada correctamente
- Administración periódica de paquetes distribuida (PPM) habilitada (PPM distribuida está habilitada de forma predeterminada)

Para configurar interfaces MEP en conmutadores que admitan mediciones de retardo de trama Ethernet:

Active la medición del retardo de trama Ethernet emitiendo el comando de modo operativo.**monitor ethernet delay-measurement** En este comando, debe especificar un tipo de medida (medida unidireccional o bidireccional) y debe especificar la dirección MAC de unidifusión del MEP par o su identificador numérico.
Opcionalmente, también puede especificar los siguientes parámetros:

- Número de tramas para enviar al eurodiputado par ()**count *count***
- Número de segundos que hay que esperar entre tramas de envío ()**wait *time***
- Valor de prioridad del marco de solicitud de medición de retardo ()**priority *value***
- Tamaño de los datos en la TLV de datos del paquete de solicitud ()**size *value***
- Supresión de la inserción del ID de sesión TLV en el paquete de solicitud ()**no-session-id-tlv**

```
user@switch> monitor ethernet delay-measurement  maintenance-domain md-name  maintenance-
association ma-name  one-way mep remote-mep-id count count wait time priority value size value
no-session-id-tlv
```

Configuración de mediciones de retardo de trama Ethernet unidireccional en conmutadores (procedimiento de CLI)

La medición del retardo de trama Ethernet es una herramienta útil para proporcionar estadísticas de rendimiento o respaldar o desafiar los acuerdos de nivel de servicio (SLA). Puede configurar las mediciones de retardo de fotogramas en modo unidireccional o bidireccional (ida y vuelta) para recopilar estadísticas de retardo de fotograma. Para la medición del retardo de trama Ethernet unidireccional, es necesario sincronizar los relojes de los eurodiputados locales y remotos. Sin embargo, la sincronización del reloj no es necesaria para la medición del retardo de trama Ethernet bidireccional.

Antes de empezar a configurar mediciones de retardo de trama Ethernet unidireccional en dos conmutadores de la serie EX, asegúrese de contar con:

- Se configuró correctamente la administración de errores de conectividad (CFM) de operación, administración y mantenimiento (OAM) en ambos conmutadores
- Se sincronizaron los relojes del sistema de ambos conmutadores

Para configurar mediciones de retardo de trama Ethernet unidireccional:

1. Configure el dominio de mantenimiento, la asociación de mantenimiento y el ID de MEP en ambos conmutadores.
2. Desde cualquiera de los conmutadores, inicie una medición de retardo de trama Ethernet unidireccional:

```
user@switch> monitor ethernet delay-measurement  maintenance-domain md-name  maintenance-
association ma-name  one-way mep remote-mep-id count count wait time
```

Puede ver el resultado en el otro conmutador:

```
user@switch> show oam ethernet connectivity-fault-management delay-statistics maintenance-domain
md-name  maintenance-association ma-name local-mep mep-id remote-mep mep-id
```

Configurar un perfil de iterador en un conmutador (procedimiento de CLI)

La medición de retardo de trama Ethernet proporciona un control preciso a los operadores para activar la medición de retardo en un servicio determinado y se puede utilizar para supervisar acuerdos de nivel de servicio (SLA). Puede crear un perfil de iterador con sus parámetros para transmitir periódicamente

paquetes de medición de SLA en forma de tramas compatibles con ITU-Y.1731 para la medición de retardo bidireccional.

Para crear un perfil de iterador:

1. Especifique un nombre para un perfil de iterador de SLA, por ejemplo, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@switch# edit sla-iterator-profiles i1
```

2. (Opcional) Configure el tiempo de ciclo, que es el tiempo (en milisegundos) entre las transmisiones consecutivas de tramas SLA.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@switch# set cycle-time cycle-time-value
```

3. (Opcional) Configure el período de iteración, que indica el número máximo de ciclos por iteración (el número de conexiones registradas en un iterador no puede superar este valor).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@switch# set iteration-period iteration-period-value
```

4. Configure el tipo de medición como medición de retardo bidireccional.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@switch# set measurement-type two-way-delay
```

5. (Opcional) Configure el peso de cálculo para el retraso.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@switch# set calculation-weight delay delay-value
```

6. (Opcional) Configure el peso de cálculo para la variación del retardo.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@switch# set calculation-weight delay-variation delay-variation-value
```

7. Configure un MEP remoto con el perfil de iterador.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@switch# set sla-iterator-profiles i1
```

Activar una sesión de medición de retardo de trama Ethernet en un conmutador

Para activar la medición de retardo de trama *Ethernet* , utilice el comando operativo de medición de retardo de Ethernet de monitor y especifique los valores siguientes:

- Medición unidireccional () o bidireccional ()one-waytwo-way
- La dirección MAC () o el ID MEP () del host remotoremote-mac-addressmep
- El dominio de mantenimiento ()maintenance-domain
- La asociación de mantenimiento ()maintenance-association
- (Opcional) Cualquiera o todas estas opciones: , , , no-session-id-tlv, countsizewaitpriority

Por ejemplo:

```
user@switch> monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6
maintenance-association ma6 count 10 size 50 wait 5 no-session-id-tlv priority 1
```

Configuración de mediciones de retardo de trama Ethernet bidireccional en conmutadores (procedimiento de CLI)

La medición del retardo de trama Ethernet es una herramienta útil para proporcionar estadísticas de rendimiento o respaldar o desafiar los acuerdos de nivel de servicio (SLA). Puede configurar las mediciones de retardo de fotogramas en modo unidireccional o bidireccional (ida y vuelta) para recopilar estadísticas de retardo de fotograma. Para la medición del retardo de trama Ethernet unidireccional, es necesario sincronizar los relojes de los eurodiputados locales y remotos. Sin embargo, la sincronización del reloj no es necesaria para la medición del retardo de trama Ethernet bidireccional.

Antes de empezar a configurar mediciones bidireccionales de retardo de trama Ethernet en dos conmutadores de la serie EX, asegúrese de tener:

- Se configuró correctamente la administración de errores de conectividad (CFM) de operación, administración y mantenimiento (OAM) en ambos conmutadores

Para configurar mediciones de retardo de trama Ethernet bidireccional:

1. Configure el dominio de mantenimiento, la asociación de mantenimiento y el ID de MEP en ambos conmutadores.
2. Desde cualquiera de los conmutadores, inicie una medición bidireccional del retardo de tramas Ethernet:

```
user@switch> monitor ethernet delay-measurement  maintenance-domain md-name  maintenance-
association ma-name  two-way mep remote-mep-id count count wait time
```

Puede ver el resultado en el otro conmutador:

```
user@switch> show oam ethernet connectivity-fault-management delay-statistics maintenance-domain
md-name  maintenance-association ma-name local-mep mep-id remote-mep mep-id
```

chapter label in part6

Oam del servicio Ethernet (ITU-ty.1731) para enrutadores

in this chapter

- Visión general de OAM del servicio Ethernet ITU-T Y.1731 | 213
- Configurar sesiones de medición de retardo de trama Ethernet | 234
- Configuración de interfaces MEP para admitir mediciones de retardo de trama Ethernet | 279
- Configurar la medición de pérdida de tramas Ethernet | 281
- Configurar un perfil de iterador | 319
- Configurar mediciones de pérdida sintética Ethernet | 338
- Indicación de alarma Ethernet | 356
- Modo de transmisión en línea | 371

Visión general de OAM del servicio Ethernet ITU-T Y.1731

summary

En esta sección se describe el servicio OAM (UIT-TY.1731) y sus dos componentes principales: gestión de fallos (monitoreo, detección y aislamiento) y monitoreo del rendimiento (medición de pérdida de trama, medición de pérdida de trama sintética y medición de retardo de trama).

in this section

- Descripción general de las mediciones de retardo de trama Ethernet | 214
- Descripción general de la medición de pérdida de trama Ethernet | 221
- Medición del acuerdo de nivel de servicio | 223
- Modo bajo demanda para la medición de SLA | 223

- Modo proactivo para la medición de SLA | 224
- Descripción general del protocolo de notificación de fallos de Ethernet | 226
- Descripción general de la medición de pérdidas sintéticas de Ethernet | 227
- Escenarios para la configuración de ETH-SLM | 228
- Formato de los mensajes ETH-SLM | 229
- Transmisión de mensajes ETH-SLM | 231

Descripción general de las mediciones de retardo de trama Ethernet

in this section

- Función de medición del retardo de trama ITU-T Y.1731 | 214
- Medición unidireccional del retardo de trama Ethernet | 217
- Medición bidireccional del retardo de trama Ethernet | 218
- Elegir entre ETH-DM unidireccional y bidireccional | 220
- Restricciones para la medición del retardo de trama Ethernet | 220

Función de medición del retardo de trama ITU-T Y.1731

El estándar IEEE 802.3-2005 para operaciones, administración y mantenimiento (OAM) de Ethernet define un conjunto de mecanismos de administración de fallos de vínculo para detectar e informar errores de vínculo en una única LAN Ethernet punto a punto.

Junos OS es compatible con estándares OAM clave que proporcionan administración y supervisión automatizadas de extremo a extremo del servicio Ethernet por parte de los proveedores de servicios:

- *Estándar IEEE 802.1ag*, también conocido como "Administración de fallas de conectividad (CFM)".
- Recomendación UIT-T Y.1731, que utiliza una terminología diferente a la IEEE 802.1ag y define las características OAM del servicio Ethernet para la supervisión de fallos, el diagnóstico y la supervisión del rendimiento.

Estas capacidades permiten a los operadores ofrecer acuerdos de nivel de servicio (SLA) vinculantes y generar nuevos ingresos a partir de paquetes de servicios con garantía de tarifa y rendimiento que se adaptan a las necesidades específicas de sus clientes.

Los enrutadores de la serie ACX admiten modos proactivos y bajo demanda.

Puede configurar las capacidades de medición de pérdida de Ethernet (ETH-LM) compatible con la norma ITU-T Y.1731, medición de pérdida sintética de Ethernet (ETH-SLM) y medición de retardo de Ethernet (ETH-DM) en tarjetas de línea MPC10 y MPC11 únicamente en 20.2R2-S3 y 20.4R1 en adelante.

NOTA: Los enrutadores ACX5048 y ACX5096 solo admiten marcas de tiempo basadas en software para la medición de retardos.

Ethernet CFM

El estándar IEEE 802.1ag para la administración de errores de conectividad (CFM) define mecanismos para proporcionar garantía de servicio Ethernet de extremo a extremo en cualquier ruta, ya sea un solo vínculo o varios enlaces que atraviesan redes compuestas por varias LAN.

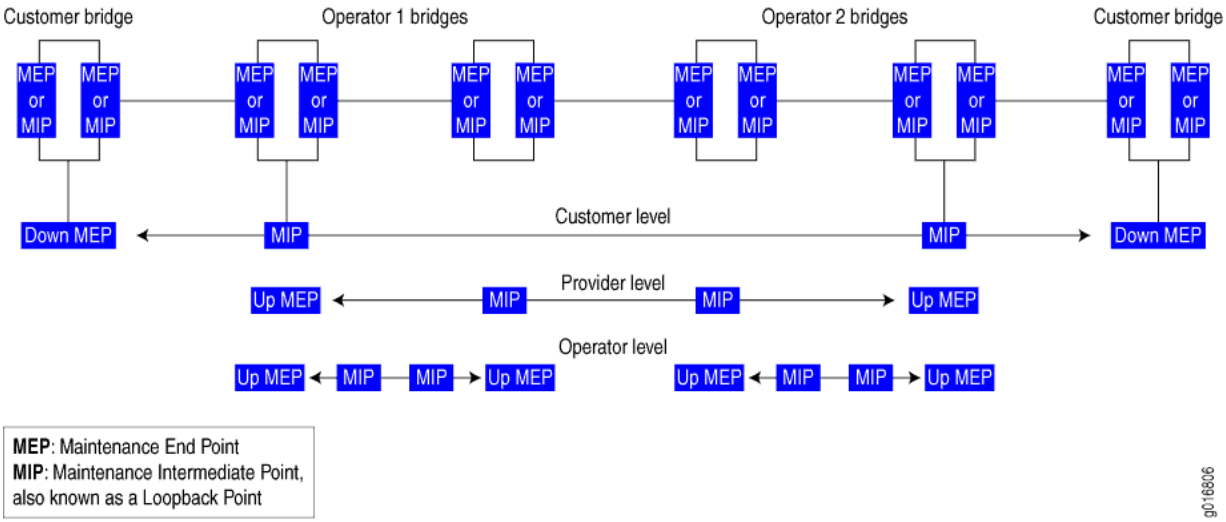
Para las interfaces Ethernet en enrutadores serie M320, MX y T, Junos OS admite los siguientes elementos clave del estándar CFM de Ethernet:

- Monitoreo de fallas mediante el protocolo de verificación de continuidad de OAM Ethernet IEEE 802.1ag
- Descubrimiento de ruta y verificación de fallas mediante el protocolo IEEE 802.1ag Ethernet OAM Linktrace
- Aislamiento de errores mediante el protocolo de bucle invertido OAM Ethernet IEEE 802.1ag

En un entorno CFM, las entidades de red, como operadores de red, proveedores de servicios y clientes, pueden formar parte de diferentes dominios administrativos. Cada dominio administrativo se asigna a un dominio de mantenimiento. Los dominios de mantenimiento se configuran con diferentes valores de nivel para mantenerlos separados. Cada dominio proporciona suficiente información para que las entidades realicen su propia administración y monitoreo de extremo a extremo, y aún así evitar violaciones de seguridad.

Figura 18 en la página 216 muestra las relaciones entre los puentes Ethernet de cliente, proveedor y operador, dominios de mantenimiento, puntos finales de asociación de mantenimiento (MEP) y puntos intermedios de mantenimiento (MIP).

Figura 18: Relación de los MEP, los MIP y los niveles de dominio de mantenimiento



NOTA: En los enrutadores de la serie ACX, los puntos intermedios de mantenimiento (MIP) solo se admiten en los enrutadores ACX5048 y ACX5096.

Medición del retardo de trama Ethernet

Dos objetivos clave de la funcionalidad OAM son medir los atributos de la calidad del servicio, como el retraso de fotogramas y la variación del retardo de fotogramas (también conocido como " fluctuación de trama"). Estas mediciones pueden permitirle identificar problemas de red antes de que los clientes se vean afectados por defectos de red.

Junos OS admite la medición del retardo de trama Ethernet entre MEP configurados en interfaces físicas o lógicas Ethernet en enrutadores de la serie MX. La medición de retardo de trama Ethernet proporciona un control preciso a los operadores para activar la medición de retardo en un servicio determinado y se puede utilizar para monitorear SLA. La medición del retardo de trama Ethernet también recopila otra información útil, como los retrasos del peor y mejor de los casos, el retraso promedio y la variación del retraso promedio. La implementación de Junos OS de la medición de retardo de trama Ethernet (ETH-DM) cumple plenamente con la Recomendación UIT-T Y.1731, Funciones y mecanismos OAM para redes basadas en Ethernet. La recomendación define los mecanismos OAM para operar y mantener la red en la capa de servicio Ethernet, que en la terminología del UIT-T se denomina "capa ETH".

Los enrutadores de la serie MX con concentradores de puerto modular (MPC) y los MPC de 10 Gigabit Ethernet con SFP+ admiten la funcionalidad ITU-T Y.1731 en VPLS para retardo y variación de retardo.

NOTA: El chasis virtual de la serie MX no admite la medición de retardo de trama (DM) de Ethernet.

Medición unidireccional del retardo de trama Ethernet

En el modo ETH-DM unidireccional, se calculan una serie de valores de retardo y variación de retardo de trama en función del tiempo transcurrido entre el momento en que se envía un fotograma de medición desde el MEP iniciador en un enrutador y el momento en que la trama se recibe en el MEP receptor en el otro enrutador.

NOTA: Los enrutadores de la serie ACX no admiten la medición unidireccional del retardo de trama de Ethernet.

Transmisión 1DM

Cuando se inicia una medición de retardo de trama unidireccional, el enrutador envía tramas 1DM (tramas que llevan la unidad de datos de protocolo (PDU) para una medición de retardo unidireccional, desde el MEP iniciador al MEP receptor a la velocidad y para el número de tramas que especifique. El enrutador marca cada trama 1DM como no elegible e inserta una marca de tiempo del tiempo de transmisión en la trama.

1DM Recepción

Cuando un MEP recibe una trama 1DM, el enrutador que contiene el MEP receptor mide el retraso unidireccional para esa trama (la diferencia entre el momento en que se recibió la trama y la marca de tiempo contenida en la propia trama) y la variación de retardo (la diferencia entre los valores de retardo actual y anterior).

Estadísticas unidireccionales de ETH-DM

El enrutador que contiene el MEP receptor almacena cada conjunto de estadísticas de retraso unidireccional en la base de datos ETH-DM. La base de datos ETH-DM recopila hasta 100 conjuntos de estadísticas para cualquier sesión determinada de CFM (par de eurodiputados pares). Puede acceder a estas estadísticas en cualquier momento mostrando el contenido de la base de datos ETH-DM.

Conteos unidireccionales de tramas ETH-DM

Cada enrutador cuenta el número de tramas ETH-DM unidireccionales enviadas y recibidas:

- Para un MEP iniciador, el enrutador cuenta el número de tramas 1DM enviadas.
- Para un MEP receptor, el enrutador cuenta el número de tramas 1DM válidas recibidas y el número de tramas 1DM no válidas recibidas.

Cada enrutador almacena los recuentos de tramas ETH-DM en la base de datos CFM. La base de datos CFM almacena estadísticas de sesión de CFM y, para las interfaces que admiten ETH-DM, cualquier trama ETH-DM cuenta. Puede acceder a los recuentos de tramas en cualquier momento mostrando la información de la base de datos CFM para las interfaces Ethernet asignadas a los eurodiputados o para los eurodiputados en sesiones CFM.

Sincronización de los relojes del sistema

La precisión de los cálculos de retardo unidireccional depende de la estrecha sincronización de los relojes del sistema en el MEP iniciador y el MEP receptor.

La precisión de la variación de retardo unidireccional no depende de la sincronización del reloj del sistema. Dado que la variación del retardo es simplemente la diferencia entre los valores consecutivos de retardo unidireccional, el período fuera de fase se elimina de los valores de fluctuación de fotogramas.

NOTA: Para una medición de retardo de trama Ethernet unidireccional determinada, los valores de retardo de trama y variación de retardo de trama solo están disponibles en el enrutador que contiene el MEP del receptor.

Medición bidireccional del retardo de trama Ethernet

En el modo bidireccional ETH-DM, los valores de retardo de trama y variación de retardo de trama se basan en la diferencia de tiempo entre el momento en que el MEP iniciador transmite una trama de solicitud y recibe una trama de respuesta del MEP que responde, restando el tiempo transcurrido en la MEP respondedora.

Transmisión DMM

Cuando se inicia una medición de retardo de trama bidireccional, el enrutador envía tramas de mensaje de medición de retardo (DMM) (tramas que llevan la PDU para una solicitud ETH-DM bidireccional) desde el MEP iniciador al MEP de respuesta a la velocidad y para el número de tramas que especifique. El enrutador marca cada trama DMM como no elegible para descarte e inserta una marca de tiempo del tiempo de transmisión en la trama.

Transmisión DMR

Cuando un MEP recibe una trama DMM, el MEP respondedor responde con una trama de respuesta de medición de retardo (DMR), que contiene información de respuesta ETH-DM y una copia de la marca de tiempo contenida en la trama DMM.

Recepción DMR

Cuando un MEP recibe un DMR válido, el enrutador que contiene el MEP mide el retraso bidireccional para esa trama en función de la siguiente secuencia de marcas de tiempo:

1. TI TxDMM
2. TR RxDMM
3. TR TxDMR
4. TI RxDMR

Un retraso de trama bidireccional se calcula de la siguiente manera:

1. [TI RxDMR – TI TxDMM] – [TR TxDMR – TRRxDMM]

El cálculo muestra que el retraso de trama es la diferencia entre el momento en que el MEP iniciador envía una trama DMM y el momento en que el MEP iniciador recibe la trama DMR asociada del MEP respondedor, menos el tiempo transcurrido en el MEP respondedor.

La variación de retardo es la diferencia entre los valores de retardo actuales y anteriores.

Estadísticas bidireccionales de ETH-DM

El enrutador que contiene el MEP del iniciador almacena cada conjunto de estadísticas de retraso bidireccional en la base de datos ETH-DM. La base de datos ETH-DM recopila hasta 100 conjuntos de estadísticas para cualquier sesión determinada de CFM (par de eurodiputados pares). Puede acceder a estas estadísticas en cualquier momento mostrando el contenido de la base de datos ETH-DM.

Conteos bidireccionales de tramas ETH-DM

Cada enrutador cuenta el número de tramas bidireccionales ETH-DM enviadas y recibidas:

- Para un MEP iniciador, el enrutador cuenta el número de tramas DMM transmitidas, el número de tramas DMR válidas recibidas y el número de tramas DMR no válidas recibidas.
- Para un MEP que responde, el enrutador cuenta el número de tramas DMR enviadas.

Cada enrutador almacena los recuentos de tramas ETH-DM en la base de datos CFM. La base de datos CFM almacena estadísticas de sesión de CFM y, para las interfaces que admiten ETH-DM, cualquier trama ETH-DM cuenta. Puede acceder a los recuentos de tramas en cualquier momento mostrando la información de la base de datos CFM para las interfaces Ethernet asignadas a los eurodiputados o para los eurodiputados en sesiones CFM.

> **NOTA**: Para una determinada medición de retardo de trama Ethernet bidireccional, los valores de retardo de trama y variación de retardo de trama solo están disponibles en el enrutador que contiene el MEP del iniciador.

Elegir entre ETH-DM unidireccional y bidireccional

La medición de retardo de trama unidireccional requiere que los relojes del sistema en el MEP iniciador y el MEP del receptor estén estrechamente sincronizados. La medición bidireccional del retardo de fotogramas no requiere la sincronización de los dos sistemas. Si no es práctico que los relojes estén sincronizados, las mediciones de retardo de fotogramas bidireccionales son más precisas.

Cuando dos sistemas están físicamente cerca el uno del otro, sus valores de retardo unidireccional son muy altos en comparación con sus valores de retardo bidireccional. La medición de retardo unidireccional requiere que la temporización de los dos sistemas se sincronice a un nivel muy granular, y los enrutadores de la serie MX actualmente no admiten esta sincronización granular.

Restricciones para la medición del retardo de trama Ethernet

Se aplican las siguientes restricciones a la función de medición de retardo de trama Ethernet:

- La función ETH-DM no se admite en pseudocables de interfaz conmutada por etiquetas (LSI).

  La función ETH-DM es compatible con interfaces Ethernet agregadas.

- La marca de tiempo asistida por hardware para tramas ETH-DM en la ruta de recepción solo se admite para interfaces MEP en DPC mejorados y DPC de cola mejorada en enrutadores de la serie MX. Para obtener información sobre la marca de tiempo asistida por hardware, consulte Directrices para configurar enrutadores para admitir una sesión de ETH-DM y habilitar la opción de marca de tiempo asistida por hardware."Directrices para configurar enrutadores que admitan una sesión de ETH-DM" en la página 235"Configurar sesiones de medición de retardo de trama Ethernet" en la página 234

- Las mediciones de retardo de trama Ethernet sólo se pueden activar cuando el demonio de administración periódica de paquetes distribuidos () está habilitado.`ppm` Para obtener más información acerca de esta limitación, consulte Directrices para configurar enrutadores para admitir una sesión ETH-DM y asegurarse de que ppm distribuida no esté deshabilitada."Directrices para configurar

enrutadores que admitan una sesión de ETH-DM" en la página 235"Configuración de enrutadores para admitir una sesión ETH-DM" en la página 245

- Solo puede supervisar una sesión a la vez en la misma dirección MEP o MAC remota. Para obtener más información acerca de cómo iniciar una sesión de ETH-DM, consulte Inicio de una sesión de ETH-DM."Inicio de una sesión de ETH-DM" en la página 253

- Las estadísticas de ETH-DM se recopilan solo en uno de los dos enrutadores pares de la sesión de ETH-DM. Para una sesión ETH-DM unidireccional, puede mostrar estadísticas de ETH-DM de fotograma solo en el MEP del receptor, utilizando comandos específicos de ETH-DM.`show` Para una sesión bidireccional de ETH-DM, puede mostrar estadísticas de retardo de fotogramas solo en el MEP del iniciador, utilizando los mismos comandos específicos de ETH-DM.`show` Para obtener más información, consulte Administración de estadísticas de ETH-DM y Recuentos de tramas de ETH-DM."Administración de estadísticas de ETH-DM y recuentos de tramas de ETH-DM" en la página 272

- Los recuentos de tramas ETH-DM se recopilan en ambos MEP y se almacenan en las respectivas bases de datos CFM.

- Si se produce un cambio correcto del motor de enrutamiento (GRES), se perderán todas las estadísticas de ETH-DM recopiladas y los recuentos de tramas de ETH-DM se restablecerán a ceros. Por lo tanto, la recopilación de estadísticas ETH-DM y contadores de tramas ETH-DM debe reiniciarse una vez completada la conmutación. GRES permite que un enrutador con motores de enrutamiento duales cambie de un motor de enrutamiento primario a un motor de enrutamiento de respaldo sin interrupción para el reenvío de paquetes. Para obtener más información, consulte la Guía del usuario de alta disponibilidad de Junos OS.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-high-availability/high-availability.html

- La precisión de las estadísticas de retardo de fotogramas se ve comprometida cuando el sistema está cambiando (por ejemplo, debido a la reconfiguración). Recomendamos realizar mediciones de retardo de trama Ethernet en un sistema estable.

Descripción general de la medición de pérdida de trama Ethernet

Los objetivos clave de la funcionalidad OAM son medir los atributos de la calidad del servicio, como el retraso de fotogramas, la variación del retardo de fotogramas (también conocido como " *fluctuación de fotogramas*") y la pérdida de fotogramas. Estas mediciones le permiten identificar problemas de red antes de que los clientes se vean afectados por defectos de red.

Junos OS admite la medición de pérdida de tramas Ethernet (ETH-LM) entre puntos finales de asociación de mantenimiento (MEP) configurados en interfaces físicas o lógicas Ethernet en enrutadores serie MX y actualmente solo se admite para el servicio VPWS . Los operadores utilizan ETH-LM para recopilar los valores de contador aplicables a las tramas de servicio de entrada y salida. Estos contadores mantienen un recuento de tramas de datos transmitidas y recibidas entre un par de eurodiputados. La medición de la pérdida de tramas Ethernet se realiza mediante el envío de tramas con información ETH-

LM a un MEP par y, de manera similar, la recepción de tramas con información ETH-LM del MEP par. Este tipo de medición de pérdida de trama también se conoce como medición de pérdida de Ethernet de extremo único.

> **NOTA**: El chasis virtual de la serie MX no admite la medición de pérdida de tramas Ethernet (ETH-LM).

ETH-LM admite las siguientes mediciones de pérdida de fotogramas:

- Medición de pérdida de tramas del extremo cercano: medición de la pérdida de tramas asociada con las tramas de datos de entrada.
- Medición de pérdida de tramas del extremo final: medición de la pérdida de tramas asociada con las tramas de datos de salida.

> **NOTA**: La funcionalidad de medición de pérdidas proactiva y de doble extremo de ITU-T Y1731 no es compatible con los enrutadores de la serie ACX.

La función ETH-LM es compatible con interfaces Ethernet agregadas.

> **NOTA**: A partir de Junos OS versión 16.1, los resultados de la medición de pérdidas de Ethernet (ETH-LM) son inexactos cuando las PDU de gestión de errores de conectividad (CFM) y supervisión del rendimiento (PM) se reciben localmente en un punto final de mantenimiento (MEP) clasificado como perteneciente a la clase amarilla o una prioridad de pérdida de paquetes (PLP) de medio-alto. Este problema de resultados incorrectos es específico de la medición de la pérdida de Ethernet para las sesiones CFM de los eurodiputados inactivos. Las estadísticas de medición de pérdidas de Ethernet son inexactas en los siguientes escenarios:
>
> - La medición de pérdida de Ethernet está funcionando en una sesión de CFM para un MEP en estado inactivo
> - Las PDU CFM recibidas en la interfaz lógica del MEP hacia abajo se clasifican por el clasificador como amarillas o PLP medias-altas
> - Un paquete se identifica como amarillo cuando el clasificador de entrada marca el PLP como medio-alto.
>
> El problema de las discrepancias con los resultados de la medición de pérdida de Ethernet no se observa al configurar la medición de pérdida de Ethernet en modo incoloro. Para evitar este

problema de resultados de medición de pérdidas inexactos, aprovisione todas las PDU CFM locales como verdes o con el PLP tan alto.

NOTA: A partir de Junos OS versión 16.1, la supervisión del rendimiento para la administración de errores de conectividad (mediante la inclusión de la instrucción y sus subinstrucciones en el nivel jerárquico) no se admite cuando la interfaz de red a red (NNI) o de salida es una interfaz Ethernet agregada con vínculos miembro en DPC.`performance-monitoring`[`edit protocols oam ethernet connectivity-fault-management`]

Medición del acuerdo de nivel de servicio

La medición del acuerdo de nivel de servicio (SLA) es el proceso de monitorear el ancho de banda, el retraso, la variación del retraso (*jitter*), la continuidad y la disponibilidad de un servicio (E-Line o E-LAN). Le permite identificar problemas de red antes de que los clientes se vean afectados por defectos de red.

NOTA: Los servicios VPN de Ethernet se pueden clasificar en:

- Servicios peer-to-peer (servicios E-Line): los servicios de E-Line se ofrecen mediante el *servicio de cable privado virtual* (VPWS) VPN de capa 2 basado en MPLS.

- Servicios de multipunto a multipunto (servicios E-LAN): los servicios de E-LAN se ofrecen mediante el servicio de LAN privada virtual (VPLS) basado en MPLS.

Para obtener más información, consulte la Guía de configuración de VPN de Junos.

En Junos OS, las mediciones de SLA se clasifican en:

- Modo bajo demanda: en el modo bajo demanda, las mediciones se activan a través de la CLI.

- Modo proactivo: en el modo proactivo, las mediciones se activan mediante una aplicación iteradora.

Tenga en cuenta que la medición de retardo de trama Ethernet y la medición de pérdida de trama Ethernet no son compatibles con la interfaz.`ae`

Modo bajo demanda para la medición de SLA

En el modo bajo demanda, el usuario activa las mediciones a través de la CLI.

Cuando el usuario activa la medición de retardo a través de la CLI, la solicitud de medición de retardo que se genera se ajusta a los formatos de trama especificados por la norma ITU-T Y.1731. Para la medición de retraso bidireccional, el procesamiento del lado del servidor se puede delegar al motor de

reenvío de paquetes para evitar la sobrecarga en el motor de enrutamiento. Para obtener más información, consulte "Configuración de enrutadores para admitir una sesión de ETH-DM" en la página 245. Cuando el procesamiento del lado del servidor se delega al motor de reenvío de paquetes, el comando no muestra los contadores de tramas del mensaje de medición de retardo (DMM) y los contadores de tramas de respuesta de medición de retardo (DMR).`receivetransmitshow`

Cuando el usuario activa la medición de pérdidas a través de la CLI, el enrutador envía los paquetes en formato estándar junto con el TLV de medición de pérdidas. De forma predeterminada, el argumento se incluye en el paquete para permitir sesiones simultáneas de medición de pérdidas del mismo MEP local.`session-id-tlv` También puede deshabilitar el TLV del ID de sesión mediante el argumento.`no-session-id-tlv`

El ETH-LM de extremo único se utiliza para fines de operación, administración y mantenimiento bajo demanda. Un MEP envía marcos con información de solicitud ETH-LM a su MEP par y recibe marcos con información de respuesta ETH-LM de su MEP par para llevar a cabo mediciones de pérdidas. La unidad de datos de protocolo (PDU) utilizada para una solicitud ETH-LM de extremo único se denomina mensaje de medición de pérdidas (LMM) y la PDU utilizada para una respuesta ETH-LM de extremo único se denomina respuesta de medición de pérdidas (LMR).

Modo proactivo para la medición de SLA

in this section

- Mediciones de retardo y medición de pérdidas de Ethernet mediante modo proactivo | **225**

En el modo proactivo, las mediciones de SLA se activan mediante una aplicación iteradora. Un iterador está diseñado para transmitir periódicamente paquetes de medición de SLA en forma de tramas compatibles con ITU-Y.1731 para la medición bidireccional de retardo o medición de pérdidas en enrutadores de la serie MX. Este modo difiere de la medición de SLA bajo demanda, que es iniciada por el usuario. El iterador envía paquetes periódicos de solicitud de medición de retrasos o pérdidas para cada una de las conexiones registradas en él. Los iteradores se aseguran de que no se produzcan ciclos de medición al mismo tiempo para la misma conexión para evitar la sobrecarga de la CPU. Junos OS admite el modo proactivo para *VPWS*. Para que un iterador forme una adyacencia remota y sea funcionalmente operativo, el mensaje de comprobación de continuidad (CCM) debe estar activo entre las configuraciones MEP local y remota de la administración de errores de conectividad (CFM). Cualquier cambio en los parámetros de adyacencia del iterador restablece las estadísticas del iterador existentes y reinicia el iterador. Aquí, el término adyacencia se refiere a un emparejamiento de dos puntos finales (ya sea conectados directa o virtualmente) con información relevante para el entendimiento mutuo, que se utiliza para el procesamiento posterior. Por ejemplo, la adyacencia del iterador se refiere a la asociación del iterador entre los dos puntos finales de los eurodiputados.

Para cada DPC o MPC, solo se admiten 30 instancias de iterador para un valor de tiempo de ciclo de 10 milisegundos (ms). En Junos OS se admiten configuraciones de perfil de 255 iteradores y 2000 asociaciones MEP remotas.

Los iteradores con un valor de tiempo de ciclo inferior a 100 ms solo se admiten para iteradores infinitos, mientras que los iteradores con un valor de tiempo de ciclo superior a 100 ms son compatibles con iteradores finitos e infinitos. Los iteradores infinitos son iteradores que se ejecutan infinitamente hasta que el iterador se deshabilita o desactiva manualmente.

> **NOTA**: ACX5048 y ACX5096 enrutadores admiten un tiempo de ciclo de iterador de solo 1 segundo o más.

Un servicio VPWS configurado en un enrutador se supervisa para las mediciones de SLA registrando la conexión (aquí, la conexión es un par de MEP remotos y locales) en un iterador y, a continuación, iniciando la transmisión periódica de tramas de medición de SLA en esas conexiones. El servicio de extremo a extremo se identifica mediante un punto final de asociación de mantenimiento (MEP) configurado en ambos extremos.

Para la medición bidireccional de retardo y la medición de pérdidas, un iterador envía un mensaje de solicitud para la conexión en la lista (si existe) y, a continuación, envía un mensaje de solicitud para la conexión que se sondeó en el ciclo de iteración anterior. Los mensajes de solicitud consecutivos para las tramas de medición de SLA y sus respuestas ayudan a calcular la variación del retardo y la medición de pérdidas.

La transmisión de trama Y.1731 para un servicio conectado a un iterador continúa sin cesar a menos que intervenga y detenga un operador o hasta que se cumpla la condición de recuento de iteraciones. Para evitar que el iterador envíe fotogramas de medición de SLA más proactivos, el operador debe realizar una de las siguientes tareas:

- Habilite la instrucción en el nivel jerárquico `.deactivate sla-iterator-profile[edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`md-name`* `maintenance association` *`ma-name`* `mep` *`mep-id`* `remote-mep` *`mep-id`*`]`
- Aprovisionar una instrucción bajo el perfil de iterador correspondiente en el nivel jerárquico `.disable[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles` *`profile-name`*`]`

Mediciones de retardo y medición de pérdidas de Ethernet mediante modo proactivo

En la medición de retardo bidireccional, la trama del mensaje de medición de retardo (DMM) se activa a través de una aplicación de iterador. La trama DMM lleva un tipo, longitud y valor de iterador (TLV), además de los campos descritos en formato de trama estándar, y el servidor copia la trama TLV iteradora desde la trama DMM a la trama de respuesta de medición de retardo (DMR).

En el cálculo de la variación de retardo unidireccional utilizando el método de medición de retardo bidireccional, el cálculo de la variación de retardo se basa en las marcas de tiempo que están presentes en el marco DMR (y no en el fotograma 1DM). Por lo tanto, no es necesario que los relojes del lado del cliente y del lado del servidor estén sincronizados. Suponiendo que la diferencia en sus relojes permanezca constante, se espera que los resultados de la variación del retardo unidireccional sean bastante precisos. Este método también elimina la necesidad de enviar tramas 1DM separadas solo para el propósito de medición de variación de retardo unidireccional.

En el modo proactivo para la medición de pérdidas, el enrutador envía paquetes en formato estándar junto con la medición de pérdidas TLV y el iterador TLV.

Descripción general del protocolo de notificación de fallos de Ethernet

El Protocolo de notificación de errores (FNP) es un mecanismo de notificación de errores que detecta errores en las redes de transporte Ethernet punto a punto en enrutadores de la serie MX. Si un vínculo de nodo falla, FNP detecta la falla y envía mensajes FNP a los nodos adyacentes de que un circuito está inactivo. Al recibir el mensaje FNP, los nodos pueden redirigir el tráfico al circuito de protección.

NOTA: FNP solo es compatible con los servicios de E-Line.

Un servicio E-Line proporciona una conectividad Ethernet punto a punto segura entre dos interfaces de red de usuario (UNI). Los servicios E-Line son un servicio protegido y cada servicio tiene un circuito de trabajo y un circuito de protección. CFM se utiliza para monitorear las rutas de trabajo y protección. Los intervalos de CCM dan como resultado un tiempo de conmutación por error de cientos de milisegundos o unos pocos segundos. FNP proporciona detección y propagación de fallas en el circuito de servicio en menos de 50 ms y proporciona conmutación por error de 50 ms para servicios E-Line.

El enrutador MX actúa como un nodo PE y maneja los mensajes FNP recibidos en la VLAN de administración y los mensajes FNP recibidos tanto en las interfaces Ethernet como en los PW creados para el VPLS de administración. Los enrutadores de la serie MX no inician mensajes FNP y responden sólo a los mensajes FNP generados por dispositivos en la red de acceso Ethernet. FNP solo se puede habilitar en interfaces lógicas que forman parte de una instancia de enrutamiento VPLS, y ninguna interfaz física en esa instancia de enrutamiento VPLS debe tener CCM configurado. FNP solo se puede habilitar en una interfaz *lógica por interfaz* física.

Todos los servicios E-Line están configurados como circuitos de capa 2 con protección de borde. Una VLAN asociada con el circuito operativo o el circuito de protección debe asignarse a una interfaz lógica. No se admite ningún puerto troncal ni puerto de acceso en el vínculo de anillo para las VLAN utilizadas por los servicios de E-LINE. FNP no controla la interfaz lógica asociada con el circuito de protección. FNP solo controla el servicio E-Line cuyo punto de terminación no se encuentra en un nodo MX.

FNP admite el reinicio correcto y las funciones Graceful Routing Engine switchover (GRES).

SEE ALSO

Mostrar interfaz FNP Ethernet OAM

Mostrar el estado de FNP de Ethernet OAM

Mostrar mensajes FNP de Ethernet OAM

gestión de errores de conectividad

Descripción general de la medición de pérdidas sintéticas de Ethernet

La medición de pérdida sintética Ethernet (ETH-SLM) es una aplicación que permite calcular la pérdida de tramas mediante el uso de tramas sintéticas en lugar de tráfico de datos. Este mecanismo puede considerarse como una muestra estadística para aproximar el índice de pérdida de tramas del tráfico de datos. Cada punto final de la asociación de mantenimiento (MEP) realiza mediciones de pérdida de trama, lo que contribuye al tiempo no disponible.

Una pérdida de tramas del extremo cercano especifica la pérdida de tramas asociadas con las tramas de datos de entrada y una pérdida de tramas del extremo final especifica la pérdida de tramas asociada con las tramas de datos de salida. Tanto las mediciones de pérdida de fotogramas del extremo cercano como del extremo lejano contribuyen a segundos con errores graves en el extremo cercano y segundos con errores graves en el extremo lejano que se utilizan en combinación para determinar el tiempo no disponible. ETH-SLM se realiza utilizando tramas de mensajes de pérdida sintéticos (SLM) y de respuesta de pérdida sintética (SLR). ETH-SLM facilita que cada MEP realice mediciones de pérdida de tramas sintéticas de extremo cercano y lejano mediante el uso de marcos sintéticos porque un servicio bidireccional se define como no disponible si se determina que alguna de las dos direcciones no está disponible.

Existen dos tipos de medición de pérdida de fotogramas, definidos por las normas ITU-T Y.1731, ETH-LM y ETH-SLM. Junos OS solo admite ETH-SLM de un solo extremo. En el ETH-SLM de un solo extremo, cada MEP envía marcos con la información de solicitud de ETH-SLM a su MEP par y recibe marcos con información de respuesta de ETH-SLM de su MEP par para realizar mediciones de pérdida sintética. El ETH-SLM de extremo único se utiliza para OAM proactivo o bajo demanda para realizar mediciones de pérdidas sintéticas aplicables a la conexión Ethernet punto a punto. Este método permite a un MEP iniciar e informar mediciones de pérdidas de extremo final y extremo cercano asociadas con un par de MEP que forman parte del mismo grupo de entidades de mantenimiento (MEG).

NOTA: El chasis virtual de la serie MX no admite la medición de pérdidas sintéticas por Ethernet (ETH-SLM).

El ETH-SLM de un solo extremo se utiliza para realizar pruebas proactivas o bajo demanda iniciando una cantidad finita de tramas ETH-SLM en uno o varios pares MEP y recibiendo la respuesta ETH-SLM de los pares. Las tramas ETH-SLM contienen la información de ETH-SLM que se utiliza para medir e informar mediciones de pérdidas sintéticas de extremo cercano y lejano. La medición del acuerdo de

nivel de servicio (SLA) es el proceso de monitorear el ancho de banda, el retraso, la variación del retraso (*jitter*), la continuidad y la disponibilidad de un servicio. Le permite identificar problemas de red antes de que los clientes se vean afectados por defectos de red. En el modo proactivo, las mediciones de SLA se activan mediante una aplicación iteradora. Un iterador está diseñado para transmitir periódicamente paquetes de medición de SLA en forma de tramas compatibles con ITU-Y.1731 para la medición de pérdida de tramas sintéticas. Este modo difiere de la medición de SLA bajo demanda, que es iniciada por el usuario. En el modo bajo demanda, el usuario activa las mediciones a través de la CLI. Cuando el usuario activa el ETH-SLM a través de la CLI, la solicitud SLM que se genera se ajusta a los formatos de trama especificados por el estándar ITU-T Y.1731.

NOTA: Los enrutadores ACX5048 y ACX5096 admiten ETH-SLM para servicios de capa 2.

Escenarios para la configuración de ETH-SLM

in this section

- MEP ascendente en túneles MPLS | **228**
- MEP descendente en redes Ethernet | **228**

ETH-SLM mide la pérdida de fotogramas de extremo cercano y extremo entre dos eurodiputados que forman parte del mismo nivel de MEG. Puede configurar ETH-SLM para medir la pérdida sintética tanto para el MEP orientado hacia arriba o hacia arriba como para el MEP orientado hacia abajo o hacia abajo. En esta sección se describen los siguientes escenarios para el funcionamiento de ETH-SLM:

MEP ascendente en túneles MPLS

Considere un escenario en el que se configura un MEP entre las interfaces de red de usuario (UNI) de dos enrutadores de la serie MX, MX1 y MX2, en la dirección ascendente. MX1 y MX2 están conectados a través de una red central MPLS. Las mediciones de ETH-SLM se realizan entre el MEP ascendente en la ruta que une los dos enrutadores. Tanto MX1 como MX2 pueden iniciar ETH-SLM proactivo o bajo demanda, que puede medir pérdidas tanto en el extremo final como en el extremo cercano en MX1 y MX2, respectivamente. Las dos UNI se conectan mediante el *servicio de cable privado virtual* (*VPWS)* VPN de capa 2 basado en MPLS.

MEP descendente en redes Ethernet

Considere un escenario en el que se configura un MEP entre dos enrutadores de la serie MX, MX1 y MX2, en las interfaces Ethernet en la dirección descendente. MX1 y MX2 se conectan en una topología

Ethernet y el MEP descendente se configura hacia la red Ethernet. Las mediciones de ETH-SLM se realizan entre el MEP aguas abajo en la ruta que une los dos enrutadores. ETH-SLM se puede medir en la ruta entre estos dos enrutadores.

Considere otro escenario en el que un MEP está configurado en la dirección descendente y la protección de servicio para un VPWS sobre MPLS se habilita especificando una ruta de trabajo o una ruta de protección en el MEP. La protección de servicio proporciona una protección de conexión de extremo a extremo de la ruta de trabajo en caso de fallo. Para configurar la protección del servicio, debe crear dos rutas de transporte independientes: una ruta de trabajo y una ruta de protección. Puede especificar la ruta de trabajo y la ruta de protección creando dos asociaciones de mantenimiento. Para asociar la asociación de mantenimiento con una ruta de acceso, debe configurar la interfaz MEP en la asociación de mantenimiento y especificar la ruta como funcional o protegida.

En una topología de ejemplo, un enrutador de la serie MX, MX1, está conectado a otros dos enrutadores de la serie MX, MX2 y MX3, a través de un núcleo MPLS. La sesión de administración de errores de conectividad (CFM) entre MX1 y MX2 es la ruta de trabajo en el MEP y la sesión CFM entre MX1 y MX3 es la ruta de protección en el MEP. MX2 y MX3 están, a su vez, conectados en interfaces Ethernet a MX4 en la red de acceso. El MEP descendente se configura entre MX1 y MX4 que pasa por MX2 (sesión CFM de trabajo) y también entre MX1 y MX4 que pasa por MX3 (sesión CFM protegida). ETH-SLM se realiza entre estos eurodiputados posteriores. En ambos MEP descendentes, la configuración se realiza en las UNI MX1 y MX4, de manera similar a la MEP ascendente.

Formato de los mensajes ETH-SLM

in this section

- Formato SLM PDU | **229**
- Formato SLR PDU | **230**
- Formato TLV del iterador de datos | **231**

Los mensajes de pérdida sintética (SLM) admiten solicitudes de medición de pérdidas sintéticas Ethernet de extremo único (ETH-SLM). Este tema contiene las siguientes secciones en las que se describen los formatos de las unidades de datos de protocolo (PDU) de SLM, las PDU de SLR y el valor de longitud de tipo iterador de datos (TLV).

Formato SLM PDU

El formato SLM PDU es utilizado por un MEP para transmitir información SLM. Los siguientes componentes están contenidos en las PDU de SLM:

- ID MEP de origen: el ID de MEP de origen es un campo de 2 octetos en el que se utilizan los últimos 13 bits menos significativos para identificar el MEP que transmite la trama SLM. El ID MEP es único dentro del MEG.
- ID de prueba: el ID de prueba es un campo de 4 octetos establecido por el MEP transmisor y se utiliza para identificar una prueba cuando se ejecutan varias pruebas simultáneamente entre los MEP (incluidas las pruebas simultáneas a pedido y proactivas).
- TxFCf—TxFCf es un campo de 4 octetos que lleva el número de tramas SLM transmitidas por el MEP hacia su MEP par.

Los siguientes son los campos de una PDU SLM:

- Nivel MEG: nivel de dominio de mantenimiento configurado en el rango 0-7.
- Versión: 0.
- OpCode: identifica un tipo de PDU OAM. Para SLM, es 55.
- Banderas: se establece en todos los ceros.
- Desplazamiento de TLV: 16.
- ID MEP de origen: campo de 2 octetos que se utiliza para identificar al MEP que transmite la trama SLM. En este campo de 2 octetos, los últimos 13 bits menos significativos se utilizan para identificar el MEP que transmite la trama SLM. El ID MEP es único dentro del MEG.
- RESV: los campos reservados se establecen en todos los ceros.
- ID de prueba: campo de 4 octetos establecido por el MEP transmisor y que se utiliza para identificar una prueba cuando se ejecutan varias pruebas simultáneamente entre los MEP (incluidas las pruebas simultáneas a pedido y proactivas).
- TxFCf: un campo de 4 octetos que transporta el número de tramas SLM transmitidas por el MEP hacia su MEP par.
- TLV opcional: se puede incluir un TLV de datos en cualquier SLM transmitido. A los efectos de ETH-SLM, la parte de valor de los datos TLV no está especificada.
- TLV final: valor del octeto de todos los ceros.

Formato SLR PDU

El formato PDU de respuesta sintética a pérdida (SLR) es utilizado por un MEP para transmitir información SLR. Los siguientes son los campos de una PDU SLR:

- Nivel MEG: campo de 3 bits cuyo valor se copia de la última PDU SLM recibida.

- Versión: campo de 5 bits cuyo valor se copia de la última PDU de SLM recibida.
- OpCode: identifica un tipo de PDU OAM. Para SLR, se establece en 54.
- Indicadores: campo de 1 octeto copiado de la PDU de SLM.
- Desplazamiento de TLV: campo de 1 octeto copiado de la PDU de SLM.
- ID MEP de origen: campo de 2 octetos copiado de la PDU de SLM.
- ID de MEP del respondedor: campo de 2 octetos que se utiliza para identificar al MEP que transmite la trama SLR.
- ID de prueba: campo de 4 octetos copiado de la PDU de SLM.
- TxFCf: campo de 4 octetos copiado de la PDU de SLM.
- TxFCb—Un campo de 4 octetos. Este valor representa el número de fotogramas SLR transmitidos para este ID de prueba.
- TLV opcional: el valor se copia de la PDU de SLM, si está presente.
- End TLV: campo de 1 octeto copiado de la PDU de SLM.

Formato TLV del iterador de datos

La TLV del iterador de datos especifica la parte del TLV de datos de la trama de datos Y.1731. El MEP utiliza un TLV de datos cuando el MEP está configurado para medir el retraso y la variación del retraso para diferentes tamaños de fotograma. Los siguientes son los campos en un TLV de datos:

- Tipo: identifica el tipo de TLV; el valor de este tipo de TLV es Datos (3).
- Longitud: identifica el tamaño, en octetos, del campo Valor que contiene el patrón de datos. El valor máximo del campo Longitud es 1440.
- Patrón de datos: un patrón de bits arbitrario -octeto (denota longitud).*nn* El receptor lo ignora.

Transmisión de mensajes ETH-SLM

in this section

- Inicio y transmisión de solicitudes de ordenación sostenible de la tierra | **232**
- Recepción de SLM y transmisión de SLR | **233**
- Recepción de réflex | **233**

Cálculo de la pérdida de fotogramas | 234

La funcionalidad ETH-SLM puede procesar múltiples solicitudes de mensajes de pérdida sintéticos (SLM) simultáneamente entre un par de eurodiputados. La sesión puede ser una sesión de SLM proactiva o bajo demanda. Cada solicitud de SLM se identifica de forma única mediante un ID de prueba.

Un eurodiputado puede enviar solicitudes de SLM o responder a solicitudes de SLM. Una respuesta a una solicitud de SLM se denomina respuesta de pérdida sintética (SLR). Después de que un MEP determina una solicitud de SLM utilizando el ID de prueba, el MEP calcula la pérdida de tramas de extremo final y final próximo en función de la información del mensaje SLM o la unidad de datos de protocolo (PDU) de SLM.

Un MEP mantiene los siguientes contadores locales para cada ID de prueba y para cada MEP par que se supervisa en una entidad de mantenimiento para la cual se deben realizar mediciones de pérdidas:

- TxFCl: Número de tramas sintéticas transmitidas hacia el MEP par para un ID de prueba. Un MEP de origen incrementa este número para la transmisión sucesiva de tramas sintéticas con información de solicitud ETH-SLM, mientras que un MEP de destino o receptor incrementa este valor para la transmisión sucesiva de tramas sintéticas con la información SLR.
- RxFCl: número de tramas sintéticas recibidas del MEP par para un ID de prueba. Un MEP fuente incrementa este número para la recepción sucesiva de tramas sintéticas con información SLR, mientras que un MEP de destino o receptor lo incrementa para la recepción sucesiva de tramas sintéticas con información de solicitud ETH-SLM.

En las secciones siguientes se describen las fases de procesamiento de PDU SLM para determinar la pérdida de tramas sintéticas:

Inicio y transmisión de solicitudes de ordenación sostenible de la tierra

Un MEP transmite periódicamente una solicitud SLM con el campo OpCode establecido como 55. El MEP genera un ID de prueba único para la sesión, agrega el ID de MEP de origen e inicializa los contadores locales para la sesión antes del inicio de SLM. Para cada PDU SLM transmitida para la sesión (ID de prueba), se envía el contador local TxFCl en el paquete.

No se requiere sincronización del valor del ID de prueba entre los MEP iniciadores y los que responden, ya que el ID de prueba está configurado en el MEP iniciador y el MEP que responde utiliza el ID de prueba que recibe del MEP iniciador. Dado que ETH-SLM es una técnica de muestreo, es menos precisa que contar las tramas de servicio. Además, la precisión de la medición depende del número de tramas SLM utilizadas o del período de transmisión de las tramas SLM.

Recepción de SLM y transmisión de SLR

Después de que el MEP de destino recibe una trama SLM válida del MEP de origen, se genera una trama SLR y se transmite al MEP solicitante o de origen. La trama SLR es válida si el nivel MEG y la dirección MAC de destino coinciden con la dirección MAC del MEP receptor. Todos los campos de las PDU de SLM se copian de la solicitud de SLM, excepto los campos siguientes:

- La dirección MAC de origen se copia en la dirección MAC de destino y la dirección de origen contiene la dirección MAC del MEP.
- El valor del campo OpCode cambia de SLM a SLR (54).
- El ID del MEP del respondedor se rellena con el ID del MEP del eurodiputado.
- TxFCb se guarda con el valor del contador local RxFCl en el momento de la transmisión de la trama SLR.
- Cada vez que se recibe una trama SLM, se genera una trama SLR; por lo tanto, RxFCl en el respondedor es igual al número de tramas SLM recibidas y también igual al número de tramas SLR enviadas. En el MEP que responde o recibe, RxFCl es igual a TxFCl.

Recepción de réflex

Después de transmitir una trama SLM (con un valor TxFCf dado), un MEP espera recibir una trama SLR correspondiente (que lleve el mismo valor TxTCf) dentro del valor de tiempo de espera de su MEP par. Las tramas SLR que se reciben después del valor de tiempo de espera (5 segundos) se descartan. Con la información contenida en los marcos SLR, un MEP determina la pérdida de cuadro para el período de medición especificado. El período de medición es un intervalo de tiempo durante el cual el número de tramas SLM transmitidas es estadísticamente adecuado para realizar una medición con una precisión dada. Un MEP utiliza los siguientes valores para determinar la pérdida de fotogramas del extremo cercano y del extremo final durante el período de medición:

- La última vez que recibió los valores TxFCf y TxFCb del cuadro SLR y el valor RxFCl del contador local al final del período de medición. Estos valores se representan como TxFCf[tc], TxFCb[tc] y RxFCl[tc], donde tc es la hora de finalización del período de medición.
- Valores TxFCf y TxFCb del primer cuadro SLR recibido después de que comience la prueba y contador local RxFCl al comienzo del período de medición. Estos valores se representan como TxFCf[tp], TxFCb[tp] y RxFCl[tp], donde tp es la hora de inicio del período de medición.

Para cada paquete SLR que se recibe, el contador RxFCl local se incrementa en el MEP de origen o envío.

Cálculo de la pérdida de fotogramas

La pérdida de fotogramas sintéticos se calcula al final del período de medición sobre la base del valor de los contadores locales y la información del último fotograma recibido. La última trama recibida contiene los valores TxFCf y TxFCb. El contador local contiene el valor RxFCl. Con estos valores, la pérdida de fotogramas se determina mediante la siguiente fórmula:

Pérdida de tramas (extremo final) = TxFCf – TxFCb

Pérdida de tramas (casi final) = TxFCb – RxFCl

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
16.1	A partir de Junos OS versión 16.1, los resultados de la medición de pérdidas de Ethernet (ETH-LM) son inexactos cuando las PDU de gestión de errores de conectividad (CFM) y supervisión del rendimiento (PM) se reciben localmente en un punto final de mantenimiento (MEP) clasificado como perteneciente a la clase amarilla o una prioridad de pérdida de paquetes (PLP) de medio-alto.
16.1	A partir de Junos OS versión 16.1, la supervisión del rendimiento para la administración de errores de conectividad (mediante la inclusión de la instrucción y sus subinstrucciones en el nivel jerárquico) no se admite cuando la interfaz de red a red (NNI) o de salida es una interfaz Ethernet agregada con vínculos miembro en DPC.`performance-monitoring`[`edit protocols oam ethernet connectivity-fault-management`]

Configurar sesiones de medición de retardo de trama Ethernet

in this section

- Directrices para configurar enrutadores que admitan una sesión de ETH-DM | **235**
- Pautas para iniciar una sesión de ETH-DM | **237**
- Directrices para administrar las estadísticas de ETH-DM y los recuentos de fotogramas de ETH-DM | **239**
- Configuración de enrutadores para admitir una sesión ETH-DM | **245**

- Activación de una sesión de mediciones de retardo de trama Ethernet | 251
- Inicio de una sesión de ETH-DM | 253
- Ejemplo: Configuración de mediciones de retardo de trama Ethernet unidireccionales con interfaces de etiqueta única | 256
- Ejemplo: Configuración de mediciones de retardo de trama Ethernet bidireccional con interfaces de etiqueta única | 263
- Gestión de estadísticas de medición de continuidad | 269
- Visualización de estadísticas de mediciones de retardo de trama Ethernet | 271
- Administración de estadísticas de ETH-DM y recuentos de tramas de ETH-DM | 272

Utilice este tema para comprender cómo configurar sesiones de medición de retardo de trama Ethernet. Puede iniciar una sesión de medición de retardo Ethernet unidireccional o una sesión de medición de retardo Ethernet bidireccional. Además, utilice este tema para ver las estadísticas de medición de retardo y los recuentos de fotogramas.

Directrices para configurar enrutadores que admitan una sesión de ETH-DM

in this section

- Requisitos de configuración para ETH-DM | 235
- Opciones de configuración para ETH-DM | 236

Tenga en cuenta las siguientes directrices cuando configure enrutadores para admitir una sesión de medición de retardo de trama Ethernet (ETH-DM):

Requisitos de configuración para ETH-DM

Puede obtener información de ETH-DM para un vínculo que cumpla los siguientes requisitos:

- Las mediciones se pueden realizar entre puntos finales de asociación de mantenimiento par (MEP) en dos enrutadores.
- Los dos eurodiputados deben configurarse en dos interfaces físicas Ethernet o en dos interfaces lógicas Ethernet. Para obtener más información, consulte "Configuración de un MEP para generar y responder a mensajes de protocolo CFM" en la página 37.

- Los dos MEP deben configurarse, en sus respectivos enrutadores, bajo el mismo identificador de asociación de mantenimiento (MA). Para obtener más información, consulte Creación de una asociación de mantenimiento."Crear una asociación de mantenimiento" en la página 30

- En ambos enrutadores, el MA debe estar asociado con el mismo nombre de dominio de mantenimiento (MD). Para obtener más información, consulte Creación de un dominio de mantenimiento."Crear un dominio de mantenimiento" en la página 29

- En ambos enrutadores, la administración periódica de paquetes (PPM) debe ejecutarse en el motor de enrutamiento y el motor de reenvío de paquetes, que es la configuración predeterminada. Puede deshabilitar PPM solo en el motor de reenvío de paquetes. Sin embargo, la función de medición de retardo de trama Ethernet requiere que PPM distribuido permanezca habilitado en el motor de reenvío de paquetes de ambos enrutadores. Para obtener más información acerca de , consulte la Biblioteca de protocolos de enrutamiento de Junos OS para dispositivos de enrutamiento.`ppm`https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-routing/index.html

- Si el proceso PPM () está deshabilitado en el motor de reenvío de paquetes, debe volver a habilitarlo.`ppm` Volver a habilitar la distribución implica reiniciar el proceso, lo que hace que se restablezcan todas las sesiones de administración de errores de conectividad (CFM).`ppmethernet-connectivity-fault-management` Para obtener más información acerca de las sesiones CFM, consulte Configuración de la interfaz de administración local de Ethernet.

> **NOTA**: La función de medición de retardo de trama Ethernet solo se admite para MEP configurados en interfaces físicas o lógicas Ethernet en DPC en enrutadores de la serie MX. La función ETH-DM no es compatible con interfaces Ethernet agregadas ni en pseudocables LSI.

Opciones de configuración para ETH-DM

De forma predeterminada, la función ETH-DM calcula los retrasos de fotogramas utilizando una marca de tiempo basada en software de las tramas PDU de ETH-DM enviadas y recibidas por los eurodiputados en la sesión. Como opción que puede aumentar la precisión de los cálculos de ETH-DM cuando el DPC se carga con tráfico intenso en la dirección de recepción, puede habilitar la marca de tiempo asistida por hardware de tramas de sesión en la dirección de recepción.

SEE ALSO

Indicación de alarma Ethernet | 356

Modo de transmisión en línea | 371

Pautas para iniciar una sesión de ETH-DM

in this section

- Prerrequisitos de sesión de ETH-DM | **237**
- Parámetros de sesión de ETH-DM | **237**
- Restricciones para una sesión ETH-DM | **238**

Tenga en cuenta las siguientes directrices cuando se prepare para iniciar una sesión de medición de retardo de trama Ethernet (ETH-DM):

Prerrequisitos de sesión de ETH-DM

Antes de poder iniciar una sesión de ETH-DM, debe configurar dos enrutadores de la serie MX para que admitan ETH-DM mediante la definición de las dos interfaces Ethernet físicas o lógicas habilitadas para CFM en cada enrutador. Esto implica crear y configurar dominios de mantenimiento CFM, asociaciones de mantenimiento y puntos finales de asociación de mantenimiento en cada enrutador. Para obtener más información acerca de cómo habilitar CFM en una interfaz Ethernet, consulte "Creación de un dominio de mantenimiento" en la página 29.

> **NOTA**: La función de medición de retardo de trama Ethernet solo se admite para los puntos finales de asociación de mantenimiento configurados en interfaces físicas o lógicas Ethernet en DPC de enrutadores de la serie MX. La función ETH-DM no es compatible con interfaces Ethernet agregadas ni en pseudocables LSI.

Para obtener información específica acerca de la configuración de enrutadores para admitir ETH-DM, consulte Directrices para configurar enrutadores para admitir una sesión ETH-DM y Configurar enrutadores para admitir una sesión ETH-DM."Directrices para configurar enrutadores que admitan una sesión de ETH-DM" en la página 235"Configuración de enrutadores para admitir una sesión ETH-DM" en la página 245

Parámetros de sesión de ETH-DM

Puede iniciar una sesión ETH-DM unidireccional o bidireccional introduciendo el comando operativo en un enrutador que contenga un extremo del servicio para el que desea medir el retraso de tramas.`monitor ethernet delay-measurement` Las opciones de comando especifican la sesión ETH-DM en términos de los elementos CFM:

- El tipo de medición de ETH-DM (unidireccional o bidireccional) que se va a realizar.
- El servicio Ethernet para el que se va a realizar la medición de ETH-DM:
  - Dominio de mantenimiento CFM: nombre del dominio de mantenimiento (MD) existente para el que desea medir los retrasos de tramas Ethernet. Para obtener más información, consulte Creación de un dominio de mantenimiento."Crear un dominio de mantenimiento" en la página 29
  - Asociación de mantenimiento de CFM: nombre de una asociación de mantenimiento (MA) existente dentro del dominio de mantenimiento. Para obtener más información, consulte Creación de una asociación de mantenimiento."Crear una asociación de mantenimiento" en la página 30
  - Punto final de la asociación de mantenimiento remoto de CFM: la dirección MAC de unidifusión o el identificador numérico del punto final de la asociación de mantenimiento remoto (MEP), la interfaz física o lógica en el enrutador remoto que reside en el MD especificado y cuyo nombre se denomina en la MA especificada, con la que realizar la sesión de ETH-DM. Para obtener más información, consulte Configuración de un MEP para generar y responder a mensajes de protocolo CFM."Configurar un MEP para generar y responder a mensajes de protocolo CFM" en la página 37
- Especificaciones opcionales:
  - Recuento: puede especificar el número de solicitudes ETH-DM que desea enviar para esta sesión de medición de retardo de fotogramas. El rango es de 1 a 65.535 cuadros. El valor predeterminado es 10 fotogramas.

    NOTE: Aunque puede activar la recopilación de retardo de tramas para hasta 65.535 solicitudes ETH-DM a la vez, un enrutador almacena solo las últimas 100 estadísticas de retraso de tramas por sesión CFM (par de MEP pares).
  - Intervalo de trama: puede especificar el número de segundos que transcurrirán entre las transmisiones de tramas ETH-DM. El valor predeterminado es 1 segundo.

Para obtener información más detallada sobre los parámetros que puede especificar para iniciar una sesión de ETH-DM, consulte la descripción del comando operativo en el Explorador de CLI.`monitor ethernet delay-measurement`https://www.juniper.net/documentation/content-applications/cli-explorer/junos/

Restricciones para una sesión ETH-DM

Las siguientes restricciones se aplican a una sesión ETH-DM:

- No puede ejecutar varias sesiones ETH-DM simultáneas con la misma dirección MEP o MAC remota.
- Para una sesión ETH-DM determinada, puede recopilar información de retardo de fotogramas para un máximo de 65 535 fotogramas.

- Para una sesión determinada de CFM (par de eurodiputados pares), la base de datos ETH-DM almacena un máximo de 100 estadísticas, y las estadísticas más antiguas se "envejecen" a medida que se recopilan estadísticas más nuevas para ese par de eurodiputados.
  - Para las mediciones de retardo unidireccional recopiladas dentro de la misma sesión de CFM, las 100 estadísticas ETH-DM más recientes se pueden recuperar en cualquier momento en el enrutador en el que se define el MEP del receptor.
  - Para las mediciones de retardo bidireccional recopiladas dentro de la misma sesión de CFM, las 100 estadísticas ETH-DM más recientes se pueden recuperar en cualquier momento en el enrutador en el que se define el MEP del iniciador.

  Dependiendo del número de tramas intercambiadas en las sesiones individuales de ETH-DM, la base de datos de ETH-DM puede contener estadísticas recopiladas a través de múltiples sesiones de ETH-DM.
- Si se produce un cambio correcto del motor de enrutamiento (GRES), se perderán todas las estadísticas de ETH-DM recopiladas y los recuentos de tramas de ETH-DM se restablecerán a ceros. GRES permite que un enrutador con motores de enrutamiento duales cambie de un motor de enrutamiento primario a un motor de enrutamiento de respaldo sin interrupción para el reenvío de paquetes. Para obtener más información, consulte la Guía del usuario de alta disponibilidad de Junos OS.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-high-availability/high-availability.html
- La precisión de los datos de retardo de trama se ve comprometida cuando el sistema está cambiando (como por reconfiguración). Recomendamos realizar mediciones de retardo de trama Ethernet en un sistema estable.

SEE ALSO

Monitoree la medición de retardo de Ethernet

Directrices para administrar las estadísticas de ETH-DM y los recuentos de fotogramas de ETH-DM

in this section

- Estadísticas de ETH-DM | **240**
- Recuperación de estadísticas de ETH-DM | **242**
- Recuentos de tramas ETH-DM | **242**
- Recuperación de recuento de tramas ETH-DM | **244**

Estadísticas de ETH-DM

Las estadísticas de retardo de trama Ethernet son los valores de retardo de trama y variación de retardo de trama determinados por el intercambio de tramas que contienen unidades de datos de protocolo (PDU) ETH-DM.

- Para una sesión ETH-DM unidireccional, las estadísticas se recopilan en una base de datos ETH-DM en el enrutador que contiene el MEP receptor. Para obtener una descripción detallada de la medición de retardo de trama Ethernet unidireccional, incluido el intercambio de tramas PDU de retardo unidireccional, consulte "Descripción general de mediciones de retardo de trama Ethernet" en la página 214.

- Para una sesión bidireccional de ETH-DM, las estadísticas se recopilan en una base de datos de ETH-DM en el enrutador que contiene el MEP iniciador. Para obtener una descripción detallada de la medición del retardo de trama Ethernet bidireccional, incluido el intercambio de tramas PDU de retardo bidireccional, consulte Descripción general de las mediciones de retardo de trama Ethernet."Descripción general de las mediciones de retardo de trama Ethernet" en la página 214

Una base de datos CFM almacena estadísticas relacionadas con CFM y, para interfaces Ethernet compatibles con ETH-DM, las 100 estadísticas de ETH-DM recopiladas más recientemente para ese par de eurodiputados. Puede ver las estadísticas de ETH-DM mediante el formulario o del comando para mostrar las estadísticas de CFM del MEP que recopila las estadísticas de ETH-DM que desea ver.`delay-statisticsmep-statisticsshow oam ethernet connectivity-fault-management`

Tabla 13 en la página 240 describe las estadísticas de ETH-DM calculadas en una sesión de ETH-DM.

Tabla 13: Estadísticas de ETH-DM

Nombre del campo	Descripción de campo
`One-way delay (µsec)`†	Para una sesión ETH-DM unidireccional, el retardo de fotograma, en microsegundos, se recoge en el MEP receptor. Para mostrar estadísticas de retardo de fotogramas para una sesión ETH-DM unidireccional determinada, utilice el formulario o del comando en el MEP del receptor para esa sesión.`delay-statisticsmep-statisticsshow oam ethernet connectivity-fault-management`

Tabla 13: Estadísticas de ETH-DM *(Continued)*

Nombre del campo	Descripción de campo
`Two-way delay (µsec)`	Para una sesión bidireccional de ETH-DM, el retardo de fotograma, en microsegundos, se recoge en el MEP iniciador. Cuando se inicia una medición de retardo de fotograma bidireccional, la salida de la CLI muestra cada marca de tiempo de recepción de trama DMR y la variación de retardo y retraso de trama DMM correspondientes recopilados a medida que avanza la sesión. Para mostrar estadísticas de retardo de fotogramas para una sesión ETH-DM bidireccional determinada, utilice el formulario o del comando en el MEP del iniciador para esa sesión.`delay-statisticsmep-statisticsshow oam ethernet connectivity-fault-management`
`Average delay`†	Cuando se inicia una medición de retardo de fotograma bidireccional, el resultado de la CLI incluye una visualización en tiempo de ejecución del retardo de fotograma bidireccional promedio entre las estadísticas recopiladas solo para la sesión ETH-DM. Cuando se muestran estadísticas de ETH-DM mediante un comando, el campo muestra los retrasos promedio de un solo sentido y de dos fotogramas entre todas las estadísticas de ETH-DM recopiladas en el nivel de sesión de CFM.`showAverage delay` Por ejemplo, supongamos que inicia dos sesiones unidireccionales de ETH-DM de 50 cuentas cada una, una después de la otra. Si, una vez completadas ambas sesiones de medición, utiliza un comando para mostrar 100 estadísticas de ETH-DM para esa sesión de CFM, el campo muestra el retraso de fotograma promedio entre las 100 estadísticas.`showAverage delay`
`Average delay variation`†	Cuando se inicia una medición de retardo de fotograma bidireccional, el resultado de la CLI incluye una visualización en tiempo de ejecución de la variación media del retardo de fotograma bidireccional entre las estadísticas recopiladas solo para la sesión ETH-DM. Cuando se muestran estadísticas de ETH-DM mediante un comando, el campo muestra las variaciones medias de retardo unidireccional y de dos fotogramas entre todas las estadísticas de ETH-DM recopiladas en el nivel de sesión de CFM.`showAverage delay variation`

Tabla 13: Estadísticas de ETH-DM *(Continued)*

Nombre del campo	Descripción de campo
`Best-case delay`†	Cuando se inicia una medición de retardo de fotograma bidireccional, el resultado de la CLI incluye una visualización en tiempo de ejecución del valor de retardo de fotograma bidireccional más bajo entre las estadísticas recopiladas solo para la sesión ETH-DM. Cuando se muestran estadísticas de ETH-DM mediante un comando, el campo muestra los retrasos de fotogramas unidireccionales y bidireccionales más bajos entre todas las estadísticas de ETH-DM recopiladas en el nivel de sesión de CFM.`showBest case delay`
`Worst-case delay`†	Cuando se inicia una medición de retardo de fotograma bidireccional, el resultado de la CLI incluye una visualización en tiempo de ejecución del valor de retardo de fotograma bidireccional más alto entre las estadísticas recopiladas solo para la sesión ETH-DM. Cuando se muestran estadísticas de ETH-DM mediante un comando, el campo muestra los retrasos de fotogramas unidireccionales y bidireccionales más altos entre todas las estadísticas recopiladas en el nivel de sesión CFM.`showWorst case delay`

†Cuando se inicia una medición de retardo de fotograma unidireccional, la salida de la CLI se muestra ("no disponible") para este campo.`NA` Las estadísticas unidireccionales de ETH-DM se recopilan en el MEP remoto (receptor). Las estadísticas para una sesión ETH-DM unidireccional dada solo están disponibles mostrando estadísticas de CFM para el MEP receptor.

Recuperación de estadísticas de ETH-DM

En el MEP receptor para una sesión unidireccional, o en el MEP iniciador para una sesión bidireccional, puede mostrar todas las estadísticas de ETH-DM recopiladas en un nivel de sesión CFM mediante los siguientes comandos operativos:

- `show oam ethernet connectivity-fault-management delay-statistics maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `<local-mep` *`mep-id`*`> <remote-mep` *`mep-id`*`> <count` *`count`*`>`
- `show oam ethernet connectivity-fault-management mep-statistics maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `<local-mep` *`mep-id`*`> <remote-mep` *`mep-id`*`> <count` *`count`*`>`

Recuentos de tramas ETH-DM

El número de tramas PDU ETH-DM intercambiadas en una sesión ETH-DM se almacena en la base de datos CFM de cada enrutador.

Tabla 14 en la página 243 describe los recuentos de tramas ETH-DM recopilados en una sesión de ETH-DM.

Tabla 14: Recuentos de tramas ETH-DM

Nombre del campo	Descripción de campo
`1DMs sent`	Número de tramas PDU de medición de retardo unidireccional (1DM) enviadas al MEP par en esta sesión. Almacenado en la base de datos CFM del MEP iniciando una medición de retardo de trama unidireccional.
`Valid 1DMs received`	Número de tramas 1DM válidas recibidas. Almacenado en la base de datos CFM del MEP que recibe una medición de retardo de trama unidireccional.
`Invalid 1DMs received`	Número de tramas 1DM no válidas recibidas. Almacenado en la base de datos CFM del MEP que recibe una medición de retardo de trama unidireccional.
`DMMs sent`	Número de tramas PDU del mensaje de medición de retardo (DMM) enviadas al MEP par en esta sesión. Almacenado en la base de datos CFM del MEP iniciando una medición de retardo de trama bidireccional.
`DMRs sent`	Número de tramas de respuesta de medición de retardo (DMR) enviadas (en respuesta a un DMM recibido). Almacenado en la base de datos CFM del MEP que responde a una medición de retardo de trama bidireccional.
`Valid DMRs received`	Número de tramas DMR válidas recibidas. Almacenado en la base de datos CFM del MEP iniciando una medición de retardo de trama bidireccional.

Tabla 14: Recuentos de tramas ETH-DM *(Continued)*

Nombre del campo	Descripción de campo
`Invalid DMRs received`	Número de tramas DMR no válidas recibidas. Almacenado en la base de datos CFM del MEP iniciando una medición de retardo de trama bidireccional.

Recuperación de recuento de tramas ETH-DM

Cada enrutador cuenta el número de tramas ETH-DM enviadas o recibidas y almacena los recuentos en una base de datos CFM.

Recuentos de tramas almacenados en bases de datos CFM

Puede mostrar los recuentos de tramas ETH-DM para los MEP asignados a interfaces Ethernet especificadas o para MEP especificados en sesiones CFM mediante los siguientes comandos operativos:

- `( | )show oam ethernet connectivity-fault-management interfacesdetailextensive`
- `show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `<local-mep` *`mep-id`*`> <remote-mep` *`mep-id`*`>`

Conteos unidireccionales de tramas ETH-DM

Para una sesión ETH-DM unidireccional, las estadísticas de retraso se recopilan solo en el MEP receptor, pero los recuentos de fotogramas se recopilan en ambos MEP. Como se indica en , los recuentos unidireccionales de tramas ETH-DM se cuentan desde la perspectiva de cada enrutador en la sesión:Tabla 14 en la página 243

- En el MEP iniciador, el enrutador cuenta el número de tramas 1DM enviadas.
- En el MEP receptor, el enrutador cuenta el número de tramas 1DM válidas recibidas y el número de tramas 1DM no válidas recibidas.

También puede ver los recuentos de tramas ETH-DM unidireccionales (para un MEP de receptor) mediante el comando para mostrar estadísticas unidireccionales y recuentos de tramas juntas.`show oam ethernet connectivity-fault-management mep-statistics`

Conteos bidireccionales de tramas ETH-DM

Para una sesión bidireccional de ETH-DM, las estadísticas de retraso se recopilan solo en el MEP iniciador, pero los recuentos de fotogramas se recopilan en ambos MEP. Como se indica en , los recuentos bidireccionales de tramas ETH-DM se cuentan desde la perspectiva de cada enrutador en la sesión:Tabla 14 en la página 243

- En el MEP del iniciador, el enrutador cuenta el número de tramas DMM enviadas, las tramas DMR válidas recibidas y las tramas DMR no válidas recibidas.
- En el MEP de respuesta, el enrutador cuenta el número de tramas DMR enviadas.

También puede ver los recuentos bidireccionales de tramas ETH-DM (para un MEP del iniciador) mediante el comando para mostrar estadísticas bidireccionales y recuentos de tramas juntos.`show oam ethernet connectivity-fault-management mep-statistics`

SEE ALSO

> *Estadísticas claras de administración de fallos de conectividad Ethernet OAM*
>
> *Mostrar estadísticas MEP de conectividad Ethernet de OAM*
>
> *Mostrar estadísticas de retraso en la administración de fallas de la conectividad Ethernet de OAM*
>
> *Mostrar interfaces de administración de fallos de conectividad Ethernet de OAM*
>
> *Mostrar base de datos MEP de conectividad Ethernet de OAM*

Configuración de enrutadores para admitir una sesión ETH-DM

in this section

- Configuración de interfaces MEP | **245**
- Asegurarse de que las ppm distribuidas no estén deshabilitadas | **247**
- Habilitación de la opción de marca de tiempo asistida por hardware | **249**
- Configuración de la opción de procesamiento del lado del servidor | **250**

Configuración de interfaces MEP

Antes de poder iniciar una sesión de medición de retardo de trama Ethernet en un servicio Ethernet, debe configurar dos enrutadores de la serie MX para que admitan ETH-DM.

Para configurar una interfaz Ethernet en un enrutador de la serie MX para que admita ETH-DM:

1. En cada enrutador, configure dos interfaces Ethernet físicas o lógicas conectadas por una VLAN. La siguiente configuración es típica de las interfaces lógicas de etiqueta única:

```
[edit interfaces]
interface {
    ethernet-interface-name {
        vlan-tagging;
        unit logical-unit-number {
            vlan-id vlan-id; # Both interfaces on this VLAN
        }
    }
}
```

   Ambas interfaces utilizarán el mismo ID de VLAN.

2. En cada enrutador, adjunte MEPs pares a las dos interfaces. La siguiente configuración es típica:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md-name { # On both routers
                level number;
                maintenance-association ma-name { # On both routers
                    continuity-check {
                        interval 100ms;
                        hold-interval 1;
                    }
                    mep mep-id { # Attach to VLAN interface
                        auto-discovery;
                        direction (up | down);
                        interface interface-name;
                        priority number;
                    }
                }
            }
        }
    }
}
```

Asegurarse de que las ppm distribuidas no estén deshabilitadas

De forma predeterminada, el proceso de administración de paquetes () del período del enrutador ejecuta sesiones distribuidas al motor de reenvío de paquetes además del motor de enrutamiento.ppm Este proceso es responsable de la transmisión periódica de paquetes en nombre de sus diversos procesos cliente, como la detección de reenvío bidireccional (BFD), y también recibe paquetes en nombre de los procesos cliente.

Además, maneja el procesamiento periódico sensible al tiempo y realiza procesos tales como el envío de paquetes específicos del proceso y la recopilación de estadísticas.ppm Con los procesos que se ejecutan distribuidos tanto en el motor de enrutamiento como en el motor de reenvío de paquetes, puede ejecutar procesos como BFD en el motor de reenvío de paquetes.ppm

Se requieren ppm distribuidas para ETH-DM

La medición del retardo de trama Ethernet requiere que permanezca distribuido al motor de reenvío de paquetes.ppm Si no se distribuye a los motores de reenvío de paquetes de ambos enrutadores, las marcas de tiempo de trama ETH-DM PDU y las estadísticas de ETH-DM no son válidas.ppm

Antes de iniciar ETH-DM, debe comprobar que la siguiente instrucción de configuración NO está presente:

```
[edit]
routing-options {
     ppm {
        no-delegate-processing;
    }
}
```

Si el procesamiento distribuido está deshabilitado (como se muestra en la estrofa anterior) en cualquiera de los enrutadores, debe volver a habilitarlo para poder usar la función ETH-DM.ppm

Procedimiento para garantizar que las ppm distribuidas no estén deshabilitadas

Para asegurarse de que la distribución no esté deshabilitada en un enrutador:ppm

1. Muestra la configuración de administración de procesamiento de paquetes (PPM) para determinar si la distribución está deshabilitada.ppm

- En el ejemplo siguiente, distribuido está habilitado en el enrutador.`ppm` En este caso, no es necesario modificar la configuración del enrutador:

```
[edit]
user@host# show routing-options
ppm;
```

- En el ejemplo siguiente, distribuido está deshabilitado en el enrutador.`ppm` En este caso, debe continuar con el paso 2 para modificar la configuración del enrutador:

```
[edit]
user@host show routing-options
ppm {
    no-delegate-processing;
}
```

2. Modifique la configuración del enrutador para volver a habilitar la distribución y reinicie el proceso de administración de errores de conectividad OAM Ethernet SOLO SI la distribución está deshabilitada (como se determinó en el paso anterior).`ppmppm`

   a) Antes de continuar, haga los preparativos necesarios para la posible pérdida de conectividad en el enrutador.

      Reiniciar el proceso tiene el siguiente efecto en la red:`ethernet-connectivity-fault-management`

      - Se restablecen todas las sesiones de administración de errores de conectividad (CFM).
      - Todas las solicitudes ETH-DM en el enrutador terminan.
      - Todas las estadísticas y recuentos de fotogramas de ETH-DM se restablecen a 0.

   b) Modifique la configuración del enrutador para volver a habilitar los archivos `.ppm` Por ejemplo:

```
[edit]
user@host# delete routing-options ppm no-delegate-processing
```

   c) Confirme la configuración actualizada del enrutador. Por ejemplo:

```
[edit]
user@host# commit and-quit
commit complete
exiting configuration mode
```

d) Para reiniciar el proceso de administración de errores de conectividad de OAM de Ethernet, ingrese el comando de modo operativo.`restart ethernet-connectivity-fault-management <gracefully | immediately | soft>` Por ejemplo:

```
user@host> restart ethernet-connectivity-fault-management
Connectivity fault management process started, pid 9893
```

Las sesiones de administración de errores de conectividad (CFM) funcionan en modo centralizado a través de interfaces AE de forma predeterminada. La supervisión del rendimiento (PM) del Y.1731 se admite en sesiones CFM centralizadas en interfaces de AE. Además, la distribución de la sesión CFM a través de interfaces AE a tarjetas de línea se admite desde Junos OS versión 13.3. Para habilitar la distribución de sesiones CFM y operar en modo centralizado, incluya la instrucción en el nivel jerárquico .`ppm delegate-processing[edit routing-options ppm]` El mecanismo que permite la distribución de sesiones CFM a través de interfaces AE proporciona la infraestructura subyacente para admitir interfaces PM sobre AE. Además, la administración periódica de paquetes (PPM) maneja el procesamiento periódico sensible al tiempo y realiza procesos tales como el envío de paquetes específicos del proceso y la recopilación de estadísticas. Con los procesos PPM ejecutándose distribuidos tanto en el motor de enrutamiento como en el motor de reenvío de paquetes, puede ejecutar procesos de supervisión del rendimiento en el motor de reenvío de paquetes.

SEE ALSO

> *Administración periódica de paquetes*
>
> *Descripción de la administración periódica de paquetes en enrutadores de la serie MX*

Habilitación de la opción de marca de tiempo asistida por hardware

De forma predeterminada, la medición de retardo de tramas Ethernet utiliza software para marcar el tiempo de las tramas ETH-DM transmitidas y recibidas. En el caso de las interfaces Ethernet, puede utilizar opcionalmente la temporización de hardware para ayudar en la marca de tiempo de las tramas ETH-DM recibidas a fin de aumentar la precisión de las mediciones de retardo.

La habilitación de la marca de tiempo asistida por hardware de las tramas recibidas puede aumentar la precisión de los cálculos de ETH-DM cuando el DPC se carga con tráfico pesado en la dirección de recepción.

A partir de Junos OS versión 20.4R1, de forma predeterminada, la asistencia de hardware se utiliza para marcar la hora de tramas de retardo de trama Ethernet en tarjetas de línea serie MX basadas en AFT, incluso si no está configurado.`hardware-assisted-timestamping`

Para habilitar la asistencia de hardware de medición de retardo de trama Ethernet en la ruta de recepción, incluya la instrucción en el nivel de jerarquía:`hardware-assisted-timestamping`[`edit protocols oam ethernet connectivity-fault-management performance-monitoring`]

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            performance-monitoring {
                hardware-assisted-timestamping;
            }
        }
    }
}
```

SEE ALSO

> *Marca de tiempo asistida por hardware*

Configuración de la opción de procesamiento del lado del servidor

Puede delegar el procesamiento del lado del servidor (tanto para la medición de retardo bidireccional como para la medición de pérdidas) al motor de reenvío de paquetes para evitar la sobrecarga en el motor de enrutamiento. De forma predeterminada, el procesamiento del lado del servidor lo realiza el motor de enrutamiento.

Para configurar la opción de procesamiento del lado del servidor:

1. En el modo de configuración, vaya al siguiente nivel de jerarquía:

```
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Configure la opción de procesamiento del lado del servidor.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set delegate-server-processing
```

3. Compruebe la configuración.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# show
performance-monitoring {
    delegate-server-processing;
}
```

SEE ALSO

delegate-server-processing

VÍNCULOS RELACIONADOS

Descripción de la administración periódica de paquetes en enrutadores de la serie MX

Modo de transmisión en línea | 371

Activación de una sesión de mediciones de retardo de trama Ethernet

Antes de que se puedan mostrar las estadísticas de medición del retardo de trama de Ethernet, deben recopilarse. Para activar la medición del retardo de trama Ethernet, utilice el comando operativo.`monitor ethernet delay-measurement (one-way | two-way) (`*`remote-mac-address`*`) maintenance-domain `*`name`*` maintenance-association `*`ma-id`*` [count `*`count`*`] [wait `*`time`*`]`

Los campos de este comando se describen en .Tabla 15 en la página 251

Tabla 15: Supervisar parámetros de comando de retardo de Ethernet

Parámetro	Rango de parámetros	Description
o bien`one-way`|`two-way`	NA	Realice una medición de retraso unidireccional o bidireccional (ida y vuelta).
remote-mac-address	Dirección MAC de unidifusión	Envíe tramas de medición de retardo a la dirección MAC de unidifusión de destino (utilice el formato xx:xx:xx:xx:xx:xx). No se admiten direcciones MAC de multidifusión.

Tabla 15: Supervisar parámetros de comando de retardo de Ethernet *(Continued)*

Parámetro	Rango de parámetros	Description
`mep` *`identifier`*	1–8191	Identificador MEP que se va a utilizar para la medición. Se utiliza la dirección MAC descubierta para este identificador MEP.
`maintenance-domain` *`name`*	Nombre de MD existente	Especifica un dominio de mantenimiento (MD) existente que se usará para la medición.
`maintenance-association` *`ma-id`*	Identificador de MA existente	Especifica un identificador de asociación de mantenimiento (MA) existente que se utilizará para la medición.
`count` *`count`*	1–65535 (valor predeterminado: 10)	(Opcional) Especifica el número de tramas de retardo de tramas Ethernet que se van a enviar. El valor predeterminado es 10.
Esperar *time*	De 1 a 255 segundos (valor predeterminado: 1)	(Opcional) Especifica el número de segundos que se deben esperar entre fotogramas. El valor predeterminado es 1 segundo.

Si intenta supervisar retrasos en una dirección MAC inexistente, debe salir de la aplicación manualmente mediante :**^C**

```
user@host> monitor ethernet delay-measurement two-way 00:11:22:33:44:55
Two-way ETH-DM request to 00:11:22:33:44:55, Interface ge-5/2/9.0
^C
--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 0
Average delay: 0 usec, Average delay variation: 0 usec
Best case delay: 0 usec, Worst case delay: 0 usec
```

SEE ALSO

Configurar la medición de pérdida de tramas Ethernet | **281**

Inicio de una sesión de ETH-DM

in this section

- Uso del comando de medición de retardo de Ethernet del monitor | **253**
- Inicio de una sesión unidireccional de ETH-DM | **254**
- Inicio de una sesión bidireccional de ETH-DM | **255**

Uso del comando de medición de retardo de Ethernet del monitor

Después de configurar dos enrutadores serie MX para que admitan la medición de retardo de trama Ethernet UIT-T Y.1731 (ETH-DM), puede iniciar una sesión de medición de retardo de trama Ethernet unidireccional o bidireccional desde el punto final de la asociación de mantenimiento (MEP) CFM en uno de los enrutadores hasta el MEP par en el otro enrutador.

Para iniciar una sesión de ETH-DM entre el MEP local especificado y el MEP remoto especificado, introduzca el comando en modo operativo.`monitor ethernet delay-measurement` La sintaxis del comando es la siguiente:

```
monitor ethernet delay-measurement
(one-way | two-way)
maintenance-domain md-name
maintenance-association ma-name
(remote-mac-address | mep remote-mep-id)
<count frame-count>
<wait interval-seconds>
<priority 802.1p value>
<size>
<no-session-id-tlv>
<xml>
```

Para una medición de retardo de trama unidireccional, el comando muestra una visualización en tiempo de ejecución del número de tramas 1DM enviadas desde el MEP del iniciador durante esa sesión ETH-DM. Las mediciones de retardo de trama unidireccional y variación de retardo de trama de una sesión ETH-DM se recopilan en una base de datos CFM en el enrutador que contiene el MEP receptor. Puede recuperar estadísticas de ETH-DM de una base de datos CFM más adelante.

Para una medición de retardo de fotograma bidireccional, el comando muestra valores de variación de retardo de fotograma bidireccional y retardo de fotograma para cada intercambio de fotogramas de ida y

vuelta durante esa sesión ETH-DM, así como una visualización en tiempo de ejecución de información resumida útil sobre la sesión: retraso promedio, variación de retraso promedio, retraso en el mejor de los casos y retraso en el peor de los casos. Las mediciones de los valores de retardo de trama bidireccional y de variación de retardo de trama de una sesión ETH-DM se recopilan en una base de datos CFM en el enrutador que contiene el MEP del iniciador. Puede recuperar estadísticas de ETH-DM de una base de datos CFM más adelante.

> **NOTA**: Aunque puede activar la recopilación de retardo de tramas para hasta 65.535 solicitudes ETH-DM a la vez, un enrutador almacena solo las últimas 100 estadísticas de retraso de tramas por sesión CFM (par de MEP pares).

Para obtener una descripción completa del comando operativo, consulte el Explorador de CLI.`monitor ethernet delay-measurement`https://www.juniper.net/documentation/content-applications/cli-explorer/junos/

SEE ALSO

> *Monitoree la medición de retardo de Ethernet*

Inicio de una sesión unidireccional de ETH-DM

Para iniciar una sesión unidireccional de medición de retardo de trama Ethernet unidireccional, introduzca el comando desde el modo operativo y especifique el MEP del mismo nivel por su dirección MAC o por su identificador MEP.`monitor ethernet delay-measurement one-way`

Por ejemplo:

```
user@host> monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6
maintenance-association ma6 count 10
One-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

NOTA: Si intenta supervisar retrasos en una dirección MAC inexistente, debe escribir para salir explícitamente del comando y volver al símbolo del sistema de la CLI.**Ctrl** + **C**`monitor ethernet delay-measurement`

SEE ALSO

Monitoree la medición de retardo de Ethernet

Inicio de una sesión bidireccional de ETH-DM

Para iniciar una sesión bidireccional de medición de retardo de trama de Ethernet, ingrese el comando desde el modo operativo y especifique el MEP del mismo nivel por su dirección MAC o por su identificador MEP.`monitor ethernet delay-measurement two-way`

Por ejemplo:

```
user@host> monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6
maintenance-association ma6 count 10
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a Delay: 100 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 111 usec Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a Delay: 110 usec Delay variation: 1 usec
DMR received from 00:05:85:73:39:4a Delay: 119 usec Delay variation: 9 usec
DMR received from 00:05:85:73:39:4a Delay: 122 usec Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec  Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 108 usec Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

NOTA: Si intenta supervisar retrasos en una dirección MAC inexistente, debe escribir para salir explícitamente del comando y volver al símbolo del sistema de la CLI.**Ctrl** + **C**`monitor ethernet delay-measurement`

SEE ALSO

Monitoree la medición de retardo de Ethernet

VÍNCULOS RELACIONADOS

Modo de transmisión en línea | **371**

Ejemplo: Configuración de mediciones de retardo de trama Ethernet unidireccionales con interfaces de etiqueta única

En este ejemplo se utilizan dos enrutadores de la serie MX: **MX-1** y **MX-2**. La configuración crea una sesión MEP CFM inactiva en una interfaz lógica etiquetada por VLAN que conecta las dos (en el enrutador y en el enrutador).**ge-5/2/9MX-1ge-0/2/5MX-2**

NOTA: Estas no son configuraciones completas del enrutador.

Configuración en el enrutador :**MX-1**

```
[edit]
interfaces {
    ge-5/2/9 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
```

```
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 201 {
                            interface ge-5/2/9.0;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

Configuración en el enrutador :**MX-2**

```
[edit]
interfaces {
    ge-0/2/5 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
```

```
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 101 {
                            interface ge-0/2/5.0;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

Desde Enrutador , inicie una medición de retardo unidireccional a Enrutador .**MX-2MX-1**

```
user@MX-2> monitor ethernet delay-measurement one-way mep 201 maintenance-domain md6 maintenance-
association ma6 count 10
One-way ETH-DM request to 00:90:69:0a:43:94, Interface ge-0/2/5.0
1DM Frames sent : 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

Los contadores se muestran como parte de la base de datos MEP local en el enrutador .**MX-2**

```
user@MX-2> show oam ethernet connectivity-fault-management mep-database maintenance-domain md6
maintenance-domain ma6
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 101, Direction: down, MAC address: 00:90:69:0a:48:57
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-0/2/5.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                  : no
    Erroneous CCM received                        : no
    Cross-connect CCM received                    : no
    RDI sent by some MEP                          : no
  Statistics:
    CCMs sent                                     : 1590
    CCMs received out of sequence                 : 0
    LBMs sent                                     : 0
    Valid in-order LBRs received                  : 0
    Valid out-of-order LBRs received              : 0
    LBRs received with corrupted data             : 0
    LBRs sent                                     : 0
    LTMs sent                                     : 0
    LTMs received                                 : 0
    LTRs sent                                     : 0
    LTRs received                                 : 0
    Sequence number of next LTM request           : 0
    1DMs sent                                     : 10
    Valid 1DMs received                           : 0
    Invalid 1DMs received                         : 0
    DMMs sent                                     : 0
    DMRs sent                                     : 0
    Valid DMRs received                           : 0
    Invalid DMRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      201     00:90:69:0a:43:94       ok    ge-0/2/5.0
```

Las estadísticas de la base de datos MEP remota están disponibles en Enrutador .**MX-1**

```
user@MX-1> show oam ethernet connectivity-fault-management mep-database maintenance-domain md6
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 201, Direction: down, MAC address: 00:90:69:0a:43:94
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                  : no
    Erroneous CCM received                        : no
    Cross-connect CCM received                    : no
    RDI sent by some MEP                          : no
  Statistics:
    CCMs sent                                     : 1572
    CCMs received out of sequence                 : 0
    LBMs sent                                     : 0
    Valid in-order LBRs received                  : 0
    Valid out-of-order LBRs received              : 0
    LBRs received with corrupted data             : 0
    LBRs sent                                     : 0
    LTMs sent                                     : 0
    LTMs received                                 : 0
    LTRs sent                                     : 0
    LTRs received                                 : 0
    Sequence number of next LTM request           : 0
    1DMs sent                                     : 0
    Valid 1DMs received                           : 10
    Invalid 1DMs received                         : 0
    DMMs sent                                     : 0
    DMRs sent                                     : 0
    Valid DMRs received                           : 0
    Invalid DMRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      101     00:90:69:0a:48:57       ok    ge-5/2/9.0
```

El enrutador remoto también debe recopilar las estadísticas de retraso (hasta 100 por sesión) para su visualización con o .**MX-1mep-statisticsdelay-statistics**

```
user@MX-1> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md6
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1
  CCMs sent                                     : 3240
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           : 0
  1DMs sent                                     : 0
  Valid 1DMs received                           : 10
  Invalid 1DMs received                         : 0
  DMMs sent                                     : 0
  DMRs sent                                     : 0
  Valid DMRs received                           : 0
  Invalid DMRs received                         : 0

  Remote MEP identifier: 101
  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        370
      2        357
      3        344
      4        332
      5        319
      6        306
      7        294
      8        281
      9        269
      10       255
    Average one-way delay          : 312 usec
```

```
    Average one-way delay variation: 11 usec
    Best case one-way delay        : 255 usec
    Worst case one-way delay       : 370 usec
```

```
user@MX-1> show oam ethernet connectivity-fault-management delay-statistics maintenance-domain
md6
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1

  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1        370
      2        357
      3        344
      4        332
      5        319
      6        306
      7        294
      8        281
      9        269
      10       255
    Average one-way delay          : 312 usec
    Average one-way delay variation: 11 usec
    Best case one-way delay        : 255 usec
```

NOTA: Cuando dos sistemas están cerca el uno del otro, sus valores de retardo unidireccional son muy altos en comparación con sus valores de retardo bidireccional. Esto se debe a que la medición de retardo unidireccional requiere que la temporización de los dos sistemas se sincronice a un nivel muy granular y los enrutadores de la serie MX no admiten esta sincronización granular. Sin embargo, la medición de retardo bidireccional no requiere sincronización sincronizada, lo que hace que las mediciones de retardo bidireccional sean más precisas.

SEE ALSO

Guía del usuario de interfaces Ethernet para dispositivos de enrutamiento

Descripción general de las mediciones de retardo de trama Ethernet | 214
Configuración de interfaces MEP para admitir mediciones de retardo de trama Ethernet
Activación de una sesión de mediciones de retardo de trama Ethernet | 251
Visualización de estadísticas de mediciones de retardo de trama Ethernet | 271

Ejemplo: Configuración de mediciones de retardo de trama Ethernet bidireccional con interfaces de etiqueta única

En este ejemplo se utilizan dos enrutadores de la serie MX: **MX-1** y **MX-2**. La configuración crea una sesión MEP CFM inactiva en una interfaz lógica etiquetada por VLAN que conecta las dos (en el enrutador y en el enrutador).**ge-5/2/9MX-1ge-0/2/5MX-2**

> **NOTA**: Estas no son configuraciones completas del enrutador.

Configuración en el enrutador :**MX-1**

```
[edit]
interfaces {
    ge-5/2/9 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
```

```
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 201 {
                            interface ge-5/2/9.0;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

Configuración en el enrutador :**MX-2**

```
[edit]
interfaces {
    ge-0/2/5 {
        vlan-tagging;
        unit 0 {
            vlan-id 512;
        }
    }
}
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                traceoptions {
                    file eoam_cfm.log size 1g files 2 world-readable;
                    flag all;
                }
                linktrace {
                    path-database-size 255;
                    age 10s;
                }
                maintenance-domain md6 {
                    level 6;
                    maintenance-association ma6 {
```

```
                        continuity-check {
                            interval 100ms;
                            hold-interval 1;
                        }
                        mep 101 {
                            interface ge-0/2/5.0;
                            direction down;
                            auto-discovery;
                        }
                    }
                }
            }
        }
    }
}
```

Desde Enrutador , inicie una medición de retardo bidireccional a Enrutador.**MX-1MX-2**

```
user@MX-1> monitor ethernet delay-measurement two-way mep 101 maintenance-domain md6 maintenance-
association ma6 count 10
Two-way ETH-DM request to 00:90:69:0a:48:57, Interface ge-5/2/9.0
DMR received from 00:90:69:0a:48:57 Delay: 100 usec Delay variation: 0 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 8 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 0 usec
DMR received from 00:90:69:0a:48:57 Delay: 111 usec Delay variation: 19 usec
DMR received from 00:90:69:0a:48:57 Delay: 110 usec Delay variation: 1 usec
DMR received from 00:90:69:0a:48:57 Delay: 119 usec Delay variation: 9 usec
DMR received from 00:90:69:0a:48:57 Delay: 122 usec Delay variation: 3 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 30 usec
DMR received from 00:90:69:0a:48:57 Delay: 92 usec Delay variation: 0 usec
DMR received from 00:90:69:0a:48:57 Delay: 108 usec Delay variation: 16 usec

--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

Los contadores se muestran como parte de la base de datos MEP en el dominio de mantenimiento del enrutador.**MX-1MD6**

```
user@MX-1> show oam ethernet connectivity-fault-management mep-database maintenance-domain md6
Maintenance domain name: md6, Format: string, Level: 6
  Maintenance association name: ma6, Format: string
  Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
  MEP identifier: 201, Direction: down, MAC address: 00:90:69:0a:43:94
  Auto-discovery: enabled, Priority: 0
  Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
  Defects:
    Remote MEP not receiving CCM                  : no
    Erroneous CCM received                        : no
    Cross-connect CCM received                    : no
    RDI sent by some MEP                          : no
  Statistics:
    CCMs sent                                     : 894
    CCMs received out of sequence                 : 0
    LBMs sent                                     : 0
    Valid in-order LBRs received                  : 0
    Valid out-of-order LBRs received              : 0
    LBRs received with corrupted data             : 0
    LBRs sent                                     : 0
    LTMs sent                                     : 0
    LTMs received                                 : 0
    LTRs sent                                     : 0
    LTRs received                                 : 0
    Sequence number of next LTM request           : 0
    1DMs sent                                     : 0
    Valid 1DMs received                           : 0
    Invalid 1DMs received                         : 0
    DMMs sent                                     : 10
    DMRs sent                                     : 0
    Valid DMRs received                           : 10
    Invalid DMRs received                         : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
      101     00:90:69:0a:48:57       ok    ge-5/2/9.0
```

Las estadísticas MEP recopiladas se guardan (hasta 100 por MEP remoto o por sesión CFM) y se muestran como parte de las estadísticas MEP en el enrutador .**MX-1**

```
user@MX-1> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain md6
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1
  CCMs sent                                     : 3154
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 0
  Valid in-order LBRs received                  : 0
  Valid out-of-order LBRs received              : 0
  LBRs received with corrupted data             : 0
  LBRs sent                                     : 0
  LTMs sent                                     : 0
  LTMs received                                 : 0
  LTRs sent                                     : 0
  LTRs received                                 : 0
  Sequence number of next LTM request           : 0
  1DMs sent                                     : 0
  Valid 1DMs received                           : 0
  Invalid 1DMs received                         : 0
  DMMs sent                                     : 10
  DMRs sent                                     : 0
  Valid DMRs received                           : 10
  Invalid DMRs received                         : 0

  Remote MEP identifier: 101
  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
              (usec)         (usec)
      1                       100
      2                       92
      3                       92
      4                       111
      5                       110
      6                       119
      7                       122
      8                       92
      9                       92
      10                      108
    Average two-way delay          : 103 usec
```

```
    Average two-way delay variation: 8 usec
    Best case two-way delay        : 92 usec
    Worst case two-way delay       : 122 usec
```

Las estadísticas de retraso recopiladas también se guardan (hasta 100 por sesión) y se muestran como parte de las estadísticas de retraso MEP en el enrutador .**MX-1**

```
user@MX-1> show oam ethernet connectivity-fault-management delay-statistics maintenance-domain
md6
MEP identifier: 201, MAC address: 00:90:69:0a:43:94
Remote MEP count: 1

  Remote MAC address: 00:90:69:0a:48:57
    Delay measurement statistics:
    Index  One-way delay  Two-way delay
                          (usec)         (usec)
      1                      100
      2                      92
      3                      92
      4                      111
      5                      110
      6                      119
      7                      122
      8                      92
      9                      92
      10                     108
    Average two-way delay          : 103 usec
    Average two-way delay variation: 8 usec
    Best case two-way delay        : 92 usec
    Worst case two-way delay       : 122 usec
```

SEE ALSO

Guía del usuario de interfaces Ethernet para dispositivos de enrutamiento

Descripción general de las mediciones de retardo de trama Ethernet | **214**

Configuración de interfaces MEP para admitir mediciones de retardo de trama Ethernet

Activación de una sesión de mediciones de retardo de trama Ethernet | **251**

Ejemplo: Configuración de mediciones de retardo de trama Ethernet unidireccionales con interfaces de etiqueta única | **256**

Configuración de ETH-DM con interfaces sin etiquetar

Gestión de estadísticas de medición de continuidad

in this section

- Visualización de estadísticas de medición de continuidad | 269
- Estadísticas de medición de continuidad de borrado | 270

Visualización de estadísticas de medición de continuidad

in this section

- Propósito | 269
- Acción | 269

Propósito

Muestre la medición de la continuidad.

El comando se ha mejorado para mostrar estadísticas de medición de continuidad para los MEP en la asociación de mantenimiento CFM (MA) especificada dentro del dominio de mantenimiento CFM (MD) especificado.`show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md1 maintenance-association ma1`

Acción

- Para mostrar las estadísticas de ETH-DM recopiladas para los eurodiputados pertenecientes a MA y dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management delay-statistics maintenance-
domain md1 maintenance-association ma1
```

SEE ALSO

show oam ethernet connectivity-fault-management delay-statistics

Estadísticas de medición de continuidad de borrado

in this section

- Propósito | **270**
- Acción | **270**

Propósito

Borrar las estadísticas de medición de continuidad

De forma predeterminada, las estadísticas se eliminan para todos los eurodiputados conectados a interfaces habilitadas para CFM en el enrutador. Sin embargo, puede filtrar el ámbito del comando especificando un nombre de interfaz.

Acción

- Para borrar las estadísticas de medición de continuidad de todos los eurodiputados conectados a interfaces habilitadas para CFM en el enrutador:

```
user@host> clear oam ethernet connectivity-fault-management continuity-measurement
maintenance-domain md-name maintenance-association ma-name local-mep local-mep-id remote-mep
remote-mep-id
```

SEE ALSO

clear oam ethernet connectivity-fault-management continuity-measurement

VÍNCULOS RELACIONADOS

Conectividad Ethernet OAM clara-gestión de fallos continuidad-medición

Mostrar estadísticas de retraso en la administración de fallas de la conectividad Ethernet de OAM

Visualización de estadísticas de mediciones de retardo de trama Ethernet

Una vez que se han recopilado las estadísticas de medición del retardo de trama de Ethernet, se pueden mostrar.

Para recuperar las últimas 100 estadísticas de medición de retardo de trama Ethernet por MEP remoto o por sesión CFM, se proporcionan dos tipos de comandos:`show`

- Para todos los contadores de tramas OAM y estadísticas de medición de retardo de trama Ethernet
- Solo para estadísticas de medición de retardo de trama Ethernet

Para recuperar todas las estadísticas de medición de retardo de trama Ethernet para una sesión determinada, utilice el comando.`show oam ethernet connectivity-fault-management mep-statistics maintenance-domain` *`name`* `maintenance-association` *`name`* `[local-mep` *`identifier`*`] [remote-mep` *`identifier`*`] [count` *`count`*`]`

Para recuperar solo estadísticas de medición de retardo de trama Ethernet para una sesión determinada, use el comando.`show oam ethernet connectivity-fault-management delay-statistics maintenance-domain` *`name`* `maintenance-association` *`name`* `[local-mep` *`identifier`*`] [remote-mep` *`identifier`*`] [count` *`count`*`]`

> **NOTA**: La única diferencia en los dos comandos es el uso de la palabra clave y `.mep-statisticsdelay-statistics`

Los campos de estos comandos se describen en .Tabla 16 en la página 271

Tabla 16: Mostrar parámetros de comando de retardo de Ethernet

Parámetro	Rango de parámetros	Description
`maintenance-domain` *`name`*	Nombre de MD existente	Especifica un dominio de mantenimiento (MD) existente que se va a usar.
`maintenance-association` *`ma-id`*	Identificador de MA existente	Especifica un identificador de asociación de mantenimiento (MA) existente que se va a usar.
`local-mep` *`identifier`*	1–8191	Cuando se haya especificado un eurodiputado, muestre las estadísticas solo para el eurodiputado local.
`remote-mep` *`identifier`*	1–8191	Cuando se haya especificado un MEP, muestre estadísticas solo para el MEP descubierto.

Tabla 16: Mostrar parámetros de comando de retardo de Ethernet *(Continued)*

Parámetro	Rango de parámetros	Description
`count` *`count`*	1–100 (valor predeterminado:100)	Número de entradas que se van a mostrar en la tabla de resultados. De forma predeterminada, se muestran las 100 entradas, si existen.

NOTA: Para cada MEP, verá contadores de tramas para tramas de medición de retardo de trama Ethernet enviadas y recibidas siempre que se muestren estadísticas MEP.

SEE ALSO

Configurar un MEP para generar y responder a mensajes de protocolo CFM | 37

Administración de estadísticas de ETH-DM y recuentos de tramas de ETH-DM

in this section

- Mostrar solo estadísticas de ETH-DM | 272
- Visualización de estadísticas y recuentos de fotogramas de ETH-DM | 274
- Visualización de los recuentos de tramas ETH-DM para los eurodiputados adjuntando la entidad CFM | 275
- Visualización de los recuentos de fotogramas ETH-DM para los eurodiputados por interfaz o nivel de dominio | 276
- Borrar estadísticas y recuentos de tramas de ETH-DM | 277

Mostrar solo estadísticas de ETH-DM

in this section

- Propósito | 273

Acción | 273

Propósito

Mostrar estadísticas de ETH-DM.

De forma predeterminada, el comando muestra estadísticas de ETH-DM para los MEP de la asociación de mantenimiento de CFM (MA) especificada dentro del dominio de mantenimiento de CFM (MD) especificado.`show oam ethernet connectivity-fault-management delay-statistics`

Acción

- Para mostrar las estadísticas de ETH-DM recopiladas para los eurodiputados pertenecientes a MA y dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management delay-statistics maintenance-
domain ma1 maintenance-association ma1
```

- Para mostrar las estadísticas de ETH-DM recopiladas para las sesiones de ETH-DM para el MEP local perteneciente a MA y dentro de MD:`201ma2md2`

```
user@host> show oam ethernet connectivity-fault-management delay-statistics maintenance-
domain md2 maintenance-association ma2 local-mep 201
```

- Para mostrar las estadísticas de ETH-DM recopiladas para las sesiones de ETH-DM de los eurodiputados locales pertenecientes a MA y dentro de MD a eurodiputados remotos:`ma3md3302`

```
user@host> show oam ethernet connectivity-fault-management delay-statistics maintenance-
domain md3 maintenance-association ma3 remote-mep 302
```

SEE ALSO

Mostrar estadísticas de retraso en la administración de fallas de la conectividad Ethernet de OAM

Visualización de estadísticas y recuentos de fotogramas de ETH-DM

in this section

- Propósito | 274
- Acción | 274

Propósito

Muestra estadísticas de ETH-DM y recuentos de fotogramas de ETH-DM.

De forma predeterminada, el comando muestra las estadísticas de ETH-DM y los recuentos de fotogramas para los MEP en la asociación de mantenimiento de CFM (MA) especificada dentro del dominio de mantenimiento (MD) de CFM especificado.`show oam ethernet connectivity-fault-management mep-statistics`

Acción

- Para mostrar las estadísticas de ETH-DM y los recuentos de marcos de ETH-DM para los eurodiputados en MA y dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
md1 maintenance-association ma1
```

- Para mostrar las estadísticas de ETH-DM y los recuentos de fotogramas de ETH-DM para el MEP local en MA y dentro de MD:`201ma2md2`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
md2 maintenance-association ma2 local-mep 201
```

- Para mostrar las estadísticas de ETH-DM y los recuentos de fotogramas de ETH-DM para el MEP local en MD y dentro de MA que participa en una sesión de ETH-DM con el MEP remoto:`md3ma3302`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
ma3 maintenance-association ma3 remote-mep 302
```

SEE ALSO

Mostrar estadísticas MEP de conectividad Ethernet de OAM

Visualización de los recuentos de tramas ETH-DM para los eurodiputados adjuntando la entidad CFM

in this section

- Propósito | 275
- Acción | 275

Propósito

Muestra los recuentos de tramas ETH-DM para los puntos finales de la asociación de mantenimiento (MEP) de CFM.

De forma predeterminada, el comando muestra la información de la base de datos de CFM para los MEP de la asociación de mantenimiento de CFM (MA) especificada dentro del dominio de mantenimiento de CFM (MD) especificado.`show oam ethernet connectivity-fault-management mep-database`

> **NOTA**: En el enrutador conectado al MEP iniciador para una sesión unidireccional, o en el enrutador conectado al MEP receptor para una sesión bidireccional, solo puede mostrar los recuentos de tramas ETH-DM.

Acción

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de fotogramas ETH-DM) para todos los eurodiputados en MA dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
ma1 maintenance-association ma1
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-DM) solo para MEP local en MA dentro de MD:`201ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
md2 maintenance-association ma2 local-mep 201
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-DM) solo para MEP remoto en MD dentro de MA:`302md3ma3`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
ma3 maintenance-association ma3 remote-mep 302
```

SEE ALSO

> *Mostrar base de datos MEP de conectividad Ethernet de OAM*

Visualización de los recuentos de fotogramas ETH-DM para los eurodiputados por interfaz o nivel de dominio

in this section

- Propósito | **276**
- Acción | **277**

Propósito

Muestra los recuentos de tramas ETH-DM para los puntos finales de la asociación de mantenimiento (MEP) de CFM.

De forma predeterminada, el comando muestra la información de la base de datos CFM para los MEP conectados a interfaces Ethernet habilitadas para CFM en el enrutador o en un nivel de dominio de mantenimiento.`show oam ethernet connectivity-fault-management interfaces` Para las interfaces Ethernet compatibles con ETH-DM, los recuentos de tramas también se muestran cuando se especifica la opción de comando o `.detailextensive`

NOTA: En el enrutador conectado al MEP iniciador para una sesión unidireccional, o en el enrutador conectado al MEP receptor para una sesión bidireccional, solo puede mostrar los recuentos de tramas ETH-DM.

Acción

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-DM) para todos los MEP conectados a interfaces Ethernet habilitadas para CFM en el enrutador:

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-DM) solo para los MEP conectados a la interfaz de enrutador habilitada para CFM:`ge-5/2/9.0`

```
user@host> show oam ethernet connectivity-fault-management interfaces ge-5/2/9.0 detail
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-DM) solo para los MEP encerrados dentro de los dominios de mantenimiento (MD) de CFM en el nivel:`6`

```
user@host> show oam ethernet connectivity-fault-management interfaces level 6 detail
```

SEE ALSO

Mostrar interfaces de administración de fallos de conectividad Ethernet de OAM

Borrar estadísticas y recuentos de tramas de ETH-DM

in this section

Propósito | **278**
Acción | **278**

Propósito

Borre las estadísticas de ETH-DM y los recuentos de marcos de ETH-DM.

De forma predeterminada, las estadísticas y los recuentos de fotogramas se eliminan para todos los MEP conectados a interfaces habilitadas para CFM en el enrutador. Sin embargo, puede filtrar el ámbito del comando especificando un nombre de interfaz.

Acción

- Para borrar las estadísticas de ETH-DM y los recuentos de tramas de ETH-DM para todos los MEP conectados a interfaces habilitadas para CFM en el enrutador:

```
user@host> clear oam ethernet connectivity-fault-management statistics
```

- Para borrar las estadísticas de ETH-DM y los recuentos de tramas ETH-DM solo para los MEP conectados a la interfaz lógica:`ge-0/5.9.0`

```
user@host> clear oam ethernet connectivity-fault-management statistics ge-0/5/9.0
```

SEE ALSO

Estadísticas claras de administración de fallos de conectividad Ethernet OAM

VÍNCULOS RELACIONADOS

Estadísticas claras de administración de fallos de conectividad Ethernet OAM

Mostrar estadísticas de retraso en la administración de fallas de la conectividad Ethernet de OAM

Mostrar interfaces de administración de fallos de conectividad Ethernet de OAM

Mostrar estadísticas MEP de conectividad Ethernet de OAM

Mostrar base de datos MEP de conectividad Ethernet de OAM

VÍNCULOS RELACIONADOS

Configurar un perfil de iterador | 319

Configurar mediciones de pérdida sintética Ethernet | 338

Indicación de alarma Ethernet | 356
Modo de transmisión en línea | 371

Configuración de interfaces MEP para admitir mediciones de retardo de trama Ethernet

La medición del retardo de trama Ethernet es una herramienta útil para proporcionar estadísticas de rendimiento o respaldar o desafiar los acuerdos de nivel de servicio (SLA). De forma predeterminada, la medición de retardo de trama Ethernet utiliza software para el sellado de tiempo y los cálculos de retardo. Opcionalmente, puede utilizar la temporización de hardware para ayudar en este proceso y aumentar la precisión de los resultados de la medición de retardo. Esta asistencia está disponible en el camino de recepción.

Antes de poder realizar mediciones de retardo de trama Ethernet en enrutadores de la serie MX, debe haber hecho lo siguiente:

- Configuró correctamente Ethernet OAM y CFM
- Preparó la medición entre dos enrutadores de la serie MX configurados de manera compatible
- Se habilitó el demonio de administración periódica distribuida de paquetes (ppmd)
- Se evitó intentar realizar la medición del retardo de trama Ethernet en interfaces Ethernet agregadas o pseudocables, que no son compatibles
- Se aseguró de que la marca de tiempo asistida por hardware sea compatible si esa característica está configurada

Al final de esta configuración, se crean dos enrutadores serie MX que pueden realizar y mostrar mediciones de retardo de trama Ethernet en interfaces Ethernet mediante marcas de tiempo de hardware opcionales. De forma predeterminada, la medición de retardo de trama Ethernet utiliza software para el sellado de tiempo y los cálculos de retardo. Opcionalmente, puede utilizar la temporización de hardware para ayudar en este proceso y aumentar la precisión de los resultados de la medición de retardo. Esta asistencia está disponible en el camino de recepción.

Para configurar la marca de tiempo asistida por hardware:

1. Para habilitar la asistencia de hardware de medición de retardo de trama Ethernet en la ruta de recepción, incluya la instrucción en el nivel de jerarquía:`hardware-assisted-timestamping`[`edit protocols oam ethernet connectivity-fault-management performance-monitoring`]

```
[edit]
protocols {
    oam {
        ethernet {
            connectivity-fault-management {
                performance-monitoring {
                    hardware-assisted-timestamping; # Enable timestamping in hardware.
                }
            }
        }
    }
```

2. La medición del retardo de trama Ethernet requiere que el PPMD distribuido esté habilitado. Antes de poder recopilar estadísticas para la medición del retardo de trama Ethernet, debe asegurarse de que PPMD esté configurado correctamente. Sin PPMD distribuido, los resultados de la medición de retardo no son válidos.

   Para realizar la medición del retardo de trama Ethernet, asegúrese de que la siguiente instrucción de configuración NO está presente:

```
[edit routing-options]
ppm {
    no-delegate-processing; # This turns distributed PPMD OFF.
}
```

VÍNCULOS RELACIONADOS

Descripción general de las mediciones de retardo de trama Ethernet | 214

Activación de una sesión de mediciones de retardo de trama Ethernet | 251

Visualización de estadísticas de mediciones de retardo de trama Ethernet | 271

Ejemplo: Configuración de mediciones de retardo de trama Ethernet unidireccionales con interfaces de etiqueta única | 256

Ejemplo: Configuración de mediciones de retardo de trama Ethernet unidireccionales con interfaces de etiqueta única | 256

Configuración de ETH-DM con interfaces sin etiquetar

Configurar la medición de pérdida de tramas Ethernet

in this section

- Configuración de la medición estadística de pérdida de tramas para conexiones VPLS | **281**
- Gestión de estadísticas de ETH-LM | **282**
- Ejemplo: Medición de la pérdida de tramas Ethernet para PDU LMM/LMR de etiqueta única | **285**
- Ejemplo: Medición de la pérdida de tramas Ethernet para PDU LMM/LMR de doble etiqueta | **302**

Utilice este tema para obtener más información sobre la medición de pérdida de fotogramas y cómo configurar la medición de pérdida de fotogramas.

Actualmente, la medición de pérdidas no está disponible para tarjetas Multi-LU (MPC3E y MPC4E), y no hay restricciones de interfaz de línea de comandos para la configuración.

Configuración de la medición estadística de pérdida de tramas para conexiones VPLS

Mediante la medición estadística proactiva de pérdida de fotogramas, puede supervisar las conexiones VPLS en los enrutadores de la serie MX. La medición estadística de pérdida de tramas le permite supervisar la calidad de las conexiones Ethernet para los acuerdos de nivel de servicio (SLA). Las conexiones punto a punto y multipunto a multipunto configuradas en los enrutadores de la serie MX se pueden monitorear registrando la conexión en un iterador e iniciando la medición periódica de SLA de las transmisiones de trama en las conexiones.

Los iteradores transmiten periódicamente paquetes de medición de SLA utilizando tramas compatibles con ITU-Y.1731. El iterador envía paquetes de medición periódicos para cada una de las conexiones registradas en él. Estos ciclos de medición se transmiten de tal manera que no se superponen, reduciendo las demandas de procesamiento impuestas a la CPU. Los paquetes de medición se intercambian entre el puerto de la interfaz de red de usuario (UNI) de origen y el puerto UNI de destino, lo que proporciona una secuencia de mediciones de rendimiento cronometradas para cada par UNI. El índice de pérdida de tramas (FLR) y la disponibilidad de conexión se pueden calcular a partir de estas mediciones mediante estadísticas.

Los siguientes pasos describen cómo configurar la medición estadística de pérdida de fotogramas para conexiones VPLS:

1. Para configurar la medición proactiva de ETH-DM para una conexión VPLS, consulte "Directrices para configurar enrutadores que admitan una sesión de ETH-DM" en la página 235.
2. Para habilitar la medición estadística de pérdidas para una conexión VPLS, configure un iterador para la conexión VPLS mediante la instrucción sla-iterator-profiles en el nivel jerárquico .*sla-iterator-*

profiles[edit protocols oam ethernet connectivity-fault-management performance-monitoring] Para obtener instrucciones detalladas, consulte Configuración de un perfil de iterador."Configuración de un perfil de iterador" en la página 319

3. Como parte de la configuración del iterador, incluya la opción para la instrucción measurement-type en el nivel de jerarquía.statistical-frame-loss*measurement-type*[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles *profile-name*]
4. Una vez habilitado el iterador, puede mostrar la pérdida de fotogramas estadística de una conexión VPLS emitiendo el comando.show oam ethernet connectivity-fault-management sla-iterator-statistics sla-iterator *identifier* maintenance-domain *name* maintenance-association *name* local-mep *identifier* remote-mep *identifier*

SEE ALSO

Configuración de un perfil de iterador | 319

Comprobación de la configuración de un perfil de iterador | 323

Gestión de estadísticas de ETH-LM

in this section

- Visualización de estadísticas ETH-LM | 282
- Borrar estadísticas de ETH-LM | 284

Visualización de estadísticas ETH-LM

in this section

- Propósito | 282
- Acción | 283

Propósito

Mostrar las estadísticas de ETH-LM.

De forma predeterminada, el comando muestra estadísticas de ETH-LM para los MEP de la asociación de mantenimiento de CFM (MA) especificada dentro del dominio de mantenimiento de CFM (MD) especificado.`show oam ethernet connectivity-fault-management loss-statistics maintenance-domain md-name maintenance-association ma-name`

La siguiente lista consta de los comandos de modo operativo relacionados con CFM que se han mejorado para mostrar estadísticas de ETH-LM:

- El comando se ha mejorado para mostrar estadísticas de ETH-DM y ETH-LM para los MEP en la asociación de mantenimiento (MA) de CFM especificada dentro del dominio de mantenimiento (MD) de CFM especificado.`show oam ethernet connectivity-fault-management interfaces detail`

- El comando se ha mejorado para mostrar estadísticas de ETH-DM y ETH-LM y recuentos de tramas para MEP en la asociación de mantenimiento (MA) de CFM especificada dentro del dominio de mantenimiento (MD) de CFM especificado.`show oam ethernet connectivity-fault-management mep-statistics`

- El comando se ha mejorado para mostrar los contadores de tramas ETH-DM y ETH-LM para los MEP en la asociación de mantenimiento CFM (MA) especificada dentro del dominio de mantenimiento (MD) CFM especificado.`show oam ethernet connectivity-fault-management mep-database`

Acción

- Para mostrar las estadísticas de ETH-LM para todos los MEP conectados a interfaces habilitadas para CFM en el enrutador:

```
user@host> show oam ethernet connectivity-fault-management loss-statistics
```

- Para mostrar las estadísticas de ETH-DM recopiladas para los eurodiputados pertenecientes a MA y dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management delay-statistics maintenance-
domain md1 maintenance-association ma1
```

- Para mostrar las estadísticas de ETH-DM y los recuentos de marcos de ETH-DM para los eurodiputados en MA y dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
md1 maintenance-association ma1
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de fotogramas ETH-DM) para todos los eurodiputados en MA dentro de MD:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
md1 maintenance-association ma1
```

SEE ALSO

clear oam ethernet connectivity-fault-management loss-statistics

show oam ethernet connectivity-fault-management delay-statistics

show oam ethernet connectivity-fault-management interfaces

show oam ethernet connectivity-fault-management mep-statistics

show oam ethernet connectivity-fault-management mep-database

show oam ethernet connectivity-fault-management loss-statistics

Borrar estadísticas de ETH-LM

in this section

Propósito | 284

Acción | 285

Propósito

Borre las estadísticas de ETH-LM.

De forma predeterminada, las estadísticas se eliminan para todos los eurodiputados conectados a interfaces habilitadas para CFM en el enrutador. Sin embargo, puede filtrar el ámbito del comando especificando un nombre de interfaz.

Acción

- Para borrar las estadísticas de ETH-LM para todos los MEP conectados a interfaces habilitadas para CFM en el enrutador:

```
user@host> clear oam ethernet connectivity-fault-management loss-statistics
```

SEE ALSO

clear oam ethernet connectivity-fault-management loss-statistics

VÍNCULOS RELACIONADOS

Administración de estadísticas de ETH-DM y recuentos de tramas de ETH-DM | 272

Ejemplo: Medición de la pérdida de tramas Ethernet para PDU LMM/LMR de etiqueta única

in this section

- Requisitos | 285
- Descripción general y topología | 286
- Configuración | 287
- Verificación | 299

En este ejemplo se muestra cómo configurar la medición de pérdida de trama Ethernet (ETH-LM) para unidades de datos de protocolo (PDU) de mensaje de medición de pérdida (LMM)/respuesta de medición de pérdidas (LMR) con etiqueta única. Al configurar ETH-LM, puede medir la pérdida de tramas Ethernet que se produce en su red.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Dos plataformas de enrutamiento universal 5G serie MX con concentradores de puerto denso (DPC) Rev-B

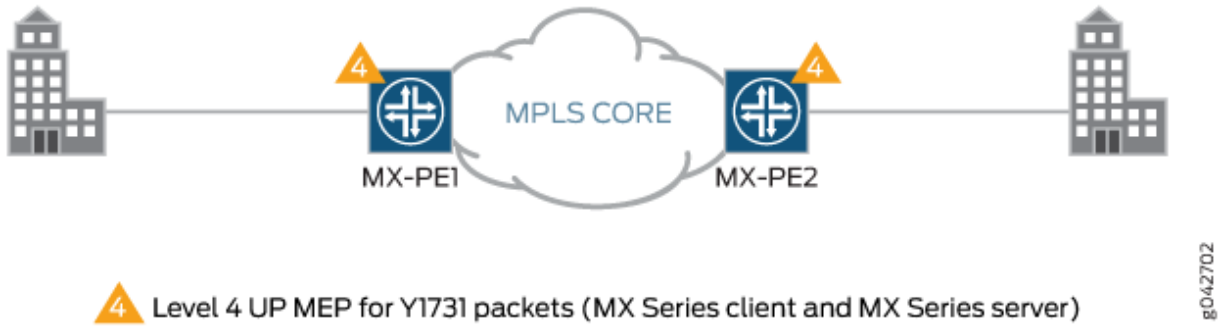
- Junos OS versión 14.2 o posterior

Descripción general y topología

Junos OS admite la medición de pérdida de tramas Ethernet (ETH-LM) entre puntos finales de asociación de mantenimiento (MEP) configurados en interfaces físicas o lógicas Ethernet en concentradores de puerto denso (DPC) Rev-B en enrutadores serie MX. Además, la funcionalidad Y.1731 admite ETH-LM solo para una conexión de extremo a extremo que utiliza el servicio de cable privado virtual (VPWS). En este ejemplo se muestra cómo configurar ETH-LM para PDU LMM/LMR de etiqueta única con mapa VLAN de entrada y salida configurado como `.swap`

Figura 19 en la página 286muestra la topología utilizada en este ejemplo. El servicio VPWS se configura entre dos enrutadores de la serie MX, MX-PE1 y MX PE2.

Figura 19: Servicio VPWS configurado entre dos enrutadores de la serie MX



El enrutador MX-PE1 tiene dos interfaces Ethernet y `.ge-5/0/4ge-5/1/9` La LAN virtual (VLAN) está configurada en la interfaz y MPLS está configurada en la interfaz.`ge-5/0/4ge-5/1/9` La interfaz se utiliza para configurar el circuito virtual de capa 2 con el enrutador MX-PE2.`ge-5/0/4.11` El MEP de la UP, , se adjunta a la interfaz.`mep 2ge-5/0/4.11` El filtro de firewall de tres colores también está configurado para el enrutador MX-PE1.

De manera similar, el enrutador MX-PE2 tiene dos interfaces Ethernet y `.ge-8/0/8ge-8/0/9` La LAN virtual (VLAN) está configurada en la interfaz y MPLS está configurada en la interfaz.`ge-8/0/8ge-8/0/9` La interfaz se utiliza para configurar el circuito virtual de capa 2 con el enrutador MX-PE1.`ge-8/0/8.11` El MEP de la UP, , se adjunta a la interfaz.`mep 1ge-8/0/8.11` El filtro de firewall de tres colores también está configurado para el enrutador MX-PE2.

Configuración

in this section

- Configuración rápida de CLI | 287
- Configuración del enrutador PE1 | 289
- Configuración del enrutador PE2 | 294

Configuración rápida de CLI

Para configurar rápidamente ETH-LM para PDU LMM/LMR de etiqueta única, copie los siguientes comandos, elimine los saltos de línea y, a continuación, pegue los comandos en la CLI de cada dispositivo.

En el enrutador PE1:

```
[edit]
set interfaces ge-5/0/4 encapsulation flexible-ethernet-services
set interfaces ge-5/0/4 unit 11 encapsulation vlan-ccc
set interfaces ge-5/0/4 unit 11 layer2-policer input-three-color abc
set interfaces ge-5/0/4 unit 11 family ccc
set interfaces ge-5/1/9 enable
set interfaces ge-5/1/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-5/1/9 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set interfaces ge-5/0/4 flexible-vlan-tagging
set interfaces ge-5/0/4 unit 11 vlan-id 2000
set interfaces ge-5/0/4 unit 11 input-vlan-map swap
set interfaces ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-5/0/4 unit 11 output-vlan-map swap
set routing-options router-id 4.4.4.4
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
```

```
set protocols oam ethernet connectivity-fault-management performance-monitoring delegate-server-processing
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 2 interface ge-5/0/4.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 2 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 2 remote-mep 1
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

En el enrutador PE2:

```
[edit]
set interfaces ge-8/0/8 encapsulation flexible-ethernet-services
set interfaces ge-8/0/8 unit 11 encapsulation vlan-ccc
set interfaces ge-8/0/8 unit 11 layer2-policer input-three-color abc
set interfaces ge-8/0/8 unit 11 family ccc
set interfaces ge-8/0/9 enable
set interfaces ge-8/0/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-8/0/9 unit 0 family mpls
set interfaces ae0 unit 0 family inet
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set interfaces ge-8/0/8 flexible-vlan-tagging
set interfaces ge-8/0/8 unit 11 vlan-id 2000
set interfaces ge-8/0/8 unit 11 input-vlan-map swap
set interfaces ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-8/0/8 unit 11 output-vlan-map swap
set routing-options router-id 3.3.3.3
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
```

```
set protocols l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 1 interface ge-8/0/8.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 1 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 1 remote-mep 2
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

Configuración del enrutador PE1

Procedimiento paso a paso

Para configurar el enrutador PE1:

1. Configure las interfaces.

```
[edit]
user@PE1# edit interfaces
[edit interfaces]
user@PE1# set ge-5/0/4 encapsulation flexible-ethernet-services
user@PE1# set ge-5/0/4 unit 11 encapsulation vlan-ccc
user@PE1# set ge-5/0/4 unit 11 layer2-policer input-three-color abc
user@PE1# set ge-5/0/4 unit 11 family ccc
user@PE1# set ge-5/1/9 enable
user@PE1# set ge-5/1/9 unit 0 family inet address 12.1.1.1/24
user@PE1# set ge-5/1/9 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 4.4.4.4/32
```

2. Configure la VLAN.

```
[edit interfaces]
user@PE1# set ge-5/0/4 flexible-vlan-tagging
user@PE1# set ge-5/0/4 unit 11 vlan-id 2000
user@PE1# set ge-5/0/4 unit 11 input-vlan-map swap
user@PE1# set ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
user@PE1# set ge-5/0/4 unit 11 output-vlan-map swap
```

3. Configure el identificador del enrutador para identificar el dispositivo de enrutamiento.

```
[edit]
user@PE1# edit routing-options
[edit routing-options]
user@PE1# set router-id 4.4.4.4
```

4. Configure los protocolos MPLS, OSPF y LDP.

```
[edit]
user@PE1# edit protocols
[edit protocols]
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE1# set ldp interface all
user@PE1# set ldp interface fxp0.0 disable
```

5. Configure el circuito de capa 2.

```
[edit protocols]
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
```

6. Configure el MEP.

```
[edit protocols]
user@PE1# set oam ethernet connectivity-fault-management performance-monitoring delegate-
```

```
server-processing
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma continuity-check interval 1s
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 interface ge-5/0/4.11
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 direction up
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 remote-mep 1
```

7. Configure el firewall.

```
[edit]
user@PE1# edit firewall
[edit firewall]
user@PE1# set three-color-policer abc logical-interface-policer
user@PE1# set three-color-policer abc two-rate color-blind
user@PE1# set three-color-policer abc two-rate committed-information-rate 10m
user@PE1# set three-color-policer abc two-rate committed-burst-size 1500
user@PE1# set three-color-policer abc two-rate peak-information-rate 20m
user@PE1# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Confirme la configuración.

```
[edit]
user@PE1# commit
```

Resultados

Desde el modo de configuración, ingrese los comandos `show interfaces`, `show protocols`, `show routing-options` y `show firewall` para confirmar la configuración. Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
user@PE1# show interfaces
interfaces {
    ge-5/0/4 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
```

```
        unit 11 {
            encapsulation vlan-ccc;
            vlan-id 2000;
            input-vlan-map {
                swap;
                vlan-id 4094;
            }
            output-vlan-map swap;
            layer2-policer {
                input-three-color abc;
            }
            family ccc;
        }
    }
    ge-5/1/9 {
        enable;
        unit 0 {
            family inet {
                address 12.1.1.1/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 4.4.4.4/32;
            }
        }
    }
}
```

```
user@PE1# show protocols
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
```

```
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    l2circuit {
        neighbor 3.3.3.3 {
            interface ge-5/0/4.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                performance-monitoring {
                    delegate-server-processing;
                }
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 2 {
                            interface ge-5/0/4.11;
                            direction up;
                            remote-mep 1;
                        }
                    }
                }
            }
        }
```

```
    }
}
```

```
user@PE1# show routing-options
routing-options {
    router-id 4.4.4.4;
}
```

```
user@PE1# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Configuración del enrutador PE2

Procedimiento paso a paso

Para configurar el enrutador PE2:

1. Configure las interfaces.

```
[edit]
user@PE2# edit interfaces
[edit interfaces]
user@PE2# set ge-8/0/8 encapsulation flexible-ethernet-services
user@PE2# set ge-8/0/8 unit 11 encapsulation vlan-ccc
user@PE2# set ge-8/0/8 unit 11 layer2-policer input-three-color abc
user@PE2# set ge-8/0/8 unit 11 family ccc
user@PE2# set ge-8/0/9 enable
user@PE2# set ge-8/0/9 unit 0 family inet address 12.1.1.1/24
```

```
user@PE2# set ge-8/0/9 unit 0 family mpls
user@PE2# set ae0 unit 0 family inet
user@PE2# set lo0 unit 0 family inet address 3.3.3.3/32
```

2. Configure la VLAN.

```
[edit interfaces]
user@PE2# set ge-8/0/8 flexible-vlan-tagging
user@PE2# set ge-8/0/8 unit 11 vlan-id 2000
user@PE2# set ge-8/0/8 unit 11 input-vlan-map swap
user@PE2# set ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
user@PE2# set ge-8/0/8 unit 11 output-vlan-map swap
```

3. Configure el identificador del enrutador para identificar el dispositivo de enrutamiento.

```
[edit]
user@PE2# edit routing-options
[edit routing-options]
user@PE2# set router-id 3.3.3.3
```

4. Configure los protocolos MPLS, OSPF y LDP.

```
[edit]
user@PE2# edit protocols
[edit protocols]
user@PE2# set mpls interface all
user@PE2# set mpls interface fxp0.0 disable
user@PE2# set ospf area 0.0.0.0 interface all
user@PE2# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE2# set ldp interface all
user@PE2# set ldp interface fxp0.0 disable
```

5. Configure el circuito de capa 2.

```
[edit protocols]
user@PE2# set l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
user@PE2# set l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
```

6. Configure el MEP.

```
[edit protocols]
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma continuity-check interval 1s
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 1 interface ge-8/0/8.11
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 1 direction up
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 1 remote-mep 2
```

7. Configure el firewall.

```
[edit]
user@PE2# edit firewall
[edit firewall]
user@PE2# set three-color-policer abc logical-interface-policer
user@PE2# set three-color-policer abc two-rate color-blind
user@PE2# set three-color-policer abc two-rate committed-information-rate 10m
user@PE2# set three-color-policer abc two-rate committed-burst-size 1500
user@PE2# set three-color-policer abc two-rate peak-information-rate 20m
user@PE2# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Confirme la configuración.

```
[edit]
user@PE2# commit
```

Resultados

Desde el modo de configuración, ingrese los comandos `show interfaces`, `show protocols`, `show routing-options` y `show firewall` para confirmar la configuración. Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
user@PE2# show interfaces
interfaces {
```

```
    ge-8/0/8 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 11 {
            encapsulation vlan-ccc;
            vlan-id 2000;
            input-vlan-map {
                swap;
                vlan-id 4094;
            }
            output-vlan-map swap;
            layer2-policer {
                input-three-color abc;
            }
            family ccc;
        }
    }
    ge-8/0/9 {
        unit 0 {
            family inet {
                address 12.1.1.2/24;
            }
            family mpls;
        }
    }
    ae0 {
        unit 0 {
            family inet;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 3.3.3.3/32;
            }
        }
    }
}
```

```
user@PE2# show protocols
protocols {
```

```
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    l2circuit {
        neighbor 4.4.4.4 {
            interface ge-8/0/8.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 1 {
                            interface ge-8/0/8.11;
                            direction up;
                            remote-mep 2;
                        }
                    }
```

```
                }
            }
        }
    }
}
```

```
user@PE2# show routing-options
routing-options {
    router-id 3.3.3.3;
}
```

```
user@PE2# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Verificación

in this section

- Visualización de ETH-LM | **300**

Para empezar a supervisar la pérdida de tramas Ethernet, ejecute el comando.`monitor ethernet loss-measurement maintenance-domain md maintenance-association ma mep 1` La pérdida de tramas se calcula recopilando los valores de contador aplicables a las tramas de servicio de entrada y salida en las que los contadores mantienen un recuento de tramas de datos transmitidas y recibidas entre un par de MEP. Las estadísticas de medición de pérdidas se recuperan como salida del comando.`monitor ethernet loss-`

`measurement` También puede emitir el comando para mostrar estadísticas de ETH-LM.`show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11`

Visualización de ETH-LM

Propósito

Vea las estadísticas de ETH-LM.

Acción

Desde el modo operativo, ingrese el comando `show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11`.

```
user@PE1> show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11
Interface name: ge-5/0/4.11 , Interface status: Active, Link status: Up
  Maintenance domain name: md, Format: string, Level: 4
    Maintenance association name: ma, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: none, Port status TLV: none
    Connection Protection TLV: no
    MEP identifier: 2, Direction: up, MAC address: 00:24:dc:9b:96:76
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                 : no
      Erroneous CCM received                       : no
      Cross-connect CCM received                   : no
      RDI sent by some MEP                         : no
      Some remote MEP's MAC in error state         : no
    Statistics:
      CCMs sent                                    : 36
      CCMs received out of sequence                : 0
      LBMs sent                                    : 0
      Valid in-order LBRs received                 : 0
      Valid out-of-order LBRs received             : 0
      LBRs received with corrupted data            : 0
      LBRs sent                                    : 0
      LTMs sent                                    : 0
      LTMs received                                : 0
      LTRs sent                                    : 0
      LTRs received                                : 0
      Sequence number of next LTM request          : 0
```

```
    1DMs sent                                    : 0
    Valid 1DMs received                          : 0
    Invalid 1DMs received                        : 0
    Out of sync 1DMs received                    : 0
    DMMs sent                                    : 0
    Valid DMMs received                          : 0
    Invalid DMMs received                        : 0
    DMRs sent                                    : 0
    Valid DMRs received                          : 0
    Invalid DMRs received                        : 0
    LMMs sent                                    : 10
    Valid LMMs received                          : 0
    Invalid LMMs received                        : 0
    LMRs sent                                    : 0
    Valid LMRs received                          : 10
    Invalid LMRs received                        : 0
    SLMs sent                                    : 0
    Valid SLMs received                          : 0
    Invalid SLMs received                        : 0
    SLRs sent                                    : 0
    Valid SLRs received                          : 0
    Invalid SLRs received                        : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
        1     00:05:85:76:e5:30       ok   ge-5/0/4.11
```

Significado

Se muestran los detalles y las estadísticas de la interfaz Ethernet. Este resultado indica que la interfaz está activa y que su estado de vínculo es `.ge-5/0/4.11up` Su nombre de dominio de mantenimiento es y su nivel es `.md4` El identificador MEP de la interfaz se indica como y su dirección es `.ge-5/0/4.112up` En la sección de estadísticas, el resultado indica que la interfaz envió LMM y que la interfaz recibió LMR válidos.`1010`

SEE ALSO

Configurar mediciones de pérdida sintética Ethernet | 338

Introducción a la administración de errores de conectividad (CFM) de OAM | 20

Ejemplo: Medición de la pérdida de tramas Ethernet para PDU LMM/LMR de doble etiqueta

in this section

- Requisitos | 302
- Descripción general y topología | 302
- Configuración | 303
- Verificación | 316

En este ejemplo se muestra cómo configurar la medición de pérdida de tramas Ethernet (ETH-LM) para unidades de datos de protocolo (PDU) de mensaje de medición de pérdidas (LMM)/respuesta de medición de pérdidas (LMR) de doble etiquetado. Al configurar ETH-LM, puede medir la pérdida de tramas Ethernet que se produce en su red.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

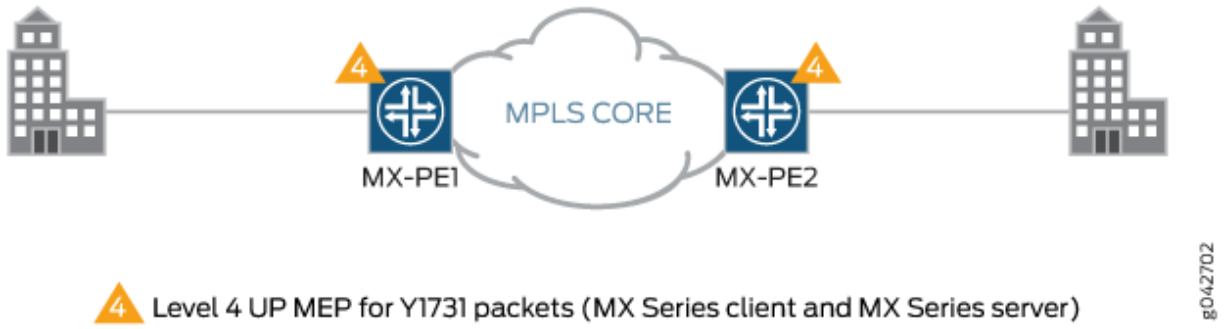
- Dos plataformas de enrutamiento universal 5G serie MX con concentradores de puerto denso (DPC) Rev-B
- Junos OS versión 14.2 o posterior

Descripción general y topología

Junos OS admite la medición de pérdida de tramas Ethernet (ETH-LM) entre puntos finales de asociación de mantenimiento (MEP) configurados en interfaces físicas o lógicas Ethernet en concentradores de puerto denso (DPC) Rev-B en enrutadores serie MX. Además, la funcionalidad Y.1731 admite ETH-LM solo para una conexión de extremo a extremo que utiliza el servicio de cable privado virtual (VPWS). En este ejemplo se ilustra cómo configurar ETH-LM para PDU LMM/LMR con etiquetas duales con mapa VLAN de entrada y salida configurado como `.swap-swap`

Figura 20 en la página 303muestra la topología utilizada en este ejemplo. El servicio VPWS se configura entre dos enrutadores MX Sereies, MX-PE1 y MX PE2.

Figura 20: Servicio VPWS configurado entre dos enrutadores de la serie MX



El enrutador MX-PE1 tiene dos interfaces Ethernet y `.ge-5/0/4ge-5/1/9` La LAN virtual (VLAN) está configurada en la interfaz y MPLS está configurada en la interfaz`.ge-5/0/4ge-5/1/9` La interfaz se utiliza para configurar el circuito virtual de capa 2 con el enrutador MX-PE2`.ge-5/0/4.11` El MEP de la UP, , se adjunta a la interfaz`.mep 2ge-5/0/4.11` El filtro de firewall de tres colores también está configurado para el enrutador MX-PE1.

De manera similar, el enrutador MX-PE2 tiene dos interfaces Ethernet y `.ge-8/0/8ge-8/0/9` La LAN virtual (VLAN) está configurada en la interfaz y MPLS está configurada en la interfaz`.ge-8/0/8ge-8/0/9` La interfaz se utiliza para configurar el circuito virtual de capa 2 con el enrutador MX-PE1`.ge-8/0/8.11` El MEP de la UP, , se adjunta a la interfaz`.mep 1ge-8/0/8.11` El filtro de firewall de tres colores también está configurado para el enrutador MX-PE2.

Configuración

in this section

- Configuración rápida de CLI | **303**
- Configuración del enrutador PE1 | **306**
- Configuración del enrutador PE2 | **311**

Configuración rápida de CLI

Para configurar rápidamente ETH-LM para PDU LMM/LMR con etiqueta dual, copie los siguientes comandos, elimine los saltos de línea y, a continuación, pegue los comandos en la CLI de cada dispositivo.

En el enrutador PE1:

```
[edit]
set interfaces ge-5/0/4 encapsulation flexible-ethernet-services
set interfaces ge-5/0/4 unit 11 encapsulation vlan-ccc
set interfaces ge-5/0/4 unit 11 layer2-policer input-three-color abc
set interfaces ge-5/0/4 unit 11 family ccc
set interfaces ge-5/1/9 enable
set interfaces ge-5/1/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-5/1/9 unit 0 family mpls
set interfaces lo0 unit 0 family inet address 4.4.4.4/32
set interfaces ge-5/0/4 flexible-vlan-tagging
set interfaces ge-5/0/4 unit 11 vlan-tags outer 2000 inner 1000
set interfaces ge-5/0/4 unit 11 input-vlan-map swap-swap
set interfaces ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-5/0/4 unit 11 input-vlan-map inner-vlan-id 4093
set interfaces ge-5/0/4 unit 11 output-vlan-map swap-swap
set routing-options router-id 4.4.4.4
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
set protocols oam ethernet connectivity-fault-management performance-monitoring delegate-server-
processing
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 interface ge-5/0/4.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 remote-mep 1
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
set firewall three-color-policer abc two-rate committed-burst-size 1500
```

```
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

En el enrutador PE2:

```
[edit]
set interfaces ge-8/0/8 encapsulation flexible-ethernet-services
set interfaces ge-8/0/8 unit 11 encapsulation vlan-ccc
set interfaces ge-8/0/8 unit 11 layer2-policer input-three-color abc
set interfaces ge-8/0/8 unit 11 family ccc
set interfaces ge-8/0/9 enable
set interfaces ge-8/0/9 unit 0 family inet address 12.1.1.1/24
set interfaces ge-8/0/9 unit 0 family mpls
set interfaces ae0 unit 0 family inet
set interfaces lo0 unit 0 family inet address 3.3.3.3/32
set interfaces ge-8/0/8 flexible-vlan-tagging
set interfaces ge-8/0/8 unit 11 vlan-tags outer 2000 inner 1000
set interfaces ge-8/0/8 unit 11 input-vlan-map swap-swap
set interfaces ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
set interfaces ge-8/0/8 unit 11 input-vlan-map inner-vlan-id 4093
set interfaces ge-8/0/8 unit 11 output-vlan-map swap-swap
set routing-options router-id 3.3.3.3
set protocols mpls interface all
set protocols mpls interface fxp0.0 disable
set protocols ospf area 0.0.0.0 interface all
set protocols ospf area 0.0.0.0 interface fxp0.0 disable
set protocols ldp interface all
set protocols ldp interface fxp0.0 disable
set protocols l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
set protocols l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
set protocols oam ethernet connectivity-fault-management maintenance-domain md level 4
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma continuity-check interval 1s
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 1 interface ge-8/0/8.11
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 1 direction up
set protocols oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 1 remote-mep 2
set firewall three-color-policer abc logical-interface-policer
set firewall three-color-policer abc two-rate color-blind
set firewall three-color-policer abc two-rate committed-information-rate 10m
```

```
set firewall three-color-policer abc two-rate committed-burst-size 1500
set firewall three-color-policer abc two-rate peak-information-rate 20m
set firewall three-color-policer abc two-rate peak-burst-size 15k
```

Configuración del enrutador PE1

Procedimiento paso a paso

Para configurar el enrutador PE1:

1. Configure las interfaces.

```
[edit]
user@PE1# edit interfaces
[edit interfaces]
user@PE1# set ge-5/0/4 encapsulation flexible-ethernet-services
user@PE1# set ge-5/0/4 unit 11 encapsulation vlan-ccc
user@PE1# set ge-5/0/4 unit 11 layer2-policer input-three-color abc
user@PE1# set ge-5/0/4 unit 11 family ccc
user@PE1# set ge-5/1/9 enable
user@PE1# set ge-5/1/9 unit 0 family inet address 12.1.1.1/24
user@PE1# set ge-5/1/9 unit 0 family mpls
user@PE1# set lo0 unit 0 family inet address 4.4.4.4/32
```

2. Configure la VLAN.

```
[edit interfaces]
user@PE1# set ge-5/0/4 flexible-vlan-tagging
user@PE1# set ge-5/0/4 unit 11 vlan-tags outer 2000 inner 1000
user@PE1# set ge-5/0/4 unit 11 input-vlan-map swap-swap
user@PE1# set ge-5/0/4 unit 11 input-vlan-map vlan-id 4094
user@PE1# set ge-5/0/4 unit 11 input-vlan-map inner-vlan-id 4093
user@PE1# set ge-5/0/4 unit 11 output-vlan-map swap-swap
```

3. Configure el identificador del enrutador para identificar el dispositivo de enrutamiento.

```
[edit]
user@PE1# edit routing-options
```

```
[edit routing-options]
user@PE1# set router-id 4.4.4.4
```

4. Configure los protocolos MPLS, OSPF y LDP.

```
[edit]
user@PE1# edit protocols
[edit protocols]
user@PE1# set mpls interface all
user@PE1# set mpls interface fxp0.0 disable
user@PE1# set ospf area 0.0.0.0 interface all
user@PE1# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE1# set ldp interface all
user@PE1# set ldp interface fxp0.0 disable
```

5. Configure el circuito de capa 2.

```
[edit protocols]
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 virtual-circuit-id 1003
user@PE1# set l2circuit neighbor 3.3.3.3 interface ge-5/0/4.11 no-control-word
```

6. Configure el MEP.

```
[edit protocols]
user@PE1# set oam ethernet connectivity-fault-management performance-monitoring delegate-
server-processing
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma continuity-check interval 1s
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 interface ge-5/0/4.11
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 direction up
user@PE1# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-
association ma mep 2 remote-mep 1
```

7. Configure el firewall.

```
[edit]
user@PE1# edit firewall
[edit firewall]
user@PE1# set three-color-policer abc logical-interface-policer
user@PE1# set three-color-policer abc two-rate color-blind
user@PE1# set three-color-policer abc two-rate committed-information-rate 10m
user@PE1# set three-color-policer abc two-rate committed-burst-size 1500
user@PE1# set three-color-policer abc two-rate peak-information-rate 20m
user@PE1# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Confirme la configuración.

```
[edit]
user@PE1# commit
```

Resultados

Desde el modo de configuración, ingrese los comandos `show interfaces`, `show protocols`, `show routing-options` y `show firewall` para confirmar la configuración. Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
user@PE1# show interfaces
interfaces {
    ge-5/0/4 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 11 {
            encapsulation vlan-ccc;
            vlan-tags outer 2000 inner 1000;
            input-vlan-map {
                swap-swap;
                vlan-id 4094;
                inner-vlan-id 4093;
            }
            output-vlan-map swap-swap;
            layer2-policer {
                input-three-color abc;
```

```
            }
            family ccc;
        }
    }
    ge-5/1/9 {
        enable;
        unit 0 {
            family inet {
                address 12.1.1.1/24;
            }
            family mpls;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 4.4.4.4/32;
            }
        }
    }
}
```

```
user@PE1# show protocols
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
        interface all;
        interface fxp0.0 {
```

```
            disable;
        }
    }
    l2circuit {
        neighbor 3.3.3.3 {
            interface ge-5/0/4.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                performance-monitoring {
                    delegate-server-processing;
                }
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
                        }
                        mep 2 {
                            interface ge-5/0/4.11;
                            direction up;
                            remote-mep 1;
                        }
                    }
                }
            }
        }
    }
}
```

```
user@PE1# show routing-options
routing-options {
```

```
    router-id 4.4.4.4;
}
```

```
user@PE1# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Configuración del enrutador PE2

Procedimiento paso a paso

Para configurar el enrutador PE2:

1. Configure las interfaces.

```
[edit]
user@PE2# edit interfaces
[edit interfaces]
user@PE2# set ge-8/0/8 encapsulation flexible-ethernet-services
user@PE2# set ge-8/0/8 unit 11 encapsulation vlan-ccc
user@PE2# set ge-8/0/8 unit 11 layer2-policer input-three-color abc
user@PE2# set ge-8/0/8 unit 11 family ccc
user@PE2# set ge-8/0/9 enable
user@PE2# set ge-8/0/9 unit 0 family inet address 12.1.1.1/24
user@PE2# set ge-8/0/9 unit 0 family mpls
user@PE2# set ae0 unit 0 family inet
user@PE2# set lo0 unit 0 family inet address 3.3.3.3/32
```

2. Configure la VLAN.

```
[edit interfaces]
user@PE2# set ge-8/0/8 flexible-vlan-tagging
user@PE2# set ge-8/0/8 unit 11 vlan-tags outer 2000 inner 1000
user@PE2# set ge-8/0/8 unit 11 input-vlan-map swap-swap
user@PE2# set ge-8/0/8 unit 11 input-vlan-map vlan-id 4094
user@PE2# set ge-8/0/8 unit 11 input-vlan-map inner-vlan-id 4093
user@PE2# set ge-8/0/8 unit 11 output-vlan-map swap-swap
```

3. Configure el identificador del enrutador para identificar el dispositivo de enrutamiento.

```
[edit]
user@PE2# edit routing-options
[edit routing-options]
user@PE2# set router-id 3.3.3.3
```

4. Configure los protocolos MPLS, OSPF y LDP.

```
[edit]
user@PE2# edit protocols
[edit protocols]
user@PE2# set mpls interface all
user@PE2# set mpls interface fxp0.0 disable
user@PE2# set ospf area 0.0.0.0 interface all
user@PE2# set ospf area 0.0.0.0 interface fxp0.0 disable
user@PE2# set ldp interface all
user@PE2# set ldp interface fxp0.0 disable
```

5. Configure el circuito de capa 2.

```
[edit protocols]
user@PE2# set l2circuit neighbor 4.4.4.4 interface ge-8/0/8.11 virtual-circuit-id 1003
user@PE2# set l2circuit neighbor 3.3.3.3 interface ge-8/0/8.11 no-control-word
```

6. Configure el MEP.

```
[edit protocols]
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md level 4
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma continuity-check interval 1s
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 1 interface ge-8/0/8.11
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 1 direction up
user@PE2# set oam ethernet connectivity-fault-management maintenance-domain md maintenance-association ma mep 1 remote-mep 2
```

7. Configure el firewall.

```
[edit]
user@PE2# edit firewall
[edit firewall]
user@PE2# set three-color-policer abc logical-interface-policer
user@PE2# set three-color-policer abc two-rate color-blind
user@PE2# set three-color-policer abc two-rate committed-information-rate 10m
user@PE2# set three-color-policer abc two-rate committed-burst-size 1500
user@PE2# set three-color-policer abc two-rate peak-information-rate 20m
user@PE2# set three-color-policer abc two-rate peak-burst-size 15k
```

8. Confirme la configuración.

```
[edit]
user@PE2# commit
```

Resultados

Desde el modo de configuración, ingrese los comandos `show interfaces`, `show protocols`, `show routing-options` y `show firewall` para confirmar la configuración. Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
user@PE2# show interfaces
interfaces {
```

```
    ge-8/0/8 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 11 {
            encapsulation vlan-ccc;
            vlan-tags outer 2000 inner 1000;
            input-vlan-map {
                swap-swap;
                vlan-id 4094;
                inner-vlan-id 4093;
            }
            output-vlan-map swap-swap;
            layer2-policer {
                input-three-color abc;
            }
            family ccc;
        }
    }
    ge-8/0/9 {
        unit 0 {
            family inet {
                address 12.1.1.2/24;
            }
            family mpls;
        }
    }
    ae0 {
        unit 0 {
            family inet;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 3.3.3.3/32;
            }
        }
```

```
    }
}
```

```
user@PE2# show protocols
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
    ldp {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    l2circuit {
        neighbor 4.4.4.4 {
            interface ge-8/0/8.11 {
                virtual-circuit-id 1003;
                no-control-word;
            }
        }
    }
    oam {
        ethernet {
            connectivity-fault-management {
                maintenance-domain md {
                    level 4;
                    maintenance-association ma {
                        continuity-check {
                            interval 1s;
```

```
                        }
                        mep 1 {
                            interface ge-8/0/8.11;
                            direction up;
                            remote-mep 2;
                        }
                    }
                }
            }
        }
    }
}
```

```
user@PE2# show routing-options
routing-options {
    router-id 3.3.3.3;
}
```

```
user@PE2# show firewall
firewall {
    three-color-policer abc {
        logical-interface-policer;
        two-rate {
            color-blind;
            committed-information-rate 10m;
            committed-burst-size 1500;
            peak-information-rate 20m;
            peak-burst-size 15k;
        }
    }
}
```

Verificación

in this section

- Visualización de ETH-LM | **317**

Para iniciar la sesión de medición de pérdida de tramas Ethernet, ejecute el comando.`monitor ethernet loss-measurement maintenance-domain md maintenance-association ma mep 1` La pérdida de tramas se calcula recopilando los valores de contador aplicables a las tramas de servicio de entrada y salida en las que los contadores mantienen un recuento de tramas de datos transmitidas y recibidas entre un par de MEP. Las estadísticas de medición de pérdidas se recuperan como salida del comando.`monitor ethernet loss-measurement` También puede emitir el comando para mostrar estadísticas de ETH-LM.`show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11`

Visualización de ETH-LM

Propósito

Vea las estadísticas de ETH-LM.

Acción

Desde el modo operativo, ingrese el comando `show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11`.

```
user@PE1> show oam ethernet connectivity-fault-management interfaces detail ge-5/0/4.11
Interface name: ge-5/0/4.11 , Interface status: Active, Link status: Up
  Maintenance domain name: md, Format: string, Level: 4
    Maintenance association name: ma, Format: string
    Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
    Interface status TLV: none, Port status TLV: none
    Connection Protection TLV: no
    MEP identifier: 2, Direction: up, MAC address: 00:24:dc:9b:96:76
    MEP status: running
    Defects:
      Remote MEP not receiving CCM                  : no
      Erroneous CCM received                        : no
      Cross-connect CCM received                    : no
      RDI sent by some MEP                          : no
      Some remote MEP's MAC in error state          : no
    Statistics:
      CCMs sent                                     : 59
      CCMs received out of sequence                 : 0
      LBMs sent                                     : 0
      Valid in-order LBRs received                  : 0
      Valid out-of-order LBRs received              : 0
      LBRs received with corrupted data             : 0
```

```
    LBRs sent                                    : 0
    LTMs sent                                    : 0
    LTMs received                                : 0
    LTRs sent                                    : 0
    LTRs received                                : 0
    Sequence number of next LTM request          : 0
    1DMs sent                                    : 0
    Valid 1DMs received                          : 0
    Invalid 1DMs received                        : 0
    Out of sync 1DMs received                    : 0
    DMMs sent                                    : 0
    Valid DMMs received                          : 0
    Invalid DMMs received                        : 0
    DMRs sent                                    : 0
    Valid DMRs received                          : 0
    Invalid DMRs received                        : 0
    LMMs sent                                    : 10
    Valid LMMs received                          : 0
    Invalid LMMs received                        : 0
    LMRs sent                                    : 0
    Valid LMRs received                          : 10
    Invalid LMRs received                        : 0
    SLMs sent                                    : 0
    Valid SLMs received                          : 0
    Invalid SLMs received                        : 0
    SLRs sent                                    : 0
    Valid SLRs received                          : 0
    Invalid SLRs received                        : 0
  Remote MEP count: 1
    Identifier    MAC address        State    Interface
        1     00:05:85:76:e5:30       ok   ge-5/0/4.11
```

Significado

Se muestran los detalles y las estadísticas de la interfaz Ethernet. Este resultado indica que la interfaz está activa y que su estado de vínculo es `.ge-5/0/4.11up` Su nombre de dominio de mantenimiento es y su nivel es `.md4` El identificador MEP de la interfaz se indica como y su dirección es `.ge-5/0/4.112up` En la sección de estadísticas, el resultado indica que la interfaz envió LMM y que la interfaz recibió LMR válidos.`1010`

SEE ALSO

Introducción a la administración de errores de conectividad (CFM) de OAM | 20

VÍNCULOS RELACIONADOS

Visión general de OAM del servicio Ethernet ITU-T Y.1731 | 213

Configurar mediciones de pérdida sintética Ethernet | 338

Configurar un perfil de iterador

in this section

- Configuración de un perfil de iterador | 319
- Comprobación de la configuración de un perfil de iterador | 323
- Administración de estadísticas de iterador | 328
- Configuración de un MEP remoto con un perfil de iterador | 337

Utilice este tema para configurar un perfil de iterador que transmita periódicamente paquetes de medición de SLA para la medición de retrasos y pérdidas. También puede ver y borrar las estadísticas del iterador, así como configurar un MEP remoto con un perfil de iterador.

Configuración de un perfil de iterador

Puede crear un perfil de iterador con sus parámetros para transmitir periódicamente paquetes de medición SLA en forma de tramas compatibles con ITU-Y.1731 para la medición de retardo o pérdida.

Para crear un perfil de iterador:

1. En el modo de configuración, vaya al siguiente nivel de jerarquía:

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Configure el iterador de supervisión de medición de SLA:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# edit sla-iterator-profiles
```

3. Configure un perfil de iterador, por ejemplo, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles]
user@host# set i1
```

4. (Opcional) Configure el tiempo de ciclo, que es la cantidad de tiempo (en milisegundos) entre la transmisión consecutiva de tramas SLA para una conexión, con valores de 10 a 3.600.000. El valor predeterminado es 1000 ms.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set cycle-time cycle-time-value
```

5. (Opcional) Configure el período de iteración, que indica el número máximo de ciclos por iteración (el número de conexiones registradas en un iterador no puede superar este valor), con valores del 1 al 2000. El valor predeterminado es 2000.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set iteration-period iteration-period-value
```

6. Configure el tipo de medición como medición de pérdida, medición estadística de pérdida de trama o medición de retardo bidireccional.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set measurement-type (loss | statistical-frame-loss | two-way-delay)
```

7. (Opcional) Configure el peso de cálculo para el retraso con valores del 1 al 65.535. El valor predeterminado es 1 (aplicable solo para la medición de retardo bidireccional).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set calculation-weight delay delay-value
```

8. (Opcional) Configure el peso de cálculo para la variación de retardo con valores del 1 al 65.535. El valor predeterminado es 1 (aplicable solo para la medición de retardo bidireccional).

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set calculation-weight delay-variation delay-variation-value
```

9. (Opcional) Configure el valor de umbral para el retraso de trama promedio, en microsegundos, para la medición de retardo de trama Ethernet bidireccional (ETH-DM). Cuando se supera el umbral configurado para el retraso medio de fotogramas, se genera una captura SNMP para ETH-DM. El rango es de 1 a 4294967295 microsegundos.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set avg-fd-twoway-threshold avg-fd-twoway-threshold-value
```

10. (Opcional) Configure el valor de umbral para la variación de retardo de trama promedio, en microsegundos, para la medición de retardo de trama Ethernet bidireccional (ETH-DM). Cuando se supera el umbral configurado para la variación de retardo de fotograma promedio, se genera una captura SNMP para ETH-DM. El rango es de 1 a 4294967295 microsegundos.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set avg-ifdv-twoway-threshold avg-ifdv-twoway-threshold-value
```

11. (Opcional) Configure el valor de umbral para el índice de pérdida de fotogramas promedio, en miliporcentaje, en la dirección ascendente o descendente para la medición de pérdida de Ethernet (ETH-LM) y la medición de pérdida sintética de Ethernet (ETH-SLM). Cuando se supera el umbral

configurado para la relación de pérdida de trama directa promedio, se genera una captura SNMP para ETH-LM y ETH-SLM. El rango es de 1 a 100000 mili-por ciento.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set avg-flr-forward-threshold avg-flr-forward-threshold-value
```

12. (Opcional) Configure el valor de umbral para el índice de pérdida de trama promedio, en miliporcentaje, en la dirección hacia atrás o hacia abajo para la medición de pérdida de Ethernet (ETH-LM) y la medición de pérdida sintética de Ethernet (ETH-SLM). Cuando se supera el umbral configurado para el promedio de la relación de pérdida de tramas hacia atrás, se genera una captura SNMP para ETH-LM y ETH-SLM. El rango es de 1 a 100000 mili-por ciento.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set avg-flr-backward-threshold avg-flr-backward-threshold-value
```

13. Configure la instrucción para detener el iterador (es decir, deshabilitar el perfil del iterador).`disable`

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set disable
```

14. Compruebe la configuración.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles]
user@host# show i1

    cycle-time cycle-time-value;
    iteration-period iteration-period-value;
    measurement-type  (loss | two-way-delay);
    avg-fd-twoway-threshold avg-fd-twoway-threshold-value;
    avg-ifdv-twoway-threshold avg-ifdv-twoway-threshold-value;
    avg-flr-forward-threshold avg-flr-forward-threshold-value;
    avg-flr-backward-threshold avg-flr-backward-threshold-value;

    calculation-weight {
        delay delay-weight;
        delay-variation delay-variation-weight;
```

```
    }
    calculation-weight {
        delay delay-weight;
        delay-variation delay-variation-weight;
    }
```

SEE ALSO

Modo proactivo para la medición de SLA | 224

Comprobación de la configuración de un perfil de iterador

in this section

- Visualización de la configuración de un perfil de iterador para la medición de retardo bidireccional | 323
- Visualización de la configuración de un perfil de iterador para la medición de pérdidas | 325
- Visualización de la configuración de un MEP remoto con un perfil de iterador | 326
- Deshabilitar un perfil de iterador | 327

Los temas siguientes ilustran la configuración de un perfil de iterador para una medición de retardo bidireccional, para la medición de pérdidas y para un punto final de asociación de mantenimiento remoto (MEP). Los temas también ilustran la desactivación de un perfil de iterador con la instrucción para la medición bidireccional y la desactivación de un perfil de iterador con el comando para un MEP remoto.`disabledeactivate`

Visualización de la configuración de un perfil de iterador para la medición de retardo bidireccional

in this section

- Propósito | 324
- Acción | 324
- Significado | 324

Propósito

Mostrar la configuración de un perfil de iterador para la medición de retardo bidireccional configurado en el tema Configuración de un perfil de iterador con los siguientes valores:"Configuración de un perfil de iterador" en la página 319

- `profile-name`—**i1**
- — milisegundos`cycle-time`**1000**
- — ciclos por segundo`iteration-period`**2000**
- `delay`—**1**
- —:`delay-variation`**1**

Acción

Para mostrar información sobre el perfil del iterador, ejecute el comando en el nivel de jerarquía:`show[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles]`

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-
profiles]
user@host# show
i1 {
    cycle-time 1000;
    iteration-period 2000;
    measurement-type two-way-delay;
    calculation-weight {
        delay 1;
        delay-variation 1;
    }
}
```

Significado

La configuración de un perfil de iterador para la medición bidireccional se muestra como se esperaba con valores establecidos.

Visualización de la configuración de un perfil de iterador para la medición de pérdidas

in this section

- Propósito | **325**
- Acción | **325**
- Significado | **326**

Propósito

Mostrar la configuración de un perfil de iterador para la medición de pérdidas tal y como se configura en el tema Configuración de un perfil de iterador con los siguientes valores:"Configuración de un perfil de iterador" en la página 319

- `profile-name`—**12**
- — milisegundos`cycle-time`**1000**
- — ciclos por segundo`iteration-period`**2000**

Acción

Para mostrar información sobre el perfil del iterador, ejecute el comando en el nivel de jerarquía:`show`[`edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles`]

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-
profiles]
user@host# show
12 {
    cycle-time 1000;
    iteration-period 2000;
    measurement-type loss;

}
```

Significado

La configuración de un perfil de iterador para la medición de pérdidas se muestra como se esperaba con valores establecidos.

Visualización de la configuración de un MEP remoto con un perfil de iterador

in this section

- Propósito | **326**
- Acción | **327**
- Significado | **327**

Propósito

Mostrar la configuración de un remoteMEP tal como está configurado en el tema Configuración de un MEP remoto con un perfil de iterador con los siguientes valores:"Configuración de un MEP remoto con un perfil de iterador" en la página 337

- `profile-name`—**i3**
- `maintenance-domain`—**default-1**
- `maintenance-association`—**1**
- `short-name-format`—**2octet**
- `mep`—**1**
- `remote-mep`—**1**
- `data-tlv-size`—**1**
- `iteration-count`—**1**
- `priority`—**1**

Acción

Para mostrar información sobre el MEP remoto, ejecute el comando en el nivel de jerarquía:`show[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance association ma1 mep 1 remote-mep 1]`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1
maintenance association 1  short-name-format 2octet mep 1 remote-mep 1]
user@host# show
sla-iterator-profile i3 {
    data-tlv-size 1;
    iteration-count 1;
    priority 1;
}
```

Significado

La configuración de un MEP remoto para la medición bidireccional se muestra como se esperaba con valores establecidos.

Deshabilitar un perfil de iterador

in this section

- Propósito | 327
- Acción | 328

Propósito

Para deshabilitar un perfil de iterador para la medición de retardo bidireccional y para un MEP remoto.

Acción

- Para deshabilitar un perfil de iterador (por ejemplo, i1) con el comando de configuración para la medición bidireccional en el nivel de jerarquía:`disable[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles i1]`

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles i1]
user@host# disable
```

- Para deshabilitar un perfil de iterador para un MEP remoto (por ejemplo, i2) con el comando de configuración en el nivel de jerarquía:`deactivate[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance association ma1 mep 1 remote-mep 1]`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain default-1 maintenance association ma1 mep 1 remote-mep 1]
user@host# deactivate sla-iterator-profile i2
```

VÍNCULOS RELACIONADOS

Modo proactivo para la medición de SLA | 224

Administración de estadísticas de iterador

in this section

Visualización de estadísticas de iterador | 328
Borrar estadísticas de iterador | 336

Visualización de estadísticas de iterador

in this section

Propósito | 329

Acción | 329

Propósito

Recuperar y mostrar estadísticas de iteradores.

Los iteradores múltiples se pueden asociar a un MEP remoto. Sin embargo, de forma predeterminada, solo se muestra un resultado perteneciente a un perfil de iterador.

Acción

- Para mostrar las estadísticas del iterador para el MEP remoto y el perfil del iterador con MEP que pertenecen a la asociación de mantenimiento y dentro del dominio de mantenimiento (aquí, el perfil del iterador está configurado para la medición de retraso bidireccional):`1i1ma1default-1i1`

```
user@host> show oam ethernet connectivity-fault-management sla-iterator-statistics sla-
iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i1, Iterator Id: 1
Iterator cycle time: 10ms, Iteration period: 1 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:24 ago)
Reset reason: Adjacency flap

Iterator delay measurement statistics:
Delay weight: 1, Delay variation weight: 1
DMM sent                                          : 23898520
DMM skipped for threshold hit                     : 11000
DMM skipped for threshold hit window              : 0
DMR received                                      : 23851165
DMR out of sequence                               : 1142
DMR received with invalid time stamps             : 36540
Average two-way delay                             : 129 usec
Average two-way delay variation                   : 15 usec
Average one-way forward delay variation           : 22 usec
Average one-way backward delay variation          : 22 usec
```

```
Weighted average two-way delay                    : 134 usec
Weighted average two-way delay variation          : 8 usec
Weighted average one-way forward delay variation  : 6 usec
Weighted average one-way backward delay variation : 2 usec
```

Los campos de salida se enumeran en el orden aproximado en el que aparecen.

Tabla 17: Visualización de estadísticas de iterador para campos de salida de medición de retardo de Ethernet

Nombre del campo de salida	Descripción del campo de salida
`Maintenance domain`	Nombre de dominio de mantenimiento.
`Level`	Nivel de dominio de mantenimiento configurado.
`Maintenance association`	Nombre de la asociación de mantenimiento.
`Local MEP id`	Identificador numérico del eurodiputado local.
`Remote MEP id`	Identificador numérico del eurodiputado remoto.
`Remote MAC address`	Dirección MAC de unidifusión del eurodiputado remoto.
`Iterator name`	Nombre del iterador.
`Iterator Id`	Identificador numérico del iterador.
`Iterator cycle time`	Número de ciclos (en milisegundos) transcurridos entre la transmisión consecutiva de tramas SLA para esta conexión
`Iteration period`	Número máximo de ciclos por iteración
`Iterator status`	Estado actual del iterador, ya sea en ejecución o detenido.

Tabla 17: Visualización de estadísticas de iterador para campos de salida de medición de retardo de Ethernet *(Continued)*

Nombre del campo de salida	Descripción del campo de salida
`Infinite iterations`	Estado de la iteración como infinito o finito.
`Counter reset time`	Fecha y hora en que se restableció el contador.
`Reset reason`	Motivo para restablecer el contador.
`Delay weight`	Cálculo del peso del retraso.
`Delay variation weight`	Cálculo del peso de la variación del retardo.
`DMM sent`	Tramas PDU del mensaje de medición de retardo (DMM) enviadas al MEP par en esta sesión.
`DMM skipped for threshold hit`	Número de tramas DMM enviadas al MEP par en esta sesión omitidas durante el alcance del umbral.
`DMM skipped for threshold hit window`	Número de tramas DMM enviadas al MEP par en esta sesión omitidas durante la última ventana de impacto de umbral.
`DMR received`	Número de fotogramas de respuesta a la medición de retardo (DMR) recibidos.
`DMR out of sequence`	Número total de paquetes DMR fuera de secuencia recibidos.
`DMR received with invalid time stamps`	Número total de tramas DMR recibidas con marcas de tiempo no válidas.
`Average two-way delay`	Retraso medio de fotogramas bidireccional para las estadísticas mostradas.

Tabla 17: Visualización de estadísticas de iterador para campos de salida de medición de retardo de Ethernet *(Continued)*

Nombre del campo de salida	Descripción del campo de salida
`Average two-way delay variation`	"fluctuación de fotogramas" bidireccional promedio para las estadísticas mostradas.
`Average one-way forward delay variation`	Variación media del retardo de avance unidireccional para las estadísticas que se muestran en microsegundos.
`Average one-way backward delay variation`	Variación media del retardo hacia atrás unidireccional para las estadísticas que se muestran en microsegundos.
`Weighted average two-way delay`	Promedio ponderado de retraso bidireccional para las estadísticas mostradas en microsegundos.
`Weighted average two-way delay variation`	Variación media ponderada del retardo bidireccional para las estadísticas mostradas en microsegundos.
`Weighted average one-way forward delay variation`	Promedio ponderado de la variación del retardo de avance unidireccional para las estadísticas que se muestran en microsegundos.
`Weighted average one-way backward delay variation`	Promedio ponderado de la variación del retraso hacia atrás en un sentido para las estadísticas que se muestran en microsegundos.

- Para mostrar las estadísticas del iterador para el MEP remoto y el perfil del iterador con MEP que pertenecen a la asociación de mantenimiento y dentro del dominio de mantenimiento (aquí, el perfil del iterador está configurado para la medición de pérdidas):`1i2ma1default-1i1`

```
user@host> show oam ethernet connectivity-fault-management sla-iterator-statistics sla-
iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i2, Iterator Id: 2
```

```
Iterator cycle time: 1000ms, Iteration period: 2000 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:25 ago)
Reset reason: Adjacency flap

Iterator loss measurement statistics:
LMM sent                              : 238970
LMM skipped for threshold hit         : 60
LMM skipped for threshold hit window  : 0
LMR received                          : 238766
LMR out of sequence                   : 43

Accumulated transmit statistics:
Near-end (CIR)                        : 0
Far-end (CIR)                         : 0
Near-end (EIR)                        : 0
Far-end (EIR)                         : 0

Accumulated loss statistics:
Near-end (CIR)                        : 0 (0.00%)
Far-end (CIR)                         : 0 (0.00%)
Near-end (EIR)                        : 0 (0.00%)
Far-end (EIR)                         : 0 (0.00%)

Last loss measurement statistics:
Near-end (CIR)                        : 0
Far-end (CIR)                         : 0
Near-end (EIR)                        : 0
Far-end (EIR)                         : 0
```

Los campos de salida se enumeran en el orden aproximado en el que aparecen.

Tabla 18: Visualización de estadísticas de iterador para campos de salida de medición de pérdida de Ethernet

Nombre del campo de salida	Descripción del campo de salida
`Maintenance domain`	Nombre de dominio de mantenimiento.

Tabla 18: Visualización de estadísticas de iterador para campos de salida de medición de pérdida de Ethernet *(Continued)*

Nombre del campo de salida	Descripción del campo de salida
`Level`	Nivel de dominio de mantenimiento configurado.
`Maintenance association`	Nombre de la asociación de mantenimiento.
`Local MEP id`	Identificador numérico del eurodiputado local.
`RemoteMEP identifier`	Identificador numérico del eurodiputado remoto.
`Remote MAC address`	Dirección MAC de unidifusión del eurodiputado remoto.
`Iterator name`	Nombre del iterador.
`Iterator Id`	Identificador numérico del iterador.
`Iterator cycle time`	Número de ciclos (en milisegundos) transcurridos entre la transmisión consecutiva de tramas SLA para esta conexión
`Iteration period`	Número máximo de ciclos por iteración
`Iterator status`	Estado actual del iterador, ya sea en ejecución o detenido.
`Infinite iterations`	Estado de la iteración como infinito o finito.
`Counter reset time`	Fecha y hora en que se restableció el contador.
`Reset reason`	Motivo para restablecer el contador.
`LMM sent`	Número de tramas PDU del mensaje de medición de pérdidas (LMM) enviadas al MEP par en esta sesión.

Tabla 18: Visualización de estadísticas de iterador para campos de salida de medición de pérdida de Ethernet *(Continued)*

Nombre del campo de salida	Descripción del campo de salida
`LMM skipped for threshold hit`	Número de tramas LMM enviadas al MEP par en esta sesión omitidas durante el alcance del umbral.
`LMM skipped for threshold hit window`	Número de tramas LMM enviadas al MEP par en esta sesión omitidas durante la última ventana de impacto de umbral.
`LMR received`	Número de tramas LMR recibidas.
`LMR out of sequence`	Número total de paquetes LMR fuera de secuencia recibidos.
`Near-end (CIR)`	Pérdida de tramas asociada con las tramas de datos de entrada para las estadísticas mostradas.
`Far-end (CIR)`	Pérdida de tramas asociada con las tramas de datos de salida para las estadísticas mostradas.
`Near-end (EIR)`	Pérdida de tramas asociada con las tramas de datos de entrada para las estadísticas mostradas.
`Far-end (EIR)`	Pérdida de tramas asociada con las tramas de datos de salida para las estadísticas mostradas.

SEE ALSO

Modo proactivo para la medición de SLA | **224**

show oam ethernet connectivity-fault-management sla-iterator-statistics

clear oam ethernet connectivity-fault-management sla-iterator-statistics

Borrar estadísticas de iterador

in this section

- Propósito | 336
- Acción | 336

Propósito

Borrar estadísticas del iterador.

Se pueden asociar varios iteradores con MEP remoto. Sin embargo, de forma predeterminada, solo se puede borrar un resultado perteneciente a un perfil de iterador.

Acción

- Para borrar las estadísticas del iterador para el MEP remoto y el perfil del iterador con MEP pertenecientes a la asociación de mantenimiento y dentro del dominio de mantenimiento:`1i1ma1default-1`

```
user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-
iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
```

- Para borrar las estadísticas del iterador para el MEP remoto y el perfil del iterador con MEP pertenecientes a la asociación de mantenimiento y dentro del dominio de mantenimiento:`1i2ma1default-1`

```
user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-
iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
```

SEE ALSO

Modo proactivo para la medición de SLA | 224

show oam ethernet connectivity-fault-management sla-iterator-statistics

clear oam ethernet connectivity-fault-management sla-iterator-statistics

Configuración de un MEP remoto con un perfil de iterador

Puede asociar un punto final de asociación de mantenimiento remoto (MEP) con más de un perfil de iterador.

Para configurar un MEP remoto con un perfil de iterador:

1. En el modo de configuración, vaya al siguiente nivel de jerarquía:

```
user@host# edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name maintenance-association ma-name mep mep-id
```

2. Configure el MEP remoto con valores del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id]
user@host# set remote-mep remote-mep-id
```

3. Establezca el perfil del iterador.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# set sla-iterator-profile profile-name
```

4. (Opcional) Establezca el tamaño de la parte del TLV de datos del marco de datos Y.1731 con valores de 1 a 1400 bytes. El valor predeterminado es 1.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile
profile-name]
user@host# set data-tlv-size size
```

5. (Opcional) Establezca el recuento de iteraciones, que indica el número de iteraciones en las que esta conexión debe participar en el iterador para adquirir mediciones de SLA, con valores del 1 al 65.535. El valor predeterminado es 0 (es decir, iteraciones infinitas).

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile
profile-name]
user@host# set iteration-count count-value
```

6. (Opcional) Establezca la prioridad, que es el valor que se envía en las tramas de datos Y.1731, con valores del 0 al 7. El valor predeterminado es 0.`vlan-pcp`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile
profile-name]
user@host# set priority priority-value
```

7. Compruebe la configuración.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# show
sla-iterator-profile profile-name  {
    data-tlv-size size;
    iteration-count count-value;
    priority priority-value;
}
```

SEE ALSO

Modo proactivo para la medición de SLA | 224

MEP remoto

VÍNCULOS RELACIONADOS

Visión general de OAM del servicio Ethernet ITU-T Y.1731 | 213

Configurar sesiones de medición de retardo de trama Ethernet | 234

Configurar mediciones de pérdida sintética Ethernet

in this section

- Directrices para configurar ETH-SLM | 339

- Inicio de una sesión proactiva de ETH-SLM | **340**
- Inicio de una sesión ETH-SLM bajo demanda | **345**
- Administración de estadísticas de ETH-SLM y recuentos de tramas de ETH-SLM | **346**
- Solución de problemas de fallas con ETH-SLM | **354**

Utilice este tema para comprender las directrices para configurar la medición de pérdidas sintéticas y cómo iniciar una sesión de medición de pérdidas sintéticas. Hay dos tipos de sesiones de medición de pérdidas sintéticas: Proactivo y bajo demanda. En este tema se describen ambos. Además, en el tema se muestra cómo ver y borrar las estadísticas sintéticas de medición de pérdidas y cómo solucionar errores con SLM.

Directrices para configurar ETH-SLM

Tenga en cuenta los siguientes puntos cuando configure la funcionalidad de ETH-SLM:

- La aplicación de supervisión para Ethernet OAM se inicia en el motor de enrutamiento principal. Cuando se produce un proceso de cambio con estado, la aplicación de supervisión se deshabilita. Para ETH-SLM bajo demanda, no se aplica la compatibilidad *con el cambio de motor de enrutamiento (*GRES). Para ETH-SLM proactivo, los iteradores del acuerdo de nivel de servicio (SLA) se restauran durante un proceso de cambio de estado. Si las adyacencias no agotan el tiempo de espera, las estadísticas de ETH-SLM se conservan y ETH-SLM proactivo admite GRES.

- ETH-SLM se inicia solo cuando finaliza la sesión del MEP. La compatibilidad unificada de actualización de software en servicio (ISSU) con ETH-SLM depende de la compatibilidad unificada de ISSU con CFM. Para CFM, se admite ISSU unificada mediante el TLV de umbral de pérdida para evitar la pérdida de conectividad de CFM durante la actualización. El MEP receptor o destino aumenta el tiempo umbral durante la terminación de las sesiones. Si inicia una operación de ISSU unificada cuando ETH-SLM a petición está en curso, los mensajes de solicitud y respuesta de SLM se pierden en el motor de reenvío de paquetes local.

  Cuando se solicita un ETH-SLM bajo demanda, si el MEP de origen local se somete a un ISSU unificado, se muestra un mensaje que indica que el MEP está experimentando un ISSU unificado. Si el MEP remoto está experimentando una ISSU unificada (detectada a través del TLV de umbral de pérdida), se muestra un mensaje que indica que el MEP remoto está experimentando una ISSU unificada. Además, si no es posible identificar si la ISSU unificada está en curso en un MEP remoto, los paquetes de SLM se pierden en el sistema donde la ISSU unificada está en curso y los resultados del cálculo de la pérdida no proporcionan una causa válida para la pérdida. La ISSU unificada no es compatible con ETH-SLM bajo demanda y proactiva.

- El número máximo de perfiles de iterador de SLA que se pueden configurar en el sistema es 255.

- ETH-SLM no es compatible con el servicio de LAN privada virtual (VPLS) (no se admiten mediciones punto a multipunto). Las tramas ETH-SLM no se generan con la dirección de destino de clase 1 de multidifusión. Del mismo modo, ETH-SLM no responde a las solicitudes de ETH-SLM con DA de multidifusión. ETH-SLM para VPLS para conexión Ethernet punto a punto se admite mediante direcciones MAC de destino de unidifusión dirigida, aunque no se admiten topologías punto a multipunto.
- Se puede usar una dirección de destino de unidifusión en entornos aprovisionados para conexiones punto a punto. Sin embargo, requiere que la dirección de destino de unidifusión del MEP descendente se haya configurado en el MEP que transmite una señal de indicación de alarma (AIS).
- ETH-SLM no es compatible con los eurodiputados intermedios en interfaces de conmutación de etiquetas (LSI).
- ETH-SLM es compatible con interfaces Ethernet agregadas (ae)
- El número de sesiones de ETH-SLM para ETH-SLM proactivas que se pueden admitir está limitado al número total de iteradores que se pueden admitir en el sistema. Esta limitación incluye la compatibilidad del iterador para otros tipos de medición, como pérdida, pérdida de fotogramas estadísticos y retraso bidireccional. Se agrega un nuevo tipo de iterador, SLM, para admitir ETH-SLM. El número total de iteradores de SLA que puede configurar en el sistema es igual al número total de iteraciones admitidas en el sistema.
- Para SLM bajo demanda, el período mínimo entre dos solicitudes de SLM es de 100 milisegundos.
- Para SLM proactivo, el período mínimo entre dos solicitudes de SLM es de 10 milisegundos para el modo distribuido y de 100 milisegundos para el modo no distribuido.
- Las tramas ETH-SLM siempre se marcan como no aptas para la caída de conformidad con la norma UIT-T Y.1731.

SEE ALSO

Descripción general de la medición de pérdidas sintéticas de Ethernet | 227

Monitoreo de medición de pérdidas sintéticas de Ethernet

Inicio de una sesión proactiva de ETH-SLM

in this section

- Configuración de interfaces MEP | 341
- Configuración de un perfil de iterador para ETH-SLM | 342

- Asociación del perfil iterador con los eurodiputados para ETH-SLM | 344

Para iniciar una sesión proactiva de medición de pérdida sintética Ethernet (ETH-SLM), debe configurar las interfaces Ethernet en puntos finales de asociación de mantenimiento (MEP) en los que deben analizarse los paquetes transmitidos con pérdida de trama sintética. A continuación, debe crear un perfil de iterador para transmitir paquetes de medición de acuerdo de nivel de servicio (SLA) para ETH-SLM y asociar los MEP locales y remotos con el perfil.

Configuración de interfaces MEP

Antes de poder iniciar una sesión de medición de pérdida de trama sintética Ethernet en un servicio Ethernet, debe configurar dos enrutadores de la serie ACX para que admitan ETH-SLM.

Para configurar una interfaz Ethernet en un enrutador de la serie ACX para que admita ETH-SLM:

1. En cada enrutador, configure dos interfaces Ethernet físicas o lógicas conectadas por una VLAN. La siguiente configuración es típica de las interfaces lógicas de etiqueta única:

```
[edit interfaces]
interface {
    ethernet-interface-name {
        vlan-tagging;
        unit logical-unit-number {
            vlan-id vlan-id; # Both interfaces on this VLAN
        }
    }
}
```

   Ambas interfaces utilizarán el mismo ID de VLAN.

2. En cada enrutador, adjunte MEPs pares a las dos interfaces. La siguiente configuración es típica:

```
[edit protocols]
oam {
    ethernet {
        connectivity-fault-management {
            maintenance-domain md-name { # On both routers
                level number;
                maintenance-association ma-name { # On both routers
                    continuity-check {
```

```
                        interval 100ms;
                        hold-interval 1;
                    }
                    mep mep-id { # Attach to VLAN interface
                        auto-discovery;
                        direction (up | down);
                        interface interface-name;
                        priority number;
                    }
                }
            }
        }
    }
}
```

Configuración de un perfil de iterador para ETH-SLM

Puede crear un perfil de iterador con sus parámetros para transmitir periódicamente paquetes de medición de SLA en forma de tramas compatibles con ITU-Y.1731 para la medición de pérdidas sintéticas.

> **NOTA**: ACX5048 y ACX5096 enrutadores admiten un tiempo de ciclo de iterador de solo 1 segundo o más.

Para crear un perfil de iterador:

1. En el modo de configuración, vaya al siguiente nivel de jerarquía:

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Configure el iterador de supervisión de medición de SLA:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# edit sla-iterator-profiles
```

3. Configure un perfil de iterador, por ejemplo, i1:

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles]
user@host# set i1
```

4. (Opcional) Configure el tiempo de ciclo, que es la cantidad de tiempo (en milisegundos) entre la transmisión consecutiva de tramas SLA para una conexión, con un valor de 10 a 3.600.000. El valor predeterminado es 1000 ms.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set cycle-time cycle-time-value
```

5. (Opcional) Configure el período de iteración, que indica el número máximo de ciclos por iteración (el número de conexiones registradas en un iterador no puede superar este valor), con un valor comprendido entre 1 y 2000. El valor predeterminado es 2000.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set iteration-period iteration-period-value
```

6. Configure el tipo de medición como medición de pérdida sintética.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set measurement-type slm
```

7. Configure la instrucción para detener el iterador (es decir, deshabilitar el perfil del iterador).`disable`

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles i1]
user@host# set disable
```

8. Compruebe la configuración.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-
iterator-profiles]
user@host# show i1
```

```
cycle-time cycle-time-value;
iteration-period iteration-period-value;
measurement-type slm;
```

Asociación del perfil iterador con los eurodiputados para ETH-SLM

Puede asociar un punto final de asociación de mantenimiento remoto (MEP) con más de un perfil de iterador.

Para configurar un MEP remoto con un perfil de iterador:

1. En el modo de configuración, vaya al siguiente nivel de jerarquía:

```
user@host# edit protocols oam ethernet connectivity-fault-management maintenance-domain md-
name maintenance-association ma-name mep mep-id
```

2. Configure el identificador MEP remoto con un valor del 1 al 8191.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id]
user@host# set remote-mep remote-mep-id
```

3. Establezca el perfil del iterador.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# set sla-iterator-profile profile-name
```

4. (Opcional) Establezca el tamaño de la parte TLV de datos del marco de datos Y.1731 con un valor de 1 a 1400 bytes. El valor predeterminado es 1.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile
profile-name]
user@host# set data-tlv-size size
```

5. (Opcional) Establezca el recuento de iteraciones, que indica el número de iteraciones en las que esta conexión debe participar en el iterador para adquirir mediciones de SLA, con un valor del 1 al 65.535. El valor predeterminado es 0 (es decir, iteraciones infinitas).

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile
profile-name]
user@host# set iteration-count count-value
```

6. (Opcional) Establezca la prioridad, que es el valor que se envía en las tramas de datos Y.1731, con un valor del 0 al 7. El valor predeterminado es 0.`vlan-pcp`

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id sla-iterator-profile
profile-name]
user@host# set priority priority-value
```

7. Compruebe la configuración.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
user@host# show
sla-iterator-profile profile-name  {
    data-tlv-size size;
    iteration-count count-value;
    priority priority-value;
}
```

VÍNCULOS RELACIONADOS

Descripción general de la medición de pérdidas sintéticas de Ethernet | 227

Monitoreo de medición de pérdidas sintéticas de Ethernet

Inicio de una sesión ETH-SLM bajo demanda

Para iniciar una sesión de medición de pérdida sintética Ethernet (ETH-SLM) bajo demanda, escriba el comando en modo operativo y especifique el MEP del mismo nivel por su dirección MAC o por su identificador MEP.`monitor ethernet synthetic-loss-measurement one-way`

Por ejemplo:

```
user@host> monitor ethernet synthetic-loss-measurement 00:05:85:73:39:4a maintenance-domain md6
maintenance-association ma6 count 10
ETH-SLM request to 00:05:85:73:39:4a, interface ge-1/0/0.0
      Synthetic Loss measurement statistics:
       SLM packets sent                          : 100
       SLR packets received                      : 100
       Accumulated SLM statistics:
       Local TXFC1 value                         : 100
       Local RXFC1 value                         : 100
       Last Received SLR frame TXFCf(tc)         : 100
       Last Received SLR frame TXFCb(tc)         : 100
       SLM Frame Loss:
       Frame Loss (far-end)                      : 0 (0.00 %)
       Frame Loss (near-end)                     : 0 (0.00 %)
```

NOTA: Si intenta supervisar retrasos en una dirección MAC inexistente, debe presionar para salir explícitamente del comando y volver al símbolo del sistema de la CLI.**Ctrl** + **C**`monitor ethernet synthetic-loss-measurement`

SEE ALSO

Descripción general de la medición de pérdidas sintéticas de Ethernet | **227**

Monitoreo de medición de pérdidas sintéticas de Ethernet

Administración de estadísticas de ETH-SLM y recuentos de tramas de ETH-SLM

in this section

- Visualización solo de estadísticas de ETH-SLM | **347**
- Visualización de estadísticas y recuentos de fotogramas de ETH-SLM | **348**
- Visualización de los recuentos de tramas ETH-SLM para los eurodiputados adjuntando la entidad CFM | **350**

- Visualización de los recuentos de tramas ETH-SLM para los eurodiputados por interfaz o nivel de dominio | **351**
- Borrar estadísticas y recuentos de tramas de ETH-SLM | **352**
- Borrar estadísticas de iterador | **353**

Visualización solo de estadísticas de ETH-SLM

in this section

- Propósito | **347**
- Acción | **347**
- Significado | **348**

Propósito

Muestre estadísticas de ETH-SLM bajo demanda.

De forma predeterminada, el comando muestra estadísticas de ETH-SLM bajo demanda para los MEP de la asociación de mantenimiento de CFM especificada dentro del dominio de mantenimiento de CFM especificado.`show oam ethernet connectivity-fault-management synthetic-loss-statistics`

Acción

- Para mostrar las estadísticas de ETH-SLM bajo demanda recopiladas para los eurodiputados que pertenecen a la asociación de mantenimiento dentro del dominio de mantenimiento:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management synthetic-loss-statistics
maintenance-domain md1 maintenance-association ma1
```

- Para mostrar las estadísticas de ETH-SLM bajo demanda recopiladas para las sesiones de ETH-SLM para el MEP local que pertenece a la asociación de mantenimiento dentro del dominio de mantenimiento:`201ma2md2`

```
user@host> show oam ethernet connectivity-fault-management synthetic-loss-statistics
maintenance-domain md2 maintenance-association ma2 local-mep 201
```

- Para mostrar las estadísticas de ETH-SLM bajo demanda recopiladas para las sesiones de ETH-SLM de los eurodiputados locales pertenecientes a la asociación de mantenimiento dentro del dominio de mantenimiento al MEP remoto:`ma3md3302`

```
user@host> show oam ethernet connectivity-fault-management synthetic-loss-statistics
maintenance-domain md3 maintenance-association ma3 remote-mep 302
```

Significado

El resultado muestra estadísticas de ETH-SLM bajo demanda para los MEP de la asociación de mantenimiento especificada dentro del dominio de mantenimiento especificado. Para obtener más información sobre el resultado de este comando y las descripciones de los campos de salida, consulte .`show oam ethernet connectivity-fault-management synthetic-loss-statistics`

SEE ALSO

> *Mostrar estadísticas de pérdidas sintéticas de conectividad Ethernet de OAM Ethernet*

Visualización de estadísticas y recuentos de fotogramas de ETH-SLM

in this section

- Propósito | **349**
- Acción | **349**
- Significado | **349**

Propósito

Muestre estadísticas de ETH-SLM bajo demanda y recuentos de tramas de ETH-SLM.

De forma predeterminada, el comando muestra estadísticas de ETH-SLM bajo demanda y recuentos de tramas para MEP en la asociación de mantenimiento de CFM especificada dentro del dominio de mantenimiento de CFM especificado.`show oam ethernet connectivity-fault-management mep-statistics`

Acción

- Para mostrar las estadísticas de ETH-SLM bajo demanda y los recuentos de tramas de ETH-SLM para los MEP en asociación de mantenimiento dentro del dominio de mantenimiento:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
md1 maintenance-association ma1
```

- Para mostrar las estadísticas de ETH-SLM bajo demanda y los recuentos de tramas de ETH-SLM para el MEP local en la asociación de mantenimiento dentro del dominio de mantenimiento:`201ma2md2`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
md2 maintenance-association ma2 local-mep 201
```

- Para mostrar las estadísticas de ETH-SLM bajo demanda y los recuentos de tramas de ETH-SLM para el MEP local en la asociación de mantenimiento dentro del dominio de mantenimiento que participa en una sesión de ETH-SLM con el MEP remoto:`ma3md3302`

```
user@host> show oam ethernet connectivity-fault-management mep-statistics maintenance-domain
ma3 maintenance-association ma3 remote-mep 302
```

Significado

El resultado muestra estadísticas de ETH-SLM bajo demanda y recuentos de tramas ETH-SLM para MEP en la asociación de mantenimiento especificada dentro del dominio de mantenimiento especificado. Para obtener más información sobre el resultado de este comando y las descripciones de los campos de salida, consulte .`show oam ethernet connectivity-fault-management mep-statistics`

SEE ALSO

> *Mostrar estadísticas MEP de conectividad Ethernet de OAM*

Visualización de los recuentos de tramas ETH-SLM para los eurodiputados adjuntando la entidad CFM

in this section

- Propósito | 350
- Acción | 350
- Significado | 351

Propósito

Muestre los recuentos de tramas ETH-SLM bajo demanda para los puntos finales de asociación de mantenimiento (MEP) de CFM.

De forma predeterminada, el comando muestra la información de la base de datos de CFM para los MEP de la asociación de mantenimiento de CFM especificada dentro del dominio de mantenimiento de CFM especificado.`show oam ethernet connectivity-fault-management mep-database`

> **NOTA**: En el enrutador conectado al MEP iniciador para una sesión unidireccional, o en el enrutador conectado al MEP receptor para una sesión bidireccional, solo puede mostrar los recuentos de tramas ETH-SLM y no los detalles de la base de datos MEP.

Acción

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-SLM) para todos los MEP en MA dentro del dominio de mantenimiento:`ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
ma1 maintenance-association ma1
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-SLM) solo para el MEP local en MA dentro del dominio de mantenimiento:`201ma1md1`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
md2 maintenance-association ma2 local-mep 201
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-SLM) solo para el MEP remoto en MA dentro del dominio de mantenimiento:`302ma3md3`

```
user@host> show oam ethernet connectivity-fault-management mep-database maintenance-domain
ma3 maintenance-association ma3 remote-mep 302
```

Significado

El resultado muestra los recuentos de fotogramas ETH-SLM para los MEP dentro de un dominio de mantenimiento particular, o para un MEP local o remoto específico. Para obtener más información sobre el resultado de este comando y las descripciones de los campos de salida, consulte .`show oam ethernet connectivity-fault-management mep-database`

Visualización de los recuentos de tramas ETH-SLM para los eurodiputados por interfaz o nivel de dominio

in this section

- Propósito | **351**
- Acción | **352**
- Significado | **352**

Propósito

Muestre los recuentos de tramas ETH-SLM bajo demanda para los puntos finales de asociación de mantenimiento (MEP) de CFM.

De forma predeterminada, el comando muestra la información de la base de datos CFM para los MEP conectados a interfaces Ethernet habilitadas para CFM en el enrutador o en un nivel de dominio de mantenimiento.`show oam ethernet connectivity-fault-management interfaces` Para las interfaces Ethernet compatibles con ETH-SLM, los recuentos de tramas también se muestran cuando se especifica la opción de comando o .`detailextensive`

> **NOTA**: En el enrutador conectado al MEP del iniciador, solo puede mostrar los recuentos de tramas ETH-SLM y no los detalles de la base de datos MEP.

Acción

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-SLM) para todos los MEP conectados a interfaces Ethernet habilitadas para CFM en el enrutador:

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-SLM) solo para los MEP conectados a la interfaz de enrutador habilitada para CFM:`ge-5/2/9.0`

```
user@host> show oam ethernet connectivity-fault-management interfaces ge-5/2/9.0 detail
```

- Para mostrar la información de la base de datos CFM (incluidos los recuentos de tramas ETH-SLM) solo para los MEP encerrados dentro de los dominios de mantenimiento de CFM en el nivel:`6`

```
user@host> show oam ethernet connectivity-fault-management interfaces level 6 detail
```

Significado

El resultado muestra los recuentos de tramas ETH-SLM para los MEP para la interfaz especificada. Para obtener más información sobre el resultado de este comando y las descripciones de los campos de salida, consulte .`show oam ethernet connectivity-fault-management interfaces`

Borrar estadísticas y recuentos de tramas de ETH-SLM

in this section

- Propósito | **352**
- Acción | **353**

Propósito

Borre las estadísticas de ETH-SLM bajo demanda y los recuentos de tramas de ETH-SLM.

De forma predeterminada, las estadísticas y los recuentos de fotogramas se eliminan para todos los MEP conectados a interfaces habilitadas para CFM en el enrutador. Sin embargo, puede filtrar el ámbito del comando especificando un nombre de interfaz.

Acción

- Para borrar las estadísticas de ETH-SLM bajo demanda y los recuentos de tramas ETH-SLM para todos los MEP conectados a interfaces habilitadas para CFM en el enrutador:

```
user@host> clear oam ethernet connectivity-fault-management synthetic-loss-measurement
```

- Para borrar las estadísticas de ETH-SLM bajo demanda y los recuentos de tramas ETH-SLM solo para los eurodiputados adjuntos a la interfaz lógica:`ge-0/5.9.0`

```
user@host> clear oam ethernet connectivity-fault-management synthetic-loss-measurement
ge-0/5/9.0
```

Borrar estadísticas de iterador

in this section

- Propósito | **353**
- Acción | **354**

Propósito

Borre las estadísticas de iterador existentes y los contadores proactivos de ETH-SLM.

Se pueden asociar varios iteradores con MEP remoto. Sin embargo, de forma predeterminada, solo se puede borrar un resultado perteneciente a un perfil de iterador.

Acción

- Para borrar las estadísticas del iterador para el MEP remoto y el perfil del iterador con MEP pertenecientes a la asociación de mantenimiento dentro del dominio de mantenimiento:`1i1ma1default-1`

```
user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-
iterator i1 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
```

- Para borrar las estadísticas del iterador para el MEP remoto y el perfil del iterador con MEP pertenecientes a la asociación de mantenimiento dentro del dominio de mantenimiento:`1i2ma1default-1`

```
user@host> clear oam ethernet connectivity-fault-management sla-iterator-statistics sla-
iterator i2 maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 1
```

VÍNCULOS RELACIONADOS

Medición de pérdidas sintéticas con conectividad Ethernet OAM Clear OAM

Mostrar estadísticas de pérdidas sintéticas de conectividad Ethernet de OAM Ethernet

Mostrar interfaces de administración de fallos de conectividad Ethernet de OAM

Mostrar estadísticas MEP de conectividad Ethernet de OAM

Mostrar base de datos MEP de conectividad Ethernet de OAM

Solución de problemas de fallas con ETH-SLM

in this section

Problema | 355

Solución | 355

Problema

Description

La aplicación de medición de pérdida sintética Ethernet (ETH-SLM) no funciona correctamente para el cálculo de la pérdida de tramas utilizando tramas sintéticas en lugar de tráfico de datos

Solución

Realice los pasos siguientes para analizar y depurar cualquier problema con la funcionalidad de ETH-SLM.

1. Asegúrese de que ETH-SLM esté configurado (ya sea proactivo o bajo demanda) para iniciar tramas SLM. Compruebe la configuración.
2. Examine cualquier error que pueda haberse producido en la sesión de CFM para la que está habilitada la función ETH-SLM. La sesión de CFM debe estar en estado activo para que la funcionalidad de ETH-SLM funcione correctamente. Utilice el comando para comprobar si la sesión de CFM está en estado activo.`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `local-mep` *`mep-id`* `remote-mep` *`remote-mep-id`*
3. Si las sesiones MEP están activas, utilice el comando show adecuado para verificar las estadísticas de ETH-SLM y analizar si las tramas ETH-SLM se transmiten o reciben.
4. Si la transmisión de tramas ETH-SLM no se realiza correctamente después de intentar todos los pasos de solución de problemas anteriores, habilite las operaciones de seguimiento para Ethernet CFM incluyendo la instrucción en el nivel de jerarquía [].`traceoptionsedit protocols oam ethernet connectivity-fault-management`

```
[edit protocols oam ethernet connectivity-fault-management]
traceoptions {
    file <filename> <files number  <match regular-expression microsecond-stamp>> <size size>
<world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

SEE ALSO

Descripción general de la medición de pérdidas sintéticas de Ethernet | 227

Monitoreo de medición de pérdidas sintéticas de Ethernet

VÍNCULOS RELACIONADOS

Visión general de OAM del servicio Ethernet ITU-T Y.1731 | 213

Configurar la medición de pérdida de tramas Ethernet | 281

Indicación de alarma Ethernet

in this section

- Descripción general de la función de señal de indicación de alarma Ethernet (ETH-AIS) | 356
- Descripción general de la señal de indicación de alarma Ethernet | 361
- Configuración de ETH-AIS en un MEP CFM | 363
- Configuración de la señal de indicación de alarma en enrutadores de la serie ACX | 368

Utilice lo siguiente para obtener más información sobre la señal de indicación de alarma Ethernet (ETH-AIS) y cómo configurar ETH-AIS en dispositivos.

Descripción general de la función de señal de indicación de alarma Ethernet (ETH-AIS)

in this section

- Descripción de ETH-AIS en un dominio de mantenimiento | 357
- Detección de errores en un dominio de mantenimiento | 357
- Términos definidos | 359

La función de señal de indicación de alarma Ethernet (ETH-AIS) permite a un proveedor de servicios desplegar un servicio Ethernet determinar si existe un error de conectividad en el nivel de dominio del proveedor o en un nivel inferior. Cuando el error se produce en el nivel de dominio del proveedor, el proveedor de servicios corrige el error y, cuando el error se produce en un nivel inferior, el proveedor puede ignorar el error o ponerse en contacto con las autoridades pertinentes para abordar el error.

Las siguientes secciones explican ETH-AIS, algunos casos de uso que determinan cuándo generar y propagar paquetes ETH-AIS y términos asociados en detalle:

Descripción de ETH-AIS en un dominio de mantenimiento

El UIT-T desarrolló la Y.1731 como recomendación para las funciones y mecanismos de operación, administración y mantenimiento (OAM) para redes basadas en Ethernet, incluidas funciones OAM como ETH-AIS, señal bloqueada de Ethernet (ETH-LCK), señal de prueba Ethernet (ETH-Test), conmutación de protección automática Ethernet (ETH-APS), canal de comunicación de mantenimiento Ethernet (ETH-MCC), OAM experimental de Ethernet (ETH-EXP), OAM específica del proveedor de Ethernet (ETH-VSP) y monitoreo del rendimiento. Para obtener información acerca del dominio de mantenimiento y términos relacionados, consulte "Términos definidos" en la página 359.

De acuerdo con los estándares Y.1731, un MEP de servidor es una función combinada de la función de terminación de la capa del servidor y la función de adaptación de la capa de servicios Ethernet del servidor. El MEP del servidor notifica a los MEP de la capa de servicios Ethernet (ETH) cuando detecta un error. A continuación, la función de terminación de la capa del servidor ejecuta los mecanismos OAM específicos de la capa del servidor y ETH-AIS suprime las alarmas en la capa del servidor.

Tenga en cuenta que ETH-AIS no es aplicable a las redes STP (Spanning Tree Protocol).

ETH-AIS le permite suprimir alarmas cuando se detecta una condición de falla. Usando ETH-AIS, un proveedor de servicios puede diferenciar entre fallas en diferentes niveles.

ETH-AIS ofrece muchas ventajas que incluyen:

- Los proveedores de servicios no necesitan activar alarmas si hay fallas de nivel inferior.
- Los proveedores de servicios pueden proporcionar un reembolso a sus suscriptores o hacer uso de un reembolso de su proveedor de Internet en función de la falta de disponibilidad del servicio.

Los enrutadores de la serie MX son compatibles con ETH-AIS UIT-ITU UIT-T Y.1731 para proporcionar administración de fallos a los proveedores de servicios que proporcionan servicios de Ethernet de operadora mediante el estándar IEEE 802.1ag.

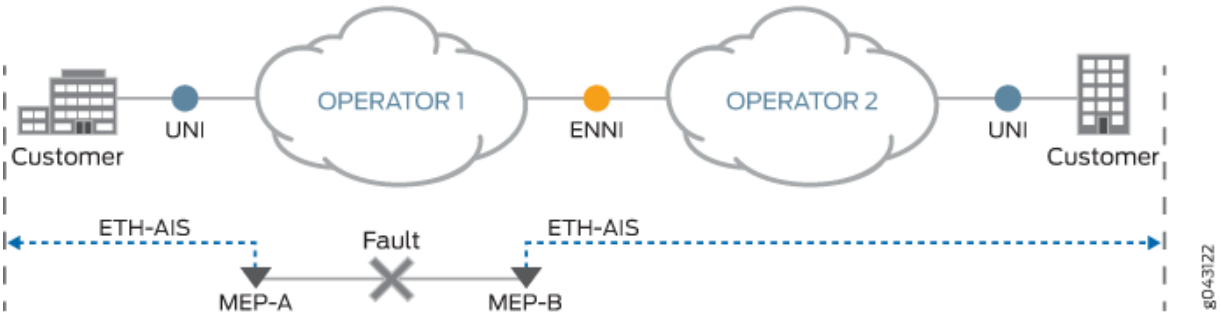
> **NOTA**: El chasis virtual de la serie MX no admite la señal de indicación de alarma Ethernet (ETH-AIS).

Detección de errores en un dominio de mantenimiento

En el escenario representado en la figura 1 de la página xyz, tiene un nivel de proveedor de servicios y un nivel de cliente. Dos proveedores de servicios, el Operador-1 y *el Operador-2*, se consideran a efectos ilustrativos. Supongamos que se produce un error en el nivel de dominio de mantenimiento del operador 1 que tiene MEP-A y MEP-B en sus límites de nivel de dominio de mantenimiento. Para notificar los fallos a un sistema de gestión de red y evitar la notificación de alarmas desde el nivel del cliente para el mismo fallo, MEP-A y MEP-B transmiten una señal de indicación de alarma (AIS) en

direcciones opuestas, señalando así a los niveles superiores y a la red del Operador-2 sobre la falla, de modo que se supriman las alarmas.

La señalización se logra a través de la transmisión y propagación de unidades de datos de protocolo AIS (PDU). Debe habilitar AIS explícitamente en todos los eurodiputados a nivel de proveedor de servicios. Un MEP que está configurado para emitir tramas con información ETH-AIS generalmente se encuentra en la capa del servidor y continúa transmitiendo tramas periódicas con información de ETH-AIS hasta que se borra la condición de defecto. Cuando un MEP cliente recibe las tramas ETH-AIS, suprime las alarmas de pérdida de continuidad asociadas con sus MEP pares.



Tenga en cuenta que, en ausencia de AIS, un MEP de cliente reanuda la generación de alarmas de pérdida de continuidad cuando detecta las condiciones de defecto de pérdida de continuidad de su capa de servidor.

Para la conectividad de capa de servicios Ethernet punto a punto, un MEP solo tiene un MEP par. Por lo tanto, no hay ambigüedad con respecto al MEP par para el cual el MEP debe suprimir las alarmas cuando recibe la información de ETH-AIS.

Para la conectividad de capa de servicios Ethernet multipunto, un MEP que recibe información de ETH-AIS no puede determinar el MEP exacto que encontró el error y, por lo tanto, no puede aislar el MEP del mismo nivel exacto para suprimir las alarmas. Para evitar este escenario, Y.1731 recomienda suprimir las alarmas para todos los MEP pares en el mismo nivel de dominio, independientemente del estado de conectividad en una configuración de conectividad de capa de servicios Ethernet multipunto.

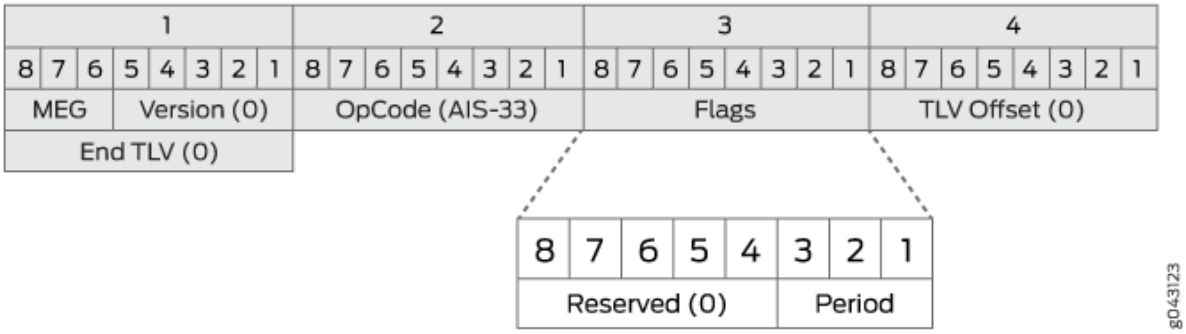
Tabla 19 en la página 359 enumera los comandos de modo operativo que puede utilizar en un dominio de mantenimiento para comprobar los distintos parámetros pertenecientes a un MEP.

Tabla 19: Comandos del modo operativo

Comprobar	Comandos del modo operativo
Si la configuración de AIS está configurada correctamente en un CFM MEP.	`show protocols oam ethernet connectivity-fault-management action-profile`
Estadísticas de tramas AIS.	`show oam ethernet connectivity-fault-management interfaces detail` `show oam ethernet connectivity-fault-management mep-statistics maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `remote-mep` *`mep-id`* `local-mep` *`mep-id`*
Si se ha producido algún evento que haya activado AIS.	`show oam ethernet connectivity-fault-management mep-database maintenance-domain` *`md-name`* `maintenance-association` *`ma-name`* `remote-mep` *`mep-id`* `local-mep` *`mep-id`*
Estado de las sesiones CFM para fallos que activan AIS en el MEP.	`show oam ethernet connectivity-fault-management interfaces detail`

Términos definidos

- Transmisión AIS: un MEP al detectar una condición de defecto transmite tramas AIS en una dirección opuesta a la de sus pares MEP. La periodicidad de la transmisión de tramas AIS se basa en el período de transmisión AIS. Se recomienda un período de transmisión AIS de 1 segundo. La primera trama AIS siempre debe transmitirse inmediatamente después de la detección de una condición de defecto.
- Recepción AIS: al recibir una trama AIS, un MEP la examina para asegurarse de que el nivel de dominio de mantenimiento de la trama es el mismo que su propio nivel de dominio de mantenimiento. El campo de período de la trama indica el período en el que se pueden esperar las tramas AIS. Cuando un MEP recibe una trama AIS, detecta la condición de defecto. Tras la detección, cuando no se reciben tramas AIS en un intervalo de 3,5 veces (el período de transmisión AIS indicado en las tramas AIS recibidas), el MEP borra la condición de defecto AIS. Cuando se borra la condición AIS y todavía existen defectos, los eurodiputados continúan informando de las alarmas.
- Formato PDU AIS: los campos del formato PDU AIS son:



1. Nivel MEG: también llamado nivel de dominio de mantenimiento, es un campo de 3 bits que se utiliza para llevar el nivel de dominio de mantenimiento del MEG cliente.

2. Versión: el valor siempre es 0.

3. OpCode: el valor de este tipo de PDU es AIS (33).

4. Indicadores: los primeros cinco bits se reservan y se establecen en 0. El elemento de información de 3 bits transportado en los tres bits menos significativos se conoce como el período que contiene el valor de la periodicidad de transmisión AIS como se ilustra en :Tabla 20 en la página 360

Tabla 20: Periodicidad de transmisión AIS

Banderas [3:1]	Valor del período	Comentarios
000-011	Valor no válido	Valor no válido para AIS
100	1s	1 fotograma por segundo
101	Valor no válido	Valor no válido para AIS
110	1 minuto	1 fotograma por minuto
111	Valor no válido	Valor no válido para AIS

5. Desplazamiento de TLV: se establece en 0.

6. TLV final: valor de octeto de todos los ceros.

- Capa de servidor y capa de cliente: estas capas forman parte del modelo funcional de red de transporte de la Recomendación UIT-T G.805. Este modelo se basa en el concepto de capas dentro de una red de transporte. Una red de transporte se divide en varias redes de capa de transporte independientes que tienen una asociación cliente-servidor entre redes de capa adyacentes.

- Dominio de mantenimiento: para habilitar la administración de errores de conectividad (CFM) en una interfaz Ethernet, se crean y configuran dominios de mantenimiento, asociaciones de mantenimiento y puntos finales de mantenimiento (MEP) en una red. Puede configurar hasta ocho niveles de dominio de mantenimiento en una red. Cada nivel de dominio de mantenimiento es una parte de la red donde se pueden supervisar y corregir los problemas de conectividad. El dominio del proveedor y el dominio del cliente son algunos ejemplos de dominios de mantenimiento. Cada dominio de mantenimiento tiene una asociación de mantenimiento. Cada asociación de mantenimiento incluye MEP y puntos intermedios de mantenimiento (MIP) en ese dominio. Los MEP se encuentran en el límite del dominio y los MIP se encuentran dentro del dominio. Los MEP generan y transmiten mensajes de verificación de continuidad (CCM) a intervalos configurados a toda la asociación de mantenimiento para verificar la conectividad en la red.

- Capa de servicios Ethernet (ETH): capa del modelo de red Ethernet metropolitano, en la que esta capa es responsable de los servicios OAM necesarios para admitir los servicios Ethernet en la red.

SEE ALSO

> Mostrar interfaces de administración de fallos de conectividad Ethernet de OAM
>
> *Mostrar estadísticas MEP de conectividad Ethernet de OAM*

Descripción general de la señal de indicación de alarma Ethernet

Los enrutadores de la serie ACX son compatibles con la función de señal de indicación de alarma Ethernet UIT-T Y.1731 (ETH-AIS) para proporcionar administración de fallos a los proveedores de servicios. ETH-AIS le permite suprimir alarmas cuando se detecta una condición de falla. Con ETH-AIS, un administrador puede diferenciar entre fallas a nivel de cliente o fallas a nivel de proveedor.

La ventaja de ETH-AIS es:

- Los clientes no necesitan activar alarmas debido a fallas de nivel inferior.

- Los clientes pueden obtener un reembolso basado en la falta de disponibilidad del servicio.

Cuando se detecta una condición de error, un punto final de mantenimiento (MEP) genera paquetes ETH-AIS para los niveles de cliente configurados durante un período especificado hasta que se borre la condición de error. Cualquier MEP configurado para generar señales de paquetes ETH-AIS a un nivel superior al suyo. Un eurodiputado que recibe ETH-AIS reconoce que el fallo está en un nivel inferior y, a continuación, suprime las alarmas en el nivel actual.

Los enrutadores de la serie ACX admiten la generación de PDU ETH-AIS para MEP de servidor en función de las siguientes condiciones de defecto:

- Pérdida de conectividad (detección de pérdida de vínculo físico)
- Circuito de capa 2 o VPN de capa 2 inactivo

La señalización de indicación de alarma se realiza a través de la transmisión y propagación de PDU ETH-AIS. ETH-AIS debería habilitarse en los eurodiputados. Un MEP que está configurado para emitir paquetes con información ETH-AIS es generalmente de capa de servidor y continúa transmitiendo paquetes periódicos con información ETH-AIS hasta que se borra la condición de defecto. Los eurodiputados del CFM, al recibir las PDU de ETH-AIS, suprimen las alarmas de pérdida de continuidad asociadas con sus pares eurodiputados. Un MEP reanuda la generación de alarmas de pérdida de continuidad al detectar condiciones de pérdida de defecto de continuidad en ausencia de una condición ETH-AIS.

Para la conectividad Ethernet punto a punto, un MEP tiene un solo MEP par. Por lo tanto, un MEP suprime las alarmas en su par MEP cuando recibe la información de ETH-AIS.

Para la conectividad Ethernet multipunto, un MEP que recibe información ETH-AIS no puede determinar el MEP exacto que encontró una condición de falla y, por lo tanto, no podrá aislar al MEP par exacto para la supresión de alarmas. El UIT-T Y.1731 recomienda suprimir las alarmas para todos los diputados al Parlamento Europeo, independientemente del estado de conectividad.

Transmisión AIS: un MEP al detectar una condición de defecto transmite PDU ETH-AIS en una dirección opuesta a sus pares MEP. La transmisión de PDU de ETH-AIS se basa en un período de transmisión de ETH-AIS configurado. Se recomienda un período de transmisión ETH-AIS de 1 segundo. La primera PDU ETH-AIS debe transmitirse inmediatamente después de la detección de una condición de defecto.

Recepción AIS: un MEP al recibir PDU ETH-AIS lo examina para asegurarse de que su nivel de dominio de mantenimiento (MD) corresponde al mismo nivel de MD. Al recibir una PDU ETH-AIS, el MEP detecta una condición de defecto. Tras la detección de una condición de defecto, si no se reciben PDU de ETH-AIS dentro de un intervalo de 3,5 veces el período de transmisión de ETH-AIS indicado en las PDU de ETH-AIS recibidas anteriormente, el MEP borra la condición de defecto. Después de que se elimine la condición de falla, los eurodiputados continúan reportando alarmas.

NOTA: Los enrutadores de la serie ACX no son compatibles con ETH-AIS UIT-T-Y.1731 para servicios de capa 2 (puente).

Las siguientes son las limitaciones para el servidor MEP

- La activación de mensajes ETH-AIS sobre servicios (circuito de capa 2 y VPN de capa 2) por parte del MEP del servidor de pérdida de enlaces se realiza con el mejor esfuerzo. Esto se debe a que la

transmisión de mensajes ETH-AIS es independiente del estado del servicio y no hay garantía para entregar los mensajes ETH-AIS antes de que el servicio deje de funcionar.

- La protección de pseudocables con sesión CFM-MEP no es supervisada por el servidor-MEP porque ya existe una entidad para supervisar la protección de pseudocables para el servicio (circuito de capa 2 y VPN de capa 2).

SEE ALSO

Mostrar estadísticas MEP de conectividad Ethernet de OAM

Configuración de ETH-AIS en un MEP CFM

in this section

- Configuración de un perfil de acción | **364**
- Configuración de una acción que debe realizarse cuando se detecta una alarma AIS | **365**
- Adjuntar el perfil de acción a un eurodiputado del CFM | **366**

Los enrutadores de la serie MX son compatibles con la función de señal de indicación de alarma Ethernet UIT-T Y.1731 (ETH-AIS) para proporcionar administración de fallos a los proveedores de servicios. ETH-AIS permite al proveedor de servicios suprimir alarmas cuando se detecta una condición de falla.

Los siguientes puntos deben tenerse en cuenta cuando ETH-AIS se configura en un dominio de mantenimiento:

- La transmisión o recepción de AIS en un MEP no anula la instrucción configurada en el nivel jerárquico .`lowest-priority-defect`[`edit protocols oam ethernet connectivity-fault-management maintenance-domain` *`domain-name`* `maintenance-association` *`ma-name`* `mep` *`mep-id`*] Por lo tanto, las alarmas se informan de acuerdo con la prioridad de defectos configurada.

- Las alarmas se reportan incluso cuando los niveles de dominio más altos intercambian MCPs a un ritmo más rápido que los niveles de dominio inferiores.

- El punto intermedio de asociación de mantenimiento (MIP) es transparente para las tramas ETH-AIS, es decir, las MIP no realizan ninguna acción en respuesta a las tramas ETH-AIS.

- Cuando el proveedor de servicios solicita al MEP que genere un AIS para un nivel inferior o para el mismo nivel, se rechaza la solicitud.

- La generación de AIS se detiene cuando el MEP borra el MEP remoto dentro de la asociación de mantenimiento.
- Cuando la instrucción está habilitada para un MEP, la información del MEP remoto se borra después de que expire el intervalo de espera configurado.`auto-discovery`

Las siguientes tareas explican cómo habilitar ETH-AIS en un dominio de mantenimiento, configurar una acción que se debe realizar cuando se detecta un defecto y adjuntar el perfil de acción a un MEP CFM:

Configuración de un perfil de acción

Para configurar un perfil de acción para ETH-AIS:

1. Vaya al nivel jerárquico .`[edit protocols oam ethernet connectivity-fault-management]`

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management
```

2. Configure un perfil de acción para usarlo cuando uno o más eurodiputados remotos estén inactivos.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# edit action-profile action-profile-name
```

3. Configure un evento que deba supervisarse.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name]
user@host# edit event
```

4. Configure la condición de defecto que genera una señal de indicación de alarma.

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
event]
user@host# edit ais-trigger-condition
```

5. Configure la instrucción para informar al operador cuando se pierda la conectividad física entre los MEP pares.`adjacency-loss`

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
event ais-trigger-condition]
user@host# set adjacency-loss
```

6. Configure la declaración para informar al operador que se deben considerar todos los posibles defectos para activar la señal de indicación de alarma.`all-defects`

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
event ais-trigger-condition]
user@host# set all-defects
```

7. Configure la instrucción para informar al operador cuando el MEP reciba mensajes de verificación de continuidad de conexión cruzada (CCM) y para activar una señal de indicación de alarma en respuesta.`cross-connect-ccm`

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
event ais-trigger-condition]
user@host# set cross-connect-ccm
```

8. Configure la instrucción para informar al operador cuando el MEP reciba CCM con ID MEP o nivel de dominio de mantenimiento inesperados y se active una alarma AIS en respuesta.`erroneous-ccm`

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
event ais-trigger-condition]
user@host# set erroneous-ccm
```

9. Configure la instrucción para informar al operador de que se ha recibido un mensaje AIS del MEP par en su propio nivel de mantenimiento.`receive-ais`

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
event ais-trigger-condition]
user@host# set receive-ais
```

Configuración de una acción que debe realizarse cuando se detecta una alarma AIS

Configure una acción que se realizará cuando se detecte una alarma AIS.

1. Vaya al nivel jerárquico .`[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name action]`

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management action-profile action-
profile-name action
```

2. Configure la instrucción para registrar el evento que generó el mensaje AIS.`log-and-generate-ais`

```
[edit protocols oam ethernet connectivity-fault-management action-profile action-profile-name
action]
user@host# edit log-and-generate-ais
```

3. Configure el intervalo entre los mensajes AIS que debe recibir el MEP como 1 minuto o 1 segundo.

```
[edit protocols oam ethernet connectivity-fault-management  action-profile action-profile-
name action log-and-generate-ais]
user@host# set interval (1m | 1s)
```

4. Configure el intervalo de nivel de dominio de mantenimiento del servidor del MEP del 1 al 7.

```
[edit protocols oam ethernet connectivity-fault-management  action-profile action-profile-
name action log-and-generate-ais]
user@host# set level level
```

5. Configure la prioridad 802.1p del paquete AIS del 1 al 7.

```
[edit protocols oam ethernet connectivity-fault-management  action-profile action-profile-
name action log-and-generate-ais]
user@host# set priority level
```

Adjuntar el perfil de acción a un eurodiputado del CFM

Después de configurar un evento y una acción para supervisar en un perfil de acción, debe adjuntar el perfil de acción a un CFM MEP.

1. Vaya al nivel jerárquico .`[edit protocols oam ethernet connectivity-fault-management]`

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management
```

2. Configure el dominio de mantenimiento con un nombre.

```
[edit protocols oam ethernet connectivity-fault-management]
user@host# edit maintenance-domain md-name
```

3. Configure el dominio de mantenimiento con un nivel de grupo de entidades de mantenimiento (MEG) de cliente o un nivel de asociación de mantenimiento (el nivel en el que existen el punto intermedio de asociación de mantenimiento (MIP) de la capa de cliente y los MEP, del 0 al 7.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# edit level level
```

NOTA: No puede configurar un nivel de dominio de mantenimiento que sea inferior o igual que el nivel de asociación de mantenimiento al que está asociado.

4. Configure la asociación de mantenimiento.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name]
user@host# edit maintenance-association ma-name
```

5. Configure la verificación de continuidad que se realiza en todos los MEPs a nivel de dominio enviando MCPs con un intervalo entre dos MCPs —100 milisegundos, 10 milisegundos, 1 segundo, 10 segundos, 1 minuto o 10 minutos— y el número de MCPs que deben perderse antes de marcar un MEP como caído.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name]
user@host# set continuity-check interval (100ms | 10m | 10ms | 1m | 1s)
user@host# set continuity-check loss-threshold value
```

6. Configure el MEP con un identificador del 1 al 8192.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name]
user@host# set mep mep-id
```

7. Adjunte el perfil de acción configurado al MEP.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id]
user@host# set action-profile action-profile-name
```

8. Configure la interfaz del MEP a través de la cual se transmiten los MCPs.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id]
user@host# set interface interface-name
```

9. Configure la dirección para que los MCPs viajen al siguiente MEP como arriba o abajo.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id]
user@host# set direction (down | up)
```

10. Configure la prioridad 802.1p para los MCPs y el paquete de seguimiento de vínculos del 0 al 7.

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain md-name
maintenance-association ma-name mep mep-id]
user@host# set priority priority-value
```

Configuración de la señal de indicación de alarma en enrutadores de la serie ACX

Los enrutadores de la serie ACX son compatibles con la función de señal de indicación de alarma Ethernet UIT-T Y.1731 (ETH-AIS) para proporcionar administración de fallos a los proveedores de servicios. ETH-AIS le permite suprimir alarmas cuando se detecta una condición de falla.

Para admitir la transmisión ETH-AIS, un MEP de CFM requiere la siguiente información de configuración:

- Nivel de grupo de entidades de mantenimiento de clientes: nivel de grupo de entidades de mantenimiento (MEG) en el que existen los puntos intermedios del dominio de mantenimiento (MIP) y los puntos finales de la asociación de mantenimiento (MEP) de la capa de cliente inmediato.
- Período de transmisión de ETH-AIS: determina el intervalo de transmisión de la PDU de ETH-AIS.
- Prioridad: determina la prioridad de los paquetes con información ETH-AIS. Esto es opcional.

Para configurar ETH-AIS en CFM MEP, debe:

- Configurar un perfil de acción con acción ETH-AIS
- Adjunte el perfil de acción al eurodiputado del CFM

Para configurar un perfil de acción con acción ETH-AIS, incluya las siguientes instrucciones en el nivel jerárquico [edit protocols oam ethernet connectivity-fault-management]:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile action-profile-name {
    event {
        adjacency-loss;
        all-defects;
        cross-connect-ccm;
        errored-ccm;
        receive-ais;
    }
    action {
        log-and-generate-ais {
            level [1-7];
            interval 1s | 1m ;
            priority [0-7];
        }
        log-ais;
    }
}
```

Para adjuntar un perfil de acción a un CFM MEP, incluya las siguientes instrucciones en el nivel jerárquico [edit protocols oam ethernet connectivity-fault-management]:

```
maintenance-domain maintenenace-domain-name {
level level-number;
    maintenance-association maintenance-domain-name {
        continuity-check {
            interval 1s;
            loss-threshold 3;
        }
        mep mep-id {
            interface interface-name;
            direction up | down;
            priority priority-value;
            action-profile action-profile-name;
        }
    }
}
```

NOTA: No puede configurar un nivel de dominio de mantenimiento que sea inferior o igual que el nivel al que está asociado.

Para admitir la transmisión ETH-AIS, un MEP de servidor requiere la siguiente información de configuración:

- Definición de MEP de servidor: define la asociación del identificador MEP de servidor a la capa de servidor.
  - Para el circuito de capa 2 y VPN de capa 2, la interfaz lógica conectada a una red de cliente (UNI) sería el identificador de la capa de servidor que debe supervisar el MEP del servidor.
  - Para la detección de pérdida de vínculo físico, la interfaz física bajo el protocolo Ethernet sería el identificador de la capa de servidor que debe ser supervisada por el MEP del servidor.
- Asociación de defectos MEP de servidor: define la asociación de defectos de MEP de servidor a la acción ETH-AIS.
- Perfil de acción de asociación y MEP de servidor: define el enlace de MEP de servidor y perfil de acción.

Para configurar ETH-AIS en el MEP del servidor, debe:

- Cree un perfil de acción con acción ETH-AIS para defectos MEP del servidor.
- Adjuntar el perfil de acción a un MEP de servidor

Para crear un perfil de acción, incluya las siguientes instrucciones en el nivel jerárquico [edit protocols oam ethernet connectivity-fault-management]:

```
[edit protocols oam ethernet connectivity-fault-management]
action-profile action-profile-name {
    event {
        server-mep-defects {
            link-loss-defect;
            l2circuit-defect;
            l2vpn-defect;
        }
    }
    action {
        log-and-generate-ais {
            level 1…n;
            interval 1 second | 1 minute;
```

```
            priority dot1p [range 0-7];
        }
    }
}
```

Para adjuntar un perfil de acción a un MEP de servidor, incluya la siguiente instrucción en el nivel jerárquico [edit protocols oam ethernet connectivity-fault-management]:

```
[edit protocols oam ethernet connectivity-fault-management]
server-mep  mep-identifier {
    protocol l2circuit | l2vpn | ethernet {
        interface interface-name;
    }
    action-profile action-profile-name;
}
```

Modo de transmisión en línea

in this section

- Habilitación de la transmisión en línea de mensajes de comprobación de continuidad para obtener la máxima escala | **371**
- Habilitación de la transmisión en línea de keepalives de gestión de fallos de vínculo para maximizar el escalado | **373**
- Habilitación del modo en línea de monitoreo del rendimiento para lograr la máxima escala | **377**
- Valores de escala CCM y PM en línea admitidos | **379**

Utilice este tema para comprender qué es la transmisión en línea y cómo habilitarla para escalar al máximo para CFM, LFM y funciones de monitoreo de rendimiento.

Habilitación de la transmisión en línea de mensajes de comprobación de continuidad para obtener la máxima escala

El escalado es la capacidad de un sistema para manejar cantidades crecientes de trabajo y continuar funcionando bien. El escalado puede referirse al aumento de la capacidad y la capacidad de manejar cargas de trabajo crecientes, número de suscriptores o sesiones, componentes de hardware, etc. El

protocolo de verificación de continuidad se utiliza para la detección de fallas dentro de una asociación de mantenimiento. Los puntos finales de la asociación de mantenimiento (MEP) envían mensajes de verificación de continuidad (MCP) periódicamente. El tiempo entre las transmisiones de los MCPs se conoce como el intervalo. El diputado receptor mantiene una base de datos de todos los diputados al Parlamento Europeo de la asociación de alimentos.

De forma predeterminada, los CCM son transmitidos por la CPU de una tarjeta de línea, como un concentrador de puerto modular (MPC). Si la duración entre las transmisiones de los MCPs es baja o si los MCPs para una escala de tarjeta de línea específica, entonces le recomendamos que delegue la transmisión de los MCPs al ASIC de reenvío (es decir, al hardware) habilitando la transmisión en línea de los MCPs. La transmisión en línea de MCPs también se conoce como keepalives en línea o Inline-KA. La transmisión en línea permite que el sistema maneje más sesiones de administración de fallas de conectividad (CFM) por tarjeta de línea. Al habilitar la transmisión en línea de MCPs, usted puede lograr la máxima escala de los MCPs.

Para habilitar la transmisión en línea de MCPs, realice los siguientes pasos:

1. En el modo de configuración, vaya al nivel de jerarquía.`[edit protocols oam ethernet connectivity-fault-management performance-monitoring]`

```
[edit]
user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
```

2. Delegue la transmisión de MCPs al hardware habilitando keepalives asistidos por hardware.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-keepalives enable
```

> **NOTA**: La transmisión en línea de MCPs no está habilitada cuando hay una sesión CFM ya establecida. Para habilitar la transmisión en línea, primero debe desactivar la sesión CFM con el comando y, a continuación, reactivar la sesión CFM con el comando.`deactivateactivate`

Para deshabilitar la transmisión en línea, utilice la instrucción.`hardware-assisted-keepalives disable` Después de deshabilitar la transmisión en línea, debe reiniciar el enrutador para que los cambios surtan efecto.

SEE ALSO

Configurar la administración de errores de conectividad para la interoperabilidad durante las actualizaciones de software unificadas en servicio | 55

Habilitación de la transmisión en línea de keepalives de gestión de fallos de vínculo para maximizar el escalado

El escalado es la capacidad de un sistema para manejar cantidades crecientes de trabajo y continuar funcionando bien. El escalado puede referirse al aumento de la capacidad y la capacidad de manejar cargas de trabajo crecientes, número de suscriptores o sesiones, componentes de hardware, etc.

De forma predeterminada, los paquetes LFM keepalive se transmiten mediante el proceso periódico de administración de paquetes en la tarjeta de línea.`ppm` Puede delegar la transmisión de paquetes keepalive de LFM al ASIC de reenvío (es decir, al hardware) habilitando la transmisión en línea. La transmisión en línea de recuerdos LFM también se conoce como keepalives en línea o Inline-KA. Al habilitar la transmisión en línea de paquetes keepalive LFM, puede lograr la máxima escalabilidad de los paquetes keepalive, reducir la carga en el proceso y admitir la actualización de software en servicio (ISSU) de LFM para pares que no sean de Juniper (para un intervalo keepalive de 1 segundo).`ppm`

> **NOTA**: No habilite ni deshabilite la transmisión en línea de LFM cuando ya se haya establecido una sesión de LFM. Para habilitar o deshabilitar la transmisión en línea, primero debe desactivar la sesión LFM existente establecida con el comando y, a continuación, reactivar la sesión LFM con el comando después de habilitar o deshabilitar LFM en línea.`deactivateactivate`

Antes de habilitar la transmisión en línea de paquetes LFM keepalive, realice las siguientes tareas:

- Verifique si alguna sesión de LFM está en línea y activa. Para comprobar si alguna sesión de LFM existente o establecida está en línea y activa, emita el siguiente comando:

```
user@host> show oam ethernet link-fault-management detail
Oct 18 02:04:17
  Interface: ge-0/0/0
    Status: Running, Discovery state: Active Send Local
    Transmit interval: 1000ms, PDU threshold: 3 frames, Hold time: 0ms
    Peer address: 00:00:00:00:00:00
    Flags:0x8
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 28, Event: 0, Variable request: 0, Variable response: 0  = after waiting
for a while count increased by 15
      Loopback control: 0, Organization specific: 0
```

```
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Disabled, Loop status: Unknown
    Detect LOC: Disabled, LOC status: Unknown
```

Las estadísticas de transmisión de OAM reflejan que el proceso está manejando la transmisión de paquetes keepalive de LFM.ppm

- Desactive la sesión LFM para poder habilitar el modo LFM en línea. Para desactivar la sesión LFM, emita el siguiente comando:

```
[edit]
user@host # deactivate protocols oam ethernet link-fault-management interface interface-name
```

- Confirme la configuración. Para confirmar la configuración, ejecute el siguiente comando:

```
[edit]
user@host # commit
```

Para habilitar la transmisión en línea de paquetes keepalive LFM, realice los pasos siguientes:

1. En el modo de configuración, vaya al nivel de jerarquía.`[edit protocols oam ethernet link-fault-management]`

```
[edit]
user@host# edit protocols oam ethernet link-fault-management
```

2. Delegue la transmisión de paquetes keepalive LFM al hardware habilitando keepalives asistidos por hardware.

```
[edit protocols oam ethernet link-fault-management]
user@host# set hardware-assisted-keepalives
```

3. Confirme la configuración.

```
[edit]
user@host # commit
```

4. Reactive la sesión de LFM de la siguiente manera:

```
[edit]
user@host # activate protocols oam ethernet link-fault-management interface interface-name
```

5. Confirme la configuración.

```
[edit]
user@host # commit
```

6. Verifique que la transmisión de los paquetes keepalive de LFM se delegue del proceso al hardware.`ppm` Para comprobar que ha habilitado la transmisión en línea, emita el comando siguiente:

```
user@host> show oam ethernet link-fault-management detail
Oct 18 02:05:05
  Interface: ge-0/0/0
    Status: Running, Discovery state: Active Send Local
    Transmit interval: 1000ms, PDU threshold: 3 frames, Hold time: 0ms
    Peer address: 00:00:00:00:00:00
    Flags:0x8
    OAM receive statistics:
      Information: 0, Event: 0, Variable request: 0, Variable response: 0
```

```
      Loopback control: 0, Organization specific: 0
    OAM flags receive statistics:
      Critical event: 0, Dying gasp: 0, Link fault: 0
    OAM transmit statistics:
      Information: 1, Event: 0, Variable request: 0, Variable response: 0  = even after 10
seconds count is still 1
      Loopback control: 0, Organization specific: 0
    OAM received symbol error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame period error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM received frame seconds error event information:
      Events: 0, Window: 0, Threshold: 0
      Errors in period: 0, Total errors: 0
    OAM transmitted symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current symbol error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM transmitted frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    OAM current frame error event information:
      Events: 0, Window: 0, Threshold: 1
      Errors in period: 0, Total errors: 0
    Loopback tracking: Disabled, Loop status: Unknown
    Detect LOC: Disabled, LOC status: Unknown
```

Las estadísticas de transmisión de OAM no se actualizan. Cuando se habilita la transmisión en línea de paquetes keepalive LFM, las estadísticas de transmisión OAM no se actualizan.

Para deshabilitar LFM en línea, verifique si alguna sesión de LFM establecida existente está en línea y activa. Desactive la sesión de LFM y confirme. Deshabilite LFM en línea eliminando la instrucción y confirme `.hardware-assisted-keepalives` A continuación, reactive la sesión LFM y confirme la configuración.

SEE ALSO

Keepalives asistidas por hardware (LFM)

Habilitación del modo en línea de monitoreo del rendimiento para lograr la máxima escala

La supervisión del rendimiento es útil para estudiar el patrón de tráfico en una red durante un período de tiempo. Ayuda a identificar problemas de red antes de que se vea afectado por defectos de red.

De forma predeterminada, los paquetes de supervisión del rendimiento son manejados por la CPU de una tarjeta de línea, como el concentrador de puerto modular (MPC). Al habilitar el modo en línea de supervisión del rendimiento, se delega el procesamiento de las unidades de datos de protocolo (PDU) al ASIC de reenvío (es decir, al hardware). Al habilitar el modo en línea de supervisión del rendimiento, se reduce la carga en la CPU de la tarjeta de línea y puede configurar un mayor número de sesiones de supervisión del rendimiento y lograr el máximo escalado para las sesiones de supervisión del rendimiento de OAM de servicio. En los enrutadores de la serie MX, puede configurar el modo en línea de supervisión del rendimiento solo si el modo de servicios de red del enrutador está configurado y está configurada la administración mejorada de errores de conectividad (`enhanced-ipenhanced-cfm-mode`).

Al habilitar el modo en línea de supervisión del rendimiento, puede lograr la máxima escala para las sesiones de supervisión del rendimiento. Para lograr la máxima escala para las sesiones de supervisión del rendimiento, debe habilitar la escala de las sesiones de mensajes de verificación de continuidad (MCP). Para habilitar el escalamiento de las sesiones del MCP, habilite la transmisión en línea de mensajes de verificación de continuidad. Para obtener más información sobre la transmisión en línea de mensajes de comprobación de continuidad, consulte Habilitar la transmisión en línea de mensajes de comprobación de continuidad para obtener la máxima escala."Habilitación de la transmisión en línea de mensajes de comprobación de continuidad para obtener la máxima escala" en la página 371 Para ver los valores de escala admitidos para CCM y PM, consulte Valores de escala de MCC en línea y PM en línea admitidos."Valores de escala CCM y PM en línea admitidos" en la página 379

El modo en línea de supervisión del rendimiento solo se admite para el modo proactivo de medición de retardo de fotogramas (mediciones de retardo bidireccional) y las sesiones de medición de pérdida sintética (SLM). Las funciones de supervisión del rendimiento configuradas mediante el perfil de iterador (CFM) se denominan supervisión proactiva del rendimiento. No se admite el modo en línea de supervisión del rendimiento para la medición de pérdida de fotogramas mediante tramas de servicio (LM).

NOTA: MPC3E (MX-MPC3E-3D) y MPC4E (MPC4E-3D-32XGE-SFPP y MPC4E-3D-2CGE-8XGE) no admiten el modo en línea de supervisión del rendimiento. La TLV de datos definidos por el usuario no es compatible si ha configurado el modo en línea de supervisión del rendimiento. Además, solo se admiten 12 registros históricos por sesión de PM.

Le recomendamos que habilite el modo en línea de supervisión del rendimiento antes de configurar las sesiones de supervisión del rendimiento, ya que el cambio puede interferir con las sesiones de supervisión del rendimiento existentes.

Para habilitar el modo en línea de supervisión del rendimiento, realice los pasos siguientes:

1. En el modo de configuración, vaya al nivel de jerarquía y configure el modo de servicios de red del enrutador.`[edit chassis]` El modo de servicio de red del enrutador debe configurarse para habilitar el modo de administración de errores de conectividad mejorada (CFM).`enhanced ip`

   NOTA: Si el modo de servicios de red no es y ha habilitado CFM mejorado, se muestra el siguiente mensaje de advertencia:`enhanced-ip`
   `[edit protocols oam ethernet] 'connectivity-fault-management' enhanced ip is not effective please configure enhanced ip and give router reboot`

   ```
   [edit chassis]
   user@host# set network-services enhanced-ip
   ```

2. En el modo de configuración, vaya al nivel de jerarquía y habilite el modo de administración de errores de conectividad mejorada con la opción.`[edit protocols oam ethernet connectivity-fault-management]``enhanced-cfm-mode`

   ```
   [edit]
   user@host# set protocols oam ethernet connectivity-fault-management enhanced-cfm-mode
   ```

3. En el modo de configuración, vaya al nivel de jerarquía.`[edit protocols oam ethernet connectivity-fault-management performance-monitoring]` Configure el perfil de iterador mejorado mediante la opción y especifique el intervalo de medición mediante la opción.`enhanced-sla-iteratormeasurement-interval`

   ```
   [edit]
   user@host# edit protocols oam ethernet connectivity-fault-management performance-monitoring
   enhanced-sla-iterator measurement-interval value
   ```

4. Habilite la supervisión del rendimiento en línea.

> **NOTA**: Puede habilitar el modo en línea de supervisión del rendimiento tanto para el originador como para el respondedor de las sesiones de supervisión del rendimiento de OAM de servicio mediante el comando.`hardware-assisted-pm`

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-pm
```

5. (Opcional) Habilite la transmisión en línea de MCPs para permitir una mejor escala si la transmisión en línea de MCPs no se habilita automáticamente.

> **NOTA**: Puede lograr una mejor escala si está habilitada tanto la supervisión del desempeño en línea como la transmisión en línea de MCPs.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# set hardware-assisted-keepalives enable
```

6. Confirme la configuración.

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]
user@host# commit
```

SEE ALSO

Habilitación del modo de administración de errores de conectividad mejorada | 54

Descripción general del modo de servicios de red

Hardware-Assisted-PM

Valores de escala CCM y PM en línea admitidos

En este tema se enumeran los valores de escala para el modo en línea de supervisión del rendimiento y la transmisión en línea de mensajes de comprobación de continuidad. Los valores de escala se basan en los diferentes valores del intervalo ciclo-tiempo. En cada tabla se enumera el número máximo de sesiones de administración de errores de conectividad (CFM) y sesiones de supervisión del rendimiento (PM) por tarjeta de línea y por chasis cuando se configura CCM en línea, CFM mejorado y PM mejorado mediante las opciones , y .`hardware-assisted-keepalivesenhanced-cfm-modehardware-assisted-pm`

NOTA: Los valores de escala no tienen en cuenta la carga de otros protocolos en el sistema, por lo que los valores de escala reales realizados para la tarjeta de línea y el chasis varían en función de otras configuraciones de protocolo y escala en el sistema. Se recomienda configurar DDoS para CFM. Limite el número de paquetes CFM, que se envían a la CPU de la tarjeta de línea, a 3000. Limitar el número de paquetes protege la CPU de configuraciones CFM escaladas de varios eventos de protocolo CFM.

Tabla 21 en la página 380 enumera el número máximo de sesiones de administración de errores de conectividad (CFM) y sesiones de supervisión del rendimiento (PM) por tarjeta de línea y por chasis cuando se configuran el intervalo CCM y el intervalo PM como 1 segundo.

Tabla 21: Valores de escala para CFM y PM (intervalo CCM: Intervalo de 1 segundo y PM: 1 segundo)

Escala de tarjeta de línea CFM	Escala de tarjeta de línea PM	Escala de chasis CFM	Escala de chasis PM
4000	4500	16 000	16 000
6000	3750	16 000	16 000
7000	3375	16 000	16 000
8000	3000	16 000	16 000

Tabla 22 en la página 380 enumera el número máximo de sesiones de administración de errores de conectividad (CFM) y sesiones de supervisión del rendimiento (PM) por tarjeta de línea y por chasis cuando se configura el intervalo CCM como 1 segundo y el intervalo PM como 100 milisegundos.

Tabla 22: Valores de escala para CFM y PM (intervalo CCM: Intervalo de 1 segundo y PM: 100 ms)

Escala de tarjeta de línea CFM	Escala de tarjeta de línea PM	Escala de chasis CFM	Escala de chasis PM
4000	450	12000	4000
6000	375	12000	4000
7000	337	12000	4000

Tabla 22: Valores de escala para CFM y PM (intervalo CCM: Intervalo de 1 segundo y PM: 100 ms) ***(Continued)***

Escala de tarjeta de línea CFM	Escala de tarjeta de línea PM	Escala de chasis CFM	Escala de chasis PM
8000	300	12000	4000

Tabla 23 en la página 381 enumera el número máximo de sesiones de administración de errores de conectividad (CFM) y sesiones de supervisión del rendimiento (PM) por tarjeta de línea y por chasis cuando se configura el intervalo CCM como 100 milisegundos y el intervalo PM como 1 segundo.

Tabla 23: Valores de escala para CFM y PM (intervalo CCM: Intervalo de 100 ms y PM: 1 segundo)

Escala de tarjeta de línea CFM	Escala de tarjeta de línea PM	Escala de chasis CFM	Escala de chasis PM
4000	3000	8000	6000
3000	3750	8000	6000
2000	4500	8000	6000
1000	4500	8000	6000

Tabla 24 en la página 381 enumera el número máximo de sesiones de administración de errores de conectividad (CFM) y sesiones de supervisión del rendimiento (PM) por tarjeta de línea y por chasis cuando se configuran el intervalo CCM y el intervalo PM como 100 milisegundos.

Tabla 24: Valores de escala para CFM y PM (intervalo CCM: Intervalo de 100 ms y PM: 100 ms)

Escala de tarjeta de línea CFM	Escala de tarjeta de línea PM	Escala de chasis CFM	Escala de chasis PM
4000	300	8000	3000
3000	375	8000	3000
2000	450	8000	3000

Tabla 24: Valores de escala para CFM y PM (intervalo CCM: Intervalo de 100 ms y PM: 100 ms) *(Continued)*

Escala de tarjeta de línea CFM	Escala de tarjeta de línea PM	Escala de chasis CFM	Escala de chasis PM
1000	450	8000	3000

SEE ALSO

modo CFM mejorado

Hardware-Assisted-PM

VÍNCULOS RELACIONADOS

Configurar mensajes de comprobación de continuidad | **114**

Introducción a la gestión de fallos de vínculo OAM (LFM) | **139**

3

PART IN COVERPAGE

Supervisión de red mediante SNMP

Descripción general de la arquitectura SNMP y las MIB SNMP | 385

Descripción de la implementación de SNMP en Junos OS | 388

Configurar SNMP en Junos OS | 395

Configurar opciones en dispositivos administrados para un mejor tiempo de respuesta SNMP | 416

MIB de utilidad específica para empresas para mejorar la cobertura SNMP | 419

Optimice la configuración del sistema de administración de red para obtener los mejores resultados | 422

Interfaces para aceptar solicitudes SNMP | 424

Configurar SNMP para instancias de enrutamiento | 427

Configurar operaciones remotas SNMP | 450

Capturas SNMP | 473

Capturas SNMP compatibles con Junos OS | 487

Rastrear actividad SNMP | 537

Privilegios de acceso para un grupo SNMP | 548

Configurar ID de motor local en SNMPv3 | 556

Configurar SNMPv3 | 558

Configurar el tipo de autenticación SNMPv3 y el tipo de cifrado | 565

Capturas SNMPv3 | 567

SNMPv3 informa | 575

Comunidades SNMP | 583

Vistas MIB | 598

MIB SNMP compatibles con Junos OS y Junos OS Evolved | 600

Preguntas frecuentes sobre SNMP de Junos OS | 687

Descripción general de la arquitectura SNMP y las MIB SNMP

in this section

- Arquitectura SNMP | 385

Arquitectura SNMP

Una implementación típica de SNMP incluye tres componentes:

- Sistema de administración de red (NMS): combinación de hardware (dispositivos) y software (el administrador SNMP) que se utiliza para monitorear y administrar una red. El administrador sondea los dispositivos de la red a medida que usted especifica para obtener información sobre la conectividad, la actividad y los eventos de red.
- Dispositivo administrado: un dispositivo administrado (también llamado elemento de red) es cualquier dispositivo en una red administrada por el NMS. Los enrutadores y conmutadores son ejemplos comunes de dispositivos administrados.
- Agente SNMP: el agente SNMP es el proceso SNMP que reside en el dispositivo administrado y se comunica con el NMS. El agente SNMP intercambia información de administración de red con el software de administración SNMP que se ejecuta en un NMS o host. El agente responde a las solicitudes de información y acciones del gerente. El agente también controla el acceso a la MIB del agente, la colección de objetos que el administrador SNMP puede ver o cambiar.

Este tema contiene las siguientes secciones:

MIB SNMP

Puede almacenar datos SNMP en un formato jerárquico altamente estructurado conocido como Base de información de administración (MIB). Una MIB define objetos administrados en un dispositivo de red.

La estructura MIB se basa en una estructura de árbol y define una agrupación de objetos en conjuntos relacionados. Cada objeto de la MIB está asociado con un identificador de objeto (OID), que asigna un nombre al objeto. La "hoja" en la estructura de árbol es la instancia real de objeto administrado, que representa un recurso, evento o actividad que ocurre en su dispositivo de red.

Las MIB son estándar o específicas de la empresa. Para obtener más información, consulte Tabla 25 en la página 386.

Tabla 25: MIB estándar y específicas de la empresa

MIB estándar	MIB específicas de la empresa
Creado por Internet Engineering Task Force (IETF) y documentado en varias RFC. Dependiendo del proveedor, muchas MIB estándar se entregan con el software NMS. También puede descargar los MIB estándar del sitio web de IETF, www.ietf.org, y compilarlos en su NMS, si es necesario.	Desarrollado y respaldado por un fabricante de equipos específico. Si la red contiene dispositivos que tienen MIB específicas de la empresa, debe obtenerlos del fabricante y compilarlos en el software de administración de red.
Para obtener una lista de las MIB compatibles con estándar, consulte .MIB SNMP estándar compatibles con Junos OS	Para obtener una lista de las MIB admitidas específicamente para la empresa de Juniper Networks, consulte .MIB SNMP específicas de la empresa compatibles con Junos OS

Administrador SNMP y autenticación y comunicación del agente

SNMP utiliza una forma básica de autenticación llamada cadenas de comunidad para controlar el acceso entre un administrador y agentes remotos. Las cadenas de comunidad son nombres administrativos que se utilizan para agrupar colecciones de dispositivos (y los agentes que se ejecutan en ellos) en dominios de administración comunes. Si un gerente y un agente comparten la misma comunidad, pueden hablar entre sí. Muchas personas asocian cadenas de comunidad SNMP con contraseñas y claves porque los trabajos que realizan son similares. Como resultado, las comunidades SNMP se conocen tradicionalmente como cadenas.

La comunicación entre el agente y el administrador se produce de una de las siguientes formas:

- , , y requests: el administrador solicita información al agente; el agente devuelve la información en un mensaje de respuesta.`GetGetBulkGetNextGet`
- requests: el gestor cambia el valor de un objeto MIB controlado por el agente; El agente indica el estado en un mensaje de respuesta.`SetSet`
- `Traps` notificación: el agente envía capturas para notificar al administrador los eventos importantes que se producen en el dispositivo de red.

SNMP captura e informa

Los enrutadores pueden enviar notificaciones a los administradores de SNMP cuando ocurren eventos significativos en un dispositivo de red, con mayor frecuencia errores o fallas. Puede enviar notificaciones SNMP como capturas o solicitudes de información.

Las capturas SNMP son notificaciones no confirmadas y los informes SNMP son notificaciones confirmadas.

Las capturas SNMP son estándar o específicas de la empresa. Para obtener más información, consulte Tabla 26 en la página 387.

Tabla 26: Trampas estándar y específicas de la empresa

Trampas estándar	Trampas específicas de la empresa
Creado por el IETF y documentado en varias RFC. Las trampas estándar se compilan en el software de administración de red. También puede descargar las trampas estándar del sitio web de IETF, www.ietf.org.http://www.ietf.org	Desarrollado y respaldado por un fabricante de equipos específico. Si la red contiene dispositivos que tienen capturas específicas de la empresa, debe obtenerlas del fabricante y compilarlas en el software de administración de red.
Para obtener más información acerca de las capturas estándar compatibles con Junos OS, consulte Capturas SNMP estándar compatibles con dispositivos que ejecutan Junos OS.https://www.juniper.net/documentation/en_US/junos15.1/topics/concept/standard-snmp-traps-overview.html	Para obtener más información acerca de las capturas específicas de la empresa compatibles con Junos OS, consulte Capturas SNMP específicas de la empresa compatibles con Junos OS.https://www.juniper.net/documentation/en_US/junos/topics/concept/enterprise-specific-traps-overview.html Para obtener información acerca de los niveles de gravedad del registro del sistema para capturas SNMP, consulte .No Link Title

Con las capturas, el receptor no envía ningún acuse de recibo cuando recibe una captura, y el remitente no puede determinar si la captura fue recibida. Para aumentar la confiabilidad, SNMPv3 admite SNMPv3 los informes. Un administrador SNMP que recibe un informe reconoce el mensaje con una respuesta. Para obtener información acerca de SNMP informa, consulte .No Link Title

Descripción de la implementación de SNMP en Junos OS

in this section

- Carga de archivos MIB en un sistema de administración de red | 392
- Descripción de la interfaz de administración local integrada | 394

SNMP en Junos OS

En Junos OS, SNMP utiliza MIB estándar (desarrollado por IETF y documentado en RFC) y específico de la empresa de Juniper Networks.

> **NOTA**: De forma predeterminada, SNMP no está habilitado en dispositivos que ejecutan Junos OS.

En Junos OS, los procesos que mantienen los datos de administración SNMP incluyen los siguientes:

- Un agente SNMP maestro reside en el dispositivo administrado y es administrado por el NMS o host.

  El software del agente SNMP de Junos OS consta de un agente principal SNMP (conocido como proceso SNMP o snmpd). Reside en el dispositivo administrado y es administrado por el NMS o el host.

- Varios subagentes que residen en distintos módulos de Junos OS, como el motor de enrutamiento. El agente SNMP principal delega todas las solicitudes SNMP a los subagentes. Cada subagente es responsable del soporte de un conjunto específico de MIB.

- Junos OS procesa que comparten datos con los subagentes cuando se sondean los datos SNMP (por ejemplo, MIB relacionadas con la interfaz).

La cadena de comunidad es el primer nivel de autenticación de administración implementado por el agente SNMP en Junos OS.

Consulte las siguientes secciones para obtener más información.

Compatibilidad de Junos OS con versiones SNMP

Junos OS admite las siguientes versiones de SNMP. Para obtener más información, consulte Tabla 27 en la página 389.

Tabla 27: Compatibilidad de Junos OS con versiones SNMP

Versiones de SNMP	Description
SNMPv1	La implementación inicial de SNMP que define la arquitectura y el marco para SNMP.
SNMPv2c	El protocolo revisado, con mejoras en el rendimiento y las comunicaciones de gerente a gerente. En concreto, SNMPv2c implementa cadenas de comunidad, que actúan como contraseñas para determinar quién, qué y cómo los clientes SNMP pueden acceder a los datos en el agente SNMP. La cadena de comunidad se encuentra en SNMP , , y las solicitudes.`GetGetBulkGetNextSet` Es posible que el agente requiera una cadena de comunidad diferente para , y solicitudes (acceso) que para solicitudes (acceso).`GetGetBulkGetNextread-onlySetread-write`
SNMPv3	SNMPv3: el protocolo más actualizado se centra en la seguridad. SNMPv3 define un modelo de seguridad, un modelo de seguridad basado en el usuario (USM) y un modelo de control de acceso basado en vistas (VACM). SNMPv3 USM proporciona integridad de datos, autenticación de origen de datos, protección de reproducción de mensajes y protección contra la divulgación de la carga del mensaje. SNMPv3 VACM proporciona control de acceso para determinar si se permite un tipo específico de acceso (lectura o escritura) a la información de administración.

Además, el software del agente SNMP de Junos OS acepta direcciones IPv4 e IPv6 para el transporte a través de IPv4 e IPv6. Para IPv6, Junos OS admite las siguientes funciones:

- Datos SNMP a través de redes IPv6
- Datos MIB específicos de IPv6
- Agentes SNMP para IPv6

Niveles de gravedad del registro del sistema para capturas SNMP

Para algunas capturas, cuando se produce una condición de interrupción, independientemente de si el agente SNMP envía una captura a un NMS, la captura se registra si el registro del sistema está configurado para registrar un evento con ese nivel de gravedad de registro del sistema.

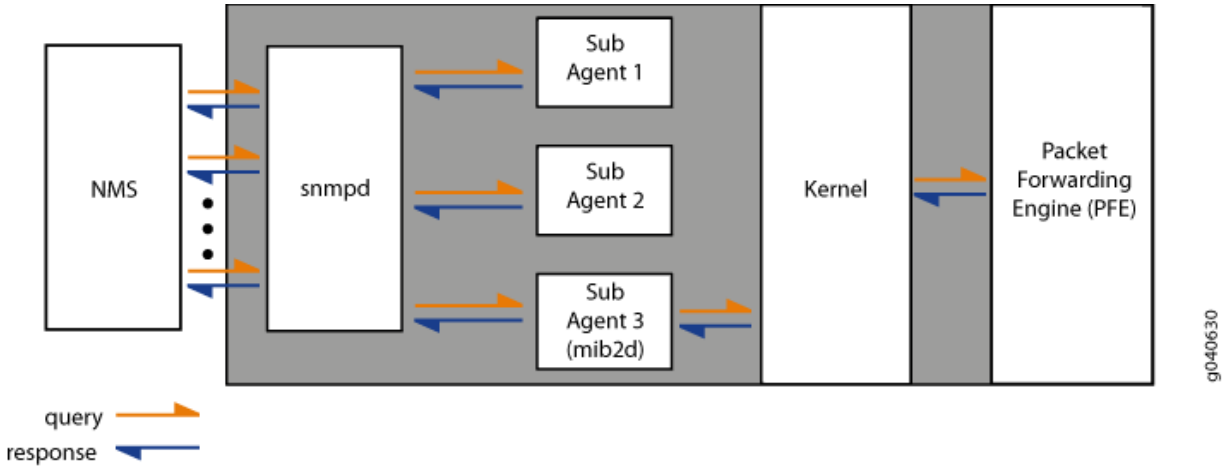
Para obtener más información acerca de los niveles de gravedad del registro del sistema para capturas estándar, consulte .Capturas SNMP estándar compatibles con Junos OS Para obtener más información acerca de los niveles de gravedad del registro del sistema para capturas específicas de la empresa, consulte Capturas SNMP específicas de la empresa compatibles con Junos OS.https://www.juniper.net/documentation/en_US/junos/topics/concept/enterprise-specific-traps-overview.html

Flujo de comunicación SNMP

Cuando un NMS sondea al agente primario en busca de datos, el agente primario comparte inmediatamente los datos con el NMS si los datos solicitados están disponibles del agente primario o de uno de los subagentes. Sin embargo, si los datos solicitados no pertenecen a las categorías que mantienen el agente principal o los subagentes, el subagente sondea el kernel de Junos OS o el proceso que mantiene esos datos. Al recibir los datos requeridos, el subagente devuelve la respuesta al agente primario, que a su vez la pasa al NMS.

Figura 21 en la página 390 muestra el flujo de comunicación entre el NMS, el agente principal SNMP (snmpd), los subagentes SNMP, el kernel de Junos OS y el motor de reenvío de paquetes.

Figura 21: Flujo de comunicación SNMP



Cuando se produce un evento importante, la mayoría de las veces un error o un error, en un dispositivo de red, el agente SNMP envía notificaciones al administrador SNMP. La implementación de SNMP en Junos OS admite dos tipos de notificaciones: atrapa e informa. Las trampas son notificaciones no

confirmadas, mientras que los informes son notificaciones confirmadas. Los informes solo se admiten en dispositivos compatibles con la configuración SNMP versión 3 (SNMPv3).

Cola de trampas

Junos OS admite la cola de capturas para garantizar que las capturas no se pierdan debido a la indisponibilidad temporal de las rutas. Se forman dos tipos de colas, colas de destino y una cola de acelerador, para garantizar la entrega de trampas y controlar el tráfico de capturas.

> **NOTA**: No puede configurar las colas de captura en Junos OS. No puede ver información sobre las colas de capturas, excepto lo que se proporciona en los registros del sistema.

Junos OS forma una cola de destino cuando se devuelve una captura a un destino determinado porque no se puede acceder al host, y agrega las capturas posteriores al mismo destino a la cola. Junos OS comprueba la disponibilidad de las rutas cada 30 segundos y envía las capturas desde la cola de destino de forma rotativa.

Si se produce un error en la entrega de capturas, la captura se vuelve a agregar a la cola y se restablecen el contador de intentos de entrega y el temporizador del siguiente intento de entrega de la cola. Los intentos posteriores ocurren a intervalos progresivos de 1 minuto, 2 minutos, 4 minutos y 8 minutos. El retraso máximo entre los intentos es de 8 minutos y el número máximo de intentos es de 10. Después de 10 intentos fallidos, se eliminan la cola de destino y todas las capturas de la cola.

Junos OS también tiene un mecanismo de aceleración para controlar el número de capturas (umbral del acelerador; valor predeterminado de 500 capturas) enviadas durante un período de tiempo determinado (intervalo del acelerador; valor predeterminado de 5 segundos) y para garantizar la coherencia en el tráfico de capturas, especialmente cuando se genera un gran número de capturas debido a cambios de estado de la interfaz. El período de intervalo del acelerador comienza cuando la primera trampa llega al acelerador. Todas las interrupciones dentro del umbral de captura se procesan y las capturas que superan el límite de umbral se ponen en cola.

El tamaño máximo de las colas de captura, es decir, la cola del acelerador y la cola de destino juntas, es de 40.000. Sin embargo, en los conmutadores Ethernet de la serie EX, el tamaño máximo de la cola de captura es 1.000. El tamaño máximo de cualquier cola es de 20.000 para dispositivos que no sean conmutadores de la serie EX. En los conmutadores de la serie EX, el tamaño máximo de una cola es 500. Cuando se agrega una captura a la cola del acelerador, o si la cola del acelerador ha superado el tamaño máximo, la captura se vuelve a agregar encima de la cola de destino y todos los intentos posteriores de la cola de destino se detienen durante un período de 30 segundos, después del cual la cola de destino se reinicia enviando las capturas.

Carga de archivos MIB en un sistema de administración de red

Para que el sistema de administración de red (NMS) identifique y comprenda los objetos MIB utilizados por Junos OS, primero debe cargar los archivos MIB en el NMS mediante un compilador MIB. Un compilador MIB es una utilidad que analiza la información MIB, como el nombre del objeto MIB, los ID y el tipo de datos del NMS.

Puede descargar el paquete MIB de Junos desde el índice MIB empresariales de Junos OS en https://www.juniper.net/documentation/en_US/release-independent/junos/mibs/mibs.html . El paquete Junos MIB está disponible en y paquetes..**zip.tar** Puede descargar el formato adecuado según sus requisitos.

El paquete MIB de Junos contiene dos carpetas: **StandardMibs** y **JuniperMibs**. La carpeta contiene las MIB y RFC estándar compatibles con dispositivos que ejecutan Junos OS, mientras que la carpeta contiene las MIB específicas de la empresa de Juniper Networks.**StandardMibsJuniperMibs**

Para cargar archivos MIB necesarios para administrar y supervisar dispositivos que ejecutan Junos OS:

1. Vaya a la página de descargas del Explorador de MIB de SNMP para ver los paquetes MIB SNMP de Juniper Networks (Explorador SNMP MIB).https://apps.juniper.net/mib-explorer/download.jsp
2. Haga clic en el vínculo o debajo del encabezado de la versión correspondiente para descargar el paquete Junos MIB para esa versión.**TARZIP**
3. Descomprima el archivo (o) utilizando una utilidad adecuada..**tar.zip**
4. Cargue los archivos MIB estándar (desde la carpeta) en el orden siguiente:**StandardMibs**

> **NOTA**: Algunos de los compiladores MIB que se usan comúnmente tienen los MIB estándar precargados en ellos. Si las MIB estándar ya están cargadas en el compilador MIB que está utilizando, omita este paso y continúe con el paso 7.

1. **mib-SNMPv2-SMI.txt**
2. **mib-SNMPv2-TC.txt**
3. **mib-IANAifType-MIB.txt**
4. **mib-IANA-RTPROTO-MIB.txt**
5. **mib-rfc1907.txt**
6. **mib-rfc4293.txt**
7. **mib-rfc2012a.txt**
8. **mib-rfc2013a.txt**

9. **mib-rfc2571.txt**
10. **mib-rfc2863a.txt**
11. **mib-rfc4001.txt**

5. Cargue los archivos MIB estándar restantes.

> **NOTA**: Debe seguir el orden especificado en este procedimiento. Esto es para asegurarse de que carga las MIB estándar antes que las MIB específicas de la empresa. Puede haber dependencias que requieran que una MIB determinada esté presente en el compilador antes de cargar otra MIB. Puede encontrar dichas dependencias enumeradas en la sección del archivo MIB.**IMPORT**

6. Cargue la MIB de SMI específica para empresa de Juniper Networks y las siguientes MIB de SMI opcionales según sus requisitos:**mib-jnx-smi.txt**
   - **mib-jnx-js-smi.txt**—(Opcional) Para objetos de árbol MIB de Juniper Security
   - **mib-jnx-ex-smi.txt**—(Opcional) Para conmutadores Ethernet serie EX
   - **mib-jnx-exp.txt**—(Recomendado) Para objetos MIB experimentales de Juniper Networks
   - **mib-jnx-cos.txt**
   - **mib-jnx-mimstp.txt**
   - **mib-jnx-l2cp-features.txt**
   - **mib-jnx-mpls-ldp.txt**
   - **mib-jnx-sp.txt**
   - **mib-jnx-ipforward.txt**
   - **mib-jnx-jsysmon.txt**
   - **mib-jnx-vpn.txt**
   - **mib-jnx-pwtdm.txt**
   - **mib-jnx-pwatm.txt**
   - **mib-jnx-mbg-smi.txt**
   - **mib-jnx-vpls-generic.txt**
   - **mib-jnx-vpls-ldp.txt**

- **mib-jnx-vpls-bgp.txt**
- **mib-jnx-mobile-gateways.txt**
- **mib-jnx-optif.txt**
- **mib-jnx-bl.txt**
- **mib-jnx-gen-set.txt**
- **mib-jnx-if-extensions.txt**
- **mib-jnx-if-accounting.txt**
- **mib-jnx-alarm.txt**
- **mib-jnx-dot3oam-capability.txt**
- **mib-jnx-ipmcast-capability.txt**

7. Cargue las MIB específicas de la empresa restantes desde la carpeta.**JuniperMibs**

CONSEJO: Al cargar un archivo MIB, si el compilador devuelve un mensaje de error que indica que alguno de los objetos no está definido, abra el archivo MIB con un editor de texto y asegúrese de que todos los archivos MIB enumerados en la sección estén cargados en el compilador.**IMPORT** Si alguno de los archivos MIB enumerados en la sección no se carga en el compilador, cargue ese archivo MIB y, a continuación, intente cargar el archivo MIB que no se pudo cargar.**IMPORT**

Por ejemplo, la MIB de PING específica de la empresa, , tiene dependencias en RFC 2925, DiSMAN-PING-MIB, .**mib-jnx-ping.txtmib-rfc2925a.txt** Si intenta cargar antes de cargar , el compilador devuelve un mensaje de error que indica que ciertos objetos en no están definidos.**mib-jnx-ping.txtmib-rfc2925a.txtmib-jnx-ping.txt** Cargue y, a continuación, intente cargar .**mib-rfc2925a.txtmib-jnx-ping.txt** A continuación, se carga sin problemas la MIB PING específica de la empresa. **mib-jnx-ping.txt**

Descripción de la interfaz de administración local integrada

La Interfaz de administración local integrada (ILMI) proporciona un mecanismo para que los dispositivos conectados al modo de transferencia asíncrono (ATM), como hosts, enrutadores y conmutadores ATM, transfieran información de administración. ILMI proporciona un intercambio bidireccional de información de administración entre dos interfaces ATM a través de una conexión física. La información de ILMI se intercambia a través de una encapsulación directa de SNMP versión 1 (RFC 1157, *A Simple Network*

Management Protocol) a través de ATM Adaptation Layer 5 (AAL5) utilizando un valor de identificador de ruta virtual/identificador de canal virtual (VPI/VCI) (VPI=0, VCI=16).

Junos OS solo admite dos variables ILMI MIB:

- `atmfMYIPNmAddress`
- `atmfPortMyIfname`

Para las interfaces de cola inteligente (IQ) ATM1 y ATM2, puede configurar la ILMI para que se comunique directamente con un conmutador ATM conectado a fin de permitir la consulta de la dirección IP y el número de puerto del conmutador.

Para obtener más información acerca de la MIB de ILMI, consulte o en el Explorador de MIB de SNMP.`atmfMYIPNmAddressatmfPortMyIfname`https://apps.juniper.net/mib-explorer/

SEE ALSO

Descripción de las funciones de administración de dispositivos en Junos OS

Configurar SNMP en Junos OS

in this section

- Configurar SNMP | **396**
- Configurar detalles de SNMP | **405**
- Configurar el temporizador de retraso de confirmación | **408**
- Configurar SNMP en un dispositivo que ejecute Junos OS | **408**
- Ejemplo: Configurar SNMP en el sistema QFabric | **411**

Configurar SNMP

in this section

- Instrucciones de configuración en el nivel de jerarquía [edit snmp] | **396**
- Configurar opciones básicas para SNMP | **401**

Puede implementar SNMP en el software Junos OS que se ejecuta en los productos de las series QFX y OCX. De forma predeterminada, SNMP no está habilitado. Para habilitar SNMP, debe incluir las instrucciones de configuración SNMP en el nivel jerárquico .`[edit]`

Para configurar los requisitos mínimos para SNMP, incluya la instrucción en el nivel de jerarquía.`community public[edit snmp]`

Para configurar funciones SNMP completas, consulte .*snmp*

Instrucciones de configuración en el nivel de jerarquía [edit snmp]

En este tema se muestran todas las instrucciones de configuración en el nivel de jerarquía y su nivel en la jerarquía de configuración.`[edit snmp]` Cuando configure Junos OS, el nivel de jerarquía actual se muestra en el banner de la línea que precede al mensaje.`user@host#`

```
[edit]
snmp {
        alarm-management {
            alarm-list-name list-name {
                alarm-id id {
                    alarm-state state {
                        description alarm-description;
                        notification-id notification-id-of-alarm;
                        resource-prefix alarm-resource-prefix;
                        varbind-index varbind-index-in-alarm-varbind-list;
                        varbind-subtree alarm-varbind-subtree;
                        varbind-value alarm-varbind-value;
                    }
                }
            }
        }
```

```
client-list client-list-name {
    ip-addresses;
}
community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
        address <restrict>;
    }
    logical-system logical-system-name {
        routing-instance routing-instance-name;
        clients {
            address <restrict>;
        }
    }
    routing-instance routing-instance-name {
        clients {
            address <restrict>;
        }
    }
    view view-name;
}
contact contact;
description description;
engine-id {
    (local engine-id | use-default-ip-address | use-mac-address);
}
filter-duplicates;
interface [ interface-names ];
location location;
name name;
nonvolatile {
    commit-delay seconds;
}
rmon {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type (get-next-request | get-request | walk-request);
        rising-event-index index;
```

```
            rising-threshold integer;
            sample-type type;
            startup-alarm alarm;
            syslog-subtag syslog-subtag;
            variable oid-variable;
        }
        event index {
            community community-name;
            description description;
            type type;
        }
    }
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable> <match
regular-expression>;
        flag flag;
        memory-trace;
        no-remote-trace;
        no-default-memory-trace;
    }
    trap-group group-name {
        categories {
            category;
        }
        destination-port port-number;
        routing-instance instance;
        logical-system logical-system-name;
        targets {
            address;
        }
        version (all | v1 | v2);
    }
    trap-options {
        agent-address outgoing-interface;
        source-address address;
        enterprise-oid;
        logical-system logical-system-name {
            routing-instance routing-instance-name {
                source-address address;
            }
        }
        routing-instance routing-instance-name {
            source-address address;
```

```
        }
    }
    v3 {
        notify name {
            tag tag-name;
            type (trap | inform);
        }
        notify-filter profile-name {
            oid oid (include | exclude);
        }
        snmp-community community-index {
            community-name community-name;
            security-name security-name;
            tag tag-name;
        }
        target-address target-address-name {
            address address;
            address-mask address-mask;
            logical-system logical-system;
            port port-number;
            retry-count number;
            routing-instance instance;
            tag-list tag-list;
            target-parameters target-parameters-name;
            timeout seconds;
        }
        target-parameters target-parameters-name {
            notify-filter profile-name;
            parameters {
                message-processing-model (v1 | v2c | v3);
                security-level (authentication | none | privacy);
                security-model (usm | v1 | v2c);
                security-name security-name;
            }
        }
        usm {
            local-engine {
                user username {
                    authentication-md5 {
                        authentication-password authentication-password;
                    }
                    authentication-none;
                    authentication-sha {
```

```
                        authentication-password authentication-password;
                    }
                    privacy-3des {
                        privacy-password privacy-password;
                    }
                    privacy-aes128 {
                        privacy-password privacy-password;
                    }
                    privacy-des {
                        privacy-password privacy-password;
                    }
                    privacy-none;
                }
            }
        }
        vacm {
            access {
                group group-name {
                    (default-context-prefix | context-prefix context-prefiix){
                        security-model (any | usm | v1 | v2c) {
                            security-level (authentication | none | privacy) {
                                notify-view view-name;
                                read-view view-name;
                                write-view view-name;
                            }
                        }
                    }
                }
            }
            security-to-group {
                security-model (usm | v1 | v2c) {
                    security-name security-name {
                        group group-name;
                    }
                }
            }
        }
    }
    view view-name {
        oid object-identifier (include | exclude);
    }
}
```

Configurar opciones básicas para SNMP

Las siguientes secciones contienen información sobre la configuración básica de SNMP y algunos ejemplos de configuración de las operaciones básicas de SNMP en dispositivos que ejecutan Junos OS:

Configurar opciones básicas para SNMPv1 y SNMPv2

No puede habilitar SNMP en dispositivos que ejecuten Junos OS de forma predeterminada. Para habilitar SNMP en dispositivos que ejecutan Junos OS, incluya la instrucción en el nivel de jerarquía.`community public[edit snmp]`

Habilitación de las operaciones Get y GetNext de SNMPv1 y SNMPv2

```
[edit]
snmp {
    community public;
}
```

Una comunidad que se define como pública concede acceso a todos los datos de MIB a cualquier cliente.

Para habilitar las operaciones SNMPv1 y SNMPv2 en el dispositivo, debe incluir las siguientes instrucciones en el nivel de jerarquía:`Set[edit snmp]`

Habilitación de las operaciones de conjunto SNMPv1 y SNMPv2

```
[edit snmp]
view all {
    oid .1;
}
community private {
    view all;
    authorization read-write;
}
```

En el ejemplo siguiente se muestra la configuración mínima básica de las capturas SNMPv1 y SNMPv2 en un dispositivo:

Configuración de capturas SNMPv1 y SNMPv2

```
[edit snmp]
trap-group jnpr {
```

```
    targets {
        192.168.69.179;
    }
}
```

Configurar opciones básicas para SNMPv3

En el ejemplo siguiente se muestra la configuración mínima de SNMPv3 para habilitar , y las operaciones en un dispositivo (tenga en cuenta que la configuración tiene autenticación establecida en y privacidad en): `GetGetNextSetmd5none`

Habilitación de las operaciones Get, GetNext y Set de SNMPv3

```
[edit snmp]
v3 {
    usm {
        local-engine {
            user jnpruser {
                authentication-md5 {
                    authentication-key "$9$guaDiQFnAuOQzevMWx7ikqP"; ## SECRET-DATA
                }
                privacy-none;
            }
        }
    }
    vacm {
        security-to-group {
            security-model usm {
                security-name jnpruser {
                    group grpnm;
                }
            }
        }
        access {
            group grpnm {
                default-context-prefix {
                    security-model any {
                        security-level authentication {
                            read-view all;
                            write-view all;
                        }
                    }
```

```
                }
            }
        }
    }
}
view all {
    oid .1;
}
```

En el siguiente ejemplo se muestra la configuración básica para SNMPv3 informa en un dispositivo (la configuración tiene valores de autenticación y privacidad para):`none`

Configuración de SNMPv3 Informs

```
[edit snmp]
v3 {
    usm {
        remote-engine 00000063200133a2c0a845c3 {
            user RU2_v3_sha_none {
                authentication-none;
                privacy-none;
            }
        }
    }
    vacm {
        security-to-group {
            security-model usm {
                security-name RU2_v3_sha_none {
                    group g1_usm_auth;
                }
            }
        }
        access {
            group g1_usm_auth {
                default-context-prefix {
                    security-model usm {
                        security-level authentication {
                            read-view all;
                            write-view all;
                            notify-view all;
                        }
                    }
```

```
                }
            }
        }
    }
    target-address TA2_v3_sha_none {
        address 192.168.69.179;
        tag-list tl1;
        address-mask 255.255.252.0;
        target-parameters TP2_v3_sha_none;
    }
    target-parameters TP2_v3_sha_none {
        parameters {
            message-processing-model v3;
            security-model usm;
            security-level none;
            security-name RU2_v3_sha_none;
        }
        notify-filter nf1;
    }
    notify N1_all_tl1_informs {
        type inform; # Replace inform with trap to convert informs to traps.
        tag tl1;
    }
    notify-filter nf1 {
        oid .1 include;
    }
}
view all {
    oid .1 include;
}
```

Puede convertir los informes SNMPv3 en capturas estableciendo el valor de la instrucción en el nivel de jerarquía en, como se muestra en el ejemplo siguiente:`type[edit snmp v3 notify N1_all_tl1_informs]trap`

Conversión de informes en trampas

```
user@host# set snmp v3 notify N1_all_tl1_informs type trap
```

SEE ALSO

Descripción de la implementación de SNMP en Junos OS | 388

Snmp

Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS | **538**

Optimice la configuración del sistema de administración de red para obtener los mejores resultados | **422**

Configurar opciones en dispositivos administrados para un mejor tiempo de respuesta SNMP | **416**

No Link Title

Configurar detalles de SNMP

Puede utilizar SNMP para almacenar detalles administrativos básicos, como el nombre de un contacto y la ubicación del dispositivo. Su sistema de gestión puede recuperar esta información de forma remota cuando esté solucionando un problema o realizando una auditoría. En la terminología SNMP, estos son los objetos sysName, sysContact, sysDescription y sysLocation que se encuentran dentro del grupo de sistemas de MIB-2 (como se define en RFC 1213, *Base de información de administración para la administración de red de Internet basadas en TCP/IP): MIB-II).* Puede establecer valores iniciales directamente en la configuración de Junos OS para cada sistema administrado por SNMP.

NOTA: Para los dispositivos administrados por SNMP, mantenga siempre configurada y actualizada el nombre, la ubicación, el contacto y la información de descripción.

Para establecer los detalles del SNMP:

1. Configure un nombre de sistema.

   Establezca los detalles del nombre del sistema incluyendo la instrucción en el nivel jerárquico `.name[edit snmp]`

   ```
   [edit groups global snmp]
   user@host# set name name
   ```

   Por ejemplo:

   ```
   [edit groups global snmp]
   user@host# set name "host” # Overrides the system name
   ```

2. Configure un contacto del sistema.

Establezca los detalles de contacto del sistema incluyendo la instrucción en el nivel de jerarquía o en un grupo de configuración adecuado, como se muestra aquí.`contact[edit snmp]`

Este contacto administrativo se coloca en el objeto sysContact de MIB II.

Si el nombre contiene espacios, escríbalo entre comillas (" ").

```
[edit groups global snmp]
user@host# set contact contact
```

Por ejemplo:

```
[edit groups global snmp]
user@host# set contact "Enterprise Support, (650) 555-1234" # Specifies the name and phone
number of the
administrator.
```

3. Configure una descripción del sistema.

   Esta cadena se coloca en el objeto sysDescription de MIB II. Si la descripción contiene espacios, escríbala entre comillas (" ").

```
[edit groups global snmp]
user@host# set description description
```

   Por ejemplo:

```
[edit groups global snmp]
user@host# set description "M10i router with 8 FPCs" # Specifies the description for the
device.
```

4. Configure una ubicación del sistema.

   Esta cadena se coloca en el objeto sysLocation de MIB II. Si la ubicación contiene espacios, escríbala entre comillas (" ").

   Para especificar la ubicación del sistema:

```
[edit]
snmp {
```

```
    location "Row 11, Rack C";
}
```

```
[edit groups global snmp]
user@host# set location location
```

Por ejemplo:

```
[edit groups global snmp]
user@host# set location "London Corporate Office, Lab 5, Row 11, Rack C" # Specifies the
location of the device.
```

5. En el nivel superior de la configuración, aplique el grupo de configuración.

   Si utiliza un grupo de configuración, debe aplicarlo para que surta efecto.

```
[edit]
user@host# set apply-groups global
```

6. Confirme la configuración.

```
user@host# commit
```

7. Para comprobar la configuración, introduzca el comando de modo operativo.`show snmp mib walk system`

   El comando realiza un recorrido MIB por la tabla del sistema (desde MIB-2 como se define en RFC 1213).`show snmp mib walk system` El agente SNMP de Junos OS responde imprimiendo cada fila de la tabla y su valor asociado. Puede utilizar el mismo comando para realizar un recorrido MIB por cualquier parte del árbol MIB admitido por el agente.

```
user@host> show snmp mib walk system
sysDescr.0    = M10i router with 8 FPCs
sysObjectID.0 = jnxProductNameM10i
sysUpTime.0   = 173676474
sysContact.0  = Enterprise Support, (650) 555-1234
sysName.0     = host
sysLocation.0 = London Corporate Office, Lab 5, Row 11, Rack C
sysServices.0 = 4
```

Configurar el temporizador de retraso de confirmación

Cuando un enrutador o conmutador recibe por primera vez una solicitud SNMP no volátil, se abre una sesión del protocolo XML de Junos OS e impide que otros usuarios o aplicaciones cambien la configuración candidata (equivalente al comando de interfaz de línea de comandos [CLI]).`Setconfigure exclusive` Si el enrutador recibe nuevas solicitudes SNMP mientras se confirma la configuración candidata, la solicitud SNMP se rechaza y se genera un error.`SetSet` Si el enrutador recibe nuevas solicitudes SNMP antes de que hayan transcurrido 5 segundos, el temporizador de retraso de confirmación (el período de tiempo entre la recepción de la última solicitud SNMP y la solicitud de confirmación) se restablece a 5 segundos.`Set`

De forma predeterminada, el temporizador se establece en 5 segundos. Para configurar el temporizador para la respuesta SNMP y el inicio de la confirmación, incluya la instrucción en el nivel de jerarquía:`Setcommit-delay[edit snmp nonvolatile]`

```
[edit snmp nonvolatile]
commit-delay seconds;
```

seconds es el período de tiempo transcurrido entre la recepción de la solicitud SNMP y la confirmación de la configuración candidata. Para obtener más información sobre el comando y el bloqueo de la configuración, consulte la Guía del usuario de la CLI de Junos OS .`configure exclusive`

Configurar SNMP en un dispositivo que ejecute Junos OS

De forma predeterminada, SNMP está deshabilitado en dispositivos que ejecutan Junos OS. Para habilitar SNMP en un enrutador o conmutador, debe incluir las instrucciones de configuración SNMP en el nivel de jerarquía.`[edit snmp]`

Para configurar los requisitos mínimos para SNMP, incluya la instrucción en el nivel de jerarquía.`community public[edit  snmp]`

La comunidad definida aquí como concede acceso de lectura a todos los datos de MIB a cualquier cliente.`public`

Para configurar funciones completas de SNMP, incluya las siguientes instrucciones en el nivel de jerarquía:`[edit snmp]`

```
snmp {
    client-list client-list-name {
        ip-addresses;
```

```
    }
    community community-name {
        authorization authorization;
        client-list-name client-list-name;
        clients {
            address restrict;
        }
        routing-instance routing-instance-name {
            clients {
            addresses;
            }
        }
        logical-system logical-system-name {
            routing-instance routing-instance-name {
                clients {
                addresses;
                }
            }
        }
        view view-name;
    }
    contact contact;
    description description;
    engine-id {
        (local engine-id | use-mac-address | use-default-ip-address);
    }
    filter-duplicates;
    health-monitor {
        falling-threshold integer;
        interval seconds;
        rising-threshold integer;
    }
    interface [ interface-names ];
    location location;
    name name;
    nonvolatile {
        commit-delay seconds;
    }
    rmon {
        alarm index {
            description text-description;
            falling-event-index index;
            falling-threshold integer;
```

```
            falling-threshold-interval seconds;
            interval seconds;
            request-type (get-next-request | get-request | walk-request);
            rising-event-index index;
            sample-type type;
            startup-alarm alarm;
            syslog-subtag syslog-subtag;
            variable oid-variable;
        }
        event index {
            community community-name;
            description text-description;
            type type;
        }
    }
    traceoptions {
        file filename <files number> <size size> <world-readable | no-world-readable> <match
regular-expression>;
        flag flag;
    }
    trap-group group-name {
        categories {
            category;
        }
        destination-port port-number;
        routing-instance instance;
        targets {
            address;
        }
        version (all | v1 | v2);
    }
    trap-options {
        agent-address outgoing-interface;
        source-address address;
    }
    view view-name {
        oid object-identifier (include | exclude);
    }
}
```

SEE ALSO

Descripción de la implementación de SNMP en Junos OS | 388

Ejemplo: Configurar SNMP en el sistema QFabric

in this section

- Requisitos | 411
- Descripción general | 411
- Configuración | 412

De forma predeterminada, SNMP está deshabilitado en dispositivos que ejecutan Junos OS. En este ejemplo se describen los pasos para configurar SNMP en el sistema QFabric.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 12.2
- Sistema de administración de red (NMS) (que ejecuta el administrador SNMP)
- Sistema QFabric (que ejecuta el agente SNMP) con varios dispositivos Node

Descripción general

in this section

- Topología | 412

Debe habilitar SNMP en el dispositivo incluyendo instrucciones de configuración en el nivel jerárquico . `[edit snmp]` Como mínimo, debe configurar la instrucción.`community public` La comunidad definida como pública concede acceso de solo lectura a los datos de MIB a cualquier cliente.

Si no se configura ninguna instrucción, se permiten todos los clientes.`clients` Se recomienda incluir siempre la opción de limitar el acceso del cliente SNMP al conmutador.`restrict`

Topología

La topología de red de este ejemplo incluye un NMS, un sistema QFabric con cuatro dispositivos de nodo y servidores SNMP externos configurados para recibir capturas.

Configuración

in this section

- Procedimiento | **412**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía.`[edit]`

```
set snmp name “snmp qfabric” description “qfabric0 switch”
set snmp location “Lab 4 Row 11” contact “qfabric-admin@qfabric0”
set snmp community public authorization read-only
set snmp client-list list0 192.168.0.0/24
set snmp community public client-list-name list0
set snmp community public clients 192.170.0.0/24 restrict
set snmp trap-group “qf-traps” destination-port 155 targets 192.168.0.100
```

Procedimiento paso a paso

El ejemplo siguiente requiere que navegue por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar SNMP en el sistema QFabric:

NOTA: Si el nombre, la descripción, la ubicación, el contacto o el nombre de la comunidad contienen espacios, escriba el texto entre comillas (" ").

1. Configure el nombre del sistema SNMP:

```
[edit snmp]
user@switch# set name “snmp qfabric”
```

NOTA: Puede acceder al nombre del sistema SNMP configurado anteriormente:

- Mediante una consulta con SNMPGet en el identificador de objeto de política (OID) sysName.0.
- Desde el genérico jnxSyslogTrap. Para enviar jnxSyslogTrap, configure los eventos de captura en la jerarquía.`[edit event-options policy]`

2. Especifique una descripción.

```
[edit snmp]
user@switch# set description “qfabric0 system”
```

Esta cadena se coloca en el objeto sysDescription de MIB II.

3. Especifique la ubicación física del sistema QFabric.

```
[edit snmp]
user@switch# set location “Lab 4 Row 11”
```

Esta cadena se coloca en el objeto sysLocation de MIB II.

4. Especifique un contacto administrativo para el sistema SNMP.

```
[edit snmp]
user@switch# set contact “qfabric-admin@qfabric0”
```

Este nombre se coloca en el objeto sysContact de MIB II.

5. Especifique un nombre de comunidad SNMP único y el nivel de autorización de solo lectura.

> **NOTA**: La opción no es compatible con el sistema QFabric.`read-write`

```
[edit snmp]
user@switch# set community public authorization read-only
```

6. Cree una lista de clientes con un conjunto de direcciones IP que puedan usar la comunidad SNMP.

```
[edit snmp]
user@switch# set client-list list0 192.168.0.0/24
user@switch# set community public client-list-name list0
```

7. Especifique las direcciones IP de los clientes a los que se les restringe el uso de la comunidad.

```
[edit snmp]
user@switch# set community public clients 198.51.100.0/24 restrict
```

8. Configure un grupo de capturas, un puerto de destino y un destino para recibir las capturas SNMP en el grupo de capturas.

```
[edit snmp]
user@switch# set trap-group “qf-traps” destination-port 155 targets 192.168.0.100
```

> **NOTA**: No es necesario incluir la instrucción si utiliza el puerto predeterminado 162.`destination-port`

El grupo de capturas qf-traps está configurado para enviar capturas a 192.168.0.100.

Resultados

Desde el modo de configuración, confírmela con el comando `show`. Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
[edit]
user@switch# show
    snmp {
        name "snmp qfabric";
        description "qfabric0 system";
        location "Lab 4 Row 11";
        contact "qfabric-admin@qfabric0";
        client-list list0 {
            192.168.0.0/24;
        }
        community public {
            authorization read-only;
            clients {
                198.51.100.0/24 restrict;
            }
        }
        trap-group qf-traps {
            destination-port 155;
            targets {
                192.168.0.100;
            }
        }
    }
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

SEE ALSO

> *Descripción de la implementación de SNMP en el sistema QFabric*
>
> Snmp

Configurar opciones en dispositivos administrados para un mejor tiempo de respuesta SNMP

in this section

- Habilitar la opción stats-cache-lifetime | 416
- Filtrar solicitudes SNMP duplicadas | 416
- Excluir interfaces que tardan en responder a las consultas SNMP | 417

Las siguientes secciones contienen información acerca de las opciones de configuración en los dispositivos administrados que pueden mejorar el rendimiento de SNMP:

Habilitar la opción stats-cache-lifetime

Junos OS le ofrece la opción de configurar el período de tiempo (en segundos) que se almacenan en caché las estadísticas de la interfaz. Si el NMS vuelve a consultar la misma interfaz dentro del tiempo de caché, se devuelven los mismos datos. Si el NMS consulta después del tiempo de caché, la memoria caché ya no es válida, se obtienen datos nuevos de las capas inferiores y se actualiza la marca de tiempo de la memoria caché. El valor predeterminado es de 5 segundos.`stats-cache-lifetime` Esto se puede sintonizar según la frecuencia de sondeo.

> **NOTA**: Reducir el valor de la opción stats-cache-lifetime da como resultado más consultas y puede afectar al rendimiento. Para obtener las estadísticas en vivo sin almacenar en caché, establezca el valor de la opción stats-cache-lifetime en 0. Sin embargo, esto no se recomienda, ya que deshabilita completamente la función de almacenamiento en caché y afecta el rendimiento.

Filtrar solicitudes SNMP duplicadas

Si una estación de administración de red retransmite una solicitud , o SNMP con demasiada frecuencia a un dispositivo, dicha solicitud podría interferir con el procesamiento de solicitudes anteriores y ralentizar

el tiempo de respuesta del agente.`GetGetNextGetBulk` El filtrado de estas solicitudes duplicadas mejora el tiempo de respuesta del agente SNMP. Junos OS permite filtrar solicitudes duplicadas , y SNMP.`GetGetNextGetBulk` Junos OS utiliza la siguiente información para determinar si una solicitud SNMP es un duplicado:

- Dirección IP de origen de la solicitud SNMP
- Puerto UDP de origen de la solicitud SNMP
- ID de solicitud de la solicitud SNMP

> **NOTA**: De forma predeterminada, el filtrado de solicitudes SNMP duplicadas está deshabilitado en dispositivos que ejecutan Junos OS.

Para habilitar el filtrado de solicitudes SNMP duplicadas en dispositivos que ejecutan Junos OS, incluya la instrucción en el nivel de jerarquía:`filter-duplicates`[`edit snmp`]

```
[edit snmp]
filter-duplicates;
```

Excluir interfaces que tardan en responder a las consultas SNMP

Una interfaz que es lenta en responder a las solicitudes SNMP para estadísticas de interfaz puede retrasar las respuestas del kernel a las solicitudes SNMP. Puede revisar el archivo de registro mib2d para averiguar cuánto tiempo tarda el kernel en responder a varias solicitudes SNMP. Para obtener más información acerca de cómo revisar el archivo de registro de los datos de respuesta del kernel, consulte "Comprobación de la respuesta del kernel y del motor de reenvío de paquetes" en Supervisión de la actividad de SNMP y seguimiento de problemas que afectan al rendimiento de SNMP en un dispositivo que ejecuta Junos OS."Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS" en la página 538

Si observa que una interfaz determinada tarda en responder y piensa que está ralentizando la respuesta del kernel a las solicitudes SNMP, excluya esa interfaz de las consultas SNMP al dispositivo. Puede excluir una interfaz de las consultas SNMP configurando la instrucción o modificando la configuración de la vista SNMP.`filter-interface`

En el ejemplo siguiente se muestra una configuración de ejemplo para excluir interfaces de las operaciones SNMP , , y :`GetGetNextSet`

```
[edit]
    snmp {
    filter-interfaces {
        interfaces { # exclude the specified interfaces
            interface1;
            interface2;
        }
        all-internal-interfaces; # exclude all internal interfaces
    }
}
```

En el ejemplo siguiente se muestra la configuración de la vista SNMP para excluir la interfaz con un valor de índice de interfaz (ifIndex) de 312 de una solicitud de información relacionada con los objetos ifTable e ifXtable:

```
[edit snmp]
    view test {
        oid .1 include;
        oid ifTable.1.*.312 exclude;
        oid ifXTable.1.*.312 exclude
    }
```

Alternativamente, puede tomar la interfaz que tarda en responder sin conexión.

VÍNCULOS RELACIONADOS

Descripción de la implementación de SNMP en Junos OS | 388

Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS | 538

No Link Title

No Link Title

MIB de utilidad específica para empresas para mejorar la cobertura SNMP

in this section

- MIB de utilidad | 419

MIB de utilidad

in this section

- Utilice la MIB de utilidad específica de la empresa para mejorar la cobertura de SNMP | 420

La MIB de utilidad específica para la empresa de Juniper Networks, cuyo identificador de objeto es {jnxUtilMibRoot 1}, define objetos para contadores, enteros y cadenas. La MIB de utilidad contiene una tabla para cada uno de los cinco tipos de datos siguientes:

- Contadores de 32 bits
- Contadores de 64 bits
- Enteros con signo
- Enteros sin signo
- Cuerdas de octeto

Puede utilizar estos objetos MIB de contenedores para almacenar los datos que no son compatibles con las operaciones SNMP. Puede rellenar los datos de estos objetos mediante comandos de CLI o con la ayuda de scripts Op y una API RPC que puede invocar los comandos de CLI.

Cada tipo de datos tiene un nombre ASCII arbitrario, que se define cuando se rellenan los datos, y una marca de tiempo que muestra la última vez que se modificó la instancia de datos. Para obtener una

versión descargable de esta MIB, consulte Guía del usuario de políticas de enrutamiento, filtros de firewall y políticas de tráfico.

Para obtener información acerca de los objetos MIB de utilidad específicos de la empresa, consulte los temas siguientes:

- jnxUtilCounter32Table
- jnxUtilCounter64Table
- jnxUtilIntegerTable
- jnxUtilUintTable
- jnxUtilStringTable

Utilice la MIB de utilidad específica de la empresa para mejorar la cobertura de SNMP

Es posible que necesite tener métricas de rendimiento personalizadas aunque Junos OS tenga métricas de rendimiento y opciones de supervisión integradas. Para facilitarle la supervisión de estos datos personalizados a través de un sistema de supervisión estándar, Junos OS le proporciona una MIB de utilidad específica para la empresa que puede almacenar dichos datos y, por lo tanto, ampliar la compatibilidad con SNMP para administrar y supervisar los datos de su elección.

Los siguientes comandos de CLI le permiten establecer y borrar valores de objeto MIB de utilidad:

- `request snmp utility-mib set instance` *`name`* `object-type <counter | counter 64 | integer | string | unsigned integer> object-value` *`value`*
- `request snmp utility-mib clear instance` *`name`* `object-type <counter | counter 64 | integer | string | unsigned integer>`

La opción del comando especifica el nombre de la instancia de datos y es el identificador principal de los datos.`instance` *`name`*`request snmp utility-mib <set | clear>` La opción permite especificar el tipo de objeto y la opción permite establecer el valor del objeto.`object-type <counter | counter 64 | integer | string | unsigned integer>object-value` *`value`*

Para automatizar el proceso de rellenar los datos MIB de la utilidad, puede usar una combinación de una directiva de eventos y un script de eventos. En los ejemplos siguientes se muestra la configuración para que una directiva de eventos se ejecute cada hora y almacene los datos en objetos MIB de utilidad mediante la ejecución de una secuencia de comandos de eventos ().`show system buffersshow system bufferscheck-mbufs.slax`

Configuración de la directiva de eventos

Para configurar una directiva de eventos que ejecute el comando cada hora e invoque para almacenar los datos en objetos MIB de utilidad, incluya las siguientes instrucciones en el nivel de jerarquía []:`show system bufferscheck-mbufs.slaxshow system buffersedit`

```
event-options {
    generate-event {
        1-HOUR time-interval 3600;
    }
    policy MBUFS {
        events 1-HOUR;
        then {
            event-script check-mbufs.slax; # script stored at /var/db/scripts/event/
        }
    }
    event-script {
        file check-mbufs.slax;
    }
}
```

Script check-mbufs.slax

En el ejemplo siguiente se muestra la secuencia de comandos almacenada en :`check-mbufs.slax/var/db/scripts/event/`

```
------ script START ------
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
ns ext = "http://xmlsoft.org/XSLT/namespace";

match / {
    <op-script-results>{
        var $result = jcs:invoke("get-buffer-informations");
        var $rpc = <request-snmp-utility-mib-set> {
                <object-type> "integer";
                <instance> "current-mbufs";
                <object-value> $result/current-mbufs;
```

```
        }
        var $res = jcs:invoke($rpc);
        expr jcs:syslog("external.info", $res/..//snmp-utility-mib-results/snmp-utility-mib-
result);
    }
}
------ script END ------
```

Puede ejecutar el siguiente comando para comprobar los datos almacenados en la MIB de la utilidad como resultado de la directiva de eventos y el script que se muestran en los ejemplos anteriores:

```
user@host> show snmp mib walk jnxUtilData ascii jnxUtilIntegerValue."current-mbufs" = 0
jnxUtilIntegerTime."current-mbufs" = 07 da 05 0c  03 14 2c 00  2d 07 00   user@caramels>
```

NOTA: El comando no está disponible en el sistema QFabric, pero puede utilizar aplicaciones cliente SNMP externas para realizar esta operación.`show snmp mib walk`

SEE ALSO

- MIB SNMP específicas de la empresa compatibles con Junos OS
- MIB SNMP estándar compatibles con Junos OS
- *Descripción de la implementación de SNMP en el sistema QFabric*

Optimice la configuración del sistema de administración de red para obtener los mejores resultados

Puede modificar la configuración del sistema de administración de red para optimizar el tiempo de respuesta de las consultas SNMP. Puede configurar el sistema de administración de red siguiendo los siguientes consejos:

- **Cambiar el método de sondeo de columna por columna a fila por fila**

Puede configurar el sistema de administración de red para que utilice el método fila por fila para el sondeo de datos SNMP. Es evidente que los métodos de sondeo fila por fila y múltiple fila por fila múltiple son más eficientes que el sondeo columna por columna.

Al configurar el sistema de administración de red para que utilice el método de sondeo de datos fila por fila, puede:

- Sondee los datos de una sola interfaz en una solicitud en lugar de una sola solicitud Sondeando datos para varias interfaces, como en el caso del sondeo columna por columna.
- Reduce el riesgo de que se agote el tiempo de espera de las solicitudes.

- **Reducir el número de enlaces variables por PDU**

  Puede mejorar el tiempo de respuesta de las solicitudes SNMP reduciendo el número de enlaces variables por unidad de datos de protocolo (PDU). Una solicitud que sondea datos relacionados con varios objetos asignados a diferentes entradas de índice, lo que se traduce en varias solicitudes en el extremo del dispositivo. Esto se debe a que es posible que el subagente tenga que sondear diferentes módulos para obtener datos vinculados a diferentes entradas de índice.

  El método recomendado es asegurarse de que una solicitud sólo tiene objetos vinculados a una entrada de índice en lugar de varios objetos vinculados a diferentes entradas de índice.

  > **NOTA**: Si las respuestas de un dispositivo son lentas, evite usar la opción para el dispositivo, ya que una solicitud puede contener objetos vinculados a varias entradas de índice y podría aumentar aún más el tiempo de respuesta.`GetBulkGetBulk`

- **snmp bulk-get número recomendado de OID y repeticiones máximas**

  Una solicitud SNMP bulk-get responde con un total de enlaces variables (máximo de repeticiones * número de OID). Cuando los objetos estadísticos de interfaz (como ifInOctets, ifOutOctets, etc.) están presentes en una consulta, las solicitudes se envían a las capas inferiores. Por lo tanto, hay un impacto en las respuestas por un aumento en las repeticiones máximas que envía en una solicitud de obtención masiva. Para consultas masivas de objetos de estadísticas de interfaz, se recomienda usar el valor 'max-repetitions' de 10, y el número máximo de OID por solicitud es 10.

- **Aumentar los valores de tiempo de espera en intervalos de sondeo y detección**

  Al aumentar los valores de tiempo de espera para los intervalos de sondeo y detección, puede:

  - Aumente el tiempo de cola en el extremo del dispositivo.
  - Reduzca el número de caídas del acelerador que se producen debido al tiempo de espera de la solicitud.

- **Reducir la velocidad de paquetes entrantes en el snmpd**

Los siguientes métodos reducen el riesgo de que las solicitudes SNMP se acumulen en cualquier dispositivo.

- Reduzca la frecuencia de envío de solicitudes SNMP a un dispositivo.
- Aumente el intervalo de sondeo.
- Controlar el uso de las solicitudes.`GetNext`
- Reduzca el número de centros de votación por dispositivo.

VÍNCULOS RELACIONADOS

Descripción de la implementación de SNMP en Junos OS

Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS | **538**

Gestión de trampas e informes

Interfaces para aceptar solicitudes SNMP

in this section

- Configurar las interfaces en las que se pueden aceptar solicitudes SNMP | **424**
- Configurar un agente SNMP de proxy | **425**
- Ejemplo: Configurar la comprobación de la lista de acceso seguro | **426**
- Filtrar la información de la interfaz de la salida SNMP Get y GetNext | **426**

Configurar las interfaces en las que se pueden aceptar solicitudes SNMP

De forma predeterminada, todas las interfaces de enrutador o conmutador tienen privilegios de acceso SNMP. Para limitar el acceso solo a través de determinadas interfaces, incluya la instrucción en el nivel jerárquico .`interface[edit snmp]`

Especifique los nombres de cualquier interfaz lógica o física que deba tener privilegios de acceso SNMP. Se descarta cualquier solicitud SNMP que entre en el enrutador o conmutador desde interfaces no enumeradas.

Configurar un agente SNMP de proxy

A partir de la versión 12.3, Junos OS permite asignar uno de los dispositivos de la red como agente SNMP proxy a través del cual el sistema de administración de red (NMS) puede consultar a otros dispositivos de la red. Al configurar un proxy, puede especificar los nombres de los dispositivos que se administrarán mediante el agente SNMP de proxy.

Cuando el NMS consulta el agente SNMP de proxy, el NMS especifica el nombre de la comunidad (para SNMPv1 y SNMPv2) o el nombre de contexto y seguridad (para SNMPv3) asociado al dispositivo del que requiere la información.

NOTA: Si ha configurado métodos de autenticación y privacidad y contraseñas para SNMPv3, esos parámetros también se especifican en la consulta de información de SNMPv3.

Para configurar un agente SNMP de proxy y especificar los dispositivos que administrará el agente SNMP de proxy, consulte *proxy (snmp)*.

NOTA: A partir de Junos OS versión 15.2, debe configurar la instrucción en el nivel de jerarquía para el agente SNMP de proxy.`interface <interface-name>[edit snmp]`

NOTA: Las configuraciones de comunidad y seguridad para el proxy deben coincidir con las configuraciones correspondientes en el dispositivo que se va a administrar.

NOTA: Los dispositivos administrados por el agente SNMP proxy envían las capturas directamente al sistema de administración de red, ya que el agente SNMP proxy no tiene capacidades de reenvío de capturas.

Puede usar el comando del modo operativo para ver los detalles del proxy en un dispositivo.`show snmp proxy` El comando devuelve los nombres de proxy, los nombres de dispositivo, la versión de SNMP, la comunidad/seguridad y la información de contexto.`show snmp proxy`

Ejemplo: Configurar la comprobación de la lista de acceso seguro

Los privilegios de acceso SNMP solo se conceden a dispositivos en interfaces y `.so-0/0/0at-1/0/1` Para ello, el ejemplo siguiente configura una lista de interfaces lógicas:

```
[edit]
snmp {
    interface [ so-0/0/0.0 so-0/0/0.1 at-1/0/1.0 at-1/0/1.1 ];
}
```

En el ejemplo siguiente se concede el mismo acceso mediante la configuración de una lista de interfaces físicas:

```
[edit]
snmp {
    interface [ so-0/0/0 at-1/0/1 ];
}
```

Filtrar la información de la interfaz de la salida SNMP Get y GetNext

Junos OS permite filtrar la información relacionada con interfaces específicas de la salida de SNMP y las solicitudes.`GetGetNext` Puede hacerlo en MIB relacionadas con la interfaz, como IF MIB, ATM MIB, RMON MIB y la MIB de IF específica de la empresa de Juniper Networks.

Puede utilizar las siguientes opciones de la instrucción en el nivel de jerarquía para especificar las interfaces que desea excluir de SNMP y las consultas:`filter-interfaces[edit snmp]GetGetNext`

- `interfaces`: interfaces que coinciden con las expresiones regulares especificadas.
- `all-internal-interfaces`—Interfaces internas.

```
[edit]
    snmp {
    filter-interfaces {
        interfaces {
            interface-name 1;
            interface-name 2;
        }
```

```
        all-internal-interfaces;
    }
}
```

A partir de la versión 12.1, Junos OS proporciona una opción excepto (operador) que permite filtrar todas las interfaces excepto aquellas interfaces que coinciden con todas las expresiones regulares con el prefijo marca.!!

Por ejemplo, para filtrar todas las interfaces excepto las interfaces del SNMP y los resultados, escriba el siguiente comando:gegetget-next

```
[edit snmp]
user@host# set filter-interfaces interfaces "!^ge-.*"
user@host# commit
```

Cuando esto está configurado, Junos OS filtra todas las interfaces excepto las interfaces del SNMP y los resultados.gegetget-next

> **NOTA**: La marca solo se admite como primer carácter de la expresión regular.! Si aparece en cualquier otro lugar de una expresión regular, Junos OS considera que la expresión regular no es válida y devuelve un error.

Sin embargo, tenga en cuenta que esta configuración solo se aplica a las operaciones SNMP. Los usuarios pueden seguir accediendo a la información relacionada con las interfaces (incluidas las que se ocultan mediante las opciones) mediante los comandos de interfaz de línea de comandos (CLI) de Junos OS adecuados.filter-interfaces

Configurar SNMP para instancias de enrutamiento

in this section

- Descripción de la compatibilidad de SNMP con instancias de enrutamiento | **428**
- Instancia de enrutamiento de administración SNMPv3 | **429**
- MIB SNMP admitidas para instancias de enrutamiento | **431**
- Clases de soporte para objetos MIB | **443**

- Capturas SNMP admitidas para instancias de enrutamiento | 444
- Identificar una instancia de enrutamiento | 445
- Habilitar el acceso SNMP a través de instancias de enrutamiento | 446
- Especificar una instancia de enrutamiento en una comunidad SNMPv1 o SNMPv2c | 446
- Ejemplo: Configuración de las opciones de interfaz para una instancia de enrutamiento | 447
- Configuración de listas de acceso para el acceso SNMP a través de instancias de enrutamiento | 449

Descripción de la compatibilidad de SNMP con instancias de enrutamiento

Junos OS habilita a los administradores SNMP de todas las instancias de enrutamiento para solicitar y administrar datos SNMP relacionados con las instancias de enrutamiento y las redes del sistema lógico correspondientes.

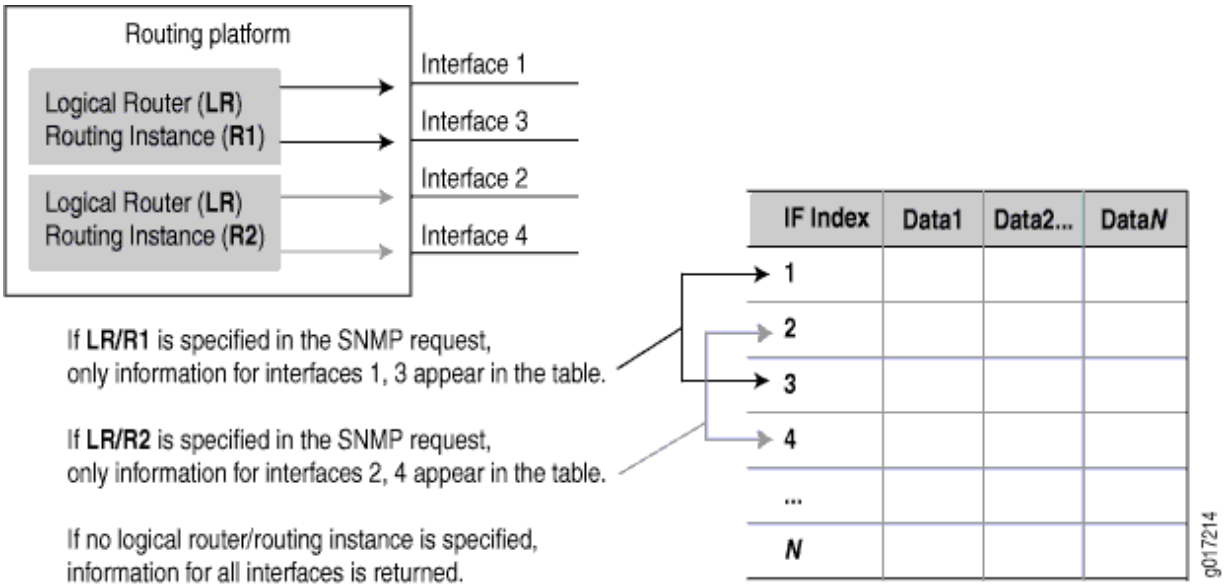
En Junos OS:

- Los clientes de instancias de enrutamiento o sistemas lógicos distintos del predeterminado pueden tener acceso a objetos MIB y realizar operaciones SNMP solo en la instancia de enrutamiento o en las redes del sistema lógico a las que pertenecen.
- Los clientes de la instancia de enrutamiento predeterminada pueden acceder a información relacionada con todas las instancias de enrutamiento y redes de sistemas lógicos.
- La instancia de enrutamiento de administración de Junos () es una instancia especial.`mgmt_junos` Los clientes de la instancia de enrutamiento de administración se tratan como si estuvieran en la instancia de enrutamiento predeterminada y pueden acceder a información relacionada con todas las instancias de enrutamiento y redes de sistemas lógicos.

Antes de Junos OS versión 8.4, sólo el administrador SNMP de la instancia de enrutamiento predeterminada (inet.0) tenía acceso a los objetos MIB.

Con el aumento de las ofertas de servicios de red privada virtual (VPN), esta función es útil especialmente para los proveedores de servicios que necesitan obtener datos SNMP para instancias de enrutamiento específicas (consulte).Figura 22 en la página 429 Los proveedores de servicios pueden utilizar esta información para sus propias necesidades de gestión o exportar los datos para que los utilicen sus clientes.

Figura 22: Datos SNMP para instancias de enrutamiento



Si no se especifica ninguna instancia de enrutamiento en la solicitud, el agente SNMP funciona como antes:

- Para los objetos de tabla que no son de enrutamiento, se exponen todas las instancias.
- Para los objetos de tabla de enrutamiento, solo se exponen aquellos asociados con la instancia de enrutamiento predeterminada.

> **NOTA**: Las unidades de datos de protocolo (PDU) reales se siguen intercambiando a través de la instancia de enrutamiento predeterminada (inet.0), pero el contenido de los datos devueltos viene dictado por la instancia de enrutamiento especificada en las PDU de solicitud.

Instancia de enrutamiento de administración SNMPv3

in this section

- Ventajas | 430
- Habilitar la instancia de enrutamiento de administración | 430
- Quitar la instancia de enrutamiento de administración | 430

A partir de Junos OS 19.4R1, puede acceder a la información relacionada con todas las instancias de enrutamiento y redes del sistema lógico, y no específica de la instancia de enrutamiento de entrada, configurando la interfaz de administración SNMPv3 en una instancia de enrutamiento necesaria. Puede configurar la instrucción de configuración de la instancia de administración en el nivel jerárquico .`[edit snmp v3]`

Ventajas

La instancia de enrutamiento de administración SNMPv3 habilita todas las solicitudes SNMPv3 de una instancia de enrutamiento no predeterminada como si las solicitudes fueran de una instancia de enrutamiento predeterminada. Mediante la instancia de enrutamiento de administración SNMPv3, se accede a la información relacionada con todas las instancias de enrutamiento y redes de sistemas lógicos.

Habilitar la instancia de enrutamiento de administración

Para habilitar la instancia de enrutamiento de administración SNMPv3:

1. Configure la instrucción management-instance.

```
[edit]
user@host# set snmp v3 management-routing-instance <routing-instance>
```

2. Confirme la configuración.

```
[edit]
user@host# commit
```

Quitar la instancia de enrutamiento de administración

Para quitar la instancia de enrutamiento de administración SNMPv3:

1. Elimine o desactive la instrucción de instancia de enrutamiento de administración SNMPv3.

```
[edit]
user@host# delete snmp v3 management-routing-instance <routing-instance>
```

No puede configurar la instancia de enrutamiento de administración de Junos () en el nivel de jerarquía [], ya que tiene acceso a todas las instancias de enrutamiento de forma predeterminada.`mgmt_junosedit snmp v3 management-routing-instance <routing-instance>mgmt_junos`

MIB SNMP admitidas para instancias de enrutamiento

Tabla 28 en la página 431 muestra objetos MIB específicos de la empresa compatibles con Junos OS y proporciona notas que detallan cómo se manejan cuando se especifica una instancia de enrutamiento en una solicitud SNMP. Un guión en (–) indica que el artículo no es aplicable.

Tabla 28: Compatibilidad con MIB para instancias de enrutamiento (MIB de Juniper Networks)

Objeto	Clase de soporte	Descripción/Notas
jnxProductos(1)	–	Id. de objeto de producto
jnxServicios(2)	–	Servicios
jnxMibs(3) jnxBoxAnatomy(1)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
MPLS(2)	Clase 2	Se exponen todas las instancias de un sistema lógico. Los datos no se segregarán hasta el nivel de instancia de enrutamiento.
ifnx(3)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxAlarmas(4)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxFirewalls(5)	Clase 4	Los datos no se segregan por instancia de enrutamiento. Se exponen todas las instancias.

Tabla 28: Compatibilidad con MIB para instancias de enrutamiento (MIB de Juniper Networks) ***(Continued)***

Objeto	Clase de soporte	Descripción/Notas
jnxDCUs(6)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxPingMIB(7)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxTraceRouteMIB(8)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxATM(10)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxIpv6(11)	Clase 4	Los datos no se segregan por instancia de enrutamiento. Se exponen todas las instancias.
jnxIpv4(12)	Clase 1	jnxIpv4AddrTable(1). Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxRmon(13)	Clase 3	jnxRmonAlarmTable(1). Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxLdp(14)	Clase 2	jnxLdpTrapVars(1). Se exponen todas las instancias de un sistema lógico. Los datos no se segregarán hasta el nivel de instancia de enrutamiento.

Tabla 28: Compatibilidad con MIB para instancias de enrutamiento (MIB de Juniper Networks) ***(Continued)***

Objeto	Clase de soporte	Descripción/Notas
jnxCos(15) jnxCosIfqStatsTable(1) jnxCosFcTable(2) jnxCosFcIdTable(3) jnxCosQstatTable(4)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxScu(16) jnxScuStatsTable(1)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxRpf(17) jnxRpfStatsTable(1)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxCfgMgmt(18)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxPMon(19) jnxPMonFlowTable(1) jnxPMonErrorTable(2) jnxPMonMemoryTable(3)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxSonet(20) jnxSonetAlarmTable(1)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.

Tabla 28: Compatibilidad con MIB para instancias de enrutamiento (MIB de Juniper Networks) ***(Continued)***

Objeto	Clase de soporte	Descripción/Notas
jnxAtmCos(21) jnxCosAtmVcTable(1) jnxCosAtmScTable(2) jnxCosAtmVcQstatsTable(3) jnxCosAtmTrunkTable(4)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
ipSecFlowMonitorMIB(22)	–	–
jnxMac(23) jnxMacStats(1)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
apsMIB(24)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxChassisDefines(25)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.
jnxVpnMIB(26)	Clase 2	Se exponen todas las instancias de un sistema lógico. Los datos no se segregarán hasta el nivel de instancia de enrutamiento.
jnxSericesInfoMib(27)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxCollectorMIB(28)	Clase 1	Solo se exponen aquellas interfaces lógicas (y sus interfaces físicas principales) que pertenecen a una instancia de enrutamiento específica.
jnxHistoria(29)	–	–

Tabla 28: Compatibilidad con MIB para instancias de enrutamiento (MIB de Juniper Networks) *(Continued)*

Objeto	Clase de soporte	Descripción/Notas
jnxSpMIB(32)	Clase 3	Los objetos sólo se exponen para el sistema lógico predeterminado.

Tabla 29 en la página 435 muestra objetos MIB de clase 1 (MIB estándar y específicos de la empresa) compatibles con Junos OS. Con los objetos de clase 1, solo se exponen aquellas interfaces lógicas (y sus interfaces físicas primarias) que pertenecen a una instancia de enrutamiento específica.

Tabla 29: Objetos MIB de clase 1 (MIB estándar y Juniper)

Clase	BIA	Objetos
Clase 1	802.3ad.mib	(dot3adAgg) Objetos MIB: dot3adAggTable dot3adAggPortListTable (dot3adAggPort) dot3adAggPortTable dot3adAggPortStatsTable dot3adAggPortDebugTable
	rfc2863a.mib	ifTable ifXTable ifStackTable
	rfc2011a.mib	ipAddrTable ipNetToMediaTable
	rtmib.mib	ipForward (ipCidrRouteTable)

Tabla 29: Objetos MIB de clase 1 (MIB estándar y Juniper) ***(Continued)***

Clase	BIA	Objetos
	rfc2665a.mib	dot3StatsTable dot3ControlTable dot3PauseTable
	rfc2495a.mib	dsx1ConfigTable dsx1CurrentTable dsx1IntervalTable dsx1TotalTable dsx1FarEndCurrentTable dsx1FarEndIntervalTable dsx1FarEndTotalTable dsx1FracTable ...
	rfc2496a.mib	dsx3 (dsx3ConfigTable)
	rfc2115a.mib	frDlcmiTable (y objetos MIB relacionados)
	rfc3592.mib	sonetMediumTable (y objetos MIB relacionados)
	rfc3020.mib	mfrMIB mfrBundleTable mfrMibBundleLinkObjects mfrBundleIfIndexMappingTable (y objetos MIB relacionados)
	ospf2mib.mib	Todos los objetos

Tabla 29: Objetos MIB de clase 1 (MIB estándar y Juniper) ***(Continued)***

Clase	BIA	Objetos
	ospf2trap.mib	Todos los objetos
	bgpmib.mib	Todos los objetos
	rfc2819a.mib	Ejemplo: etherStatsTable
Clase 1	rfc2863a.mib	Ejemplos: ifXtable ifStackTable
	rfc2665a.mib	etherMIB
	rfc2515a.mib	objetos atmMIB Ejemplos: atmInterfaceConfTable atmVplTable atmVclTable
	rfc2465.mib	IP-V6MIB Ejemplos: ipv6IfTable ipv6AddrPrefixTable ipv6NetToMediaTable ipv6RouteTable
	rfc2787a.mib	MIB VRRP

Tabla 29: Objetos MIB de clase 1 (MIB estándar y Juniper) ***(Continued)***

Clase	BIA	Objetos
	rfc2932.mib	ipMRouteMIB ipMRouteStdMIB
	mroutemib.mib	ipMRoute1MIBObjects
	isismib.mib	isisMIB
	pimmib.mib	pimMIB
	msdpmib.mib	msdpmib
	jnx-if-extensions.mib	Ejemplos: ifJnxTable ifChassisTable
	jnx-dcu.mib	jnxDCU
	jnx-atm.mib	Ejemplos: jnxAtmIfTable jnxAtmVCTable jnxAtmVpTable
	jnx-ipv4.mib	jnxipv4 Ejemplo: jnxIpv4AddrTable
	jnx-cos.mib	Ejemplos: jnxCosIfqStatsTable jnxCosQstatTable

Tabla 29: Objetos MIB de clase 1 (MIB estándar y Juniper) ***(Continued)***

Clase	BIA	Objetos
	jnx-scu.mib	Ejemplo: jnxScuStatsTable
	jnx-rpf.mib	Ejemplo: jnxRpfStatsTable
	jnx-pmon.mib	Ejemplo: jnxPMonFlowTable
	jnx-sonet.mib	Ejemplo: jnxSonetAlarmTable
Clase 1	jnx-atm-cos.mib	Ejemplos: jnxCosAtmVcTable jnxCosAtmVcScTable jnxCosAtmVcQstatsTable jnxCosAtmTrunkTable
	jnx-mac.mib	Ejemplo: jnxMacStatsTable
	jnx-services.mib	Ejemplo: jnxSvcFlowTableAggStatsTable
	jnx-coll.mib	jnxCollectorMIB Ejemplos: jnxCollPicIfTable jnxCollFileEntry

Tabla 30 en la página 440 muestra objetos MIB de clase 2 (MIB estándar y específicos de la empresa) compatibles con Junos OS. Con los objetos de clase 2, se exponen todas las instancias de un sistema lógico. Los datos no se segregarán hasta el nivel de instancia de enrutamiento.

Tabla 30: Objetos MIB de clase 2 (MIB estándar y Juniper)

Clase	BIA	Objetos
Clase 2	rfc3813.mib	mplsLsrStdMIB Ejemplos: mplsInterfaceTable mplsInSegmentTable mplsOutSegmentTable mplsLabelStackTable mplsXCTable (y objetos MIB relacionados)
	igmpmib.mib	igmpStdMIB **NOTA**: El es la versión preliminar del IGMP Standard MIB en el árbol experimental.`igmpmib.mib` Junos OS no es compatible con la MIB estándar IGMP original.
	l3vpnmib.mib	mplsVpnmib
	jnx-mpls.mib	Ejemplo: mplsLspList
	jnx-ldp.mib	jnxLdp Ejemplo: jnxLdpStatsTable
	jnx-vpn.mib	jnxVpnMIB
	jnx-bgpmib2.mib	jnxBgpM2Experiment

Tabla 31 en la página 441 muestra objetos MIB de clase 3 (MIB estándar y específicos de la empresa) compatibles con Junos OS. Con la clase 3, los objetos se exponen sólo para el sistema lógico predeterminado.

Tabla 31: Objetos MIB de clase 3 (MIB estándar y Juniper)

Clase	BIA	Objetos
Clase 3	rfc2819a.mib	rmonEventos alarmTable logTable eventTable agentxMIB
	rfc2925a.mib	pingmib
	rfc2925b.mib	tracerouteMIB
	jnxchasis.mib	jnxBoxAnatomía
	jnx-chassis-alarm.mib	jnxAlarmas De forma predeterminada, los firewalls de la serie SRX consultan mib jnxAlarms solo en el nodo principal del grupo de redundancia 0 (RG0) y no en el nodo secundario.
	jnx-ping.mib	jnxPingMIB
	jnx-traceroute.mib	jnxTraceRouteMIB
	jnx-rmon.mib	jnxRmonAlarmTable
	jnx-cos.mib	Ejemplo: jnxCosFcTable
	jnx-cfgmgmt.mib	Ejemplo: jnxCfgMgmt
	jnx-sonetaps.mib	apsMIBObjects

Tabla 31: Objetos MIB de clase 3 (MIB estándar y Juniper) ***(Continued)***

Clase	BIA	Objetos
	jnx-sp.mib	jnxSpMIB
	ggsn.mib	ejnmobileipABmib
	rfc1907.mib	snmpModules
	snmpModules	Ejemplos: snmpMIB snmpFrameworkMIB

Tabla 32 en la página 442 muestra objetos MIB de clase 4 (MIB estándar y específicos de la empresa) compatibles con Junos OS. Con los objetos de clase 4, los datos no se segregan por instancia de enrutamiento. Se exponen todas las instancias.

Tabla 32: Objetos MIB de clase 4 (MIB estándar y Juniper)

Clase	BIA	Objetos
Clase 4	Sistema	Ejemplo: sysORTable
	rfc2011a.mib	ip (ipDefaultTTL, ipInReceives) Icmp
	rfc2012a.mib	Tcp tcpConnTable ipv6TcpConnTable
	rfc2013a.mib	Udp udpTable ipv6UdpTable

Tabla 32: Objetos MIB de clase 4 (MIB estándar y Juniper) ***(Continued)***

Clase	BIA	Objetos
	rfc2790a.mib	hrSystem
	rfc2287a.mib	sysApplOBJ
	jnx-firewall.mib	jnxFirewalls
	jnx-ipv6.mib	jnxIpv6

Clases de soporte para objetos MIB

Cuando se especifica una instancia de enrutamiento, todos los objetos MIB relacionados con el enrutamiento devuelven datos mantenidos por la instancia de enrutamiento en la solicitud. Para todos los demás objetos MIB, los datos devueltos se segregan según esa instancia de enrutamiento. Por ejemplo, el agente SNMP solo expone las interfaces asignadas a esa instancia de enrutamiento (por ejemplo, las interfaces lógicas [ifls] así como sus interfaces físicas correspondientes [ifds]). Del mismo modo, los objetos con un enlace inequívoco a una interfaz (por ejemplo, direcciones) también se segregan.

Para aquellos objetos en los que el archivo adjunto es ambiguo (por ejemplo, objetos en sysApplMIB), no se realiza ninguna segregación y todas las instancias son visibles en todos los casos.

Otra categoría de objetos sólo es visible cuando no se especifica ningún sistema lógico (sólo dentro del sistema lógico predeterminado), independientemente de la instancia de enrutamiento dentro del sistema lógico predeterminado. Los objetos de esta categoría son objetos MIB de chasis, objetos del grupo SNMP, alarma RMON, grupos de eventos y registros, objetos MIB de ping, objetos de administración de configuración y objetos V3.

En resumen, para admitir instancias de enrutamiento, los objetos MIB se dividen en una de las siguientes categorías:

- Clase 1: los datos se segregan según la instancia de enrutamiento de la solicitud. Esta es la más granular de las clases de segregación.
- Clase 2: los datos se segregan según el sistema lógico especificado en la solicitud. Se devuelven los mismos datos para todas las instancias de enrutamiento que pertenecen a un sistema lógico

determinado. Normalmente, esto se aplica a objetos de tabla de enrutamiento donde es difícil extraer información de instancia de enrutamiento o donde no se aplican instancias de enrutamiento.

- Clase 3: los datos se exponen solo para el sistema lógico predeterminado. Se devuelve el mismo conjunto de datos para todas las instancias de enrutamiento que pertenecen al sistema lógico predeterminado. Si especifica otro sistema lógico (no el predeterminado), no se devuelve ningún dato. Normalmente, esta clase se aplica a objetos implementados en subagentes que no supervisan los cambios lógicos del sistema y registran sus objetos utilizando únicamente el contexto predeterminado (por ejemplo, objetos MIB de chasis).
- Clase 4: los datos no se segregan por instancia de enrutamiento. Se devuelven los mismos datos para todas las instancias de enrutamiento. Normalmente, esto se aplica a los objetos implementados en subagentes que supervisan los cambios del sistema lógico y registran o anulan el registro de todos sus objetos para cada cambio en el sistema lógico. Los objetos cuyos valores no se pueden segregar por instancia de enrutamiento pertenecen a esta clase.

Consulte "MIB SNMP admitidas para instancias de enrutamiento para" en la página 431 obtener una lista de los objetos asociados a cada clase.

Capturas SNMP admitidas para instancias de enrutamiento

Puede restringir la recepción de capturas de los receptores de capturas que no estén relacionadas con las redes del sistema lógico a las que pertenecen. Para ello, incluya la instrucción en el nivel jerárquico :`logical-system-trap-filter`[`edit snmp`]

```
[edit snmp]
logical-system-trap-filter;
```

Si la instrucción no se incluye en la configuración SNMP, todas las capturas se reenvían a los destinos de la instancia de enrutamiento configurada.`logical-system-trap-filter` Sin embargo, incluso cuando esta instrucción está configurada, el receptor de capturas asociado con la instancia de enrutamiento predeterminada recibirá todas las capturas SNMP.

Cuando se configuran bajo el objeto trap-group, todas las capturas v1 y v2c que se aplican a instancias de enrutamiento (o interfaces que pertenecen a una instancia de enrutamiento) tienen el nombre de instancia de enrutamiento codificado en la cadena de comunidad. La codificación es idéntica a la utilizada en las PDU de solicitud.

Para las capturas configuradas en el marco v3, el nombre de la instancia de enrutamiento se lleva en el campo de contexto cuando se ha configurado el modelo de procesamiento de mensajes v3. Para otros modelos de procesamiento de mensajes (v1 o v2c), el nombre de la instancia de enrutamiento no se incluye en el encabezado del mensaje de captura (ni se codifica en la cadena de comunidad).

Identificar una instancia de enrutamiento

Con esta característica, las instancias de enrutamiento se identifican mediante el campo de contexto en las solicitudes v3 o codificadas en la cadena de comunidad en las solicitudes v1 o v2c.

Cuando se codifica en una cadena de comunidad, el nombre de la instancia de enrutamiento aparece primero y el carácter lo separa de la cadena de comunidad real.`@`

Para evitar conflictos con cadenas de comunidad válidas que contienen el carácter, la comunidad sólo se analiza si se produce un error en el procesamiento típico de cadenas de comunidad.`@` Por ejemplo, si se configura una instancia de enrutamiento denominada , se procesa una solicitud SNMP con en el contexto de la instancia de enrutamiento.`RIRI@publicRI` El control de acceso (vistas, restricciones de dirección de origen, privilegios de acceso, etc.) se aplica de acuerdo con la cadena de comunidad real (el conjunto de datos después del carácter, en este caso).`@public` Sin embargo, si se configura la cadena de comunidad, la unidad de datos de protocolo (PDU) se procesa de acuerdo con esa comunidad y se omite el nombre de instancia de enrutamiento incrustado.`RI@public`

Los sistemas lógicos realizan un subconjunto de las acciones de un enrutador físico y tienen sus propias tablas de enrutamiento, interfaces, políticas e instancias de enrutamiento. Cuando se define una instancia de enrutamiento dentro de un sistema lógico, el nombre del sistema lógico debe codificarse junto con la instancia de enrutamiento mediante una barra diagonal ( ) para separar ambas./ Por ejemplo, si la instancia de enrutamiento está configurada en el sistema lógico , dicha instancia de enrutamiento debe codificarse dentro de una cadena de comunidad como .`RILSLS/RI@public` Cuando se configura una instancia de enrutamiento fuera de un sistema lógico (dentro del sistema lógico predeterminado), no se necesita ningún nombre (o carácter) de sistema lógico./

Además, cuando se crea un sistema lógico, siempre se crea una instancia de enrutamiento predeterminada (denominada) dentro del sistema lógico.`default` Este nombre debe utilizarse al consultar datos para esa instancia de enrutamiento (por ejemplo,).`LS/default@public` Para las solicitudes v3, el nombre debe identificarse directamente en el campo de contexto.*logical system/routing instance*

> **NOTA**: Para identificar una instancia de árbol de expansión de LAN virtual (VLAN) (VSTP en plataformas de enrutamiento universal 5G de la serie MX), especifique el nombre de la instancia de enrutamiento seguido de dos puntos () y el ID de VLAN.`::` Por ejemplo, para identificar la instancia de VSTP para VLAN 10 en la instancia de enrutamiento predeterminada global, incluya en la cadena (SNMPv3) o (SNMPv1 o v2).`default::10@publiccontextcommunity`

Habilitar el acceso SNMP a través de instancias de enrutamiento

Para permitir que los administradores SNMP de instancias de enrutamiento distintas de la predeterminada tengan acceso a la información de SNMP, incluya la instrucción en el nivel de jerarquía.`routing-instance-access`[`edit snmp`]

Si esta instrucción no se incluye en la configuración de SNMP, los administradores SNMP de instancias de enrutamiento distintas de la instancia de enrutamiento predeterminada no pueden tener acceso a la información de SNMP. Esta configuración se aplica a las solicitudes de cualquier versión de SNMP (SNMP v1, v2 o v3).

Especificar una instancia de enrutamiento en una comunidad SNMPv1 o SNMPv2c

Puede especificar la instancia de enrutamiento junto con la información del cliente cuando agregue un cliente a una comunidad SNMP. Para especificar la instancia de enrutamiento a la que pertenece un cliente, incluya la instrucción seguida del nombre de la instancia de enrutamiento y la información del cliente en la configuración SNMP.`routing-instance`

En el ejemplo siguiente se muestra la instrucción configuration para agregar la instancia de enrutamiento test-ri a la comunidad SNMP1.

> **NOTA**: Las instancias de enrutamiento especificadas en el nivel de jerarquía se agregan al sistema lógico predeterminado de la comunidad.[`edit snmp community` *`community-name`*]

```
[edit snmp]
community community1 {
    clients {
        10.209.152.33/32;
    }
    routing-instance test-ri {
        clients {
            10.19.19.1/32;
        }
    }
}
```

Si la instancia de enrutamiento se define dentro de un sistema lógico, incluya la instrucción en el nivel de jerarquía [], como en el ejemplo siguiente:`routing-instanceedit snmp community` *`community-name`* `logical-system` *`logical-system-name`*

```
[edit snmp]
community community1 {
    clients {
        10.209.152.33/32;
    }
    logical-system test-LS {
        routing-instance test-ri {
            clients {
                10.19.19.1/32;
            }
        }
    }
}
```

Ejemplo: Configuración de las opciones de interfaz para una instancia de enrutamiento

En este ejemplo se muestra una configuración de interfaz 802.3ad ae0 asignada a una instancia de enrutamiento denominada INFrtd:

```
[edit chassis]
aggregated-devices {
    ethernet {
        device-count 5;
    }
}
[edit interfaces ae0]
vlan-tagging;
aggregated-ether-options {
    minimum-links 2;
    link-speed 100m;
}
unit 0 {
    vlan-id 100;
```

```
    family inet {
        address 10.1.0.1/24;
    }
}
[edit interfaces fe-1/1/0]
fastether-options {
    802.3ad ae0;
}
[edit interfaces fe-1/1/1]
fastether-options {
    802.3ad ae0;
}
[edit routing-instances]
INFrtd {
    instance-type virtual-router;
    interface fe-1/1/0.0;
    interface fe-1/1/1.0;
    interface fe-1/1/5.0;
    interface ae0.0;
    protocols {
        ospf {
            area 0.0.0.0 {
                interface all;
            }
        }
    }
}
```

El siguiente comando muestra cómo recuperar información relacionada con SNMP del enrutador1 y la interfaz del paquete 802.3ae que pertenece a la instancia de enrutamiento INFrtd con la comunidad SNMP:`snmpwalkpublic`

```
router# snmpwalk -Os router1 INFrtd@public dot3adAggTable
dot3adAggMACAddress.59 = 0:90:69:92:93:f0
dot3adAggMACAddress.65 = 0:90:69:92:93:f0
dot3adAggActorSystemPriority.59 = 0
dot3adAggActorSystemPriority.65 = 0
dot3adAggActorSystemID.59 = 0:0:0:0:0:0
dot3adAggActorSystemID.65 = 0:0:0:0:0:0
dot3adAggAggregateOrIndividual.59 = true(1)
dot3adAggAggregateOrIndividual.65 = true(1)
dot3adAggActorAdminKey.59 = 0
```

```
dot3adAggActorAdminKey.65 = 0
dot3adAggActorOperKey.59 = 0
dot3adAggActorOperKey.65 = 0
dot3adAggPartnerSystemID.59 = 0:0:0:0:0:0
dot3adAggPartnerSystemID.65 = 0:0:0:0:0:0
dot3adAggPartnerSystemPriority.59 = 0
dot3adAggPartnerSystemPriority.65 = 0
dot3adAggPartnerOperKey.59 = 0
dot3adAggPartnerOperKey.65 = 0
dot3adAggCollectorMaxDelay.59 = 0
dot3adAggCollectorMaxDelay.65 = 0
```

Configuración de listas de acceso para el acceso SNMP a través de instancias de enrutamiento

Puede crear y mantener listas de acceso para administrar el acceso a la información SNMP. La configuración de la lista de acceso permite permitir o denegar el acceso SNMP a clientes de una instancia de enrutamiento específica y se aplica a las solicitudes de cualquier versión de SNMP.

En el ejemplo siguiente se muestra cómo crear una lista de acceso:

```
[edit snmp]
routing-instance-access {
    access-list {
        ri1 restrict;
        ls1/default;
        ls1/ri2;
        ls1*;
    }
}
```

La configuración dada en el ejemplo:

- Restringe el acceso de los clientes a la información SNMP.`ri1`
- Permite que los clientes de , , y todas las demás instancias de enrutamiento con nombres que comiencen por tengan acceso a la información de SNMP.`ls1/default``ls1/ri2``ls1`

Puede utilizar el carácter comodín (*) para representar una cadena en el nombre de la instancia de enrutamiento.

NOTA: No puede restringir el acceso al administrador SNMP de la instancia de enrutamiento predeterminada a la información SNMP.

Configurar operaciones remotas SNMP

in this section

- Descripción general de las operaciones remotas de SNMP | **450**
- Uso de Ping MIB para dispositivos de supervisión remota que ejecutan Junos OS | **454**
- Iniciar una prueba de ping | **455**
- Supervisar una prueba de ping en ejecución | **457**
- Recopilar resultados de pruebas de ping | **460**
- Detener una prueba de ping | **462**
- Interpretar variables de ping | **462**
- Uso de la MIB de Traceroute para dispositivos de supervisión remota que ejecutan Junos OS | **463**
- Iniciar una prueba de Traceroute | **464**
- Supervisión de una prueba de Traceroute en ejecución | **465**
- Supervisión de la finalización de la prueba de Traceroute | **469**
- Recopilar los resultados de las pruebas de Traceroute | **470**
- Detener una prueba de Traceroute | **472**
- Interpretar variables de traceroute | **472**

Descripción general de las operaciones remotas de SNMP

in this section

- Requisitos de operación remota de SNMP | **451**

- Establecer vistas SNMP | 451
- Establecer notificación de captura para operaciones remotas | 453
- Usar índices de cadena de longitud variable | 453
- Habilitar registro | 454

Una operación remota SNMP es cualquier proceso en el enrutador que se puede controlar de forma remota mediante SNMP. Actualmente, Junos OS es compatible con dos operaciones remotas SNMP: la MIB de ping y la MIB de Traceroute, definidas en RFC 2925. Con estas MIB, un cliente SNMP en el sistema de administración de red (NMS) puede:

- Iniciar una serie de operaciones en un enrutador
- Recibir una notificación cuando se hayan completado las operaciones
- Recopilar los resultados de cada operación

Junos OS también proporciona funcionalidad extendida a estas MIB en las extensiones específicas de la empresa de Juniper Networks y `.jnxPingMIBjnxTraceRouteMIB` Para obtener más información acerca de y , consulte PING MIB y Traceroute MIB.`jnxPingMIBjnxTraceRouteMIB`https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-ping.txthttps://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-traceroute.txt

En este tema se tratan las siguientes secciones:

Requisitos de operación remota de SNMP

Para utilizar operaciones remotas SNMP, debe tener experiencia con las convenciones SNMP. También debe configurar Junos OS para permitir el uso de las MIB de operación remota.

Antes de iniciar la MIB de ping, consulte Inicio de una prueba de ping."Iniciar una prueba de ping" en la página 455

Antes de iniciar la MIB de Traceroute, consulte Inicio de una prueba de Traceroute."Iniciar una prueba de Traceroute" en la página 464

Establecer vistas SNMP

Todas las MIB de operación remota compatibles con Junos OS requieren que los clientes SNMP tengan privilegios de lectura y escritura. La configuración SNMP predeterminada de Junos OS no proporciona a los clientes una cadena de comunidad con tales privilegios.

Para establecer privilegios de lectura y escritura para una cadena de comunidad SNMP, incluya las siguientes instrucciones en el nivel de jerarquía:`[edit snmp]`

```
[edit snmp]
community community-name {
    authorization authorization;
    view view-name;
}
view view-name {
    oid object-identifier (include | exclude);
}
```

Ejemplo: Establecer vistas SNMP

Para crear una comunidad denominada que conceda a los clientes SNMP acceso de lectura y escritura a Ping MIB, MIB, Traceroute MIB y MIB, incluya las siguientes instrucciones en el nivel de jerarquía:`remote-communityjnxPingjnxTraceRoute[edit snmp]`

```
snmp {
    view remote-view {
        oid 1.3.6.1.2.1.80 include; # pingMIB
        oid 1.3.6.1.4.1.2636.3.7 include; # jnxPingMIB
        oid 1.3.6.1.2.1.81 include; # traceRouteMIB
        oid 1.3.6.1.4.1.2636.3.8 include; # jnxTraceRouteMIB
    }
    community remote-community {
        view remote-view;
        authorization read-write;
    }
}
```

Para obtener más información acerca de la instrucción, vea y comunidad (SNMP).`community`Configurar comunidades SNMP*community (SNMP)*

Para obtener más información acerca de la instrucción, vea , view (Comunidad SNMP) y view (Configuración de una vista MIB).`view`Configurar vistas MIB*view (SNMP Community)view (Configuring a MIB View)*

Establecer notificación de captura para operaciones remotas

Además de configurar la MIB de operaciones remotas para la notificación de capturas, también debe configurar Junos OS. Debe especificar un host de destino para las capturas de operaciones remotas.

Para configurar la notificación de captura para operaciones remotas SNMP, incluya las instrucciones y en el nivel jerárquico :`categoriestargets`[`edit snmp trap-group` *`group-name`*]

```
[edit snmp trap-group group-name]
    categories {
        category;
    }
    targets {
        address;
    }
}
```

Ejemplo: Establecer notificación de captura para operaciones remotas

Especifique como host de destino para todas las capturas de operación remota:`172.17.12.213`

```
snmp {
    trap-group remote-traps {
        categories remote-operations;
        targets {
            172.17.12.213;
        }
    }
}
```

Para obtener más información acerca de los grupos de interrupción, consulte .Configuración de grupos de capturas SNMP

Usar índices de cadena de longitud variable

Todos los objetos tabulares de las MIB de operaciones remotas compatibles con Junos OS se indexan mediante dos variables de tipo .`SnmpAdminString` Para obtener más información acerca de , consulte RFC 2571.`SnmpAdminString`

Junos OS no se maneja de manera diferente al tipo de variable de cadena de octeto.`SnmpAdminString` Sin embargo, los índices se definen como longitud variable. Cuando se utiliza una cadena de longitud

variable como índice, la longitud de la cadena debe incluirse como parte del identificador de objeto (OID).

Ejemplo: Establecer índices de cadena de longitud variable

Para hacer referencia a la variable de una fila en donde es y es , utilice el siguiente identificador de objeto (OID):`pingCtlTargetAddresspingCtlTablepingCtlOwnerIndexbobpingCtlTestNametest`

```
pingMIB.pingObjects.pingCtlTable.pingCtlEntry.pingCtlTargetAddress."bob"."test"
1.3.6.1.2.1.80.1.2.1.4.3.98.111.98.4.116.101.115.116
```

Para obtener más información acerca de la definición de la MIB de ping, consulte RFC 2925.

Habilitar registro

El código de error SNMP devuelto en respuesta a las solicitudes SNMP sólo puede proporcionar una descripción genérica del problema. Las descripciones de errores registradas por el proceso de operaciones remotas a menudo pueden proporcionar información más detallada sobre el problema y ayudarle a resolverlo más rápido. Este registro no está habilitado de forma predeterminada. Para habilitar el registro, incluya la instrucción en el nivel de jerarquía:`flag general[edit snmp traceoptions]`

```
[edit]
snmp {
    traceoptions {
        flag general;
    }
}
```

Si el proceso de operaciones remotas recibe una solicitud SNMP que no puede acomodar, el error se registra en el archivo.`/var/log/rmopd` Para supervisar este archivo de registro, ejecute el comando en modo operativo de la interfaz de línea de comandos (CLI).`monitor start rmopd`

Uso de Ping MIB para dispositivos de supervisión remota que ejecutan Junos OS

Una prueba de ping se utiliza para determinar si los paquetes enviados desde el host local llegan al host designado y se devuelven. Si se puede contactar con el host designado, la prueba de ping proporciona el

tiempo aproximado de ida y vuelta para los paquetes. Los resultados de las pruebas de ping se almacenan en y .`pingResultsTablepingProbeHistoryTable`

RFC 2925 es la descripción autorizada de la MIB de ping en detalle y proporciona la definición de MIB ASN.1 de la MIB de ping.

Iniciar una prueba de ping

in this section

- Antes de empezar | 455
- Iniciar una prueba de ping | 455
- Usar múltiples PDU de conjunto | 456
- Usar una PDU de un solo conjunto | 456

Utilice este tema para iniciar una prueba de ping ICMP. Hay dos formas de iniciar una prueba de ping: utilizando varias unidades de datos de protocolo Set (PDU) o usando una sola PDU Set.

Antes de empezar

Antes de iniciar una prueba de ping, configure una vista Ping MIB. Esto permite solicitudes SNMP en .`SetpingMIB` Para obtener más información, consulte Configurar vistas MIB.

A partir de Junos OS versión 17.2X75-D100, debe configurar RPM antes de iniciar un ping ICMP. Configure RPM mediante el comando.`edit services rpm`

Iniciar una prueba de ping

Para iniciar una prueba de ping, cree una fila en y establezca en .`pingCtlTablepingCtlAdminStatusenabled` La información mínima que debe especificarse antes de establecer en es:`pingCtlAdminStatusenabled`

- `pingCtlOwnerIndexSnmpAdminString`
- `pingCtlTestNameSnmpAdminString`
- `pingCtlTargetAddressInetAddress`
- `pingCtlTargetAddressTypeInetAddressType`
- `pingCtlRowStatusRowStatus`

Para todos los demás valores, se eligen valores predeterminados a menos que se especifique lo contrario. y se utilizan como índice, por lo que sus valores se especifican como parte del identificador de objeto (OID).`pingCtlOwnerIndexpingCtlTestName` Para crear una fila, establezca en o sobre una fila que aún no existe.`pingCtlRowStatuscreateAndWaitcreateAndGo` Un valor de para indica que se ha proporcionado toda la información necesaria y que la prueba puede comenzar; se puede establecer en .`activepingCtlRowStatuspingCtlAdminStatusenabled` Una solicitud SNMP que se establece en fallará si la información necesaria en la fila no se especifica o es incoherente.`SetpingCtlRowStatusactive`

Para obtener información acerca de cómo configurar una vista, consulte Configuración de vistas SNMP."Supervisión de una prueba de Traceroute en ejecución" en la página 465

Lea las siguientes secciones para saber cómo ordenar las variables.

Usar múltiples PDU de conjunto

Puede utilizar PDU de varias solicitudes (varias PDU, con uno o más varbinds cada una) y establecer las siguientes variables en este orden para iniciar la prueba:`Set`

- `pingCtlRowStatus` Para `createAndWait`
- Todas las variables de prueba apropiadas
- `pingCtlRowStatus` Para `active`

  Junos OS ahora verifica que se haya especificado toda la información necesaria para ejecutar una prueba.
- `pingCtlAdminStatus` Para `enabled`

Usar una PDU de un solo conjunto

Puede usar una sola PDU de solicitud (una PDU, con varios varbinds) para establecer las siguientes variables para iniciar la prueba:`Set`

- `pingCtlRowStatus` Para `createAndGo`
- Todas las variables de prueba apropiadas
- `pingCtlAdminStatus` Para `enabled`

Supervisar una prueba de ping en ejecución

in this section

- pingResultsTable | 457
- pingProbeHistoryTable | 459
- Generar trampas | 460

Cuando se establece correctamente en , se realiza lo siguiente antes de que se envíe de vuelta al cliente el acuse de recibo de la solicitud SNMP :`pingCtlAdminStatusenabledSet`

- `pingResultsEntry` se crea si aún no existe.
- transiciones a .`pingResultsOperStatusenabled`

Para obtener más información, consulte las secciones siguientes:

pingResultsTable

Mientras se ejecuta la prueba, realiza un seguimiento del estado de la prueba.`pingResultsEntry` El valor de es mientras se ejecuta la prueba y cuando se ha detenido.`pingResultsOperStatusenableddisabled`

El valor de permanece hasta que lo establezca en .`pingCtlAdminStatusenableddisabled` Por lo tanto, para obtener el estado de la prueba, debe examinar .`pingResultsOperStatus`

La variable se puede utilizar para programar muchas pruebas para uno .`pingCtlFrequencypingCtlEntry` Después de que una prueba finaliza normalmente (no la detuvo) y ha transcurrido el número de segundos, la prueba se inicia de nuevo, como si hubiera establecido en .`pingCtlFrequencypingCtlAdminStatusenabled` Si interviene en cualquier momento entre pruebas repetidas (configurado en o en), la función de repetición se desactiva hasta que se inicie otra prueba y finalice normalmente.`pingCtlAdminStatusdisabledpingCtlRowStatusnotInService` Un valor de 0 para indica que esta característica de repetición no está activa.`pingCtlFrequency`

y se establecen en el valor de la dirección de destino resuelta cuando el valor de es .`pingResultsIpTgtAddrpingResultsIpTgtAddrTypepingCtlTargetAddressTypedns` Cuando una prueba se inicia correctamente y pasa a :`pingResultsOperStatusenabled`

- se establece en .`pingResultsIpTgtAddrnull-string`
- se establece en .`pingResultsIpTgtAddrTypeunknown`

y no se establecen hasta que se puedan resolver en una dirección numérica.`pingResultsIpTgtAddrpingResultsIpTgtAddrTypepingCtlTargetAddress` Para recuperar estos valores, busque cualquier valor que no sea después de establecer correctamente en .`pingResultsIpTgtAddrTypeunknownpingCtlAdminStatusenabled`

Al inicio de una prueba, se inicializa en 1 y se envía la primera sonda. aumenta en 1 cada vez que se envía una sonda. `pingResultsSentProbespingResultsSentProbes`

A medida que se ejecuta la prueba, cada segundo, ocurre lo siguiente:`pingCtlTimeOut`

- para el correspondiente en se establece en .`pingProbeHistoryStatuspingProbeHistoryEntrypingProbeHistoryTablerequestTimedOut`
- Se genera una trampa, si es necesario.`pingProbeFailed`
- Se intenta enviar la siguiente sonda.

> **NOTA**: No existe más de una sonda pendiente para cada prueba.

Para cada sonda, puede recibir uno de los siguientes resultados:

- El host de destino reconoce la sonda con una respuesta.
- Se agota el tiempo de espera de la sonda; No hay respuesta del host de destino reconociendo la sonda.
- No se pudo enviar la sonda.

Cada resultado de la sonda se registra en .`pingProbeHistoryTable` Para obtener más información acerca de , consulte .`pingProbeHistoryTable`"pingProbeHistoryTable" en la página 459

Cuando se recibe una respuesta del host de destino reconociendo la sonda actual:

- `pingResultsProbeResponses` aumenta en 1.
- Se actualizan las siguientes variables:
  - `pingResultsMinRtt`—Tiempo mínimo de ida y vuelta
  - `pingResultsMaxRtt`—Tiempo máximo de ida y vuelta
  - `pingResultsAverageRtt`—Tiempo promedio de ida y vuelta
  - `pingResultsRttSumOfSquares`—Suma de cuadrados de tiempos de ida y vuelta
  - `pingResultsLastGoodProbe`: marca de tiempo de la última respuesta

> **NOTA**: Solo los sondeos que dan como resultado una respuesta del host de destino contribuyen al cálculo de las variables de tiempo de ida y vuelta (RTT).

Cuando se recibe una respuesta a la última sonda o se agota el tiempo de espera de la última sonda, la prueba se completa.

pingProbeHistoryTable

Una entrada en () representa el resultado de una sonda y está indexada por tres variables:`pingProbeHistoryTablepingProbeHistoryEntry`

- Las dos primeras variables, y , son las mismas que se utilizan para , que identifica la prueba.`pingCtlOwnerIndexpingCtlTestNamepingCtlTable`
- La tercera variable, , es un contador para identificar de forma exclusiva cada resultado de la sonda.`pingProbeHistoryIndex`

El número máximo de entradas creadas para una prueba determinada está limitado por .`pingProbeHistoryTablepingCtlMaxRows` Si se establece en 0, no se crean entradas para esa prueba.`pingCtlMaxRowspingProbeHistoryTable`

Cada vez que se determina el resultado de un sondeo, se crea a y se agrega a . de los nuevos es 1 mayor que el último agregado a para esa prueba. se establece en 1 si esta es la primera entrada de la tabla. `pingProbeHistoryEntrypingProbeHistoryTablepingProbeHistoryIndexpingProbeHistoryEntrypingProbeHistoryEntrypingProbeHistoryTablepingProbeHistoryIndex` La misma prueba se puede ejecutar varias veces, por lo que este índice sigue creciendo.

Si del último agregado es 0xFFFFFFFF, el siguiente agregado se ha establecido en 1.`pingProbeHistoryIndexpingProbeHistoryEntrypingProbeHistoryEntrypingProbeHistoryIndex`

Se registra lo siguiente para el resultado de cada sonda:

- `pingProbeHistoryResponse`—Tiempo de vida (TTL)
- `pingProbeHistoryStatus`—Qué pasó y por qué
- `pingProbeHistoryLastRC`—Valor del código de retorno (RC) del paquete ICMP
- `pingProbeHistoryTime`—Marca de tiempo cuando se determinó el resultado de la sonda

Cuando no se puede enviar un sondeo, se establece en 0. Cuando se agota el tiempo de espera de una sonda, se establece en la diferencia entre el momento en que se descubrió que se agotó el tiempo de espera de la sonda y la hora en que se envió la sonda.`pingProbeHistoryResponsepingProbeHistoryResponse`

Generar trampas

Para que se genere cualquier trampa, se debe establecer el bit apropiado de .`pingCtlTrapGeneration` También debe configurar un grupo de capturas para recibir operaciones remotas. Se genera una captura en las siguientes condiciones:

- Se genera una captura cada vez que un número de sondas consecutivas fallan durante la prueba.`pingProbeFailedpingCtlTrapProbeFailureFilter`
- Se genera una interrupción cuando se completa la prueba y se produce un error en al menos un número de sondas.`pingTestFailedpingCtlTrapTestFailureFilter`
- Se genera una captura cuando se completa la prueba y fallan menos de sondas.`pingTestCompletedpingCtlTrapTestFailureFilter`

> **NOTA**: Una sonda se considera un fallo cuando el resultado de la sonda es algo más que .`pingProbeHistoryStatusresponseReceived`

Para obtener información acerca de cómo configurar un grupo de capturas para recibir operaciones remotas, consulte Configuración de grupos de capturas SNMP y ejemplo:" Configuración de la notificación de captura para operaciones remotas." en la página 465

Recopilar resultados de pruebas de ping

Puede sondear para averiguar cuándo se completó la prueba o solicitar que se envíe una trampa cuando se complete la prueba.`pingResultsOperStatus` Para obtener más información acerca de , vea pingResultsTable.`pingResultsOperStatus`"Supervisión de una prueba de Traceroute en ejecución" en la página 465 Para obtener más información acerca de las capturas Ping MIB, consulte Generación de capturas."Supervisión de una prueba de Traceroute en ejecución" en la página 465

Las estadísticas calculadas y luego almacenadas en incluyen:`pingResultsTable`

- `pingResultsMinRtt`—Tiempo mínimo de ida y vuelta
- `pingResultsMaxRtt`—Tiempo máximo de ida y vuelta
- `pingResultsAverageRtt`—Tiempo promedio de ida y vuelta
- `pingResultsProbeResponses`—Número de respuestas recibidas
- `pingResultsSentProbes`—Número de intentos de enviar sondeos
- `pingResultsRttSumOfSquares`—Suma de cuadrados de tiempos de ida y vuelta

- `pingResultsLastGoodProbe`: marca de tiempo de la última respuesta

También puede consultar para obtener información más detallada sobre cada sonda.`pingProbeHistoryTable` El índice utilizado para comienza en 1, pasa a 0xFFFFFFFF y vuelve a ser 1.`pingProbeHistoryTable`

Por ejemplo, si es 15 y es 5, al finalizar la primera ejecución de esta prueba, contiene sondas como las de .`pingCtlProbeCountpingCtlMaxRowspingProbeHistoryTable`Tabla 33 en la página 461

Tabla 33: Resultados en pingProbeHistoryTable: Después de la primera prueba de ping

pingProbeHistoryIndex	Resultado de la sonda
11	Resultado de la 11ª sonda de la ejecución 1
12	Resultado de la 12ª sonda de la ejecución 1
13	Resultado de la 13ª sonda de la carrera 1
14	Resultado de la 14ª sonda de la ejecución 1
15	Resultado de la 15ª sonda de la ejecución 1

Al finalizar la primera sonda de la segunda ejecución de esta prueba, contendrá sondas como las de .`pingProbeHistoryTable`Tabla 34 en la página 461

Tabla 34: Resultados en pingProbeHistoryTable: Después de la primera sonda de la segunda prueba

pingProbeHistoryIndex	Resultado de la sonda
12	Resultado de la 12ª sonda de la ejecución 1
13	Resultado de la 13ª sonda de la carrera 1
14	Resultado de la 14ª sonda de la ejecución 1
15	Resultado de la 15ª sonda de la ejecución 1
16	Resultado de la 1ª sonda de la ejecución 2

Al finalizar la segunda ejecución de esta prueba, contendrá sondas como las de .`pingProbeHistoryTable`Tabla 35 en la página 462

Tabla 35: Resultados en pingProbeHistoryTable: Después de la segunda prueba de ping

pingProbeHistoryIndex	Resultado de la sonda
26	Resultado de la 11ª sonda de la carrera 2
27	Resultado de la 12ª sonda de la carrera 2
28	Resultado de la 13ª sonda de la carrera 2
29	Resultado de la 14ª sonda de la carrera 2
30	Resultado de la 15ª sonda de la carrera 2

Las entradas del historial se pueden eliminar de la MIB de dos maneras:

- Se agregan más entradas de historial para una prueba determinada y el número de entradas de historial supera .`pingCtlMaxRows` Las entradas de historial más antiguas se eliminan para dejar espacio para las nuevas.
- Para eliminar toda la prueba, establezca en .`pingCtlRowStatusdestroy`

Detener una prueba de ping

Para detener una prueba activa, establezca en .`pingCtlAdminStatusdisabled` Para detener la prueba y quitar su , y cualquier objeto de la MIB, establezca en .`pingCtlEntrypingResultsEntrypingHistoryEntrypingCtlRowStatusdestroy`

Interpretar variables de ping

En esta sección se aclaran los intervalos de las siguientes variables que no se especifican explícitamente en la MIB de ping:

- `pingCtlDataSize`: el valor de esta variable representa el tamaño total de la carga útil (en bytes) de un paquete de sondeo saliente. Esta carga incluye la marca de tiempo (8 bytes) que se utiliza para cronometrar la sonda. Esto es coherente con la definición de (valor máximo de 65.507) y la aplicación de ping estándar.`pingCtlDataSize`

  Si el valor de está comprendido entre 0 y 8 inclusive, se omite y la carga es de 8 bytes (la marca de tiempo).`pingCtlDataSize` La MIB de ping asume que todos los sondeos están temporizados, por lo que la carga siempre debe incluir la marca de tiempo.

  Por ejemplo, si desea agregar 4 bytes adicionales de carga útil al paquete, debe establecer en 12.`pingCtlDataSize`

- `pingCtlDataFill`: los primeros 8 bytes del segmento de datos del paquete son para la marca de tiempo. Después de eso, el patrón se usa en repetición.`pingCtlDataFill` El patrón predeterminado (cuando no se especifica) es (00, 01, 02, 03 ...`pingCtlDataFill` FF, 00, 01, 02, 03 ... FF, ...).

- `pingCtlMaxRows`—El valor máximo es 255.

- `pingMaxConcurrentRequests`: el valor máximo es 500.

- y —Un valor de 0 para o no está bien definido por la MIB de ping.`pingCtlTrapProbeFailureFilterpingCtlTrapTestFailureFilterpingCtlTrapProbeFailureFilterpingCtlTrapTestFailureFilter` Si es 0, no se generarán trampas para la prueba bajo ninguna circunstancia.`pingCtlTrapProbeFailureFilterpingProbeFailed` Si es 0, no se generarán trampas para la prueba bajo ninguna circunstancia.`pingCtlTrapTestFailureFilterpingTestFailed`

Uso de la MIB de Traceroute para dispositivos de supervisión remota que ejecutan Junos OS

Una prueba de traceroute se aproxima a la ruta que los paquetes toman desde el host local al host remoto.

RFC 2925 es la descripción autorizada de la MIB de Traceroute en detalle y proporciona la definición de MIB ASN.1 de la MIB de Traceroute.

Iniciar una prueba de Traceroute

in this section

- Usar múltiples PDU de conjunto | **464**
- Usar una PDU de un solo conjunto | **465**

Antes de iniciar una prueba de traceroute, configure una vista MIB de Traceroute. Esto permite solicitudes SNMP en .`SettracerouteMIB` Para iniciar una prueba, cree una fila en y establézcala en .`traceRouteCtlTabletraceRouteCtlAdminStatusenabled` Debe especificar al menos lo siguiente antes de establecer en :`traceRouteCtlAdminStatusenabled`

- `traceRouteCtlOwnerIndexSnmpAdminString`
- `traceRouteCtlTestNameSnmpAdminString`
- `traceRouteCtlTargetAddressInetAddress`
- `traceRouteCtlRowStatusRowStatus`

Para todos los demás valores, se eligen valores predeterminados a menos que se especifique lo contrario. y se utilizan como índice, por lo que sus valores se especifican como parte del OID.`traceRouteCtlOwnerIndextraceRouteCtlTestName` Para crear una fila, establezca en o sobre una fila que aún no existe.`traceRouteCtlRowStatuscreateAndWaitcreateAndGo` Un valor de para indica que se ha especificado toda la información necesaria y que la prueba puede comenzar; se puede establecer en .`activetraceRouteCtlRowStatustraceRouteCtlAdminStatusenabled` Una solicitud SNMP que se establece en fallará si la información necesaria en la fila no se especifica o es incoherente.`SettraceRouteCtlRowStatusactive` Para obtener información acerca de cómo configurar una vista, consulte Configuración de vistas SNMP."Supervisión de una prueba de Traceroute en ejecución" en la página 465

Hay dos formas de iniciar una prueba de traceroute:

Usar múltiples PDU de conjunto

Puede utilizar PDU de varias solicitudes (varias PDU, con uno o más varbinds cada una) y establecer las siguientes variables en este orden para iniciar la prueba:`Set`

- `traceRouteCtlRowStatus` para crearAndWait
- Todas las variables de prueba apropiadas
- `traceRouteCtlRowStatus` Para `active`

Junos OS ahora verifica que se haya especificado toda la información necesaria para ejecutar una prueba.

- `traceRouteCtlAdminStatus` Para `enabled`

Usar una PDU de un solo conjunto

Puede usar una sola PDU de solicitud (una PDU, con varios varbinds) para establecer las siguientes variables para iniciar la prueba:`Set`

- `traceRouteCtlRowStatus` Para `createAndGo`
- Todas las variables de prueba apropiadas
- `traceRouteCtlAdminStatus` a habilitado

Supervisión de una prueba de Traceroute en ejecución

in this section

- traceRouteResultsTable | 465
- traceRouteProbeResultsTable | 466
- traceRouteHopsTable | 468
- Generar trampas | 469

Cuando traceRouteCtlAdminStatus se establece correctamente en habilitado, se hace lo siguiente antes de que se envíe de vuelta al cliente la confirmación de la solicitud SNMP Set:

- traceRouteResultsEntry se crea si aún no existe.
- traceRouteResultsOperStatus pasa a habilitado.

Para obtener más información, consulte las secciones siguientes:

traceRouteResultsTable

Mientras se ejecuta la prueba, traceRouteResultsTable realiza un seguimiento del estado de la prueba. El valor de traceRouteResultsOperStatus se habilita mientras se ejecuta la prueba y se deshabilita cuando se ha detenido.

El valor de traceRouteCtlAdminStatus permanece habilitado hasta que lo establezca en deshabilitado. Por lo tanto, para obtener el estado de la prueba, debe examinar traceRouteResultsOperStatus.

La variable traceRouteCtlFrequency se puede utilizar para programar muchas pruebas para un traceRouteCtlEntry. Después de que una prueba finaliza normalmente (no la detuvo) y ha transcurrido el número de segundos de traceRouteCtlFrequency, la prueba se inicia de nuevo, como si hubiera establecido traceRouteCtlAdminStatus en habilitado. Si interviene en cualquier momento entre pruebas repetidas (establece traceRouteCtlAdminStatus en disabled o traceRouteCtlRowStatus en notInService), la función de repetición se deshabilita hasta que se inicie otra prueba y finalice normalmente. Un valor de 0 para traceRouteCtlFrequency indica que esta característica de repetición no está activa.

traceRouteResultsIpTgtAddr y traceRouteResultsIpTgtAddrType se establecen en el valor de la dirección de destino resuelta cuando el valor de traceRouteCtlTargetAddressType es dns. Cuando una prueba se inicia correctamente y traceRouteResultsOperStatus cambia a habilitado:

- traceRouteResultsIpTgtAddr se establece en null-string.
- traceRouteResultsIpTgtAddrType se establece en desconocido.

traceRouteResultsIpTgtAddr y traceRouteResultsIpTgtAddrType no se establecen hasta que traceRouteCtlTargetAddress se pueda resolver en una dirección numérica. Para recuperar estos valores, sondee traceRouteResultsIpTgtAddrType para cualquier valor que no sea desconocido después de establecer correctamente traceRouteCtlAdminStatus en habilitado.

Al inicio de una prueba, traceRouteResultsCurHopCount se inicializa en traceRouteCtlInitialTtl, y traceRouteResultsCurProbeCount se inicializa en 1. Cada vez que se determina el resultado de un sondeo, traceRouteResultsCurProbeCount aumenta en 1. Mientras se ejecuta la prueba, el valor de traceRouteResultsCurProbeCount refleja el sondeo pendiente actual para el que aún no se han determinado los resultados.

El número de sondeos traceRouteCtlProbesPerHop se envía para cada valor de tiempo de vida (TTL). Cuando se determina el resultado del último sondeo para el salto actual, siempre que el salto actual no sea el salto de destino, traceRouteResultsCurHopCount aumenta en 1 y traceRouteResultsCurProbeCount se restablece en 1.

Al inicio de una prueba, si es la primera vez que se ejecuta esta prueba para este traceRouteCtlEntry, traceRouteResultsTestAttempts y traceRouteResultsTestSuccesses se inicializan en 0.

Al final de cada ejecución de prueba, traceRouteResultsOperStatus pasa a deshabilitado y traceRouteResultsTestAttempts aumenta en 1. Si la prueba logró determinar correctamente la ruta completa al destino, traceRouteResultsTestSuccesses aumenta en 1 y traceRouteResultsLastGoodPath se establece en la hora actual.

traceRouteProbeResultsTable

Cada entrada de traceRouteProbeHistoryTable está indexada por cinco variables:

- Las dos primeras variables, traceRouteCtlOwnerIndex y traceRouteCtlTestName, son las mismas que se utilizan para traceRouteCtlTable y para identificar la prueba.
- La tercera variable, traceRouteProbeHistoryIndex, es un contador que comienza desde 1 y se ajusta en FFFFFFFF. El número máximo de entradas está limitado por traceRouteCtlMaxRows.
- La cuarta variable, traceRouteProbeHistoryHopIndex, indica para qué salto es este sondeo (el valor de tiempo de vida real o TTL). Por lo tanto, el primer número traceRouteCtlProbesPerHop de entradas creadas cuando se inicia una prueba tiene el valor traceRouteCtlInitialTtl para traceRouteProbeHistoryHopIndex.
- La quinta variable, traceRouteProbeHistoryProbeIndex, es la sonda para el salto actual. Va desde 1 hasta traceRouteCtlProbesPerHop.

Mientras se ejecuta una prueba, tan pronto como se determina el resultado de una sonda, se envía la siguiente sonda. Transcurre un máximo de segundos traceRouteCtlTimeOut antes de que un sondeo se marque con status requestTimedOut y se envíe el siguiente sondeo. Nunca hay más de una sonda pendiente por prueba de traceroute. Cualquier resultado de la sonda que regrese después de que se agote el tiempo de espera de una sonda se ignora.

Cada sonda puede:

- Resultado en una respuesta de un host que reconoce la sonda
- Tiempo de espera sin respuesta de un host que reconozca la sonda
- Error al ser enviado

Cada estado de sonda se registra en traceRouteProbeHistoryTable con traceRouteProbeHistoryStatus establecido en consecuencia.

Los sondeos que dan como resultado una respuesta de un host registran los siguientes datos:

- traceRouteProbeHistoryResponse: tiempo de ida y vuelta (RTT)
- traceRouteProbeHistoryHAddrType: el tipo de HAddr (siguiente argumento)
- traceRouteProbeHistoryHAddr: la dirección del salto

Todas las sondas, independientemente de si se recibe una respuesta para la sonda, tienen registrado lo siguiente:

- traceRouteProbeHistoryStatus: qué ha ocurrido y por qué
- traceRouteProbeHistoryLastRC: valor de código de retorno (RC) del paquete ICMP
- traceRouteProbeHistoryTime: marca de tiempo cuando se determinó el resultado del sondeo

Cuando no se puede enviar una sonda, traceRouteProbeHistoryResponse se establece en 0. Cuando se agota el tiempo de espera de una sonda, traceRouteProbeHistoryResponse se establece en la diferencia entre la hora en que se descubrió que se agotó el tiempo de espera de la sonda y la hora en que se envió la sonda.

traceRouteHopsTable

Las entradas de traceRouteHopsTable están indexadas por tres variables:

- Los dos primeros, traceRouteCtlOwnerIndex y traceRouteCtlTestName, son los mismos que se usan para traceRouteCtlTable e identifican la prueba.
- La tercera variable, traceRouteHopsHopIndex, indica el salto actual, que comienza en 1 (no traceRouteCtlInitialTtl).

Cuando se inicia una prueba, se eliminan todas las entradas de traceRouteHopsTable con traceRouteCtlOwnerIndex y traceRouteCtlTestName dados. Las entradas de esta tabla sólo se crean si traceRouteCtlCreateHopsEntries se establece en true.

Se crea un nuevo traceRouteHopsEntry cada vez que se determina el primer resultado del sondeo para un TTL determinado. La nueva entrada se crea independientemente de que la primera sonda llegue o no a un host. El valor de traceRouteHopsHopIndex se incrementa en 1 para esta nueva entrada.

> **NOTA**: Cualquier traceRouteHopsEntry puede carecer de un valor para traceRouteHopsIpTgtAddress si no hay respuestas a los sondeos con el TTL dado.

Cada vez que un sondeo llega a un host, la dirección IP de ese host está disponible en el resultado del sondeo. Si no se establece el valor de traceRouteHopsIpTgtAddress de la traceRouteHopsEntry actual, el valor de traceRouteHopsIpTgtAddress se establece en esta dirección IP. Si el valor de traceRouteHopsIpTgtAddress de la traceRouteHopsEntry actual es el mismo que la dirección IP, el valor no cambia. Si el valor de traceRouteHopsIpTgtAddress de la traceRouteHopsEntry actual es diferente de esta dirección IP, lo que indica un cambio de ruta, se crea una nueva traceRouteHopsEntry con:

- Variable traceRouteHopsHopHopIndex aumentada en 1
- traceRouteHopsIpTgtAddress establecido en la dirección IP

> **NOTA**: Se agrega una nueva entrada para una prueba a traceRouteHopsTable cada vez que se usa un nuevo valor TTL o cambia la ruta. Por lo tanto, el número de entradas para una prueba puede exceder el número de valores TTL diferentes utilizados.

Cuando se determina el resultado de un sondeo, el valor traceRouteHopsSentProbes del traceRouteHopsEntry actual aumenta en 1. Cuando se determina el resultado de un sondeo y el sondeo llega a un host:

- El valor traceRouteHopsProbeResponses del traceRouteHopsEntry actual se incrementa en 1.
- Se actualizan las siguientes variables:
  - traceRouteResultsMinRtt: tiempo mínimo de ida y vuelta
  - traceRouteResultsMaxRtt: tiempo máximo de ida y vuelta
  - traceRouteResultsAverageRtt: tiempo promedio de ida y vuelta
  - traceRouteResultsRttSumOfSquares: suma de cuadrados de tiempos de ida y vuelta
  - traceRouteResultsLastGoodProbe: marca de tiempo de la última respuesta

> **NOTA**: Sólo los sondeos que llegan a un host afectan a los valores de tiempo de ida y vuelta.

Generar trampas

Para generar cualquier captura, se debe establecer un bit apropiado de traceRouteCtlTrapGeneration. También debe configurar un grupo de capturas para recibir operaciones remotas. Las capturas se generan en las siguientes condiciones:

- traceRouteHopsIpTgtLa dirección de la sonda actual es diferente de la última sonda con el mismo valor TTL (traceRoutePathChange).
- No se pudo determinar una ruta de acceso al destino (traceRouteTestFailed).

Se determinó una ruta de acceso al destino (traceRouteTestCompleted).

Para obtener información acerca de cómo configurar un grupo de capturas para recibir operaciones remotas, consulte *Configuración de grupos de capturas* SNMP y "Descripción general de las operaciones remotas SNMP" en la página 450.

Supervisión de la finalización de la prueba de Traceroute

Cuando se completa una prueba, se pasa de a `.traceRouteResultsOperStatusenableddisabled` Esta transición se produce en las siguientes situaciones:

- La prueba finaliza correctamente. El resultado de un sondeo indica que se ha llegado al destino. En este caso, el salto actual es el último salto. Se envían el resto de las sondas para este salto. Cuando se determina el último resultado de la sonda para el salto actual, finaliza la prueba.
- `traceRouteCtlMaxTtl` se ha superado el umbral. Nunca se llega al destino. La prueba finaliza después de que se haya enviado el número de sondas con un valor TTL igual .`traceRouteCtlMaxttl`
- `traceRouteCtlMaxFailures` se ha superado el umbral. El número de sondeos consecutivos que terminan con estado supera .`requestTimedOuttraceRouteCtlMaxFailures`
- Finaliza la prueba. Para establecer o eliminar la fila, establezca en .`traceRouteCtlAdminStatusdisabledtraceRouteCtlRowStatusdestroy`
- Configuró mal la prueba traceroute. Un valor o variable especificado en es incorrecto y no permitirá que se envíe ni un solo sondeo.`traceRouteCtlTable` Debido a la naturaleza de los datos, este error no se pudo determinar hasta que se inició la prueba; es decir, hasta después de la transición a .`traceRouteResultsOperStatusenabled` Cuando esto ocurre, se agrega una entrada a con establecido en el código de error apropiado.`traceRouteProbeHistoryTabletraceRouteProbeHistoryStatus`

Si se establece correctamente, se genera la captura o .`traceRouteCtlTrapGenerationtraceRouteTestFailedtraceRouteTestCompleted`

Recopilar los resultados de las pruebas de Traceroute

Puede sondear traceRouteResultsOperStatus para averiguar cuándo se ha completado la prueba o solicitar que se envíe una captura cuando se complete la prueba. Para obtener más información acerca de traceResultsOperStatus, vea "traceRouteResultsTable" en la página 465. Para obtener más información acerca de las capturas MIB de Traceroute, consulte la sección Generación de capturas en Supervisión de una prueba de Traceroute en ejecución."Supervisión de una prueba de Traceroute en ejecución" en la página 465

Las estadísticas se calculan por salto y, a continuación, se almacenan en traceRouteHopsTable. Incluyen lo siguiente para cada salto:

- traceRouteHopsIpTgtAddressType: tipo de dirección del host en este salto
- traceRouteHopsIpTgtAddress: dirección del host en este salto
- traceRouteHopsMinRtt: tiempo mínimo de ida y vuelta
- traceRouteHopsMaxRtt: tiempo máximo de ida y vuelta
- traceRouteHopsAverageRtt: tiempo promedio de ida y vuelta
- traceRouteHopsRttSumOfSquares: suma de cuadrados de tiempos de ida y vuelta

- traceRouteHopsSentProbes: número de intentos de enviar sondeos
- traceRouteHopsProbeResponses: número de respuestas recibidas
- traceRouteHopsLastGoodProbe: marca de tiempo de la última respuesta

También puede consultar traceRouteProbeHistoryTable para obtener información más detallada sobre cada sonda. El índice utilizado para traceRouteProbeHistoryTable comienza en 1, va a 0xFFFFFFFF y vuelve a ajustarse a 1.

Por ejemplo, suponga lo siguiente:

- traceRouteCtlMaxRows es 10.
- traceRouteCtlProbesPerHop es 5.
- Hay ocho saltos al objetivo (el objetivo es el número ocho).
- Cada sondeo enviado da como resultado una respuesta de un host (el número de sondeos enviados no está limitado por traceRouteCtlMaxFailures).

En esta prueba, se envían 40 sondas. Al final de la prueba, traceRouteProbeHistoryTable tendría un historial de sondeos como los de Tabla 36 en la página 471.

Tabla 36: traceRouteProbeHistoryTable

HistoryIndex	HistoryHopIndex	HistoryProbeIndex
31	7	1
32	7	2
33	7	3
34	7	4
35	7	5
36	8	1
37	8	2

Tabla 36: traceRouteProbeHistoryTable *(Continued)*

HistoryIndex	HistoryHopIndex	HistoryProbeIndex
38	8	3
39	8	4
40	8	5

Detener una prueba de Traceroute

Para detener una prueba activa, establezca en .`traceRouteCtlAdminStatusdisabled` Para detener una prueba y quitar sus , , y objetos de la MIB, establezca en .`traceRouteCtlEntrytraceRouteResultsEntrytraceRouteProbeHistoryEntrytraceRouteProbeHistoryEntrytraceRouteCtlRowStatusdestroy`

Interpretar variables de traceroute

Este tema contiene información sobre los intervalos de las siguientes variables que no se especifican explícitamente en la MIB de Traceroute:

- —El valor máximo para es 2550.`traceRouteCtlMaxRowstraceRouteCtlMaxRows` Esto representa el TTL máximo (255) multiplicado por el máximo para (10).`traceRouteCtlProbesPerHop` Por lo tanto, el acomoda una prueba completa en los valores máximos para uno .`traceRouteProbeHistoryTabletraceRouteCtlEntry` Por lo general, los valores máximos no se utilizan y el es capaz de acomodar el historial completo para muchas pruebas para el mismo .`traceRouteProbeHistoryTabletraceRouteCtlEntry`
- `traceRouteMaxConcurrentRequests`: el valor máximo es 50. Si una prueba se está ejecutando, tiene una sonda pendiente. Representa el número máximo de pruebas de traceroute que tiene con un valor de .`traceRouteMaxConcurrentRequeststraceRouteResultsOperStatusenabled` Cualquier intento de iniciar una prueba con pruebas en ejecución dará como resultado la creación de una sonda con establecido en y esa prueba finalizará inmediatamente.`traceRouteMaxConcurrentRequeststraceRouteProbeHistoryStatusmaxConcurrentLimitReached`

- `traceRouteCtlTable`—El número máximo de entradas permitidas en esta tabla es 100. Cualquier intento de crear una entrada 101 dará como resultado un mensaje para SNMPv1 y un mensaje para SNMPv2.`BAD_VALUERESOURCE_UNAVAILABLE`

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.2X75-D100	A partir de Junos OS versión 17.2X75-D100, debe configurar RPM antes de iniciar un ping ICMP.

Capturas SNMP

in this section

- Configurar capturas SNMP | **473**
- Configurar opciones de captura SNMP | **475**
- Configuración de grupos de capturas SNMP | **480**
- Configurar opciones y grupos de capturas SNMP en un dispositivo que ejecute Junos OS | **483**
- Ejemplo: Configuración de grupos de capturas SNMP | **484**
- Administrar trampas | **484**

Configurar capturas SNMP

Las capturas son mensajes no solicitados enviados desde un agente SNMP a sistemas de administración de red remotos o receptores de capturas. Las empresas utilizan trampas SNMP como parte de una solución de monitoreo de fallas, además del registro del sistema. En Junos OS, debe configurar un grupo de capturas si desea utilizar capturas SNMP.

Puede crear y asignar un nombre a un grupo de uno o más tipos de capturas SNMP y definir qué sistemas reciben el grupo de capturas SNMP. El nombre del grupo de capturas está incrustado en los

paquetes de notificación de captura SNMP como un enlace de variable (varbind) conocido como nombre de comunidad.

Para configurar una captura SNMP:

1. Cree una dirección de origen única y coherente que Junos OS aplique a todas las capturas salientes del dispositivo.

   Una dirección de origen es útil, ya que aunque la mayoría de los dispositivos Junos OS tienen varias interfaces salientes, el uso de una dirección de origen ayuda a un NMS remoto a asociar el origen de las capturas con un dispositivo individual

```
[edit groups global snmp]
user@host# set trap-options source-address address
```

   En este ejemplo se utiliza la dirección IP de la interfaz de circuito cerrado (lo0) como dirección de origen para todas las capturas SNMP que se originan en el dispositivo.

```
[edit groups global snmp]
user@host# set trap-options source-address lo0
```

2. Cree un grupo de capturas en el que pueda enumerar los tipos de capturas que se van a reenviar y los destinos (direcciones) de los sistemas de gestión remota receptores.

```
[edit groups global snmp trap-group group-name]
user@host# set version (all | v1 | v2) targets address
```

   En este ejemplo se crea un grupo de capturas denominado , permite enviar notificaciones con formato SNMP versión 2 (capturas) al host en la dirección 192.168.1.15.`managers` Esta declaración remite todas las categorías de trampas.

```
[edit groups global snmp trap-group managers]
user@host# set version v2 targets 192.168.1.15
```

3. Defina el subconjunto específico de categorías de capturas que se reenviarán.

   Para obtener una lista de categorías, consulte .Configuración de grupos de capturas SNMP

```
[edit groups global snmp trap-group group-name]
user@host# set categories category
```

La siguiente instrucción configura los errores de autenticación MIB-II estándar en el agente (el dispositivo).

```
[edit groups global snmp trap-group managers]
user@host# set categories authentication
```

4. En el nivel superior de la configuración, aplique el grupo de configuración.

   Si utiliza un grupo de configuración, debe aplicarlo para que surta efecto.

```
[edit]
user@host# set apply-groups global
```

5. Confirme la configuración.

```
user@host# commit
```

6. Para comprobar la configuración, genere una captura de error de autenticación.

   Esto significa que el agente SNMP recibió una solicitud con una comunidad desconocida. Otros tipos de trampas también pueden ser falsificados.

   Esta función le permite activar capturas SNMP desde enrutadores y asegurarse de que se procesan correctamente dentro de su infraestructura de administración de red existente. Esto también es útil para probar y depurar el comportamiento SNMP en el conmutador o NMS.

   Con el comando, puede comprobar que la captura se envía al sistema de administración de red.`monitor traffic`

```
user@host> request snmp spoof-trap authenticationFailure
Spoof-trap request result: trap sent successfully
```

Configurar opciones de captura SNMP

in this section

Configuración de la dirección de origen para capturas SNMP | **476**

Configuración de la dirección del agente para capturas SNMP | 479
Agregar identificador de objeto snmpTrapEnterprise a capturas SNMP estándar | 480

Mediante las opciones de captura SNMP, puede establecer la dirección de origen de cada paquete de captura SNMP enviado por el enrutador en una sola dirección, independientemente de la interfaz de salida. Además, puede establecer la dirección del agente de las capturas SNMPv1. Para obtener más información acerca del contenido de las capturas SNMPv1, consulte RFC 1157.

NOTA: Puede asociar SNMP solo con la instancia de enrutamiento maestra.

Para configurar las opciones de captura SNMP, consulte *trap-options*.

También debe configurar un grupo de capturas para que las opciones de captura surtan efecto. Para obtener información acerca de los grupos de interrupción, consulte .Configuración de grupos de capturas SNMP

Este tema contiene las siguientes secciones:

Configuración de la dirección de origen para capturas SNMP

Puede configurar la dirección de origen de los paquetes de captura de varias maneras: lo0, una dirección IPv4 válida o una dirección IPv6 configurada en una de las interfaces del enrutador, una dirección del sistema lógico o la dirección de una instancia de enrutamiento. El valor lo0 indica que la dirección de origen de los paquetes de captura SNMP está establecida en la dirección de circuito cerrado más baja configurada en la interfaz lo0.

NOTA: Puede generar capturas SNMP sólo si la dirección de origen es una dirección IPv4 o IPv6 válida o si está configurada.

Puede configurar la dirección de origen de los paquetes de captura en uno de los formatos siguientes:

- Una dirección IPv4 válida configurada en una de las interfaces del enrutador
- Una dirección IPv6 válida configurada en una de las interfaces del enrutador
- `lo0`; es decir, la dirección de circuito cerrado más baja configurada en la interfaz lo0
- Un nombre de sistema lógico

- Un nombre de instancia de enrutamiento

Una dirección IPv4 válida como dirección de origen

Para especificar una dirección de interfaz IPv4 válida como dirección de origen para las capturas SNMP en una de las interfaces del enrutador, incluya la instrucción en el nivel de jerarquía:`source-address[edit snmp trap-options]`

```
[edit snmp trap-options]
source-address address;
```

address es una dirección IPv4 válida configurada en una de las interfaces del enrutador.

Una dirección IPv6 válida como dirección de origen

Para especificar una dirección de interfaz IPv6 válida como dirección de origen para las capturas SNMP en una de las interfaces del enrutador, incluya la instrucción en el nivel de jerarquía:`source-address[edit snmp trap-options]`

```
[edit snmp trap-options]
source-address address;
```

address es una dirección IPv6 válida configurada en una de las interfaces del enrutador.

La dirección de circuito cerrado más baja como dirección de origen

Para especificar la dirección de origen de las capturas SNMP de modo que utilicen la dirección de circuito cerrado más baja configurada en la interfaz lo0 como dirección de origen, incluya la instrucción en el nivel de jerarquía:`source-address[edit snmp trap-options]`

```
[edit snmp trap-options]
source-address lo0;
```

Para habilitar y configurar la dirección de circuito cerrado, incluya la instrucción en el nivel de jerarquía:`address[edit interfaces lo0 unit 0 family inet]`

```
[edit interfaces]
lo0 {
    unit 0 {
        family inet {
            address ip-address;
        }
```

```
    }
}
```

Para configurar la dirección de circuito cerrado como dirección de origen de los paquetes de captura:

```
[edit snmp]
trap-options {
    source-address lo0;
}
trap-group "urgent-dispatcher" {
    version v2;
    categories link startup;
    targets {
        192.168.10.22;
        172.17.1.2;
    }
}
[edit interfaces]
lo0 {
    unit 0 {
        family inet {
            address 10.0.0.1/32;
            address 127.0.0.1/32;
        }
    }
}
```

En este ejemplo, la dirección IP 10.0.0.1 es la dirección de origen de cada captura enviada desde este enrutador.

Nombre del sistema lógico como dirección de origen

Para especificar un nombre de sistema lógico como dirección de origen de las capturas SNMP, incluya la instrucción en el nivel de jerarquía.`logical-system` *`logical-system-name`*`[edit snmp trap-options]`

Por ejemplo, la siguiente configuración establece el nombre lógico del sistema como la dirección de origen de las capturas SNMP:`ls1`

```
[edit snmp]
    trap-options{
    logical-system ls1;
}
```

Nombre de instancia de enrutamiento como dirección de origen

Para especificar un nombre de instancia de enrutamiento como dirección de origen de las capturas SNMP, incluya la instrucción en el nivel de jerarquía.`routing-instance` *`routing-instance-name`*`[edit snmp trap-options]`

Por ejemplo, la siguiente configuración establece el nombre de la instancia de enrutamiento como dirección de origen para las capturas SNMP:`ri1`

```
[edit snmp]
    trap-options {
    routing-instance ri1;
}
```

Configuración de la dirección del agente para capturas SNMP

La dirección del agente solo está disponible en paquetes de captura SNMPv1 (consulte RFC 1157). De forma predeterminada, la dirección local predeterminada del enrutador no se especifica en el campo dirección del agente de la captura SNMPv1. Para configurar la dirección del agente, incluya la instrucción en el nivel de jerarquía.`agent-address[edit snmp trap-options]` Actualmente, la dirección del agente solo puede ser la dirección de la interfaz de salida:

```
[edit snmp]
trap-options {
    agent-address outgoing-interface;
}
```

Para configurar la interfaz de salida como la dirección del agente:

```
[edit snmp]
trap-options {
    agent-address outgoing-interface;
}
trap-group “ urgent-dispatcher” {
    version v1;
    categories link startup;
    targets {
        192.168.10.22;
        172.17.1.2;
    }
}
```

En este ejemplo, cada paquete de captura SNMPv1 enviado tiene su valor de dirección de agente establecido en la dirección IP de la interfaz de salida.

Agregar identificador de objeto snmpTrapEnterprise a capturas SNMP estándar

El objeto snmpTrapEnterprise ayuda a identificar la empresa que ha definido la interrupción. Normalmente, el objeto snmpTrapEnterprise aparece como el último varbind en las capturas SNMP versión 2 específicas de la empresa. Sin embargo, a partir de la versión 10.0, Junos OS permite agregar también el identificador de objeto snmpTrapEnterprise a las capturas SNMP estándar.

Para agregar snmpTrapEnterprise a capturas estándar, incluya la instrucción en el nivel de jerarquía.`enterprise-oid`[`edit snmp trap-options`] Si la instrucción no se incluye en la configuración, snmpTrapEnterprise se agrega sólo para capturas específicas de la empresa.`enterprise-oid`

```
[edit snmp]
trap-options {
    enterprise-oid;
}
```

Configuración de grupos de capturas SNMP

Puede crear y asignar un nombre a un grupo de uno o más tipos de capturas SNMP y, a continuación, definir qué sistemas reciben el grupo de capturas SNMP. Debe configurar el grupo de capturas para enviar las capturas SNMP. Para crear un grupo de capturas SNMP, consulte *trap-group*.

Para cada grupo de capturas que defina, debe incluir la instrucción para definir al menos un sistema como destinatario de las capturas SNMP en el grupo de capturas.`target` Especifique la dirección IPv4 o IPv6 de cada destinatario, no su nombre de host.

Especifique los tipos de interrupciones que el grupo de capturas puede recibir en la instrucción.`categories` Para obtener información sobre la categoría a la que pertenecen las capturas, consulte los temas y Capturas SNMP específicas de la empresa compatibles con Junos OS .Capturas SNMP estándar compatibles con Junos OShttps://www.juniper.net/documentation/en_US/junos/topics/concept/enterprise-specific-traps-overview.html

Especifique la instancia de enrutamiento utilizada por el grupo de capturas en la instrucción.`routing-instance` Todos los destinos configurados en el grupo de capturas utilizan esta instancia de enrutamiento.

Un grupo de captura puede recibir las siguientes categorías:

- `authentication`—Errores de autenticación

- `chassis`—Notificaciones de chasis o entorno
- `chassis-cluster`—Notificaciones de agrupación
- `configuration`—Notificaciones de configuración
- `link`—Notificaciones relacionadas con el vínculo (transiciones ascendentes y descendentes, cambio de estado de las líneas DS-3 y DS-1, cambio de estado de la interfaz IPv6 y sobrecarga de PIC de monitoreo pasivo)

  NOTA: Para enviar capturas de interfaz de sobrecarga de PIC de supervisión pasiva, seleccione la categoría de interrupción.`link`

- `otn-alarms`—Subcategorías de trampas de alarma OTN
- `remote-operations`—Notificaciones de operación remota
- `rmon-alarm`—Alarma para eventos RMON
- `routing`—Notificaciones de protocolo de enrutamiento
- `services`—Notificaciones de servicios, como circuito apagado o arriba, conexión abajo o arriba, CPU superada, alarmas y cambios de estado.
- `sonet-alarms`—Alarmas SONET/SDH

  NOTA: Si omite las subcategorías SONET/SDH, todos los tipos de alarma de captura SONET/SDH se incluyen en las notificaciones de captura.

  - `loss-of-light`—Notificación de alarma de pérdida de luz
  - `pll-lock`—Notificación de alarma de bloqueo PLL
  - `loss-of-frame`—Notificación de pérdida de alarma de trama
  - `loss-of-signal`—Notificación de pérdida de señal de alarma
  - `severely-errored-frame`—Notificación de alarma de trama con errores graves
  - `line-ais`—Notificación de alarma de señal de indicación de alarma de línea (AIS)
  - `path-ais`—Notificación de alarma AIS de ruta
  - `loss-of-pointer`—Notificación de pérdida de alarma de puntero

  - `ber-defect`—Notificación de defecto de alarma de velocidad de errores de bits SONET/SDH
  - `ber-fault`—Notificación de fallo de alarma de velocidad de error SONET/SDH
  - `line-remote-defect-indication`—Notificación de alarma de indicación de defecto remota de línea
  - `path-remote-defect-indication`—Notificación de alarma de indicación de defecto remota de ruta
  - `remote-error-indication`—Notificación de alarma de indicación de error remoto
  - `unequipped`—Notificación de alarma no equipada
  - `path-mismatch`—Notificación de alarma de discrepancia de ruta
  - `loss-of-cell`—Notificación de alarma de pérdida de delineación celular
  - `vt-ais`—Notificación de alarma AIS tributaria virtual (VT)
  - `vt-loss-of-pointer`—VT pérdida de notificación de alarma de puntero
  - `vt-remote-defect-indication`—Notificación de alarma de indicación remota de defectos de VT
  - `vt-unequipped`—Notificación de alarma VT no equipada
  - `vt-label-mismatch`—Notificación de error de discrepancia de etiqueta VT
  - `vt-loss-of-cell`—VT pérdida de notificación de delineación celular
- `startup`—Arranques en caliente y en frío del sistema
- `timing-events`—Notificación de eventos de temporización y defectos
- `vrrp-events`—Eventos del Protocolo de redundancia de enrutador virtual (VRRP), como errores de autenticación o nuevas primarias

Si incluye subcategorías SONET/SDH, solo se incluyen esos tipos de alarma de captura SONET/SDH en las notificaciones de captura.

La instrucción permite especificar la versión SNMP de las capturas enviadas a los destinos del grupo de capturas.`version` Si especifica sólo, se envían capturas SNMPv1.`v1` Si especifica sólo, se envían capturas SNMPv2.`v2` Si especifica , se envían una captura SNMPv1 y SNMPv2 para cada condición de interrupción.`all` Para obtener más información acerca de la instrucción, consulte versión (SNMP).`version` *version (SNMP)*

Configurar opciones y grupos de capturas SNMP en un dispositivo que ejecute Junos OS

Algunos portadores tienen más de un receptor de trampa que reenvía las trampas a un NMS central. Esto permite más de una ruta para capturas SNMP desde un enrutador al NMS central a través de diferentes receptores de captura. Puede configurar un dispositivo que ejecute Junos OS para que envíe la misma copia de cada captura SNMP a cada receptor de capturas configurado en el grupo de capturas.

La dirección de origen en el encabezado IP de cada paquete de captura SNMP se establece en la dirección de la interfaz saliente de forma predeterminada. Cuando un receptor de captura reenvía el paquete al NMS central, se conserva la dirección de origen. El NMS central, mirando sólo la dirección de origen de cada paquete de captura SNMP, asume que cada captura SNMP proviene de una fuente diferente.

En realidad, las trampas SNMP provenían del mismo enrutador, pero cada una salía del enrutador a través de una interfaz de salida diferente.

Las instrucciones descritas en las secciones siguientes se proporcionan para permitir que el NMS reconozca las capturas duplicadas y las distinga las capturas SNMPv1 en función de la interfaz de salida.

Para configurar las opciones de captura SNMP y los grupos de interrupción, incluya las instrucciones y en el nivel jerárquico :`trap-optionstrap-group[edit snmp]`

```
[edit snmp]
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
trap-group group-name {
    categories {
        category;
    }
    destination-port port-number;
    targets {
        address;
    }
    version (all | v1 | v2);
}
```

Ejemplo: Configuración de grupos de capturas SNMP

Configure una lista de notificaciones de capturas denominada para capturas de vínculo e inicio.`urgent-dispatcher` Esta lista se utiliza para identificar los hosts de administración de red (y) a los que se deben enviar las capturas generadas por el enrutador local.`1.2.3.4fe80::1:2:3:4` El nombre especificado para un grupo de capturas se utiliza como cadena de comunidad SNMP cuando el agente envía capturas a los destinos enumerados.

```
[edit]
snmp {
    trap-group "urgent-dispatcher" {
        version v2;
        categories link startup;
        targets {
            1.2.3.4;
            fe80::1:2:3:4;
        }
    }
}
```

Administrar trampas

A continuación se proporcionan detalles sobre la administración de notificaciones SNMP:

- **Genere capturas basadas en eventos de SysLog:**

  Las directivas de eventos pueden incluir una acción que genere capturas para eventos en función de los mensajes de registro del sistema. Esta característica permite notificar a una aplicación basada en capturas SNMP cuando se produce un mensaje importante de registro del sistema. Puede convertir cualquier mensaje de registro del sistema, para el que no haya ninguna interrupción correspondiente, en una trampa. Si utiliza capturas del sistema de administración de red en lugar de mensajes de registro del sistema para supervisar la red, puede utilizar esta función para asegurarse de que se le notifiquen todos los eventos importantes.

  Para configurar una directiva que genere una interrupción al recibir un evento, incluya las siguientes instrucciones en el nivel de jerarquía: `[edit event-options policy policy-name]`

En el ejemplo siguiente se muestra la configuración de ejemplo para generar una interrupción para el evento :`ui_mgd_terminate`

```
[edit event-options policy p1]
events ui_mgd_terminate;
then {
    raise-trap;
}
```

- **Filtre las capturas según la categoría de captura:**

  Las capturas SNMP se clasifican en muchas categorías. Junos OS proporciona una opción de configuración, en el nivel de jerarquía, que le permite especificar categorías de capturas que desea recibir en un host determinado.`categories`[`edit snmp trap-group` *`trap-group`*] Puede utilizar esta opción cuando desee supervisar solo módulos específicos de Junos OS.

  En el ejemplo siguiente se muestra una configuración de ejemplo para recibir solo , , y capturas:`link`,`vrrp-events`,`services`,`otn-alarms`

```
[edit snmp]
trap-group jnpr {
    categories {
        link;
        vrrp-events;
        services;
        otn-alarms;
    }
    targets {
        192.168.69.179;
    }
}
```

- **Filtre las capturas según el identificador del objeto:**

  Junos OS también proporciona una opción de filtro más avanzada que le permite filtrar capturas específicas en función de sus identificadores de objeto. Puede utilizar la opción para filtrar una captura específica o un grupo de capturas.`notify-filter`

  En el siguiente ejemplo se muestra la configuración de ejemplo para excluir las capturas de administración de configuración específicas de la empresa de Juniper Networks (tenga en cuenta que

la configuración de SNMPv3 también admite el filtrado de capturas SNMPv1 y SNMPv2, como se muestra en el siguiente ejemplo):

```
[edit snmp]
v3 {
    vacm {
        security-to-group {
            security-model v2c {
                security-name sn_v2c_trap {
                    group gr_v2c_trap;
                }
            }
        }
        access {
            group gr_v2c_trap {
                default-context-prefix {
                    security-model v2c {
                        security-level none {
                            read-view all;
                            notify-view all;
                        }
                    }
                }
            }
        }
    }
    target-address TA_v2c_trap {
        address 10.209.196.166;
        port 9001;
        tag-list tg1;
        target-parameters TP_v2c_trap;
    }
    target-parameters TP_v2c_trap {
        parameters {
            message-processing-model v2c;
            security-model v2c;
            security-level none;
            security-name sn_v2c_trap;
        }
        notify-filter nf1;
    }
    notify v2c_notify {
```

```
        type trap;
        tag tg1;
    }
    notify-filter nf1 {
        oid .1.3.6.1.4.1.2636.4.5 exclude;
        oid .1 include;
    }
    snmp-community index1 {
        community-name "$9$tDLl01h7Nbw2axN"; ## SECRET-DATA
        security-name sn_v2c_trap;
        tag tg1;
    }
    view all {
        oid .1 include;
    }
}
```

Capturas SNMP compatibles con Junos OS

in this section

- Soporte de trampas SNMP | **488**
- Capturas SNMP estándar compatibles con Junos OS | **509**
- MIB SNMP personalizadas para capturas syslog | **520**

Los conmutadores independientes de la serie QFX, el chasis virtual de la serie QFX y los sistemas QFabric admiten capturas SNMP estándar y capturas específicas de la empresa de Juniper Networks.

Soporte de trampas SNMP

in this section

- Capturas SNMP compatibles con los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX | 488
- Capturas SNMP compatibles con sistemas QFabric | 503

Capturas SNMP compatibles con los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX

Los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX admiten capturas SNMPv1 y v2. Para obtener más información, consulte:

Capturas SNMPv1

Los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX admiten capturas SNMPv1 estándar y capturas SNMPv1 específicas para empresas de Juniper Networks. Ver:

- Tabla 37 en la página 489 para capturas SNMPv1 estándar.
- Tabla 38 en la página 493 para capturas SNMPv1 específicas de la empresa.

Las trampas se organizan primero por categoría de captura y luego por nombre de captura. Los niveles de gravedad del registro del sistema se enumeran para las capturas que los tienen. Las capturas que no tienen los niveles de gravedad correspondientes del registro del sistema se marcan con un guión (–).

Tabla 37: Capturas SNMP versión 1 estándar compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog
Notificaciones de enlaces						
RFC 1215, Convenciones para definir interrupciones para su uso con SNMP	linkDown	1.3.6.1.4.1.2636	2	0	Advertencia	SNMP_ TRAP_ LINK_DOWN
	Linkup	1.3.6.1.4.1.2636	3	0	Información	SNMP_TRAP_ LINK_UP
Notificaciones de operaciones remotas						
RFC 2925, Definiciones de objetos administrados para operaciones remotas de ping, traceroute y búsqueda	pingProbeFailed	1.3.6.1.2.1.80.0	6	1	Información	SNMP_TRAP _PING_ PROBE_ FALLÓ
	pingTestFailed	1.3.6.1.2.1.80.0	6	2	Información	SNMP_TRAP_ PING_TEST _FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0	6	3	Información	SNMP_TRAP_ PING_TEST_ COMPLETADO
	traceRoutePathChange	1.3.6.1.2.1.81.0	6	1	Información	SNMP_TRAP_ TRACE_ROUTE_ PATH_CHANGE

Tabla 37: Capturas SNMP versión 1 estándar compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog
	traceRouteTestFailed	1.3.6.1.2.1.81.0	6	2	Información	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0	6	3	Información	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETED
Alarmas RMON						
RFC 2819a, RMON MIB	caídaAlarma	1.3.6.1.2.1.16	6	2	–	–
	alarma ascendente	1.3.6.1.2.1.16	6	1	–	–
Notificaciones de enrutamiento						
BGP 4 MIB	bgpEstablecido	1.3.6.1.2.1.15.7	6	1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7	6	2	–	–
TRAMPA OSPF MIB	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2	6	1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2	6	2	–	–

Tabla 37: Capturas SNMP versión 1 estándar compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2	6	3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2	6	4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2	6	5	–	–
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2	6	6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2	6	7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2	6	9	–	–
	ospfTxRetransmitir	1.3.6.1.2.1.14.16.2	6	10	–	–
	ospfVirtIfTxRetransmitir	1.3.6.1.2.1.14.16.2	6	11	–	–

Tabla 37: Capturas SNMP versión 1 estándar compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2	6	13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2	6	16	–	–
Notificaciones de inicio						
RFC 1215, Convenciones para definir interrupciones para su uso con SNMP	authenticationFailure	1.3.6.1.4.1.2636	4	0	Aviso	SNMPD_ TRAP_ GEN_FAILURE
	coldStart	1.3.6.1.4.1.2636	0	0	Crítico	SNMPD_TRAP_ COLD_START
	warmStart	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_ WARM_START
Notificaciones VRRP						
RFC 2787, Definiciones de objetos administrados para el protocolo de redundancia de enrutador virtual	vrrpTrapNewMaster	1.3.6.1.2.1.68	6	1	Advertencia	VRRPD_NEW MASTER_TRAP
	vrrpTrapAuthFailure	1.3.6.1.2.1.68	6	2	Advertencia	VRRPD_AUTH_ FAILURE_TRAP

Tabla 38: Capturas SNMPv1 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
Notificaciones del chasis (condiciones de alarma)						
MIB de chasis (jnx-chassis. mib)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1	6	1	Advertencia	CHASSISD_SNMP_TRAMPA
	jnxFanFailure	1.3.6.1.4.1.26361	6	2	Crítico	CHASSISD_SNMP_TRAMPA
	jnxOverTemperature	11.4.1.2636.4.1	6	3	Alerta	CHASSISD_SNMP_TRAMPA
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1	6	5	Aviso	CHASSISD_SNMP_TRAMPA
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1	6	6	Aviso	CHASSISD_SNMP_TRAMPA
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1	6	7	Aviso	CHASSISD_SNMP_TRAMPA
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1	6	8	Aviso	CHASSISD_SNMP_TRAMPA

Tabla 38: Capturas SNMPv1 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxFruFailed	1.3.6.1.4.1.2636.4.1	6	9	Advertencia	CHASSISD_SNMP_TRAMPA
	jnxFruOffline	1.3.6.1.4.1.2636.4.1	6	10	Aviso	CHASSISD_SNMP_TRAMPA
	jnxFruOnline	1.3.6.1.4.1.2636.4.1	6	11	Aviso	CHASSISD_SNMP_TRAMPA
	jnxFruCheck	1.3.6.1.4.1.2636.4.1	6	12	Advertencia	CHASSISD_SNMP_TRAMPA
	jnxPowerSupplyOk	1.3.6.1.4.1.2636.4.2	6	1	Crítico	CHASSISD_SNMP_TRAMPA
	jnxFanOK	1.3.6.1.4.1.2636.4.2	6	2	Crítico	CHASSISD_SNMP_TRAMPA
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2	6	3	Alerta	CHASSISD_SNMP_TRAMPA
Notificaciones de configuración						

Tabla 38: Capturas SNMPv1 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
MIB de administración de la configuración (jnx- configmgmt.mib)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5	6	1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5	6	2	–	–
Operaciones remotas						
Ping MIB (jnx-ping.mib)	jnxPingRttThresholdExceeded	1.3.6.1.4.1.2636.4.9	6	1	–	–
	jnxPingRttStdDevThreshold excedido	1.3.6.1.4.1.2636.4.9	6	2	–	–
	jnxPingRttJitterThreshold excedido	1.3.6.1.4.1.2636.4.9	6	3	–	–
	jnxPingEgressThreshold excedido	1.3.6.1.4.1.2636.4.9	6	4	–	–
	jnxPingEgressStdDevThresholdExcedido	1.3.6.1.4.1.2636.4.9	6	5	–	–
	jnxPingEgressJitterThreshold excedido	1.3.6.1.4.1.2636.4.9	6	6	–	–
	jnxPingIngressThreshold excedido	1.3.6.1.4.1.2636.4.9	6	7	–	–

Tabla 38: Capturas SNMPv1 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxPingIngressStddevThreshold excedido	1.3.6.1.4.1.2636.4.9	6	8	–	–
	jnxPingIngressJitterThreshold excedido	1.3.6.1.4.1.2636.4.9	6	9	–	–
Alarmas RMON						
MIB RMON (jnx-rmon. mib)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4.3	6	1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4.3	6	2	–	–

Capturas SNMPv2

- Tabla 39 en la página 496 enumera las capturas SNMP estándar
- Tabla 40 en la página 500 enumera las capturas específicas de la empresa de Juniper Networks

Tabla 39: Capturas SNMPv2 estándar admitidas en conmutadores independientes de la serie QFX y chasis virtual de la serie QFX

Definido en	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta syslog
Notificaciones de enlaces				

Tabla 39: Capturas SNMPv2 estándar admitidas en conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta syslog
RFC 2863, El grupo de interfaces MIB	linkDown	1.3.6.1.6.3.1.1.5.3	Advertencia	SNMP_TRAP_LINK_DOWN
	Linkup	1.3.6.1.6.3.1.1.5.4	Información	SNMP_TRAP_LINK_UP
Notificaciones de operaciones remotas				
RFC 2925, Definiciones de objetos administrados para operaciones remotas de ping, traceroute y búsqueda	pingProbeFailed	1.3.6.1.2.1.80.0.1	Información	SNMP_TRAP_PING_PROBE_FALLIDO
	pingTestFailed	1.3.6.1.2.1.80.0.2	Información	SNMP_TRAP_PING_TEST_FAILED
	pingTestCompleted	1.3.6.1.2.1.80.0.3	Información	SNMP_TRAP_PING_TEST_COMPLETED
	traceRoutePathChange	1.3.6.1.2.1.81.0.1	Información	SNMP_TRAP_TRACE_ROUTE_PATH_CAMBIO
	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	Información	SNMP_TRAP_TRACE_ROUTE_TEST_FAILED
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	Información	SNMP_TRAP_TRACE_ROUTE_TEST_COMPLETADO
Alarmas RMON				

Tabla 39: Capturas SNMPv2 estándar admitidas en conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta syslog
RFC 2819a, RMON MIB	caídaAlarma	1.3.6.1.2.1.16.0.1	–	–
	alarma ascendente	1.3.6.1.2.1.16.0.2	–	–
Notificaciones de enrutamiento				
BGP 4 MIB	bgpEstablecido	1.3.6.1.2.1.15.7.1	–	–
	bgpBackwardTransition	1.3.6.1.2.1.15.7.2	–	–
MIB de captura OSPF	ospfVirtIfStateChange	1.3.6.1.2.1.14.16.2.1	–	–
	ospfNbrStateChange	1.3.6.1.2.1.14.16.2.2	–	–
	ospfVirtNbrStateChange	1.3.6.1.2.1.14.16.2.3	–	–
	ospfIfConfigError	1.3.6.1.2.1.14.16.2.4	–	–
	ospfVirtIfConfigError	1.3.6.1.2.1.14.16.2.5	–	–

Tabla 39: Capturas SNMPv2 estándar admitidas en conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta syslog
	ospfIfAuthFailure	1.3.6.1.2.1.14.16.2.6	–	–
	ospfVirtIfAuthFailure	1.3.6.1.2.1.14.16.2.7	–	–
	ospfIfRxBadPacket	1.3.6.1.2.1.14.16.2.8	–	–
	ospfVirtIfRxBadPacket	1.3.6.1.2.1.14.16.2.9	–	–
	ospfTxRetransmitir	1.3.6.1.2.1.14.16.2.10	–	–
	ospfVirtIfTxRetransmitir	1.3.6.1.2.1.14.16.2.11	–	–
	ospfMaxAgeLsa	1.3.6.1.2.1.14.16.2.13	–	–
	ospfIfStateChange	1.3.6.1.2.1.14.16.2.16	–	–
Notificaciones de inicio				
RFC 1907, Base de información de administración para la versión 2 del Protocolo	coldStart	1.3.6.1.6.3.1.1.5.1	Crítico	SNMPD_TRAP_COLD_START

Tabla 39: Capturas SNMPv2 estándar admitidas en conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

Definido en	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta syslog
simple de administración de redes (SNMPv2)	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Aviso	SNMPD_TRAP_GEN_FAILURE
Notificaciones VRRP				
RFC 2787, Definiciones de objetos administrados para el protocolo de redundancia de enrutador virtual	vrrpTrapNewMaster	1.3.6.1.2.1.68.0.1	Advertencia	VRRPD_NEWMASTER_TRAMPA
	vrrpTrapAuthFailure	1.3.6.1.2.1.68.0.2	Advertencia	VRRPD_AUTH_FAILURE_ TRAMPA

Tabla 40: Capturas SNMPv2 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
Notificaciones del chasis (condiciones de alarma)				
MIB de chasis (mib-jnx-chasis)	jnxPowerSupplyFailure	1.3.6.1.4.1.2636.4.1.1	Alerta	CHASSISD_SNMP_ TRAMPA
	jnxFanFailure	1.3.6.1.4.1.2636.4.1.2	Crítico	CHASSISD_SNMP_ TRAMPA

Tabla 40: Capturas SNMPv2 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxOverTemperature	1.3.6.1.4.1.2636.4.1.3	Crítico	CHASSISD_ SNMP_ TRAMPA
	jnxFruRemoval	1.3.6.1.4.1.2636.4.1.5	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxFruInsertion	1.3.6.1.4.1.2636.4.1.6	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxFruPowerOff	1.3.6.1.4.1.2636.4.1.7	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxFruPowerOn	1.3.6.1.4.1.2636.4.1.8	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxFruFailed	1.3.6.1.4.1.2636.4.1.9	Advertenci a	CHASSISD_ SNMP_ TRAMPA
	jnxFruOffline	1.3.6.1.4.1.2636.4.1.10	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxFruOnline	1.3.6.1.4.1.2636.4.1.11	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxFruCheck	1.3.6.1.4.1.2636.4.1.12	Aviso	CHASSISD_ SNMP_ TRAMPA
	jnxPowerSupplyOK	1.3.6.1.4.1.2636.4.2.1	Crítico	CHASSISD_ SNMP_ TRAMPA

Tabla 40: Capturas SNMPv2 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxFanOK	1.3.6.1.4.1.2636.4.2.2	Crítico	CHASSISD_ SNMP_ TRAMPA
	jnxTemperatureOK	1.3.6.1.4.1.2636.4.2.3	Alerta	CHASSISD_ SNMP_ TRAMPA
Notificaciones de configuración				
MIB de administración de la configuración (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Notificaciones de operaciones remotas				
Ping MIB (mib-jnx-ping)	jnxPingRttThreshold excedido	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshol d excedido	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold excedido	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold excedido	1.3.6.1.4.1.2636.4.9.0.4	–	–
	jnxPingEgressStdDevThres hold superado	1.3.6.1.4.1.2636.4.9.0.5	–	–

Tabla 40: Capturas SNMPv2 específicas de la empresa compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxPingEgressJitterThreshold excedido	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold excedido	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold excedido	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold excedido	1.3.6.1.4.1.2636.4.9.0.9	–	–
Alarmas RMON				
MIB de RMON (mib-jnx-rmon)	jnxRmonAlarmGetFailure	1.3.6.1.4.1.2636.4. 3.0.1	–	–
	jnxRmonGetOk	1.3.6.1.4.1.2636.4. 3.0.2	–	–

Capturas SNMP compatibles con sistemas QFabric

Los sistemas QFabric admiten capturas SNMPv2 estándar y capturas SNMPv2 específicas para empresas de Juniper Networks.

NOTA: Los sistemas QFabric no admiten capturas SNMPv1.

Para obtener más información, consulte:

- Tabla 41 en la página 504 para capturas SNMPv2 estándar
- Tabla 42 en la página 504 para capturas SNMPv2 específicas de la empresa de Juniper Networks

Tabla 41: Capturas SNMPv2 estándar admitidas en sistemas QFabric

Definido en	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta syslog
Notificaciones de enlaces				
RFC 2863, El grupo de interfaces MIB	linkDown	1.3.6.1.6.3.1.1.5.3	Advertencia	SNMP_TRAP_LINK_DOWN
	Linkup	1.3.6.1.6.3.1.1.5.4	Información	SNMP_TRAP_LINK_UP
Notificaciones de inicio				
RFC 1907, Base de información de administración para la versión 2 del Protocolo simple de administración de redes (SNMPv2)	coldStart	1.3.6.1.6.3.1.1.5.1	Crítico	SNMPD_TRAP_COLD_START
	warmStart	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START
	authenticationFailure	1.3.6.1.6.3.1.1.5.5	Aviso	SNMPD_TRAP_GEN_FAILURE

Tabla 42: Capturas SNMPv2 específicas de la empresa compatibles con sistemas QFabric

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
MIB de chasis de estructura (mib-jnx-fabric-chasis)	**Notificaciones de chasis de estructura (condiciones de alarma)**			
	jnxFabricPowerSupplyFailure	1.3.6.1.4.1.2636.4.19.1	Advertencia	–

Tabla 42: Capturas SNMPv2 específicas de la empresa compatibles con sistemas QFabric *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxFabricFanFailure	1.3.6.1.4.1.2636.4.19.2	Crítico	–
	jnxFabricOverTemperature	1.3.6.1.4.1.2636.4.19.3	Alerta	–
	jnxFabricRedundancySwitchover	1.3.6.1.4.1.2636.4.19.4	Aviso	–
	jnxFabricFruRemoval	1.3.6.1.4.1.2636.4.19.5	Aviso	–
	jnxFabricFruInsertion	1.3.6.1.4.1.2636.4.19.6	Aviso	–
	jnxFabricFruPowerOff	1.3.6.1.4.1.2636.4.19.7	Aviso	–
	jnxFabricFruPowerOn	1.3.6.1.4.1.2636.4.19.8	Aviso	–
	jnxFabricFruFailed	1.3.6.1.4.1.2636.4.19.9	Advertencia	–
	jnxFabricFruOffline	1.3.6.1.4.1.2636.4.19.10	Aviso	–
	jnxFabricFruOnline	1.3.6.1.4.1.2636.4.19.11	Aviso	–
	jnxFabricFruCheck	1.3.6.1.4.1.2636.4.19.12	Advertencia	–
	jnxFabricFEBSwitchover	1.3.6.1.4.1.2636.4.19.13	Advertencia	–

Tabla 42: Capturas SNMPv2 específicas de la empresa compatibles con sistemas QFabric *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxFabricHardDiskFailed	1.3.6.1.4.1.2636.4.19.14	Advertencia	–
	jnxFabricHardDiskMissing	1.3.6.1.4.1.2636.4.19.15	Advertencia	–
	jnxFabricBootFromBackup	1.3.6.1.4.1.2636.4.19.16	Advertencia	–
	Notificaciones de chasis de estructura (condiciones de alarma despejada)			
	jnxFabricPowerSupplyOK	1.3.6.1.4.1.2636.4.20.1	Crítico	–
	jnxFabricFanOK	1.3.6.1.4.1.2636.4.20.2	Crítico	–
	jnxFabricTemperatureOK	1.3.6.1.4.1.2636.4.20.3	Alerta	–
	jnxFabricFruOK	1.3.6.1.4.1.2636.4.20.4	–	–
MIB QFabric (mib-jnx-qf-smi)	**Notificaciones de QFabric MIB**			
	jnxQFabricDownloadIssued	1.3.6.1.4.1.2636.3.42.1.0.1	–	–
	jnxQFabricDownloadFailed	1.3.6.1.4.1.2636.3.42.1.0.2	–	–
	jnxQFabricDownloadSucceeded	1.3.6.1.4.1.2636.3.42.1.0.3	–	–

Tabla 42: Capturas SNMPv2 específicas de la empresa compatibles con sistemas QFabric *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxQFabricUpgradeIssued	1.3.6.1.4.1.2636.3.42.1.0.4	–	–
	jnxQFabricUpgradeFailed	1.3.6.1.4.1.2636.3.42.1.0.5	–	–
	jnxQFabricUpgradeSucceeded	1.3.6.1.4.1.2636.3.42.1.0.6	–	–
Notificaciones de configuración				
MIB de administración de la configuración (mib-jnx-cfgmgmt)	jnxCmCfgChange	1.3.6.1.4.1.2636.4.5.0.1	–	–
	jnxCmRescueChange	1.3.6.1.4.1.2636.4.5.0.2	–	–
Notificaciones de operaciones remotas				
Ping MIB (mib-jnx-ping)	jnxPingRttThreshold excedido	1.3.6.1.4.1.2636.4.9.0.1	–	–
	jnxPingRttStdDevThreshold excedido	1.3.6.1.4.1.2636.4.9.0.2	–	–
	jnxPingRttJitterThreshold excedido	1.3.6.1.4.1.2636.4.9.0.3	–	–
	jnxPingEgressThreshold excedido	1.3.6.1.4.1.2636.4.9.0.4	–	–

Tabla 42: Capturas SNMPv2 específicas de la empresa compatibles con sistemas QFabric *(Continued)*

MIB de origen	Nombre de la trampa	OID de captura SNMP	Nivel de gravedad del registro del sistema	Etiqueta de registro del sistema
	jnxPingEgressStdDevThreshold superado	1.3.6.1.4.1.2636.4.9.0.5	–	–
	jnxPingEgressJitterThreshold excedido	1.3.6.1.4.1.2636.4.9.0.6	–	–
	jnxPingIngressThreshold excedido	1.3.6.1.4.1.2636.4.9.0.7	–	–
	jnxPingIngressStddevThreshold excedido	1.3.6.1.4.1.2636.4.9.0.8	–	–
	jnxPingIngressJitterThreshold excedido	1.3.6.1.4.1.2636.4.9.0.9	–	–

SEE ALSO

Explorador SNMP MIB

No Link Title

Descripción de la implementación de SNMP en el sistema QFabric

Compatibilidad con MIB SNMP

Capturas SNMP estándar compatibles con Junos OS

in this section

- Capturas SNMP versión 1 estándar | **509**
- Capturas SNMP versión 2 estándar | **514**

En este tema se proporciona la lista de capturas SNMPv1 y SNMPv2 estándar compatibles con dispositivos que ejecutan Junos OS. Para obtener más información acerca de las capturas, consulte SNMP MIB Explorer.

A partir de Junos OS versión 20.1, después de un cambio correcto del motor de enrutamiento (GRES), el nuevo motor de enrutamiento principal envía una única notificación warmStart. El motor de enrutamiento principal envía una notificación cuando aparece el dispositivo.`coldStart` El motor de enrutamiento principal también envía notificaciones para reinicios posteriores del demonio SNMP.`warmStart` Después de GRES, el nuevo motor de enrutamiento principal envía una sola notificación y el motor de enrutamiento de reserva no envía ninguna notificación.`warmStart`

Capturas SNMP versión 1 estándar

Tabla 43 en la página 510 proporciona información general sobre las capturas estándar para SNMPv1. Las capturas se organizan primero por categoría de captura y luego por nombre de captura, e incluyen su identificador de empresa, número genérico de captura y número de captura específico. Los niveles de gravedad del registro del sistema se enumeran para aquellas capturas que los tienen con su etiqueta de registro del sistema correspondiente. Las capturas que no tienen los niveles de gravedad correspondientes del registro del sistema se marcan con un guión (–) en la tabla.

Para obtener más información acerca de los mensajes de registro del sistema, consulte el Explorador de registros del sistema.https://apps.juniper.net/syslog-explorer/

Tabla 43: Capturas SNMP versión 1 compatibles con estándar

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
Notificaciones de inicio							
RFC 1215, Convenciones para definir interrupciones para su uso con SNMP	`authenticationFailure`	1.3.6.1.4.1.2636	4	0	Aviso	SNMPD_ TRAP_ GEN_FAILURE	Todos los dispositivos que ejecutan Junos OS.
	`coldStart`	1.3.6.1.4.1.2636	0	0	Crítico	SNMPD_TRAP_ COLD_START	Todos los dispositivos que ejecutan Junos OS.
	`warmStart`	1.3.6.1.4.1.2636	1	0	Error	SNMPD_TRAP_ WARM_START	Todos los dispositivos que ejecutan Junos OS.
Notificaciones de enlaces							
RFC 1215, Convenciones para definir interrupciones para su uso con SNMP	`linkDown`	1.3.6.1.4.1.2636	2	0	Advertencia	SNMP_ TRAP_ LINK_DOWN	Todos los dispositivos que ejecutan Junos OS.
	`linkUp`	1.3.6.1.4.1.2636	3	0	Información	SNMP_TRAP_ LINK_UP	Todos los dispositivos que ejecutan Junos OS.
Notificaciones de operaciones remotas							
RFC 2925, Definiciones de	`pingProbeFailed`	1.3.6.1.2.1.80.0	6	1	Información	SNMP_TRAP _PING_ PROBE_ FALLÓ	Todos los dispositivos que ejecutan Junos OS.

Tabla 43: Capturas SNMP versión 1 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
objetos administrados para operaciones remotas de ping, traceroute y búsqueda	`pingTestFailed`	1.3.6.1.2.1.80.0	6	2	Información	SNMP_TRAP_PING_TEST_FAILED	Todos los dispositivos que ejecutan Junos OS.
	`pingTestCompleted`	1.3.6.1.2.1.80.0	6	3	Información	SNMP_TRAP_PING_TEST_COMPLETADO	Todos los dispositivos que ejecutan Junos OS.
Alarmas RMON							
RFC 2819a, RMON MIB	`fallingAlarm`	1.3.6.1.2.1.16	6	2	–	–	Todos los dispositivos que ejecutan Junos OS.
	`risingAlarm`	1.3.6.1.2.1.16	6	1	–	–	Todos los dispositivos que ejecutan Junos OS.
Notificaciones de enrutamiento							
BGP 4 MIB	`bgpEstablished`	1.3.6.1.2.1.15.7	6	1	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`bgpBackwardTransition`	1.3.6.1.2.1.15.7	6	2	–	–	Firewalls de las series M, T, MX, J, EX y SRX.

Tabla 43: Capturas SNMP versión 1 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
TRAMPA OSPF MIB	`ospfVirtIfStateChange`	1.3.6.1.2.1.14.16.2	6	1	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfNbrStateChange`	1.3.6.1.2.1.14.16.2	6	2	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfVirtNbrStateChange`	1.3.6.1.2.1.14.16.2	6	3	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfIfConfigError`	1.3.6.1.2.1.14.16.2	6	4	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfVirtIfConfigError`	1.3.6.1.2.1.14.16.2	6	5	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfIfAuthFailure`	1.3.6.1.2.1.14.16.2	6	6	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfVirtIfAuthFailure`	1.3.6.1.2.1.14.16.2	6	7	–	–	Firewalls de las series M, T, MX, J, EX y SRX.

Tabla 43: Capturas SNMP versión 1 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
	`ospfIfRxBadPacket`	1.3.6.1.2.1.14.16.2	6	8	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfVirtIfRxBadPacket`	1.3.6.1.2.1.14.16.2	6	9	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfTxRetransmit`	1.3.6.1.2.1.14.16.2	6	10	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfVirtIfTxRetransmit`	1.3.6.1.2.1.14.16.2	6	11	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfMaxAgeLsa`	1.3.6.1.2.1.14.16.2	6	13	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
	`ospfIfStateChange`	1.3.6.1.2.1.14.16.2	6	16	–	–	Firewalls de las series M, T, MX, J, EX y SRX.
Notificaciones VRRP							
RFC 2787, Definiciones de objetos	`vrrpTrapNewMaster`	1.3.6.1.2.1.68	6	1	Advertencia	VRRPD_NEW MASTER_TRAP	Todos los dispositivos que ejecutan Junos OS.

Tabla 43: Capturas SNMP versión 1 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	Enterprise ID	Número genérico de trampa	Número de trampa específico	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
administrados para el protocolo de redundancia de enrutador virtual	`vrrpTrapAuthFailure`	1.3.6.1.2.1.68	6	2	Advertencia	VRRPD_AUTH_FAILURE_TRAP	Todos los dispositivos que ejecutan Junos OS.
RFC 6527, Definiciones de objetos administrados para el protocolo de redundancia de enrutador virtual versión 3 (VRRPv3)	`vrrpv3NewMaster`	1.3.6.1.2.1.207	6	1	Advertencia	VRRPD_NEW_MASTER	M y MX
	`vrrpv3ProtoError`	1.3.6.1.2.1.207	6	2	Advertencia	VRRPD_V3_PROTO_ERROR	M y MX

Capturas SNMP versión 2 estándar

Tabla 44 en la página 515 proporciona una descripción general de las capturas SNMPv2 estándar compatibles con Junos OS. Las trampas se organizan primero por categoría de trampa y luego por nombre de trampa e incluyen su archivo `.snmpTrapOID` Los niveles de gravedad del registro del sistema se enumeran para aquellas capturas que los tienen con su etiqueta de registro del sistema correspondiente. Las capturas que no tienen los niveles de gravedad correspondientes del registro del sistema se marcan con un guión (–) en la tabla.

Tabla 44: Capturas SNMP versión 2 compatibles con estándar

Definido en	Nombre de la trampa	snmpTrapOID	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
Notificaciones de inicio					
RFC 1907, Base de información de administración para la versión 2 del Protocolo simple de administración de redes (SNMPv2)	`coldStart`	1.3.6.1.6.3.1.1.5.1	Crítico	SNMPD_TRAP_COLD_START	Todos los dispositivos que ejecutan Junos OS.
	`warmStart`	1.3.6.1.6.3.1.1.5.2	Error	SNMPD_TRAP_WARM_START	Todos los dispositivos que ejecutan Junos OS.
	`authenticationFailure`	1.3.6.1.6.3.1.1.5.5	Aviso	SNMPD_TRAP_GEN_FAILURE	Todos los dispositivos que ejecutan Junos OS.
Notificaciones de enlaces					
RFC 2863, El grupo de interfaces MIB	`linkDown`	1.3.6.1.6.3.1.1.5.3	Advertencia	SNMP_TRAP_LINK_DOWN	Todos los dispositivos que ejecutan Junos OS.
	`linkUp`	1.3.6.1.6.3.1.1.5.4	Información	SNMP_TRAP_LINK_UP	Todos los dispositivos que ejecutan Junos OS.
Notificaciones de operaciones remotas					
RFC 2925, Definiciones de objetos administrados para operaciones	`pingProbeFailed`	1.3.6.1.2.1.80.0.1	Información	SNMP_TRAP_PING_PROBE_FALLIDO	Todos los dispositivos que ejecutan Junos OS.

Tabla 44: Capturas SNMP versión 2 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	snmpTrapOID	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
remotas de ping, traceroute y búsqueda	`pingTestFailed`	1.3.6.1.2.1.80.0.2	Información	SNMP_TRAP_PING_ TEST_FAILED	Todos los dispositivos que ejecutan Junos OS.
	`pingTestCompleted`	1.3.6.1.2.1.80.0.3	Información	SNMP_TRAP_PING_ TEST_COMPLETED	Todos los dispositivos que ejecutan Junos OS.
Alarmas RMON					
RFC 2819a, RMON MIB	`fallingAlarm`	1.3.6.1.2.1.16.0.1	–	–	Todos los dispositivos que ejecutan Junos OS.
	`risingAlarm`	1.3.6.1.2.1.16.0.2	–	–	Todos los dispositivos que ejecutan Junos OS.
Notificaciones de enrutamiento					
BGP 4 MIB	`bgpEstablished`	1.3.6.1.2.1.15.7.1	–	–	Todos los dispositivos que ejecutan Junos OS.
	`bgpBackwardTransition`	1.3.6.1.2.1.15.7.2	–	–	Todos los dispositivos que ejecutan Junos OS.
MIB de captura OSPF	`ospfVirtIfStateChange`	1.3.6.1.2.1.14.16.2.1	–	–	Todos los dispositivos que ejecutan Junos OS.

Tabla 44: Capturas SNMP versión 2 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	snmpTrapOID	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
	`ospfNbrStateChange`	1.3.6.1.2.1.14.16.2.2	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfVirtNbrStateChange`	1.3.6.1.2.1.14.16.2.3	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfIfConfigError`	1.3.6.1.2.1.14.16.2.4	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfVirtIfConfigError`	1.3.6.1.2.1.14.16.2.5	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfIfAuthFailure`	1.3.6.1.2.1.14.16.2.6	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfVirtIfAuthFailure`	1.3.6.1.2.1.14.16.2.7	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfIfRxBadPacket`	1.3.6.1.2.1.14.16.2.8	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfVirtIfRxBadPacket`	1.3.6.1.2.1.14.16.2.9	–	–	Todos los dispositivos que ejecutan Junos OS.

Tabla 44: Capturas SNMP versión 2 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	snmpTrapOID	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
	`ospfTxRetransmit`	1.3.6.1.2.1.14.16.2.10	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfVirtIfTxRetransmit`	1.3.6.1.2.1.14.16.2.11	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfMaxAgeLsa`	1.3.6.1.2.1.14.16.2.13	–	–	Todos los dispositivos que ejecutan Junos OS.
	`ospfIfStateChange`	1.3.6.1.2.1.14.16.2.16	–	–	Todos los dispositivos que ejecutan Junos OS.
Notificaciones MPLS					
RFC 3812, Base de información de administración de ingeniería de tráfico (TE) de conmutación de etiquetas multiprotocolo (MPLS)	`mplsTunnelUp`				
	`mplsTunnelDown`				
	`mplsTunnelRerouted`				
	`mplsTunnelReoptimized`				
Notificaciones MIB de estado de entidad					

Tabla 44: Capturas SNMP versión 2 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	snmpTrapOID	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
RFC 4268, MIB de estado de entidad	`entStateOperEnabled`	1.3.6.1.2.1.131.0.1	Aviso	CHASSISD_SNMP_TRAP3	MX240, MX480 y MX960
	`entStateOperDisabled`	1.3.6.1.2.1.131.0.2	Aviso	CHASSISD_SNMP_TRAP3	MX240, MX480 y MX960
Notificaciones de L3VPN					
RFC 4382, Red privada virtual (VPN) MPLS/BGP de capa 3	`mplsL3VpnVrfUp`				
	`mplsL3VpnVrfDown`				
	`mplsL3VpnVrf RouteMidThresh Exceeded`				
	`mplsL3VpnVrf NumVrfRouteMax ThreshExceeded`				
	`mplsL3VpnNum VrfRouteMax ThreshCleared`				
Notificaciones VRRP					
RFC 2787, Definiciones de objetos administrados	`vrrpTrapNewMaster`	1.3.6.1.2.1.68.0.1	Advertencia	VRRPD_NEWMASTER_TRAMPA	Todos los dispositivos que ejecutan Junos OS.

Tabla 44: Capturas SNMP versión 2 compatibles con estándar *(Continued)*

Definido en	Nombre de la trampa	snmpTrapOID	Nivel de gravedad del registro del sistema	Etiqueta syslog	Admitido en
para el protocolo de redundancia de enrutador virtual	`vrrpTrapAuthFailure`	1.3.6.1.2.1.68.0.2	Advertencia	VRRPD_AUTH_FAILURE_TRAMPA	Todos los dispositivos que ejecutan Junos OS.
RFC 6527, Definiciones de objetos administrados para el protocolo de redundancia de enrutador virtual versión 3 (VRRPv3)	`vrrpv3NewMaster`	1.3.6.1.2.1.207.0.1	Advertencia	VRRPD_NEW_MASTER	M y MX
	`vrrpv3ProtoError`	1.3.6.1.2.1.207.0.2	Advertencia	VRRPD_V3_PROTO_ERROR	M y MX

SEE ALSO

Configurar opciones y grupos de capturas SNMP en un dispositivo que ejecute Junos OS

No Link Title

MIB SNMP personalizadas para capturas syslog

in this section

- Descripción general de las MIB SNMP personalizadas | **521**
- Definir una MIB personalizada para una captura syslog | **523**

- Limitaciones del uso de capturas SNMP personalizadas | 530
- Ejemplo de captura de syslog personalizada | 530

Las capturas syslog de SNMP son mensajes de alerta enviados desde un dispositivo remoto habilitado para SNMP a un recopilador central en los que se le notifica un fallo de componente o cuando los recursos críticos están fuera de los límites configurables. Esta información se captura en una base de información de gestión (MIB). La MIB de registro del sistema específica para empresas de Juniper Networks permite notificar a una aplicación basada en capturas SNMP cuando se produce un mensaje de registro del sistema importante. La MIB se define para asignar la entrada syslog al OID genérico jnxSyslogTrap.

El OID jnxSyslogTrap es una captura basada en los registros generados en syslog. El proceso de eventos (eventd) supervisa syslog y, basándose en la instrucción de configuración de la política de eventos para eventos syslog, envía todos los eventos syslog a una MIB de captura genérica definida por syslog, que es jnxSyslogTrap.`raise-trap`

El uso de un OID MIB genérico es un inconveniente para los clientes que desean procesar valores OID de captura syslog para descubrir eventos específicos porque es imposible distinguir las alarmas que tienen el mismo OID. Pero a partir de Junos OS versión 18.3R1, puede asignar un OID personalizado a un registro determinado y cargarlo en el dispositivo de forma dinámica.

La ventaja de esta característica es que, dado que existe una manera de asignar OID específicos a diferentes tipos de eventos syslog, ahora puede supervisar eficazmente cada tipo diferente de evento syslog.

Descripción general de las MIB SNMP personalizadas

in this section

- Escribir el archivo MIB | 522
- Convertir a un archivo YANG | 522
- Comandos de CLI que se usarán para administrar archivos YANG | 522

Para crear una MIB SNMP personalizada para una captura syslog, debe completar las siguientes tareas:

- Escriba la MIB personalizada.
- Convierta el archivo MIB al formato YANG y copie el archivo YANG en el dispositivo.

- Cargue el archivo YANG en el dispositivo.

En las secciones siguientes se describen estos pasos.

Escribir el archivo MIB

Antes de poder asignar un registro determinado con un OID personalizado, debe escribir una MIB personalizada. Para evitar colisiones, debe definir los objetos MIB y las capturas sólo bajo las raíces reservadas que se muestran en .Tabla 9

Tabla 45: Raíces MIB para módulos MIB personalizados

Raíz	Description	OID
`.iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnxCustomMibRoot`	Módulo MIB personalizado	.1.3.6.1.4.1.2636.3.86
`.iso.org.dod.internet.private.enterprises.juniperMIB.jnxTraps.jnxCustomSyslogNotifications`	Notificación de captura personalizada	.1.3.6.1.4.1.2636.4.30

Convertir a un archivo YANG

Antes de cargar su definición MIB en el dispositivo, debe convertir el archivo MIB a formato YANG. La forma recomendada de convertir el archivo MIB en YANG es usar la herramienta smidump v0.5.0. La herramienta smidump es una aplicación de código abierto que se puede instalar en su computadora portátil (consulte https://www.ibr.cs.tu-bs.de/projects/libsmi/smidump.html).https://www.ibr.cs.tu-bs.de/projects/libsmi/smidump.html

Una vez que el archivo esté en formato YANG, debe copiarlo en el dispositivo. A continuación, mediante un comando de la CLI, se carga el en el proceso SNMP (snmpd). Luego se genera un archivo JSON correspondiente, que snmpd analiza y a partir de él construye la base de datos de la jerarquía OID. Si se encuentra alguna etiqueta desconocida, snmpd devuelve el mensaje de error apropiado.

Comandos de CLI que se usarán para administrar archivos YANG

Para cargar el módulo YANG en snmpd, utilice la opción con el comando:`snmprequest system yang add`

```
user@host> request system yang add snmp module yang-filename package package-name
```

El incluye la ruta absoluta.*`yang-filename`*

NOTA: Para ejecutar el comando, debe tener acceso de superusuario.`request system yang add`

Hay otros dos comandos para administrar archivos YANG en dispositivos: `show system yang package` y `request system yang delete`.

SEE ALSO

> *mostrar paquete yang del sistema*
>
> *sistema de solicitud yang delete*
>
> *sistema de solicitud yang add*

Definir una MIB personalizada para una captura syslog

En este procedimiento, usamos los siguientes archivos de ejemplo:

- Archivo MIB para convertir
- Salida

NOTA: Aunque YANG se puede escribir manualmente consultando el ejemplo de YANG proporcionado en esta documentación, le recomendamos que convierta el formato MIB a YANG utilizando la herramienta smidump v0.5.0.

Para definir una MIB personalizada para una captura syslog:

1. Cargue su MIB en el sistema de administración de red (NMS) y verifique si hay algún error.
2. Invoque la herramienta smidump mediante el siguiente comando, donde , , y son variables para nombres de archivo específicos:***dependency-mibinput-custom-mib-fileYANG-MODULE-NAME***

   ```
   $ smidump -p dependency-mib input-custom-mib-file -f yang -o YANG-MODULE-NAME.yang
   ```

   Por ejemplo:

   ```
   $ smidump -p mib-jnx-smi.txt mib-jnx-example-custom-syslog.txt -f yang -o JUNIPER-EXAMPLE-
   CUSTOM-SYSLOG-MIB.yang
   ```

Como salida, obtendrá el archivo YANG convertido **JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang.**

Observe que el archivo MIB personalizado de entrada depende de SNMPv2-SMI, JUNIPER-SMI e IF-MIB.**mib-jnx-example-custom-syslog.txt** Pero dado que SNMPv2-SMI e IF-MIB son MIB estándar, sus definiciones ya están presentes en smidump. Por lo tanto, el único archivo MIB dependiente requerido es , que tiene definiciones de módulo JUNIPER-SMI.**mib-jnx-smi.txt**

3. Copie el archivo en cualquier ruta del dispositivo y copie todos los archivos YANG dependientes en el dispositivo en la siguiente ruta de acceso:**JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang /opt/lib/python2.7/site-packages/pyang/modules**.

> **NOTA**: Debe convertir todas las MIB dependientes a archivos YANG y copiarlas en el dispositivo.

A continuación se presentan algunas de las MIB estándar que se han convertido a módulos YANG y están presentes en la ruta anterior:, , , , , , . **IANAifType-MIB.yangietf-yang-types.yangietf-inet-types.yangIF-MIB.yangJUNIPER-SMI.yangSNMPv2-TC.yang**

4. Con la CLI, cargue los módulos YANG en snmpd mediante este comando:

```
user@host> request system yang add snmp module yang-filename package package-name
```

Por ejemplo:

```
user@host> request system yang add snmp module /var/tmp/JUNIPER-EXAMPLE-CUSTOM-SYSLOG-
MIB.yang package p1
```

El módulo YANG se convierte al formato JSON y va a snmpd para analizar y crear la base de datos interna.

5. Para comprobar que la captura basada en syslog con las definiciones de captura recién agregadas está funcionando, suplantar (imitar) la captura. Puede hacerlo mediante la CLI o mediante una política de eventos. A continuación se muestra un ejemplo de suplantación de la captura mediante la CLI.

```
user@host> request snmp spoof-trap jnxExampleSyslogTrap?
Possible completions:
  <trap>               The name of the trap to spoof
  jnxExampleSyslogTrap1   (Dynamic)
  jnxExampleSyslogTrap2   (Dynamic)
  jnxExampleSyslogTrap3   (Dynamic)
```

```
user@host> request snmp spoof-trap jnxExampleSyslogTrap1
Spoof-trap request result: trap sent
successfully
```

mib-jnx-example-custom-syslog.txt

```
-- ******************************************************************
-- Juniper enterprise specific custom syslog MIB.
--
-- Copyright (c) 2002-2004, 2006, Juniper Networks, Inc.
-- All rights reserved.
--
-- The contents of this document are subject to change without notice.
-- ******************************************************************

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Integer32
        FROM SNMPv2-SMI
    jnxCustomMibRoot, jnxCustomSyslogNotifications
        FROM JUNIPER-SMI
    ifName
        FROM IF-MIB
;

jnxExampleCustomSyslog MODULE-IDENTITY
    LAST-UPDATED "201711270000Z"
    ORGANIZATION "Juniper Networks, Inc."
    CONTACT-INFO
            "Juniper Technical Assistance Center
             Juniper Networks, Inc.
             1133 Innovation Way
             Sunnyvale, CA 94089
             E-mail: support@juniper.net"
    DESCRIPTION
    "Example MIB objects for custom syslog"
    REVISION     "201711270000Z"
    DESCRIPTION
    "Initial draft"
    ::= { jnxCustomMibRoot 1 }
```

```
jnxExampleCustomSyslogMessage OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "The syslog message string."
        ::= { jnxExampleCustomSyslog 1 }

jnxExampleCustomSyslogInteger OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Example OID for adding custom Integer OID"
        ::= { jnxExampleCustomSyslog 2 }

jnxExampleSyslogTrap1 NOTIFICATION-TYPE
    OBJECTS { jnxExampleCustomSyslogMessage }
    STATUS  current
    DESCRIPTION
            "This TRAP is reserved to be sent when event 1 occurs"
    ::= { jnxCustomSyslogNotifications 1 }

jnxExampleSyslogTrap2 NOTIFICATION-TYPE
    OBJECTS { jnxExampleCustomSyslogInteger, jnxExampleCustomSyslogMessage }
    STATUS  current
    DESCRIPTION
            "This TRAP is reserved to be sent when event 2 occurs"
    ::= { jnxCustomSyslogNotifications 2 }

jnxExampleSyslogTrap3 NOTIFICATION-TYPE
    OBJECTS { ifName, jnxExampleCustomSyslogMessage }
    STATUS  current
    DESCRIPTION
            "This TRAP is reserved to be sent when event 3 occurs"
    ::= { jnxCustomSyslogNotifications 3 }

END
```

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB.yang

```
/*
 * This YANG module has been generated by smidump 0.5.0:
 *
 *      smidump -f yang JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB
 *
 * Do not edit. Edit the source file instead!
 */

module JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {

  namespace "urn:ietf:params:xml:ns:yang:smiv2:JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB";
  prefix "juniper-example";

  import IF-MIB {
    prefix "if-mib";
  }

  import JUNIPER-SMI {
    prefix "juniper-smi";
  }

  import ietf-yang-smiv2 {
    prefix "smiv2";
  }

  organization
   "Juniper Networks, Inc.";

  contact
   "Juniper Technical Assistance Center
    Juniper Networks, Inc.
    1133 Innovation Way
    Sunnyvale, CA 94089
    E-mail: support@juniper.net";

  description
   "Example MIB objects for custom syslog";

  revision 2017-11-27 {
    description
```

```
   "Initial draft";
}


container JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {
  config false;
}

notification jnxExampleSyslogTrap1 {
  description
   "This TRAP is reserved to be sent when event 1 occurs";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.1";

  container object-1 {

    leaf jnxExampleCustomSyslogMessage {
      type binary;
      description
       "The syslog message string.";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
  }
}

notification jnxExampleSyslogTrap2 {
  description
   "This TRAP is reserved to be sent when event 2 occurs";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.2";

  container object-1 {

    leaf jnxExampleCustomSyslogInteger {
      type int32;
      description
       "Example OID for adding custom Integer OID";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.2";
    }
  }

  container object-2 {
```

```
      leaf jnxExampleCustomSyslogMessage {
        type binary;
        description
         "The syslog message string.";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
      }
    }
  }

  notification jnxExampleSyslogTrap3 {
    description
     "This TRAP is reserved to be sent when event 3 occurs";
    smiv2:oid "1.3.6.1.4.1.2636.4.30.3";

    container object-1 {

      leaf ifIndex {
        type leafref {
          path "/if-mib:IF-MIB/if-mib:ifTable/if-mib:ifEntry/if-mib:ifIndex";
        }
      }

      leaf ifName {
        type leafref {
          path "/if-mib:IF-MIB/if-mib:ifTable/if-mib:ifEntry/if-mib:ifName";
        }
      }
    }

    container object-2 {

      leaf jnxExampleCustomSyslogMessage {
        type binary;
        description
         "The syslog message string.";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
      }
    }
  }

  smiv2:alias "jnxExampleCustomSyslog" {
```

```
    smiv2:oid "1.3.6.1.4.1.2636.3.86.1";
  }

}
```

Limitaciones del uso de capturas SNMP personalizadas

Tenga cuidado de escribir los scripts de eventos de tal manera que no activen capturas para syslogs que ocurren con frecuencia. Esta práctica evita introducir más carga en el dispositivo.

Si agrega un objeto cuyo tipo de acceso es o , ese objeto no estará disponible para sondeo en operaciones de sondeo snmpp como snmpget o snmpwalk; se tratará como tipo de acceso .`readonlyreadwritenotifyonly` Esto se debe a que esta característica sirve para agregar definiciones dinámicas de OID de TRAP al dispositivo, de modo que el cliente pueda escribir scripts para enviar capturas personalizadas para cada syslog. Tipos de acceso y son para sondeo SNMP, mientras que es para capturas.`readonlyreadwritenotifyonly`

Para MIB personalizadas, no se admite la definición de una tabla personalizada. Si desea enviar una captura que tiene un objeto table como varbind, utilice la tabla ya definida en las MIB de Junos en lugar de definir una tabla personalizada en la MIB personalizada.

El archivo YANG debe cargarse en todos los nodos del chasis y en los motores de enrutamiento por separado. El comando no lo copia automáticamente en el motor de enrutamiento de copia de seguridad.`request system yang add`

Ejemplo de captura de syslog personalizada

Este ejemplo de captura syslog personalizada ilustra un caso de uso en el que el operador desea recibir capturas cuando se produce alguna de las siguientes situaciones:

- Un usuario entra en el modo de configuración en la CLI (evento definido como)`ui_dbase_login_event`
- Un usuario realiza una confirmación (evento definido como) `ui_commit`

Antes de que se admitiera la característica de captura syslog personalizada, la única forma de hacerlo era usar jnxSyslogTrap, que tiene un OID fijo, para ambos eventos. Con la función de captura syslog personalizada, ahora puede generar capturas que tengan OID definidos de forma personalizada.

Para definir una captura syslog personalizada:

1. Utilice el archivo de ejemplo proporcionado y conviértalo en .JUNIPER-EXAMPLE-CUSTOM-SYSLOIG-MIB.yang

```
smidump -p mib-jnx-smi.txt mib-jnx-example-custom-syslog.txt -f yang -o JUNIPER-EXAMPLE-
CUSTOM-SYSLOG-MIB.yang
```

2. Copie el archivo YANG en su dispositivo.
3. Cargue el archivo SNMP YANG.

```
root@host> request system yang add snmp package p1 module ~/JUNIPER-EXAMPLE-CUSTOM-SYSLOG-
MIB.yang
```

4. Copie el script slax a para suplantar la trampa **./var/db/scripts/event**

   Por ui_dbase_login_event, configurará la captura enteredConfigMode que tiene el nombre de usuario varbind.

   Por ui_commit, configurará la captura configCommitted que tiene el comando username y un comentario como tres varbinds.
5. Configure la captura:

```
set event-options policy custom-trap events ui_dbase_login_event
set event-options policy custom-trap events ui_commit
set event-options policy custom-trap then event-script custom-trap.slax
set event-options event-script file custom-trap.slax
```

6. Habilite snmpd traceoptions y trap target para comprobar las capturas que se envían.

```
set snmp trap-group trap-group targets ip-address
set snmp traceoptions flag all
```

7. Compruebe que la trampa funciona.

Archivo MIB de ejemplo

```
-- ******************************************************************
-- Juniper enterprise specific custom syslog MIB.
--
-- Copyright (c) 2002-2004, 2006, Juniper Networks, Inc.
-- All rights reserved.
--
```

```
-- The contents of this document are subject to change without notice.
-- ******************************************************************

JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE
        FROM SNMPv2-SMI
    jnxCustomMibRoot, jnxCustomSyslogNotifications
        FROM JUNIPER-SMI
;

jnxExampleCustomSyslog MODULE-IDENTITY
    LAST-UPDATED "201806220000Z"
    ORGANIZATION "Juniper Networks, Inc."
    CONTACT-INFO
            "Juniper Technical Assistance Center
             Juniper Networks, Inc.
             1133 Innovation Way
             Sunnyvale, CA 94089
             E-mail: support@juniper.net"
    DESCRIPTION
    "Example MIB objects for custom syslog"
    REVISION     "201806220000Z"
    DESCRIPTION
    "Initial draft"
    ::= { jnxCustomMibRoot 1 }

username OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Username"
        ::= { jnxExampleCustomSyslog 1 }

command OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Executed command"
        ::= { jnxExampleCustomSyslog 2 }
```

```
comment OBJECT-TYPE
        SYNTAX      OCTET STRING
        MAX-ACCESS  accessible-for-notify
        STATUS      current
        DESCRIPTION
            "Additional comment"
        ::= { jnxExampleCustomSyslog 3 }

enteredConfigMode NOTIFICATION-TYPE
    OBJECTS { username }
    STATUS  current
    DESCRIPTION
            "This TRAP is sent when a user enteres config mode. "
    ::= { jnxCustomSyslogNotifications 1 }

configCommitted NOTIFICATION-TYPE
    OBJECTS { username, command, comment }
    STATUS  current
    DESCRIPTION
            "This TRAP is sent when a user does config commit"
    ::= { jnxCustomSyslogNotifications 2 }

END
```

Ejemplo de archivo convertido de YANG

```
/*
 * This YANG module has been generated by smidump 0.5.0:
 *
 *      smidump -f yang JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB
 *
 * Do not edit. Edit the source file instead!
 */

module JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {

  namespace "urn:ietf:params:xml:ns:yang:smiv2:JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB";
  prefix "juniper-example";

  import JUNIPER-SMI {
    prefix "juniper-smi";
```

```
}

import ietf-yang-smiv2 {
  prefix "smiv2";
}

organization
 "Juniper Networks, Inc.";

contact
 "Juniper Technical Assistance Center
  Juniper Networks, Inc.
  1133 Innovation Way
  Sunnyvale, CA 94089
  E-mail: support@juniper.net";

description
 "Example MIB objects for custom syslog";

revision 2018-06-22 {
  description
   "Initial draft";
}


container JUNIPER-EXAMPLE-CUSTOM-SYSLOG-MIB {
  config false;
}

notification enteredConfigMode {
  description
   "This TRAP is sent when a user enteres config mode. ";
  smiv2:oid "1.3.6.1.4.1.2636.4.30.1";

  container object-1 {

    leaf username {
      type binary;
      description
       "Username";
      smiv2:max-access "accessible-for-notify";
      smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
    }
```

```
    }
  }

  notification configCommitted {
    description
     "This TRAP is sent when a user does config commit";
    smiv2:oid "1.3.6.1.4.1.2636.4.30.2";

    container object-1 {

      leaf username {
        type binary;
        description
         "Username";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.1";
      }
    }

    container object-2 {

      leaf command {
        type binary;
        description
         "Executed command";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.2";
      }
    }

    container object-3 {

      leaf comment {
        type binary;
        description
         "Additional comment";
        smiv2:max-access "accessible-for-notify";
        smiv2:oid "1.3.6.1.4.1.2636.3.86.1.3";
      }
    }
  }

  smiv2:alias "jnxExampleCustomSyslog" {
```

```
    smiv2:oid "1.3.6.1.4.1.2636.3.86.1";
  }

}
```

slax Script cutom_trap.slax (en /var/db/scripts/event)

```
version 1.0;
ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";
import "../import/junos.xsl";
match / {
    <event-script-results> {
        expr jcs:syslog("external.warning",event-script-input/trigger-event/id);
        var $id = event-script-input/trigger-event/id;
        if ($id == 'UI_DBASE_LOGIN_EVENT'){
            var $committing-user = event-script-input/trigger-event/attribute-list/
attribute[name=="username"]/value;
            var $requestSnmpTrap = <request-snmp-spoof-trap> {
                <trap> "enteredConfigMode";
                <variable-bindings>
                    "username=" _ $committing-user;
            }
            var $snmpTrapResults = jcs:invoke( $requestSnmpTrap );
        }
        else if ($id == 'UI_COMMIT'){
           var $committing-user = event-script-input/trigger-event/attribute-list/
attribute[name=="username"]/value;
           var $committing-command = event-script-input/trigger-event/attribute-list/
attribute[name=="command"]/value;
           var $committing-comment = event-script-input/trigger-event/attribute-list/
attribute[name=="message"]/value;

            var $requestSnmpTrap = <request-snmp-spoof-trap> {
                <trap> "configCommitted";
                <variable-bindings>
                    "username=" _ $committing-user _ ", command=" _ $committing-command _ ",
comment=" _ $committing-comment;
            }
            var $snmpTrapResults = jcs:invoke( $requestSnmpTrap );
        }
```

```
    }
}
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
20.1R1	A partir de Junos OS versión 20.1, después de un cambio correcto del motor de enrutamiento (GRES), el nuevo motor de enrutamiento principal envía una única notificación warmStart.

Rastrear actividad SNMP

in this section

- Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS | **538**
- Rastrear la actividad SNMP en un dispositivo que ejecuta Junos OS | **541**
- Ejemplo: Seguimiento de la actividad SNMP | **546**
- Configurar la captura de caducidad del certificado | **546**
- Habilitar capturas de emparejamiento y de túnel IPsec | **547**

Supervise la actividad de SNMP y realice un seguimiento de los problemas que afectan el rendimiento de SNMP en un dispositivo que ejecuta Junos OS

in this section

- Compruebe si hay objetos MIB registrados con SNMPd | 538
- Seguimiento de la actividad SNMP | 539
- Supervisar estadísticas SNMP | 540
- Comprobar el uso de la CPU | 540
- Comprobar la respuesta del motor de reenvío de paquetes y del kernel | 540

En dispositivos Junos OS, puede ver la información sobre cómo supervisar la actividad de SNMP e identificar los problemas que afectan al rendimiento de SNMP:

Compruebe si hay objetos MIB registrados con SNMPd

Para acceder a datos relacionados con un objeto MIB, el objeto MIB debe estar registrado en el snmpd. Cuando un subagente SNMP está en línea, registra los objetos MIB asociados con el snmpd. El snmpd mantiene una asignación de los objetos y los subagentes con los que están asociados los objetos. Sin embargo, el intento de registro falla ocasionalmente y los objetos permanecen sin registrar con el snmpd hasta la próxima vez que el subagente se reinicie y registre correctamente los objetos.

Cuando un sistema de administración de red sondea datos relacionados con objetos que no están registrados con el snmpd, el snmpd devuelve un error (para objetos SNMPv1) o un error (para objetos SNMPv2).`noSuchNamenoSuchObject`

Puede utilizar los siguientes comandos para comprobar si hay objetos MIB registrados con el snmpd:

- : crea un archivo que contiene la lista de objetos registrados y su asignación a varios subagentes.`show snmp registered-objects/var/log/snmp_reg_objs`
- : muestra el contenido del archivo.`file show /var/log/snmp_reg_objs/var/log/snmp_reg_objs`

En el ejemplo siguiente se muestran los pasos para crear y mostrar el archivo:`/var/log/snmp_reg_objs`

```
user@host> show snmp registered-objects
user@host> file show /var/log/snmp_reg_objs
```

```
-----------------------------------------------------------
 Registered MIB Objects
 root_name =
-----------------------------------------------------------
.1.2.840.10006.300.43.1.1.1.1.2 (dot3adAggMACAddress) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.3 (dot3adAggActorSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.4 (dot3adAggActorSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.5 (dot3adAggAggregateOrIndividual) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.6 (dot3adAggActorAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.7 (dot3adAggActorOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.8 (dot3adAggPartnerSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.9 (dot3adAggPartnerSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.10 (dot3adAggPartnerOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.1.1.11 (dot3adAggCollectorMaxDelay) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.1.2.1.1 (dot3adAggPortListPorts) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.2 (dot3adAggPortActorSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.3 (dot3adAggPortActorSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.4 (dot3adAggPortActorAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.5 (dot3adAggPortActorOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.6 (dot3adAggPortPartnerAdminSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.7 (dot3adAggPortPartnerOperSystemPriority) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.8 (dot3adAggPortPartnerAdminSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.9 (dot3adAggPortPartnerOperSystemID) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.10 (dot3adAggPortPartnerAdminKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.11 (dot3adAggPortPartnerOperKey) (/var/run/mib2d-11)
.1.2.840.10006.300.43.1.2.1.1.12 (dot3adAggPortSelectedAggID) (/var/run/mib2d-11)
---(more)---
```

El archivo contiene objetos asociados a los procesos de Junos OS registrados en el snmpd.**/var/log/snmp_reg_objs** Puede ver los objetos mediante el comando.`show snmp registered-objects` Si un objeto MIB relacionado con un proceso de Junos OS que está en funcionamiento no se muestra en la lista de objetos registrados, es posible que desee reiniciar el proceso de software para volver a intentar el registro de objetos con el snmpd.

Seguimiento de la actividad SNMP

Las operaciones de rastreo SNMP rastrean la actividad de los agentes SNMP y registran la información en archivos de registro. De forma predeterminada, Junos OS no rastrea ninguna actividad SNMP. Para habilitar el seguimiento de las actividades de SNMP en un dispositivo que ejecuta Junos OS, incluya la instrucción en el nivel de jerarquía.`set traceoptions flag all[edit snmp]`

Se crean los siguientes archivos de registro:

- Snmpd

- mib2d
- rmopd

Puede utilizar el comando operativo para ver el contenido del archivo de registro.`show log log-filename` En el archivo de registro snmpd (consulte el ejemplo siguiente), una secuencia de representa un paquete entrante, mientras que una secuencia de representa un paquete saliente .>>><<< Puede usar las combinaciones de ID de origen y solicitud para hacer coincidir las solicitudes y las respuestas, si hay varios sistemas de administración de red sondeando el dispositivo al mismo tiempo. El registro de respuestas no se crea en el archivo de registro si el agente maestro SNMP o el subagente SNMP no han respondido a una solicitud.

Puede analizar el tiempo de solicitud-respuesta para identificar y comprender las respuestas retrasadas.

Puede revisar el archivo de registro mediante el comando.`show log snmpd`

Supervisar estadísticas SNMP

El comando operativo le ofrece una opción para revisar el tráfico SNMP, incluidas las capturas, en un dispositivo.`show snmp statistics extensive` El resultado del comando muestra valores en tiempo real y se puede usar para monitorear valores como caídas del acelerador, actualmente activo, máximo activo, no encontrado, tiempo de espera, latencia máxima, actual en cola, total en cola y desbordamientos.`show snmp statistics extensive` Puede identificar la lentitud en las respuestas SNMP supervisando el recuento actualmente activo, ya que un aumento constante en el recuento actualmente activo está directamente relacionado con una respuesta lenta o nula a las solicitudes SNMP.

Comprobar el uso de la CPU

El alto uso de CPU de los procesos de software que se están consultando, como snmpd o mib2d, es otro factor que puede conducir a una respuesta lenta o ninguna respuesta. Puede utilizar el comando operativo para comprobar los niveles de uso de CPU de los procesos de Junos OS.`show system processes extensive`

Comprobar la respuesta del motor de reenvío de paquetes y del kernel

Como se mencionó en , algunos datos SNMP MIB son mantenidos por el kernel o el motor de reenvío de paquetes."Descripción de la implementación de SNMP en Junos OS" en la página 388 Para que dichos datos estén disponibles para el sistema de administración de red, el núcleo tiene que proporcionar la información requerida al subagente SNMP en mib2d. Una respuesta lenta del kernel puede causar un retraso en mib2d que devuelve los datos al sistema de administración de red. Junos OS agrega una entrada al archivo de registro mib2d cada vez que una interfaz tarda más de 10.000 microsegundos en responder a una solicitud de estadísticas de interfaz. Puede usar el comando para averiguar el tiempo de respuesta que tarda el kernel.`show log log-filename | grep “kernel response time”`

Comprobación del tiempo de respuesta del kernel

```
user@host> show log mib2d | grep “kernel response time”
 Aug 17 22:39:37  == kernel response time for
 COS_IPVPN_DEFAULT_OUTPUT-t1-7/3/0:10:27.0-o: 9.126471 sec, range
 (0.000007, 11.000806)

 Aug 17 22:39:53  == kernel response time for
 COS_IPVPN_DEFAULT_INPUT-t1-7/2/0:5:15.0-i: 5.387321 sec, range
 (0.000007, 11.000806)

 Aug 17 22:39:53  == kernel response time for ct1-6/1/0:9:15: 0.695406
 sec, range (0.000007, 11.000806)

 Aug 17 22:40:04  == kernel response time for t1-6/3/0:6:19: 1.878542
 sec, range (0.000007, 11.000806)

 Aug 17 22:40:22  == kernel response time for lsq-7/0/0: 2.556592 sec,
 range (0.000007, 11.000806)
```

Rastrear la actividad SNMP en un dispositivo que ejecuta Junos OS

in this section

- Configurar el número y el tamaño de los archivos de registro SNMP | **543**
- Configurar el acceso al archivo de registro | **543**
- Configurar una expresión regular para las líneas que se van a registrar | **544**
- Configurar las operaciones de seguimiento | **544**

Las operaciones de rastreo de SNMP rastrean la actividad de los agentes SNMP y registran la información en archivos de registro. Las descripciones de errores registradas proporcionan información detallada para resolver problemas.

De forma predeterminada, Junos OS no rastrea ninguna actividad SNMP. Si incluye la instrucción en el nivel de jerarquía, el comportamiento de seguimiento predeterminado es:`traceoptions[edit snmp]`

- Las actividades importantes se registran en archivos ubicados en el directorio.**/var/log** Cada registro lleva el nombre del agente SNMP que lo genera. Actualmente, se crean los siguientes archivos de registro en el directorio cuando se utiliza la instrucción:**/var/log**`traceoptions`
  - chasis
  - Artesanía
  - ilmid
  - mib2d
  - rmopd
  - Serviced
  - Snmpd
- Cuando un archivo de seguimiento denominado alcanza su tamaño máximo, se le cambia el nombre , luego , y así sucesivamente, hasta que se alcanza el número máximo de archivos de seguimiento.***filenamefilename*.0*filename*.1** A continuación, se sobrescribe el archivo de seguimiento más antiguo. (Para obtener más información acerca de cómo se crean los archivos de registro, consulte el Explorador de registros del sistema).https://apps.juniper.net/syslog-explorer/
- Solo puede tener acceso a los archivos de registro el usuario que configuró la operación de seguimiento.

No puede cambiar el directorio () en el que se encuentran los archivos de seguimiento.**/var/log** Sin embargo, puede personalizar las demás configuraciones del archivo de seguimiento incluyendo las siguientes instrucciones en el nivel de jerarquía:`[edit snmp]`

```
[edit snmp]
traceoptions {
    file <files number> <match regular-expression> <size size> <world-readable | no-world-
readable>;
    flag flag;
    memory-trace;
    no-remote-trace;
    no-default-memory-trace;
}
```

Estas declaraciones se describen en las secciones siguientes:

Configurar el número y el tamaño de los archivos de registro SNMP

De forma predeterminada, cuando el archivo de seguimiento alcanza los 128 kilobytes (KB) de tamaño, se le cambia el nombre , luego , y así sucesivamente, hasta que haya tres archivos de seguimiento.***filename*.0*filename*.1** A continuación, se sobrescribe el archivo de seguimiento () más antiguo.***filename*.2**

Puede configurar los límites del número y tamaño de los archivos de seguimiento incluyendo las siguientes instrucciones en el nivel de jerarquía:`[edit snmp traceoptions]`

```
[edit snmp traceoptions]
file files number size size;
```

Por ejemplo, establezca el tamaño máximo de archivo en 2 MB y el número máximo de archivos en 20. Cuando el archivo que recibe el resultado de la operación de seguimiento () alcanza los 2 MB, se cambia el nombre y se crea un nuevo archivo llamado .***filenamefilenamefilename*.0*filename*** Cuando el nuevo alcanza los 2 MB, se cambia el nombre y se le cambia el nombre .***filenamefilename*.0*filename*.1*filenamefilename*.0** Este proceso se repite hasta que haya 20 archivos de seguimiento. A continuación, el archivo más antiguo () se sobrescribe con el archivo más reciente ().***filename*.19*filename*.0**

El número de archivos puede ser de 2 a 1000 archivos. El tamaño de cada archivo puede ser de 10 KB a 1 gigabyte (GB).

Configurar el acceso al archivo de registro

De forma predeterminada, solo puede tener acceso a los archivos de registro el usuario que configuró la operación de seguimiento.

Para especificar que cualquier usuario pueda leer todos los archivos de registro, incluya la instrucción en el nivel de jerarquía:`file world-readable[edit snmp traceoptions]`

```
[edit snmp traceoptions]
file world-readable;
```

Para establecer explícitamente el comportamiento predeterminado, incluya la instrucción en el nivel de jerarquía:`file no-world-readable[edit snmp traceoptions]`

```
[edit snmp traceoptions]
file no-world-readable;
```

Configurar una expresión regular para las líneas que se van a registrar

De forma predeterminada, el resultado de la operación de seguimiento incluye todas las líneas relevantes para las actividades registradas.

Puede refinar el resultado incluyendo la instrucción en el nivel de jerarquía y especificando una expresión regular (regex) para que coincida:`match`[`edit snmp traceoptions file` *`filename`*]

```
[edit snmp traceoptions]
file filename match regular-expression;
```

Configurar las operaciones de seguimiento

De forma predeterminada, solo se registran las actividades importantes. Puede especificar qué operaciones de seguimiento se registrarán incluyendo la siguiente instrucción (con uno o más indicadores de seguimiento) en el nivel de jerarquía:`flag`[`edit snmp traceoptions`]

```
[edit snmp traceoptions]
flag {
    all;
    configuration;
    database;
    events;
    general;
    interface-stats;
    nonvolatile-sets;
    pdu;
    policy;
    protocol-timeouts;
    routing-socket;
    server;
    subagent;
    timer;
    varbind-error;
}
```

Tabla 46 en la página 545 describe el significado de los indicadores de seguimiento SNMP.

Tabla 46: Indicadores de rastreo SNMP

Bandera	Description	Configuración predeterminada
`all`	Registre todas las operaciones.	Desactivado
`configuration`	Lectura de registros de la configuración en el nivel jerárquico.`[edit snmp]`	Desactivado
`database`	Registre los eventos que implican almacenamiento y recuperación en la base de datos de eventos.	Desactivado
`events`	Registre eventos importantes.	Desactivado
`general`	Registrar eventos generales.	Desactivado
`interface-stats`	Registrar estadísticas de interfaz física y lógica.	Desactivado
`nonvolatile-set`	Registre el manejo de solicitudes de conjunto SNMP no volátil.	Desactivado
`pdu`	Registre los paquetes de solicitud y respuesta SNMP.	Desactivado
`policy`	Procesamiento de políticas de registro.	Desactivado
`protocol-timeouts`	Registre los tiempos de espera de respuesta SNMP.	Desactivado
`routing-socket`	Registrar llamadas de socket de enrutamiento.	Desactivado
`server`	Registre la comunicación con los procesos que generan eventos.	Desactivado
`subagent`	Se reinicia el subagente de registro.	Desactivado

Tabla 46: Indicadores de rastreo SNMP *(Continued)*

Bandera	Description	Configuración predeterminada
`timer`	Registrar eventos del temporizador interno.	Desactivado
`varbind-error`	Registrar errores de enlace de variables.	Desactivado

Para mostrar el final del registro de un agente, ejecute el comando de modo operativo:`show log` *`agent`*`d | last`

```
[edit]
user@host# run show log agentd | last
```

donde es el nombre de un agente SNMP.*`agent`*

Ejemplo: Seguimiento de la actividad SNMP

Información de seguimiento de los paquetes SNMP:

```
[edit]
snmp {
    traceoptions {
        file size 10k files 5;
        flag pdu;
        flag protocol-timeouts;
        flag varbind-error;
    }
}
```

Configurar la captura de caducidad del certificado

Antes de empezar:

- Comprender cómo funcionan los certificados en VPN. Lea Descripción de las cadenas de certificados.

En este tema se muestra cómo configurar la captura de caducidad del certificado y cómo configurar el número de días anteriores para generar la captura.

1. Configure el número de días anteriores para generar la captura para todos los certificados.

```
user@host# set security pki trap all-certificates number-of-days
```

2. Configure el número de días antes para generar la captura para el certificado de CA.

```
user@host# set security pki trap ca-identity ca-profile-name number-of-days
```

3. Configure el número de días antes para generar la captura para el certificado local.

```
user@host# set security pki trap certificate-idcertificate-id-name number-of-days
```

4. Confirme la configuración introduciendo el comando.`show security pki trap`

```
user@host# show security pki trap
certificate-id crt_spk1 {
    30;
}
ca-identity Root-CA {
    30;
}
all-certificates {
    30;
}
```

SEE ALSO

trap (Security PKI)

Mostrar estadísticas de seguridad IPsec

Habilitar capturas de emparejamiento y de túnel IPsec

En este tema se muestra cómo habilitar y capturar.`peer-downipsec-tunnel-down`

1. Habilite el emparejamiento de captura IKE. La captura se genera cuando el par está inactivo.

```
user@host# set security ike trap peer-down
```

2. Habilite el túnel IPsec de captura IKE hacia abajo. La captura se genera cuando el par está activo y la SA de IPsec está inactiva.

```
user@host# set security ike trap ipsec-tunnel-down
```

3. Confirme la configuración introduciendo el comando.`show security ike trap`

```
user@host# show security ike trap
ipsec-tunnel-down;
peer-down;
```

SEE ALSO

> *trap (Security PKI)*
>
> *Mostrar estadísticas de seguridad IPsec*

Privilegios de acceso para un grupo SNMP

in this section

- Configurar los privilegios de acceso concedidos a un grupo | **549**
- Ejemplo: Configurar los privilegios de acceso concedidos a un grupo | **553**
- Asignar modelo de seguridad y nombre de seguridad a un grupo | **554**
- Ejemplo: Configuración del grupo de seguridad | **556**

SNMP versión 3 (SNMPv3) usa el modelo de control de acceso basado en vista (VACM), que permite configurar los privilegios de acceso concedidos a un grupo. Puede controlar el acceso filtrando los objetos MIB disponibles para una operación específica a través de una vista predefinida. Las vistas se asignan para determinar los objetos visibles para las operaciones de lectura, escritura y notificación de un grupo determinado, utilizando un contexto determinado, un modelo de seguridad determinado (v1, v2c o usm) y un nivel de seguridad determinado (autenticado, privacidad o ninguno). Para obtener información acerca de cómo configurar vistas, consulte "Configurar vistas MIB" en la página 598.

El acceso de los usuarios a la información de administración se define en el nivel jerárquico .`[edit snmp v3 vacm]` Todo el control de acceso dentro de VACM opera en grupos, que son colecciones de usuarios definidas por USM o cadenas de comunidad como se definen en los modelos de seguridad SNMPv1 y SNMPv2c.

El término se refiere a estos usuarios finales genéricos.*security-name* El grupo al que pertenece un nombre de seguridad específico se configura en el nivel de jerarquía.`[edit snmp v3 vacm security-to-group]` Ese nombre de seguridad se puede asociar a un grupo definido en el nivel de jerarquía.`[edit snmp v3 vacm security-to-group]` Un grupo identifica una colección de usuarios SNMP que comparten la misma directiva de acceso. A continuación, defina los privilegios de acceso asociados a un grupo en el nivel jerárquico . `[edit snmp v3 vacm access]` Puede definir el acceso mediante vistas. Para cada grupo, puede aplicar diferentes vistas dependiendo de la operación SNMP; por ejemplo, leer (, , o) escribir (), notificaciones, el nivel de seguridad utilizado (autenticación, privacidad o ninguno) y el modelo de seguridad (v1, v2c o usm) utilizado en una solicitud SNMP.`getgetNextgetBulkset`

Los miembros de un grupo se configuran con la instrucción.`security-name` Para los paquetes v3 que usan USM, el nombre de seguridad es el mismo que el nombre de usuario. Para los paquetes SNMPv1 o SNMPv2c, el nombre de seguridad se determina en función de la cadena de comunidad. Los nombres de seguridad son específicos de un modelo de seguridad. Si también está configurando directivas de acceso VACM para paquetes SNMPv1 o SNMPv2c, debe asignar nombres de seguridad a grupos para cada modelo de seguridad (SNMPv1 o SNMPv2c) en el nivel jerárquico .`[edit snmp v3 vacm security-to-group]` También debe asociar un nombre de seguridad a una comunidad SNMP en el nivel jerárquico .`[edit snmp v3 snmp-community community-index]`

Para configurar los privilegios de acceso para un grupo SNMP, incluya instrucciones en el nivel de jerarquía.`[edit snmp v3 vacm]` Para obtener más información acerca de esta instrucción, consulte .*vacm*

Configurar los privilegios de acceso concedidos a un grupo

in this section

Configurar el grupo | 550

- Configurar el modelo de seguridad | 550
- Configurar el nivel de seguridad | 551
- Asociar vistas MIB a un grupo de usuarios SNMP | 551

En este tema, se incluyen las siguientes secciones:

Configurar el grupo

Para configurar los privilegios de acceso concedidos a un grupo, incluya la instrucción en el nivel de jerarquía:`group[edit snmp v3 vacm access]`

```
[edit snmp v3 vacm access]
group group-name;
```

group-name es una colección de usuarios SNMP que pertenecen a una lista SNMP común que define una política de acceso. Los usuarios que pertenecen a un grupo SNMP determinado heredan todos los privilegios de acceso concedidos a ese grupo.

Configurar el modelo de seguridad

Para configurar el modelo de seguridad, incluya la instrucción en el nivel de jerarquía:`security-model[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)]`

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-
prefix)]
security-model (any | usm | v1 | v2c);
```

- `any`—Cualquier modelo de seguridad
- `usm`—Modelo de seguridad SNMPv3
- `v1`—Modelo de seguridad SNMPV1
- `v2c`—Modelo de seguridad SNMPv2c

Configurar el nivel de seguridad

Para configurar los privilegios de acceso concedidos a paquetes con un nivel de seguridad determinado, incluya la instrucción en el nivel de jerarquía:`security-level`[`edit snmp v3 vacm access group` *`group-name`* `(default-context-prefix | context-prefix` *`context-prefix`*`) security-model (any | usm | v1 | v2c)`]

```
[edit snmp v3 vacm access group group-name default-context-prefix security-model (any | usm | v1 |
v2c)]
security-level (authentication | none | privacy);
```

- `none`: no proporciona autenticación ni cifrado.
- `authentication`: proporciona autenticación, pero no cifrado.
- `privacy`: proporciona autenticación y cifrado.

Puede conceder privilegios de acceso a todos los paquetes con un nivel de seguridad igual o superior al configurado. Si está configurando el modelo de seguridad SNMPv1 o SNMPv2c, utilícelo como nivel de seguridad.`none` Si está configurando el modelo de seguridad SNMPv3 (USM), utilice el , o el nivel de seguridad.`authenticationnoneprivacy`

Asociar vistas MIB a un grupo de usuarios SNMP

in this section

- Configurar la vista de notificación | 552
- Configurar la vista de lectura | 552
- Configurar la vista de escritura | 552

Las vistas MIB definen privilegios de acceso para los miembros de un grupo. Puede aplicar vistas independientes para cada operación SNMP (lectura, escritura y notificación) dentro de cada modelo de seguridad (usm, v1 y v2c) y cada nivel de seguridad (autenticación, ninguno y privacidad) admitido por SNMP.

Para asociar vistas MIB a un grupo de usuarios SNMP, incluya las siguientes instrucciones en el nivel de jerarquía.`[edit snmp v3 vacm access group` *`group-name`* `(default-context-prefix | context-prefix` *`context-prefix`*`) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` Para obtener más información acerca de esta instrucción, consulte .*access (SNMP)*

Debe asociar al menos una vista (notificar, leer o escribir) en el nivel jerárquico .`[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]`

Debe configurar la vista MIB en el nivel de jerarquía.`[edit snmp view view-name]` Para obtener información acerca de cómo configurar vistas MIB, consulte Configurar vistas MIB."Configurar vistas MIB" en la página 598

En esta sección se describen los siguientes temas relacionados con esta configuración:

Configurar la vista de notificación

Para asociar el acceso de notificación con un grupo de usuarios SNMP, incluya la instrucción en el nivel de jerarquía.`notify-view[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` Para obtener más información acerca de esta instrucción, consulte .*notify-view*

`view-name` especifica el acceso de notificación, que es una lista de notificaciones que se pueden enviar a cada usuario de un grupo SNMP. Un nombre de vista no puede superar los 32 caracteres.

Configurar la vista de lectura

Para asociar una vista de lectura a un grupo SNMP, incluya la instrucción en el nivel jerárquico .`read-view[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` Para obtener más información acerca de esta instrucción, consulte .*read-view*

`view-name` especifica el acceso de lectura para un grupo de usuarios SNMP. Un nombre de vista no puede superar los 32 caracteres.

Configurar la vista de escritura

Para asociar una vista de escritura a un grupo de usuarios SNMP, incluya la instrucción en el nivel jerárquico .`write-view[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]` Para obtener más información acerca de esta instrucción, consulte .*write-view*

`view-name` especifica el acceso de escritura para un grupo de usuarios SNMP. Un nombre de vista no puede superar los 32 caracteres.

Ejemplo: Configurar los privilegios de acceso concedidos a un grupo

Defina los privilegios de acceso:

```
[edit snmp v3 vacm]
access {
    group group1 {
        default-context-prefix {
            security-model usm {            #Define an SNMPv3 security model
                security-level privacy {
                    notify-view nv1;
                    read-view rv1;
                    write-view wv1;
                }
            }
        }
        context-prefix lr1/ri1{ # routing instance ri1 in logical system lr1
            security-model usm {
                security-level privacy {
                    notify-view nv1;
                    read-view rv1;
                    write-view wv1;
                }
            }
        }
    }
    group group2 {
        default-context-prefix {
            security-model usm {            #Define an SNMPv3 security model
                security-level authentication {
                    read-view rv2;
                    write-view wv2;
                }
            }
        }
    }
    group group3 {
        default-context-prefix {
            security-model v1 {            #Define an SNMPv3 security model
                security-level none {
                    read-view rv3;
```

```
                    write-view wv3;
                }
            }
        }
    }
}
```

Asignar modelo de seguridad y nombre de seguridad a un grupo

in this section

- Configurar el modelo de seguridad | 554
- Asignar nombres de seguridad a grupos | 555
- Configurar el grupo | 555

Para asignar nombres de seguridad a grupos, incluya las siguientes instrucciones en el nivel jerárquico. `[edit snmp v3 vacm security-to-group]` Para obtener más información acerca de esta instrucción, consulte .*security-model (Group)*

En este tema, se incluyen las siguientes secciones:

Configurar el modelo de seguridad

Para configurar el modelo de seguridad, incluya la instrucción en el nivel de jerarquía:`security-model[edit snmp v3 vacm security-to-group]`

```
[edit snmp v3 vacm security-to-group]
security-model (usm | v1 | v2c);
```

- `usm`—Modelo de seguridad SNMPv3
- `v1`—Modelo de seguridad SNMPv1
- `v2c`—Modelo de seguridad SNMPv2

Asignar nombres de seguridad a grupos

Para asociar un nombre de seguridad a un usuario SNMPv3 o a una cadena de comunidad v1 o v2, incluya la instrucción en el nivel de jerarquía:`security-name`[`edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)`]

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
security-name security-name;
```

Para SNMPv3, es el nombre de usuario configurado en el nivel de jerarquía.*security-name*[`edit snmp v3 usm local-engine user` *username*] Para SNMPv1 y SNMPv2c, el nombre de seguridad es la cadena de comunidad configurada en el nivel de jerarquía.[`edit snmp v3 snmp-community` *community-index*] Para obtener información acerca de cómo configurar nombres de usuario, consulte Crear usuarios SNMPv3."Crear usuarios de SNMPv3" en la página 559 Para obtener información acerca de cómo configurar una cadena de comunidad, consulte Configurar comunidad SNMPv3."Configurar la comunidad SNMPv3" en la página 591

NOTA: El nombre de seguridad USM es independiente del nombre de seguridad SNMPv1 y SNMPv2c. Si admite SNMPv1 y SNMPv2c además de SNMPv3, debe configurar nombres de seguridad independientes dentro de la configuración de seguridad para grupo en el nivel jerárquico .[`edit snmp v3 vacm access`]

Configurar el grupo

Después de crear usuarios SNMPv3 o nombres de seguridad v1 o v2, asócielos a un grupo. Un grupo es un conjunto de nombres de seguridad que pertenecen a un modelo de seguridad determinado. Un grupo define los derechos de acceso para todos los usuarios que pertenecen a él. Los derechos de acceso definen lo que los objetos SNMP pueden leer, escribir o crear. Un grupo también define las notificaciones que puede recibir un usuario.

Si ya tiene un grupo configurado con todos los permisos de vista y acceso que desea conceder a un usuario, puede agregar el usuario a ese grupo. Si desea conceder a un usuario permisos de vista y acceso que ningún otro grupo tiene, o si no tiene ningún grupo configurado, cree un grupo y agréguelo a él.

Para configurar los privilegios de acceso concedidos a un grupo, incluya la instrucción en el nivel de jerarquía.`group`[`edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c) security-name` *security-name*] Para obtener más información acerca de esta instrucción, consulte .*group (Defining Access Privileges for an SNMPv3 Group)*

Ejemplo: Configuración del grupo de seguridad

Asigne nombres de seguridad a los grupos:

```
vacm {
    security-to-group {
        security-model usm {
            security-name user1 {
                group group1;
            }
            security-name user2 {
                group group2;
            }
            security-name user3 {
                group group3;
            }
        }
    }
}
```

Configurar ID de motor local en SNMPv3

De forma predeterminada, el ID del motor local utiliza la dirección IP predeterminada del enrutador. El ID del motor local es el identificador único desde el punto de vista administrativo del motor SNMPv3. Esta instrucción es opcional. Para configurar el ID del motor local, incluya la instrucción en el nivel de jerarquía.`engine-id`[`edit snmp`] Para obtener más información acerca de esta instrucción, consulte *.engine-id*

NOTA: Si utiliza SNMPv3 y si el ID del motor se basa en la dirección MAC y actualiza desde una versión anterior a una de las versiones (14.1X53-D50, 16.1R5, 17.1R2, 17.2R1, 15.1X53-D231, 14.1X53-D43, 15.1X53-D232), debe volver a configurar SNMPv3 porque la actualización cambia el ID del motor. Si no vuelve a configurar SNMPv3, verá un error de autenticación para el sondeo SNMPv3 porque el ID del motor se cambia después de la actualización. Solo necesita volver a configurar SNMPv3 en la primera actualización de este tipo. Si, a continuación, actualiza de una

de las versiones mencionadas a otra de estas versiones, no tiene que actualizar SNMPv3 de nuevo.

Para volver a configurar SNMPv3, utilice el procedimiento siguiente. No utilice el comando.`rollback 1`

1. Compruebe cuál es la configuración de SNMPv3.

```
user@host# show snmp v3
```

2. Elimine la configuración de SNMPv3.

```
user@host# delete snmp v3
```

3. Vuelva a configurar SNMPv3 (consulte la salida del paso 1).

El ID del motor local se define como el identificador único administrativo de un motor SNMPv3 y se utiliza para la identificación, no para el direccionamiento. Hay dos partes de un ID de motor: prefijo y sufijo. El prefijo tiene el formato de acuerdo con las especificaciones definidas en RFC 3411, Una arquitectura para describir marcos de administración del Protocolo simple de administración de red (SNMP). Puede configurar el sufijo aquí.

NOTA: Las claves de autenticación y cifrado SNMPv3 se generan en función de las contraseñas asociadas y del ID del motor. Si configura o cambia el ID del motor, debe confirmar el nuevo ID del motor antes de configurar los usuarios de SNMPv3. De lo contrario, las claves generadas a partir de las contraseñas configuradas se basan en el ID del motor anterior.

Para el ID del motor, recomendamos usar la dirección IP principal del dispositivo si el dispositivo tiene varios motores de enrutamiento y tiene configurada la dirección IP principal. Como alternativa, puede utilizar la dirección MAC del puerto de administración si el dispositivo solo tiene un motor de enrutamiento.

Configurar SNMPv3

in this section

- Crear usuarios de SNMPv3 | 559
- Configuración mínima de SNMPv3 en un dispositivo que ejecuta Junos OS | 559
- Ejemplo: Configuración de SNMPv3 | 561

El conmutador QFX3500 admite SNMP versión 3 (SNMPv3). SNMPv3 mejora la funcionalidad de SNMPv1 y SNMPv2c al admitir la autenticación de usuarios y el cifrado de datos. SNMPv3 usa el modelo de seguridad basado en el usuario (USM) para proporcionar seguridad a los mensajes SNMP y el modelo de control de acceso basado en la vista (VACM) para el control de acceso de los usuarios.

Las características de SNMPv3 incluyen:

- Con USM, los mensajes SNMP entre el administrador SNMP y el agente pueden tener el origen del mensaje autenticado y la integridad de los datos comprobada. USM reduce los retrasos de mensajería y las repeticiones de mensajes mediante la aplicación de límites de tiempo de espera y la comprobación de ID de solicitud de mensajes duplicados.

- VACM complementa USM proporcionando control de acceso de usuario para consultas SNMP al agente. Defina los privilegios de acceso que desea extender a un grupo de uno o más usuarios. Los privilegios de acceso vienen determinados por los parámetros del modelo de seguridad (, , o) y los parámetros de nivel de seguridad (, , o).`usmv1v2authenticationprivacynone` Para cada nivel de seguridad, debe asociar una vista MIB para el grupo. La asociación de una vista MIB con un grupo concede permiso de lectura, escritura o notificación a un conjunto de objetos MIB para el grupo.

- Los parámetros de seguridad se configuran para cada usuario, incluidos el nombre de usuario, el tipo de autenticación y la contraseña de autenticación, así como el tipo de privacidad y la contraseña de privacidad. El nombre de usuario asignado a cada usuario está en un formato que depende del modelo de seguridad configurado para ese usuario.

- Para garantizar la seguridad de la mensajería, se incluye otro tipo de nombre de usuario, denominado nombre de seguridad, en los datos de mensajería que se envían entre el servidor SNMP local y el servidor SNMP de destino. Cada nombre de usuario se asigna a un nombre de seguridad, pero el nombre de seguridad tiene un formato que es independiente del modelo de seguridad.

- Las entradas de captura en SNMPv3 se crean configurando los parámetros notify, notify filter, target address y target. La instrucción especifica el tipo de notificación (interrupción) y contiene una sola

etiqueta que define un conjunto de direcciones de destino para recibir una interrupción.`notify` El filtro de notificación define el acceso a una colección de identificadores de objetos de captura (OID). La dirección de destino define la dirección de una aplicación de administración SNMP y otros atributos utilizados en el envío de notificaciones. Los parámetros de destino definen el procesamiento de mensajes y los parámetros de seguridad utilizados para enviar notificaciones a un destino determinado.

Para configurar SNMPv3, realice las siguientes tareas:

- "Configurar vistas MIB" en la página 598
- "Privilegios de acceso para un grupo SNMP" en la página 548
- "Configurar capturas SNMPv3 en un dispositivo que ejecute Junos OS" en la página 568
- "Configurar SNMP Informa" en la página 575

Crear usuarios de SNMPv3

Para cada usuario SNMPv3, puede especificar el nombre de usuario, el tipo de autenticación, la contraseña de autenticación, el tipo de privacidad y la contraseña de privacidad. Después de que un usuario introduce una contraseña, se genera una clave basada en el ID del motor y la contraseña y se escribe en el archivo de configuración. Después de generar la clave, puede eliminar la contraseña de este archivo de configuración.

Solo puede configurar un tipo de cifrado para cada usuario SNMPv3.

Para crear usuarios, incluya la instrucción en el nivel jerárquico .`user`[`edit snmp v3 usm local-engine`]

Para configurar la autenticación y el cifrado de usuarios, incluya las siguientes instrucciones en el nivel de jerarquía.[`edit snmp v3 usm local-engine user` *`username`*]

Configuración mínima de SNMPv3 en un dispositivo que ejecuta Junos OS

Para configurar los requisitos mínimos para SNMPv3, incluya las siguientes instrucciones en los niveles de jerarquía y .[`edit snmp v3`][`edit snmp`]

Debe configurar al menos una vista (notificar, leer o escribir) en el nivel jerárquico .[`edit snmp view-name`]

1. Crear usuarios y configurar la autenticación.

```
user@host# set snmp v3 usm local-engine user superuser authentication-md5 authentication-
password 12345678
user@host#set snmp v3 usm local-engine user superuser privacy-aes128 privacy-password 12345678
```

2. Configurar privilegios de acceso a un grupo.

```
user@host# set snmp v3 vacm access group supergroup default-context-prefix security-model usm
security-level authentication context-match exact
user@host# set snmp v3 vacm access group supergroup default-context-prefix security-model usm
security-level authentication read-view readview
user@host# set snmp v3 vacm access group supergroup default-context-prefix security-model usm
security-level authentication write-view writeview
user@host# set snmp v3 vacm access group supergroup default-context-prefix security-model usm
security-level authentication notify-view notifyview
user@host# set snmp v3 vacm security-to-group security-model usm security-name superuser group
supergroup
```

3. (Opcional) Configure las propiedades de la dirección de destino a las que se envía la notificación de interrupción.

```
user@host# set snmp v3 target-address TA address <nms-ipaddress> tag-list trap_recv target-
parameters tp1
user@host# set snmp v3 target-parameters tp1 parameters message-processing-model v3 security-
model usm security-level authentication security-name superuser
user@host# set snmp v3 target-parameters tp1 notify-filter nfilter1
user@host# set snmp v3 notify-filter nfilter1 oid .1 include
user@host# set snmp v3 notify notify1 type trap tag trap_recv
```

4. Configure la vista SNMP para leer, escribir y notificar el acceso a la MIB.

```
user@host# set snmp view readview oid .1 include
user@host# set snmp view writeview oid .1 include
user@host# set snmp view notifyview oid .1 include
```

SEE ALSO

v3

Ejemplo: Configuración de SNMPv3

Defina una configuración de SNMPv3:

```
[edit snmp]
engine-id {
    use-mac-address;
}
view jnxAlarms {
    oid 1.3.6.1.4.1.2636.3.4 include;
}
view interfaces {
    oid 1.3.6.1.2.1.2 include;
}
view ping-mib {
    oid 1.3.6.1.2.1.80 include;
}
[edit snmp v3]
notify n1 {
    tag router1; # Identifies a set of target addresses
    type trap;# Defines type of notification
}
notify n2 {
    tag host1;
    type trap;
}
notify-filter nf1 {
    oid .1 include; # Defines which traps to send
} # In this case, includes all traps
notify-filter nf2 {
    oid 1.3.6.1.4.1 include; # Sends enterprise-specific traps only
}
notify-filter nf3 {
    oid 1.3.6.1.2.1.1.5 include; # Sends BGP traps only
}
snmp-community index1 {
    community-name "$9$JOZi.QF/AtOz3";  # SECRET-DATA
    security-name john; # Matches the security name at the target parameters
    tag host1; # Finds the addresses that are allowed to be used with
}
target-address ta1 {# Associates the target address with the group
```

```
                 # san-francisco.
    address 10.1.1.1;
    address-mask 255.255.255.0;  # Defines the range of addresses
    port 162;
    tag-list router1;
    target-parameters tp1;  # Applies configured target parameters
}
target-address ta2 {
    address 10.1.1.2;
    address-mask 255.255.255.0;
    port 162;
    tag-list host1;
    target-parameters tp2;
}
target-address ta3 {
    address 10.1.1.3;
    address-mask 255.255.255.0;
    port 162;
    tag-list “router1 host1”;
    target-parameters tp3;
}
target-parameters tp1 { # Defines the target parameters
    notify-filter nf1; # Specifies which notify filter to apply
    parameters {
        message-processing-model v1;
        security-model v1;
        security-level none;
        security-name john; # Matches the security name configured at the
    } # [edit snmp v3 snmp-community community-index hierarchy level.
}
target-parameters tp2 {
    notify-filter nf2;
    parameters {
        message-processing-model v1;
        security-model v1;
        security-level none;
        security-name john;
    }
}
target-parameters tp3 {
    notify-filter nf3;
    parameters {
        message-processing-model v1;
```

```
        security-model v1;
        security-level none;
        security-name john;
    }
}
usm {
    local-engine { # Defines authentication and encryption for SNMPv3 users
        user john { # security-name john is defined here
            authentication-md5 {
                authentication-password authentication-password;
            }
            privacy-des {
                privacy-password privacy-password;
            }
        }
        user bob { # security-name bob is defined here
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-none;
        }
        user julia { # security-name julia is defined here
            authentication-none;
            privacy-none;
        }
        user lauren { # security-name lauren is defined here
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-aes128 {
                privacy-password privacy-password;
            }
        }
        user richard { # security-name richard is defined here
            authentication-sha {
                authentication-password authentication-password;
            }
            privacy-none;
        }
    }
}
vacm {
    access {
```

```
        group san-francisco { #Defines the access privileges for the group
            default-context-prefix { # called san-francisco
                security-model v1 {
                    security-level none {
                        notify-view ping-mib;
                        read-view interfaces;
                        write-view jnxAlarms;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model v1 {
            security-name john { # Assigns john to security group san-fancisco
                group san-francisco;
            }
            security-name bob { # Assigns bob to security group new-york
                group new-york;
            }
            security-name julia {# Assigns julia to security group chicago
                group chicago;
            }
            security-name lauren {# Assigns lauren to security group paris
                group paris;
            }
            security-name richard {# Assigns richard to security group geneva
                group geneva;
            }
        }
    }
}
```

Configurar el tipo de autenticación SNMPv3 y el tipo de cifrado

in this section

- Configurar el tipo de autenticación SNMPv3 | 565
- Configurar el tipo de cifrado SNMPv3 | 566

Configurar el tipo de autenticación SNMPv3

in this section

- Configurar autenticación MD5 | 565
- Configurar autenticación SHA | 565
- Configurar sin autenticación | 566

De forma predeterminada, en una configuración de Junos OS, el tipo de autenticación SNMPv3 se establece en ninguno.

En este tema, se incluyen las siguientes secciones:

Configurar autenticación MD5

Para configurar el algoritmo de síntesis de mensajes (MD5) como tipo de autenticación para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`authentication-md5`[`edit snmp v3 usm local-engine user` *`username`*] Para obtener más información acerca de esta instrucción, consulte *.authentication-md5*

Configurar autenticación SHA

Puede configurar el siguiente algoritmo hash seguro (SHA) como tipo de autenticación para un usuario SNMPv3:

- `authentication-sha`

- `authentication-sha224`
- `authentication-sha256`

Para configurar el algoritmo hash seguro (SHA) como tipo de autenticación para un usuario SNMPv3, incluya la instrucción , en el nivel de jerarquía.`authentication-sha`[`edit snmp v3 usm local-engine user` *`username`*] Para obtener más información acerca de esta instrucción, consulte .*authentication-sha*

Para configurar el algoritmo hash seguro (SHA) como tipo de autenticación para un usuario SNMPv3, incluya el en el nivel de jerarquía.`authentication-sha224`[`edit snmp v3 usm local-engine user` *`username`*] Para obtener más información acerca de esta instrucción, consulte .*authentication-sha224*

Para configurar el algoritmo hash seguro (SHA) como tipo de autenticación para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`authentication-sha256`[`edit snmp v3 usm local-engine user` *`username`*] Para obtener más información acerca de esta instrucción, consulte .*authentication-sha256*

Configurar sin autenticación

Para no configurar ninguna autenticación para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`authentication-none`[`edit snmp v3 usm local-engine user` *`username`*] Para obtener más información acerca de esta instrucción, consulte .*authentication-none*

SEE ALSO

v3

Configurar el tipo de cifrado SNMPv3

in this section

- Configurar el algoritmo estándar de cifrado avanzado | **567**
- Configurar algoritmo de cifrado de datos | **567**
- Configurar Triple DES | **567**
- No configurar cifrado | **567**

De forma predeterminada, el cifrado se establece en ninguno.

Antes de configurar el cifrado, debe configurar la autenticación MD5 o SHA.

En este tema, se incluyen las siguientes secciones:

Configurar el algoritmo estándar de cifrado avanzado

Para configurar el algoritmo del estándar de cifrado avanzado (AES) para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`privacy-aes128[edit snmp v3 usm local-engine user *username*]` Para obtener más información acerca de esta instrucción, consulte *.privacy-aes128*

Configurar algoritmo de cifrado de datos

Para configurar el algoritmo de cifrado de datos (DES) para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`privacy-des[edit snmp v3 usm local-engine user *username*]` Para obtener más información acerca de esta instrucción, consulte *.privacy-des*

Configurar Triple DES

Para configurar el DES triple para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`privacy-3des[edit snmp v3 usm local-engine user *username*]` Para obtener más información acerca de esta instrucción, consulte *.privacy-3des*

No configurar cifrado

Para no configurar ningún cifrado para un usuario SNMPv3, incluya la instrucción en el nivel de jerarquía.`privacy-none[edit snmp v3 usm local-engine user *username*]` Para obtener más información acerca de esta instrucción, consulte *.privacy-none*

Capturas SNMPv3

in this section

- Configurar capturas SNMPv3 en un dispositivo que ejecute Junos OS | **568**
- Configurar la notificación de captura SNMPv3 | **568**
- Ejemplo: Configurar la notificación de captura SNMPv3 | **569**
- Configurar el filtro de notificación de captura | **569**
- Configuración de la dirección de destino de captura | **570**
- Ejemplo: Configurar la lista de etiquetas | **572**
- Definir y configurar los parámetros de destino de captura | **573**

En SNMPv3, se crean capturas e informes mediante la configuración de los parámetros, , y .`notifytarget-addresstarget-parameters` Las trampas son notificaciones no confirmadas, mientras que los informes son notificaciones confirmadas. En esta sección se describe cómo configurar capturas SNMP.

Configurar capturas SNMPv3 en un dispositivo que ejecute Junos OS

La dirección de destino define la dirección y los parámetros de una aplicación de administración utilizados en el envío de notificaciones. Los parámetros de destino definen los parámetros de procesamiento de mensajes y seguridad utilizados para enviar notificaciones a un destino de administración determinado. SNMPv3 también permite definir capturas SNMPv1 y SNMPv2c.

> **NOTA**: Cuando configure capturas SNMP, asegúrese de que los privilegios de acceso configurados permiten el envío de las capturas. Puede configurar privilegios de acceso en los niveles jerárquico y .`[edit snmp v3 vacm access][edit snmp v3 vacm security-to-group]`

Para obtener más información sobre la traducción de la captura SNMP v1 o v2 al OID y los detalles de las capturas enviadas por cada categoría, consulte el Explorador de MIB.https://apps.juniper.net/mib-explorer/

Configurar la notificación de captura SNMPv3

La instrucción especifica el tipo de notificación (interrupción) y contiene una sola etiqueta.`notify` La etiqueta define un conjunto de direcciones de destino para recibir una captura. La lista de etiquetas contiene una o más etiquetas y se configura en el nivel jerárquico .`[edit snmp v3 target-address` *`target-address-name`*`]` Si la lista de etiquetas contiene esta etiqueta, Junos OS envía una notificación a todas las direcciones de destino asociadas a esta etiqueta.

Para configurar las notificaciones de captura, incluya la instrucción en el nivel jerárquico .`notify[edit snmp v3]`

Cada nombre de entrada de notificación debe ser único.

Junos OS admite dos tipos de notificación: `trap` y `inform`.

SEE ALSO

v3

Ejemplo: Configurar la notificación de captura SNMPv3

Especifique tres conjuntos de destinos para enviar capturas:

```
[edit snmp v3]
notify n1 {
    tag router1;
    type trap;
}
notify n2 {
    tag router2;
    type trap
}
notify n3 {
    tag router3;
    type trap;
}
```

Configurar el filtro de notificación de captura

SNMPv3 utiliza el filtro de notificación para definir qué capturas (o qué objetos desde qué capturas) se envían al sistema de administración de red (NMS). El filtro de notificación de capturas limita el tipo de capturas que se envían al NMS.

Cada identificador de objeto representa un subárbol de la jerarquía de objetos MIB. Puede representar el subárbol mediante una secuencia de enteros punteados (como 1.3.6.1.2.1.2) o mediante su nombre de subárbol (como).`interfaces` También puede utilizar el asterisco de carácter comodín (*) en el identificador de objeto (OID) para especificar identificadores de objeto que coincidan con un patrón determinado.

Para configurar el filtro de notificaciones de capturas, incluya la instrucción en el nivel jerárquico .`notify-filter`[`edit snmp v3`]

De forma predeterminada, el OID se establece en .`include` Para definir el acceso a las capturas (u objetos de las capturas), incluya la instrucción en el nivel de jerarquía.`oid`[`edit snmp v3 notify-filter` *`profile-name`*] Para obtener más información acerca de esta instrucción, consulte .*notify-filter (Configuring the Profile Name)*

Configuración de la dirección de destino de captura

in this section

- Configurar la dirección | 571
- Configurar la máscara de dirección | 571
- Configurar el puerto | 571
- Configurar la instancia de enrutamiento | 571
- Configuración de la dirección de destino de captura | 571
- Aplicar parámetros de destino | 572

La dirección de destino define la dirección de una aplicación de administración y los parámetros que se utilizan para enviar notificaciones. También puede identificar estaciones de administración a las que se les permite usar cadenas de comunidad específicas. Cuando recibe un paquete con una cadena de comunidad reconocida y se asocia una etiqueta, Junos OS busca todas las direcciones de destino con esta etiqueta y comprueba que la dirección de origen de este paquete coincida con una de las direcciones de destino configuradas.

Debe configurar la máscara de dirección al configurar la comunidad SNMP.

Para especificar dónde desea que se envíen las capturas y definir qué paquetes SNMPv1 y SNMPv2cc están permitidos, incluya la instrucción en el nivel de jerarquía.`target-address`[`edit snmp v3`]

Para configurar las propiedades de la dirección de destino, incluya las siguientes instrucciones en el nivel de jerarquía:[`edit snmp v3 target-address` *`target-address-name`*]

A diferencia de SNMP v2, en SNMPv3 no hay ninguna opción de configuración para limitar el sondeo entrante. Sin embargo, puede configurar un filtro lo0 para limitar el sondeo entrante creando una regla que permita SNMP desde las IP del sistema de supervisión. Por ejemplo:

```
set policy-options prefix-list SNMP 10.1.1.1/32
set policy-options prefix-list SNMP 192.168.1.0/24

set firewall family inet filter CoPP term SNMP from source-prefix-list SNMP
set firewall family inet filter CoPP term SNMP from protocol udp
set firewall family inet filter CoPP term SNMP from destination-port snmp
set firewall family inet filter CoPP term SNMP then accept
```

```
set firewall family inet filter CoPP term SNMP then count SNMP
```

Configurar la dirección

Para configurar la dirección, incluya la instrucción en el nivel de jerarquía.`address`[`edit snmp v3 target-address` *`target-address-name`*] Para obtener más información acerca de esta instrucción, consulte .*address*

`address` es la dirección de destino SNMP.

Configurar la máscara de dirección

La máscara de direcciones especifica un conjunto de direcciones a las que se permite usar una cadena de comunidad y comprueba las direcciones de origen para un grupo de direcciones de destino.

Para configurar la máscara de dirección, incluya la instrucción en el nivel de jerarquía. .`address-mask`[`edit snmp v3 target-address` *`target-address-name`*]*address-mask*

`address-mask` combinado con la dirección define un rango de direcciones.

Configurar el puerto

De forma predeterminada, el puerto UDP se establece en 162. Para configurar un número de puerto diferente, incluya la instrucción en el nivel de jerarquía.`port`[`edit snmp v3 target-address` *`target-address-name`*] Para obtener más información acerca de esta instrucción, consulte .*port*

Configurar la instancia de enrutamiento

Las capturas se envían a través de la instancia de enrutamiento predeterminada. Para configurar la instancia de enrutamiento para enviar capturas, incluya la instrucción en el nivel de jerarquía.`routing-instance`[`edit snmp v3 target-address` *`target-address-name`*] Para obtener más información acerca de esta instrucción, consulte .*routing-instance*

Configuración de la dirección de destino de captura

Cada instrucción puede tener una o más etiquetas configuradas en su lista de etiquetas.`target-address` Cada etiqueta puede aparecer en más de una lista de etiquetas. Cuando se produce un evento significativo en el dispositivo de red, la lista de etiquetas identifica los destinos a los que se envía una notificación.

Para configurar la lista de etiquetas, incluya la instrucción en el nivel de jerarquía.`tag-list`[`edit snmp v3 target-address` *`target-address-name`*] Para obtener más información acerca de esta instrucción, consulte .*tag-list*

`tag-list` Especifica una o más etiquetas como una lista separada por espacios entre comillas dobles.

Cuando configure capturas SNMP, asegúrese de que los privilegios de acceso configurados permiten el envío de las capturas. Configure los privilegios de acceso en el nivel jerárquico .`[edit snmp v3 vacm access]`

Aplicar parámetros de destino

La instrucción en el nivel de jerarquía aplica los parámetros de destino configurados en el nivel de jerarquía.`target-parameters``[edit snmp v3]``[edit snmp v3 target-parameters *target-parameters-name*]`

Para hacer referencia a los parámetros de destino configurados, incluya la instrucción en el nivel de jerarquía:`target-parameters``[edit snmp v3 target-address *target-address-name*]`

Ejemplo: Configurar la lista de etiquetas

En el ejemplo siguiente, se definen dos entradas de etiqueta (y) en el nivel de jerarquía.`router1``router2``[edit snmp v3 notify *notify-name*]` Cuando un evento activa una notificación, Junos OS envía una captura a todas las direcciones de destino que tienen o configuradas en su lista de etiquetas de direcciones de destino.`router1``router2` Esto da como resultado que los dos primeros objetivos obtengan una trampa cada uno, y el tercer objetivo obtenga dos trampas.

```
[edit snmp v3]
notify n1 {
    tag router1; # Identifies a set of target addresses
    type trap; # Defines the type of notification
}
notify n2 {
    tag router2;
    type trap;
}
target-address ta1 {
    address 10.1.1.1;
    address-mask 255.255.255.0;
    port 162;
    tag-list router1;
    target-parameters tp1;
}
target-address ta2 {
    address 10.1.1.2;
    address-mask 255.255.255.0;
    port 162;
    tag-list router2;
    target-parameters tp2;
```

```
}
target-address ta3 {
    address 10.1.1.3;
    address-mask 255.255.255.0;
    port 162;
    tag-list “router1 router2”;  #Define multiple tags in the target address tag list
    target-parameters tp3;
}
```

Definir y configurar los parámetros de destino de captura

in this section

- Aplicar el filtro de notificación de captura | **573**
- Configurar los parámetros de destino | **574**

Los parámetros de destino definen el procesamiento de mensajes y los parámetros de seguridad que se utilizan para enviar notificaciones a un destino de administración determinado.

Para definir un conjunto de parámetros de destino, incluya la instrucción en el nivel de jerarquía:`target-parameters[edit snmp v3]`

Para obtener más información acerca de cómo configurar directivas de seguridad de suscriptores, consulte Descripción general de políticas de seguridad de suscriptores.*Subscriber Secure Policy Overview*

En este tema, se incluyen las siguientes secciones:

Aplicar el filtro de notificación de captura

Para aplicar el filtro de notificación de capturas, incluya la instrucción en el nivel jerárquico .`notify-filter[edit snmp v3 target-parameters` *`target-parameter-name`*`]` Para obtener más información acerca de esta instrucción, consulte .*notify-filter (Applying to the Management Target)*

Configurar los parámetros de destino

in this section

- Configurar el modelo de procesamiento de mensajes | 574
- Configurar el modelo de seguridad | 574
- Configurar el nivel de seguridad | 574
- Configurar el nombre de seguridad | 575

Para configurar las propiedades de los parámetros de destino, incluya las siguientes instrucciones en el nivel de jerarquía.`[edit snmp v3 target-parameters target-parameter-name parameters]`

Esta sección incluye los siguientes temas:

Configurar el modelo de procesamiento de mensajes

El modelo de procesamiento de mensajes define qué versión de SNMP se debe usar al generar notificaciones SNMP. Para configurar el modelo de procesamiento de mensajes, incluya la instrucción en el nivel de jerarquía.`message-processing-model`[`edit snmp v3 target-parameters target-parameter-name parameters`] Para obtener más información acerca de esta instrucción, consulte .*message-processing-model*

La política de seguridad de suscriptores de los enrutadores de la serie MX requiere el modelo de procesamiento de mensajes.`v3` Consulte Descripción general de la política de suscripción Secure.*Subscriber Secure Policy Overview*

Configurar el modelo de seguridad

Para definir el modelo de seguridad que se utilizará al generar notificaciones SNMP, incluya la instrucción en el nivel de jerarquía.`security-model`[`edit snmp v3 target-parameters target-parameter-name parameters`] Para obtener más información acerca de esta instrucción, consulte .*security-model (SNMP Notifications)*

La política de seguridad del suscriptor en los enrutadores de la serie MX requiere el modelo de seguridad.`usm` Consulte Descripción general de la política de suscripción Secure.*Subscriber Secure Policy Overview*

Configurar el nivel de seguridad

La instrucción especifica si la captura se autentica y cifra antes de enviarse.`security-level`

Para configurar el nivel de seguridad que se utilizará al generar notificaciones SNMP, incluya la instrucción en el nivel de jerarquía.`security-level`[`edit snmp v3 target-parameters` *`target-parameter-name`* `parameters`] Para obtener más información acerca de esta instrucción, consulte .*security-level (Generating SNMP Notifications)*

Si está configurando el modelo de seguridad SNMPv1 o SNMPV2c, utilícelo como nivel de seguridad.`none` Si está configurando el modelo de seguridad SNMPv3 (USM), utilice el nivel de seguridad o .`authenticationprivacy`

La política de seguridad del suscriptor en los enrutadores de la serie MX requiere el nivel de seguridad.`privacy` Consulte Descripción general de la política de seguridad del suscriptor para obtener más información.*Subscriber Secure Policy Overview*

Configurar el nombre de seguridad

Para configurar el nombre de seguridad que se utilizará al generar notificaciones SNMP, incluya la instrucción en el nivel de jerarquía.`security-name`[`edit snmp v3 target-parameters` *`target-parameter-name`* `parameters`] Para obtener más información acerca de esta instrucción, consulte .*security-name (SNMP Notifications)*

Si utiliza USM como modelo de seguridad, el identifica al usuario que se utiliza cuando se genera la notificación.`security-name` Si utiliza v1 o v2c como modelos de seguridad, identifica la comunidad SNMP utilizada cuando se genera la notificación.`security-name`

Los privilegios de acceso para el grupo asociado a un nombre de seguridad deben permitir el envío de esta notificación.

Si utiliza los modelos de seguridad v1 o v2, el nombre de seguridad en el nivel de jerarquía debe coincidir con el nombre de seguridad en el nivel de jerarquía.[`edit snmp v3 vacm security-to-group`][`edit snmp v3 snmp-community` *`community-index`*]

SNMPv3 informa

in this section

- Ejemplo: Configurar el tipo de notificación de informe y la dirección de destino | **577**
- Ejemplo: Configurar el ID del motor remoto y el usuario remoto | **578**

Junos OS admite dos tipos de notificaciones: atrapa e informa.

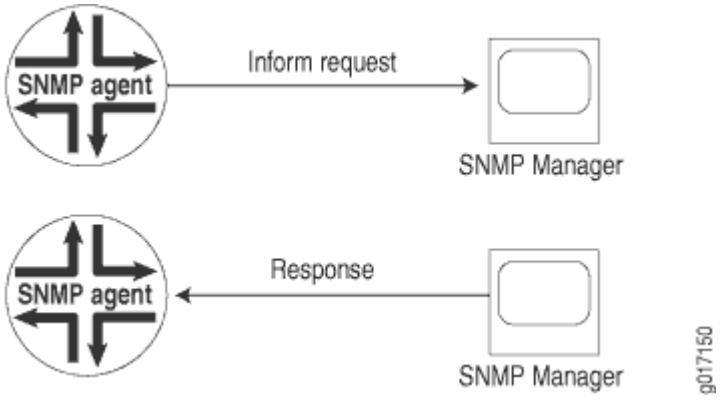
Con las trampas, el receptor no envía ningún acuse de recibo cuando recibe una trampa. Por lo tanto, el remitente no puede determinar si se recibió la captura. Es posible que se pierda una trampa porque se produjo un problema durante la transmisión. Para aumentar la confiabilidad, un informe es similar a una trampa, excepto que el informe se almacena y retransmite a intervalos regulares hasta que se produce una de estas condiciones:

- El receptor (destino) de la información devuelve un acuse de recibo al agente SNMP.
- Se ha intentado realizar un número determinado de retransmisiones fallidas y el agente descarta el mensaje de información.

Si el remitente nunca recibe una respuesta, el informe puede ser enviado de nuevo. Por lo tanto, es más probable que los informados lleguen a su destino previsto que las trampas. Los informadores utilizan el mismo canal de comunicaciones que las capturas (mismo socket y puerto) pero tienen diferentes tipos de unidades de datos de protocolo (PDU).

Los informes son más confiables que las trampas, pero consumen más recursos de red, enrutador y conmutador. A diferencia de una trampa, una información se mantiene en la memoria hasta que se recibe una respuesta o se alcanza el tiempo de espera. Además, las trampas se envían solo una vez, mientras que un informe puede volver a intentarse varias veces. Use informa cuándo es importante que el administrador SNMP reciba todas las notificaciones. Sin embargo, si le preocupa más el tráfico de red o la memoria del enrutador y del conmutador, use capturas.

Figura 23: Informar solicitud y respuesta



Ejemplo: Configurar el tipo de notificación de informe y la dirección de destino

En el ejemplo siguiente, el destino 172.17.20.184 está configurado para responder a los informes. El tiempo de espera de información es de 30 segundos y el recuento máximo de retransmisiones es de 3. El informe se envía a todos los destinos de la lista tl1. El modelo de seguridad para el usuario remoto es usm y el nombre de usuario del motor remoto es u10.

```
[edit snmp v3]
notify n1 {
    type inform;
    tag tl1;
}
notify-filter nf1 {
    oid .1.3 include;
}
target-address ta1 {
    address 172.17.20.184;
    retry-count 3;
    tag-list tl1;
    address-mask 255.255.255.0;
    target-parameters tp1;
    timeout 30;
}
target-parameters tp1 {
    parameters {
        message-processing-model v3;
        security-model usm;
        security-level privacy;
        security-name u10;
    }
    notify-filter nf1;
}
```

Ejemplo: Configurar el ID del motor remoto y el usuario remoto

in this section

- Requisitos | 578
- Descripción general | 578
- Configuración | 580
- Verificación | 581

En este ejemplo se muestra cómo configurar un motor remoto y un usuario remoto para que pueda recibir y responder a notificaciones de información SNMP. Las notificaciones de Inform se pueden autenticar y cifrar. También son más confiables que las trampas, otro tipo de notificación que admite Junos OS. A diferencia de las trampas, las notificaciones de información se almacenan y retransmiten a intervalos regulares hasta que se produce una de estas condiciones:

- El destino de la notificación de información devuelve una confirmación al agente SNMP.
- Se ha intentado un número determinado de retransmisiones infructuosas.

Requisitos

Esta función requiere el uso de contraseñas de texto sin formato válidas para SNMPv3. SNMPv3 tiene los siguientes requisitos al crear contraseñas de texto sin formato en un enrutador o un conmutador:

- La contraseña debe tener al menos ocho caracteres.
- La contraseña puede incluir caracteres alfabéticos, numéricos y especiales, pero no puede incluir caracteres de control.

Es mejor usar comillas para encerrar contraseñas, aunque no es necesario. Necesita comillas si la contraseña contiene espacios o, en el caso de ciertos caracteres especiales o signos de puntuación.

Descripción general

Las notificaciones Inform son compatibles con SNMPv3 para aumentar la confiabilidad. Por ejemplo, un agente SNMP que recibe una notificación de información acusa recibo.

Para las notificaciones de información, el ID de motor remoto identifica al agente SNMP en el dispositivo remoto donde reside el usuario, y el nombre de usuario identifica al usuario en un motor SNMP remoto que recibe las notificaciones de información.

Considere un escenario en el que tiene los valores en para usar en la configuración del ID de motor remoto y el usuario remoto en Tabla 47 en la página 579 este ejemplo.

Para enviar mensajes de información a un usuario SNMPv3 en un dispositivo remoto, primero debe especificar el identificador del motor para el agente SNMP en el dispositivo remoto donde reside el usuario. El ID del motor remoto se utiliza para calcular el resumen de seguridad para autenticar y cifrar los paquetes enviados a un usuario en el host remoto. Al enviar un mensaje de información, el agente utiliza las credenciales del usuario configuradas en el motor remoto (destino de información).

Para informa, es el identificador del agente SNMP en el dispositivo remoto donde reside el usuario.`remote-engine` *`engine-id`*

Para los informes, es el usuario en un motor SNMP remoto que recibe los informes.`user` *`username`*

Los informes generados pueden ser , , o , dependiendo del nivel de seguridad del usuario SNMPv3 configurado en el motor remoto (el receptor de información).`unauthenticatedauthenticatedauthenticated_and_encrypted` La clave de autenticación se utiliza para generar código de autenticación de mensajes (MAC). La clave de privacidad se utiliza para cifrar la parte del mensaje de la PDU de información.

Tabla 47: Valores que se van a utilizar en el ejemplo

Nombre de la variable	valor
username	u10
ID de motor remoto	800007E5804089071BC6D10A41
Tipo de autenticación	autenticación-md5
contraseña de autenticación	qol67R%?
Tipo de cifrado	privacidad-des
contraseña de privacidad	m*72Jl9v

Configuración

in this section

- Configuración rápida de CLI | 580
- Configuración del motor remoto y del usuario remoto | 580
- Resultados | 581

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos y péguelos en un archivo de texto, elimine los saltos de línea y cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue estos comandos en la CLI en el nivel de jerarquía y, a continuación, ingrese desde el modo de configuración.`[edit snmp v3]commit`

```
set usm remote-engine 800007E5804089071BC6D10A41 user u10 authentication-md5 authentication-
password "qol67R%?"
set usm remote-engine 800007E5804089071BC6D10A41 user u10 privacy-des privacy-password "m*72Jl9v"
```

Configuración del motor remoto y del usuario remoto

Procedimiento paso a paso

El ejemplo siguiente requiere que navegue a varios niveles en la jerarquía de configuración. Para obtener información acerca de cómo navegar por la CLI, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS.*Usar el editor de CLI en el modo de configuración*

Para configurar el ID del motor remoto y el usuario remoto:

1. Configure el ID del motor remoto, el nombre de usuario y el tipo de autenticación y la contraseña.

```
[edit snmp v3]
user@host# set usm remote-engine 800007E5804089071BC6D10A41 user u10 authentication-md5
authentication-password "qol67R%?"
```

2. Configure el tipo de cifrado y la contraseña de privacidad.

Solo puede configurar un tipo de cifrado por usuario SNMPv3.

```
[edit snmp v3]
user@host# set usm remote-engine 800007E5804089071BC6D10A41 user u10 privacy-des privacy-
password "m*72Jl9v"
```

Resultados

En el modo de configuración, confirme la configuración introduciendo el comando.`show` Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
[edit snmp v3]
user@ host# show
usm {
    remote-engine 800007E5804089071BC6D10A41 {
        user u10 {
            authentication-md5 {
                authentication-key "$9$hagSyKNdbY2acyvLN-2g69CtpBRhSvMX/CLx-
V4oZUjkqfQz69CuF36Apu1Idbw2ZUiHm3/C.mF/CA1IVws4oGkqf6CtzF";## SECRET-DATA
            }
            privacy-des {
                privacy-key "$9$GJDmf3nCtO1zFnCu0hcrevM87bs2oaUbwqmP5F3Ap0O1hrevMLxcSYgoaUDqmf5n/
Ap0REyk.BIREyr4aJZUHfTz9tu5T";## SECRET-DATA
            }
        }
    }
}
```

Después de haber confirmado que la configuración es correcta, ingrese `commit` en el modo de configuración.

Verificación

in this section

- Verificar la configuración del ID y el nombre de usuario del motor remoto | **582**

Verificar la configuración del ID y el nombre de usuario del motor remoto

Propósito

Verifique el estado del ID del motor y la información del usuario.

Acción

Muestra información sobre el ID y el usuario del motor SNMPv3.

```
user@host> show snmp v3
Local engine ID: 80 00 0a 4c 01 0a ff 03 e3
Engine boots:           3
Engine time:       769187 seconds
Max msg size:       65507 bytes

Engine ID: 80 00 07 e5 80 40 89 07 1b c6 d1 0a 41
    User                            Auth/Priv   Storage      Status
    u10                              md5/des    nonvolatile  active
```

Significado

El resultado muestra la siguiente información:

- ID del motor local y detalles sobre el motor
- ID remoto del motor (etiquetado)`Engine ID`
- Nombre de usuario
- Tipo de autenticación y tipo de cifrado (privacidad) configurados para el usuario
- Tipo de almacenamiento para el nombre de usuario, ya sea no volátil (configuración guardada) o volátil (no guardado)
- Estado del nuevo usuario; solo los usuarios con un estado activo pueden usar SNMPv3

SEE ALSO

Mostrar SNMP v3

Comunidades SNMP

in this section

- Configurar comunidades SNMP | 583
- Configurar cadena de comunidad SNMP | 589
- Ejemplos: Configurar la cadena de comunidad SNMP | 589
- Configurar la comunidad SNMPv3 | 591
- Ejemplo: Configurar la comunidad SNMPv3 | 593

Una comunidad SNMP define el nivel de autorización concedido a sus miembros, como los objetos MIB disponibles, las operaciones (de solo lectura o lectura-escritura) que son válidas para esos objetos y los clientes SNMP autorizados, en función de sus direcciones IP de origen.

Configurar comunidades SNMP

in this section

- Agregar un grupo de clientes a una comunidad SNMP | 587

Configurar el agente SNMP en Junos OS es una tarea sencilla que comparte la configuración familiar con otros dispositivos administrados de la red. Por ejemplo, debe configurar Junos OS con una cadena de comunidad SNMP y un destino para las capturas. Las cadenas de comunidad son nombres administrativos que agrupan colecciones de dispositivos y los agentes que se ejecutan en ellos juntos en dominios de administración comunes. Si un gerente y un agente comparten la misma comunidad, pueden comunicarse entre sí.

La cadena de comunidad SNMP define la relación entre un sistema servidor SNMP y el sistema cliente. Esta cadena es una contraseña para controlar el acceso del cliente al servidor.

Para crear una comunidad SNMP de solo lectura:

1. Ingrese la comunidad SNMP utilizada en su red.

   Si el nombre de la comunidad contiene espacios, escríbalo entre comillas (" ").

   Los nombres de las comunidades deben ser únicos.

   No puede configurar el mismo nombre de comunidad en los niveles de jerarquía y .`[edit snmp community]`[`edit snmp v3 snmp-community` *`community-index`*]

   ```
   [edit groups global]
   user@host# set snmp community name
   ```

   En este ejemplo se usa el nombre estándar para crear una comunidad que ofrece acceso limitado de solo lectura.`public`

   ```
   [edit groups global]
   user@host# set snmp community public
   ```

2. Defina el nivel de autorización para la comunidad.

   El nivel de autorización predeterminado para una comunidad es .`read-only`

   Para permitir solicitudes dentro de una comunidad, debe definir esa comunidad como .`Setauthorization read-write` Para las solicitudes, también debe incluir los objetos MIB específicos a los que se puede acceder con privilegios de lectura y escritura mediante la instrucción.`Setview` La vista predeterminada incluye todos los objetos MIB compatibles a los que se puede acceder con privilegios de solo lectura. No se puede acceder a ningún objeto MIB con privilegios de lectura y escritura. Para obtener más información acerca de la instrucción, vea Configurar vistas MIB.`view`"Configurar vistas MIB" en la página 598

   ```
   [edit groups global snmp community name]
   user@host# set authorization authorization
   ```

   En este ejemplo, se limita la comunidad pública al acceso de solo lectura. Cualquier cliente SNMP (por ejemplo, un sistema de gestión SNMP) que pertenezca a la comunidad pública puede leer variables MIB pero no puede establecerlas (cambiarlas).

   ```
   [edit groups global snmp community public]
   user@host# set authorization read-only
   ```

3. Defina una lista de clientes de la comunidad que están autorizados para comunicarse con el agente SNMP en Junos OS.

La instrucción enumera las direcciones IP de los clientes (miembros de la comunidad) a los que se les permite usar esta comunidad.`clients` Enumere los clientes por dirección IP y prefijo. Normalmente, la lista incluye el sistema de administración de red SNMP en su red o la dirección de su red de administración. Si no hay ninguna instrucción presente, se permiten todos los clientes.`clients` Para , debe especificar una dirección IPv4 o IPv6, no un nombre de host.*address*

```
[edit groups global snmp community name]
user@host# set clients address
```

La siguiente instrucción define los hosts de la red 192.168.1.0/24 como autorizados en la comunidad pública.

```
[edit groups global snmp community public]
user@host# set clients 192.168.1.0/24
```

4. Defina los clientes que no están autorizados dentro de la comunidad especificando su dirección IP, seguida de la instrucción.`restrict`

```
[edit groups global snmp community name]
user@host# set clients address resrict
```

La siguiente instrucción define todos los demás hosts como restringidos de la comunidad pública.

```
[edit groups global snmp community public]
user@host# set clients 0/0 restrict
```

5. En el nivel superior de la configuración, aplique el grupo de configuración.

   Si utiliza un grupo de configuración, debe aplicarlo para que surta efecto.

```
[edit]
user@host# set apply-groups global
```

6. Confirme la configuración.

```
user@host# commit
```

Para crear una comunidad SNMP de lectura y escritura:

1. Ingrese la comunidad SNMP utilizada en su red.

```
[edit groups global]
user@host# set snmp community name
```

En este ejemplo, se describe una cadena de comunidad estándar para identificar la comunidad a la que se concedió acceso de lectura y escritura al agente SNMP que se ejecuta en el dispositivo.`private`

```
[edit groups global]
user@host# set snmp community private
```

2. Defina el nivel de autorización para la comunidad.

```
[edit groups global snmp community name]
user@host# set authorization authorization
```

En este ejemplo, se limita la comunidad pública al acceso de solo lectura. Cualquier cliente SNMP (por ejemplo, un sistema de gestión SNMP) que pertenezca a la comunidad pública puede leer variables MIB pero no puede establecerlas (cambiarlas).

```
[edit groups global snmp community public]
user@host# set authorization read-write
```

3. Defina una lista de clientes de la comunidad que están autorizados a realizar cambios en el agente SNMP en Junos OS.

Enumere los clientes por dirección IP y prefijo.

```
[edit groups global snmp community name]
user@host# set clients address
```

Por ejemplo:

```
[edit groups global snmp community private]
user@host# set clients 192.168.1.15/24
user@host# set clients 192.168.1.18/24
```

4. Defina los clientes que no están autorizados dentro de la comunidad especificando su dirección IP, seguida de la instrucción.`restrict`

```
[edit groups global snmp community name]
user@host# set clients address resrict
```

La siguiente instrucción define todos los demás hosts como restringidos de la comunidad pública.

```
[edit groups global snmp community private]
user@host# set clients 0/0 restrict
```

5. En el nivel superior de la configuración, aplique el grupo de configuración.

   Si utiliza un grupo de configuración, debe aplicarlo para que surta efecto.

```
[edit]
user@host# set apply-groups global
```

6. Confirme la configuración.

```
user@host# commit
```

Agregar un grupo de clientes a una comunidad SNMP

Junos OS permite agregar uno o varios grupos de clientes a una comunidad SNMP. Puede incluir la instrucción en el nivel jerárquico para agregar todos los miembros de la lista de clientes o de la lista de prefijos a una comunidad SNMP.`client-list-name` *`name`*`[edit snmp community` *`community-name`*`]`

Para definir una lista de clientes, utilice la instrucción seguida de las direcciones IP de los clientes.`set snmp client-list` *`client-list-name`*

Puede configurar una lista de prefijos en el nivel jerárquico .`[edit policy options]` La compatibilidad con listas de prefijos en la configuración de la comunidad SNMP permite utilizar una sola lista para configurar las directivas SNMP y de enrutamiento. Para obtener más información acerca de la instrucción, consulte la Guía del usuario de directivas de enrutamiento, filtros de firewall y políticas de tráfico.`prefix-list`https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.html

Para agregar una lista de clientes o una lista de prefijos a una comunidad SNMP, utilice la instrucción.`set snmp commmunity` *`community-name`* `client-list-name`

La lista de clientes y la lista de prefijos no deben tener el mismo nombre.

En el ejemplo siguiente se muestra cómo definir una lista de clientes:

```
[edit]
snmp {
    client-list clentlist1 {
        10.1.1.1/32;
        10.2.2.2/32;
    }
}
```

En el ejemplo siguiente se muestra cómo agregar una lista de clientes a una comunidad SNMP:

```
[edit]
snmp {
    community community1 {
        authorization read-only;
        client-list-name clientlist1;
    }
}
```

En el ejemplo siguiente se muestra cómo agregar una lista de prefijos a una comunidad SNMP:

```
[edit]
policy-options {
    prefix-list prefixlist {
    10.3.3.3/32;
    10.5.5.5/32;
    }
}
snmp {
    community community2 {
    client-list-name prefixlist;
    }
}
```

Configurar cadena de comunidad SNMP

La cadena de comunidad SNMP define la relación entre un sistema servidor SNMP y el sistema cliente. Esta cadena actúa como una contraseña para controlar el acceso del cliente al servidor.

Para configurar una cadena de comunidad en una configuración de Junos OS, utilice la instrucción.`set snmp community`

Si el nombre de la comunidad contiene espacios, escríbalo entre comillas (" ").

El nivel de autorización predeterminado para una comunidad es .`read-only` Para permitir solicitudes dentro de una comunidad, debe definir esa comunidad como .`Setauthorization read-write` Para las solicitudes, también debe incluir los objetos MIB específicos a los que se puede acceder con privilegios de lectura y escritura mediante la instrucción.`Setview` La vista predeterminada incluye todos los objetos MIB compatibles a los que se puede acceder con privilegios de solo lectura; no se puede acceder a ningún objeto MIB con privilegios de lectura y escritura. Para obtener más información acerca de la instrucción, vea Configurar vistas MIB.`view`"Configurar vistas MIB" en la página 598

Las direcciones IP de los clientes (miembros de la comunidad) a los que se les permite usar esta comunidad se enumeran en las listas de instrucciones.`clients` Si no hay ninguna instrucción presente, se permiten todos los clientes.`clients` Para , debe especificar una dirección IPv4, no un nombre de host.*address* Incluya la opción de denegar el acceso a todos los clientes SNMP para los que no se haya concedido acceso.`default restrict` Se recomienda incluir siempre la opción de limitar el acceso del cliente SNMP al conmutador local.`default restrict`

Los nombres de comunidad deben ser únicos dentro de cada sistema SNMP.

SEE ALSO

community

Ejemplos: Configurar la cadena de comunidad SNMP

Conceda acceso de solo lectura a todos los clientes. Con la siguiente configuración, el sistema responde a SNMP , y a las solicitudes que contienen la cadena de comunidad:`GetGetNextGetBulkpublic`

```
[edit]
snmp {
    community public {
        authorization read-only;
```

```
    }
}
```

Conceda a todos los clientes acceso de lectura y escritura a ping MIB y .`jnxPingMIB` Con la siguiente configuración, el sistema responde a SNMP , , y a las solicitudes que contienen la cadena de comunidad y especifican un OID contenido en la MIB o jerarquía de ping:`GetGetNextGetBulkSetprivatejnxPingMIB`

```
[edit]
snmp {
    view ping-mib-view {
        oid pingMIB include;
        oid jnxPingMIB include;
        community private {
            authorization read-write;
            view ping-mib-view;
        }
    }
}
```

La siguiente configuración permite el acceso de sólo lectura a clientes con direcciones IP en el intervalo y deniega el acceso a los sistemas del intervalo :`1.2.3.4/24fe80::1:2:3:4/64`

```
[edit]
snmp {
    community field-service {
        authorization read-only;
        clients {
            default restrict; # Restrict access to all SNMP clients not explicitly
             # listed on the following lines.
            1.2.3.4/24; # Allow access by all clients in 1.2.3.4/24 except
            fe80::1:2:3:4/64 restrict;# fe80::1:2:3:4/64.
        }
    }
}
```

Configurar la comunidad SNMPv3

in this section

- Configuración del nombre de la comunidad | 592
- Configuración del contexto | 592
- Configuración de los nombres de seguridad | 593
- Configuración de la etiqueta | 593

La comunidad SNMP define la relación entre un sistema de servidor SNMP y los sistemas cliente. Esta instrucción es opcional.

Para configurar la comunidad SNMP, incluya la instrucción en el nivel jerárquico :`snmp-community`[`edit snmp v3`]

```
[edit snmp v3]
snmp-community community-index;
```

community-index es el índice de la comunidad SNMP.

Para configurar las propiedades de la comunidad SNMP, incluya las siguientes instrucciones en el nivel de jerarquía:[`edit snmp v3 snmp-community` *community-index*]

```
[edit snmp v3 snmp-community community-index]
community-name community-name;
context context-name;
security-name security-name;
tag tag-name;
```

A continuación se muestra un conjunto mínimo de configuración de ejemplo necesario para la configuración:`snmp v3 snmp-community`

```
set snmp v3 vacm security-to-group security-model v2c security-name NOSNMPV3 group SNMPV3GROUP
set snmp v3 vacm access group SNMPV3GROUP default-context-prefix security-model any security-
level none read-view SNMPVIEW
set snmp v3 vacm access group SNMPV3GROUP default-context-prefix security-model any security-
```

```
level none write-view SNMPVIEW
set snmp v3 snmp-community SNMPV3COMMUNITY community-name JTACCOMMUNITY
set snmp v3 snmp-community SNMPV3COMMUNITY security-name NOSNMPV3
set snmp view SNMPVIEW oid .1 include
```

NOTA: La comunidad utilizada por el usuario que no admite SNMPv3, seguirá utilizando SNMPv2.

Para obtener más información, consulte la siguiente configuración:

```
snmpget -v 2c -c JTACCOMMUNITY 10.52.170.100 sysUpTime.0
```

Esta sección incluye los siguientes temas:

Configuración del nombre de la comunidad

El nombre de la comunidad define la comunidad SNMP. La comunidad SNMP autoriza clientes SNMPv1 o SNMPv2c. Los privilegios de acceso asociados con el nombre de seguridad configurado definen qué objetos MIB están disponibles y las operaciones (lectura, escritura o notificación) permitidas en esos objetos.

Para configurar el nombre de comunidad SNMP, incluya la instrucción en el nivel jerárquico `.community-name[edit snmp v3 snmp-community community-index]` Para obtener más información acerca de esta instrucción, consulte *.community-name*

Configuración del contexto

Un contexto SNMP define una colección de información de administración a la que puede acceder una entidad SNMP. Normalmente, una entidad SNMP tiene acceso a varios contextos. Un contexto puede ser un sistema físico o lógico, una colección de varios sistemas o incluso un subconjunto de un sistema. Cada contexto en un dominio de administración tiene un identificador único.

Para configurar un contexto SNMP, incluya la instrucción en el nivel de jerarquía`.context context-name[edit snmp v3 snmp-community community-index]` Para obtener más información acerca de esta instrucción, consulte *.context (SNMPv3)*

NOTA: Para consultar una instancia de enrutamiento o un sistema lógico,

Configuración de los nombres de seguridad

Para asignar una cadena de comunidad a un nombre de seguridad, incluya la instrucción en el nivel de jerarquía:`security-name`[`edit snmp v3 snmp-community` *`community-index`*]

```
[edit snmp v3 snmp-community community-index]
security-name security-name;
```

`security-name` se utiliza cuando se configura el control de acceso. La configuración en el nivel de jerarquía identifica el grupo.`security-to-group`[`edit snmp v3 vacm`]

> **NOTA**: Este nombre de seguridad debe coincidir con el nombre de seguridad configurado en el nivel de jerarquía al configurar capturas.[`edit snmp v3 target-parameters` *`target-parameters-name`* `parameters`]

Configuración de la etiqueta

Para configurar la etiqueta, incluya la instrucción en el nivel de jerarquía.`tag`[`edit snmp v3 snmp-community` *`community-index`*] Para obtener más información acerca de esta instrucción, consulte *.tag*

Ejemplo: Configurar la comunidad SNMPv3

in this section

- Requisitos | 593
- Descripción general | 594
- Configuración | 594
- Verificación | 597

En este ejemplo se muestra cómo configurar una comunidad SNMPv3.

Requisitos

No se necesita ninguna configuración especial más allá de la inicialización del dispositivo antes de configurar este ejemplo.

Descripción general

En este ejemplo se muestra cómo crear una comunidad SNMPv3. Defina el nombre de la comunidad SNMP, especifique el nombre de seguridad para realizar el control de acceso y defina el nombre de la etiqueta que identifica la dirección de los administradores a los que se les permite usar una cadena de comunidad. La dirección de destino define la dirección de una aplicación de administración y los parámetros que se utilizan para enviar notificaciones.

Cuando el dispositivo recibe un paquete con una cadena de comunidad reconocida y se asocia una etiqueta a ese paquete, el software de Junos busca todas las direcciones de destino con esta etiqueta y comprueba que la dirección de origen de este paquete coincida con una de las direcciones de destino configuradas.

Especifique dónde desea que se envíen las capturas y defina qué paquetes SNMPv1 y SNMPv2c están permitidos. Especifique el nombre de la dirección de destino que identifica la dirección de destino, defina la dirección de destino, el intervalo de máscara de dirección, el número de puerto, la lista de etiquetas y el parámetro de destino.

Configuración

in this section

- Configuración rápida de CLI | **594**
- Procedimiento | **595**
- Resultados | **596**

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit snmp v3]` y, luego, ingrese `commit` desde el modo de configuración.

```
set snmp-community index1 community-name "public"
set snmp-community index1 security-name john
set snmp-community index1 tag router1
set target-address ta1 address 10.1.1.1
set target-address ta1 address-mask 255.255.255.0
set target-address ta1 port 162
```

```
set target-address ta1 tag-list router1
set target-address ta1 target-parameters tp1
```

Procedimiento

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .

1. Configure el nombre de la comunidad SNMP.

```
[edit snmp v3]
user@host# set snmp-community index1 community-name "public"
```

> **NOTA**: El nombre de la comunidad SNMP debe ser único.

2. Configure el nombre de seguridad para realizar el control de acceso.

```
[edit snmp v3]
user@host# set snmp-community index1 security-name john
```

3. Defina el nombre de la etiqueta. El nombre de la etiqueta identifica la dirección de los administradores a los que se les permite usar una cadena de comunidad.

```
[edit snmp v3]
user@host# set snmp-community index1 tag router1
```

4. Configure la dirección de destino SNMP.

```
[edit snmp v3]
user@host# set target-address ta1 address 10.1.1.1
```

5. Configure el intervalo de máscaras de la dirección para el control de acceso de cadenas de comunidad.

```
[edit snmp v3]
user@host#set target-address ta1 address-mask 255.255.255.0
```

6. Configure el número de puerto de destino SNMPv3.

```
[edit snmp v3]
user@host#set target-address ta1 port 162
```

7. Configure la lista de etiquetas SNMPv3 para seleccionar las direcciones de destino.

```
[edit snmp v3]
user@host#set target-address ta1 tag-list router1
```

8. Configure el nombre del parámetro de destino SNMPv3 en la tabla de parámetros de destino.

```
[edit snmp v3]
user@host#set target-address ta1 target-parameters tp1
```

Resultados

Desde el modo de configuración, confírmela con el comando `show snmp v3` . Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo.

```
[edit]
user@host# show snmp v3
target-address ta1 {
    address 10.1.1.1;
    port 162;
    tag-list router1;
    address-mask 255.255.255.0;
    target-parameters tp1;
}
snmp-community index1 {
    community-name "$9$JOZi.QF/AtOz3"; ## SECRET-DATA
    security-name john;
```

```
    tag router1;
}
```

Verificación

in this section

- Comprobación de la comunidad SNMPv3 | **597**

Comprobación de la comunidad SNMPv3

Propósito

Compruebe si la comunidad SNMPv3 está habilitada.

Acción

Para comprobar la configuración de la comunidad SNMPv3, escriba comando.`show snmp v3 community` Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
Community            Security  Context  Tag          Storage      Status
index1               john               router1      nonvolatile  active
```

Significado

El resultado muestra la información sobre la comunidad SNMPv3 que se habilita en el sistema.

Vistas MIB

in this section

- Configurar vistas MIB | 598
- Configurar MIB de proxy de ping | 599

SNMPv3 define el concepto de vistas MIB en RFC 3415, *Modelo de control de acceso basado en vistas (VACM) para el Protocolo simple de administración de redes (SNMP).* Las vistas MIB proporcionan a un agente un mejor control sobre quién puede acceder a ramas y objetos específicos dentro de su árbol MIB. Una vista consta de un nombre y una colección de identificadores de objeto SNMP, que se incluyen o excluyen explícitamente. Una vez definida, se asigna una vista a un grupo SNMPv3 o comunidad SNMPv1/v2c (o varias comunidades), enmascarando automáticamente a qué partes del árbol MIB del agente pueden (o no) acceder los miembros del grupo o comunidad.

Configurar vistas MIB

De forma predeterminada, una comunidad SNMP concede acceso de lectura y deniega el acceso de escritura a todos los objetos MIB compatibles (incluso a las comunidades configuradas como).`authorization read-write` Para restringir o conceder acceso de lectura o escritura a un conjunto de objetos MIB, debe configurar una vista MIB y asociarla a una comunidad.

Para configurar vistas MIB, consulte .*view (Configuring a MIB View)*

Para quitar un OID por completo, utilice el comando pero omita el parámetro.`delete view all oid` *`oid-number`*`include`

```
[edit groups global snmp]
user@host# set view view-name oid object-identifier (include | exclude)
```

En el ejemplo siguiente se crea una vista MIB denominada ping-mib-view. La instrucción no requiere un punto al principio del identificador de objeto.`oid` La instrucción incluye la rama bajo el identificador de objeto .1.3.6.1.2.1.80.`snmp view` Esto incluye todo el subárbol DISMAN-PINGMIB (tal como se define en

RFC 2925, Definiciones de objetos administrados para operaciones remotas de ping, traceroute y búsqueda), que permite efectivamente el acceso a cualquier objeto bajo esa rama.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid 1.3.6.1.2.1.80 include
```

En el ejemplo siguiente se agrega una segunda rama en la misma vista MIB.

```
[edit groups global snmp]
user@host# set view ping-mib-view oid jnxPingMIB include
```

Asigne una vista MIB a una comunidad que desee controlar.

Para asociar vistas MIB a una comunidad, consulte .*view (SNMP Community)*

Para obtener más información acerca de Ping MIB, consulte RFC 2925 y PING MIB.https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-ping.txt

SEE ALSO

Oid

Configurar MIB de proxy de ping

Restrinja el acceso de lectura y escritura de la MIB de Ping y sólo.*ping-mib*`jnxpingMIB` No se permite el acceso de lectura o escritura a ningún otro MIB que utilice esta comunidad.

```
[edit snmp]
view ping-mib-view {
    oid 1.3.6.1.2.1.80 include; #pingMIB
    oid jnxPingMIB include; #jnxPingMIB
}
community ping-mib {
    authorization read-write;
    view ping-mib-view;
}
```

La siguiente configuración impide que la comunidad acceda a Ping MIB y objetos.*no-ping-mib*`jnxPingMIB` Sin embargo, esta configuración no impide que la comunidad acceda a cualquier otro objeto MIB compatible con el dispositivo.*no-ping-mib*

```
[edit snmp]
view no-ping-mib-view {
    oid 1.3.6.1.2.1.80 exclude; # deny access to pingMIB objects
    oid jnxPingMIB exclude; # deny access to jnxPingMIB objects
}
community no-ping-mib {
    authorization read-write;
    view ping-mib-view;
}
```

SEE ALSO

view (Configuración de una vista MIB)

Oid

MIB SNMP compatibles con Junos OS y Junos OS Evolved

in this section

- Compatibilidad con MIB SNMP | **601**
- Objetos MIB para la serie QFX | **610**
- MIB de chasis de estructura | **614**
- MIB SNMP estándar compatibles con Junos OS | **621**
- Las MIB específicas de la empresa para Junos OS evolucionaron | **637**
- MIB SNMP específicas de la empresa compatibles con Junos OS | **650**
- MIB estándar para Junos OS evolucionado | **674**

Compatibilidad con MIB SNMP

in this section

- MIB compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX | 601
- MIB compatibles con sistemas QFabric | 607

Los conmutadores independientes de la serie QFX, el chasis virtual de la serie QFX y los sistemas QFabric admiten MIB estándar y MIB específicas de la empresa de Juniper Networks.

Para obtener información acerca de los objetos SNMP MIB específicos de la empresa, consulte el Explorador de SNMP MIB. Puede usar el Explorador de MIB SNMP para ver información sobre varias MIB, objetos MIB y notificaciones SNMP admitidas en dispositivos de Juniper Networks.

MIB compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX

Los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX admiten tanto MIB estándar como MIB específicas para empresas de Juniper Networks. Para obtener más información, consulte:

- Tabla 48 en la página 602 para MIB estándar.
- Tabla 49 en la página 604 para las MIB específicas de la empresa de Juniper Networks.

Tabla 48: MIB estándar compatibles con los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX

RFC	Información adicional
IEEE 802.1ab sección 12.1, Protocolo de descubrimiento de capa de vínculo (LLDP) MIB	Tablas y objetos admitidos: • lldpRemManAddrOID • lldpLocManAddrOID • lldpReinitDelay • lldpNotificationInterval • lldpStatsRxPortFramesDiscardedTotal • lldpStatsRxPortFramesError • lldpStatsRxPortTLVsDiscardedTotal • lldpStatsRxPortTLVsNo reconocidoTotal • lldpStatsRxPortAgeoutsTotal
IEEE 802.3ad, agregación de múltiples segmentos de vínculo	Se admiten las siguientes tablas y objetos: • dot3adAggPortTable, dot3adAggPortListTable, dot3adAggTable y dot3adAggPortStatsTable • dot3adAggPortDebugTable (solo dot3adAggPortDebugRxState, dot3adAggPortDebugMuxState, dot3adAggPortDebugActorSyncTransitionCount, dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugActorChangeCount y dot3adAggPortDebugPartnerChangeCount) • dot3adTablesLastChanged
RFC 1286, Definiciones de objetos administrados para puentes	—

Tabla 48: MIB estándar compatibles con los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX *(Continued)*

RFC	Información adicional
RFC 2576, Coexistencia entre la versión 1, la versión 2 y la versión 3 del marco de administración de red estándar de Internet	**NOTA**: RFC 2576 ha sido reemplazado por RFC 3584. Sin embargo, Junos OS es compatible con RFC 2576 y RFC 3584.
RFC 2933, Protocolo de administración de grupos de Internet (IGMP) MIB	—
RFC 4318, Definiciones de objetos administrados para puentes con protocolo de árbol de expansión rápida	Admite extensiones 802.1w y 802.1t para RSTP. No es compatible con dispositivos de la serie OCX.
RFC 4363b, Q-Bridge VLAN MIB	**NOTA**: En los conmutadores QFX3500 y QFX3600, la tabla dot1dTpFdbTable (RFC 4188, Definiciones de objetos administrados para puentes) se rellena únicamente con direcciones MAC aprendidas en la VLAN predeterminada. Para ver las direcciones MAC de todas las VLAN, especifique la tabla dot1qTpFdbTable (en esta MIB) cuando ejecute el comando.`show snmp mib walk` No es compatible con dispositivos de la serie OCX.
Autoridad de números asignados de Internet, MIB de convención textual IANAiftype (referenciada por RFC 2233)	Consulte http://www.iana.org/assignments/ianaiftype-mib .http://www.iana.org/assignments/ianaiftype-mib
Borrador de Internet draft-reeder-snmpv3-usm-3desede-00.txt, Extensión del modelo de seguridad basado en el usuario (USM) para admitir el EDE de triple DES en modo CBC "externo"	—

Tabla 48: MIB estándar compatibles con los conmutadores independientes de la serie QFX y el chasis virtual de la serie QFX *(Continued)*

RFC	Información adicional
Borrador de Internet draft-ietf-idmr-igmp-mib-13.txt, MIB del Protocolo de administración de grupos de Internet (IGMP)	—
Consorcio MIB de ESO	**NOTA**: El ESO Consortium MIB ha sido reemplazado por RFC 3826. Véase http://www.snmp.com/eso/.http://www.snmp.com/eso/

Tabla 49: MIB específicas para empresas de Juniper Networks compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX

BIA	Description
MIB de alarma (mib-jnx-chassis-alarm)	Proporciona soporte para las alarmas del conmutador.
Analizador MIB (mib-jnx-analyzer)	Contiene datos del analizador y del analizador remoto relacionados con la creación de reflejo de puertos. No es compatible con dispositivos de la serie OCX.
MIB de chasis (mib-jnx-chasis)	Proporciona soporte para monitoreo ambiental (estado de la fuente de alimentación, voltajes de placa, ventiladores, temperaturas y flujo de aire) y soporte de inventario para el chasis, concentradores PIC flexibles (FPC) y PIC. **NOTA**: La tabla jnxLEDTable ha quedado obsoleta.
Definiciones de chasis para MIB de modelo de enrutador (mib-jnx-chas-defines)	Contiene los identificadores de objeto (OID) que utiliza la MIB del chasis para identificar las plataformas de enrutamiento y conmutación y los componentes del chasis. La MIB de chasis proporciona información que cambia con frecuencia, mientras que las definiciones de chasis para MIB de modelo de enrutador proporcionan información que cambia con menos frecuencia.
MIB de clase de servicio (mib-jnx-cos)	Proporciona compatibilidad para supervisar estadísticas de cola de salida de interfaz por interfaz y por clase de reenvío.

Tabla 49: MIB específicas para empresas de Juniper Networks compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

BIA	Description
MIB de administración de la configuración (mib-jnx-cfgmgmt)	Proporciona notificaciones para cambios de configuración y cambios de configuración de rescate en forma de capturas SNMP. Cada interrupción contiene la hora a la que se confirmó el cambio de configuración, el nombre del usuario que realizó el cambio y el método mediante el cual se realizó el cambio. Un historial de los últimos 32 cambios de configuración se mantiene en jnxCmChgEventTable.
MIB MAC Ethernet (mib-jnx-mac)	Supervisa las estadísticas de control de acceso a medios (MAC) en las interfaces de cola inteligente (IQ) de Gigabit Ethernet. Recopila estadísticas MAC; por ejemplo, inoctetos, inframes, outoctetos y outframes en cada dirección MAC de origen e ID de LAN virtual (VLAN) para cada puerto Ethernet. No es compatible con dispositivos de la serie OCX.
MIB de evento (mib-jnx-event)	Define una interrupción genérica que se puede generar mediante un script de operaciones o una política de eventos. Esta MIB permite especificar una cadena de registro del sistema y generar una interrupción si se encuentra dicha cadena de registro del sistema. En Junos OS versión 13.2X51-D10 o posterior, si configuró una política de eventos para generar una captura cuando se agrega un nuevo destino de captura SNMP, la captura SNMPD_TRAP_TARGET_ADD_NOTICE se genera con información sobre el nuevo destino.
MIB de firewall (mib-jnx-firewall)	Proporciona compatibilidad para supervisar contadores de filtros de firewall .
MIB de recursos de host (mib-jnx-hostresources)	Extiende el objeto hrStorageTable y proporciona una medida del uso de cada sistema de archivos en el conmutador como porcentaje. Anteriormente, los objetos de hrStorageTable medían el uso solo en unidades de asignación (hrStorageUsed y hrStorageAllocationUnits). Con la medición porcentual, puede supervisar y aplicar umbrales de uso más fácilmente.
MIB de interfaz (extensiones) (mib-jnx-if-extensions)	Amplía el estándar ifTable (RFC 2863) con estadísticas adicionales e información de chasis específica de la empresa de Juniper Networks en las tablas ifJnxTable e ifChassisTable.

Tabla 49: MIB específicas para empresas de Juniper Networks compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

BIA	Description
MIB L2ALD (mib-jnx-l2ald)	Proporciona información sobre el aprendizaje de direcciones de capa 2 y las capturas relacionadas, como la instancia de enrutamiento, la captura de límite de MAC y la captura de límite de MAC de interfaz. Esta MIB también proporciona información de VLAN en la tabla jnxL2aldVlanTable para conmutadores serie EX y QFX de software de capa 2 mejorado (ELS). **NOTA**: Los conmutadores que no son de la serie EX de ELS utilizan la VLAN MIB (jnxExVlanTable) para la información de VLAN en lugar de esta MIB.
MIB MPLS (mib-jnx-mpls)	Proporciona información de MPLS y define las notificaciones MPLS. **NOTA**: Esta MIB no es compatible con el conmutador QFX5100.
MPLS LDP MIB (mib-jnx-mpls-ldp)	Contiene definiciones de objetos como se describe en RFC 3815, Definiciones de objetos administrados para la conmutación de etiquetas multiprotocolo (MPLS), Protocolo de distribución de etiquetas (LDP). **NOTA**: Esta MIB no es compatible con el conmutador QFX5100.
Ping MIB (mib-jnx-ping)	Amplía la tabla de control Ping MIB estándar (RFC 2925). Los elementos de esta MIB se crean cuando se crean entradas en pingCtlTable de la MIB de ping. Cada elemento se indexa exactamente como está en la MIB de ping.
MIB de eventos y alarmas RMON (MIB-JNX-RMON)	Admite extensiones de Junos OS para la MIB de eventos y alarmas de monitoreo remoto (RMON) estándar (RFC 2819). La extensión aumenta el objeto alarmTable con información adicional sobre cada alarma. También se definen dos trampas adicionales para indicar cuándo se encuentran problemas con una alarma.
Estructura de la información de gestión MIB (mib-jnx-smi)	Explica cómo se estructuran las MIB específicas de la empresa de Juniper Networks.
MIB de registro del sistema (mib-jnx-syslog)	Permite la notificación de una aplicación basada en capturas SNMP cuando aparece un mensaje importante de registro del sistema.

Tabla 49: MIB específicas para empresas de Juniper Networks compatibles con conmutadores independientes de la serie QFX y chasis virtual de la serie QFX *(Continued)*

BIA	Description
MIB de utilidad (mib-jnx-util)	Proporciona objetos contenedores SNMP MIB de los siguientes tipos: Contadores de 32 bits, contadores de 64 bits, enteros con signo, enteros sin signo y cadenas de octetos. Puede utilizar estos objetos para almacenar datos que se pueden recuperar mediante otras operaciones SNMP.
VLAN MIB (mib-jnx-vlan)	Contiene información acerca de las VLAN IEEE 802.10 preestándar y su asociación con clientes de emulación LAN. **NOTA**: Para los conmutadores de las series EX y QFX de ELS, la información de VLAN está disponible en la MIB L2ALD en la tabla jnxL2aldVlanTable en lugar de en la MIB de VLAN Para los conmutadores que no son de la serie EX de ELS, la información de VLAN se proporciona en la MIB de VLAN en la tabla jnxExVlanTable. No es compatible con dispositivos de la serie OCX.

MIB compatibles con sistemas QFabric

Los sistemas QFabric admiten tanto MIB estándar como MIB específicas de la empresa de Juniper Networks. Para obtener más información, consulte:

- Tabla 50 en la página 607 para MIB estándar.
- Tabla 51 en la página 608 para las MIB específicas de la empresa de Juniper Networks.

Tabla 50: MIB estándar compatibles con sistemas QFabric

RFC	Información adicional
RFC 1286, Definiciones de objetos administrados para puentes	—
RFC 2576, Coexistencia entre la versión 1, la versión 2 y la versión 3 del marco de administración de red estándar de Internet	**NOTA**: RFC 2576 ha sido reemplazado por RFC 3584. Sin embargo, Junos OS es compatible con RFC 2576 y RFC 3584.

Tabla 50: MIB estándar compatibles con sistemas QFabric *(Continued)*

RFC	Información adicional
RFC 2933, Protocolo de administración de grupos de Internet (IGMP) MIB	—
RFC 4363b, Q-Bridge VLAN MIB	El sistema QFabric solo admite las siguientes tablas: • dot1qTpFdbTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1qFdbTable No es compatible con dispositivos de la serie OCX.

NOTA: Las MIB específicas de QFabric no son compatibles con dispositivos de la serie OCX.

Tabla 51: MIB específicas para la empresa de Juniper Networks compatibles con sistemas QFabric

BIA	Description
Analizador MIB (mib-jnx-analyzer)	Contiene datos del analizador y del analizador remoto relacionados con la creación de reflejo de puertos. El sistema QFabric soporta: • Tabla del analizador: jnxAnalyzerName, jnxMirroringRatio, jnxLossPriority. • Tabla de entrada del analizador: jnxAnalyzerInputValue, jnxAnalyzerInputOption, jnxAnalyzerInputType. • Tabla de salida del analizador: jnx AnalyzerOutputValue, jnxAnalyzerOutputType.
MIB de chasis (mib-jnx-chasis)	**NOTA**: La MIB del chasis ha quedado obsoleta para el sistema QFabric. Se recomienda utilizar la MIB de chasis de estructura (mib-jnx-fabric-chassis) para obtener información sobre el sistema QFabric.

Tabla 51: MIB específicas para la empresa de Juniper Networks compatibles con sistemas QFabric *(Continued)*

BIA	Description
MIB de clase de servicio (mib-jnx-cos)	Proporciona compatibilidad para supervisar estadísticas de cola de salida de interfaz por interfaz y por clase de reenvío. El sistema QFabric admite las siguientes tablas y objetos: • Jnxcosifstatflagtable: jnxCosIfstatFlags y jnxCosIfIndex. • Jnxcosqstattable: jnxCosQstatTxedPkts, jnxCosQstatTxedPktRate, jnxCosQstatTxedBytes y jnxCosQstatTxedByteRate. • Jnxcosfcidtable—jnxCosFcIdToFcName. • Jnxcosfctable—jnxCosFcQueueNr. El sistema QFabric no admite ninguna trampa para esta MIB.
MIB de administración de la configuración (mib-jnx-cfgmgmt)	Proporciona notificaciones para cambios de configuración y cambios de configuración de rescate en forma de capturas SNMP. Cada interrupción contiene la hora a la que se confirmó el cambio de configuración, el nombre del usuario que realizó el cambio y el método mediante el cual se realizó el cambio. Un historial de los últimos 32 cambios de configuración se mantiene en jnxCmChgEventTable. **NOTA**: En el sistema QFabric, se aplican estas condiciones: • Se admiten todas las variables escalares de la tabla jnxCmCfgChg. • Los OID escalares admitidos son jnxCmCfgChgLatestIndex, jnxCmCfgChgLatestTime, jnxCmCfgChgLatestDate, jnxCmCfgChgLatestSource, jnxCmCfgChgLatestUser y jnxCmCfgChgMaxEventEntries. • No se admiten variables escalares de la tabla jnxCmRescueChg.
MIB de chasis de estructura (mib-jnx-fabric-chassis)	Proporciona información de hardware sobre el sistema QFabric y sus dispositivos componentes. Esta MIB se basa en la MIB de chasis específica para la empresa de Juniper Networks, pero agrega otro nivel de indexación que proporciona información para los dispositivos de componentes del sistema QFabric.

Tabla 51: MIB específicas para la empresa de Juniper Networks compatibles con sistemas QFabric *(Continued)*

BIA	Description
MIB de interfaz (extensiones) (mib-jnx-if-extensions)	Amplía el estándar ifTable (RFC 2863) con estadísticas adicionales e información de chasis específica de la empresa de Juniper Networks en las tablas ifJnxTable e ifChassisTable. **NOTA**: En el sistema QFabric, no se admiten variables escalares.
Unidad de fuente de alimentación MIB (mib-jnx-power-supply-unit)	Proporciona soporte para el monitoreo ambiental de la unidad de fuente de alimentación para el dispositivo de interconexión del sistema QFabric. **NOTA**: En el sistema QFabric, no se admiten variables escalares para el identificador de objeto jnxPsuObjects 1 de la tabla jnxPsuScalars.
QFabric MIB (jnx-qf-smi)	Explica cómo se estructuran las MIB de QFabric específicas para empresa de Juniper Networks. Define los objetos MIB notificados por el sistema QFabric y el contenido de las capturas que puede emitir el sistema QFabric.
MIB de utilidad (mib-jnx-util)	Proporciona objetos contenedores SNMP MIB de los siguientes tipos: Contadores de 32 bits, contadores de 64 bits, enteros con signo, enteros sin signo y cadenas de octetos. Puede utilizar estos objetos para almacenar datos que se pueden recuperar mediante otras operaciones SNMP.

SEE ALSO

Explorador SNMP MIB

Descripción de la implementación de SNMP en el sistema QFabric

Objetos MIB para la serie QFX

in this section

Conmutadores independientes serie QFX | **611**

- Sistemas QFabric | 612
- Dispositivo QFabric System QFX3100 Director | 612
- Dispositivo de interconexión QFX3008-I del sistema QFabric | 612
- Dispositivo de interconexión QFX3600-I del sistema QFabric | 613
- Dispositivos de nodo del sistema QFabric | 613

En este tema se enumeran los objetos de definición MIB de chasis SNMP específicos de la empresa de Juniper Networks para la serie QFX:

Conmutadores independientes serie QFX

```
jnxProductLineQFXSwitch       OBJECT IDENTIFIER ::= { jnxProductLine      82 }
  jnxProductNameQFXSwitch       OBJECT IDENTIFIER ::= { jnxProductName      82 }
  jnxProductModelQFXSwitch      OBJECT IDENTIFIER ::= { jnxProductModel     82 }
  jnxProductVariationQFXSwitch  OBJECT IDENTIFIER ::= { jnxProductVariation 82 }
    jnxProductQFX3500s          OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 1 }
    jnxProductQFX360016QS       OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 2 }
    jnxProductQFX350048T4QS     OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 3 }
    jnxProductQFX510024Q        OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 4 }
    jnxProductQFX510048S6Q      OBJECT IDENTIFIER ::= { jnxProductVariationQFXSwitch 5 }

  jnxChassisQFXSwitch           OBJECT IDENTIFIER ::= { jnxChassis          82 }

  jnxSlotQFXSwitch              OBJECT IDENTIFIER ::= { jnxSlot             82 }
    jnxQFXSwitchSlotFPC         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   1 }
    jnxQFXSwitchSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   2 }
    jnxQFXSwitchSlotPower       OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   3 }
    jnxQFXSwitchSlotFan         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   4 }
    jnxQFXSwitchSlotFPB         OBJECT IDENTIFIER ::= { jnxSlotQFXSwitch   5 }

  jnxMediaCardSpaceQFXSwitch    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   82 }
    jnxQFXSwitchMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXSwitch 1 }
```

Sistemas QFabric

```
jnxProductLineQFX3000        OBJECT IDENTIFIER ::= { jnxProductLine 84 }
  jnxProductNameQFX3000         OBJECT IDENTIFIER ::= { jnxProductName 84 }
  jnxProductModelQFX3000        OBJECT IDENTIFIER ::= { jnxProductModel 84 }
  jnxProductVariationQFX3000    OBJECT IDENTIFIER ::= { jnxProductVariation 84 }
   jnxProductQFX3000-G          OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000 1 }
   jnxProductQFX3000-M          OBJECT IDENTIFIER ::= { jnxProductVariationQFX3000 2 }
  jnxChassisQFX3000             OBJECT IDENTIFIER ::= { jnxChassis          84 }
```

Dispositivo QFabric System QFX3100 Director

```
jnxProductLineQFX3100 OBJECT IDENTIFIER ::= { jnxProductLine      100 }
  jnxProductNameQFX3100 OBJECT IDENTIFIER ::= { jnxProductName      100 }
  jnxProductModelQFX3100 OBJECT IDENTIFIER ::= { jnxProductModel     100 }
  jnxProductVariationQFX3100  OBJECT IDENTIFIER ::= { jnxProductVariation 100 }
  jnxChassisQFX3100     OBJECT IDENTIFIER ::= { jnxChassis          100 }

  jnxSlotQFX3100            OBJECT IDENTIFIER ::= { jnxSlot             100 }
    jnxQFX3100SlotCPU       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   1 }
    jnxQFX3100SlotMemory    OBJECT IDENTIFIER ::= { jnxSlotQFX3100   2 }
    jnxQFX3100SlotPower     OBJECT IDENTIFIER ::= { jnxSlotQFX3100   3 }
    jnxQFX3100SlotFan       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   4 }
    jnxQFX3100SlotHardDisk  OBJECT IDENTIFIER ::= { jnxSlotQFX3100   5 }
    jnxQFX3100SlotNIC       OBJECT IDENTIFIER ::= { jnxSlotQFX3100   6 }
```

Dispositivo de interconexión QFX3008-I del sistema QFabric

```
jnxProductLineQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      60 }
  jnxProductNameQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductName      60 }
  jnxProductModelQFXInterconnect OBJECT IDENTIFIER ::= { jnxProductModel     60 }
  jnxProductVariationQFXInterconnect  OBJECT IDENTIFIER ::= { jnxProductVariation 60 }
    jnxProductQFX3008           OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect
1 }    jnxProductQFXC083008        OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 2 }
    jnxProductQFX3008I          OBJECT IDENTIFIER ::= { jnxProductVariationQFXInterconnect 3 }

  jnxChassisQFXInterconnect     OBJECT IDENTIFIER ::= { jnxChassis          60 }

  jnxSlotQFXInterconnect        OBJECT IDENTIFIER ::= { jnxSlot             60 }
```

```
    jnxQFXInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   1 }
    jnxQFXInterconnectSlotHM    OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   2 }
    jnxQFXInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   3 }
    jnxQFXInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   4 }
    jnxQFXInterconnectSlotCBD   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   5 }
    jnxQFXInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXInterconnect   6 }

  jnxMediaCardSpaceQFXInterconnect    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   60 }
    jnxQFXInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXInterconnect
1 }

  jnxMidplaneQFXInterconnect    OBJECT IDENTIFIER ::= { jnxBackplane        60 }
```

Dispositivo de interconexión QFX3600-I del sistema QFabric

```
jnxProductLineQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductLine      91 }
  jnxProductNameQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductName      91 }
  jnxProductModelQFXMInterconnect OBJECT IDENTIFIER ::= { jnxProductModel     91 }
  jnxProductVariationQFXMInterconnect  OBJECT IDENTIFIER ::= { jnxProductVariation 91 }
    jnxProductQFX3600I          OBJECT IDENTIFIER ::= { jnxProductVariationQFXMInterconnect 1 }

  jnxChassisQFXMInterconnect     OBJECT IDENTIFIER ::= { jnxChassis          91 }

  jnxSlotQFXMInterconnect        OBJECT IDENTIFIER ::= { jnxSlot             91 }
    jnxQFXMInterconnectSlotFPC   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   1 }
    jnxQFXMInterconnectSlotHM    OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   2 }
    jnxQFXMInterconnectSlotPower OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   3 }
    jnxQFXMInterconnectSlotFan   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   4 }
    jnxQFXMInterconnectSlotFPB   OBJECT IDENTIFIER ::= { jnxSlotQFXMInterconnect   5 }

  jnxMediaCardSpaceQFXMInterconnect    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   91 }
    jnxQFXMInterconnectMediaCardSpacePIC OBJECT IDENTIFIER ::=
{ jnxMediaCardSpaceQFXMInterconnect 1 }
```

Dispositivos de nodo del sistema QFabric

```
jnxProductLineQFXNode       OBJECT IDENTIFIER ::= { jnxProductLine      61 }
  jnxProductNameQFXNode       OBJECT IDENTIFIER ::= { jnxProductName      61 }
  jnxProductModelQFXNode      OBJECT IDENTIFIER ::= { jnxProductModel     61 }
```

```
jnxProductVariationQFXNode  OBJECT IDENTIFIER ::= { jnxProductVariation 61 }
  jnxProductQFX3500         OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode 1 }
  jnxProductQFX360016Q      OBJECT IDENTIFIER ::= { jnxProductVariationQFXNode 3 }

jnxChassisQFXNode           OBJECT IDENTIFIER ::= { jnxChassis          61 }

jnxSlotQFXNode              OBJECT IDENTIFIER ::= { jnxSlot             61 }
  jnxQFXNodeSlotFPC         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   1 }
  jnxQFXNodeSlotHM          OBJECT IDENTIFIER ::= { jnxSlotQFXNode   2 }
  jnxQFXNodeSlotPower       OBJECT IDENTIFIER ::= { jnxSlotQFXNode   3 }
  jnxQFXNodeSlotFan         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   4 }
  jnxQFXNodeSlotFPB         OBJECT IDENTIFIER ::= { jnxSlotQFXNode   5 }

jnxMediaCardSpaceQFXNode    OBJECT IDENTIFIER ::= { jnxMediaCardSpace   61 }
  jnxQFXNodeMediaCardSpacePIC OBJECT IDENTIFIER ::= { jnxMediaCardSpaceQFXNode 1 }
```

SEE ALSO

> *Descripción de la implementación de SNMP en el sistema QFabric*

MIB de chasis de estructura

La MIB de chasis de estructura SNMP específica para empresas de Juniper Networks (mib-jnx-fabric-chassis) proporciona información de hardware sobre el sistema QFabric y sus dispositivos componentes en una sola MIB. La MIB de chasis de estructura se basa en la MIB de chasis específica para empresa de Juniper Networks que proporciona información para dispositivos individuales. A diferencia de la MIB del chasis, la MIB del chasis de estructura representa los dispositivos componentes del sistema QFabric como parte del sistema QFabric. Solo la información de la MIB del chasis de estructura (y no de las MIB de chasis individuales) está disponible para los clientes de administración SNMP del sistema QFabric.

La MIB de chasis de estructura utiliza la estructura de información básica de la MIB de chasis, pero agrega otro nivel de indexación que proporciona información detallada sobre los dispositivos del sistema QFabric. Cada dispositivo físico en un sistema QFabric (como un dispositivo de nodo o un dispositivo de interconexión) está representado con sus componentes de hardware, incluida la fuente de alimentación, los ventiladores y las tarjetas delanteras y traseras.

Al igual que en otros sistemas SNMP, el gestor SNMP reside en el sistema de gestión de red (NMS) de la red a la que pertenece el sistema QFabric. El agente SNMP (snmpd) reside en el software QFabric system Director y es responsable de recibir y distribuir todas las capturas, así como de responder a todas las consultas del administrador SNMP.

Además, hay un subagente SNMP ejecutándose en el motor de enrutamiento de cada grupo de nodos y dispositivo de interconexión. El subagente SNMP administra la información sobre el dispositivo componente, y esa información se comunica al agente SNMP en el software Director según sea necesario. Las capturas generadas por un dispositivo Node se envían al agente SNMP en el software Director, que a su vez las procesa y envía a las direcciones IP de destino definidas en la configuración SNMP.

Tabla 52 en la página 615 describe las tablas y los objetos de la MIB del chasis de estructura.

Tabla 52: Tablas y objetos MIB de chasis de estructura

Nombre de tabla u objeto	OID raíz	Description
Tablas con homólogos en la MIB del chasis		
jnxFabricContainersTable	1.3.6.1.4.1.2636.3.42.2.2.2	Proporciona información sobre los diferentes tipos de contenedores en dispositivos del sistema QFabric. • Los contenedores para dispositivos de interconexión incluyen bandejas de ventilador, unidades de fuente de alimentación, tableros de control, etc. • Los contenedores para dispositivos de nodo incluyen bandejas de ventilador, unidades de fuente de alimentación, concentrador de PIC flexible (FPC), PIC, etc. • Los contenedores para los dispositivos Director incluyen CPU, memoria, bandejas de ventilador, unidades de fuente de alimentación y discos duros. Los contenedores tienen una estructura no jerárquica o plana, y los componentes en ellos están organizados como hermanos entre sí.

Tabla 52: Tablas y objetos MIB de chasis de estructura *(Continued)*

Nombre de tabla u objeto	OID raíz	Description
jnxFabricContentsTable	1.3.6.1.4.1.2636.3.42.2.2.3	Contiene contenido presente en todos los dispositivos representados en el objeto jnxFabricDeviceTable. Esta tabla incluye todas las unidades reemplazables in situ (FRU) y no FRU para dispositivos del sistema QFabric. • El contenido de los dispositivos de interconexión incluye bandejas de ventilador y tarjetas de control. • El contenido de los dispositivos Node incluye bandejas de ventilador y unidades de fuente de alimentación. • El contenido de los dispositivos Director incluye CPU, memoria, bandejas de ventilador, unidades de fuente de alimentación y discos duros, pero no incluye tarjetas de interfaz de red (NIC).
jnxFabricFilledTable	1.3.6.1.4.1.2636.3.42.2.2.4	Muestra el estado de los contenedores en dispositivos QFabric. El objeto jnxFabricFilledState representa el estado del componente: (1) desconocido, (2) vacío o (3) lleno. **NOTA**: El objeto jnxFabricFilledTable no contiene información sobre el grupo Director.

Tabla 52: Tablas y objetos MIB de chasis de estructura *(Continued)*

Nombre de tabla u objeto	OID raíz	Description
jnxFabricOperatortingTable	1.3.6.1.4.1.2636.3.42.2.2.5	Representa diferentes parámetros operativos para el contenido que se rellena en el objeto jnxFabricContentsTable. • El contenido de cada dispositivo de nodo y dispositivo de interconexión incluye bandejas de ventilador, unidades de fuente de alimentación, FPC, PIC y motor de enrutamiento. • El contenido del dispositivo Director incluye CPU, memoria, bandejas de ventilador, unidades de fuente de alimentación y discos duros, pero no incluye tarjetas de interfaz de red (NIC). El objeto jnxFabricOperatingState proporciona el estado del dispositivo: (1) desconocido, (2) en ejecución, (3) listo, (4) reinicio, (5) ejecuciónAtFullSpeed (solo para ventiladores), (6) apagado, (6) apagado (para unidades de fuente de alimentación) o (7) en espera.
jnxFabricRedundancyTable	1.3.6.1.4.1.2636.3.42.2.2.6	Representa la información de redundancia que está disponible en diferentes niveles de subsistema en todo el sistema QFabric. Se incluye información acerca de los motores de enrutamiento en dispositivos de nodo, pero no hay entradas correspondientes para dispositivos de interconexión en esta tabla. El objeto jnxFabricRedundancyState indica el estado del subsistema: (1) desconocido, (2) primario, (3) copia de seguridad o (4) deshabilitado. **NOTA**: La información sobre dispositivos de director, máquinas virtuales (VM) redundantes dentro de grupos de directores y dispositivos de chasis virtual no está disponible en este momento.

Tabla 52: Tablas y objetos MIB de chasis de estructura *(Continued)*

Nombre de tabla u objeto	OID raíz	Description
jnxFabricFruTable	1.3.6.1.4.1.2636.3.42.2.2.7	Contiene todas las FRU para el sistema QFabric en la tabla jnxFabricDeviceTable. Las FRU se enumeran independientemente de si están instaladas o en línea. El objeto jnxFabricFruState representa el estado de la FRU, incluidos en línea, sin conexión o vacío, etc. Esta tabla también contiene información sobre cada FRU, como nombre, tipo, temperatura, hora del último encendido y hora de la última vez. **NOTA**: La tabla jnxFabricFruTable no incluye tarjetas de interfaz de red (NIC) en dispositivos Director.
Tabla específica de la MIB del chasis de estructura		
jnxFabricDeviceTable	1.3.6.1.4.1.2636.3.42.2.2.1	Contiene información sobre todos los dispositivos del sistema QFabric. Esta tabla organiza las variables escalares representadas en la MIB del chasis en un formato de tabla para los dispositivos componentes del sistema QFabric. Las columnas de esta tabla incluyen información del dispositivo, como el modelo, el alias del dispositivo y el número de serie. jnxFabricDeviceIndex identifica cada dispositivo del sistema QFabric (dispositivo de nodo, dispositivo de interconexión y dispositivo director). **NOTA**: En este momento, la información sobre el chasis virtual no está disponible. **NOTA**: No se admiten los siguientes objetos: • jnxFabricDeviceEntryRevision • jnxFabricDeviceEntryFirmwareRevision • jnxFabricDeviceEntryKernelMemoryUsedPercent
Variables escalares		

Tabla 52: Tablas y objetos MIB de chasis de estructura *(Continued)*

Nombre de tabla u objeto	OID raíz	Description
Se admiten las siguientes variables escalares: • jnxFabricClass • jnxFabricDescr • jnxFabricSerialNo • jnxFabricRevision • jnxFabricLastInstalled • jnxFabricContentsLastChange • jnxFabricFilledLastChange	1.3.6.1.4.1.2636.3.42.2.1	Describir el sistema QFabric como un todo. **NOTA**: La variable escalar jnxFabricFirmwareRevision no se admite en este momento.

Tabla 53 en la página 620 describe las interrupciones SNMPv2 definidas en la MIB del chasis de estructura.

NOTA: Solo se admiten capturas SNMPv2 en el sistema QFabric.

Tabla 53: Trampas de SNMPv2 de MIB de chasis de estructura

Grupo de captura y nombre	OID raíz	Description
jnxFabricChassisTraps: incluye las siguientes interrupciones: • jnxFabricPowerSupplyFailure • jnxFabricFanFailure • jnxFabricOverTemperature • jnxFabricRedundancySwitchover • jnxFabricFruRemoval • jnxFabricFruInsertion • jnxFabricFruPowerOff • jnxFabricFruPowerOn • jnxFabricFruFailed • jnxFabricFruOffline • jnxFabricFruOnline • jnxFabricFruCheck • jnxFabricFEBSwitchover • jnxFabricHardDiskFailed • jnxFabricHardDiskMissing • jnxFabricBootFromBackup • jnxFabricHighPower	1.3.6.1.4.1.2636.4.19	Indica una condición de alarma. **NOTA**: Los eventos de hardware en el grupo Director se detectan mediante el análisis. Como resultado, es posible que no se genere una captura hasta 30 segundos después de que se haya producido el evento. **NOTA**: El software no distingue entre los eventos de extracción y fallo del ventilador en el grupo Director. En cada caso, se generan las capturas jnxFabricFanFailure y jnxFabricFruFailed.

Tabla 53: Trampas de SNMPv2 de MIB de chasis de estructura *(Continued)*

Grupo de captura y nombre	OID raíz	Description
jnxFabricChassisOKTraps group: incluye las siguientes capturas: • jnxFabricPowerSupplyOK • jnxFabricFanOK • jnxFabricTemperatureOK • jnxFabricFruOK • jnxFabricHighPowerCleared	1.3.6.1.4.1.2636.4.20	Indica una condición de alarma borrada.

SEE ALSO

Descripción de la implementación de SNMP en el sistema QFabric

MIB SNMP estándar compatibles con Junos OS

Junos OS admite las MIB estándar enumeradas en Tabla 54 en la página 621.

Tabla 54: MIB estándar compatibles con Junos OS

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
IEEE 802.1ab sección 12.1, *Protocolo de descubrimiento de capa de vínculo (LLDP) MIB*	La implementación de la serie EX de LLDP MIB admite la configuración de IPv4 e IPv6.	Serie EX y Serie MX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
IEEE, 802.3ad, agregación de múltiples segmentos de vínculo	Tablas y objetos admitidos: • , , , ydot3adAggPortTabledot3adAggPortListTabledot3adAggTable dot3adAggPortStatsTable **NOTA**: Los conmutadores de la serie EX no admiten el y .dot3adAggPortTabledot3adAggPortStatsTable • (sólo , , , , , y)dot3adAggPortDebugTabledot3adAggPortDebugRxStatedot3adAggPortDebugMuxStatedot3adAggPortDebugActorSyncTransitionCountdot3adAggPortDebugPartnerSyncTransitionCountdot3adAggPortDebugActorChangeCountdot3adAggPortDebugPartnerChangeCount **NOTA**: Los conmutadores de la serie EX no admiten el archivo .dot3adAggPortDebugTable • dot3adTablesLastChanged	Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX, Serie T y vSRX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
IEEE, 802.1ag, administración de errores de conectividad	Tablas y objetos admitidos: • dot1agCfmMdTableNextIndex • (excepto)dot1agCfmMdTabledot1agCfmMdMhfldPermission • dot1agCfmMaNetTable • dot1agCfmMaMepListTable • dot1agCfmDefaultMdDefLevel • dot1agCfmDefaultMdDefMhfCreation • (excepto , , , , y)dot1agCfmMepTabledot1agCfmMepLbrBadMsdudot1agCfmMepTransmitLbmVlanPrioritydot1agCfmMepTransmitLbmVlanDropEnabledot1agCfmMepTransmitLtmFlagsdot1agCfmMepPbbTeCanReportPbbTePresence dot1agCfmMepPbbTeTrafficMismatchDefectdot1agCfmMepPbbTransmitLbmLtmReverseViddot1agCfmMepPbbTeMismatchAlarmdot1agCfmMepPbbTeLocalMismatchDefectdot1agCfmMepPbbTeMismatchSinceReset • (excepto , , , , , y)dot1agCfmLtrTabledot1agCfmLtrChassisIdSubtypedot1agCfmLtrChassisIddot1agCfmLtrManAddressDomaindot1agCfmLtrManAddressdot1agCfmLtrIngressPortIdSubtypedot1agCfmLtrIngressPortIddot1agCfmLtrEgressPortIdSubtypedot1agCfmLtrEgressPortIddot1agCfmLtrOrganizationSpecificTlv • (excepto , , , y)dot1agCfmMepDbTabledot1agCfmMebDbChassisIdSubtypedot1agCfmMebDbChassisIddot1agCfmMebDbManAddressDomaindot1agCfmMebDbManAddress	Serie EX, Serie MX, Serie PTX y Serie QFX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
IEEE, 802.1ap, definiciones de base de información de administración (MIB) para puentes VLAN	Tablas y objetos admitidos: • `ieee8021CfmStackTable` • `ieee8021CfmVlanTable` • (excepto)`ieee8021CfmDefaultMdTableieee8021CfmDefaultMdIdPermission` • (excepto)`ieee8021CfmMaCompTableieee8021CfmMaCompIdPermission`	serie MX
RFC 2576, Coexistencia entre la versión 1, la versión 2 y la versión 3 del marco de administración de red estándar de Internet **NOTA**: RFC 2576 ha sido reemplazado por RFC 3584. Sin embargo, Junos OS es compatible con RFC 2576 y RFC 3584.	Sin excepciones	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T
RFC 2922, La topología física (PTOPO) MIB	Objetos admitidos: • `ptopoConnDiscAlgorithm` • `ptopoConnAgentNetAddrType` • `ptopoConnAgentNetAddr` • `ptopoConnMultiMacSASeen` • `ptopoConnMultiNetSASeen` • `ptopoConnIsStatic` • `ptopoConnLastVerifyTime` • `ptopoConnRowStatus`	Serie EX y serie SRX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
Objetos administrados RFC 3591 para el tipo de interfaz óptica	Tablas y objetos admitidos: • (excepto , , y)`optIfOTMnTableoptIfOTMnOpticalReachoptIfOTMnInterfaceTypeoptIfOTMnOrder` • (excepto y)`optIfOChConfigTableoptIfOChDirectionalityoptIfOChCurrentStatus` • (excepto , , , , , y)`optIfOTUkConfigTableoptIfOTUkTraceIdentifierAcceptedoptIfOTUkTIMDetModeoptIfOTUkTIMActEnabledoptIfOTUkTraceIdentifierTransmittedoptIfOTUkDEGThroptIfOTUkDEGMoptIfOTUkSinkAdaptActiveoptIfOTUkSourceAdaptActive` • (excepto y)`optIfODUkConfigTableoptIfODUkPositionSeqCurrentSizeoptIfODUkTtpPresent`	Serie M, Serie MX, Serie PTX y Serie T
RFC 3621, Power Ethernet MIB	Sin excepciones	serie EX
RFC 3637, Definiciones de objetos administrados para la subcapa de interfaz WAN Ethernet	Tablas y objetos no compatibles: • `etherWisDeviceTable`, • `etherWisSectionCurrentTable` • `etherWisFarEndPathCurrentTable`	Serie M, Serie MX, Serie PTX y Serie T
RFC 3877, Base de información de gestión de alarmas	• Junos OS no admite la `alarmActiveStatsTable`. • No se admiten capturas que no se ajusten al modelo de alarma. Sin embargo, estas trampas se pueden redefinir para ajustarse al modelo de alarma.	serie MX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
RFC 3896, Definiciones de objetos administrados para el tipo de interfaz DS3/E3	Tablas y objetos no compatibles: • `dsx3FarEndConfigTable` • `dsx3FarEndCurrentTable` • `dsx3FarEndIntervalTable` • `dsx3FarEndTotalTable` • `dsx3FracTable`	Series M y T
RFC 4318, Definiciones de objetos administrados para puentes con protocolo de árbol de expansión rápida	Admite extensiones 802.1w y 802.1t para RSTP.	Serie EX, Serie M, Serie MX y Serie T
RFC 4363b, Q-Bridge VLAN MIB	Sin excepciones	Serie MX y Serie EX
RFC 4668, Base de información de administración de clientes (MIB) de RADIUS Accounting para IPv6 (acceso de solo lectura)	Sin excepciones	serie MX
RFC 4670, Base de información de administración de clientes (MIB) de RADIUS Accounting (acceso de solo lectura)	Sin excepciones	serie MX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
RFC 4801, Definiciones de convenciones textuales para la base de información de administración (MIB) de conmutación generalizada de etiquetas multiprotocolo (GMPLS) (acceso de solo lectura)	Sin excepciones	Serie M, MX y T
RFC 4802, Conmutación generalizada de etiquetas multiprotocolo (GMPLS) Ingeniería de tráfico (TE) Base de información de gestión (MIB) (acceso de solo lectura)	Tablas y objetos no compatibles: • `gmplsTunnelReversePerfTable` • `gmplsTeScalars` • `gmplsTunnelTable` • `gmplsTunnelARHopTable` • `gmplsTunnelCHopTable` • `gmplsTunnelErrorTable`	Serie M, MX y T
RFC 4803, Conmutación generalizada de etiquetas multiprotocolo (GMPLS) Base de información de administración (MIB) del enrutador de conmutación de etiquetas (LSR) (acceso de solo lectura) **NOTA**: Las tablas de las MIB GMPLS TE (RFC 4802) y LSR (RFC 4803) son extensiones de las tablas correspondientes de las MIB MPLS TE (RFC 3812) y LSR (RFC 3813) y utilizan el mismo índice que las tablas MIB MPLS.	Tablas y objetos no compatibles: • `gmplsLabelTable` • `gmplsOutsegmentTable`	Serie M, MX y T

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
RFC 5132, MIB de multidifusión IP **NOTA**: Este RFC deja obsoleto RFC2932.	Tabla no compatible: • `ipMcastZoneTable`	Todas las plataformas

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
RFC 5643, Base de información de administración para OSPFv3 (acceso de solo lectura)	Tablas y objetos no compatibles: • `ospfv3HostTable` • `ospfv3CfgNbrTable` • `ospfv3ExitOverflowInterval` • `ospfv3ReferenceBandwidth` • `ospfv3RestartSupport` • `ospfv3RestartInterval` • `ospfv3RestartStrictLsaChecking` • `ospfv3RestartStatus` • `ospfv3RestartAge` • `ospfv3RestartExitReason` • `ospfv3NotificationEnable` • `ospfv3StubRouterSupport` • `ospfv3StubRouterAdvertisement` • `ospfv3DiscontinuityTime` • `ospfv3RestartTime` • `ospfv3AreaNssaTranslatorRole` • `ospfv3AreaNssaTranslatorState` • `ospfv3AreaNssaTranslatorStabInterval` • `ospfv3AreaNssaTranslatorEvents` • `ospfv3AreaTEEnabled` • `ospfv3IfMetricValue`	Serie M, Serie MX, Serie PTX, Serie SRX y Serie T

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
	• `ospfv3IfDemandNbrProbe`	

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
RFC 7420, Comunicación de elementos de cálculo de ruta	El módulo PCEP MIB está limitado al acceso de "solo lectura", excepto para pcePcepNotificationsMaxRate, que se utiliza para limitar la velocidad a la que la implementación genera notificaciones. En las tablas mencionadas, solo se admitirán en esta versión el par PCEP y la tabla de sesión PCEP. Para , no se admiten los siguientes miembros:`pcePcepPeerTable` • `pcePcepPeerDiscontinuityTime TimeStamp,` • `pcePcepPeerLWMRspTime Unsigned32,` • `pcePcepPeerHWMRspTime Unsigned32,` • `pcePcepPeerNumPCReqSent Counter32,` • `pcePcepPeerNumPCReqRcvd Counter32,` • `pcePcepPeerNumPCRepSent Counter32,` • `pcePcepPeerNumPCRepRcvd Counter32,` • `pcePcepPeerAvgRspTime Unsigned32,` • `pcePcepPeerNumReqSent Counter32,` • `pcePcepPeerNumReqSentEroRcvd Counter32,` • `pcePcepPeerNumReqSentErrorRcvd Counter32,` • `pcePcepPeerNumReqSentTimeout Counter32,` • `pcePcepPeerNumReqSentPendRep Counter32,` • `pcePcepPeerNumReqSentCancelSent Counter32,` • `pcePcepPeerNumReqSentClosed Counter32,` • `pcePcepPeerNumReqRcvd Counter32,` • `pcePcepPeerNumPCNtfSent Counter32,`	Serie MX y PTX

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
	• pcePcepPeerNumPCNtfRcvd Counter32, • pcePcepPeerNumSvecSent Counter32, • pcePcepPeerNumSvecReqSent Counter32, • pcePcepPeerNumSvecRcvd Counter32, • pcePcepPeerNumSvecReqRcvd Counter32, • pcePcepPeerNumReqRcvdPendRep Counter32, • pcePcepPeerNumReqRcvdEroSent Counter32, • pcePcepPeerNumReqRcvdNoPathSent Counter32, • pcePcepPeerNumReqRcvdCancelSent Counter32, • pcePcepPeerNumReqRcvdErrorSent Counter32, • pcePcepPeerNumReqRcvdCancelRcvd Counter32, • pcePcepPeerNumReqRcvdClosed Counter32, • pcePcepPeerNumRepRcvdUnknown Counter32, • pcePcepPeerNumReqRcvdUnknown Counter32, • pcePcepPeerNumReqSentNoPathRcvd Counter32, • pcePcepPeerNumReqSentCancelRcvd Counter32	

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
	Para , no se admiten los siguientes miembros:`pcePcepSessTable` • `pcePcepSessNumPCReqSent Counter32,` • `pcePcepSessNumPCReqRcvd Counter32,` • `pcePcepSessKAHoldTimeRem Unsigned32,` • `pcePcepSessOverloaded TruthValue,` • `pcePcepSessOverloadTime Unsigned32,` • `pcePcepSessPeerOverloaded TruthValue,` • `pcePcepSessPeerOverloadTime Unsigned32,` • `pcePcepSessNumPCNtfSent Counter32,` • `pcePcepSessNumPCNtfRcvd Counter32,` • `pcePcepSessNumReqSent Counter32,` • `pcePcepSessNumReqSentPendRep Counter32,` • `pcePcepSessNumReqSentEroRcvd Counter32,` • `pcePcepSessNumReqSentNoPathRcvd Counter32,` • `pcePcepSessNumReqSentCancelRcvd Counter32,` • `pcePcepSessNumReqSentErrorRcvd Counter32,` • `pcePcepSessNumReqSentTimeout Counter32,` • `pcePcepSessNumReqSentCancelSent Counter32,` • `pcePcepSessAvgRspTime Unsigned32,` • `pcePcepSessLWMRspTime Unsigned32,` • `pcePcepSessHWMRspTime Unsigned32,`	

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
	• `pcePcepSessNumSvecSent Counter32,` • `pcePcepSessNumSvecReqSent Counter32,` • `pcePcepSessNumReqRcvd Counter32,` • `pcePcepSessNumSvecRcvd Counter32,` • `pcePcepSessNumSvecReqRcvd Counter32,` • `pcePcepSessNumReqRcvdPendRep Counter32,` • `pcePcepSessNumReqRcvdEroSent Counter32,` • `pcePcepSessNumReqRcvdNoPathSent Counter32,` • `pcePcepSessNumReqRcvdCancelSent Counter32,` • `pcePcepSessNumReqRcvdErrorSent Counter32,` • `pcePcepSessNumReqRcvdCancelRcvd Counter32,` • `pcePcepSessNumRepRcvdUnknown Counter32,` • `pcePcepSessNumReqRcvdUnknown Counter32`	
ESO Consortium MIB, que se puede encontrar en http://www.snmp.com/eso/http://www.snmp.com/eso/ **NOTA**: El ESO Consortium MIB ha sido reemplazado por RFC 3826.	Sin excepciones	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T
Autoridad de asignación de números de Internet, IANAiftype Textual Convention MIB	Sin excepciones	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
Borrador de Internet draft-ietf-atommib-sonetaps-mib-10.txt, Definiciones de objetos administrados para arquitecturas APS lineales SONET	Como se define en la rama empresarial de Juniper Networks [] solamente`jnxExperiment`	Serie M, MX y T
Borrador de Internet draft-ieft-bfd-mib-02.txt, Base de información de administración de detección de reenvío bidireccional	(Representada por la sucursal empresarial de Juniper Networks [] e implementada en ella.`mib-jnx-bfd-exp.txt``jnxExperiment` Sólo lectura. Incluye y trampas.`bfdSessUp``bfdSessDown` No admite y .)`bfdSessPerfTable``bfdSessMapTable`	Serie ACX, Serie EX, Serie M, Serie MX, Serie SRX y Serie T
Borrador de Internet draft-ietf-idmr-igmp-mib-13.txt, MIB del Protocolo de administración de grupos de Internet (IGMP)	Sin excepciones	Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T
Borrador de Internet draft-ietf-idmr-pim-mib-09.txt, MIB de multidifusión independiente del protocolo (PIM)	Sin excepciones	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T
Borrador de Internet draft-ietf-isis-wg-mib-07.txt, Base de información de gestión para IS-IS **NOTA**: Reemplazado por RFC 4444, IS-IS MIB en Junos OS versión 11.3 y posteriores.	Tablas y objetos no compatibles: • `isisISAdjTable` • `isisISAdjAreaAddrTable` • `isisISAdjIPAddrTable` • `isisISAdjProtSuppTable`)	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
Borrador de Internet draft-ietf-l3vpn-mvpn-mib-03.txt, Base de información de administración de multidifusión VPN de capa 3 MPLS/BGP	(Implementado en la sucursal empresarial de Juniper Networks [].`jnxExperiment` OID para es .`jnxMvpnExperiment.1.3.6.1.4.1.2636.5.12` Sólo lectura. Incluye trampas.)`jnxMvpnNotifications`	Serie M, MX y T
Borrador de Internet draft-ietf-mpls-mldp-mib-02.txt, Definiciones de objetos administrados para las rutas conmutadas de etiquetas punto a multipunto y multipunto a multipunto de LDP	Sin excepciones	Serie M, Serie MX, Serie PTX y Serie T
Borrador de Internet draft-ietf-mpls-p2mp-te-mib-09.txt, P2MP MPLS-TE MIB (acceso de solo lectura)	Tabla no compatible: • `mplsTeP2mpTunnelBranchPerfTable`	Serie ACX, Serie M, Serie MX, Serie PTX y Serie T
Borrador de Internet draft-ietf-ospf-ospfv3-mib-11.txt, Base de información de gestión para OSPFv3	Soporte para sólo.`ospfv3NbrTable`	Serie M, Serie MX, Serie PTX, Serie SRX y Serie T
Borrador de Internet draft-ietf-ppvpn-mpls-vpn-mib-04.txt, base de información de administración de red privada virtual MPLS/BGP mediante SMIv2	Tablas y objetos admitidos: • `mplsVpnScalars` • `mplsVpnVrfTable` • `mplsVpnPerTable` • `mplsVpnVrfRouteTargetTable`	Serie M, Serie MX, Serie PTX y Serie T

Tabla 54: MIB estándar compatibles con Junos OS *(Continued)*

MIB estándar	Tablas y objetos admitidos y no admitidos	Plataformas
Borrador de Internet draft-kamarthy-gdoi-mib-01, Base de Información de Gestión para el Dominio de Interpretación del Grupo (GDOI)	Advertencias: • El GDOI MIB del borrador del IETF se modifica para incluir solo las tablas y notificaciones de miembros del grupo. • Solo se admiten las notificaciones SNMP aplicables a los miembros del grupo de la serie MX.	serie MX
Borrador de Internet draft-reeder-snmpv3-usm-3desede-00.txt, Extensión del modelo de seguridad basado en el usuario (USM) para admitir el EDE de triple DES en modo CBC "externo"	Sin excepciones	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie SRX y Serie T

Para obtener información acerca de los objetos SNMP MIB estándar, consulte el Explorador de MIB SNMP.https://apps.juniper.net/mib-explorer/

Para obtener información acerca de las RFC, consulte la Guía de referencia de estándares.https://www.juniper.net/documentation/us/en/software/junos/standards/index.html

Las MIB específicas de la empresa para Junos OS evolucionaron

A partir de Junos OS Evolved versión 19.1R1, se admiten las MIB específicas de la empresa enumeradas en Tabla 55 en la página 638 . Para obtener información acerca de los objetos SNMP MIB específicos de la empresa, consulte el Explorador de SNMP MIB.

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
BGP4 V2 MIB	Proporciona compatibilidad para supervisar contadores de prefijos BGP recibidos del mismo nivel. Se basa en objetos similares en el MIB documentado en el borrador de Internet draft-ietf-idr-bgp4-mibv2-03.txt, Definiciones de objetos administrados para la cuarta versión de BGP (BGP-4), segunda versión.	Sin excepciones	PTX10003 y PTX10001-36 MR

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
MIB de chasis	Proporciona soporte para monitoreo ambiental (estado de la fuente de alimentación, voltajes de la placa, ventiladores, temperaturas y flujo de aire) y soporte de inventario para el chasis, la placa de control del sistema (SCB), la placa de sistema y conmutación (SSB), el módulo de conmutación y reenvío (SFM), la placa de estructura del conmutador (SFB), los concentradores de PIC flexibles (FPC) y las PIC.	Capturas compatibles: • jnxFruInsertion • jnxFruRemoval • jnxFruPowerOn • jnxFruPowerOff • jnxFruOnline • jnxFruOffline • jnxFruFailed • jnxFruOK • jnxPowerSupplyFailure • jnxPowerSupplyOK • jnxPowerSupplyInputFailure • jnxPowerSupplyInputOK • jnxFanFailure • jnxFanOK • jnxOverTemperature • jnxTemperatureOK Tablas y objetos admitidos: • jnxBoxClass • jnxBoxDescr • jnxBoxSerialNo • jnxBoxRevision	PTX10003 y PTX10001-36 MR

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
		• jnxBoxInstalled • jnxContentsLastChange • jnxContainersTable • jnxOperatortingTable • jnxRedundancyTable • jnxContentsTable • jnxFilledTable • jnxFruTable	
MIB de clase de servicio	Proporciona compatibilidad para supervisar estadísticas de cola de salida de interfaz por interfaz y por clase de reenvío. Proporciona compatibilidad para supervisar estadísticas de control de flujo basado en prioridades (PFC). Las entradas en el de MIB de clase de servicio incluyen , , , y `.jnxCosPfcPriorityTablejnxCosPfcPriorityEntryjnxCosIfIndexjnxCosPfcPriorityIndexjnxCosPfcPriorityRequestsTxjnxCosPfcPriorityRequestsRx`	Sin excepciones	Serie PTX y Serie QFX

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
MIB de uso de clase de destino (DCU)	Proporciona compatibilidad para supervisar contadores SCU y DCU.	Sin excepciones	PTX10001-36MR, PTX10004, PTX10008 y PTX10016
DHCP	Proporciona compatibilidad con SNMP (solo obtener) para las configuraciones de relé sin estado de DHCP. La retransmisión sin estado no incluye compatibilidad con tablas de enlaces y arrendamientos. Tablas y objetos admitidos: • jnxJdhcpRelayStatistics • jnxJdhcpRelayIfcStats	La compatibilidad no incluye los siguientes objetos MIB: • jnxJdhcpLocalServerObjects • jnxJdhcpRelayBindings • jnxJdhcpRelayTraps • jnxJdhcpRelayTrapVars	PTX10001-36MR, PTX10004, PTX10008, PTX10016, QFX5130, QFX5220
DHCPv6	Proporciona compatibilidad SNMP (solo obtención) para configuraciones de relé sin estado DHCPv6. La retransmisión sin estado no incluye compatibilidad con tablas de enlaces y arrendamientos. Tablas y objetos admitidos: • jnxJdhcpv6RelayStatistics • jnxJdhcpv6RelayIfcStats	La compatibilidad no incluye el siguiente objeto MIB: • jnxJdhcpv6LocalServerObjects	PTX10001-36MR, PTX10004, PTX10008, PTX10016, QFX5130, QFX5220

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
Firewall MIB	Proporciona un recuento de bytes y paquetes de los aplicadores de policía conectados a la interfaz.	Tablas y objetos admitidos: • jnxFWCntrXTable • jnxFWCntrPolicerOutSpecPktCount • jnxFWCntrPolicerOutSpecByteCount Se admiten los valores de los siguientes objetos en jnxFWCntrPolicerOutSpecPktCount y jnxFWCntrPolicerOutSpecByteCount, mientras que el resto de las MIB no son compatibles y siempre serán cero.	PTX10001-36 MR, PTX10003, PTX10004 y PTX10008

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
MIB de recursos de host	Extiende el objeto hrStorageTable y proporciona una medida del uso de cada sistema de archivos en el enrutador en formato de porcentaje. Anteriormente, los objetos de hrStorageTable medían el uso solo en unidades de asignación (hrStorageUsed y hrStorageAllocationUnits). Con la medición porcentual, puede supervisar y aplicar umbrales de uso más fácilmente. Los montajes se leen en cada nodo del sistema y se compilan en una lista.	Tablas y objetos admitidos: • hrStorageTable • jnxHrStorage • hrSWInstalledTable • hrSystemTiempo de actividad • hrSystemDate • hrSystemInitialLoadDevice • hrSystemInitialLoadParameters • hrSystemNumUsers • hrSystemProcesses • hrSystemMaxProcesses • hrMemorySize • hrSWInstalledLastChange • hrSWInstalledLastUpdateTime	PTX10003
MIB de interfaz	Amplía la tabla ifTable estándar (RFC 2863) con estadísticas adicionales e información de chasis específica para la empresa de Juniper Networks en los contadores de entrega de paquetes y colas de entrada marcados ECN.`ifJnxTable`	Sin excepciones	PTX10003 y QFX5220

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
IPv4 MIB	Proporciona información adicional sobre direcciones IPv4, lo que admite la asignación de direcciones IPv4 idénticas a interfaces independientes.	Sin excepciones	PTX10003
MIB IPv6 e ICMPv6	Proporciona estadísticas de IPv6 y Protocolo de mensajes de control de Internet versión 6 (ICMPv6).	Objetos no compatibles • Rama jnxIcmpv6GlobalStats y los objetos que contiene	PTX10003
LDP MIB	Proporciona estadísticas de LDP y define las notificaciones de ruta de conmutación de etiquetas (LSP) de LDP. Las capturas de LDP solo admiten estándares IPv4.	Sin excepciones	PTX10003
MPLS LDP MIB	Contiene definiciones de objetos como se describe en RFC 3815, Definiciones de objetos administrados para la conmutación de etiquetas multiprotocolo (MPLS), Protocolo de distribución de etiquetas (LDP).	Sin excepciones	PTX10003
MPLS MIB	Proporciona información de MPLS y define las notificaciones MPLS.	Sin excepciones	PTX10003

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
RSVP MIB	Proporciona información acerca de las sesiones de ingeniería de tráfico RSVP que corresponden a los LSP MPLS en enrutadores de tránsito en la red principal del proveedor de servicios.	Sin excepciones	PTX10003
Monitor óptico digital SFF MIB	Define los objetos utilizados para el monitor óptico digital en interfaces de productos Juniper.	Tablas admitidas: • jnxDomCurrentTable • jnxDomModuleLaneTable	PTX10003
SNMP USM HMAC-SHA-2 MIB	Contiene la implementación de Juniper Networks de MIB específica para la empresa para SNMP USM HMAC-SHA-2.	Objetos admitidos: • usmHMAC128SHA224AuthProtocol • usmHMAC192SHA256AuthProtocol	ACX7100 - 32C, ACX7100 - 48L, ACX7509, ACX7900, ACX7024, PTX1000136 MR, PTX10003, PTX10004, PTX10008, PTX10016, QFX5130 - 32CD, QFX5130 - 48C, QFX5130 - 48CM, QFX5700, QFX5220, QFX5230 - 64CD

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
MIB de uso de clase de origen (SCU)	Proporciona compatibilidad para supervisar contadores SCU y DCU.	Sin excepciones	PTX10001-36 MR, PTX10004, PTX10008 y PTX10016

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
MIB TWAMP (jnxTwampMib)	Supervisa el rendimiento de la red mediante el protocolo de medición activa bidireccional.	Tablas admitidas: • jnxTwampClientResultsSampleTable • jnxTwampClientResultsSummaryTable • jnxTwampClientResultsCalculatedTable • jnxTwampClientHistorySampleTable • jnxTwampClientHistorySummaryTable • jnxTwampClientHistoryCalculatedTable • jnxTwampClientControlConnectionTable • jnxTwampClientTestSessionsTable Capturas compatibles: • jnxTwampClientControlConnectionClosed • jnxTwampClientTestIterationFinished • pingProbeFailed • pingTestFailed • pingTestCompleted • jnxPingRttThresholdExceeded	PTX10001-36MR, PTX10003, PTX10004 y PTX10008

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
		• jnxPingRttJitterThresholdExceeded • jnxPingEgressThresholdExceeded • jnxPingEgressJitterThresholdExceeded • jnxPingIngressThresholdExceeded • jnxPingIngressJitterThresholdExceeded • jnxPingMaxRttThresholdExceeded	

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
Temporización MIB (jnxTimingNotfnsMIB)	Define objetos, errores y eventos de Ethernet sincrónica (SyncE).	Capturas compatibles: • jnxTimingFaultLOSSet • jnxTimingFaultLOSClear • jnxTimingFaultEFDSet • jnxTimingFaultEFDClear • jnxTimingFaultLOESMCSet • jnxTimingFaultLOESMCClear • jnxTimingFaultQLFailSet • jnxTimingFaultQLFailClear • jnxTimingFaultLTISet • jnxTimingFaultLTIClear • jnxTimingFaultPriSrcFailed • jnxTimingFaultSecSrcFailed • jnxTimingEventPriSrcRecovered • jnxTimingEventSecSrcRecovered • jnxTimingEventPriRefChanged • jnxTimingEventSecRefChanged • jnxTimingEventQLChangedRx • jnxTimingEventQLChangedTx • jnxTimingEventDpllStatus • jnxTimingEventSynceDpllStatus Objetos y tablas admitidos:	PTX10008

Tabla 55: Las MIB específicas de la empresa compatibles con Junos OS evolucionaron *(Continued)*

MIB específica de la empresa	Description	Tablas y objetos admitidos y no admitidos	Plataforma
		• jnxClksyncIfIndex • jnxClksyncIntfName • jnxClksyncQualityCode • jnxClksyncQualityCodeStr • jnxClksyncDpllState • jnxClksyncDpllStateStr • jnxClksyncSynceLockedIfIndex • jnxClksyncSynceLockedIntfName • jnxClksyncSynceQualityTable	
VPN MIB	Proporciona supervisión para VPN de capa 3, VPN de capa 2 y servicio de LAN privada virtual (VPLS).	Objetos no compatibles • jnxVpnActiveVpns • jnxVpnConfiguredVpns	PTX10003

MIB SNMP específicas de la empresa compatibles con Junos OS

Junos OS admite las MIB específicas de la empresa enumeradas en Tabla 56 en la página 651. Para obtener información acerca de los objetos SNMP MIB específicos de la empresa, consulte el Explorador de SNMP MIB.

Tabla 56: MIB específicas de la empresa compatibles con Junos OS

MIB específica de la empresa	Description	Plataformas
MIB de objetos AAA	Proporciona compatibilidad para supervisar la autenticación, autorización y contabilidad de usuarios a través de RADIUS, LDAP, SecurID y servidores de autenticación locales.	Serie SRX y firewall virtual vSRX
MIB de objetos de autenticación de acceso	Proporciona compatibilidad para supervisar la autenticación de firewall, incluidos datos sobre los usuarios que intentan tener acceso a recursos protegidos por firewall y el servicio de autenticación de firewall.	Serie SRX y firewall virtual vSRX
MIB de alarma	Proporciona información sobre las alarmas del chasis del enrutador.	Todas las plataformas excepto los dispositivos MX10003 y MX204.
Analizador MIB	Proporciona información sobre el analizador y el analizador remoto relacionados con la duplicación de puertos en los conmutadores Ethernet de la serie EX.	Serie EX, sistema QFabric y serie QFX
MIB de objetos antivirus	Proporciona información sobre el motor antivirus, los análisis antivirus y las capturas relacionadas con el análisis antivirus.	Serie SRX y firewall virtual vSRX
MIB de clase de servicio ATM	Proporciona compatibilidad con interfaces ATM y conexiones virtuales.	Serie ACX, Serie M y Serie T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
ATM MIB	Proporciona compatibilidad para supervisar las configuraciones de clase de servicio (CoS) del circuito virtual (VC) de la versión 2 (ATM2). También proporciona estadísticas de cola de CoS para todos los VC que tienen CoS configurado.	Firewall virtual de las series M, SRX, T y vSRX
BGP4 V2 MIB	Proporciona compatibilidad para supervisar contadores de prefijos BGP recibidos del mismo nivel. Se basa en objetos similares en el MIB documentado en el borrador de Internet draft-ietf-idr-bgp4-mibv2-03.txt, Definiciones de objetos administrados para la cuarta versión de BGP (BGP-4), segunda versión.	Todas las plataformas
BGP MIB	Contiene los objetos para la versión BGP.	serie MX
MIB de detección de reenvío bidireccional	Proporciona compatibilidad para supervisar sesiones de detección de reenvío bidireccional (BFD).	Todas las plataformas
MIB de clúster de chasis	Proporciona información sobre los objetos que se usan siempre que el estado de las interfaces de vínculo de control o de vínculo de estructura cambia (de arriba a abajo o de abajo a arriba) en una implementación de clúster de chasis.	Serie SRX y firewall virtual vSRX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Definiciones de chasis para MIB modelo de enrutador	Contiene los identificadores de objeto (OID) que utiliza la MIB del chasis para identificar la plataforma y los componentes del chasis. La MIB de chasis proporciona información que cambia con frecuencia, mientras que las definiciones de chasis para MIB de modelo de enrutador proporcionan información que cambia con menos frecuencia.	Serie ACX, Serie M, Serie MX, Serie PTX, Serie QFX, SRX550, SRX1500 y Serie T
MIB de chasis	Proporciona soporte para monitoreo ambiental (estado de la fuente de alimentación, voltajes de la placa, ventiladores, temperaturas y flujo de aire) y soporte de inventario para el chasis, la placa de control del sistema (SCB), la placa de sistema y conmutación (SSB), el módulo de conmutación y reenvío (SFM), la placa de estructura del conmutador (SFB), los concentradores de PIC flexibles (FPC) y las PIC.	Todas las plataformas
MIB de clase de servicio	Proporciona compatibilidad para supervisar estadísticas de cola de salida de interfaz por interfaz y por clase de reenvío. Proporciona compatibilidad para supervisar estadísticas de control de flujo basado en prioridades (PFC). Las entradas en el de MIB de clase de servicio incluyen , , , y `.jnxCosPfcPriorityTablejnxCosPfcPriorityEntryjnxCosIfIndexjnxCosPfcPriorityIndexjnxCosPfcPriorityRequestsTxjnxCosPfcPriorityRequestsRx`	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Sistema QFabric, Serie QFX, Serie SRX, Serie T y Firewall virtual vSRX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
CGNAT MIB	Proporciona información sobre las interfaces de servicios utilizadas para la implementación de CGNAT. • SRX – USF (MX-SPC3) JUNIPER-JS-NAT-MIB • MS-MPC JUNIPER-NET-MIB	Serie MX y serie SRX
MIB de administración de la configuración	Proporciona notificaciones para los cambios de configuración como capturas SNMP. Cada interrupción contiene la hora a la que se confirmó el cambio de configuración, el nombre del usuario que realizó el cambio y el método mediante el cual se realizó el cambio. El historial de los últimos 32 cambios de configuración se mantiene en `.jnxCmChgEventTable`	Todas las plataformas
MIB de uso de clase de destino	Proporciona compatibilidad para supervisar los recuentos de paquetes en función de los puntos de entrada y salida del tráfico que transita por las redes. Los puntos de entrada se identifican mediante la interfaz de entrada. Los puntos de salida se identifican mediante prefijos de destino agrupados en uno o más conjuntos, conocidos como clases de destino. Se administra un contador por interfaz por clase de destino, hasta un máximo de 16 contadores por interfaz.	Firewall virtual de las series EX, M, SRX y T y vSRX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
DHCP MIB	Proporciona compatibilidad SNMP (obtener y capturar) para las configuraciones del servidor local y la retransmisión DHCP. También proporciona soporte para tablas de encuadernaciones y arrendamientos, y para estadísticas.	Serie M, MX y T
DHCPv6 MIB	Proporciona compatibilidad SNMP (obtener y capturar) para las configuraciones de servidor local y relé DHCPv6. También proporciona soporte para tablas de encuadernaciones y arrendamientos, y para estadísticas.	Serie M, MX y T
MIB de monitoreo óptico digital	Proporciona soporte para la solicitud de estadísticas y notificaciones de alarmas.**SNMP GetSNMP Trap**	Serie EX, Serie M, Serie MX, Serie PTX y Serie T
MIB de objetos DNS	Proporciona compatibilidad para supervisar consultas, solicitudes, respuestas y errores de proxy DNS.	Serie SRX y firewall virtual vSRX
MIB de captura dinámica de flujo	Proporciona compatibilidad para supervisar el estado operativo de las PIC de captura dinámica de flujo (DFC).	Series M y T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Ethernet MAC MIB	Supervisa las estadísticas de control de acceso a medios (MAC) en las interfaces de cola inteligente (IQ) de Gigabit Ethernet. Recopila estadísticas MAC; por ejemplo, , , , y en cada dirección MAC de origen e ID de LAN virtual (VLAN) para cada puerto Ethernet.`inoctetsinframesoutoctetsoutframes`	Serie EX, Serie M, Serie MX, Serie QFX, SRX300, SRX320, SRX340, SRX550, Serie SRX1500 y T
MIB de eventos	Define una interrupción genérica que se puede generar mediante una secuencia de comandos operacional o una política de eventos. Esta MIB permite especificar una cadena de registro del sistema y generar una interrupción si se encuentra dicha cadena de registro del sistema.	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Sistema QFabric, Serie QFX, SRX1500, SRX300, SRX320, SRX340, SRX550 y Serie T
Experimental MIB	Contiene identificadores de objeto para MIB experimentales.	Serie ACX, Serie M, Serie MX y Serie T
MIB de notificación MAC de la serie EX	Contiene la implementación de Juniper Networks de MIB específica para la empresa para las estadísticas de Mac de Ethernet para la serie EX.	serie EX
MIB SMI serie EX	Contiene la estructura de la información de administración para las plataformas de la serie EX de Juniper Networks.	serie EX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Firewall MIB	Proporciona compatibilidad para supervisar contadores de filtros de firewall . Los enrutadores deben tener el ASIC del procesador de Internet II para realizar la supervisión del firewall.	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Sistema QFabric, Serie QFX, SRX300, SRX320, SRX340, SRX550, Serie SRX1500 y T
MIB de servicios de recolección de flujo	Proporciona estadísticas sobre archivos, registros, memoria, FTP y estados de error de una interfaz de servicios de supervisión. También proporciona capturas SNMP para destinos no disponibles, transferencias de archivos fallidas, sobrecarga de flujo y sobrecarga de memoria.	Series M y T
GRE Keepalive Monitoreo MIB	Proporciona compatibilidad para supervisar el estado keepalive de la encapsulación de enrutamiento genérico (GRE). Esta MIB también proporciona una captura SNMP cuando cambia el estado keepalive GRE.	Instancias de la serie SRX y del firewall virtual vSRX
MIB de recursos de host	Extiende el objeto y proporciona una medida del uso de cada sistema de archivos en el enrutador en formato de porcentaje.`hrStorageTable` Anteriormente, los objetos en el miden el uso en unidades de asignación — y — solamente.`hrStorageTablehrStorageUsedhrStorageAllocationUnits` Con la medición porcentual, puede supervisar y aplicar umbrales de uso.	Serie ACX, Serie EX, Serie M, Serie MX, Serie QFX, SRX300, SRX320, SRX340, SRX550, Serie SRX1500 y T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Interfaz de reenvío contable clase MIB	Amplía la MIB de interfaz empresarial de Juniper y proporciona soporte para monitorear datos estadísticos para la contabilidad de la interfaz y la estandarización del IETF.	Firewall virtual serie M, MX, SRX y vSRX
MIB de interfaz	Amplía el estándar (RFC 2863) con estadísticas adicionales e información de chasis específica para la empresa de Juniper Networks.`ifTable`	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Sistema QFabric, Serie QFX, SRX300, SRX320, SRX340, SRX550, Serie SRX1500 y T
MIB de reenvío IP	Amplía la tabla de reenvío IP estándar MIB (RFC 4292) para incluir información de reenvío de CIDR.	Todas las plataformas
MIB de objeto genérico de supervisión de flujo IPsec	Basada en , esta MIB proporciona compatibilidad para supervisar objetos de administración VPN IPsec e IPsec.`jnx-ipsec-monitor-mib`	Serie SRX y firewall virtual vSRX
MIB de supervisión IPsec	Proporciona información operativa y estadística relacionada con los túneles IPsec e IKE en los enrutadores de Juniper Networks.	Serie M, Serie SRX y Serie T
MIB de objetos VPN IPsec	Proporciona compatibilidad para supervisar objetos de administración VPN IPsec e IPsec para productos Juniper. Esta MIB es una extensión de .`jnx-ipsec-flow-mon.mib`	Serie SRX y Serie MX con USF

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
IPv4 MIB	Proporciona información adicional de direcciones del protocolo de Internet versión 4 (IPv4), lo que admite la asignación de direcciones IPv4 idénticas a interfaces independientes.	Todas las plataformas
MIB IPv6 e ICMPv6	Proporciona estadísticas de IPv6 y Protocolo de mensajes de control de Internet versión 6 (ICMPv6).	Serie M, serie MX, serie PTX, serie SRX, serie T y firewall virtual vSRX
jnxASICExternalMemTraps	Proporciona información sobre el error de memoria externa ASIC.	QFX10002-36Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016, PTX1000, PTX10002-60C, PTX10008, PTX10016
jnxASICExternalMemOKTraps	Proporciona información sobre el error de memoria externa ASIC.	QFX10002-36Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016, PTX1000, PTX10002-60C, PTX10008, PTX10016
jnxHmcFatal	Proporciona información cuando ha fallado la HMC especificada en una FPC específica.	QFX10002-36Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016, PTX1000, PTX10002-60C, PTX10008, PTX10016
jnxHmcOK	Proporciona información cuando la HMC especificada en una FPC específica se ha recuperado del fallo.	QFX10002-36Q, QFX10002-60C, QFX10002-72Q, QFX10008, QFX10016, PTX1000, PTX10002-60C, PTX10008, PTX10016

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
jnxJsChassisHA	Proporciona alta disponibilidad del chasis y garantiza una interrupción mínima de los servicios en caso de conmutación por error. Si uno de los chasis en un entorno de alta disponibilidad falla, el otro chasis asume la función del chasis fallido con una interrupción mínima del servicio. Este módulo define los objetos pertenecientes a la alta disponibilidad del chasis.	SRX5400, SRX5600 y SRX5800.
jnxJsFlowSofSummary MIB	Proporciona el número total de sesiones en modo Express Path (anteriormente conocido como descarga de servicios) en uso y el número total de paquetes procesados hasta ahora en el sistema lógico.	SRX4600, SRX5400, SRX5600 y SRX5800.
jnxJsChNodeCPUStatus	Supervisa el uso de carga de CPU del motor de enrutamiento. Envía una notificación a los usuarios cuando la carga de la CPU del motor de enrutamiento está por debajo del umbral establecido.	SRX5400, SRX5600, SRX5800, SRX4600, SRX4200, SRX4100 y SRX1500.
jnxJsChNodeJunosKernelStatus	Supervisa el uso del kernel de Junos.	SRX5400, SRX5600, SRX5800, SRX4600, SRX4200, SRX4100 y SRX1500.
MIB de jnxUserFirewalls	Exporta estadísticas de los contadores de administración de identidades de Firewall de usuario.	Serie SRX y firewall virtual vSRX
jnxTLBMIB	Exporta estadísticas de la aplicación Traffic Load Balancer	MX240, MX480 y MX960

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
JNX BGP MIB2	Admite objetos IPV6 y contadores de prefijos para BGP.	serie MX
MIB VPN JNX (L2VPN)	Contiene información sobre el protocolo L2VPN.	serie MX
L2ALD MIB	Contiene información sobre el proceso de aprendizaje de direcciones de capa 2 (L2ALD) y las capturas relacionadas, como la captura de límite MAC de instancia de enrutamiento y la captura de límite MAC de interfaz. Esta MIB también proporciona información de VLAN en la tabla para los conmutadores de las series EX y QFX del software mejorado de capa 2 (ELS).`jnxL2aldVlanTable` **NOTA**: Los conmutadores que no son de la serie EX que no son ELS admiten la VLAN MIB (tabla) para información de VLAN en lugar de esta MIB. `jnxExVlanTable`	Serie EX, Serie MX, Serie QFX y Serie T
L2CP MIB	Proporciona información sobre las características basadas en los protocolos de control de capa 2 (L2CP). Actualmente, Junos OS solo admite los objetos , y .`jnxDot1dStpPortRootProtectEnable` `djnxDot1dStpPortRootProtectStatejnx` `PortRootProtectStateChangeTrap`	serie MX
L2TP MIB	Proporciona información acerca de los túneles y las sesiones del Protocolo de transporte de capa 2 (L2TP).	Serie M, MX y T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
LDP MIB	Proporciona estadísticas de LDP y define las notificaciones de ruta de conmutación de etiquetas (LSP) de LDP. Las capturas de LDP solo admiten estándares IPv4.	Serie ACX, Serie M, Serie PTX, Serie SRX y Serie T
Licencia MIB	Amplía la compatibilidad con SNMP a la información de licencias e introduce capturas SNMP que alertan a los usuarios cuando las licencias están a punto de caducar, han caducado o cuando el número total de usuarios supera el número especificado en la licencia.	Serie M, MX, Serie SRX y Serie T
MIB de sistemas lógicos	Extienda la compatibilidad con SNMP al perfil de seguridad de sistemas lógicos mediante varias MIB definidas en `.jnxLsysSecurityProfile`	serie SRX
LTE MIB	Amplíe la compatibilidad con SNMP para supervisar el estado del módulo de interfaz minifísica (Mini-PIM) LTE 4G LTE mediante la gestión de red remota SNMP.	SRX300, SRX320, SRX340, SRX345 y SRX550M.

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
LSYSTSYS MIB (jnxLsysVD)	Proporciona los siguientes detalles de los sistemas lógicos configurados y del inquilino: • recuento total de LSYS • recuento total de TSYS • Número total de perfiles de seguridad • capacidad LSYS máxima permitida • capacidad TSYS máxima permitida • Capacidad máxima permitida de perfiles de seguridad	Firewall virtual SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800 y vSRX
MIMSTP MIB	Proporciona información acerca de las instancias de MSTP (es decir, las instancias de enrutamiento de tipo conmutador virtual/control de capa 2, también conocidas como contextos virtuales), MSTI dentro de la instancia MSTP y VLAN asociadas con MSTI.	Serie MX y Serie T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
MPLS LDP MIB	Contiene definiciones de objetos como se describe en RFC 3815, Definiciones de objetos administrados para la conmutación de etiquetas multiprotocolo (MPLS), Protocolo de distribución de etiquetas (LDP). **NOTA**: Los objetos de la MIB de LDP de MPLS se admiten en versiones anteriores de Junos OS como una MIB de LDP propietaria ().`mib-ldpmib.txt` Como la rama utilizada por el LDP propietario () entra en conflicto con RFC 3812, la MIB LDP propietaria () ha quedado obsoleta y se ha reemplazado por la MPLS LDP MIB () específica de la empresa.`mib-ldpmib.txtmib-ldpmib.txtmib-jnx-mpls-ldp.txt`	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie QFX y Serie T
MPLS MIB	Proporciona información de MPLS y define las notificaciones MPLS. **NOTA**: Para recopilar información acerca de las estadísticas de MPLS en enrutadores de tránsito, utilice la MIB RSVP específica de la empresa () en lugar de la MIB de MPLS específica de la empresa ().`mib-jnx-rsvp.txtmib-jnx-mpls.txt`	Serie ACX, Serie EX, Serie M, Serie MX, Serie PTX, Serie QFX, Serie SRX y Serie T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
MVPN MIB	Contiene objetos que permiten al administrador SNMP supervisar las conexiones MVPN en los enrutadores perimetrales del proveedor. La MIB MVPN específica de la empresa es la extensión de Juniper Networks de las MIB estándar IETF definidas en el borrador de Internet draft-ietf-l3vpn-mvpn-mib-03.txt, Base de información de administración de multidifusión VPN de capa 3 MPLS/BGP.	Todas las plataformas
MPLS L3VPN MIB	Contiene los atributos de MPLS basada en L3VPN.	serie MX
MPLS VPN MIB	Contiene los objetos de VPN MPLS.	serie MX
MIB de objetos NAT	Proporciona compatibilidad para supervisar la traducción de direcciones de red (NAT).	Serie EX y serie SRX
MIB de monitoreo de recursos NAT	Proporciona compatibilidad para supervisar el uso de grupos NAT y reglas NAT. Esta MIB también proporciona notificaciones del uso de recursos NAT. Actualmente, esta MIB solo se admite en la PIC multiservicio y en el DPC multiservicio solo en enrutadores serie M y MX.	Serie M y MX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
MIB de administración de interfaces OTN	Define objetos para administrar interfaces de red de transporte óptico (OTN) en dispositivos que ejecutan Junos OS.	Serie M, Serie MX, Serie PTX y Serie T
MIB del motor de reenvío de paquetes	Proporciona estadísticas de notificación para los motores de reenvío de paquetes.	Serie ACX, Serie EX, Serie M, Serie PTX, Serie SRX y Serie T
MIB de espejo de paquetes	Le permite capturar y ver información relacionada con la duplicación de paquetes. Actualmente, Junos OS solo admite esta MIB para enrutadores de la serie MX. Las capturas de duplicación de paquetes son una extensión de la implementación estándar de SNMP y solo están disponibles para usuarios de SNMPv3.	serie MX
MIB de extensión PAE	Amplía la MIB de extensión PAE IEEE802.1x estándar y contiene información para la autenticación MAC estática.	serie EX
MIB de monitoreo pasivo	Realiza monitoreo de flujo de tráfico e interceptación legal de paquetes que transitan entre dos enrutadores.	Series M y T

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Ping MIB	Amplía la tabla de control Ping MIB estándar (RFC 2925). Los elementos de esta MIB se crean cuando se crean entradas en la MIB de ping.`pingCtlTable` Cada elemento se indexa exactamente como está en la MIB de ping.	Serie ACX, Serie EX, Serie M, Serie MX, Serie QFX, Serie SRX y Serie T
MIB de objetos de directiva	Proporciona compatibilidad para supervisar las directivas de seguridad que controlan el flujo de tráfico de una zona a otra.	serie SRX
Unidad de fuente de alimentación MIB	Permite la supervisión y administración de la fuente de alimentación en un dispositivo que ejecuta Junos OS.	Serie EX y sistema QFabric
PPP MIB	Proporciona compatibilidad SNMP con información relacionada con PPP, como el tipo de autenticación utilizada, las características de la interfaz, el estado y las estadísticas. Esta MIB es compatible con el proceso PPP de Common Edge, jpppd.	Serie M y MX
PPPoE MIB	Proporciona compatibilidad SNMP con información relacionada con PPPoE, como el tipo de autenticación utilizada, las características de la interfaz, el estado y las estadísticas. Esta MIB es compatible con el proceso PPPoE de Common Edge, jpppoed.	Serie M y MX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Pseudowire ATM MIB	Amplía la MIB de pseudocable estándar y define los objetos utilizados para administrar los pseudocables ATM en los productos de Juniper. La MIB ATM de pseudocable específica para la empresa es la implementación de Juniper Networks del RFC 5605, Objetos administrados para ATM a través de redes conmutadas de paquetes (PSN).	Serie M y MX
MIB TDM de pseudocable	Extiende la MIB de pseudocable estándar y contiene información sobre la configuración y las estadísticas de tipos específicos de pseudocables. La MIB de TDM de pseudocable específica para la empresa es la implementación de Juniper Networks de los objetos administrados estándar para TDM a través de MIB de red conmutada de paquetes (draft-ietf-pwe3-tdm-mib-08.txt).	Serie ACX, Serie M y Serie T
PTP MIB	Supervisa el funcionamiento de los relojes PTP dentro de la red.	serie MX
MIB de monitoreo de rendimiento en tiempo real	Proporciona datos relacionados con el rendimiento en tiempo real y le permite acceder a mediciones y cálculos de fluctuación mediante SNMP.	Serie EX, Serie M, Serie MX, Serie SRX y Serie T
MIB de reenvío de ruta inversa	Supervisa las estadísticas del tráfico rechazado debido al procesamiento del reenvío de rutas inversas (RPF).	Todas las plataformas

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
MIB de eventos y alarmas de RMON	Admite las extensiones de Junos OS para la MIB de eventos y alarmas de monitoreo remoto (RMON) estándar (RFC 2819). La extensión aumenta con información adicional sobre cada alarma.`alarmTable` También se definen dos nuevas trampas para indicar cuándo se encuentran problemas con una alarma.	Todas las plataformas
RSVP MIB	Proporciona información acerca de las sesiones de ingeniería de tráfico RSVP que corresponden a los LSP MPLS en enrutadores de tránsito en la red principal del proveedor de servicios. **NOTA**: Para recopilar información acerca de las estadísticas de MPLS en enrutadores de tránsito, utilice la MIB RSVP específica de la empresa () en lugar de la MIB de MPLS específica de la empresa ().`mib-jnx-rsvp.txt``mib-jnx-mpls.txt`	Serie ACX, Serie M, Serie MX, Serie PTX y Serie T
Servicio OAM MIB	La MIB proporciona compatibilidad con SNMP para las funciones de supervisión del rendimiento de OAM de servicio.`jnx-soam-pm.mib`	Serie SRX380, SRX300, SRX320, SRX340, SRX345 y MX.
Objetos de extensión de interfaz de seguridad MIB	Proporciona compatibilidad para la administración de seguridad de interfaces.	Firewall virtual de las series EX, SRX y vSRX
MIB de objetos de control de seguridad	Define la MIB para la funcionalidad de pantalla del firewall empresarial de Juniper Networks.	Serie SRX y firewall virtual vSRX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Servicios PIC MIB	Proporciona las estadísticas de PIC de servicios adaptativos (AS) y define las notificaciones para PIC de AS.	Series M y T
SNMP IDP MIB	Contiene la implementación de Juniper Networks de MIB específica de la empresa para IDP.	Serie SRX y firewall virtual vSRX
MIB DE PUNTOS DE ACCESO SONET	Supervisa cualquier interfaz SONET que participe en la conmutación automática de protección (APS).	Series M y T
MIB de administración de interfaces SONET/SDH	Monitorea la alarma actual para cada interfaz SONET/SDH.	Series M y T
MIB de uso de clase de origen	Cuenta los paquetes enviados a los clientes realizando una búsqueda en la dirección IP de origen y la dirección IP de destino. La MIB de uso de clase de origen (SCU) permite realizar un seguimiento del tráfico que se origina en prefijos específicos en el núcleo del proveedor y se destina a prefijos específicos en el borde del cliente.	Serie M, T y SRX
MIB de monitoreo de SPU	Proporciona compatibilidad para supervisar SPU en dispositivos SRX5600 y SRX5800.	Serie SRX y firewall virtual vSRX
Estructura de la información de gestión MIB	Explica cómo se estructuran las MIB específicas de la empresa de Juniper Networks.	Serie ACX, Serie EX, Serie M, Serie MX, Serie QFX, Serie SRX, Serie T y Firewall virtual vSRX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Estructura de la información de administración MIB para conmutadores Ethernet serie EX	Define una rama MIB para definiciones MIB relacionadas con la conmutación para los conmutadores Ethernet de la serie EX.	serie EX
Estructura de la información de gestión MIB para la serie SRX	Contiene identificadores de objeto (OID) para la rama de seguridad de las MIB usadas en Junos OS para firewalls, servicios y capturas de la serie SRX.	Serie SRX y firewall virtual vSRX
MIB de suscriptor	Proporciona compatibilidad con SNMP para información relacionada con el suscriptor.	Serie ACX, Serie MX y Serie T
MIB de registro del sistema	Permite la notificación de una aplicación basada en capturas SNMP cuando aparece un mensaje importante de registro del sistema.	Serie EX, Serie M, Serie MX, Serie PTX, Serie QFX, Serie SRX y Serie T
MIB de temporización	Define objetos, errores y eventos de Ethernet sincrónico (SyncE) y Protocolo de tiempo de precisión (PTP).	ACX710
Traceroute MIB	Admite las extensiones de Junos OS de traceroute y operaciones remotas. Los elementos de esta MIB se crean cuando se crean entradas en la MIB de Traceroute.`traceRouteCtlTable` Cada elemento se indexa exactamente de la misma manera que en la MIB de Traceroute.	Firewall virtual de las series EX, M, MX, SRX y T y vSRX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
Estadísticas de túnel MIB	Admite la supervisión de estadísticas de túnel para túneles IPV4 sobre IPV6. Esta MIB muestra actualmente tres contadores: recuento de túneles en rpd, recuento de túneles en kernel y recuento de túneles en el motor de reenvío de paquetes.	Todas las plataformas
MIB de utilidad	Proporciona compatibilidad SNMP para exponer los datos de Junos OS y tiene tablas que contienen información sobre cada tipo de datos, como enteros y cadenas.	Serie EX, Serie M, Serie MX, Sistema QFabric, Serie QFX, Serie SRX, Serie T y Firewall virtual vSRX
MIB de chasis virtual	Contiene información sobre el chasis virtual de los conmutadores Ethernet de la serie EX y de la serie MX.	Serie EX y Serie MX
VLAN MIB	Contiene información acerca de las VLAN IEEE 802.10 preestándar y su asociación con clientes de emulación LAN. **NOTA**: Para los conmutadores serie ELS EX y QFX, la información de VLAN se proporciona en la MIB L2ALD de la tabla en lugar de en esta MIB.`jnxL2aldVlanTable` Los conmutadores Ethernet que no son de la serie EX de ELS utilizan la tabla de esta MIB para proporcionar información de configuración de VLAN, y la tabla de esta MIB ha quedado obsoleta y ya no se utiliza.`jnxExVlanTablejnxVlanTable`	Series EX y QFX

Tabla 56: MIB específicas de la empresa compatibles con Junos OS *(Continued)*

MIB específica de la empresa	Description	Plataformas
MIB de VPLS	Proporciona información sobre VPLS genéricos, basados en BGP y en LDP, y pseudocables asociados con las redes VPLS. Las MIB VPLS específicas de la empresa son extensiones de Juniper Networks de las siguientes MIB estándar IETF definidas en el borrador de Internet draft-ietf-l2vpn-vpls-mib-05.txt y se implementan como parte de la rama:`jnxExperiment` • `VPLS-Generic-Draft-01-MIB` implementado como `mib-jnx-vpls-generic.txt` • `VPLS-BGP-Draft-01-MIB` implementado como `mib-jnx-vpls-bgp.txt` • `VPLS-LDP-Draft-01-MIB` implementado como `mib-jnx-vpls-ldp.txt`	Serie M, MX y T
MIB de objetos de certificado VPN	Proporciona compatibilidad para supervisar los certificados locales y de CA cargados en el enrutador.	Firewall virtual de las series EX, SRX y vSRX
VPN MIB	Proporciona supervisión para VPN de capa 3, VPN de capa 2 y servicio de LAN privada virtual (VPLS) (solo acceso de lectura).	Serie ACX, Serie EX, Serie M, Serie MX y Serie T

A partir de Junos OS versión 18.4R1, puede supervisar el estado de Mini-PIM 4G LTE mediante la administración de red remota SNMP.

Puede usar los siguientes comandos para monitorear el estado de Mini-PIM 4G LTE:

```
show snmp mib walk ascii jnxWirelessWANNetworkInfoTable
```

```
show snmp mib walk ascii jnxWirelessWANFirmwareInfoTable
```

A partir de Junos OS versión 19.4R1, en dispositivos de línea SRX5000 con tarjeta SRX5K-SPC3, hemos mejorado la MIB del monitor de flujo VPN IPsec existente para admitir las estadísticas globales de IKE para túneles que usan IKEv2.**jnxIpSecFlowMonMIB** Utilice el comando para mostrar las estadísticas globales de los túneles, como las negociaciones en curso, establecidas y caducadas mediante IKEv2.`show security ike stats`

A partir de Junos OS versión 20.1R1, puede habilitar las capturas de túnel emparejado e IPsec, así como configurar las capturas de certificados (CA) y locales. Hemos mejorado la MIB de monitor de flujo VPN IPsec existente para admitir el plano de datos global, SA IKE activa, SA IPsec activa y estadísticas de pares activas para túneles que usan IKEv2.**jnxIpSecFlowMonMIB** También hemos mejorado la salida del comando para agregar opciones adicionales.`show security ike stats(<brief> | <detail>)` Use el comando para borrar los contadores de estadísticas de IKEv2.`clear security ike stats`

A partir de Junos OS versión 20.4R1, puede supervisar el uso de la CPU y del kernel en el motor de enrutamiento mediante el proceso reswatch.

SEE ALSO

Guía de administración y monitoreo de red

MIB estándar para Junos OS evolucionado

Tabla 57 en la página 674 muestra las MIB estándar admitidas en Junos OS Evolved. Para obtener información acerca de los objetos MIB estándar, consulte el Explorador de MIB SNMP.https://apps.juniper.net/mib-explorer/

Tabla 57: MIB estándar compatibles con Junos OS Evolved

MIB estándar	Excepciones	Plataformas
RFC 1155, Estructura e identificación de la información de administración para Internets basadas en TCP/IP	Sin excepciones	PTX10003
RFC 1157, Un protocolo simple de administración de red (SNMP)	Sin excepciones	PTX10003
RFC 1212, Definiciones MIB concisas	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 1213, *Base de información de administración para la administración de red de Internets basadas en TCP/IP: MIB-II*	Tablas y objetos no compatibles: • Grupo ICMP	PTX10003
RFC 1215, Una convención para definir trampas para su uso con SNMP	Sin excepciones	PTX10003
RFC 1850, OSPF versión 2 Base de información de administración	Sin excepciones	PTX10003
RFC 1901, Introducción al SNMPv2 basado en la comunidad	Sin excepciones	PTX10003
RFC 2011, Base de información de administración SNMPv2 para el protocolo de Internet mediante SMIv2	Sin excepciones	PTX10003
RFC 2096, Tabla de reenvío IP MIB	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 2465, Base de información de administración para IP versión 6: *Convenciones textuales y Grupo General*	Tablas y objetos admitidos: • ipv6AddrTable • ipv6NetToMediaTable • ipv6IfTable • ipv6IfStatsTable • ipv6AddrPrefixTable • ipv6IfTableLastChange • ipv6Interfaces • ipv6Reenvío • ipv6DefaultHopLimit	PTX10003
RFC 2576, Coexistencia entre la versión 1, la versión 2 y la versión 3 del marco de administración de red estándar de Internet	Sin excepciones	PTX10003
RFC 2578, Estructura de la información de gestión versión 2 (SMIv2)	Sin excepciones	PTX10003
RFC 2579, Convenciones textuales para SMIv2	Sin excepciones	PTX10003
RFC 2580, Declaraciones de conformidad para SMIv2	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 2665, Definiciones de objetos administrados para los tipos de interfaz similares a Ethernet	Tablas y objetos no compatibles: • dot3	PTX10003
RFC 2790, MIB de recursos de host	Tablas y objetos no compatibles: • hrDeviceTable • hrSWRunTable • hrSWRunPerfTabl e	PTX10003
RFC 2863, El grupo de interfaces MIB	Sin excepciones	PTX10003
RFC 2864, La extensión de tabla de pila invertida para el grupo de interfaces MIB	Sin excepciones	PTX10003
RFC 2925, Definiciones de objetos administrados para operaciones remotas de ping, traceroute y búsqueda	Sin excepciones	PTX10003
RFC 2932, MIB de enrutamiento de multidifusión IPv4	Sin excepciones	PTX10003
RFC 2934, MIB de multidifusión independiente del protocolo para IPv4	Sin excepciones	PTX10003
RFC 2981, MIB de eventos	Sin excepciones	PTX10003
RFC 3014, MIB de registro de notificaciones	Sin excepciones	PTX10003
RFC 3019, Base de información de administración IP versión 6 para el protocolo de detección de escucha de multidifusión	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 3410, Declaraciones de introducción y aplicabilidad para el marco de administración estándar de Internet	Sin excepciones	PTX10003
RFC 3411, Una arquitectura para describir marcos de administración del Protocolo simple de administración de red (SNMP)	Sin excepciones	PTX10003
RFC 3412, Procesamiento y envío de mensajes para el Protocolo simple de administración de red (SNMP)	Sin excepciones	PTX10003
RFC 3413, Aplicaciones del Protocolo simple de administración de redes (SNMP)	Sin excepciones	PTX10003
RFC 3414, Modelo de seguridad basado en el usuario (USM) para la versión 3 del Protocolo simple de administración de redes (SNMPv3)	Sin excepciones	PTX10003
RFC 3415, Modelo de control de acceso basado en vista (VACM) para el Protocolo simple de administración de redes (SNMP)	Sin excepciones	PTX10003
RFC 3416, versión 2 de las operaciones de protocolo para el protocolo simple de administración de red (SNMP)	Sin excepciones	PTX10003
RFC 3417, Asignaciones de transporte para el Protocolo simple de administración de redes (SNMP)	Sin excepciones	PTX10003
RFC 3418, Base de información de administración (MIB) para el Protocolo simple de administración de redes (SNMP)	Sin excepciones	PTX10003
RFC 3584, Coexistencia entre la versión 1, la versión 2 y la versión 3 del marco de administración de red estándar de Internet	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 3635, Definiciones de objetos administrados para los tipos de interfaz similares a Ethernet	Sin excepciones	PTX10003, PTX10008
RFC 3637, Definiciones de objetos administrados para la subcapa de interfaz WAN Ethernet	Sin excepciones	PTX10003
RFC 3811, Definiciones de convenciones textuales (TC) para la administración de conmutación de etiquetas multiprotocolo (MPLS)	Sin excepciones	PTX10003
RFC 3812, Base de información de gestión (MIB) de ingeniería de tráfico (TE) de conmutación de etiquetas multiprotocolo (MPLS) (acceso de solo lectura)	Sin excepciones	PTX10003
RFC 3813, Base de información de administración (MIB) del enrutador de conmutación de etiquetas (LSR) de conmutación de etiquetas multiprotocolo (MPLS)	Tablas y objetos no compatibles (acceso de solo lectura): • mplsInterfacePerf Table • mplsInSegmentPe rfTable • mplsOutSegment PerfTable • mplsInSegmentMa pTable • mplsXCUp • mplsXCDown	PTX10003
RFC 3826, El algoritmo de cifrado del estándar de cifrado avanzado (AES) en el modelo de seguridad basado en el usuario SNMP	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 3877, Base de información de gestión de alarmas	Sin excepciones	PTX10003
RFC 4087, MIB de túnel IP	Describe los objetos MIB en las tablas siguientes para administrar túneles de cualquier tipo en redes IPv4 e IPv6: • tunnelIfTable: proporciona información sobre los túneles conocidos por un enrutador. • tunnelInetConfigTable: ayuda a la creación dinámica de túneles y proporciona la asignación desde las direcciones del punto de conexión al valor de índice de la interfaz actual.	Serie PTX (PTX10008, PTX10001-36MR, PTX10001 y PTX10004)

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 4133, Entidad MIB	Tabla admitida: • entPhysicalTable • entPhysicalModelName: proporciona información para el inventario de FRU (unidades reemplazables en campo) y la comprobación de estado mediante SNMP.	PTX10003
RFC 4292, MIB de reenvío de IP	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 4293, Base de información de administración para el protocolo de Internet (IP)	Tablas admitidas: • ipAddressTable • ipAddrTable • ipNetToPhysicalTable • ipNetToMediaTable • ipSystemStatsTable Objetos no compatibles: • icmpMsgStatsIPVersion • icmpMsgStatsType • icmpMsgStatsInPkts • icmpMsgStatsOutPkts • icmpStatsIPVersion • icmpStatsInMsgs • icmpStatsInErrors • icmpStatsOutMsgs • icmpStatsOutErrors	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
RFC 4293, Base de información de administración para el protocolo de Internet (IP)	Tablas admitidas: • icmpStatsTable • icmpMsgStatsTable	ACX7100-32C, PTX10008 y QFX10008
RFC 4444, IS-IS MIB	Sin excepciones	PTX10003
RFC 5643, Base de información de administración para OSPFv3 (acceso de solo lectura)	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
IEEE, 802.3ad, agregación de múltiples segmentos de vínculo	Objetos admitidos para PTX10008 en Junos OS Evolved versión 20.1R1: • , , , , , , ydot3adAggPortStatsLACPDUsRxdot3adAggPortStatsMarkerPDUsRxdot3adAggPortStatsMarkerResponsePDUsRxdot3adAggPortStatsUnknownRxdot3adAggPortStatsIllegalRxdot3adAggPortStatsLACPDUsTxdot3adAggPortStatsMarkerPDUsTxdot3adAggPortStatsMarkerResponsePDUsTx • , , , y .dot3adInterfaceNamedot3adOperStatedot3adAggnamedot3adInterfaceTimeout Objetos no admitidos para PTX10008 en Junos OS Evolved versión 20.1R1: • , , , y .dot3adAggActorSystemPrioritydot3adAggActorSystemIDdot3adAggActorAdminKeydot3adAggActorOperKey	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
	• , , , , , , ydot3adAggMACAddressdot3adAggAggregateOrIndividualdot3adAggPartnerSystemIDdot3adAggPartnerSystemPrioritydot3adAggPartnerOperKeydot3adAggCollectorMaxDelaydot3adAggPortListPortsdot3adTablesLastChanged • , , , , „ ydot3adAggPortActorSystemPrioritydot3adAggPortActorSystemIDdot3adAggPortActorAdminKeydot3adAggPortActorOperKeydot3adAggPortActorPortdot3adAggPortActorPortPrioritydot3adAggPortActorAdminStatedot3adAggPortActorOperState • , , , , „ , , , y dot3adAggPortPartnerAdminSystemPrioritydot3adAggPortPartnerOperSystemPrioritydot3adAggPortPartnerAdminSystemIDdot3adAggPortPartnerOperSystemIDdot3adAggPortPartner	

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
	AdminKeydot3adAggPortPartnerOperKeydot3adAggPortPartnerAdminPortdot3adAggPortPartnerOperPortdot3adAggPortPartnerAdminPortPrioritydot3adAggPortPartnerOperPortPriority • , , , , , y .dot3adAggPortDebugRxStatedot3adAggPortDebugLastRxTimedot3adAggPortDebugMuxStatedot3adAggPortDebugMuxReasondot3adAggPortDebugActorChurnStatedot3adAggPortDebugPartnerChurnStatedot3adAggPortDebugActorChurnCountdot3adAggPortDebugPartnerChurnCountdot3adAggPortDebugActorSyncTransitionCountdot3adAggPortDebugPartnerSyncTransitionCountdot3adAggPortDebugActorChangeCountdot3adAggPortDebugPartnerChangeCount	
Autoridad de asignación de números de Internet, IANAiftype Textual Convention MIB	Sin excepciones	PTX10003

Tabla 57: MIB estándar compatibles con Junos OS Evolved *(Continued)*

MIB estándar	Excepciones	Plataformas
Borrador de Internet draft-ietf-idmr-igmp-mib-13.txt, MIB del Protocolo de administración de grupos de Internet (IGMP)	Sin excepciones	PTX10003
Borrador de Internet draft-reeder-snmpv3-usm-3desede-00.txt, Extensión del modelo de seguridad basado en el usuario (USM) para admitir el EDE de triple DES en modo CBC "externo"	Sin excepciones	PTX10003
Borrador de Internet draft-ietf-isis-wg-mib-07.txt, Base de información de gestión para IS-IS	Sin excepciones	PTX10003
Borrador de Internet draft-ietf-ospf-ospfv3-mib-11.txt, Base de información de gestión para OSPFv3	Sin excepciones	PTX10003
Borrador de Internet draft-ietf-idmr-pim-mib-09.txt, MIB de multidifusión independiente del protocolo (PIM)	Sin excepciones	PTX10003
Borrador de Internet P2MP MPLS-TE MIB (draft-ietf-mpls-p2mp-te-mib-09.txt) (acceso de solo lectura)	Sin excepciones	PTX10003

Preguntas frecuentes sobre SNMP de Junos OS

summary

Este documento presenta las preguntas más frecuentes sobre las funciones y tecnologías utilizadas para implementar servicios SNMP en dispositivos de Juniper Networks con el sistema operativo Junos.

in this section

- Preguntas frecuentes de soporte SNMP de Junos OS | **688**
- Preguntas frecuentes sobre MIB de Junos OS | **689**

- Preguntas frecuentes sobre la configuración SNMP de Junos OS | 698
- Preguntas frecuentes sobre SNMPv3 | 703
- Preguntas frecuentes sobre la interacción SNMP con dispositivos de Juniper Networks | 706
- Preguntas frecuentes sobre capturas e informes SNMP | 708
- Preguntas frecuentes de la configuración del motor de enrutamiento dual de Junos OS | 715
- Preguntas frecuentes sobre la compatibilidad de SNMP con instancias de enrutamiento | 717
- Preguntas frecuentes sobre contadores SNMP | 718

SNMP permite a los usuarios monitorear dispositivos de red desde una ubicación central.

Preguntas frecuentes de soporte SNMP de Junos OS

En esta sección se proporcionan las preguntas y respuestas más frecuentes relacionadas con la compatibilidad con SNMP en Junos OS.

Which SNMP versions does Junos OS support?

Junos OS admite SNMP versión 1 (SNMPv1), versión 2 (SNMPv2c) y versión 3 (SNMPv3). De forma predeterminada, SNMP está deshabilitado en un dispositivo de Juniper Networks.

Which ports (sockets) does SNMP use?

El puerto predeterminado para las consultas SNMP es el puerto 161. El puerto predeterminado para las capturas e informes SNMP es el puerto 162. El puerto utilizado para las capturas e informes SNMP es configurable y puede configurar el sistema para que utilice puertos distintos del puerto predeterminado 162. Sin embargo, el puerto de escucha SNMP seguirá siendo el mismo; esto se establece en el RFC.

Is SNMP support different among the Junos OS platforms?

No, la compatibilidad con SNMP no es diferente entre las plataformas de Junos OS. La configuración, la interacción y el comportamiento de SNMP son los mismos en cualquier dispositivo Junos OS. La única diferencia que puede ocurrir entre plataformas es el soporte MIB.

Consulte también Explorador de MIB SNMP para obtener una lista de las MIB compatibles con las plataformas de Junos OS.

Does Junos OS support the user-based security model (USM)?

Sí, Junos OS admite USM como parte de su compatibilidad con SNMPv3. SNMPv3 contiene más medidas de seguridad que las versiones anteriores de SNMP, incluido el suministro de un USM definido. SNMPv3 USM proporciona seguridad de mensajes mediante la integridad de datos, la autenticación de origen de datos, la protección de reproducción de mensajes y la protección contra la divulgación de la carga del mensaje.

Does Junos OS support the view-based access control model (VACM)?

Sí, Junos OS admite VACM como parte de su compatibilidad con SNMPv3. SNMPv3 contiene más medidas de seguridad que las versiones anteriores de SNMP, incluido el suministro de un VACM definido. SNMPv3 VACM determina si se permite un tipo específico de acceso (lectura o escritura) a la información de administración.

Does Junos OS support SNMP informs?

Sí, Junos OS admite SNMP informa como parte de su compatibilidad con SNMPv3. Los informes SNMP son notificaciones confirmadas enviadas por agentes SNMP a los administradores SNMP cuando ocurren eventos significativos en un dispositivo de red. Cuando un administrador SNMP recibe un informe, envía una respuesta al remitente para verificar la recepción del informe.

Can I provision or configure a device using SNMP on Junos OS?

No, no se permite el aprovisionamiento o la configuración de un dispositivo mediante SNMP en Junos OS.

Preguntas frecuentes sobre MIB de Junos OS

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con las MIB de Junos OS.

What is a MIB?

Una base de información de administración (MIB) es una tabla de definiciones para objetos administrados en un dispositivo de red. SNMP utiliza las MIB para mantener definiciones estándar de todos los componentes y sus condiciones de funcionamiento dentro de un dispositivo de red. Cada objeto en el MIB tiene un código de identificación llamado identificador de objeto (OID).

Las MIB son estándar o específicas de la empresa. Las MIB estándar son creadas por el Grupo de trabajo de ingeniería de Internet (IETF) y documentadas en varias RFC. Las MIB específicas de la empresa son desarrolladas y respaldadas por un fabricante de equipos específico.

Para obtener una lista de las MIB estándar compatibles, consulte MIB SNMP estándar compatibles con Junos OS."MIB SNMP estándar compatibles con Junos OS" en la página 621

Para obtener una lista de las MIB específicas de la empresa de Juniper Networks, consulte MIB SNMP específicas de la empresa compatibles con Junos OS."MIB SNMP específicas de la empresa compatibles con Junos OS" en la página 650

Do MIB files reside on the Junos OS devices?

No, los archivos MIB no residen en los dispositivos Junos OS. Debe descargar los archivos MIB de la página de publicaciones técnicas de Juniper Networks para la versión necesaria de Junos OS: Explorador SNMP MIB.https://apps.juniper.net/mib-explorer/

How do I compile and load the Junos OS MIBs onto an SNMP manager or NMS?

Para que los sistemas de administración de red (NMS) identifiquen y comprendan los objetos MIB utilizados por Junos OS, primero debe cargar los archivos MIB en el NMS mediante un compilador MIB. Un compilador MIB es una utilidad que analiza la información MIB, como los nombres de objeto, identificadores y tipos de datos MIB para el NMS.

Puede descargar el paquete MIB de Junos OS desde la sección MIB y capturas específicas de la empresa en SNMP MIB Explorer o https://www.juniper.net/documentation/software/junos/index.html .https://apps.juniper.net/mib-explorer/https://www.juniper.net/documentation/software/junos/index.html

El paquete MIB de Junos OS tiene dos carpetas: , que contiene MIB estándar compatibles con dispositivos Juniper Networks y , que contiene MIB específicas de la empresa de Juniper Networks.`StandardMibsJuniperMibs` Debe tener las MIB estándar necesarias descargadas y descomprimidas antes de descargar cualquier MIB específica de la empresa. Puede haber dependencias que requieran que una MIB estándar determinada esté presente en el compilador antes de cargar una MIB específica de la empresa.

El paquete MIB de Junos OS está disponible en formatos y ..`zip.tar` Descargue el formato adecuado a sus necesidades.

Siga estos pasos para cargar archivos MIB en dispositivos que ejecutan Junos OS:

1. Vaya a la página de descarga del software de Juniper Networks correspondiente y busque el vínculo debajo de la sección.`Enterprise MIBsEnterprise-Specific MIBs and Traps`

> **NOTA**: Aunque el vínculo se titula , tanto las MIB estándar como las MIB específicas de la empresa están disponibles para su descarga desde esta ubicación.`Enterprise MIBs`

2. Haga clic en el vínculo o para descargar el paquete MIB de Junos OS.`TARZIP`

3. Descomprima el archivo (o) utilizando una utilidad adecuada.`.tar.zip`

> **NOTA**: Algunos compiladores MIB de uso común están precargados con MIB estándar. Puede omitir los pasos 4 y 5 y continuar con el paso 6 si ya tiene las MIB estándar cargadas en el sistema.

4. Cargue los archivos MIB estándar desde la carpeta.`StandardMibs`

   Cargue los archivos en el orden siguiente:

   1. mib-SNMPv2-SMI.txt
   2. mib-SNMPv2-TC.txt
   3. mib-IANAifType-MIB.txt
   4. mib-IANA-RTPROTO-MIB.txt
   5. mib-rfc1907.txt
   6. mib-rfc2011a.txt
   7. mib-rfc2012a.txt
   8. mib-rfc2013a.txt
   9. mib-rfc2863a.txt

5. Cargue los archivos MIB estándar restantes.

> **NOTA**: Debe seguir el orden especificado en este procedimiento y asegurarse de que todas las MIB estándar estén cargadas antes de cargar las MIB específicas de la empresa. Puede haber dependencias que requieran que una MIB estándar determinada esté presente en el compilador antes de cargar una MIB específica de la empresa. Las dependencias se enumeran en la sección del archivo MIB.`IMPORT`

6. Después de cargar las MIB estándar, cargue la MIB de SMI específica para empresa de Juniper Networks y las siguientes MIB de SMI opcionales según sus requisitos:`mib-jnx-smi.txt`

   - mib-jnx-exp.txt: (recomendado) para objetos MIB experimentales de Juniper Networks
   - mib-jnx-js-smi.txt: (Opcional) para objetos de árbol MIB de Juniper Security

- mib-jnx-ex-smi.txt: (Opcional) para conmutadores Ethernet de la serie EX

7. Cargue desde la carpeta las MIB específicas de empresa que desee restantes.`JuniperMibs`

> **CONSEJO**: Al cargar un archivo MIB, si el compilador devuelve un mensaje de error que indica que alguno de los objetos no está definido, abra el archivo MIB con un editor de texto y asegúrese de que todos los archivos MIB enumerados en la sección estén cargados en el compilador.`IMPORT` Si alguno de los archivos MIB enumerados en la sección no está cargado en el compilador, cargue primero el archivo o archivos que faltan y, a continuación, intente cargar el archivo MIB que falló.`IMPORT`
>
> El sistema puede devolver un error si los archivos no se cargan en un orden determinado.

What is SMI?

La versión de estructura de la información de administración (SMI) es un subconjunto de la notación abstracta de sintaxis uno (ASN.1), que describe la estructura de los objetos. SMI es la sintaxis de notación, o "gramática", que es el estándar para escribir MIB.

Which versions of SMI does Junos OS support?

Junos OS admite SMIv1 para MIB SNMPv1 y SMIv2 para SNMPv2c y MIB empresariales.

Does Junos OS support MIB II?

Sí, Junos OS es compatible con MIB II, la segunda versión del estándar MIB.

Las características de MIB II incluyen:

- Adiciones que reflejan los nuevos requisitos operativos.
- Compatibilidad con versiones anteriores de las MIB y SNMP originales.
- Soporte mejorado para entidades multiprotocolo.
- Legibilidad mejorada.

Are the same MIBs supported across all Juniper Networks devices?

Existen algunas MIB comunes compatibles con todos los dispositivos Junos OS, como la MIB de interfaz (ifTable), la MIB de sistema y la MIB de chasis. Algunas MIB solo son compatibles con funcionalidades de plataformas específicas. Por ejemplo, la MIB de puente es compatible con los conmutadores Ethernet de la serie EX y los firewalls de la serie SRX para la sucursal.

What is the system object identifier (SYSOID) of a device? How do I determine the SYSOID of my device?

La MIB jnx-chas-defines (definiciones de chasis para el modelo de enrutador) tiene una rama para cada dispositivo Junos OS.`jnxProductName` El ID de objeto del sistema de un dispositivo es idéntico al ID de objeto del para la plataforma.`jnxProductName` Por ejemplo, para un enrutador perimetral multiservicio M7i, jnxProductNameM7i es .1.3.6.1.4.1.2636.1.1.1.2.10 en la rama jnxProductName, que es idéntico al SYSOID del M7i (.1.3.6.1.4.1.2636.1.1.1.2.10).

How can I determine if a MIB is supported on a platform? How can I determine which MIBs are supported by a device?

La compatibilidad con dispositivos y plataformas MIB se enumera en la documentación técnica de Junos OS. Consulte MIB SNMP estándar compatibles con Junos OS y MIB SNMP específicas de la empresa compatibles con documentos de Junos OS para ver la lista de MIB y dispositivos Junos OS compatibles."MIB SNMP estándar compatibles con Junos OS" en la página 621"MIB SNMP específicas de la empresa compatibles con Junos OS" en la página 650

What can I do if the MIB OID query is not responding?

Puede haber varias razones por las que la consulta OID MIB deja de responder. Una razón podría ser que el propio MIB no responde. Para comprobar que la MIB responde, utilice el comando:`show snmp mib walk | get MIB name | MIB OID`

- Si la MIB responde, el problema de comunicación existe entre el SNMP principal y el agente SNMP. Las posibles razones de este problema incluyen problemas de red, una configuración de comunidad incorrecta, una configuración SNMP incorrecta, etc.

- Si la MIB no responde, habilite SNMP para registrar PDU y errores.`traceoptions` Se registran todas las PDU SNMP entrantes y salientes. Compruebe el resultado para ver si hay algún error.`traceoptions`

Si sigue teniendo problemas con la consulta OID de MIB, el soporte técnico del producto está disponible a través del Centro de asistencia técnica de Juniper Networks (JTAC).

What is the enterprise branch number for Junos OS?

El número de sucursal empresarial de Junos OS es 2636. Los números de sucursal empresarial se utilizan en las configuraciones SNMP MIB y también se conocen como códigos de empresa privada de administración de red SMI.

Which MIB displays the hardware and chassis details on a Juniper Networks device?

La MIB del chasis (jnxchassis.mib) muestra los detalles del hardware y del chasis de cada dispositivo de Juniper Networks. Proporciona información sobre el enrutador y sus componentes. Los objetos MIB del chasis representan cada componente y su estado.

Which MIB objects can I query to determine the CPU and memory utilization of the Routing Engine, Flexible PIC Concentrator (FPC), and PIC components on a device?

Consulte los objetos MIB del chasis y averigüe el uso de CPU y memoria de los componentes de hardware de un dispositivo.`jnxOperatingMemoryjnxOperatingtBufferjnxOperatingCPU`

Is the interface index (ifIndex) persistent?

El ifIndex es persistente cuando se producen reinicios si la versión de Junos OS sigue siendo la misma, lo que significa que los valores asignados a las interfaces en el ifIndex no cambian.

Cuando hay una actualización de software, el dispositivo intenta mantener el ifIndex persistente en el mejor esfuerzo. Para Junos OS versión 10.0 y anteriores, el ifIndex no es persistente cuando hay una actualización de software a Junos OS versión 10.1 y posteriores.

Is it possible to set the ifAdminStatus?

SNMP no puede establecer ifAdminStatus.

Which MIB objects support SNMP set operations?

Las operaciones del conjunto SNMP de Junos OS se admiten en las siguientes tablas y variables MIB:

- snmpCommunityTable
- eventTable
- alarmTable
- snmpTargetAddrExtTable
- jnxPingCtlTable
- pingCtlTable
- traceRouteCtlTable
- jnxTraceRouteCtlTable
- sysContact.0
- sysName.0
- sysLocation.0
- pingMaxConcurrentRequests.0
- traceRouteMaxConcurrentRequests.0
- usmUserSpinLock
- usmUserOwnAuthKeyChange
- usmUserPublic
- vacmSecurityToGroupTable (vacmGroupName, vacmSecurityToGroupStorageType y vacmSecurityToGroupStatus)

- vacmAccessTable (vacmAccessContextMatch, vacmAccessReadViewName, vacmAccessWriteViewName, vacmAccessNotifyViewName, vacmAccessStorageType y vacmAccessStatus)
- vacmViewSpinLock
- vacmViewTreeFamilyTable (vacmViewTreeFamilyMask, vacmViewTreeFamilyType, vacmViewTreeFamilyStorageType y vacmViewTreeFamilyStatus)

Does Junos OS support remote monitoring (RMON)?

Sí, Junos OS admite RMON tal y como se define en RFC 2819, Base de información de administración de supervisión remota de red. Sin embargo, no se admite la supervisión remota versión 2 (RMON 2).

Can I use SNMP to determine the health of the processes running on the Routing Engine?

Sí, puede usar SNMP para determinar el estado de los procesos del motor de enrutamiento configurando la característica de supervisión de estado. En los dispositivos de Juniper Networks, las alarmas y los eventos de RMON proporcionan gran parte de la infraestructura necesaria para reducir la sobrecarga de sondeo del NMS. Sin embargo, debe configurar el NMS para configurar objetos MIB específicos en alarmas RMON. Esto a menudo requiere experiencia específica del dispositivo y personalización de la aplicación de monitoreo. Además, algunas instancias de objetos MIB que necesitan supervisión solo se establecen en la inicialización o cambian en tiempo de ejecución y no se pueden configurar de antemano.

Para solucionar estos problemas, la supervisión de estado amplía la infraestructura de alarma RMON para proporcionar una supervisión predefinida para un conjunto seleccionado de instancias de objetos, como el uso del sistema de archivos, el uso de la CPU y el uso de memoria, e incluye compatibilidad con instancias de objetos desconocidos o dinámicos, como los procesos de software de Junos OS.

Para mostrar la configuración de supervisión de estado, use el comando:`show snmp health-monitor`

```
user@host> show snmp health-monitor
interval 300;
rising-threshold 90;
falling-threshold 80;
```

Al configurar el monitor de estado, la información de supervisión para determinadas instancias de objeto está disponible, como se muestra en .Tabla 58 en la página 696

Tabla 58: Instancias de objetos supervisados

Objeto	Description
jnxHrStoragePercentUsed.1	Supervisa el siguiente sistema de archivos en el enrutador o conmutador: /dev/ad0s1a: Este es el sistema de archivos raíz montado en ./
jnxHrStoragePercentUsed.2	Supervisa el siguiente sistema de archivos en el enrutador o conmutador: /dev/ad0s1e: Este es el sistema de archivos de configuración montado en `./config`
jnxCPU operativa (RE0)	Supervise el uso de la CPU para los motores de enrutamiento RE0 y RE1. Los valores de índice asignados a los motores de enrutamiento dependen de si la MIB del chasis utiliza un esquema de indización basado en cero o en unos. Dado que el esquema de indización es configurable, se determina el índice correcto cada vez que se inicializa el enrutador y cuando se produce un cambio en la configuración. Si el enrutador o conmutador solo tiene un motor de enrutamiento, el RE1 de monitoreo de entrada de alarma se elimina después de cinco intentos fallidos de obtener el valor de CPU.
jnxCPU operativa (RE1)	
jnxOperatingBuffer (RE0)	Supervise la cantidad de memoria disponible en los motores de enrutamiento RE0 y RE1. Dado que la indización de este objeto es idéntica a la utilizada para jnxOperatingCPU, los valores de índice se ajustan en función del esquema de indización utilizado en la MIB del chasis. Al igual que con jnxOperatingCPU, el RE1 de monitoreo de entrada de alarma se elimina si el enrutador o conmutador tiene un solo motor de enrutamiento.
jnxOperatingBuffer (RE1)	
sysApplElmtRunCPU	Supervisa el uso de la CPU para cada proceso de software de Junos OS. Varias instancias del mismo proceso se supervisan e indexan por separado.
sysApplElmtRunMemory	Supervisa el uso de memoria para cada proceso de software de Junos OS. Varias instancias del mismo proceso se supervisan e indexan por separado.

Las entradas de registro del sistema generadas para cualquier evento de supervisión de estado, como umbrales cruzados y errores, tienen una etiqueta correspondiente en lugar de una etiqueta genérica `.HEALTHMONITORSNMPD_RMON_EVENTLOG` Sin embargo, el monitor de estado envía RMON genérico y capturas.`risingThresholdfallingThreshold`

Are the Ping MIBs returned in decimal notation and ASCII?

Sí, se admiten tanto la notación decimal como ASCII, que es la implementación estándar en SNMP. Todas las cadenas están codificadas ASCII.

En el ejemplo siguiente se muestra la MIB de ping en notación hexadecimal:

```
pingCtlTargetAddress.2.69.72.9.116.99.112.115.97.109.112.108.101 = 0a fa 01 02
```

Esto se traduce en ASCII:

```
pingCtlTargetAddress."EH"."tcpsample" = 0a fa 01 02
2= length of the string
69=E
72=H
9=length of second string
116=t
99 =c
112=p
115=s
97=a
109=m
112 =p
108 =l
101 =e
```

A partir de la versión 9.6 de Junos OS y posteriores, la CLI de Junos OS devuelve valores ASCII mediante el comando .`show snmp mib` *`get`* / *`get-next`* / *`walk`* `ascii`

En el ejemplo siguiente se muestra el resultado con la opción ASCII:

```
user@host> show snmp mib walk pingCtlTargetAddress ascii
pingCtlTargetAddress."EH"."httpgetsample" = http://www.yahoo.com
pingCtlTargetAddress."p1"."t2" = 74 c5 b3 06
pingCtlTargetAddress."p1"."t3" = 74 c5 b2 0c
```

En el ejemplo siguiente se muestra el resultado sin la opción ASCII:

```
user@host> show snmp mib walk pingCtlTargetAddress
pingCtlTargetAddress.2.69.72.13.104.116.116.112.103.101.116.115.97.109.112.108.101 = http://
www.yahoo.com
```

```
pingCtlTargetAddress.2.112.49.2.116.50 = 74 c5 b3 06
pingCtlTargetAddress.2.112.49.2.116.51 = 74 c5 b2 0c
```

Puede convertir valores decimales y ASCII utilizando un gráfico ASCII decimal como el de http://www.asciichart.com .http://www.asciichart.com

Is IPv6 supported by the Ping MIB for remote operations?

No, IPv6 no es compatible.

Is there an SNMP MIB to show Address Resolution Protocol (ARP) table information? Are both IP and MAC addresses displayed in the same table?

Sí, Junos OS es compatible con la MIB estándar, que se describe en RFC 2011, Base de información de administración SNMPv2 para el protocolo de Internet mediante SMIv2.`ipNetToMediaTable` Esta tabla se utiliza para asignar direcciones IP a sus direcciones MAC correspondientes.

Preguntas frecuentes sobre la configuración SNMP de Junos OS

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con la configuración de SNMP de Junos OS.

Can the Junos OS be configured for SNMPv1 and SNMPv3 simultaneously?

Sí, SNMP tiene compatibilidad con versiones anteriores, lo que significa que las tres versiones se pueden habilitar simultáneamente.

Can I filter specific SNMP queries on a device?

Sí, puede filtrar consultas SNMP específicas en un dispositivo mediante instrucciones and .`excludeinclude`

En el ejemplo siguiente se muestra una configuración que bloquea la operación de lectura y escritura en todos los OID en .1.3.6.1.2.1.1 para la comunidad :`test`

```
user@host# show snmp
view system-exclude {
    oid .1.3.6.1.2.1.1 exclude;
    oid .1 include;
}
    community test {
        view system-exclude;
        authorization read-write;
    }
```

Can I change the SNMP agent engine ID?

Sí, el ID del motor del agente SNMP se puede cambiar a la dirección MAC del dispositivo, la dirección IP del dispositivo o cualquier otro valor deseado. Aquí se incluyen varios ejemplos.

En el ejemplo siguiente se muestra cómo utilizar la dirección MAC de un dispositivo como ID del motor del agente SNMP:

```
user@host# show snmp
engine-id {
    use-mac-address;
}
```

En el ejemplo siguiente se muestra cómo utilizar la dirección IP de un dispositivo como ID del motor del agente SNMP:

```
user@host# show snmp
engine-id {
    use-default-ip-address;
}
```

En el ejemplo siguiente se muestra el uso de un valor seleccionado, en este caso, como ID del motor del agente SNMP de un dispositivo:`AA`

```
user@host# show snmp
engine-id {
    local AA;
}
```

How can I configure a device with dual Routing Engines or a chassis cluster (SRX Series Services Gateways) for continued communication during a switchover?

Al configurar la comunicación continua, la configuración SNMP debe ser idéntica entre los motores de enrutamiento. Sin embargo, es mejor tener identificadores de motor de enrutamiento independientes configurados para cada motor de enrutamiento, especialmente cuando se usa SNMPv3.

En el ejemplo siguiente se muestra la configuración de los motores de enrutamiento en un dispositivo de motor de enrutamiento dual. Observe que los ID del motor de enrutamiento se establecen en las direcciones MAC de cada motor de enrutamiento:

```
user@host# show groups
re0 {
    system {
        host-name PE3-re0;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 116.197.178.14/27;
                    address 116.197.178.29/27 {
                        master-only;
                    }
                }
            }
        }
    }
    snmp {
        engine-id {
            use-mac-address;
        }
    }
}
re1 {
    system {
        host-name PE3-re1;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 116.197.178.11/27;
                    address 116.197.178.29/27 {
                        master-only;
                    }
                }
            }
        }
```

```
    }
    snmp {
        engine-id {
            use-mac-address;
        }
    }
}
```

El siguiente es un ejemplo de una configuración SNMPv3 en un dispositivo de motor de enrutamiento dual:

```
user@host> show snmp name host1
v3 {
    vacm {
        security-to-group {
            security-model usm {
                security-name test123 {
                    group test1;
                }
                security-name juniper {
                    group test1;
                }
            }
        }
        access {
            group test1 {
                default-context-prefix {
                    security-model any {
                        security-level authentication {
                            read-view all;
                        }
                    }
                }
                context-prefix MGMT_10 {
                    security-model any {
                        security-level authentication {
                            read-view all;
                        }
                    }
                }
            }
        }
```

```
    }
    target-address server1 {
        address 116.197.178.20;
        tag-list router1;
        routing-instance MGMT_10;
        target-parameters test;
    }
    target-parameters test {
        parameters {
            message-processing-model v3;
            security-model usm;
            security-level authentication;
            security-name juniper;
        }
        notify-filter filter1;
    }
    notify server {
        type trap;
        tag router1;
    }
    notify-filter filter1 {
        oid .1 include;
    }
    view all {
        oid .1 include;
    }
    community comm1 {
        view all;
    }
    community comm2;
    community comm3;
    community comm3 {
        view all;
        authorization read-only;
        logical-system LDP-VPLS {
            routing-instance vpls-server1;
        }
    }
    trap-group server1 {
        targets {
            116.197.179.22;
        }
    }
```

```
    routing-instance-access;
    traceoptions {
        flag all;
    }
}
```

How can I track SNMP activities?

Las operaciones de rastreo SNMP rastrean la actividad de los agentes SNMP y registran la información en archivos de registro.

Una configuración de ejemplo podría tener este aspecto:`traceoptions`

```
[edit snmp]
user@host# set traceoptions flag all
```

Cuando la instrucción se incluye en el nivel de jerarquía, se crean los siguientes archivos de registro:`traceoptions flag all[edit snmp]`

- Snmpd
- mib2d
- rmopd

Preguntas frecuentes sobre SNMPv3

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con SNMPv3.

Why is SNMPv3 important?

SNMP v3 proporciona seguridad mejorada en comparación con las otras versiones de SNMP. Proporciona autenticación y cifrado de datos. La seguridad mejorada es importante para administrar dispositivos en sitios remotos desde las estaciones de administración.

In my system, the MIB object snmpEngineBoots is not in sync between two Routing Engines in a dual Routing Engine device. Is this normal behavior?

Sí, este es el comportamiento esperado. Cada motor de enrutamiento ejecuta su propio proceso SNMP (snmpd), lo que permite que cada motor de enrutamiento mantenga sus propios arranques del motor. Sin embargo, si ambos motores de enrutamiento tienen el mismo identificador de motor y el motor de enrutamiento con menor valor se selecciona como motor de enrutamiento principal durante el proceso

de cambio, el valor del motor de enrutamiento principal se sincroniza con el valor del otro motor de enrutamiento.snmpEngineBootssnmpEngineBootssnmpEngineBoots

Do I need the SNMP manager engine object identifier (OID) for informs?

Sí, el OID del motor del administrador SNMP es necesario para la autenticación, y los informes no funcionan sin él.

I see the configuration of informs under the [edit snmp v3] hierarchy. Does this mean I cannot use informs with SNMPv2c?

Los informes se pueden utilizar con SNMPv2c. En el siguiente ejemplo se muestra la configuración básica para SNMPv3 informa en un dispositivo (tenga en cuenta que la autenticación y privacidad están establecidas en ninguna):

```
[edit snmp]
v3 {
    usm {
        remote-engine 00000063000100a2c0a845b3 {
            user RU2_v3_sha_none {
                authentication-none;
                privacy-none;
            }
        }
    }
    vacm {
        security-to-group {
            security-model usm {
                security-name RU2_v3_sha_none {
                    group g1_usm_auth;
                }
            }
        }
        access {
            group g1_usm_auth {
                default-context-prefix {
                    security-model usm {
                        security-level authentication {
                            read-view all;
                            write-view all;
                            notify-view all;
                        }
                    }
                }
```

```
            }
        }
    }
    target-address TA2_v3_sha_none {
        address 192.168.69.179;
        tag-list tl1;
        address-mask 255.255.252.0;
        target-parameters TP2_v3_sha_none;
    }
    target-parameters TP2_v3_sha_none {
        parameters {
            message-processing-model v3;
            security-model usm;
            security-level none;
            security-name RU2_v3_sha_none;
        }
        notify-filter nf1;
    }
    notify N1_all_tl1_informs {
        type inform; # Replace “inform” with “trap” to convert informs to traps.
        tag tl1;
    }
    notify-filter nf1 {
        oid .1 include;
    }
    view all {
        oid .1 include;
    }
}
```

Puede convertir los informes SNMPv3 en capturas estableciendo el valor de la instrucción en el nivel de jerarquía en, como se muestra en el ejemplo siguiente:`type[edit snmp v3 notify N1_all_tl1_informs]trap`

```
user@host# set snmp v3 notify N1_all_tl1_informs type trap
```

Preguntas frecuentes sobre la interacción SNMP con dispositivos de Juniper Networks

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con la forma en que SNMP interactúa con los dispositivos de Juniper Networks.

How frequently should a device be polled? What is a good polling rate?

Es difícil dar un número absoluto para la tasa de encuestas SNMP por segundo, ya que la tasa depende de los siguientes dos factores:

- El número de enlaces de variables en una unidad de datos de protocolo (PDU)
- El tiempo de respuesta de una interfaz desde el motor de reenvío de paquetes

En un escenario normal donde el motor de reenvío de paquetes no introduce ningún retraso y hay una variable por PDU (una solicitud Get), el tiempo de respuesta es de 130+ respuestas por segundo. Sin embargo, con varias variables en una PDU de solicitud SNMP (30 a 40 para solicitudes GetBulk), el número de respuestas por segundo es mucho menor. Debido a que la carga del motor de reenvío de paquetes puede variar para cada sistema, hay una mayor variación en la frecuencia con la que se debe sondear un dispositivo.

El sondeo frecuente de un gran número de contadores, especialmente las estadísticas, puede afectar al dispositivo. Recomendamos la siguiente optimización en los administradores SNMP:

- Utilice el método de sondeo fila por fila, no el método columna por columna.
- Reduzca el número de enlaces variables por PDU.
- Aumente los valores de tiempo de espera en los intervalos de sondeo y detección.
- Reduzca la velocidad de paquetes entrantes en el proceso SNMP (snmpd).

Para obtener una mejor respuesta SNMP en el dispositivo, Junos OS hace lo siguiente:

- Filtra las solicitudes SNMP duplicadas.
- Excluye las interfaces que responden lentamente de las consultas SNMP.

Una forma de determinar un límite de velocidad es observar un aumento en el conteo desde el comando.`Currently Activeshow snmp statistics extensive`

A continuación se muestra un resultado de ejemplo del comando:`show snmp statistics extensive`

```
user@host> show snmp statistics extensive
  SNMP statistics:
```

```
    Input:
      Packets: 226656, Bad versions: 0, Bad community names: 0,
      Bad community uses: 0, ASN parse errors: 0,
      Too bigs: 0, No such names: 0, Bad values: 0,
      Read onlys: 0, General errors: 0,
      Total request varbinds: 1967606, Total set varbinds: 0,
      Get requests: 18478, Get nexts: 75794, Set requests: 0,
      Get responses: 0, Traps: 0,
      Silent drops: 0, Proxy drops: 0, Commit pending drops: 0,
      Throttle drops: 27084, Duplicate request drops: 0
    V3 Input:
      Unknown security models: 0, Invalid messages: 0
      Unknown pdu handlers: 0, Unavailable contexts: 0
      Unknown contexts: 0, Unsupported security levels: 0
      Not in time windows: 0, Unknown user names: 0
      Unknown engine ids: 0, Wrong digests: 0, Decryption errors: 0
    Output:
      Packets: 226537, Too bigs: 0, No such names: 0,
      Bad values: 0, General errors: 0,
      Get requests: 0, Get nexts: 0, Set requests: 0,
      Get responses: 226155, Traps: 382
    SA Control Blocks:
      Total: 222984, Currently Active: 501, Max Active: 501,
      Not found: 0, Timed Out: 0, Max Latency: 25
    SA Registration:
      Registers: 0, Deregisters: 0, Removes: 0
    Trap Queue Stats:
      Current queued: 0, Total queued: 0, Discards: 0, Overflows: 0
    Trap Throttle Stats:
      Current throttled: 0, Throttles needed: 0
    Snmp Set Stats:
      Commit pending failures: 0, Config lock failures: 0
      Rpc failures: 0, Journal write failures: 0
      Mgd connect failures: 0, General commit failures: 0
```

Does SNMP open dynamic UDP ports? Why?

El proceso SNMP abre dos puertos adicionales (sockets): uno para IPv4 y otro para IPv6. Esto permite que el proceso SNMP envíe capturas.

I am unable to perform a MIB walk on the ifIndex. Why is this?

Los enlaces de variables o valores con un nivel de acceso de no se pueden consultar directamente porque forman parte de otros enlaces de variables de la tabla SNMP MIB.`not-accessible` El ifIndex tiene

un nivel de acceso de `.not-accessible` Por lo tanto, no se puede tener acceso directamente porque forma parte de los enlaces variables. Sin embargo, se puede acceder al ifIndex indirectamente a través de los enlaces de variables.

I see SNMP_IPC_READ_ERROR messages when the SNMP process restarts on my system and also during Routing Engine switchover. Is this acceptable?

Sí, es aceptable ver mensajes cuando se reinicia el proceso SNMP, se reinicia el sistema o durante un cambio de motor de enrutamiento.`SNMP_IPC_READ_ERROR` Si todos los procesos se producen correctamente y las operaciones SNMP funcionan correctamente, estos mensajes se pueden ignorar.

What is the source IP address used in the response PDUs for SNMP requests? Can this be configured?

La dirección IP de origen utilizada en las PDU de respuesta para las solicitudes SNMP es la dirección IP de la interfaz saliente para llegar al destino. No se puede configurar la dirección IP de origen para las respuestas. Solo se puede configurar para capturas.

Preguntas frecuentes sobre capturas e informes SNMP

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con las capturas e informes de SNMP.

Does the Junos OS impose any rate limiting on SNMP trap generation?

Junos OS implementa un mecanismo de cola de captura para limitar el número de capturas que se generan y envían.

Si se produce un error en la entrega de una captura, la captura se vuelve a agregar a la cola y se restablecen el contador de intentos de entrega y el temporizador del siguiente intento de entrega de la cola. Los intentos posteriores ocurren a intervalos progresivos de 1, 2, 4 y 8 minutos. El retraso máximo entre los intentos es de 8 minutos y el número máximo de intentos es de 10. Después de 10 intentos fallidos, se eliminan la cola de destino y todas las capturas de la cola.

Junos OS también tiene un mecanismo de umbral de aceleración para controlar el número de capturas enviadas (500 capturas predeterminadas) durante un intervalo de aceleración determinado (5 segundos predeterminado). Esto ayuda a garantizar la coherencia en el tráfico de capturas, especialmente cuando se genera un gran número de capturas debido a cambios de estado en la interfaz.

El intervalo del acelerador comienza cuando la primera trampa llega al acelerador. Se procesan todas las capturas dentro del valor de umbral del acelerador y las capturas que superan el valor de umbral se ponen en cola. El tamaño máximo de todas las colas de captura (la cola del acelerador y la cola de destino) es de 40.000 capturas. El tamaño máximo de cualquier cola es de 20.000 trampas. Cuando se agrega una interrupción a la cola del acelerador, o si la cola del acelerador ha superado el tamaño máximo, la captura se mueve a la parte superior de la cola de destino. Los intentos posteriores de enviar

la captura desde la cola de destino se detienen durante un período de 30 segundos, después del cual la cola de destino se reinicia a enviar las capturas.

> **NOTA**: Para el conmutador Ethernet de la serie EX de Juniper Networks, el tamaño máximo de todas las colas de captura (la cola del acelerador y la cola de destino) es de 1.000 capturas. El tamaño máximo para cualquier cola de la serie EX es de 500 trampas.

I did not see a trap when I had a syslog entry with a critical severity. Is this normal? Can it be changed?

No todas las entradas de syslog con gravedad crítica son una trampa. Sin embargo, puede convertir cualquier entrada syslog en una interrupción mediante la instrucción.`event-options`

En el ejemplo siguiente se muestra cómo configurar un error cada vez que se produce un mensaje de entrada syslog .`jnxSyslogTraprpd_ldp_nbrdown`

```
user@host> show event-options
policy snmptrap {
    events rpd_ldp_nbrdown;
    then {
        raise-trap;
    }
}
```

Are SNMP traps compliant with the Alarm Reporting Function (X.733) on the Junos OS?

No, las capturas SNMP en Junos OS no son compatibles con X.733.

Can I set up filters for traps or informs?

Las capturas y los informes se pueden filtrar según la categoría de captura y el identificador del objeto. Puede especificar categorías de capturas que se van a recibir por host utilizando la instrucción en el nivel de jerarquía.`categories[edit snmp trap-group trap-group]` Utilice esta opción cuando desee supervisar solo módulos específicos de Junos OS.

En el ejemplo siguiente se muestra una configuración de ejemplo para recibir solo , , y capturas:`linkvrrp-eventsservicesotn-alarms`

```
[edit snmp]
trap-group jnpr {
    categories {
        link;
        vrrp-events;
```

```
        services;
        otn-alarms;
    }
    targets {
        192.168.69.179;
    }
}
```

Junos OS también tiene una opción de filtro más avanzada () para filtrar capturas específicas o un grupo de capturas basadas en sus identificadores de objeto.`notify-filter`

La configuración SNMPv3 también admite el filtrado de capturas SNMPv1 y SNMPv2 y excluye las capturas de administración de configuración específicas de la empresa de Juniper Networks, como se muestra en el siguiente ejemplo de configuración:

```
[edit snmp]
v3 {
    vacm {
        security-to-group {
            security-model v2c {
                security-name sn_v2c_trap {
                    group gr_v2c_trap;
                }
            }
        }
        access {
            group gr_v2c_trap {
                default-context-prefix {
                    security-model v2c {
                        security-level none {
                            read-view all;
                            notify-view all;
                        }
                    }
                }
            }
        }
    }
    target-address TA_v2c_trap {
        address 10.209.196.166;
        port 9001;
        tag-list tg1;
```

```
        target-parameters TP_v2c_trap;
    }
    target-parameters TP_v2c_trap {
        parameters {
            message-processing-model v2c;
            security-model v2c;
            security-level none;
            security-name sn_v2c_trap;
        }
        notify-filter nf1;
    }
    notify v2c_notify {
        type trap;
        tag tg1;
    }
    notify-filter nf1 {
        oid .1.3.6.1.4.1.2636.4.5 exclude;
        oid .1 include;
    }
    snmp-community index1 {
        community-name "$9$tDLl01h7Nbw2axN"; ## SECRET-DATA
        security-name sn_v2c_trap;
        tag tg1;
    }
view all {
    oid .1 include;
}
}
```

Can I simulate traps on a device?

Sí, puede usar el comando para simular una captura en el NMS que normalmente recibe las capturas de su dispositivo.`request snmp spoof-trap` *`trap name`* También puede agregar los valores necesarios mediante el parámetro.`variable-bindings`

En el ejemplo siguiente se muestra cómo simular una captura en el NMS local mediante enlaces variables:

```
user@host> request snmp spoof-trap linkDown variable-bindings "ifIndex[116]=116,
ifAdminStatus[116]=1 ,ifOperStatus[116]=2 , ifName[116]=ge-1/0/1"
```

How do I generate a warm start SNMPv1 trap?

Cuando el proceso SNMP se reinicia en condiciones normales, se genera una captura de arranque en caliente si el tiempo de actividad del sistema es superior a 5 minutos. Si el tiempo de actividad del sistema es inferior a 5 minutos, se genera una trampa de arranque en frío.

The NMS sees only the MIB OIDs and numbers, but not the names of the SNMP traps. Why?

Antes de que el NMS pueda reconocer los detalles de la captura SNMP, como los nombres de las capturas, primero debe compilar y comprender las MIB y, a continuación, analizar los OID de MIB.

In the Junos OS, how can I determine to which category a trap belongs?

Para obtener una lista de capturas comunes y sus categorías, consulte SNMP MIB Explorer.https://apps.juniper.net/mib-explorer/

Can I configure a trap to include the source IP address?

Sí, puede configurar el , o el nombre de la dirección IP de origen mediante el comando:`source-addressrouting-instancelogical-instancetrap-options`

```
user@host> show snmp trap-options
source-address 10.1.1.1;
```

Can I create a custom trap?

Sí, puede utilizar el script de eventos para crear capturas personalizadas según sea necesario.`jnxEventTrap`

En el ejemplo siguiente, se activa un script de operaciones (op) de Junos OS cuando se recibe un evento.`UI_COMMIT_NOT_CONFIRMED` El script op de Junos OS coincide con el mensaje completo del evento y genera una captura SNMP.

Ejemplo: Junos OS Op Script

```
version 1.0;

ns junos = "http://xml.juniper.net/junos/*/junos";
ns xnm = "http://xml.juniper.net/xnm/1.1/xnm";
ns jcs = "http://xml.juniper.net/junos/commit-scripts/1.0";

param $event;
param $message;

match / {

    /*
     * trapm utilty wants the following characters in the value to be escaped
```

```
     * '[', ']', ' ', '=', and ','
     */
    var $event-escaped = {
        call escape-string($text = $event, $vec = '[] =,');
    }

    var $message-escaped = {
        call escape-string($text = $message, $vec = '[] =,');
    }

    <op-script-results> {
    var $rpc = <request-snmp-spoof-trap> {
        <trap> "jnxEventTrap";
        <variable-bindings> "jnxEventTrapDescr[0]='Event-Trap' , "
        _ "jnxEventAvAttribute[1]='event' , "
        _ "jnxEventAvValue[1]='" _ $event-escaped _ "' , "
        _ "jnxEventAvAttribute[2]='message' , "
        _ "jnxEventAvValue[1]='" _ $message-escaped _ "'";
    }

    var $res = jcs:invoke($rpc);
    }
}

template escape-string ($text, $vec) {

    if (jcs:empty($vec)) {
        expr $text;

    } else {
        var $index = 1;
        var $from = substring($vec, $index, 1);
        var $changed-value = {
            call replace-string($text, $from) {
                with $to = {
                    expr "\\";
                    expr $from;
                 }
            }
        }

        call escape-string($text = $changed-value, $vec = substring($vec, $index
 + 1));
```

```
    }
}

template replace-string ($text, $from, $to) {

    if (contains($text, $from)) {
        var $before = substring-before($text, $from);
        var $after = substring-after($text, $from);
        var $prefix = $before _  $to;

        expr $before;
        expr $to;
        call replace-string($text = $after, $from, $to);

    } else {
        expr $text;
    }
}
```

Después de crear la captura personalizada, debe configurar una política en el dispositivo para indicarle qué acciones debe realizar después de recibir la captura.

Este es un ejemplo de una directiva configurada bajo la jerarquía:`[edit event-options]`

```
[edit event-options]
user@host> show
policy trap-on-event {
    events UI_COMMIT_NOT_CONFIRMED;
    attributes-match {
        UI_COMMIT_NOT_CONFIRMED.message matches complete;
    }
    then {
        event-script ev-syslog-trap.junos-op {
            arguments {
                event UI_COMMIT_NOT_CONFIRMED;
                message "{$$.message}";
            }
        }
    }
}
```

Can I disable link up and link down traps on interfaces?

Sí, las capturas de vínculo hacia arriba y hacia abajo se pueden deshabilitar en la configuración de la interfaz. Para deshabilitar las capturas, utilice la instrucción en las jerarquías y para las interfaces físicas y lógicas.`no-traps`[`edit interfaces` *`interface-name`* `unit` *`logical-unit-number`*][`edit logical-systems` *`logical-system-name`* `interfaces` *`interface-name`* `unit` *`logical-unit-number`*]

```
(traps | no-traps);
```

I see the link up traps on logical interfaces, but I do not see the link down traps. Is this normal behavior?

Para los tipos de interfaces Ethernet y ATM, Junos OS no envía capturas de vínculos a una interfaz lógica si la interfaz física está inactiva para evitar alarmas de inundación por la misma causa raíz. Sin embargo, cuando la interfaz física y las interfaces lógicas vuelven a funcionar, se envían capturas que indican el vínculo. Esto se debe a que la interfaz física que aparece no significa necesariamente que las interfaces lógicas también estén apareciendo.

Para los tipos de interfaces SONET con encapsulación PPP, Junos OS envía capturas de vínculos hacia abajo para una interfaz lógica si la interfaz física está inactiva. Cuando la interfaz física y las interfaces lógicas vuelven a funcionar, se envían capturas para las interfaces físicas y lógicas que indican el vínculo.

Para los tipos de interfaces SONET con encapsulación HDLC, Junos OS no envía capturas de vínculo hacia abajo para una interfaz lógica si la interfaz física está inactiva. Cuando la interfaz física y las interfaces lógicas vuelven a funcionar, se envían capturas para las interfaces físicas y lógicas que indican el vínculo.

Para las interfaces de canalización con encapsulación PPP, Junos OS envía capturas de vínculo hacia abajo para una interfaz lógica si la interfaz física está inactiva. Cuando la interfaz física y las interfaces lógicas vuelven a funcionar, se envían capturas para las interfaces físicas y lógicas que indican el vínculo.

Para las interfaces de canalización con encapsulación HDLC, Junos OS no envía capturas de vínculo hacia abajo para una interfaz lógica si la interfaz física está inactiva. Cuando la interfaz física y las interfaces lógicas vuelven a funcionar, se envían capturas para las interfaces físicas y lógicas que indican el vínculo.

Preguntas frecuentes de la configuración del motor de enrutamiento dual de Junos OS

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con la configuración de motores de enrutamiento duales.

La configuración SNMP debe ser idéntica entre los motores de enrutamiento al configurar la comunicación continua. Sin embargo, recomendamos tener identificadores de motor de enrutamiento independientes configurados para cada motor de enrutamiento, cuando se utiliza SNMPv3.

In my system, the MIB object snmpEngineBoots is not in sync between two Routing Engines in a dual Routing Engine device. Is this normal behavior?

Sí. Este es el comportamiento normal. Cada motor de enrutamiento ejecuta su propio agente de proceso SNMP (snmpd), lo que permite que cada motor de enrutamiento mantenga sus propios arranques del motor.

Is there a way to identify that an address belongs to RE0, RE1, or the master Routing Engine management interface (fxp0) by looking at an SNMP walk?

No. Cuando realiza una caminata SNMP en el dispositivo, solo muestra la dirección principal de la interfaz de administración del motor de enrutamiento.

What is the best way to tell if the current IP address belongs to fxp0 or a Routing Engine, from a CLI session?

Los motores de enrutamiento se asignan con la interfaz.`fxp0` Esto significa que cuando consulta RE0, ifTable notifica únicamente la dirección de interfaz de RE0.`fxp0` Del mismo modo, si consulta RE1, ifTable notifica únicamente la dirección de interfaz de RE1.`fxp0`

When there is a failover, the master hostname is changed since the hostname belongs to the Routing Engine. Is this correct?

Sí. Puede configurar el mismo nombre de host o nombres de host diferentes. Cualquiera de los dos funcionaría.

Si solo se configura la dirección IP principal (por ejemplo, 192.168.2.5) y el objeto tiene la misma cadena configurada en ambos motores de enrutamiento, incluso después de un cambio, el objeto devuelve el mismo valor.`sysDescr.0``sysDescr.0` En el ejemplo siguiente se muestran los resultados que se obtienen mediante el comando:`snmpget`

```
bng-junos-pool02: /c/svivek/PR_BRANCH/src> snmpget -c jnpr -v2c 192.168.2.5
sysDescr.0 system.sysDescr.0 = foo
```

Preguntas frecuentes sobre la compatibilidad de SNMP con instancias de enrutamiento

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con la forma en que SNMP admite instancias de enrutamiento.

Can the SNMP manager access data for routing instances?

Sí, Junos OS permite que los administradores SNMP de todas las instancias de enrutamiento soliciten y administren datos SNMP relacionados con las instancias de enrutamiento y las redes del sistema lógico correspondientes.

Pueden producirse dos comportamientos de instancia de enrutamiento diferentes, dependiendo de dónde se originen los clientes:

- Los clientes de instancias de enrutamiento distintas de la predeterminada pueden tener acceso a objetos MIB y realizar operaciones SNMP solo en las redes del sistema lógico a las que pertenecen.
- Los clientes de la instancia de enrutamiento predeterminada pueden acceder a información relacionada con todas las instancias de enrutamiento y redes de sistemas lógicos.

Las instancias de enrutamiento se identifican mediante el campo de contexto de las solicitudes SNMPv3 o codificadas en la cadena de comunidad en las solicitudes SNMPv1 o SNMPv2c.

Cuando se codifica en una cadena de comunidad, el nombre de la instancia de enrutamiento aparece primero y está separado de la cadena de comunidad real por el carácter @.

Para evitar conflictos con cadenas de comunidad válidas que contienen el carácter @, la comunidad se analiza solo si se produce un error en el procesamiento típico de cadenas de comunidad. Por ejemplo, si se configura una instancia de enrutamiento denominada , se procesa una solicitud SNMP con en el contexto de la instancia de enrutamiento.`RIRI@publicRI` El control de acceso (incluidas las vistas, las restricciones de dirección de origen y los privilegios de acceso) se aplica de acuerdo con la cadena de comunidad real (el conjunto de datos después del carácter @, en este caso).`public` Sin embargo, si se configura la cadena de comunidad, la PDU se procesa de acuerdo con esa comunidad y se omite el nombre de la instancia de enrutamiento incrustado.`RI@public`

Los sistemas lógicos realizan un subconjunto de las acciones de un enrutador físico y tienen sus propias tablas de enrutamiento, interfaces, políticas e instancias de enrutamiento. Cuando se define una instancia de enrutamiento dentro de un sistema lógico, el nombre del sistema lógico debe codificarse junto con la instancia de enrutamiento mediante una barra diagonal (/) para separar ambas. Por ejemplo, si la instancia de enrutamiento está configurada en el sistema lógico , dicha instancia de enrutamiento debe codificarse dentro de una cadena de comunidad como `.RILSLS/RI@public` Cuando se configura una instancia de enrutamiento fuera de un sistema lógico (dentro del sistema lógico predeterminado), no se necesita ningún nombre o carácter de sistema lógico./

Además, cuando se crea un sistema lógico, siempre se crea una instancia de enrutamiento predeterminada denominada dentro del sistema lógico.`default` Este nombre debe utilizarse al consultar datos para esa instancia de enrutamiento, por ejemplo .`LS/default@public` Para las solicitudes SNMPv3, el nombre debe identificarse directamente en el campo de contexto.*`logical system/routing instance`*

Can I access a list of all routing instances on a device?

Sí, puede acceder a una lista de todas las instancias de enrutamiento de un dispositivo mediante el objeto vacmContextName de la MIB SNMP-VIEW-BASED-ACM. En SNMP, cada instancia de enrutamiento se convierte en un contexto VACM; esta es la razón por la que las instancias de enrutamiento aparecen en el objeto vacmContextName.

Can I access a default routing instance from a client in another logical router or routing instance?

No, el agente SNMP sólo puede acceder a los datos del enrutador lógico al que está conectado.

Preguntas frecuentes sobre contadores SNMP

En esta sección se presentan las preguntas y respuestas más frecuentes relacionadas con los contadores SNMP.

Which MIB should I use for interface counters?

La administración de interfaces a través de SNMP se basa en dos tablas: el y su extensión el .`ifTableifXTable` Ambos se describen en RFC 1213, Base de información de administración para la administración de red de Internets basados en TCP/IP: *MIB-II y RFC 2233, The Interfaces Group MIB using SMIv2.*

Las interfaces pueden tener varias capas, dependiendo del medio, y cada subcapa está representada por una fila independiente en la tabla. La relación entre la capa superior y las capas inferiores se describe en el archivo .`ifStackTable`

El define contadores de 32 bits para octetos entrantes y salientes (ifInOctets/ifOutOctets), paquetes (ifInUcastPkts/ifOutUcastPkts, ifInNUcastPkts /ifOutNUcastPkts), errores y descartes.`ifTable`

El proporciona contadores similares de 64 bits, también llamados contadores de alta capacidad (HC), para octetos de entrada y salida (ifHCInOctets/ifHCOutOctets) y paquetes entrantes (ifHCInUcastPkts).`ifXTable`

When should 64-bit counters be used?

Siempre es bueno usar contadores de 64 bits porque contienen estadísticas para componentes de baja y alta capacidad.

Are the SNMP counters ifInOctets and ifOutOctets the same as the command reference show interfaces statistics in and out counters?

Sí, estos son los mismos, pero solo si SNMP está habilitado cuando se inicia el enrutador. Si enciende un dispositivo de Juniper Networks y luego habilita SNMP, los contadores SNMP comienzan desde 0. Los contadores SNMP no reciben automáticamente sus estadísticas de la salida del comando.`show` Del mismo modo, el uso del comando no borra las estadísticas recopiladas por los contadores SNMP, lo que puede provocar una discrepancia en los datos que ven ambos procesos.`clear statistics`

Do the SNMP counters ifInOctets and ifOutOctets include the framing overhead for Point-to-Point Protocol (PPP) and High-Level Data Link Control (HDLC)?

Sí.

4

PART IN COVERPAGE

Monitoreo remoto de red (RMON) con alarmas y eventos SNMP

Monitoreo remoto de redes (RMON) | 721

Configurar el muestreo del historial de RMON | 750

Supervisión de la calidad del servicio de red mediante RMON | 752

Supervisión de estado con SNMP | 786

Monitoreo remoto de redes (RMON)

summary

En esta sección se describe cómo Junos OS admite la MIB *de supervisión remota de redes* (RMON) (RFC 2819) que permite a un dispositivo de administración supervisar los valores de objetos MIB, o variables, con respecto a umbrales configurados. Cuando el valor de una variable cruza un umbral, se genera una alarma y su evento correspondiente. El evento se puede registrar y puede generar una captura SNMP.

in this section

- Descripción general de RMON | **721**
- Configuración de eventos y alarmas RMON | **726**
- Configurar alarmas y eventos de RMON | **727**
- Monitorear tablas MIB de RMON | **730**
- Tablas de control de eventos, alarmas, registros e historial de RMON MIB | **731**
- Configuración mínima de alarma RMON y entrada de eventos | **734**
- Configurar una entrada de alarma RMON y sus atributos | **735**
- Configurar una entrada de evento RMON y sus atributos | **740**
- Ejemplo: Configurar una alarma RMON y la entrada de eventos | **741**
- Utilice alarmTable para supervisar objetos MIB | **742**
- Usar eventTable para registrar alarmas | **747**

Descripción general de RMON

in this section

- Alarmas RMON | **722**
- Eventos RMON | **724**
- Umbrales y eventos de alarma | **725**

Se puede usar un sistema de soporte operativo (OSS) o un sistema de monitoreo de fallas para monitorear automáticamente eventos que rastrean muchas métricas diferentes, incluidos el rendimiento, la disponibilidad, las fallas y los datos ambientales. Por ejemplo, es posible que un administrador desee saber cuándo la temperatura interna de un chasis ha superado un umbral configurado, lo que podría indicar que una bandeja de ventilador del chasis está defectuosa, que el flujo de aire del chasis está impedido o que el sistema de refrigeración de la instalación cerca del chasis no funciona normalmente.

La MIB de RMON también define tablas que almacenan diversas estadísticas para interfaces Ethernet, incluidas las y .`etherStatsTableetherHistoryTable` Contiene estadísticas acumulativas en tiempo real para interfaces Ethernet, como el número de paquetes de unidifusión, multidifusión y difusión recibidos en una interfaz.`etherStatsTable` El mantiene un ejemplo histórico de estadísticas para interfaces Ethernet.`etherHistoryTable` El control del , incluidas las interfaces de seguimiento y el intervalo de muestreo, está definido por RMON .`etherHistoryTablehistoryControlTable`

Para habilitar las alarmas RMON, realice los pasos siguientes:

1. Configure SNMP, incluidos los grupos de capturas. SNMP se configura en el nivel de jerarquía [].`edit snmp`

2. Configure eventos ascendentes y descendentes en el , incluidos los tipos de eventos y los grupos de interrupción.`eventTable` También puede configurar eventos mediante la CLI en el nivel de jerarquía [].`edit snmp rmon event`

3. Configure alarmas en el , incluidas las variables a monitorear, los umbrales ascendentes y descendentes, los tipos e intervalos de muestreo, y los eventos correspondientes que se generarán cuando se produzcan alarmas.`alarmTable` También puede configurar alarmas mediante la CLI en el nivel jerárquico [].`edit snmp rmon alarm`

   Las extensiones del se definen en el JNXRmon de MIB específico para la empresa de Juniper Networks (mib-jnx-rmon.txt).`alarmTable`

En este tema se tratan las siguientes secciones:

Alarmas RMON

Una alarma RMON identifica:

- Un objeto MIB específico que se supervisa.
- La frecuencia del muestreo.
- El método de muestreo.
- Los umbrales con los que se comparan los valores supervisados.

Una alarma RMON también puede identificar una entrada específica que se activará cuando se cruza un umbral.`eventTable`

La configuración y los valores operativos se definen en RFC 2819.`alarmTable` Los valores operativos adicionales se definen en las extensiones específicas de la empresa de Juniper Networks para ().`alarmTablejnxRmonAlarmTable`

En este tema se tratan las siguientes secciones:

alarmTable

`alarmTable` en la MIB de RMON le permite supervisar y sondear lo siguiente:

- : el valor de índice para que identifica una entrada específica.`alarmIndexalarmTable`
- `alarmInterval`—El intervalo, en segundos, durante el cual se muestrean los datos y se comparan con los umbrales ascendentes y descendentes.
- `alarmVariable`: variable MIB supervisada por la entrada de alarma.
- `alarmSampleType`—El método de muestreo de la variable seleccionada y de cálculo del valor que debe compararse con los umbrales.
- `alarmValue`—El valor de la variable durante el último período de muestreo. Este valor se compara con los umbrales ascendentes y descendentes.
- `alarmStartupAlarm`: la alarma que se envía cuando se activa la entrada por primera vez.
- `alarmRisingThreshold`: umbral superior de la variable muestreada.
- `alarmFallingThreshold`: umbral inferior de la variable muestreada.
- : la entrada utilizada cuando se cruza un umbral ascendente.`alarmRisingEventIndexeventTable`
- : la entrada utilizada cuando se cruza un umbral descendente.`alarmFallingEventIndexeventTable`
- `alarmStatus`: método para agregar y quitar entradas de la tabla. También se puede utilizar para cambiar el estado de una entrada para permitir modificaciones.

> **NOTA**: Si este objeto no se establece en , la alarma de sucesos asociada no realiza ninguna acción.`valid`

jnxRmonAlarmTable

El es una extensión específica de la empresa de Juniper Networks para .`jnxRmonAlarmTablealarmTable` Proporciona información operativa adicional e incluye los siguientes objetos:

- : el número de veces que ha fallado la solicitud interna de la variable supervisada por esta entrada.`jnxRmonAlarmGetFailCntGet`
- : el valor de cuándo falló por última vez una solicitud interna para la variable supervisada por esta entrada.`jnxRmonAlarmGetFailTimesysUpTimeGet`
- : el motivo por el que falló por última vez una solicitud interna de la variable supervisada por esta entrada.`jnxRmonAlarmGetFailReasonGet`
- : el valor de cuando una solicitud interna para la variable supervisada por esta entrada se realizó correctamente y la entrada salió del estado.`jnxRmonAlarmGetOkTimesysUpTimeGetgetFailure`
- `jnxRmonAlarmState`: el estado actual de esta entrada de alarma RMON.

Para ver las extensiones específicas para empresa de Juniper Networks para la MIB de eventos y alarmas y eventos de RMON, consulte https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-rmon.txt.https://www.juniper.net/documentation/en_US/junos16.1/topics/reference/mibs/mib-jnx-rmon.txt

Eventos RMON

Un evento RMON permite registrar el cruce de umbrales de otros objetos MIB. Se define en para la MIB de RMON.`eventTable`

En esta sección se tratan los siguientes temas:

eventTable

`eventTable` contiene los siguientes objetos:

- : índice que identifica de forma exclusiva una entrada en .`eventIndexeventTable` Cada entrada define un evento que se genera cuando se dan las condiciones adecuadas.
- `eventDescription`: un comentario que describe la entrada del evento.
- `eventType`: tipo de notificación que realiza la sonda sobre este evento.
- `eventCommunity`: grupo de capturas que se utiliza si se va a enviar una captura SNMP. Si no está configurado, se envía una captura a cada grupo de capturas configurado con la categoría.`eventCommunityrmon-alarm`
- : valor de cuándo se generó por última vez un evento esta entrada de evento.`eventLastTimeSentsysUpTime`
- `eventOwner`: cualquier cadena de texto especificada por la aplicación de administración creadora o la interfaz de línea de comandos (CLI). Normalmente, se utiliza para identificar un administrador de red

(o aplicación) y se puede utilizar para un control de acceso preciso entre las aplicaciones de administración participantes.

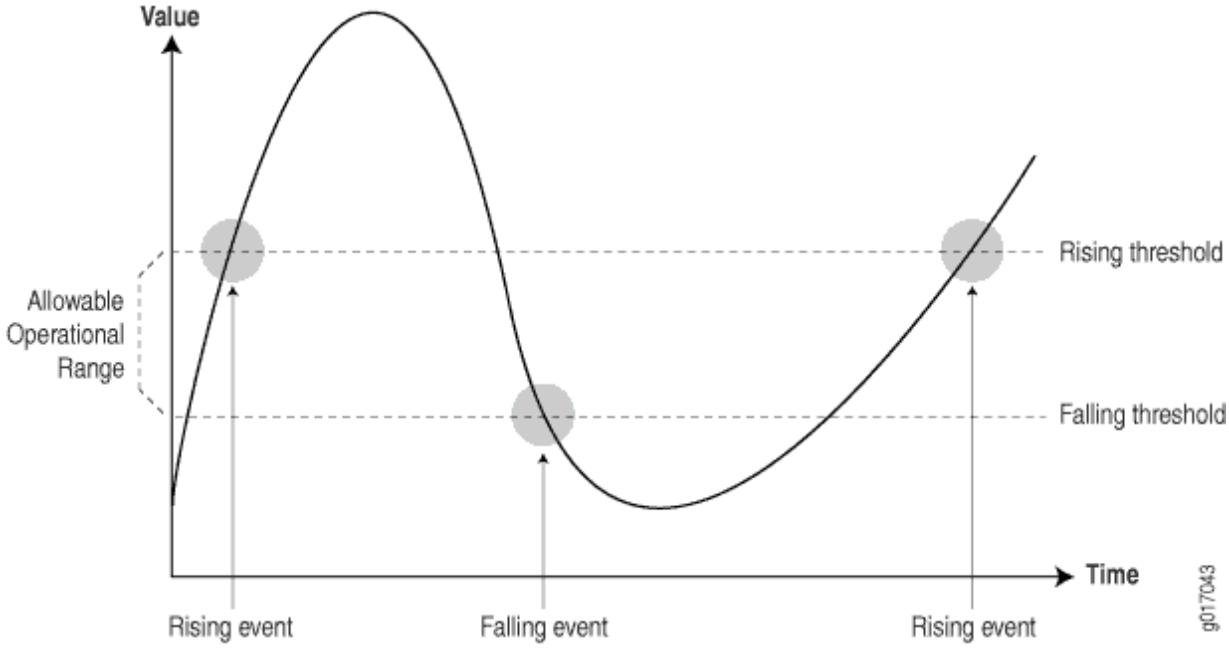
- `eventStatus`: estado de esta entrada del evento.

> **NOTA**: Si este objeto no se establece en , la entrada de evento asociada no realiza ninguna acción.`valid` Cuando este objeto se establece en , se eliminan todas las entradas de registro anteriores asociadas a esta entrada (si las hubiera).`valid`

Umbrales y eventos de alarma

Al establecer un umbral ascendente y descendente para una variable supervisada, se le puede alertar cada vez que el valor de la variable caiga fuera del rango operativo permitido (consulte).Figura 24 en la página 725

Figura 24: Configuración de umbrales



Los eventos solo se generan cuando el umbral de alarma se cruza por primera vez en una dirección en lugar de después de cada intervalo de muestra. Por ejemplo, si se activa una alarma de umbral ascendente, junto con su evento correspondiente, no se producen más eventos de cruce de umbral hasta que se produce una alarma de caída correspondiente. Esto reduce considerablemente la cantidad de eventos que produce el sistema, lo que facilita que el personal de operaciones reaccione cuando ocurran eventos.

Antes de configurar la supervisión remota, debe identificar qué variables deben supervisarse y su rango operativo permitido. Esto requiere un período de referencia para determinar los rangos operativos permitidos. Un período inicial de referencia de al menos 3 meses no es inusual cuando se identifican por primera vez los rangos operativos y se definen los umbrales, pero el monitoreo de línea de base debe continuar durante la vida útil de cada variable monitoreada.

SEE ALSO

MIB específicas para empresas de Juniper Networks

Configuración de eventos y alarmas RMON

Junos OS admite la supervisión de enrutadores desde dispositivos remotos. Estos valores se miden con respecto a umbrales y desencadenan eventos cuando se cruzan los umbrales. Configurar alarma de supervisión remota (RMON) y entradas de sucesos para supervisar el valor de un objeto MIB.

Para configurar las entradas de eventos y alarmas de RMON, incluya instrucciones en el nivel jerárquico de la configuración:`[edit snmp]`

```
[edit snmp]
rmon {
    alarm index {
        description text-description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        rising-event-index index;
        rising-threshold integer;
        request-type (get-next-request | get-request | walk-request);
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
        syslog-subtag syslog-subtag;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type type;
```

```
    }
}
```

Configurar alarmas y eventos de RMON

in this section

- Configurar SNMP | 727
- Configurar un evento | 728
- Configurar una alarma | 729

Junos OS admite la MIB de *monitoreo remoto de red* (RPMON) (RFC 2819). Esto permite que un dispositivo de administración supervise los valores de los objetos MIB, o variables, con respecto a los umbrales configurados. Cuando el valor de una variable cruza un umbral, se genera una alarma y su evento correspondiente. El evento se puede registrar y puede generar una captura SNMP.

Para configurar alarmas y eventos de RMON mediante la CLI, realice estas tareas:

Configurar SNMP

Para configurar SNMP:

1. Conceder acceso de solo lectura a todos los clientes SNMP:

```
[edit snmp]
user@switch# set community community-name authorization authorization
```

Por ejemplo:

```
[edit snmp]
user@switch# set community public authorization read-only
```

2. Conceda acceso de lectura y escritura a las MIB de RMON y jnx-rmon:

```
[edit snmp]
user@switch# set view view-name oid object-identifier include
user@switch# set view view-name oid object-identifier include
user@switch# set community community-name authorization authorization view view-name
```

Por ejemplo:

```
[edit snmp]
user@switch# set view rmon-mib-view oid .1.3.6.1.2.1.16 include
user@switch# set view rmon-mib-view oid .1.3.6.1.4.1.2636.13 include
user@switch# set community private authorization read-write view rmon-mib-view
```

Los OID 1.3.6.1.2.1.16 y 1.3.6.1.4.1.2636.13 corresponden a las MIB RMON y jnxRmon.

3. Configure un grupo de capturas SNMP:

```
[edit snmp]
user@switch# set trap-group group-name categories category
user@switch# set trap-group group-name targets address
```

Por ejemplo:

```
[edit snmp]
user@switch# set trap-group rmon-trap-group categories rmon-alarm
user@switch# set trap-group rmon-trap-group targets 192.168.5.5
```

El grupo de capturas rmon-trap-group está configurado para enviar capturas RMON a 192.168.5.5.

Configurar un evento

Para configurar un evento:

1. Configure un índice de eventos, un nombre de comunidad y un tipo:

```
[edit snmp rmon]
user@switch# set event index community community-name  type type
```

Por ejemplo:

```
[edit snmp rmon]
user@switch# set event 1 community rmon-trap-group type log-and-trap
```

La comunidad de eventos corresponde al grupo de captura SNMP y no es lo mismo que una comunidad SNMP. Este evento genera una captura SNMP y agrega una entrada a logTable en la MIB de RMON.

2. Configure una descripción para el evento:

```
[edit snmp rmon]
user@switch# set event index description description
```

Por ejemplo:

```
[edit snmp rmon]
user@switch# set event 1 description “rmon event”
```

Configurar una alarma

Para configurar una alarma:

1. Configure un índice de alarma, la variable a monitorear, los umbrales ascendentes y descendentes, y los eventos de subida y bajada correspondientes:

```
[edit snmp rmon]
user@switch# set alarm index variable oid-variable falling-threshold integer  rising-
threshold integer rising-event-index index falling-event-index index
```

Por ejemplo:

```
[edit snmp rmon]
user@switch# set alarm 5 variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 falling-threshold 75
rising-threshold 90 rising-event-index 1 falling-event-index 1
```

La variable .1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0 corresponde al objeto jnxRmon MIB jnxOperatingCPU, que representa la utilización de la CPU del motor de enrutamiento. Los enteros de umbral descendente y ascendente son 75 y 90. Los eventos ascendentes y descendentes generan el mismo evento (índice de eventos 1).

2. Configure el intervalo y el tipo de muestra, así como el tipo de alarma:

```
[edit snmp rmon]
user@switch# set alarm index  interval seconds sample-type (absolute-value | delta-value)
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm)
```

Por ejemplo:

```
[edit snmp rmon]
user@switch# set alarm 5 interval 30 sample-type absolute-value startup-alarm rising-or-
falling-alarm
```

El valor absoluto de la variable monitoreada se muestrea cada 30 segundos. La alarma inicial puede ocurrir debido a elevarse por encima del umbral ascendente o caer por debajo del umbral descendente.

Monitorear tablas MIB de RMON

in this section

- Propósito | 730
- Acción | 730
- Significado | 731

Propósito

Monitoree las tablas de alarma, eventos y registro de monitoreo remoto (RMON).

Acción

Para mostrar las tablas RMON:

```
user@switch> show snmp rmon
Alarm
```

```
Index  Variable description                          Value State

     5 monitor
       jnxOperatingCPU.9.1.0.0                           5 falling threshold

Event
Index  Type                        Last Event
    1  log and trap                2010-07-10 11:34:17 PDT
Event Index: 1
    Description: Event 1 triggered by Alarm 5, rising threshold (90) crossed, (variable:
jnxOperatingCPU.9.1.0.0, value: 100)
    Time: 2010-07-10 11:34:07 PDT
    Description: Event 1 triggered by Alarm 5, falling threshold (75) crossed, (variable:
jnxOperatingCPU.9.1.0.0, value: 5)
    Time: 2010-07-10 11:34:17 PDT
```

Significado

La pantalla muestra que se ha definido una alarma para supervisar el objeto jnxRmon MIB jnxOperatingCPU, que representa la utilización de la CPU del motor de enrutamiento. La alarma está configurada para generar un evento que envía una captura SNMP y agrega una entrada a logTable en la MIB de RMON. La tabla del registro muestra que se han generado dos repeticiones del evento: una para elevarse por encima de un umbral del 90 por ciento y otra para caer por debajo de un umbral del 75 por ciento.

SEE ALSO

- Configuración de alarmas y eventos de RMON
- Mostrar SNMP RMON
- Mostrar el historial de RMON SNMP
- Borrar estadísticas SNMP
- Borrar historial SNMP

Tablas de control de eventos, alarmas, registros e historial de RMON MIB

Tabla 59 en la página 732 proporciona cada campo de la eventTable de RMON, la descripción del campo y la instrucción Junos OS correspondiente que puede utilizar para configurar el campo. Las instrucciones de Junos OS residen en el nivel de jerarquía [].`edit snmp rmon`

Tabla 59: Tabla de eventos RMON

Campo	Description	Declaración [edit snmp rmon]
descripción del evento	Descripción textual de este evento.	`description`
eventType	Tipo de evento (por ejemplo, registro, captura o registro y captura).	`type`
eventoComunidad	Grupo de capturas al que enviar este evento, tal como se define en la configuración de Junos OS. (Esto no es lo mismo que la comunidad SNMP).	`community`
eventOwner	Entidad (por ejemplo, administrador) que creó este evento.	—
eventStatus	Estado de esta fila (por ejemplo, válido, no válido o createRequest).	—

Tabla 60 en la página 732 proporciona cada campo de RMON alarmTable, la descripción del campo y la instrucción Junos OS correspondiente que puede utilizar para configurar el campo. Las instrucciones de Junos OS residen en el nivel de jerarquía [].`edit snmp rmon`

Tabla 60: Tabla de alarma RMON

Campo	Description	Declaración [edit snmp rmon]
alarmStatus	Estado de esta fila (por ejemplo, válido, no válido o createRequest)	—
alarmInterval	Período de muestreo (en segundos) de la variable monitoreada	`interval`
alarmaVariable	Identificador de objeto (OID) e instancia de la variable que se va a supervisar	—
alarmValue	Valor real de la variable muestreada	—

Tabla 60: Tabla de alarma RMON *(Continued)*

Campo	Description	Declaración [edit snmp rmon]
alarmSampleType	Tipo de muestra (cambios absolutos o delta)	`sample-type`
alarmaStartupAlarm	Alarma inicial (subida, caída o cualquiera de las dos)	`startup-alarm`
alarmRisingThreshold	Umbral ascendente con el que comparar el valor	`rising-threshold`
alarmaFallingThreshold	Umbral descendente con el que comparar el valor	`falling-threshold`
alarmRisingEventIndex	Índice (fila) del evento ascendente en la tabla de eventos	`rising-event-index`
alarmFallingEventIndex	Índice (fila) del evento descendente en la tabla de eventos	`falling-event-index`

Tabla 61 en la página 733 proporciona cada campo de jnxRmon jnxRmonAlarmTable, que es una extensión de RMON alarmTable. Puede solucionar problemas del agente RMON, rmopd, que se ejecuta en un conmutador inspeccionando el contenido del objeto jnxRmonAlarmTable.

Tabla 61: Tabla de alarma jnxRmon

Campo	Description
jnxRmonAlarmGetFailCnt	Número de veces que se produjo un error en la solicitud interna de la variable`Get`
jnxRmonAlarmGetFailTime	Valor del objeto sysUpTime cuando se produjo el último error
jnxRmonAlarmGetFailReason	Motivo por el que se produjo un error en la solicitud`Get`
jnxRmonAlarmGetOkTime	Valor del objeto sysUpTime cuando la variable salió del estado de error
jnxRmonAlarmState	Estado de esta entrada de alarma

Tabla 62 en la página 734 proporciona cada campo de la tabla historyControlTable de RMON, la descripción del campo y la instrucción Junos OS correspondiente que puede usar para configurar el campo. Las instrucciones de Junos OS residen en el nivel de jerarquía [].`edit snmp rmon history` El historyControlTable controla etherHistoryTable de RMON.

Tabla 62: Tabla de control del historial de RMON

Campo	Description	Declaración [edit snmp rmon history]
historyControlDataSource	Identifica el origen de los datos para los que se recopilaron datos históricos.	`interface`
historialControlBucketsRequested	Número solicitado de intervalos de tiempo discretos durante los cuales se guardarán los datos.	`bucket-size`
historyControlBucketsGranted	Número de intervalos de muestreo discretos durante los cuales se guardarán los datos.	—
historyControlInterval	Intervalo, en segundos, sobre el cual se muestrean los datos para cada bucket.	`interval`
historialControlOwner	Entidad que configuró esta entrada.	`owner`
historyControlStatus	Estado de esta entrada.	—

Configuración mínima de alarma RMON y entrada de eventos

Para habilitar RMON en el enrutador, debe configurar una entrada de alarma y una entrada de evento. Para ello, incluya las siguientes instrucciones en el nivel de jerarquía:`[edit snmp rmon]`

```
[edit snmp rmon]
alarm index {
    rising-event-index index;
    rising-threshold integer;
    sample-type type;
    variable oid-variable;
```

```
}
event index;
```

Configurar una entrada de alarma RMON y sus atributos

in this section

- Configurar la entrada de alarma | 735
- Configure la descripción | 736
- Configurar el índice de eventos descendentes o el índice de eventos ascendentes | 736
- Configurar el umbral descendente o ascendente | 737
- Configurar el intervalo | 738
- Configurar el intervalo de umbral descendente | 738
- Configurar el tipo de solicitud | 738
- Configurar el tipo de ejemplo | 739
- Configurar la alarma de inicio | 739
- Configurar la etiqueta de registro del sistema | 740
- Configurar la variable | 740

Una entrada de alarma monitorea el valor de una variable MIB. Puede configurar la frecuencia con la que se muestrea el valor, el tipo de muestreo que se va a realizar y el evento que se desencadena si se cruza un umbral.

En esta sección se tratan los siguientes temas:

Configurar la entrada de alarma

Una entrada de alarma monitorea el valor de una variable MIB. Las instrucciones, , , y son obligatorias.`rising-event-index`` rising-threshold`` sample-type`` variable` Todas las demás instrucciones son opcionales.

Para configurar la entrada de alarma, incluya la instrucción y especifique un índice en el nivel de jerarquía:`alarm[edit snmp rmon]`

```
[edit snmp rmon]
alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising alarm | rising-or-falling-alarm);
    variable oid-variable;
}
```

index es un entero que identifica una alarma o entrada de evento.

Configure la descripción

La descripción es una cadena de texto que identifica la entrada de alarma.

Para configurar la descripción, incluya la instrucción y una descripción de la entrada de alarma en el nivel jerárquico:`description[edit snmp rmon alarm index]`

```
[edit snmp rmon alarm index]
description description;
```

Configurar el índice de eventos descendentes o el índice de eventos ascendentes

El índice de eventos decrecientes identifica la entrada de evento que se activa cuando se cruza un umbral descendente. El índice de eventos ascendentes identifica la entrada de eventos que se activa cuando se cruza un umbral ascendente.

Para configurar el índice de eventos descendentes o el índice de eventos ascendentes, incluya la instrucción o y especifique un índice en el nivel jerárquico :`falling-event-indexrising-event-index`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
falling-event-index index;
rising-event-index index;
```

`index` puede ser de 0 a 65.535. El valor predeterminado para el índice de eventos descendentes y ascendentes es 0.

Configurar el umbral descendente o ascendente

El umbral descendente es el umbral inferior para la variable monitoreada. Cuando el valor muestreado actual es menor o igual que este umbral y el valor en el último intervalo de muestreo es mayor que este umbral, se genera un solo evento. También se genera un único evento si la primera muestra después de que esta entrada sea válida es menor o igual que este umbral y la alarma de inicio asociada es igual a o .`falling-alarmrising-or-falling-alarm` Después de generar un evento descendente, no se puede generar otro evento descendente hasta que el valor muestreado se eleve por encima de este umbral y alcance el umbral ascendente. Debe especificar el umbral descendente como un número entero. Su valor predeterminado es un 20 por ciento menor que el umbral creciente.

De forma predeterminada, el umbral ascendente es 0. El umbral ascendente es el umbral superior para la variable monitoreada. Cuando el valor muestreado actual es mayor o igual que este umbral y el valor en el último intervalo de muestreo es menor que este umbral, se genera un solo evento. También se genera un único evento si la primera muestra después de que esta entrada sea válida es mayor o igual que este umbral, y la asociada es igual a o .`startup-alarmrising-alarmrising-or-falling-alarm` Después de generar un evento ascendente, no se puede generar otro evento ascendente hasta que el valor muestreado caiga por debajo de este umbral y alcance el umbral descendente. Debe especificar el umbral ascendente como un número entero.

Para configurar el umbral descendente o el umbral ascendente, incluya la instrucción o en el nivel jerárquico :`falling-thresholdrising-threshold`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
falling-threshold integer;
rising-threshold integer;
```

`integer` puede ser un valor comprendido entre -2.147.483.647 y 2.147.483.647.

Configurar el intervalo

El intervalo representa el período de tiempo, en segundos, durante el cual se muestrea la variable monitoreada y se compara con los umbrales ascendentes y descendentes.

Para configurar el intervalo, incluya la instrucción y especifique el número de segundos en el nivel de jerarquía:`interval`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
interval seconds;
```

seconds puede ser un valor comprendido entre 1 y 2.147.483.647. El valor predeterminado es de 60 segundos.

Configurar el intervalo de umbral descendente

El intervalo de umbral descendente representa el intervalo entre muestras cuando se cruza el umbral ascendente. Una vez que la alarma cruza el umbral descendente, se utiliza el intervalo de muestreo regular.

> **NOTA**: No puede configurar el intervalo de umbral descendente para alarmas que tengan el tipo de solicitud establecido en `.walk-request`

Para configurar el intervalo de umbral descendente, incluya la instrucción en el nivel de jerarquía y especifique el número de segundos:`falling-threshold interval`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
falling-threshold-interval seconds;
```

seconds puede ser un valor comprendido entre 1 y 2.147.483.647. El valor predeterminado es de 60 segundos.

Configurar el tipo de solicitud

De forma predeterminada, una alarma RMON solo puede supervisar una instancia de objeto (como se especifica en la configuración). Puede configurar una instrucción para ampliar el alcance de la alarma RMON a fin de incluir todas las instancias de objetos que pertenecen a una rama MIB o para incluir la siguiente instancia de objeto después de la instancia especificada en la configuración.`request-type`

Para configurar el tipo de solicitud, incluya la instrucción en el nivel de jerarquía y especifique , , o :`request-type`[`edit snmp rmon alarm` *`index`*]`get-next-request`get-request`walk-request`

```
[edit snmp rmon alarm index]
request-type (get-next-request | get-request | walk-request);
```

extiende la configuración de alarma RMON a todas las instancias de objetos que pertenecen a una rama MIB. amplía la configuración de la alarma RMON para incluir la siguiente instancia de objeto después de la instancia especificada en la configuración.`walknext`

Configurar el tipo de ejemplo

El tipo de muestra identifica el método de muestreo de la variable seleccionada y el cálculo del valor que debe compararse con los umbrales. Si el valor de este objeto es , el valor de la variable seleccionada se compara directamente con los umbrales al final del intervalo de muestreo.`absolute-value` Si el valor de este objeto es , el valor de la variable seleccionada en la última muestra se resta del valor actual y la diferencia se compara con los umbrales.`delta-value`

Para configurar el tipo de ejemplo, incluya la instrucción y especifique el tipo de ejemplo en el nivel de jerarquía:`sample-type`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
sample-type (absolute-value | delta-value);
```

- `absolute-value`: el valor real de la variable seleccionada se compara con los umbrales.
- `delta-value`—La diferencia entre las muestras de la variable seleccionada se compara con los umbrales.

Configurar la alarma de inicio

La alarma de inicio identifica el tipo de alarma que se puede enviar cuando se activa esta entrada por primera vez. Puede especificarlo como , , o .`falling-alarm`rising-alarm`rising-or-falling-alarm`

Para configurar la alarma de inicio, incluya la instrucción y especifique el tipo de alarma en el nivel jerárquico:`startup-alarm`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);
```

- `falling-alarm`: se genera si la primera muestra después de que la entrada de alarma se active es menor o igual que el umbral descendente.

- `rising-alarm`: se genera si la primera muestra después de que la entrada de alarma se activa es mayor o igual que el umbral ascendente.
- `rising-or-falling-alarm`: se genera si la primera muestra después de que la entrada de alarma se active satisface cualquiera de los umbrales correspondientes.

El valor predeterminado es .`rising-or-falling-alarm`

Configurar la etiqueta de registro del sistema

La instrucción especifica la etiqueta que se agregará al mensaje de registro del sistema.`syslog-subtag` Puede especificar una cadena de no más de 80 caracteres en mayúsculas como etiqueta de registro del sistema.

Para configurar la etiqueta de registro del sistema, incluya la instrucción en el nivel de jerarquía:`syslog-subtag`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
syslog-subtag syslog-subtag;
```

Configurar la variable

La variable identifica el objeto MIB que se está supervisando.

Para configurar la variable, incluya la instrucción y especifique el identificador de objeto o el nombre de objeto en el nivel de jerarquía:`variable`[`edit snmp rmon alarm` *`index`*]

```
[edit snmp rmon alarm index]
variable oid-variable;
```

es un decimal punteado (por ejemplo,) o un nombre de objeto MIB (por ejemplo,).*`oid-variable`*`1.3.6.1.2.1.2.1.2.2.1.10.1ifInOctets.1`

Configurar una entrada de evento RMON y sus atributos

Una entrada de evento genera una notificación para una entrada de alarma cuando se cruza su umbral ascendente o descendente. Puede configurar el tipo de notificación que se genera. Para configurar la

entrada del evento, incluya la instrucción en el nivel de jerarquía.`event`[`edit snmp rmon`] Todas las instrucciones, excepto la instrucción, son opcionales.`event`

```
[edit snmp rmon]
event index {
    community community-name;
    description description;
    type type;
}
```

`index` identifica un evento de entrada.

`community-name` es el grupo de capturas que se utiliza al generar una captura. Si ese grupo de capturas tiene configurada la categoría de captura, se envía una captura a todos los destinos configurados para ese grupo de capturas.`rmon-alarm` La cadena de comunidad de la captura coincide con el nombre del grupo de captura. Si no se configura nada, se examinan todos los grupos de capturas y las capturas se envían utilizando cada grupo con la categoría establecida.`rmon-alarm`

`description` es una cadena de texto que identifica la entrada.

La variable de una entrada de evento especifica dónde se va a registrar el evento.*`type`* Puede especificar el tipo como una de las siguientes opciones:

- : agrega la entrada del evento al archivo .`loglogTable`
- `log-and-trap`: envía una captura SNMP y crea una entrada de registro.
- `none`: no envía ninguna notificación.
- `snmptrap`: envía una captura SNMP.

El valor predeterminado para el tipo de entrada de evento es .`log-and-trap`

Ejemplo: Configurar una alarma RMON y la entrada de eventos

Configure una alarma RMON y la entrada de eventos:

```
[edit snmp]
rmon {
    alarm 100 {
        description “input traffic on fxp0”;
        falling-event-index 100;
```

```
        falling-threshold 10000;
        interval 60;
        rising-event-index 100;
        rising-threshold 100000;
        sample-type delta-value;
        startup-alarm rising-or-falling-alarm;
        variable ifInOctets.1;
    }
    event 100 {
        community bedrock;
        description” emergency events”;
        type log-and-trap;
    }
}
```

Utilice alarmTable para supervisar objetos MIB

in this section

- Crear una entrada de alarma | **742**
- Configurar los objetos MIB de alarma | **743**
- Activar una nueva fila en alarmTable | **746**
- Modificar una fila activa en alarmTable | **746**
- Desactivar una fila en alarmTable | **746**

Para utilizar alarmTable para supervisar un objeto MIB, realice las siguientes tareas:

Crear una entrada de alarma

Para crear una entrada de alarma, cree primero una nueva fila en alarmTable mediante el objeto alarmStatus. Por ejemplo, cree la alarma #1 usando las utilidades de línea de comandos de UCD:

```
snmpset -Os -v2c router community alarmStatus.1 i createRequest
```

Configurar los objetos MIB de alarma

in this section

- alarmInterval | 743
- alarmaVariable | 743
- alarmSampleType | 744
- alarmValue | 744
- alarmaStartupAlarm | 744
- alarmRisingThreshold | 744
- alarmaFallingThreshold | 745
- alarmaPropietario | 745
- alarmRisingEventIndex | 745
- alarmFallingEventIndex | 746

Una vez que haya creado la nueva fila en alarmTable, configure los siguientes objetos MIB de alarma:

NOTA: Aparte de alarmStatus, no puede modificar ninguno de los objetos de la entrada si el objeto alarmStatus asociado está establecido en `.valid`

alarmInterval

El intervalo, en segundos, sobre el cual se muestrean los datos y se comparan con los umbrales ascendentes y descendentes. Por ejemplo, para configurar la alarma #1 a 30 segundos, utilice la siguiente solicitud SNMP :`alarmIntervalSet`

```
snmpset -Os -v2c router community alarmInterval.1 i 30
```

alarmaVariable

Identificador de objeto de la variable que se va a muestrear. Durante una solicitud, si el nombre de la variable proporcionada no está disponible en la vista MIB seleccionada, se devuelve un error badValue.`Set` Si en algún momento el nombre de variable de un alarmEntry establecido ya no está disponible en la vista MIB seleccionada, el sondeo cambia el estado de alarmVariable a no válido. Por

ejemplo, para identificar ifInOctets.61 como la variable que se va a supervisar, utilice la siguiente solicitud SNMP :`Set`

```
snmpset -Os -v2c router community alarmVariable.1 o .1.3.6.1.2.1.2.2.1.10.61
```

alarmSampleType

El método de muestreo de la variable seleccionada y cálculo del valor que debe compararse con los umbrales. Si el valor de este objeto es absoluteValue, el valor de la variable seleccionada se compara directamente con los umbrales al final del intervalo de muestreo. Si el valor de este objeto es deltaValue, el valor de la variable seleccionada en la última muestra se resta del valor actual y la diferencia se compara con los umbrales. Por ejemplo, para establecer alarmSampleType para la alarma #1 en deltaValue, utilice la siguiente solicitud SNMP :`Set`

```
snmpset -Os -v2c router community alarmSampleType.1 i deltaValue
```

alarmValue

El valor de la variable durante el último período de muestreo. Este valor se compara con los umbrales ascendentes y descendentes. Si el tipo de muestra es deltaValue, este valor es igual a la diferencia entre las muestras al principio y al final del período. Si el tipo de muestra es , este valor es igual al valor muestreado al final del período.`absoluteValue`

alarmaStartupAlarm

Una alarma que se envía cuando esta entrada se establece por primera vez en válida. Si la primera muestra después de que esta entrada sea válida es mayor o igual que , y es igual a o , se genera una única alarma ascendente.`risingThresholdalarmStartupAlarmrisingAlarmrisingOrFallingAlarm` Si la primera muestra después de que esta entrada sea válida es menor o igual que y es igual a o , se genera una sola alarma de caída.`fallingThresholdalarmStartupAlarmfallingAlarmrisingOrFallingAlarm` Por ejemplo, para configurar la alarma #1 en , utilice la siguiente solicitud SNMP :`alarmStartupAlarmrisingOrFallingAlarmSet`

```
snmpset -Os -v2c router community alarmStartupAlarm.1 i risingOrFallingAlarm
```

alarmRisingThreshold

Un umbral para la variable muestreada. Cuando el valor muestreado actual es mayor o igual que este umbral y el valor en el último intervalo de muestreo es menor que este umbral, se genera un solo

evento. También se genera un único evento si la primera muestra después de que esta entrada sea válida es mayor o igual que este umbral, y la asociada es igual a o `.alarmStartupAlarmrisingAlarmrisingOrFallingAlarm` Después de generar un evento ascendente, no se puede generar otro evento ascendente hasta que el valor muestreado caiga por debajo de este umbral y alcance `.alarmFallingThreshold` Por ejemplo, para configurar la alarma #1 en , utilice la siguiente solicitud SNMP :`alarmRisingThreshold100000Set`

```
snmpset -Os -v2c router community alarmRisingThreshold.1 i 100000
```

alarmaFallingThreshold

Un umbral para la variable muestreada. Cuando el valor muestreado actual es menor o igual que este umbral y el valor en el último intervalo de muestreo es mayor que este umbral, se genera un solo evento. También se genera un solo evento si la primera muestra después de que esta entrada sea válida es menor o igual que este umbral, y la asociada es igual a o `.alarmStartupAlarmfallingAlarmrisingOrFallingAlarm` Después de generar un evento de caída, no se puede generar otro evento de caída hasta que el valor muestreado se eleve por encima de este umbral y alcance `.alarmRisingThreshold` Por ejemplo, para configurar la alarma #1 en , utilice la siguiente solicitud SNMP :`alarmFallingThreshold10000Set`

```
snmpset -Os -v2c router community alarmFallingThreshold.1 i 10000
```

alarmaPropietario

Cualquier cadena de texto especificada por la aplicación de administración creadora o la interfaz de línea de comandos (CLI). Normalmente, se utiliza para identificar un administrador de red (o aplicación) y se puede utilizar para un control de acceso preciso entre las aplicaciones de administración participantes.

alarmRisingEventIndex

Índice del objeto eventEntry que se utiliza cuando se cruza un umbral ascendente. Si no hay ninguna entrada correspondiente en eventTable, entonces no existe ninguna asociación. Si este valor es cero, no se genera ningún evento asociado porque cero no es un índice de eventos válido. Por ejemplo, para establecer alarmRisingEventIndex para la alarma #1 en , utilice la siguiente solicitud SNMP :`10Set`

```
snmpset -Os -v2c router community alarmRisingEventIndex.1 i 10
```

alarmFallingEventIndex

Índice del objeto eventEntry que se utiliza cuando se cruza un umbral descendente. Si no hay ninguna entrada correspondiente en eventTable, entonces no existe ninguna asociación. Si este valor es cero, no se genera ningún evento asociado porque cero no es un índice de eventos válido. Por ejemplo, para establecer alarmFallingEventIndex para la alarma #1 en , utilice la siguiente solicitud SNMP :`10Set`

```
snmpset -Os -v2c router community alarmFallingEventIndex.1 i 10
```

Activar una nueva fila en alarmTable

Para activar una nueva fila en alarmTable, establezca alarmStatus en mediante una solicitud SNMP :`validSet`

```
snmpset -Os -v2c router community alarmStatus.1 i valid
```

Modificar una fila activa en alarmTable

Para modificar una fila activa, establezca primero alarmStatus en underCreation mediante una solicitud SNMP :`Set`

```
snmpset -Os -v2c router community alarmStatus.1 i underCreation
```

A continuación, cambie el contenido de la fila mediante una solicitud SNMP :`Set`

```
snmpset -Os -v2c router community alarmFallingThreshold.1 i 1000
```

Por último, active la fila estableciendo alarmStatus para usar una solicitud SNMP :`validSet`

```
snmpset -Os -v2c router community alarmStatus.1 i valid
```

Desactivar una fila en alarmTable

Para desactivar una fila en alarmTable, establezca alarmStatus en mediante una solicitud SNMP :`invalidSet`

```
snmpset -Os -v2c router community alarmStatus.1 i invalid
```

Usar eventTable para registrar alarmas

in this section

- Crear una entrada de evento | 747
- Configurar los objetos MIB | 747
- Activar una nueva fila en eventTable | 749
- Desactivar una fila en eventTable | 750

Para utilizar eventTable para registrar alarmas, realice las siguientes tareas:

Crear una entrada de evento

La tabla de eventos de RMON controla la generación de notificaciones desde el enrutador. Las notificaciones pueden ser registros (entradas a logTable y syslogs) o capturas SNMP. Cada entrada de evento se puede configurar para generar cualquier combinación de estas notificaciones (o ninguna notificación). Cuando un evento especifica que se va a generar una captura SNMP, el grupo de capturas que se utiliza al enviar la captura se especifica mediante el valor del objeto eventCommunity asociado. Por consiguiente, la comunidad del mensaje de captura coincidirá con el valor especificado por eventCommunity. Si no hay nada configurado para eventCommunity, se envía una captura utilizando cada grupo de capturas que tenga configurada la categoría rmon-alarm.

Configurar los objetos MIB

in this section

- eventType | 748
- eventoComunidad | 748
- eventOwner | 749
- descripción del evento | 749

Una vez que haya creado la nueva fila en eventTable, establezca los siguientes objetos:

NOTA: El objeto eventType es obligatorio. Todos los demás objetos son opcionales.

eventType

Tipo de notificación que genera el enrutador cuando se activa el evento.

Este objeto se puede establecer en los siguientes valores:

- `log`: agrega la entrada del evento a logTable.
- `log-and-trap`: envía una captura SNMP y crea una entrada de registro.
- `none`: no envía ninguna notificación.
- `snmptrap`: envía una captura SNMP.

Por ejemplo, para establecer el evento #1 en , use la siguiente solicitud SNMP :`eventTypelog-and-trapSet`

```
snmpset -Os -v2c router community eventType.1 i log-and-trap
```

eventoComunidad

El grupo de capturas que se utiliza al generar una captura (si eventType está configurado para enviar capturas). Si ese grupo de capturas tiene configurada la categoría de captura rmon-alarm, se envía una captura a todos los destinos configurados para ese grupo de capturas. La cadena de comunidad de la captura coincide con el nombre del grupo de captura (y, por lo tanto, con el valor de eventCommunity). Si no se configura nada, las capturas se envían a cada grupo con la categoría rmon-alarm establecida. Por ejemplo, para establecer eventCommunity para el evento #1 en boy-elroy, use la siguiente solicitud SNMP :`Set`

```
snmpset -Os -v2c router community eventCommunity.1 s "boy-elroy"
```

NOTA: El objeto eventCommunity es opcional. Si no establece este objeto, el campo se deja en blanco.

eventOwner

Cualquier cadena de texto especificada por la aplicación de administración creadora o la interfaz de línea de comandos (CLI). Normalmente, se utiliza para identificar un administrador de red (o aplicación) y se puede utilizar para un control de acceso preciso entre las aplicaciones de administración participantes.

Por ejemplo, para establecer eventOwner para el evento #1 en george jetson, utilice la siguiente solicitud SNMP :`Set`

```
snmpset -Os -v2c router community eventOwner.1 s "george jetson"
```

NOTA: El objeto eventOwner es opcional. Si no establece este objeto, el campo se deja en blanco.

descripción del evento

Cualquier cadena de texto especificada por la aplicación de administración creadora o la interfaz de línea de comandos (CLI). El uso de esta cadena depende de la aplicación.

Por ejemplo, para establecer eventDescription para el evento #1 en ruedas dentadas spacelys, use la siguiente solicitud SNMP :`Set`

```
snmpset -Os -v2c router community eventDescription.1 s "spacelys sprockets"
```

NOTA: El objeto eventDescription es opcional. Si no establece este objeto, el campo se deja en blanco.

Activar una nueva fila en eventTable

Para activar la nueva fila en eventTable, establezca eventStatus en el uso de una solicitud SNMP como:`validSet`

```
snmpset -Os -v2c router community eventStatus.1 i valid
```

Desactivar una fila en eventTable

Para desactivar una fila en eventTable, establezca eventStatus en el uso de una solicitud SNMP como:`invalidSet`

```
snmpset -Os -v2c router community eventStatus.1 i invalid
```

Configurar el muestreo del historial de RMON

in this section

- Configurar la recopilación de muestreo del historial de RMON | **750**
- Ver y borrar estadísticas del historial de RMON | **751**

Junos OS admite el grupo de control de historial () de la MIB de supervisión remota de red (RPON) (RFC 2819).etherHistoryTable Las tablas de control de historial registran muestras estadísticas de una red Ethernet y las almacenan para su posterior recuperación.

Para configurar el muestreo del historial de RMON y ver o borrar las estadísticas recopiladas mediante la CLI de Junos OS, realice las siguientes tareas:

Configurar la recopilación de muestreo del historial de RMON

Utilice la instrucción en el nivel de jerarquía para configurar los parámetros de recopilación de muestreo del historial de RMON.`history[edit snmp rmon]` Se requieren los siguientes parámetros:

- Índice de historia: La entrada de historial se identifica mediante un valor de índice de historial entero (campo MIB) especificado al configurar esta instrucción, que se utiliza para mostrar o borrar los resultados recopilados posteriormente.`historyControlIndex`
- Interfaz: Interfaz que se va a supervisar para el índice de historial especificado. Solo se puede asociar una interfaz a un índice de historial de RMON determinado.

Además de los parámetros requeridos, puede especificar un muestreo personalizado (en segundos) y el muestreo (número de muestras discretas que se recogerán en un intervalo determinado).`intervalbucket-size`

```
[edit snmp]
user@switch# set rmon history history-index interface interface-name
user@switch# set rmon history history-index interval seconds
user@switch# set rmon history history-index bucket-size number
```

También se puede asignar a la colección una etiqueta opcional () asociada al índice de historial.`owner`

Ver y borrar estadísticas del historial de RMON

Utilice el comando para mostrar las entradas de la tabla de historial RMON recopiladas.`show snmp rmon history` También puede utilizar el comando para ver ejemplos de campos de tabla de historial de RMON.`show snmp mib walk`

La siguiente configuración RMON de ejemplo configura un muestreo de tabla de historial para la interfaz xe-0/0/20.0 utilizando un valor de índice de historial de 1:

```
user@switch# show snmp | display set
set snmp rmon history 1 interface xe-0/0/20.0
set snmp rmon history 1 bucket-size 1000
set snmp rmon history 1 interval 5
set snmp rmon history 1 owner test
```

Con el comando, puede ver las estadísticas de campo recopiladas para el índice de historial 1:`show snmp mib walketherHistoryPkts`

```
user@switch> show snmp mib walk etherHistoryPkts
etherHistoryPkts.1.1 = 0
<...>
etherHistoryPkts.1.148 = 10
etherHistoryPkts.1.149 = 14
```

Para borrar las estadísticas del historial de RMON recopiladas, utilice el comando.`clear snmp history` Después de borrar las muestras recolectadas hasta ese punto, la recolección continúa nuevamente en el intervalo configurado y se registran nuevas muestras. Este comando tiene opciones para borrar las

muestras recopiladas de un determinado índice de historial configurado o borrar todas las muestras de todos los índices configurados.

Por ejemplo, el siguiente comando borra los ejemplos de historial de RMON recopilados para el índice de control de historial 1 configurado anteriormente:

```
user@switch> clear snmp history 1
Samples collected are cleared.

user@switch> show snmp mib walk etherHistoryPkts | no-more


user@switch> show snmp mib walk etherHistoryPkts | no-more
etherHistoryPkts.1.1 = 0
```

Supervisión de la calidad del servicio de red mediante RMON

in this section

- RMON para monitorear la calidad del servicio | **753**
- Descripción de los puntos de medición, los indicadores clave de rendimiento y los valores de referencia | **758**
- Definir y medir la disponibilidad de la red | **760**
- Medir la salud | **768**
- Mida el rendimiento | **777**

RMON para monitorear la calidad del servicio

in this section

- Configuración de umbrales | **753**
- Interfaz de línea de comandos RMON | **755**
- Tabla de eventos RMON | **755**
- Tabla de alarma RMON | **756**
- Solución de problemas de RMON | **757**

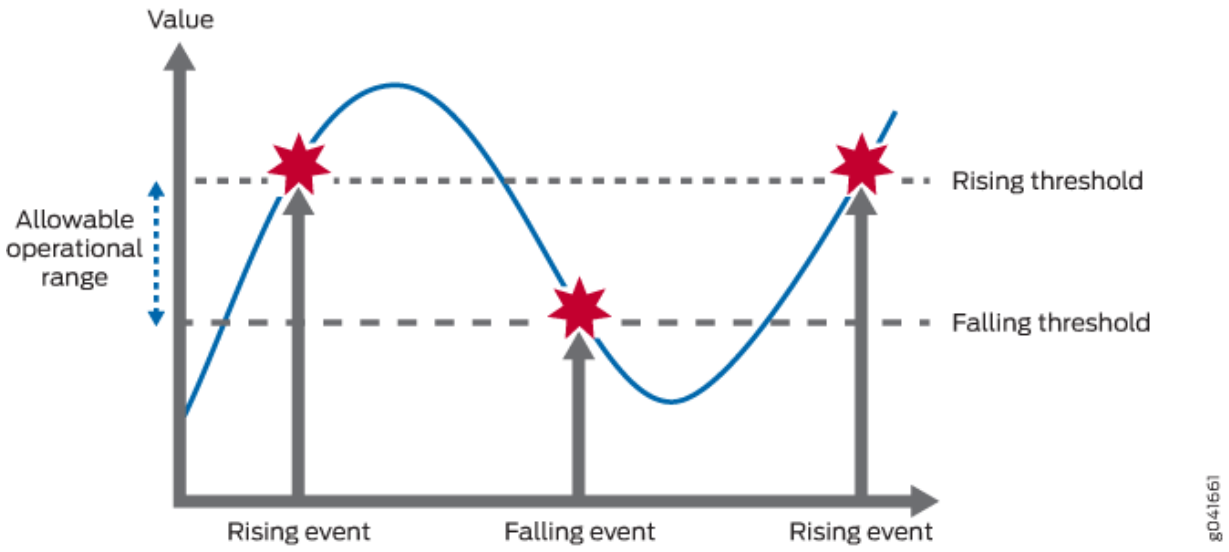
La supervisión del estado y el rendimiento puede beneficiarse de la supervisión remota de variables SNMP por parte de los agentes SNMP locales que se ejecutan en cada enrutador. Los agentes SNMP comparan los valores MIB con umbrales predefinidos y generan alarmas de excepción sin necesidad de sondeo por parte de una plataforma de administración SNMP central. Este es un mecanismo eficaz para la gestión proactiva, siempre que los umbrales tengan líneas de base determinadas y establecidas correctamente. Para obtener más información, consulte RFC 2819, *MIB de supervisión remota de red*.

En este tema, se incluyen las siguientes secciones:

Configuración de umbrales

Al establecer un umbral ascendente y descendente para una variable supervisada, se le puede alertar cada vez que el valor de la variable caiga fuera del rango operativo permitido. (Consulte Figura 25 en la página 754.)

Figura 25: Configuración de umbrales



Los eventos solo se generan cuando el umbral se cruza por primera vez en una dirección en lugar de después de cada período de muestreo. Por ejemplo, si se eleva un evento de cruce de umbral ascendente, no se producirán más eventos de cruce de umbral hasta un evento de caída correspondiente. Esto reduce considerablemente la cantidad de alarmas que produce el sistema, lo que facilita que el personal de operaciones reaccione cuando se producen alarmas.

Para configurar la supervisión remota, especifique los siguientes datos:

- La variable que se va a supervisar (por su identificador de objeto SNMP)
- El tiempo transcurrido entre cada inspección
- Un umbral ascendente
- Un umbral descendente
- Un evento en alza
- Un evento de caída

Antes de poder configurar correctamente la supervisión remota, debe identificar qué variables deben supervisarse y su rango operativo permitido. Esto requiere un período de referencia para determinar los rangos operativos permitidos. Un período inicial de referencia de al menos tres meses no es inusual cuando se identifican por primera vez los rangos operativos y se definen los umbrales, pero el monitoreo de línea de base debe continuar durante la vida útil de cada variable monitoreada.

Interfaz de línea de comandos RMON

Junos OS proporciona dos mecanismos que se utilizan para controlar el agente de supervisión remota en el enrutador: interfaz de línea de comandos (CLI) y SNMP. Para configurar una entrada de RMON mediante la CLI, incluya las siguientes instrucciones en el nivel de jerarquía:`[edit snmp]`

```
rmon {
    alarm index {
        description;
        falling-event-index;
        falling-threshold;
        intervals;
        rising-event-index;
        rising-threshold;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling | rising | rising-or-falling);
        variable;
    }
    event index {
        community;
        description;
        type (log | trap | log-and-trap | none);
    }
}
```

Si no tiene acceso a la CLI, puede configurar la supervisión remota mediante SNMP Manager o la aplicación de administración, suponiendo que se haya concedido acceso SNMP. (Véase .) Para configurar RMON mediante SNMP, realice solicitudes SNMP a las tablas de eventos y alarmas de RMON.Tabla 63 en la página 756`Set`

Tabla de eventos RMON

Configure un evento para cada tipo que desee generar. Por ejemplo, podría tener dos eventos genéricos, subida y bajada, o muchos eventos diferentes para cada variable que se está supervisando (por ejemplo, evento de aumento de temperatura, evento de caída de temperatura, evento de golpe de firewall, evento de utilización de interfaz, etc.). Una vez configurados los eventos, no es necesario actualizarlos.

Tabla 63: Tabla de eventos RMON

Campo	Description
`eventDescription`	Descripción textual de este evento
`eventType`	Tipo de evento (por ejemplo, , , o y)`logtraplogtrap`
`eventCommunity`	Grupo de captura al que enviar este evento (como se define en la configuración de Junos OS, que no es lo mismo que la comunidad)
`eventOwner`	Entidad (por ejemplo,) que creó este evento`manager`
`eventStatus`	Estado de esta fila (por ejemplo, , , o)`validinvalidcreateRequest`

Tabla de alarma RMON

La tabla de alarmas RMON almacena los identificadores de objeto SNMP (incluidas sus instancias) de las variables que se supervisan, junto con los umbrales ascendentes y descendentes y sus índices de eventos correspondientes. Para crear una solicitud RMON, especifique los campos que se muestran en .Tabla 64 en la página 756

Tabla 64: Tabla de alarma RMON

Campo	Description
`alarmStatus`	Estado de esta fila (por ejemplo, , , o)`validinvalidcreateRequest`
`alarmInterval`	Período de muestreo (en segundos) de la variable monitoreada
`alarmVariable`	OID (e instancia) de la variable a monitorear
`alarmValue`	Valor real de la variable muestreada
`alarmSampleType`	Tipo de muestra (o cambios)`absolutedelta`

Tabla 64: Tabla de alarma RMON *(Continued)*

Campo	Description
alarmStartupAlarm	Alarma inicial (, , o)risingfallingeither
alarmRisingThreshold	Umbral ascendente con el que comparar el valor
alarmFallingThreshold	Umbral descendente con el que comparar el valor
alarmRisingEventIndex	Índice (fila) del evento ascendente en la tabla de eventos
alarmFallingEventIndex	Índice (fila) del evento descendente en la tabla de eventos

Tanto los campos como los son primitivos, como se define en RFC 2579, Convenciones textuales para SMIv2.alarmStatuseventStatusentryStatus

Solución de problemas de RMON

Para solucionar los problemas del agente RMON, , que se ejecuta en el enrutador, inspeccione el contenido de la MIB de RMON empresarial de Juniper Networks, , que proporciona las extensiones enumeradas en el RFC 2819.rmopdjnxRmonTabla 65 en la página 757alarmTable

Tabla 65: Extensiones de alarma jnxRmon

Campo	Description
jnxRmonAlarmGetFailCnt	Número de veces que se produjo un error en la solicitud interna de la variableGet
jnxRmonAlarmGetFailTime	Valor de cuándo se produjo el último errorsysUpTime
jnxRmonAlarmGetFailReason	Motivo por el que se produjo un error en la solicitudGet
jnxRmonAlarmGetOkTime	Valor de cuando la variable salió del estado de errorsysUpTime

Tabla 65: Extensiones de alarma jnxRmon *(Continued)*

Campo	Description
`jnxRmonAlarmState`	Estado de esta entrada de alarma

La supervisión de las extensiones de esta tabla proporciona pistas sobre por qué las alarmas remotas pueden no comportarse como se esperaba.

Descripción de los puntos de medición, los indicadores clave de rendimiento y los valores de referencia

in this section

- Puntos de medición | **758**
- Indicadores clave básicos de rendimiento | **759**
- Configuración de líneas base | **760**

En este tema del capítulo se proporcionan directrices para supervisar la calidad del servicio de una red IP. Describe cómo los proveedores de servicios y los administradores de red pueden usar la información proporcionada por los enrutadores de Juniper Networks para monitorear el rendimiento y la capacidad de la red. Debe tener un conocimiento profundo del SNMP y de la MIB asociada compatible con Junos OS.

NOTA: Para obtener una buena introducción al proceso de supervisión de una red IP, consulte RFC 2330, *Framework for IP Performance Metrics*.

Este tema contiene las siguientes secciones:

Puntos de medición

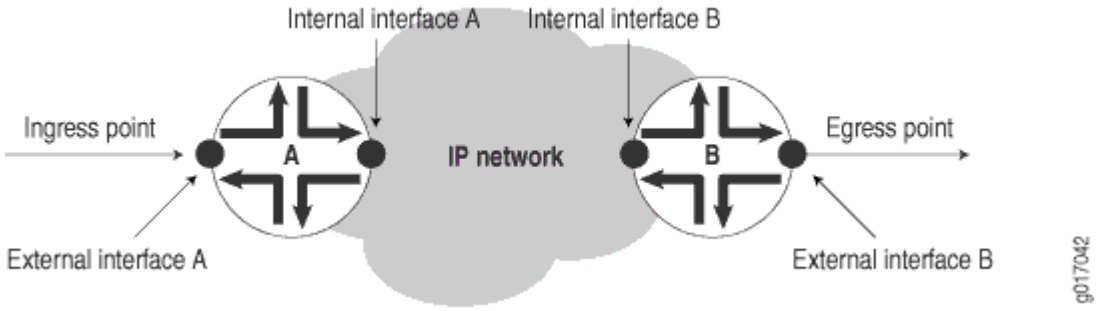
Definir los puntos de medición donde se miden las métricas es tan importante como definir las métricas en sí. En esta sección se describen los puntos de medición en el contexto de este capítulo y se ayuda a identificar dónde se pueden realizar mediciones desde una red de proveedores de servicios. Es

importante entender exactamente dónde está un punto de medición. Los puntos de medición son vitales para comprender la implicación de lo que significa la medición real.

Una red IP consiste en una colección de enrutadores conectados por vínculos físicos que ejecutan el protocolo de Internet. Puede ver la red como una colección de enrutadores con un punto de entrada y un punto de salida. Consulte Figura 26 en la página 759.

- Las mediciones centradas en la red se toman en los puntos de medición que se corresponden más estrechamente con los puntos de entrada y salida de la propia red. Por ejemplo, para medir el retraso en toda la red del proveedor desde el sitio A hasta el sitio B, los puntos de medición deben ser el punto de entrada a la red del proveedor en el sitio A y el punto de salida en el sitio B.
- Las mediciones centradas en el enrutador se toman directamente de los propios enrutadores, pero tenga cuidado de asegurarse de que los subcomponentes correctos del enrutador se hayan identificado de antemano.

Figura 26: Puntos de entrada a la red



NOTA: Figura 26 en la página 759 no muestra las redes del cliente en las instalaciones del cliente, pero estarían ubicadas a ambos lados de los puntos de entrada y salida. Aunque en este capítulo no se describe cómo medir los servicios de red tal como los perciben estas redes cliente, puede utilizar las mediciones tomadas para la red del proveedor de servicios como entrada en dichos cálculos.

Indicadores clave básicos de rendimiento

Por ejemplo, podría supervisar una red de proveedores de servicios en busca de tres indicadores clave de rendimiento (KPI) básicos:

- mide la "accesibilidad" de un punto de medición desde otro punto de medición en la capa de red (por ejemplo, utilizando ping ICMP). La infraestructura subyacente de enrutamiento y transporte de la red

de proveedores admitirá las mediciones de disponibilidad, y las fallas se destacarán como indisponibilidad.

- Mide el número y el tipo de errores que se producen en la red del proveedor, y puede consistir en mediciones centradas tanto en el enrutador como en la red, como fallas de hardware o pérdida de paquetes.
- de la red de proveedores mide en qué medida puede soportar los servicios de IP (por ejemplo, en términos de retraso o utilización).

Configuración de líneas base

¿Qué tan bien está funcionando la red de proveedores? Recomendamos un período inicial de monitoreo de tres meses para identificar los parámetros operativos normales de una red. Con esta información, puede reconocer excepciones e identificar comportamientos anormales. Debe continuar con el monitoreo de línea base durante la vida útil de cada métrica medida. Con el tiempo, debe ser capaz de reconocer las tendencias de rendimiento y los patrones de crecimiento.

En el contexto de este capítulo, muchas de las métricas identificadas no tienen un rango operativo permitido asociado. En la mayoría de los casos, no se puede identificar el rango operativo permitido hasta que se haya determinado una línea base para la variable real en una red específica.

Definir y medir la disponibilidad de la red

in this section

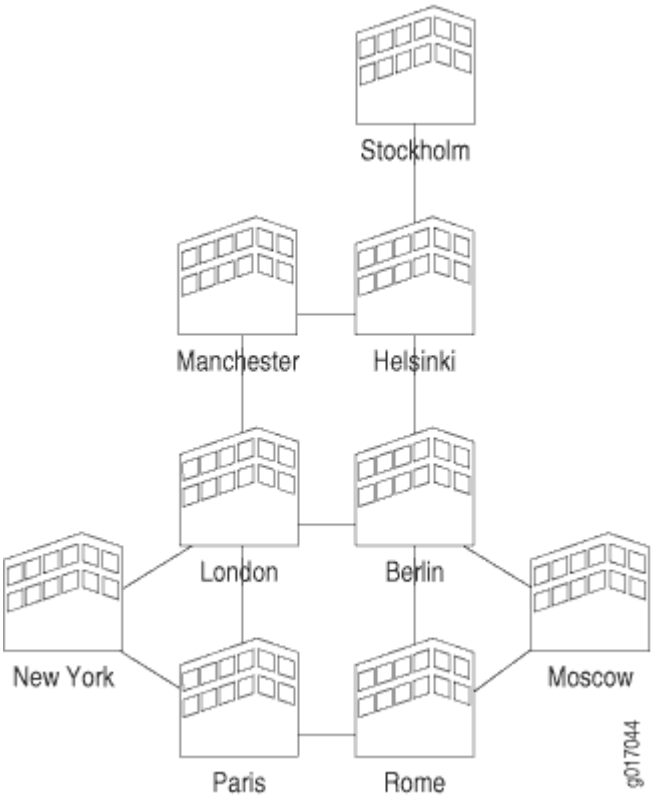
- Definir la disponibilidad de la red | **760**
- Mida la disponibilidad | **764**

En este tema, se incluyen las siguientes secciones:

Definir la disponibilidad de la red

La disponibilidad de la red IP de un proveedor de servicios puede considerarse como la accesibilidad entre los puntos de presencia regionales (POP), como se muestra en Figura 27 en la página 761.

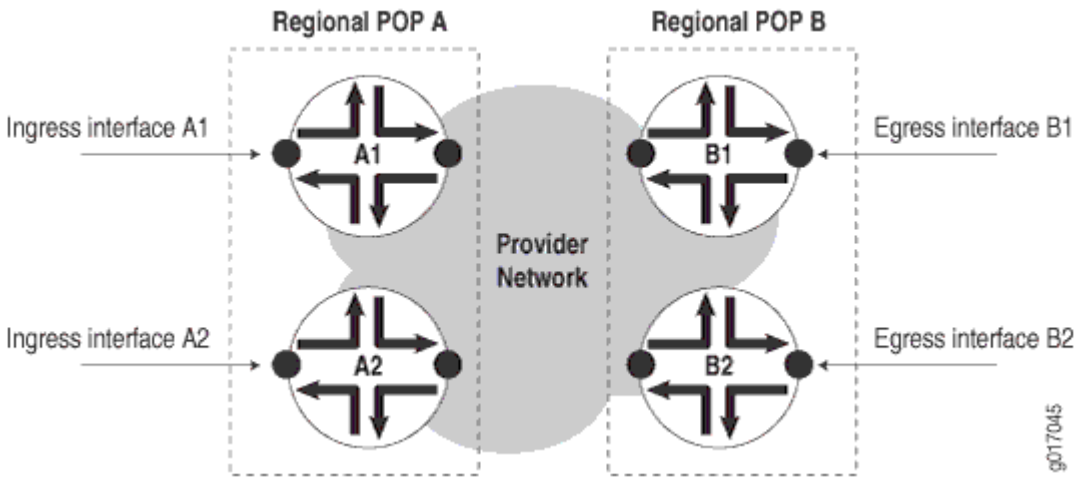
Figura 27: Puntos de presencia regionales



Con el ejemplo anterior, cuando se utiliza una malla completa de puntos de medición, donde cada POP mide la disponibilidad de cada otro POP, se puede calcular la disponibilidad total de la red del proveedor de servicios. Este KPI también se puede usar para ayudar a monitorear el nivel de servicio de la red, y puede ser utilizado por el proveedor de servicios y sus clientes para determinar si están operando dentro de los términos de su acuerdo de nivel de servicio (SLA).

Cuando un POP pueda constar de varios enrutadores, tome medidas en cada enrutador como se muestra en .Figura 28 en la página 762

Figura 28: Mediciones a cada enrutador



Las mediciones incluyen:

- Disponibilidad de ruta: disponibilidad de una interfaz de salida B1 vista desde una interfaz de entrada A1.
- Disponibilidad del enrutador: porcentaje de disponibilidad de rutas de todas las rutas medidas que terminan en el enrutador.
- Disponibilidad de COP: porcentaje de disponibilidad del enrutador entre dos POP regionales, A y B.
- Disponibilidad de red: porcentaje de disponibilidad de POP para todos los POP regionales de la red del proveedor de servicios.

Para medir la disponibilidad de POP de POP A a POP B en , debe medir las cuatro rutas siguientes:Figura 28 en la página 762

```
Path A1 => B1
Path A1 => B2
Path A2 => B1
Path A2 => B2
```

La medición de la disponibilidad de COP B a COP A requeriría otras cuatro mediciones, y así sucesivamente.

Una malla completa de mediciones de disponibilidad puede generar un tráfico de administración significativo. Del diagrama de ejemplo anterior:

- Cada POP tiene dos enrutadores perimetrales de proveedor (PE) coubicados, cada uno con interfaces 2xSTM1, para un total de 18 enrutadores PE y 36xSTM1 interfaces.

- Hay seis enrutadores de proveedor principal (P), cuatro con interfaces 2xSTM4 y 3xSTM1 cada uno, y dos con interfaces 3xSTM4 y 3xSTM1 cada uno.

Esto hace un total de 68 interfaces. Una malla completa de rutas entre cada interfaz es:

[n x (–)] / da [x (–)] / = rutas$_{nl}$ 26868122278

Para reducir el tráfico de administración en la red del proveedor de servicios, en lugar de generar una malla completa de pruebas de disponibilidad de interfaz (por ejemplo, de cada interfaz a cualquier otra interfaz), puede medir a partir de la dirección de circuito cerrado de cada enrutador. Esto reduce el número de mediciones de disponibilidad necesarias a un total de una para cada enrutador o:

[x (–)] / da [x (–)] / = mediciones$_{nn}$ 12242412276

Esto mide la disponibilidad de cada enrutador a todos los demás.

Supervisión del SLA y del ancho de banda necesario

Un SLA típico entre un proveedor de servicios y un cliente podría indicar:

```
A Point of Presence is the connection of two back-to-back provider edge routers to separate core
provider routers using different links for resilience. The system is considered to be
unavailable when either an entire POP becomes unavailable or for the duration of a Priority 1
fault.
```

Una cifra de disponibilidad de SLA del 99,999 por ciento para la red de un proveedor se relacionaría con un tiempo de inactividad de aproximadamente 5 minutos por año. Por lo tanto, para medir esto de manera proactiva, tendría que tomar medidas de disponibilidad con una granularidad de menos de una cada cinco minutos. Con un tamaño estándar de 64 bytes por solicitud de ping ICMP, una prueba de ping por minuto generaría 7680 bytes de tráfico por hora por destino, incluidas las respuestas de ping. Una malla completa de pruebas de ping a 276 destinos generaría 2.119.680 bytes por hora, lo que representa lo siguiente:

- En un vínculo OC3/STM1 de 155,52 Mbps, una utilización del 1,362 por ciento
- En un vínculo OC12/STM4 de 622,08 Mbps, una utilización del 0,340 por ciento

Con un tamaño de 1500 bytes por solicitud de ping ICMP, una prueba de ping por minuto generaría 180.000 bytes por hora por destino, incluidas las respuestas de ping. Una malla completa de pruebas de ping a 276 destinos generaría 49.680.000 bytes por hora, lo que representa lo siguiente:

- En un vínculo OC3/STM1, 31,94 por ciento de utilización
- En un vínculo OC12/STM4, 7,986 por ciento de utilización

Cada enrutador puede registrar los resultados de cada destino probado. Con una prueba por minuto a cada destino, un total de 1 x 60 x 24 x 276 = 397.440 pruebas por día serían realizadas y registradas por cada router. Todos los resultados del ping se almacenan en el (consulte RFC 2925) y pueden ser recuperados por una aplicación de informes de rendimiento SNMP (por ejemplo, software de gestión del rendimiento del servicio de InfoVista, Inc. o Concord Communications, Inc.) para el procesamiento posterior.`pingProbeHistoryTable` Esta tabla tiene un tamaño máximo de 4.294.967.295 filas, que es más que adecuado.

Mida la disponibilidad

Hay dos métodos que puede utilizar para medir la disponibilidad:

- Proactivo: la disponibilidad se mide automáticamente con la mayor frecuencia posible mediante un sistema de soporte operativo.
- Reactivo: la disponibilidad es registrada por un servicio de asistencia cuando un usuario o un sistema de monitoreo de fallas reportan por primera vez una falla.

En esta sección se describe la supervisión del rendimiento en tiempo real como una solución de supervisión proactiva.

Monitoreo de desempeño en tiempo real

Juniper Networks ofrece un servicio de monitoreo de desempeño en tiempo real (RPM) para monitorear el desempeño de la red en tiempo real. Utilice la función de configuración rápida de J-Web para configurar los parámetros de supervisión del rendimiento en tiempo real utilizados en las pruebas de supervisión del rendimiento en tiempo real. (La configuración rápida de J-Web es una GUI basada en navegador que se ejecuta en los enrutadores de Juniper Networks. Para obtener más información, consulte la Guía del usuario de la interfaz J-Web.)

Configuración de la supervisión del rendimiento en tiempo real

Algunas de las opciones más comunes que puede configurar para las pruebas de supervisión del rendimiento en tiempo real se muestran en .Tabla 66 en la página 764

Tabla 66: Opciones de configuración de supervisión del rendimiento en tiempo real

Campo	Description
Solicitar información	

Tabla 66: Opciones de configuración de supervisión del rendimiento en tiempo real *(Continued)*

Campo	Description
`Probe Type`	Tipo de sonda que se va a enviar como parte de la prueba. Los tipos de sondeo pueden ser: • `http-get` • `http-get-metadata` • `icmp-ping` • `icmp-ping-timestamp` • `tcp-ping` • `udp-ping`
`Interval`	Tiempo de espera (en segundos) entre cada transmisión de sonda. El rango es de 1 a 255 segundos.
`Test Interval`	Tiempo de espera (en segundos) entre pruebas. El rango es de 0 a 86400 segundos.
`Probe Count`	Número total de sondas enviadas para cada prueba. El rango es de 1 a 15 sondas.
`Destination Port`	Puerto TCP o UDP al que se envían las sondeos. Utilice el número 7, un número de puerto TCP o UDP estándar, o seleccione un número de puerto del 49152 al 65535.
`DSCP Bits`	Bits de punto de código de servicios diferenciados (DSCP). Este valor debe ser un patrón de 6 bits válido. El valor predeterminado es 000000.
`Data Size`	Tamaño (en bytes) de la parte de datos de las sondas ICMP. El intervalo es de 0 a 65507 bytes.
`Data Fill`	Contenido de la parte de datos de las sondas ICMP. El contenido debe ser un valor hexadecimal. El rango es de 1 a 800h.

Tabla 66: Opciones de configuración de supervisión del rendimiento en tiempo real *(Continued)*

Campo	Description
Umbrales máximos de sonda	
`Successive Lost Probes`	Número total de sondeos que deben perderse sucesivamente para desencadenar un error de sonda y generar un mensaje de registro del sistema. El rango es de 0 a 15 sondas.
`Lost Probes`	Número total de sondeos que deben perderse para desencadenar un error de sonda y generar un mensaje de registro del sistema. El rango es de 0 a 15 sondas.
`Round Trip Time`	Tiempo total de ida y vuelta (en microsegundos) desde el enrutador de servicios hasta el servidor remoto, el cual, si se supera, desencadena un error de sondeo y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Jitter`	Fluctuación total (en microsegundos) de una prueba que, si se supera, desencadena un fallo de la sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Standard Deviation`	Desviación estándar máxima permitida (en microsegundos) para una prueba que, si se supera, desencadena un fallo de la sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Egress Time`	Tiempo unidireccional total (en microsegundos) desde el enrutador hasta el servidor remoto, que, si se supera, desencadena un error de sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Ingress Time`	Tiempo unidireccional total (en microsegundos) desde el servidor remoto hasta el enrutador que, si se supera, desencadena un error de sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Jitter Egress Time`	Fluctuación total en tiempo de salida (en microsegundos) de una prueba que, si se supera, desencadena un error de la sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.

Tabla 66: Opciones de configuración de supervisión del rendimiento en tiempo real *(Continued)*

Campo	Description
`Jitter Ingress Time`	Fluctuación total en tiempo de entrada (en microsegundos) para una prueba que, si se supera, desencadena un error de la sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Egress Standard Deviation`	Desviación estándar máxima permitida de los tiempos de salida (en microsegundos) para una prueba que, si se supera, desencadena un error de sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.
`Ingress Standard Deviation`	Desviación estándar máxima permitida de los tiempos de entrada (en microsegundos) para una prueba que, si se supera, desencadena un error de la sonda y genera un mensaje de registro del sistema. El rango es de 0 a 60,000,000 microsegundos.

Visualización de información de supervisión del rendimiento en tiempo real

Para cada prueba de monitoreo de desempeño en tiempo real configurada en el enrutador, la información de monitoreo incluye el tiempo de ida y vuelta, la fluctuación y la desviación estándar. Para ver esta información, seleccione en la interfaz J-Web o escriba el comando de interfaz de línea de comandos (CLI).`Monitor > RPMshow services rpm`

Para mostrar los resultados de las sondas de monitoreo de rendimiento en tiempo real más recientes, ingrese el comando de la CLI:`show services rpm probe-results`

```
user@host> show services rpm probe-results
Owner: p1, Test: t1
   Target address: 10.8.4.1, Source address: 10.8.4.2, Probe type: icmp-ping
   Destination interface name: lt-0/0/0.0
   Test size: 10 probes
   Probe results:
      Response received, Sun Jul 10 19:07:34 2005
      Rtt: 50302 usec
   Results over current test:
      Probes sent: 2, Probes received: 1, Loss percentage: 50
      Measurement: Round trip time
        Minimum: 50302 usec, Maximum: 50302 usec, Average: 50302 usec,
```

```
        Jitter: 0 usec, Stddev: 0 usec
    Results over all tests:
       Probes sent: 2, Probes received: 1, Loss percentage: 50
       Measurement: Round trip time
        Minimum: 50302 usec, Maximum: 50302 usec, Average: 50302 usec,
        Jitter: 0 usec, Stddev: 0 usec
```

Medir la salud

Puede supervisar las métricas de estado de forma reactiva mediante el uso de software de administración de errores como SMARTS InCharge, Micromuse Netcool Omnibus o Concord Live Exceptions. Le recomendamos que supervise las métricas de estado que se muestran en Tabla 67 en la página 768.

Tabla 67: Métricas de salud

Métricas	Description	Parámetros	
		Nombre	valor
Errores en	Número de paquetes entrantes que contenían errores, lo que impedía que se entregaran	**Nombre MIB**	IF-MIB (RFC 2233)
		Nombre de la variable	ifInErrors
		Variable OID	.1.3.6.1.31.2.2.1.14
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Interfaces lógicas
Errores de salida	Número de paquetes salientes que contenían	**Nombre MIB**	IF-MIB (RFC 2233)

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
	errores, lo que impedía su transmisión	**Nombre de la variable**	ifOutErrors
		Variable OID	.1.3.6.1.31.2.2.1.20
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Interfaces lógicas
Descartes en	Número de paquetes entrantes descartados, aunque no se detectaron errores	**Nombre MIB**	IF-MIB (RFC 2233)
		Nombre de la variable	ifInDiscards
		Variable OID	.1.3.6.1.31.2.2.1.13
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Interfaces lógicas
Protocolos desconocidos	Número de paquetes entrantes descartados porque eran de un protocolo desconocido	**Nombre MIB**	IF-MIB (RFC 2233)
		Nombre de la variable	ifInUnknownProtos

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
		Variable OID	.1.3.6.1.31.2.2.1.15
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Interfaces lógicas
Estado operativo de la interfaz	Estado operativo de una interfaz	**Nombre MIB**	IF-MIB (RFC 2233)
		Nombre de la variable	ifOperStatus
		Variable OID	.1.3.6.1.31.2.2.1.8
		Frecuencia (minutos)	15
		Rango permitido	1 (arriba)
		Objetos administrados	Interfaces lógicas
Estado de ruta conmutada de etiquetas (LSP)	Estado operativo de una ruta de conmutación de etiquetas MPLS	**Nombre MIB**	MPLS-MIB
		Nombre de la variable	mplsLspState
		Variable OID	mplsLspEntry.2

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
		Frecuencia (minutos)	60
		Rango permitido	2 (arriba)
		Objetos administrados	Todas las rutas de conmutación de etiquetas de la red
Estado operativo de los componentes	Estado operativo de un componente de hardware del enrutador	**Nombre MIB**	JUNIPER-MIB
		Nombre de la variable	jnxEstadooperativo
		Variable OID	.1.3.6.1.4.1.2636.1.13.1.6
		Frecuencia (minutos)	60
		Rango permitido	2 (en ejecución) o 3 (listo)
		Objetos administrados	Todos los componentes de cada enrutador de Juniper Networks
Temperatura de funcionamiento de los componentes	Temperatura de funcionamiento de un componente de hardware, en grados Celsius	**Nombre MIB**	JUNIPER-MIB
		Nombre de la variable	jnxOperatingTemp
		Variable OID	.1.3.6.1.4.1.2636.1.13.1.7
		Frecuencia (minutos)	60

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
		Rango permitido	A base
		Objetos administrados	Todos los componentes de un chasis
Tiempo de actividad del sistema	Tiempo, en milisegundos, que el sistema ha estado operativo.	**Nombre MIB**	MIB-2 (RFC 1213)
		Nombre de la variable	Sysuptime
		Variable OID	.1.3.6.1.1.3
		Frecuencia (minutos)	60
		Rango permitido	Solo aumentando (disminución indica un reinicio)
		Objetos administrados	Todos los enrutadores
Sin errores de ruta IP	Número de paquetes que no se pudieron entregar porque no había una ruta IP a su destino.	**Nombre MIB**	MIB-2 (RFC 1213)
		Nombre de la variable	ipOutNoRoutes
		Variable OID	IP.12
		Frecuencia (minutos)	60
		Rango permitido	A base

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
		Objetos administrados	Cada enrutador
Nombres de comunidad SNMP incorrectos	Número de nombres de comunidad SNMP incorrectos recibidos	**Nombre MIB**	MIB-2 (RFC 1213)
		Nombre de la variable	snmpInBadCommunityNames
		Variable OID	SNMP.4
		Frecuencia (minutos)	24
		Rango permitido	A base
		Objetos administrados	Cada enrutador
Infracciones de la comunidad SNMP	Número de comunidades SNMP válidas utilizadas para intentar operaciones no válidas (por ejemplo, intentar realizar solicitudes SNMP Set)	**Nombre MIB**	MIB-2 (RFC 1213)
		Nombre de la variable	snmpInBadCommunityUses
		Variable OID	SNMP.5
		Frecuencia (minutos)	24
		Rango permitido	A base
		Objetos administrados	Cada enrutador

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
Cambio de redundancia	Número total de cambios de redundancia notificados por esta entidad	**Nombre MIB**	JUNIPER-MIB
		Nombre de la variable	jnxRedundancySwitchoverCount
		Variable OID	jnxRedundancyEntry.8
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Todos los enrutadores de Juniper Networks con motores de enrutamiento redundantes
Estado de FRU	Estado operativo de cada unidad reemplazable en el campo (FRU)	**Nombre MIB**	JUNIPER-MIB
		Nombre de la variable	jnxFruState
		Variable OID	jnxFruEntry.8
		Frecuencia (minutos)	15
		Rango permitido	2 a 6 para estados listos/en línea. Consulte jnxFruOfflineReason en caso de que se produzca un error en la FRU.

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
		Objetos administrados	Todas las FRU en todos los enrutadores de Juniper Networks.
Tasa de paquetes caídos de cola	Tasa de paquetes caídos por cola de salida, por clase de reenvío y por interfaz.	**Nombre MIB**	JUNIPER-COS-MIB
		Nombre de la variable	jnxCosIfqTailDropPktRate
		Variable OID	jnxCosIfqStatsEntry.12
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Para cada clase de reenvío por interfaz en la red del proveedor, cuando CoS está habilitado.
Utilización de la interfaz: Octetos recibidos	Número total de octetos recibidos en la interfaz, incluidos los caracteres de trama.	**Nombre MIB**	IF-MIB
		Nombre de la variable	ifInOctets
		Variable OID	.1.3.6.1.2.1.2.2.1.10.x
		Frecuencia (minutos)	60
		Rango permitido	A base

Tabla 67: Métricas de salud *(Continued)*

Métricas	Description	Parámetros	
		Nombre	valor
		Objetos administrados	Todas las interfaces operativas de la red
Utilización de la interfaz: Octetos transmitidos	Número total de octetos transmitidos fuera de la interfaz, incluidos los caracteres de trama.	**Nombre MIB**	IF-MIB
		Nombre de la variable	ifOutOctets
		Variable OID	.1.3.6.1.2.1.2.2.1.16.x
		Frecuencia (minutos)	60
		Rango permitido	A base
		Objetos administrados	Todas las interfaces operativas de la red

NOTA: El recuento de bytes varía según el tipo de interfaz, la encapsulación utilizada y la PIC admitida. Por ejemplo, con la encapsulación vlan-ccc en un PIC 4xFE, GE o GE 1Q, el recuento de bytes incluye la sobrecarga de palabras de encuadre y control. (Consulte Tabla 68 en la página 777.)

Tabla 68: Valores de contador para encapsulación vlan-CCC

Tipo de PIC	Encapsulación	entrada (nivel de unidad)	Resultado (nivel de unidad)	SNMP
4xFE	VLAN-CCC	Fotograma (sin secuencia de comprobación de fotogramas [FCS])	Marco (incluido FCS y palabra de control)	ifInOctets, ifOutOctets
GE	VLAN-CCC	Marco (sin FCS)	Marco (incluido FCS y palabra de control)	ifInOctets, ifOutOctets
GE IQ	VLAN-CCC	Marco (sin FCS)	Marco (incluido FCS y palabra de control)	ifInOctets, ifOutOctets

Las trampas SNMP también son un buen mecanismo para usar en la gestión de la salud. Para obtener más información, consulte "" y "Capturas SNMP específicas de la empresa compatibles con Junos OS"."Capturas SNMP compatibles con Junos OS" en la página 487https://www.juniper.net/documentation/en_US/junos/topics/concept/enterprise-specific-traps-overview.html

Mida el rendimiento

in this section

- Medir la clase de servicio | **781**
- Contadores de filtro de firewall entrantes por clase | **782**
- Supervisar bytes de salida por cola | **784**
- Calcular el tráfico perdido | **785**

El rendimiento de la red de un proveedor de servicios generalmente se define como qué tan bien puede soportar los servicios, y se mide con métricas como el retraso y la utilización. Le sugerimos que supervise las siguientes métricas de rendimiento mediante aplicaciones como InfoVista Service Performance Management o Concord Network Health (consulte Tabla 69 en la página 778).

Tabla 69: Métricas de rendimiento

Métricas:	Retraso medio
Description	Tiempo medio de ida y vuelta (en milisegundos) entre dos puntos de medición.
Nombre MIB	DISMAN-PING-MIB (RFC 2925)
Nombre de la variable	`pingResultsAverageRtt`
Variable OID	pingResultsEntry.6
Frecuencia (minutos)	15 (o dependiendo de la frecuencia de la prueba de ping)
Rango permitido	A base
Objetos administrados	Cada ruta medida en la red
Métricas:	Utilización de la interfaz
Description	Porcentaje de utilización de una conexión lógica.
Nombre MIB	IF-MIB
Nombre de la variable	(&) * 8 `/ifInOctetsifOutOctetsifSpeed`
Variable OID	Entradas ifTable
Frecuencia (minutos)	60
Rango permitido	A base
Objetos administrados	Todas las interfaces operativas de la red

Métricas:	Utilización del disco
Description	Utilización del espacio en disco dentro del enrutador de Juniper Networks
Nombre MIB	HOST-RESOURCES-MIB (RFC 2790)
Nombre de la variable	**hrStorageSize** – **hrStorageUsed**
Variable OID	hrStorageEntry.5 – hrStorageEntry.6
Frecuencia (minutos)	1440
Rango permitido	A base
Objetos administrados	Todos los discos duros del motor de enrutamiento
Métricas:	Utilización de memoria
Description	Utilización de memoria en el motor de enrutamiento y FPC.
Nombre MIB	JUNIPER-MIB (MIB de chasis empresarial de Juniper Networks)
Nombre de la variable	**jnxOperatingHeap**
Variable OID	Tabla para cada componente
Frecuencia (minutos)	60
Rango permitido	A base
Objetos administrados	Todos los enrutadores de Juniper Networks
Métricas:	Carga de CPU

Description	Uso promedio durante el último minuto de una CPU.
Nombre MIB	JUNIPER-MIB (MIB de chasis empresarial de Juniper Networks)
Nombre de la variable	**jnxOperatingCPU**
Variable OID	Tabla para cada componente
Frecuencia (minutos)	60
Rango permitido	A base
Objetos administrados	Todos los enrutadores de Juniper Networks
Métricas:	Utilización de LSP
Description	Utilización de la ruta de conmutación de etiquetas MPLS.
Nombre MIB	MPLS-MIB
Nombre de la variable	**mplsPathBandwidth / (mplsLspOctets * 8)**
Variable OID	mplsLspEntry.21 y mplsLspEntry.3
Frecuencia (minutos)	60
Rango permitido	A base
Objetos administrados	Todas las rutas de conmutación de etiquetas de la red
Métricas:	Tamaño de la cola de salida
Description	Tamaño, en paquetes, de cada cola de salida por clase de reenvío, por interfaz.

Nombre MIB	JUNIPER-COS-MIB
Nombre de la variable	**jnxCosIfqQedPkts**
Variable OID	jnxCosIfqStatsEntry.3
Frecuencia (minutos)	60
Rango permitido	A base
Objetos administrados	Para cada clase de reenvío por interfaz en la red, una vez que CoS esté habilitado.

Esta sección incluye los siguientes temas:

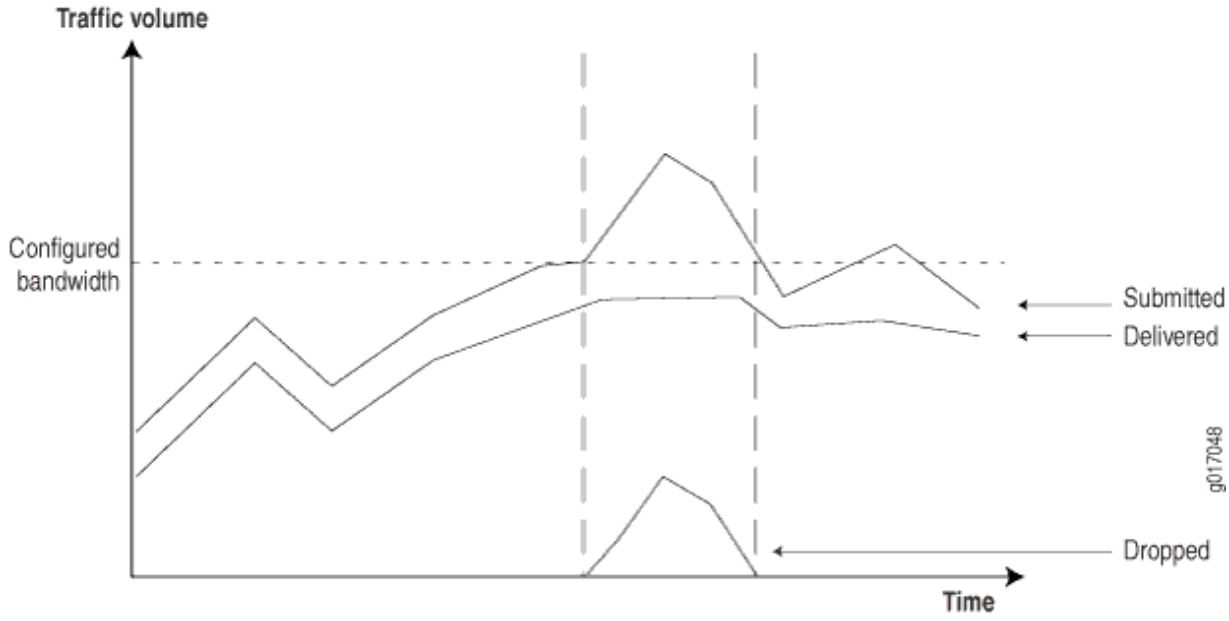
Medir la clase de servicio

Puede usar mecanismos de clase de servicio (CoS) para regular cómo se manejan ciertas clases de paquetes dentro de su red durante los momentos de máxima congestión. Normalmente, debe realizar los pasos siguientes al implementar un mecanismo de CoS:

- Identifique el tipo de paquetes que se aplica a esta clase. Por ejemplo, incluya todo el tráfico del cliente desde una interfaz de borde de entrada específica dentro de una clase, o incluya todos los paquetes de un protocolo determinado, como voz sobre IP (VoIP).
- Identificar el comportamiento determinista requerido para cada clase. Por ejemplo, si VoIP es importante, otorgue al tráfico VoIP la máxima prioridad durante los momentos de congestión de la red. Por el contrario, puede degradar la importancia del tráfico web durante la congestión, ya que puede no afectar demasiado a los clientes.

Con esta información, puede configurar mecanismos en la entrada de red para supervisar, marcar y controlar las clases de tráfico. El tráfico marcado se puede manejar de una manera más determinista en las interfaces de salida, normalmente aplicando diferentes mecanismos de cola para cada clase durante los momentos de congestión de la red. Puede recopilar información de la red para proporcionar a los clientes informes que muestren cómo se comporta la red en tiempos de congestión. (Consulte Figura 29 en la página 782.)

Figura 29: Comportamiento de la red durante la congestión



Para generar estos informes, los enrutadores deben proporcionar la siguiente información:

- Tráfico enviado: cantidad de tráfico recibido por clase.
- Tráfico entregado: cantidad de tráfico transmitido por clase.
- Tráfico perdido: cantidad de tráfico eliminado debido a los límites de CoS.

La siguiente sección describe cómo los enrutadores de Juniper Networks proporcionan esta información.

Contadores de filtro de firewall entrantes por clase

Los contadores de filtros de firewall son un mecanismo muy flexible que puede usar para hacer coincidir y contar el tráfico entrante por clase e interfaz. Por ejemplo:

```
firewall {
    filter f1 {
        term t1 {
            from {
                dscp af11;
            }
            then {
                # Assured forwarding class 1 drop profile 1 count inbound-af11;
                accept;
            }
```

```
        }
    }
}
```

Por ejemplo, muestra los filtros adicionales utilizados para que coincidan con las otras clases.Tabla 70 en la página 783

Tabla 70: Tráfico entrante por clase

Valor DSCP	Condición de coincidencia del firewall	Description
10	af11	Reenvío garantizado clase 1 perfil de caída 1
12	af12	Reenvío garantizado clase 1 perfil de caída 2
18	af21	Mejor esfuerzo clase 2 perfil de caída 1
20	af22	Mejor esfuerzo clase 2 perfil de caída 2
26	af31	Mejor esfuerzo clase 3 perfil de caída 1

Cualquier paquete con un punto de código CoS DiffServ (DSCP) conforme a RFC 2474 se puede contar de esta manera. La MIB del filtro de firewall específico para empresa de Juniper Networks presenta la información del contador en las variables que se muestran en .Tabla 71 en la página 783

Tabla 71: Contadores entrantes

Nombre del indicador	Contadores entrantes
BIA	`jnxFirewalls`
Mesa	`jnxFirewallCounterTable`
Índice	`jnxFWFilter.jnxFWCounter`

Tabla 71: Contadores entrantes *(Continued)*

Nombre del indicador	Contadores entrantes

Variables	`jnxFWCounterPacketCount`
	
	`jnxFWCounterByteCount`

Description	Número de bytes que se cuentan en relación con el contador de filtros de firewall especificado
Versión de SNMP	SNMPv2

Esta información puede ser recopilada por cualquier aplicación de administración SNMP que admita SNMPv2. Los productos de proveedores como Concord Communications, Inc. e InfoVista, Inc., proporcionan compatibilidad con la MIB del firewall de Juniper Networks con sus controladores de dispositivo nativos de Juniper Networks.

Supervisar bytes de salida por cola

Puede usar la MIB CoS ATM empresarial de Juniper Networks para supervisar el tráfico saliente, por clase de reenvío de circuito virtual, por interfaz. (Consulte Tabla 72 en la página 784.)

Tabla 72: Contadores de salida para interfaces de cajeros automáticos

Nombre del indicador	Contadores de salida
BIA	`JUNIPER-ATM-COS-MIB`
Variable	`jnxCosAtmVcQstatsOutBytes`
Índice	`ifIndex.atmVclVpi.atmVclVci.jnxCosFcId`
Description	Número de bytes pertenecientes a la clase de reenvío especificada que se transmitieron en el circuito virtual especificado.
Versión de SNMP	SNMPv2

Los contadores de interfaz que no son ATM son proporcionados por la MIB de CoS específica para la empresa de Juniper Networks, que proporciona la información que se muestra en .Tabla 73 en la página 785

Tabla 73: Contadores de salida para interfaces que no son ATM

Nombre del indicador	Contadores de salida
BIA	`JUNIPER-COS-MIB`
Mesa	`jnxCosIfqStatsTable`
Índice	`jnxCosIfqIfIndex.jnxCosIfqFc`
Variables	`jnxCosIfqTxedBytes` `jnxCosIfqTxedPkts`
Description	Número de bytes o paquetes transmitidos por interfaz por clase de reenvío
Versión de SNMP	SNMPv2

Calcular el tráfico perdido

Puede calcular la cantidad de tráfico perdido restando el tráfico saliente del tráfico entrante:

```
Dropped = Inbound Counter - Outbound Counter
```

También puede seleccionar contadores de la MIB de CoS, como se muestra en .Tabla 74 en la página 785

Tabla 74: Contadores de tráfico caídos

Nombre del indicador	Tráfico perdido
BIA	`JUNIPER-COS-MIB`

Tabla 74: Contadores de tráfico caídos *(Continued)*

Nombre del indicador	Tráfico perdido
Mesa	`jnxCosIfqStatsTable`
Índice	`jnxCosIfqIfIndex.jnxCosIfqFc`
Variables	`jnxCosIfqTailDropPkts` `jnxCosIfqTotalRedDropPkts`
Description	El número de paquetes descartados o descartados en rojo por interfaz por clase de reenvío
Versión de SNMP	SNMPv2

Supervisión de estado con SNMP

in this section

- Información general sobre la supervisión de estado | **786**
- Configurar la supervisión de estado en dispositivos que ejecutan Junos OS | **788**
- Configurar la supervisión de estado | **792**

Información general sobre la supervisión de estado

La supervisión de estado es una función SNMP que amplía la infraestructura de alarma RMON para proporcionar supervisión para un conjunto predefinido de objetos (como el uso del sistema de archivos, el uso de la CPU y el uso de la memoria) y para los procesos de Junos OS.

La característica de supervisión de estado se habilita mediante la instrucción en el nivel de jerarquía.`health-monitor[edit snmp]` También puede configurar parámetros de supervisión de estado, como un umbral descendente, un umbral ascendente y un intervalo. Si el valor de un objeto monitoreado supera el umbral ascendente o descendente, se activa una alarma y se puede registrar un evento.

El umbral descendente es el umbral inferior para la instancia del objeto supervisado. El umbral ascendente es el umbral superior para la instancia de objeto supervisada. Cada umbral se expresa como un porcentaje del valor máximo posible. El intervalo representa el período de tiempo, en segundos, durante el cual se muestrea la instancia del objeto y se compara con los umbrales ascendentes y descendentes.

Los eventos solo se generan cuando se cruza un umbral por primera vez en cualquier dirección, en lugar de después de cada intervalo de muestra. Por ejemplo, si se activa una alarma de umbral ascendente, junto con su evento correspondiente, no se producen más eventos de cruce de umbral hasta que se produce una alarma de caída correspondiente.

Las entradas del registro del sistema para eventos de monitor de estado tienen una etiqueta HEALTHMONITOR correspondiente y no una etiqueta SNMPD_RMON_EVENTLOG genérica. Sin embargo, el monitor de estado envía capturas de RMON genéricos upingThreshold y descendingThreshold. Puede usar el comando operativo para ver información acerca de los registros y las alarmas del monitor de estado.`show snmp health-monitor`

Al configurar el monitor de estado, la información de supervisión para determinadas instancias de objeto está disponible, como se muestra en .Tabla 75 en la página 787

Tabla 75: Instancias de objetos supervisados

Objeto	Description
jnxHrStoragePercentUsed.1	Supervisa el sistema de archivos en el conmutador.**/dev/ad0s1a:** Este es el sistema de archivos raíz montado en /.
jnxHrStoragePercentUsed.2	Supervisa el sistema de archivos en el conmutador.**/dev/ad0s1e:** Este es el sistema de archivos de configuración montado en **./config**
jnxCPU operativa (RE0)	Supervisa el uso de la CPU mediante el motor de enrutamiento (RE0).
jnxOperatingBuffer (RE0)	Supervisa la cantidad de memoria disponible en el motor de enrutamiento (RE0).

Tabla 75: Instancias de objetos supervisados *(Continued)*

Objeto	Description
sysApplElmtRunCPU	Supervisa el uso de la CPU para cada proceso de Junos OS (también denominado demonio). Varias instancias del mismo proceso se supervisan e indexan por separado.
sysApplElmtRunMemory	Supervisa el uso de memoria para cada proceso de Junos OS. Varias instancias del mismo proceso se supervisan e indexan por separado.

SEE ALSO

umbral descendente (Monitor de estado)

intervalo (Monitor de estado)

umbral ascendente (Monitor de estado)

Mostrar monitor de estado SNMP

Configurar la supervisión de estado en dispositivos que ejecutan Junos OS

in this section

- Objetos supervisados | **790**
- Configuración mínima de supervisión de estado | **791**
- Configurar el umbral descendente o ascendente | **791**
- Configurar el intervalo | **792**
- Entradas de registro y capturas | **792**

A medida que crece el número de dispositivos administrados por un sistema de administración de red típico (NMS) y aumenta la complejidad de los propios dispositivos, se vuelve cada vez menos práctico

para el NMS usar sondeos para monitorear los dispositivos. Un enfoque más escalable es confiar en los dispositivos de red para notificar al NMS cuando algo requiere atención.

En los enrutadores de Juniper Networks, las alarmas y los eventos de RMON proporcionan gran parte de la infraestructura necesaria para reducir la sobrecarga de sondeo del NMS. Sin embargo, con este enfoque, debe configurar el NMS para configurar objetos MIB específicos en alarmas RMON. Esto a menudo requiere experiencia específica del dispositivo y personalización de la aplicación de monitoreo. Además, algunas instancias de objetos MIB que necesitan supervisión solo se establecen en la inicialización o cambian en tiempo de ejecución y no se pueden configurar de antemano.

Para solucionar estos problemas, la supervisión de estado amplía la infraestructura de alarma RMON para proporcionar una supervisión predefinida para un conjunto seleccionado de instancias de objeto (para el uso del sistema de archivos, el uso de la CPU y el uso de memoria) e incluye compatibilidad con instancias de objetos desconocidos o dinámicos (como los procesos de Junos OS).

La supervisión del estado está diseñada para minimizar los requisitos de configuración del usuario. Para configurar entradas de supervisión de estado, incluya la instrucción en el nivel de jerarquía:`health-monitor`[`edit snmp`]

```
[edit snmp]
health-monitor {
    falling-threshold percentage;
    interval seconds;
    rising-threshold percentage;
    idp {
        falling-threshold percentage;
        interval seconds;
        rising-threshold percentage;
    }
}
```

La configuración de eventos de supervisión en el nivel jerárquico establece intervalos de sondeo para el estado general del sistema.[`edit snmp health-monitor`] Si establece estas mismas opciones en el nivel de jerarquía, el dispositivo genera un evento SNMP si el porcentaje de memoria del plano de datos utilizado por el sistema de detección y prevención de intrusiones (IDP) se eleva por encima o por debajo de la configuración.[`edit snmp health-monitor idp`]

Puede usar el comando operativo para ver información acerca de los registros y las alarmas del monitor de estado.`show snmp health-monitor`

En este tema se describe la configuración mínima necesaria y se describen las siguientes tareas para configurar el monitor de estado:

Objetos supervisados

Al configurar el monitor de estado, la información de supervisión para determinadas instancias de objeto está disponible, como se muestra en .Tabla 76 en la página 790

Tabla 76: Instancias de objetos supervisados

Objeto	Description
jnxHrStoragePercentUsed.1	Supervisa el siguiente sistema de archivos en el enrutador o conmutador: /dev/ad0s1a: Este es el sistema de archivos raíz montado en /.
jnxHrStoragePercentUsed.2	Supervisa el siguiente sistema de archivos en el enrutador o conmutador: /dev/ad0s1e: Este es el sistema de archivos de configuración montado en ./config
jnxOperatingCPU (RE0)	Supervisa el uso de la CPU en busca de motores de enrutamiento (y).RE0RE1 Los valores de índice asignados a los motores de enrutamiento dependen de si la MIB del chasis utiliza un esquema de indexación basado en cero o en unos. Dado que el esquema de indización es configurable, el índice adecuado se determina cuando se inicializa el enrutador o conmutador y cuando se produce un cambio en la configuración. Si el enrutador o conmutador tiene un solo motor de enrutamiento, la supervisión de entrada de alarma se elimina después de cinco intentos fallidos de obtener el valor de CPU.RE1
jnxOperatingCPU (RE1)	
jnxOperatingBuffer (RE0)	Supervisa la cantidad de memoria disponible en los motores de enrutamiento (y).RE0RE1 Dado que la indización de este objeto es idéntica a la utilizada para , los valores de índice se ajustan en función del esquema de indización utilizado en la MIB del chasis.jnxOperatingCPU Al igual que con , la supervisión de entrada de alarma se elimina si el enrutador o conmutador solo tiene un motor de enrutamiento.jnxOperatingCPURE1
jnxOperatingBuffer (RE1)	
sysApplElmtRunCPU	Supervisa el uso de la CPU para cada proceso de Junos OS (también denominado demonio). Varias instancias del mismo proceso se supervisan e indexan por separado.
sysApplElmtRunMemory	Supervisa el uso de memoria para cada proceso de Junos OS. Varias instancias del mismo proceso se supervisan e indexan por separado.

Configuración mínima de supervisión de estado

Para habilitar la supervisión de estado en el enrutador o conmutador, incluya la instrucción en el nivel de jerarquía:`health-monitor`[`edit snmp`]

```
[edit snmp]
health-monitor;
```

Configurar el umbral descendente o ascendente

El umbral descendente es el umbral inferior (expresado como un porcentaje del valor máximo posible) para la variable monitoreada. Cuando el valor muestreado actual es menor o igual que este umbral y el valor en el último intervalo de muestreo es mayor que este umbral, se genera un solo evento. También se genera un solo evento si la primera muestra después de que esta entrada sea válida es menor o igual que este umbral. Después de generar un evento descendente, no se puede generar otro evento descendente hasta que el valor muestreado se eleve por encima de este umbral y alcance el umbral ascendente. Debe especificar el umbral descendente como un porcentaje del valor máximo posible. El valor predeterminado es porcentaje.`70`

De forma predeterminada, el umbral ascendente es el porcentaje del valor máximo posible para la instancia del objeto supervisado.`80` El umbral ascendente es el umbral superior para la variable monitoreada. Cuando el valor muestreado actual es mayor o igual que este umbral y el valor en el último intervalo de muestreo es menor que este umbral, se genera un solo evento. También se genera un solo evento si la primera muestra después de que esta entrada sea válida es mayor o igual que este umbral. Después de generar un evento ascendente, no se puede generar otro evento ascendente hasta que el valor muestreado caiga por debajo de este umbral y alcance el umbral descendente. Debe especificar el umbral ascendente como un porcentaje del valor máximo posible para la variable supervisada.

Para configurar el umbral descendente o el umbral ascendente, incluya la instrucción o en el nivel jerárquico :`falling-thresholdrising-threshold`[`edit snmp health-monitor`]

```
[edit snmp health-monitor]
falling-threshold percentage;
rising-threshold percentage;
```

puede ser un valor de a .*percentage*`1100`

Los umbrales descendente y ascendente se aplican a todas las instancias de objetos supervisadas por el monitor de estado.

Configurar el intervalo

El intervalo representa el período de tiempo, en segundos, durante el cual se muestrea la instancia del objeto y se compara con los umbrales ascendentes y descendentes.

Para configurar el intervalo, incluya la instrucción y especifique el número de segundos en el nivel de jerarquía:`interval[edit snmp health-monitor]`

```
[edit snmp health-monitor]
interval seconds;
```

puede ser un valor de a .*seconds*`12147483647` El valor predeterminado es segundos (5 minutos).`300`

Entradas de registro y capturas

Las entradas de registro del sistema generadas para cualquier evento de supervisión de estado (umbrales cruzados, errores, etc.) tienen una etiqueta correspondiente en lugar de una etiqueta genérica .`HEALTHMONITORSNMPD_RMON_EVENTLOG` Sin embargo, el monitor de estado envía RMON genérico y capturas.`risingThresholdfallingThreshold`

SEE ALSO

> *monitor de salud*

Configurar la supervisión de estado

En este tema se describe cómo configurar la característica de monitor de estado para dispositivos de la serie QFX.

La función de supervisión de estado amplía la infraestructura de alarma SNMP RMON para proporcionar una supervisión predefinida para un conjunto seleccionado de instancias de objetos (como el uso del sistema de archivos, el uso de la CPU y el uso de memoria) e instancias de objetos dinámicos (como los procesos de Junos OS).

En este procedimiento, el intervalo de muestreo es cada segundo (10 minutos), el umbral descendente es el porcentaje del valor máximo posible para cada instancia de objeto supervisada y el umbral ascendente es el porcentaje del valor máximo posible para cada instancia de objeto supervisada.`6008575`

Para configurar la supervisión de estado:

1. Configure la supervisión de estado:

```
[edit snmp]
user@switch# set health-monitor
```

2. Configure el umbral descendente:

```
[edit snmp]
user@switch# set health-monitor falling-threshold percentage
```

Por ejemplo:

```
user@switch# set health-monitor falling-threshold 85
```

3. Configure el umbral ascendente:

```
[edit snmp]
user@switch# set health-monitor rising-threshold percentage
```

Por ejemplo:

```
user@switch# set health-monitor rising-threshold 75
```

4. Configure el intervalo:

```
[edit snmp]
user@switch# set health-monitor interval seconds
```

Por ejemplo:

```
user@switch# set health-monitor interval 600
```

SEE ALSO

umbral descendente

intervalo (Monitor de estado)

umbral ascendente (Monitor de estado)

5

PART IN COVERPAGE

Opciones de contabilidad

Descripción general de las opciones de contabilidad | 796

Configurar opciones de contabilidad, uso de clase de origen y opciones de uso de clase de destino | 797

Descripción general de las opciones de contabilidad

Un perfil contable representa características comunes de los datos contables recopilados, incluidas las siguientes:

- Intervalo de recogida
- Archivo que contiene datos contables
- Campos específicos y nombres de contador para recopilar estadísticas

Puede configurar varios perfiles de contabilidad, como se describe en Tabla 77 en la página 796.

Tabla 77: Tipos de perfiles contables

Tipo de perfil	Description
Perfil de interfaz	Recopila la información estadística y de errores especificada.
Perfil de filtro	Recopila los recuentos de bytes y paquetes para los nombres de contador especificados en el perfil de filtro.
Perfil MIB	Recopila estadísticas MIB seleccionadas y las registra en un archivo especificado.
Perfil del motor de enrutamiento	Recopila estadísticas seleccionadas del motor de enrutamiento y las registra en un archivo especificado.
Perfil de uso de clase	Recopila estadísticas de uso de clases y las registra en un archivo especificado.

Configurar opciones de contabilidad, uso de clase de origen y opciones de uso de clase de destino

in this section

- Instrucciones de configuración en el nivel jerárquico [edit accounting-options] | 797
- Configuración de opciones de contabilidad | 799
- Configurar archivos de registro de datos contables | 809
- Administrar archivos de contabilidad | 816
- Configurar el perfil de interfaz | 817
- Configurar el perfil de filtro | 821
- Ejemplo: Configurar un perfil de filtro | 823
- Ejemplo: Configurar perfiles de filtro y contadores de firewall específicos de la interfaz | 824
- Configurar perfiles de uso de clase | 826
- Configurar el perfil MIB | 829
- Configurar el perfil del motor de enrutamiento | 832

Instrucciones de configuración en el nivel jerárquico [edit accounting-options]

En este tema se muestran todas las instrucciones de configuración posibles en el nivel de jerarquía y su nivel en la jerarquía de configuración.`[edit accounting-options]` Cuando configure Junos OS, el nivel de jerarquía actual se muestra en el banner de la línea que precede al mensaje.`user@host#`

```
[edit]
accounting-options {
    class-usage-profile profile-name {
        file filename;
        interval minutes;
        destination-classes {
            destination-class-name;
        }
```

```
        source-classes {
            source-class-name;
        }
    }
    file filename {
        archive-sites {
        }
        files number;
        nonpersistent;
        size bytes;
        start-time time;
        transfer-interval minutes;
    }
    filter-profile profile-name {
        counters {
            counter-name;
        }
        file filename;
        interval minutes;
    }
}
interface-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
mib-profile profile-name {
    file filename;
    interval seconds;
    object-names {
        mib-object-name;
    }
    operation operation-name;
}
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
```

```
    interval minutes;
}
```

Configuración de opciones de contabilidad

in this section

- Opciones de contabilidad: configuración completa | 799
- Configuración de las opciones mínimas de contabilidad | 804

Este tema contiene las siguientes secciones:

Opciones de contabilidad: configuración completa

Para configurar las opciones de contabilidad, incluya las siguientes instrucciones en el nivel de jerarquía: `[edit accounting-options]`

```
accounting-options {
    class-usage-profile profile-name {
        file filename;
        interval minutes;
        destination-classes {
            destination-class-name;
        }
        source-classes {
            source-class-name;
        }
        file filename {
            archive-sites {
                site-name;
            }
            files number;
            nonpersistent;
            size bytes;
            source-classes time;
```

```
            transfer-interval minutes;
        }
        filter-profile profile-name {
            counters {
                counter-name;
            }
            file filename;
            interval minutes;
        }
    }
    flat-file-profile profile-name{
        fields {
            all-fields;
            egress-stats {
                all-fields;
                input-bytes;
                input-packets;
                output-bytes;
                output-packets;
                queue-id;
                red-drop-bytes;
                red-drop-packets;
                tail-drop-packets;
                total-drop-packets;
            }
            general-param {
                all-fields;
                accounting-type;
                descr;
                line-id;
                logical-interface;
                nas-port-id;
                physical-interface;
                routing-instance;
                timestamp;
                vlan-id;
            }
            ingress-stats {
                all-fields;
                drop-packets;
                input-bytes;
                input-packets;
                output-bytes;
```

```
                output-packets;
                queue-id;
            }
            l2-stats {
                all-fields;
                input-mcast-bytes;
                input-mcast-packets;
            }
            fields {
                all-fields;
                egress-stats {
                    all-fields;
                    input-bytes;
                    input-packets;
                    output-bytes;
                    output-packets;
                    queue-id;
                    red-drop-bytes;
                    red-drop-packets;
                    tail-drop-packets;
                    total-drop-packets;
                }
                general-param {
                    all-fields;
                    accounting-type;
                    descr;
                    line-id;
                    logical-interface;
                    nas-port-id;
                    physical-interface;
                    routing-instance;
                    timestamp;
                    vlan-id;
                }
                ingress-stats {
                    all-fields;
                    drop-packets;
                    input-bytes;
                    input-packets;
                    output-bytes;
                    output-packets;
                    queue-id;
                }
```

```
general-param {
    all-fields;
    accounting-type;
    descr;
    line-id;
    logical-interface;
    nas-port-id;
    physical-interface;
    routing-instance;
    timestamp;
    vlan-id;
}
ingress-stats {
    all-fields;
    drop-packets;
    input-bytes;
    input-packets;
    output-bytes;
    output-packets;
    queue-id;
}
l2-stats {
    all-fields;
    input-mcast-bytes;
    input-mcast-packets;
}
overall-packet {
    all-fields;
    input-bytes;
    input-discards;
    input-errors;
    input-packets;
    inputv6-bytes;
    inputv6-packets;
    output-bytes;
    output-errors;
    output-packets;
    outputv6-bytes;
    outputv6-packets;
    input-v4-bytes;
    input-v4-packets;
    output-v4-bytes;
    output-v4-packets;
```

```
                    input-bytes-per-sec;
                    input-packets-per-sec;
                }
            }
            file filename;
            format (csv | ipdr)
            interval minutes;
             schema-version schema-name;
        }
        interface-profile profile-name {
            fields {
                field-name;
            }
            file filename;
            interval minutes;
        }
        mib-profile profile-name {
            file filename;
            interval (Accounting Options) seconds;
            object-names {
                mib-object-name;
            }
            operation operation-name;
        }
        routing-engine-profile profile-name {
            fields {
                field-name;
            }
            file filename;
            interval minutes;
        }
    }
}
```

De forma predeterminada, las opciones de contabilidad están deshabilitadas.

NOTA: No configure objetos MIB relacionados con octetos o paquetes de interfaz para un perfil MIB, ya que si lo hace, puede hacer que se agote el tiempo de espera de la caminata SNMP o de un comando show de la CLI.

Configuración de las opciones mínimas de contabilidad

Para habilitar las opciones de contabilidad en el enrutador, debe realizar al menos las siguientes tareas:

- Configure las opciones de contabilidad incluyendo una instrucción y una o más , , , , o instrucciones en el nivel jerárquico:`filesource-class-usagedestination-class-profilefilter-profileinterface-profilemib-profilerouting-engine-profile[edit accounting-options]`

```
[edit]
accounting-options {
    class-usage-profile profile-name {
        file filename;
        interval minutes;
        source-classes {
            source-class-name;
        }
        destination-classes {
            destination-class-name;
        }
        file filename {
            archive-sites {
                site-name;
            }
            files number;
            size bytes;
            transfer-interval minutes;
        }
        filter-profile profile-name {
            counters {
                counter-name;
            }
            file filename;
            interval minutes;
        }
        flat-file-profile profile-name{
            fields {
                all-fields;
                egress-stats {
                    all-fields;
                    input-bytes;
                    input-packets;
                    output-bytes;
```

```
            output-packets;
            queue-id;
            red-drop-bytes;
            red-drop-packets;
            tail-drop-packets;
            total-drop-packets;
        }
        general-param {
            all-fields;
            accounting-type;
            descr;
            line-id;
            logical-interface;
            nas-port-id;
            physical-interface;
            routing-instance;
            timestamp;
            vlan-id;
        }
        ingress-stats {
            all-fields;
            drop-packets;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
        }
        l2-stats {
            all-fields;
            input-mcast-bytes;
            input-mcast-packets;
        }
        overall-packet {
            all-fields;
            input-bytes;
            input-discards;
            input-errors;
            input-packets;
            inputv6-bytes;
            inputv6-packets;
            output-bytes;
            output-errors;
```

```
                output-packets;
                outputv6-bytes;
                outputv6-packets;
                input-v4-bytes;
                input-v4-packets;
                output-v4-bytes;
                output-v4-packets;
                input-bytes-per-sec;
                input-packets-per-sec;
            }
        }
        file filename;
        format (csv | ipdr)
        interval minutes;
         schema-version schema-name;
    }
    flat-file-profile profile-name{
        fields {
            all-fields;
            egress-stats {
                all-fields;
                input-bytes;
                input-packets;
                output-bytes;
                output-packets;
                queue-id;
                red-drop-bytes;
                red-drop-packets;
                tail-drop-packets;
                total-drop-packets;
            }
            general-param {
                all-fields;
                accounting-type;
                descr;
                line-id;
                logical-interface;
                nas-port-id;
                physical-interface;
                routing-instance;
                timestamp;
                vlan-id;
            }
```

```
            ingress-stats {
                all-fields;
                drop-packets;
                input-bytes;
                input-packets;
                output-bytes;
                output-packets;
                queue-id;
            }
            l2-stats {
                all-fields;
                input-mcast-bytes;
                input-mcast-packets;
            }
            overall-packet {
                all-fields;
                input-bytes;
                input-discards;
                input-errors;
                input-packets;
                inputv6-bytes;
                inputv6-packets;
                output-bytes;
                output-errors;
                output-packets;
                outputv6-bytes;
                outputv6-packets;
                input-v4-bytes;
                input-v4-packets;
                output-v4-bytes;
                output-v4-packets;
                input-bytes-per-sec;
                input-packets-per-sec;
            }
        }
        file filename;
        format (csv | ipdr)
        interval minutes;
         schema-version schema-name;
    }
    interface-profile profile-name {
        fields {
            field-name;
```

```
            }
            file filename;
            interval minutes;
        }
        mib-profile profile-name {
            file filename;
            interval minutes;
            object-names {
                mib-object-name;
            }
            operation operation-name;
        }
        routing-engine-profile profile-name {
            fields {
                field-name;
            }
            file filename;
            interval minutes;
        }
    }
}
```

- Aplique los perfiles a las interfaces o filtros elegidos.

  Aplique un perfil de interfaz a una interfaz física o lógica incluyendo la instrucción en el nivel jerárquico o en el nivel jerárquico.`accounting-profile`[`edit interfaces` *`interface-name`*][`edit interfaces` *`interface-name`* `unit` *`logical-unit-number`*]

```
[edit interfaces]
interface-name {
    accounting-profile profile-name;
    unit logical-unit-number {
        accounting-profile profile-name;
    }
}
```

> **NOTA**: No se aplican perfiles de clase de destino a las interfaces. Aunque la interfaz debe tener configurada la instrucción, el perfil de clase de destino busca automáticamente todas las interfaces con la clase de destino configurada.`destination-class-usage`

Aplique un perfil de filtro a un filtro de firewall incluyendo la instrucción en el nivel de jerarquía:`accounting-profile`[`edit firewall filter` *`filter-name`*]

```
[edit firewall]
filter filter-name {
    accounting-profile profile-name;
}
```

No es necesario aplicar el perfil del motor de enrutamiento a una interfaz porque las estadísticas se recopilan en el propio motor de enrutamiento.

Configurar archivos de registro de datos contables

in this section

- Configurar cuánto tiempo se conservan los archivos de copia de seguridad | **810**
- Configurar el tamaño máximo del archivo | **811**
- Configurar sitios de almacenamiento para los archivos | **811**
- Configurar copia de seguridad local para archivos de contabilidad | **812**
- Configurar archivos para que se compriman | **813**
- Configurar el número máximo de archivos | **813**
- Configurar la ubicación de almacenamiento del archivo | **813**
- Configurar archivos para guardarlos después de un cambio en el rol principal | **814**
- Configurar la hora de inicio para la transferencia de archivos | **814**
- Configurar el intervalo de transferencia del archivo | **815**

Un perfil de contabilidad especifica qué estadísticas recopilar y escribir en un archivo de registro. Para configurar un archivo de registro de datos de contabilidad, incluya la instrucción en el nivel de jerarquía:`file`[`edit accounting-options`]

```
[edit accounting-options]
cleanup-interval {
    interval days;
```

```
}
file filename {
    archive-sites {
        site-name;
    }
    backup-on-failure  (master-and-slave | master-only);
    files number;
    nonpersistent;
    push-backup-to-master;
    size bytes;
    start-time time;
    transfer-interval minutes;
}
```

donde es el nombre del archivo en el que se van a escribir los datos contables.*filename*

Si el nombre de archivo contiene espacios, escríbalo entre comillas (" "). El nombre de archivo no puede contener una barra diagonal ().`/` El archivo se crea en el directorio y puede contener datos de varios perfiles.`/var/log`

Todos los archivos de registro de datos contables incluyen secciones de encabezado y remolque que comienzan con una en la primera columna.`#` El encabezado contiene la hora de creación del archivo, el nombre de host y las columnas que aparecen en el archivo. El tráiler contiene la hora a la que se cerró el archivo.

Siempre que cambie algún valor configurado que afecte a las columnas de un archivo, el archivo crea un nuevo registro de diseño de perfil que contiene una nueva lista de columnas.

Debe configurar el tamaño del archivo; Todas las demás propiedades son opcionales.

Configurar cuánto tiempo se conservan los archivos de copia de seguridad

Puede configurar cuántos días se conservan los archivos en el directorio local antes de eliminarlos.

> **NOTA**: Los archivos guardados en el directorio siempre se comprimen para conservar el almacenamiento local, independientemente de si la instrucción está configurada.**/var/log/pfedBackup**`compress`

Para configurar la retención de archivos de copia de seguridad:

- Especifique el número de días.

```
[edit accounting-options]
user@host# set cleanup-interval interval days
```

NOTA: Los archivos se conservan durante 1 día si no configura esta opción.

Este valor, configurado o predeterminado, se aplica a todos los archivos configurados en el nivel jerárquico .`[edit accounting-options file]`

Configurar el tamaño máximo del archivo

Para configurar el tamaño máximo del archivo:

- Especifique el tamaño.

```
[edit accounting-options file filename]
size bytes;
```

La instrucción es el tamaño máximo del archivo de registro, en bytes, kilobytes (KB), megabytes (MB) o gigabytes (GB).`size` El valor mínimo para es 256 KB.*bytes* Debe configurar ; los atributos restantes son opcionales.*bytes*

Configurar sitios de almacenamiento para los archivos

Después de que un archivo alcanza su tamaño máximo o se supera el tiempo, el archivo se cierra, se le cambia el nombre y, si configuró un sitio de archivado, se transfiere a un host remoto.`transfer-interval`

Para configurar los sitios donde se archivan los archivos:

- Especifique uno o varios nombres de sitio.

```
[edit accounting-options file filename]
user@host# set archive-sites site-name
```

donde es cualquier URL FTP válida.*site-name* Para obtener más información acerca de cómo especificar URL FTP válidas, consulte la Biblioteca de administración de Junos OS.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/index.html Puede especificar más de una URL, en cualquier orden. Cuando se archiva un archivo, el enrutador o conmutador intenta transferir el archivo a la primera URL de la lista, probando el siguiente sitio de la lista

sólo si la transferencia no se realiza correctamente. El archivo de registro se almacena en el sitio de archivado con un nombre de archivo con el formato *.router-name_log-filename_timestamp* Cuando se configura el archivado de archivos mediante una instrucción, la utilidad de transferencia de archivos utiliza la instancia de enrutamiento predeterminada para conectarse al servidor de destino.`archive-states` Si la instancia de enrutamiento predeterminada no puede conectarse al servidor de destino, la utilidad de transferencia de archivos no funciona.

A partir de Junos OS 18.4R1, cuando se configura el archivado de archivos mediante la instrucción, la utilidad de transferencia de archivos no funciona si ha habilitado la instancia de administración.`archive-sites`

Configurar copia de seguridad local para archivos de contabilidad

Puede configurar el enrutador para guardar una copia del archivo de contabilidad localmente cuando falle la transferencia normal de los archivos al sitio de archivado. El archivo se guarda en el directorio del motor de enrutamiento correspondiente.**/var/log/pfedBackup** Debe especificar si solo se guardan los archivos del motor de enrutamiento principal o si los archivos se guardan tanto del motor de enrutamiento principal como del motor de enrutamiento de copia de seguridad (cliente).

> **NOTA**: Los archivos guardados en el directorio siempre se comprimen para conservar el almacenamiento local, independientemente de si la instrucción está configurada.**/var/log/pfedBackup**`compress`

Para configurar la copia de seguridad local en caso de error:

- Especifique la copia de seguridad local y qué archivos se guardan.

```
[edit accounting-options file filename]
user@host# set backup-on-failure  (master-and-slave | master-only)
```

Al deshabilitar esta característica, se eliminan los archivos de contabilidad de los que se ha realizado una copia de seguridad del directorio.

> **NOTA**: Cuando no se configura esta opción, el archivo se guarda en caso de error en el directorio local especificado como el último sitio de la lista de sitios de archivo.

Configurar archivos para que se compriman

De forma predeterminada, los archivos de contabilidad se transfieren en un formato sin comprimir. Para conservar los recursos durante la transmisión y en el sitio de archivo, puede configurar la compresión de los archivos.

> **NOTA**: Los archivos guardados en el directorio siempre se comprimen para conservar el almacenamiento local, independientemente de si la instrucción está configurada.**/var/log/pfedBackup**`compress`

Para configurar el enrutador para comprimir los archivos de contabilidad cuando se transfieren:

- Especifique la compresión.

```
[edit accounting-options file filename]
user@host# set compress
```

Configurar el número máximo de archivos

Para configurar el número máximo de archivos:

- Especifique el número.

```
[edit accounting-options file filename]
user@host# set files number
```

Cuando un archivo de registro alcanza su tamaño máximo, se le cambia el nombre , luego , y así sucesivamente, hasta que se alcanza el número máximo de archivos de registro.*filename*`.0`*filename*`.1` A continuación, se sobrescribe el archivo de registro más antiguo. El valor mínimo para es 3 y el valor predeterminado es 10.*number*

Configurar la ubicación de almacenamiento del archivo

En los enrutadores de servicios de la serie J, los archivos se almacenan de forma predeterminada en la unidad flash compacta. Como alternativa, puede configurar los archivos para que se almacenen en el directorio (en DRAM) en lugar del directorio (en la unidad flash compacta).**mfs/var/log**`cf/var/log`

Para configurar la ubicación de almacenamiento en DRAM:

- Especifique el almacenamiento no persistente.

```
[edit accounting-options file filename]
user@host# set nonpersistent
```

Esta función es útil para minimizar el tráfico de lectura/escritura en la unidad flash compacta del router.

NOTA: Si los archivos de registro para los datos de contabilidad se almacenan en DRAM, estos archivos se pierden al reiniciar el enrutador. Le recomendamos que realice copias de seguridad de estos archivos periódicamente.

Configurar archivos para guardarlos después de un cambio en el rol principal

Puede configurar el enrutador para guardar los archivos de contabilidad del nuevo motor de enrutamiento de copia de seguridad al nuevo motor de enrutamiento principal cuando se produzca un cambio en el rol principal. Los archivos se almacenan en el directorio del enrutador.**/var/log/pfedBackup** El motor de enrutamiento principal incluye estos archivos de contabilidad con sus propios archivos de contabilidad actuales cuando transfiere los archivos del directorio de copia de seguridad al sitio de archivado en el siguiente intervalo de transferencia. Configure esta opción cuando el nuevo motor de enrutamiento de copia de seguridad no pueda conectarse al sitio de archivo; Por ejemplo, cuando el sitio no está conectado por medio de una interfaz fuera de banda o la ruta al sitio se enruta a través de una tarjeta de línea.

Para configurar los archivos del motor de enrutamiento de copia de seguridad que se guardarán cuando cambie el rol principal:

- Especifique la copia de seguridad.

```
[edit accounting-options file filename]
user@host# set push-backup-to-master
```

NOTA: Los archivos del motor de enrutamiento de copia de seguridad en el motor de enrutamiento principal se envían en cada intervalo, aunque los archivos sigan siendo los mismos. Si esto es más actividad de la que desea, considere usar la instrucción en su lugar.`backup-on-failure master-and-slave`

Configurar la hora de inicio para la transferencia de archivos

Para configurar la hora de inicio de la transferencia de archivos:

- Especifique la hora.

```
[edit accounting-options file filename]
user@host# set start-time YYYY-MM-DD.hh:mm
```

Por ejemplo, las 10:00 a.m. del 30 de enero de 2007 se representan como `.2007-01-30.10:00`

Configurar el intervalo de transferencia del archivo

Para configurar el intervalo en el que se transfieren los archivos:

- Especifique el intervalo.

```
[edit accounting-options file filename]
user@host# set transfer-interval minutes
```

El rango para es de 5 a 2880 minutos.`transfer-interval` El valor predeterminado es de 30 minutos.

CONSEJO: Junos OS guarda el archivo de registro existente y crea uno nuevo en los intervalos de transferencia configurados, independientemente de si:

- El archivo ha alcanzado el tamaño máximo.
- Se configura un sitio de archivado.

Cuando tiene configurado un intervalo de transferencia relativamente pequeño y no se configura ningún sitio de archivado, se pueden perder datos, ya que Junos OS sobrescribe los archivos de registro cuando se alcanza el número máximo de archivos de registro. Para garantizar que la información de registro se guarde durante un tiempo razonablemente largo:

- Configure un sitio de archivado para archivar los archivos de registro cada vez que se cree un nuevo archivo de registro.
- Configure el valor máximo (2880 minutos) para que los archivos nuevos se creen con menos frecuencia; es decir, solo cuando el archivo supere el límite de tamaño máximo o una vez cada 2 días.`transfer-interval`

Administrar archivos de contabilidad

Si configura dispositivos SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200 y SRX4600 para capturar datos de contabilidad en archivos de registro, establezca la ubicación de los archivos de contabilidad en la DRAM.

La ubicación predeterminada para los archivos de contabilidad es el directorio de la tarjeta CompactFlash (CF).`cfs/var/log` La opción minimiza el tráfico de lectura/escritura a su tarjeta CF. `nonpersistent` Le recomendamos que utilice la opción para todos los archivos de contabilidad configurados en su sistema.`nonpersistent`

Para almacenar archivos de registro de contabilidad en DRAM en lugar de la tarjeta CF:

1. Ingrese al modo de configuración en la CLI.
2. Cree un archivo de registro de datos contables en DRAM y reemplácelo por el nombre del archivo.*filename*

```
[edit]
user@host# edit accounting-options file filename
```

3. Almacene los archivos de registro de contabilidad en el archivo DRAM.

```
[edit]
user@host# set file filename nonpersistent
```

PRECAUCIÓN: Si los archivos de registro de datos de contabilidad se almacenan en DRAM, estos archivos se pierden cuando se reinicia el dispositivo. Por lo tanto, le recomendamos que realice copias de seguridad de estos archivos periódicamente.

NOTA: La opción CLI no se admite en SRX5000 línea.`nonpersistent`

Configurar el perfil de interfaz

in this section

- Configurar campos | 818
- Configurar la información de archivo | 818
- Configurar estadísticas borradas para que se notifiquen en el archivo sin formato | 818
- Configurar el intervalo | 819
- Ejemplo: Configurar el perfil de interfaz | 819

Un perfil de interfaz especifica la información recopilada y escrita en un archivo de registro. Puede configurar un perfil para recopilar información estadística y de errores para paquetes de entrada y salida en una interfaz física o lógica determinada.

Para configurar un perfil de interfaz, incluya la instrucción en el nivel de jerarquía:`interface-profile[edit accounting-options]`

```
[edit accounting-options]
interface-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

De forma predeterminada, el motor de reenvío de paquetes (PFE) recopila periódicamente las estadísticas de todas las interfaces. Para mejorar el rendimiento, puede deshabilitar opcionalmente la actualización periódica incluyendo la instrucción en el nivel de jerarquía.`periodic-refresh disable[edit accounting-options]`

Cada perfil contable debe tener un archivo .*`profile-name`* Para aplicar un perfil a una interfaz física o lógica, incluya la instrucción en el nivel jerárquico o en el nivel jerárquico.`accounting-profile[edit interfaces interface-name][edit interfaces interface-name unit logical-unit-number]` También puede aplicar un perfil de contabilidad en el nivel jerárquico .`[edit firewall family family-type filter filter-name]` Para obtener más información, consulte la Guía del usuario de políticas de enrutamiento, filtros de firewall y políticas de tráfico.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.html

Para configurar un perfil de interfaz, realice las tareas descritas en las secciones siguientes:

Configurar campos

Un perfil de interfaz debe especificar qué estadísticas se recopilan. Para configurar qué estadísticas deben recopilarse para una interfaz, incluya la instrucción en el nivel de jerarquía:`fields`[`edit accounting-options interface-profile` *`profile-name`*]

```
[edit accounting-options interface-profile profile-name]
fields {
    field-name;
}
```

Configurar la información de archivo

Cada perfil de contabilidad registra sus estadísticas en un archivo del directorio.**/var/log**

Para configurar el archivo que se va a usar, incluya la instrucción en el nivel de jerarquía:`file`[`edit accounting-options interface-profile` *`profile-name`*]

```
[edit accounting-options interface-profile profile-name]
file filename;
```

Debe especificar una instrucción para el perfil de interfaz que ya se haya configurado en el nivel de jerarquía.`file`[`edit accounting-options`]

Configurar estadísticas borradas para que se notifiquen en el archivo sin formato

Cuando se ejecuta el comando para una interfaz lógica configurada para recopilar estadísticas contables, se borran todas las estadísticas contables recibidas en esa interfaz desde el motor de reenvío de paquetes.`clear interfaces statistics` Los valores actuales cuando se emite el comando se convierten en la nueva línea base y los contadores de estadísticas se restablecen a cero. Los nuevos valores, empezando desde cero, se muestran en la CLI. Sin embargo, no se informan de esa manera en el archivo plano de contabilidad asociado con la interfaz. En su lugar, los valores indicados en el archivo siguen incrementándose como si no se hubiera emitido el comando.

Puede cambiar este resultado incluyendo la instrucción en el perfil de interfaz.`allow-clear` En este caso, cuando se ejecuta el comando, las estadísticas se restablecen a cero y se notifican al archivo plano.`clear interfaces statistics`

Para configurar los informes de estadísticas contables compensadas en el archivo plano, especifique los informes:

```
[edit accounting-options interface-profile profile-name]
 allow-clear;
```

Configurar el intervalo

Cada interfaz con un perfil de contabilidad habilitado tiene estadísticas recopiladas una vez por intervalo de tiempo especificado para el perfil de contabilidad. El tiempo de recopilación de estadísticas se programa de manera uniforme durante el intervalo configurado. Para configurar el intervalo, incluya la instrucción en el nivel de jerarquía:`interval`[`edit accounting-options interface-profile` *`profile-name`*]

```
[edit accounting-options interface-profile profile-name]
interval minutes;
```

> **NOTA**: El intervalo mínimo permitido es de 1 minuto. La configuración de un intervalo bajo en un perfil de contabilidad para un gran número de interfaces puede provocar una grave degradación del rendimiento.

El intervalo de la instrucción es de 1 a 2880 minutos.`interval` El valor predeterminado es de 30 minutos.

Ejemplo: Configurar el perfil de interfaz

Configure el perfil de interfaz:

```
[edit]
accounting-options {
    file if_stats {
        size 40 files 5;
    }
    interface-profile if_profile1 {
        file if_stats;
        interval 30;
        fields {
            input-bytes;
            output-bytes;
            input-packets;
            output-packets;
```

```
            input-multicast;
            output-multicast;
        }
    }
    interface-profile if_profile2 {
        file if_stats;
        interval 30;
        fields {
            input-bytes;
            output-bytes;
            input-packets;
            output-packets;
            input-multicast;
            output-multicast;
        }
    }
    interfaces {
        xe-1/0/0 {
            accounting-profile if_profile1;
            unit 0 {
                accounting-profile if_profile2;
                ...
            }
        }
    }
}
```

Los dos perfiles de interfaz, if-profile1 y if-profile2, escriben datos en el mismo archivo, if-stats. El archivo if-stats podría ser similar al siguiente:

```
#FILE CREATED 976823478 2000-12-14-19:51:18
#hostname host
#profile-layout if_profile2,epoch-timestamp,interface-name,snmp-index,input-bytes,output-bytes,
input-packets,output-packets,input-multicast,output-multicast
#profile-layout if_profile1,epoch-timestamp,interface-name,snmp-index,input-bytes,output-bytes,
input-packets
if_profile2,976823538,xe-1/0/0.0,8,134696815,3681534,501088,40723,0,0
if_profile1,976823538,xe-1/0/0,7,134696815,3681534,501088
...
#FILE CLOSED 976824378 2000-12-14-20:06:18
```

Configurar el perfil de filtro

in this section

- Configurar los contadores | 821
- Configurar la información de archivo | 822
- Configurar el intervalo | 822

Un perfil de filtro especifica información de errores y estadísticas recopilada y escrita en un archivo. Un perfil de filtro debe especificar nombres de contador para los que se recopilan estadísticas.

Para configurar un perfil de filtro, incluya la instrucción en el nivel de jerarquía:`filter-profile`[`edit accounting-options`]

```
[edit accounting-options]
filter-profile profile-name {
    counters {
        counter-name;
    }
    file filename;
    interval minutes;
}
```

Para aplicar el perfil de filtro, incluya la instrucción en el nivel de jerarquía.`accounting-profile`[`edit firewall filter filter-name`]

Para configurar un perfil de filtro, realice las tareas descritas en las secciones siguientes:

Configurar los contadores

Se recopilan estadísticas para todos los contadores especificados en el perfil de filtro. Para configurar los contadores, incluya la instrucción en el nivel de jerarquía:`counters`[`edit accounting-options filter-profile profile-name`]

```
[edit accounting-options filter-profile profile-name]
counters {
}
```

Configurar la información de archivo

Cada perfil de contabilidad registra sus estadísticas en un archivo del directorio./var/log

Para configurar el archivo que se va a usar, incluya la instrucción en el nivel de jerarquía:file[edit accounting-options filter-profile *profile-name*]

```
[edit accounting-options filter-profile profile-name]
file filename;
```

Debe especificar un nombre de archivo para el perfil de filtro que ya se haya configurado en el nivel de jerarquía.[edit accounting-options]

NOTA: El límite del número total de caracteres por línea en un archivo de registro es igual a 1023. Si se supera este límite, el resultado escrito en el archivo de registro está incompleto. Asegúrese de limitar el número de contadores o datos solicitados para que no se supere este límite de caracteres.

NOTA: Si se supera el tamaño de archivo configurado o el intervalo de transferencia, Junos OS cierra el archivo e inicia uno nuevo. De forma predeterminada, el valor del intervalo de transferencia es de 30 minutos. Si el intervalo de transferencia no está configurado, Junos OS cierra el archivo e inicia uno nuevo cuando el tamaño del archivo supere su valor configurado o el valor predeterminado del intervalo de transferencia supere los 30 minutos. Para evitar transferir archivos cada 30 minutos, especifique un valor diferente para el intervalo de transferencia.

Configurar el intervalo

Cada filtro con un perfil de contabilidad habilitado tiene estadísticas recopiladas una vez por intervalo de tiempo especificado para el perfil de contabilidad. El tiempo de recopilación de estadísticas se programa de manera uniforme durante el intervalo configurado. Para configurar el intervalo, incluya la instrucción en el nivel de jerarquía:interval[edit accounting-options filter-profile *profile-name*]

```
[edit accounting-options filter-profile profile-name]
interval;
```

> **NOTA**: El intervalo mínimo permitido es de 1 minuto. La configuración de un intervalo bajo en un perfil de contabilidad para un gran número de filtros puede provocar una grave degradación del rendimiento.

El intervalo de la instrucción es de 1 a 2880 minutos.`interval` El valor predeterminado es de 30 minutos.

Ejemplo: Configurar un perfil de filtro

Configure un perfil de filtro:

```
[edit]
accounting-options {
    file fw_accounting {
        size 500k files 4;
    }
    filter-profile fw_profile1 {
        file fw_accounting;
        interval 60;
        counters {
            counter1;
            counter2;
            counter3;
        }
    }
}
firewall {
    filter myfilter {
        accounting-profile fw_profile1;
        ...
        term accept-all {
            then {
                count counter1;
                accept;
            }
        }
    }
}
```

El perfil de filtro, , escribe datos en el archivo .`fw-profile1fw_accounting` El archivo podría tener el siguiente aspecto:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#hostname host
#profile-layout fw_profile1,epoch-timestamp,filter-name,counter-name,packet-count,byte-count
fw_profile1,976826058,myfilter,counter1,163,10764
...
#FILE CLOSED 976826178 2000-12-14-20:36:18
```

Ejemplo: Configurar perfiles de filtro y contadores de firewall específicos de la interfaz

Para recopilar y registrar estadísticas de recuento recopiladas por filtros de firewall por interfaz, debe configurar un perfil de filtro e incluir la instrucción específica de la interfaz en el nivel de jerarquía.[`edit firewall filter` *`filter-name`*]

Configure el perfil de contabilidad del filtro del firewall:

```
[edit accounting-options]
file cust1_accounting {
    size 500k;
}
filter-profile cust1_profile {
    file cust1_accounting;
    interval 1;
    counters {
        r1;
    }
}
```

Configure el contador de firewall específico de la interfaz:

```
[edit firewall]
filter f3 {
    accounting-profile cust1_profile;
    interface-specific;
    term f3-term {
```

```
        then {
            count r1;
            accept;
        }
    }
}
```

Aplique el filtro de firewall a una interfaz:

```
[edit interfaces]
xe-1/0/0 {
    unit 0 {
        family inet {
            filter {
                input f3;
                output f3;
            }
            address 20.20.20.30/24;
        }
    }
}
```

En el ejemplo siguiente se muestra el contenido del archivo de la carpeta que podría resultar de la configuración anterior:`cust1_accounting/var/log`

```
#FILE CREATED 995495212 2001-07-18-22:26:52
#hostname host
#profile-layout cust1_profile,epoch-timestamp,interfaces,filter-name,
counter-name,packet-count,byte-count
cust1_profile,995495572,xe-1/0/0.0,f3-xe-1/0/0.0-i,r1-xe-1/0/0.0-i,5953,1008257
cust1_profile,995495602,xe-1/0/0.0,f3-xe-1/0/0.0-o,r1-xe-1/0/0.0-o,5929,1006481
...
```

Si la instrucción no se incluye en la configuración, puede producirse el resultado siguiente:`interface-specific`

```
#FILE CREATED 995495212 2001-07-18-22:26:52
#hostname host
#profile-layout cust1_profile,epoch-timestamp,interfaces,filter-name,
counter-name,packet-count,byte-count
```

```
cust1_profile,995495572,xe-1/0/0.0,f3,r1,5953,1008257
cust1_profile,995495632,xe-1/0/0.0,f3,r1,5929,1006481
```

Configurar perfiles de uso de clase

in this section

- Configurar un perfil de uso de clase | 826
- Configurar la información de archivo | 827
- Configurar el intervalo | 827
- Crear un perfil de uso de clase para recopilar estadísticas de uso de clase de origen | 827
- Crear un perfil de uso de clase para recopilar estadísticas de uso de clase de destino | 828

Para recopilar estadísticas de uso de clases, realice las tareas descritas en estas secciones:

Configurar un perfil de uso de clase

Puede configurar el perfil de uso de la clase para recopilar estadísticas para determinadas clases de origen y destino.

Para configurar el perfil de uso de clase para filtrar por clases de origen, incluya la instrucción en el nivel de jerarquía:`source-classes`[`edit accounting-options class-usage-profile` *`profile-name`*]

```
[edit accounting-options class-usage-profile profile-name]
source-classes {
    source-class-name;
}
```

Para configurar el perfil de uso de clase para filtrar por clases de destino, incluya la instrucción en el nivel de jerarquía:`destination-classes`[`edit accounting-options class-usage-profile` *`profile-name`*]

```
[edit accounting-options class-usage-profile profile-name]
destination-classes {
```

```
    destination-class-name;
}
```

Configurar la información de archivo

Cada perfil de contabilidad registra sus estadísticas en un archivo del directorio.`/var/log`

Para especificar el archivo que se va a usar, incluya la instrucción en el nivel de jerarquía:`file`[`edit accounting-options class-usage-profile` *`profile-name`*]

```
[edit accounting-options class-usage-profile profile-name]
file filename;
```

Debe especificar un nombre de archivo para el perfil de uso de la clase de origen que ya se haya configurado en el nivel de jerarquía.[`edit accounting-options`] También puede especificar un nombre de archivo para el perfil de uso de la clase de destino configurado en el nivel jerárquico .[`edit accounting-options`]

Configurar el intervalo

Cada interfaz con un perfil de uso de clase habilitado tiene estadísticas recopiladas una vez por intervalo especificado para el perfil de contabilidad. El tiempo de recopilación de estadísticas se programa de manera uniforme durante el intervalo configurado. Para configurar el intervalo, incluya la instrucción en el nivel de jerarquía:`interval`[`edit accounting-options class-usage-profile` *`profile-name`*]

```
[edit accounting-options class-usage-profile profile-name]
interval;
```

Crear un perfil de uso de clase para recopilar estadísticas de uso de clase de origen

Para crear un perfil de uso de clase para recopilar estadísticas de uso de clases de origen:

```
[edit]
accounting-options {
    class-usage-profile scu-profile1;
    file usage-stats;
    interval 15;
    source-classes {
        gold;
        silver;
        bronze;
```

```
    }
}
```

El perfil de uso de la clase, , escribe datos en el archivo .scu-profile1usage_stats El archivo podría tener el siguiente aspecto:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, scu_profile,epoch-timestamp,interface-name,source-class,
packet-count,byte-count
scu_profile,980313078,xe-1/0/0.0,gold,82,6888
scu_profile,980313078,xe-1/0/0.0,silver,164,13776
scu_profile,980313078,xe-1/0/0.0,bronze,0,0
scu_profile,980313678,xe-1/0/0.0,gold,82,6888
scu_profile,980313678,xe-1/0/0.0,silver,246,20664
scu_profile,980313678,xe-1/0/0.0,bronze,0,0
```

Crear un perfil de uso de clase para recopilar estadísticas de uso de clase de destino

Para crear un perfil de uso de clase para recopilar estadísticas de uso de clases de destino:

```
[edit]
accounting-options {
    class-usage-profile dcu-profile1;
    file usage-stats
    interval 15;
    destination-classes {
        gold;
        silver;
        bronze;
    }
}
```

El perfil de uso de la clase, , escribe datos en el archivo .dcu-profile1usage-stats El archivo podría tener el siguiente aspecto:

```
#FILE CREATED 976825278 2000-12-14-20:21:18
#profile-layout, dcu_profile,epoch-timestamp,interface-name,destination-class,
packet-count,byte-count
dcu_profile,980313078,xe-1/0/0.0,gold,82,6888
dcu_profile,980313078,xe-1/0/0.0,silver,164,13776
```

```
dcu_profile,980313078,xe-1/0/0.0,bronze,0,0
dcu_profile,980313678,xe-1/0/0.0,gold,82,6888
dcu_profile,980313678,xe-1/0/0.0,silver,246,20664
dcu_profile,980313678,xe-1/0/0.0,bronze,0,0
...
#FILE CLOSED 976826178 2000-12-14-20:36:18
```

Configurar el perfil MIB

in this section

- Configurar la información de archivo | **830**
- Configurar el intervalo | **830**
- Configurar la operación MIB | **830**
- Configurar nombres de objetos MIB | **831**
- Ejemplo: Configurar un perfil MIB | **831**

El perfil MIB recopila estadísticas MIB y las registra en un archivo. El perfil MIB especifica la operación SNMP y los nombres de objeto MIB para los que se recopilan estadísticas.

Para configurar un perfil MIB, incluya la instrucción en el nivel de jerarquía:`mib-profile[edit accounting-options]`

```
[edit accounting-options]
mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
        mib-object-name;
    }
    operation operation-name;
}
```

Para configurar un perfil MIB, realice las tareas descritas en las secciones siguientes:

Configurar la información de archivo

Cada perfil de contabilidad registra sus estadísticas en un archivo del directorio./var/log

Para configurar el archivo que se va a usar, incluya la instrucción en el nivel de jerarquía:file[edit accounting-options mib-profile *profile-name*]

```
[edit accounting-options mib-profile profile-name]
file filename;
```

Debe especificar un para el perfil MIB que ya se haya configurado en el nivel de jerarquía.*filename*[edit accounting-options]

Configurar el intervalo

Un perfil MIB tiene estadísticas recopiladas una vez por intervalo de tiempo especificado para el perfil. El tiempo de recopilación de estadísticas se programa de manera uniforme durante el intervalo configurado. Para configurar el intervalo, incluya la instrucción en el nivel de jerarquía:interval[edit accounting-options mib-profile *profile-name*]

```
[edit accounting-options mib-profile profile-name]
interval;
```

El intervalo de la instrucción es de 1 a 2880 minutos.interval El valor predeterminado es de 30 minutos.

Configurar la operación MIB

Un perfil MIB debe especificar la operación que se utiliza para recopilar estadísticas MIB. Para configurar qué operación se usa para recopilar estadísticas MIB, incluya la instrucción en el nivel de jerarquía:operation[edit accounting-options mib-profile *profile-name*]

```
[edit accounting-options mib-profile profile-name]
operation operation-name;
```

Puede configurar una operación , o .getget-nextwalk La operación predeterminada es .walk

Configurar nombres de objetos MIB

Un perfil MIB debe especificar los objetos MIB para los que se van a recopilar estadísticas. Para configurar los objetos MIB para los que se recopilan estadísticas, incluya la instrucción en el nivel de jerarquía:`objects-names`[`edit accounting-options mib-profile` *`profile-name`*]

```
[edit accounting-options mib-profile profile-name]
object-names {
    mib-object-name;
}
```

Puede incluir varios nombres de objeto MIB en la configuración.

> **NOTA**: En Junos OS versión 15.1X49-D10 y posteriores, no configure objetos MIB relacionados con octetos o paquetes de interfaz para un perfil MIB, ya que puede provocar que se agote el tiempo de espera de la caminata SNMP o de un comando show de la CLI.

Ejemplo: Configurar un perfil MIB

Configure un perfil MIB:

```
[edit accounting-options]
mib-profile mstatistics {
    file stats;
    interval 60;
    operation walk;
    objects-names {
        ipCidrRouteStatus;
    }
}
```

Configurar el perfil del motor de enrutamiento

in this section

- Configurar campos | 832
- Configurar la información de archivo | 833
- Configurar el intervalo | 833
- Ejemplo: Configurar un perfil de motor de enrutamiento | 833

El perfil del motor de enrutamiento recopila estadísticas del motor de enrutamiento y las registra en un archivo. El perfil Motor de enrutamiento especifica los campos para los que se recopilan estadísticas.

Para configurar un perfil de motor de enrutamiento, incluya la instrucción en el nivel de jerarquía:`routing-engine-profile`[`edit accounting-options`]

```
[edit accounting-options]
routing-engine-profile profile-name {
    fields {
        field-name;
    }
    file filename;
    interval minutes;
}
```

Para configurar un perfil de motor de enrutamiento, realice las tareas descritas en las secciones siguientes:

Configurar campos

Un perfil de motor de enrutamiento debe especificar qué estadísticas se recopilan. Para configurar qué estadísticas deben recopilarse para el motor de enrutamiento, incluya la instrucción en el nivel de jerarquía:`fields`[`edit accounting-options routing-engine-profile` *`profile-name`*]

```
[edit accounting-options routing-engine-profile profile-name]
fields {
    field-name;
}
```

Configurar la información de archivo

Cada perfil de contabilidad registra sus estadísticas en un archivo del directorio./var/log

Para configurar el archivo que se va a usar, incluya la instrucción en el nivel de jerarquía:file[edit accounting-options routing-engine-profile *profile-name*]

```
[edit accounting-options routing-engine-profile profile-name]
file filename;
```

Debe especificar un perfil para el motor de enrutamiento que ya se haya configurado en el nivel de jerarquía.*filename*[edit accounting-options]

Configurar el intervalo

Un perfil de motor de enrutamiento tiene estadísticas recopiladas una vez por intervalo de tiempo especificado para el perfil. El tiempo de recopilación de estadísticas se programa de manera uniforme durante el intervalo configurado. Para configurar el intervalo, incluya la instrucción en el nivel de jerarquía:interval[edit accounting-options routing-engine-profile *profile-name*]

```
[edit accounting-options routing-engine-profile profile-name]
interval;
```

El rango para es de 1 a 2880 minutos.interval El valor predeterminado es de 30 minutos.

Ejemplo: Configurar un perfil de motor de enrutamiento

Configure un perfil de motor de enrutamiento:

```
[edit accounting-options]
file my-file {
    size 300k;
}
routing-engine-profile profile-1 {
    file my-file;
    fields {
        host-name;
        date;
        time-of-day;
        uptime;
        cpu-load-1;
        cpu-load-5;
```

```
        cpu-load-15;
    }
}
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
18.4R1	A partir de Junos OS 18.4R1, cuando se configura el archivado de archivos mediante la instrucción, la utilidad de transferencia de archivos no funciona si ha habilitado la instancia de administración.`archive-sites`
15.1X49-D10	En Junos OS versión 15.1X49-D10 y posteriores, no configure objetos MIB relacionados con octetos o paquetes de interfaz para un perfil MIB, ya que puede provocar que se agote el tiempo de espera de la caminata SNMP o de un comando show de la CLI.

6

PART IN COVERPAGE

Opciones de monitoreo

Alarmas de interfaz | 836

Monitoreo de IP | 848

Tecnología de monitoreo de sFlow | 869

Muestreo adaptable para enrutadores y conmutadores | 897

Software de diagnóstico del acelerador de flujo de paquetes | 902

chapter label in part7

Alarmas de interfaz

in this chapter

- Descripción general de alarmas | 836
- Ejemplo: Configurar alarmas de interfaz | 844

Descripción general de alarmas

summary

En esta sección se describen las alarmas de interfaz y cómo configurarlas.

in this section

- Tipos de alarma | 836
- Gravedad de la alarma | 837
- Condiciones de alarma | 838

Las alarmas le alertan de condiciones en una interfaz de red, en el chasis del dispositivo o en el software del sistema que podrían impedir que el dispositivo funcione normalmente. Puede establecer las condiciones que activan las alarmas en una interfaz. Las condiciones de alarma del chasis y del sistema están preestablecidas.

Una alarma activa enciende el LED en el panel frontal del dispositivo.**ALARM** Puede monitorear las alarmas activas desde la interfaz de usuario de J-Web o la CLI. Cuando una condición de alarma activa una alarma, el dispositivo enciende el LED amarillo (ámbar) en el panel frontal.**ALARM** Cuando se corrige la condición, la luz se apaga.

Tipos de alarma

El dispositivo admite tres tipos de alarmas:

- Las alarmas de interfaz indican un problema en el estado de los vínculos físicos en módulos de interfaz física (PIM) fijos o instalados. Para habilitar las alarmas de interfaz, debe configurarlas.

- Las alarmas del chasis indican un fallo en el dispositivo o en uno de sus componentes. Las alarmas del chasis están preestablecidas y no se pueden modificar.
- Las alarmas del sistema indican que falta una configuración de rescate o una licencia de software, si son válidas. Las alarmas del sistema están preestablecidas y no se pueden modificar, aunque puede configurarlas para que aparezcan automáticamente en la interfaz de usuario o CLI de J-Web.

A partir de Junos OS versión 15.1X49-D60 y Junos OS versión 17.3R1, se introduce una nueva alarma del sistema para indicar que las PIC (tarjeta de E/S o SPC) no se han conectado durante la hora de inicio del sistema.

A partir de Junos OS versiones 12.3X48-D85, 15.1X49-D180 y 19.2R1, se activa una alarma del sistema cuando el proceso de seguridad de red (NSD) no puede reiniciarse debido a un fallo de uno o más subcomponentes NSD. Los registros de alarma sobre el NSD se guardan en el registro de mensajes. La alarma se borra automáticamente cuando NSD se reinicia correctamente. Los comandos y se actualizan para mostrar el siguiente resultado cuando NSD no puede reiniciarse - .`show chassis alarmsshow system alarmsNSD fails to restart because subcomponents fail`

> **NOTA**: Ejecute los siguientes comandos cuando el indicador de CLI indique que se generó una alarma:
>
> - `show system alarms`
> - `show chassis alarms`
> - `show chassis fpc pic-status`

Para obtener más información acerca de los comandos de la CLI, consulte show system alarms, show chassis alarms, y show chassis fpc.https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/system-mgmt-monitoring/topics/ref/command/show-system-alarms.html*show chassis alarms*https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-fpc-security.html

Gravedad de la alarma

Las alarmas tienen dos niveles de gravedad:

- Mayor (rojo): indica una situación crítica en el dispositivo que ha resultado de una de las siguientes condiciones. Una condición de alarma roja requiere una acción inmediata.
  - Uno o más componentes de hardware han fallado.
  - Uno o más componentes de hardware han superado los umbrales de temperatura.
  - Una condición de alarma configurada en una interfaz ha desencadenado una advertencia crítica.

- Menor (amarillo): indica una condición no crítica en el dispositivo que, si no se marca, podría causar una interrupción en el servicio o una degradación en el rendimiento. Una condición de alarma amarilla requiere monitoreo o mantenimiento.

  Una configuración de rescate o licencia de software faltante genera una alarma amarilla del sistema.

Condiciones de alarma

Para habilitar las alarmas en la interfaz de un dispositivo, debe seleccionar una condición de alarma y una gravedad de alarma. Por el contrario, las condiciones y la gravedad de las alarmas están preconfiguradas para las alarmas del chasis y las alarmas del sistema.

> **NOTA**: Para obtener información acerca de las alarmas de chasis para su dispositivo, consulte la Guía de hardware para su dispositivo.

Esta sección contiene los siguientes temas:

Condiciones de alarma de interfaz

Tabla 78 en la página 838 enumera las condiciones de la interfaz, ordenadas por tipo de interfaz, que puede configurar para una alarma. Puede configurar cada condición de alarma para activar una alarma mayor (roja) o una alarma menor (amarilla). Se incluye la opción de configuración correspondiente.

Para los filtros de firewall con estado de servicios (NAT, IDP e IPsec), que funcionan en un módulo interno de servicios adaptables dentro de un dispositivo, puede configurar condiciones de alarma en los servicios integrados y las interfaces de servicios.

Tabla 78: Condiciones de alarma de interfaz

Interfaz	Condición de alarma	Description	Opción de configuración
DS1 (T1)	Señal de indicación de alarma (AIS)	La señal de tráfico T1 normal contenía una condición de defecto y ha sido reemplazada por el AIS. Se produjo una interrupción de la transmisión en el extremo remoto o aguas arriba del extremo remoto. Esta señal integral se transmite para evitar fallas o alarmas posteriores.	**ais**

Tabla 78: Condiciones de alarma de interfaz *(Continued)*

Interfaz	Condición de alarma	Description	Opción de configuración
	Alarma amarilla	El punto de conexión remoto tiene un error de alarma amarilla. Esta condición también se conoce como falla de alarma de extremo final.	**ylw**
Ethernet	El enlace está inactivo	El vínculo físico no está disponible.	**link-down**
Servicios integrados	Error de hardware o software	En el módulo de servicios adaptables, se produjo un error en el hardware asociado al módulo o en el software que controla el módulo.	**failure**
Serial	Señal de borrar para enviar (CTS) ausente	El extremo remoto del vínculo serie no está transmitiendo una señal CTS. La señal CTS debe estar presente antes de que los datos puedan transmitirse a través de un enlace serie.	**cts-absent**
	Señal de detección de portador de datos (DCD) ausente	El extremo remoto del vínculo serie no transmite una señal DCD. Dado que la señal DCD transmite el estado del dispositivo, es probable que ninguna señal indique que el extremo remoto del vínculo serie no esté disponible.	**dcd-absent**
	Ausencia de señal de conjunto de datos (DSR)	El extremo remoto del vínculo serie no transmite una señal DSR. La señal DSR indica que el punto de conexión remoto está listo para recibir y transmitir datos a través del enlace serie.	**dsr-absent**
	Pérdida del reloj de recepción	La señal de reloj del extremo remoto no está presente. Las conexiones serie requieren que las señales de reloj se transmitan desde un punto final y sean recibidas por el otro punto final del vínculo.	**loss-of-rx-clock**

Tabla 78: Condiciones de alarma de interfaz *(Continued)*

Interfaz	Condición de alarma	Description	Opción de configuración
	Pérdida del reloj de transmisión	La señal de reloj local no está presente. Las conexiones serie requieren que las señales de reloj se transmitan desde un punto final y sean recibidas por el otro punto final del vínculo.	**loss-of-tx-clock**
Servicios	Hardware del módulo de servicios inactivo	Se ha producido un problema de hardware en el módulo de servicios del dispositivo. Este error normalmente significa que una o más de las CPU del módulo han fallado.	**hw-down**
	Enlace de servicios hacia abajo	El vínculo entre el dispositivo y su módulo de servicios no está disponible.	**linkdown**
	Módulo de servicios retenido en el restablecimiento	El módulo de servicios del dispositivo está atascado en modo de restablecimiento. Si el módulo de servicios no se inicia cinco o más veces seguidas, el módulo de servicios se mantiene en modo de restablecimiento. El inicio falla cuando la cantidad de tiempo desde la liberación de la CPU hasta la detención de la CPU es inferior a 300 segundos.	**pic-hold-reset**
	Restablecimiento del módulo de servicios	El módulo de servicios del dispositivo se está restableciendo. El módulo se reinicia después de que se bloquea o se restablece desde la CLI, o cuando tarda más de 60 segundos en iniciarse.	**pic-reset**
	Software del módulo de servicios inactivo	Se ha producido un problema de software en el módulo de servicios del dispositivo.	**sw-down**

Tabla 78: Condiciones de alarma de interfaz *(Continued)*

Interfaz	Condición de alarma	Description	Opción de configuración
E3	Señal de indicación de alarma (AIS)	La señal de tráfico E3 normal contenía una condición de defecto y ha sido reemplazada por el AIS. Se produjo una interrupción de la transmisión en el extremo remoto o aguas arriba del extremo remoto. Esta señal integral se transmite para evitar fallas o alarmas posteriores.	**ais**
	Pérdida de señal (LOS)	No se recibe ninguna señal E3 remota en la interfaz E3.	**los**
	Fuera de marco (OOF)	Una condición OOF ha existido durante 10 segundos. Esta alarma solo se aplica a las interfaces E3 configuradas en modo de trama. El error de OOF se borra cuando no se han producido defectos de OOF o LOS durante 20 segundos.	**oof**
	Indicación remota de defectos	Existe una condición AIS, LOS u OOF. Esta alarma solo se aplica a las interfaces E3 configuradas en modo de trama.	**rdi**
T3 (DS3)	Señal de indicación de alarma	La señal de tráfico T3 normal contenía una condición de defecto y ha sido reemplazada por el AIS. Se produjo una interrupción de la transmisión en el extremo remoto o aguas arriba del extremo remoto. Esta señal integral se transmite para evitar fallas o alarmas posteriores.	**ais**
	Número excesivo de ceros	La secuencia de bits recibida del host ascendente tiene más ceros consecutivos de los permitidos en una trama T3.	**exz**

Tabla 78: Condiciones de alarma de interfaz *(Continued)*

Interfaz	Condición de alarma	Description	Opción de configuración
	Error de recepción del extremo final (FERF)	Error en el extremo remoto de la conexión. Un FERF difiere de una alarma amarilla, porque la falla puede ser cualquier falla, no solo una falla OOF o LOS.	**ferf**
	Alarma de inactividad	La señal de inactividad se recibe desde el extremo remoto.	**idle**
	Infracción del código de línea	La codificación de línea a lo largo del vínculo T3 está dañada o se produjo una falta de coincidencia entre la codificación en los extremos local y remoto de una conexión T3.	**lcv**
	Pérdida de trama (LOF)	Una condición OOF o LOS de pérdida de señal ha existido durante 10 segundos. La falla de LOF se borra cuando no se han producido defectos OOF o LOS durante 20 segundos. Una falla de LOF también se denomina falla roja.	**lof**
	Pérdida de señal (LOS)	No se recibe ninguna señal T3 remota en la interfaz T3.	**los**
	Bucle de bloqueo de fase fuera de bloqueo	Las señales de sincronización para los puntos de conexión locales y remotos ya no funcionan en el mismo paso.	**pll**
	Alarma amarilla	El punto de conexión remoto tiene un error de alarma amarilla. Esta condición también se conoce como falla de alarma de extremo final.	**ylw**

Condiciones de alarma del sistema

Tabla 79 en la página 843 enumera las dos alarmas predefinidas del sistema, la condición que activa cada alarma y la acción que debe realizar para corregir la condición.

Tabla 79: Condiciones de alarma del sistema y acciones correctivas

Tipo de alarma	Condición de alarma	Acción correctiva
Configuración	La configuración de rescate no está establecida.	Establezca la configuración de rescate.
Licencia	Ha configurado al menos una característica de software que requiere una licencia de características, pero actualmente no hay ninguna licencia válida para la característica. **NOTA**: Esta alarma indica que está infringiendo el acuerdo de licencia de software. Debe instalar una clave de licencia válida para cumplir con todos los acuerdos.	Instale una clave de licencia válida.

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
15.1X49-D60	A partir de Junos OS versión 15.1X49-D60 y Junos OS versión 17.3R1, se introduce una nueva alarma del sistema para indicar que las PIC (tarjeta de E/S o SPC) no se han conectado durante la hora de inicio del sistema.
12.3X48-D85 15.1X49-D180 19.2R1	A partir de Junos OS versiones 12.3X48-D85, 15.1X49-D180 y 19.2R1, se activa una alarma del sistema cuando el proceso de seguridad de red (NSD) no puede reiniciarse debido a un fallo de uno o más subcomponentes NSD. Los registros de alarma sobre el NSD se guardan en el registro de mensajes. La alarma se borra automáticamente cuando NSD se reinicia correctamente. Los comandos y se actualizan para mostrar el siguiente resultado cuando NSD no puede reiniciarse - `.show chassis alarmsshow system alarmsNSD fails to restart because subcomponents fail`

Ejemplo: Configurar alarmas de interfaz

in this section

- Requisitos | 844
- Descripción general | 844
- Configuración | 845
- Verificación | 847

En este ejemplo se muestra cómo configurar alarmas de interfaz.

Requisitos

Antes de empezar:

- Establecer conectividad básica.
- Configure las interfaces de red. Consulte la Guía del usuario de interfaces para dispositivos de seguridad.
- Seleccione la interfaz de red en la que desea aplicar una alarma y la condición en la que desea activar la alarma.

Descripción general

En este ejemplo, las alarmas de interfaz se habilitan estableciendo explícitamente las condiciones de alarma. El sistema se configura para generar una alarma de interfaz roja cuando se detecta una alarma amarilla en un vínculo DS1. El sistema se configura para generar una alarma de interfaz roja cuando se detecta un error de vínculo caído en un vínculo Ethernet.

Para un vínculo serie, establezca cts-absent y dcd-absent en amarillo para indicar que no se detecta la señal CST o DCD. Configure la alarma de pérdida de reloj y pérdida de reloj en rojo para indicar que la señal del reloj del receptor o la señal del reloj de transmisión no se detecta.

Para un vínculo T3, establezca la alarma de interfaz en rojo cuando el extremo remoto experimente un error. Se establece exz en amarillo alarma cuando el bit ascendente tiene más ceros consecutivos de los permitidos en una interfaz T3. A continuación, configure una alarma roja cuando haya pérdida de señal en la interfaz.

Por último, configure el sistema para que muestre las alarmas activas del sistema cada vez que un usuario con el administrador de la clase de inicio de sesión inicie sesión en el dispositivo.

Configuración

in this section

- Procedimiento | 845

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
set chassis alarm ds1 ylw red
set chassis alarm ethernet link-down red
set chassis alarm serial cts-absent yellow dcd-absent yellow
set chassis alarm serial loss-of-rx-clock red loss-of-tx-clock red
set chassis alarm t3 ylw red exz yellow los red
set system login class admin login-alarms
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar alarmas de interfaz:

1. Configure una alarma.

```
[edit]
user@host# edit chassis alarm
```

2. Especifique las alarmas de interfaz en un DS1 y un vínculo Ethernet.

```
[edit chassis alarm]
user@host# set ds1 ylw red
user@host# set ethernet link-down red
```

3. Especifique las alarmas de interfaz en un vínculo serie.

```
[edit chassis alarm]
user@host# set serial cts-absent yellow
user@host# set serial dcd-absent yellow
user@host# set serial loss-of-rx-clock red
user@host# set serial loss-of-tx-clock red
```

4. Especifique las alarmas de interfaz en un vínculo T3.

```
[edit chassis alarm]
user@host# set t3 ylw red
user@host# set t3 exz yellow
user@host# set t3 los red
```

5. Configure el sistema para que muestre las alarmas activas del sistema.

```
[edit]
user@host# edit system login
user@host# set class admin login-alarms
```

Resultados

Desde el modo de configuración, escriba los comandos `show chassis alarms` y `show system login` para confirmar la configuración. Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

```
[edit]
    user@host# show chassis alarms
    t3 {
    exz yellow;
        los red;
```

```
    ylw red;
    }
    ds1 {
        ylw red;
    }
    ethernet {
        link-down red;
    }
    serial {
        loss-of-rx-clock red;
        loss-of-tx-clock red;
        dcd-absent yellow;
        cts-absent yellow;
    }
    [edit]
        user@host# show system login
        show system login
    show system login
}
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Verificación

in this section

- Verificación de las configuraciones de alarma | **847**

Verificación de las configuraciones de alarma

Propósito

Confirme que la configuración funcione correctamente.

Verifique que las alarmas estén configuradas.

Acción

En el modo de configuración, escriba el comando `show chassis alarms`. Verifique que el resultado muestre la configuración prevista de las alarmas.

chapter label in part8

Monitoreo de IP

in this chapter

- Descripción general de la supervisión de IP | 848
- Ejemplo: Configurar la supervisión de IP en firewalls de la serie SRX | 851
- Ejemplo: Configurar la supervisión de IP en SRX5000 línea | 855
- Ejemplo: Configurar la supervisión de direcciones IP del grupo de redundancia del clúster de chasis | 863

Descripción general de la supervisión de IP

summary

En esta sección se describe cómo realizar un seguimiento del estado del sistema en uso.

in this section

- Parámetros de prueba de monitoreo de IP | 849
- Monitoreo de IP a través de grupos de agregación de vínculos de interfaz Ethernet redundantes | 850

Esta función monitorea IP en firewalls independientes de la serie SRX o en una interfaz Ethernet redundante (reth) *de clúster de chasis* . Las sondas RPM existentes se envían a una dirección IP para comprobar su accesibilidad. El usuario realiza una acción en función del resultado de accesibilidad. La acción admitida actualmente es la inyección de ruta estática preferida a la tabla de rutas del sistema.

Las acciones apoyadas son:

- Agregar o eliminar una nueva ruta estática que tenga un valor de prioridad más alto (preferencia menor) que una ruta configurada mediante el comando de la CLI `set routing-options static route`
- Definir varios nombres de sondeo bajo la misma directiva de supervisión de IP. Si se produce un error en alguna sonda, se realiza la acción. Si se puede acceder a todos los sondeos, la acción se revierte

- Configuración de varias pruebas en una sonda RPM. Todas las pruebas deben fallar para que la sonda RPM se considere inalcanzable. Si al menos una prueba alcanza su objetivo, la sonda RPM se considera accesible
- Configuración de varios umbrales de error en una prueba de RPM. Si se alcanza un umbral, la prueba falla. Si no se alcanza ningún umbral, la prueba se realiza correctamente.
- Especificar la opción sin preferencia. Si se especifica la opción de preferencia, la política no realiza una conmutación por recuperación preventiva cuando se encuentra en un estado de conmutación por error o cuando la prueba de sondeo RPM se recupera de un error.
- Establecer valores de métrica preferidos. Si se establece el valor de métrica preferido, durante la conmutación por error, la ruta se inyecta con el valor de métrica preferido establecido.
- Habilitar y deshabilitar interfaces.
  - : en una interfaz física o lógica, cuando se configura la acción de habilitación de interfaz, el estado inicial de la interfaz se desactiva después del inicio y permanece en el estado de desactivación mientras la sonda RPM asociada esté en el estado de paso.**Interface-Enable** Cuando se produce un error en el sondeo RPM asociado, se habilitan las interfaces físicas y lógicas configuradas.
  - **Interface-Disable**: en una interfaz física o lógica, cuando se configura la acción de desactivar interfaz, el estado de la interfaz permanece sin cambios. Cuando se produce un error en la sonda RPM asociada, se deshabilitan las interfaces físicas y lógicas.

NOTA: Se pueden definir varios nombres de sonda y acciones para la misma política de supervisión de IP.

Parámetros de prueba de monitoreo de IP

Cada objetivo sondeado se monitorea en el transcurso de una prueba, que representa una colección de sondas durante las cuales se recopilan estadísticas como la desviación estándar y la fluctuación . Durante una prueba, se generan sondas y se recogen respuestas a una velocidad definida por el intervalo de sonda, el número de segundos entre sondas.

NOTA: Para evitar el flap, una acción solo se revierte al final de un ciclo de prueba. Durante el ciclo de prueba, si no se alcanza ningún umbral, la acción se revierte. Aunque la conmutación por error de acción se lleva a cabo en función de una condición predefinida de una IP supervisada, cuando se invierte la condición, se puede acceder a la IP en la ruta original y se elimina la ruta

recién agregada. La recuperación sólo se realiza cuando todos los sondeos RPM informan que la IP es accesible.

No Link Title enumera los parámetros de prueba y sus valores predeterminados:

Tabla 80: Parámetros de prueba y valores predeterminados

Parámetro	Valor predeterminado
recuento de sondeos	1
intervalo de sondeo	3 segundos
intervalo de prueba	1 segundo

No Link Title enumera el umbral admitido y su descripción:

Tabla 81: Umbral admitido y descripción

Umbral	Description
Pérdida sucesiva	Recuento sucesivo de pérdidas de sondas
Pérdida total	Cuenta total de sonda perdida

Monitoreo de IP a través de grupos de agregación de vínculos de interfaz Ethernet redundantes

La supervisión de IP comprueba la accesibilidad de un dispositivo ascendente. Está diseñado para comprobar la conectividad de extremo a extremo de las direcciones IP configuradas y permite que un grupo de redundancia (RG) conmute por error automáticamente cuando no se puede acceder a la dirección IP supervisada a través de la Ethernet redundante. Tanto el dispositivo principal como el secundario del clúster de chasis supervisan direcciones IP específicas para determinar si se puede acceder a un dispositivo ascendente de la red.

Una interfaz Ethernet redundante contiene interfaces físicas de los nodos primario y secundario del clúster de chasis de la serie SRX. En una interfaz Ethernet redundante, se configuran dos interfaces

físicas en las que cada nodo aporta una interfaz física. En un LAG de interfaz Ethernet redundante, se configuran más de dos interfaces físicas en la interfaz Ethernet redundante.

Ejemplo: Configurar la supervisión de IP en firewalls de la serie SRX

in this section

- Requisitos | 851
- Descripción general | 851
- Configuración | 852
- Verificación | 854

En este ejemplo se muestra cómo supervisar IP en un firewall de la serie SRX.

Requisitos

Antes de empezar:

Configure las siguientes opciones de RPM para la prueba de RPM:

- dirección de destino
- recuento de sondeos
- intervalo de sondeo
- intervalo de prueba
- Umbrales
- Siguiente salto

Descripción general

En este ejemplo se muestra cómo configurar la supervisión de IP en un firewall de la serie SRX.

Configuración

in this section

- Procedimiento | 852

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía y, a continuación, ingrese desde el modo de configuración.`[edit]commit`

```
set services rpm probe Probe-Payment-Server test paysvr target address 1.1.1.10
set services rpm probe Probe-Payment-Server test paysvr probe-count 10
set services rpm probe Probe-Payment-Server test paysvr probe-interval 5
set services rpm probe Probe-Payment-Server test paysvr test-interval 5
set services rpm probe Probe-Payment-Server test paysvr thresholds successive-loss 10
set services rpm probe Probe-Payment-Server test paysvr next-hop 2.2.2.1
set services ip-monitoring policy Payment-Server-Tracking match rpm-probe Probe-Payment-Server
set services ip-monitoring policy Payment-Server-Tracking then preferred-route route 1.1.1.0/24
next-hop 1.1.1.99
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar la supervisión de IP en un firewall de la serie SRX:

1. Configure la dirección de destino en la sonda RPM.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr target address 1.1.1.10
```

2. Configure el recuento de sondas en la sonda RPM.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr probe-count 10
```

3. Configure el intervalo de la sonda (en segundos) bajo la sonda RPM.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr probe-interval 5
```

4. Configure el intervalo de prueba (en segundos) bajo la sonda RPM.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr test-interval 5
```

5. Configure el recuento de pérdidas sucesivas de umbral bajo RPM

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr thresholds successive-
loss 10
```

6. Configure la dirección IP del próximo salto en la sonda RPM.

```
[edit ]
user@host# set services rpm probe Probe-Payment-Server test paysvr next-hop 2.2.2.1
```

7. Configure la directiva de supervisión de IP en servicios.

```
[edit ]
user@host# set services ip-monitoring policy Payment-Server-Tracking match rpm-probe Probe-
Payment-Server
```

NOTA: Los siguientes pasos no son obligatorios. Puede configurar las acciones de interfaz y las acciones de ruta de forma independiente, o puede configurar la acción de interfaz y la acción de ruta juntas en una política de supervisión de IP.

8. Configure la ruta preferida de supervisión de IP en servicios.

```
[edit ]
user@host# set services ip-monitoring policy Payment-Server-Tracking then preferred-route
route 1.1.1.0/24 preferred-metric 4
```

9. Configure las acciones de la interfaz de supervisión de IP.

   - Habilitar

```
[edit ]
user@host# set services ip-monitoring policy Payment-Server-Tracking then interface
ge-0/0/1 enable
```

   - Deshabilitar

```
[edit ]
user@host# set services ip-monitoring policy Payment-Server-Tracking then interface
fe-0/0/[4-6] disable
```

10. Configure la opción sin preferencia.

```
[edit ]
user@host# set services ip-monitoring policy Payment-Server-Tracking no-preempt
```

Verificación

in this section

- Verificación de la supervisión de IP | 854

Verificación de la supervisión de IP

Propósito

Comprobar el estado de supervisión IP de una directiva.

Acción

Para comprobar que la configuración funciona correctamente, escriba el siguiente comando:

```
show services ip-monitoring status <policy-name>
```

Ejemplo: Configurar la supervisión de IP en SRX5000 línea

in this section

- Requisitos | 855
- Descripción general | 855
- Configuración | 857
- Verificación | 860

En este ejemplo, se muestra cómo supervisar los firewalls de la serie SRX con el clúster de chasis habilitado.

Requisitos

- Necesita dos puertas de enlace de servicios SRX5800 con configuraciones de hardware idénticas, un firewall de la serie SRX y un conmutador Ethernet EX8208.
- Conecte físicamente los dos dispositivos SRX5800 (espalda con espalda para la estructura y los puertos de control) y asegúrese de que sean los mismos modelos. Configure o agregue estos dos dispositivos en un clúster.

Descripción general

in this section

- Topología | 856

La supervisión de direcciones IP comprueba la accesibilidad de extremo a extremo de la dirección IP configurada y permite que un grupo de redundancia conmute por error automáticamente cuando no sea

accesible a través del vínculo secundario de la interfaz Ethernet redundante (conocida como reth). Los grupos de redundancia en ambos dispositivos de un clúster se pueden configurar para supervisar direcciones IP específicas a fin de determinar si se puede acceder a un dispositivo ascendente de la red.

Cuando se configuran varias direcciones IP en la interfaz reth en una configuración de clúster de chasis, la supervisión de IP utiliza la primera dirección IP de la lista de direcciones IP configuradas para esa interfaz reth en el nodo principal y la primera dirección IP de la lista de direcciones IP secundarias configuradas para esa interfaz reth en el nodo de copia de seguridad. La primera dirección IP es la que tiene el prefijo más pequeño (máscara de red).

En este ejemplo se muestra cómo configurar la supervisión de IP en un firewall de la serie SRX.

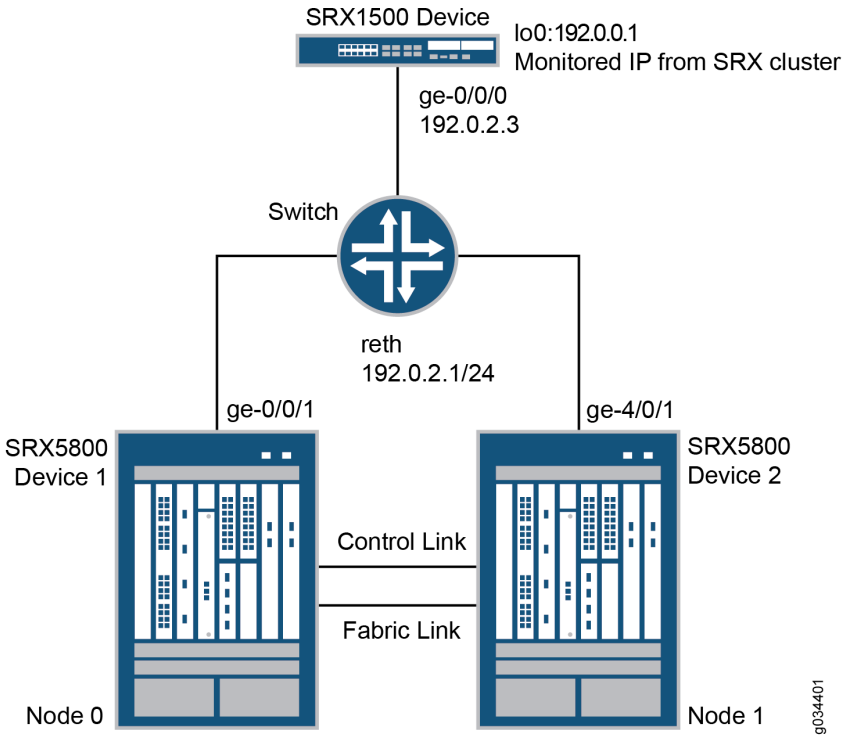
NOTA: La supervisión de IP no es compatible con una tarjeta NP-IOC.

NOTA: La supervisión de IP no admite el estado de MIC en línea/fuera de línea en los firewalls de la serie SRX.

Topología

Figura 30 en la página 857muestra la topología utilizada en este ejemplo.

Figura 30: Ejemplo de monitoreo de IP en una topología de firewall de la serie SRX



En este ejemplo, dos dispositivos SRX5800 de un clúster de chasis están conectados a un dispositivo SRX1500 a través de un conmutador Ethernet EX8208. En el ejemplo se muestra cómo se pueden configurar los grupos de redundancia para supervisar recursos clave ascendentes accesibles a través de interfaces Ethernet redundantes en cualquiera de los dos nodos de un clúster.

Configuración

in this section

- Configuración rápida de CLI | **857**
- Configuración de la supervisión de IP en el firewall de la serie SRX | **858**

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles para que coincidan con su configuración de red,

copie y pegue los comandos en la CLI en el nivel de jerarquía y, a continuación, ingrese desde el modo de configuración.`[edit]commit`

```
set chassis cluster reth-count 1
set chassis cluster redundancy-group 0 node 0 priority 254
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 200
set chassis cluster redundancy-group 1 node 1 priority 199
set chassis cluster redundancy-group 1 ip-monitoring global-weight 255
set chassis cluster redundancy-group 1 ip-monitoring global-threshold 80
set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1 weight 80
set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1 interface reth0.0
secondary-ip-address 192.0.2.2
set interfaces ge-0/0/1 gigether-options redundant-parent reth0
set interfaces ge-4/0/1 gigether-options redundant-parent reth0
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 192.0.2.1/24
set routing-options static route 192.0.0.1/32 next-hop 192.0.2.3
```

Configuración de la supervisión de IP en el firewall de la serie SRX

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar la supervisión de IP en un firewall de la serie SRX:

1. Especifique el número de interfaces Ethernet redundantes.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 1
```

2. Especifique la prioridad de primacía de un grupo de redundancia en cada nodo del clúster. El número más alto tiene prioridad.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 0 node 0 priority 254
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
user@host# set chassis cluster redundancy-group 1 node 0 priority 200
user@host# set chassis cluster redundancy-group 1 node 1 priority 199
```

3. Configure las interfaces Ethernet redundantes para el grupo de redundancia 1.

```
{primary:node0}[edit]
user@host# set interfaces reth0 redundant-ether-options redundancy-group 1
user@host# set interfaces reth0 unit 0 family inet address 192.0.2.1/24
```

4. Asigne interfaces secundarias para las interfaces Ethernet redundantes desde el nodo 0 y el nodo 1.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth0
user@host# set interfaces ge-4/0/1 gigether-options redundant-parent reth0
```

5. Configure la ruta estática a la dirección IP que se va a supervisar.

```
{primary:node0}[edit]
user@host# set routing-options static route 192.0.0.1/32 next-hop 192.0.2.3
```

6. Configure la supervisión de IP en el grupo de redundancia 1 con peso global y umbral global.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-weight 255
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-threshold 80
```

7. Especifique el intervalo de reintento.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
```

8. Especifique el recuento de reintentos.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
```

9. Asigne un peso a la dirección IP que se va a supervisar y configure una dirección IP secundaria que se utilizará para enviar paquetes ICMP desde el nodo secundario para realizar un seguimiento de la IP que se está supervisando.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1 weight
80
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 192.0.0.1
interface reth0.0 secondary-ip-address 192.0.2.2
```

NOTA:

- La dirección IP Ethernet redundante (reth0), , se utiliza para enviar paquetes ICMP desde el nodo 0 para comprobar la accesibilidad de la IP supervisada.**192.0.2.1/24**
- La dirección IP secundaria, , debe pertenecer a la misma red que la dirección IP reth0.**192.0.2.2**
- La dirección IP secundaria se utiliza para enviar paquetes ICMP desde el nodo 1 para comprobar la accesibilidad de la IP supervisada.

Verificación

in this section

- Verificación del estado del clúster del chasis: antes de la conmutación por error | **861**
- Verificación del estado de supervisión de IP del clúster de chasis: antes de la conmutación por error | **861**
- Verificación del estado del clúster del chasis: después de la conmutación por error | **862**
- Verificación del estado de supervisión IP del clúster de chasis: después de la conmutación por error | **862**

Confirme que la configuración funciona correctamente.

Verificación del estado del clúster del chasis: antes de la conmutación por error

Propósito

Compruebe el estado del clúster de chasis, el estado de conmutación por error y la información del grupo de redundancia antes de la conmutación por error.

Acción

Desde el modo operativo, ingrese el comando `show chassis cluster status`.

```
show chassis cluster status

Cluster ID: 11
Node Priority Status Preempt Manual failover
Redundancy group: 0 , Failover count: 0
node0 254 primary no no
node1 1 secondary no no
Redundancy group: 1 , Failover count: 0
node0 200 primary no no
node1 199 secondary no no
```

Verificación del estado de supervisión de IP del clúster de chasis: antes de la conmutación por error

Propósito

Compruebe el estado de IP que se supervisa desde ambos nodos y el recuento de conmutación por error para ambos nodos antes de la conmutación por error.

Acción

Desde el modo operativo, ingrese el comando `show chassis cluster ip-monitoring status redundancy-group 1`.

```
show chassis cluster ip-monitoring status redundancy-group 1

node0:
--------------------------------------------------------------------------
Redundancy group: 1
```

```
IP address Status Failure count Reason
192.0.0.1 reachable 0 n/a
node1:
--------------------------------------------------------------------------
Redundancy group: 1
IP address Status Failure count Reason
192.0.0.1 reachable 0 n/a
```

Verificación del estado del clúster del chasis: después de la conmutación por error

Propósito

Compruebe el estado del clúster de chasis, el estado de conmutación por error y la información del grupo de redundancia después de la conmutación por error.

NOTA: Si no se puede acceder a la dirección IP, se mostrará el siguiente resultado.

Acción

Desde el modo operativo, ingrese el comando `show chassis cluster status`.

```
show chassis cluster status

Cluster ID: 11
Node Priority Status Preempt Manual failover
Redundancy group: 0 , Failover count: 0
node0 254 primary no no
node1 1 secondary no no
Redundancy group: 1 , Failover count: 1
node0 0 secondary no no
node1 199 primary no no
```

Verificación del estado de supervisión IP del clúster de chasis: después de la conmutación por error

Propósito

Compruebe el estado de IP que se supervisa desde ambos nodos y el recuento de conmutación por error para ambos nodos después de la conmutación por error.

Acción

Desde el modo operativo, ingrese el comando `show chassis cluster ip-monitoring status redundancy-group 1`.

```
show chassis cluster ip-monitoring status redundancy-group 1

node0:
--------------------------------------------------------------------------
Redundancy group: 1
IP address Status Failure count Reason
192.0.0.1 unreachable 1 unknown
node1:
--------------------------------------------------------------------------
Redundancy group: 1
IP address Status Failure count Reason
192.0.0.1 reachable 0 n/a
```

VÍNCULOS RELACIONADOS

Ejemplo: Configuración de un clúster de chasis activo/pasivo en dispositivos SRX5800

Ejemplo: Configurar la supervisión de direcciones IP del grupo de redundancia del clúster de chasis

in this section

- Requisitos | **864**
- Descripción general | **864**
- Configuración | **865**
- Verificación | **867**

En este ejemplo se muestra cómo configurar la supervisión de direcciones IP del grupo de redundancia para un firewall de la serie SRX en un clúster de chasis.

Requisitos

Antes de empezar:

- Establezca el ID de nodo y el ID de clúster del clúster del chasis. Consulte *Ejemplo: Configuración del ID de nodo y el ID de clúster para dispositivos de seguridad en un clúster de chasis*
- Configure la interfaz de administración del clúster del chasis. Consulte *Ejemplo: Configuración de la interfaz de administración del clúster de chasis.*
- Configure la estructura del clúster de chasis. Consulte *Ejemplo: Configuración de las interfaces de estructura del clúster de chasis.*

Descripción general

Puede configurar grupos de redundancia para supervisar los recursos ascendentes haciendo ping a direcciones IP específicas a las que se puede acceder a través de interfaces Ethernet redundantes en cualquiera de los dos nodos de un clúster. También puede configurar parámetros globales de umbral, peso, intervalo de reintento y recuento de reintentos para un grupo de redundancia. Cuando una dirección IP supervisada se vuelve inaccesible, el peso de esa dirección IP supervisada se deduce del umbral global de supervisión de direcciones IP del grupo de redundancia. Cuando el umbral global alcanza 0, el peso global se deduce del umbral del grupo de redundancia. El intervalo de reintento determina el intervalo ping para cada dirección IP supervisada por el grupo de redundancia. Los pings se envían tan pronto como se confirma la configuración. El recuento de reintentos establece el número de errores de ping consecutivos permitidos para cada dirección IP supervisada por el grupo de redundancia.

En este ejemplo, se configuran las siguientes opciones para el grupo de redundancia 1:

- Dirección IP para monitorear: 10.1.1.10
- Monitoreo de direcciones IP de peso global: 100
- Umbral global de monitoreo de direcciones IP: 200

  El umbral se aplica acumulativamente a todas las direcciones IP supervisadas por el grupo de redundancia.
- Intervalo de reintento de dirección IP: 3 segundos
- Número de reintentos de direcciones IP: 10
- Peso: 100
- Interfaz Ethernet redundante: reth1.0
- Dirección IP secundaria: 10.1.1.101

Configuración

in this section

- Procedimiento | 865

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
{primary:node0}[edit]
user@host#
set chassis cluster redundancy-group 1 ip-monitoring global-weight 100
set chassis cluster redundancy-group 1 ip-monitoring global-threshold 200
set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
set chassis cluster redundancy-group 1 ip-monitoring family inet 10.1.1.10 weight 100 interface
reth1.0 secondary-ip-address 10.1.1.101
```

Procedimiento paso a paso

Para configurar la supervisión de direcciones IP del grupo de redundancia:

1. Especifique un peso de supervisión global.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-weight 100
```

2. Especifique el umbral de supervisión global.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring global-threshold 200
```

3. Especifique el intervalo de reintento.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-interval 3
```

4. Especifique el recuento de reintentos.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring retry-count 10
```

5. Especifique la dirección IP que se va a supervisar, el peso, la interfaz Ethernet redundante y la dirección IP secundaria.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 ip-monitoring family inet 10.1.1.10 weight
100 interface reth1.0 secondary-ip-address 10.1.1.101
```

Resultados

Desde el modo de configuración, confírmela con el comando `show chassis cluster redundancy-group 1`. Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

Para fines de brevedad, este resultado del comando `show` solo incluye la configuración relevante para este ejemplo. Cualquier otra configuración en el sistema se reemplazó por puntos suspensivos (...).

```
{primary:node0}[edit]
user@host# show chassis cluster redundancy-group 1
ip-monitoring {
    global-weight 100;
    global-threshold 200;
    family {
        inet {
```

```
            10.1.1.10 {
                weight 100;
                interface reth1.0 secondary-ip-address 10.1.1.101;
            }
        }
    }
}
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Verificación

in this section

- Comprobación del estado de las direcciones IP supervisadas para un grupo de redundancia | **867**

Comprobación del estado de las direcciones IP supervisadas para un grupo de redundancia

Propósito

Compruebe el estado de las direcciones IP supervisadas para un grupo de redundancia.

Acción

Desde el modo operativo, ingrese el comando `show chassis cluster ip-monitoring status`. Para obtener información sobre un grupo específico, escriba el comando.`show chassis cluster ip-monitoring status redundancy-group`

```
{primary:node0}
user@host> show chassis cluster ip-monitoring status
node0:
--------------------------------------------------------------------------

Redundancy group: 1
Global threshold: 200
Current threshold: -120

IP address                Status        Failure count  Reason    Weight
10.1.1.10                 reachable       0            n/a       100
```

```
10.1.1.101                reachable       0            n/a       100

node1:
--------------------------------------------------------------------------

Redundancy group: 1
Global threshold: 200
Current threshold: -120

IP address                Status        Failure count  Reason    Weight
10.1.1.10                 reachable       0            n/a       100
10.1.1.101                reachable       0            n/a       100
```

chapter label in part9

Tecnología de monitoreo de sFlow

in this chapter

- Descripción general de la tecnología sFlow | 869
- Soporte de sFlow en conmutadores | 870
- Ejemplo: Configurar sFlow para redes EVPN-VXLAN | 878
- Soporte de sFlow en enrutadores | 883
- Ejemplo: Configurar la tecnología sFlow para monitorear el tráfico de red | 888
- Asignación de direcciones del agente de sFlow | 895

Descripción general de la tecnología sFlow

in this section

- Beneficios de la tecnología sFlow | 870

La tecnología sFlow es una tecnología de monitoreo para redes conmutadas o enrutadas de alta velocidad. La tecnología de monitoreo sFlow recolecta muestras de paquetes de red y las envía en un datagrama UDP a una estación de monitoreo llamada *colector*. Puede configurar la tecnología sFlow en un dispositivo para monitorear el tráfico continuamente a velocidad de cable en todas las interfaces simultáneamente. Debe habilitar la supervisión de sFlow en cada interfaz individualmente; no puede habilitar globalmente la supervisión de sFlow en todas las interfaces con una sola instrucción de configuración. Junos OS es compatible con el estándar de tecnología sFlow descrito en RFC 3176, sFlow de InMon Corporation: *Un método para monitorear el tráfico en redes conmutadas y enrutadas (consulte http://faqs.org/rfcs/rfc3176.html).*http://faqs.org/rfcs/rfc3176.html

La tecnología sFlow implementa los siguientes dos mecanismos de muestreo:

- Muestreo basado en paquetes: toma muestras de un paquete de un número especificado de paquetes desde una interfaz habilitada para la tecnología sFlow. Sólo se envían al recopilador los

primeros 128 bytes de cada paquete. Los datos recopilados incluyen los encabezados de Ethernet, IP y capa de transporte, junto con otros encabezados de nivel de aplicación (si están presentes). Aunque es posible que este tipo de muestreo no capture flujos de paquetes poco frecuentes, la mayoría de los flujos se notifican a lo largo del tiempo, lo que permite al recopilador generar una representación razonablemente precisa de la actividad de la red. El muestreo basado en paquetes se configura cuando se especifica una frecuencia de muestreo.

- Muestreo basado en el tiempo: muestra estadísticas de interfaz (contadores) en un intervalo especificado desde una interfaz habilitada para la tecnología sFlow. Se capturan estadísticas como errores de interfaz Ethernet. El muestreo basado en el tiempo se configura cuando se especifica un intervalo de sondeo.

  Las estadísticas de interfaz son la fuente del muestreo basado en el tiempo. El muestreo basado en el tiempo proporciona datos estadísticos en la salida del comando.`show interface statistics` Si borra las estadísticas de la interfaz con el comando , el muestreo basado en tiempo muestra los valores de restablecimiento.`clear interfaces statistics`

Beneficios de la tecnología sFlow

- sFlow puede ser utilizado por herramientas de software como un analizador de red para monitorear continuamente decenas de miles de puertos de conmutadores o enrutadores simultáneamente.
- Dado que sFlow utiliza el muestreo de red (reenvío de un paquete del número total de paquetes) para el análisis, no consume muchos recursos (por ejemplo, procesamiento, memoria, etc.).*n* El muestreo se realiza en los circuitos integrados específicos de la aplicación de hardware (ASIC) y, por lo tanto, es simple y más preciso.

Soporte de sFlow en conmutadores

in this section

- sFlow para túneles IP a través de IP | **872**
- sFLow para el sistema QFabric | **872**
- sFlow para EVPN-VXLAN | **873**
- Limitaciones de sFlow en conmutadores | **877**

La tecnología sFlow en los conmutadores solo toma muestras de encabezados de paquetes sin procesar. Un paquete Ethernet sin formato es la trama de red completa de capa 2.

Un sistema de monitoreo sFlow consiste en un agente sFlow integrado en el dispositivo (conmutador) y hasta cuatro colectores externos. Las dos actividades principales del agente sFlow son el muestreo aleatorio y la recopilación de estadísticas. El agente sFlow realiza el muestreo de paquetes y recopila estadísticas de la interfaz y, a continuación, combina la información en datagramas UDP que se envían a los recopiladores sFlow. Se puede conectar un recolector sFlow al conmutador a través de la red de administración o de datos. El demonio de infraestructura de reenvío de software (SFID) del conmutador busca la dirección del próximo salto para la dirección IP del recopilador especificado para determinar si se puede acceder al recopilador a través de la red de administración o de la red de datos.

Cada datagrama contiene la siguiente información:

- La dirección IP del agente sFlow
- El número de muestras
- La interfaz a través de la cual los paquetes entraron en el agente
- La interfaz a través de la cual los paquetes salieron del agente
- La interfaz de origen y destino de los paquetes
- La VLAN de origen y destino para los paquetes

Puede ver los encabezados de datos del **enrutador** extendido y de **datos del conmutador extendido** en el recopilador como parte de los registros de sFlow.

Los datos del conmutador extendido contienen información de campos*Flow data length (byte), Incoming 802.1Q VLAN, Incoming 802.1p priority, Outgoing 802.1Q VLAN, and Outgoing 802.1p priority*

Los datos del enrutador extendido contienen información de campos.*Flow data length (byte), Next hop, Next hop source mask, and Next hop destination mask*

Los conmutadores de la serie EX adoptan la arquitectura distribuida sFlow. El agente sFlow tiene dos entidades de muestreo independientes que están asociadas a cada motor de reenvío de paquetes. Estas entidades de muestreo se conocen como subagentes. Cada subagente tiene un identificador único que el recopilador utiliza para identificar el origen de datos. Un subagente tiene su propio estado independiente y reenvía sus propios paquetes de ejemplo al agente sFlow. El agente sFlow es responsable de empaquetar las muestras en datagramas y enviarlas al recopilador sFlow. Debido a que el muestreo se distribuye entre los subagentes, la sobrecarga del protocolo asociada con la tecnología sFlow se reduce significativamente en el recopilador.

Para el conmutador EX9200 y los enrutadores de la serie MX, se recomienda configurar la misma frecuencia de muestreo para todos los puertos de una tarjeta de línea. Si configura diferentes frecuencias de muestreo, se utilizará el valor más bajo para todos los puertos de la tarjeta de línea.

En el caso de VLAN duales, es posible que no se notifiquen todos los campos.

Si la asignación de roles principales cambia en una configuración de Virtual Chassis , la tecnología sFlow seguirá funcionando.

sFlow para túneles IP a través de IP

A partir de Junos OS versión 20.4R1, puede utilizar la tecnología sFlow para muestrear el tráfico de IP a través de IP en un puerto físico en dispositivos QFX5100 y QFX5200. Esta característica se admite para túneles IP a través de IP con un encabezado externo IPv4 que transportan tráfico IPv4 o IPv6. Utilice la tecnología de monitoreo sFlow para muestrear aleatoriamente paquetes de red desde túneles IP a través de IP y enviar las muestras a un recolector de destino para su monitoreo. Los dispositivos que actúan como punto de entrada de túnel IP a través de IP, dispositivo de tránsito o punto de conexión de túnel admiten el muestreo de sFlow. muestra los campos que se notifican cuando se muestrea un paquete en la interfaz de entrada o salida de un dispositivo que actúa como punto de entrada de túnel IP a través de IP, dispositivo de tránsito o extremo de túnel.No Link Title

Tabla 82: Metadatos admitidos

Campo sFlow	Punto de entrada del túnel	Dispositivo de tránsito	Extremo de túnel
Raw packet header	Incluye solo carga útil	Incluye carga útil y encabezado de túnel	Salida: Incluye solo carga útil Ingreso: Incluye carga útil y encabezado de túnel
Input interface	Índice SNMP IFD entrante	Índice SNMP IFD entrante	Índice SNMP IFD entrante
Output interface	Índice SNMP IFD saliente	Índice SNMP IFD saliente	Índice SNMP IFD saliente

sFLow para el sistema QFabric

En un sistema QFabric, la tecnología sFlow monitorea las interfaces en cada dispositivo de nodo como un grupo e implementa el algoritmo de retroceso binario basado en el tráfico en ese grupo de interfaces.

En el sistema QFabric, se utilizan los siguientes valores predeterminados si no se configuran los parámetros opcionales:

- El ID del agente es la dirección IP de administración de la partición predeterminada.
- La IP de origen es la dirección IP de administración de la partición predeterminada.

Además, el ID de subagente del sistema QFabric (que se incluye en los datagramas sFlow) es el identificador del grupo de nodos desde el que se envía el datagrama al recopilador.

En un sistema QFabric, la arquitectura de la tecnología sFlow se distribuye. La configuración global de la tecnología sFlow definida en el dispositivo QFabric system Director se distribuye a los grupos de nodos que tienen configurado el muestreo de sFlow en sus interfaces. El agente sFlow tiene una entidad de muestreo independiente, conocida como subagente, que se ejecuta en cada dispositivo de nodo. Cada subagente tiene su propio estado independiente y reenvía su propia información de muestra (datagramas) directamente a los recopiladores sFlow.

En el sistema QFabric, se debe poder acceder a un recolector sFlow a través de la red de datos. Dado que cada dispositivo de nodo tiene todas las rutas almacenadas en la instancia de enrutamiento predeterminada, la dirección IP del recopilador debe incluirse en la instancia de enrutamiento predeterminada para garantizar la accesibilidad del recopilador desde el dispositivo del nodo.

Independientemente de la velocidad de tráfico o del intervalo de muestreo configurado, un datagrama se envía siempre que su tamaño alcance la unidad de transmisión Ethernet (MTU) máxima de 1500 bytes o cuando caduque un temporizador de 250 ms, lo que ocurra primero. El temporizador garantiza que un recolector reciba datos muestreados regularmente.

El muestreo basado en paquetes en sFlow se implementa en el hardware. Si los niveles de tráfico son inusualmente altos, el hardware genera más muestras de las que puede manejar, y las muestras adicionales se eliminan, produciendo resultados inexactos. Al habilitar la instrucción, se deshabilita el algoritmo de limitación de velocidad de software y se permite que la frecuencia de muestreo del hardware permanezca dentro de la frecuencia de muestreo máxima.`disable-sw-rate-limiter`

sFlow para EVPN-VXLAN

En los conmutadores de la serie QFX10000, puede usar la tecnología sFlow para muestrear el tráfico de multidifusión conocido que se transporta a través de EVPN-VXLAN. El muestreo de tráfico de multidifusión conocido se admite para el tráfico que ingresa al conmutador a través de EVPN-VXLAN o, en otras palabras, la interfaz orientada al núcleo y sale del conmutador de los puertos orientados al cliente. Además, el muestreo de tráfico de multidifusión conocido solo se admite en la dirección de salida. Para habilitar el muestreo sFlow de salida del tráfico de multidifusión conocido en un puerto orientado hacia el cliente, debe habilitar sFlow en la interfaz en la dirección de salida, tal como se hace para el escenario de muestreo de tráfico de unidifusión estándar. Además, debe incluir la opción en el nivel de jerarquía.`egress-multicast enable`[`edit forwarding options sflow`] La tasa máxima de replicación para muestras de tráfico de multidifusión se puede configurar mediante la opción en el nivel de jerarquía.`eggress-multicast max-replication-rate` *rate*[`edit forwarding options sflow eggress-multicast`]

Cuando un conjunto de interfaces habilitadas para muestreo de salida de sFlow se suscribe a un grupo de multidifusión determinado y la opción de muestreo de multidifusión de sFlow de salida está habilitada, todas las interfaces se muestrearán a la misma velocidad. El mínimo de la velocidad de flujo sFlow configurada, o en otras palabras, la frecuencia de muestreo más agresiva entre este conjunto de

interfaces se utiliza para el muestreo en todas las interfaces del conjunto. Un solo puerto generará muestras a diferentes velocidades si forma parte de varios grupos de multidifusión, ya que el muestreo de multidifusión para un grupo específico depende de la frecuencia de muestreo más agresiva entre los puertos de ese grupo en particular.

En EVPN-VXLAN, la arquitectura de puente de enrutamiento centralizado (CRB) y de puente de borde enrutado (ERB) son compatibles con sFlow. EVPN-VXLAN solo admite direcciones IPv4.

Tabla 83: Metadatos admitidos

Interfaz entrante y encapsulación	Interfaz saliente y encapsulación	Contenido de muestra requerido	Escenario de reenvío	Metadatos
Tráfico de capa 2 del puerto de acceso	Puerto de red	Encabezado entrante de capa 2 + carga útil de capa 2	Los paquetes se encapsulan con un encabezado VXLAN y se reenvían.	Identificador o índice de interfaz entrante. Índice o identificador de interfaz saliente
Tráfico de capa 3 del puerto de red	Puerto de acceso	Encabezado entrante de capa 3 + encabezado VXLAN + Carga interna	Los paquetes se desencapsulan y se reenvían.	Identificador o índice de interfaz de punto final de túnel virtual (VTEP) entrante. Índice o identificador de interfaz saliente
Tráfico de capa 2 del puerto de acceso	Puerto de red	Encabezado entrante de capa 2 + carga de capa 2	Los paquetes se encapsulan con un encabezado VXLAN y se reenvían.	Identificador o índice de interfaz entrante. Índice o identificador de interfaz saliente
Tráfico de capa 3 del puerto de red	Puerto de acceso	Carga útil interna	Los paquetes se desencapsulan y se reenvían.	Identificador o índice de interfaz VTEP entrante. Índice o identificador de interfaz saliente

No Link Title proporciona información de metadatos para datos de conmutadores extendidos y datos de enrutamiento extendidos.

Tabla 84: Metadatos admitidos para datos de conmutadores extendidos y datos de enrutamiento extendidos

EVPN-VXLAN	Escenario	Tipo de tráfico	Lado de la interfaz sFlow	Tipo de túnel VXLAN	Datos ampliados del conmutador				Datos de enrutamiento extendidos		
					IIF VLAN	Prioridad de VLAN IIF	OIF VLAN	Prioridad de VLAN OIF	NH IP	NH SMASK	NH DMASK
CRB	Capa 2 GW Leaf	Capa 2	Ingreso	Encap	Sí	Sí	No	No	Sí	Sí	Sí
				Decapear	No	No	Sí	No	No	No	No
			Salida	Encap	Sí	No	No	No	Sí	Sí	Sí
				Decapear	No	No	Sí	No	No	No	No
	Capa 3 GW de columna vertebral	Capa 2	Ingreso	No	No	No	No	No	No	No	No
				No	No	No	No	No	No	No	No
				Tránsito	No	No	No	No	Sí	Sí	Sí
			Salida	No	No	No	No	No	No	No	No
				No	No	No	No	No	No	No	No
				Tránsito	No	No	No	No	Sí	Sí	Sí
		Tráfico de capa 3	Ingreso	Encap	No	No	No	No	Sí	Sí	Sí

Tabla 84: Metadatos admitidos para datos de conmutadores extendidos y datos de enrutamiento extendidos *(Continued)*

EVPN-VXLAN	Escenario	Tipo de tráfico	Lado de la interfaz sFlow	Tipo de túnel VXLAN	Datos ampliados del conmutador				Datos de enrutamiento extendidos		
					IIF VLAN	Prioridad de VLAN IIF	OIF VLAN	Prioridad de VLAN OIF	NH IP	NH SMASK	NH DMASK
		(caso entre VLAN)		Decapear	No	No	No	No	Sí	Sí	Sí
				Tránsito	No	No	No	No	Sí	Sí	Sí
			Salida	Encap	No	No	No	No	Sí	Sí	Sí
				Decapear	No	No	No	No	Sí	Sí	Sí
				Tránsito	No	No	No	No	Sí	Sí	Sí
ERB	Capa 2+Capa 3	Capa 2	Ingreso	Encap	Sí	Sí	No	No	Sí	Sí	Sí
				Decapear	No	No	Sí	No	No	No	No
			Salida	Encap	Sí	No	No	No	Sí	No	Sí
				Decapear	No	No	Sí	No	No	No	No
		Tráfico de capa 3	Ingreso	Encap	Sí	Sí	No	No	Sí	Sí	Sí

Tabla 84: Metadatos admitidos para datos de conmutadores extendidos y datos de enrutamiento extendidos *(Continued)*

EVPN-VXLAN	Escenario	Tipo de tráfico	Lado de la interfaz sFlow	Tipo de túnel VXLAN	Datos ampliados del conmutador				Datos de enrutamiento extendidos		
					IIF VLAN	Prioridad de VLAN IIF	OIF VLAN	Prioridad de VLAN OIF	NH IP	NH SMASK	NH DMASK
		(caso entre VLAN)		Decapear	No	No	Sí	No	No	No	No
			Salida	Encap	Sí	No	No	No	Sí	Sí	Sí
				Decapear	No	No	Sí	No	No	No	No

Limitaciones de sFlow en conmutadores

En los conmutadores, las limitaciones del muestreo de tráfico de sFlow incluyen las siguientes:

- Los conmutadores de las series EX3400, EX4100, EX4300, EX4400 y QFX5K utilizan el muestreo de pseudosalida para el muestreo de salida. Los paquetes no son verdaderos ejemplos de salida. Son copias sin modificar tal y como aparecen en la canalización de entrada del dispositivo de instancia de sflow que utiliza el muestreo de salida.

- En los dispositivos QFX5130-32CD y QFX5700, el sFlow de salida utiliza el paquete de canalización de entrada, a diferencia de otros dispositivos de la serie QFX que utilizan direcciones IP de origen y destino originales. Los paquetes muestreados en la interfaz de salida muestran el encabezado VXLAN con las direcciones IP de origen y destino de la VXLAN de entrada.

  Los paquetes muestreados de salida para los dispositivos QFX5130-32CD y QFX5700 muestran las direcciones IP de los extremos VXLAN del túnel VXLAN anterior. El comando muestra que los paquetes de ejemplo se enrutan a través de la interfaz VXLAN VTEP.`show interfaces vtep extensive` Esto no es un verdadero muestreo de salida.

- En los conmutadores EX9200, sFlow no admite OIF (interfaz de salida) verdadero.

Los conmutadores EX9200 admiten la configuración de una sola frecuencia de muestreo (incluidas las tasas de entrada y salida) en una FPC (o tarjeta de línea). Para admitir la compatibilidad con la configuración sFlow de otros productos de Juniper Networks, los conmutadores EX9200 aún aceptan configuraciones de velocidad múltiple en diferentes interfaces de la misma FPC. Sin embargo, el conmutador programa la tasa más baja como la frecuencia de muestreo para todas las interfaces de ese FPC. El comando () muestra la velocidad configurada y la velocidad real (efectiva).`show sflow interfaces` Sin embargo, en los conmutadores EX9200 todavía se admiten diferentes velocidades en diferentes FPC.

Ejemplo: Configurar sFlow para redes EVPN-VXLAN

in this section

- Requisitos | **878**
- Descripción general y topología | **878**
- Configuración | **880**
- Verificación | **882**

Utilice este ejemplo para configurar y usar la supervisión de sFlow para el tráfico EVPN-VXLAN con una base IPv4 en QFX10000 línea de conmutadores.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador QFX10002-60C, QFX10002, QFX10008 o QFX10016.
- Junos OS versión 21.3R1, 21.2R2 y posteriores.

En este ejemplo se supone que ya tiene una EVPN-VXLAN con una red basada en base IPv4 y desea habilitar la supervisión de sFlow en un conmutador QFX10000.

Descripción general y topología

in this section

- Topología | **879**

En este ejemplo, habilita la inspección sFlow para un tráfico de red EVPN-VXLAN existente y en funcionamiento con una base IPv4.

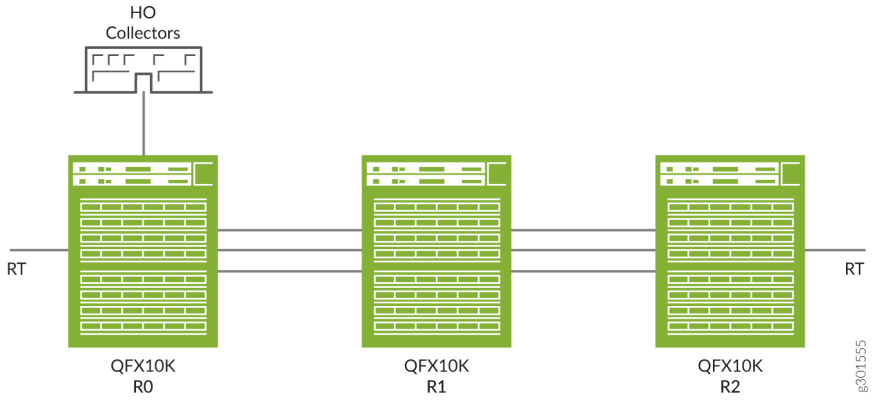
Topología

Figura 31 en la página 879 muestra la compatibilidad con sFlow en un entorno de red EVPN-VXLAN con una base IPv4. En esta topología, el agente sFlow realiza el muestreo de paquetes y recopila estadísticas de la interfaz y, a continuación, combina la información en datagramas UDP que se envían a los recopiladores sFlow. Puede conectar un recolector sFlow al conmutador a través de la red de administración o de la red de datos. El programa sFlow del conmutador busca la dirección del próximo salto para la dirección IP del recopilador especificado para determinar si se puede acceder al recopilador a través de la red de administración o de la red de datos.

Debe configurar sFlow en el puerto físico del conmutador de hardware y en la interfaz lógica donde están configurados los VTEP (puerto virtual) y no en los propios VTEP. Cuando configura sFlow en una interfaz orientada a la estructura, se muestrea el tráfico subyacente junto con el tráfico VXLAN. Puede configurar sFlow en cualquiera de los dispositivos R0, R1 o R2 mencionados en la topología.

Para obtener información sobre la configuración básica de EVPN-VXLAN, consulte Ejemplo : Configuración de un conmutador QFX10000 como puerta de enlace VXLAN de capa 3 en una superposición de puente de enrutamiento centralizado EVPN-VXLAN.

Figura 31: Soporte de sFlow en la red EVPN-VXLAN



Configuración

in this section

- Configuración rápida de CLI | 880
- Procedimiento paso a paso | 880
- Resultados | 881

Siga estos pasos para configurar la tecnología sFlow en el conmutador QFX10000 con red EVPN-VXLAN:

Configuración rápida de CLI

Para configurar rápidamente este ejemplo en el conmutador QFX10000, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía [editar].

```
[edit protocols sflow]
set polling-interval 20
set sample-rate ingress 10
set source-ip 10.1.12.0
set collector 10.102.70.200set interfaces et-0/0/1.1 sample-rate ingress 100 egress 100
```

Procedimiento paso a paso

Para configurar la tecnología sFlow:

1. Especifique en segundos la frecuencia con la que el agente sFlow sondea la interfaz:

```
[edit protocols sflow]
user@switch# set polling-interval 0
```

2. Especifique la velocidad a la que se deben muestrear los paquetes de entrada:

```
[edit protocols sflow]
user@switch# set sample-rate ingress 100
```

3. Configure la dirección IP de origen:

```
[edit protocols sflow]
user@switch# set source-ip 10.1.12.0
```

4. Configure la dirección IP del recopilador:

```
[edit protocols sflow]
user@switch# set collector 192.168.200.100
```

5. Habilite la tecnología sFlow en una interfaz específica:

```
[edit protocols sflow]
user@switch# set interfaces et-0/0/1.1 sample rate ingress 100 egress 100
```

6. Confirme su configuración:

```
[edit protocols sflow]
user@switch# commit
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch#  show protocols sflow
agent-id 10.1.12.0/24;
polling-interval 0;
sample-rate {
ingress 16000;
egress 16000;
}
```

```
collector 192.168.200.100;
interfaces et-0/0/54.1 {
sample-rate {
ingress 100;
egress 100;
}
}
interfaces et-0/0/56.0;
interfaces et-0/0/57.1 {
sample-rate {
ingress 100;
egress 100;
}
}
```

Verificación

in this section

- Verificar la tecnología sFlow configurada | **882**

Para confirmar que la configuración de sFlow está habilitada y es correcta.

Verificar la tecnología sFlow configurada

in this section

- Propósito | **882**
- Acción | **883**

Propósito

Verifique que la supervisión de sFlow esté habilitada para una red EVPN-VXLAN.

Acción

Desde el modo operativo, ingrese el comando `show protocols sflow`.

```
user@switch> show protocols sflow
sFlow                    : Enabled
Adaptive fallback        : Disabled
Sample limit             : 300 packets/second
Sample limit Threshold   : 0 packets/second
Polling interval         : 0 second
Sample rate egress       : 1:2048: Disabled
Sample rate ingress      : 1:100: Enabled
Agent ID                 : 10.1.12.0/24
Source IP address        : 10.1.12.0
```

VÍNCULOS RELACIONADOS

Descripción de la compatibilidad de servicios Ethernet flexibles con EVPN-VXLAN

No Link Title

Soporte de sFlow en enrutadores

in this section

- sFlow para encapsulación GRE | 884
- Tamaño de la muestra de sFlow | 887
- Limitaciones de sFlow en enrutadores | 887

En los enrutadores PTX1000 y conmutadores de la serie QFX10000, la tecnología sFlow siempre funciona a nivel de la interfaz física. Habilitar la supervisión de sFlow en una interfaz lógica lo habilita en todas las interfaces lógicas que pertenecen a esa interfaz física.

En enrutadores PTX1000, enrutadores PTX10000 y conmutadores serie QFX10000, solo puede configurar sFlow en una interfaz lógica activa. Utilice el comando para mostrar la información de estado

de las interfaces.`show interfaces terse` Si el estado operativo y administrativo de una interfaz está activo, entonces es una interfaz activa.

En enrutadores PTX10000, enrutadores PTX5000 y conmutadores de la serie QFX10000, sFlow no generará muestras como se esperaba cuando las interfaces de entrada o salida forman parte de una instancia de enrutamiento específicamente en el escenario ECMP.

El agente sFlow es responsable de monitorear el puerto de red, tomar muestras de todos los paquetes entrantes, incluido el tráfico de control y el tráfico que llega a todos los puertos del sistema.

La tecnología sFlow solo se admite en la línea ACX5000 de enrutadores; otros enrutadores de la serie ACX no admiten esta tecnología.

Las siguientes funciones de sFlow son compatibles con la línea ACX5000 de enrutadores:

- Muestreo basado en paquetes

  NOTA: Esta función no es compatible con ACX5448 enrutador.

- Muestreo basado en el tiempo
- Muestreo adaptativo

Las siguientes limitaciones de la tecnología sFlow se aplican en ACX5000 línea de enrutadores:

- El muestreo de entrada y salida solo se puede configurar en una de las unidades de una interfaz física y el sFlow está habilitado para la interfaz física (puerto). El sFlow no se puede habilitar si la unidad bajo una interfaz física no está configurada.
- No se admite el muestreo de salida para el tráfico de difusión, unidifusión desconocida y multidifusión (BUM) porque no se puede rellenar el campo de los datagramas sFlow.**source-interface**
- Los campos VLAN de destino y Prioridad de destino no se rellenan en el caso del reenvío de capa 3.
- El muestreo sFlow no se admite en la interfaz de salida de un analizador.
- La compatibilidad con SNMP MIB para sFlow no está disponible.
- sFlow no se puede habilitar en interfaces IRB.
- sFlow no se puede habilitar en interfaces de túnel lógico (lt-) y LSI.

sFlow para encapsulación GRE

En dispositivos PTX10001-36MR, PTX10003, PTX10004, PTX10008 y PTX10016, sFlow admite la exportación de campos de estructura de salida de túnel extendida para el tráfico que entra en túneles

GRE IPv4 o IPv6. Esto permite que sFlow proporcione información sobre el túnel GRE en el que puede encapsularse un paquete que entra en el dispositivo. El túnel GRE podría ser IPv4 o IPv6. La función solo se admite cuando sFlow está habilitado en la dirección de entrada en la que la encapsulación GRE basada en firewall ocurre en paquetes IPv4 o IPv6.

La característica es compatible con los siguientes escenarios de tráfico cuando está habilitado el muestreo de flujo de entrada:

- Tráfico IPv4 entrante que se somete a encapsulación IPv4 GRE
- Tráfico IPv6 entrante que se somete a encapsulación IPv4 GRE
- Tráfico IPv4 entrante que se somete a encapsulación IPv6 GRE
- Tráfico IPv6 entrante que se somete a encapsulación IPv6 GRE

Para obtener más información sobre las estructuras de túnel sFlow y sFlow, consulte Estructuras de túnel sFlow.https://sflow.org/sflow_tunnels.txt

No Link Title describe los campos de estructura de salida de túnel extendidos para el tráfico que entra en túneles GRE IPv4 o IPv6.

Tabla 85: Campos y valores de la estructura de salida de túnel extendido

Nombre del campo	valor
Protocolo notificado	0x2f (GRE)
IP de origen	Dirección IPv4 o IPv6 del origen del túnel
IP de destino	Dirección IPv4 o IPv6 del extremo de destino del túnel
Longitud	0
puerto de origen	0
puerto de destino	0
Indicadores TCP	0
Prioridad	0

La estructura ampliada para los túneles GRE IPv4 e IPv6 se encuentra a continuación:

```
/* opaque = flow_data; enterprise = 0; format = 1023 */

struct extended_ipv4_tunnel_egress {

    sampled_ipv4 header;

}
/* opaque = flow_data; enterprise = 0; format = 1025 */

struct extended_ipv6_tunnel_egress {

    sampled_ipv6 header;

}
```

A continuación, se muestra la estructura de encabezado IPv4 de ejemplo:

```
/* Packet IP version 4 data */
/* opaque = flow_data; enterprise = 0; format = 3 */
struct sampled_ipv4 {
   unsigned int length;     /* The length of the IP packet excluding
                               lower layer encapsulations */
   unsigned int protocol;   /* IP Protocol type
                                  (for example, TCP = 6, UDP = 17) */
   ip_v4 src_ip;            /* Source IP Address */
   ip_v4 dst_ip;            /* Destination IP Address */
   unsigned int src_port;   /* TCP/UDP source port number or equivalent */
   unsigned int dst_port;   /* TCP/UDP destination port number or equivalent
   unsigned int tcp_flags;  /* TCP flags */
   unsigned int tos;        /* IP type of service */
}
```

A continuación, se muestra la estructura de encabezado IPv6 de ejemplo:

```
/* Packet IP Version 6 Data */
/* opaque = flow_data; enterprise = 0; format = 4 */
struct sampled_ipv6 {
```

```
    unsigned int length;     /* The length of the IP packet excluding
                                lower layer encapsulations */
    unsigned int protocol;   /* IP next header
                                (for example, TCP = 6, UDP = 17) */
    ip_v6 src_ip;            /* Source IP Address */
    ip_v6 dst_ip;            /* Destination IP Address */
    unsigned int src_port;   /* TCP/UDP source port number or equivalent */
    unsigned int dst_port;   /* TCP/UDP destination port number or equivalent*/
    unsigned int tcp_flags;  /* TCP flags */
    unsigned int priority;   /* IP priority */
}
```

Tamaño de la muestra de sFlow

A partir de la versión 23.1R1 de Junos OS evolucionado para dispositivos de la serie PTX, puede configurar el tamaño de muestra sFlow del encabezado del paquete sin formato que se exportará como parte del registro sFlow al recopilador. El rango configurable de tamaño de muestra es de 128 bytes a 512 bytes. Utilice el comando para configurar el tamaño de la muestra.`set protocols sflow sample-size` *`Sample-Size`* Si el tamaño de muestra configurado es mayor que el tamaño real del paquete, se exporta el tamaño real del paquete. Si no configura el tamaño de muestra, el tamaño predeterminado del encabezado del paquete sin formato exportado al recopilador es de 128 bytes.

El tamaño de muestra configurado en la configuración global de sFlow lo heredan todas las interfaces configuradas en los protocolos sFlow.

Limitaciones de sFlow en enrutadores

En enrutadores, las limitaciones del muestreo de tráfico de sFlow incluyen las siguientes:

- El chipset Trio no puede admitir diferentes frecuencias de muestreo para cada familia. Por lo tanto, solo se puede admitir una frecuencia de muestreo por tarjeta de línea.
- El muestreo de equilibrio de carga adaptable se aplica por tarjeta de línea y no por interfaz debajo de la tarjeta de línea.

Los enrutadores admiten la configuración de una sola frecuencia de muestreo (incluidas las tasas de entrada y salida) en una tarjeta de línea. Para admitir la compatibilidad con la configuración sFlow de otros productos de Juniper Networks, los enrutadores aún aceptan configuraciones de velocidad múltiple en diferentes interfaces de la misma tarjeta de línea. Sin embargo, el enrutador programa la tasa más baja como la frecuencia de muestreo para todas las interfaces de esa tarjeta de línea. El comando () muestra la velocidad configurada y la velocidad real (efectiva).`show sflow interfaces` Sin embargo, los enrutadores de Juniper Networks todavía admiten diferentes velocidades en diferentes tarjetas de línea.

En Junos OS Evolved, solo puede configurar sFlow en interfaces Ethernet () para los siguientes dispositivos de la serie PTX:`et-*`

- PTX10003-80C y PTX10003-160C
- PTX10008
- PTX10001-36MR
- PTX10004
- PTX10016

No puede configurar sFlow en interfaces de circuito cerrado ().`lo0`

Ejemplo: Configurar la tecnología sFlow para monitorear el tráfico de red

in this section

- Requisitos | 888
- Topología | 889
- Configuración | 890
- Verificación | 892

En este ejemplo se describe cómo configurar y usar la tecnología sFlow para supervisar el tráfico de red.

Requisitos

Puede usar dispositivos de las series QFX, EX, PTX y MX para el ejemplo mediante los siguientes componentes de hardware y software:

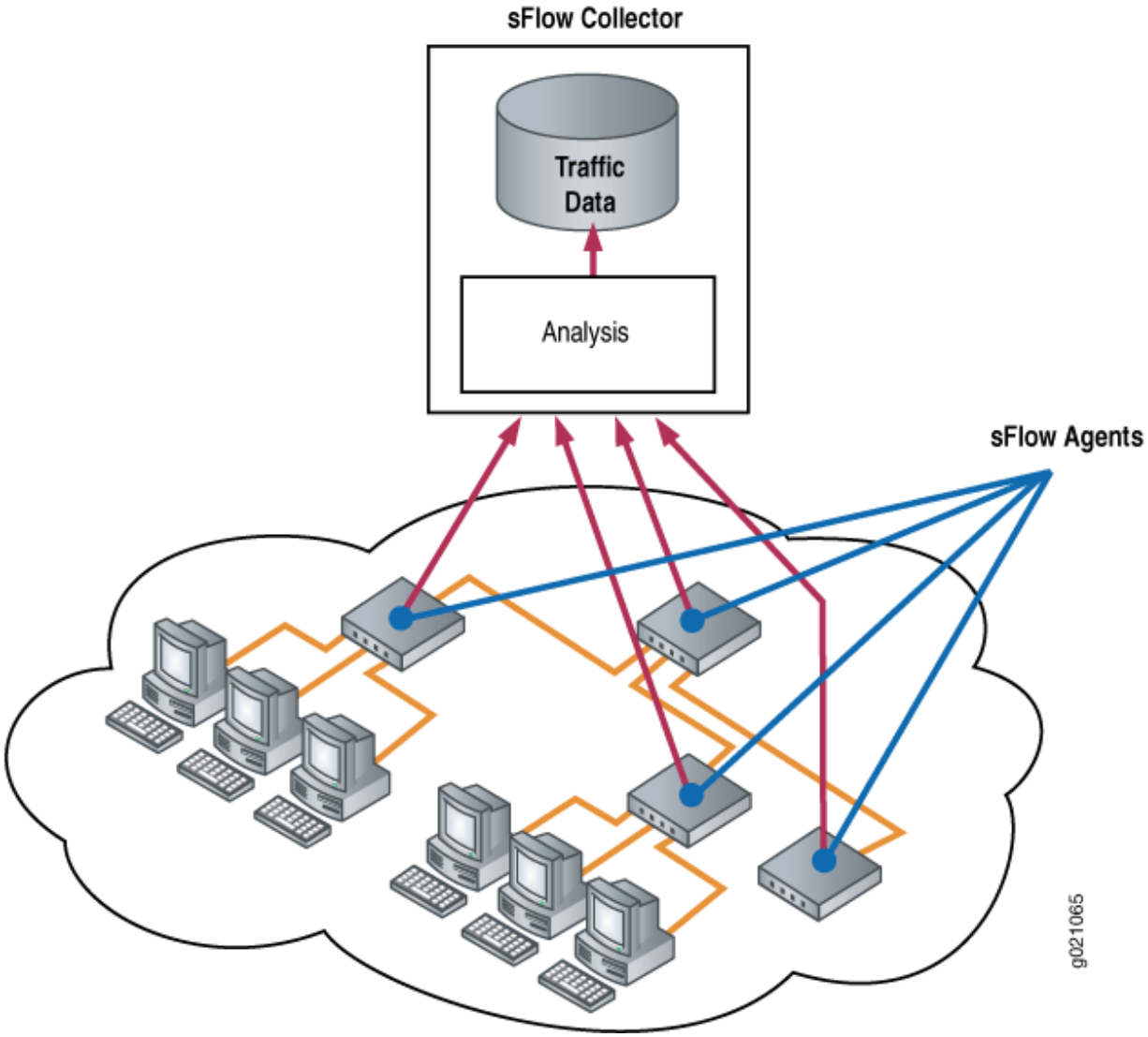
- Un conmutador de la serie EX
- Junos OS versión 9.3 o posterior para conmutadores serie EX
- Un enrutador serie MX
- Junos OS versión 18.1 o posterior para enrutadores serie MX
- Junos OS versión 11.3 o posterior

- Un conmutador QFX3500

Topología

El agente sFlow se ejecuta en el conmutador. Combina contadores de interfaz y muestras de flujo y los envía a través de la red al recopilador sFlow. representa los elementos básicos del sistema sFlow.Figura 32 en la página 889

Figura 32: Sistema de monitoreo de tecnología sFlow



Configuración

in this section

- Configuración rápida de CLI | 890
- Procedimiento | 890

Para configurar la tecnología sFlow, realice las siguientes tareas:

Configuración rápida de CLI

Para configurar rápidamente la tecnología sFlow, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

```
[edit protocols]
set sflow collector 10.204.32.46 udp-port 5600
set sflow interfaces ge-0/0/0
set sflow polling-interval 20
set sflow sample-rate egress 1000
```

Procedimiento

Procedimiento paso a paso

Para configurar la tecnología sFlow:

1. Configure la dirección IP y el puerto UDP del recopilador:

```
[edit protocols]
user@switch# set sflow collector 10.204.32.46 udp-port 5600
```

> **NOTA**: Puede configurar un máximo de 4 recopiladores.
> El puerto UDP predeterminado es 6343.

2. Habilite la tecnología sFlow en una interfaz específica:

```
[edit protocols sflow]
user@switch# set interfaces ge-0/0/0
```

NOTA: No puede habilitar la tecnología sFlow en una interfaz etiquetada por VLAN de capa 3.

3. Especifique en segundos la frecuencia con la que el agente sFlow sondea la interfaz:

```
[edit protocols sflow]
user@switch# set polling-interval 20
```

NOTA: El intervalo de sondeo también se puede especificar como un parámetro global. Especifique si no desea sondear la interfaz.**0**

4. Especifique la velocidad a la que se deben muestrear los paquetes de salida:

```
[edit protocols sflow]
user@switch# set sample-rate egress 1000
```

NOTA: Puede especificar frecuencias de muestreo de entrada y salida. Si solo establece la frecuencia de muestreo, la frecuencia de muestreo se deshabilitará.**egressingress**

NOTA: Se recomienda configurar las mismas frecuencias de muestreo en todos los puertos de una tarjeta de línea. Si configura diferentes frecuencias de muestreo diferentes, se utilizará el valor más bajo para todos los puertos. Aún puede configurar diferentes tarifas en diferentes tarjetas de línea.

5. (Opcional) Especifique el tamaño de muestra para el encabezado del paquete sin formato. La configuración del tamaño de muestra se aplica en dispositivos PTX10003-80C, PTX10003-160C, PTX10001-36MR, PTX10004, PTX10008 y PTX10016 de la versión 23.1R1 Junos OS Evolved.

```
[edit protocols sflow]
user@switch# set sample-size 135
```

Resultados

Compruebe los resultados de la configuración:

```
[edit protocols sflow]
user@switch# show

polling-interval 20;
    sample-rate egress 1000;
    collector 10.204.32.46 {
        udp-port 5600;
    }
interfaces ge-0/0/0.0;
```

```
[edit protocols sflow]
user@router# show
polling-interval 20;
source-ip 45.1.1.1;
collector 45.1.1.100;
sample-size 135;
```

Verificación

in this section

- Verificar que la tecnología sFlow esté configurada correctamente | 893
- Verificación de que la tecnología sFlow esté habilitada en la interfaz especificada | 894
- Verificación de la configuración del recopilador sFlow | 894

Para confirmar que la configuración es correcta, realice estas tareas:

Verificar que la tecnología sFlow esté configurada correctamente

Propósito

Verifique que la tecnología sFlow esté configurada correctamente.

Acción

Utilice el comando:`show sflow`

```
user@switch> show sflow
sFlow: Enabled
Sample limit: 300 packets/second
Polling interval: 20 seconds
Sample rate egress: 1:1000: Enabled
Sample rate ingress: 1:2048: Disabled
Agent ID: 10.204.96.222
```

```
user@router> show sflow
sFlow                   : Enabled
Adaptive fallback       : False
Sample limit            : 2000 packets/second
Sample limit Threshold  : 0 packets/second
Polling interval        : 20 second
Sample rate egress      : 1:2048:Disabled
Sample rate ingress     : 1:2048:Disabled
Agent ID                : 10.204.96.222
Agent ID IPv6           : No valid agent IPv6
Source IP address       : 45.1.1.1
Source IPv6 address     : No valid source IPv6
Sample Size             : 128 Bytes
```

NOTA: El límite de muestreo no se puede configurar y se establece en 300 paquetes/segundo por FPC.

Significado

El resultado muestra que la tecnología sFlow está habilitada y especifica los valores para el límite de muestreo, el intervalo de sondeo y la frecuencia de muestreo de salida.

Verificación de que la tecnología sFlow esté habilitada en la interfaz especificada

Propósito

Compruebe que la tecnología sFlow esté habilitada en las interfaces especificadas y muestre los parámetros de muestreo.

Acción

Utilice el comando:`show sflow interface`

```
user@switch> show sflow interface
Interface        Status      Sample rate    Adapted sample rate   Polling-interval
            Egress Ingress   Egress Ingress   Egress Ingress
ge-0/0/0.0  Enabled  Disabled  1000    2048    1000     2048            20
```

Significado

El resultado indica que la tecnología sFlow está habilitada en la interfaz ge-0/0/0.0 con una frecuencia de muestreo de salida de 1000, una frecuencia de muestreo de entrada deshabilitada y un intervalo de sondeo de 20 segundos.

Verificación de la configuración del recopilador sFlow

Propósito

Compruebe la configuración del recolector sFlow.

Acción

Utilice el comando:`show sflow collector`

```
user@switch> show sflow collector

Collector         Udp-port    No. of samples
```

```
 address
10.204.32.46      5600        1000
10.204.32.76      3400        1000
```

```
user@router> show sflow collector
Collector                                   Udp-port    Dscp     Forwarding-Class
No. of samples
 address
45.1.1.100                                  6343        0        best-effort                    0
```

Significado

El resultado muestra la dirección IP de los recopiladores y los puertos UDP. También muestra el número de muestras.

Asignación de direcciones del agente de sFlow

El recopilador sFlow utiliza la dirección IP del agente sFlow para determinar el origen de los datos de sFlow. Puede configurar la dirección IP del agente sFlow para asegurarse de que el ID del agente de sFlow permanece constante. Si no especifica la dirección IP que se asignará al agente, se asignará automáticamente una dirección IP al agente según el siguiente orden de prioridad de las interfaces configuradas en el dispositivo:

Tabla 86: Interfaces en los dispositivos

Enrutadores y conmutadores de la serie EX	Dispositivos de la serie QFX
1. Interfaz Ethernet de administración virtual (VME) 2. Interfaz Ethernet de administración	1. Dirección IP em0 de interfaz Ethernet de administración 2. Cualquier interfaz de capa 3 si la dirección IP em0 no está disponible

Si no se ha configurado ninguna de las interfaces anteriores, se asigna al agente la dirección IP de cualquier interfaz de capa 3 o la interfaz VLAN enrutada (RVI). Se debe configurar al menos una interfaz en el conmutador para que se asigne automáticamente una dirección IP al agente. Cuando la dirección IP del agente se asigna automáticamente, la dirección IP es dinámica y cambia cuando se reinicia el conmutador.

Los datos de sFlow se pueden utilizar para proporcionar información de visibilidad del tráfico de red. Puede configurar explícitamente la dirección IP que se asignará a los datos de origen (datagramas sFlow). Si no configura explícitamente esa dirección, se utilizará como dirección IP de origen la dirección IP de la interfaz de Gigabit Ethernet configurada, la interfaz de 10 Gigabit Ethernet o la RVI.

chapter label in part10

Muestreo adaptable para enrutadores y conmutadores

in this chapter

- Descripción general del muestreo adaptativo | 897

Descripción general del muestreo adaptativo

in this section

- Cómo funciona el muestreo adaptativo | 899
- Respaldo de muestreo adaptativo | 900
- Limitaciones del muestreo adaptativo | 900

El muestreo adaptativo es el proceso de supervisar la tasa general de tráfico entrante en el dispositivo de red y proporcionar retroalimentación inteligente a las interfaces para adaptar dinámicamente las frecuencias de *muestreo* en las interfaces en función de las condiciones del tráfico. El muestreo adaptativo evita que la CPU se sobrecargue y mantiene el sistema en un nivel óptimo, incluso cuando los patrones de tráfico cambian en las interfaces. Mientras que la frecuencia de muestreo es el número configurado de paquetes de salida o entrada de los cuales se muestrea un paquete, la frecuencia de muestreo adaptativa es el número máximo de muestras que se deben generar por tarjeta de línea, es decir, es el límite dado al *muestreo* adaptativo. La carga de muestra es la cantidad de datos (o número de paquetes) que se mueven a través de una red en un momento dado en el que se muestrea. A medida que aumenta la frecuencia de muestreo, disminuye la carga de muestra y viceversa. Por ejemplo, supongamos que la frecuencia de muestreo configurada es 2 (lo que significa que se muestrea 1 paquete de cada 2 paquetes) y luego esa velocidad se duplica, lo que la convierte en 4 o solo se muestrea 1 paquete de cada 4 paquetes.

La frecuencia de muestreo adaptable se configura, que es el número máximo de muestras que deben generarse por tarjeta de línea, en el nivel de jerarquía.`[edit protocols sflow adaptive-sample-rate]`

Para garantizar la precisión y eficiencia del muestreo, los dispositivos de la serie QFX utilizan el muestreo adaptativo sFlow. El muestreo adaptativo supervisa la tasa general de tráfico entrante en el dispositivo y proporciona información a las interfaces para adaptar dinámicamente su frecuencia de muestreo a las condiciones del tráfico. El agente sFlow lee las estadísticas de las interfaces cada 5 segundos e identifica cinco interfaces con el mayor número de muestras. En un conmutador independiente, cuando se alcanza el límite de procesamiento de la CPU, se implementa un algoritmo de retroceso binario para reducir a la mitad la carga de muestreo de las cinco interfaces principales. La frecuencia de muestreo adaptada se aplica a esas cinco interfaces principales.

El uso del muestreo adaptativo evita la sobrecarga de la CPU y mantiene el dispositivo funcionando a su nivel óptimo incluso cuando hay un cambio en los patrones de tráfico en las interfaces. La carga de muestreo reducida se utiliza hasta:

- Reinicie el dispositivo.
- Configure una nueva frecuencia de muestreo.
- La función de reserva de muestreo adaptable, si está configurada, aumenta la carga de muestreo porque el número de muestras generadas es inferior al umbral configurado.

Si no se configura una interfaz determinada, la dirección IP de la siguiente interfaz de la lista de prioridades se utiliza como dirección IP del agente. Una vez asignada una dirección IP al agente, el ID del agente no se modifica hasta que se reinicia el servicio sFlow. Se debe configurar al menos una interfaz para que se asigne una dirección IP al agente.

Consideraciones

En la serie QFX, las limitaciones del muestreo de tráfico sFlow incluyen:

- El muestreo de sFlow en las interfaces de entrada no captura el tráfico vinculado a la CPU.
- El muestreo de sFlow en interfaces de salida no admite paquetes de difusión ni multidifusión.
- Los ejemplos de salida no contienen modificaciones realizadas en el paquete en la canalización de salida.
- Si un paquete se descarta debido a un filtro de firewall, el código de motivo para descartar el paquete no se envía al recopilador.
- El campo para una VLAN siempre se establece en 0 (cero) en las muestras de entrada y salida.`out-priority`
- No puede configurar la supervisión de sFlow en un grupo de agregación de vínculos (LAG), pero puede configurarla individualmente en una interfaz miembro del LAG.

- En los conmutadores serie QFX10000, para un conjunto de puertos de un grupo de multidifusión, dado que el muestreo real ocurre en la canalización de entrada para paquetes de salida, se usa el mínimo de la velocidad sFlow configurada o la frecuencia de muestreo más agresiva entre esos puertos para el muestreo en todos los puertos de ese grupo.

- A partir de Junos OS versión 19.4 y posteriores, en conmutadores serie QFX10000, si el puerto de destino de un paquete UDP muestreado es 6635 y el paquete no incluye un encabezado MPLS válido, el paquete muestreado de flujo se corrompe o se trunca. Se reenvía el paquete real.

- En los conmutadores independientes de la serie QFX10000 y el chasis virtual de la serie QFX (con conmutadores QFX3500 y QFX3600), los filtros de firewall de salida no se aplican a los paquetes de muestreo sFlow. En estas plataformas, la arquitectura del software es diferente a la de otros dispositivos de la serie QFX, y los paquetes sFlow son enviados por el motor de enrutamiento (no por la tarjeta de línea en el host) y no transitan por el conmutador. Los filtros de firewall de salida afectan a los paquetes de datos que transitan por un conmutador, pero no afectan a los paquetes enviados por el motor de enrutamiento. Como resultado, los paquetes de muestreo sFlow siempre se envían al recopilador sFlow.

Cómo funciona el muestreo adaptativo

Cada pocos segundos, o ciclo, el agente sFlow recopila las estadísticas de la interfaz. A partir de estas estadísticas agregadas, se calcula un número promedio de muestras por segundo para el ciclo. La duración del ciclo depende de la plataforma:

- Cada 12 segundos para conmutadores serie EX y QFX5K y enrutadores serie MX y PTX

- Cada 5 segundos para conmutadores de la serie QFX que no sean QFX5K

Si la frecuencia de muestreo combinada de todas las interfaces de una tarjeta de línea supera la frecuencia de muestreo adaptable, se inicia un algoritmo de retroceso binario, lo que reduce la carga de muestreo en las interfaces. El muestreo adaptativo duplica la frecuencia de muestreo en las interfaces afectadas, lo que reduce la carga de muestreo a la mitad. Este proceso se repite hasta que la carga de la CPU debido a sFlow en una tarjeta de línea determinada se reduce a un nivel aceptable.

Las interfaces de una tarjeta de línea que participan en el muestreo adaptable dependen de la plataforma:

- Para los enrutadores de la serie MX y los conmutadores de la serie EX, se adaptan las frecuencias de muestreo en todas las interfaces de la tarjeta de línea.

- Para los enrutadores de la serie PTX y los conmutadores de la serie QFX, solo se adaptan las cinco interfaces con las frecuencias de muestreo más altas en la tarjeta de línea.

Para todas las plataformas, el aumento de las tasas de muestreo permanece vigente hasta que se cumpla una de las siguientes condiciones:

- El dispositivo se reinicia.
- Se configura una nueva frecuencia de muestreo.

Si ha habilitado la función de reserva de muestreo adaptativo y, debido a un pico de tráfico, el número de muestras aumenta al umbral de límite de muestra configurado, la frecuencia de muestreo adaptativa se invierte.

Respaldo de muestreo adaptativo

La función de reserva de muestreo adaptativo, cuando se configura y después de que se haya realizado el muestreo adaptativo, utiliza un algoritmo de copia de seguridad binario para disminuir la frecuencia de muestreo (aumentando así la carga de muestreo) cuando el número de muestras generadas es menor que el valor configurado , sin afectar al tráfico normal.`sample-limit-threshold`

A partir de la versión 18.3R1 de Junos OS, para los conmutadores de la serie EX, Junos OS admite la función de reserva de muestreo adaptable. A partir de la versión 19.1R1 de Junos OS, para dispositivos de las series MX, PTX y QFX, Junos OS admite la función de reserva de muestreo adaptable.

La reserva de muestreo adaptable está deshabilitada de forma predeterminada. Para habilitar esta característica, incluya las opciones y en el nivel de jerarquía.`fallbackadaptive-sample-rate` *`sample-limit-threshold`*`[edit protocols sflow adaptive-sample-rate]`

Después de que se ha llevado a cabo el muestreo adaptativo y la tarjeta de línea tiene un rendimiento inferior (es decir, el número de muestras generadas en un ciclo es menor que el valor configurado para la instrucción), para cinco ciclos continuos de muestreo adaptativo, la velocidad adaptada se invierte.`sample-limit-threshold` Si se ha producido la adaptación inversa y el número de muestras generadas en un ciclo es inferior a la mitad de la tasa adaptada actual de nuevo (y, por lo tanto, para cinco ciclos continuos), puede ocurrir otra adaptación inversa.

La adaptación inversa no se produce si las interfaces ya están a la velocidad configurada.

Limitaciones del muestreo adaptativo

Las siguientes son limitaciones de la característica de ejemplo adaptable:

- En enrutadores independientes o conmutadores independientes de la serie QFX, si configura sFlow en varias interfaces y con una frecuencia de muestreo alta, se recomienda especificar un recopilador que esté en la red de datos en lugar de en la red de administración. Tener un alto volumen de tráfico sFlow en la red de administración puede interferir con otro tráfico de la interfaz de administración.
- En los enrutadores, sFlow no admite un reinicio correcto. Cuando se produce un reinicio correcto, la frecuencia de muestreo adaptable se establece en la frecuencia de muestreo configurada por el usuario.

- En una tarjeta de línea seleccionable por velocidad (que admite varias velocidades), se seleccionan las interfaces con el recuento de muestras más alto para la reserva de muestreo adaptativo. El algoritmo de copia de seguridad selecciona aquellas interfaces en las que la frecuencia de muestreo adaptable aumenta el número máximo de veces y, a continuación, disminuye la frecuencia de muestreo en cada una de esas interfaces cada cinco segundos. Sin embargo, en una tarjeta de línea de velocidad única, solo se admite una frecuencia de muestreo por tarjeta de línea, y el mecanismo de reserva de muestreo adaptativo realiza una copia de seguridad de la frecuencia de muestreo en todas las interfaces de la tarjeta de línea.

chapter label in part11

Software de diagnóstico del acelerador de flujo de paquetes

in this chapter

- Descripción general del software de diagnóstico del acelerador de flujo de paquetes y otras utilidades | 902
- Instalar scripts Ethernet y PTP | 938
- Instalar el software de diagnóstico del acelerador de flujo de paquetes | 941

Descripción general del software de diagnóstico del acelerador de flujo de paquetes y otras utilidades

in this section

- Puertos externos e internos y puertos de tarjeta de interfaz de red | 903
- Acelerador de flujo de paquetes Pruebas y scripts de software de diagnóstico | 905
- Comando Ikondiag | 906
- Pruebas de funcionalidad básica | 907
- Pruebas y scripts de Ethernet | 911
- Pruebas de esfuerzo | 918
- Pruebas de PTP | 919
- Pruebas LED del módulo QFX-PFA-4Q | 922
- Utilidades de diagnóstico del acelerador de flujo de paquetes | 924
- Resultado de ejemplo para el software de diagnóstico del acelerador de paquetes | 930

Puede utilizar el software de diagnóstico del acelerador de flujo de paquetes para validar la integridad del módulo QFX-PFA-4Q y del conmutador QFX5100-24Q-AA. El software de diagnóstico del acelerador de flujo de paquetes contiene diagnósticos estándar, diagnósticos de orquestación, protocolo de tiempo de precisión (PTP) y diagnósticos de sincronización, y otras utilidades. El software de diagnóstico del acelerador de flujo de paquetes se ejecuta en una máquina virtual (VM) invitada en el conmutador QFX5100-24Q-AA y requiere que configure las opciones de la máquina virtual invitada en la CLI de Junos OS.

El módulo QFX-PFA-4Q contiene cuatro interfaces QSFP+ de 40 Gigabit Ethernet, un módulo FPGA e interfaces de entrada y salida de temporización para admitir aplicaciones de Protocolo de tiempo de precisión. El módulo FPGA contiene lógica que puede personalizar para procesar transacciones de alto volumen y con un uso intensivo de la latencia.

Antes de poder ejecutar el software y las utilidades de Packet Flow Accelerator Diagnostics, asegúrese de haber realizado las siguientes tareas:

- Verifique que haya instalado el módulo QFX-PFA-4Q instalado en el conmutador QFX5100-24Q-AA. Para obtener más información, consulte Instalación de un módulo de expansión en un dispositivo QFX5100

- Asegúrese de tener instalado Junos OS versión 14.1X53-D27 con automatización mejorada en el conmutador QFX5100-24Q-AA. Para obtener más información, consulte Instalación de paquetes de software en dispositivos de la serie QFX.*Installing Software on QFX Series Devices*

- Instale el software Packet Flow Accelerator Diagnostics. Para obtener más información, consulte No Link Title.

Puertos externos e internos y puertos de tarjeta de interfaz de red

El software y las utilidades de Packet Flow Accelerator Diagnostics validan las rutas de datos entre los puertos externo e interno en el conmutador QFX5100-24Q-AA y el módulo QFX-PFA-4Q. ilustra los nombres de los puertos del conmutador QFX5100-24Q-AA y del módulo QFX-PFA-4Q y cómo se conectan.Figura 33 en la página 904

Figura 33: Puertos en el conmutador QFX5100-24Q-AA y en el módulo QFX-PFA-4Q

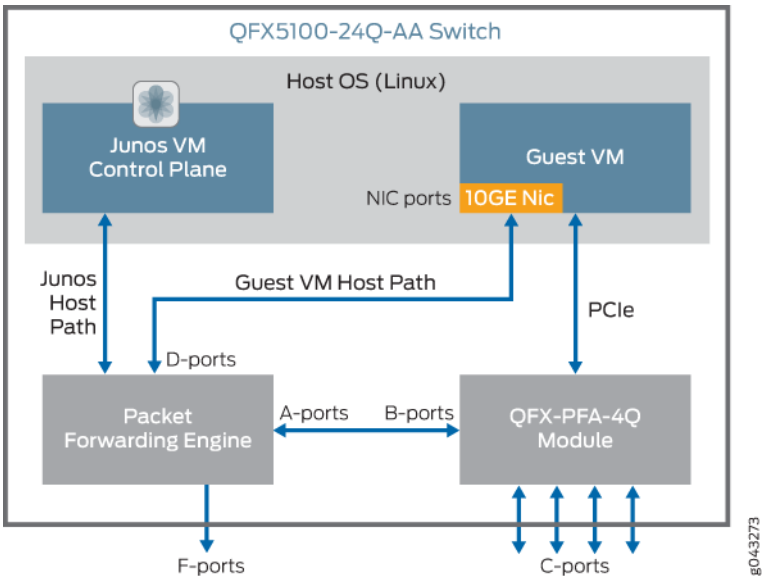


Tabla 87 en la página 904 proporciona información sobre los puertos externos e internos, así como sobre los puertos NIC del conmutador QFX5100-24Q-AA y del módulo QFX-PFA-4Q.

Tabla 87: Puertos externos e internos en el conmutador QFX5100-24Q-AA y el módulo QFX-PFA-4Q

Puertos A	Las interfaces xe-0/0/24 a xe-0/0/39 en el motor de reenvío de paquetes (PFE) del conmutador QFX5100-24Q-AA se conectan a los puertos B del módulo FPGA del módulo de expansión QFX-PFA-4Q. Los puertos A requieren los puertos B correspondientes en el módulo FPGA. Puede administrar estas interfaces a través de Junos OS.
Puertos B	Los puertos internos de 10 Gigabit Ethernet se conectan al módulo FPGA del módulo QFX-PFA-4Q, que luego se conecta a los puertos A del PFE del conmutador QFX5100-24Q-AA. La convención de nomenclatura para estos puertos viene determinada por la máquina virtual invitada. La máquina virtual invitada controla el módulo FPGA.
Puertos C	Cuatro puertos frontales de 40 Gigabit Ethernet del módulo QFX-PFA-4Q se conectan al módulo FPGA que se ejecuta en el conmutador QFX5100-24Q-AA y a los puertos F del conmutador QFX5100-24Q-AA. La máquina virtual invitada controla el módulo FPGA.
Puertos D	Dos puertos internos Ethernet de 10 Gigabit en el motor de reenvío de paquetes del conmutador QFX5100-24Q-AA se conectan a la NIC Ethernet en el conmutador QFX5100-24Q-AA. La convención de nomenclatura para estos puertos es la misma que se utiliza para los puertos F. Puede administrar estos puertos a través de Junos OS.

Puertos F	Veinticuatro puertos frontales de 40 Gigabit Ethernet en el conmutador QFX5100-24Q-AA. Estos puertos contienen un prefijo "et" cuando están en modo 40 Gigabit Ethernet. Si canaliza estas interfaces, el prefijo es "xe". Puede administrar estos puertos a través de Junos OS.
Puertos NIC	Las interfaces internas xe-0/0/40 y xe-0/0/41 en el conmutador QFX5100-24Q-AA se conectan al PFE para su uso en la máquina virtual invitada. Los puertos NIC realizan las mismas funciones que cualquier otro puerto NIC del sistema operativo Linux. Los puertos NIC no funcionan a menos que esté instalado el módulo QFX-PFA-4Q.

Acelerador de flujo de paquetes Pruebas y scripts de software de diagnóstico

Puede ejecutar el software de diagnóstico del acelerador de flujo de paquetes para probar los siguientes subsistemas en el módulo QFX-PFA-4Q:

- FPGA
- Memoria QDR SRAM
- Memoria DRAM
- SPD de DRAM
- Vínculos PCI Express conectados a FPGA
- Datos Ethernet conectados a FPGA (interfaces QSFP)
- E/S QSFP I2C
- E/S PTP

Antes de poder ejecutar cualquier prueba o script, debe conectarse a la conexión de consola de la máquina virtual invitada. .

Están disponibles los siguientes conjuntos de pruebas:

- prueba rápida: le permite realizar una prueba básica de todas las funciones asociadas a FPGA. Estas pruebas tardan uno o dos minutos en completarse.
- burn-in: le permite ejercer toda la funcionalidad adjunta a FPGA. Estas pruebas tardan varias horas en completarse.
- modo de prueba individual: permite probar un único subsistema con opciones de configuración adicionales.

Comando Ikondiag

Para ejecutar cualquiera de las pruebas, emita el comando con los siguientes argumentos:**ikondiag**

> **NOTA**: Antes de poder ejecutar las pruebas, debe conectarse a la conexión de consola de la máquina virtual invitada.

- -t (prueba rápida | quemado | <nombre de la prueba>)

  Este argumento identifica la prueba.

- -H

  Este argumento proporciona detalles de uso para la prueba.

- -V

  Este argumento proporciona resultados detallados para las pruebas.

Por ejemplo, para ejecutar la prueba PTP, ejecute el comando ikondiag -t PTP en el símbolo de la máquina virtual invitada:

ikondiag -t PTP

```
[2015-05-07 03:12:20][BEGIN TEST -
PTP]


**********************************************************************

PTP PHY interrupt:
PASS

1G Ethernet PHY packet loopback test:
PASS

PTP clock generation/check:
PASS

UART (ToD) loopback:
PASS

**********************************************************************
```

```
[2015-05-07 03:13:30][END TEST PTP RESULT
PASS]
```

Pruebas de funcionalidad básica

Puede probar la funcionalidad básica en la interfaz PCI Express y los componentes de memoria. enumera los nombres de las pruebas y sus funciones.Tabla 88 en la página 907

Tabla 88: Pruebas básicas

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
FPGABasic	Prueba el funcionamiento básico de FPGA.	Configura la FPGA y lee algunos registros simples a través de PCI Express.	Ninguno.	Prueba rápida y quemado	Cualquier error en esta prueba hace que el comando genere mensajes de error y estado de prueba normales y, a continuación, finalice con otro mensaje de error.**ikondiag** No puede continuar con las pruebas porque todas las pruebas dependen de la funcionalidad probada por esta.

Tabla 88: Pruebas básicas *(Continued)*

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
Pcie	Verifica la funcionalidad y estabilidad de las transferencias masivas de datos PCIe.	Devuelve repetidamente los datos pseudoaleatorios generados en la CPU a la FPGA y luego de vuelta a la CPU. Los datos devueltos se verifican en la CPU.	-i <n> número de repeticiones (por defecto = 1 prueba rápida, 10.000 quemados) -j <n> tamaño de la transferencia individual en Mebibytes (valor predeterminado = 100 MiB).	Prueba rápida y quemado	Esta prueba notifica valores de datos erróneos y desplazamientos en la transferencia de datos. Cualquier error en esta prueba hará que el comando ikondiag genere mensajes de error y estado de prueba normales y luego terminará con un error adicional. No puede continuar con las pruebas adicionales porque todas las pruebas dependen de la funcionalidad probada por esta prueba.

Tabla 88: Pruebas básicas *(Continued)*

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
DIMM	Comprueba la funcionalidad de consulta SPD y comprueba que están instalados los DIMM correctos.	Lee datos del dispositivo SPD en módulos DIMM, informa del contenido y comprueba si hay valores erróneos y verifica: • Datos de piezas DIMM contra datos de piezas esperados. • La temperatura SPD está en el rango nominal de funcionamiento.	Ninguno.	Prueba rápida y quemado	Si algún valor es inesperado, la prueba informa de valores erróneos y proporciona valores y rangos esperados.

Tabla 88: Pruebas básicas *(Continued)*

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error

DRAMMemory	Prueba la funcionalidad de transferencia de datos y la estabilidad de los dispositivos de memoria DRAM conectados a FPGA.	• Comprueba que las PHY se inicialicen correctamente.
		• Realiza repetidamente las siguientes tareas:
		  • Escribe en memoria desde la FPGA
		  • Cada pasada cambia los datos entre: ceros, unos, contador, aleatorio, ceros, aleatorio, unos, aleatorio.
		  • Bucle de memoria dentro de la FPGA (lecturas y escrituras simultáneas).
		  • Verifica la memoria de la FPGA
			-i <n> varía el número de iteraciones) predeterminado = 1 para prueba rápida, 500 para burn-in)	Prueba rápida y quemado	Esta prueba informa el número de errores durante la verificación. El número de errores se especifica como un número acumulado de errores por byte-lane y módulo DIMM.

Pruebas y scripts de Ethernet

Las pruebas y scripts de Ethernet prueban los puertos C y el tráfico entre los puertos A y B. El tráfico entre los puertos A y B se prueba pasando los datos en los puertos F. Para los puertos C, debe retroceder el tráfico enviado en los puertos C. Puede utilizar cables de bucle invertido de cobre físicos para este propósito. Para los puertos F, , debe retroceder el tráfico enviado en los puertos F. Puede utilizar cables de bucle invertido de cobre para este propósito. Incluya los puertos F en una VLAN. Puede usar el script python PFAD_exec.py -t 1, así como las pruebas a continuación. El script python PFAD_exec.py -t 1 verifica el tráfico L2 de extremo a extremo en los puertos QSFP externos y comprueba las estadísticas de las interfaces de Junos OS y las estadísticas de las interfaces de la máquina virtual del software Packet Flow Diagnostics. Esta prueba fallará si se observa pérdida de tráfico en cualquiera de las interfaces. También hay una disposición para probar todas las combinaciones de puertos QSFP.

Tabla 89 en la página 911 enumera los nombres de las pruebas de Ethernet y sus funciones. Para obtener información acerca de cómo instalar la secuencia de comandos, consulte .No Link Title

Tabla 89: Pruebas y scripts de Ethernet

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
QSFPEthernet	Comprueba la funcionalidad de los vínculos Ethernet (QSFP).	Genera, recibe y verifica que las tramas Ethernet tengan velocidad de línea a través del módulo FPGA. El contenido y la longitud de los paquetes consisten en datos pseudoaleatorios. Durante el funcionamiento, todas las conexiones QSFP se canalizan para utilizar 10 Gigabit Ethernet con los 32 canales Ethernet funcionando en paralelo en modo dúplex completo.	-i <n> número variado de iteraciones (valor predeterminado = 1.000 para prueba rápida, 1e9 para burn-in)	Prueba rápida y quemado	Si se verifica que el número de paquetes enviados o recibidos correctamente no es igual, esta prueba se considera un fallo y se informan las discrepancias entre estas cantidades. Esta prueba falla si las conexiones Ethernet externas no están configuradas para circuito cerrado.

Tabla 89: Pruebas y scripts de Ethernet *(Continued)*

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
QSFPI2C	Comprueba si hay acceso a los cuatro módulos QSFP situados en la parte frontal del módulo QFX-PFA-4Q.	Realiza lecturas de registros en los módulos I2C y verifica que los resultados sean los esperados. Para que esta prueba sea aprobada, los medios QSFP deben insertarse en los cuatro puertos del módulo QFX-PFA-4Q. Se puede utilizar cualquier tipo de medio externo (por ejemplo, cables DAC, bucle invertido de cobre, módulos y módulos ópticos).	Ninguno.	Prueba rápida y quemado	Esta prueba falla si no puede detectar la presencia de un módulo QSFP o si los valores que lee son inesperados.

Antes de poder ejecutar correctamente las pruebas y secuencias de comandos de Ethernet, debe realizar las siguientes tareas:

- Realice un bucle externo de todas las conexiones Ethernet (QSFP) en el módulo QFX-PFA-4Q.

  Para retroceder las interfaces QSFP en el módulo QFX-PFA-4Q, conecte módulos de bucle invertido de cobre en las cuatro interfaces QSFP+ instaladas en el módulo QFX-PFA-4Q.

  Conecte módulos de bucle invertido de cobre en las interfaces QSFP+ (puertos 10 a 13) instaladas en el conmutador QFX5100-24Q-AA.

- Canalizar los puertos 10 a 13 en el conmutador QFX5100-24Q-AA.

- Empareje cada uno de los 16 carriles ikonDiag utilizando los nombres de interfaz Junos OS equivalentes con cada una de las interfaces Junos OS correspondientes que se canalizaron desde los puertos 10 a 13 del conmutador QFX5100-24Q-AA.

> **NOTA**: Cada VLAN debe ser independiente y contener exactamente dos puertos asociados: un puerto 10 Gigabit Ethernet que es un puerto F y un puerto 10 Gigabit Ethernet que es un puerto A.

Tabla 90 en la página 913 muestra las asignaciones para los canales de 10 Gigabit Ethernet en los puertos F del módulo QFX-PFA-4Q.

Tabla 90: Mapeos de canal Ethernet de 10 Gigabit en los puertos F del módulo QFX-PFA-4Q

ikondiag Nombres	Description
JDFE_XE32_10G	xe-0/0/32
JDFE_XE33_10G	xe-0/0/33
JDFE_XE34_10G	xe-0/0/34
JDFE_XE35_10G	xe-0/0/35
JDFE_XE24_10G	xe-0/0/24
JDFE_XE25_10G	xe-0/0/25
JDFE_XE26_10G	xe-0/0/26
JDFE_XE27_10G	xe-0/0/27
JDFE_XE28_10G	xe-0/0/28
JDFE_XE29_10G	xe-0/0/29
JDFE_XE30_10G	xe-0/0/30
JDFE_XE31_10G	xe-0/0/31

Tabla 90: Mapeos de canal Ethernet de 10 Gigabit en los puertos F del módulo QFX-PFA-4Q *(Continued)*

ikondiag Nombres	Description
JDFE_XE36_10G	xe-0/0/36
JDFE_XE37_10G	xe-0/0/37
JDFE_XE38_10G	xe-0/0/38
JDFE_XE39_10G	xe-0/0/39

Tabla 91 en la página 914 muestra las asignaciones para los canales de 10 Gigabit Ethernet en los puertos C del módulo QFX-PFA-4Q.

Tabla 91: Mapeos de canal Ethernet de 10 Gigabit en los puertos C del módulo QFX-PFA-4Q

ikondiag Nombres	Description
JDFE_QSFP0_10G_PORT0	Puerto QSFP #0 Subcanal 0 de 10G
JDFE_QSFP0_10G_PORT1	Puerto QSFP #0 Subcanal 10G 1
JDFE_QSFP0_10G_PORT2	Puerto QSFP #0 10G subcanal 2
JDFE_QSFP0_10G_PORT3	Puerto QSFP #0 Subcanal 3 de 10G
JDFE_QSFP1_10G_PORT0	Puerto QSFP #1 10G subcanal 0
JDFE_QSFP1_10G_PORT1	Puerto QSFP #1 Subcanal 1 de 10G
JDFE_QSFP1_10G_PORT2	Puerto QSFP #1 Subcanal 2 de 10G
JDFE_QSFP1_10G_PORT3	Puerto QSFP #1 Subcanal 3 de 10G

Tabla 91: Mapeos de canal Ethernet de 10 Gigabit en los puertos C del módulo QFX-PFA-4Q *(Continued)*

ikondiag Nombres	Description
JDFE_QSFP2_10G_PORT0	Puerto QSFP #2 Subcanal 0 de 10G
JDFE_QSFP2_10G_PORT1	Puerto QSFP #2 Subcanal 10G 1
JDFE_QSFP2_10G_PORT2	Puerto QSFP #2 Subcanal 2 de 10G
JDFE_QSFP2_10G_PORT3	Puerto QSFP #2 Subcanal 3 de 10G
JDFE_QSFP3_10G_PORT0	Puerto QSFP #3 Subcanal 0 de 10G
JDFE_QSFP3_10G_PORT1	Puerto QSFP #3 Subcanal 10G 1
JDFE_QSFP3_10G_PORT2	Puerto QSFP #3 Subcanal 2 de 10G
JDFE_QSFP3_10G_PORT3	Puerto QSFP #3 Subcanal 3 de 10G

Tabla 92 en la página 915 proporciona una conectividad exacta entre los puertos C y A.

Tabla 92: Conectividad exacta entre los puertos C y los puertos A

Número de puerto QSFP	Número de canal	Interfaz de Junos OS
Puerto QSFP #0	Canal 0	xe-0/0/32
Puerto QSFP #0	Canal 1	xe-0/0/33
Puerto QSFP #0	Canal 2	xe-0/0/34
Puerto QSFP #0	Canal 3	xe-0/0/35

Tabla 92: Conectividad exacta entre los puertos C y los puertos A *(Continued)*

Número de puerto QSFP	Número de canal	Interfaz de Junos OS
Puerto QSFP #1	Canal 0	xe-0/0/24
Puerto QSFP #1	Canal 1	xe-0/0/25
Puerto QSFP #1	Canal 2	xe-0/0/26
Puerto QSFP #1	Canal 3	xe-0/0/27
Puerto QSFP #2	Canal 0	xe-0/0/28
Puerto QSFP #2	Canal 1	xe-0/0/29
Puerto QSFP #2	Canal 2	xe-0/0/30
Puerto QSFP #2	Canal 3	xe-0/0/31
Puerto QSFP #3	Canal 0	xe-0/0/36
Puerto QSFP #3	Canal 1	xe-0/0/37
Puerto QSFP #3	Canal 2	xe-0/0/38
Puerto QSFP #3	Canal 3	xe-0/0/39

- Agregue estas interfaces a una VLAN.

Canalizar los puertos 10 a 13 mediante la CLI de Junos.

1. Configure los puertos 10 a 13 en PIC 1 para que funcionen como puertos 10 Gigabit Ethernet.

```
[edit chassis fpc 0 pic 1]
user@switch# set port-range 10 13 channel-speed 10g
```

2. Revise la configuración y ejecute el comando.`commit`

```
[edit]
user@switch# commit
commit complete
```

Agregue las 16 interfaces canalizadas que acaba de configurar a 16 VLAN.

Para agregar las 16 interfaces canalizadas:

1. Cree 16 VLAN.

```
[edit vlans]
user@switch# set v0_0 vlan-id 10
user@switch# set v0_1 vlan-id 11
user@switch# set v0_2 vlan-id 12
user@switch# set v0_3 vlan-id 13
user@switch# set v1_0 vlan-id 14
user@switch# set v1_1 vlan-id 15
user@switch# set v1_2 vlan-id 16
user@switch# set v1_3 vlan-id 17
user@switch# set v2_0 vlan-id 18
user@switch# set v2_1 vlan-id 19
user@switch# set v2_2 vlan-id 20
user@switch# set v2_3 vlan-id 21
user@switch# set v3_0 vlan-id 22
user@switch# set v3_1 vlan-id 23
user@switch# set v3_2 vlan-id 24
user@switch# set v3_3 vlan-id 25
```

2. Agregue las interfaces canalizadas a las VLAN.

```
[edit interfaces]
user@switch# set xe-0/0/24 unit 0 family ethernet-switching vlan members v0_0
user@switch# set xe-0/0/25 unit 0 family ethernet-switching vlan members v0_1
user@switch# set xe-0/0/10:0 unit 0 family ethernet-switching vlan members v0_0
user@switch# set xe-0/0/10:1 unit 0 family ethernet-switching vlan members v0_1
user@switch# set xe-0/0/10:2 unit 0 family ethernet-switching vlan members v0_2
user@switch# set xe-0/0/10:3 unit 0 family ethernet-switching vlan members v0_3
user@switch# set xe-0/0/11:0 unit 0 family ethernet-switching vlan members v1_0
user@switch# set xe-0/0/11:1 unit 0 family ethernet-switching vlan members v1_1
```

```
user@switch# set xe-0/0/11:2 unit 0 family ethernet-switching vlan members v1_2
user@switch# set xe-0/0/11:3 unit 0 family ethernet-switching vlan members v1_3
user@switch# set xe-0/0/12:0 unit 0 family ethernet-switching vlan members v2_0
user@switch# set xe-0/0/12:1 unit 0 family ethernet-switching vlan members v2_1
user@switch# set xe-0/0/12:2 unit 0 family ethernet-switching vlan members v2_2
user@switch# set xe-0/0/12:3 unit 0 family ethernet-switching vlan members v2_3
user@switch# set xe-0/0/13:0 unit 0 family ethernet-switching vlan members v3_0
user@switch# set xe-0/0/13:1 unit 0 family ethernet-switching vlan members v3_1
user@switch# set xe-0/0/13:2 unit 0 family ethernet-switching vlan members v3_2
user@switch# set xe-0/0/13:3 unit 0 family ethernet-switching vlan members v3_3
```

3. Revise la configuración y ejecute el comando.`commit`

```
[edit]
user@switch# commit
commit complete
```

Pruebas de esfuerzo

Las pruebas de esfuerzo ejercitan todas las E/S de alta velocidad en paralelo. Las pruebas de esfuerzo requieren el mismo medio externo que utilizó para las pruebas de Ethernet. enumera el nombre de la prueba y sus funciones.Tabla 93 en la página 919

Tabla 93: Pruebas de esfuerzo

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
Estrés	Ejercita todas las E/S de alta velocidad en paralelo.	Ejerza todas las E/S de alta velocidad conectadas a la FPGA en paralelo, incluyendo: • DRAM • QDR • Ethernet Cada subsistema de prueba se ejerce de manera similar a las pruebas individuales descritas anteriormente.	-i <n> número variado de iteraciones) predeterminado = 1 para prueba rápida, 1.000 para burn-in)	Prueba rápida y quemado	Si algún subsistema falla, la prueba se detiene. Se notifica el primer subsistema que se detectó que ha fallado. **NOTA**: Si se produce un error en varios subsistemas, solo se notificará el primer subsistema que haya fallado.

Pruebas de PTP

Puede ejecutar PTP para hardware usado con PTP . Estas pruebas son útiles si está creando aplicaciones de temporización. Para ejecutar las pruebas, debe conectar cables Subminiatura versión B (SMB), cables de bucle invertido Ethernet y cables de bucle invertido ToD para la E/S de sincronización, el puerto serie ToD y los conectores 1 Gigabit Ethernet. Debe conectar los cables SMB, Ethernet y Bucle invertido ToD entre los conectores de salida y entrada 10M y PPS. El cable de circuito cerrado ToD es un cable RJ45 estándar con el Pin 3 (Tx Data) conectado al Pin 6 (Rx Data). Además de las pruebas de PTP, puede ejecutar scripts incluidos en el software Packet Flow Accelerator Diagnostics para probar PTP. Consulte para obtener información sobre los scripts PTP.Tabla 95 en la página 921 Los scripts PTP requieren que tenga instalada una imagen de Junos OS con automatización mejorada en el conmutador QFX5100-24Q-AA. Para obtener información acerca de cómo instalar las secuencias de comandos, consulte .No Link Title

Tabla 94 en la página 920 enumera los nombres de las pruebas PTP y sus funciones:

Tabla 94: Pruebas de PTP

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error

PTP	Comprueba la funcionalidad de varias funciones de sincronización de tiempo conectadas a FPGA del módulo QFX-PFA-4Q.	Realiza varias pruebas sobre la funcionalidad de sincronización de tiempo del módulo QFX-PFA-4Q.
		
		Las subpruebas cubiertas por esta prueba incluyen:
		
		• Verificación de las comunicaciones adjuntas a PFE.
		
		• Prueba de la PTP PHY
		
		  • Configuración básica.
		
		  • Línea de interrupción conectada a FPGA.
		
		  • Circuito cerrado Ethernet de 1 Gigabit (requiere medios de circuito cerrado externos).
		
		  • Generadores de reloj relacionados con la sincronización de tiempo del módulo QFX-PFA-4Q y enrutamiento de retroalimentación.
		
		  • Puerto UART ToD (requiere medios de bucle invertido externos).
			Ninguno.	Prueba rápida y quemado	Un error en cualquiera de los subsistemas anteriores hace que se produzca un error en toda la prueba y genera un informe al final de la prueba que indica el estado de aprobación y reprobación de las subpruebas.

Tabla 95 en la página 921 enumera el nombre de la secuencia de comandos y su función. Este script no forma parte del comando.**ikondiag** Puede ejecutar este comando Junos OS.

Tabla 95: PTP Script

Nombre del script	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error

./ run_ptp_test	Comprueba la funcionalidad de varias funciones de sincronización de tiempo conectadas a FPGA del módulo QFX-PFA-4Q.	Realiza varias pruebas sobre la funcionalidad de sincronización de tiempo del módulo QFX-PFA-4Q.
		
		Las subpruebas cubiertas por esta prueba incluyen:
		
		• Verificación de comunicaciones adjuntas PFE.
		
		• Prueba de la PTP PHY
		
		  • Configuración básica.
		
		  • Línea de interrupción conectada a FPGA.
		
		  • Bucle invertido Ethernet de 1 gigabith (requiere medios de bucle cerrado externos).
		
		  • Generadores de reloj relacionados con la sincronización de tiempo del módulo QFX-PFA-4Q y enrutamiento de retroalimentación.
		
		  • Puerto UART ToD (requiere medios de bucle invertido externos).
			Ninguno.	Ninguno. Esta prueba debe ejecutarse manualmente.	Un error en cualquiera de los subsistemas anteriores hace que se produzca un error en toda la prueba y genera un informe al final de la prueba que indica el estado de aprobación y reprobación de las subpruebas.

Pruebas LED del módulo QFX-PFA-4Q

Las pruebas de LED examinan los LED del módulo QFX-PFA-4Q.

Para ejecutar la prueba del LED, ejecute el comando.**ikon_led_toggle** La prueba puede tardar unos segundos en iniciarse porque se está configurando la FPGA. Cuando vea el mensaje , comenzará la prueba.`Toggling LEDs. Send SIGINT (^C) to exit` Para finalizar la prueba, escriba Ctrl-C. enumera el nombre de la prueba y su función.Tabla 96 en la página 923

Tabla 96: Prueba LED del módulo QFX-PFA-4Q

Nombre de la prueba	Description	Detalles	Argumentos opcionales	Conjuntos de prueba	Comportamiento de error
ikon_led_toggle	Parpadea los LED del módulo QFX-PFA-4Q para una inspección visual.	Los siguientes LED del módulo QFX-PFA-4Q pasarán repetidamente por los siguientes patrones: **NOTA**: Los LED AL y ST no se incluyen en esta prueba. • Los dieciséis LED bicolores para el ciclo de estado QSFP a través de verde, naranja y apagado. • Los LED S0 y S1 pasan por verde y apagado. • El LED de estado PTP RJ-45 inferior izquierda pasa por verde, naranja y apagado. • El LED de estado PTP RJ-45 inferior derecha pasa por verde y se apaga rápidamente. • Los LED de alarma cambian de color naranja, rojo y apagado.	Ninguno.	Ninguno. Esta prueba debe ejecutarse manualmente.	Es posible que los LED no parpadeen.

Utilidades de diagnóstico del acelerador de flujo de paquetes

Además de las pruebas del software de diagnóstico del acelerador de flujo de paquetes, hay utilidades incluidas en el software de diagnóstico del acelerador de flujo de paquetes que puede utilizar para diagnosticar problemas adicionales en el módulo QFX-PFA-4Q.

> **NOTA**: Antes de poder ejecutar las utilidades, debe conectarse a la consola de la máquina virtual invitada. Para obtener más información sobre cómo acceder a la máquina virtual invitada, consulte .No Link Title

Tabla 97 en la página 924 enumera el nombre de la utilidad y su función.

Tabla 97: Servicios públicos

Nombre de la prueba	Descripciones	Detalles	Resultado y comportamiento esperados
maxtop	Informa del estado de FPGA.	Muestra información sobre el estado configurado actualmente del módulo FPGA y si el módulo está en funcionamiento. Comprueba que las operaciones básicas del controlador y del vínculo FPGA PCI Express funcionan correctamente. Si esta utilidad se cierra con un error o errores, es muy poco probable que otras operaciones de FPGA funcionen.	La salida debe ser similar a la que se muestra a continuación. Si no se muestra este resultado, es posible que se produzca un error crítico en el entorno del software de diagnóstico o que el vínculo PCI Express a la FPGA no funcione. `MaxTop Tool 2015.1 Found 1 card(s) running MaxelerOS 2015.1 Card 0: QFX-PFA-4Q (P/N: 241124) S/N: 96362301684266423 Mem: 24GB Load average: 0.00, 0.00, 0.00 DFE %BUSY TEMP MAXFILE PID USER TIME COMMAND 0 0.0% - 2fcf249cc7... - - - -`

Tabla 97: Servicios públicos *(Continued)*

Nombre de la prueba	Descripciones	Detalles	Resultado y comportamiento esperados
ikon_snake	Permite la conectividad snake entre todos los canales de 10 Gigabit Ethernet.	Conecta el canal Rx de los 32 canales de 10 Gigabit Ethernet del módulo FPGA (interfaces QSFP) al canal Tx de la conexión vecina respectiva. Esto permite probar los 32 canales utilizando solo un generador de paquetes externo de interfaz 10 Gigabit Ethernet, módulos de bucle invertido de cobre y un cable de conexión QSFP <-> 4xSFP.	Después de emitir esta prueba, todos los datos de Ethernet se reenviarán después de que se muestre el mensaje . `‘Snake tool loaded. hit 'enter' to exit.’` **NOTA**: Durante el tiempo antes de imprimir el mensaje de funcionamiento, es posible que el módulo FPGA esté en proceso de configuración, por lo que no se reenvían datos. Al presionar 'enter' saldrá de la utilidad. Una vez finalizada la prueba, los datos del paquete continúan reenviándose hasta que se ejecuta otra utilidad o prueba de Ethernet.

Tabla 97: Servicios públicos *(Continued)*

Nombre de la prueba	Descripciones	Detalles	Resultado y comportamiento esperados
ikon_eth_util todo --digitalloopback	Permite el circuito cerrado digital en todas las interfaces de 10 Gigabit Ethernet en el Permite la conectividad "serpiente" entre todos los canales de 10 Gigabit Ethernet del módulo QFX-PFA-4Q.	Conecta el lado Rx de todos los 32 canales de 10 Gigabit Ethernet del módulo FPGA (QSFP) al lado Tx del mismo canal.	Después de realizar esta prueba, todos los datos de Ethernet se reenviarán como se describe después de que se muestre el mensaje .`'running press return key to exit'` **NOTA**: Antes de que se muestre el mensaje de funcionamiento, es posible que el módulo FPGA esté en proceso de configuración y no se reenvíen datos. Al presionar Intro, se cierra la utilidad. Una vez finalizada la prueba, los datos del paquete continúan reenviándose hasta que se ejecuta otra utilidad o prueba de Ethernet.

Tabla 97: Servicios públicos *(Continued)*

Nombre de la prueba	Descripciones	Detalles	Resultado y comportamiento esperados
ikon_eth_util	Permite que los datos pasen a través de los puertos QSFP del módulo QFX-PFA-4Q.	Permite que los datos pasen a través de los puertos QSFP del módulo QFX-PFA-4Q en el módulo QFX-PFA-4Q. **NOTA**: Dado que todos los puertos QSFP se canalizan a 10 Gigabit Ethernet, debe utilizar cables de conexión SFP al conectar medios externos.	Después de realizar esta prueba, todos los datos de Ethernet se reenvían como se describe después de que aparezca el mensaje ' en ejecución, presione la tecla Retorno para salir '. **NOTA**: Antes de que aparezca el mensaje de funcionamiento, es posible que el módulo FPGA esté en proceso de configuración y no se reenvíen datos. Al presionar 'enter' saldrá de la utilidad. Una vez finalizada la prueba, los datos del paquete seguirán reenviándose hasta que se ejecute otra utilidad o prueba de Ethernet.

Tabla 97: Servicios públicos *(Continued)*

Nombre de la prueba	Descripciones	Detalles	Resultado y comportamiento esperados

maxnet -v enlace mostrar	Volca las estadísticas de paquetes FPGA.	Muestra estadísticas sobre los paquetes enviados y recibidos en todos los vínculos (QSFP) desde los núcleos IP MAC y PHY de la FPGA. El uso de la opción 'v' proporciona una salida detallada.
		
		Aquí hay algunos elementos importantes a tener en cuenta:
		
		• Las estadísticas de paquetes se restablecen cada vez que se reconfigura la FPGA de Altera; es decir, cuando se ejecutan diferentes aplicaciones que hacen uso de la FPGA.
		
		• La herramienta solo muestra datos para los enlaces Ethernet que se incluyen en el diseño de FPGA. Como tal, si el módulo FPGA aún no se ha configurado o está configurado con una aplicación que no utiliza algunos de los vínculos Ethernet, es posible que se muestren detalles de vínculo reducidos.
			El resultado de ejemplo para un único vínculo de 10 Gigabit Ethernet es el siguiente:
			
			`MaxTop Tool 2015.1`
			`Found 1 card(s) running MaxelerOS 2015.1`
			`Card 0: QFX-PFA-4Q (P/N: 241124) S/N: 96362301684266423 Mem: 24GB`
			
			`Load average: 0.00, 0.00, 0.00`
			
			`DFE %BUSY TEMP MAXFILE PID USER TIME COMMAND`
			`0 0.0% - 2fcf249cc7... - - - -`

Tabla 97: Servicios públicos *(Continued)*

Nombre de la prueba	Descripciones	Detalles	Resultado y comportamiento esperados
host2mem I <filename> -o <filename> -t <DDR | QDR0 | QDRPARITY0 | QDR1 | QDRPARITY1>	Escribe y, a continuación, lee datos arbitrarios de QDR SRAM o DRAM.	Funciona transmitiendo el contenido de un archivo binario a uno de los recursos de memoria del módulo QFX-PFA-4Q a través de la FPGA y, a continuación, transmite los mismos datos desde la memoria a otro archivo. **NOTA**: No puede leer solo datos de RAM porque el contenido no se conserva entre la ejecución de varias pruebas.	Informa APROBADO o FALLIDO dependiendo de si los datos devueltos coinciden con los datos de entrada.

Tabla 98 en la página 929 enumera los argumentos de la línea de comandos para la utilidad host2mem.

Tabla 98: Argumentos de la línea de comandos

Argumento	Description
-- ayuda | -H	Imprima el uso y salga.
-i <input file>	Archivo de datos de entrada.
-o <output file>	Archivo de datos de salida.
-- prueba | -t <nombre de prueba>	Recurso de prueba. Consulte para obtener información sobre los recursos.Tabla 99 en la página 930
-- detallado | -V	Habilite el modo detallado.

El formato de archivo para los archivos de entrada y salida es idéntico. Los datos se empaquetan consecutivamente como palabras según el ancho especificado en la tabla de modo de prueba a

continuación. El tamaño de un archivo de entrada puede ser menor, pero no debe superar el tamaño total del recurso que se está probando. El tamaño del archivo de salida es el mismo que el del archivo de entrada y, siempre que no haya errores, tiene el mismo contenido.

Tabla 99: Detalles del formato de archivo

Modo de prueba	Recursos	Ancho de palabra	Tamaño de los datos de prueba
DDR	DDR SDRAM	192 B	24 GB
QDR0	Datos QDR0	16 B	32 MB
QDRPARITY0	Bits de paridad QDR0	2 B	4 MB
QDR1	Datos QDR1	16 B	32 MB
QDRPARITY1	Bits de paridad QDR1	2 B	4 MB

La memoria dinámica de acceso aleatorio (DRAM) del módulo QFX-PFA-4Q contiene tres módulos de memoria en línea duales (DIMM3, DIMM4, DIMM6), y cada palabra de datos se divide en los tres DIMM. enumera la asignación de bytes a DIMM.Tabla 100 en la página 930

Tabla 100: Módulos de memoria duales en línea

0	DIMM3	63	64	DIMM4	127	128	DIMM6	191

Resultado de ejemplo para el software de diagnóstico del acelerador de paquetes

En esta sección se proporcionan algunos resultados de ejemplo para pruebas básicas, pruebas de Ethernet, pruebas de PTP y utilidades.

- ikondiag -t FPGABasic

```
[2015-05-07 03:00:17][BEGIN TEST - FPGABasic]
[2015-05-07 03:00:17][END TEST FPGABasic RESULT PASSED]
```

- ikondiag -t DIMM

```
[2015-05-07 03:01:09][BEGIN TEST - DIMM]
[2015-05-07 03:01:09][END TEST DIMM RESULT PASSED]
```

- ikondiag -t QSFPEthernet

```
[2015-05-07 03:02:33][BEGIN TEST -
QSFPEthernet]

***********************************************

Test
Failed:

  QSFP0_10G_PORT0: FAIL - packets received =
0/1000

  QSFP0_10G_PORT1: FAIL - packets received =
0/1000

  QSFP0_10G_PORT2: FAIL - packets received =
0/1000

  QSFP0_10G_PORT3: FAIL - packets received = 0/1000
  QSFP1_10G_PORT0: FAIL - packets received =
0/1000

  QSFP1_10G_PORT1: FAIL - packets received =
0/1000

  QSFP1_10G_PORT2: FAIL - packets received =
0/1000

  QSFP1_10G_PORT3: FAIL - packets received =
0/1000

  QSFP2_10G_PORT0: FAIL - packets received =
0/1000

  QSFP2_10G_PORT1: FAIL - packets received =
```

```
0/1000

  QSFP2_10G_PORT2: FAIL - packets received =
0/1000

  QSFP2_10G_PORT3: FAIL - packets received =
0/1000

  QSFP3_10G_PORT0: FAIL - packets received = 0/1000
  QSFP3_10G_PORT1: FAIL - packets received =
0/1000

  QSFP3_10G_PORT2: FAIL - packets received =
0/1000

  QSFP3_10G_PORT3: FAIL - packets received =
0/1000

  QSFP4_10G_PORT0: PASS - packets received =
1000/1000

  QSFP4_10G_PORT1: PASS - packets received =
1000/1000

  QSFP4_10G_PORT2: PASS - packets received =
1000/1000

  QSFP4_10G_PORT3: PASS - packets received =
1000/1000

  QSFP5_10G_PORT0: PASS - packets received =
1000/1000

  QSFP5_10G_PORT1: PASS - packets received =
1000/1000

  QSFP5_10G_PORT2: PASS - packets received =
1000/1000

  QSFP5_10G_PORT3: PASS - packets received =
1000/1000

  QSFP6_10G_PORT0: PASS - packets received =
```

```
1000/1000

  QSFP6_10G_PORT1: PASS - packets received =
1000/1000

  QSFP6_10G_PORT2: PASS - packets received =
1000/1000

  QSFP6_10G_PORT3: PASS - packets received =
1000/1000

  QSFP7_10G_PORT0: PASS - packets received =
1000/1000

  QSFP7_10G_PORT1: PASS - packets received =
1000/1000

  QSFP7_10G_PORT2: PASS - packets received =
1000/1000

  QSFP7_10G_PORT3: PASS - packets received =
1000/1000

**********************************************

[2015-05-07 03:02:41][END TEST QSFPEthernet RESULT
PASSED]
```

- ikondiag -t DRAMMemory -i 3

```
[2015-05-07 03:03:37][BEGIN TEST -
DRAMMemory]

[2015-05-07 03:04:21][END TEST DRAMMemory RESULT
PASSED]
```

- ikondiag -t QDRMemory -p -i 3

```
[2015-05-07 03:10:38][BEGIN TEST -
QDRMemory]

[2015-05-07 03:10:45][END TEST QDRMemory RESULT
PASSED]
```

- ikondiag -t Estrés -p -i 10

```
[2015-05-07 03:11:24][BEGIN TEST -
Stress]

**********************************************

Test
Failed:

  QSFP0_10G_PORT0: PASS - packets received =
650000/650000

  QSFP0_10G_PORT1: PASS - packets received =
650000/650000

  QSFP0_10G_PORT2: PASS - packets received =
650000/650000

  QSFP0_10G_PORT3: PASS - packets received =
650000/650000

  QSFP1_10G_PORT0: PASS - packets received =
650000/650000

  QSFP1_10G_PORT1: PASS - packets received =
650000/650000

  QSFP1_10G_PORT2: PASS - packets received =
650000/650000

  QSFP1_10G_PORT3: PASS - packets received =
```

```
650000/650000

  QSFP2_10G_PORT0: PASS - packets received = 650000/650000
  QSFP2_10G_PORT1: PASS - packets received = 650000/650000
  QSFP2_10G_PORT2: PASS - packets received =
650000/650000

  QSFP2_10G_PORT3: PASS - packets received =
650000/650000

  QSFP3_10G_PORT0: PASS - packets received =
650000/650000

  QSFP3_10G_PORT1: PASS - packets received =
650000/650000

  QSFP3_10G_PORT2: PASS - packets received =
650000/650000

  QSFP3_10G_PORT3: PASS - packets received =
650000/650000

  QSFP4_10G_PORT0: PASS - packets received =
650000/650000

  QSFP4_10G_PORT1: PASS - packets received =
650000/650000

  QSFP4_10G_PORT2: PASS - packets received = 650000/650000
  QSFP4_10G_PORT3: PASS - packets received =
650000/650000

  QSFP5_10G_PORT0: PASS - packets received =
650000/650000

  QSFP5_10G_PORT1: PASS - packets received =
650000/650000

  QSFP5_10G_PORT2: PASS - packets received =
650000/650000

  QSFP5_10G_PORT3: PASS - packets received =
650000/650000
```

```
  QSFP6_10G_PORT0: PASS - packets received =
650000/650000

  QSFP6_10G_PORT1: PASS - packets received = 650000/650000
  QSFP6_10G_PORT2: PASS - packets received =
650000/650000

  QSFP6_10G_PORT3: PASS - packets received =
650000/650000

  QSFP7_10G_PORT0: PASS - packets received =
650000/650000

  QSFP7_10G_PORT1: PASS - packets received =
650000/650000

  QSFP7_10G_PORT2: PASS - packets received =
650000/650000

  QSFP7_10G_PORT3: PASS - packets received =
650000/650000

***********************************************
```

- ikondiag -t PTP

```
[2015-05-07 03:12:20][BEGIN TEST -
PTP]



************************************************************************

PTP PHY interrupt:
PASS

1G Ethernet PHY packet loopback test:
PASS

PTP clock generation/check:
PASS
```

```
UART (ToD) loopback:
PASS

************************************************************************

[2015-05-07 03:13:30][END TEST PTP RESULT
PASS]
```

- ikondiag -t Application -i 2

```
iterations =
2

[2015-05-07 03:14:11][BEGIN TEST - Application
Test]

[2015-05-07 03:17:33][END TEST Application Test RESULT PASSED]
```

- maxtop

```
MaxTop Tool 2015.1
Found 1 card(s) running MaxelerOS 2015.1
Card 0: (P/N: 241124) S/N: 96362301684266423 Mem: 24GB

Load average: 0.00, 0.00, 0.00

DFE  %BUSY  TEMP   MAXFILE        PID    USER       TIME      COMMAND
 0   0.0%   -      7e2198e5c0...  -      -          -         -
```

- ikon_eth_util --all-pass-through

```
Ikon Ethernet Pass Through Utility
setting portConnect_QSFP4_10G_PORT0_QSFP0_10G_PORT0 to 1
setting portConnect_QSFP4_10G_PORT1_QSFP0_10G_PORT1 to 1
setting portConnect_QSFP4_10G_PORT2_QSFP0_10G_PORT2 to 1
setting portConnect_QSFP4_10G_PORT3_QSFP0_10G_PORT3 to 1
setting portConnect_QSFP1_10G_PORT0_QSFP5_10G_PORT0 to 1
```

```
setting portConnect_QSFP1_10G_PORT1_QSFP5_10G_PORT1 to 1
setting portConnect_QSFP1_10G_PORT2_QSFP5_10G_PORT2 to 1
setting portConnect_QSFP1_10G_PORT3_QSFP5_10G_PORT3 to 1
setting portConnect_QSFP2_10G_PORT0_QSFP6_10G_PORT0 to 1
setting portConnect_QSFP2_10G_PORT1_QSFP6_10G_PORT1 to 1
setting portConnect_QSFP2_10G_PORT2_QSFP6_10G_PORT2 to 1
setting portConnect_QSFP2_10G_PORT3_QSFP6_10G_PORT3 to 1
setting portConnect_QSFP3_10G_PORT0_QSFP7_10G_PORT0 to 1
setting portConnect_QSFP3_10G_PORT1_QSFP7_10G_PORT1 to 1
setting portConnect_QSFP3_10G_PORT2_QSFP7_10G_PORT2 to 1
setting portConnect_QSFP3_10G_PORT3_QSFP7_10G_PORT3 to 1
running press return key to exit
```

Instalar scripts Ethernet y PTP

in this section

- Instalar scripts Ethernet y PTP | **938**

Instalar scripts Ethernet y PTP

Puede utilizar scripts Ethernet y PTP que se incluyen en el software de diagnóstico del acelerador de flujo de paquetes para probar la funcionalidad de Ethernet y PTP. Antes de poder instalar los scripts, debe realizar las siguientes tareas:

- Asegúrese de que el módulo QFX-PFA-4Q esté instalado en el conmutador QFX5100. Consulte Instalación de un módulo de expansión en un dispositivo QFX5100 .
- Instale el software Junos OS versión 14.1X53-D27 o posterior con automatización mejorada para el conmutador QFX5100. Consulte Instalación de paquetes de software en dispositivos de la serie QFX .*Installing Software on QFX Series Devices*
- Habilite los servicios SSH y Telnet en el conmutador. Consulte Configuración del servicio SSH para el acceso remoto al enrutador o conmutador y Configuración del servicio Telnet para el acceso remoto a un conmutador.https://www.juniper.net/documentation/en_US/junos/topics/topic-map/junos-software-remote-access-overview.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/task/configuration/telnet-configuring-qfx-series.html

- Instale el software de diagnóstico del acelerador de flujo de paquetes. Consulte No Link Title .

Para instalar los scripts:

1. Inicie sesión en la máquina virtual invitada con el archivo `.request app-engine virtual-machine-shell` *`guest-VM-name`* La longitud máxima del nombre de la máquina virtual invitada es de 255 caracteres. Asegúrese de haber iniciado sesión como root cuando ingrese este comando.

```
root>  request app-engine virtual-machine-shell diagnostics
```

2. Escriba una combinación válida de nombre de usuario y contraseña para la máquina virtual invitada.
3. Escriba el comando en el símbolo del shell.**guest-util diag-install *guest VM IP address***

   Use la misma dirección IP que usó para configurar la dirección de administración local para la máquina virtual invitada.

```
[root@localhost ~] guest-util diag-install 192.168.1.10
```

4. Cambie los directorios a /var/tmp para editar el archivo PFAD_params.cfg.

```
[root@localhost ~] cd /var/tmp
```

5. Abra el archivo PFAD_params.cfg utilizando un editor de su elección.

   Este es un ejemplo de lo que contiene el archivo:

```
[params]


# log level
LOGLEVEL = 'TRACE'


# my variables
VLAN1_NAME      = 'VLAN100'
VLAN1_ID        = '100'
JUNOS_USERNAME  = 'test'
ROOT_USERNAME   = 'root'
JUNOS_PSWD      = 'juniper123'
GUEST_PSWD      = 'diag'
ROOT_PSWD       = 'root123'
```

```
# my duts
DUTS = {
    'R0': "10.204.43.170",
    }



TOPOLOGY = 'IF1 = 'et-0/0/2'
                                IF2 = ‘et-0/0/3’

PFAD_params.cfg: unmodified: line 1
```

6. Configure la dirección IP de administración.

```
                                DUTS = {
                                                ‘R0':
"10.204.43.170”,                                                                }
```

7. Configure las interfaces PTP.

   IF1 es la fuente primaria e IF2 es la fuente secundaria.

   Configure IF1 como et-0/0/2 e IF2 como et-0/0/3.

```
                                IF1 = '2’  <<<<< Change it
                                IF2 = ‘3’  <<<<< Change it
```

8. Guarde los cambios realizados en el archivo PFAD_params.cfg.
9. Ejecute los scripts emitiendo uno de los siguientes comandos en el indicador de la máquina virtual invitada.
   - Para probar la orquestación del tráfico:

     python PFAD_exec.py -t 1

   - Para probar PTP:

     ./run_ptp_test

   - Para probar Broadsync:

     ./run_broadsync_test

Instalar el software de diagnóstico del acelerador de flujo de paquetes

in this section

- Descripción general del software de diagnóstico del acelerador de flujo de paquetes | 941
- Verifique que el módulo de expansión QFX-PFA-4Q esté instalado | 942
- Descargue el software de diagnóstico de flujo de paquetes | 943
- Copie el paquete de software de diagnóstico de flujo de paquetes en el conmutador | 943
- Instale el software de diagnóstico de flujo de paquetes en el conmutador | 944
- Configure las opciones de la máquina virtual invitada para iniciar la máquina virtual invitada en el host | 945
- Comprobar que la máquina virtual invitada funciona | 948
- Acceda a la máquina virtual invitada | 949
- Verifique que el módulo FPGA esté funcionando | 951
- Validar las conexiones entre los puertos de red del conmutador QFX5100-24Q-AA y los puertos del módulo QFX-PFA-4Q | 952
- Desinstalar la máquina virtual invitada | 955

Descripción general del software de diagnóstico del acelerador de flujo de paquetes

Puede utilizar el software de diagnóstico del acelerador de flujo de paquetes para probar el módulo FPGA en el módulo QFX-PFA-4Q instalado en el conmutador QFX5100-24Q-AA, así como las rutas de datos entre el módulo FPGA y el conmutador QFX5100-24Q-AA. El software de diagnóstico del acelerador de flujo de paquetes contiene diagnósticos estándar, diagnósticos de orquestación y diagnósticos de sincronización y protocolo de tiempo de precisión (PTP). Además de las pruebas del software de diagnóstico del acelerador de flujo de paquetes, hay utilidades incluidas en el software de diagnóstico del acelerador de flujo de paquetes que puede utilizar para diagnosticar problemas adicionales en el módulo QFX-PFA-4Q. Para obtener información sobre cómo instalar el módulo QFX-PFA-4Q, consulte Instalación de un módulo de expansión en un dispositivo QFX5100.

Para ejecutar los diagnósticos de orquestación, los diagnósticos de PTP y sincronización, y las utilidades contenidas en el software de diagnóstico del acelerador de flujo de paquetes, debe tener instalado en el conmutador QFX5100 un software Junos OS versión 14.1X53-D27 o posterior con automatización mejorada. Para obtener información sobre cómo descargar e instalar el software de Junos OS, consulte Instalación de paquetes de software en dispositivos de la serie QFX.*Installing Software on QFX Series Devices*

El software de diagnóstico del acelerador de flujo de paquetes se ejecuta en una máquina virtual invitada en el conmutador y requiere que configure las opciones de la máquina virtual invitada en la CLI de Junos OS.

Verifique que el módulo de expansión QFX-PFA-4Q esté instalado

Antes de instalar el software de diagnóstico del acelerador de flujo de paquetes, compruebe que el módulo QFX-PFA-4Q esté instalado.

Desde el símbolo del CLI, emita el comando.`show chassis hardware`

```
{master:0}
root> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                VX3715020024      QFX5100-24Q-AA
Pseudo CB 0
Routing Engine 0          BUILTIN      BUILTIN           QFX Routing Engine
FPC 0            REV 02   650-057155   VX3715020024      QFX5100-24Q-AA
  CPU                     BUILTIN      BUILTIN           FPC CPU
  PIC 0                   BUILTIN      BUILTIN           24x 40G-QSFP-AA
    Xcvr 6       REV 01   740-032986   QD334902          QSFP+-40G-SR4
  PIC 1          REV 01   711-060247   VY3115060052      QFX-PFA-4Q
Power Supply 0   REV 03   740-041741   1GA24082731       JPSU-650W-AC-AFO
Power Supply 1   REV 03   740-041741   1GA24082726       JPSU-650W-AC-AFO
Fan Tray 0                                               QFX5100 Fan Tray 0, Front to Back
Airflow - AFO
Fan Tray 1                                               QFX5100 Fan Tray 1, Front to Back
Airflow - AFO
Fan Tray 2                                               QFX5100 Fan Tray 2, Front to Back
Airflow - AFO
Fan Tray 3                                               QFX5100 Fan Tray 3, Front to Back
Airflow - AFO
Fan Tray 4                                               QFX5100 Fan Tray 4, Front to Back
Airflow - AFO
```

En la salida de la CLI, puede ver las cuatro interfaces QSFP+ (4x40G QSFP+) contenidas en el módulo QFX-PFA-4Q. están instalados.

Descargue el software de diagnóstico de flujo de paquetes

> **NOTA**: Para acceder al sitio de descarga, debe tener un contrato de servicio con Juniper Networks y una cuenta de acceso. Si necesita ayuda para obtener una cuenta, complete el formulario de registro en el sitio web de Juniper Networks https://www.juniper.net/registration/Register.jsp .https://www.juniper.net/registration/Register.jsp

Para descargar el paquete de software Packet Flow Diagnostics del sitio web de soporte de Juniper Networks, vaya a https://www.juniper.net/support/ :https://www.juniper.net/support/

1. Con un explorador Web, vaya a https://www.juniper.net/support .https://www.juniper.net/support
2. Haga clic en .**Download Software**
3. En el cuadro Conmutación, haga clic en .**Junos OS Platforms**
4. En la sección Serie QFX, haga clic en el nombre de la plataforma para la que desea descargar el software.
5. Haga clic en la ficha Software y seleccione el número de versión en la lista desplegable Versión.
6. En la sección Instalar paquete de la ficha Software, seleccione el paquete de instalación de la versión.

   Aparecerá una pantalla de inicio de sesión.
7. Introduzca su nombre y contraseña y pulse Intro.
8. Lea el Contrato de licencia para el usuario final, haga clic en el botón de opción y, a continuación, haga clic en .`I agreeProceed`
9. Guarde el archivo en el equipo.`pfadiag_vm-rXXXXX.img.gz`
10. Abra o guarde el paquete de software Packet Flow Diagnostics en el sistema local del directorio o en una ubicación remota.**var/tmp** Si va a guardar el paquete de instalación en un sistema remoto, asegúrese de que puede acceder a él mediante HTTP, TFTP, FTP o scp.

Copie el paquete de software de diagnóstico de flujo de paquetes en el conmutador

Para copiar el paquete del software de diagnóstico de flujo de paquetes en el conmutador:

Copie el paquete de diagnóstico de flujo de paquetes en el conmutador mediante cualquier protocolo de transferencia de archivos:

Por ejemplo:

```
root% scp //hostname/pathname/pfadiag_vm-rXXXXX.img.gz /var/tmp
```

Instale el software de diagnóstico de flujo de paquetes en el conmutador

Para instalar el paquete de software de diagnóstico de flujo de paquetes en el conmutador:

1. Instale el software de diagnóstico de flujo de paquetes en el conmutador.

   Esto puede tardar unos minutos.

   Si el software de diagnóstico de flujo de paquetes reside localmente en el conmutador, emita el siguiente comando:

```
{master:0}
root> request system software add virtual-machine-package /var/tmp/pfadiag_vm-rXXXXX.img.gz

Installing virtual-machine package..
Copying virtual-machine package..
Uncompressing virtual-machine package..
Finished virtual-machine package installation.
```

2. Emita el comando para comprobar que la instalación se realizó correctamente.`show version`

```
{master:0}
root> show version
fpc0:

--------------------------------------------------------------------------

Hostname:
switch

Model: qfx5100-24q-
aa

Junos: 14.1X53-
D27_vjunos.62

JUNOS Base OS Software Suite [14.1X53-
D26_vjunos.62]

JUNOS Base OS boot [14.1X53-
D27_vjunos.62]

JUNOS Crypto Software Suite [14.1X53-
```

```
D27_vjunos.62]

JUNOS Online Documentation [14.1X53-
D27_vjunos.62]

JUNOS Kernel Software Suite [14.1X53-
D27_vjunos.62]

JUNOS Packet Forwarding Engine Support (qfx-ex-x86-32) [14.1X53-
D27_vjunos.62]

JUNOS Routing Software Suite [14.1X53-
D27_vjunos.62]

JUNOS Enterprise Software Suite [14.1X53-
D27_vjunos.62]

JUNOS py-base-i386 [14.1X53-
D27_vjunos.62]

JUNOS py-extensions-i386 [14.1X53-
D27_vjunos.62]

JUNOS Host Software [14.1X53-
D27_vjunos.62]

Junos for Automation
Enhancement

JUNOS GUEST-VM Software [pfadiag_vm-rXXXXX-
ve]



{master:0}
```

El resultado de la CLI muestra que se instaló el software de diagnóstico del acelerador de flujo de paquetes.

Configure las opciones de la máquina virtual invitada para iniciar la máquina virtual invitada en el host

Para configurar las opciones de la máquina virtual invitada:

1. Configure las siguientes opciones para la compatibilidad con máquinas virtuales invitadas en la CLI de Junos OS en la jerarquía [edit].
   - Nombre del clúster de cómputo
   - Nombre del nodo de proceso
   - Nombre de instancia de VM
   - Interfaz de administración dedicada para VM invitada
   - Nombre del paquete de terceros
   - Dirección IP interna de la máquina virtual invitada
2. Configure el nombre del clúster de proceso y del nodo de proceso.

   El nombre del clúster de proceso debe ser default-cluster y el nombre del nombre del nodo de proceso debe ser default-node; de lo contrario, se produce un error al iniciar la máquina virtual invitada.

```
{master:0}
root# set services app-engine compute-cluster default-cluster compute-node default-node
hypervisor
```

3. Configure el nombre de la instancia de máquina virtual y el nombre de la aplicación de terceros.

```
{master:0}
root# set services app-engine virtual-machines instance instance-name package package-name
```

> **NOTA**: Los nombres de paquete en el comando y el comando deben coincidir.`show app-engine virtual-machine-packageshow version`

```
{master:0}
root# set services app-engine virtual-machines instance diagnostics package pfadiag_vm-rXXXXX-
ve
```

4. Asocie la instancia de máquina virtual con el clúster de proceso y el nodo de proceso configurados.

```
{master:0}
root# set services app-engine virtual-machines instance instance-name compute-cluster name
compute-node name
```

```
{master:0}
root# set services app-engine virtual-machines instance diagnostics compute-cluster default-
cluster compute-node default-node
```

> **NOTA**: El nombre del clúster de proceso debe ser default-cluster y el nombre del nodo de proceso debe ser default-node; de lo contrario, se produce un error al iniciar la máquina virtual invitada.

5. Configure la dirección IP de administración local.

   Esta dirección IP se utiliza para la interfaz de puente interna. El host usa esta dirección IP para comprobar la disponibilidad de la máquina virtual invitada.

> **NOTA**: No utilice 192.168.1.1 y 192.168.1.2 como direcciones IP, ya que son utilizadas por Host-OS y Junos OS respectivamente.

```
{master:0}
root# set services app-engine virtual-machines instance instance-name local-management family
inet address 192.168.1.X
```

```
{master:0}
root# set services app-engine virtual-machines instance diagnostics local-management family
inet address 192.168.1.10
```

6. Configure la interfaz de administración para la máquina virtual invitada.

   Esta interfaz de administración es independiente de la que se usa para Junos OS.

```
{master:0}
root # set services app-engine virtual-machines instance diagnostics management-interface em1
```

> **NOTA**: El nombre de la interfaz de administración debe ser em0 o em1. Se producirá un error en la configuración si no configura una interfaz de administración y, a continuación, confirma la configuración.

La nueva interfaz de administración se aprovisiona para la máquina virtual invitada.

7. Confirme la configuración.

```
{master:0}
root# commit
```

Estos son los resultados de la configuración:

```
services {
    app-engine {
        compute-cluster default-cluster {
            compute-node default-node {
                hypervisor;
            }
        }
        virtual-machines {
            instance diagnostics {
                package pfadiag_vm-rXXXXX-ve;
                local-management {
                    family inet {
                        address 192.168.1.10;
                    }
                }
                compute-cluster default-cluster {
                    compute-node default-node;
                }
                management-interface em1;
            }
        }
    }
}
```

Comprobar que la máquina virtual invitada funciona

Para comprobar que la máquina virtual invitada funciona:

Emita los siguientes comandos para comprobar que todo funciona correctamente:`show`

- raíz> **show app-engine status**

```
Compute cluster: default-cluster
  Compute Node: default-node, Online
```

  El estado debe ser En línea.

- raíz> **show app-engine virtual-machine instance**

```
VM name                  Compute cluster           VM status
diagnostics               default-cluster           ACTIVE
```

  El estado de la máquina virtual debe estar activo.

- raíz> **show app-engine virtual-machine package**

```
VM package: pfadiag_vm-rXXXXX-ve
Compute cluster                    Package download status
default-cluster                    DOWNLOADED
```

Acceda a la máquina virtual invitada

Para acceder a la máquina virtual invitada:

1. Inicie sesión en la máquina virtual invitada.
   - Especifique el nombre de la máquina virtual invitada mediante el comando.`request app-engine virtual-machine-shell` *`guest-VM-name`* La longitud máxima del nombre de la máquina virtual invitada es de 255 caracteres. Asegúrese de haber iniciado sesión como root cuando ingrese este comando.

```
root> request app-engine virtual-machine-shell diagnostics
```

   - Escriba una combinación válida de nombre de usuario y contraseña para la máquina virtual invitada.

> **NOTA**: La primera vez que inicie sesión, el nombre de usuario es root. No hay contraseña. Después de iniciar sesión, se le pedirá que cree una contraseña.

Por ejemplo:

```
Maxeler Ikon Diagnostics VM r44702

diagnostics login: root
You are required to change your password immediately (root enforced)
New password:
Retype new password:
```

2. Emita el comando para ver los nombres de la interfaz de administración que se usa para acceder a la máquina virtual invitada desde fuera de la red, el nombre de la interfaz de administración que se usa para uso interno y los puertos NIC usados en la máquina virtual de diagnóstico.`ifconfig -a`

   En este ejemplo, la dirección es la dirección IP que se usa para uso interno, la interfaz se usa para comunicaciones externas y las interfaces xe-0/0/40 y xe-0/0/41 son los puertos NIC usados en la máquina virtual de diagnóstico.`heartbeatmanagement` El está configurado de forma predeterminada.`heartbeat` La dirección IP del es la misma que la que configuró para Junos OS.`heartbeat`

   Puede asociar una de las interfaces a la máquina virtual invitada emitiendo el comando .`set services app-engine virtual-machines instance` *`name`* `management-interface` *`interface-name`* Utilice la misma dirección IP que la que configuró con el archivo .`set services app-engine virtual-machines instance test local-management family inet address 192.168.1.10` Las direcciones MAC asociadas con estas interfaces se utilizan para puentes internos.

```
[root@ikondiag ~]# ifconfig -a
heartbeat Link encap:Ethernet  HWaddr 52:54:00:5D:DB:01
          inet addr:192.168.1.10  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe5d:db01/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:282 errors:0 dropped:0 overruns:0 frame:0
          TX packets:266 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:24955 (24.3 KiB)  TX bytes:24232 (23.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

```
management Link encap:Ethernet  HWaddr 52:54:00:76:B3:C4
          inet6 addr: fe80::5054:ff:fe76:b3c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:438 (438.0 b)  TX bytes:1836 (1.7 KiB)

xe-0-0-40 Link encap:Ethernet  HWaddr EA:8B:BB:75:56:FE
          inet6 addr: fe80::e88b:bbff:fe75:56fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:140 (140.0 b)

xe-0-0-41 Link encap:Ethernet  HWaddr 3E:1A:00:94:ED:5B
          inet6 addr: fe80::3c1a:ff:fe94:ed5b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:230 (230.0 b)
```

Verifique que el módulo FPGA esté funcionando

Puede utilizar las siguientes utilidades para comprobar que el módulo FPGA del módulo QFX-PFA-4Q funciona.

Para comprobar que el módulo FPGA funciona:

1. Emita el comando en el indicador de inicio de sesión de la máquina virtual invitada.**lspci |grep "RAM memory"**

```
[root@ikondiag ~]# lspci |grep "RAM memory"
00:09.0 RAM memory: Juniper Networks Device 0078
```

El resultado muestra que el dispositivo 0078 de Juniper Networks está funcionando.

2. Emita el comando en el indicador de inicio de sesión de la máquina virtual invitada:**lspci |grep Co-processor**

```
[root@ikondiag ~]# lspci |grep Co-processor
:0a.0 Co-processor: Maxeler Technologies Ltd. Device 0006
```

El resultado muestra que Maxeler Technologies Ltd. El dispositivo 0006 está funcionando.

3. Emita el comando en el indicador de inicio de sesión de la máquina virtual invitada:**maxtop**

> **NOTA**: Si hay errores en la salida del comando, reinicie la máquina virtual invitada.

```
[root@ikondiag ~]# maxtop
```

```
MaxTop Tool 2015.1
Found 1 card(s) running MaxelerOS 2015.1
Card 0: QFX-PFA-4Q (P/N: 241124) S/N: 96362301684266423 Mem: 24GB

Load average: 0.00, 0.00, 0.00

DFE  %BUSY  TEMP   MAXFILE        PID    USER       TIME      COMMAND
 0   0.0%   -      2fcf249cc7...  -      -          -         -
```

Validar las conexiones entre los puertos de red del conmutador QFX5100-24Q-AA y los puertos del módulo QFX-PFA-4Q

Puede utilizar la utilidad para validar las conexiones entre los puertos de red del conmutador QFX5100-24Q-AA y los puertos del módulo QFX-PFA-4Q.**ikon_eth_util –all-pass-through**

En este ejemplo, la utilidad validará las siguientes conexiones entre los puertos F, A, B y C. proporciona los puertos que se validan en este ejemplo. **ikon_eth_util --all-pass-through**Tabla 101 en la página 952

Tabla 101: Validación de puertos

Puertos F	Puertos A	Puertos B	Puertos C

xe-0/0/10:2 Esta interfaz es uno de los puertos 10 Gigabit Ethernet del conmutador QFX5100-24Q-AA. Puede administrar estos puertos a través de Junos OS.	xe-0/0/32 Esta interfaz conecta el PFE del conmutador QFX5100-24Q-AA a los puertos B del módulo FPGA del módulo QFX-PFA-4Q.	JDFE_XE32_10G Esta interfaz es un puerto interno de 10 Gigabit Ethernet en el módulo FPGA en el módulo QFX-PFA-4Q y se conecta a los puertos A en el PFE del conmutador QFX5100-24Q-AA.	JDFE_QSFP0_10G_PORT0 [Puerto externo 0-0] Esta interfaz es uno de los puertos 40 Gigabit Ethernet frontales del módulo QFX-PFA-4Q y se conecta a la máquina virtual invitada que se ejecuta en el conmutador QFX5100-24Q-AA y los puertos F en el conmutador QFX5100-24Q-AA.

Para validar las conexiones entre los puertos de red del conmutador QFX5100-24Q-AA y los puertos del módulo QFX-PFA-4Q:

1. Configure una VLAN y un ID de VLAN:

```
[edit vlans]
user@switch # set VLAN_TEST vlan-id 100
```

2. Asocie el puerto F y el puerto A en esta VLAN para que la FPGA y el PFE puedan comunicarse:

```
[edit interfaces]
user@switch # set xe-0/0/10:2 unit 0 family ethernet-switching vlan members VLAN_TEST
user@switch # set xe-0/0/32 unit 0 family ethernet-switching vlan members VLAN_TEST
```

3. Confirme su configuración:

```
[edit]
user@switch # commit synchronize
```

4. Verifique que se haya creado la VLAN.

```
[edit]
user@switch # run show vlans
    Routing instance        VLAN name             Tag          Interfaces
    default-switch          VLAN_TEST              100
                                                                xe-0/0/10:2.0*
                                                                xe-0/0/32.0*
```

```
    default-switch          default               1
```

5. Emita el comando en el indicador de inicio de sesión de la máquina virtual invitada:**ikon_eth_util --all-pass-through**

```
[root@ikondiag ~]# ikon_eth_util --all-pass-through
Ikon Ethernet Pass Through Utility
setting portConnect_JDFE_QSFP0_10G_PORT0_JDFE_XE32_10G to 1
setting portConnect_JDFE_QSFP0_10G_PORT1_JDFE_XE33_10G to 1
setting portConnect_JDFE_QSFP0_10G_PORT2_JDFE_XE34_10G to 1
setting portConnect_JDFE_QSFP0_10G_PORT3_JDFE_XE35_10G to 1
setting portConnect_JDFE_XE24_10G_JDFE_QSFP1_10G_PORT0 to 1
setting portConnect_JDFE_XE25_10G_JDFE_QSFP1_10G_PORT1 to 1
setting portConnect_JDFE_XE26_10G_JDFE_QSFP1_10G_PORT2 to 1
setting portConnect_JDFE_XE27_10G_JDFE_QSFP1_10G_PORT3 to 1
setting portConnect_JDFE_XE28_10G_JDFE_QSFP2_10G_PORT0 to 1
setting portConnect_JDFE_XE29_10G_JDFE_QSFP2_10G_PORT1 to 1
setting portConnect_JDFE_XE30_10G_JDFE_QSFP2_10G_PORT2 to 1
setting portConnect_JDFE_XE31_10G_JDFE_QSFP2_10G_PORT3 to 1
setting portConnect_JDFE_XE36_10G_JDFE_QSFP3_10G_PORT0 to 1
setting portConnect_JDFE_XE37_10G_JDFE_QSFP3_10G_PORT1 to 1
setting portConnect_JDFE_XE38_10G_JDFE_QSFP3_10G_PORT2 to 1
setting portConnect_JDFE_XE39_10G_JDFE_QSFP3_10G_PORT3 to 1
running press return key to exit
```

6. Envíe tráfico a xe-0/0/10:2 en el conmutador QFX5100-24Q-AA y reciba tráfico en el puerto 0-0 del panel frontal del módulo QFX-PFA-4Q.
7. Envíe tráfico al puerto 0-0 del panel frontal del módulo QFX-PFA-4Q y reciba tráfico en xe-0/0/10:2 en el conmutador QFX5100-24Q-AA.
8. Compruebe las estadísticas de las interfaces xe-0/0/10:2 y xe-0/0/32 emitiendo los comandos y `.show interfaces xe-0/0/10:2 extensiveshow interfaces xe-0/0/32 extensive`
9. Compruebe las estadísticas de las interfaces JDFE_XE32_10G y JDFE_QSFP0_10G_PORT0 emitiendo los comandos en el indicador de máquina virtual invitada para el software de diagnóstico del acelerador de flujo de paquetes.`maxnet link`

   [root@ikondiag ~] # **maxnet link show JDFE_XE32_10G**

```
JDFE_XE32_10G:
         Link Up: true
     MAC address: 00:11:22:33:44:55
      RX Enabled: true
```

```
        RX Frames: 1 ok
                   0 error
                   0 CRC error
                   0 invalid/errored
                   1 total
      TX Enabled: true
       TX Frames: 0 ok
                   0 error
                   0 CRC error
                   0 invalid/errored
                   0 total
```

[root@ikondiag ~] # **maxnet link show JDFE_QSFP0_10G_PORT0**

```
JDFE_QSFP0_10G_PORT0:
         Link Up: true
     MAC address: 00:11:22:33:44:55
      RX Enabled: true
       RX Frames: 0 ok
                   0 error
                   0 CRC error
                   0 invalid/errored
                   0 total
      TX Enabled: true
       TX Frames: 1 ok
                   0 error
                   0 CRC error
                   0 invalid/errored
                   1 total
```

Desinstalar la máquina virtual invitada

Para quitar la máquina virtual invitada:

1. Elimine las instrucciones de configuración y desinstale el paquete de software Packet Flow Accelerator Diagnostics.

   Por ejemplo, para quitar la instrucción:`app-engine`

```
root # delete services app-engine
```

2. Confirme la configuración.

```
root# commit
```

3. (Opcional) Emita el comando para aprender el nombre del paquete de software Packet Flow Accelerator Diagnostics.`show version`

```
{master:0}
root> show version
fpc0:

--------------------------------------------------------------------------

Hostname:
switch

Model: qfx5100-24q-
aa

Junos: 14.1X53-
D27_vjunos.62

JUNOS Base OS Software Suite [14.1X53-
D27_vjunos.62]

JUNOS Base OS boot [14.1X53-
D27_vjunos.62]

JUNOS Crypto Software Suite [14.1X53-
D27_vjunos.62]

JUNOS Online Documentation [14.1X53-
D27_vjunos.62]

JUNOS Kernel Software Suite [14.1X53-
D27_vjunos.62]

JUNOS Packet Forwarding Engine Support (qfx-ex-x86-32) [14.1X53-
D26_vjunos.62]

JUNOS Routing Software Suite [14.1X53-
```

```
D27_vjunos.62]

JUNOS Enterprise Software Suite [14.1X53-
D27_vjunos.62]

JUNOS py-base-i386 [14.1X53-
D27_vjunos.62]

JUNOS py-extensions-i386 [14.1X53-
D27_vjunos.62]

JUNOS Host Software [14.1X53-
D27_vjunos.62]

Junos for Automation
Enhancement

JUNOS GUEST-VM Software [pfadiag_vm-rXXXXX-
ve]



{master:0}
```

4. Ejecute el comando para desinstalar el software de diagnóstico del acelerador de flujo de paquetes.`request system software delete virtual-machine-package <package-name>`

```
root> request system software delete virtual-machine-package pfadiag_vm-rXXXXX-ve
fpc0:
--------------------------------------------------------------------------
Deleted virtual-machine package dpfadiag_vm-rXXXXX-ve ...
```

7

PART IN COVERPAGE

Supervisión de características de seguridad comunes

Mostrar información en tiempo real del dispositivo al host | 959

Supervisar las políticas de seguridad | 967

Interfaces de supervisión y funciones de conmutación | 968

Mostrar información en tiempo real del dispositivo al host

summary

En esta sección se describe cómo mostrar información de supervisión en tiempo real sobre cada dispositivo entre el dispositivo y un host de destino.

in this section

- Mostrar información de monitoreo en tiempo real | 959
- Mostrar información de ruta de multidifusión | 963

Mostrar información de monitoreo en tiempo real

Para mostrar información de supervisión en tiempo real sobre cada dispositivo entre el dispositivo y un host de destino especificado, escriba el comando con la siguiente sintaxis:`traceroute monitor`

```
user@host> traceroute monitor host <count number> <inet | inet6> <interval seconds> <no-resolve>
<size bytes><source source-address> <summary>
```

Tabla 102 Describe las opciones de comando.traceroute monitor

Tabla 102: Opciones de comando de CLI traceroute monitor

La opción	Description
host	Envía paquetes de traceroute al nombre de host o a la dirección IP que especifique.
`count` *number*	(Opcional) Limita el número de solicitudes de ping, en paquetes, para enviar en modo resumen. Si no especifica un recuento, las solicitudes de ping se envían continuamente hasta que presione Q.
`inet`	(Opcional) Fuerza los paquetes traceroute a un destino IPv4.

Tabla 102: Opciones de comando de CLI traceroute monitor *(Continued)*

La opción	Description
`inet6`	(Opcional) Fuerza los paquetes traceroute a un destino IPv6.
`interval` *seconds*	(Opcional) Establece el intervalo entre las solicitudes de ping, en segundos. El valor predeterminado es segundo.1
`no-resolve`	(Opcional) Suprime la visualización de los nombres de host de los saltos a lo largo de la ruta de acceso.
`size` *bytes*	(Opcional) Establece el tamaño del paquete de solicitud de ping. El tamaño puede ser de bytes .`065,468` El tamaño predeterminado del paquete es bytes.`64`
`source` *address*	(Opcional) Utiliza la dirección de origen que especifique en el paquete traceroute.
`summary`	(Opcional) Muestra la información de traceroute de resumen.

Para salir del comando, presione Q.`traceroute monitor`

A continuación se muestra un ejemplo de salida de un comando:`traceroute monitor`

```
user@host> traceroute monitor host2
```

```
                                                        My traceroute  [v0.69]
 host (0.0.0.0)(tos=0x0 psize=64
bitpattern=0x00)                                                    Wed Mar 14 23:14:11
2007
 Keys:  Help   Display mode   Restart statistics   Order of fields   quit

Packets               Pings
  Host                                                                                Loss
%   Snt   Last   Avg  Best  Wrst StDev
  1. 173.24.232.66
0.0%     5    9.4   8.6   4.8   9.9   2.1
  2. 173.24.232.66
0.0%     5    7.9  17.2   7.9  29.4  11.0
```

```
  3. 173.24.232.66
0.0%     5    9.9   9.3   8.7   9.9   0.5
  4. 173.24.232.66
0.0%     5    9.9   9.8   9.5  10.0   0.2
```

Tabla 103 en la página 961 Resume los campos de salida de la pantalla.

Tabla 103: Resumen de salida del comando de CLI traceroute monitor

Campo	Description
`host`	Nombre de host o dirección IP del dispositivo que emite el comando.`traceroute monitor`
`psize`*size*	Tamaño del paquete de solicitud de ping, en bytes.
Llaves	
`Help`	Muestra la Ayuda de los comandos de la CLI. Presione H para mostrar la Ayuda.
`Display mode`	Alterna el modo de visualización. Presione D para alternar el modo de visualización
`Restart statistics`	Reinicia el comando.`traceroute monitor` Presione R para reiniciar el comando.`traceroute monitor`
`Order of fields`	Establece el orden de los campos mostrados. Pulse O para establecer el orden de los campos mostrados.
`quit`	Cierra el comando.`traceroute monitor` Presione Q para salir del comando.`traceroute monitor`
Paquetes	

Tabla 103: Resumen de salida del comando de CLI traceroute monitor *(Continued)*

Campo	Description
number	Número del salto (dispositivo) a lo largo de la ruta hasta el host de destino final.
`Host`	Nombre de host o dirección IP del dispositivo en cada salto.
`Loss%`	Porcentaje de pérdida de paquetes. El número de respuestas ping dividido por el número de solicitudes de ping, especificado como un porcentaje.
Pings	
`Snt`	Número de solicitudes de ping enviadas al dispositivo en este salto.
`Last`	El tiempo de ida y vuelta más reciente, en milisegundos, al dispositivo en este salto.
`Avg`	Tiempo promedio de ida y vuelta, en milisegundos, al dispositivo en este salto.
`Best`	El tiempo de ida y vuelta más corto, en milisegundos, al dispositivo en este salto.
`Wrst`	El tiempo de ida y vuelta más largo, en milisegundos, al dispositivo en este salto.
`StDev`	Desviación estándar de los tiempos de ida y vuelta, en milisegundos, al dispositivo en este salto.

Mostrar información de ruta de multidifusión

Para mostrar información acerca de una ruta de multidifusión desde un origen al dispositivo, escriba el comando con la siguiente sintaxis:`mtrace from-source`

```
user@host> mtrace from-source source host <extra-hops number> <group address> <interval seconds>
<max-hops number> <max-queries number> <response host> <routing-instance routing-instance-name>
<ttl number> <wait-time seconds> <loop> <multicast-response | unicast-response> <no-resolve> <no-
router-alert> <brief | detail>
```

Tabla 104 Describe las opciones de comando.mtrace from-source

Tabla 104: Opciones de comandos de CLI mtrace from-source

La opción	Description
`source` *host*	Rastrea la ruta al nombre de host o dirección IP especificados.
`extra-hops` *number*	(Opcional) Establece el número de saltos adicionales para rastrear los dispositivos que no responden. Especifique un valor de a `.0255`
`group` *address*	(Opcional) Rastrea la ruta de acceso de la dirección de grupo especificada. El valor predeterminado es `.192.0.2.0`
`interval` *seconds*	(Opcional) Establece el intervalo entre la recopilación de estadísticas. El valor predeterminado es `.10`
`max-hops` *number*	(Opcional) Establece el número máximo de saltos que se van a rastrear hacia el origen. Especifique un valor de a `.0255` El valor predeterminado es `.32`
`max-queries` *number*	(Opcional) Establece el número máximo de intentos de consulta para cualquier salto. Especifique un valor de a `.132` El valor predeterminado es `.3`
`response` *host*	(Opcional) Envía los paquetes de respuesta al nombre de host o dirección IP especificados. De forma predeterminada, los paquetes de respuesta se envían al dispositivo.

Tabla 104: Opciones de comandos de CLI mtrace from-source *(Continued)*

La opción	Description
routing-instance *routing-instance-name*	(Opcional) Realiza un seguimiento de la instancia de enrutamiento especificada.
ttl *number*	(Opcional) Establece el valor de tiempo de vida (TTL) en el encabezado IP de los paquetes de consulta. Especifique un recuento de saltos desde .0255 El valor predeterminado para las consultas locales al grupo de multidifusión es .*all routers*1 De lo contrario, el valor predeterminado es .127
wait-time *seconds*	(Opcional) Establece el tiempo de espera de un paquete de respuesta. El valor predeterminado es segundos.3
loop	(Opcional) Bucles indefinidamente, mostrando estadísticas de tasas y pérdidas. Para salir del comando, presione Ctrl-C.mtrace
multicast-response	(Opcional) Fuerza a las respuestas a usar multidifusión.
unicast-response	(Opcional) Fuerza a los paquetes de respuesta a usar unidifusión.
no-resolve	(Opcional) No muestra nombres de host.
no-router-alert	(Opcional) No utiliza la opción IP de alerta de dispositivo en el encabezado IP.
brief	(Opcional) No muestra las tasas y pérdidas de paquetes.
detail	(Opcional) Muestra las tasas y pérdidas de paquetes si se especifica una dirección de grupo.

A continuación se muestra un ejemplo de salida del comando:`mtrace from-source`

```
user@host> mtrace from-source source 192.1.4.1 group 224.1.1.1
```

```
Mtrace from 192.1.4.1 to 192.1.30.2 via group 224.1.1.1 Querying full reverse path... * *
0  ? (192.1.30.2)  -1  ? (192.1.30.1)  PIM  thresh^ 1    -2  routerC.mycompany.net (192.1.40.2)
PIM  thresh^ 1    -3  hostA.mycompany.net (192.1.4.1) Round trip time 22 ms; total ttl of 2
required.  Waiting to accumulate statistics...Results after 10 seconds:    Source
Response Dest    Overall     Packet Statistics For Traffic From 192.1.4.1  192.1.30.2
Packet      192.1.4.1 To 224.1.1.1      v       __/  rtt   16 ms     Rate       Lost/Sent = Pct
Rate 192.168.195.37  192.1.40.2      routerC.mycompany.net       v     ^      ttl
2                     0/0    = --    0 pps 192.1.40.1      192.1.30.1      ?
v      \__   ttl    3                     ?/0            0 pps 192.1.30.2      192.1.30.2
Receiver      Query Source
```

Cada línea de la pantalla de seguimiento suele tener el siguiente formato (según las opciones seleccionadas y las respuestas de los dispositivos a lo largo de la ruta):

```
hop-number host (ip-address) protocolttl
```

Tabla 105 en la página 965 Resume los campos de salida de la pantalla.

> **NOTA**: Las estadísticas de paquetes recopiladas de los dispositivos y nodos de enrutamiento de Juniper Networks siempre se muestran como `.0`

Tabla 105: Resumen de salida del comando mtrace from-source de CLI

Campo	Description
hop-number	Número del salto (dispositivo) a lo largo de la ruta.
host	Nombre de host, si está disponible, o dirección IP del dispositivo. Si se introdujo la opción en el comando, no se muestra el nombre de host.`no-resolve`
ip-address	Dirección IP del dispositivo.

Tabla 105: Resumen de salida del comando mtrace from-source de CLI *(Continued)*

Campo	Description
protocol	Protocolo utilizado.
ttl	Umbral TTL.
`Round trip time` *milliseconds* `ms`	Tiempo total entre el envío del paquete de consulta y la recepción del paquete de respuesta.
`total ttl of` *number* `required`	Número total de lúpulos necesarios para llegar a la fuente.
`Source`	Dirección IP de origen del paquete de respuesta.
`Response Dest`	Dirección IP de destino de la respuesta.
`Overall`	Velocidad media de paquetes para todo el tráfico en cada salto.
`Packet Statistics For Traffic From`	Número de paquetes perdidos, número de paquetes enviados, porcentaje de paquetes perdidos y tasa promedio de paquetes en cada salto.
`Receiver`	Dirección IP que recibe los paquetes de multidifusión.
`Query Source`	Dirección IP del host que envía los paquetes de consulta.

Supervisar las políticas de seguridad

summary

En esta sección se describe la supervisión de las políticas de seguridad y el registro del tráfico permitido o denegado.

in this section

- Supervisar las estadísticas de la política de seguridad | **967**

Supervisar las estadísticas de la política de seguridad

in this section

- Propósito | **967**
- Acción | **967**

Propósito

Supervise y registre el tráfico que Junos OS permite o deniega en función de las políticas configuradas previamente.

Acción

Para supervisar el tráfico, habilite las opciones de recuento y registro.

Count—Configurable en una política individual. Si el recuento está habilitado, se recopilan estadísticas para las sesiones que entran en el dispositivo para una directiva determinada y para el número de paquetes y bytes que pasan a través del dispositivo en ambas direcciones para una directiva determinada. Para los recuentos (solo para paquetes y bytes), puede especificar que se generen alarmas siempre que el tráfico supere los umbrales especificados. Consulte recuento (Políticas de seguridad).https://www.juniper.net/documentation/en_US/junos15.1x49-d60/topics/reference/configuration-statement/security-edit-count-security-policies.html

La capacidad de registro se puede habilitar con políticas de seguridad durante la inicialización de la sesión () o la etapa de cierre de sesión ().**Log—session-initsession-close** Consulte el registro (Políticas de

seguridad).https://www.juniper.net/documentation/en_US/junos15.1x49-d60/topics/reference/configuration-statement/security-edit-log-security-policies.html

- Para ver los registros de conexiones denegadas, habilite el inicio de sesión .**session-init**
- Para registrar sesiones después de su conclusión o desmontaje, habilite el inicio de sesión.**session-close**

> **NOTA**: El registro de sesión se habilita en tiempo real en el código de flujo, lo que afecta el rendimiento del usuario. Si ambos y están habilitados, el rendimiento se degrada aún más en comparación con la habilitación solamente.**session-closesession-initsession-init**

Para obtener más información sobre la información recopilada para los registros de sesión, consulte Información proporcionada en las entradas del registro de sesión para las puertas de enlace de servicios de la serie SRX.https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-flow-session-and-error-handling.html

Interfaces de supervisión y funciones de conmutación

summary

En esta sección se describe cómo supervisar las interfaces y las funciones de conmutación.

in this section

- Mostrar información de la interfaz en tiempo real | **969**
- Monitor Interfaces | **972**
- Monitorear PPP | **974**

Mostrar información de la interfaz en tiempo real

Ingrese el comando para mostrar estadísticas de tráfico, errores, alarmas y filtros en tiempo real de una interfaz física o lógica:`monitor interface`

```
user@host> monitor interface (interface-name | traffic)
```

Reemplazar por el nombre de una interfaz física o lógica.*`interface-name`* Si especifica la opción, se muestran las estadísticas de todas las interfaces activas.`traffic`

Las estadísticas en tiempo real se actualizan cada segundo. Las columnas y muestran la cantidad que han cambiado los contadores de estadísticas desde que se escribió el comando o desde que borró los contadores delta. y enumere las teclas que utiliza para controlar la visualización mediante las opciones y. `Current deltaDeltamonitor interface`Tabla 106 en la página 969Tabla 107 en la página 970*`interface-name`*`traffic` (Las claves no distinguen entre mayúsculas y minúsculas).

Tabla 106: Interfaz de monitor CLI Teclas de control de salida

Clave	Acción
c	Borra (devuelve a 0) los contadores delta de la columna.`Current delta` Los contadores de estadísticas no se borran.
F	Congela la pantalla, deteniendo la actualización de las estadísticas y los contadores delta.
i	Muestra información sobre una interfaz diferente. Se le pedirá el nombre de una interfaz específica.
N	Muestra información sobre la siguiente interfaz. El dispositivo se desplaza por las interfaces físicas y lógicas en el mismo orden en que se muestran mediante el comando.`show interfaces terse`
q o ESC	Sale del comando y vuelve al símbolo del sistema.
T	Descongela la pantalla, reanudando la actualización de las estadísticas y los contadores delta.

Tabla 107: Tráfico de interfaz de monitoreo de CLI Teclas de control de salida

Clave	Acción
B	Muestra las estadísticas en unidades de bytes y bytes por segundo (bps).
C	Borra (devuelve a 0) los contadores delta de la columna.`Delta` Los contadores de estadísticas no se borran.
D	Muestra la columna en lugar de la columna de velocidad, en bps o paquetes por segundo (pps).`Delta`
P	Muestra las estadísticas en unidades de paquetes y paquetes por segundo (pps).
q o ESC	Sale del comando y vuelve al símbolo del sistema.
R	Muestra la columna de velocidad (en bps y pps) en lugar de la columna.`Delta`

A continuación se muestran pantallas de ejemplo del comando:`monitor interface`

```
user@host> monitor interface fe-0/0/0
```

```
host1                          Seconds: 5                   Time: 04:38:40
                                                          Delay: 3/0/10
Interface: fe-0/0/0, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 1000mbps
Traffic statistics:                                          Current delta
  Input bytes:                 885405423 (3248 bps)                 [2631]
  Output bytes:                137411893 (3344 bps)                [10243]
  Input packets:                 7155064 (2 pps)                      [28]
  Output packets:                 636071 (1 pps)                      [23]
Error statistics:
  Input errors:                        0                                [0]
  Input drops:                         0                                [0]
  Input framing errors:                0                                [0]
  Policed discards:                    0                                [0]
```

```
  L3 incompletes:                      0                                [0]
  L2 channel errors:                   0                                [0]
  L2 mismatch timeouts:                0                                [0]
  Carrier transitions:                 1                                [0]
  Output errors:                       0                                [0]
  Output drops:                        0                                [0]
  Aged packets:                        0                                [0]
Active alarms : None
Active defects: None
Input MAC/Filter statistics:
  Unicast packets                  73083                               [16]
  Broadcast packets              3629058                                [5]
  Multicast packets              3511364                                [3]
  Oversized frames                     0                                [0]
  Packet reject count                  0                                [0]
  DA rejects                           0                                [0]
  SA rejects                           0                                [0]
Output MAC/Filter Statistics:
  Unicast packets                 629555                               [28]
  Broadcast packets                 6494  Multicast packet              [0]
```

NOTA: Los campos de salida que se muestran al introducir el comando vienen determinados por la interfaz que especifique.`monitor interface` *`interface-name`*

```
user@host> monitor interface traffic
```

```
Interface    Link  Input packets        (pps)     Output packets        (pps)  fe-0/0/0
Up          42334          (5)              23306          (3)  fe-0/0/1      Up
587525876      (12252)          589621478      (12891)
```

Monitor Interfaces

in this section

- Propósito | 972
- Acción | 972

Propósito

Ver información general sobre todas las interfaces físicas y lógicas de un dispositivo.

Acción

Escriba los siguientes comandos en la CLI para ver el estado de la interfaz y las estadísticas de tráfico.`show`

- `show interfaces terse`

  NOTA: En los firewalls de la serie SRX, al configurar IP idénticas en una sola interfaz, no verá un mensaje de advertencia; En su lugar, verá un mensaje syslog.

- `show interfaces extensive`
- `show interfaces` *`interface-name`*

NOTA: Si utiliza las interfaces de usuario de J-Web, selecciónelas en la interfaz de usuario de J-Web.**Monitor>Interfaces** La página Interfaces J-Web muestra los siguientes detalles sobre cada interfaz de dispositivo:

- Puerto: indica el nombre de la interfaz.
- Estado del administrador: indica si la interfaz está activada (Arriba) o desactivada (Abajo).
- Estado del vínculo: indica si la interfaz está vinculada (Arriba) o no vinculada (Abajo).
- Dirección: indica la dirección IP de la interfaz.

- Zona: indica si la zona es una zona que no es de confianza o una zona de confianza.
- Servicios: indica los servicios que están habilitados en el dispositivo, como HTTP y SSH.
- Protocolos: indica los protocolos que están habilitados en el dispositivo, como BGP e IGMP.
- Gráfico de velocidad de entrada: muestra la utilización del ancho de banda de la interfaz. Las velocidades de entrada se muestran en bytes por segundo.
- Gráfico de velocidad de salida: muestra la utilización del ancho de banda de la interfaz. Las velocidades de salida se muestran en bytes por segundo.
- Gráfico de contadores de errores: muestra los contadores de errores de entrada y salida en forma de gráfico de barras.
- Gráfico de contadores de paquetes: muestra el número de contadores de paquetes de difusión, unidifusión y multidifusión en forma de gráfico circular. (Los gráficos de contador de paquetes solo se admiten para interfaces que admiten estadísticas de MAC).

Para cambiar la visualización de la interfaz, utilice las siguientes opciones:

- Puerto para FPC: controla el miembro para el que se muestra la información.
- Botón Inicio/Detener: inicia o detiene la supervisión de las interfaces seleccionadas.
- Mostrar gráfico: muestra los contadores de paquetes de entrada y salida y los contadores de errores en forma de gráficos.
- Botón emergente: muestra los gráficos de la interfaz en una ventana emergente independiente.
- Detalles: muestra estadísticas extensas sobre la interfaz seleccionada, incluido su estado general, información de tráfico, dirección IP, errores de E/S, datos de clase de servicio y estadísticas.
- Intervalo de actualización: indica el período de tiempo transcurrido el cual desea que se actualicen los datos de la página.
- Borrar estadísticas: borra las estadísticas de la interfaz seleccionada.

SEE ALSO

Guía del usuario de interfaces para dispositivos de seguridad

Monitorear PPP

in this section

- Propósito | 974
- Acción | 974

Propósito

Muestra información de supervisión de PPP, incluida la información del grupo de direcciones PPP, el estado de la sesión de las interfaces PPP, las estadísticas acumulativas de todas las interfaces PPP y un resumen de las sesiones PPP.

NOTA: La información de monitoreo de PPP solo está disponible en la CLI. La interfaz de usuario de J-Web no incluye páginas para mostrar información de monitoreo de PPP.

Acción

Escriba los siguientes comandos de CLI:

- `show ppp address-pool` *`pool-name`*
- `show ppp interface` *`interface-name`*
- `show ppp statistics`
- `show ppp summary`

8

PART IN COVERPAGE

Gestión del rendimiento

Análisis de red | 976

Análisis de red

summary

En esta sección se describe la función de análisis de red que proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Recopila datos del conmutador, analiza los datos mediante algoritmos sofisticados y captura los resultados en informes. Los administradores de red pueden usar los informes para solucionar problemas, tomar decisiones y ajustar los recursos según sea necesario.

in this section

- Descripción general de análisis de red | **976**
- Comprender los datos de streaming de análisis de red | **987**
- Descripción de la salida de archivos locales de Enhanced Analytics | **995**
- Comprender la configuración y el estado de Network Analytics | **998**
- Configurar la supervisión de colas y tráfico | **1000**
- Configurar un archivo local para datos de análisis de red | **1003**
- Configurar un recopilador remoto para datos de Streaming Analytics | **1004**
- Ejemplo: Configurar estadísticas de cola y tráfico | **1006**
- Ejemplo: Configurar la supervisión de colas y tráfico | **1015**

Descripción general de análisis de red

in this section

- Descripción general de las funciones de análisis | **977**
- Descripción general de las mejoras de análisis de red | **978**
- Resumen de los cambios en la CLI | **980**

El administrador de análisis (analyticsm) del motor de reenvío de paquetes recopila estadísticas de tráfico y colas, y el demonio de análisis (analyticsd) del motor de enrutamiento analiza los datos y genera informes.

NOTA: En Junos OS versión 13.2X51-D15, se mejoró la función de análisis de red y se realizaron cambios exhaustivos en las jerarquías y las instrucciones de la CLI. Si actualiza a Junos OS versión 13.2X51-D15 o posterior desde una versión anterior a 13.2X51-D15, las configuraciones de análisis de red confirmadas en versiones anteriores aparecerán en su dispositivo, pero la función está deshabilitada. Para habilitar esta característica, debe volver a configurarla mediante las nuevas jerarquías e instrucciones de CLI.

Descripción general de las funciones de análisis

El análisis de red se habilita configurando la supervisión de colas (microráfaga) y la supervisión de estadísticas de tráfico de alta frecuencia.

Monitoreo de colas (microrráfagas):

La supervisión de microrráfagas se utiliza para examinar las condiciones de las colas de tráfico en la red. Una ocurrencia de microráfaga indica al motor de reenvío de paquetes que se ha alcanzado una profundidad de cola especificada por el usuario o un umbral de latencia. La profundidad de la cola es el búfer (en bytes) que contiene los datos, y la latencia es el tiempo (en nanosegundos o microsegundos) que los datos permanecen en la cola.

Puede configurar la supervisión de colas en función de la profundidad o la latencia de la cola (pero no ambas), y configurar la frecuencia (intervalo de sondeo) con la que el motor de reenvío de paquetes comprueba si hay microráfagas y envía los datos al motor de enrutamiento para su procesamiento. Puede configurar la supervisión de colas globalmente para todas las interfaces físicas del sistema o para una interfaz específica en el conmutador. Sin embargo, el intervalo de supervisión de cola especificado se aplica a todas las interfaces o a ninguna; No puede configurar el intervalo para cada interfaz.

Monitoreo de estadísticas de tráfico de alta frecuencia:

Utilice la supervisión de estadísticas de tráfico de alta frecuencia para recopilar estadísticas de tráfico en intervalos de sondeo especificados. De manera similar al intervalo de supervisión de cola, el intervalo de supervisión de tráfico se aplica a todas las interfaces o a ninguna; No puede configurar el intervalo para cada interfaz.

Tanto el monitoreo de tráfico como el de colas están deshabilitados de forma predeterminada. Debe configurar cada tipo de supervisión mediante la CLI. En cada caso, la configuración de una interfaz siempre tiene prioridad sobre la configuración global.

NOTA: Puede configurar la supervisión de tráfico y colas solo para interfaces físicas; no se admiten las interfaces lógicas ni las interfaces de puerto de chasis virtual (VCP).

El demonio analítico del motor de enrutamiento genera archivos de registro locales que contienen registros de estadísticas de tráfico y cola. Puede especificar el nombre y el tamaño del archivo de registro, así como el número de archivos de registro. Si no configura un nombre de archivo, los datos no se guardan.

Puede mostrar el archivo de registro local o especificar un servidor para recibir los datos de streaming que contienen las estadísticas de cola y tráfico.

Para cada puerto, la información de los últimos 10 registros de estadísticas de tráfico y 100 registros de estadísticas de cola se almacena en caché. Puede ver esta información mediante los comandos.`show analytics`

Para almacenar datos de traceoptions, configure la instrucción en el nivel de jerarquía.`traceoptions[edit services analytics]`

Descripción general de las mejoras de análisis de red

A partir de Junos OS versión 13.2X51-D15, la función de análisis de red proporciona las siguientes mejoras:

- Recursos: constan de interfaces y sistema. El recurso interfaces permite configurar un nombre de interfaz y un nombre de perfil de recursos asociado para cada interfaz. Con el recurso del sistema, puede configurar los intervalos de sondeo para la supervisión de colas y la supervisión del tráfico, así como un perfil de recursos asociado para el sistema.

- Perfil de recursos: plantilla que contiene las configuraciones para la supervisión de colas y tráfico, como los valores de umbral de profundidad y umbral de latencia, y si cada tipo de supervisión está habilitado o deshabilitado. Una vez configurado un perfil de recursos, se aplica a un recurso del sistema o de las interfaces.

- Recopilador: un servidor para recopilar estadísticas de monitoreo de tráfico y colas, y puede ser un servidor local o remoto. Puede configurar un servidor local para almacenar estadísticas de supervisión en un archivo de registro o un servidor remoto para recibir datos estadísticos transmitidos.

- Exportar perfil: debe configurar un perfil de exportación si desea enviar datos de streaming a un recopilador remoto. En el perfil de exportación, se define la categoría de datos transmitidos (específicos de todo el sistema o de la interfaz) para determinar el tipo de secuencia que recibirá el recopilador. Puede especificar categorías de flujo de sistema e interfaz. Los datos del sistema incluyen información del sistema y el estado de la cola y la supervisión del tráfico. Los datos

específicos de la interfaz incluyen información de la interfaz, estadísticas de cola y tráfico, y estado del vínculo, la cola y el tráfico.

- Formato de flujo de búfer de protocolo de Google (GBP): un nuevo formato de transmisión para monitorear datos estadísticos que se envían a un recopilador remoto en un solo mensaje AnRecord. El formato de esta corriente que proporciona nueve tipos de información se muestra en .Tabla 108 en la página 979

Tabla 108: Formato de flujo de búfer de protocolo de Google (GBP)

Mensaje	Description
Información del sistema	Información general del sistema, incluida la hora de arranque, la información del modelo, el número de serie, el número de puertos, etc.
Estado de la cola del sistema	Estado de la cola para el sistema en general
Estado del tráfico del sistema	Estado del tráfico del sistema en general
Información de la interfaz	Incluye índice, ranura, puerto y otra información SNMP
Estadísticas de cola para interfaces	Estadísticas de cola para interfaces específicas
Estadísticas de tráfico para interfaces	Estadísticas de tráfico para interfaces específicas
Estado del vínculo para interfaces	Incluye velocidad de vínculo, estado, etc.
Estado de la cola para las interfaces	Estado de la cola para interfaces específicas
Estado del tráfico de las interfaces	Estado del tráfico para interfaces específicas

- El archivo analytics.proto: proporciona una plantilla para el formato de secuencia GBP. Este archivo se puede utilizar para escribir la aplicación de servidor de análisis. Para descargar el archivo, vaya a: /documentation/en_US/junos13.2/topics/reference/proto-files/analytics-proto.txt

- Uso de valores de umbral: Analytics Manager (analyticsm) generará un registro de estadísticas de cola cuando se supere el valor de umbral de latencia o profundidad de cola inferior.

- Protocolo de datagramas de usuario (UDP): protocolo de transporte adicional que puede configurar, además del Protocolo de control de transmisión (TCP), para el puerto del servidor de transmisión por secuencias remoto.
- Archivo único para registro local: reemplaza los archivos de registro independientes para las estadísticas de cola y tráfico.
- Cambio en la medición de la latencia: la configuración y la notificación de los valores de latencia han cambiado de microsegundos a nanosegundos.
- Cambio en la notificación del tiempo de recopilación en formato UTC: el tiempo de recopilación de estadísticas se informa en microsegundos en lugar de milisegundos.
- Nuevo comando de modo operativo: reemplaza al comando.`show analytics collectorshow analytics streaming-server`
- Cambios en el formato de salida del comando: incluye los siguientes cambios:
  - Adición de contadores de paquetes de unidifusión, multidifusión y difusión en las estadísticas de cola y tráfico.
  - Inversión de la secuencia de información estadística en la salida. El registro más reciente se muestra al principio y el registro más antiguo al final de la salida.
  - Eliminación de la información de estado de supervisión de tráfico o cola de la parte global de la salida del comando y si no hay una configuración global.`show analytics configurationshow analytics status`
  - Adición de a la parte específica de la interfaz de la salida del comando y si no se configura un parámetro (por ejemplo, umbral de profundidad o umbral de latencia).`n/ashow analytics configurationshow analytics status`

Resumen de los cambios en la CLI

A partir de Junos OS versión 13.2X51-D15, las mejoras en la función de análisis de red provocan cambios en la CLI al configurar la función. Consulte para obtener un resumen de los cambios en la CLI.Tabla 109 en la página 981

Tabla 109: Cambios en la CLI de Network Analytics

Tarea	CLI para Junos OS versión 13.2X50-D15 y 13.2X51-D10	CLI para Junos OS versión 13.2X51-D15 y posteriores

Configuración de la cola global y el intervalo de sondeo de supervisión del tráfico	`[edit services analytics]`
	
	`traffic-statistics {`
	`  interval interval;`
	`}`
	`queue-statistics {`
	`  interval interval;`
	`}`
		`[edit services analytics]`
		
		`resource {`
		`  system {`
		`  polling-interval {`
		`  queue-monitoring interval;`
		`  traffic-monitoring interval;`
		`  }`
		`  }`
		`}`

Configuración de archivos locales para informes de estadísticas de tráfico y colas	`[edit services analytics]`
	
	`traffic-statistics {`
	`  file filename;`
	`  size size;`
	`  files number;`
	`}`
	`queue-statistics {`
	`  file filename;`
	`  size size;`
	`  files number;`
	`}`
		`[edit services analytics]`
		
		`collector {`
		`  local {`
		`  file filename {`
		`  files number;`
		`  size size;`
		`  }`
		`  }`
		`}`

Tabla 109: Cambios en la CLI de Network Analytics *(Continued)*

Tarea	CLI para Junos OS versión 13.2X50-D15 y 13.2X51-D10	CLI para Junos OS versión 13.2X51-D15 y posteriores

Habilitar estadísticas de colas y monitoreo de tráfico, y especificar el umbral de profundidad para todas las interfaces (globalmente)	`[edit services analytics]`
	
	`interfaces {`
	`  all {`
	`  queue-statistics;`
	`  traffic-statistics;`
	`  depth-threshold {`
	`  high number;`
	`  low number;`
	`  }`
	`  }`
	`}`
		Requiere definir un perfil de recursos y aplicarlo al sistema:
		
		1. Para definir un perfil de recursos:
		
		`[edit services analytics]`
		
		`resource-profiles {`
		`  profile-name{`
		`  queue-monitoring;`
		`  traffic-monitoring;`
		`  depth-threshold {`
		`  high number;`
		`  low number;`
		`  }`
		`  }`
		`}`
		
		2. Para aplicar un perfil al sistema:
		
		`[edit services analytics]`
		
		`resource {`
		`  system {`
		`  resource-profile profile-name;`
		`  }`
		`}`

Tabla 109: Cambios en la CLI de Network Analytics *(Continued)*

Tarea	CLI para Junos OS versión 13.2X50-D15 y 13.2X51-D10	CLI para Junos OS versión 13.2X51-D15 y posteriores

Habilitar las estadísticas de cola y la supervisión del tráfico, y especificar el umbral de latencia para una interfaz	`[edit services analytics]`
	
	`interfaces {`
	`  interface{`
	`  queue-statistics;`
	`  traffic-statistics;`
	`  latency-threshold`
	`  high number;`
	`  low number;`
	`  }`
	`}`
		Requiere definir un perfil de recursos y aplicarlo a la interfaz:
		
		1. Para definir un perfil de recursos:
		
		`[edit services analytics]`
		
		`resource-profiles {`
		`  profile-name{`
		`  queue-monitoring;`
		`  traffic-monitoring;`
		`  latency-threshold {`
		`  high number;`
		`  low number;`
		`  }`
		`  }`
		`}`
		
		2. Para aplicar un perfil a la interfaz:
		
		`[edit services analytics]`
		
		`resource {`
		`  interfaces {`
		`  interface-name {`
		`  resource-profile profile-name;`
		`  }`
		`  }`
		`}`

Tabla 109: Cambios en la CLI de Network Analytics *(Continued)*

Tarea	CLI para Junos OS versión 13.2X50-D15 y 13.2X51-D10	CLI para Junos OS versión 13.2X51-D15 y posteriores

Configuración del formato de datos de streaming (JSON, CSV o TSV) para enviar a un servidor remoto
 	
NOTA: Junos OS versión 13.2X51-D15 agregó compatibilidad con el formato de flujo GPB y la configuración de los protocolos de transporte (TCP o UDP).
	`[edit services analytics]`
	
	`streaming-servers {`
	`  address ip-address {`
	`  port number {`
	`  stream-format format;`
	`  }`
	`  }`
	`}`
		Requiere definir el formato de secuencia en un perfil de exportación y aplicar el perfil al recopilador.
		
		1. Para configurar el formato de transmisión:
		
		`[edit services analytics]`
		
		`export-profiles {`
		`  profile-name {`
		`  stream-format format;`
		`  }`
		`}`
		
		2. Para aplicar un perfil de exportación al recopilador:
		
		`[edit services analytics]`
		
		`collector {`
		`  address ip-address {`
		`  port number {`
		`  transport protocol {`
		`  export-profile profile-name;`
		`  }`
		`  }`
		`  }`
		`}`

Tabla 109: Cambios en la CLI de Network Analytics *(Continued)*

Tarea	CLI para Junos OS versión 13.2X50-D15 y 13.2X51-D10	CLI para Junos OS versión 13.2X51-D15 y posteriores

Configuración de los tipos de mensajes de streaming (estadísticas de cola o tráfico) que se enviarán a un servidor remoto	`[edit services analytics]`
	
	`streaming-servers {`
	`  address ip-address {`
	`  port number {`
	`  stream-type type;`
	`  stream-type type;`
	`  }`
	`  }`
	`}`
		Requiere definir un perfil de exportación y aplicarlo al recopilador:
		
		1. Para definir un perfil de exportación:
		
		`[edit services analytics]`
		
		`export-profiles {`
		`  profile-name {`
		`  interface {`
		`  information;`
		`  statistics {`
		`  queue;`
		`  traffic;`
		`  }`
		`  status {`
		`  link;`
		`  queue;`
		`  traffic;`
		`  }`
		`  }`
		`  system {`
		`  information;`
		`  status {`
		`  queue;`
		`  traffic;`
		`  }`
		`  }`
		`  }`
		`}`
		
		2. Para aplicar un perfil de exportación al recopilador:
		
		`[edit services analytics]`
		
		`collector {`
		`  address ip-address {`
		`  port number {`

Tabla 109: Cambios en la CLI de Network Analytics *(Continued)*

Tarea	CLI para Junos OS versión 13.2X50-D15 y 13.2X51-D10	CLI para Junos OS versión 13.2X51-D15 y posteriores
		`export-profile` *`profile-name`*; } } }

Configuración del protocolo de transporte para enviar datos de streaming a un servidor externo	No hay ninguna configuración disponible. Solo se admite el protocolo TCP.	La configuración está disponible. Los protocolos TCP y UDP son compatibles y se pueden configurar para el mismo puerto.
		`[edit services analytics]`
		`collector {`
		`address` *`ip-address`* `{`
		`port` *`number1`* `{`
		`transport tcp;`
		`transport udp;`
		`}`
		`port` *`number2`* `{`
		`transport udp;`
		`}`
		`}`
		`}`

Mostrar información sobre el recopilador o el servidor de transmisión remota	Emita el comando.`show analytics streaming-sever`	Emita el comando.`show analytics collector`

Comprender los datos de streaming de análisis de red

in this section

- Notación de objetos JavaScript (JSON) | 987
- Valores separados por comas (CSV) | 988
- Valores separados por tabulaciones (TSV) | 988
- Búfer de protocolo de Google (GPB) | 991

Los datos de monitoreo de análisis de red se pueden transmitir a servidores remotos llamados recopiladores. Puede configurar uno o varios recopiladores para recibir datos transmitidos que contengan estadísticas de tráfico y cola. En este tema se describe la salida de datos transmitidos.

En Junos OS versión 13.2X51-D10, los análisis de red proporcionan compatibilidad con los siguientes formatos de datos y salida de streaming:

- Notación de objetos JavaScript (JSON)
- Valores separados por comas (CSV)
- Valores separados por tabulaciones (TSV)

NOTA: Para la salida que se muestra en este tema para los formatos JSON, CSV y TSV, la hora se muestra en el formato de época de Unix (también conocido como tiempo de Unix o tiempo POSIX).

A partir de Junos OS versión 13.2X51-D15, se agregó compatibilidad con el siguiente formato y salida de streaming junto con los formatos JSON, CSV y TSV.

- Búfer de protocolo de Google (GPB)

Notación de objetos JavaScript (JSON)

El formato de streaming JavaScript Object Notation (JSON) admite los siguientes datos:

- Datos estadísticos de cola. Por ejemplo:

```
{"record-type":"queue-stats","time":1383453988263,"router-id":"qfx5100-switch",
"port":"xe-0/0/18","latency":0,"queue-depth":208}
```

  Consulte Tabla 110 en la página 989 para obtener más información acerca de los campos de salida de estadísticas de cola.

- Estadísticas de tráfico. Por ejemplo:

```
{"record-type":"traffic-stats","time":1383453986763,"router-id":"qfx5100-switch",
"port":"xe-0/0/16","rxpkt":26524223621,"rxpps":8399588,"rxbyte":3395100629632,
"rxbps":423997832,"rxdrop":0,"rxerr":0,"txpkt":795746503,"txpps":0,"txbyte":101855533467,
"txbps":0,"txdrop":0,"txerr":0}
```

  Consulte para obtener más información sobre los campos de salida de estadísticas de tráfico.Tabla 111 en la página 990

Valores separados por comas (CSV)

El formato de streaming de valores separados por comas (CSV) admite los siguientes datos:

- Estadísticas de cola. Por ejemplo:

```
q,1383454067604,qfx5100-switch,xe-0/0/18,0,208
```

  Consulte para obtener más información acerca de los campos de salida de estadísticas de cola.Tabla 110 en la página 989

- Estadísticas de tráfico. Por ejemplo:

```
t,1383454072924,qfx5100-switch,xe-0/0/19,1274299748,82950,163110341556,85603312,0,0,
27254178291,8300088,3488534810679,600002408,27268587050,3490379142400
```

  Consulte para obtener más información sobre los campos de salida de estadísticas de tráfico.Tabla 111 en la página 990

Valores separados por tabulaciones (TSV)

El formato de streaming de valores separados por tabulaciones (TSV) admite los siguientes datos:

- Estadísticas de cola. Por ejemplo:

```
q       585870192561703872      qfx5100-switch       xe-0/0/18       (null)
208     2
```

Consulte para obtener más información acerca de los campos de salida de estadísticas de cola.Tabla 110 en la página 989

- Estadísticas de tráfico. Por ejemplo:

```
t       1383454139025   qfx5100-switch  xe-0/0/19       1279874033      82022
163823850036    84801488        0       0       27811618258     8199630
3559887126455   919998736       27827356915     3561901685120
```

Consulte para obtener más información sobre los campos de salida de estadísticas de tráfico.Tabla 111 en la página 990

Salida de estadísticas de cola para JSON, CSV y TSV

Tabla 110 en la página 989 Describe los campos de salida de los datos de estadísticas de cola transmitidas en el orden en que aparecen.

Tabla 110: Estadísticas de colas transmitidas Campos de salida de datos

Campo	Description
tipo de registro	Tipo de estadística. Se muestra como: • `queue-stats` (formato JSON) • `q` (Formato CSV o TSV)
hora	Hora (en formato época Unix) en la que se capturaron las estadísticas.
enrutador-id	ID del dispositivo host de análisis de red.
puerto	Nombre del puerto físico configurado para el análisis de red.
latencia	Latencia de la cola de tráfico en milisegundos.

Tabla 110: Estadísticas de colas transmitidas Campos de salida de datos *(Continued)*

Campo	Description
profundidad de cola	Profundidad de la cola de tráfico en bytes.

Salida de estadísticas de tráfico para JSON, CSV y TSV

Tabla 111 en la página 990 Describe los campos de salida de los datos de estadísticas de tráfico transmitido en el orden en que aparecen.

Tabla 111: Estadísticas de tráfico transmitido Campos de salida de datos

Campo	Description
tipo de registro	Tipo de estadística. Se muestra como: • `traffic-stats` (formato JSON) • t (Formato CSV o TSV)
hora	Hora (en formato época Unix) en la que se capturaron las estadísticas.
enrutador-id	ID del dispositivo host de análisis de red.
puerto	Nombre del puerto físico configurado para el análisis de red.
rxpkt	Total de paquetes recibidos.
rxpps	Total de paquetes recibidos por segundo.
rxbyte	Total de bytes recibidos.
rxbps	Total de bytes recibidos por segundo.
rxdrop	Total de paquetes entrantes caídos.

Tabla 111: Estadísticas de tráfico transmitido Campos de salida de datos *(Continued)*

Campo	Description
rxerr	Total de paquetes con errores.
txpkt	Total de paquetes transmitidos.
txpps	Total de paquetes transmitidos por segundo.
txbyte	Total de bytes transmitidos.
txbps	Total de bytes transmitidos por segundo.
txdrop	Total de bytes transmitidos eliminados.
txerr	Total de paquetes transmitidos con errores (descartados).

Búfer de protocolo de Google (GPB)

Este formato de transmisión proporciona:

- Soporte para nueve tipos de mensajes, según el tipo de recurso (para todo el sistema o específico de la interfaz).
- Envía mensajes en un formato jerárquico.
- Puede generar otros mensajes de formato de secuencia (JSON, CSV, TSV) a partir de mensajes con formato GPB.
- Incluye un encabezado de mensaje de 8 bytes. Consulte para obtener más información.Tabla 112 en la página 992

Tabla 112 en la página 992 describe el encabezado del mensaje de formato de secuencia GPB.

Tabla 112: Información del encabezado del mensaje en formato de secuencia GPB

Posición de bytes	Campo
De 0 a 3	Longitud del mensaje
4	Versión del mensaje
De 5 a 7	Reservado para uso futuro

El siguiente archivo de prototipo GPB () proporciona detalles sobre los datos transmitidos:**analytics.proto**

```
package analytics;

// Traffic statistics related info
message TrafficStatus {
    optional uint32             status          = 1;
    optional uint32             poll_interval   = 2;
}

// Queue statistics related info
message QueueStatus {
    optional uint32             status          = 1;
    optional uint32             poll_interval   = 2;
    optional uint64             lt_high         = 3;
    optional uint64             lt_low          = 4;
    optional uint64             dt_high         = 5;
    optional uint64             dt_low          = 6;
}

message LinkStatus {
    optional uint64             speed           = 1;
    optional uint32             duplex          = 2;
    optional uint32             mtu             = 3;
    optional bool               state           = 4;
    optional bool               auto_negotiation= 5;
}
```

```
message InterfaceInfo {
    optional uint32             snmp_index      = 1;
    optional uint32             index           = 2;
    optional uint32             slot            = 3;
    optional uint32             port            = 4;
    optional uint32             media_type      = 5;
    optional uint32             capability      = 6;
    optional uint32             porttype        = 7;
}

message InterfaceStatus {
    optional LinkStatus         link            = 1;
    optional QueueStatus        queue_status    = 2;
    optional TrafficStatus      traffic_status  = 3;
}

message QueueStats {
    optional uint64             timestamp       = 1;
    optional uint64             queue_depth     = 2;
    optional uint64             latency         = 3;
}

message TrafficStats {
    optional uint64             timestamp       = 1;
    optional uint64             rxpkt           = 2;
    optional uint64             rxucpkt         = 3;
    optional uint64             rxmcpkt         = 4;
    optional uint64             rxbcpkt         = 5;
    optional uint64             rxpps           = 6;
    optional uint64             rxbyte          = 7;
    optional uint64             rxbps           = 8;
    optional uint64             rxcrcerr        = 9;
    optional uint64             rxdroppkt       = 10;
    optional uint64             txpkt           = 11;
    optional uint64             txucpkt         = 12;
    optional uint64             txmcpkt         = 13;
    optional uint64             txbcpkt         = 14;
    optional uint64             txpps           = 15;
    optional uint64             txbyte          = 16;
    optional uint64             txbps           = 17;
    optional uint64             txcrcerr        = 18;
    optional uint64             txdroppkt       = 19;
}
```

```
message InterfaceStats {
    optional TrafficStats       traffic_stats   = 1;
    optional QueueStats         queue_stats     = 2;
}

//Interface message
message Interface {
    required string             name            = 1;
    optional bool               deleted         = 2;
    optional InterfaceInfo      information     = 3;
    optional InterfaceStats     stats           = 4;
    optional InterfaceStatus    status          = 5;
}

message SystemInfo {
    optional uint64             boot_time       = 1;
    optional string             model_info      = 2;
    optional string             serial_no       = 3;
    optional uint32             max_ports       = 4;
    optional string             collector       = 5;
    repeated string             interface_list  = 6;
}

message SystemStatus {
    optional QueueStatus        queue_status    = 1;
    optional TrafficStatus      traffic_status  = 2;
}

//System message
message System {
    required string             name            = 1;
    optional bool               deleted         = 2;
    optional SystemInfo         information     = 3;
    optional SystemStatus       status          = 4;
}

message AnRecord {
    optional uint64             timestamp       = 1;
    optional System             system          = 2;
    repeated Interface          interface       = 3;
}
```

SEE ALSO

recopilador (Analytics)

Descripción de la salida de archivos locales de Enhanced Analytics

La función de análisis de red proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. El análisis de red se habilita configurando la supervisión de las estadísticas de tráfico o de cola, o ambas. Además, puede configurar un archivo local para almacenar los registros estadísticos de tráfico y cola.

NOTA: En este tema se describe la salida del archivo local en Junos OS versión 13.2X51-D15 y posteriores.

A partir de Junos OS versión 13.2X51-D15, las estadísticas de monitoreo de tráfico y colas se pueden almacenar localmente en un solo archivo. En el ejemplo siguiente se muestra el resultado del comando.`monitor start`

```
root@qfx5100-33> monitor start an

root@qfx5100-33>
*** an ***
q,1393947567698432,qfx5100-33,xe-0/0/19,1098572,1373216
q,1393947568702418,qfx5100-33,xe-0/0/19,1094912,1368640
q,1393947569703415,qfx5100-33,xe-0/0/19,1103065,1378832
t,1393947569874528,qfx5100-33,xe-0/0/16,12603371884,12603371884,0,0,
8426023,1613231610488,8628248712,0,3,5916761,5916761,0,0,0,757345408,0,0,0
t,1393947569874528,qfx5100-33,xe-0/0/18,12601953614,12601953614,0,0,
8446737,1613050071660,8649421552,0,5,131761619,131761619,0,0,84468,
16865487232,86495888,0,0
t,1393947569874528,qfx5100-33,xe-0/0/19,126009250,126009250,0,0,84469,
16129184128,86496392,0,0,12584980342,12584980342,0,0,8446866,1610877487744,
8649588432,12593703960,0
q,1393947575698402,qfx5100-33,xe-0/0/19,1102233,1377792
q,1393947576701398,qfx5100-33,xe-0/0/19,1107724,1384656
```

Consulte Tabla 113 en la página 996 para obtener la salida de estadísticas de cola y la salida de estadísticas de tráfico.Tabla 114 en la página 996 Los campos de las tablas se enumeran en el orden en que aparecen en el ejemplo de salida.

Tabla 113: Campos de salida para estadísticas de cola en archivos de análisis local

Campo	Description	Ejemplo en la salida
Tipo de registro	Tipo de estadística (monitoreo de colas o tráfico)	`q`
Tiempo (microsegundos)	Época de Unix (o tiempo de Unix) en microsegundos en los que se capturaron las estadísticas.	`1393947567698432`
Identificación de enrutadores	ID del dispositivo host de análisis de red.	`qfx5100-33`
Puerto	Nombre del puerto físico configurado para el análisis de red.	`xe-0/0/19`
Latencia (nanosegundos)	Latencia de la cola de tráfico en nanosegundos.	`1098572`
Profundidad de cola (bytes)	Profundidad de la cola de tráfico en bytes.	`1373216`

Tabla 114: Campos de salida para estadísticas de tráfico en archivos de análisis local

Campo	Description	Ejemplo en la salida
Tipo de registro	Tipo de estadística (monitoreo de colas o tráfico)	`t`
Tiempo (microsegundos)	Época de Unix (o tiempo de Unix) en microsegundos en los que se capturaron las estadísticas.	`1393947569874528`
Identificación de enrutadores	ID del dispositivo host de análisis de red.	`qfx5100-33`
Puerto	Nombre del puerto físico configurado para el análisis de red.	`xe-0/0/16`
rxpkt	Total de paquetes recibidos.	`12603371884`
rxucpkt	Total de paquetes de unidifusión recibidos.	`12603371884`

Tabla 114: Campos de salida para estadísticas de tráfico en archivos de análisis local *(Continued)*

Campo	Description	Ejemplo en la salida
rxmcpkt	Total de paquetes de multidifusión recibidos.	0
rxbcpkt	Total de paquetes de difusión recibidos.	0
rxpps	Total de paquetes recibidos por segundo.	8426023
rxbyte	Total de octetos recibidos.	1613231610488
rxbps	Total de bytes recibidos por segundo.	8628248712
rxdroppkt	Total de paquetes entrantes caídos.	0
rxcrcerr	Errores de CRC/Align recibidos.	3
txpkt	Total de paquetes transmitidos.	5916761
txucpkt	Total de paquetes de unidifusión transmitidos.	5916761
txmcpkt	Total de paquetes de multidifusión transmitidos.	0
txbcpkt	Total de paquetes de difusión transmitidos.	0
txpps	Total de paquetes transmitidos por segundo.	0
txbyte	Total de octetos transmitidos.	757345408
txbps	Bytes por segundo transmitidos.	0
txdroppkt	Total de paquetes transmitidos caídos.	0

Tabla 114: Campos de salida para estadísticas de tráfico en archivos de análisis local *(Continued)*

Campo	Description	Ejemplo en la salida
txcrcerr	Errores de CRC/Align transmitidos.	`0`

Comprender la configuración y el estado de Network Analytics

La función de análisis de red proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Puede habilitar el análisis de red configurando la supervisión de estadísticas de tráfico y colas.

> **NOTA**: En este tema se describe la configuración y el resultado de estado únicamente de Junos OS versión 13.2X50-D15 y 13.2X51-D10.

Si había habilitado la supervisión de tráfico o colas, puede emitir los comandos y para ver la configuración y el estado de la interfaz global, así como la de interfaces específicas.`show analytics configurationshow analytics status` El resultado que se muestra depende de su configuración en la interfaz global y en los niveles de interfaz específicos. Por ejemplo:

- Una configuración de interfaz global (para todas las interfaces) para deshabilitar la supervisión reemplaza la configuración para habilitarla en una interfaz.
- La configuración de interfaz para habilitar o deshabilitar la supervisión reemplaza a la configuración de interfaz global, a menos que la supervisión se haya deshabilitado globalmente para todas las interfaces.
- Si no hay ninguna configuración, ya sea para todas las interfaces o para una interfaz específica, la supervisión está desactivada de forma predeterminada (consulte).Tabla 115 en la página 999

Tabla 115 en la página 999 Describe la correlación entre la configuración de usuario y los valores que se muestran.

Tabla 115: Salida de configuración y estado en Junos OS versión 13.2X51-D10 y 13.2X50-D15

Configuración del usuario	Configuración global o del sistema		Configuración específica de la interfaz	
	Configuración	Estado	Configuración	Estado
No hay configuración de interfaz global o específica. Esta es la configuración predeterminada.	Automático	Automático	Automático	Deshabilitado
No hay configuración de interfaz global, pero la supervisión de interfaz específica está deshabilitada.	Automático	Automático	Deshabilitado	Deshabilitado
No hay configuración de interfaz global, pero la supervisión de interfaz específica está habilitada.	Automático	Automático	Habilitado	Habilitado
La supervisión se deshabilita globalmente y no hay configuración de interfaz.	Deshabilitado	Deshabilitado	Automático	Deshabilitado
La supervisión está deshabilitada tanto en el nivel de interfaz global como en el específico.	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado
La supervisión está deshabilitada en el nivel de interfaz global, pero se habilita en el nivel de interfaz específico. La configuración global de interfaz deshabilitada reemplaza a la configuración Habilitada para una interfaz específica.	Deshabilitado	Deshabilitado	Habilitado	Deshabilitado
La supervisión está habilitada para todas las interfaces, pero no hay ninguna configuración para la interfaz específica.	Habilitado	Habilitado	Automático	Habilitado

Tabla 115: Salida de configuración y estado en Junos OS versión 13.2X51-D10 y 13.2X50-D15 *(Continued)*

Configuración del usuario	Configuración global o del sistema		Configuración específica de la interfaz	
	Configuración	Estado	Configuración	Estado
La supervisión está habilitada tanto a nivel de interfaz global como específico.	Habilitado	Habilitado	Habilitado	Habilitado
La supervisión está habilitada para todas las interfaces, pero está deshabilitada para la interfaz específica.	Habilitado	Habilitado	Deshabilitado	Deshabilitado

SEE ALSO

queue-statistics

estadísticas de tráfico

Configurar la supervisión de colas y tráfico

La cola de análisis de red y la supervisión del tráfico proporcionan visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Esta función recopila datos del conmutador, analiza los datos mediante algoritmos sofisticados y captura los resultados en informes. Puede usar los informes para ayudar a solucionar problemas, tomar decisiones y ajustar los recursos según sea necesario.

Para habilitar la supervisión de colas y tráfico, defina primero una plantilla de perfil de recursos y, a continuación, aplique el perfil al sistema (para una configuración global) o a interfaces individuales.

NOTA: Puede configurar la supervisión de colas y tráfico solo en interfaces de red físicas; no se admiten las interfaces lógicas ni las interfaces físicas de Virtual Chassis (VCP).

NOTA: El procedimiento para configurar la supervisión de colas y tráfico en un conmutador independiente de la serie QFX requiere que Junos OS versión 13.2X51-D15 o posterior esté instalado en el dispositivo.

Para configurar la supervisión de colas en un conmutador independiente de la serie QFX:

1. Configure el intervalo de sondeo de supervisión de cola (en milisegundos) globalmente (para el sistema):

```
[edit]
set services analytics resource system polling-interval queue-monitoring interval
```

2. Configure un perfil de recursos para el sistema y habilite la supervisión de colas:

```
[edit]
set services analytics resource-profiles profile-name queue-monitoring
```

3. Configure valores altos y bajos del umbral de profundidad (en bytes) para la supervisión de colas en el perfil del sistema:

```
[edit]
set services analytics resource-profiles profile-name depth-threshold high number low number
```

Para valores altos y bajos, el intervalo es de 1 a 1.250.000.000 bytes y el valor predeterminado es 0 bytes.

NOTA: Puede configurar el umbral de profundidad o el umbral de latencia para el sistema, pero no ambos.

4. Aplique la plantilla de perfil de recursos al sistema para una configuración global:

```
[edit]
set services analytics resource system resource-profile profile-name
```

5. Configure un perfil de recursos específico de la interfaz y habilite la supervisión de colas para la interfaz:

```
[edit]
set services analytics resource-profiles profile-name queue-monitoring
```

6. Configure el umbral de latencia (valores altos y bajos) para la supervisión de colas en el perfil específico de la interfaz:

```
[edit]
set services analytics resource-profiles profile-name latency-threshold high number low number
```

Para valores altos y bajos, el rango es de 1 a 100,000,000 nanosegundos, y el valor predeterminado es 1,000,000 nanosegundos.

> **NOTA**: Puede configurar el umbral de profundidad o el umbral de latencia para las interfaces, pero no para ambas.

7. Aplique la plantilla de perfil de recursos para interfaces a una o más interfaces:

```
[edit]
set services analytics resource interfaces interface-name resource-profile profile-name
```

> **NOTA**: Si surge un conflicto entre las configuraciones del sistema y de la interfaz, la configuración específica de la interfaz reemplaza a la configuración global (del sistema).

Para configurar la supervisión del tráfico en un conmutador independiente de la serie QFX:

1. Configure el intervalo de sondeo de supervisión de tráfico (en segundos) para el sistema:

```
[edit]
set services analytics resource system polling-interval traffic-monitoring interval
```

2. Configure un perfil de recursos para el sistema y habilite la supervisión del tráfico en el perfil:

```
[edit]
set services analytics resource-profiles profile-name traffic-monitoring
```

3. Aplique el perfil de recursos al sistema para una configuración global:

```
[edit]
set services analytics resource system resource-profile profile-name
```

4. Configure un perfil de recursos para las interfaces y habilite la supervisión del tráfico en el perfil:

```
[edit]
set services analytics resource-profiles profile-name traffic-monitoring
```

> **NOTA**: Si surge un conflicto entre las configuraciones del sistema y de la interfaz, la configuración específica de la interfaz reemplaza a la configuración global (del sistema).

5. Aplique la plantilla de perfil de recursos a una o varias interfaces:

```
[edit]
set services analytics resource interfaces interface-name resource-profile profile-name
```

Configurar un archivo local para datos de análisis de red

La función de análisis de red proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Esta función recopila datos del conmutador, analiza los datos mediante algoritmos sofisticados y captura los resultados en informes. Los administradores de red pueden usar los informes para ayudar a solucionar problemas, tomar decisiones y ajustar los recursos según sea necesario.

Para guardar los datos de cola y estadísticas de tráfico en un archivo local, debe configurar un nombre de archivo para almacenarlos.

NOTA: El procedimiento para configurar un archivo local para almacenar estadísticas de supervisión de tráfico y colas requiere que Junos OS versión 13.2X51-D15 o posterior esté instalado en el dispositivo.

Para configurar un archivo local para almacenar estadísticas de supervisión de tráfico y colas:

1. Configure un nombre de archivo:

```
[edit]
set services analytics collector local file filename
```

   No hay ningún nombre de archivo predeterminado. Si no configura un nombre de archivo, las estadísticas de análisis de red no se guardan localmente.

2. Configure el número de archivos (de 2 a 1000 archivos):

```
[edit]
set services analytics collector local file filename files number
```

3. Configure el tamaño del archivo (de 10 a 4095 MB) en el formato de m:*x*

```
[edit]
set services analytics collector local file an size size
```

Configurar un recopilador remoto para datos de Streaming Analytics

La función de análisis de red proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Esta función recopila datos del conmutador, analiza los datos mediante algoritmos sofisticados y captura los resultados en informes. Los administradores de red pueden usar los informes para ayudar a solucionar problemas, tomar decisiones y ajustar los recursos según sea necesario.

Puede configurar un perfil de exportación para definir el formato de transmisión y el tipo de datos, y uno o más servidores remotos (recopiladores) para recibir datos de análisis de red de transmisión.

NOTA: El procedimiento para configurar un recopilador para recibir datos analíticos transmitidos requiere que Junos OS versión 13.2X51-D15 o posterior esté instalado en el dispositivo.

Para configurar un recopilador para recibir datos analíticos transmitidos:

1. Cree un perfil de exportación y especifique el formato de secuencia:

```
[edit]
set services analytics export-profiles profile-name stream-format format
```

2. Configure el perfil de exportación para que incluya información de interfaz:

```
[edit]
set services analytics export-profiles profile-name interface information
```

3. Configure el perfil de exportación para que incluya estadísticas de cola de interfaz:

```
[edit]
set services analytics export-profiles profile-name interface statistics queue
```

4. Configure el perfil de exportación para que incluya estadísticas de tráfico de la interfaz:

```
[edit]
set services analytics export-profiles profile-name interface statistics traffic
```

5. Configure el perfil de exportación para que incluya información del vínculo de estado de la interfaz:

```
[edit]
set services analytics export-profiles profile-name interface status link
```

6. Configure el perfil de exportación para que incluya información del sistema:

```
[edit]
set services analytics export-profiles profile-name system information
```

7. Configure el perfil de exportación para que incluya el estado de la cola del sistema:

```
[edit]
set services analytics export-profiles profile-name system status queue
```

8. Configure el perfil de exportación para incluir el estado del tráfico del sistema:

```
[edit]
set services analytics export-profiles profile-name system status traffic
```

9. Configure el protocolo de transporte para las direcciones del recopilador y aplique el perfil de exportación:

```
[edit]
set services analytics collector address ip-address port port transport protocol export-
profile profile-name
set services analytics collector address ip-address port port transport protocol export-
profile profile-name
```

NOTA: Si configura la opción o para los formatos JSON, CSV y TSV, también debe configurar el software cliente TCP o UDP en el recopilador remoto para procesar los registros separados por el carácter de nueva línea (\n) en el servidor remoto.`tcpudp`

Si configura la opción o para el formato GPB, también debe configurar el servidor de transmisión por secuencias de compilación TCP o UDP mediante el archivo.`tcpudp`**analytics.proto**

Ejemplo: Configurar estadísticas de cola y tráfico

in this section

- Requisitos | **1007**
- Descripción general | **1007**
- Configuración | **1008**

- Verificación | 1011

En este ejemplo, se muestra cómo configurar el análisis de red, que incluye la supervisión de colas y tráfico en un conmutador QFX3500 independiente.

NOTA: La configuración que se muestra en este ejemplo solo se admite en Junos OS versión 13.2X50-D15 y 13.2X51-D10.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador independiente QFX3500
- Un servidor de streaming externo para recopilar datos
- Software Junos OS versión 13.2X50-D15
- Software de servidor TCP (para servidores de transmisión remota)

Antes de configurar el análisis de red, asegúrese de contar con lo siguiente:

- Software de Junos OS versión 13.2X50-D15 o posterior instalado y ejecutándose en el conmutador QFX3500
- (Opcional para servidores de streaming) Software de servidor TCP configurado para procesar registros separados por un carácter de nueva línea (\n) en el servidor de transmisión por secuencias remoto
- Todos los demás dispositivos en ejecución

Descripción general

in this section

- Topología | 1008

La función de análisis de red proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Esta función recopila datos del conmutador, analiza los datos mediante algoritmos sofisticados y captura los resultados en informes. Los administradores de red pueden usar los informes para ayudar a solucionar problemas, tomar decisiones y ajustar los recursos según sea necesario. Puede habilitar el análisis de red configurando la supervisión de las estadísticas de tráfico y colas.

Topología

En este ejemplo, el conmutador QFX3500 está conectado a un servidor externo que se usa para transmitir datos estadísticos.

Configuración

in this section

- Configuración rápida de CLI | **1008**
- Configurar la supervisión de estadísticas de tráfico y colas | **1009**
- Configurar archivos de estadísticas locales | **1009**
- Configurar servidores de streaming | **1010**
- Resultados | **1011**

Para configurar el análisis de red, realice estas tareas:

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía.`[edit]`

```
[edit]
set services analytics interfaces all queue-statistics
set services analytics interfaces all latency-threshold high 900 low 300
set services analytics interfaces xe-0/0/1 traffic-statistics
set services analytics queue-statistics file qstats1.qs files 3 size 10
set services analytics queue-statistics interval 10
set services analytics traffic-statistics file tstats1.ts files 3 size 10
set services analytics traffic-statistics interval 2
```

```
set services analytics streaming-servers address 10.94.198.11 port 50001 stream-format json
stream-type queue-statistics
set services analytics streaming-servers address 10.94.198.11 port 50005 stream-format csv
stream-type traffic-statistics
```

Configurar la supervisión de estadísticas de tráfico y colas

Procedimiento paso a paso

Para configurar la supervisión de colas y tráfico en interfaces físicas:

> **NOTA**: La desactivación de la cola o la supervisión del tráfico sustituye a la configuración (habilitación) de esta característica. Para deshabilitar la supervisión, emita el o en el nivel de jerarquía.`no-queue-statisticsno-traffic-statistics[edit services analytics interfaces]`

1. Configure todas las interfaces para la supervisión de colas y establezca los umbrales de latencia (en microsegundos):

```
[edit]
set services analytics interfaces all queue-statistics
set services analytics interfaces all latency-threshold high 900 low 300
```

2. Configure una interfaz para la supervisión del tráfico:

```
[edit]
set services analytics interfaces xe-0/0/1 traffic-statistics
```

Configurar archivos de estadísticas locales

Procedimiento paso a paso

Para configurar archivos de estadísticas locales:

1. Configure el número de archivos de estadísticas de cola y cada tamaño de archivo en MB:

```
[edit]
set services analytics queue-statistics file qstats1.qs files 3 size 10m
```

2. Configurar el intervalo de recopilación de estadísticas de cola en milisegundos

```
[edit]
set services analytics queue-statistics interval 10
```

3. Configure el número de archivos de estadísticas de tráfico y cada tamaño de archivo en MB:

```
[edit]
set services analytics traffic-statistics file tstats1.ts files 3 size 10m
```

4. Configure el intervalo de recopilación de estadísticas de tráfico en segundos:

```
[edit]
set services analytics traffic-statistics interval 2
```

Configurar servidores de streaming

Procedimiento paso a paso

Para configurar servidores de streaming para recibir datos de supervisión:

> **NOTA**: Además de configurar los servidores de streaming, también debe configurar el software cliente TCP para procesar los registros separados por el carácter de nueva línea (\n) en el servidor remoto.

1. Configure una dirección IP y un puerto del servidor para la supervisión de estadísticas de cola:

```
[edit]
set services analytics streaming-servers address 10.94.198.11 port 50001 stream-format json
stream-type queue-statistics
```

2. Configure una dirección IP y un puerto del servidor para la supervisión de estadísticas de tráfico:

```
[edit]
set services analytics streaming-servers address 10.94.198.11 port 50005 stream-format csv
stream-type traffic-statistics
```

Resultados

Mostrar los resultados de la configuración:

```
[edit services analytics]
user@switch> show configuration
    queue-statistics {
        file qstats1.qs size 10m files 3;
        interval 10;
    }
    traffic-statistics {
        file tstats1.ts size 10m files 3;
        interval 2;
    }
    interfaces {
        xe-0/0/1 {
            traffic-statistics;
        }
        all {
            queue-statistics;
            latency-threshold high 900 low 300;
        }
    }
```

Verificación

in this section

- Comprobar la configuración de Network Analytics | **1012**
- Verificar el estado de análisis de red | **1012**
- Comprobar la configuración de los servidores de streaming | **1013**

Verificar estadísticas de cola | 1014
Verificar estadísticas de tráfico | 1014

Confirme que la configuración es correcta y funciona según lo esperado realizando estas tareas:

Comprobar la configuración de Network Analytics

Propósito

Verifique la configuración para el análisis de red.

Acción

Desde el modo operativo, escriba el comando para mostrar la configuración de supervisión de tráfico y colas.`show analytics configuration`

```
user@host> show analytics configuration

Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Enabled, Poll interval: 10 milliseconds
   Depth threshold high: 0 bytes, low: 0 bytes
   Latency threshold high: 900 microseconds, low: 300 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                             (bytes)            (microseconds)
xe-0/0/1     Enabled      Auto            0         0           900       300
```

Significado

El resultado muestra información sobre el monitoreo de tráfico y colas en el conmutador.

Verificar el estado de análisis de red

Propósito

Verifique el estado operativo de análisis de red del conmutador.

Acción

Desde el modo operativo, escriba el comando para mostrar el estado de supervisión del tráfico y la cola.`show analytics status`

```
user@host> show analytics status

Global configurations:
   Traffic statistics: Auto, Poll interval: 2 seconds
   Queue statistics: Auto, Poll interval: 10 milliseconds
   Depth threshold high: 1228800 bytes, low: 1024 bytes
   Latency threshold high: 900 microseconds, low: 300 microseconds
Interface     Traffic       Queue        Depth-threshold      Latency-threshold
            Statistics    Statistics      High      Low         High      Low
                                             (bytes)            (microseconds)
xe-0/0/1     Enabled       Auto          1228800   1024         900       300
xe-0/0/7     Auto          Auto          1228800   1024         900       300
xe-0/0/8     Auto          Auto          1228800   1024         900       300
```

Comprobar la configuración de los servidores de streaming

Propósito

Compruebe que la configuración para transmitir datos a servidores remotos está funcionando.

Acción

Desde el modo operativo, escriba el comando para mostrar la configuración de los servidores de streaming.`show analytics streaming-servers`

```
user@host> show analytics streaming-servers

Address        Port     Stream-Format    Stream-Type   State         Sent
10.94.198.11   50001    json             QS            Established   1100
10.94.198.11   50005    csv              TS/QS         In Progress      0
```

Significado

El resultado muestra información sobre el servidor de transmisión por secuencias remoto.

Verificar estadísticas de cola

Propósito

Compruebe que la recopilación de estadísticas de cola funciona.

Acción

Desde el modo operativo, escriba el comando para mostrar las estadísticas de la cola.`show analytics queue-statistics`

```
user@host> show analytics queue-statistics

Time                Interface   Queue-length (bytes)   Latency (us)
Apr 6 0:17:18.224   xe-0/0/1            1043952            835
Apr 6 0:17:18.234   xe-0/0/1            1053520            842
Apr 6 0:17:18.244   xe-0/0/1            1055184            844
```

Significado

El resultado muestra información de estadísticas de cola como se esperaba.

Verificar estadísticas de tráfico

Propósito

Compruebe que la recopilación de estadísticas de tráfico funciona.

Acción

Desde el modo operativo, introduzca el comando para mostrar las estadísticas de tráfico.`show analytics traffic-statistics`

```
user@host> show analytics traffic-statistics

Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/1
  Traffic Statistics:                Receive            Transmit
  Total octets:                4797548752936        408886273632
  Total packet:                   5658257464          3190613435
  Octets per second:                       0                   0
```

```
  Packet per second:                        0                   0
  Octets dropped:                           0           252901000
  Packet dropped:                           0              252901
  Utilization:                           0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/7
  Traffic Statistics:                Receive            Transmit
  Total octets:                4790866253100           477139024
  Total packet:                   5624473639              477944
  Octets per second:                        0                   0
  Packet per second:                        0                   0
  Octets dropped:                           0           166582000
  Packet dropped:                           0              166582
  Utilization:                           0.0%                0.0%
Time: Apr 5 19:52:48.549, Physical interface: xe-0/0/8
  Traffic Statistics:                Receive            Transmit
  Total octets:                4789797668456           764910024
  Total packet:                   5623280870              765715
  Octets per second:                        0                   0
  Packet per second:                        0                   0
  Octets dropped:                           0           156099000
  Packet dropped:                           0              156099
  Utilization:                           0.0%                0.0%
```

Significado

El resultado muestra información de estadísticas de tráfico como se esperaba.

Ejemplo: Configurar la supervisión de colas y tráfico

in this section

- Requisitos | **1016**
- Descripción general | **1016**
- Configuración | **1017**
- Verificación | **1025**

En este ejemplo se muestra cómo configurar la característica de análisis de red mejorada, incluida la supervisión de colas y tráfico.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador independiente QFX5100
- Un servidor de streaming externo para recopilar datos
- Software Junos OS versión 13.2X51-D15
- Software de servidor TCP (para servidores de transmisión remota)

Antes de configurar el análisis de red, asegúrese de contar con lo siguiente:

- Software de Junos OS versión 13.2X51-D15 o posterior instalado y ejecutándose en el conmutador QFX5100.
- (Opcional para servidores de streaming para los formatos JSON, CSV y TSV) Software de servidor TCP o UDP configurado para procesar registros separados por un carácter de nueva línea (\n) en el servidor de transmisión por secuencias remoto.
- (Opcional para servidores de streaming para el formato GPB) TCP o UDP compilan el servidor de streaming utilizando el archivo.**analytics.proto**
- Todos los demás dispositivos de red en ejecución.

Descripción general

in this section

- Topología | **1017**

La función de análisis de red proporciona visibilidad del rendimiento y el comportamiento de la infraestructura del centro de datos. Esta función recopila datos del conmutador, analiza los datos mediante algoritmos sofisticados y captura los resultados en informes. Los administradores de red pueden usar los informes para ayudar a solucionar problemas, tomar decisiones y ajustar los recursos según sea necesario.

Para habilitar el análisis de red, primero defina una plantilla de perfil de recursos y, a continuación, aplique el perfil al sistema (para una configuración global) o a interfaces individuales.

> **NOTA**: La desactivación de la cola o la supervisión del tráfico sustituye a la configuración (habilitación) de esta característica. Para deshabilitar la supervisión, aplique un perfil de recursos que incluya la instrucción de configuración or en el nivel de jerarquía.`no-queue-monitoringno-traffic-monitoring`[`edit services analytics resource-profiles`]

Topología

En este ejemplo, el conmutador QFX5100 está conectado a un servidor externo que se usa para transmitir datos estadísticos.

Configuración

in this section

- Configuración rápida de CLI | **1017**
- Configurar el intervalo de sondeo para la supervisión de colas y tráfico | **1018**
- Configurar un archivo de estadísticas locales | **1019**
- Configurar y aplicar un perfil de recursos para el sistema | **1019**
- Configurar y aplicar un perfil de recursos para una interfaz | **1020**
- Configurar un perfil y un recopilador de exportación para datos de streaming | **1021**

Para configurar las características de análisis de red, realice estas tareas:

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía.`[edit]`

```
[edit]
set services analytics resource system polling-interval queue-monitoring 1000
set services analytics resource system polling-interval traffic-monitoring 5
set services analytics collector local file an.stats
set services analytics collector local file an files 3
set services analytics collector local file an size 10m
```

```
set services analytics resource-profiles sys-rp queue-monitoring
set services analytics resource-profiles sys-rp traffic-monitoring
set services analytics resource-profiles sys-rp depth-threshold high 999999 low 99
set services analytics resource system resource-profile sys-rp
set services analytics resource-profiles if-rp queue-monitoring
set services analytics resource-profiles if-rp traffic-monitoring
set services analytics resource-profiles if-rp latency-threshold high 2300 low 20
set services analytics resource interfaces xe-0/0/16 resource-profile if-rp
set services analytics resource interfaces xe-0/0/18 resource-profile if-rp
set services analytics resource interfaces xe-0/0/19 resource-profile if-rp
set services analytics export-profiles ep stream-format gpb
set services analytics export-profiles ep interface information
set services analytics export-profiles ep interface statistics queue
set services analytics export-profiles ep interface statistics traffic
set services analytics export-profiles ep interface status link
set services analytics export-profiles ep system information
set services analytics export-profiles ep system status queue
set services analytics export-profiles ep system status traffic
set services analytics collector address 10.94.198.11 port 50001 transport tcp export-profile ep
set services analytics collector address 10.94.184.25 port 50013 transport udp export-profile ep
```

Configurar el intervalo de sondeo para la supervisión de colas y tráfico

Procedimiento paso a paso

Para configurar la cola del intervalo de sondeo y la supervisión del tráfico globalmente:

1. Configure el intervalo de sondeo de supervisión de cola (en milisegundos) para el sistema:

```
[edit]
set services analytics resource system polling-interval queue-monitoring 1000
```

2. Configure el intervalo de sondeo de supervisión de tráfico (en segundos) para el sistema:

```
[edit]
set services analytics resource system polling-interval traffic-monitoring 5
```

Configurar un archivo de estadísticas locales

Procedimiento paso a paso

Para configurar un archivo para la recopilación de estadísticas locales:

1. Configure el nombre de archivo:

```
[edit]
set services analytics collector local file an.stats
```

2. Configure el número de archivos:

```
[edit]
set services analytics collector local file an files 3
```

3. Configure el tamaño del archivo:

```
[edit]
set services analytics collector local file an size 10m
```

Configurar y aplicar un perfil de recursos para el sistema

Procedimiento paso a paso

Para definir una plantilla de perfil de recursos para recursos de supervisión de tráfico y cola:

1. Configure un perfil de recursos y habilite la supervisión de colas:

```
[edit]
set services analytics resource-profiles sys-rp queue-monitoring
```

2. Habilite la supervisión del tráfico en el perfil:

```
[edit]
set services analytics resource-profiles sys-rp traffic-monitoring
```

3. Configure el umbral de profundidad (valores altos y bajos) para la supervisión de colas en el perfil:

```
[edit]
set services analytics resource-profiles sys-rp depth-threshold high 999999 low 99
```

4. Aplique la plantilla de perfil de recursos al tipo de recurso del sistema para una configuración global:

```
[edit]
set services analytics resource system resource-profile sys-rp
```

Configurar y aplicar un perfil de recursos para una interfaz

Procedimiento paso a paso

Puede configurar la supervisión de colas y tráfico para una o varias interfaces específicas. La configuración específica de la interfaz reemplaza a la configuración global (del sistema). Para definir una plantilla de perfil de recursos para recursos de supervisión de tráfico y cola para una interfaz:

1. Configure un perfil de recursos y habilite la supervisión de colas:

```
[edit]
set services analytics resource-profiles if-rp queue-monitoring
```

2. Habilite la supervisión del tráfico en el perfil:

```
[edit]
set services analytics resource-profiles if-rp traffic-monitoring
```

3. Configure el umbral de latencia (valores altos y bajos) para la supervisión de colas en el perfil:

```
[edit]
set services analytics resource-profiles if-rp latency-threshold high 2300 low 20
```

4. Aplique la plantilla de perfil de recursos al tipo de recurso de interfaces para interfaces específicas:

```
[edit]
set services analytics resource interfaces xe-0/0/16 resource-profile if-rp
```

```
set services analytics resource interfaces xe-0/0/18 resource-profile if-rp
set services analytics resource interfaces xe-0/0/19 resource-profile if-rp
```

Configurar un perfil y un recopilador de exportación para datos de streaming

Procedimiento paso a paso

Para configurar un recopilador (servidor de streaming) para recibir datos de supervisión:

1. Cree un perfil de exportación y especifique el formato de secuencia:

```
[edit]
set services analytics export-profiles ep stream-format gpb
```

2. Configure el perfil de exportación para que incluya información de interfaz:

```
[edit]
set services analytics export-profiles ep interface information
```

3. Configure el perfil de exportación para que incluya estadísticas de cola de interfaz:

```
[edit]
set services analytics export-profiles ep interface statistics queue
```

4. Configure el perfil de exportación para que incluya estadísticas de tráfico de la interfaz:

```
[edit]
set services analytics export-profiles ep interface statistics traffic
```

5. Configure el perfil de exportación para que incluya información del vínculo de estado de la interfaz:

```
[edit]
set services analytics export-profiles ep interface status link
```

6. Configure el perfil de exportación para que incluya información del sistema:

```
[edit]
set services analytics export-profiles ep system information
```

7. Configure el perfil de exportación para que incluya el estado de la cola del sistema:

```
[edit]
set services analytics export-profiles ep system status queue
```

8. Configure el perfil de exportación para incluir el estado del tráfico del sistema:

```
[edit]
set services analytics export-profiles ep system status traffic
```

9. Configure el protocolo de transporte para las direcciones del recopilador y aplique un perfil de exportación:

```
[edit]
set services analytics collector address 10.94.198.11 port 50001 transport tcp export-profile
ep
set services analytics collector address 10.94.184.25 port 50013 transport udp export-profile
ep
```

NOTA: Si configura la opción o para los formatos JSON, CSV y TSV, también debe configurar el software cliente TCP o UDP en el recopilador remoto para procesar los registros separados por el carácter de nueva línea (\n) en el servidor remoto.`tcpudp`

Si configura la opción o para el formato GPB, también debe configurar el servidor de transmisión por secuencias de compilación TCP o UDP mediante el archivo.`tcpudp`**analytics.proto**

Resultados

Mostrar los resultados de la configuración:

```
[edit services analytics]
user@switch# run show configuration
services {
    analytics {
        export-profiles {
            ep {
                stream-format gpb;
                interface {
                    information;
                    statistics {
                        traffic;
                        queue;
                    }
                    status {
                        link;
                    }
                }
                system {
                    information;
                    status {
                        traffic;
                        queue;
                    }
                }
            }
        }
        resource-profiles {
            sys-rp {
                queue-monitoring;
                traffic-monitoring;
                depth-threshold high 99999 low 99;
            }
            if-rp {
                queue-monitoring;
                traffic-monitoring;
                latency-threshold high 2300 low 20;
            }
        }
```

```
        resource {
            system {
                resource-profile sys-rp;
                polling-interval {
                    traffic-monitoring 5;
                    queue-monitoring 1000;
                }
            }
            interfaces {
                xe-0/0/16 {
                    resource-profile if-rp;
                }
                xe-0/0/18 {
                    resource-profile if-rp;
                }
                xe-0/0/19 {
                    resource-profile if-rp;
                }
            }
        }
        collector {
            local {
                file an size 10m files 3;
            }
            address 10.94.184.25 {
                port 50013 {
                    transport udp {
                        export-profile ep;
                    }
                }
            }
            address 10.94.198.11 {
                port 50001 {
                    transport tcp {
                        export-profile ep;
                    }
                }
            }
        }
    }
}
```

Verificación

in this section

- Comprobar la configuración de Network Analytics | 1025
- Verificar el estado de análisis de red | 1026
- Comprobar la configuración del recopilador | 1027

Confirme que la configuración es correcta y funciona según lo esperado realizando estas tareas:

Comprobar la configuración de Network Analytics

Propósito

Verifique la configuración para el análisis de red.

Acción

Desde el modo operativo, escriba el comando para mostrar la configuración de supervisión de tráfico y colas.`show analytics configuration`

```
user@host> show analytics configuration

Traffic monitoring status is enabled
Traffic monitoring polling interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes

Interface     Traffic       Queue        Queue depth              Latency
            Statistics    Statistics      threshold              threshold
                                        High         Low      High      Low
                                           (bytes)            (nanoseconds)
xe-0/0/16   enabled       enabled        n/a          n/a      2300      20
xe-0/0/18   enabled       enabled        n/a          n/a      2300      20
xe-0/0/19   enabled       enabled        n/a          n/a      2300      20
```

Significado

El resultado muestra la información de configuración de monitoreo de tráfico y cola en el conmutador.

Verificar el estado de análisis de red

Propósito

Verifique el estado operativo de análisis de red del conmutador.

Acción

Desde el modo operativo, escriba el comando para mostrar el tráfico global y el estado de supervisión de colas.`show analytics status global`

```
user@host> show analytics status global

Traffic monitoring status is enabled
Traffic monitoring pollng interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes
```

Desde el modo operativo, escriba el comando para mostrar el estado de supervisión de la interfaz y de la cola global.`show analytics status`

```
user@host> show analytics status

Traffic monitoring status is enabled
Traffic monitoring pollng interval : 5 seconds
Queue monitoring status is enabled
Queue monitoring polling interval : 1000 milliseconds
Queue depth high threshold : 99999 bytes
Queue depth low threshold : 99 bytes

Interface     Traffic    Queue      Queue depth             Latency
            Statistics Statistics    threshold             threshold
                                   High       Low        High      Low
                                      (bytes)            (nanoseconds)
xe-0/0/16   enabled    enabled     n/a        n/a        2300      20
```

```
xe-0/0/18   enabled    enabled     n/a        n/a        2300      20
xe-0/0/19   enabled    enabled     n/a        n/a        2300      20
```

Significado

El resultado muestra el estado global y de interfaz de la supervisión de tráfico y colas en el conmutador.

Comprobar la configuración del recopilador

Propósito

Acción

Compruebe que la configuración del recopilador de datos transmitidos está funcionando.

Desde el modo operativo, escriba el comando para mostrar la configuración de los servidores de streaming.`show analytics collector`

```
user@host> show analytics collector

Address        Port   Transport  Stream format  State           Sent
10.94.184.25   50013  udp        gpb            n/a             484
10.94.198.11   50001  tcp        gpb            In progress     0
```

Significado

El resultado muestra la configuración del recopilador.

> **NOTA**: El estado de conexión de un puerto configurado con el protocolo de transporte siempre se muestra como .`udpn/a`

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
13.2X51-D15	En Junos OS versión 13.2X51-D15, se mejoró la función de análisis de red y se realizaron cambios exhaustivos en las jerarquías y las instrucciones de la CLI.
13.2X51-D15	A partir de Junos OS versión 13.2X51-D15, la función de análisis de red proporciona las siguientes mejoras:
13.2X51-D15	A partir de Junos OS versión 13.2X51-D15, las mejoras en la función de análisis de red provocan cambios en la CLI al configurar la función.
13.2X51-D15	A partir de Junos OS versión 13.2X51-D15, el análisis de red admite los siguientes formatos de datos y salida de streaming:
13.2X51-D15	A partir de Junos OS versión 13.2X51-D15, las estadísticas de monitoreo de tráfico y colas se pueden almacenar localmente en un solo archivo.
13.2X51-D15	El procedimiento para configurar la supervisión de colas en un conmutador independiente de la serie QFX requiere que Junos OS versión 13.2X51-D15 o posterior esté instalado en el dispositivo.
13.2X51-D15	El procedimiento para configurar un archivo local para almacenar estadísticas de supervisión de tráfico y colas requiere que Junos OS versión 13.2X51-D15 o posterior esté instalado en el dispositivo.
13.2X51-D15	El procedimiento para configurar un recopilador para recibir datos analíticos transmitidos requiere que Junos OS versión 13.2X51-D15 o posterior esté instalado en el dispositivo.

9

PART IN COVERPAGE

Imitación de puerto

Duplicación de puertos y analizadores | 1030

chapter label in part12

Duplicación de puertos y analizadores

in this chapter

- Duplicación de puertos y analizadores | **1030**
- Configuración de analizadores y duplicación de puertos | **1071**
- Configuración de instancias de creación de reflejo de puertos | **1179**
- Configuración de la duplicación de puertos en interfaces físicas | **1191**
- Configuración de la creación de reflejo de puertos en interfaces lógicas | **1207**
- Configuración de la duplicación de puertos para varios destinos | **1248**
- Configuración de la duplicación de puertos para destinos remotos | **1261**
- Configuración del análisis local y remoto de creación de reflejo de puertos | **1274**
- Duplicación de puerto 1:N a múltiples destinos en conmutadores | **1298**
- Supervisión de la duplicación de puertos | **1303**
- Configurar la duplicación de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3 | **1304**
- Solución de problemas de duplicación de puertos | **1313**

Duplicación de puertos y analizadores

summary

En esta sección se describe cómo la creación de reflejo de puertos envía tráfico de red a las aplicaciones del analizador.

in this section

- Descripción de la duplicación de puertos y los analizadores | **1031**
- Duplicación de puertos en conmutadores EX2300, EX3400 y EX4300 | **1047**

- Duplicación de puertos en conmutadores ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 y EX8200 | **1053**
- Duplicación de puertos en firewalls de la serie SRX | **1060**
- Descripción de la creación de reflejo de puertos de capa 2 | **1060**
- Propiedades de duplicación de puertos de capa 2 | **1061**
- Aplicación de tipos de duplicación de puertos de capa 2 | **1063**
- Restricciones en la duplicación de puertos de capa 2 | **1069**

Descripción de la duplicación de puertos y los analizadores

in this section

- Términos y definiciones del analizador y la creación de reflejo de puertos | **1033**
- Tipos de instancias | **1037**
- Duplicación de puertos y STP | **1038**
- Restricciones y limitaciones | **1039**
- Duplicación de puertos en conmutadores de la serie QFX10000 | **1044**
- Duplicación de puertos en QFabric | **1044**
- Duplicación de puertos en conmutadores de la serie OCX | **1046**

La duplicación de puertos y los analizadores envían tráfico de red a dispositivos que ejecutan aplicaciones de análisis. Una réplica de puerto copia el tráfico IP de capa 3 en una interfaz. Un analizador copia paquetes en puente (capa 2) en una interfaz. El tráfico reflejado puede obtenerse de una o varias interfaces. Puede utilizar un dispositivo conectado a una interfaz de salida reflejada que ejecute una aplicación de analizador para realizar tareas como supervisar el cumplimiento, aplicar directivas, detectar intrusiones, supervisar el rendimiento de la red, correlacionar eventos y otros problemas de la red.

En enrutadores que contienen un circuito integrado específico de la aplicación (ASIC) o un procesador de Internet de la serie T, la duplicación de puertos copia paquetes de unidifusión que entran o salen de un puerto o que ingresan una VLAN y envía esas copias a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. El tráfico reflejado es recibido por aplicaciones que le ayudan a analizar ese tráfico.

La duplicación de puertos es diferente del muestreo de tráfico. En el muestreo de tráfico, se envía una clave de muestreo basada en el encabezado IPv4 al motor de enrutamiento, donde se coloca una clave en un archivo o se cflowd. Los paquetes basados en esa clave se envían a un servidor cflowd. En la duplicación de puertos, todo el paquete se copia y se envía a través de la interfaz especificada, donde se puede capturar y analizar en detalle.

Use la duplicación de puertos para enviar tráfico a dispositivos que analizan el tráfico con fines como supervisar el cumplimiento, aplicar políticas, detectar intrusiones, supervisar y predecir patrones de tráfico, correlacionar eventos, etc. La creación de reflejo de puertos es necesaria cuando se desea realizar un análisis de tráfico, ya que un conmutador normalmente envía paquetes únicamente al puerto al que está conectado el dispositivo de destino. Probablemente no desee enviar los paquetes originales para su análisis antes de que se reenvíen debido a la demora que esto causaría, por lo que la alternativa común es configurar la duplicación de puertos para enviar copias del tráfico de unidifusión a otra interfaz y ejecutar una aplicación de analizador en un dispositivo conectado a esa interfaz. .

Para configurar la creación de reflejo de puertos, configure una instancia de creación de reflejo de puertos. pero no especifique una entrada para ella. En su lugar, cree un filtro de firewall que especifique el tráfico necesario y lo dirija a la instancia. Utilice la acción en un término del filtro para esto.`port-mirror` `then` El filtro del firewall debe configurarse como .`family inet`

Tenga en cuenta el rendimiento al configurar la duplicación de puertos. La configuración del filtro de firewall para reflejar solo los paquetes necesarios reduce la posibilidad de un impacto en el rendimiento.

Puede configurar una instrucción del analizador para definir tanto el tráfico de entrada como el tráfico de salida en la misma configuración del analizador. El tráfico que se va a analizar puede ser el tráfico que entra o sale de una interfaz, o el tráfico que entra en una VLAN. La configuración del analizador le permite enviar este tráfico a una interfaz de salida, instancia o VLAN. Puede configurar un analizador en la jerarquía.`[edit forwarding-options analyzer]`

> **NOTA**: En los conmutadores de la serie EX, cuando deshabilite cualquier interfaz en una VLAN de duplicación de puerto remoto, deberá volver a habilitar la interfaz deshabilitada y volver a configurar la sesión del analizador para reanudar la duplicación de puertos.

Puede utilizar la creación de reflejo de puertos para copiar:

- Todos los paquetes que entran o salen de una interfaz en cualquier combinación. Las copias de los paquetes que entran en algunas interfaces y de los paquetes que salen de otras interfaces se pueden enviar a la misma interfaz local o VLAN. Si configura la creación de reflejo de puertos para copiar

paquetes que salen de una interfaz, el tráfico que se origina en ese conmutador o dispositivo de nodo (en un sistema QFabric) no se copia cuando sale. Solo el tráfico conmutado se copia al salir. (Consulte la limitación de la duplicación de salida a continuación).

- Todos o cualquiera de los paquetes que ingresan a una VLAN. No puede utilizar la creación de reflejo de puertos para copiar paquetes que salen de una VLAN.
- Una muestra filtrada por firewall de paquetes que ingresan a un puerto o VLAN.
- Los filtros de firewall no son compatibles con los puertos de salida; Es decir, no puede especificar un muestreo basado en políticas de paquetes que salgan de una interfaz
- En entornos VXLAN, la duplicación de puertos basada en filtros de firewall no se admite en interfaces orientadas al núcleo o al spine.

Puede configurar tanto el muestreo de tráfico como la duplicación de puertos, estableciendo una frecuencia de muestreo independiente y una longitud de ejecución para los paquetes reflejados en puertos. Sin embargo, si se selecciona un paquete tanto para el muestreo de tráfico como para la creación de reflejo de puertos, solo se ejecuta la creación de reflejo de puerto, ya que tiene prioridad. En otras palabras, si configura una interfaz para muestrear el tráfico de cada entrada de paquete a la interfaz y la creación de reflejo del puerto también selecciona ese paquete para copiarlo y enviarlo al puerto de destino, solo se ejecutará el proceso de creación de reflejo del puerto. Los paquetes muestreados de tráfico que no están seleccionados para la creación de reflejo de puertos se siguen muestreando y reenviando al servidor cflowd.

Términos y definiciones del analizador y la creación de reflejo de puertos

En las tablas siguientes se proporcionan términos y definiciones para la documentación del analizador y la creación de reflejo de puertos.

Tabla 116: Terminología

Término	Definición
Analizador	Para los conmutadores EX2300, EX3400 o EX4300, en una configuración de duplicación (analizador) en un analizador incluye: • El nombre del analizador • Puertos de origen (entrada) o VLAN (opcional)
Instancia del analizador	Configuración de duplicación de puertos que incluye un nombre, interfaces de origen o VLAN de origen, y un destino para paquetes reflejados (ya sea una interfaz local o una VLAN).

Interfaz de salida del analizador (también conocida como puerto de monitor)	Interfaz a la que se envía el tráfico reflejado y a la que está conectada una aplicación de analizador de protocolos. Para los conmutadores EX2300, EX3400 y EX4300, las interfaces utilizadas como salida para un analizador deben configurarse como conmutación Ethernet de familia. Además, se aplican las siguientes limitaciones para las interfaces de salida del analizador: • No puede ser también un puerto de origen. • No se puede utilizar para cambiar. • No participe en protocolos de capa 2, como el protocolo de árbol de expansión (STP), cuando forme parte de una configuración de creación de reflejo de puertos. • Si el ancho de banda de la interfaz de salida del analizador no es suficiente para manejar el tráfico de los puertos de origen, se descartarán los paquetes de desbordamiento.
VLAN del analizador (también conocida como VLAN de monitor)	VLAN a la que se envía el tráfico reflejado. El tráfico reflejado puede ser utilizado por una aplicación de analizador de protocolos. Las interfaces miembro de la VLAN de monitor se distribuyen por los conmutadores de la red.
Analizador basado en dominios de puente	Una sesión de analizador configurada para usar dominios de puente para entrada, salida o ambos.
Analizador predeterminado	Un analizador con parámetros de duplicación predeterminados. De forma predeterminada, la velocidad de creación de reflejo es 1 y la longitud máxima del paquete es la longitud del paquete completo.
Espejo de puerto global	Una configuración de creación de reflejo de puerto que no tiene un nombre de instancia. La acción del filtro del firewall port-mirror será la acción para la configuración del filtro del firewall.
Interfaz de entrada (también conocida como interfaz reflejada o monitoreada)	Una interfaz que copia el tráfico en la interfaz reflejada. Este tráfico puede entrar o salir (entrada o salida) de la interfaz. Una interfaz de entrada reflejada no se puede utilizar como interfaz de salida para el dispositivo analizador.
Analizador basado en LAG	Un analizador que tiene un grupo de agregación de vínculos (LAG) especificado como interfaz de entrada (entrada) en la configuración del analizador.

Duplicación de puerto local	Configuración de creación de reflejo de puertos en la que los paquetes reflejados se copian en una interfaz del mismo conmutador.
Estación de monitoreo	Equipo que ejecuta una aplicación de analizador de protocolos.
Analizador basado en el siguiente salto	Una configuración de analizador que utiliza el grupo del salto siguiente como salida a un analizador.
Sesión de analizador nativo	Una sesión de analizador que tiene definiciones de entrada y salida en su configuración de analizador.
Espejado basado en políticas	Duplicación de paquetes que coinciden con un término de filtro de firewall. La acción se utiliza en el filtro del firewall para enviar paquetes especificados al analizador.`analyzer` *`analyzer-name`*
Analizador basado en puertos	Una sesión de analizador cuya configuración define interfaces tanto para la entrada como para la salida.
Instancia de creación de reflejo de puerto	Una configuración de duplicación de puertos que no especifica un origen de entrada; Solo especifica un destino de salida. Se debe definir una configuración de filtro de firewall para el origen de entrada. Se debe definir una configuración de filtro de firewall para reflejar paquetes que coincidan con las condiciones de coincidencia definidas en el término de filtro de firewall. El elemento de acción port-mirror-instance instance-name en la configuración del filtro de firewall se utiliza para enviar paquetes al analizador y estos paquetes forman el origen de entrada. Utilice la acción de la configuración del filtro del firewall para enviar paquetes al espejo de puerto.`port-mirror-instance` *`instance-name`* **NOTA**: La instancia de duplicación de puertos no es compatible con dispositivos NFX150.
Aplicación del analizador de protocolos	Una aplicación utilizada para examinar paquetes transmitidos a través de un segmento de red. También se suele llamar analizador de red, rastreador de paquetes o sonda.

Interfaz de salida (también conocida como interfaz de monitor)	Interfaz a la que se envían las copias de paquetes y a la que está conectado un dispositivo que ejecuta un analizador. Las siguientes limitaciones se aplican a una interfaz de salida (la interfaz espejo de destino): • No puede ser también un puerto de origen. • No se puede utilizar para cambiar. • No puede ser una interfaz Ethernet agregada (LAG). • No se puede participar en protocolos de capa 2, como el protocolo de árbol de expansión (STP). • Las asociaciones de VLAN existentes se pierden cuando se aplica la duplicación de puertos a la interfaz. • Los paquetes se descartan si la capacidad de la interfaz de salida es insuficiente para manejar el tráfico de los puertos de origen reflejados.
Dirección IP de salida	Dirección IP del dispositivo que ejecuta una aplicación de análisis. El dispositivo puede estar en una red remota. Cuando utilice esta función: • Los paquetes duplicados están encapsulados en Gre. La aplicación del analizador debe ser capaz de desencapsular paquetes encapsulados en GRE o los paquetes encapsulados en GRE deben desencapsularse antes de llegar a la aplicación del analizador. (Puede usar un rastreador de red para desencapsular los paquetes). • La dirección IP de salida no puede estar en la misma subred que ninguna de las interfaces de administración del conmutador. • Si crea instancias de enrutamiento virtual y una configuración de analizador que incluye una dirección IP de salida, la dirección IP de salida pertenece a la instancia de enrutamiento virtual predeterminada (tabla de enrutamiento inet.0).

VLAN de salida (también conocida como VLAN de monitor o analizador)	VLAN a donde se envían copias de los paquetes y a donde está conectado un dispositivo que ejecuta un analizador. La VLAN del analizador puede abarcar varios conmutadores. Se aplican las siguientes limitaciones a una VLAN de salida: • No puede ser una VLAN privada ni un rango de VLAN. • No se puede compartir mediante varias instrucciones.`analyzer` • No puede ser miembro de ninguna otra VLAN. • No puede ser una interfaz Ethernet agregada (LAG). • En algunos conmutadores, solo una interfaz puede ser miembro de la VLAN del analizador. Esta limitación no se aplica en el conmutador QFX10000. Cuando se refleja el tráfico de entrada, varias interfaces de QFX10000 pueden pertenecer a la VLAN de salida y el tráfico se refleja desde todas esas interfaces. Si el tráfico de salida se refleja en un conmutador QFX10000, solo una interfaz puede ser miembro de la VLAN del analizador.
Duplicación remota de puertos	Funciona igual que la creación de reflejo del puerto local, excepto que el tráfico reflejado no se copia en un puerto del analizador local, sino que se inunda en una VLAN del analizador que se crea específicamente para recibir tráfico reflejado. No puede enviar paquetes reflejados a una dirección IP remota en un sistema QFabric.
Analizador basado en VLAN	Una sesión de analizador cuya configuración utiliza VLAN tanto para la entrada como para la salida, o para la entrada o la salida.

SEE ALSO

Duplicación de puertos y analizadores | **1030**

Tipos de instancias

Para configurar la creación de reflejo de puertos, configure una instancia de uno de los siguientes tipos:

- Instancia del analizador: especifique la entrada y la salida de la instancia. Este tipo de instancia es útil para garantizar que todo el tráfico que transita por una interfaz o entra en una VLAN se refleje y se envíe al analizador.

- Instancia de duplicación de puertos: se crea un filtro de firewall que identifica el tráfico deseado y lo copia en el puerto reflejado. No especifique una entrada para este tipo de instancia. Este tipo de instancia es útil para controlar los tipos de tráfico que se reflejan. Puede dirigir el tráfico a él de las siguientes maneras:
  - Especifique el nombre de la instancia de duplicación de puertos en el filtro de firewall mediante la acción cuando haya varias instancias de creación de reflejo de puerto definidas.`port-mirror-instance` *`instance-name`*
  - Envíe los paquetes reflejados a la interfaz de salida definida en la instancia mediante la acción cuando solo haya una instancia de creación de reflejo de puerto definida.`port-mirror`

Para los conmutadores QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, EX4600 y EX4650, se aplican las siguientes pautas de duplicación de puertos:

- Se puede configurar un máximo de cuatro instancias de creación de reflejo de puertos, o cuatro sesiones de analizador, al mismo tiempo. En otras palabras, no puede configurar cuatro instancias de creación de reflejo de puertos y cuatro sesiones de analizador juntas.
- Si no hay instancias de creación de reflejo de puertos (es decir, solo se configuran sesiones de analizador), puede habilitar hasta tres sesiones de analizador para la creación de reflejo de entrada y salida. La sesión restante del analizador debe utilizarse únicamente para la creación de reflejo de entrada.
- Si solo tiene configurada una instancia de creación de reflejo de puerto, de las instancias restantes, puede configurar hasta tres analizadores para la creación de reflejo de entrada y dos analizadores para la creación de reflejo de salida.
- Si tiene configurada una instancia de duplicación de dos puertos, de las instancias restantes, puede configurar hasta dos analizadores para la creación de reflejo de entrada y un analizador para la creación de reflejo de salida.
- Si tiene configurada una instancia de creación de reflejo de tres puertos, la instancia restante solo se puede configurar como analizador (para la duplicación de entrada o salida),

Duplicación de puertos y STP

El comportamiento de STP en una configuración de creación de reflejo de puertos depende de la versión de Junos OS que esté utilizando:

- Junos OS 13.2X50, Junos OS 13.2X51-D25 o anterior, Junos OS 13.2X52: Cuando STP está habilitado, es posible que la creación de reflejo de puertos no se realice correctamente porque STP podría bloquear los paquetes reflejados.
- Junos OS 13.2X51-D30, Junos OS 14.1X53: STP está deshabilitado para el tráfico reflejado. Debe asegurarse de que la topología evita bucles de este tráfico.

Restricciones y limitaciones

in this section

- Restricciones y limitaciones para conmutadores QFX5100 y QFX5200 | **1043**

Las siguientes restricciones y limitaciones se aplican a la creación de reflejo de puertos:

La duplicación de sólo los paquetes necesarios para el análisis reduce la posibilidad de reducir el rendimiento general. Si refleja el tráfico de varios puertos, el tráfico reflejado podría superar la capacidad de la interfaz de salida. Los paquetes de desbordamiento se descartan. Le recomendamos que limite la cantidad de tráfico reflejado seleccionando interfaces específicas y evite usar la palabra clave.`all` También puede limitar la cantidad de tráfico reflejado mediante un filtro de firewall para enviar tráfico específico a la instancia de creación de reflejo del puerto.

- Puede crear un total de cuatro configuraciones de duplicación de puertos.
- En los conmutadores EX9200, la duplicación de puertos no se admite en las tarjetas de línea EX9200-15C.
- Cada grupo de nodos en un sistema QFabric está sujeto a las siguientes restricciones:
  - Se pueden usar hasta cuatro de las configuraciones para la creación de reflejo de puertos locales.
  - Se pueden utilizar hasta tres de las configuraciones para la duplicación remota de puertos.
- Independientemente de si está configurando un conmutador independiente o un grupo de nodos:
  - No puede haber más de dos configuraciones que reflejen el tráfico de entrada. Si configura un filtro de firewall para enviar tráfico reflejado a un puerto, esto cuenta como una configuración de duplicación de entrada para el conmutador o grupo de nodos al que se aplica el filtro.
  - No puede haber más de dos configuraciones que reflejen el tráfico de salida.
  - En los sistemas QFabric, no hay límite para todo el sistema en el número total de sesiones de espejo.
- Solo puede configurar un tipo de salida en una configuración de creación de reflejo de puerto para completar una instrucción:`set analyzer` *`name`* `output`
  - `interface`
  - `ip-address`

- `vlan`

- Configure la creación de reflejo en un analizador (con) en una sola interfaz lógica para la misma interfaz física.`set forwarding-options analyzer` Si intenta configurar la creación de reflejo en varias interfaces lógicas configuradas en una interfaz física, solo se configura correctamente la primera interfaz lógica; Las interfaces lógicas restantes devuelven errores de configuración.

- Si refleja los paquetes de salida, no configure más de 2000 VLAN en un conmutador independiente o sistema QFabric. Si lo hace, es posible que algunos paquetes de VLAN contengan ID de VLAN incorrectos. Esto se aplica a cualquier paquete de VLAN, no solo a las copias reflejadas.

- Las opciones y no son compatibles.`ratioloss-priority`

- Los paquetes con errores de capa física no se envían al puerto de salida ni a la VLAN.

- Si utiliza la supervisión de sFlow para muestrear el tráfico, no muestrea las copias reflejadas cuando salen de la interfaz de salida.

- No puede reflejar paquetes que salen o entran en los siguientes puertos:

  - Interfaces de chasis virtual dedicadas

  - Interfaces de administración (me0 o vme0)

  - Interfaces de canal de fibra

  - Interfaces de enrutamiento y puente integrados (IRB) (también conocidas como interfaces VLAN enrutadas o RVI)

- En una instancia de creación de reflejo de puertos, no se puede configurar una interfaz inet o inet6 como interfaz de salida. Los siguientes conmutadores no admiten la configuración:`set forwarding-options port-mirroring instance <instance-name> family inet output interface <interface-name>`

Tabla 117: Conmutadores que no admiten la familia inet/inet6 como interfaz de salida

Conmutadores EX	Conmutadores QFX
EX2300	QFX3500
EX3400	QFX5100
EX4100	QFX5110
EX4300	QFX5120

Tabla 117: Conmutadores que no admiten la familia inet/inet6 como interfaz de salida *(Continued)*

Conmutadores EX	Conmutadores QFX
EX4400	QFX5130
EX4600	QFX5200
EX4650	QFX5210
	QFX5220
	QFX5700

- Una interfaz Ethernet agregada no puede ser una interfaz de salida si la entrada es una VLAN o si el tráfico se envía al analizador mediante un filtro de firewall.
- Cuando los paquetes reflejados se envían desde una interfaz de salida, no se modifican para ningún cambio que pueda aplicarse a los paquetes originales al salir, como la reescritura de CoS.
- Una interfaz puede ser la interfaz de entrada para una sola configuración de creación de reflejo. No utilice la misma interfaz que la interfaz de entrada para varias configuraciones de creación de reflejo.
- Los paquetes generados por la CPU (como los paquetes ARP, ICMP, BPDU y LACP) no se pueden reflejar en la salida.
- La creación de reflejo basada en VLAN no es compatible con el tráfico STP.
- (Solo sistemas QFabric) Si configura un analizador QFabric para reflejar el tráfico de salida y las interfaces de entrada y salida se encuentran en dispositivos de nodo diferentes, las copias duplicadas tendrán ID de VLAN incorrectos.

  Esta limitación no se aplica si configura un analizador QFabric para reflejar el tráfico de salida y las interfaces de entrada y salida se encuentran en el mismo dispositivo de nodo. En este caso, las copias duplicadas tendrán los ID de VLAN correctos (siempre y cuando no configure más de 2000 VLAN en el sistema QFabric).
- La duplicación de salida verdadera se define como la duplicación del número exacto de copias y las modificaciones exactas de paquetes que salieron del puerto de salida. Debido a que los procesadores de los conmutadores QFX5100 y EX4600 implementan la duplicación de salida en la canalización de entrada, dichos conmutadores no proporcionan modificaciones precisas de los paquetes de salida,

por lo que el tráfico reflejado de salida puede llevar etiquetas VLAN incorrectas que difieren de las etiquetas del tráfico original.

- Si configura una instancia de duplicación de puertos para reflejar el tráfico que sale de una interfaz que realiza la encapsulación de VLAN, las direcciones MAC de origen y destino de los paquetes reflejados no son las mismas que las de los paquetes originales.
- No se admite la creación de reflejo en interfaces miembro de un LAG.
- No se admite la duplicación de VLAN de salida.

Las siguientes restricciones y limitaciones se aplican a la creación de reflejo de puerto remoto:

- Si configura una dirección IP de salida, esa dirección no puede estar en la misma subred que ninguna de las interfaces de administración del conmutador.
- Si crea instancias de enrutamiento virtual y crea una configuración de analizador que incluya una dirección IP de salida, la dirección IP de salida pertenece a la instancia de enrutamiento virtual predeterminada (tabla de enrutamiento inet.0).
- Una VLAN de salida no puede ser una VLAN privada ni un rango de VLAN.
- Una VLAN de salida no puede ser compartida por varias sesiones del analizador o instancias de espejo de puerto.
- Una interfaz VLAN de salida no puede ser miembro de ninguna otra VLAN.
- Una interfaz VLAN de salida no puede ser una interfaz Ethernet agregada.
- Si la VLAN de salida tiene más de una interfaz miembro, el tráfico se refleja solo en el primer miembro de la VLAN y otros miembros de la misma VLAN no llevan ningún tráfico reflejado.
- Para la creación remota de reflejo de puerto a una dirección IP (encapsulación GRE), si configura más de una sesión de analizador o instancia de espejo de puerto, y se puede acceder a las direcciones IP de los analizadores o de la instancia de espejo de puerto a través de la misma interfaz, solo se configurará una sesión de analizador o una instancia de espejo de puerto.
- El número de interfaces de salida posibles en la duplicación de puerto remoto varía entre los conmutadores de la línea QFX5K:
  - QFX5110, QFX5120 QFX5210: admite un máximo de 4 interfaces de salida
  - QFX5100 y QFX5200: admite un máximo de 3 interfaces de salida.
- Siempre que se elimine de esa VLAN de espejado de puerto remoto, vuelva a configurar la sesión del analizador para esa VLAN.

Restricciones y limitaciones para conmutadores QFX5100 y QFX5200

Las siguientes consideraciones se aplican a la duplicación de puertos en conmutadores QFX5100 y QFX5200:

- Al configurar la duplicación con salida a la dirección IP, la dirección IP de destino debe ser accesible y ARP debe estar resuelto.
- El equilibrio de carga ECMP (ruta múltiple de igual costo) no se admite para destinos reflejados.
- El número de interfaces de salida en la creación de reflejo de puerto remoto (RSPAN) varía. Para los conmutadores QFX5110, QFX5120 y QFX5210, el máximo es de cuatro interfaces de salida. Para los conmutadores QFX5100 y QFX5200, el máximo es tres.
- Cuando se especifica un grupo de agregación de vínculos (LAG) como interfaz de salida de reflejo, se reflejan un máximo de ocho interfaces.
- La entrada de duplicación puede ser un LAG, una interfaz física con cualquier unidad (como ae0.101 o xe-0/0/0.100) o una subinterfaz. En cualquier caso, todo el tráfico del LAG o de la interfaz física se refleja.
- No puede configurar una instancia de creación de reflejo independiente en una interfaz miembro de un LAG.
- Una interfaz de salida que se incluye en una instancia de creación de reflejo no se puede utilizar también en otra instancia de creación de reflejo.
- En una instancia de duplicación de puertos, los paquetes perdidos en la canalización de salida de la ruta de reenvío no dejan de ser reflejados en el destino. Esto se debe a que la acción de creación de reflejo se produce en la canalización de entrada, antes de la acción de eliminación.
- En una instancia de duplicación de puertos, solo se puede especificar un destino de salida reflejada.
- Los destinos de espejo de salida que se configuran en varias instancias de analizador o duplicación de puertos deben ser únicos.
- Para las direcciones IPv6 de ERSPAN, la duplicación de salida no se admite cuando el resultado del analizador/reflejo de puerto es una dirección IPv6 remota. No se admite el espejo de salida.
- Para la creación de reflejo local, la interfaz de salida debe ser de conmutación Ethernet familiar, con o sin VLAN (es decir, no una interfaz de capa 3).
- Cuando configure una instancia de analizador o duplicación de puertos en un entorno de proveedor de servicios, utilice el nombre de VLAN en lugar del ID de VLAN.

Duplicación de puertos en conmutadores de la serie QFX10000

En la siguiente lista se describen las restricciones y limitaciones que se aplican específicamente a los conmutadores de la serie QFX10000. Para obtener información general acerca de la duplicación de puertos en conmutadores, consulte las secciones anteriores de este documento Analizadores y creación de duplicación de puertos que no mencionan específicamente otros nombres de plataforma en el título de la sección.

- Solo se admite la duplicación de puerto global de entrada. Puede configurar la creación de reflejo global de puertos con parámetros de entrada como , , y .`raterun-lengthmaximum-packet-length` No se admite la creación de reflejo de puerto global de salida.
- Las instancias de creación de reflejo de puerto solo se admiten para la creación de reflejo de puertos remotos. Las instancias globales de creación de reflejo de puertos son compatibles con la creación de reflejo local.
- La creación de reflejo de puerto local solo se admite en estas familias de filtros de firewall: `inet` y `inet6`.
- La creación de reflejo de puerto local no se admite en las familias de filtros de firewall ni en .`anyccc`

Duplicación de puertos en QFabric

Las siguientes restricciones y limitaciones se aplican a la creación de reflejo de puertos locales y remotos:

- Puede crear un total de cuatro configuraciones de duplicación de puertos.
- Cada grupo de nodos en un sistema QFabric está sujeto a las siguientes restricciones:
  - Se pueden usar hasta cuatro de las configuraciones para la creación de reflejo de puertos locales.
  - Se pueden utilizar hasta tres de las configuraciones para la duplicación remota de puertos.
- Independientemente de si está configurando un conmutador independiente o un grupo de nodos:
  - No puede haber más de dos configuraciones que reflejen el tráfico de entrada. Si configura un filtro de firewall para enviar tráfico reflejado a un puerto, es decir, utiliza el modificador de acción en un término de filtro, esto cuenta como una configuración de creación de reflejo de entrada para el conmutador o grupo de nodos al que se aplica el filtro.`analyzer`
  - No puede haber más de dos configuraciones que reflejen el tráfico de salida.
  - En los sistemas QFabric, no hay límite para todo el sistema en el número total de sesiones de espejo.

- Solo puede configurar un tipo de salida en una configuración de creación de reflejo de puerto para completar una instrucción:`set analyzer name output`
  - `interface`
  - `ip-address`
  - `vlan`
- Configure la creación de reflejo en un analizador (con) en una sola interfaz lógica para la misma interfaz física.`set forwarding-options analyzer` Si intenta configurar la creación de reflejo en varias interfaces lógicas configuradas en una interfaz física, solo se configura correctamente la primera interfaz lógica; Las interfaces lógicas restantes devuelven errores de configuración.
- Si refleja los paquetes de salida, no configure más de 2000 VLAN en un conmutador serie QFX. Si lo hace, es posible que algunos paquetes de VLAN contengan ID de VLAN incorrectos. Esto se aplica a cualquier paquete de VLAN, no solo a las copias reflejadas.
- Las opciones y no son compatibles.`ratioloss-priority`
- Los paquetes con errores de capa física no se envían al puerto de salida ni a la VLAN.
- Si utiliza la supervisión de sFlow para muestrear el tráfico, no muestrea las copias reflejadas cuando salen de la interfaz de salida.
- No puede reflejar paquetes que salen o entran en los siguientes puertos:
  - Interfaces de chasis virtual dedicadas
  - Interfaces de administración (me0 o vme0)
  - Interfaces de canal de fibra
  - Interfaces de enrutamiento y puente integrados (IRB) (también conocidas como interfaces VLAN enrutadas o RVI)
- Una interfaz Ethernet agregada no puede ser una interfaz de salida si la entrada es una VLAN o si el tráfico se envía al analizador mediante un filtro de firewall.
- Cuando los paquetes reflejados se envían desde una interfaz de salida, no se modifican para ningún cambio que pueda aplicarse a los paquetes originales al salir, como la reescritura de CoS.
- Una interfaz puede ser la interfaz de entrada para una sola configuración de creación de reflejo. No utilice la misma interfaz que la interfaz de entrada para varias configuraciones de creación de reflejo.
- Los paquetes generados por la CPU (como los paquetes ARP, ICMP, BPDU y LACP) no se pueden reflejar en la salida.
- La creación de reflejo basada en VLAN no es compatible con el tráfico STP.

- (Solo sistemas QFabric) Si configura un analizador QFabric para reflejar el tráfico de salida y las interfaces de entrada y salida se encuentran en dispositivos de nodo diferentes, las copias duplicadas tendrán ID de VLAN incorrectos.

  Esta limitación no se aplica si configura un analizador QFabric para reflejar el tráfico de salida y las interfaces de entrada y salida se encuentran en el mismo dispositivo de nodo. En este caso, las copias duplicadas tendrán los ID de VLAN correctos (siempre y cuando no configure más de 2000 VLAN en el sistema QFabric).

- La duplicación de salida verdadera se define como la duplicación del número exacto de copias y las modificaciones exactas de paquetes que salieron del puerto de salida. Debido a que los procesadores de los conmutadores QFX5xxx (incluidos QFX5100, QFX5110, QFX5120, QFX5200 y QFX5210) y EX4600 (incluidos EX4600 y EX4650) implementan la duplicación de salida en la canalización de entrada, esos conmutadores no proporcionan modificaciones precisas de los paquetes de salida, por lo que el tráfico reflejado de salida puede llevar etiquetas VLAN incorrectas que difieren de las etiquetas del tráfico original.

- Si configura una instancia de duplicación de puertos para reflejar el tráfico que sale de una interfaz que realiza la encapsulación de VLAN, las direcciones MAC de origen y destino de los paquetes reflejados no son las mismas que las de los paquetes originales.

- No se admite la creación de reflejo en interfaces miembro de un LAG.

- No se admite la duplicación de VLAN de salida.

Duplicación de puertos en conmutadores de la serie OCX

Las siguientes restricciones y limitaciones se aplican a la duplicación de puertos en los conmutadores de la serie OCX:

- Puede crear un total de cuatro configuraciones de duplicación de puertos. No puede haber más de dos configuraciones que reflejen el tráfico de entrada o salida.

- Si utiliza la supervisión de sFlow para muestrear el tráfico, no muestrea las copias reflejadas cuando salen de la interfaz de salida.

- Solo puede crear una sesión de creación de reflejo de puertos.

- No puede reflejar paquetes que salen o entran en los siguientes puertos:

  - Interfaces de chasis virtual dedicadas

  - Interfaces de administración (me0 o vme0)

  - Interfaces de canal de fibra

  - Interfaces VLAN enrutadas o interfaces IRB

- Una interfaz Ethernet agregada no puede ser una interfaz de salida.
- No incluya una subinterfaz 802.1Q que tenga un número de unidad distinto de 0 en una configuración de creación de reflejo de puerto. La duplicación de puertos no funciona con subinterfaces si su número de unidad no es 0. (Las subinterfaces 802.1Q se configuran mediante la instrucción.)`vlan-tagging`
- Cuando se envían copias de paquetes a la interfaz de salida, no se modifican para ningún cambio que normalmente se aplica a la salida, como la reescritura de CoS.
- Una interfaz puede ser la interfaz de entrada para una sola configuración de creación de reflejo. No utilice la misma interfaz que la interfaz de entrada para varias configuraciones de creación de reflejo.
- Los paquetes generados por la CPU (como los paquetes ARP, ICMP, BPDU y LACP) no se pueden reflejar en la salida.
- La creación de reflejo basada en VLAN no es compatible con el tráfico STP.

Duplicación de puertos en conmutadores EX2300, EX3400 y EX4300

in this section

- Descripción general | **1047**
- Directrices de configuración para analizadores y duplicación de puertos en conmutadores EX2300, EX3400 y EX4300 | **1048**

La creación de reflejo puede ser necesaria para el análisis del tráfico en un conmutador, ya que a diferencia de un concentrador, un conmutador no difunde paquetes a todos los puertos del dispositivo de destino. El conmutador envía paquetes solo al puerto al que está conectado el dispositivo de destino.

Descripción general

Junos OS que se ejecuta en conmutadores serie EX2300, EX3400 y EX4300 admite las configuraciones de software de capa 2 mejorada (ELS) que facilitan el análisis del tráfico en estos conmutadores a nivel de paquete.

La creación de reflejo de puertos se utiliza para copiar paquetes en una interfaz local para la supervisión local o en una VLAN para la supervisión remota. Puede utilizar analizadores para aplicar políticas relativas al uso de la red y el uso compartido de archivos, y para identificar los orígenes de problemas en la red mediante la localización de un uso de ancho de banda anormal o intenso por estaciones o aplicaciones específicas.

La duplicación de puertos se configura en el nivel jerárquico .`[edit forwarding-options port-mirroring]` Para reflejar paquetes enrutados (capa 3), puede utilizar la configuración de creación de reflejo de puerto en la que la instrucción está establecida en o .`family inetinet6`

Puede utilizar la creación de reflejo de puertos para copiar estos paquetes:

- **Packets entering or exiting a port**: puede reflejar los paquetes en cualquier combinación de paquetes que entren o salgan de puertos de hasta 256 puertos.

  En otras palabras, puede enviar copias de los paquetes que entran en algunos puertos y los paquetes que salen de otros puertos al mismo puerto del analizador local o VLAN del analizador.

- **Packets entering a VLAN**: puede reflejar los paquetes que ingresan en una VLAN a un puerto del analizador local o a una VLAN del analizador. Puede configurar hasta 256 VLAN, incluido un rango de VLAN y PVLAN, como entrada de entrada a un analizador.

- **Policy-based sample packets**: puede reflejar una muestra basada en políticas de paquetes que entran en un puerto o una VLAN. Configure un filtro de firewall para establecer una directiva para seleccionar los paquetes que se reflejarán y enviar el ejemplo a una instancia de duplicación de puertos o a una VLAN de analizador.

Puede configurar la duplicación de puertos en el conmutador para enviar copias del tráfico de unidifusión a un destino de salida, como una interfaz, una instancia de enrutamiento o una VLAN. A continuación, puede analizar el tráfico reflejado mediante una aplicación de analizador de protocolos. La aplicación del analizador de protocolos puede ejecutarse en un equipo conectado a la interfaz de salida del analizador o en una estación de supervisión remota. Para el tráfico de entrada, puede configurar un término de filtro de firewall para especificar si la creación de reflejo de puerto debe aplicarse a todos los paquetes de la interfaz a la que se aplica el filtro de firewall. Puede aplicar un filtro de firewall configurado con la acción o a las interfaces lógicas de entrada o salida (incluidas las interfaces lógicas Ethernet agregadas), al tráfico reenviado o inundado a una VLAN, o al tráfico reenviado o inundado a una instancia de enrutamiento VPLS.`port-mirrorport-mirror-instance` *`name`* Los conmutadores EX2300, EX3400 y EX4300 admiten la duplicación de puertos del tráfico VPLS (o) y el tráfico VPN en un entorno de capa 2.`family ethernet-switchingfamily vplsfamily ccc`

Dentro de un término de filtro de firewall, puede especificar las propiedades de duplicación de puertos en la instrucción de las siguientes maneras:`then`

- Haga referencia implícita a las propiedades de duplicación de puertos vigentes en el puerto.

- Haga referencia explícita a una instancia con nombre concreta de creación de reflejo de puertos.

Directrices de configuración para analizadores y duplicación de puertos en conmutadores EX2300, EX3400 y EX4300

Cuando configure la duplicación de puertos, le recomendamos que siga ciertas directrices para asegurarse de obtener un beneficio óptimo de la creación de reflejos. Además, se recomienda

deshabilitar la creación de reflejo cuando no la esté utilizando y seleccionar interfaces específicas para las que se deben reflejar los paquetes (es decir, seleccionar interfaces específicas como entrada para el analizador) en lugar de usar la opción de palabra clave que habilita la creación de reflejo en todas las interfaces y puede afectar al rendimiento general.`all` Duplicar solo los paquetes necesarios reduce cualquier impacto potencial en el rendimiento.

Con la creación de reflejo local, el tráfico de varios puertos se replica en la interfaz de salida del analizador. Si la interfaz de salida de un analizador alcanza su capacidad, los paquetes se descartan. Por lo tanto, al configurar un analizador, debe considerar si el tráfico que se refleja supera la capacidad de la interfaz de salida del analizador.

Puede configurar un analizador en la jerarquía.`[edit forwarding-options analyzer]`

> **NOTA**: La verdadera duplicación de salida se define como la duplicación del número exacto de copias y las modificaciones exactas de los paquetes que salieron del puerto conmutado de salida. Debido a que el procesador de los conmutadores EX2300 y EX3400 implementa la duplicación de salida en la canalización de entrada, esos conmutadores no proporcionan modificaciones precisas de los paquetes de salida, por lo que el tráfico reflejado de salida puede transportar etiquetas VLAN que difieren de las etiquetas del tráfico original.

Tabla 118 en la página 1049 resume las pautas de configuración adicionales para la creación de reflejo en conmutadores EX2300, EX3400 y EX4300.

Tabla 118: Directrices de configuración para analizadores y duplicación de puertos en conmutadores EX2300, EX3400 y EX4300

Pauta	Información de valor o soporte	Comentario
Número de VLAN que puede utilizar como entrada de entrada a un analizador.	256	

Tabla 118: Directrices de configuración para analizadores y duplicación de puertos en conmutadores EX2300, EX3400 y EX4300 *(Continued)*

Pauta	Información de valor o soporte	Comentario
Número de sesiones de creación de reflejo de puertos y analizadores que puede habilitar simultáneamente.	4	Puede configurar un total de cuatro sesiones y solo puede habilitar una de las siguientes opciones en cualquier momento: • Un máximo de cuatro sesiones de creación de reflejo de puertos (incluida la sesión global de creación de reflejo de puertos). • Un máximo de cuatro sesiones de analizador. • Una combinación de sesiones de analizador y duplicación de puertos, y el total de esta combinación debe ser cuatro. Puede configurar más de la cantidad especificada de instancias o analizadores de duplicación de puertos en el conmutador, pero solo puede habilitar el número especificado para una sesión.

Tabla 118: Directrices de configuración para analizadores y duplicación de puertos en conmutadores EX2300, EX3400 y EX4300 *(Continued)*

Pauta	Información de valor o soporte	Comentario
Tipos de puertos en los que no se puede reflejar el tráfico.	• Puertos de chasis virtual (VCP) • Puertos Ethernet de administración (me0 o vme0) • Interfaces integradas de enrutamiento y puente (IRB); también conocidas como interfaces VLAN enrutadas (RVI). • Interfaces de capa 3 etiquetadas por VLAN	
Familias de protocolos que puede incluir en una configuración de creación de reflejo de puertos para tráfico remoto.	`any`	
Instrucciones de tráfico que puede configurar para la creación de reflejo en puertos en configuraciones basadas en filtros de firewall.	Entrada y salida	
Paquetes duplicados que salen de una interfaz que reflejan DSCP de clase de servicio (CoS) reescritos o bits de 802.1p.	Aplicable	
Paquetes con errores de capa física.	Aplicable	Los paquetes con estos errores se filtran y, por lo tanto, no se envían al analizador.

Tabla 118: Directrices de configuración para analizadores y duplicación de puertos en conmutadores EX2300, EX3400 y EX4300 *(Continued)*

Pauta	Información de valor o soporte	Comentario
La duplicación de puertos no admite tráfico de velocidad de línea.	Aplicable	La duplicación de puertos para el tráfico de velocidad de línea se realiza con el mejor esfuerzo.
Duplicación de paquetes que salen de una VLAN.	No compatible	
Salida del analizador o duplicación de puertos en una interfaz LAG.	Compatible	
Número máximo de miembros secundarios en una interfaz LAG de salida de analizador o duplicación de puertos.	8	
Número máximo de interfaces en una VLAN de analizador o duplicación de puerto remota.	1	
Reflejo de salida de paquetes de control generados por el host.	No compatible	
Configuración de interfaces lógicas de capa 3 en la estrofa de un analizador.`input`	No compatible	Esta funcionalidad se puede lograr configurando la duplicación de puertos.
Se deben evitar las estrofas de entrada y salida del analizador que contengan miembros de la misma VLAN o de la propia VLAN.	Aplicable	

Duplicación de puertos en conmutadores ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 y EX8200

in this section

- Descripción general | **1053**
- Pautas de configuración para conmutadores de las series ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 y EX8200 | **1054**

El sistema operativo Junos de Juniper Networks (Junos OS) que se ejecuta en conmutadores ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 o EX8200 no admite configuraciones de software de capa 2 mejorada (ELS). Como tal, Junos OS no incluye la instrucción que se encuentra en el nivel de la jerarquía de otros paquetes de Junos OS ni la acción en términos de filtro de firewall.`port-mirroringedit forwarding-optionsport-mirror`

Puede usar la duplicación de puertos para facilitar el análisis del tráfico en su conmutador Ethernet de la serie EX de Juniper Networks a nivel de paquete. Puede utilizar la duplicación de puertos como parte de la supervisión del tráfico del conmutador con fines tales como aplicar políticas relativas al uso de la red y el uso compartido de archivos, y para identificar fuentes de problemas en la red mediante la localización de un uso de ancho de banda anormal o intensivo por estaciones o aplicaciones particulares.

Puede utilizar la creación de reflejo de puertos para copiar estos paquetes en una interfaz local o en una VLAN:

- Paquetes que entran o salen de un puerto
- Puede enviar copias de los paquetes que entran en algunos puertos y los paquetes que salen de otros puertos al mismo puerto del analizador local o VLAN del analizador.
- Paquetes que ingresan a una VLAN en conmutadores ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550 o EX6200
- Paquetes que salen de una VLAN en conmutadores EX8200

Descripción general

La duplicación de puertos se utiliza para el análisis del tráfico en un conmutador porque a diferencia de un concentrador, no difunde paquetes a todos los puertos del dispositivo de destino. El conmutador envía paquetes solo al puerto al que está conectado el dispositivo de destino.

Configure la creación de reflejo de puertos en el conmutador para enviar copias del tráfico de unidifusión a un puerto del analizador local o a una VLAN del analizador. A continuación, puede analizar

el tráfico reflejado mediante un analizador de protocolos. El analizador de protocolo puede ejecutarse en un ordenador conectado a la interfaz de salida del analizador o en una estación de supervisión remota.

Puede utilizar la creación de reflejo de puertos para reflejar cualquiera de las siguientes opciones:

- **Packets entering or exiting a port**: puede reflejar los paquetes en cualquier combinación de paquetes que entren o salgan de puertos de hasta 256 puertos.

  En otras palabras, puede enviar copias de los paquetes que entran en algunos puertos y los paquetes que salen de otros puertos al mismo puerto del analizador local o VLAN del analizador.

- **Packets entering a VLAN on an ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, or EX6200 switch**: puede duplicar los paquetes que ingresan a una VLAN en una VLAN de analizador. En los conmutadores EX3200, EX4200, EX4500 y EX4550, puede configurar varias VLAN (hasta 256 VLAN), incluido un rango de VLAN y PVLAN, como entrada de entrada a un analizador.

- **Packets exiting a VLAN on an EX8200 switch**: puede reflejar los paquetes que salen de una VLAN en un conmutador EX8200 en un puerto del analizador local o en una VLAN del analizador. Puede configurar varias VLAN (hasta 256 VLAN), incluido un rango de VLAN y PVLAN, como entrada de salida a un analizador.

- **Statistical samples**: puede reflejar una muestra estadística de paquetes que sean:

  - Entrar o salir de un puerto
  - Introducción de una VLAN en un conmutador ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550 o EX6200
  - Salir de una VLAN en un conmutador EX8200

  El número de paquetes de muestra se especifica estableciendo la proporción. Puede enviar la muestra a un puerto del analizador local o a una VLAN del analizador.

- **Policy-based sample**: puede reflejar una muestra basada en políticas de paquetes que entran en un puerto o una VLAN. Configure un filtro de firewall para establecer una directiva para seleccionar los paquetes que se van a reflejar. Puede enviar la muestra a un puerto del analizador local o a una VLAN del analizador.

Pautas de configuración para conmutadores de las series ACX7024, ACX7100, ACX7509, EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX6200 y EX8200

Cuando configure la creación de reflejo de puertos, le recomendamos que siga ciertas directrices para asegurarse de obtener un beneficio óptimo de la función de creación de reflejo de puertos. Además, se recomienda deshabilitar la creación de reflejo de puertos cuando no la esté utilizando y que seleccione interfaces específicas para las que se deben reflejar los paquetes (es decir, seleccionar interfaces específicas como entrada para el analizador) en lugar de utilizar la palabra clave que habilita la creación

de reflejo de puertos en todas las interfaces y puede afectar al rendimiento general.`all` También puede limitar la cantidad de tráfico reflejado mediante el muestreo estadístico, estableciendo una proporción para seleccionar una muestra estadística o utilizando un filtro de firewall. Duplicar solo los paquetes necesarios reduce cualquier impacto potencial en el rendimiento.

Con la creación de reflejo de puerto local, el tráfico de varios puertos se replica en la interfaz de salida del analizador. Si la interfaz de salida de un analizador alcanza su capacidad, los paquetes se descartan. Por lo tanto, al configurar un analizador, debe considerar si el tráfico que se refleja supera la capacidad de la interfaz de salida del analizador.

NOTA: En enrutadores ACX5448, en el nivel de jerarquía [], la entrada del analizador debe configurarse únicamente en interfaces lógicas .0 para las interfaces de entrada y salida.`edit forwarding-options analyzer an input egress` Si configura interfaces lógicas distintas de .0, se mostrará un error durante la confirmación. A continuación se muestra un ejemplo de error de confirmación que se muestra cuando la entrada del analizador está configurada como interfaz lógica .100:

```
[edit forwarding-options analyzer an input egress]
  'interface ge-0/0/12.100'
    Analyzer input can only be on .0 interfaces
error: configuration check-out failed
```

NOTA:
https://apps.juniper.net/feature-explorer/

Tabla 119: Directrices de configuración

Pauta	Description	Comentario
Número de VLAN que puede utilizar como entrada de entrada a un analizador	• 16 Dispositivos de entrada u 8 de entrada y 8 de salida: ACX7024 1—Conmutadores EX2200 • Conmutadores EX3200, EX4200, EX4500, EX4550 y EX6200 • No aplica: conmutadores EX8200	

Tabla 119: Directrices de configuración *(Continued)*

Pauta	Description	Comentario
Número de analizadores que puede habilitar simultáneamente (se aplica tanto a conmutadores independientes como a Virtual Chassis)	• 1: Conmutadores EX2200, EX3200, EX4200, EX3300 y EX6200 • Conmutadores EX4500 y EX4550 basados en 7 puertos o 1 global: EX4500 y EX4550 • 7 en total, con uno basado en una VLAN, filtro de firewall o LAG y los 6 restantes basados en filtros de firewall: conmutadores EX8200 **NOTA**: Un analizador configurado mediante un filtro de firewall no admite la creación de reflejo de paquetes que están saliendo de puertos.	• Puede configurar más del número especificado de analizadores en el conmutador, pero solo puede habilitar el número especificado para una sesión. Se utiliza para desactivar un analizador.**disable ethernet-switching-options analyzer name** • Consulte la entrada de la siguiente fila de esta tabla para ver la excepción al número de analizadores basados en filtros de firewall permitidos en los conmutadores EX4500 y EX4550. • En un Virtual Chassis EX4550, sólo puede configurar un analizador si los puertos de las definiciones de entrada y salida se encuentran en distintos conmutadores de un Virtual Chassis. Para configurar varios analizadores, se debe configurar una sesión completa del analizador en el mismo conmutador de un Virtual Chassis.
Número de analizadores basados en filtros de firewall que puede configurar en conmutadores EX4500 y EX4550	• 1—Conmutadores EX4500 y EX4550	Si configura varios analizadores, no podrá adjuntar ninguno de ellos a un filtro de firewall.

Tabla 119: Directrices de configuración *(Continued)*

Pauta	Description	Comentario
Tipos de puertos en los que no se puede reflejar el tráfico	• Puertos de chasis virtual (VCP) • Puertos Ethernet de administración (me0 o vme0) • Interfaces VLAN enrutadas (RVI) • Interfaces de capa 3 etiquetadas por VLAN	
Si la duplicación de puertos está configurada para reflejar paquetes que salen de puertos 10 Gigabit Ethernet en conmutadores EX8200, los paquetes se eliminan tanto en el tráfico de red como en el reflejado cuando los paquetes reflejados superan el 60 por ciento del tráfico de puertos 10 Gigabit Ethernet.	• Conmutadores EX8200	
Direcciones de tráfico para las que puede especificar una proporción	• Solo entrada: conmutadores EX8200 • Entrada y salida: todos los demás conmutadores	
Familias de protocolos que puede incluir en un analizador remoto basado en filtros de firewall	• Cualquier conmutador excepto y —EX8200`inetinet6` • Cualquiera: todos los demás conmutadores	Puede usar y en conmutadores EX8200 en un analizador local.`inetinet6`

Tabla 119: Directrices de configuración *(Continued)*

Pauta	Description	Comentario
Instrucciones de tráfico que puede configurar para la creación de reflejo en puertos en configuraciones basadas en filtros de firewall	• Solo entrada: todos los conmutadores	
Los paquetes reflejados en interfaces etiquetadas pueden contener un ID de VLAN o un Ethernet incorrectos.	• ID de VLAN y Ethertype: conmutadores EX2200 • Solo ID de VLAN: conmutadores EX3200 y EX4200 • Solo Ethertype: conmutadores EX4500 y EX4550 • No aplica: conmutadores EX8200	
Los paquetes reflejados que salen de una interfaz no reflejan el DSCP de clase de servicio (CoS) reescrito ni los bits 802.1p.	• Todos los conmutadores	
El analizador anexa un encabezado 802.1Q () incorrecto a los paquetes reflejados en el tráfico enrutado o no refleja ningún paquete en el tráfico enrutado cuando una VLAN de salida que pertenece a una interfaz VLAN enrutada (RVI) está configurada como entrada para ese analizador.`dot1q`	• Conmutadores EX8200 • No se aplica: todos los demás conmutadores	Como solución alternativa, configure un analizador que utilice cada puerto (interfaz miembro) de la VLAN como entrada de salida.
Los paquetes con errores de capa física no se envían al analizador local o remoto.	• Todos los conmutadores	Los paquetes con estos errores se filtran y, por lo tanto, no se envían al analizador.

Tabla 119: Directrices de configuración *(Continued)*

Pauta	Description	Comentario
La configuración de duplicación de puertos en una interfaz de capa 3 con la salida configurada en una VLAN no está disponible en los conmutadores EX8200.	• Conmutadores EX8200 • No se aplica: todos los demás conmutadores	
La duplicación de puertos no admite tráfico de velocidad de línea.	• Todos los conmutadores	La duplicación de puertos para el tráfico de velocidad de línea se realiza con el mejor esfuerzo.
En un Virtual Chassis EX8200, para reflejar el tráfico a través del Virtual Chassis, el puerto de salida debe ser un LAG.	• Chasis virtual EX8200 • No se aplica: todos los demás conmutadores	En un chasis virtual EX8200: • Puede configurar LAG como puerto de monitor solo para analizadores nativos. • No puede configurar LAG como puerto de supervisión para analizadores basados en filtros de firewall. • Si una configuración de analizador contiene LAG como puerto de monitor, no puede configurar VLAN en la definición de entrada de un analizador.
En los conmutadores EX8200 independientes, puede configurar LAG en la definición de salida.	• Conmutadores independientes EX8200 • No se aplica: todos los demás conmutadores	En los conmutadores independientes EX8200: • Puede configurar un LAG como puerto de supervisión en analizadores nativos y basados en firewall. • Si una configuración contiene LAG como puerto de monitor, no puede configurar VLAN en la definición de entrada de un analizador.

Duplicación de puertos en firewalls de la serie SRX

La duplicación de puertos copia los paquetes que entran o salen de un puerto y envía las copias a una interfaz local para su supervisión. La duplicación de puertos se usa para enviar tráfico a aplicaciones que analizan el tráfico con fines como supervisar el cumplimiento, aplicar políticas, detectar intrusiones, supervisar y predecir patrones de tráfico, correlacionar eventos, etc. </para><para>La duplicación de puertos se utiliza para enviar una copia de todos los paquetes o solo los paquetes muestreados que se ven en un puerto a una conexión de monitoreo de red. Puede reflejar los paquetes en el puerto entrante (duplicación del puerto de entrada) o en el puerto de salida (creación de reflejo del puerto de salida).

La duplicación de puertos solo se admite en los firewalls de la serie SRX con las siguientes tarjetas de E/S:

- SRX1K-SYSIO-GE
- SRX1K-SYSIO-XGE
- SRX3K-SFB-12GE
- SRX3K-2XGE-XFP
- E/S flexibles SRX5K-FPC-IOC

En los firewalls de la serie SRX, todos los paquetes que pasan por el puerto se copian y se envían al puerto especificado `.mirroredmirror-to` Estos puertos deben estar en el mismo chipset Broadcom en las tarjetas de E/S.

En los firewalls de la serie SRX, la duplicación de puertos solo funciona en interfaces físicas.

Descripción de la creación de reflejo de puertos de capa 2

En plataformas de enrutamiento y conmutadores que contienen un ASIC de procesador de Internet II, puede enviar una copia de cualquier paquete entrante desde la plataforma de enrutamiento o conmutador a una dirección de host externa o a un analizador de paquetes para su análisis. Esto se conoce como *duplicación de puertos*.

En Junos OS versión 9.3 y posteriores, las plataformas de enrutamiento universal 5G serie MX de Juniper Networks en un entorno de capa 2 admiten la duplicación de puertos para el tráfico de puente de capa 2 y el tráfico del servicio de LAN privada virtual (VPLS).

En Junos OS versión 9.4 y posteriores, los enrutadores serie MX en un entorno de capa 2 admiten la creación de reflejo de puertos para el tráfico VPN de capa 2 a través de una conexión cruzada de circuito (CCC) que conecta de forma transparente interfaces lógicas del mismo tipo.

En Junos OS versión 12.3R2, los conmutadores de la serie EX de Juniper Networks admiten la duplicación de puertos para el tráfico de puente de capa 2.

La duplicación de puertos de capa permite especificar la manera en que se supervisan los paquetes entrantes y salientes en los puertos especificados y la manera en que las copias de los paquetes seleccionados se reenvían a otro destino, donde se pueden analizar los paquetes.

Los enrutadores serie MX y los conmutadores serie EX admiten la duplicación de puertos de capa 2 mediante la realización de funciones de monitoreo de flujo mediante el uso de una arquitectura de clase de servicio (CoS) que, en concepto, es similar a, pero en particular diferente de, otras plataformas de enrutamiento y conmutadores.

Al igual que el enrutador perimetral multiservicio M120 y el enrutador perimetral multiservicio M320, los enrutadores serie MX y los conmutadores serie EX admiten la duplicación de paquetes IPv4, IPv6 y VPLS simultáneamente.

En un entorno de capa 3, los enrutadores serie MX y los conmutadores serie EX admiten la duplicación del tráfico IPv4 () e IPv6 ().`family inetfamily inet6` Para obtener información acerca de la creación de reflejo de puertos de capa 3, consulte la Guía del usuario de políticas de enrutamiento, filtros de firewall y políticas de tráfico.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.html

Propiedades de duplicación de puertos de capa 2

in this section

- Selección de paquetes | **1061**
- Familia de direcciones de paquetes | **1062**
- Propiedades de destino de réplica | **1062**
- Opción Mirror-Once | **1063**

La creación de reflejo de puertos especifica los siguientes tipos de propiedades:

Selección de paquetes

Las propiedades de selección de paquetes de la duplicación de puertos de capa 2 especifican cómo se seleccionarán los paquetes muestreados para la creación de reflejo:

- Número de paquetes de cada muestra.
- Número de paquetes que se van a reflejar de cada muestra.
- Longitud a la que se van a truncar los paquetes reflejados.

Familia de direcciones de paquetes

El tipo de familia de direcciones de paquete especifica el tipo de tráfico que se va a reflejar. En un entorno de capa 2, los enrutadores serie MX y los conmutadores serie EX admiten la duplicación de puertos para las siguientes familias de direcciones de paquetes:

- Tipo de familia: para duplicar el tráfico VPLS cuando la interfaz física está configurada con el tipo de encapsulación.`ethernet-switchingethernet-bridge`
- Tipo de familia: para duplicar el tráfico VPN de capa 2.`ccc`
- Tipo de familia: para duplicar el tráfico de VPLS.`vpls`

> **NOTA**: En aplicaciones típicas, los paquetes duplicados se envían directamente a un analizador, no a otro enrutador o conmutador. Si debe enviar paquetes duplicados a través de una red, debe usar túneles. Para las implementaciones de VPN de capa 2, puede utilizar el tipo de instancia de enrutamiento VPN de capa 2 para tunelizar los paquetes a un destino remoto.`l2vpn`

Para obtener información acerca de cómo configurar una instancia de enrutamiento para VPN de capa 2, consulte la Biblioteca de VPN de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/index.html Para obtener un ejemplo detallado de configuración de VPN de capa 2, consulte Junos OS.https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/junos/product/index.html Para obtener información acerca de las interfaces de túnel, consulte la Biblioteca de interfaces de red de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces.html

Propiedades de destino de réplica

Para una familia de direcciones de paquete dada, las propiedades de destino reflejado de una instancia de duplicación de puertos de capa 2 especifican cómo se enviarán los paquetes seleccionados en una interfaz física determinada:

- Interfaz física por la que se envían los paquetes seleccionados.
- Si se va a deshabilitar la comprobación de filtros para la interfaz de destino reflejada. De forma predeterminada, la comprobación de filtros está habilitada en todas las interfaces.

> **NOTA**: Si aplica un filtro a una interfaz que también es un destino de creación de reflejo de puerto de capa 2, se produce un error de confirmación, a menos que haya deshabilitado la comprobación de filtros para esa interfaz de destino reflejada.

Opción Mirror-Once

Si la duplicación de puertos está habilitada en las interfaces de entrada y salida, puede impedir que el enrutador de la serie MX y un conmutador de la serie EX envíen paquetes duplicados al mismo destino (lo que complicaría el análisis del tráfico reflejado).

> **NOTA**: La opción de duplicación de puerto único es una configuración global. La opción es independiente de las propiedades de selección de paquetes y de las propiedades de destino de reflejo específicas de la familia de paquetes.

Aplicación de tipos de duplicación de puertos de capa 2

Puede aplicar distintos conjuntos de propiedades de duplicación de puertos de capa 2 a los paquetes VPLS en distintos puntos de entrada o salida de una ruta de la serie MX o de una serie EX.

Tabla 120 en la página 1064 describe los tres tipos de *duplicación de puertos* de capa 2 que puede configurar en enrutadores serie MX y conmutadores serie EX: instancia global, instancias con nombre y filtros de firewall.

Tabla 120: Aplicación de tipos de duplicación de puertos de capa 2

Tipo de definición de duplicación de puertos de capa 2	Punto de aplicación	Alcance de la creación de reflejo	Description	Detalles de configuración
Instancia global de creación de reflejo de puertos de capa 2	Todos los puertos del chasis del enrutador (o conmutador) serie MX.	Paquetes VPLS recibidos en todos los puertos del chasis del enrutador (o conmutador) serie MX.	Si se configura, las propiedades globales de duplicación de puertos se aplican implícitamente a todos los paquetes VPLS recibidos en todos los puertos del chasis del enrutador (o conmutador).	Consulte Configuración de la instancia global de creación de reflejo de puertos de capa 2https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-global-instance-configuring.html

Tabla 120: Aplicación de tipos de duplicación de puertos de capa 2 *(Continued)*

Tipo de definición de duplicación de puertos de capa 2	Punto de aplicación	Alcance de la creación de reflejo	Description	Detalles de configuración
Instancia con nombre de duplicación de puertos de capa 2	Puertos agrupados a nivel de FPC Consulte Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de FPC."Enlace de la creación de reflejo de puertos de capa 2 a puertos agrupados en el nivel de FPC" en la página 1192	Paquetes VPLS recibidos en puertos asociados con un DPC o FPC específico y sus motores de reenvío de paquetes.	Anula todas las propiedades de creación de reflejo de puertos configuradas por la instancia global de creación de reflejo de puertos.	Consulte Definición de una instancia con nombre de creación de reflejo de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-named-instance-configuring.html La cantidad de destinos de duplicación de puertos admitidos para un enrutador serie MX y para un conmutador serie EX está limitada a la cantidad de motores de reenvío de paquetes contenidos en los DPC o FPC

Tabla 120: Aplicación de tipos de duplicación de puertos de capa 2 *(Continued)*

Tipo de definición de duplicación de puertos de capa 2	Punto de aplicación	Alcance de la creación de reflejo	Description	Detalles de configuración
	Puertos agrupados a nivel de PIC Consulte Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC."Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC" en la página 1194	Paquetes VPLS recibidos en puertos asociados con un motor de reenvío de paquetes específico.	Anula cualquier propiedad de creación de reflejo de puertos configurada en el nivel de FPC o en la instancia global de creación de reflejo de puertos.	instalados en el chasis del enrutador o conmutador.

Tabla 120: Aplicación de tipos de duplicación de puertos de capa 2 *(Continued)*

Tipo de definición de duplicación de puertos de capa 2	Punto de aplicación	Alcance de la creación de reflejo	Description	Detalles de configuración
Filtro de firewall de duplicación de puerto de capa 2	Interfaz lógica (incluida una interfaz Ethernet agregada) Consulte Aplicación de la creación de reflejo de puertos de capa 2 a una interfaz lógica.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-applying-logical-interface.html	Paquetes VPLS recibidos o enviados en una interfaz lógica.	En la configuración del filtro del firewall , incluya y términos para aplicar a los paquetes seleccionados para la creación de reflejo:*actionaction-modifier* • Se recomienda la acción.`accept` • El modificador hace referencia implícitamente a las propiedades de duplicación de puertos actualmente enlazadas a las interfaces físicas subyacentes.`port-mirror` • El modificador hace referencia explícitamente a una instancia con nombre de creación de reflejo de puertos.`port-mirror-instance` *`pm-instance-name`* • (Opcional) Solo para paquetes de entrada de interfaz de túnel, para reflejar los paquetes en destinos adicionales, incluya el modificador.`next-hop-group` *`next-hop-group-name`* Este modificador hace referencia a un grupo de salto siguiente que especifica las direcciones del salto siguiente (para enviar copias adicionales de paquetes a un analizador).	Consulte Definición de un filtro de firewall de duplicación de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-configuring.html **NOTA**: Los filtros de firewall de duplicación de puertos de capa 2 no son compatibles con los sistemas lógicos. Para reflejar paquetes de entrada de interfaz de túnel a varios destinos, consulte también Definición de un grupo de salto

Tabla 120: Aplicación de tipos de duplicación de puertos de capa 2 *(Continued)*

Tipo de definición de duplicación de puertos de capa 2	Punto de aplicación	Alcance de la creación de reflejo	Description	Detalles de configuración
	Tabla de reenvío de VLAN o tabla de inundación Consulte Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente."Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente" en la página 1231	Tráfico de capa 2 reenviado o inundado a una VLAN		siguiente para la creación de reflejo de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-next-hop-group-configuring.html

Tabla 120: Aplicación de tipos de duplicación de puertos de capa 2 *(Continued)*

Tipo de definición de duplicación de puertos de capa 2	Punto de aplicación	Alcance de la creación de reflejo	Description	Detalles de configuración
	Tabla de reenvío de instancias de enrutamiento VPLS o tabla de inundación Consulte Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a una instancia de enrutamiento VPLS.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-applying-vpls-routing-instance.html	Tráfico de capa 2 reenviado o inundado a una instancia de enrutamiento VPLS		

Restricciones en la duplicación de puertos de capa 2

Las siguientes restricciones se aplican a la *duplicación de puertos de* capa 2:

- Solo se pueden reflejar los datos de tránsito de capa 2 (paquetes que contienen fragmentos de datos que transitan por la plataforma de enrutamiento o el conmutador a medida que se reenvían desde un

origen a un destino). Los datos locales de capa 2 (paquetes que contienen fragmentos de datos destinados o enviados por el motor de enrutamiento, como los paquetes de control de capa 2) no se reflejan.

- Si aplica un filtro de duplicación de puertos a la salida de una interfaz lógica, sólo se reflejan los paquetes de unidifusión. Para reflejar paquetes de difusión, paquetes de multidifusión, paquetes de unidifusión con una dirección MAC (Media Access Control) de destino desconocido o paquetes con una entrada MAC en la tabla de enrutamiento MAC de destino (DMAC), aplique un filtro a la entrada a la tabla de inundación de una instancia de enrutamiento de VLAN o de servicio LAN privada virtual (VPLS).

- El dispositivo de destino espejo debe estar en una VLAN dedicada y no debe participar en ninguna actividad de puente; El dispositivo de destino reflejado no debe tener un puente hacia el destino de tráfico final y el dispositivo de destino reflejado no debe enviar los paquetes reflejados de vuelta a la dirección de origen.

- Para la instancia global de creación de reflejo de puertos o una instancia de creación de reflejo de puerto con nombre, sólo puede configurar una interfaz de salida de reflejo por instancia de creación de reflejo de puerto y familia de direcciones de paquetes. Si incluye más de una instrucción en la instrucción, la instrucción anterior se invalida.`interfacefamily (ethernet-switching | ccc | vpls) outputinterface`

- El filtrado de firewall de espejado de puertos de capa 2 no es compatible con los sistemas lógicos.

  En una definición de filtro de firewall de duplicación de puertos de capa 2, el filtro (o) se basa en las propiedades de duplicación de puertos definidas en la instancia global o en instancias con nombre de creación de reflejo de puertos de capa 2, que se configuran en la jerarquía.*action-modifier*`port-mirrorport-mirror-instance` *pm-instance-name*`[edit forwarding-options port-mirroring]` Por lo tanto, el filtro no puede admitir la creación de reflejo de puertos de capa 2 para sistemas lógicos.*term*

- Para un filtro de firewall de creación de reflejo de puerto de capa 2 en el que se hace referencia implícitamente a las propiedades de creación de reflejo de puerto de capa 2 mediante la inclusión de la instrucción, si varias instancias con nombre de creación de reflejo de puerto de capa 2 están enlazadas a la interfaz física subyacente, solo se utiliza el primer enlace de la estrofa (o el único enlace) en la interfaz lógica.`port-mirror` Esto se hace para la compatibilidad con versiones anteriores.

- Los filtros de firewall de duplicación de puertos de capa 2 no admiten el uso de subgrupos del próximo salto para equilibrar la carga del tráfico reflejado.

Configuración de analizadores y duplicación de puertos

in this section

- Descripción de los analizadores de duplicación de puertos | **1071**
- Configuración de la creación de reflejo en conmutadores EX9200 para analizar el tráfico (procedimiento de la CLI) | **1079**
- Configuración de la creación de reflejo en conmutadores EX4300 para analizar el tráfico (procedimiento de la CLI) | **1089**
- Configuración de la creación de reflejo de puertos para analizar el tráfico (procedimiento de la CLI) | **1094**
- Verificación de entrada y salida para analizadores de duplicación de puertos en conmutadores de la serie EX | **1099**
- Ejemplo: Configuración de analizadores de creación de reflejo de puertos para la supervisión local del uso de recursos de los empleados | **1101**
- Ejemplo: Configuración de la creación de reflejo de puertos para la supervisión remota del uso de los recursos de los empleados | **1107**
- Ejemplo: Configuración de la creación de reflejo en varias interfaces para el monitoreo remoto del uso de recursos de los empleados en conmutadores EX9200 | **1121**
- Ejemplo: Configuración de la duplicación para la supervisión remota del uso de recursos de los empleados mediante un conmutador de tránsito en conmutadores EX9200 | **1133**
- Ejemplo: Configuración de la duplicación para el monitoreo local del uso de recursos de los empleados en conmutadores EX4300 | **1144**
- Ejemplo: Configuración de la duplicación para la supervisión remota del uso de recursos de los empleados en conmutadores EX4300 | **1154**
- Ejemplo: Configuración de la duplicación para el monitoreo remoto del uso de recursos de los empleados a través de un conmutador de tránsito en conmutadores EX4300 | **1168**

Descripción de los analizadores de duplicación de puertos

in this section

- Descripción general del analizador | **1073**
- Descripción general del analizador estadístico | **1073**
- Descripción general del analizador predeterminado | **1073**

- Creación de reflejo de puertos en un grupo de puertos enlazados a varios analizadores estadísticos | **1073**
- Terminología del analizador de duplicación de puertos | **1074**
- Directrices de configuración para analizadores de duplicación de puertos | **1076**

La duplicación de puertos se puede usar para el análisis de tráfico en enrutadores y conmutadores que, a diferencia de los concentradores, no difunden paquetes a todos los puertos del dispositivo de destino. La duplicación de puertos envía copias de todos los paquetes o paquetes de muestra basados en políticas a analizadores locales o remotos donde puede supervisar y analizar los datos.

En el contexto de los analizadores de duplicación de puertos, utilizamos el término *dispositivo de conmutación*. El término indica que el dispositivo (incluidos los enrutadores) está realizando una función de conmutación.

Puede utilizar analizadores a nivel de paquete para ayudarle a:

- Supervisar el tráfico de red
- Aplicar políticas de uso de red
- Aplicar políticas de uso compartido de archivos
- Identificar las causas de los problemas
- Identificar estaciones o aplicaciones con un uso intensivo o anormal del ancho de banda

Puede configurar la duplicación de puertos para duplicar:

- Paquetes en puente (paquetes de capa 2)
- Paquetes enrutados (paquetes de capa 3)

Los paquetes duplicados se pueden copiar en una interfaz local para el monitoreo local o en un dominio de VLAN o puente para el monitoreo remoto.

Se pueden copiar los siguientes paquetes:

- **Packets entering or exiting a port**: puede duplicar paquetes que entran o salen de puertos, en cualquier combinación, para un máximo de 256 puertos. Por ejemplo, puede enviar copias de los paquetes que entran en algunos puertos y los paquetes que salen de otros puertos al mismo puerto del analizador local o VLAN del analizador.
- **Packets entering or exiting a VLAN or bridge domain**: puede reflejar los paquetes que entran o salen de un dominio de VLAN o puente en un puerto del analizador local o en una VLAN o dominio de

puente del analizador. Puede configurar varias VLAN (hasta 256 VLAN) o dominios de puente como entradas de entrada a un analizador, incluido un rango de VLAN y VLAN privadas (PVLAN).

- **Policy-based sample packets**: puede reflejar una muestra basada en políticas de paquetes que ingresan a un dominio de puerto, VLAN o puente. Configure un filtro de firewall con una directiva para seleccionar los paquetes que se van a reflejar. Puede enviar la muestra a una instancia de duplicación de puertos, a una VLAN de analizador o a un dominio de puente.

Descripción general del analizador

Puede configurar un analizador para definir tanto el tráfico de entrada como el tráfico de salida en la misma configuración del analizador. El tráfico de entrada que se va a analizar puede ser el tráfico que entra o el tráfico que sale de una interfaz o VLAN. La configuración del analizador le permite enviar este tráfico a una interfaz de salida, instancia, grupo del próximo salto, VLAN o dominio de puente. Puede configurar un analizador en el nivel jerárquico .`[edit forwarding-options analyzer]`

Descripción general del analizador estadístico

Puede definir un conjunto de propiedades de duplicación, como la velocidad de creación de reflejo y la longitud máxima de paquete para el tráfico, que puede enlazar explícitamente a puertos físicos del enrutador o conmutador. Este conjunto de propiedades de reflejo constituye un analizador estadístico (también denominado analizador no predeterminado). En este nivel, puede enlazar una instancia con nombre a los puertos físicos asociados a un FPC específico.

Descripción general del analizador predeterminado

Puede configurar un analizador sin configurar ninguna propiedad de creación de reflejo (como la velocidad de creación de reflejo o la longitud máxima del paquete). De forma predeterminada, la velocidad de creación de reflejo se establece en 1 y la longitud máxima del paquete se establece en la longitud completa del paquete. Estas propiedades se aplican a nivel global y no necesitan estar enlazadas a un FPC específico.

Creación de reflejo de puertos en un grupo de puertos enlazados a varios analizadores estadísticos

Puede aplicar hasta dos analizadores estadísticos a los mismos grupos de puertos del dispositivo de conmutación. Al aplicar dos instancias de analizador estadístico diferentes al mismo FPC o motor de reenvío de paquetes, puede enlazar dos especificaciones de duplicación de capa 2 distintas a un único grupo de puertos. Las propiedades de creación de reflejo enlazadas a una FPC invalidan cualquier propiedad del analizador (analizador predeterminado) enlazada a nivel global en el dispositivo de conmutación. Las propiedades predeterminadas del analizador se reemplazan mediante el enlace de una segunda instancia del analizador en el mismo grupo de puertos.

Terminología del analizador de duplicación de puertos

Tabla 121 en la página 1074 enumera algunos términos del analizador de duplicación de puertos y sus descripciones.

Tabla 121: Terminología del analizador

Término	Description
Analizador	En una configuración de duplicación, el analizador incluye: • El nombre del analizador • Puertos de origen (entrada), VLAN o dominios de puente • El destino de los paquetes reflejados (ya sea un puerto local, VLAN o dominio de puente)
Interfaz de salida del analizador (También conocido como puerto de monitor)	Interfaz donde se envía el tráfico reflejado y se conecta un analizador de protocolos. Las interfaces utilizadas como salida a un analizador deben configurarse bajo el nivel de jerarquía.`forwarding-options` Las interfaces de salida del analizador tienen las siguientes limitaciones: • Tampoco pueden ser un puerto de origen. • No participan en protocolos de capa 2, como el protocolo de árbol de expansión (STP). • Si el ancho de banda de la interfaz de salida del analizador no es suficiente para manejar el tráfico de los puertos de origen, se descartarán los paquetes de desbordamiento.
Analizador VLAN o dominio de puente (También conocido como VLAN de monitor o dominio de puente)	VLAN o dominio de puente al que se envía el tráfico reflejado para que lo utilice un analizador de protocolos. Las interfaces miembro en la VLAN de monitor o en el dominio de puente se distribuyen por los dispositivos de conmutación de la red.
Analizador basado en dominios de puente	Una sesión de analizador configurada para usar dominios de puente para entrada, salida o ambos.

Tabla 121: Terminología del analizador *(Continued)*

Término	Description
Analizador predeterminado	Un analizador con parámetros de duplicación predeterminados. De forma predeterminada, la velocidad de creación de reflejo es 1 y la longitud máxima del paquete es la longitud del paquete completo.
Interfaz de entrada (También conocidos como puertos duplicados o interfaces monitoreadas)	Una interfaz en el dispositivo de conmutación donde se refleja el tráfico que entra o sale de esta interfaz.
Analizador basado en LAG	Un analizador que tiene un grupo de agregación de vínculos (LAG) especificado como interfaz de entrada (entrada) en la configuración del analizador.
Duplicación local	Configuración del analizador en la que los paquetes se reflejan en un puerto del analizador local.
Estación de monitoreo	Equipo que ejecuta un analizador de protocolos.
Analizador basado en el grupo del siguiente salto	Una configuración de analizador que utiliza el grupo del salto siguiente como salida a un analizador.
Analizador basado en puertos	Una configuración de analizador que define interfaces para entrada y salida.
Aplicación del analizador de protocolos	Una aplicación utilizada para examinar paquetes transmitidos a través de un segmento de red. También se le suele llamar analizador de red, rastreador de paquetes o sonda.
Duplicación remota	Funciona de la misma manera que la creación de reflejo local, excepto que el tráfico reflejado no se copia en un puerto del analizador local, sino que se inunda a una VLAN del analizador o a un dominio de puente que se crea específicamente con el fin de recibir tráfico reflejado. Los paquetes duplicados tienen una etiqueta externa adicional de la VLAN del analizador o del dominio de puente.

Tabla 121: Terminología del analizador *(Continued)*

Término	Description
Analizador estadístico (También conocido como analizador no predeterminado)	Un conjunto de propiedades de creación de reflejo que se pueden enlazar explícitamente a los puertos físicos del conmutador. Este conjunto de propiedades del analizador se conoce como analizador estadístico.
Analizador basado en VLAN	Una configuración de analizador que utiliza VLAN para entregar el tráfico reflejado al analizador.

Directrices de configuración para analizadores de duplicación de puertos

Al configurar analizadores de duplicación de puertos. Le recomendamos que siga estas pautas para garantizar un beneficio óptimo. Se recomienda deshabilitar la creación de reflejo cuando no la esté utilizando y seleccionar interfaces específicas como entrada para el analizador en lugar de utilizar la opción de palabra clave, que habilita la creación de reflejo en todas las interfaces.`all` La duplicación de solo los paquetes necesarios reduce cualquier impacto potencial en el rendimiento.

También puede limitar la cantidad de tráfico reflejado de la siguiente manera:

- Uso del muestreo estadístico
- Uso de un filtro de firewall
- Establecer una proporción para seleccionar una muestra estadística

Con la creación de reflejo local, el tráfico de varios puertos se replica en la interfaz de salida del analizador. Si la interfaz de salida de un analizador alcanza su capacidad, los paquetes se descartan. Debe considerar si el tráfico que se refleja supera la capacidad de la interfaz de salida del analizador.

Tabla 122 en la página 1077 Resume otras directrices de configuración para los analizadores.

Tabla 122: Directrices de configuración para analizadores de duplicación de puertos

Pauta	Información de valor o soporte	Comentario
Número de analizadores que puede habilitar simultáneamente.	64 Analizadores predeterminados 2 por FPC–Analizador estadístico	Los analizadores estadísticos deben estar enlazados a una FPC para reflejar el tráfico en los puertos que pertenecen a esa FPC. **NOTA**: Las propiedades predeterminadas del analizador están implícitamente enlazadas en la última (o penúltima) instancia de todos los FPC del sistema. Por lo tanto, cuando se enlaza explícitamente un segundo analizador estadístico en la FPC, se reemplazan las propiedades predeterminadas del analizador.
Número de interfaces, VLAN o dominios de puente que puede utilizar como entrada de entrada a un analizador.	256	–
Tipos de puertos en los que no se puede reflejar el tráfico.	• Puertos de chasis virtual (VCP) • Puertos Ethernet de administración (me0 o vme0) • Interfaces de enrutamiento y puente integrados (IRB) • Interfaces de capa 3 etiquetadas por VLAN	
Familias de protocolos que puede incluir en un analizador.	para los conmutadores de la serie EX y para los enrutadores de la serie MX.`ethernet-switchingbridge`	Un analizador solo refleja el tráfico en puente. Para reflejar el tráfico enrutado, utilice la configuración de creación de reflejo de puertos con como o `.familyinetinet6`

Tabla 122: Directrices de configuración para analizadores de duplicación de puertos *(Continued)*

Pauta	Información de valor o soporte	Comentario
Los paquetes con errores de capa física no se envían al analizador local o remoto.	Aplicable	Los paquetes con estos errores se filtran y, por lo tanto, no se envían al analizador.
El analizador no admite tráfico de velocidad de línea.	Aplicable	La creación de reflejo para el tráfico de velocidad de línea se realiza con el mejor esfuerzo.
Salida del analizador en una interfaz LAG.	Compatible	
El analizador genera el modo de interfaz como modo troncal.	Compatible	• La interfaz troncal debe ser miembro de todas las VLAN o dominios de puente relacionados con la configuración de entrada del analizador. • Debe usar la opción si la entrada se ha configurado como VLAN o dominio de puente y el resultado es una interfaz troncal. `mirror-once` **NOTA**: Con la opción de reflejar una vez, si la entrada del analizador proviene de la duplicación de entrada y salida, solo se refleja el tráfico de entrada. Si se requiere reflejo de entrada y salida, la interfaz de salida no puede ser un troncal. En tales casos, configure la interfaz como una interfaz de acceso.
Reflejo de salida de paquetes de control generados por el host.	No compatible	
Configuración de interfaces lógicas de capa 3 en la estrofa de un analizador.`input`	No compatible	

Tabla 122: Directrices de configuración para analizadores de duplicación de puertos *(Continued)*

Pauta	Información de valor o soporte	Comentario
Se deben evitar las estrofas de entrada y salida del analizador que contengan miembros de la misma VLAN o de la propia VLAN.	Aplicable	
Soporte para VLAN y sus interfaces miembro en diferentes sesiones de analizador	No compatible	Si se configura la creación de reflejo, cualquiera de los analizadores estará activo.
Duplicación de salida de interfaces Ethernet (ae) agregadas y sus interfaces lógicas secundarias configuradas para diferentes analizadores.	No compatible	

Configuración de la creación de reflejo en conmutadores EX9200 para analizar el tráfico (procedimiento de la CLI)

in this section

- Configuración de un analizador para el análisis de tráfico local | **1080**
- Configuración de un analizador para el análisis de tráfico remoto | **1081**
- Configuración de un analizador estadístico para el análisis de tráfico local | **1083**
- Configuración de un analizador estadístico para el análisis de tráfico remoto | **1084**
- Enlazar analizadores estadísticos a puertos agrupados en el nivel de FPC | **1086**
- Configurar un analizador con varios destinos mediante grupos de salto siguiente | **1087**
- Definición de un grupo de salto siguiente para la creación de reflejo de capa 2 | **1088**

Los conmutadores EX9200 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para supervisión local o a una VLAN para supervisión remota. Puede utilizar la creación de reflejo para copiar los siguientes paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o salen de una VLAN

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Desactive los analizadores que haya configurado cuando no los esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado de la siguiente manera:
  - Uso de muestreo estadístico.
  - Establecer ratios para seleccionar muestras estadísticas.
  - Uso de filtros de firewall.

NOTA: Si desea crear analizadores adicionales sin eliminar los analizadores existentes, deshabilite los analizadores existentes mediante la instrucción de la interfaz de línea de comandos (CLI) o de la página de configuración de J-Web para la creación de reflejo.`disable analyzer` *`analyzer-name`*

NOTA: Las interfaces utilizadas como salida a un analizador deben configurarse en el comando y deben estar asociadas a una VLAN.`ethernet-switching family`

Configuración de un analizador para el análisis de tráfico local

Para reflejar el tráfico de red o el tráfico de VLAN en el conmutador a una interfaz en el conmutador mediante el uso de analizadores:

1. Elija un nombre para el analizador y especifique la entrada:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

Por ejemplo, cree un analizador llamado para monitorear los paquetes que ingresan a las interfaces ge-0/0/0.0 y ge-0/0/1.0:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0

[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure la interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output interface interface-name
```

Por ejemplo, configure ge-0/0/10.0 como interfaz de destino para el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Configuración de un analizador para el análisis de tráfico remoto

Para reflejar el tráfico que atraviesa las interfaces o una VLAN del conmutador a una VLAN utilizada para el análisis desde una ubicación remota:

1. Configure una VLAN para transportar el tráfico reflejado:

```
[edit]
user@switch# set vlans analyzer-name vlan-id vlan-ID
```

Por ejemplo, defina una VLAN del analizador llamada y asígnele el ID de VLAN:`remote-analyzer999`

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Establezca la interfaz conectada al conmutador de distribución en modo de acceso y asóciela a la VLAN del analizador:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode
access vlan members vlan-ID
```

Por ejemplo, establezca la interfaz ge-0/1/1 en modo de acceso y asóciela al ID de VLAN del analizador:`999`

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode access
vlan members 999
```

3. Configure el analizador:

   a) Defina un analizador y especifique el tráfico que se va a reflejar:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

   Por ejemplo, defina que el analizador para el que el tráfico que se va a reflejar comprende paquetes que entran en las interfaces ge-0/0/0.0 y ge-0/0/1.0:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

   b) Especifique la VLAN del analizador como salida para el analizador:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

Por ejemplo, especifique la VLAN como analizador de salida para el analizador:`remote-analyzeremployee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

Configuración de un analizador estadístico para el análisis de tráfico local

Para reflejar el tráfico de interfaz o VLAN del conmutador a una interfaz del conmutador mediante un analizador estadístico:

1. Elija un nombre para el analizador y especifique las interfaces de entrada:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name

[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

   Por ejemplo, especifique un analizador llamado y especifique las interfaces de entrada ge-0/0/0 y ge-0/0/1:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0

[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure la interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface interface-name
```

   Por ejemplo, configure ge-0/0/10.0 como interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

3. Especifique las propiedades de creación de reflejo.

1. Especifique la velocidad de creación de reflejo, es decir, el número de paquetes que se reflejarán por segundo:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input rate number
```

   El intervalo válido es de 1 a 65.535.

2. Especifique a qué longitud se truncan los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input maximum-packet-length number
```

El intervalo válido es de 0 a 9216. El valor predeterminado es 0, lo que indica que los paquetes reflejados no se truncan.

Configuración de un analizador estadístico para el análisis de tráfico remoto

Para reflejar el tráfico que atraviesa las interfaces o una VLAN en el conmutador a una VLAN para su análisis desde una ubicación remota mediante un analizador estadístico:

1. Configure una VLAN para transportar el tráfico reflejado:

```
[edit]
user@switch# set vlans vlan-name vlan-id vlan-ID
```

   Por ejemplo, configure una VLAN llamada con ID de VLAN :`remote-analyzer999`

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Establezca la interfaz conectada al conmutador de distribución en modo de acceso y asóciela a la VLAN:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode
access vlan members vlan-ID
```

Por ejemplo, establezca la interfaz ge-0/1/1.0 que está conectada al conmutador de distribución en modo de acceso y asóciela a la VLAN:`remote-analyzer`

```
[edit]
user@switch# set interfaces ge-0/1/1.0 unit 0 family ethernet-switching interface-mode access
vlan members 999
```

3. Configure el analizador estadístico:

   a) Especifique el tráfico que se va a reflejar:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name input ingress interface interface-name
   ```

   Por ejemplo, especifique los paquetes que ingresan en los puertos ge-0/0/0.0 y ge-0/0/1.0 que se reflejarán:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
   ```

   b) Especifique una salida para el analizador:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name output vlan vlan-ID
   ```

   Por ejemplo, especifique la VLAN como salida para el analizador:`remote-analyzer`

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output vlan 999
   ```

4. Especifique las propiedades de creación de reflejo.

   1. Especifique la velocidad de creación de reflejo, es decir, el número de paquetes que se reflejarán por segundo:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input rate number
   ```

El intervalo válido es de 1 a 65.535.

2. Especifique la longitud a la que se van a truncar los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input  maximum-packet-length number
```

El intervalo válido es de 0 a 9216. El valor predeterminado es 0, lo que significa que los paquetes reflejados no se truncan.

Enlazar analizadores estadísticos a puertos agrupados en el nivel de FPC

Puede enlazar un analizador estadístico a una FPC específica en el conmutador, es decir, puede enlazar la instancia del analizador estadístico en el nivel de FPC del conmutador. Las propiedades de duplicación especificadas en el analizador estadístico se aplican a todos los puertos físicos asociados con todos los motores de reenvío de paquetes en la FPC especificada.

Para enlazar una instancia con nombre del analizador de capa 2 a una FPC:

1. Habilite la configuración de las propiedades del chasis del conmutador:

```
[edit]
user@switch# edit chassis
```

2. Habilitar la configuración de una FPC (y sus PIC instaladas):

```
[edit chassis]
user@switch# edit fpc slot-number
```

3. Enlazar una instancia de analizador estadístico a la FPC:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-1
```

4. (Opcional) Para enlazar una segunda instancia de analizador estadístico de creación de reflejo de capa 2 a la misma FPC, repita el paso 3 y especifique un nombre de analizador estadístico diferente:

```
[edit chassis fpc slot-number]
user@switch# set port-mirror-instance stats_analyzer-2
```

5. Compruebe la configuración mínima del enlace:

```
[edit chassis fpc slot-number port-mirror-instance analyzer_name]
user@switch# top
[edit]
user@switch# show chassis
chassis {
   fpc slot-number { # Bind two statistical analyzers or port mirroring
                     named instances at the FPC level.
   port-mirror-instance stats_analyzer-1;
   port-mirror-instance stats_analyzer-2;
                  }
               }
```

NOTA: Al enlazar una segunda instancia (en este ejemplo), las propiedades de creación de reflejo de esta sesión, si están configuradas, anulan cualquier analizador predeterminado.`stats_analyzer-2`

Configurar un analizador con varios destinos mediante grupos de salto siguiente

Puede reflejar el tráfico a varios destinos configurando los grupos del próximo salto como salida del analizador. La duplicación de paquetes a múltiples destinos también se conoce como duplicación de puertos multipaquete.

Para reflejar el tráfico de interfaz o VLAN en el conmutador a una interfaz en el conmutador (mediante el uso de analizadores):

1. Elija un nombre para el analizador y especifique la entrada:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

Por ejemplo, cree un analizador llamado para el cual el tráfico de entrada comprende paquetes que ingresan a las interfaces ge-0/0/0.0 y ge-0/0/1.0:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure la interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output next-hop-group next-hop-group-name
```

Por ejemplo, configure el grupo del próximo salto como destino del analizador:`nhgemployee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output next-hop-group nhg
```

Definición de un grupo de salto siguiente para la creación de reflejo de capa 2

La configuración del grupo del salto siguiente en el nivel de configuración permite definir un nombre de grupo del salto siguiente, el tipo de direcciones que se usarán en el grupo del salto siguiente y las interfaces lógicas que forman los múltiples destinos a los que se puede reflejar el tráfico.`[edit forwarding-options]` De forma predeterminada, el grupo del salto siguiente se especifica utilizando direcciones de capa 3 mediante la instrucción.`[edit forwarding-options next-hop-group next-hop-group-name group-type inet]` Para especificar un grupo de salto siguiente utilizando direcciones de capa 2 en su lugar, incluya la instrucción.`[edit forwarding-options next-hop-group next-hop-group-name group-type layer-2]`

Para definir un grupo de salto siguiente para la creación de reflejo de capa 2:

1. Habilite la configuración de un grupo del próximo salto para la creación de reflejo de capa 2:

```
[edit forwarding-options ]
user@switch# set next-hop-group next-hop-group-name
```

Por ejemplo, configure con el nombre :`next-hop-groupnhg`

```
[edit forwarding-options]
user@switch# set next-hop-group nhg
```

2. Especifique el tipo de direcciones que se utilizarán en la configuración del grupo del próximo salto:

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set group-type layer-2
```

Por ejemplo, configure como porque la salida del analizador solo debe ser :`next-hop-group typelayer-2layer-2`

```
[edit forwarding-options]
user@switch# set next-hop-group nhg group-type layer-2
```

3. Especifique las interfaces lógicas del grupo del próximo salto:

```
[edit forwarding-options next-hop-group next-hop-group-name]
user@switch# set interface logical-interface-name-1
user@switch# set interface logical-interface-name-2
```

Por ejemplo, para especificar ge-0/0/10.0 y ge-0/0/11.0 como interfaces lógicas del grupo del próximo salto:`nhg`

```
[edit forwarding-options]
user@switch# set next-hop-group nhg interface ge-0/0/10.0
user@switch# set next-hop-group nhg interface ge-0/0/11.0
```

Configuración de la creación de reflejo en conmutadores EX4300 para analizar el tráfico (procedimiento de la CLI)

in this section

- Configuración de un analizador para el análisis de tráfico local | **1090**
- Configuración de un analizador para el análisis de tráfico remoto | **1091**
- Configuración de la creación de reflejo de puertos | **1093**

NOTA: Esta tarea utiliza Junos OS para conmutadores serie EX compatibles con el estilo de configuración Enhanced Layer 2 software (ELS).

Los conmutadores EX4300 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que ingresan a una VLAN

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Deshabilite las configuraciones de creación de reflejo configuradas cuando no las esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado mediante filtros de firewall.

NOTA: Si desea crear analizadores adicionales sin eliminar los analizadores existentes, deshabilite los analizadores existentes mediante la instrucción de la interfaz de línea de comandos o la página de configuración de J-Web para la creación de reflejo.`disable analyzer` *`analyzer-name`*

NOTA: Las interfaces utilizadas como salida para un analizador deben configurarse bajo la familia.`ethernet-switching`

Configuración de un analizador para el análisis de tráfico local

Para reflejar el tráfico de interfaz o VLAN en el conmutador a una interfaz en el conmutador (mediante el uso de analizadores):

1. Elija un nombre para el analizador y especifique la entrada:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

Por ejemplo, cree un analizador llamado para el cual el tráfico de entrada son paquetes que entran en las interfaces ge-0/0/0.0 y ge-0/0/1.0:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0

[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Configure la interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output interface interface-name
```

Por ejemplo, configure ge-0/0/10.0 como interfaz de destino para el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Configuración de un analizador para el análisis de tráfico remoto

Para reflejar el tráfico que atraviesa las interfaces o una VLAN en el conmutador a una VLAN para su análisis desde una ubicación remota (mediante el uso de analizadores):

1. Configure una VLAN para transportar el tráfico reflejado:

```
[edit]
user@switch# set vlans analyzer-name vlan-id vlan-ID
```

Por ejemplo, defina una VLAN del analizador llamada y asígnele un ID de VLAN de :`remote-analyzer999`

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Configure la interfaz del módulo de vínculo ascendente que está conectada al conmutador de distribución en modo troncal y asóciela a la VLAN del analizador:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode
trunk vlan members vlan-ID
```

Por ejemplo, establezca la interfaz ge-0/1/1 en modo troncal y asóciela al ID de VLAN del analizador:`999`

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode trunk
vlan members 999
```

3. Configure el analizador:

a) Defina un analizador y especifique el tráfico que se va a reflejar:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

Por ejemplo, defina el analizador para el que el tráfico que se va a reflejar son los paquetes que entran en las interfaces ge-0/0/0.0 y ge-0/0/1.0:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

b) Especifique la VLAN del analizador como salida para el analizador:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

Por ejemplo, especifique la VLAN como analizador de salida para el analizador:`remote-analyzeremployee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

Configuración de la creación de reflejo de puertos

Para filtrar los paquetes que se reflejarán en una instancia de creación de reflejo de puertos, cree la instancia y, a continuación, utilícela como acción en el filtro de firewall. Puede usar filtros de firewall en configuraciones de creación de reflejo local y remota.

Si se utiliza la misma instancia de duplicación de puertos en varios filtros o términos, los paquetes se copian en el puerto de salida del analizador o en la VLAN del analizador solo una vez.

Para filtrar el tráfico reflejado, cree una instancia de creación de reflejo de puertos en el nivel de jerarquía y, a continuación, cree un filtro de firewall.`[edit forwarding-options]` El filtro puede usar cualquiera de las condiciones de coincidencia disponibles y debe tenerlo como acción.`port-mirror-instance` *`instance-name`* Esta acción en la configuración del filtro del firewall proporciona la entrada a la instancia de duplicación de puertos.

Para configurar una instancia de creación de reflejo de puerto con filtros de firewall:

1. Configure el nombre de la instancia de duplicación de puertos (aquí,) y el resultado:`employee-monitor`
   a) Para el análisis local, establezca el resultado en la interfaz local donde conectará el equipo que ejecuta el analizador de protocolos:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance employee-monitor output interface ge-0/0/10.0
   ```

   b) Para el análisis remoto, establezca el resultado en la VLAN:`remote-analyzer`

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring instance employee-monitor output vlan 999
   ```

2. Cree un filtro de firewall utilizando cualquiera de las condiciones de coincidencia disponibles y asígnelo a la acción:`employee-monitorport-mirror-instance`

   Este paso muestra un filtro de firewall, con dos términos (y):`example-filterno-analyzerto-analyzer`

a) Cree el primer término para definir el tráfico que no debe pasar a través de la instancia de creación de reflejo de puertos: `employee-monitor`

```
[edit firewall family ethernet-switching
user@switch# set filter example-filter term no-analyzer from source-address ip-address
user@switch# set filter example-filter term no-analyzer from destination-address ip-address
user@switch# set filter example-filter term no-analyzer then accept
```

b) Cree el segundo término para definir el tráfico que debe pasar a través de la instancia de duplicación de puertos:`employee-monitor`

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer from destination-port 80
user@switch# set filter example-filter term to-analyzer then port-mirror-instance employee-
monitor
user@switch# set filter example-filter term to-analyzer then accept
```

3. Aplique el filtro de firewall a las interfaces o VLAN que proporcionan entrada a la instancia de creación de reflejo de puertos:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input example-
filter
ser@switch# set vlan remote-analyzer filter input example-filter
```

Configuración de la creación de reflejo de puertos para analizar el tráfico (procedimiento de la CLI)

in this section

- Configuración de la creación de reflejo de puertos para el análisis de tráfico local | **1096**
- Configuración de la creación de reflejo de puertos para el análisis de tráfico remoto | **1096**
- Filtrado del tráfico que entra en un analizador | **1098**

Esta tarea de configuración utiliza Junos OS para conmutadores serie EX que no admiten el estilo de configuración Enhanced Layer 2 Software (ELS).

Los conmutadores de la serie EX le permiten configurar la duplicación de puertos para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. Puede utilizar la creación de reflejo de puertos para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que ingresan a una VLAN en conmutadores EX2200, EX3200, EX3300, EX4200, EX4500 o EX6200
- Paquetes que salen de una VLAN en conmutadores EX8200

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Desactive los analizadores de creación de reflejo de puertos configurados cuando no los esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado de la siguiente manera:
  - Uso de muestreo estadístico.
  - Establecer ratios para seleccionar muestras estadísticas.
  - Uso de filtros de firewall.

Antes de comenzar a configurar la creación de reflejo de puertos, tenga en cuenta las siguientes limitaciones para las interfaces de salida del analizador:

- No puede ser también un puerto de origen.
- No se puede utilizar para cambiar.
- No participe en protocolos de capa 2 (como RSTP) cuando forme parte de una configuración de creación de reflejo de puerto.
- No conserve ninguna asociación de VLAN que tenían antes de configurarse como interfaces de salida del analizador.

NOTA: Si desea crear analizadores adicionales sin eliminar el analizador existente, desactive primero el analizador existente mediante el comando o la página de configuración de J-Web para la creación de reflejo de puertos.`disable analyzer` *`analyzer-name`*

NOTA: Las interfaces utilizadas como salida para un analizador deben configurarse como familia `.ethernet-switching`

Configuración de la creación de reflejo de puertos para el análisis de tráfico local

Para reflejar el tráfico de interfaz o VLAN del conmutador a otra interfaz del conmutador:

1. Elija un nombre para el analizador, en este caso, y especifique la entrada (en este caso , los paquetes que ingresan y `:employee-monitorge-0/0/0ge-0/0/1`

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ingress interface ge-0/0/0.0

[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

2. Opcionalmente, puede especificar un muestreo estadístico de los paquetes estableciendo una proporción:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

   Cuando la proporción se establece en 200, 1 de cada 200 paquetes se refleja en el analizador. Puede utilizar el muestreo estadístico para reducir el volumen de tráfico reflejado, ya que un volumen elevado de tráfico reflejado puede requerir mucho rendimiento del conmutador. En los conmutadores EX8200, puede establecer una relación solo para los paquetes de entrada.

3. Configure la interfaz de destino para los paquetes reflejados:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Configuración de la creación de reflejo de puertos para el análisis de tráfico remoto

Para reflejar el tráfico que atraviesa las interfaces o una VLAN en el conmutador a una VLAN para su análisis desde una ubicación remota:

1. Configure una VLAN para transportar el tráfico reflejado. En esta documentación se llama a esta VLAN y se le asigna el ID de 999 por convención:`remote-analyzer`

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Establezca la interfaz del módulo de vínculo ascendente que está conectada al conmutador de distribución en modo troncal y asócielo a la VLAN:`remote-analyzer`

```
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching port-mode trunk vlan
members 999
```

3. Configure el analizador:

   a) Elija un nombre y establezca la prioridad de pérdida en alta. La prioridad de pérdida siempre debe establecerse en alta cuando se configura la duplicación remota de puertos:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor loss-priority high
```

   b) Especifique el tráfico que se va a reflejar: en este ejemplo, los paquetes que entran en los puertos y :`ge-0/0/0`ge-0/0/1

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

   c) Especifique la VLAN como salida para el analizador:`remote-analyzer`

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor output vlan 999
```

4. Opcionalmente, puede especificar un muestreo estadístico de los paquetes estableciendo una proporción:

```
[edit ethernet-switching-options]
user@switch# set analyzer employee-monitor ratio 200
```

Cuando la proporción se establece en 200, 1 de cada 200 paquetes se refleja en el analizador. Puede utilizarlo para reducir el volumen de tráfico reflejado, ya que un volumen muy alto de tráfico reflejado puede requerir mucho rendimiento del conmutador.

Filtrado del tráfico que entra en un analizador

Para filtrar los paquetes que se reflejan en un analizador, cree el analizador y, a continuación, utilícelo como acción en el filtro de firewall. Puede usar filtros de firewall en configuraciones de creación de reflejo de puertos locales y remotos.

Si se utiliza el mismo analizador en varios filtros o términos, los paquetes se copian en el puerto de salida del analizador o en la VLAN del analizador solo una vez.

Para filtrar el tráfico reflejado, cree un analizador y, a continuación, cree un filtro de firewall. El filtro puede utilizar cualquiera de las condiciones de coincidencia disponibles y debe tener una acción de `.analyzer` La acción del filtro de firewall proporciona la entrada al analizador.

Para configurar la creación de reflejo de puertos con filtros:

1. Configure el nombre del analizador (aquí,) y el resultado:`employee-monitor`

   a) Para el análisis local, establezca el resultado en la interfaz local a la que conectará el equipo que ejecuta la aplicación de analizador de protocolos:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

   b) Para el análisis remoto, establezca la prioridad de pérdida en alta y establezca la salida en la VLAN:`remote-analyzer`

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer employee-monitor loss-priority high output vlan 999
   ```

2. Cree un filtro de firewall utilizando cualquiera de las condiciones de coincidencia disponibles y especifique la acción como :`analyzer`

   Este paso muestra un filtro de firewall denominado , con dos términos:`example-filter`

a) Cree el primer término para definir el tráfico que no debe pasar al analizador:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from source-address ip-address
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from destination-address ip-address
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer then accept
```

b) Cree el segundo término para definir el tráfico que debe pasar al analizador:

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer from destination-port 80
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then analyzer employee-monitor
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then accept
```

3. Aplique el filtro de firewall a las interfaces o VLAN que se introducen en el analizador:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input example-
filter

[edit]
user@switch# set vlan remote-analyzer filter input example-filter
```

Verificación de entrada y salida para analizadores de duplicación de puertos en conmutadores de la serie EX

in this section

- Propósito | 1100
- Acción | 1100
- Significado | 1101

Propósito

Esta tarea de verificación utiliza Junos OS para conmutadores serie EX que no admiten el estilo de configuración Enhanced Layer 2 Software (ELS).

Verifique que se haya creado un analizador en el conmutador y que tenga las interfaces de entrada de espejo adecuadas y la interfaz de salida del analizador adecuada.

Acción

Puede comprobar que el analizador de reflejos de puertos está configurado como se esperaba mediante el comando.`show analyzer`

```
[edit]
user@switch>                      show analyzer
Analyzer name                  : employee-monitor
  Output VLAN                  : remote-analyzer
  Mirror ratio                 : 1
  Loss priority                : High
  Ingress monitored interfaces : ge-0/0/0.0
  Ingress monitored interfaces : ge-0/0/1.0
```

Puede ver todos los analizadores de espejo de puertos configurados en el conmutador, incluidos los que estén deshabilitados, mediante el comando en modo de configuración.`show ethernet-switching-options`

```
user@switch# show ethernet-switching-options
inactive: analyzer employee-web-monitor {
    loss-priority high;
    output {

analyzer employee-monitor {
    loss-priority high;
    input {
        ingress {
            interface ge-0/0/0.0;
            interface ge-0/0/1.0;
        }
    }
    output {
        vlan {
            remote-analyzer;
        }
```

```
    }
}
```

Significado

Esta salida muestra que el analizador empleado-monitor tiene una relación de 1 (duplicación de cada paquete, el valor predeterminado), una prioridad de pérdida de (establezca esta opción en siempre que la salida del analizador sea a una VLAN), está reflejando el tráfico que entra en ge-0/0/0 y ge-0/0/1, y está enviando el tráfico reflejado al analizador llamado remote-analyzer.`highhigh`

Ejemplo: Configuración de analizadores de creación de reflejo de puertos para la supervisión local del uso de recursos de los empleados

in this section

- Requisitos | **1102**
- Descripción general y topología | **1102**
- Duplicación de todo el tráfico de empleados para análisis local | **1103**
- Verificación | **1106**

Los dispositivos de Juniper Networks le permiten configurar la duplicación de puertos para enviar copias de paquetes a una interfaz local para monitoreo local, a una VLAN o a un dominio de puente para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o salen de un dominio de VLAN o puente

A continuación, puede analizar el tráfico reflejado de forma local o remota mediante un analizador de protocolos. Puede instalar un analizador en una interfaz de destino local. Si va a enviar tráfico duplicado a una VLAN analizadora o a un dominio de puente, puede utilizar un analizador en una estación de supervisión remota.

En este tema se describe cómo configurar la creación de reflejo local en un dispositivo de conmutación. En los ejemplos de este tema se describe cómo configurar un dispositivo de conmutación para reflejar el tráfico que entra en las interfaces conectadas a los equipos de los empleados en una interfaz de salida del analizador en ese mismo dispositivo.

Requisitos

Utilice uno de los siguientes componentes de hardware y software:

- Un conmutador EX9200 con Junos OS versión 13.2 o posterior
- Un enrutador serie MX con Junos OS versión 14.1 o posterior

Antes de configurar la creación de reflejo de puertos, asegúrese de que comprende los conceptos de creación de reflejos. Para obtener información acerca de los analizadores, consulte "Descripción de los analizadores de creación de reflejo de puertos" en la página 1071. Para obtener información acerca de la creación de reflejo de puertos, consulte Descripción de la creación de reflejo de puertos de capa 2."Descripción de la creación de reflejo de puertos de capa 2" en la página 1060

Descripción general y topología

En este tema se describe cómo reflejar todo el tráfico que entra en los puertos del dispositivo de conmutación a una interfaz de destino en el mismo dispositivo (creación de reflejo local). En este caso, el tráfico entra en los puertos conectados a los equipos de los empleados.

> **NOTA**: La duplicación de todo el tráfico requiere un ancho de banda significativo y solo debe realizarse durante una investigación activa.

Las interfaces ge-0/0/0 y ge-0/0/1 sirven como conexiones para los equipos de los empleados.

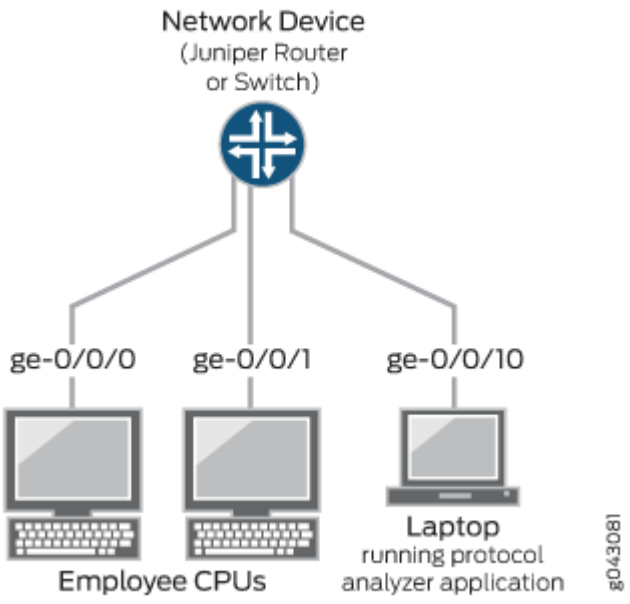
La interfaz ge-0/0/10 está reservada para el análisis del tráfico reflejado.

Conecte un PC que ejecute un analizador de protocolos a la interfaz de salida del analizador.

> **NOTA**: Varios puertos reflejados en una interfaz pueden provocar el desbordamiento del búfer, lo que provoca que los paquetes reflejados se descarten en la interfaz de salida.

Figura 34 en la página 1103 muestra la topología de red de este ejemplo.

Figura 34: Ejemplo de topología de red para creación de reflejo de puerto local



Duplicación de todo el tráfico de empleados para análisis local

in this section

- Procedimiento | **1103**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la duplicación local para el tráfico de entrada enviado en dos puertos conectados a las computadoras de los empleados, copie cualquiera de los siguientes comandos para conmutadores de la serie EX o para enrutadores de la serie MX y péguelos en la ventana de terminal del dispositivo de conmutación:

Serie EX

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family ethernet-switching
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0
```

Serie MX

```
[edit]
set interfaces ge-0/0/0 unit 0 family bridge interface-mode access vlan-id 99
set interfaces ge-0/0/1 unit 0 family bridge interface-mode access vlan-id 98
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0
```

Procedimiento paso a paso

Para configurar un analizador llamado y especificar las interfaces de entrada (origen) y la interfaz de salida del analizador:`employee-monitor`

1. Configure cada interfaz que se utilizará en la configuración del analizador. Utilice el protocolo de familia que sea correcto para su plataforma.

   ```
   EX Series
   [edit]
   set interfaces ge-0/0/0 unit 0 family ethernet-switching
   set interfaces ge-0/0/1 unit 0 family ethernet-switching
   ```

   Para configurar en una interfaz, debe configurar o también.`family bridgeinterface-mode accessinterface-mode trunk` También debe configurar .`vlan-id`

   ```
   MX Series
   [edit]
   set interfaces ge-0/0/0 unit 0 family bridge interface-mode access vlan-id 99
   set interfaces ge-0/0/1 unit 0 family bridge interface-mode access vlan-id 98
   ```

2. Configure cada interfaz conectada a los equipos de los empleados como una interfaz de analizador de salida.`employee-monitor`

```
[edit forwarding-options]
set analyzer employee-monitor input ingress interface ge-0/0/0.0
set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

3. Configure la interfaz del analizador de salida para el analizador.`employee-monitor`

   Esta será la interfaz de destino para los paquetes reflejados.

```
[edit forwarding-options]
set analyzer employee-monitor output interface ge-0/0/10.0
```

Resultados

Compruebe los resultados de la configuración.

```
[edit]
user@device# show forwarding-options
analyzer {
    employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            interface ge-0/0/10.0;
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | 1106

Comprobación de que el analizador se ha creado correctamente

Propósito

Compruebe que el analizador se ha creado en el dispositivo de conmutación con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitor`

Acción

Utilice el comando operativo para comprobar que un analizador está configurado como se esperaba.`show forwarding-options analyzer`

```
user@device> show forwarding-options analyzer
Analyzer name                        : employee-monitor
  Mirror rate                       : 1
  Maximum packet length             : 0
  State                                : up
  Ingress monitored interfaces      : ge-0/0/0.0
  Output interface                     : ge-0/0/10.0
```

Significado

El resultado muestra que el analizador tiene una proporción de 1 (es decir, duplicar cada paquete, la configuración predeterminada), el tamaño máximo del paquete original reflejado es 0 (lo que indica que todo el paquete está reflejado), el estado de la configuración es , y el analizador está reflejando el tráfico que entra en la interfaz ge-0/0/0 y envía el tráfico reflejado a la interfaz ge-0/0/10.`employee-monitorup`

Si el estado de la interfaz de salida es o si la interfaz de salida no está configurada, el valor de indicará que el analizador no recibirá tráfico reflejado.`downStatedown`

Ejemplo: Configuración de la creación de reflejo de puertos para la supervisión remota del uso de los recursos de los empleados

in this section

- Requisitos | **1108**
- Descripción general y topología | **1108**
- Duplicación del tráfico de empleados para el análisis remoto mediante un analizador estadístico | **1110**
- Verificación | **1120**

Los dispositivos de Juniper Networks le permiten configurar la duplicación de puertos para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN o dominio de puente para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o salen de una VLAN
- Paquetes que entran o salen de un dominio de puente

Si envía tráfico reflejado a una VLAN de analizador o a un dominio de puente, puede analizar el tráfico reflejado mediante un analizador de protocolos que se ejecute en una estación de supervisión remota.

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que haga lo siguiente:

- Deshabilite las sesiones de creación de reflejo configuradas cuando no las esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado de la siguiente manera:
  - Uso de muestreo estadístico.
  - Establecer ratios para seleccionar muestras estadísticas.
  - Uso de filtros de firewall.

En los ejemplos de este tema se describe cómo configurar la creación de reflejo de puertos remotos para analizar el uso de recursos de los empleados.

Requisitos

En este ejemplo se utiliza uno de los siguientes pares de componentes de hardware y software:

- Un conmutador EX9200 conectado a otro conmutador EX9200, ambos con la versión 13.2 o posterior de Junos OS
- Un enrutador de la serie MX conectado a otro enrutador de la serie MX, ambos con Junos OS versión 14.1 o posterior

Antes de configurar la creación remota de reflejos, asegúrese de que:

- Tienes una comprensión de los conceptos de reflejo. Para obtener información acerca de los analizadores, consulte "Descripción de los analizadores de creación de reflejo de puertos" en la página 1071. Para obtener información acerca de la creación de reflejo de puertos, consulte Descripción de la creación de reflejo de puertos de capa 2."Descripción de la creación de reflejo de puertos de capa 2" en la página 1060
- Las interfaces que utilizará el analizador como interfaces de entrada ya se han configurado en el dispositivo de conmutación.

Descripción general y topología

in this section

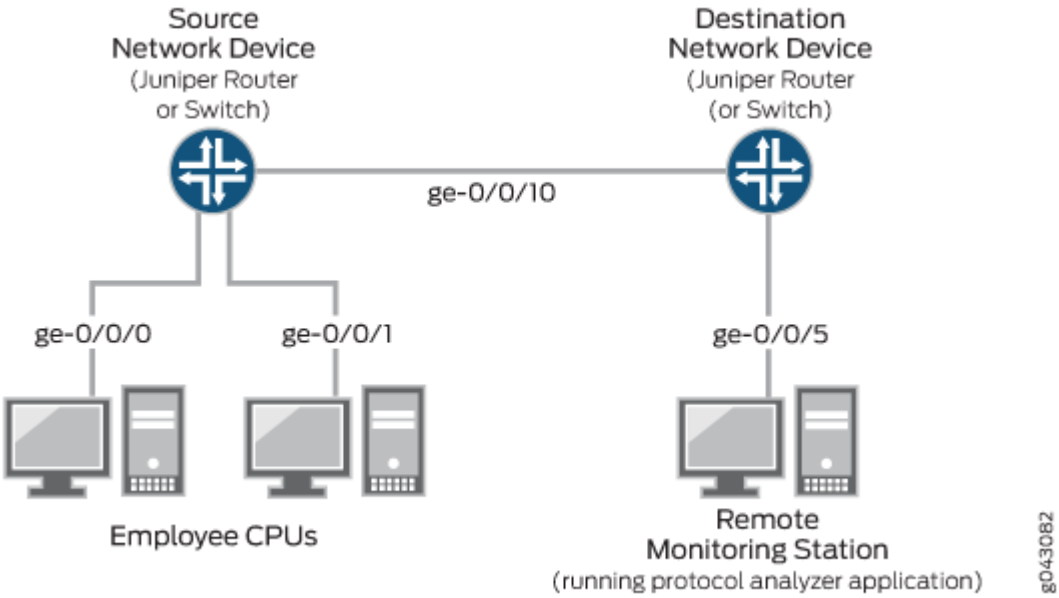
- Topología | **1109**

En este tema se describe cómo configurar la creación de reflejo de puertos en una VLAN de analizador remoto o en un dominio de puente para que el análisis se pueda realizar desde una estación de supervisión remota.

Figura 35 en la página 1109 muestra la topología de red para los escenarios de ejemplo de la serie EX y de la serie MX.

Topología

Figura 35: Topología de red para la creación de reflejo y el análisis de puertos remotos



En este ejemplo:

- La interfaz ge-0/0/0 es una interfaz de capa 2 y la interfaz ge-0/0/1 es una interfaz de capa 3 (ambas son interfaces en el dispositivo fuente) que sirven como conexiones para las computadoras de los empleados.
- La interfaz ge-0/0/10 es una interfaz de capa 2 que conecta el dispositivo de conmutación de fuente con el dispositivo de conmutación de destino.
- La interfaz ge-0/0/5 es una interfaz de capa 2 que conecta el dispositivo de conmutación de destino a la estación de monitoreo remoto.
- El analizador está configurado en todos los dispositivos de conmutación de la topología para transportar el tráfico reflejado.`remote-analyzer` Esta topología puede usar un dominio de VLAN o de puente.

Duplicación del tráfico de empleados para el análisis remoto mediante un analizador estadístico

in this section

- Duplicación del tráfico de empleados para análisis remoto para conmutadores de la serie EX | 1110
- Duplicación del tráfico de empleados para análisis remoto para enrutadores de la serie MX | 1115

Para configurar un analizador estadístico para el análisis de tráfico remoto para todo el tráfico de empleados entrantes y salientes, seleccione uno de los siguientes ejemplos:

Duplicación del tráfico de empleados para análisis remoto para conmutadores de la serie EX

Configuración rápida de CLI

Para configurar rápidamente un analizador estadístico para el análisis de tráfico remoto del tráfico entrante y saliente de empleados, copie los siguientes comandos para los conmutadores de la serie EX y péguelos en la ventana correcta del terminal del dispositivo de conmutación.

- Copie y pegue los siguientes comandos en la ventana terminal del dispositivo de conmutación de origen :

  Serie EX

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
set forwarding-options analyzer employee-monitor input rate 2
set forwarding-options analyzer employee-monitor input maximum-packet-length 128
set chassis fpc 0 port-mirror-instance employee-monitor
```

- Copie y pegue los siguientes comandos en la ventana Terminal del dispositivo de conmutación de destino :

Serie EX

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
```

Procedimiento paso a paso

Para configurar la creación de reflejo remota básica:

1. En el dispositivo de conmutación de origen, haga lo siguiente:

   - Configure el ID de VLAN para la VLAN.`remote-analyzer`

     ```
     [edit]
     user@device# set vlans remote-analyzer vlan-id 999
     ```

   - Configure la interfaz en el puerto de red conectado al dispositivo de conmutación de destino para el modo de acceso y asócielo a la VLAN.`remote-analyzer`

     ```
     [edit]
     user@device# set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode
     access
     user@device# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```

   - Configure el analizador estadístico .`employee-monitor`

     ```
     [edit forwarding-options]
     user@device# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@device# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@device# set analyzer employee-monitor input egress interface ge-0/0/0.0
     user@device# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@device# set analyzer employee-monitor output vlan remote-analyzer
     user@device# set analyzer employee-monitor input rate 2
     user@device# set analyzer employee-monitor input maximum-packet-length 128
     ```

- Enlazar el analizador estadístico a la FPC que contiene la interfaz de entrada.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

2. En el dispositivo de red de destino, haga lo siguiente:

- Configure el ID de VLAN para la VLAN.`remote-analyzer`

```
[edit]
user@device# set vlans remote-analyzer vlan-id 999
```

- Configure la interfaz en el dispositivo de conmutación de destino para el modo de acceso y asóciela a la VLAN.`remote-analyzer`

```
[edit interfaces]
user@device# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
user@device# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure la interfaz conectada al dispositivo de conmutación de destino para el modo de acceso.

```
[edit interfaces]
user@device# set ge-0/0/5 unit 0 family ethernet-switching interface-mode access
```

- Configure el analizador.`employee-monitor`

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress vlan remote-analyzer
user@device# set analyzer employee-monitor output interface ge-0/0/5.0
```

- Especifique parámetros de creación de reflejo, como la velocidad y la longitud máxima del paquete para el analizador.`employee-monitor`

```
[edit]
user@device# set forwarding-options analyzer employee-monitor input rate 2
user@device# set forwarding-options analyzer employee-monitor input maximum-packet-length
128
```

- Vincule el analizador a la FPC que contiene los puertos de entrada.`employee-monitor`

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

Resultados

Compruebe los resultados de la configuración en el dispositivo de conmutación de origen:

```
[edit]
user@device# show
 forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }

            maximum-packet-length 128;
            rate 2;
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members 999;
                }
```

```
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Compruebe los resultados de la configuración en el dispositivo de conmutación de destino.

```
[edit]
user@device# show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0;
        }
    }
}
forwarding-options {
```

```
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/5.0;
            }
        }
    }
}
```

Duplicación del tráfico de empleados para análisis remoto para enrutadores de la serie MX

Configuración rápida de CLI

Para configurar rápidamente un analizador estadístico para el análisis de tráfico remoto del tráfico entrante y saliente de empleados, copie los siguientes comandos para enrutadores serie MX y péguelos en la ventana correcta del terminal del dispositivo de conmutación.

- Copie y pegue los siguientes comandos en la ventana terminal del dispositivo de conmutación de origen :

  Serie MX

```
[edit]
set bridge-domains remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
set interfaces ge-0/0/10 unit 0 family bridge vlan-id 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output bridge-domain remote-analyzer
set forwarding-options analyzer employee-monitor input rate 2
set forwarding-options analyzer employee-monitor input maximum-packet-length 128
set chassis fpc 0 port-mirror-instance employee-monitor
```

- Copie y pegue los siguientes comandos en la ventana Terminal del dispositivo de conmutación de destino :

Serie MX

```
[edit]
set bridge-domains remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
set interfaces ge-0/0/10 unit 0 family bridge vlan-id 999
set interfaces ge-0/0/5 unit 0 family bridge interface-mode access
set forwarding-options analyzer employee-monitor input ingress bridge-domain remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
```

Procedimiento paso a paso

Para configurar la duplicación remota básica con enrutadores de la serie MX:

1. En el dispositivo de conmutación de origen, haga lo siguiente:

   - Configure el ID de VLAN para el dominio de puente.`remote-analyzer`

     ```
     [edit]
     user@device# set bridge-domains remote-analyzer vlan-id 999
     ```

   - Configure la interfaz en el puerto de red conectado al dispositivo de conmutación de destino para el modo de acceso y asócielo al dominio de puente.`remote-analyzer`

     ```
     [edit]
     user@device# set interfaces ge-0/0/10 unit 0 family bridge interface-mode access
     user@device# set interfaces ge-0/0/10 unit 0 family bridge vlan members 999
     ```

   - Configure el analizador estadístico .`employee-monitor`

     ```
     [edit forwarding-options]
     user@device# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@device# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@device# set analyzer employee-monitor input egress interface ge-0/0/0.0
     user@device# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@device# set analyzer employee-monitor output bridge-domain remote-analyzer
     user@device# set analyzer employee-monitor input rate 2
     user@device# set analyzer employee-monitor input maximum-packet-length 128
     ```

- Enlazar el analizador estadístico a la FPC que contiene la interfaz de entrada.

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

2. En el dispositivo de conmutación de destino, haga lo siguiente:

- Configure el ID de VLAN para el dominio de puente.`remote-analyzer`

```
[edit bridge-domains]
user@device# set remote-analyzer vlan-id 999
```

- Configure la interfaz en el dispositivo de conmutación de destino para el modo de acceso y asóciela al dominio del puente.`remote-analyzer`

```
[edit interfaces]
user@device# set ge-0/0/10 unit 0 family bridge interface-mode access
user@device# set ge-0/0/10 unit 0 family bridge vlan members 999
```

- Configure la interfaz conectada al dispositivo de conmutación de destino para el modo de acceso.

```
[edit interfaces]
user@device# set ge-0/0/5 unit 0 family bridge interface-mode access
```

- Configure el analizador.`employee-monitor`

```
[edit forwarding-options]
user@device# set analyzer employee-monitor input ingress bridge-domain remote-analyzer
user@device# set analyzer employee-monitor output interface ge-0/0/5.0
```

- Especifique parámetros de creación de reflejo, como la velocidad y la longitud máxima del paquete para el analizador.`employee-monitor`

```
[edit]
user@device# set forwarding-options analyzer employee-monitor input rate 2
user@device# set forwarding-options analyzer employee-monitor input maximum-packet-length
128
```

- Vincule el analizador a la FPC que contiene los puertos de entrada.`employee-monitor`

```
[edit]
user@device# set chassis fpc 0 port-mirror-instance employee-monitor
```

Resultados

Compruebe los resultados de la configuración en el dispositivo de conmutación de origen:

```
[edit]
user@device# show
bridge-domains {
    remote-analyzer {
        vlan-id 999;
    }
}
forwarding-options {
    analyzer {
        employee-monitor {
            input {
                ingress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                }
                egress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                }
                maximum-packet-length 128;
                rate 2;
            }
            output {
                bridge-domain {
                    remote-analyzer;
                }
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
```

```
        unit 0 {
            family bridge {
                interface-mode access;
                vlan-id 99;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family bridge {
                interface-mode access;
                vlan-id 98;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family bridge {
                interface-mode access;
                vlan-id 999;
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el dispositivo de conmutación de destino.

```
[edit]
user@device# show
bridge-domains {
    remote-analyzer {
        vlan-id 999;
    }
}
forwarding-options {
    analyzer {
        employee-monitor {
            input {
                ingress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                    bridge-domain remote-analyzer;
```

```
                }
            }
            output {
                interface ge-0/0/5.0;
            }
        }
    }
}
interfaces {
    ge-0/0/5 {
        unit 0 {
            family bridge {
                interface-mode access;
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | 1120

Comprobación de que el analizador se ha creado correctamente

Propósito

Compruebe que el analizador denominado se haya creado en el dispositivo con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitor`

Acción

Para comprobar que el analizador está configurado como se esperaba mientras supervisa todo el tráfico de empleados en el dispositivo de conmutación de origen, ejecute el comando en el dispositivo de

conmutación de origen.`show forwarding-options analyzer` Se muestra el siguiente resultado para este ejemplo de configuración.

```
user@device> show forwarding-options analyzer

Analyzer name                    : employee-monitor
  Mirror rate                        : 2
  Maximum packet length            : 128
  State                              : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces      : ge-0/0/0.0
  Egress monitored interfaces      : ge-0/0/1.0
  Output VLAN                      : default-switch/remote-analyzer
```

Significado

Este resultado muestra que la instancia tiene una relación de 2, el tamaño máximo del paquete original que se reflejó es 128, el estado de la configuración es , que indica el estado correcto y que el analizador está programado, y el analizador está reflejando el tráfico que entra en ge-0/0/0.0 y ge-0/0/1.0, y está enviando el tráfico reflejado a la VLAN llamada remote-analyzer.`employee-monitorup`

Si el estado de la interfaz de salida es o si la interfaz de salida no está configurada, el valor de estará inactivo y el analizador no podrá supervisar el tráfico.`downState`

Ejemplo: Configuración de la creación de reflejo en varias interfaces para el monitoreo remoto del uso de recursos de los empleados en conmutadores EX9200

in this section

- Requisitos | **1122**
- Descripción general y topología | **1123**
- Duplicación de todo el tráfico de empleados a múltiples interfaces miembro de VLAN para análisis remoto | **1125**
- Verificación | **1132**

Los conmutadores EX9200 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o salen de una VLAN en

Puede analizar el tráfico reflejado mediante una aplicación de analizador de protocolos que se ejecute en una estación de supervisión remota si envía tráfico reflejado a una VLAN de analizador.

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Desactive los analizadores de creación de reflejo configurados cuando no los esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado de la siguiente manera:
  - Uso de muestreo estadístico.
  - Establecer ratios para seleccionar muestras estadísticas.
  - Uso de filtros de firewall.

En este ejemplo se describe cómo configurar la creación remota de reflejo en varias interfaces en una VLAN de analizador:

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Tres conmutadores EX9200
- Junos OS versión 13.2 o posterior para conmutadores serie EX

Antes de configurar la creación remota de reflejos, asegúrese de que:

- Las interfaces que el analizador utilizará como interfaces de entrada se han configurado en el conmutador.

Descripción general y topología

in this section

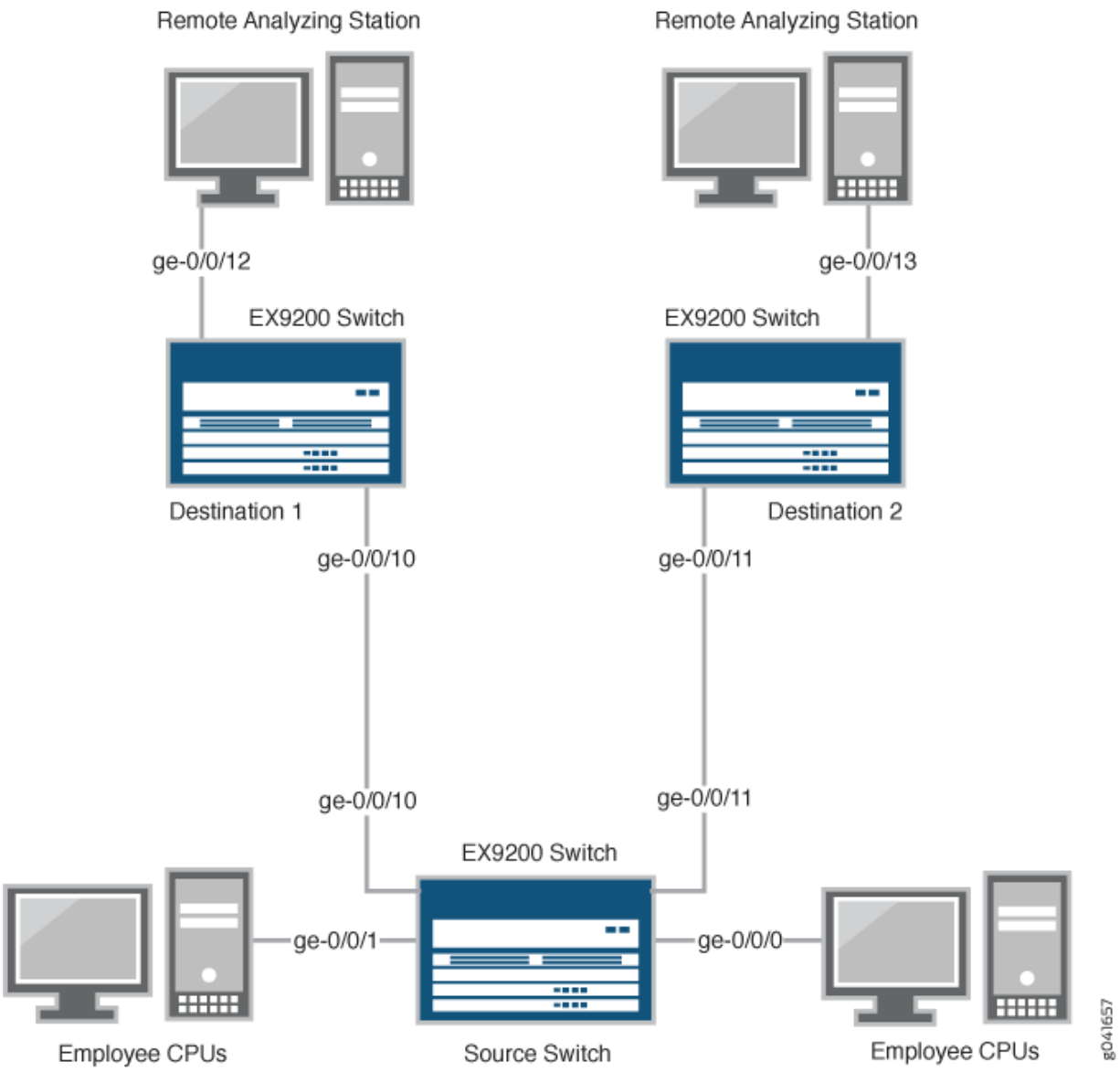
- Topología | **1124**

En este ejemplo se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN del analizador remoto para que pueda realizar el análisis desde una estación de supervisión remota. La VLAN del analizador remoto de este ejemplo contiene varias interfaces miembro. Por lo tanto, el mismo tráfico se refleja en todas las interfaces miembro de la VLAN del analizador remoto para que los paquetes reflejados puedan enviarse a diferentes estaciones de supervisión remota. Puede instalar aplicaciones, como sniffers y sistemas de detección de intrusos, en estaciones de monitoreo remoto para analizar estos paquetes duplicados y obtener datos estadísticos útiles. Por ejemplo, si hay dos estaciones de monitoreo remoto, puede instalar un sniffer en una estación de monitoreo remoto y un sistema de detección de intrusos en la otra estación. Puede utilizar una configuración de analizador de filtros de firewall para reenviar un tipo específico de tráfico a una estación de supervisión remota.

En este ejemplo se describe cómo configurar un analizador para reflejar el tráfico a varias interfaces del grupo del salto siguiente, de modo que el tráfico se envíe a diferentes estaciones de supervisión para su análisis.

Figura 36 en la página 1124 muestra la topología de red de este ejemplo.

Figura 36: Ejemplo de espejado remoto Topología de red con varias interfaces miembro de VLAN en el grupo del salto siguiente



Topología

En este ejemplo:

- Las interfaces ge-0/0/0 y ge-0/0/1 son interfaces de capa 2 (ambas interfaces en el conmutador de origen) que sirven como conexiones para los equipos de los empleados.
- Las interfaces ge-0/0/10 y ge-0/0/11 son interfaces de capa 2 que están conectadas a diferentes conmutadores de destino.

- La interfaz ge-0/0/12 es una interfaz de capa 2 que conecta el conmutador de destino 1 a la estación de monitoreo remoto.
- La interfaz ge-0/0/13 es una interfaz de capa 2 que conecta el conmutador de destino 2 a la estación de monitoreo remoto.
- La VLAN está configurada en todos los conmutadores de la topología para transportar el tráfico reflejado.`remote-analyzer`

Duplicación de todo el tráfico de empleados a múltiples interfaces miembro de VLAN para análisis remoto

in this section

- Procedimiento | **1125**

Para configurar la creación de reflejo en varias interfaces miembro de VLAN para el análisis de tráfico remoto para todo el tráfico de empleados entrantes y salientes, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la creación de reflejo para el análisis de tráfico remoto para el tráfico de empleados entrantes y salientes, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

- En la ventana terminal del conmutador de origen, copie y pegue los siguientes comandos:

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
 set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members 999
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
 set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
 set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
```

```
set forwarding-options analyzer employee-monitor output next-hop-group remote-analyzer-nhg
set forwarding-options next-hop-group remote-analyzer-nhg interface ge-0/0/10.0
set forwarding-options next-hop-group remote-analyzer-nhg interface ge-0/0/11.0
set forwarding-options next-hop-group remote-analyzer-nhg group-type layer-2
```

- En la ventana Terminal del conmutador Destino 1, copie y pegue los siguientes comandos:

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode acess
 set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor loss-priority high output interface
ge-0/0/12.0
```

- En la ventana Terminal del conmutador Destino 2, copie y pegue los siguientes comandos:

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
 set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor loss-priority high output interface
ge-0/0/13.0
```

Procedimiento paso a paso

Para configurar la creación de reflejo remota básica en dos interfaces miembro de VLAN:

1. En el conmutador de origen:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure las interfaces en el puerto de red conectado a los conmutadores de destino para el modo de acceso y asócielo a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/11 unit 0 family ethernet-switching vlan members 999
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output next-hop-group remote-analyzer-nhg
```

  En esta configuración del analizador, el tráfico que entra y sale de las interfaces ge-0/0/0.0 y ge-0/0/1.0 se envía al destino de salida definido por el grupo del próximo salto denominado .`remote-analyzer-nhg`

- Configure el grupo del próximo salto:`remote-analyzer-nhb`

```
[edit forwarding-options]
user@switch# set next-hop-group remote-analyzer-nhg interface ge-0/0/10.0
user@switch# set next-hop-group remote-analyzer-nhg interface ge-0/0/11.0
user@switch# set next-hop-group remote-analyzer-nhg group-type layer-2
```

2. En el conmutador Destino 1:

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz ge-0/0/10 en el conmutador de destino 1 para el modo de acceso:

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
```

- Configure la interfaz conectada a la estación de monitoreo remoto para el modo de acceso:

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode access
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface ge-0/0/12.0
```

3. En el conmutador Destino 2:

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz ge-0/0/11 en el conmutador de destino 2 para el modo de acceso:

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode access
```

- Configure la interfaz conectada a la estación de monitoreo remoto para el modo de acceso:

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode access
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor loss-priority high output interface ge-0/0/13.0
```

Resultados

Compruebe los resultados de la configuración en el conmutador de origen:

```
[edit]
user@switch# show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            next-hop-group {
                remote-analyzer-nhg;
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            ge-0/0/11.0
        }
    }
}
interfaces {
```

```
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador Destino 1:

```
[edit]
user@switch# show
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            ethernet-switching {
                interface-mode acess;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
            interface-mode access;
            }
        }
    }
}
forwarding-options {
```

```
    analyzer employee-monitor {
        input {
            ingress {
            vlan remote-analyzer;
            }
        }
        loss-priority high;
        output {
            interface {
                ge-0/0/12.0;
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador Destino 2:

```
[edit]
user@switch# show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0
        }
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
        family ethernet-switching {
            interface-mode access;
        }
        }
    }
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
```

```
}
forwarding-options {
    employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        loss-priority high;
        output {
            interface {
                ge-0/0/13.0;
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | **1132**

Para confirmar que la configuración funcione correctamente, realice las siguientes tareas:

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador denominado se haya creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitor`

Acción

Puede comprobar que el analizador está configurado como se esperaba mediante el comando.`show forwarding-options analyzer`

Para comprobar que el analizador está configurado como se esperaba mientras supervisa todo el tráfico de empleados en el conmutador de origen, ejecute el comando en el conmutador de origen.`show forwarding-options analyzer` Se muestra el siguiente resultado para esta configuración de ejemplo en el conmutador de origen:

```
user@switch> show forwarding-options analyzer
  Analyzer name                    : employee-monitor
  Mirror rate                          : 1
  Maximum packet length            : 0
  State                                : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces     : ge-0/0/0.0
  Egress monitored interfaces     : ge-0/0/1.0
  Output nhg                       : remote-analyzer-nhg
user@switch> show forwarding-options next-hop-group
Next-hop-group: remote-analyzer-nhg
  Type:  layer-2
  State: up
  Members Interfaces:
    ge-0/0/10.0
    ge-0/0/11.0
```

Significado

Este resultado muestra que el analizador tiene una relación de 1 (duplicación de cada paquete, que es el comportamiento predeterminado), el estado de la configuración es , que indica el estado correcto y que el analizador está programado, refleja el tráfico que entra o sale de las interfaces ge-0/0/0 y ge-0/0/1, y envía el tráfico reflejado a varias interfaces ge-0/0/10.0 y ge-0/0/11.0 a través del grupo del siguiente salto.`employee-monitorupremote-analyzer-nhg` Si el estado de la interfaz de salida es o si la interfaz de salida no está configurada, el valor de estado estará inactivo y el analizador no podrá reflejar el tráfico.`down`

Ejemplo: Configuración de la duplicación para la supervisión remota del uso de recursos de los empleados mediante un conmutador de tránsito en conmutadores EX9200

in this section

Requisitos | 1135

- Descripción general y topología | **1135**
- Duplicación de todo el tráfico de empleados para análisis remoto a través de un conmutador de tránsito | **1137**
- Verificación | **1143**

Los conmutadores EX9200 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para supervisión local o a una VLAN para supervisión remota. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o salen de una VLAN

Puede analizar el tráfico reflejado mediante una aplicación de analizador de protocolos que se ejecute en una estación de supervisión remota si envía tráfico reflejado a una VLAN de analizador.

En este tema se incluye un ejemplo en el que se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN del analizador remoto a través de un conmutador de tránsito, de modo que pueda realizar análisis desde una estación de supervisión remota.

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Deshabilite las sesiones de creación de reflejo configuradas cuando no las esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado de la siguiente manera:
  - Uso de muestreo estadístico.
  - Establecer ratios para seleccionar muestras estadísticas.
  - Uso de filtros de firewall.

En este ejemplo se describe cómo configurar la creación remota de reflejo mediante un conmutador de tránsito:

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador EX9200 conectado a otro conmutador EX9200 a través de un tercer conmutador EX9200
- Junos OS versión 13.2 o posterior para conmutadores serie EX

Antes de configurar la creación remota de reflejos, asegúrese de que:

- Las interfaces que el analizador utilizará como interfaces de entrada se han configurado en el conmutador.

Descripción general y topología

in this section

- Topología | **1136**

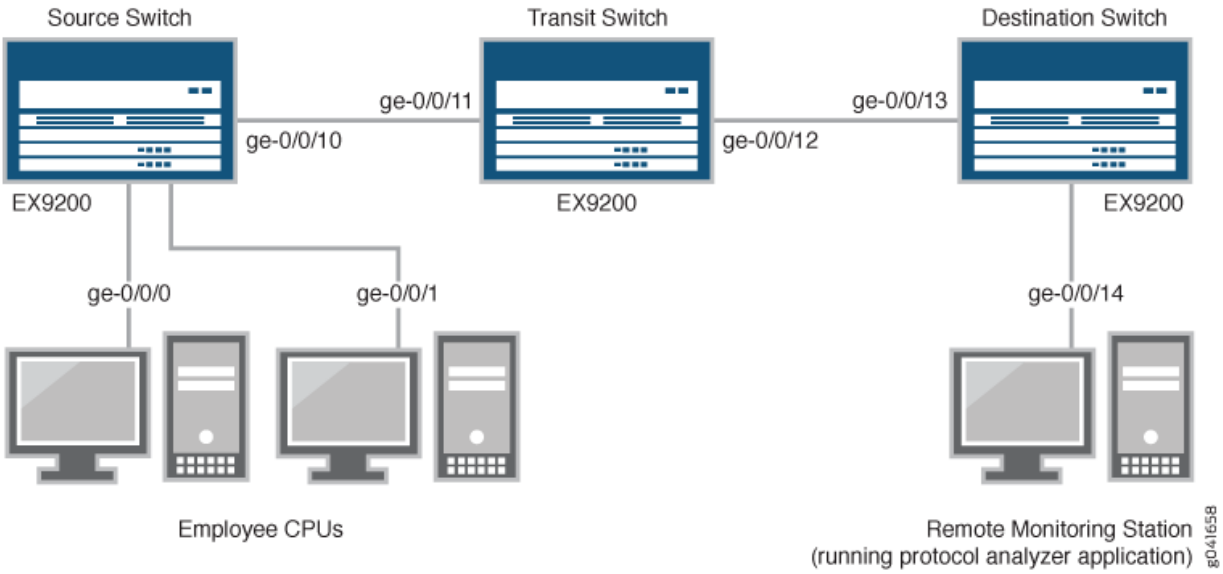
En este ejemplo se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN a través de un conmutador de tránsito para que pueda realizar análisis en todo el tráfico de los equipos de los empleados.`remote-analyzer`

En esta configuración, se requiere una sesión de analizador en el conmutador de destino para reflejar el tráfico entrante desde la VLAN del analizador a la interfaz de salida a la que está conectada la estación de monitoreo remoto.

Figura 37 en la página 1136 muestra la topología de red de este ejemplo.

Topología

Figura 37: Monitoreo de red para duplicación remota a través de un conmutador de tránsito



En este ejemplo:

1. La interfaz ge-0/0/0 es una interfaz de capa 2 y la interfaz ge-0/0/1 es una interfaz de capa 3 (ambas interfaces en el conmutador de origen) que sirven como conexiones para las computadoras de los empleados.
2. La interfaz ge-0/0/10 es una interfaz de capa 2 que se conecta al conmutador de tránsito.
3. La interfaz ge-0/0/11 es una interfaz de capa 2 en el conmutador de tránsito.
4. La interfaz ge-0/0/12 es una interfaz de capa 2 en el conmutador de tránsito y se conecta al conmutador de destino.
5. La interfaz ge-0/0/13 es una interfaz de capa 2 en el conmutador de destino.
6. La interfaz ge-0/0/14 es una interfaz de capa 2 en el conmutador de destino y se conecta a la estación de monitoreo remoto.
7. La VLAN está configurada en todos los conmutadores de la topología para transportar el tráfico reflejado.`remote-analyzer`

Duplicación de todo el tráfico de empleados para análisis remoto a través de un conmutador de tránsito

in this section

- Procedimiento | 1137

Para configurar la creación de reflejo para el análisis de tráfico remoto a través de un conmutador de tránsito, para todo el tráfico de empleados entrante y saliente, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la creación de reflejo para el análisis de tráfico remoto a través de un conmutador de tránsito, para el tráfico de empleados entrante y saliente, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

- Copie y pegue los siguientes comandos en la ventana del terminal del conmutador de origen (conmutador supervisado):

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
```

- Copie y pegue los siguientes comandos en la ventana del conmutador de tránsito:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/11
```

```
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/12
```

- Copie y pegue los siguientes comandos en la ventana del conmutador de destino:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode access
set vlans remote-analyzer interface ge-0/0/13 ingress
set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode access
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/14.0
```

Procedimiento paso a paso

Para configurar la creación remota de reflejo mediante un conmutador de tránsito:

1. En el conmutador de origen:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure las interfaces en el puerto de red conectado al conmutador de tránsito para el modo de acceso y asócielo a la VLAN:`remote-analyzer`

     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```

   - Configure el analizador:`employee-monitor`

     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
     ```

```
user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

2. En el conmutador de tránsito:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

   - Configure la interfaz ge-0/0/11 para el modo de acceso, asóciela a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode access
```

   - Configure la interfaz ge-0/0/12 para el modo de acceso, asóciela a la VLAN y establezca la interfaz solo para el tráfico de salida:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode access
user@switch# set vlans remote-analyzer interface ge-0/0/12
```

3. En el conmutador de destino:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

   - Configure la interfaz ge-0/0/13 para el modo de acceso, asóciela a la VLAN y establezca la interfaz solo para el tráfico de entrada:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode access
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
```

- Configure la interfaz conectada a la estación de monitoreo remoto para el modo de acceso:

```
[edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching interface-mode access
```

- Configure el analizador:`remote-analyzer`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/14.0
```

Resultados

Compruebe los resultados de la configuración en el conmutador de origen:

```
[edit]
user@switch> show
 forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
    }
```

```
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    member 999;
                }
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador de tránsito:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0 {
            }
            ge-0/0/12.0 {
            }
        }
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
```

```
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador de destino:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/13.0 {
                ingress;
            }
        }
    }
}
interfaces {
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
            }
        }
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
```

```
            interface {
                ge-0/0/14.0;
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | 1143

Para confirmar que la configuración funcione correctamente, realice las siguientes tareas:

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador denominado se haya creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitor`

Acción

Puede comprobar que el analizador está configurado como se esperaba mediante el comando.`show forwarding-options analyzer`

Para comprobar que el analizador está configurado como se esperaba mientras supervisa todo el tráfico de empleados en el conmutador de origen, ejecute el comando en el conmutador de origen.`show forwarding-options analyzer` Se muestra el siguiente resultado para esta configuración de ejemplo:

```
user@switch> show forwarding-options analyzer
Analyzer name                     : employee-monitor
  Mirror rate                       : 1
  Maximum packet length             : 0
  State                             : up
  Ingress monitored interfaces      : ge-0/0/0.0
  Ingress monitored interfaces      : ge-0/0/1.0
```

```
Egress monitored interfaces      : ge-0/0/0.0
Egress monitored interfaces      : ge-0/0/1.0
Output vlan                      : default-switch/remote-analyzer
```

Significado

Este resultado muestra que el analizador tiene una relación de duplicación de 1 (reflejo de cada paquete, el valor predeterminado), el estado de la configuración es , que indica el estado correcto y que el analizador está programado, está reflejando el tráfico que entra en ge-0/0/0 y ge-0/0/1, y está enviando el tráfico reflejado al analizador llamado `.employee-monitorupremote-analyzer` Si el estado de la interfaz de salida es o si la interfaz de salida no está configurada, el valor de estado estará inactivo y el analizador no podrá reflejar el tráfico.`down`

Ejemplo: Configuración de la duplicación para el monitoreo local del uso de recursos de los empleados en conmutadores EX4300

in this section

- Requisitos | **1145**
- Descripción general y topología | **1145**
- Duplicación de todo el tráfico de empleados para análisis local | **1146**
- Duplicación del tráfico de empleados a la web para análisis local | **1148**
- Verificación | **1152**

NOTA: En este ejemplo se utiliza Junos OS para conmutadores serie EX compatibles con el estilo de configuración Enhanced Layer 2 Software (ELS). Si el conmutador ejecuta software que no admite ELS, consulte el ejemplo: Configuración de la duplicación de puertos para la supervisión local del uso de recursos de los empleados en los conmutadores de la serie EX. Para obtener detalles de ELS, consulte Introducción al software de capa 2 mejorado.

Los conmutadores EX4300 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que ingresan a una VLAN

Puede analizar el tráfico reflejado mediante un analizador de protocolos instalado en un sistema conectado a la interfaz de destino local o una estación de supervisión remota si envía tráfico reflejado a una VLAN de analizador.

En este ejemplo se describe cómo configurar la creación de reflejo local en un conmutador EX4300. En este ejemplo se describe cómo configurar el conmutador para reflejar el tráfico que entra en las interfaces conectadas a los equipos de los empleados a una interfaz de salida del analizador en el mismo conmutador.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador EX4300
- Junos OS versión 13.2X50-D10 o posterior para conmutadores serie EX

Descripción general y topología

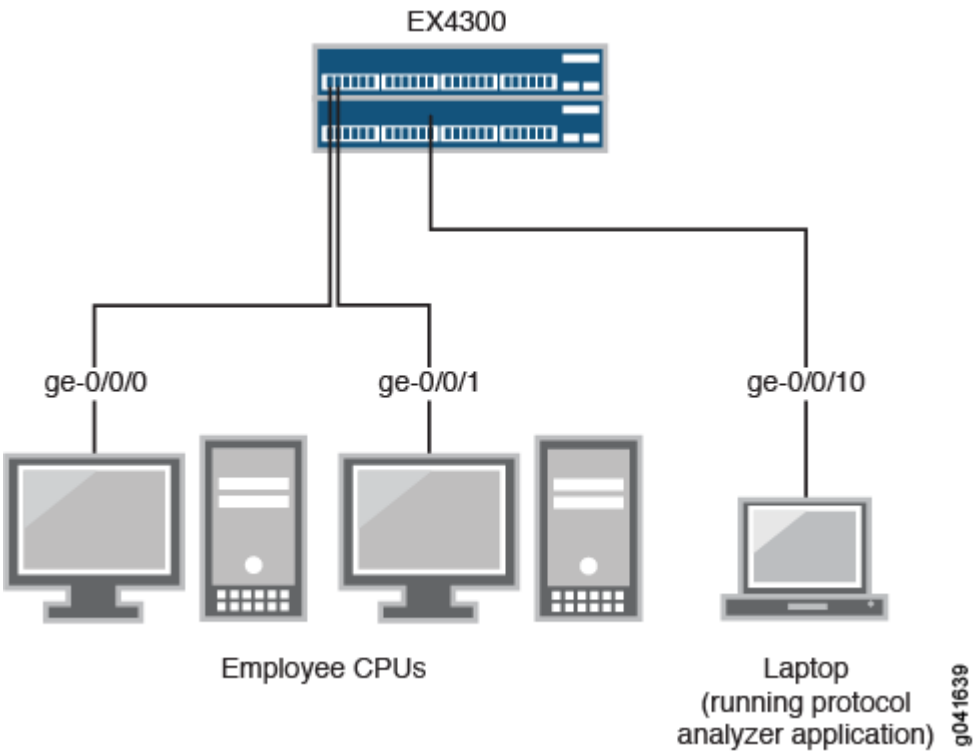
En este tema se incluyen dos ejemplos en los que se describe cómo reflejar el tráfico que entra en los puertos del conmutador a una interfaz de destino en el mismo conmutador (creación de reflejo local). El primer ejemplo muestra cómo reflejar todo el tráfico que entra en los puertos conectados a las computadoras de los empleados. El segundo ejemplo muestra el mismo escenario, pero incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

Las interfaces ge-0/0/0 y ge-0/0/1 sirven como conexiones para los equipos de los empleados. La interfaz ge0/0/10 está reservada para el análisis del tráfico reflejado. Conecte un equipo que ejecute una aplicación de analizador de protocolos a la interfaz de salida del analizador para analizar el tráfico reflejado.

> **NOTA**: Varios puertos reflejados en una interfaz pueden provocar el desbordamiento del búfer y la pérdida de paquetes.

En ambos ejemplos se utiliza la topología de red que se muestra en .Figura 38 en la página 1146

Figura 38: Ejemplo de topología de red para creación de reflejo local



Duplicación de todo el tráfico de empleados para análisis local

in this section

- Procedimiento | 1147

Para configurar la creación de reflejo para todo el tráfico de empleados para el análisis local, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la creación de reflejo local para el tráfico de entrada a los dos puertos conectados a los equipos de los empleados, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

```
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1/24
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members analyzer_vlan
set vlans analyzer-vlan vlan-id 1000
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output interface ge-0/0/10.0
```

Procedimiento paso a paso

Para configurar un analizador llamado y especificar las interfaces de entrada (origen) y la interfaz de salida del analizador:`employee-monitor`

1. Configure cada interfaz conectada a los equipos de los empleados como una interfaz de entrada para el analizador :`employee-monitor`

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
   ```

2. Configure la interfaz de salida del analizador como parte de una VLAN:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members analyzer_vlan
   ```

   ```
   [edit vlans]
   user@switch# set analyzer-vlan vlan-id 1000
   ```

3. Configure la interfaz del analizador de salida para el analizador `.employee-monitor` Esta será la interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
            interface ge-0/0/1.0;}
        }
        output {
            interface {
                ge-0/0/10.0;
            }
        }
    }
}
```

Duplicación del tráfico de empleados a la web para análisis local

in this section

- Procedimiento | **1149**

Para configurar la creación de reflejo para el tráfico de empleados a web, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la creación de reflejo local del tráfico de los dos puertos conectados a los equipos de los empleados, filtrando de modo que sólo se refleje el tráfico a la Web externa, copie los siguientes comandos y péguelos en la ventana de terminal del conmutador:

```
[edit]
set forwarding-options port-mirroring instance employee-web-monitor output interface ge-0/0/10.0
 set firewall family ethernet-switching filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/24
 set firewall family ethernet-switching filter watch-employee term employee-to-corp from source-
address 192.0.2.16/24
 set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then port-
mirroring-instance employee-web-monitor
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
 set interfaces ge-0/0/1  unit 0 family ethernet-switching filter input watch-employee
```

Procedimiento paso a paso

Para configurar la creación de reflejo local del tráfico de empleados a Web desde los dos puertos conectados a los equipos de los empleados:

1. Configure la interfaz del analizador local:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/10 unit 0 family ethernet-switching
   ```

2. Configure la instancia de salida (la entrada a la instancia proviene de la acción del filtro):`employee-web-monitor`

   ```
   [edit forwarding-options port-mirroring]
   user@switch# set instance employee-web-monitor output interface ge-0/0/10.0
   ```

3. Configure un filtro de firewall llamado para enviar copias reflejadas de las solicitudes de los empleados a la Web a la instancia.`watch-employeeemployee-web-monitor` Acepte todo el tráfico hacia y desde la subred corporativa (dirección de destino o origen de 192.0.2.16/24). Envíe copias duplicadas de todos los paquetes destinados a Internet (puerto de destino 80) a la instancia.`employee-web-monitor`

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp from source-address 192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp then accept
ser@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirroring-instance
employee-web-monitor
```

4. Aplique el filtro a los puertos adecuados:`watch-employee`

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show
 forwarding-options {
    port-mirroring {
        instance     {
            employee-web-monitor {
                family ethernet-switching {
                    output {
                        interface ge-0/0/10.0;
                        }
                    }
                }
            }
    }
```

```
}
...
firewall family ethernet-switching {
    filter watch-employee {
        term employee-to-corp {
            from {
                destination-address 192.0.2.16/24;
                source-address 192.0.2.16/24;
            }
            then accept {
        }
        term employee-to-web {
            from {
                destination-port 80;
            }
            then port-mirroring-instance employee-web-monitor;
        }
    }
}
...
interfaces {
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan members [employee-vlan, voice-vlan];
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        family ethernet-switching {
            filter {
                input watch-employee;
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | 1152
- Comprobación de que la instancia de creación de reflejo de puertos está configurada correctamente | 1153

Para confirmar que la configuración es correcta, realice estas tareas:

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador o se haya creado en el conmutador con las interfaces de entrada adecuadas y la interfaz de salida adecuada.`employee-monitoremployee-web-monitor`

Acción

Puede utilizar el comando para comprobar que el analizador está configurado correctamente.`show forwarding-options analyzer`

```
user@switch> show forwarding-options analyzer
  Analyzer name                        : employee-monitor
  Mirror rate                         : 1
  Maximum packet length             : 0
  State                                : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Output interface                     : ge-0/0/10.0
```

Significado

Este resultado muestra que el analizador tiene una relación de 1 (duplicación de cada paquete, la configuración predeterminada), el tamaño máximo del paquete original que se reflejó (indica todo el

paquete), el estado de la configuración (está activo indica que el analizador está reflejando el tráfico que entra en las interfaces ge-0/0/0 y ge-0/0/1, y envía el tráfico reflejado a la interfaz ge-0/0/10).`employee-monitor0` Si el estado de la interfaz de salida está inactivo o si la interfaz de salida no está configurada, el valor de estado será y el analizador no se programará para la duplicación.`down`

Comprobación de que la instancia de creación de reflejo de puertos está configurada correctamente

Propósito

Verifique que la instancia de duplicación de puertos se haya configurado correctamente en el conmutador con las interfaces de entrada adecuadas.`employee-web-monitor`

Acción

Puede comprobar que la instancia de creación de reflejo de puerto está configurada correctamente mediante el comando.`show forwarding-options port-mirroring`

```
user@switch> show forwarding-options port-mirroring
Instance Name: employee-web-monitor
  Instance Id: 3
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    ethernet-switching  up        ge-0/0/10.0
```

Significado

Este resultado muestra que la instancia tiene una proporción de 1 (duplicación de cada paquete, el valor predeterminado), el tamaño máximo del paquete original que se reflejó (indica un paquete completo), el estado de la configuración está activo y la duplicación de puertos está programada, y que el tráfico reflejado desde la acción de filtro de firewall se envía en la interfaz ge-0/0/10.0. Si el estado de la interfaz de salida está inactivo o si la interfaz no está configurada, el valor de estado estará inactivo y la duplicación de puertos no se programará para la duplicación.`employee-web-monitor0`

Ejemplo: Configuración de la duplicación para la supervisión remota del uso de recursos de los empleados en conmutadores EX4300

in this section

- Requisitos | 1155
- Descripción general y topología | 1155
- Duplicación de todo el tráfico de empleados para análisis remoto | 1156
- Duplicación del tráfico de empleados a la web para análisis remoto | 1161
- Verificación | 1167

NOTA: En este ejemplo se utiliza Junos OS para conmutadores serie EX compatibles con el estilo de configuración Enhanced Layer 2 Software (ELS). Si el conmutador ejecuta software que no admite ELS, consulte "el ejemplo: Configuración de la creación de reflejo para el monitoreo remoto del uso de recursos de los empleados en conmutadores EX4300." en la página 1154 Para obtener más información sobre ELS, consulte: Introducción al software de capa 2 mejorado.

Los conmutadores EX4300 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que ingresan a una VLAN en conmutadores EX4300

Puede analizar el tráfico reflejado mediante una aplicación de analizador de protocolos que se ejecute en una estación de supervisión remota si envía tráfico reflejado a una VLAN de analizador.

En este tema se incluyen dos ejemplos relacionados en los que se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN para que pueda realizar análisis desde una estación de supervisión remota.`remote-analyzer` El primer ejemplo muestra cómo reflejar todo el tráfico que entra en los puertos conectados a las computadoras de los empleados. El segundo ejemplo muestra el mismo escenario, pero incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Deshabilite las sesiones de creación de reflejo configuradas cuando no las esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado mediante filtros de firewall.

En este ejemplo se describe cómo configurar la creación de reflejo remota:

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 13.2X50-D10 o posterior para conmutadores serie EX
- Un conmutador EX4300 conectado a otro conmutador EX4300

El diagrama muestra un chasis virtual EX4300 conectado a un conmutador de destino EX4300.

Antes de configurar la creación remota de reflejos, asegúrese de que:

- Tienes una comprensión de los conceptos de reflejo.
- Las interfaces que el analizador utilizará como interfaces de entrada se han configurado en el conmutador.

Descripción general y topología

in this section

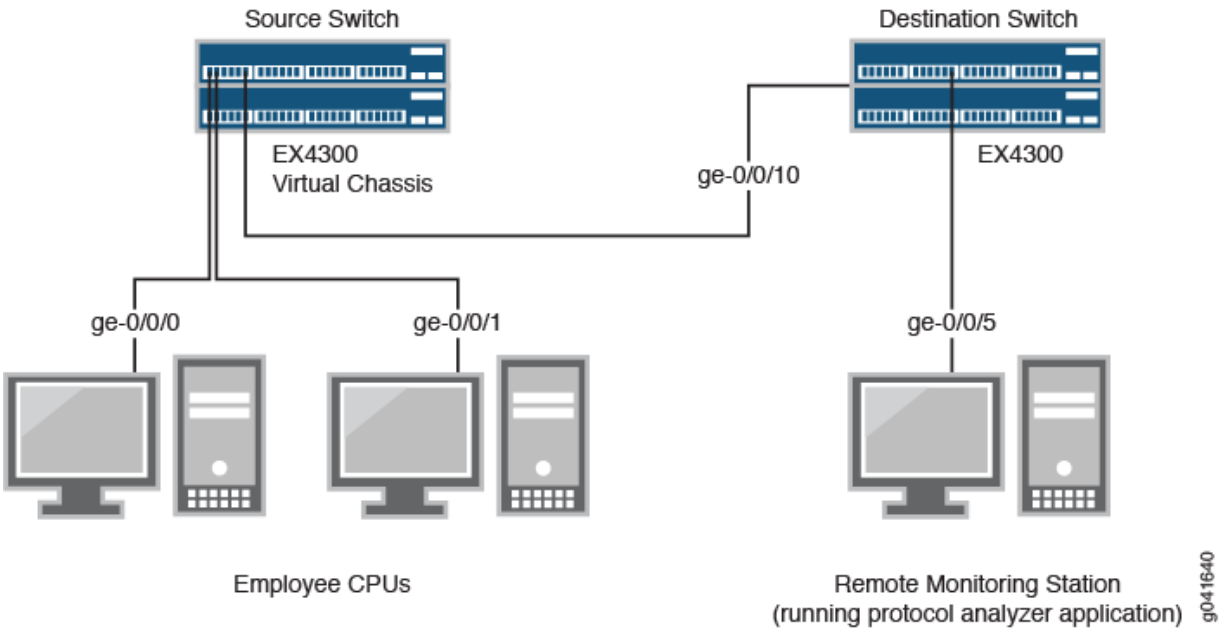
- Topología | **1156**

En este tema se incluyen dos ejemplos relacionados en los que se describe cómo configurar la creación de reflejo en la VLAN para que el análisis se pueda realizar desde una estación de supervisión remota.`remote-analyzer` En el primer ejemplo se muestra cómo configurar un conmutador para reflejar todo el tráfico de los equipos de los empleados. El segundo ejemplo muestra el mismo escenario, pero la configuración incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

Figura 39 en la página 1156 muestra la topología de red para estos dos escenarios de ejemplo.

Topología

Figura 39: Ejemplo de topología de red de espejado remoto



En este ejemplo:

1. La interfaz ge-0/0/0 es una interfaz de capa 2 y la interfaz ge-0/0/1 es una interfaz de capa 3 (ambas interfaces en el conmutador de origen) que sirven como conexiones para las computadoras de los empleados.
2. La interfaz ge-0/0/10 es una interfaz de capa 2 que conecta el conmutador de origen al conmutador de destino.
3. La interfaz ge-0/0/5 es una interfaz de capa 2 que conecta el conmutador de destino a la estación de monitoreo remoto.
4. La VLAN está configurada en todos los conmutadores de la topología para transportar el tráfico reflejado.`remote-analyzer`

Duplicación de todo el tráfico de empleados para análisis remoto

in this section

- Procedimiento | **1157**

Para configurar un analizador para el análisis de tráfico remoto para todo el tráfico de empleados entrantes y salientes, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente un analizador para el análisis de tráfico remoto para el tráfico entrante y saliente de empleados, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

- Copie y pegue los siguientes comandos en la ventana terminal del conmutador de origen:

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
 set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
 set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
```

- Copie y pegue los siguientes comandos en la ventana terminal del conmutador de destino:

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/5.0
```

Procedimiento paso a paso

Para configurar la creación básica de reflejo de puerto remoto:

1. En el conmutador de origen:

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz en el puerto de red conectado al conmutador de destino para el modo troncal y asócielo a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@switch# set instance employee-monitor input egress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

2. En el conmutador de destino:

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz en el conmutador de destino para el modo troncal y asóciela a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure la interfaz conectada al conmutador de destino para el modo troncal:

```
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/5.0
```

Resultados

Compruebe los resultados de la configuración en el conmutador de origen:

```
[edit]
user@switch> show
 forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
```

```
                interface-mode trunk;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador de destino:

```
[edit]
user@switch> show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 999;
                }
            }
        }
    }
}
vlans {
```

```
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
            }
        }
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/5.0;
            }
        }
    }
}
```

Duplicación del tráfico de empleados a la web para análisis remoto

in this section

- Procedimiento | **1161**

Para configurar la creación de reflejo de puertos para el análisis del tráfico remoto del tráfico de empleados a web, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la duplicación de puertos para reflejar el tráfico de empleados a la Web externa, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

- Copie y pegue los siguientes comandos en la ventana terminal del conmutador de origen:

```
[edit]
user@switch# set forwarding-options port-mirroring instance employee-web-monitor output vlan
999
user@switch# set vlans remote-analyzer vlan-id 999
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-
corp from destination-address 192.0.2.16/24
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-
corp from source-address 192.0.2.16/24
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-
corp then accept
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-
web from destination-port 80
user@switch# set firewall family ethernet-switching filter watch-employee term employee-to-
web then port-mirror-instance employee-web-monitor
user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-
employee
user@switch# set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-
employee
```

- Copie y pegue los siguientes comandos en la ventana terminal del conmutador de destino:

```
[edit]
user@switch# set vlans remote-analyzer vlan-id 999
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
user@switch# set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
user@switch# set forwarding-options analyzer employee-web-monitor input ingress vlan remote-
analyzer
user@switch# set forwarding-options analyzer employee-web-monitor output interface ge-0/0/5.0
```

Procedimiento paso a paso

Para configurar la duplicación de puertos de todo el tráfico de los dos puertos conectados a las computadoras de los empleados a la VLAN para su uso desde una estación de monitoreo remota:`remote-analyzer`

1. En el conmutador de origen:

- Configure la instancia de creación de reflejo de puerto:`employee-web-monitor`

```
[edit ]
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
user@switch# set forwarding-options port-mirroring instance employee-web-monitor output
vlan 999
```

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz para asociarla con la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure el filtro de firewall llamado :`watch-employee`

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/24
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

- Aplique el filtro de firewall a las interfaces de empleados:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

2. En el conmutador de destino:

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz en el conmutador de destino para el modo troncal y asóciela a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure la interfaz conectada al conmutador de destino para el modo troncal:

```
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options port-mirroring]
user@switch# set instance employee-web-monitor input ingress vlan remote-analyzer
user@switch# set instance employee-web-monitor output interface ge-0/0/5.0
```

Resultados

Compruebe los resultados de la configuración en el conmutador de origen:

```
[edit]
user@switch> show
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members remote-analyzer;
                }
```

```
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
}
firewall {
     family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
                from {
                    source-address {
                        192.0.2.16/24;
                    }
                    destination-address {
                        192.0.2.16/24;
                    }
                }
                then accept;
            }
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
            }
        }
```

```
    }
}
 forwarding-options {
    analyzer employee-web-monitor {
        output {
            vlan {
                999;
            }
        }
    }
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Compruebe los resultados de la configuración en el conmutador de destino:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
```

```
    }
}
 forwarding-options {
    port-mirroring {
        instance employee-web-monitor {
            input {
                ingress {
                    vlan remote-analyzer;
                }
            }
            output {
                interface {
                    ge-0/0/5.0;
                }
            }
        }
    }
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | **1167**

Para confirmar que la configuración funcione correctamente, realice las siguientes tareas:

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador denominado o creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitoremployee-web-monitor`

Acción

Puede comprobar que el analizador está configurado como se esperaba mediante el comando.`show forwarding-options analyzer` Para ver los analizadores creados anteriormente que están deshabilitados, vaya a la interfaz de J-Web.

Para comprobar que el analizador está configurado como se esperaba mientras supervisa todo el tráfico de empleados en el conmutador de origen, ejecute el comando en el conmutador de origen.`show analyzer` Se muestra el siguiente resultado para este ejemplo de configuración:

```
user@switch> show forwarding-options analyzer
  Analyzer name                    : employee-monitor
  Mirror rate                            : 1
  Maximum packet length        : 0
  State                                  : up
  Ingress monitored interfaces     : ge-0/0/0.0
  Ingress monitored interfaces     : ge-0/0/1.0
  Egress monitored interfaces     : ge-0/0/0.0
  Egress monitored interfaces     : ge-0/0/1.0
  Output VLAN                        : default-switch/remote-analyzer
```

Significado

Este resultado muestra que la instancia tiene una relación de 1 (duplicación de cada paquete, el valor predeterminado), el tamaño máximo del paquete original que se reflejó (0 indica todo el paquete), el estado de la configuración está activo (lo que indica el estado correcto y que el analizador está programado, y está reflejando el tráfico que entra en ge-0/0/0 y ge-0/0/1 y está enviando el tráfico reflejado a la VLAN llamada).`employee-monitorremote-analyzer` Si el estado de la interfaz de salida está inactivo o si la interfaz de salida no está configurada, el valor de estado estará inactivo y el analizador no se programará para la duplicación.

Ejemplo: Configuración de la duplicación para el monitoreo remoto del uso de recursos de los empleados a través de un conmutador de tránsito en conmutadores EX4300

in this section

- Requisitos | **1169**
- Descripción general y topología | **1170**
- Duplicación de todo el tráfico de empleados para análisis remoto a través de un conmutador de tránsito | **1172**
- Verificación | **1178**

NOTA: En este ejemplo se utiliza Junos OS para conmutadores serie EX compatibles con el estilo de configuración Enhanced Layer 2 Software (ELS).

Los conmutadores EX4300 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que ingresan a una VLAN en conmutadores EX4300

Puede analizar el tráfico reflejado mediante una aplicación de analizador de protocolos que se ejecute en una estación de supervisión remota si envía tráfico reflejado a una VLAN de analizador.

En este tema se incluye un ejemplo en el que se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN a través de un conmutador de tránsito, de modo que pueda realizar análisis desde una estación de supervisión remota.`remote-analyzer`

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Deshabilite las sesiones de creación de reflejo configuradas cuando no las esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado mediante filtros de firewall.

En este ejemplo se describe cómo configurar la creación remota de reflejo mediante un conmutador de tránsito:

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador EX4300 conectado a otro conmutador EX4300 a través de un tercer conmutador EX4300
- Junos OS versión 13.2X50-D10 o posterior para conmutadores serie EX

Antes de configurar la creación remota de reflejos, asegúrese de que:

- Tienes una comprensión de los conceptos de reflejo.

- Las interfaces que el analizador utilizará como interfaces de entrada se han configurado en el conmutador.

Descripción general y topología

in this section

- Topología | **1171**

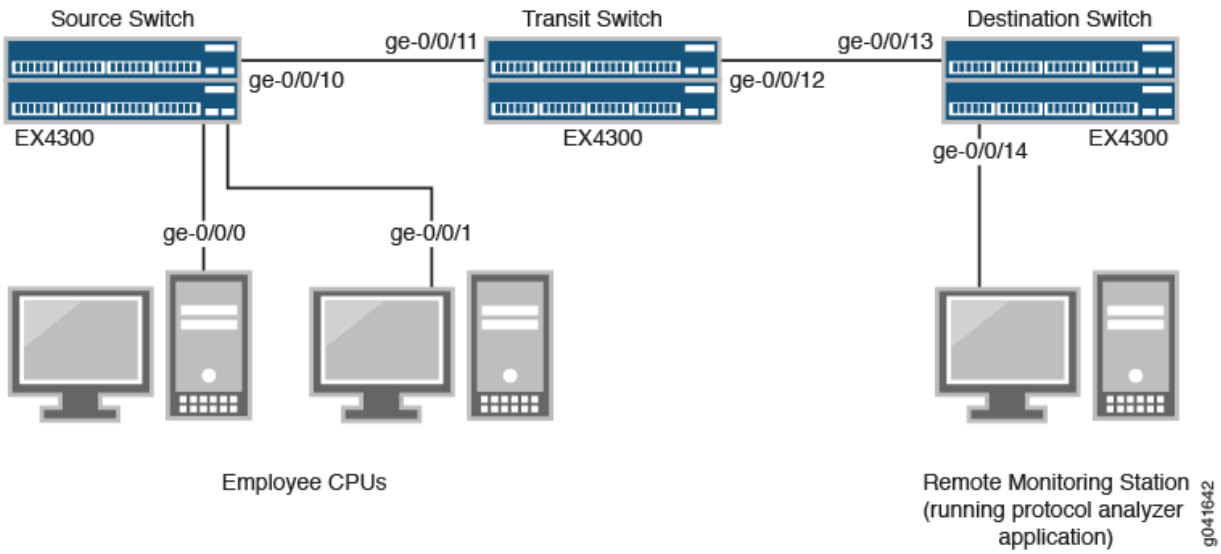
En este ejemplo se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN a través de un conmutador de tránsito para que pueda realizar análisis desde una estación de supervisión remota.`remote-analyzer` En el ejemplo se muestra cómo configurar un conmutador para reflejar todo el tráfico desde los equipos de los empleados a un analizador remoto.

En esta configuración, se requiere una sesión de analizador en el conmutador de destino para reflejar el tráfico entrante desde la VLAN del analizador a la interfaz de salida a la que está conectada la estación de monitoreo remoto. Debe deshabilitar el aprendizaje de MAC en el conmutador de tránsito para la VLAN, de modo que el aprendizaje de MAC esté deshabilitado para todas las interfaces miembro de la VLAN en el conmutador de tránsito.`remote-analyzerremote-analyzer`

Figura 40 en la página 1171 muestra la topología de red de este ejemplo.

Topología

Figura 40: Espejado remoto mediante una red de conmutador de tránsito: topología de ejemplo



En este ejemplo:

- La interfaz ge-0/0/0 es una interfaz de capa 2 y la interfaz ge-0/0/1 es una interfaz de capa 3 (ambas interfaces en el conmutador de origen) que sirven como conexiones para las computadoras de los empleados.
- La interfaz ge-0/0/10 es una interfaz de capa 2 que se conecta al conmutador de tránsito.
- La interfaz ge-0/0/11 es una interfaz de capa 2 en el conmutador de tránsito.
- La interfaz ge-0/0/12 es una interfaz de capa 2 en el conmutador de tránsito y se conecta al conmutador de destino.
- La interfaz ge-0/0/13 es una interfaz de capa 2 en el conmutador de destino.
- La interfaz ge-0/0/14 es una interfaz de capa 2 en el conmutador de destino y se conecta a la estación de monitoreo remoto.
- La VLAN está configurada en todos los conmutadores de la topología para transportar el tráfico reflejado.`remote-analyzer`

Duplicación de todo el tráfico de empleados para análisis remoto a través de un conmutador de tránsito

in this section

- Procedimiento | **1172**

Para configurar la creación de reflejo para el análisis de tráfico remoto a través de un conmutador de tránsito, para todo el tráfico de empleados entrante y saliente, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la creación de reflejo para el análisis de tráfico remoto a través de un conmutador de tránsito, para el tráfico de empleados entrante y saliente, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

- Copie y pegue los siguientes comandos en la ventana del terminal del conmutador de origen (conmutador supervisado):

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0.0
set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
set forwarding-options analyzer employee-monitor output vlan remote-analyzer
```

- Copie y pegue los siguientes comandos en la ventana del conmutador de tránsito:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
set vlans remote-analyzer interface ge-0/0/11
set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode trunk
```

```
set vlans remote-analyzer interface ge-0/0/12
set vlans remote-analyzer no-mac-learning
```

- Copie y pegue los siguientes comandos en la ventana del conmutador de destino:

```
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
set vlans remote-analyzer interface ge-0/0/13 ingress
set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
set forwarding-options analyzer employee-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-monitor output interface ge-0/0/14.0
```

Procedimiento paso a paso

Para configurar la creación remota de reflejo mediante un conmutador de tránsito:

1. En el conmutador de origen:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure las interfaces en el puerto de red conectado al conmutador de tránsito para el modo troncal y asócielo a la VLAN:`remote-analyzer`

     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```

   - Configure el analizador:`employee-monitor`

     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
     ```

```
user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

2. En el conmutador de tránsito:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

   - Configure la interfaz ge-0/0/11 para el modo troncal, asóciela a la VLAN:`remote-analyzer`

     ```
     [edit interfaces]
     user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
     ```

   - Configure la interfaz para el modo de troncalización, asóciela a la VLAN y establezca la interfaz solo para el tráfico de salida:`ge-0/0/12remote-analyzer`

     ```
     [edit interfaces]
     user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set vlans remote-analyzer interface ge-0/0/12
     ```

   - Configure la opción de la VLAN para deshabilitar el aprendizaje de MAC en todas las interfaces que son miembros de la VLAN:`no-mac-learningremote-analyzerremote-analyzer`

     ```
     [edit interfaces]
     user@switch# set vlans remote-analyzer no-mac-learning
     ```

3. En el conmutador de destino:

   - Configure el ID de VLAN para la VLAN:`remote-analyzer`

     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```

- Configure la interfaz ge-0/0/13 para el modo troncal, asóciela a la VLAN y establezca la interfaz solo para el tráfico de entrada:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
```

- Configure la interfaz conectada a la estación de monitoreo remoto para el modo troncal:

```
[edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
```

- Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/14.0
```

Resultados

Compruebe los resultados de la configuración en el conmutador de origen:

```
[edit]
user@switch> show
 forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
            egress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            vlan {
```

```
                remote-analyzer;
            }
        }
    }
}
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    member 999;
                }
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador de tránsito:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/11.0 {
            }
            ge-0/0/12.0 {
            }
        }
        no-mac-learning;
    }
}
interfaces {
    ge-0/0/11 {
        unit 0 {
```

```
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/12 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
}
```

Compruebe los resultados de la configuración en el conmutador de destino:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/13.0 {
                ingress;
            }
        }
    }
}
interfaces {
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
```

```
    }
}
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                vlan remote-analyzer;
            }
        }
        output {
            interface {
                ge-0/0/14.0;
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | **1178**

Para confirmar que la configuración funcione correctamente, realice las siguientes tareas:

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador denominado se haya creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitor`

Acción

Puede comprobar si el analizador está configurado como se esperaba mediante el comando.`show analyzer` Para ver los analizadores creados anteriormente que están deshabilitados, vaya a la interfaz de J-Web.

Para comprobar que el analizador está configurado como se esperaba mientras supervisa todo el tráfico de empleados en el conmutador de origen, ejecute el comando en el conmutador de origen.`show analyzer` Se muestra el siguiente resultado para esta configuración de ejemplo:

```
user@switch> show forwarding-options analyzer
Analyzer name                     : employee-monitor
  Mirror rate                       : 1
  Maximum packet length             : 0
  State                             : up
  Ingress monitored interfaces      : ge-0/0/0.0
  Ingress monitored interfaces      : ge-0/0/1.0
  Egress monitored interfaces       : ge-0/0/0.0
  Egress monitored interfaces       : ge-0/0/1.0
  Output vlan                       : default-switch/remote-analyzer
```

Significado

Este resultado muestra que el analizador tiene una relación de 1 (duplicación de cada paquete, el valor predeterminado), está reflejando el tráfico que entra en ge-0/0/0 y ge-0/0/1, y enviando el tráfico reflejado al analizador .`employee-monitorremote-analyzer`

Configuración de instancias de creación de reflejo de puertos

in this section

- Instancia global de creación de reflejo de puertos de capa 2 | **1180**
- Configuración de la instancia global de creación de reflejo de puertos de capa 2 | **1180**
- Instancias con nombre de creación de reflejo de puertos de capa 2 | **1183**
- Definición de una instancia con nombre de creación de reflejo de puertos de capa 2 | **1185**
- Deshabilitar instancias de creación de reflejo de puertos de capa 2 | **1189**
- Configuración de la duplicación de puerto en línea | **1190**

Instancia global de creación de reflejo de puertos de capa 2

En un enrutador serie MX y en un conmutador serie EX, puede configurar un conjunto de propiedades de duplicación de puertos que se aplican implícitamente a los paquetes recibidos en todos los puertos del chasis del enrutador (o conmutador). Este conjunto de propiedades de duplicación de puertos es la *instancia global* de *creación de reflejo de puerto* de capa 2 para el enrutador o conmutador.

Dentro de la configuración de instancia global, puede especificar un conjunto de propiedades de destino reflejado para cada familia de direcciones de paquete admitidas por la creación de reflejo de puertos de capa 2.

Para obtener una descripción general de las propiedades de duplicación de puertos de capa 2, consulte Descripción de las propiedades de creación de reflejo de puertos de capa 2."Propiedades de duplicación de puertos de capa 2" en la página 1061 Para obtener una comparación de los tipos de duplicación de puertos de capa 2 disponibles en un enrutador de la serie MX y en un conmutador de la serie EX, consulte Aplicación de tipos de duplicación de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-services-port-mirroring-application.html

Configuración de la instancia global de creación de reflejo de puertos de capa 2

En un enrutador serie MX y en un conmutador serie EX, puede configurar un conjunto de propiedades de duplicación de puertos de capa 2 que se aplican implícitamente a los paquetes recibidos en todos los puertos del chasis del enrutador (o conmutador).

Para configurar la instancia global de duplicación de puertos de capa 2 en un enrutador de la serie MX y en un conmutador de la serie EX:

1. Habilite la configuración de la duplicación de puertos de capa 2:

```
[edit]
user@host# edit forwarding-options port-mirroring
```

2. Habilite la configuración de las propiedades de selección de paquetes:

```
[edit forwarding-options port-mirroring]
user@host# edit input
```

3. Especifique las propiedades de selección de paquetes a nivel global.

   a) Especifique el número de paquetes que desea seleccionar:

```
[edit forwarding-options port-mirroring input]
user@host# set rate number
```

El intervalo válido es del 1 al 65535.

b) Especifique el número de paquetes que desea reflejar de cada selección:

```
[edit forwarding-options port-mirroring input]
user@host# set run-length number
```

El intervalo válido es de 0 a 20. El valor predeterminado es 0.

c) Especifique la longitud a la que se van a truncar los paquetes reflejados:

```
[edit forwarding-options port-mirroring input]
user@host# set maximum-packet-length number
```

El intervalo válido es de 0 a 9216. El valor predeterminado es 0, lo que significa que los paquetes reflejados no se truncan.

4. Especifique la familia de tipos de direcciones de capa 2 a nivel global en la que se va a seleccionar el tráfico para la creación de reflejo:

```
[edit forwarding-options port-mirroring input]
user@host# up
[edit forwarding-options port-mirroring]
user@host# edit family family
```

El valor de la opción puede ser , o .*family*`ethernet-switching`cccvpls

> **NOTA**: En el nivel de jerarquía, la instrucción de familia protocol es un alias para .`[edit forwarding-options port-mirroring]family ethernet-switching`family `vpls` La interfaz de línea de comandos (CLI) muestra las configuraciones de duplicación de puertos de capa 2 como , incluso para la duplicación de puertos de capa 2 configurada como .`family vpls`family `ethernet-switching` Se utiliza cuando la interfaz física está configurada con .`family ethernet-switching`encapsulation `ethernet-bridge`

5. Habilite la configuración de las propiedades de destino de réplica a nivel global para esta familia de direcciones:

```
[edit forwarding-options port-mirroring family family]
user@host# edit output
```

6. Especifique las propiedades de destino de réplica de nivel global para esta familia de direcciones.

   a) Especifique la interfaz física en la que se enviarán los paquetes reflejados:

```
[edit forwarding-options port-mirroring family family output]
user@host# set interface interface-name
```

   También puede especificar una interfaz de enrutamiento y puente integrados (IRB) como interfaz de salida.

   b) (Opcional) Permitir la configuración de filtros en la interfaz de destino para la instancia de creación de reflejo de puerto con nombre:

```
[edit forwarding-options port-mirroring family family output]
user@host# set no-filter-check
```

7. (Opcional) Especifique que los paquetes seleccionados para la creación de reflejo se reflejarán una sola vez en cualquier destino de creación de reflejo:

```
[edit forwarding-options port-mirroring family family output]
user@host# up 2
[edit forwarding-options port-mirroring]
user@host# set mirror-once
```

> **CONSEJO**: Active la opción cuando un enrutador de la serie MX o un conmutador de la serie EX esté configurado para realizar la duplicación de puertos de capa 2 en las interfaces de entrada y salida, lo que podría resultar en el envío de paquetes duplicados al mismo destino (lo que complicaría el análisis del tráfico reflejado).`mirror-once`

8. Verifique la configuración mínima de la instancia global de creación de reflejo de puerto de capa 2:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show forwarding-options

forwarding-options {
    port-mirroring {
        input { # Global packet-selection properties.
```

```
            maximum-packet-length number; # Default is 0.
            rate number;
            run-length number;
        }
        family (ccc | vpls) { # Address- type 'ethernet-switching' displays as 'vpls'.
            output { # Global mirror destination properties.
                interface interface-name;
                no-filter-check; # Optional. Allow filters on interface.
            }
        }
        mirror-once; # Optional. Mirror destinations do not receive duplicate packets.
    }
}
```

Instancias con nombre de creación de reflejo de puertos de capa 2

in this section

- Descripción general de instancias con nombre de creación de reflejo de puertos de capa 2 | **1183**
- Duplicación en puertos agrupados a nivel de FPC | **1184**
- Duplicación en puertos agrupados a nivel de PIC | **1185**
- Creación de reflejo en un grupo de puertos enlazados a varias instancias con nombre | **1185**

En este tema se describe la siguiente información:

Descripción general de instancias con nombre de creación de reflejo de puertos de capa 2

En un enrutador de la serie MX y en un conmutador de la serie EX, puede definir un conjunto de propiedades de duplicación de puertos que puede enlazar explícitamente a puertos físicos del enrutador o conmutador. Este conjunto de propiedades de creación de reflejo de puertos se conoce como *instancia con nombre* de *creación de reflejo de puertos* de capa 2.

Puede enlazar una instancia con nombre de duplicación de puertos de capa 2 a puertos físicos asociados con los componentes del motor de reenvío de paquetes de un enrutador serie MX o de un conmutador serie EX en diferentes niveles del chasis del enrutador (o conmutador):

- En el nivel de FPC: puede enlazar una instancia con nombre a los puertos físicos asociados con un concentrador de puerto denso (DPC) específico o a los puertos físicos asociados con un concentrador de puerto flexible (FPC) específico.

- En el nivel de PIC: puede enlazar una instancia con nombre de creación de reflejo de puertos a un motor de reenvío de paquetes específico (en un DPC específico) o a una PIC específica.

> **NOTA**: Los enrutadores de la serie MX admiten DPC, así como FPC y PIC. A diferencia de los FPC, los DPC no admiten PIC. Sin embargo, en la CLI de Junos OS, se usa la sintaxis de FPC y PIC para configurar o mostrar información acerca de los DPC y los motores de reenvío de paquetes en los DPC.

Los siguientes puntos resumen el comportamiento de la creación de reflejo de puertos de capa 2 en función de las instancias con nombre:

- El alcance de la selección de paquetes viene determinado por el destino del enlace: en los puertos (o puertos) enlazados a una instancia con nombre de duplicación de puertos de capa 2, el enrutador o conmutador selecciona los paquetes de entrada de acuerdo con las propiedades de selección de paquetes en la instancia nombrada.

- El destino de un paquete seleccionado viene determinado por la familia de direcciones de paquetes: de los paquetes seleccionados, el enrutador o conmutador refleja sólo los paquetes que pertenecen a una familia de direcciones para la cual la instancia con nombre de la creación de reflejo de puerto de capa 2 especifica un conjunto de propiedades de destino reflejado. En un entorno de capa 2, los enrutadores serie MX y los conmutadores serie EX admiten la duplicación de puertos del tráfico VPLS (o) y el tráfico VPN de capa 2 con .`family ethernet-switchingfamily vplsfamily ccc`

Para obtener una descripción general de las propiedades de duplicación de puertos de capa 2, consulte Descripción de las propiedades de creación de reflejo de puertos de capa 2."Propiedades de duplicación de puertos de capa 2" en la página 1061 Para obtener una comparación de los tipos de duplicación de puertos de capa 2 disponibles en un enrutador de la serie MX y en un conmutador de la serie EX, consulte Aplicación de tipos de duplicación de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-services-port-mirroring-application.html

Duplicación en puertos agrupados a nivel de FPC

En un enrutador serie MX y en un conmutador serie EX, puede enlazar una instancia con nombre de duplicación de puertos de capa 2 a un DPC o FPC específico instalado en el chasis del enrutador (o conmutador). Las propiedades de creación de reflejo de puertos en la instancia se aplican a todos los motores de reenvío de paquetes (y sus puertos asociados) en el DPC especificado o a todas las PIC (y sus puertos asociados) instaladas en la FPC especificada. Las propiedades de duplicación de puertos enlazadas a un DPC o FPC invalidan cualquier propiedad de creación de reflejo de puerto enlazada a nivel global o al chasis del enrutador (o conmutador) de la serie MX.

Duplicación en puertos agrupados a nivel de PIC

En un enrutador de la serie MX y en un conmutador de la serie EX, puede enlazar una instancia con nombre de la duplicación de puertos de capa 2 a un motor de reenvío de paquetes o PIC específico. Las propiedades de creación de reflejo de puertos en esa instancia se aplican a todos los puertos asociados con el motor de reenvío de paquetes o PIC especificado. Las propiedades de duplicación de puertos enlazadas a un motor de reenvío de paquetes o PIC invalidan cualquier propiedad de creación de reflejo de puertos enlazada en el DPC o FPC que las contiene.

NOTA: Para los enrutadores MX960, hay una asignación uno a uno de motores de reenvío de paquetes a puertos Ethernet. Por lo tanto, solo en los enrutadores MX960, puede configurar enlaces específicos de puerto de instancias de duplicación de puertos.

Creación de reflejo en un grupo de puertos enlazados a varias instancias con nombre

En un enrutador de la serie MX y en un conmutador de la serie EX, puede aplicar hasta dos instancias con nombre de duplicación de puertos de capa 2 al mismo grupo de puertos dentro del chasis del enrutador (o conmutador). Al aplicar dos instancias diferentes de duplicación de puertos al mismo DPC, FPC, motor de reenvío de paquetes o PIC, puede enlazar dos especificaciones distintas de creación de reflejo de puertos de capa 2 a un único grupo de puertos.

NOTA: Solo puede configurar una instancia global de duplicación de puertos de capa 2 en un enrutador de la serie MX y en un conmutador de la serie EX.

NOTA: Puede configurar más de dos instancias de creación de reflejo de puerto para cada FPC configurando la creación de reflejo de puerto en línea. Para obtener información sobre la creación de reflejo de puertos en línea, consulte Configuración de la creación de reflejo de puerto en línea."Configuración de la duplicación de puerto en línea" en la página 1190

Definición de una instancia con nombre de creación de reflejo de puertos de capa 2

En un enrutador serie MX y en un conmutador serie EX, puede definir un conjunto de propiedades de duplicación de puerto de capa 2 que puede enlazar a un motor de reenvío de paquetes determinado (en el nivel PIC del chasis del enrutador o conmutador) o a un grupo de motores de reenvío de paquetes (en el nivel DPC o FPC del chasis).

Para definir una instancia con nombre de duplicación de puertos de capa 2 en un enrutador de la serie MX o en un conmutador de la serie EX:

1. Habilite la configuración de una instancia con nombre de duplicación de puertos de capa 2:

```
[edit]
user@host# edit forwarding-options port-mirroring instance pm-instance-name
```

2. Habilite la configuración de las propiedades de muestreo de paquetes:

```
[edit forwarding-options port-mirroring instance pm-instance-name]
user@host# edit input
```

3. Especifique las propiedades de selección de paquetes:

   a) Especifique el número de paquetes que desea seleccionar:

   ```
   [edit forwarding-options port-mirroring instance pm-instance-name input]
   user@host# set rate number
   ```

   El intervalo válido es a través de .165535

   b) Especifique el número de paquetes que desea reflejar de cada selección:

   ```
   [edit forwarding-options port-mirroring instance pm-named-instance input]
   user@host# set run-length number
   ```

   El intervalo válido es a través de .020 El valor predeterminado es .0

   > **NOTA**: La instrucción no se admite en enrutadores MX80.run-length

   c) Especifique la longitud a la que se van a truncar los paquetes reflejados:

   ```
   [edit forwarding-options port-mirroring instance pm-instance-name input]
   user@host# set maximum-packet-length number
   ```

   El intervalo válido es a través de .09216 El valor predeterminado es , lo que significa que los paquetes reflejados no se truncan.0

   > **NOTA**: La instrucción no se admite en enrutadores MX80.maximum-packet-length

4. Habilite la configuración de las propiedades de destino reflejado para los paquetes de capa 2 que forman parte del dominio de puente, las conexiones cruzadas de conmutación de capa 2 o el servicio de LAN privada virtual (VPLS):

   a) Especifique el tipo de tráfico de la familia de direcciones de capa 2 que se va a reflejar:

```
[edit forwarding-options port-mirroring instance pm-instance-name input]
user@host# up
[edit forwarding-options port-mirroring instance pm-instance-name]
user@host# edit family family
```

   El valor de la opción puede ser , , o .*family*`ethernet-switching`cccvpls

   NOTA: En el nivel de jerarquía, la instrucción de familia protocol es un alias para .`[edit forwarding-options port-mirroring]family ethernet-switching`family `vpls` La interfaz de línea de comandos (CLI) muestra las configuraciones de duplicación de puertos de capa 2 como , incluso para la duplicación de puertos de capa 2 configurada como .`family vpls`family `ethernet-switching` Se utiliza cuando la interfaz física está configurada con .`family ethernet-switching`encapsulation `ethernet-bridge`

   b) Habilite la configuración de las propiedades de destino del reflejo:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family]
user@host# edit output
```

5. Especifique las propiedades de destino del reflejo.

   a) Especifique la interfaz física en la que se enviarán los paquetes reflejados:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family output]
user@host# set interface interface-name
```

   b) (Opcional) Permitir la configuración de filtros en la interfaz de destino para la instancia global de creación de reflejo de puertos:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family output]
user@host# set no-filter-check
```

NOTA: No puede configurar instancias de duplicación de puertos en enrutadores MX80. Solo puede configurar la duplicación de puertos a nivel global en enrutadores MX80.

6. (Opcional) Especifique que los paquetes seleccionados para la creación de reflejo se reflejarán una sola vez en cualquier destino de creación de reflejo:

```
[edit forwarding-options port-mirroring instance pm-instance-name family family output]
user@host# up 3
[edit forwarding-options port-mirroring]
user@host# set mirror-once
```

CONSEJO: Active la opción global cuando un enrutador de la serie MX o un conmutador de la serie EX esté configurado para realizar la creación de reflejo del puerto de capa 2 en las interfaces de entrada y salida, lo que podría dar como resultado el envío de paquetes duplicados al mismo destino (lo que a su vez complicaría el análisis del tráfico reflejado).`mirror-once`

7. Para configurar un destino de creación de reflejo para un tipo de familia de paquetes diferente, repita los pasos del 4 al 6.
8. Verifique la configuración mínima de las instancias con nombre de la creación de reflejo del puerto de capa 2:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show forwarding-options

forwarding-options {
    port-mirroring {
        ... optional-global-port-mirroring-configuration ...
        instance {
            pm-instance-name ( # A named instance of port mirroring
                input { # Packet-selection properties
                    maximum-packet-length number; # Default is 0.
                    rate number;
                    run-length number;
                }
                family (ccc | vpls) { # Address- type 'ethernet-switching' displays as 'vpls'.
```

```
                    output { # Mirror destination properties
                        interface interface-name;
                        no-filter-check; # Optional. Allow filters on interface.
                    }
                }
            }
        }
        mirror-once; # Optional. Mirror destinations do not receive duplicate packets.
    }
}
```

Deshabilitar instancias de creación de reflejo de puertos de capa 2

Puede deshabilitar la instancia global de creación de reflejo de puertos de capa 2, una instancia con nombre en particular o todas las instancias de creación de reflejo de puertos:

- Para deshabilitar la instancia global de creación de reflejo de puerto de capa 2, incluya la instrucción en el nivel de jerarquía:`disable`[`edit forwarding-options port-mirroring`]

```
[edit]
forwarding-options {
    port-mirroring {
        disable; Disables the global instance of Layer 2 port mirroring.
        ...global-instance-of-layer-2-port-mirroring-configuration...
    }
}
```

- Para deshabilitar la definición de una instancia con nombre concreta de creación de reflejo de puertos de capa 2, incluya la instrucción en el nivel de jerarquía:`disable`[`edit forwarding-options port-mirroring instance  instance-name`]

```
[edit]
forwarding-options {
    port-mirroring {
        ...optional-configuration-of-the-global-instance-of-layer-2-port-mirroring...
        instance {
            port-mirroring-instance-name {
                disable; Disables this named instance of Layer 2 port mirroring.
                ...definition-of-a-named-instance-of-layer-2-port-mirroring...
            }
        }
```

```
    }
}
```

- Para deshabilitar la instancia global y todas las instancias con nombre de creación de reflejo de puerto de capa 2, incluya la instrucción en el nivel de jerarquía:`disable-all-instances`[`edit forwarding-options port-mirroring`]

```
[edit]
forwarding-options {
    port-mirroring {
        disable-all-instances; Disables all instances of Layer 2 port mirroring.
        ...optional-configuration-of-the-global-instance-of-layer-2-port-mirroring...
        instance {
            port-mirroring-instance-name {
                ...definition-of-a-named-instance-of-layer-2-port-mirroring...
            }
        }
    }
}
```

Configuración de la duplicación de puerto en línea

La creación de reflejo de puerto en línea le permite especificar instancias que no están vinculadas al concentrador de PIC flexible (FPC) en la acción de filtro de firewall.`then port-mirror-instance` De esta manera, no está limitado a solo dos instancias de espejo de puerto por FPC. La duplicación de puertos en línea desacopla el destino puerto-espejo de los parámetros de entrada como `.rate` Mientras que los parámetros de entrada están programados en la placa de interfaz del conmutador, el destino del siguiente salto del paquete reflejado está disponible en el propio paquete. La duplicación de puertos en línea solo se admite en concentradores de puertos modulares (MPC) basados en Trio.

Mediante la creación de reflejo de puerto en línea, una instancia de espejo de puerto tendrá la opción de heredar parámetros de entrada de otra instancia que lo especifique, como se muestra en el siguiente ejemplo de configuración de CLI:

```
instance pm2 {
    +  input-parameters-instance pm1;
    family inet {
        output {
            interface ge-1/2/3.0 {
                next-hop 192.0.2.10;
            }
```

```
        }
    }
}
```

No se permiten varios niveles de herencia. Una instancia puede ser referida por varias instancias. Una instancia puede hacer referencia a otra instancia definida antes de ella. No se permiten referencias hacia adelante y una instancia no puede hacer referencia a sí misma, lo que provocará un error durante el análisis de la configuración.

El usuario puede especificar una instancia que no esté enlazada a la FPC en el filtro de firewall. El filtro especificado debe heredar una de las dos instancias que se han enlazado a la FPC. Si no es así, el paquete no está marcado para la duplicación de puertos. Si lo hace, entonces el paquete se muestreará utilizando los parámetros de entrada especificados por la instancia referida, pero la copia se enviará a su propio destino.

Configuración de la duplicación de puertos en interfaces físicas

in this section

- Precedencia de múltiples niveles de duplicación de puertos de capa 2 en una interfaz física | **1191**
- Enlace de la creación de reflejo de puertos de capa 2 a puertos agrupados en el nivel de FPC | **1192**
- Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC | **1194**
- Ejemplos: Duplicación de puertos de capa 2 en varios niveles del chasis | **1196**
- Configuración de la duplicación de puertos de capa 2 a través de la interfaz GRE | **1198**
- Ejemplo: Configuración de la duplicación de puertos de capa 2 a través de una interfaz GRE | **1200**

Precedencia de múltiples niveles de duplicación de puertos de capa 2 en una interfaz física

Puede enlazar diferentes conjuntos de propiedades de *duplicación de puertos* de capa 2 (la instancia global y una o más instancias con nombre) en varios niveles de un enrutador serie MX o de un chasis de conmutador serie EX (en el nivel del chasis, en el nivel de FPC o en el nivel de PIC). Por lo tanto, es posible que un único grupo de interfaces físicas esté enlazado a varias definiciones de creación de reflejo de puertos de capa 2.

Si un grupo de puertos (o, en el caso de un enlace a nivel de PIC en un enrutador MX960, un solo puerto) está enlazado a varias definiciones de duplicación de puertos de capa 2, el enrutador (o

conmutador) aplica las propiedades de duplicación de puertos de capa 2 a esos puertos de la siguiente manera:

1. Las propiedades de duplicación de puertos a nivel de chasis se aplican implícitamente a todos los puertos del chasis. Si un enrutador de la serie MX o un conmutador de la serie EX está configurado con la instancia global de duplicación de puertos, esas propiedades de creación de reflejo de puerto se aplican a todos los puertos. Consulte Configuración de la instancia global de creación de reflejo de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-global-instance-configuring.html

2. Las propiedades de duplicación de puertos a nivel de FPC invalidan las propiedades a nivel de chasis. Si un DPC o FPC está enlazado a una instancia con nombre de creación de reflejo de puerto, esas propiedades de creación de reflejo de puerto se aplican a todos los puertos asociados con ese DPC o FPC, anulando cualquier propiedad de creación de reflejo de puerto enlazada en el nivel del chasis. Consulte Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de FPC."Enlace de la creación de reflejo de puertos de capa 2 a puertos agrupados en el nivel de FPC" en la página 1192

3. Las propiedades de duplicación de puertos a nivel PIC anulan las propiedades de nivel FPC. Si un motor de reenvío de paquetes o PIC está enlazado a una instancia con nombre de duplicación de puertos, esas propiedades de creación de reflejo de puertos se aplican a todos los puertos asociados con el motor de reenvío de paquetes o PIC, anulando cualquier propiedad de duplicación de puertos enlazada a esos puertos en el nivel de FPC. Consulte Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC."Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC" en la página 1194

Enlace de la creación de reflejo de puertos de capa 2 a puertos agrupados en el nivel de FPC

En un enrutador de la serie MX y en un conmutador de la serie EX, puede enlazar una instancia con nombre de duplicación de puertos de capa 2 a un DPC específico o a una FPC específica del chasis del enrutador (o conmutador). Esto se conoce como enlace de una instancia con nombre de duplicación de puertos de capa 2 *en el nivel FPC* del chasis del enrutador (o conmutador). Las propiedades de creación de reflejo de puertos especificadas en la instancia nombrada se aplican a todos los puertos físicos asociados con todos los motores de reenvío de paquetes en el DPC o FPC especificado.

NOTA: También puede enlazar una instancia con nombre de creación de reflejo de puertos de capa 2 a un motor de reenvío de paquetes específico en un DPC o FPC del chasis del enrutador (o conmutador).

Para cualquier familia de tipo de paquete compatible con la creación de reflejo de puertos de capa 2

- Las propiedades de duplicación de puertos enlazadas a un DPC o FPC específico invalidan cualquier propiedad de creación de reflejo de puerto configurada a nivel global.
- Las propiedades de duplicación de puertos enlazadas a un motor de reenvío de paquetes específico invalidan cualquier propiedad de duplicación de puertos configurada en el nivel de DPC o FPC.

Puede aplicar hasta dos instancias con nombre de duplicación de puertos de capa 2 al mismo grupo de puertos dentro del chasis del enrutador (o conmutador). Al aplicar dos instancias diferentes de duplicación de puertos al mismo DPC o FPC, puede enlazar dos especificaciones distintas de duplicación de puertos de capa 2 a un único grupo de puertos.

Antes de comenzar, realice las siguientes tareas:

- Defina una instancia con nombre de la creación de reflejo del puerto de capa 2. Consulte Definición de una instancia con nombre de creación de reflejo de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-named-instance-configuring.html
- Muestra información sobre el número y los tipos de DPC o FPC en el enrutador de la serie MX y en el conmutador de la serie EX, el número de motores de reenvío de paquetes en cada uno, y el número y los tipos de puertos por motor de reenvío de paquetes.

Para enlazar una instancia con nombre de creación de reflejo de puertos de capa 2 a una DPC o FPC y sus motores de reenvío de paquetes:

1. Habilite la configuración de las propiedades del chasis del enrutador (o conmutador):

```
[edit]
user@host# edit chassis
```

2. Habilite la configuración de un DPC (y sus motores de reenvío de paquetes correspondientes) o un FPC (y sus PIC instalados):

```
[edit chassis]
user@host# edit fpc slot-number
```

3. Vincule una instancia con nombre de creación de reflejo de puertos de capa 2 () al DPC o FPC:*pm-instance-name*

```
[edit chassis fpc slot-number]
user@host# set port-mirror-instance pm-instance-name
```

4. (Opcional) Para enlazar una segunda instancia con nombre de creación de reflejo del puerto de capa 2 al mismo DPC o FPC, repita el paso anterior (paso 3) y especifique una instancia con nombre diferente de creación de reflejo del puerto de capa 2.
5. Compruebe la configuración mínima del enlace:

```
[edit chassis fpc slot-number port-mirror-instance pm-instance-name]
user@host# top
[edit]
user@host# show chassis

chassis {
    fpc slot-number { # Bind two port mirroring named instances at the FPC level.
        port-mirror-instance pm-instance-name-1;
        port-mirror-instance pm-instance-name-2;
    }
}
```

Vinculación de la creación de reflejo de puertos de capa 2 a puertos agrupados a nivel de PIC

En un enrutador de la serie MX y en un conmutador de la serie EX, puede enlazar una instancia con nombre de la duplicación de puertos de capa 2 a los puertos asociados con un motor de reenvío de paquetes específico (en un DPC) o a los puertos asociados con una PIC específica (instalada en una FPC). Esto se conoce como enlace de una instancia con nombre de duplicación de puertos de capa 2 *en el nivel de PIC* del chasis del enrutador (o conmutador). Las propiedades de duplicación de puertos especificadas en la instancia nombrada se aplican a todos los puertos físicos asociados con el motor de reenvío de paquetes especificado.

NOTA: También puede enlazar una instancia con nombre de creación de reflejo de puertos de capa 2 a un DPC o FPC específico en el chasis del enrutador (o conmutador).

Para cualquier familia de tipos de paquetes compatible con la creación de reflejo de puertos de capa 2:

- Las propiedades de duplicación de puertos enlazadas a un motor de reenvío de paquetes específico invalidan cualquier propiedad de duplicación de puertos configurada en el nivel de DPC o FPC.
- Las propiedades de duplicación de puertos enlazadas a un DPC o FPC específico invalidan cualquier propiedad de creación de reflejo de puerto configurada a nivel global.

Puede aplicar hasta dos instancias con nombre de duplicación de puertos de capa 2 al mismo grupo de puertos dentro del chasis del enrutador (o conmutador). Al aplicar dos instancias de creación de reflejo de puertos diferentes al mismo motor de reenvío de paquetes o PIC, puede enlazar dos especificaciones distintas de creación de reflejo de puertos de capa 2 a un único grupo de puertos.

Para los enrutadores MX960, hay una asignación uno a uno de motores de reenvío de paquetes a puertos Ethernet. Por lo tanto, sólo en los enrutadores MX960, puede enlazar una instancia con nombre de la duplicación de puertos de capa 2 a un puerto específico enlazando la instancia al motor de reenvío de paquetes asociado con el puerto .

Antes de comenzar, realice las siguientes tareas:

- Defina una instancia con nombre de la creación de reflejo del puerto de capa 2. Consulte Definición de una instancia con nombre de creación de reflejo de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-named-instance-configuring.html
- Muestra información sobre el número y los tipos de CPC en el enrutador de la serie MX o en el conmutador de la serie EX, el número de motores de reenvío de paquetes en cada DPC, y el número y los tipos de puertos por motor de reenvío de paquetes.

Para enlazar una instancia con nombre de creación de reflejo de puertos de capa 2 a un motor de reenvío de paquetes:

1. Habilite la configuración de las propiedades del chasis del enrutador (o conmutador):

```
[edit]
user@host# edit chassis
```

2. Habilite la configuración de un motor de reenvío de paquetes o PIC:

```
[edit chassis]
user@host# edit fpc slot-number
user@host# edit pic slot-number
```

3. Vincule una instancia con nombre de creación de reflejo de puerto de capa 2 () al motor de reenvío de paquetes o PIC:*pm-instance-name*

```
[edit chassis fpc slot-number pic slot-number]
user@host# set port-mirror-instance pm-instance-name
```

4. (Opcional) Para enlazar una segunda instancia con nombre de creación de reflejo de puertos de capa 2 al mismo motor de reenvío de paquetes o PIC, repita el paso anterior (paso 3) y especifique una instancia con nombre diferente de creación de reflejo de puerto de capa 2.
5. Compruebe la configuración mínima del enlace:

```
[edit forwarding-options ... ]
user@host# top
[edit]
user@host# show chassis
chassis {
    fpc slot-number {
        ... optional-binding-of-a-port-mirroring-instance-at-the-dpc-level ...
        pic slot-number { # Bind two port-mirroring named instances at the PIC level.
            port-mirror-instance pm-instance-name-1;
            port-mirror-instance pm-instance-name-2;
        }
    }
}
```

Ejemplos: Duplicación de puertos de capa 2 en varios niveles del chasis

in this section

- Duplicación de puertos de capa 2 a nivel de FPC | **1197**
- Duplicación de puertos de capa 2 a nivel de PIC | **1197**
- Duplicación de puertos de capa 2 en los niveles de FPC y PIC | **1198**

En un enrutador de la serie MX o en un conmutador de la serie EX, puede aplicar instancias con nombre de duplicación de puertos de capa 2 en el nivel FPC o DPC del chasis, o en el nivel PIC del chasis. Sin embargo, solo puede configurar (y aplicar implícitamente) una instancia global de creación de reflejo de puertos de capa 2 en todo el chasis.

Duplicación de puertos de capa 2 a nivel de FPC

En esta configuración de ejemplo de un enrutador de la serie MX o de un chasis de conmutador de la serie EX, una instancia con nombre de duplicación de puertos de capa 2 () está enlazada a puertos físicos agrupados en el nivel de FPC:**pm1**

```
[edit]
chassis {
    fpc 2 {
        port-mirror-instance pm1;
    }
}
```

Esta no es una configuración completa. Las interfaces físicas asociadas con la FPC o DPC en la ranura 2 deben configurarse en el nivel de jerarquía.`[edit interfaces]` La instancia denominada de creación de reflejo de puertos de capa 2 debe configurarse en el nivel jerárquico .**pm1**`[edit forwarding-options port-mirroring instance]`

Duplicación de puertos de capa 2 a nivel de PIC

En esta configuración de ejemplo de un enrutador de la serie MX o de un chasis de conmutador de la serie EX, una instancia con nombre de creación de reflejo de puerto de capa 2 () está enlazada a los puertos físicos agrupados en el nivel de PIC:**pm2**

```
[edit]
chassis {
    fpc 2 {
        pic 0 {
            port-mirror-instance pm2;
        }
    }
}
```

Esta no es una configuración completa. Las interfaces físicas asociadas con la FPC o DPC en la ranura 2 deben configurarse en el nivel de jerarquía.`[edit interfaces]` La instancia denominada de creación de reflejo de puertos de capa 2 debe configurarse en el nivel jerárquico .**pm2**`[edit forwarding-options port-mirroring instance]`

Duplicación de puertos de capa 2 en los niveles de FPC y PIC

En esta configuración de ejemplo de un chasis de enrutador serie MX o de un conmutador serie EX, se aplica una instancia con nombre de duplicación de puerto de capa 2 () en el nivel FPC del chasis del enrutador (o conmutador).**pm1** Se aplica una segunda instancia con nombre () en el nivel de PIC:**pm2**

```
[edit]
chassis {
    fpc 2 {
        port-mirror-instance pm1;
        pic 0 {
            port-mirror-instance pm2;
        }
    }
}
```

Esta no es una configuración completa. Las interfaces físicas asociadas con la FPC o DPC en la ranura 2, incluidas las interfaces físicas asociadas con , deben configurarse en el nivel de jerarquía.**pic 0**`[edit interfaces]` La creación de reflejo del puerto de capa 2 denomina instancias y debe configurarse en el nivel de jerarquía.**pm1pm2**`[edit forwarding-options port-mirroring instance]`

Configuración de la duplicación de puertos de capa 2 a través de la interfaz GRE

La duplicación de puertos es la capacidad de un enrutador para enviar una copia de un paquete a una dirección de host externa o a un analizador de paquetes para su análisis. Una aplicación para la duplicación de puertos envía un paquete duplicado a un túnel virtual. A continuación, se puede configurar un grupo de salto siguiente para reenviar copias de este paquete duplicado a varias interfaces. Junos OS admite la creación de reflejo de puertos de capa 2 en un recopilador remoto a través de una interfaz GRE.

Para configurar la duplicación de puertos de capa 2 en una interfaz GRE, haga lo siguiente:

1. Configure la interfaz GRE con la dirección de origen y destino.

```
[edit interfaces inteface-name unit unit-number tunnel]
set source ip-address
set  destination ip-address
```

2. Configure los parámetros de puente de familia en la interfaz GRE.

```
[edit interfaces interface-name unit unit-number family bridge]
set interface-mode trunk
set vlan-id valn-id
```

3. Configure la velocidad a la que se reflejan los paquetes de entrada.

```
[edit forwarding-options port-mirroring]
set f input rate rate
```

4. Configure la interfaz de salida para VPLS de familia para la interfaz GRE.

```
[edit forwarding-options family vpls]
set output  interface gre-interface-name
```

5. Configure el término de filtro de firewall para el puente de familia para contar los paquetes que llegan a la interfaz.

```
[edit firewall family bridge]
set filter f1 term term then count count
```

6. Configure el término de filtro de firewall para el puente de familia para reflejar los paquetes.

```
[edit firewall family bridge]
set filter filter-name term term then port-mirror
```

SEE ALSO

Descripción general de los servicios de túnel

Ejemplo: Configuración de la duplicación de puertos de capa 2 a través de una interfaz GRE

in this section

- Requisitos | 1200
- Descripción general | 1200
- Configuración | 1201
- Verificación | 1206

En este ejemplo, se muestra cómo configurar la creación de reflejo del puerto de capa 2 en una interfaz GRE para su análisis.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un enrutador serie MX
- Junos OS versión 16.1 o posterior ejecutándose en todos los dispositivos

Descripción general

in this section

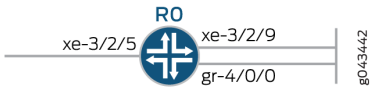
- Topología | 1201

La duplicación de puertos es la capacidad de un enrutador para enviar una copia de un paquete a una dirección de host externa o a un analizador de paquetes para su análisis. Una aplicación para la duplicación de puertos envía un paquete duplicado a un túnel virtual. A continuación, se puede configurar un grupo de salto siguiente para reenviar copias de este paquete duplicado a varias interfaces. A partir de Junos OS versión 16.1, se admite la creación de reflejo de puertos de capa 2 en un recopilador remoto a través de una interfaz GRE.

Topología

Figura 41 en la página 1201 muestra la duplicación de puertos configurada a través de una interfaz GRE. La interfaz gr-4/0/0 está configurada como puente de familia. El filtro de puente f1 de la familia de firewall está configurado como puerto-espejo. El destino del espejo se configura como gr-4/0/0. El filtro de puente f1 de la familia de firewall se aplica en la entrada y salida de la interfaz xe-3/2/5.0, que refleja los paquetes para reflejar el destino gr-4/0/0.

Figura 41: Ejemplo de duplicación de puertos de capa 2 a través de interfaz GRE



Configuración

in this section

- Configuración rápida de CLI | **1201**
- Configuración de R0 | **1202**
- Resultados | **1204**

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía **[edit]** y, luego, ingrese `commit` desde el modo de configuración.

R0

```
set chassis fpc4 pic0 tunnel-services bandwidth 10g
set chassis network-services enhanced-ip
set interfaces xe-3/2/5 flexible-vlan-tagging
set interfaces xe-3/2/5 encapsulation flexible-ethernet-services
set interfaces xe-3/2/5  unit 0 encapsulation vlan-bridge
set interfaces xe-3/2/5 unit 0 vlan-id 100
```

```
set interfaces xe-3/2/5 unit 0 family bridge filter  input f1
set interfaces xe-3/2/5 unit 0 family bridge filter output f1
set interfaces xe-3/2/9 flexible-vlan-tagging
set interfaces xe-3/2/9 encapsulation flexible-ethernet-services
set interfaces xe-3/2/9  unit 0 encapsulation vlan-bridge
set interfaces xe-3/2/9  unit 0 vlan-id 100
set interfaces gr-4/0/0  unit 0 tunnel source 10.1.1.1
set interfaces gr-4/0/0  unit 0 tunnel  destination 10.1.1.2
set interfaces gr-4/0/0  unit 0  family bridge  interface-mode trunk
set interfaces gr-4/0/0  unit 0  family bridge   vlan-id 100
set forwarding-options port-mirroring input rate 1
set forwarding-options  family vpls output  interface gr-4/0/0.0
set firewall family bridge  filter f1 term t  then count c
set firewall family bridge  filter f1 term t  then port-mirror
set bridge-domains  b vlan-id 100
set bridge-domains  b  interface xe-3/2/5.0
set bridge-domains  b  interface xe-3/2/9.0
```

Configuración de R0

Procedimiento paso a paso

El ejemplo siguiente requiere que navegue por varios niveles en la jerarquía de configuración. Para obtener información acerca de cómo navegar por la CLI, consulte "" en la Guía del usuario de la CLI de Junos OS .*Using the CLI Editor in Configuration Mode*

Para configurar el dispositivo R0:

1. Configure los parámetros flexibles del concentrador PIC del chasis.

```
[edit chassis]
user@R0# set fpc4 pic0 tunnel-services bandwidth 10g
user@R0# set network-services enhanced-ip
```

2. Configure los servicios de red de IP mejorada del chasis.

```
[edit chassis]
user@R0# set network-services enhanced-ip
```

3. Configure las interfaces.

```
[edit interfaces]
user@R0# set xe-3/2/5 flexible-vlan-tagging
user@R0# set xe-3/2/5 encapsulation flexible-ethernet-services
user@R0# set xe-3/2/5  unit 0 encapsulation vlan-bridge
user@R0# set xe-3/2/5 unit 0 vlan-id 100
user@R0# set xe-3/2/5 unit 0 family bridge filter  input f1
user@R0# set xe-3/2/5 unit 0 family bridge filter output f1
user@R0# set xe-3/2/9 flexible-vlan-tagging
user@R0# set xe-3/2/9 encapsulation flexible-ethernet-services
user@R0# set xe-3/2/9  unit 0 encapsulation vlan-bridge
user@R0# set xe-3/2/9  unit 0 vlan-id 100
user@R0# set gr-4/0/0  unit 0 tunnel source 10.1.1.1
user@R0# set gr-4/0/0  unit 0 tunnel  destination 10.1.1.2
user@R0# set gr-4/0/0  unit 0  family bridge  interface-mode trunk
user@R0# set gr-4/0/0  unit 0  family bridge   vlan-id 100
```

4. Configure la velocidad de los paquetes de entrada que se van a muestrear.

```
[edit forwarding-options]
user@R0# set port-mirroring input rate 1
```

5. Configure la interfaz de salida para la familia de paquetes de direcciones VPLS que se va a reflejar.

```
[edit forwarding-options]
user@R0# set family vpls output  interface gr-4/0/0.0
```

6. Configure la familia de protocolos BRIDGE para el filtro de firewall.

```
[edit firewall]
user@R0# set family bridge  filter f1 term t  then count c
user@R0# set family bridge  filter f1 term t  then port-mirror
```

7. Configure el ID de VLAN para el dominio de puente.

```
[edit bridge-domains]
user@R0# set  b vlan-id 100
```

```
user@R0# set  b  interface xe-3/2/5.0
user@R0# set  b  interface xe-3/2/9.0
```

8. Configure la interfaz para el dominio de puente.

```
[edit bridge-domains]
user@R0# set  b  interface xe-3/2/5.0
user@R0# set  b  interface xe-3/2/9.0
```

Resultados

Desde el modo de configuración, escriba los comandos , , , y para confirmar la configuración.**show bridge-domainsshow chassisshow forwarding-optionsshow firewallshow interfaces** Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
user@R0# show chassis
fpc 4 {
    pic 0 {
        tunnel-services {
            bandwidth 10g;
        }
    }
}
network-services enhanced-ip;
```

```
user@R0# show interfaces
}
xe-3/2/5 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 100;
        family bridge {
            filter {
                input f1;
```

```
                output f1;
            }
        }
    }
}
xe-3/2/9 {
    flexible-vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 0 {
        encapsulation vlan-bridge;
        vlan-id 100;
    }
}
gr-4/0/0 {
    unit 0 {
        tunnel {
            source 10.1.1.1;
            destination 10.1.1.2;
        }
        family bridge {
            interface-mode trunk;
            vlan-id 100;
        }
    }
}
```

```
user@R0# show forwarding-options
port-mirroring {
    input {
        rate 1;
    }
    family vpls {
        output {
            interface gr-4/0/0.0;
        }
    }
}
```

```
user@R0# show firewall
family bridge {
```

```
    filter f1 {
        term t {
            then {
                count c;
                port-mirror;
            }
        }
    }
}
```

```
user@R0# show bridge-domains
b {
    vlan-id 100;
    interface xe-3/2/5.0;
    interface xe-3/2/9.0;
}
```

Verificación

in this section

- Verificación de la duplicación de puertos del tráfico | **1206**

Confirme que la configuración funcione correctamente.

Verificación de la duplicación de puertos del tráfico

Propósito

Muestra la duplicación de puertos de la información de tráfico.

Acción

En el dispositivo R0, desde el modo operativo, ejecute el comando para mostrar la duplicación del puerto de la información de tráfico.`show forwarding-options port-mirroring`

```
user@R0> show forwarding-options port-mirroring
Instance Name: & globalinstance
  Instance Id: 1
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    vpls                up        gr-4/0/0.0

Instance Name: pm_instance
  Instance Id: 2
  Input parameters:
    Rate                  : 10
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    vpls                up        gr-4/0/0.0
```

Significado

El resultado muestra la duplicación del puerto de la información de tráfico.

Configuración de la creación de reflejo de puertos en interfaces lógicas

in this section

- Filtros de firewall de duplicación de puertos de capa 2 | **1208**
- Definición de un filtro de firewall de duplicación de puertos de capa 2 | **1211**

- Configuración del filtro de firewall independiente del protocolo para la creación de reflejo de puertos | **1214**
- Ejemplo: Duplicación del tráfico web de los empleados con un filtro de firewall | **1217**
- Duplicación de puertos de capa 2 de interfaces lógicas de enrutador PE o conmutador de PE | **1223**
- Duplicación de puertos de capa 2 de interfaces Ethernet agregadas de enrutador PE o conmutador PE | **1227**
- Aplicación de la creación de reflejo de puertos de capa 2 a una interfaz lógica | **1228**
- Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente | **1231**
- Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a una instancia de enrutamiento VPLS | **1234**
- Aplicación de la duplicación de puertos de capa 2 al tráfico reenviado o inundado a una VLAN | **1236**
- Ejemplo: Creación de reflejo de puertos de capa 2 en una interfaz lógica | **1238**
- Ejemplo: Duplicación de puertos de capa 2 para una VPN de capa 2 | **1241**
- Ejemplo: Duplicación de puertos de capa 2 para una VPN de capa 2 con vínculos LAG | **1244**

Filtros de firewall de duplicación de puertos de capa 2

in this section

- Descripción general de los filtros de firewall de duplicación de puertos de capa 2 | **1208**
- Creación de reflejo de paquetes recibidos o enviados en una interfaz lógica | **1210**
- Duplicación de paquetes reenviados o inundados a una VLAN | **1210**
- Creación de reflejo de paquetes reenviados o inundados a una instancia de enrutamiento VPLS | **1211**

En este tema se describe la siguiente información:

Descripción general de los filtros de firewall de duplicación de puertos de capa 2

En un enrutador de la serie MX y en un conmutador de la serie EX, puede configurar un *término* de filtro de firewall para especificar que la *duplicación de puerto* de capa 2 se debe aplicar a todos los paquetes de la interfaz a la que se aplica el *filtro de firewall*.

Puede aplicar un filtro de firewall de duplicación de puertos de capa 2 a las interfaces lógicas de entrada o salida (incluidas las interfaces lógicas Ethernet agregadas), al tráfico reenviado o inundado a una VLAN, o al tráfico reenviado o inundado a una instancia de enrutamiento VPLS.

Los enrutadores y conmutadores de la serie MX admiten la duplicación del puerto de capa 2 del tráfico VPLS (o) y el tráfico VPN de capa 2 en un entorno de capa 2`family ethernet-switchingfamily vplsfamily ccc`

Dentro de un filtro de firewall, puede especificar las propiedades de duplicación de puertos de capa 2 en la instrucción de cualquiera de las siguientes maneras:`termthen`

- Haga referencia implícita a las propiedades de duplicación de puertos de capa 2 vigentes en el puerto.
- Haga referencia explícita a una instancia con nombre concreta de creación de reflejo de puertos de capa 2.

NOTA: Cuando configure un filtro de firewall de duplicación de puertos de capa 2, no incluya la instrucción opcional que especifica condiciones de coincidencia según la dirección de origen de la ruta.`from` Omita esta instrucción para que se considere que todos los paquetes coinciden y se tomen todos y cada uno especificados en la instrucción.*actionsaction-modifiers*`then`

Si desea reflejar todos los paquetes entrantes, no debe utilizar la instrucción de; /*Comentario: Uno configura los términos de filtro con desde si están interesados en reflejar solo un subconjunto de paquetes.

NOTA: Si asocia enrutamiento y puente integrados (IRB) con la VLAN (o instancia de enrutamiento VPLS) y también configura dentro de la VLAN (o instancia de enrutamiento VPLS) un filtro de tabla de reenvío con la acción o , el paquete IRB se refleja como un paquete de capa 2.`port-mirrorport-mirror-instance` Puede deshabilitar este comportamiento configurando la instrucción no-irb-layer-2-copy en la VLAN (o instancia de enrutamiento VPLS).https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/no-irb-layer-2-copy-edit-bridge-domains.html

Para obtener una descripción detallada de cómo configurar un filtro de firewall de duplicación de puertos de capa 2, consulte Definición de un filtro de firewall de duplicación de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-configuring.html

Para obtener información detallada acerca de cómo puede usar los filtros de firewall de duplicación de puertos de capa 2 con enrutadores MX y conmutadores serie EX configurados como enrutadores perimetrales de proveedor (PE) o conmutadores PE, consulte Descripción de la creación de reflejo de puertos de capa 2 de interfaces lógicas de enrutadores PE.https://www.juniper.net/documentation/

en_US/junos/topics/concept/layer-2-services-port-mirroring-firewall-filters-on-pe-routers.html Para obtener información detallada acerca de la configuración de filtros de firewall en general (incluso en un entorno de capa 3), consulte la Guía del usuario de Políticas de enrutamiento, filtros de firewall y Controladores de tráfico.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.html

Creación de reflejo de paquetes recibidos o enviados en una interfaz lógica

Para reflejar el tráfico de capa 2 recibido o enviado en una interfaz lógica, aplique un filtro de firewall de duplicación de puertos a la entrada o salida de la interfaz.

También se puede aplicar un filtro de firewall de duplicación de puertos a una interfaz lógica Ethernet agregada. Para obtener más información, consulte Descripción de la creación de reflejo de puertos de capa 2 de interfaces Ethernet agregadas del enrutador PE.https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-services-port-mirroring-firewall-filters-on-aggregated-ethernet-interfaces.html

> **NOTA**: Si se aplican filtros de firewall de duplicación de puertos tanto en la entrada como en la salida de una interfaz lógica, se reflejan dos copias de cada paquete. Para evitar que el enrutador o conmutador reenvíe paquetes duplicados al mismo destino, puede habilitar la opción "mirror-once" para la duplicación de puertos de capa 2 en la instancia global para la familia de direcciones de paquetes de capa 2.

Duplicación de paquetes reenviados o inundados a una VLAN

Para reflejar el tráfico de capa 2 reenviado o inundado a una VLAN, aplique un filtro de firewall de duplicación de puertos a la entrada a la tabla de reenvío o a la tabla de inundación. Cualquier paquete recibido para la tabla de reenvío o inundación de VLAN y que coincida con las condiciones del filtro se refleja.

Para obtener más información acerca de las VLAN, consulte Descripción de los dominios de puente de capa 2 .https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-services-bridging-overview.html Para obtener información sobre el comportamiento de inundación en una VLAN, consulte Descripción del aprendizaje y reenvío de capa 2 para dominios de puente .https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-services-learning-and-forwarding-for-bridge-domains.html

> **NOTA**: Cuando se configura la creación de reflejo de puertos en cualquier interfaz bajo una VLAN, el paquete reflejado puede moverse a un analizador externo ubicado en VLAN diferentes.

Creación de reflejo de paquetes reenviados o inundados a una instancia de enrutamiento VPLS

Para reflejar el tráfico de capa 2 reenviado o inundado a una instancia de enrutamiento VPLS, aplique un filtro de firewall de duplicación de puertos a la entrada a la tabla de reenvío o a la tabla de inundación. Se refleja cualquier paquete recibido para la tabla de inundación o reenvío de la instancia de enrutamiento de VPLS y que coincida con la condición de filtro.

Para obtener más información acerca de las instancias de enrutamiento VPLS, consulte Configuración de una instancia de enrutamiento VPLS y Configuración de identificadores de VLAN para dominios de puente e instancias de enrutamiento VPLS.*Configuring a VPLS Routing Instance*https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-bridge-domains-and-vpls-routing-instances-configuring-vlan-ids-for.html Para obtener información sobre el comportamiento de inundación en VPLS, consulte la Biblioteca de VPN de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/index.html

Definición de un filtro de firewall de duplicación de puertos de capa 2

Para el tráfico del servicio de LAN privada virtual (VPLS) (o) y para las VPN de capa 2 con familia en enrutadores serie MX y solo en conmutadores serie EX, puede definir un filtro de firewall que especifique la creación de reflejo del puerto de capa 2 como la acción que debe realizarse si un paquete cumple las condiciones configuradas en el término del filtro de firewall.`family ethernet-switchingfamily vplsccc`

Puede utilizar un filtro de firewall de duplicación de puertos de capa 2 de las siguientes maneras:

- Para reflejar paquetes recibidos o enviados en una interfaz lógica.
- Para reflejar paquetes reenviados o inundados a una VLAN.
- Para reflejar paquetes reenviados o inundados a una instancia de enrutamiento VPLS.
- Para reflejar paquetes de entrada de interfaz de túnel solo a varios destinos.

Para obtener un resumen de los tres tipos de duplicación de puertos de capa 2 que puede configurar en un enrutador de la serie MX y en un conmutador de la serie EX, consulte Aplicación de los tipos de duplicación de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/concept/layer-2-services-port-mirroring-application.html

Para definir un filtro de firewall con una acción de duplicación de puertos de capa 2:

1. Habilite la configuración de filtros de firewall para paquetes de capa 2 que forman parte de una VLAN, una conexión cruzada de conmutación de capa 2 o un servicio de LAN privada virtual (VPLS):

```
[edit]
user@host# edit firewall family family
```

El valor de la opción puede ser , , o .familyethernet-switchingcccvpls

2. Habilite la configuración de un filtro de firewall:pm-filter-name

```
[edit firewall family family]
user@host# edit filter pm-filter-name
```

3. Habilite la configuración de un término de filtro de firewall:pm-filter-term-name

```
[edit firewall family family filter pm-filter-name]
user@host# edit term pm-filter-term-name
```

4. (Opcional) Especifique las condiciones de coincidencia del filtro de firewall en función de la dirección de origen de la ruta solo si desea reflejar un subconjunto de los paquetes de muestra.

   - Para obtener información detallada acerca de las condiciones de coincidencia del filtro del firewall de puente de capa 2 (que solo son compatibles con los enrutadores de la serie MX y los conmutadores de la serie EX), consulte Condiciones de coincidencia del filtro de firewall para el tráfico de puente de capa 2.*Firewall Filter Match Conditions for Layer 2 Bridging Traffic*

   - Para obtener información detallada acerca de las condiciones de coincidencia del filtro del firewall VPLS, consulte Condiciones de coincidencia del filtro de firewall para el tráfico VPLS.*Firewall Filter Match Conditions for VPLS Traffic*

   - Para obtener información detallada acerca de las condiciones de coincidencia del filtro de firewall de conexión cruzada de circuito (CCC) de capa 2, consulte Condiciones de coincidencia de filtro de firewall para tráfico de CCC de capa 2.*Firewall Filter Match Conditions for Layer 2 CCC Traffic*

NOTA: Si desea que todos los paquetes muestreados se consideren coincidentes (y que estén sujetos a las acciones especificadas en la instrucción), omita la instrucción por completo.thenfrom

5. Habilite la configuración de y para aplicar a los paquetes coincidentes:`actionaction-modifier`

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name]
user@host# edit then
```

6. Especifique las acciones que se deben realizar en los paquetes coincidentes:

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set action
```

El valor recomendado para el es .`actionaccept` Si no especifica una acción, o si omite la instrucción por completo, se aceptarán todos los paquetes que coincidan con las condiciones de la instrucción.`thenfrom`

7. Especifique la creación de reflejo del puerto de capa 2 o un grupo del próximo salto como:`action-modifier`

   - Para hacer referencia a las propiedades de creación de reflejo de puerto de capa 2 actualmente vigentes para el motor de reenvío de paquetes o PIC asociado con la interfaz física subyacente, utilice la instrucción:`port-mirror`

     ```
     [edit firewall family family filter pm-filter-name term pm-filter-term-name then]
     user@host# set port-mirror
     ```

   - Para hacer referencia a las propiedades de creación de reflejo de puertos de capa 2 configuradas en una instancia con nombre específica, utilice el modificador de acción port-mirror-instance :*pm-instance-name*

     ```
     [edit firewall family family filter pm-filter-name term pm-filter-term-name then]
     user@host# set port-mirror-instance pm-instance-name
     ```

     Si la interfaz física subyacente no está enlazada a una instancia con nombre de creación de reflejo de puerto de capa 2, sino que está implícitamente enlazada a la instancia global de creación de reflejo de puerto de capa 2, el tráfico en la interfaz lógica se refleja de acuerdo con las propiedades especificadas en la instancia con nombre a la que hace referencia el modificador de acción.`port-mirror-instance`

- Para hacer referencia a un grupo del salto siguiente que especifica las direcciones del salto siguiente (para enviar copias adicionales de paquetes a un analizador), utilice el modificador de acción `:next-hop-group` *pm-next-hop-group-name*

```
[edit firewall family family filter pm-filter-name term pm-filter-term-name then]
user@host# set next-hop-group pm-next-hop-group-name
```

  Para obtener información de configuración acerca de los grupos del próximo salto, consulte Definición de un grupo del siguiente salto para la creación de reflejo de puertos de capa 2.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-next-hop-group-configuring.html Si especifica un grupo de salto siguiente para la creación de reflejo de puertos de capa 2, el término filtro de firewall se aplica únicamente a la entrada de la interfaz de túnel.

8. Verifique la configuración mínima del filtro de firewall de duplicación de puertos de capa 2:

```
[edit firewall ... ]
user@host# top
[edit]
user@host# show firewall

family (ethernet-switching | ccc | vpls) { # Type of packets to mirror
    filter pm-filter-name { # Firewall filter name
        term pm-filter-term-name {
            from { # Do not specify match conditions based on route source address
            }
            then {
                action; # Recommended action is 'accept'
                action-modifier; # Three options for Layer 2 port mirroring
            }
        }
    }
}
```

  En la instrucción de término del filtro del firewall, el puede ser , , o `.then` *action-modifier* `port-mirror` `port-mirror-instance` `next-hop-group` *pm-next-hop-group-name*

Configuración del filtro de firewall independiente del protocolo para la creación de reflejo de puertos

En los enrutadores de la serie MX con MPC, puede configurar un filtro de firewall para reflejar los paquetes de capa 2 y capa 3 a nivel global y a nivel de instancia. Cuando se configura el espejo de

puerto en la entrada o salida, se copia el paquete que entra o sale de una interfaz y las copias se envían a la interfaz local para la supervisión local.

> **NOTA**: A partir de Junos OS versión 13.3R6, solo las interfaces MPC admiten la creación de reflejo de puertos.`family any` Las interfaces DPC no admiten archivos .`family any`

Normalmente, el filtro de firewall está configurado de tal manera que refleja los paquetes de capa 2 o capa 3 según la familia configurada en la interfaz. Sin embargo, en el caso de una interfaz de enrutamiento y puente integrados (IRB), los paquetes de capa 2 no se reflejan completamente porque las interfaces IRB están configuradas para reflejar solo paquetes de capa 3. En una interfaz de este tipo, puede configurar un filtro de firewall y parámetros de duplicación de puertos en la familia para garantizar que un paquete se refleje completamente, independientemente de si se trata de un paquete de capa 2 o de capa 3.**any**

> **NOTA**:
>
> - Para la creación de reflejo de puertos en una instancia, puede configurar una o más familias como , , , y simultáneamente para la misma instancia.**inetinet6cccvpls**
> - En el caso de la duplicación de puertos de capa 2, las etiquetas VLAN y los encabezados MPLS se conservan y se pueden ver en la copia duplicada a la salida.
> - Para la normalización de VLAN, la información antes de la normalización se ve para un paquete reflejado en la entrada. Del mismo modo, en la salida, la información después de la normalización se ve para el paquete reflejado.

Antes de empezar a configurar la creación de reflejo de puertos, debe configurar interfaces físicas válidas.

Para configurar un filtro de firewall independiente del protocolo para la creación de reflejo de puertos:

1. Configure un filtro de firewall global para reflejar el tráfico de salida, salida o entrada.

```
[edit firewall family any]
user@host# set filter filter-name {
    term term-name {
        then {
            port-mirror;
            accept;
        }
```

```
    }
}
```

2. Configure un filtro de firewall para reflejar el tráfico de una instancia.

```
[edit firewall family any]
user@host# set filter filter-name {
    term term-name {
        then {
            port-mirror-instance instance-name;
            accept;
        }
    }
}
```

3. Configure los parámetros de creación de reflejo para el tráfico de salida y de entrada.

```
[edit forwarding-options port-mirroring]
user@host# input {
    maximum-packet-length bytes
    rate rate;
}
family any {
    output {
        (next-hop-group group-name | interface interface-name);
    }
}
```

4. Configure los parámetros de creación de reflejo para una instancia. En esta configuración, puede especificar el resultado o el destino de los paquetes de capa 2 para que sean un grupo de próximo salto válido o una interfaz de capa 2.

```
[edit forwarding-options port-mirroring]
user@host#instance instance-name {
    family any{
        output {
            (next-hop-group group-name | interface interface-name);
        }
    }
}
```

5. Configure el filtro de firewall en la interfaz de entrada o salida en la que se transmiten los paquetes.

```
[edit interface interface-name unit]
user@host# filter {
    output filter-name;
    input filter-name;
}
```

Ejemplo: Duplicación del tráfico web de los empleados con un filtro de firewall

in this section

- Requisitos | 1217
- Descripción general | 1217
- Configurar | 1218
- Verificación | 1222

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador
- Junos 14.1X53-D20

Descripción general

in this section

- Topología | 1218

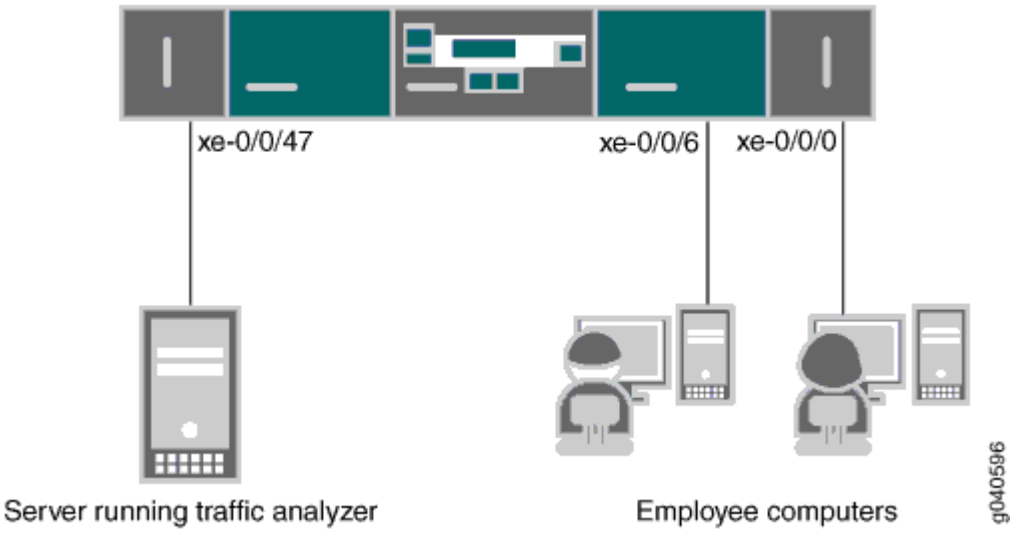
En este ejemplo, y sirven como conexiones para las computadoras de los empleados.`xe-0/0/0``xe-0/0/6` La interfaz está conectada a un dispositivo que ejecuta una aplicación analizadora.`xe-0/0/47`

En lugar de reflejar todo el tráfico, generalmente es deseable reflejar solo cierto tráfico. Este es un uso más eficiente de su ancho de banda y hardware y puede ser necesario debido a restricciones en estos activos. En este ejemplo solo se refleja el tráfico enviado desde los equipos de los empleados a la Web.

Topología

Figura 42 en la página 1218 muestra la topología de red de este ejemplo.

Figura 42: Ejemplo de topología de red para creación de reflejo de puerto local



Configurar

in this section

- Procedimiento | **1219**

Para especificar que el único tráfico que se reflejará es el tráfico enviado por los empleados a la Web, realice las tareas explicadas en esta sección. Para seleccionar este tráfico para la creación de reflejos, utilice un filtro de firewall para especificar este tráfico y dirigirlo a una instancia de creación de reflejo de puertos.

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la duplicación del puerto local del tráfico de los equipos de los empleados destinado a la Web, copie los comandos siguientes y péguelos en una ventana de terminal de conmutador:

```
[edit]
 set forwarding-options port-mirroring family inet output interface xe-0/0/47.0 next-hop
192.0.2.100/24
 set firewall family inet filter watch-employee term employee-to-corp from destination-address
192.0.2.16/24
 set firewall family inet filter watch-employee term employee-to-corp from source-address
192.0.2.16/24
 set firewall family inet filter watch-employee term employee-to-corp then accept
 set firewall family inet filter watch-employee term employee-to-web from destination-port 80
 set firewall family inet filter watch-employee term employee-to-web then port-mirror
 set interfaces xe-0/0/0 unit 0 family address 192.0.1.1/24
 set interfaces xe-0/0/6 unit 0 family address 192.0.1.2/24
 set interfaces xe-0/0/47 unit 0 family address 192.0.1.3/24
 set interfaces xe-0/0/0 unit 0 family inet filter input watch-employee
 set interfaces xe-0/0/6 unit 0 family inet filter input watch-employee
```

Procedimiento paso a paso

Para configurar la creación de reflejo del puerto local del tráfico de empleados a la web desde los dos puertos conectados a los equipos de los empleados:

1. Configure una instancia de duplicación de puertos, incluida la interfaz de salida y la dirección IP del dispositivo que ejecuta la aplicación del analizador como el próximo salto. (Configure solo la salida: la entrada proviene del filtro). También debe especificar que la réplica es para el tráfico IPv4 ().`family inet`

   ```
   [edit forwarding-options]
   user@switch# set forwarding-options port-mirroring family inet output interface xe-0/0/47.0
   next-hop 192.0.2.100/28
   ```

2. Configure un filtro de firewall IPv4 () llamado que incluya un término para hacer coincidir el tráfico enviado a la Web y enviarlo a la instancia de creación de reflejo de puertos.`family inetwatch-employee` No es necesario copiar el tráfico enviado a y procedente de la subred corporativa (destino o dirección

de origen de) , así que primero cree otro término para aceptar ese tráfico antes de que llegue al término que envía el tráfico web a la instancia:`192.0.nn.nn/24`

```
[edit firewall family inet]
er@switch# set filter watch-employee term employee-to-corp from destination-address
192.0.nn.nn/24
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.nn.nn/24
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror
```

3. Configure direcciones para las interfaces IPv4 conectadas a los equipos de los empleados y al dispositivo analizador:

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet address 192.0.1.1/24
user@switch# set xe-0/0/6 unit 0 family inet address 192.0.1.2/24
user@switch# set interfaces xe-0/0/47 unit 0 family address 192.0.1.3/24
```

4. Aplique el filtro de firewall a las interfaces apropiadas como filtro de entrada:

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family inet filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family inet filter input watch-employee
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show
forwarding-options {
    port-mirroring {
            employee-web-monitor    {
                output {
                    ip-address 192.0.2.100.0;
                    }
                }
```

```
            }
        }
    }
}
...
firewall family inet {
    filter watch-employee {
        term employee-to-corp {
            from {
                destination-address 192.0.2.16/24;
                source-address 192.0.2.16/24;
            }
            then accept {
        }
        term employee-to-web {
            from {
                destination-port 80;
            }
            then port-mirror;
        }
    }
}
...
interfaces {
    xe-0/0/0 {
        unit 0 {
            family inet {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    xe-0/0/6 {
        family inet {
            filter {
                input watch-employee;
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | 1222

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador se haya creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.

Acción

Puede comprobar que el analizador de espejo de puertos se ha configurado como se esperaba mediante el comando.`show forwarding-options port-mirroring`

```
user@switch> show forwarding-options port-mirroring
Instance Name: &global_instance
  Instance Id: 1
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination          Next-hop
    inet                up      xe-0/0/47.0          192.0.2.100
```

Significado

Este resultado muestra que la instancia de duplicación de puertos tiene una proporción de 1 (duplicación de cada paquete, la configuración predeterminada) y el tamaño máximo del paquete original que se reflejó (indica todo el paquete).`0` Si el estado de la interfaz de salida está inactivo o si la interfaz de salida no está configurada, el valor de estado será y la instancia no se programará para la creación de reflejo.`down`

Duplicación de puertos de capa 2 de interfaces lógicas de enrutador PE o conmutador de PE

Para un enrutador o conmutador configurado como dispositivo perimetral de proveedor (PE) en el borde orientado al cliente de una red de proveedor de servicios, puede aplicar un filtro de *firewall* de duplicación de puerto de capa 2 en los siguientes puntos de entrada y salida para reflejar el tráfico entre el enrutador o conmutador y los dispositivos perimetrales del cliente (CE), que normalmente también son enrutadores y conmutadores Ethernet.

Tabla 123 en la página 1224 describe las formas en que puede aplicar filtros de firewall de duplicación de puertos de capa 2 a un enrutador o conmutador configurado como dispositivo PE.

Tabla 123: Aplicación de filtros de firewall de duplicación de puertos de capa 2 en dispositivos PE

Punto de aplicación	Alcance de la creación de reflejo	Notas	Detalles de configuración
Interfaz lógica orientada al cliente de entrada	Paquetes que se originan en la red de un cliente proveedor de servicios, se envían primero a un dispositivo CE y se envían junto al dispositivo PE.	También puede configurar interfaces Ethernet agregadas entre dispositivos CE y PE para instancias de enrutamiento VPLS. El tráfico tiene un equilibrio de carga en todos los vínculos de la interfaz agregada. El tráfico recibido en una interfaz Ethernet agregada se reenvía a través de una interfaz diferente según una búsqueda de la dirección MAC de destino (DMAC): • Los paquetes destinados a un sitio local se envían fuera de la interfaz secundaria con equilibrio de carga. • Los paquetes destinados al sitio remoto se encapsulan y reenvían a través de una ruta de conmutación de etiquetas (LSP).	Consulte Aplicación de la creación de reflejo de puertos de capa 2 a una interfaz lógica.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-applying-logical-interface.html Para obtener más información acerca de las instancias de enrutamiento VPLS, consulte Configuración de una instancia de enrutamiento VPLS y Configuración de identificadores de VLAN para dominios de puente e instancias de enrutamiento VPLS.*Configuring a VPLS Routing Instance*https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-bridge-domains-and-vpls-routing-instances-configuring-vlan-ids-for.html

Tabla 123: Aplicación de filtros de firewall de duplicación de puertos de capa 2 en dispositivos PE *(Continued)*

Punto de aplicación	Alcance de la creación de reflejo	Notas	Detalles de configuración
Interfaz lógica de salida orientada al cliente	Paquetes de unidifusión reenviados por el dispositivo PE a otro dispositivo PE. Si aplica un filtro de duplicación de puertos a la salida de una interfaz lógica, solo se reflejan los paquetes de unidifusión.**NOTE:** Para reflejar paquetes de multidifusión, unidifusión desconocida y difusión, aplique un filtro a la entrada a la tabla de inundación de una instancia de enrutamiento VLAN o VPLS.		Consulte Aplicación de la creación de reflejo de puertos de capa 2 a una interfaz lógica.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-applying-logical-interface.html

Tabla 123: Aplicación de filtros de firewall de duplicación de puertos de capa 2 en dispositivos PE *(Continued)*

Punto de aplicación	Alcance de la creación de reflejo	Notas	Detalles de configuración
Entrada a una tabla de reenvío de VLAN o una tabla de inundación	Reenvío de tráfico o tráfico de inundación enviado a la VLAN desde un dispositivo CE.	El tráfico de reenvío e inundación suele estar compuesto por paquetes de difusión, paquetes de multidifusión, paquetes de unidifusión con una dirección MAC de destino desconocida o paquetes con una entrada MAC en la tabla de enrutamiento DMAC.	Consulte Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente."Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente" en la página 1231 Para obtener información sobre el comportamiento de inundación en VPLS, consulte la Biblioteca de VPN de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/index.html

Tabla 123: Aplicación de filtros de firewall de duplicación de puertos de capa 2 en dispositivos PE *(Continued)*

Punto de aplicación	Alcance de la creación de reflejo	Notas	Detalles de configuración
Entrada a una tabla de reenvío de instancia de enrutamiento VPLS o tabla de inundación	Reenvío de tráfico o tráfico de inundación enviado a la instancia de enrutamiento VPLS desde un dispositivo CE.		Consulte Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a una instancia de enrutamiento VPLS.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-port-mirroring-firewall-filter-applying-vpls-routing-instance.html Para obtener información sobre el comportamiento de inundación en VPLS, consulte la Biblioteca de VPN de Junos OS para dispositivos de enrutamiento.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-vpns/index.html

Duplicación de puertos de capa 2 de interfaces Ethernet agregadas de enrutador PE o conmutador PE

Una interfaz Ethernet agregada es un vínculo agregado virtual que consta de un conjunto de interfaces físicas de la misma velocidad y que funcionan en modo de conexión de vínculo dúplex completo. Puede configurar interfaces Ethernet agregadas entre dispositivos CE y dispositivos PE para instancias de enrutamiento VPLS. El tráfico tiene un equilibrio de carga en todos los vínculos de la interfaz agregada. Si se produce un error en uno o más vínculos de la interfaz agregada, el tráfico se cambia a los vínculos restantes.

Puede aplicar un *filtro de firewall* de duplicación de puertos de capa 2 a una interfaz Ethernet agregada para configurar la *duplicación de puertos* en la interfaz principal. Sin embargo, si alguna interfaz secundaria está enlazada a diferentes instancias de duplicación de puertos de capa 2, los paquetes recibidos en las interfaces secundarias se reflejarán en los destinos especificados por sus respectivas instancias de duplicación de puertos. Por lo tanto, varias interfaces secundarias pueden reflejar paquetes a múltiples destinos.

Por ejemplo, supongamos que la instancia de interfaz Ethernet agregada principal tiene dos interfaces secundarias:`ae0`

- `xe-2/0/0`
- `xe-3/1/2`

Supongamos que estas interfaces secundarias en están enlazadas a dos instancias diferentes de duplicación de puertos de capa 2:`ae0`

- : una instancia con nombre de duplicación de puertos de capa 2, enlazada a la interfaz secundaria.`pm_instance_Axe-2/0/0`
- : una instancia con nombre de duplicación de puertos de capa 2, enlazada a la interfaz secundaria.`pm_instance_Bxe-3/1/2`

Ahora supongamos que aplica un filtro de firewall de duplicación de puertos de capa 2 al tráfico de capa 2 enviado (unidad lógica en la instancia de interfaz Ethernet agregada).`ae0.000` Esto habilita la creación de reflejo de puertos en , lo que tiene el siguiente efecto en el procesamiento del tráfico recibido en las interfaces secundarias para las que se especifican propiedades de duplicación de puertos de capa 2:`ae0.0`

- Los paquetes recibidos se reflejan en las interfaces de salida configuradas en la instancia de duplicación de puertos.`xe-2/0/0pm_instance_A`
- Los paquetes recibidos se reflejan en las interfaces de salida configuradas en la instancia de duplicación de puertos.`xe-3/1/2.0pm_instance_B`

Dado que y puede especificar diferentes propiedades de selección de paquetes o propiedades de destino reflejado, los paquetes recibidos en y pueden reflejar diferentes paquetes a diferentes destinos.`pm_instance_Apm_instance_Bxe-2/0/0xe-3/1/2.0`

Aplicación de la creación de reflejo de puertos de capa 2 a una interfaz lógica

Puede aplicar un filtro de firewall de duplicación de puertos de capa 2 a la entrada o a la salida de una interfaz lógica, incluida una interfaz lógica Ethernet agregada. Sólo se reflejan los paquetes de la familia de tipos de direcciones especificada por la acción de filtrado.

Antes de comenzar, realice la tarea siguiente:

- Defina un filtro de firewall de duplicación de puertos de capa 2 para aplicarlo a la entrada a una interfaz lógica o a una interfaz lógica. Para obtener más información, consulte Definición de un filtro de firewall de duplicación de puertos de capa 2.

> **NOTA**: Esta tarea de configuración muestra dos filtros de firewall de duplicación de puertos de capa 2: un filtro aplicado al tráfico de entrada de la interfaz lógica y un filtro aplicado al tráfico de salida de la interfaz lógica.

Para aplicar un filtro de firewall de duplicación de puertos de capa 2 a una interfaz lógica de entrada o salida:

1. Configure la interfaz física subyacente para la interfaz lógica.

   a) Habilite la configuración de la interfaz física subyacente:

```
[edit]
user@host# edit interfaces interface-name
```

> **NOTA**: También se puede aplicar un filtro de firewall de duplicación de puertos a una interfaz lógica Ethernet agregada.

   b) Para las interfaces Gigabit Ethernet y las interfaces Ethernet agregadas configuradas para VPLS, habilite la recepción y transmisión de tramas etiquetadas con VLAN 802.1Q en la interfaz:

```
[edit interfaces interface-name]
user@host# set vlan-tagging
```

   c) Para las interfaces Ethernet que tienen habilitado el etiquetado y el puente de VLAN IEEE 802.1Q y que deben aceptar paquetes que llevan 0x8100 TPID o un TPID definido por el usuario, establezca el tipo de encapsulación de capa de vínculo lógico:

```
[edit interfaces interface-name]
user@host# set encapsulation extended-vlan-ethernet-switching
```

2. Configure la interfaz lógica a la que desea aplicar un filtro de firewall de duplicación de puertos de capa 2.

   a)

Especifique el número de unidad lógica:

```
[edit interfaces interface-name]
user@host# edit unit logical-unit-number
```

b) Para una interfaz Gigabit Ethernet o Ethernet agregada, enlace un ID de etiqueta VLAN 802.1Q a la interfaz lógica:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set vlan-id number
```

3. Habilite la especificación de un filtro de entrada o salida que se aplicará a los paquetes de capa 2 que forman parte del dominio de puente, las conexiones cruzadas de conmutación de capa 2 o el servicio de LAN privada virtual (VPLS).

   - Si el filtro se va a evaluar cuando se reciben paquetes en la interfaz:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set family family filter input pm-filter-name-a
```

   - Si el filtro debe evaluarse cuando se envían paquetes en la interfaz:

```
[edit interfaces interface-name unit logical-unit-number]
user@host# set family family filter output pm-filter-name-b
```

El valor de la opción puede ser *family*, , o `.ethernet-switchingcccvpls`

> **NOTA**: Si se aplican filtros de firewall de duplicación de puertos tanto en la entrada como en la salida de una interfaz lógica, se reflejan dos copias de cada paquete. Para evitar que el enrutador o conmutador reenvíe paquetes duplicados al mismo destino, incluya la instrucción opcional en el nivel de jerarquía.`mirror-once[edit forwarding-options]`

4. Compruebe la configuración mínima para aplicar un filtro de firewall de creación de reflejo de puerto de capa 2 con nombre a una interfaz lógica:

```
[edit interfaces interface-name unit logical-unit-number family family filter ... ]
user@host# top
[edit]
```

```
user@host# show interfaces

interfaces {
    interface-name {
        vlan-tagging;
        encapsulation extended-vlan-ethernet-switching;
        unit number { # Apply a filter to the input of this interface
            vlan-id number;
            family (ethernet-switching | ccc | vpls) {
                filter {
                    input pm-filter-for-logical-interface-input;
                }
            }
        }
        unit number { # Apply a filter to the output of this interface
            vlan-id number;
            family (ethernet-switching | ccc | vpls) {
                filter {
                    output pm-filter-for-logical-interface-output;
                }
            }
        }
    }
}
```

Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a un dominio de puente

Puede aplicar un filtro de firewall de duplicación de puertos de capa 2 al tráfico que se reenvía o inunda a un dominio de puente. Sólo se reflejan los paquetes del tipo de familia especificado y reenviados o inundados a ese dominio de puente.

Antes de comenzar, realice la tarea siguiente:

- Defina un filtro de firewall de duplicación de puertos de capa 2 que se aplicará al tráfico que se reenvía a un dominio de puente o se inunda a un dominio de puente. Para obtener más información, consulte Definición de un filtro de firewall de duplicación de puertos de capa 2.

NOTA: Esta tarea de configuración muestra dos filtros de firewall de duplicación de puertos Layer_2: Un filtro aplicado al tráfico de entrada de la tabla de reenvío del dominio del puente y un filtro aplicado al tráfico de entrada de la tabla de inundación del dominio del puente.

Para aplicar un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío o a la tabla de inundación de un dominio de puente:

1. Habilite la configuración del dominio de puente al que desea aplicar un filtro de firewall de duplicación de puertos de capa 2 para el tráfico reenviado o inundado:*bridge-domain-name*
   - Para un dominio de puente:

     ```
     [edit]
     user@host# edit bridge-domains bridge-domain-name
     ```

   - Para un dominio puente en una instancia de enrutamiento:

     ```
     [edit]
     user@host# edit routing-instances routing-instance-name bridge-domains bridge-domain-name
     user@host# set instance-type virtual-switch
     ```

     Para obtener información de configuración más detallada, consulte Configuración de una instancia de enrutamiento VPLS.*Configuring a VPLS Routing Instance*
2. Configure el dominio de puente:

   ```
   [edit]
   user@host# set domain-type bridge
   user@host# set interface interface-name
   user@host# set routing-interface routing-interface-name
   ```

   Para obtener información detallada sobre la configuración, consulte Configuración de un dominio de puente y Configuración de identificadores de VLAN para dominios de puente e instancias de enrutamiento VPLS.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-bridge-domains-configuring.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-bridge-domains-and-vpls-routing-instances-configuring-vlan-ids-for.html
3. Habilite la configuración del reenvío de tráfico en el dominio del puente:

   ```
   [edit ... bridge-domains bridge-domain-name]
   user@host# edit forwarding-options
   ```

4. Aplique un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío de dominio de puente o a la tabla de inundación.

- Para reflejar los paquetes que se reenvían al dominio del puente:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set filter input pm-filter-for-bd-ingress-forwarded
```

- Para reflejar los paquetes que se inundan al dominio del puente:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set flood input pm-filter-for-bd-ingress-flooded
```

5. Compruebe la configuración mínima para aplicar un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío o a la tabla de inundación del dominio del puente.

   a) Desplácese hasta el nivel de jerarquía en el que está configurado el dominio de puente:

   - `[edit]`
   - `[edit routing-instances routing-instance-name]`

   b) Mostrar las configuraciones de dominio de puente:

```
user@host# show bridge domains

bridge-domains {
    bridge-domain-name {
        instance-type virtual-switch; # For a bridge domain under a routing instance.
        domain-type bridge;
        interface interface-name;
        forwarding-options {
            filter { # Mirror ingress forwarded traffic
                input pm-filter-for-bd-ingress-forwarded;
            }
            flood { # Mirror ingress flooded traffic
                input pm-filter-for-bd-ingress-flooded;
            }
        }
    }
}
```

Aplicación de la creación de reflejo de puertos de capa 2 al tráfico reenviado o inundado a una instancia de enrutamiento VPLS

Puede aplicar un filtro de firewall de duplicación de puertos de capa 2 al tráfico que se reenvía o inunda a una instancia de enrutamiento VPLS. Solo se reflejan los paquetes del tipo de familia especificado y reenviados o inundados a esa instancia de enrutamiento VPLS.

Antes de comenzar, realice la tarea siguiente:

- Defina un filtro de firewall de duplicación de puertos de capa 2 que se aplicará al tráfico que se reenvía a una instancia de enrutamiento VPLS o se inunda a una VLAN. Para obtener más información, consulte Definición de un filtro de firewall de duplicación de puertos de capa 2.

> **NOTA**: Esta tarea de configuración muestra dos filtros de firewall de duplicación de puertos Layer_2: un filtro aplicado al tráfico de entrada de la tabla de reenvío de la instancia de enrutamiento VPLS y un filtro aplicado al tráfico de entrada de la tabla de inundación de la instancia de enrutamiento VPLS.

Para aplicar un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío o a la tabla de inundación de una instancia de enrutamiento VPLS:

1. Habilite la configuración de la instancia de enrutamiento VPLS a la que desea aplicar un filtro de firewall de duplicación de puertos de capa 2 para el tráfico reenviado o inundado:

```
[edit]
user@host# edit routing-instances routing-instance-name
user@host# set instance-type vpls
user@host# set interface interface-name
user@host# set route-distinguisher (as-number:number | ip-address:number)
user@host# set vrf-import [policy-names]
user@host# set vrf-export [policy-names]
user@host# edit protocols vpls
user@host@ ... vpls-configuration ...
```

   Para obtener información de configuración más detallada, consulte Configuración de una instancia de enrutamiento VPLS.*Configuring a VPLS Routing Instance*

2. Habilite la configuración del reenvío de tráfico en la instancia de enrutamiento VPLS:

```
[edit routing-instances routing-instance-name protocols vpls]
user@host# up 2
```

```
[edit routing-instances routing-instance-name]
user@host# edit forwarding-options
```

3. Aplique un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío de instancias de enrutamiento VPLS o a la tabla de inundación.

   - Para reflejar los paquetes que se reenvían a la instancia de enrutamiento VPLS:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# set filter input pm-filter-for-vpls-ri-forwarded
```

   - Para reflejar los paquetes que se inundan a la instancia de enrutamiento de VPLS:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# set flood input pm-filter-for-vpls-ri-flooded
```

4. Verifique la configuración mínima para aplicar un filtro de firewall de duplicación de puerto de capa 2 a la tabla de reenvío o tabla de inundación de la instancia de enrutamiento VPLS:

```
[edit routing-instances routing-instance-name forwarding-options]
user@host# top
[edit]
user@host# show routing-instances

routing-instances {
    routing-instance-name {
        instance-type vpls;
        interface interface-name;
        route-distinguisher (as-number:number | ip-address:number);
        vrf-import [policy-names];
        vrf-export [policy-names];
        protocols {
            vpls {
                ...vpls-configuration...
            }
        }
        forwarding-options {
            family vpls {
                filter { # Mirror ingress forwarded traffic
                    input pm-filter-for-vpls-ri-forwarded;
                }
```

```
                flood { # Mirror ingress flooded traffic
                    input pm-filter-for-vpls-ri-flooded;
                }
            }
        }
    }
}
```

Aplicación de la duplicación de puertos de capa 2 al tráfico reenviado o inundado a una VLAN

Puede aplicar un filtro de firewall de duplicación de puertos de capa 2 al tráfico que se reenvía o inunda a una VLAN. Solo se reflejan los paquetes del tipo de familia especificado y reenviados o inundados a esa VLAN.

Antes de comenzar, realice la tarea siguiente:

- Defina un filtro de firewall de duplicación de puertos de capa 2 que se aplicará al tráfico que se reenvía a una VLAN o se inunda a una VLAN. Para obtener más información, consulte Definición de un filtro de firewall de duplicación de puertos de capa 2.

> **NOTA**: Esta tarea de configuración muestra dos filtros de firewall de duplicación de puertos Layer_2: un filtro aplicado al tráfico de entrada de la tabla de reenvío de VLAN y un filtro aplicado al tráfico de entrada de la tabla de inundación de VLAN.

Para aplicar un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío o de inundación de una VLAN:

1. Habilite la configuración de la VLAN a la que desea aplicar un filtro de firewall de duplicación de puertos de capa 2 para el tráfico reenviado o inundado:***bridge-domain-name***
   - Para una VLAN:

```
[edit]
user@host# edit bridge-domains bridge-domain-name
```

- Para una VLAN en una instancia de enrutamiento:

```
[edit]
user@host# edit routing-instances routing-instance-name bridge-domains bridge-domain-name
user@host# set instance-type virtual-switch
```

Para obtener información de configuración más detallada, consulte Configuración de una instancia de enrutamiento VPLS.*Configuring a VPLS Routing Instance*

2. Configure la VLAN:

```
[edit]
user@host# set domain-type bridge
user@host# set interface interface-name
user@host# set routing-interface routing-interface-name
```

Para obtener información de configuración más detallada, consulte Configuración de un dominio de puente y Configuración de identificadores de VLAN para dominios de puente e instancias de enrutamiento VPLS.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-bridge-domains-configuring.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/task/configuration/layer-2-services-bridge-domains-and-vpls-routing-instances-configuring-vlan-ids-for.html

3. Habilite la configuración del reenvío de tráfico en la VLAN:

```
[edit ... bridge-domains bridge-domain-name]
user@host# edit forwarding-options
```

4. Aplique un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío de VLAN o a la tabla de inundación.

- Para reflejar los paquetes que se reenvían a la VLAN:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set filter input pm-filter-for-bd-ingress-forwarded
```

- Para reflejar los paquetes que se inundan a la VLAN:

```
[edit ... bridge-domains bridge-domain-name forwarding-options]
user@host# set flood input pm-filter-for-bd-ingress-flooded
```

5. Compruebe la configuración mínima para aplicar un filtro de firewall de duplicación de puertos de capa 2 a la tabla de reenvío o tabla de inundación de la VLAN.

   a) Desplácese hasta el nivel de jerarquía en el que está configurada la VLAN:

      - `[edit]`
      - `[edit routing-instances routing-instance-name]`

   b) Mostrar las configuraciones de VLAN:

```
user@host# show vlans

vlans {
    vlan-name {
        instance-type virtual-switch; # For a bridge domain under a routing instance.
        domain-type bridge;
        interface interface-name;
        forwarding-options {
            filter { # Mirror ingress forwarded traffic
                input pm-filter-for-bd-ingress-forwarded;
            }
            flood { # Mirror ingress flooded traffic
                input pm-filter-for-bd-ingress-flooded;
            }
        }
    }
}
```

Ejemplo: Creación de reflejo de puertos de capa 2 en una interfaz lógica

Los pasos siguientes describen un ejemplo en el que se utilizan la instancia global de duplicación de puertos y un filtro de firewall de duplicación de puertos para configurar la creación de reflejo de puertos de capa 2 para la entrada a una interfaz lógica.

1. Configure la VLAN, que contiene el analizador de paquetes externo, y la VLAN, que contiene el origen y el destino del tráfico de capa 2 que se está reflejando:**example-bd-with-analyzerexample-bd-with-traffic**

```
[edit]
bridge-domains {
    example-bd-with-analyzer { # Contains an external traffic analyzer
        vlan-id 1000;
```

```
        interface ge-2/0/0.0; # External analyzer
    }
    example-bd-with-traffic { # Contains traffic input and output interfaces
        vlan-id 1000;
        interface ge-2/0/6.0; # Traffic input port
        interface ge-3/0/1.2; # Traffic output port
    }
}
```

Suponga que la interfaz lógica está asociada con un analizador de tráfico externo que va a recibir paquetes duplicados de puerto.**ge-2/0/0.0** Supongamos que las interfaces lógicas y serán puertos de entrada y salida de tráfico, respectivamente.**ge-2/0/6.0ge-3/0/1.2**

2. Configure la duplicación de puertos de capa 2 para la instancia global, siendo el destino de la duplicación de puertos la interfaz VLAN asociada con el analizador externo (interfaz lógica en VLAN).**ge-2/0/0.0example-bd-with-analyzer** Asegúrese de habilitar la opción que permite aplicar filtros a este destino de duplicación de puertos:

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 10;
            run-length 5;
        }
        family ethernet-switching {
            output {
                interface ge-2/0/0.0; # Mirror packets to the external analyzer
                no-filter-check; # Allow filters on the mirror destination interface
            }
        }
    }
}
```

La instrucción en el nivel de jerarquía especifica que el muestreo comienza cada décimo paquete y que cada uno de los primeros cinco paquetes seleccionados debe reflejarse.`input[edit forwarding-options port-mirroring]`

La instrucción en el nivel de jerarquía especifica la interfaz de reflejo de salida para los paquetes de capa 2 en un entorno de puente:`output[edit forwarding-options port-mirroring family ethernet-switching]`

- La interfaz lógica , que está asociada con el analizador de paquetes externo, se configura como el destino de duplicación de puertos.**ge-2/0/0.0**

- La instrucción opcional permite configurar filtros en esta interfaz de destino.`no-filter-check`

3. Configure el filtro de firewall de duplicación de puerto de capa 2:**example-bridge-pm-filter**

```
[edit]
firewall {
    family ethernet-switching {
        filter example-bridge-pm-filter {
            term example-filter-terms {
                then {
                    accept;
                    port-mirror;
                }
            }
        }
    }
}
```

Cuando este filtro de firewall se aplica a la entrada o salida de una interfaz lógica para el tráfico en un entorno de puente, la creación de reflejo del puerto de capa 2 se realiza de acuerdo con las propiedades de muestreo de paquetes de entrada y las propiedades de destino de reflejo configuradas para la instancia global de creación de reflejo de puerto de capa 2. Dado que este filtro de firewall está configurado con la única acción de filtro predeterminada, todos los paquetes seleccionados por las propiedades (= y =) coinciden con este filtro.**acceptinputrate10run-length5**

4. Configure las interfaces lógicas:

```
[edit]
interfaces {
    ge-2/0/0 { # Define the interface to the external analyzer
        encapsulation ethernet-bridge;
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-2/0/6 { # Define the traffic input port
        flexible-vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit 0 {
            vlan-id 100;
            family ethernet-switching {
                filter {
```

```
                    input example-bridge-pm-filter; # Apply the port-mirroring firewall filter
                }
            }
        }
    }
    ge-3/0/1 { # Define the traffic output port
        flexible-vlan-tagging;
        encapsulation extended-vlan-bridge;
        unit 2 {
            vlan-tags outer 10 inner 20;
            family ethernet-switching;
        }
    }
}
```

Los paquetes recibidos en la interfaz lógica en VLAN se evalúan mediante el filtro de firewall de duplicación de puertos.**ge-2/0/6.0example-bd-with-trafficexample-bridge-pm-filter** El filtro de firewall actúa sobre el tráfico de entrada de acuerdo con las acciones de filtro configuradas en el propio filtro de firewall, más las propiedades de muestreo de paquetes de entrada y las propiedades de destino de reflejo configuradas en la instancia global de creación de reflejo de puertos:

- Todos los paquetes recibidos en se reenvían a su (supuesto) destino normal en la interfaz lógica.**ge-2/0/6.0ge-3/0/1.2**
- Por cada diez paquetes de entrada, se reenvían copias de los primeros cinco paquetes de esa selección al analizador externo en la interfaz lógica de la otra VLAN, .**ge-0/0/0.0example-bd-with-analyzer**

Si configura el filtro de firewall de duplicación de puertos para que realice la acción en lugar de la acción, todos los paquetes originales se descartan, mientras que las copias de los paquetes seleccionados mediante las propiedades globales de duplicación de puertos se envían al analizador externo.**example-bridge-pm-filterdiscardacceptinput**

Ejemplo: Duplicación de puertos de capa 2 para una VPN de capa 2

El siguiente ejemplo no es una configuración completa, pero muestra todos los pasos necesarios para configurar la duplicación de puertos en una L2VPN mediante .**family ccc**

1. Configure la VLAN , que contiene el analizador de paquetes externo:**port-mirror-bd**

```
[edit]
vlans {
    port-mirror-vlan { # Contains an external traffic analyzer
        interface ge-2/2/9.0; # External analyzer
```

```
    }
}
```

2. Configure la CCC VPN de capa 2 para conectar la interfaz lógica y la interfaz lógica:**ge-2/0/1.0ge-2/0/1.1**

```
[edit]
protocols {
    mpls {
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ge-2/0/1.0;
            interface ge-2/0/1.1;
        }
    }
}
```

3. Configure la duplicación de puertos de capa 2 para la instancia global, siendo el destino de la duplicación de puertos la interfaz VLAN asociada con el analizador externo (interfaz lógica en VLAN):**ge-2/2/9.0example-bd-with-analyzer**

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 1;
            maximum-packet-length 200;
        }
        family ccc {
            output {
                interface ge-2/2/9.0; # Mirror packets to the external analyzer
            }
        }
        instance {
            inst1 {
                input {
                    rate 1;
                    maximum-packet-length 300;
                }
```

```
                family ccc {
                    output {
                        interface ge-2/2/9.0;
                    }
                {
            }
        }
    }
}
```

4. Defina el filtro de firewall de duplicación de puertos de capa 2 para :**pm_filter_cccfamily ccc**

```
[edit]
firewall {
    family ccc {
        filter pm_filter_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
}
```

5. Aplique la instancia de réplica de puerto al chasis:

```
[edit]
chassis {
    fpc 2 {
        port-mirror-instance inst1;
    }
}
```

6. Configure la interfaz para las VLAN y configure la interfaz para la creación de reflejo de puertos con el filtro de firewall:**ge-2/2/9ge-2/0/1pm_filter_ccc**

```
[edit]
interfaces {
    ge-2/2/9 {
        encapsulation ethernet-bridge;
        unit 0 {
```

```
            family ethernet-switching;
        }
    }
    ge-2/0/1 {
        vlan-tagging;
        encapsulation extended-vlan-ccc;
        unit 0 {
            vlan-id 10;
            family ccc {
                filter {
                    input pm_filter_ccc;
                }
            }
        }
        unit 1 {
            vlan-id 20;
            family ccc {
                filter {
                    output pm_filter_ccc;
                }
            }
        }
    }
}
```

Ejemplo: Duplicación de puertos de capa 2 para una VPN de capa 2 con vínculos LAG

El siguiente ejemplo no es una configuración completa, pero muestra todos los pasos necesarios para configurar la duplicación de puertos en una L2VPN mediante vínculos Ethernet agregados.**family ccc**

1. Configure la VLAN , que contiene el analizador de paquetes externo:**port_mirror_bd**

```
[edit]
vlans {
    port_mirror_vlan { # Contains an external traffic analyzer
        interface ge-2/2/8.0; # External analyzer
    }
}
```

2. Configure la CCC VPN de capa 2 para conectar la interfaz y la interfaz :**ae0.0ae0.1**

```
[edit]
protocols {
    mpls {
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ae0.0;
            interface ae0.1;
        }
    }
}
```

3. Configure la duplicación de puertos de capa 2 para la instancia global, siendo el destino de la duplicación de puertos la interfaz VLAN asociada con el analizador externo (interfaz lógica en VLAN):**ge-2/2/9.0example_bd_with_analyzer**

```
[edit]
forwarding-options {
    port-mirroring {
        input {
            rate 1;
            maximum-packet-length 200;
        }
        family ccc {
            output {
                interface ge-2/2/8.0; # Mirror packets to the external analyzer
            }
        }
        instance {
            pm_instance_1 {
                input {
                    rate 1;
                    maximum-packet-length 300;
                }
                family ccc {
                    output {
                        interface ge-2/2/8.0;
                    }
```

```
                {
            }
        }
    }
}
```

4. Configure el filtro de firewall para :**pm_cccfamily ccc**

```
[edit]
firewall {
    family ccc {
        filter pm_ccc {
            term pm {
                then port-mirror;
            }
        }
    }
}
```

5. Aplique las interfaces Ethernet agregadas y la instancia de espejo de puerto al chasis:

```
[edit]
chassis {
    aggregated-devices {
        ethernet {
            device-count 10;
        }
    }
    fpc 2 {
        port-mirror-instance pm_instance_1;
    }
}
```

6. Configure las interfaces y (para Ethernet agregada) y (para la duplicación de puertos) con el filtro:**ae0ge-2/0/2ge-2/2/8pm_ccc**

```
[edit]
interfaces {
    ae0 {
        vlan-tagging;
```

```
        encapsulation extended-vlan-ccc;
        unit 0 {
            vlan-id 10;
            family ccc {
                filter {
                    input pm_ccc;
                }
            }
        }
        unit 1 {
            vlan-id 20;
            family ccc {
                filter {
                    output pm_ccc;
                }
            }
        }
    }
    ge-2/0/2 {
        gigether-options {
            802.3ad ae0;
        }
    }
    ge-2/2/8 {
        encapsulation ethernet-bridge;
        unit 0 {
            family ethernet-switching;
        }
    }
}
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
13.3R6	A partir de Junos OS versión 13.3R6, solo las interfaces MPC admiten la creación de reflejo de puertos.`family any`

Configuración de la duplicación de puertos para varios destinos

in this section

- Descripción de la creación de reflejo de puertos de capa 2 a múltiples destinos mediante grupos de salto siguiente | **1248**
- Definición de un grupo de salto siguiente en enrutadores de la serie MX para la duplicación de puertos | **1249**
- Ejemplo: Configuración de duplicación de múltiples puertos con grupos de salto en enrutadores serie M, MX y T | **1251**
- Ejemplo: Duplicación de puertos de capa 2 a múltiples destinos | **1256**

Descripción de la creación de reflejo de puertos de capa 2 a múltiples destinos mediante grupos de salto siguiente

En un enrutador de la serie MX y en un conmutador de la serie EX, puede reflejar el tráfico a varios destinos mediante la configuración de grupos de salto siguiente en filtros de firewall de duplicación de puertos de capa 2 aplicados a interfaces de túnel. La duplicación de paquetes a múltiples destinos también se conoce como *duplicación de puertos multipaquete,*

> **NOTA**: Junos OS versión 9.5 introdujo compatibilidad con la duplicación de puertos de capa 2 mediante grupos de salto siguiente en enrutadores de la serie MX, pero requirió la instalación de una PIC de túnel. A partir de la versión 9.6 de Junos OS, la creación de reflejo de puertos de capa 2 mediante grupos de salto siguiente en enrutadores de la serie MX no requiere PIC de túnel.

En los enrutadores de la serie MX y en los conmutadores de la serie EX, puede definir un filtro de firewall para duplicar paquetes a un grupo del salto siguiente. El grupo del salto siguiente puede contener miembros de capa 2, miembros de capa 3 y subgrupos que sean de lista de unidades (duplicación de paquetes en cada interfaz) o de carga equilibrada (creación de reflejo de paquetes en una de varias interfaces). El enrutador de la serie MX y el conmutador de la serie EX admiten hasta 30 grupos de salto siguiente. Cada grupo de salto siguiente admite hasta 16 direcciones de salto siguiente. Cada grupo del salto siguiente debe especificar al menos dos direcciones.

Para habilitar la creación de reflejo de puertos a los miembros de un grupo de salto siguiente, especifique el grupo de salto siguiente como la acción de filtro de un filtro de firewall y, a continuación, aplique el filtro de firewall a interfaces de túnel lógico () o interfaces de túnel virtual () en el enrutador de la serie MX o en el conmutador de la serie EX.`lt-vt-`

NOTA: No se admite el uso de subgrupos para equilibrar la carga del tráfico reflejado.

Definición de un grupo de salto siguiente en enrutadores de la serie MX para la duplicación de puertos

A partir de la versión 14.2, en enrutadores que contengan un circuito integrado específico de la aplicación (ASIC) de procesador de Internet II o un procesador de Internet de la serie T, puede enviar una copia de un paquete IP versión 4 (IPv4) o IP versión 6 (IPv6) desde el enrutador a una dirección de host externa o a un analizador de paquetes para su análisis. Esto se conoce como *duplicación de puertos*.

La duplicación de puertos es diferente del muestreo de tráfico. En el muestreo de tráfico, se envía al motor de enrutamiento una clave de muestreo basada en el encabezado IPv4. Allí, la clave se puede colocar en un archivo, o los paquetes cflowd basados en la clave se pueden enviar a un servidor cflowd. En la duplicación de puertos, todo el paquete se copia y se envía a través de una interfaz de salto siguiente.

Puede configurar el uso simultáneo del muestreo y la creación de reflejo de puertos, y establecer una frecuencia de muestreo y una longitud de ejecución independientes para los paquetes reflejados en puertos. Sin embargo, si se selecciona un paquete tanto para el muestreo como para la creación de reflejo de puertos, sólo se puede realizar una acción y la creación de reflejo de puertos tiene prioridad. Por ejemplo, si configura una interfaz para muestrear cada entrada de paquete a la interfaz y un filtro también selecciona el paquete para que se refleje en otra interfaz, solo surtirá efecto la creación de reflejo de puertos. Todos los demás paquetes que no coinciden con los criterios explícitos de duplicación de puertos de filtro siguen siendo muestreados cuando se reenvían a su destino final.

Los grupos de salto siguiente le permiten incluir la duplicación de puertos en varias interfaces.

En los enrutadores de la serie MX, puede reflejar el tráfico de entrada de la interfaz de túnel a varios destinos. Para esta forma de duplicación de puertos multipaquete, especifique dos o más destinos en un grupo de salto siguiente, defina un filtro de firewall que haga referencia al grupo de salto siguiente como acción de filtrado y, a continuación, aplique el filtro a una interfaz de túnel lógico) o interfaces de túnel virtual (en el enrutador de la serie MX.`lt-vt-`

Para definir un grupo de salto siguiente para una acción de filtro de firewall de duplicación de puertos de capa 2:

1. Habilite la configuración de las opciones de reenvío.

```
[edit]
user@host set forwarding-options port-mirroring family (inet | inet6) output
```

2. Habilite la configuración de un grupo de próximo salto para la creación de reflejo del puerto de capa 2.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output]
user@host# set next-hop-group next-hop-group-name
```

3. Especifique el tipo de direcciones que se utilizarán en la configuración del grupo del salto siguiente.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-
hop-group-name]
user@host# set group-type inet6
```

4. Especifique las interfaces de la ruta del próximo salto.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-
hop-group-name]
user@host# set interface logical-interface-name-1
user@host# set interface logical-interface-name-2
```

o

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-
hop-group-name]
user@host# set interface interface-name next-hop next-hop-address
```

El enrutador de la serie MX admite hasta 30 grupos de salto siguiente. Cada grupo de salto siguiente admite hasta 16 direcciones de salto siguiente. Cada grupo del salto siguiente debe especificar al menos dos direcciones. Puede ser una dirección IPv4 o IPv6.*next-hop-address*

5. (Opcional) Especifique el subgrupo del próximo salto.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-
hop-group-name]
user@host# set next-hop-subgroup subgroup-name interface interface-name next-hop next-hop-
address
```

6. Compruebe la configuración del grupo del próximo salto.

```
[edit forwarding-options port-mirroring ... family (inet | inet6) output next-hop-group next-
hop-group-name]
```

```
user@host# top
[edit]
user@host# show forwarding-options

...
next-hop-group next-hop-group-name {
    group-type inet6;
    interface logical-interface-name-1;
    interface interface-name{
        next-hop next-hop-address;
    }
    next-hop-subgroup subgroup-name{
        interface interface-name{
            next-hop next-hop-address;
        }
    }
}
...
```

Ejemplo: Configuración de duplicación de múltiples puertos con grupos de salto en enrutadores serie M, MX y T

Cuando necesite analizar tráfico que contenga más de un tipo de paquete, o desee realizar varios tipos de análisis en un único tipo de tráfico, puede implementar varios grupos de creación de reflejo de puertos y del próximo salto. Puede hacer hasta 16 copias de tráfico por grupo y enviar el tráfico a los miembros del grupo del próximo salto. Se puede configurar un máximo de 30 grupos en un enrutador en un momento dado. El tráfico duplicado de puerto se puede enviar a cualquier interfaz, excepto a SONET/SDH agregada, Ethernet agregada, interfaz de circuito cerrado (lo0) o administrativa ().**fxp0** Para enviar tráfico duplicado de puerto a varios servidores de flujo o analizadores de paquetes, puede utilizar la instrucción en el nivel de jerarquía.`next-hop-group`[`edit forwarding-options`]

Figura 43: Monitoreo activo del flujo: creación de reflejo de múltiples puertos con el diagrama de topología de grupos del próximo salto

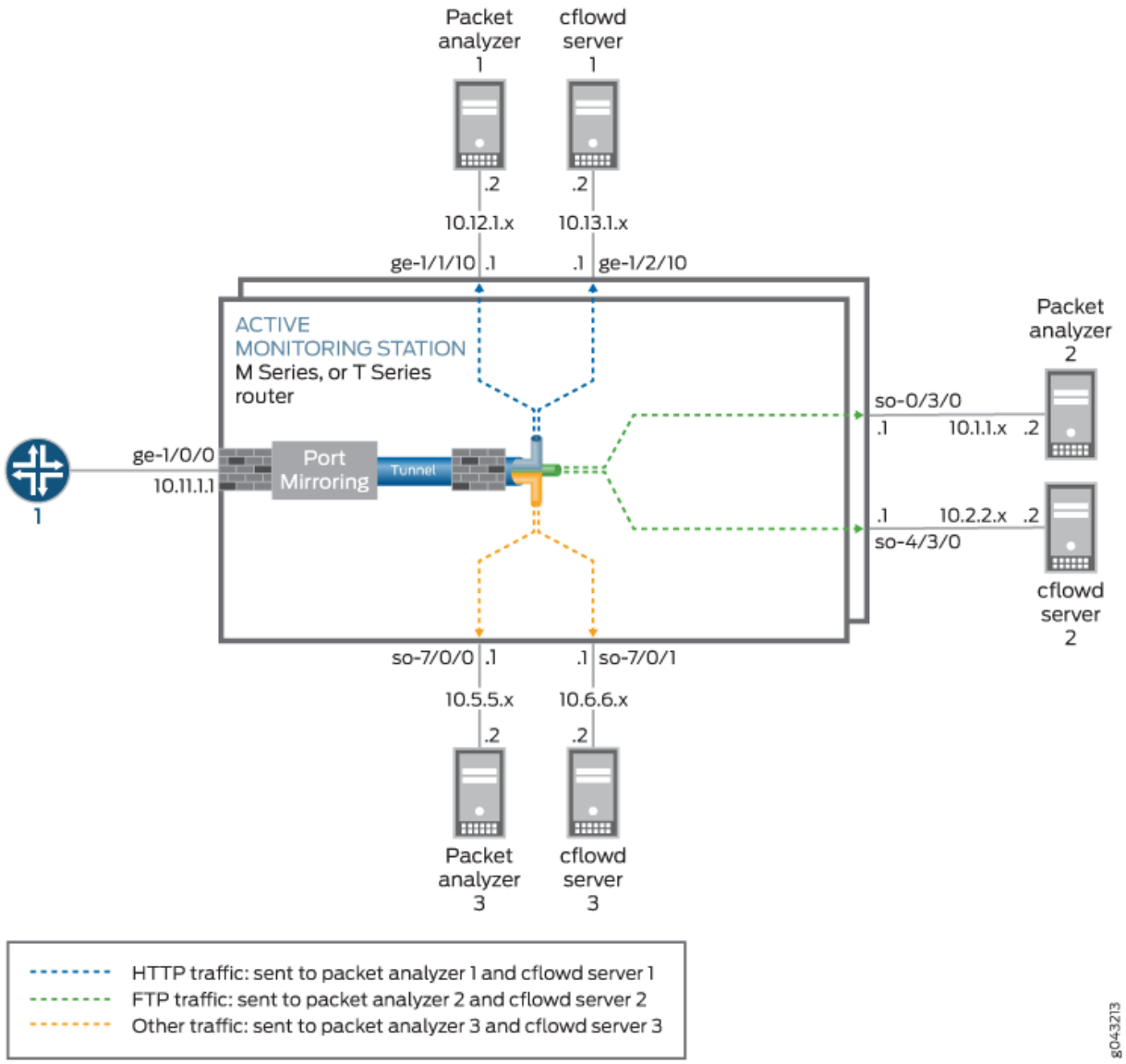


Figura 43 en la página 1252 muestra un ejemplo de cómo configurar la creación de reflejo de varios puertos con grupos del próximo salto. Todo el tráfico ingresa al enrutador de monitoreo en la interfaz ge-1/0/0. Un filtro de firewall cuenta y refleja el puerto de todos los paquetes entrantes a una PIC de servicios de túnel. Se aplica un segundo filtro a la interfaz del túnel y divide el tráfico en tres categorías: tráfico HTTP, tráfico FTP y el resto del tráfico. Los tres tipos de tráfico se asignan a tres grupos independientes del próximo salto. Cada grupo del salto siguiente contiene un par único de interfaces de salida que conducen a diferentes grupos de analizadores de paquetes y servidores de flujo.

NOTA: Las instancias habilitadas para reflejar paquetes a diferentes destinos desde el mismo PFE también utilizan diferentes parámetros de muestreo para cada instancia. Cuando configuramos la duplicación de puertos de capa 2 tanto con la duplicación de puertos global como con la duplicación de puertos basada en instancias, las instancias de nivel PIC anularán el nivel de FPC y el nivel de FPC anulará la instancia global.

```
[edit]
interfaces {
                   ge-1/0/0 { # This is the input interface where packets enter the router.
        unit 0 {
            family inet {
                filter {
                                                input mirror_pkts; # Here is where you apply the first
filter.
                }
                address 10.11.1.1/24;
            }
        }
    }
                   ge-1/1/0 { # This is an exit interface for HTTP packets.
        unit 0 {
            family inet {
                address 10.12.1.1/24;
            }
        }
    }
                   ge-1/2/0 { # This is an exit interface for HTTP packets.
        unit 0 {
            family inet {
                address 10.13.1.1/24;
            }
        }
    }
                   so-0/3/0 { # This is an exit interface for FTP packets.
        unit 0 {
            family inet {
                address 10.1.1.1/30;
            }
        }
```

```
    }
                    so-4/3/0 { # This is an exit interface for FTP packets.
        unit 0 {
            family inet {
                address 10.2.2.1/30;
            }
        }
    }
                    so-7/0/0 { # This is an exit interface for all remaining packets.
        unit 0 {
            family inet {
                address 10.5.5.1/30;
            }
        }
    }
                    so-7/0/1 { # This is an exit interface for all remaining packets.
        unit 0 {
            family inet {
                address 10.6.6.1/30;
            }
        }
    }
                    vt-3/3/0 { # The tunnel interface is where you send the port-mirrored traffic.
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet {
                filter {
                                        input collect_pkts;  # This is where you apply the
second firewall filter.
                }
            }
        }
    }
}
forwarding-options {
                    port-mirroring { # This is required when you configure next-hop groups.
        family inet {
            input {
                                    rate 1; # This port-mirrors all packets (one copy for every
packet received).
            }
```

```
                                output { # Sends traffic to a tunnel interface to enable
multiport mirroring.
                interface vt-3/3/0.1;
                no-filter-check;
            }
        }
    }
    next-hop-group ftp-traffic { # Point-to-point interfaces require you to specify the
        interface so-4/3/0.0; # interface name.
        interface so-0/3/0.0;
    }
    next-hop-group http-traffic { # Configure a next hop for all multipoint interfaces.
        interface ge-1/1/0.0 {
            next-hop 10.12.1.2;
        }
        interface ge-1/2/0.0 {
            next-hop 10.13.1.2;
        }
    }
    next-hop-group default-collect {
        interface so-7/0/0.0;
        interface so-7/0/1.0;
    }
}
firewall {
    family inet {
                        filter mirror_pkts { # Apply this filter to the input interface.
            term catch_all {
                then {
                    count input_mirror_pkts;
                                        port-mirror; # This action sends traffic to be copied
and port-mirrored.
                }
            }
        }
                        filter collect_pkts { # Apply this filter to the tunnel interface.
                              term ftp-term { # This term sends FTP traffic to an FTP next-hop
group.
                from {
                    protocol ftp;
                }
                                    then next-hop-group ftp-traffic;
            }
```

```
                                term http-term { # This term sends HTTP traffic to an HTTP next-
hop group.
                 from {
                     protocol http;
                 }
                                    then next-hop-group http-traffic;
             }
                                term default { # This sends all remaining traffic to a final next-
hop group.
                                    then next-hop-group default-collectors;
             }
         }
     }
}
```

Ejemplo: Duplicación de puertos de capa 2 a múltiples destinos

En los enrutadores de la serie MX, puede reflejar el tráfico a varios destinos mediante la configuración de grupos de salto siguiente en filtros de firewall de duplicación de puertos de capa 2 aplicados a interfaces de túnel.

1. Configure el chasis para admitir servicios de túnel en PIC 0 en FPC 2. Esta configuración incluye dos interfaces de túnel lógico en FPC 2, PIC 0, puerto 10.

```
[edit]
chassis {
    fpc 2 {
        pic 0 {
            tunnel-services {
                bandwidth 1g;
            }
        }
    }
}
```

2. Configure las interfaces físicas y lógicas para tres dominios de puente y una CCC VPN de capa 2:

   - El dominio de puente abarcará las interfaces lógicas y .**bdge-2/0/1.0ge-2/0/1.1**
   - El dominio de puente abarcará las interfaces lógicas y .**bd_next_hop_groupge-2/2/9.0ge-2/0/2.0**
   - El dominio de puente utilizará la interfaz de túnel lógico.**bd_port_mirrorlt-2/0/10.2**

- La CCC VPN de capa 2 conectará interfaces lógicas y .**if_switchge-2/0/1.2lt-2/0/10.1**

```
[edit]
interfaces {
    ge-2/0/1 {
        flexible-vlan-tagging;
        encapsulation flexible-ethernet-services;
        unit 0 { # An interface on bridge domain 'bd'.
            encapsulation vlan-bridge;
            vlan-id 200;
            family bridge {
                filter {
                    input pm_bridge;
                }
            }
        }
        unit 1 { # An interface on bridge domain 'bd'.
            encapsulation vlan-bridge;
            vlan-id 201;
            family bridge {
                filter {
                    input pm_bridge;
                }
            }
        }
        unit 2 {
            encapsulation vlan-ccc;
            vlan-id 1000;
        }
    }
    ge-2/0/2 { # For 'bd_next_hop_group'
        encapsulation ethernet-bridge;
        unit 0 {
            family bridge;
        }
    }
    lt-2/0/10 {
        unit 1 {
            encapsulation ethernet-ccc;
            peer-unit 2;
        }
        unit 2 {
```

```
            encapsulation ethernet-bridge;
            peer-unit 1;
            family bridge {
                filter {
                    output redirect_to_nhg;
                }
            }
        }
    }
    ge-2/2/9 {
        encapsulation ethernet-bridge;
        unit 0 { # For 'bd_next_hop_group'
            family bridge;
        }
    }
}
```

3. Configure los tres dominios de puente y el CCC de conmutación VPN de capa 2:

   - El dominio de puente abarca las interfaces lógicas y .**bdge-2/0/1.0ge-2/0/1.1**
   - El dominio de puente abarca las interfaces lógicas y .**bd_next_hop_groupge-2/2/9.0ge-2/0/2.0**
   - El dominio de puente utiliza la interfaz de túnel lógico.**bd_port_mirrorlt-2/0/10.2**
   - El CCC VPN de capa 2 conecta las interfaces y .**if_switchge-2/0/1.2lt-2/0/10.1**

```
[edit]
bridge-domains {
    bd {
        interface ge-2/0/1.0;
        interface ge-2/0/1.1;
    }
    bd_next_hop_group {
        interface ge-2/2/9.0;
        interface ge-2/0/2.0;
    }
    bd_port_mirror {
        interface lt-2/0/10.2;
    }
}
protocols {
    mpls {
```

```
        interface all;
    }
    connections {
        interface-switch if_switch {
            interface ge-2/0/1.2;
            interface lt-2/0/10.1;
        }
    }
}
```

Para obtener información detallada acerca de la configuración de la conexión CCC para conexiones cruzadas de conmutación de capa 2, consulte la Guía del usuario de aplicaciones MPLS.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-mpls-applications/config-guide-mpls-applications.html

4. Configure las opciones de reenvío:

   - Configure las propiedades globales de creación de reflejo de puertos para reflejar el tráfico a una interfaz en el dominio del puente .**family vplsbd_port_mirror**

   - Configure el grupo del próximo salto para reenviar el tráfico de capa 2 al dominio del puente .**nhg_mirror_to_bdbd_next_hop_group**

   El filtro de firewall de duplicación de puertos hará referencia a ambas opciones de reenvío:

```
[edit]
forwarding-options {
    port-mirroring { # Global port mirroring properties.
        input {
            rate 1;
        }
        family vpls {
            output {
                interface lt-2/0/10.2; # Interface on 'bd_port_mirror' bridge domain.
                no-filter-check;
            }
        }
    }
    next-hop-group nhg_mirror_to_bd { # Configure a next-hop group.
        group-type layer-2; # Specify 'layer-2' for Layer 2; default 'inet' is for Layer 3.
        interface ge-2/0/2.0; # Interface on 'bd_next_hop_group' bridge domain.
        interface ge-2/2/9.0; # Interface on 'bd_next_hop_group' bridge domain.
```

```
    }
}
```

5. Configure dos filtros de firewall de duplicación de puertos de capa 2 para el tráfico:**family bridge**

   - : envía todo el tráfico al destino global de creación de reflejo del puerto.**filter_pm_bridgefamily bridge**
   - : envía todo el tráfico al grupo final del próximo salto .**filter_redirect_to_nhgfamily bridgenhg_mirror_to_bd**

   Los filtros de firewall de espejado de puerto de capa 2 para el tráfico se aplican al tráfico en una interfaz física configurada con encapsulación .**family bridgeethernet-bridge**

```
[edit]
firewall {
    family bridge {
        filter filter_pm_bridge {
            term term_port_mirror {
                then port-mirror;
            }
        }
        filter filter_redirect_to_nhg {
            term term_nhg {
                then next-hop-group nhg_mirror_to_bd;
            }
        }
    }
}
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
14.2	A partir de la versión 14.2, en enrutadores que contengan un circuito integrado específico de la aplicación (ASIC) de procesador de Internet II o un procesador de Internet de la serie T, puede enviar una copia de un paquete IP versión 4 (IPv4) o IP versión 6 (IPv6) desde el enrutador a una dirección de host externa o a un analizador de paquetes para su análisis.

Configuración de la duplicación de puertos para destinos remotos

in this section

- Espejado de puerto de capa 2 a destino remoto mediante el uso de destino como VLAN | 1261
- Espejado de puertos de capa 2 de configuración a una VLAN remota | 1261
- Ejemplo: Configuración de la duplicación de puertos de capa 2 para VLAN remota | 1265

Espejado de puerto de capa 2 a destino remoto mediante el uso de destino como VLAN

Configurar la creación de reflejo de puertos en un conmutador EX9200 para enviar copias del tráfico a un destino de salida, como una interfaz, una instancia de enrutamiento o una VLAN; Y para el tráfico de entrada, puede configurar un término de filtro de firewall con varias condiciones y acciones de coincidencia.

Cuando se configura la VLAN como destino de salida en una configuración de duplicación de puertos, el tráfico de cada sesión de duplicación de puertos se transfiere a través de una VLAN especificada por el usuario que está dedicada para esa sesión de creación de reflejo en todos los conmutadores participantes. El tráfico reflejado se copia en esa VLAN (también denominada VLAN espejo) y se reenvía a interfaces, que son miembros de la VLAN reflejada. Las interfaces de destino, que son miembros de la VLAN reflejada, pueden abarcar varios conmutadores de la red, siempre que se utilice la misma VLAN de espejado remoto para una sesión de espejado en todos los conmutadores.

Puede usar la acción o en la configuración del filtro de firewall cuando refleje el tráfico a destinos remotos configurando una VLAN como destino de salida de duplicación de puertos.`port-mirror``port-mirror-instance`

Espejado de puertos de capa 2 de configuración a una VLAN remota

in this section

- Configuración de la duplicación de puertos en una VLAN remota | 1262

Los conmutadores EX9200 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para supervisión local o a una VLAN para supervisión remota. Puede utilizar la creación de reflejo para copiar los siguientes paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o salen de una VLAN

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Deshabilite la creación de reflejo de puertos que haya configurado cuando no los esté utilizando.
- Especifique interfaces individuales como entrada en lugar de especificar todas las interfaces como entrada en una configuración de creación de reflejo de puerto.
- Limite la cantidad de tráfico reflejado de la siguiente manera:
  - Uso de muestreo estadístico.
  - Establecer ratios para seleccionar muestras estadísticas.
  - Uso de filtros de firewall.

Configuración de la duplicación de puertos en una VLAN remota

Para filtrar los paquetes que se reflejarán en una instancia de creación de reflejo de puertos, cree la instancia y, a continuación, utilícela como acción en el filtro de firewall. Puede usar filtros de firewall en configuraciones de creación de reflejo local y remota.

Si se usa la misma instancia de duplicación de puerto en varios filtros o términos, los paquetes se copian en el puerto de salida de duplicación de puerto o en la VLAN de duplicación de puerto solo una vez.

Para filtrar el tráfico reflejado, cree una instancia de creación de reflejo de puertos en el nivel de jerarquía y, a continuación, cree un filtro de firewall.`[edit forwarding-options]` El filtro puede usar cualquiera de las condiciones de coincidencia disponibles y debe tenerlo como acción.`port-mirror-instance` *`instance-name`* Esta acción en la configuración del filtro del firewall proporciona la entrada a la instancia de duplicación de puertos.

Para configurar una instancia de creación de reflejo de puerto con filtros de firewall:

1. Configure el nombre de la instancia de duplicación de puertos y establezca el destino de salida en una VLAN:

```
[edit forwarding-options]
user@switch# set port-mirroring instance instance-name output vlan (vlan-ID | vlan-name)
```

Por ejemplo, configure una instancia de duplicación de puertos y establezca el destino de salida en un ID de VLAN:`employee-monitor999`

```
[edit forwarding-options]
user@switch# set port-mirroring instance employee-monitor output vlan 999
```

2. Cree un filtro de firewall utilizando cualquiera de las condiciones de coincidencia disponibles y asigne el nombre de instancia de duplicación de puertos como una acción en la configuración del filtro de firewall.

```
[edit firewall family ethernet-switching]
user@switch set filter filter-name term term-name from match-condition
user@switch set filter filter-name term term-name then match-condition
user@switch# set filter filter-name term term-namethen port-mirror-instance instance-name
```

Por ejemplo, cree un filtro de firewall llamado con dos términos y , y asigne el término a la instancia de duplicación de puertos:`example-filterno-analyzerto-analyzerto-analyzeremployee-monitor`

a) Cree el primer término para definir el tráfico que no debe pasar a través de la instancia de creación de reflejo de puertos: `employee-monitor`

```
[edit firewall family ethernet-switching]
user@switch# set filter (Firewall Filters) example-filter term no-analyzer from source-
address 192.0.2.14
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer from protocol tcp
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term no-analyzer then accept
```

b) Cree el segundo término para definir el tráfico que debe pasar a través de la instancia de duplicación de puertos:`employee-monitor`

```
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer from destination-port 80
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then port-mirror-instance employee-monitor
[edit firewall family ethernet-switching]
user@switch# set filter example-filter term to-analyzer then accept
```

3. Aplique el filtro de firewall a una interfaz o VLAN que proporcione entrada a la instancia de creación de reflejo de puertos.

   Para aplicar un filtro de firewall a una interfaz:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching filer (input | output) filter-name
```

   Para aplicar un filtro de firewall a una VLAN:

```
[edit]
user@switch# set vlan (vlan-ID or vlan-name) filter (input | output) filter-name
```

   Por ejemplo, para aplicar el filtro de firewall a la interfaz ge-0/0/1:`example-filter`

```
[edit]
user@switch# set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input example-filter
```

   Por ejemplo, para aplicar el filtro a la VLAN:`example-filtersource-vlan`

```
[edit]
user@switch# set vlan source-vlan filter input example-filter
```

Ejemplo: Configuración de la duplicación de puertos de capa 2 para VLAN remota

in this section

- Requisitos | **1266**
- Descripción general y topología | **1266**
- Duplicación del tráfico de empleados a la web para análisis remoto | **1268**
- Verificación | **1273**

Los conmutadores EX9200 permiten configurar la creación de reflejo para enviar copias de paquetes a una interfaz local para supervisión local o a una VLAN para supervisión remota. Puede utilizar la creación de reflejo para copiar estos paquetes:

- Paquetes que entran o salen de un puerto
- Paquetes que entran o existen en una VLAN

Puede analizar el tráfico reflejado mediante una aplicación de analizador de protocolos que se ejecute en una estación de supervisión remota si envía tráfico reflejado a una VLAN de analizador.

En este tema se incluyen dos ejemplos relacionados en los que se describe cómo reflejar el tráfico que entra en los puertos del conmutador a la VLAN para que pueda realizar análisis desde una estación de supervisión remota.`remote-analyzer` El primer ejemplo muestra cómo reflejar todo el tráfico que entra en los puertos conectados a las computadoras de los empleados. El segundo ejemplo muestra el mismo escenario, pero incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

MEJORES PRÁCTICAS: Refleje solo los paquetes necesarios para reducir el impacto potencial en el rendimiento. Le recomendamos que:

- Deshabilite las sesiones de creación de reflejo configuradas cuando no las esté utilizando.
- Especifique interfaces individuales como entrada para los analizadores en lugar de especificar todas las interfaces como entrada.
- Limite la cantidad de tráfico reflejado mediante filtros de firewall.

En este ejemplo se describe cómo configurar la creación de reflejo remota:

Requisitos

Antes de configurar la creación remota de reflejos, asegúrese de que:

- Tienes una comprensión de los conceptos de reflejo.
- Las interfaces que utilizará la duplicación de puertos como interfaces de salida se han configurado en el conmutador.

Descripción general y topología

in this section

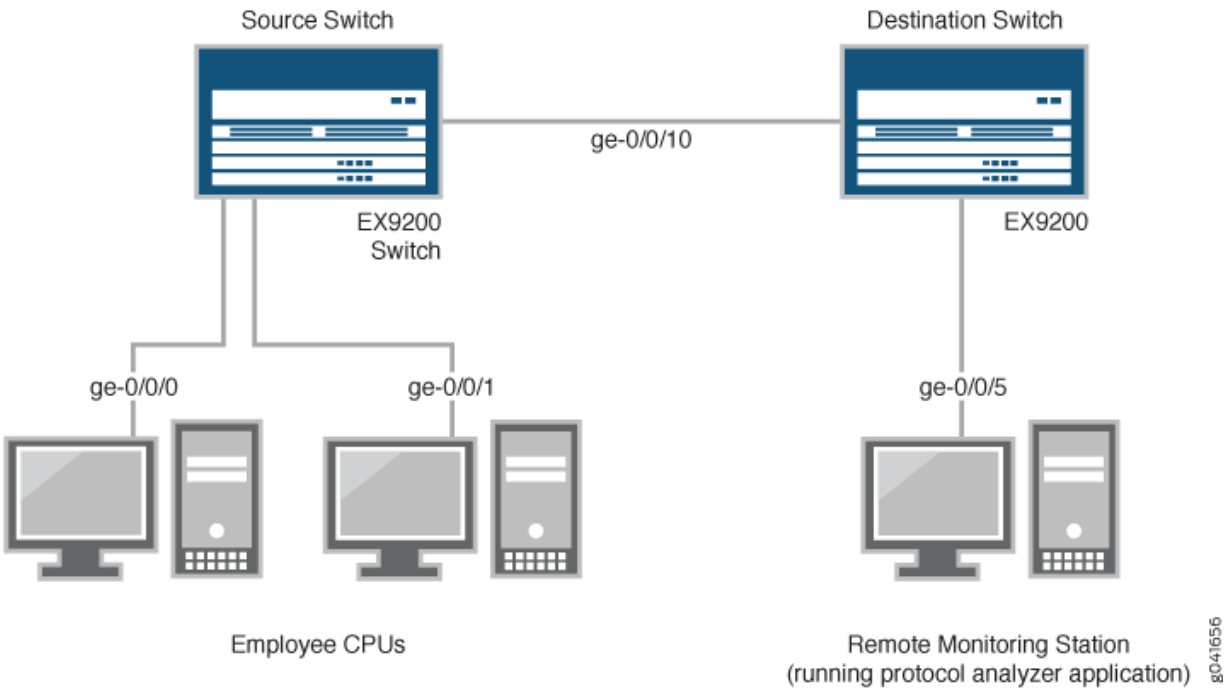
- Topología | **1267**

En este tema se incluyen dos ejemplos relacionados en los que se describe cómo configurar la creación de reflejo en la VLAN para que el análisis se pueda realizar desde una estación de supervisión remota.`remote-analyzer` En el primer ejemplo se muestra cómo configurar un conmutador para reflejar todo el tráfico de los equipos de los empleados. El segundo ejemplo muestra el mismo escenario, pero la configuración incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

Figura 44 en la página 1267 muestra la topología de red para estos dos escenarios de ejemplo.

Topología

Figura 44: Ejemplo de topología de red de espejado remoto



En este ejemplo:

1. La interfaz ge-0/0/0 es una interfaz de capa 2 y la interfaz ge-0/0/1 es una interfaz de capa 2 (ambas interfaces en el conmutador de origen) que sirven como conexiones para los equipos de los empleados.

2. La interfaz ge-0/0/10 es una interfaz de capa 2 que conecta el conmutador de origen al conmutador de destino.

3. La interfaz ge-0/0/5 es una interfaz de capa 2 que conecta el conmutador de destino a la estación de monitoreo remoto.

4. La VLAN está configurada en todos los conmutadores de la topología para transportar el tráfico reflejado.`remote-analyzer`

Duplicación del tráfico de empleados a la web para análisis remoto

in this section

- Procedimiento | 1268

Para configurar la creación de reflejo de puertos para el análisis de tráfico remoto del tráfico de empleados a web, realice estas tareas:

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la duplicación de puertos para reflejar el tráfico de empleados a la Web externa, copie los siguientes comandos y péguelos en la ventana terminal del conmutador:

- Copie y pegue los siguientes comandos en la ventana terminal del conmutador de origen:

```
[edit]
set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set firewall family ethernet-switching filter watch-employee term employee-to-corp from
destination-address 192.0.2.16/28
 set firewall family ethernet-switching filter watch-employee term employee-to-corp from
source-address 192.0.2.16/28
 set firewall family ethernet-switching filter watch-employee term employee-to-corp then
accept
 set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
 set firewall family ethernet-switching filter watch-employee term employee-to-web then port-
mirror-instance employee-web-monitor
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
 set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

- Copie y pegue los siguientes comandos en la ventana terminal del conmutador de destino:

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode access
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members 999
```

Procedimiento paso a paso

Para configurar la duplicación de puertos de todo el tráfico de los dos puertos conectados a las computadoras de los empleados a la VLAN para su uso desde una estación de monitoreo remota:`remote-analyzer`

1. En el conmutador de origen:

   1. Configure la instancia de creación de reflejo de puertos:`employee-web-monitor`

      ```
      [edit ]
      user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode access
      user@switch# set forwarding-options port-mirroring instance employee-web-monitor output
      vlan 999
      ```

   2. Configure el ID de VLAN para la VLAN:`remote-analyzer`

      ```
      [edit vlans]
      user@switch# set remote-analyzer vlan-id 999
      ```

   3. Configure la interfaz para asociarla con la VLAN:`remote-analyzer`

      ```
      [edit interfaces]
      user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
      ```

   4. Configure el filtro de firewall llamado :`watch-employee`

      ```
      [edit firewall family ethernet-switching]
      user@switch# set filter watch-employee term employee-to-corp from destination-address
      ```

```
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

En esta configuración, el término define que se puede aceptar que el tráfico desde la dirección de destino y la dirección de origen pase a través del conmutador, y el término define que el tráfico desde el puerto debe enviarse a la instancia de creación de reflejo de puerto.`employee-to-corp192.0.2.16/28192.0.2.16/28employee-to-web80employee-web-monitor`

5. Aplique el filtro de firewall a las interfaces de empleados:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

2. En el conmutador de destino:

- Configure el ID de VLAN para la VLAN:`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

- Configure la interfaz en el conmutador de destino para el modo de acceso y asóciela a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

- Configure la interfaz conectada al conmutador de destino para el modo de acceso y asóciela a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode access
user@switch# set ge-0/0/5 unit 0 family ethernet-switching vlan members 999
```

Resultados

Compruebe los resultados de la configuración en el conmutador de origen:

```
[edit]
user@switch> show
interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
}
firewall {
     family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
                from {
                    source-address {
```

```
                        192.0.2.16/28;
                    }
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then accept;
            }
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
            }
        }
    }
}
 forwarding-options {
    analyzer employee-web-monitor {
        output {
            vlan {
                999;
            }
        }
    }
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Compruebe los resultados de la configuración en el conmutador de destino:

```
[edit]
user@switch> show
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
interfaces {
    ge-0/0/10 {
```

```
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode access;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
}
```

Verificación

in this section

- Comprobación de que la instancia de creación de reflejo de puertos se haya creado correctamente | **1273**

Para confirmar que la configuración funcione correctamente, realice las siguientes tareas:

Comprobación de que la instancia de creación de reflejo de puertos se haya creado correctamente

Propósito

Verifique que la instancia de puerto-espejo se haya creado en el conmutador con la VLAN de salida adecuada.`employee-web-monitor`

Acción

Puede comprobar que el puerto-espejo está configurado como se esperaba mediante el comando.`show forwarding-options port-mirror` Para ver los analizadores creados anteriormente que están deshabilitados, vaya a la interfaz de J-Web.

Para verificar que el espejo de puerto está configurado como se esperaba mientras supervisa el tráfico de empleados en el conmutador de origen, ejecute el comando en el conmutador de origen.`show forwarding-options port-miror` Se muestra el siguiente resultado para este ejemplo de configuración:

```
user@switch> show forwarding-options port-mirror

Instance Name: employee-web-monitor
  Instance Id: 3
  Input parameters:
    Rate                  : 1
    Run-length            : 0
    Maximum-packet-length : 0
  Output parameters:
    Family              State     Destination                          Next-hop
    ethernet-switching  up       default-switch/remote-analyzer
```

Significado

Esta salida muestra que la instancia tiene una relación de 1 (duplicar cada paquete, que es el valor predeterminado), el tamaño máximo del paquete original que se reflejó (0 indica todo el paquete), el estado de la configuración está activo (lo que indica el estado correcto y que el analizador está programado, está reflejando el tráfico que ingresa a ge-0/0/0 y ge-0/0/1, y envía el tráfico reflejado a la VLAN llamada).`employee-web-monitorremote-analyzer`

Configuración del análisis local y remoto de creación de reflejo de puertos

in this section

- Configuración de la creación de reflejo de puertos | **1275**
- Configuración de la duplicación de puertos en firewalls de la serie SRX | **1279**
- Ejemplos: Configuración de la creación de reflejo de puertos para el análisis local | **1282**

- Ejemplo: Duplicación del tráfico web de los empleados con un filtro de firewall | **1285**
- Ejemplo: Configuración de la creación de reflejo de puertos para el análisis remoto | **1291**

Configuración de la creación de reflejo de puertos

in this section

- Configuración de la creación de reflejo de puertos para el análisis local | **1276**
- Configuración de la creación de reflejo de puertos para el análisis remoto | **1277**
- Filtrado del tráfico que entra en un analizador | **1278**

Utilice la creación de reflejo de puertos para copiar paquetes y enviar las copias a un dispositivo que ejecute una aplicación, como un analizador de red o una aplicación de detección de intrusiones, de modo que pueda analizar el tráfico sin retrasarlo. Puede reflejar el tráfico que entra o sale de un puerto o entrar en una VLAN, y puede enviar las copias a una interfaz de acceso local o a una VLAN a través de una interfaz troncal.

Le recomendamos que deshabilite la creación de reflejo de puertos cuando no la esté utilizando. Para evitar crear un problema de rendimiento Si habilita la creación de reflejo de puertos, le recomendamos que seleccione interfaces de entrada específicas en lugar de usar la palabra clave.`all` También puede limitar la cantidad de tráfico reflejado mediante un filtro de firewall.

NOTA: Esta tarea utiliza el estilo de configuración Enhanced Layer 2 Software (ELS). Si el conmutador utiliza software que no admite ELS, consulte Configuración de la creación de reflejo de puertos.https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/port-mirroring-qfx-series-cli.html Para obtener detalles de ELS, consulte Uso de la CLI de Enhanced Layer 2 Software.

NOTA: Si desea crear analizadores adicionales sin eliminar un analizador existente, desactive primero el analizador existente mediante el comando.**disable analyzer** ***analyzer-name***

NOTA: Debe configurar las interfaces de salida de creación de reflejo de puerto como **.family ethernet-switching**

Configuración de la creación de reflejo de puertos para el análisis local

Para reflejar el tráfico de la interfaz a una interfaz local en el conmutador:

1. Si desea reflejar el tráfico que entra o sale de interfaces específicas, elija un nombre para la configuración de duplicación de puertos y configure qué tráfico debe reflejarse especificando las interfaces y la dirección del tráfico:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input (ingress | egress) interface interface-name
```

NOTA: Si configura Junos OS para reflejar paquetes de salida, no configure más de 2000 VLAN. Si lo hace, es posible que algunos paquetes de VLAN contengan ID de VLAN incorrectos.

NOTA: Si configura la creación de reflejo para los paquetes que salen de una interfaz de acceso, los paquetes originales pierden cualquier etiqueta VLAN cuando salen de la interfaz de acceso, pero los paquetes reflejados (copiados) conservan las etiquetas VLAN cuando se envían al sistema del analizador.

2. Si desea especificar que todo el tráfico que entre en una VLAN se refleje, elija un nombre para la configuración de duplicación de puertos y especifique la VLAN:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress vlan vlan-name
```

NOTA: No puede configurar la creación de reflejo de puertos para copiar el tráfico que sale de una VLAN.

3. Configure la interfaz de destino para los paquetes reflejados:

```
[edit forwarding-options]
user@switch# set analyzer analyzer-name output interface interface-name
```

Configuración de la creación de reflejo de puertos para el análisis remoto

Para reflejar el tráfico a una VLAN para su análisis en una ubicación remota:

1. Configure una VLAN para transportar el tráfico reflejado:

```
[edit]
user@switch# set vlans vlan-name vlan-id number
```

2. Configure la interfaz que se conecta a otro conmutador (la interfaz de vínculo ascendente) en modo troncal y asóciela a la VLAN adecuada:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching port-mode trunk
vlan members (vlan-name | vlan-id)
```

3. Configure el analizador:

   a) Elija un nombre para el analizador:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name
   ```

   b) Especifique la interfaz que se reflejará y si el tráfico debe reflejarse al entrar o al salir:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name input (ingress | egress) interface interface-name
   ```

   c) Especifique la dirección IP o VLAN adecuada como resultado (en este ejemplo, se especifica una VLAN:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name output vlan (vlan-name | vlan-id)
   ```

Si especifica una dirección IP como salida, tenga en cuenta las siguientes restricciones:

- La dirección no puede estar en la misma subred que ninguna de las interfaces de administración del conmutador.
- Si crea instancias de enrutamiento virtual y también crea una configuración de analizador que incluya una dirección IP de salida, la dirección de salida pertenece a la instancia de enrutamiento virtual predeterminada (tabla de enrutamiento).`inet.0`
- El dispositivo analizador debe ser capaz de desencapsular paquetes encapsulados en GRE o los paquetes encapsulados en GRE deben desencapsularse antes de llegar al dispositivo analizador. (Puede usar un rastreador de red para desencapsular los paquetes).

Filtrado del tráfico que entra en un analizador

> **NOTA**: Esta funcionalidad no es compatible con dispositivos NFX150.

Además de especificar qué tráfico reflejar mediante la configuración de un analizador, también puede utilizar un filtro de firewall para ejercer más control sobre qué paquetes se copian. Por ejemplo, puede usar un filtro para especificar que solo se refleje el tráfico de determinadas aplicaciones. El filtro puede utilizar cualquiera de las condiciones de coincidencia disponibles y debe tener una acción de modificador de Si utiliza el mismo analizador en varios filtros o términos, los paquetes de salida se copian una sola vez.`port-mirror-instance` *`instance-name`*.

Cuando se utiliza un filtro de firewall como entrada para una instancia de duplicación de puertos, se envía el tráfico copiado a una interfaz local o a una VLAN del mismo modo que se hace cuando no interviene un firewall.

Para configurar la creación de reflejo de puertos con filtros:

1. Configure una instancia de duplicación de puertos para el análisis local o remoto. Configure solo la salida. Por ejemplo, para el análisis local, escriba:

   ```
   [edit forwarding-options]
   user@switch# set port-mirroring-instance instance-name output interface interface-name
   ```

   > **NOTA**: No puede configurar la entrada para esta instancia.

2. Cree un filtro de firewall utilizando cualquiera de las condiciones de coincidencia disponibles. En un término, especifique include el modificador de acción .`then` `port-mirror-instance` *`instance-name`*

3. Aplique el filtro de firewall a las interfaces o VLAN que deben proporcionar la entrada al analizador:

```
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching filter input
filter-name

[edit]
user@switch# set vlan (vlan-name | vlan-id) filter input filter-name
```

VÍNCULOS RELACIONADOS

Descripción general de los filtros de firewall (serie QFX)

Configuración de la duplicación de puertos en firewalls de la serie SRX

Para configurar la creación de reflejo de puertos en un dispositivo SRX, primero debe configurar el y en el nivel de jerarquía.`forwarding-optionsinterfaces[edit]`

Debe configurar la instrucción para definir una instancia del puerto para la creación de reflejo del puerto y también configurar la interfaz que se reflejará.`forwarding-optionsmirror-to`

NOTA: El puerto duplicado y el puerto espejo a deben estar bajo el mismo chipset Broadcom en una tarjeta de E/S.

Para configurar la creación de reflejo de puertos:

1. Especifique el y en el nivel jerárquico:`raterun-length[edit forwarding-options port-mirroring input]`

NOTA:

- `rate`: Proporción de paquetes a muestrear (1 de cada) (de 1 a 65535)*N*
- `run-length`: Número de muestras después del disparo inicial (0 a 20)

```
[edit]
    forwarding-options
        port-mirroring {
                input {
                    rate number;
```

```
                run-length number;
            }
        }
```

2. Para enviar las copias del paquete al puerto, incluya la instrucción en el nivel jerárquico.`mirror-to interface` *`intf-name`*`[edit forwarding-options port-mirroring family any output]`

```
output {
    interface intf-name;
}
```

NOTA: La creación de reflejo de puertos en los firewalls de la serie SRX se utiliza para transferir la información del puerto al motor de reenvío de paquetes (PFE).`family anymirror-to` El motor de creación de reflejo copia todos los paquetes del puerto al puerto.`mirroredmirror-to`

NOTA: Puede configurar una cláusula para especificar varios puertos.`instancemirror-to`

Para reflejar una interfaz, incluya la instrucción en el nivel jerárquico . `port-mirror-instance[edit interface mirrored-intf-name]`

La interfaz reflejada se configura con un nombre de instancia, definido en el archivo .`forwarding-options` El puerto y el puerto están vinculados a través de esa instancia.`mirroredmirror-to`

```
instance {
    inst-name {
        input {
            rate number;
            run-length number;
        }
        family any {
            output {
                interface intf-name;
            }
        }
    }
}
interfaces
        mirrored-intf-name {
```

```
            port-mirror-instance instance-name;
        }
```

NOTA: La duplicación de puertos en los firewalls de la serie SRX no diferencia la dirección del tráfico, pero refleja las muestras de entrada y salida juntas .

A continuación se muestra un ejemplo de configuración para la creación de reflejo de puertos:

```
mirror port ge-1/0/2 to port ge-1/0/9.0
forwarding-options
    port-mirroring {
        input {
            rate 1;
            run-length 10;
        }
        family any {
            output {
                interface ge-1/0/9.0;
            }
        }
        instance {
            inst1 {
                input {
                    rate 1;
                    run-length 10;
                }
                family any {
                    output {
                        interface ge-1/0/9.0;
                    }
                }
            }
        }
interfaces {
    ge-1/0/2  {
        port-mirror-instance inst1;
    }
}
```

Ejemplos: Configuración de la creación de reflejo de puertos para el análisis local

in this section

- Requisitos | 1282
- Descripción general y topología | 1282
- Ejemplo: Duplicación de todo el tráfico de empleados para análisis local | 1283

Use la creación de reflejo de puertos para enviar tráfico a aplicaciones que analizan el tráfico con fines como supervisar el cumplimiento, aplicar políticas, detectar intrusiones, supervisar y predecir patrones de tráfico, correlacionar eventos, etc. La duplicación de puertos copia los paquetes que entran o salen de una interfaz o que ingresan a una VLAN y envía las copias a una interfaz local para el monitoreo local.

NOTA: En este ejemplo se utiliza el estilo de configuración Enhanced Layer 2 Software (ELS). Para obtener detalles de ELS, consulte Uso de la CLI de Enhanced Layer 2 Software.

En este ejemplo se describe cómo configurar la creación de reflejo de puertos para copiar el tráfico enviado por los equipos de los empleados a un conmutador a una interfaz de acceso en el mismo conmutador.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 13.2
- Un conmutador

Descripción general y topología

in this section

- Topología | 1283

En este tema se incluyen dos ejemplos relacionados en los que se describe cómo reflejar el tráfico que entra en las interfaces del conmutador y una interfaz de acceso del mismo conmutador. En el primer ejemplo, se muestra cómo reflejar todo el tráfico enviado por los equipos de los empleados al conmutador. El segundo ejemplo incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

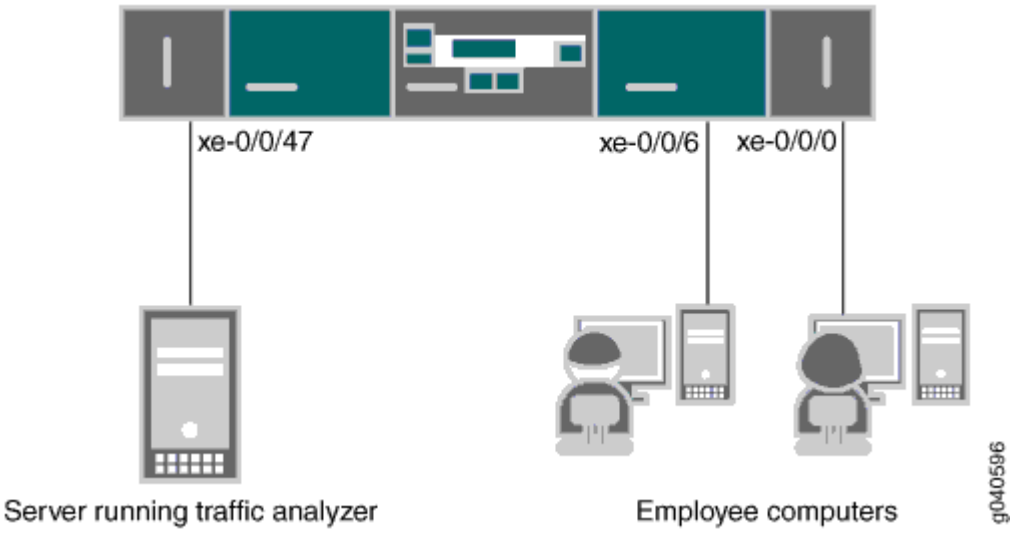
Topología

En este ejemplo, y sirven como conexiones para las computadoras de los empleados.`xe-0/0/0``xe-0/0/6` La interfaz está conectada a un dispositivo que ejecuta una aplicación analizadora.`xe-0/0/47`

> **NOTA**: Varios puertos reflejados en una interfaz pueden provocar el desbordamiento del búfer y la pérdida de paquetes.

Figura 45 en la página 1283 muestra la topología de red de este ejemplo.

Figura 45: Ejemplo de topología de red para creación de reflejo de puerto local



Ejemplo: Duplicación de todo el tráfico de empleados para análisis local

in this section

- Procedimiento | **1284**

Para configurar la creación de reflejo de puertos para todo el tráfico enviado por los equipos de los empleados para su análisis local, realice las tareas que se explican en esta sección.

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la duplicación de puertos locales para el tráfico de entrada a los dos puertos conectados a los equipos de los empleados, copie los siguientes comandos y péguelos en una ventana de terminal de conmutación:

```
[edit]
 set interfaces xe-0/0/0 unit 0 family ethernet-switching
 set interfaces xe-0/0/6 unit 0 family ethernet-switching

 set interfaces xe-0/0/47 unit 0 family ethernet-switching
 set forwarding-options analyzer employee-monitor input ingress interface xe-0/0/0.0
 set forwarding-options analyzer employee-monitor input ingress interface xe-0/0/6.0
 set forwarding-options analyzer employee-monitor output interface xe-0/0/47.0
```

Procedimiento paso a paso

Para configurar un analizador llamado y especificar las interfaces de entrada (origen) y la interfaz de salida:`employee-monitor`

1. Configure las interfaces conectadas a los equipos de los empleados como interfaces de entrada para el analizador de espejo de puerto:`employee-monitor`

   ```
   [edit forwarding-options]
    user@switch# set analyzer employee-monitor input ingress interface xe-0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface xe-0/0/6.0
   ```

2. Configure la interfaz del analizador de salida para el analizador.`employee-monitor` Esta será la interfaz de destino para los paquetes reflejados:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface xe-0/0/47.0
   ```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show forwarding-options analyzer
    employee-monitor {
        input {
            ingress {
                interface xe-0/0/0.0;
                interface xe-0/0/6.0;
            }
        }
        output {
            interface {
                xe-0/0/47.0;
            }
        }
    }
}
```

Ejemplo: Duplicación del tráfico web de los empleados con un filtro de firewall

in this section

- Requisitos | **1285**
- Descripción general | **1286**
- Configurar | **1286**
- Verificación | **1289**

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Un conmutador QFX5100
- Junos OS versión 14.1X53-D30

Descripción general

En lugar de reflejar todo el tráfico, generalmente es deseable reflejar solo cierto tráfico. Este es un uso más eficiente de su ancho de banda y hardware y puede ser necesario debido a restricciones en estos activos. Para seleccionar tráfico específico para la creación de reflejos, utilice un filtro de firewall para que coincida con el tráfico deseado y lo dirija a una instancia de creación de reflejo de puertos. A continuación, la instancia de duplicación de puertos copia los paquetes y los envía a la VLAN, interfaz o dirección IP de salida.

Configurar

in this section

- Procedimiento | **1286**

Para especificar que el único tráfico que se reflejará es el tráfico enviado por los empleados a la Web, realice las tareas explicadas en esta sección. Para seleccionar este tráfico para la creación de reflejos, utilice un filtro de firewall para especificar este tráfico y dirigirlo a una instancia de creación de reflejo de puertos.

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente la duplicación del puerto local del tráfico de los equipos de los empleados destinado a la Web, copie los comandos siguientes y péguelos en una ventana de terminal de conmutador:

```
[edit]
 set interface xe-0/0/47 unit 0 family ethernet-switching
 set forwarding-options port-mirroring instance employee-web-monitor family ethernet-switching
output interface xe-0/0/47.0
 set firewall family ethernet-switching filter watch-employee term employee-to-corp from ip-
destination-address 192.0.2.16/28
 set firewall family ethernet-switching filter watch-employee term employee-to-corp from ip-
source-address 192.0.2.16/28
 set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
 set firewall family ethernet-switching filter watch-employee term employee-to-web from
```

```
destination-port 80
 set firewall family ethernet-switching filter watch-employee term employee-to-web then port-
mirror-instance employee-web-monitor
 set interfaces xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
 set interfaces xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Procedimiento paso a paso

Para configurar la creación de reflejo del puerto local del tráfico de empleados a web desde los dos puertos conectados a los equipos de los empleados:

1. Configure la interfaz de salida:

```
[edit interfaces]
user@switch# set xe-0/0/47 unit 0 family ethernet-switching
```

2. Configure la interfaz de salida.`employee-web-monitor` (Configure solo la salida: la entrada proviene del filtro).

```
[edit forwarding-options]
user@switch# set port-mirroring instance employee-web-monitor family ethernet-switching
output interface xe-0/0/47.0
```

3. Configure un filtro de firewall llamado que incluya un término para que coincida con el tráfico enviado a la Web y envíelo a la instancia de creación de reflejo de puertos.`watch-employeeemployee-web-monitor` No es necesario copiar el tráfico hacia y desde la subred corporativa (destino o dirección de origen de) , así que cree otro término para aceptar ese tráfico antes de que llegue al término que envía el tráfico web a la instancia:`192.0.2.16/28`

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-corp from ip-destination-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp from ip-source-address
192.0.2.16/28
user@switch# set filter watch-employee term employee-to-corp then accept
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

4. Aplique el filtro de firewall a las interfaces apropiadas como filtro de entrada (los filtros de salida no permiten analizadores):

```
[edit interfaces]
user@switch# set xe-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set xe-0/0/6 unit 0 family ethernet-switching filter input watch-employee
```

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show
forwarding-options {
    port-mirroring {
        instance     {
            employee-web-monitor    {
                family ethernet-switching {
                        output {
                            interface xe-0/0/47.0;
                        }
                }
            }
        }
    }
}
...
firewall {
    family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
            from {
                    ip-source-address 192.0.2.16/28;
                    ip-destination-address 192.0.2.16/28;
                }
                then accept;
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
```

```
            }
        }
    }
}
...
interfaces {
    xe-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    xe-0/0/6 {
        family ethernet-switching {
            filter {
                input watch-employee;
            }
        }
    }
    xe-0/0/47 {
        family ethernet-switching;
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | **1290**

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que la instancia de duplicación de puertos denominada se haya creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.`employee-web-monitor`

Acción

Puede comprobar que la instancia de duplicación de puertos se ha configurado según lo esperado mediante el comando.`show forwarding-options port-mirroring`

```
user@switch> show forwarding-options port-mirroring
Instance name                 : employee-web-monitor
Instance Id:  2
Input parameters:
    Rate                              :1
    Run-length                        :0
    Maximum packet length             :0
Output parameters:
    Family                 State      Destination      Next-hop
    ethernet-switching     up         xe-0/0/47.0
```

Significado

Este resultado muestra la siguiente información acerca de la instancia de creación de reflejo de puertos:`employee-web-monitor`

- Tiene una velocidad de (duplicar cada paquete, la configuración predeterminada)`1`
- El número de paquetes consecutivos muestreados (longitud de ejecución) es `0`
- El tamaño máximo del paquete original que se reflejó es (indica todo el paquete)`00`
- El estado de los parámetros de salida: `up` Indica que la instancia refleja el tráfico que entra en las interfaces xe-0/0/0 y xe-0/0/6 y envía el tráfico reflejado a la interfaz xe-0/0/47

Si el estado de la interfaz de salida es o si la interfaz de salida no está configurada, el valor será y la instancia no se programará para la creación de reflejo.`downstatedown`

Ejemplo: Configuración de la creación de reflejo de puertos para el análisis remoto

in this section

- Requisitos | 1291
- Descripción general y topología | 1291
- Duplicación de todo el tráfico de empleados para análisis remoto | 1292
- Duplicación del tráfico de empleados a la web para análisis remoto | 1294
- Verificación | 1297

Use la creación de reflejo de puertos para enviar tráfico a aplicaciones que analizan el tráfico con fines como supervisar el cumplimiento, aplicar políticas, detectar intrusiones, supervisar y predecir patrones de tráfico, correlacionar eventos, etc. La duplicación de puertos copia los paquetes que entran o salen de una interfaz o que ingresan una VLAN y envía las copias a una interfaz local para monitoreo local o a una VLAN para monitoreo remoto. En este ejemplo se describe cómo configurar la creación de reflejo de puertos para el análisis remoto.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 13.2 para la serie QFX
- Un conmutador

Descripción general y topología

in this section

- Topología | 1292

En este tema se incluyen dos ejemplos relacionados en los que se describe cómo reflejar el tráfico que entra en los puertos del conmutador a una VLAN del analizador para que pueda realizar el análisis mediante un dispositivo remoto. En el primer ejemplo, se muestra cómo reflejar todo el tráfico enviado por los equipos de los empleados al conmutador. El segundo ejemplo incluye un filtro para reflejar sólo el tráfico de empleados que va a la Web.

Topología

En este ejemplo:

- Interfaces y son interfaces de capa 2 que se conectan a los equipos de los empleados.`ge-0/0/0`ge-0/0/1
- La interfaz es una interfaz de capa 2 que se conecta a otro conmutador.`ge-0/0/2`
- La VLAN está configurada en todos los conmutadores de la topología para transportar el tráfico reflejado.`remote-analyzer`

> **NOTA**: Además de realizar los pasos de configuración descritos aquí, también debe configurar la VLAN del analizador (en este ejemplo) en los demás conmutadores que se utilizan para conectar el conmutador de origen (el de esta configuración) al que está conectada la estación de supervisión.`remote-analyzer`

Duplicación de todo el tráfico de empleados para análisis remoto

in this section

- Procedimiento | **1292**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente esta sección del ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía:`edit`

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
 set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
 set forwarding-options analyzer employee-monitor output vlan remote-analyzer
```

Procedimiento paso a paso

Para configurar la creación básica de reflejo de puerto remoto:

1. Configure la VLAN del analizador (llamada en este ejemplo):`remote-analyzer`

```
[edit vlans]
user@switch# set vlans remote-analyzer vlan-id 999
```

2. Configure la interfaz conectada a otro conmutador para el modo troncal y asóciela a la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set ge-0/0/10 unit 0 family ethernet-switching port-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

3. Configure el analizador:`employee-monitor`

```
[edit forwarding-options]
user@switch# set analyzer employee-monitor
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
user@switch# set analyzer employee-monitor output vlan remote-analyzer
```

4. Configure la VLAN en los conmutadores que conectan este conmutador a la estación de trabajo de supervisión.`remote-analyzer`

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show
 forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
```

```
            }
        }
        output {
            vlan {
                remote-analyzer;
            }
        }
    }
}
```

Duplicación del tráfico de empleados a la web para análisis remoto

in this section

- Configuración rápida de CLI | **1294**
- Procedimiento | **1295**

Configuración rápida de CLI

Para configurar rápidamente esta sección del ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía:`edit`

```
[edit]
 set vlans remote-analyzer vlan-id 999
 set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
 set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
 set forwarding-options port-mirroring instance employee-web-monitor loss-priority high output
vlan 999
 set firewall family ethernet-switching filter watch-employee term employee-to-web from
destination-port 80
 set firewall family ethernet-switching filter watch-employee term employee-to-web then port-
mirror-instance employee-web-monitor
 set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
 set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

Procedimiento

Procedimiento paso a paso

1. Configure la VLAN del analizador (llamada en este ejemplo):`remote-analyzer`

```
[edit vlans]
user@switch# set remote-analyzer vlan-id 999
```

2. Configure una interfaz para asociarla con la VLAN:`remote-analyzer`

```
[edit interfaces]
user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
```

3. Configure el analizador.`employee-web-monitor` (Configure solo la salida: la entrada proviene del filtro).

```
[edit forwarding-options]
user@switch# set forwarding-options port-mirroring instance employee-web-monitor output vlan
999
```

4. Configure un filtro de firewall llamado para que coincida con el tráfico enviado a la Web y envíelo al analizador :`watch-employeeemployee-web-monitor`

```
[edit firewall family ethernet-switching]
user@switch# set filter watch-employee term employee-to-web from destination-port 80
user@switch# set filter watch-employee term employee-to-web then port-mirror-instance
employee-web-monitor
```

5. Aplique el filtro de firewall a las interfaces apropiadas como filtro de entrada:

```
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filterinput watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

6. Configure la VLAN en los conmutadores que conectan este conmutador a la estación de trabajo de supervisión.`remote-analyzer`

Resultados

Compruebe los resultados de la configuración:

```
[edit]
user@switch# show
interfaces {
    ...
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members remote-analyzer;
                }
            }
        }
    }
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                filter {
                    input watch-employee;
                }
            }
        }
    }
}
...
firewall {
     family ethernet-switching {
        ...
        filter watch-employee {
```

```
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirror-instance employee-web-monitor;
            }
        }
    }
}
 forwarding-options analyzer {
    employee-web-monitor {
        output {
            vlan {
                999;
            }
        }
    }
vlans {
    remote-analyzer {
        vlan-id 999;
    }
}
```

Verificación

in this section

- Comprobación de que el analizador se ha creado correctamente | **1297**

Comprobación de que el analizador se ha creado correctamente

Propósito

Verifique que el analizador denominado o creado en el conmutador con las interfaces de entrada y la interfaz de salida adecuadas.`employee-monitoremployee-web-monitor`

Acción

Puede comprobar que el analizador de espejo de puertos está configurado como se esperaba mediante el comando.`show analyzer`

```
user@switch> show analyzer
    Analyzer name                : employee-monitor
    Output VLAN                  : remote-analyzer
    Ingress monitored interfaces : ge-0/0/0.0
    Ingress monitored interfaces : ge-0/0/1.0
```

Significado

Este resultado muestra que el analizador está reflejando el tráfico que entra y está enviando el tráfico de reflejo al analizador.`employee-monitorge-0/0/0ge-0/0/1remote-analyzer`

Duplicación de puerto 1:N a múltiples destinos en conmutadores

summary

Puede utilizar la función de creación de reflejo de puertos descrita en este documento para reflejar el tráfico a varios destinos de capa 2.

in this section

- Duplicación de puertos 1:N: descripción y directrices de configuración | **1299**
- Configurar la instancia de creación de reflejo de puertos | **1301**
- Configurar el analizador nativo | **1301**
- Configurar grupos de salto siguiente | **1302**
- Configurar el filtro de firewall | **1302**
- Configurar las interfaces | **1302**
- Configurar las VLAN | **1302**
- Resultados de configuración de ejemplo | **1303**

Duplicación de puertos 1:N: descripción y directrices de configuración

in this section

- ¿Qué es la duplicación de puertos 1:N? | **1299**
- Preparación para configurar la duplicación de puertos 1:N: directrices y limitaciones | **1299**
- Descripción general de las tareas de configuración para la creación de reflejo de puertos 1:N | **1301**

¿Qué es la duplicación de puertos 1:N?

Usamos el término *duplicación de puerto 1:N* en este documento para referirnos a la función que le permite reflejar paquetes a múltiples destinos. "1" representa el origen del paquete que se está reflejando y "N" representa los múltiples destinos a los que se envía el paquete. También es posible que vea esta característica descrita como duplicación de múltiples paquetes.

La duplicación de puertos ayuda a los administradores de red a depurar problemas de red y a defenderse de los ataques a la red. Puede usar la duplicación de puertos para el análisis de tráfico en dispositivos de red como enrutadores y conmutadores que, a diferencia de los concentradores, no difunden paquetes a todas las interfaces del dispositivo de destino. La duplicación de puertos envía copias de todos los paquetes a analizadores locales o remotos donde puede supervisar y analizar los datos.

La creación de reflejo del puerto 1:N se utiliza para reflejar el tráfico a varios destinos de capa 2. Los grupos del salto siguiente se utilizan en esta configuración de características.

Puede configurar estos múltiples puertos de observación con conexiones a diferentes dispositivos de supervisión.

Preparación para configurar la duplicación de puertos 1:N: directrices y limitaciones

Puede configurar la función de creación de reflejo de puerto 1:N en los dos métodos de configuración siguientes:

- Creación de reflejo de puertos (mediante un método basado en filtros de firewall) en la jerarquía`[edit forwarding-options port-mirroring instance]`
- Analizador nativo en la jerarquía`[edit forwarding-options analyzer]`

NOTA: Puede configurar los dos métodos anteriores en el mismo dispositivo. Consulte Ejemplos de resultados de configuración para ver un ejemplo."Resultados de configuración de ejemplo" en la página 1303

Las siguientes familias de direcciones son compatibles con la creación de reflejo de puerto 1:N:

- `ethernet-switching`
- `inet`
- `inet6`

Estas son las limitaciones que debe tener en cuenta al configurar la función:

- Los miembros del grupo del siguiente salto pueden ser solo de capa 2, no de capa 3.
- Solo puede configurar la compatibilidad con la creación de reflejo de puerto local , es decir, no para la creación de reflejo remota de puertos ni para la creación de reflejo de puertos remotos en una dirección IP (encapsulación GRE).`next-hop-group output`
- Puede configurar hasta 4 grupos de salto siguiente y agregar hasta 4 interfaces a cada grupo de salto siguiente. Debe definir al menos 2 destinos para enviar paquetes a más de un destino; Sin embargo, solo puede definir un destino en un grupo de salto siguiente.

enumera las combinaciones de jerarquía de configuración que se usan para crear la topología de creación de reflejo 1:N:Tabla 124 en la página 1300

Tabla 124: Jerarquías de configuración para la duplicación de puertos 1:N

Método de configuración	Jerarquías
Duplicación de puertos (basada en filtros)	`[edit forwarding-options port-mirroring instance]`
	`[edit firewall family` *`family-name`* `filter]`
	`[edit forwarding-options next-hop-group]`
	`[edit interfaces]`
	`[edit vlans]`

Tabla 124: Jerarquías de configuración para la duplicación de puertos 1:N *(Continued)*

Método de configuración	Jerarquías
Analizador nativo	`[edit forwarding-options analyzer]`
	`[edit forwarding-options next-hop-group]`
	`[edit interfaces]`
	`[edit vlans]`

NOTA: Puede leer las subsecciones de la tarea de configuración o puede ir a los Resultados de configuración de ejemplo que muestran los resultados combinados de la tarea."Resultados de configuración de ejemplo" en la página 1303

Descripción general de las tareas de configuración para la creación de reflejo de puertos 1:N

En las siguientes subsecciones de tareas de configuración se muestra cómo configurar cada una de las jerarquías enumeradas en la tabla 1.Tabla 124 en la página 1300 Puede leer las subsecciones de la tarea de configuración o puede ir a los Resultados de configuración de ejemplo que muestran los resultados combinados de la tarea."Resultados de configuración de ejemplo" en la página 1303

Configurar la instancia de creación de reflejo de puertos

Para configurar la instancia de duplicación de puertos, introduzca los siguientes comandos en el modo de configuración:`[edit]`

set forwarding-options familia de instancias de duplicación de puertos salida next-hop-group *instance-namefamily-namenext-hop-group-name*

Configurar el analizador nativo

Para configurar el analizador nativo, introduzca los siguientes comandos en el modo de configuración: `[edit]`

1. establecer opciones de reenvío interfaz de entrada de entrada del analizador *analyzer-nameinterface-name*
2. set forwarding-options analyzer output next-hop-group *analyzer-namenext-hop-group-name*

Configurar grupos de salto siguiente

Para configurar grupos del salto siguiente, escriba el comando siguiente en el modo de configuración: `[edit]`

> **NOTA**: Debe configurar el valor como `.group-typelayer-2`

Establecer opciones de reenvío Interfaz de tipo grupo de siguiente salto de capa 2 *next-hop-group-nameinterface-name*

Configurar el filtro de firewall

Para configurar el filtro de firewall, introduzca los siguientes comandos en el modo de configuración: `[edit]`

> **NOTA**: Defina un filtro de firewall que haga referencia al grupo del salto siguiente como acción de filtro.

Para obtener información acerca de la configuración de filtros de firewall en general, consulte la Guía del usuario de directivas de enrutamiento, filtros de firewall y políticas de tráfico.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-policy/config-guide-policy.html

1. Establezca el término de filtro de la familia de firewall y, a continuación, la instancia de espejo de puerto*family-namefilter-nameterm-nameinstance-name*
2. Establecer el término de filtro de familia de firewall desde el puerto de origen*family-namefilter-nameterm-nameport-number*

Configurar las interfaces

Para configurar las interfaces, introduzca los siguientes comandos en el modo de configuración:`[edit]`

1. establecer familia de unidades de interfaces modo de interfaz*interface-namelogical-unit-number family-namemode*
2. establecer interfaces familia de unidades filtrar entrada*interface-namelogical-unit-number family-namefilter-name*

Configurar las VLAN

Para configurar VLAN, ingrese los siguientes comandos en el modo de configuración:`[edit]`

Establecer VLAN vlan-id *vlan-name vlan-id*

Resultados de configuración de ejemplo

```
set interfaces ge-2/1/9 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-2/1/9 unit 0 family ethernet-switching vlan members 100-102
set interfaces ge-2/2/7 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-2/2/7 unit 0 family ethernet-switching vlan members 100-102
set interfaces ge-2/3/0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-2/3/0 unit 0 family ethernet-switching vlan members 100-102
set interfaces ge-2/3/0 unit 0 family ethernet-switching filter input f1
set forwarding-options analyzer analyz1 input ingress interface ge-2/3/0.0
set forwarding-options analyzer analyz1 output next-hop-group nhg1
set forwarding-options port-mirroring instance inst1 family ethernet-switching output next-hop-
group
nhg1
set forwarding-options next-hop-group nhg1 group-type layer-2
set forwarding-options next-hop-group nhg1 interface ge-2/2/7.0
set firewall family ethernet-switching filter f1 term t1 from source-port 7023
set firewall family ethernet-switching filter f1 term t1 then port-mirror-instance inst1
```

Supervisión de la duplicación de puertos

in this section

- Visualización de la configuración y el estado de la instancia de duplicación de puertos de capa 2 | **1303**
- Visualización de la configuración y el estado del grupo del próximo salto | **1304**

Visualización de la configuración y el estado de la instancia de duplicación de puertos de capa 2

Para mostrar el estado actual de las instancias de creación de reflejo de puertos, utilice el comando operativo.`show forwarding-options port-mirroring <terse | detail> <instance-name>`

Para obtener más información acerca de cómo mostrar la configuración y el estado de la instancia de creación de reflejo de puertos, consulte la Biblioteca de administración de Junos OS.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/system-basics/index.html

Visualización de la configuración y el estado del grupo del próximo salto

Para mostrar el estado actual de los grupos del próximo salto, utilice el comando operativo.`show forwarding-options next-hop-group <terse | brief | detail> <group-name>`

Para obtener más información, consulte el Explorador de CLI.https://www.juniper.net/documentation/content-applications/cli-explorer/junos/

Configurar la duplicación de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3

summary

Los filtros selectivos de duplicación de paquetes pueden servir como un mecanismo de solución de problemas altamente efectivo y también se pueden usar para fines de monitoreo del rendimiento.

in this section

- Descripción de la creación de reflejo de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3 | **1304**
- Configurar un filtro con una instancia de creación de reflejo de puerto o con creación de reflejo de puerto global | **1305**
- Configurar la creación de reflejo para túneles FTI | **1309**
- Puntos de fijación para filtros | **1312**
- Sugerencias para mejorar la configuración del filtrado de paquetes | **1313**

Descripción de la creación de reflejo de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3

in this section

- Características de la duplicación de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3 | **1305**
- Limitaciones para la configuración de creación de reflejo a nivel de paquete | **1305**

Este documento se centra en la capacidad de seleccionar tráfico mediante una amplia variedad de condiciones de coincidencia de filtros IPv4 o IPv6 y de reflejar paquetes enteros con su información original de encabezado de capa 2.

La información del encabezado de capa 2 puede ser esencial para identificar a un cliente específico en una implementación de enrutador perimetral o a un par de Internet específico en un caso de emparejamiento público.

Características de la duplicación de paquetes con encabezados de capa 2 para el tráfico reenviado de capa 3

En pocas palabras, puede reflejar el encabezado original del paquete de capa 2 cuando la acción está configurada en un filtro o .`l2-mirrorfamily inetfamily inet6` Los paquetes se pueden duplicar local o remotamente mediante túneles GRE.

Si especifica la interfaz de salida en la configuración de creación de reflejo como una interfaz de túnel GRE, los paquetes se encapsulan en GRE antes de la transmisión. Una instancia de duplicación de puertos se puede configurar con varias familias de protocolos de salida.

Limitaciones para la configuración de creación de reflejo a nivel de paquete

- La nueva acción, , sólo se admite para y filtra.`l2-mirrorfamily inetfamily inet6`
- La duplicación de capa 2 no es compatible con interfaces gr-*/*/**.

Configurar un filtro con una instancia de creación de reflejo de puerto o con creación de reflejo de puerto global

Puede configurarse en (creación de reflejo de puerto global) o (instancias de duplicación de puertos, o "instancias de PM").`l2-mirrorfirewall family (inet | inet6) filter` *`filter-name`* `term then port-mirrorfirewall (inet | inet6) filter` *`filter-name`* `term then port-mirror-instance` *`instance-name`*

Haber configurado para un término indica que para los paquetes que coinciden con este término, el paquete de capa 2 se refleja.`l2-mirror` El software realiza comprobaciones de confirmación en busca de configuraciones no válidas, como cuando está configurado pero no se configura ninguna interfaz de salida de duplicación de puerto en la configuración de duplicación de puertos a nivel global o de instancia.`l2-mirrorfamily any` Si desactiva , el comportamiento de creación de reflejo vuelve a la creación de reflejo de capa 3.`l2-mirror`

Los dos ejemplos siguientes muestran la configuración de un filtro (el nombre del filtro en los ejemplos es f1) con una instancia de creación de reflejo de puertos y con una creación de reflejo de puerto global. En ambos ejemplos, el tráfico se refleja en el destino remoto a través de un túnel GRE.

NOTA: Las configuraciones de duplicación de puertos, que se encuentran en , se configuran con , pero las condiciones de coincidencia en la configuración del filtro se realizan en `.forwarding-optionsfamily anyfamily inet` El uso permite la creación de reflejo de paquetes de capa 2.`family any`

1. Para configurar el filtro con una instancia de duplicación de puertos:

NOTA: Puede especificar una interfaz gr- como destino espejo. Consulte Configuración de tunelización de encapsulación de enrutamiento genérico en la serie ACX para obtener información sobre la configuración de interfaces gr- (el documento se refiere específicamente a los enrutadores de la serie ACX; la misma información se aplica a otros enrutadores, incluidos MX10003).https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/gre-tunnel-services-cli-acx-series.html

```
forwarding-options {
  port-mirroring {
    instance {
      mirror-instance-1 {
        input {
          rate 2;
        }
        family any {
          output {
            interface gr-0/0/0.0;
          }
        }
      }
    }
  }
}
firewall {
  family inet {
    filter f1 {
      term tcp-flags {
        from {
          protocol tcp;
          tcp-flags "(syn & fin & rst)";
        }
        then {
```

```
          port-mirror-instance mirror-instance-1;
          l2-mirror;
        }
      }
    }
  }
}
interfaces {
    gr-0/0/0 {
        unit 0 {
            tunnel {
                source 10.1.1.2/32;
                destination 10.1.1.1/32;
            }
            family bridge {
                interface-mode access;
                vlan-id 100;
            }
        }
    }
}
routing-instances {
    i1 {
        instance-type virtual-switch;
        interface gr-0/0/0.0;
        bridge-domains {
            bd100 {
                vlan-id 100;
            }
        }
    }
}
```

2. Para configurar el filtro con la creación de reflejo global de puertos:

```
forwarding-options {
  port-mirroring {
    input {
      rate 2;
    }
    family any {
      output {
```

```
        interface gr-0/0/0.0;
      }
    }
  }
}
firewall {
  family inet {
    filter f1 {
      term tcp-flags {
        from {
          protocol tcp;
          tcp-flags "(syn & fin & rst)";
        }
        then {
          port-mirror;
          l2-mirror;
        }
      }
    }
  }
}
interfaces {
    gr-0/0/0 {
        unit 0 {
            tunnel {
                source 10.1.1.2/32;
                destination 10.1.1.1/32;
            }
            family bridge {
                interface-mode access;
                vlan-id 100;
            }
        }
    }
}
routing-instances {
    i1 {
        instance-type virtual-switch;
        interface gr-0/0/0.0;
        bridge-domains {
            bd100 {
                vlan-id 100;
            }
```

```
        }
    }
}
```

Configurar la creación de reflejo para túneles FTI

Cuando la ruta de datos atraviesa un túnel de interfaz de túnel flexible (FTI), el paquete de salida se envía con encapsulación de túnel. Puede configurar una configuración que refleje el paquete original, así como el paquete con todas las encapsulaciones a medida que sale.

Para reflejar el paquete original, configure la duplicación de entrada en la interfaz WAN de entrada.

Para reflejar el paquete con todas las encapsulaciones, habilite la creación de reflejo de salida en la interfaz WAN de salida.

Para habilitar la creación de reflejo basada en un filtro instalado en la interfaz FTI, utilice un proceso de dos pasos:

1. Los paquetes se marcan para la creación de reflejo mediante la acción de política en la interfaz fti-. La acción de política se utiliza normalmente para seleccionar la regla de reescritura de salida, pero en este caso, la acción de política se utiliza para marcar paquetes interesantes con un atributo de política interna, sin ninguna regla de reescritura especial configurada.

2. Tiene los paquetes de intercepción de software que coinciden con la política específica en el lado de la WAN de salida e inicia la acción.`l2-mirror` Los paquetes se notifican con información del encabezado de capa 2, incluida la encapsulación del túnel.

> **NOTA**: En el siguiente ejemplo se muestra la creación de reflejo de puertos de capa 3. Para obtener la duplicación de puertos de capa 2, simplemente configure la acción como se muestra en los ejemplos anteriores de este documento.`l2-mirror`

1. Defina bajo la estrofa:`policy-map` *`policy-map-name`* `class-of-service`

```
class-of-service {
  policy-map {
    pm1;
  }
}
```

2. Aplique un filtro de salida en la FTI con la acción :`policy-map pm1`

```
family inet {
  filter mirror-all {
    term mirror {
      from {
        policy-map pm1;
      }
      then {
        count all;
        port-mirror-instance mirror-to-gre;
        accept;
      }
    }
     term default {
       then accept;
     }
   }
  filter f1 {
    term t1 {
      from {
        source-address {
          10.1.1.2/32;
        }
      }
      then {
        policy-map pm1;
        count c1;
      }
    }
    term t2 {
      from {
        source-address {
          10.36.100.1/32;
        }
      }
      then accept;
     }
   }
}
```

3. El siguiente resultado de configuración muestra la configuración de FTI en la interfaz fti0.1001. (Para obtener más detalles sobre la configuración de un túnel FTI, consulte Descripción general de interfaces de túnel flexibles.) https://www.juniper.net/documentation/en_US/junos/topics/concept/flexible_tunnel_interfaces_overview.html

```
interfaces {
  fti0 {
    unit 1001 {
     tunnel {
       encapsulation vxlan-gpe {
         source {
           address 198.51.100.1;
         }
         destination {
           address 198.51.100.2;
         }
         tunnel-endpoint vxlan;
         destination-udp-port 4789;
         vni 22701;
       }
     }
     family inet {
       filter {
         output f1;
       }
       address 10.18.1.1/27;
     }
     family inet6 {
       address 2001:db8::1:1/126;
     }
   }
  }
}
```

4. Agregue un filtro (aquí denominado) en la interfaz WAN de salida con coincidencia de :`mirror-allpolicy-map pm1 then port-mirror`

```
family inet {
  filter mirror-all {
    term mirror {
      from {
```

```
        policy-map policy-map-name;
      }
      then {
        count all;
        port-mirror-instance mirror-to-gre;
                accept;
      }
    }
    term default {
      then accept;
    }
  }
}
```

```
interfaces {
 ge-0/0/1 {
  unit 0 {
    family inet {
      filter {
        output mirror-all;
      }
      address 10.200.0.1/24;
    }
    family iso;
  }
 }
}
```

Puntos de fijación para filtros

Punto de conexión del filtro	Tipo de interfaz	Encabezado de capa 2 de paquete duplicado
Entrada	Cualquier Ethernet excepto gr- y fti-	Se informa del encabezado de capa 2 del paquete entrante
Salida	Cualquier Ethernet excepto gr- y fti-	Se informa del encabezado de capa 2 del paquete entrante
Entrada o salida	Interfaz GR-	No compatible

Entrada	Interfaz FTI	Encabezado entrante de capa 2 del paquete original (como se vio en el puerto WAN)
Salida	Interfaz FTI	Encabezado entrante de capa 2 del paquete original (como se vio en el puerto WAN)
Entrada	Interfaz IRB	Encabezado entrante de capa 2 del paquete original (como se vio en el puerto WAN)
Salida	Interfaz IRB	No compatible

Sugerencias para mejorar la configuración del filtrado de paquetes

Tenga en cuenta lo siguiente como práctica adicional para mejorar la configuración de la telemetría de red de filtros:

Puede utilizar filtros de cadena de entrada y de cadena de salida para separar la configuración de filtros utilizada para la creación de reflejo de los filtros existentes, lo que le ayudará a evitar errores de configuración inadvertidos durante la solución de problemas. Para obtener más información sobre esta característica, consulte Ejemplo: Uso de cadenas de filtro de firewall.

Solución de problemas de duplicación de puertos

in this section

- Solución de problemas de duplicación de puertos | **1314**
- Mensajes de error de configuración de creación de reflejo de puerto | **1316**

Solución de problemas de duplicación de puertos

in this section

- Egress Port Mirroring with VLAN Translation | 1314
- Duplicación de puertos de salida con VLAN privadas | 1315

Egress Port Mirroring with VLAN Translation

IN THIS SECTION

- Problem | 1314
- Solution | 1314

Problem

Description

If you create a port-mirroring configuration that mirrors customer VLAN (CVLAN) traffic on egress and the traffic undergoes VLAN translation before being mirrored, the VLAN translation does not apply to the mirrored packets. That is, the mirrored packets retain the service VLAN (SVLAN) tag that should be replaced by the CVLAN tag on egress. The original packets are unaffected—on these packets VLAN translation works properly, and the SVLAN tag is replaced with the CVLAN tag on egress.

Solution

This is expected behavior.

SEE ALSO

- Understanding Q-in-Q Tunneling and VLAN Translation

Duplicación de puertos de salida con VLAN privadas

in this section

- Problema | 1315
- Solución | 1315

Problema

Description

Si crea una configuración de duplicación de puertos que refleja el tráfico de VLAN privada (PVLAN) en la salida, el tráfico reflejado (el tráfico que se envía al sistema del analizador) tiene la etiqueta VLAN de la VLAN de entrada en lugar de la VLAN de salida. Por ejemplo, supongamos la siguiente configuración de PVLAN:

- Puerto troncal promiscuo que transporta VLAN principales pvlan100 y pvlan400.
- Puerto de acceso aislado que lleva VLAN secundaria aislada200. Esta VLAN es miembro de la VLAN principal pvlan100.
- Puerto de comunidad que transporta la VLAN secundaria comm300. Esta VLAN también es miembro de la VLAN principal pvlan100.
- Interfaz de salida (interfaz de monitor) que se conecta al sistema del analizador. Esta interfaz reenvía el tráfico reflejado al analizador.

Si un paquete para pvlan100 entra en el puerto troncal promiscuo y sale en el puerto de acceso aislado, el paquete original se desetiqueta al salir porque está saliendo en un puerto de acceso. Sin embargo, la copia reflejada conserva la etiqueta para pvlan100 cuando se envía al analizador.

Aquí hay otro ejemplo: Si un paquete para comm300 ingresa en el puerto comunitario y sale en el puerto troncal promiscuo, el paquete original lleva la etiqueta pvlan100 al salir, como se esperaba. Sin embargo, la copia reflejada conserva la etiqueta para comm300 cuando se envía al analizador.

Solución

Este es el comportamiento esperado.

Mensajes de error de configuración de creación de reflejo de puerto

in this section

- Una configuración del analizador devuelve el mensaje de error "No se pueden configurar varias interfaces como miembro de la VLAN de salida del analizador" | **1316**

Solución de problemas relacionados con la duplicación de puertos en conmutadores de la serie EX:

Una configuración del analizador devuelve el mensaje de error "No se pueden configurar varias interfaces como miembro de la VLAN de salida del analizador"

in this section

- Problema | **1316**
- Solución | **1316**

Problema

Description

En una configuración de analizador, si la VLAN a la que se envía el tráfico reflejado contiene más de una interfaz miembro, se muestra el siguiente mensaje de error en la CLI cuando confirma la configuración del analizador y se produce un error en la confirmación:

```
Multiple interfaces cannot be configured as a member of Analyzer output VLAN <vlan name>
```

Solución

Debe dirigir el tráfico reflejado a una VLAN que tenga una interfaz de miembro único. Puede hacerlo completando cualquiera de estas tareas:

- Vuelva a configurar la VLAN existente para que contenga una interfaz de un solo miembro. Puede elegir este método si desea utilizar la VLAN existente.

- Cree una nueva VLAN con una interfaz de un solo miembro y asocie la VLAN con el analizador.

Para volver a configurar la VLAN existente para que contenga solo una interfaz miembro:

1. Elimine las interfaces miembro de la VLAN repetidamente utilizando el comando o el comando hasta que la VLAN contenga una interfaz de miembro único:`delete vlan``delete interface`

   - ```
     [edit]
     user@switch# delete vlan vlan-id interface interface-name
     ```

   - ```
     [edit]
     user@switch# delete interface interface-name unit 0 family family-name vlan member vlan-id
     ```

2. (Opcional) Confirme que la VLAN contiene solo una interfaz:

   ```
   [edit]
   user@switch# show vlans vlan-name
   ```

   El resultado de este comando debe mostrar solo una interfaz.

Para crear una nueva VLAN con una interfaz de un solo miembro:

1. Configure una VLAN para transportar el tráfico reflejado:

   ```
   [edit]
   user@switch# set vlans vlan-name
   ```

2. Asocie una interfaz con la VLAN:

   ```
   [edit]
   user@switch# set interfaces interface-name unit logical-unit-number family family-name vlan
   members vlan-name
   ```

3. Asocie la VLAN con el analizador:

   ```
   [edit ethernet-switching-options]
   user@switch# set analyzer analyzer-name output vlan vlan-name
   ```

10

PART IN COVERPAGE

Mensajes de registro del sistema

Información general sobre el registro del sistema | 1319

Registro del sistema en un sistema de chasis único | 1333

Registro del sistema para un enrutador TX Matrix o TX Matrix Plus | 1357

Dirija los mensajes de registro del sistema a un destino remoto | 1379

Mostrar archivos de registro del sistema | 1396

Configurar el registro del sistema para dispositivos de seguridad | 1402

Configurar Syslog a través de TLS | 1436

Supervisar mensajes de registro | 1447

Información general sobre el registro del sistema

summary

En esta sección se describen los mensajes de registro del sistema que identifican el proceso de Junos OS responsable de generar el mensaje y se proporciona una breve descripción de la operación o error que se produjo.

in this section

- Descripción general del registro del sistema | **1319**
- Funciones de registro del sistema y niveles de gravedad de los mensajes | **1322**
- Configuración predeterminada del registro del sistema | **1324**
- Mensajes de registro del sistema predeterminados específicos de la plataforma | **1326**
- Interpretar mensajes generados en formato estándar | **1327**
- Administrar el registro del sistema operativo host y los archivos principales | **1329**

Descripción general del registro del sistema

Junos OS genera mensajes de registro del sistema (también denominados *mensajes syslog*) para registrar los eventos que se producen en el dispositivo, incluidos los siguientes:

- Operaciones rutinarias, como la creación de una adyacencia de protocolo Open Shortest Path First (OSPF) o un inicio de sesión de usuario en la base de datos de configuración.
- Condiciones de error y error, como la falta de acceso a un archivo de configuración o el cierre inesperado de una conexión a un proceso del mismo nivel.
- Condiciones de emergencia o críticas, como el apagado del dispositivo debido a una temperatura excesiva.

Cada mensaje de registro del sistema identifica el proceso de Junos OS responsable de generar el mensaje y proporciona una breve descripción de la operación o error que se produjo. Para obtener información detallada acerca de mensajes de registro del sistema específicos, consulte el Explorador de registros del sistema.https://apps.juniper.net/syslog-explorer/

Para configurar el dispositivo para que registre mensajes del sistema, configure la instrucción syslog en el nivel jerárquico [edit system].*syslog (System)*

En Junos OS versión 17.3R1, el demonio syslog-event controla el fxp0 en una instancia de enrutamiento de administración dedicada para el host remoto con dirección IPv4. En Junos OS versión 18.1R1, el demonio syslog-event admite la configuración basada en IPv6 cuando se conecta a un host remoto o a un sitio de archivado y fxp0 se mueve a una instancia de administración dedicada. En Junos OS versión 18.4R1, el cliente syslog puede enviar mensajes a través de cualquier instancia de enrutamiento que defina en las jerarquías adecuadas. Consulte routing-instance (Syslog).*routing-instance (Syslog)*

> **NOTA**: En este tema se describen los mensajes de registro del sistema para los procesos y bibliotecas de Junos OS, y no los servicios de registro del sistema en una tarjeta de interfaz física (PIC), como la PIC de Adaptive Services.

En Junos OS evolucionado, cada nodo tiene la herramienta estándar , que es una interfaz para recuperar y filtrar el diario del sistema.`journalctl` Los mensajes de registro del sistema se extraen del diario del sistema. El proceso se ejecuta en todos los nodos y recupera eventos (basados en la configuración syslog) del diario del sistema, así como mensajes de error de las diferentes aplicaciones y los reenvía al proceso.`relay-eventd``master-eventd` El proceso se ejecuta en el motor de enrutamiento principal y escribe los mensajes de registro y los errores en el disco.`master-eventd`

Utilice la aplicación System Log Explorer para ver o comparar mensajes de registro del sistema en diferentes versiones.https://apps.juniper.net/syslog-explorer/

En Junos OS Evolved no hay ningún archivo en el motor de enrutamiento de reserva.`messages` Todos los registros del motor de enrutamiento de copia de seguridad se encuentran en el archivo del nodo principal Motor de enrutamiento.`messages`

De forma predeterminada, Junos OS Evolved anexa el nombre de nodo al nombre de host en los mensajes de registro del sistema; Junos OS no. Esta acción mantiene los mensajes de registro del sistema Junos OS Evolved en conformidad con RFC5424. Sin embargo, es posible que algunos sistemas de supervisión no identifiquen correctamente un nombre de host de Junos OS Evolved, ya que la combinación nombre-nodo no coincide con ningún nombre de host del inventario de nombres de host.

A partir de Junos OS Evolved versión 20.4R2, para garantizar una identificación precisa de los nombres de host de Junos OS Evolved en el sistema de supervisión, utilice el comando de modo de configuración.`set system syslog alternate-format` Este comando cambia el formato de los mensajes de registro del sistema de Junos OS Evolved. El nombre del nodo se antepone al nombre del proceso en el mensaje en lugar de anexarse al nombre de host, lo que permite que el sistema de supervisión identifique el nombre de host correctamente.

Por ejemplo, los mensajes de registro del sistema de Junos OS no imprimen el proceso de origen en los mensajes de registro del sistema procedentes de una FPC:

```
user@mxhost> show log messages
Dec 19 13:22:41.959  mxhost chassisd[5290]: CHASSISD_IFDEV_DETACH_FPC: ifdev_detach_fpc(0)
Dec 19 13:23:22.900  mxhost  fpc2  Ukern event counter Sock_tx init delayed
```

Sin embargo, los mensajes evolucionados de Junos OS anexan el nombre de nodo al nombre de host e imprimen el proceso de origen de los mensajes procedentes de un nodo, incluidos los FPC:

```
user@ptxhost-re0> show log messages
May 25 18:41:05.375  ptxhost-re0  mgd[16201]:  UI_CHILD_STATUS: Cleanup child '/usr/sbin/
dot1xd', PID 21322, status 0
May 25 18:42:34.632  ptxhost-fpc0  evo-cda-bt[14299]:  Register bt.igp_misc.debug.hdr_length_cnt
not found
May 25 18:42:34.753  ptxhost-fpc1  evo-cda-bt[14427]:  HBM: hbm_gf_register_inst
May 25 18:47:14.498  ptxhost-re0  ehmd[5598]:  SYSTEM_APP_READY: App is ready re0-ehmd
```

Si ha configurado el formato alternativo para los mensajes de registro del sistema de Junos OS Evolved, el mismo conjunto de mensajes de registro del sistema tendría este aspecto, con el nombre de host solo:

```
user@ptxhost-re0> show log messages
May 25 18:41:05.375  ptxhost re0- mgd[16201]:  UI_CHILD_STATUS: Cleanup child '/usr/sbin/
dot1xd', PID 21322, status 0
May 25 18:42:34.632  ptxhost fpc0- evo-cda-bt[14299]:  Register bt.igp_misc.debug.hdr_length_cnt
not found
May 25 18:42:34.753  ptxhost fpc1- evo-cda-bt[14427]:  HBM: hbm_gf_register_inst
May 25 18:47:14.498  ptxhost re0- ehmd[5598]:  SYSTEM_APP_READY: App is ready re0-ehmd
```

A partir de Junos OS versión 22.1R1 en dispositivos serie SRX y NFX y Junos OS Evolved versión 22.2R1 en dispositivos QFX5130, QFX5200, QFX5220 y QFX5700, agregamos varios eventos dentro de la etiqueta de evento usando el formato, que tiene una opción () para separar los eventos y generar mensajes de registro del sistema.`<event>UI_LOGIN_EVENT|UI_LOGOUT_EVENT</event>|` Antes de estas versiones, la etiqueta de evento usaba el formato y para varias combinaciones de filtros no se registraba.`<event>UI_LOGIN_EVENT UI_LOGOUT_EVENT</event><get-syslog-events> rpc`

Funciones de registro del sistema y niveles de gravedad de los mensajes

Tabla 125 en la página 1322 enumera los recursos de registro del sistema de Junos OS que puede especificar en las instrucciones de configuración en el nivel jerárquico `.[edit system syslog]`

Tabla 125: Funciones de registro del sistema Junos OS

Instalación (número)	Tipo de evento o error
`kernel` (0)	El kernel de Junos OS realiza acciones y encuentra errores.
`user` (1)	El espacio de usuario realiza acciones o encuentra errores.
`daemon` (3)	El sistema realiza acciones o encuentra errores.
`authorization` (4)	Intentos de autenticación y autorización.
`ftp` (11)	FTP realiza acciones o encuentra errores.
`ntp` (12)	El protocolo de tiempo de red realiza acciones o encuentra errores.
`security` (13)	Eventos o errores relacionados con la seguridad.
`dfc` (17)	Eventos relacionados con la captura dinámica de flujo.
`external` (18)	Las aplicaciones externas locales realizan acciones o encuentran errores.
`firewall` (19)	El filtro de firewall realiza acciones de filtrado de paquetes.
`pfe` (20)	El motor de reenvío de paquetes realiza acciones o encuentra errores.
`conflict-log` (21)	La configuración especificada no es válida en el tipo de enrutador.
`change-log` (22)	Cambios en la configuración de Junos OS.

Tabla 125: Funciones de registro del sistema Junos OS *(Continued)*

Instalación (número)	Tipo de evento o error
`interactive-commands` (23)	Una aplicación cliente, como un protocolo XML de Junos o un cliente XML de NETCONF, emite comandos en el símbolo de la interfaz de línea de comandos (CLI) de Junos OS.

enumera los niveles de gravedad que puede especificar en las instrucciones de configuración en el nivel jerárquico .Tabla 126 en la página 1323`[edit system syslog]` Los niveles a través están en el orden de mayor gravedad (mayor efecto sobre el funcionamiento) a más bajo.`emergency` `info`

A diferencia de los otros niveles de gravedad, el nivel deshabilita el registro de una instalación en lugar de indicar la gravedad con la que un evento desencadenante afecta a las funciones de enrutamiento.`none` Para obtener más información, consulte Deshabilitar el registro del sistema de una instalación."Deshabilitar el registro del sistema de una instalación" en la página 1353

Tabla 126: Niveles de gravedad de los mensajes de registro del sistema

valor	Nivel de gravedad	Description
NA	`none`	Deshabilita el registro de la instalación asociada a un destino.
0	`emergency`	Fallo del sistema u otra condición que hace que el enrutador deje de funcionar.
1	`alert`	Condiciones que requieren corrección inmediata, como una base de datos del sistema dañada.
2	`critical`	Condiciones críticas, como errores graves.
3	`error`	Condiciones de error que generalmente tienen consecuencias menos graves que los errores en los niveles de emergencia, alerta y críticos.
4	`warning`	Condiciones que justifican el seguimiento.
5	`notice`	Condiciones que no son errores, pero que pueden justificar un tratamiento especial.

Tabla 126: Niveles de gravedad de los mensajes de registro del sistema *(Continued)*

valor	Nivel de gravedad	Description
6	`info`	Eventos o condiciones de no error de interés.
7	`any`	Incluye todos los niveles de gravedad.

Configuración predeterminada del registro del sistema

Tabla 127 en la página 1324 resume la configuración predeterminada del registro del sistema que se aplica a todos los enrutadores que ejecutan Junos OS y especifica qué instrucción incluir en la configuración para anular el valor predeterminado.

Tabla 127: Configuración predeterminada del registro del sistema

Ajuste	Predeterminado	Declaración primordial	Instrucciones

Facilidad alternativa para mensajes reenviados a una máquina remota	Para :`change-log` `local6`
	
	Para :`conflict-log` `local5`
	
	Para :`dfc` `local1`
	
	Para :`firewall` `local3`
	
	Para :`interactive-commands` `local7`
	
	Para :`pfe` `local4`
		`[edit system syslog]`
		`host` *`hostname`* `{`
		`  facility-override` *`facility`*`;`
		`}`
			"Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1388

Formato de los mensajes registrados en un archivo	Formato Junos OS estándar, basado en el formato UNIX	`[edit system syslog]`
		`file` *`filename`* `{`
		`  structured-data;`
		`}`
			"Registro de mensajes en formato de datos estructurados" en la página 1341

Tabla 127: Configuración predeterminada del registro del sistema *(Continued)*

Ajuste	Predeterminado	Declaración primordial	Instrucciones

Número máximo de archivos en el conjunto archivado	10	`[edit system syslog]`
		`archive {`
		`  files number;`
		`}`
		`file filename {`
		`  archive {`
		`  files number;`
		`  }`
		`}`
			"Especificación del tamaño, el número y las propiedades de archivado del archivo de registro" en la página 1341

Tamaño máximo del archivo de registro	Serie M, MX y T: 1 megabyte (MB)
	
	Matriz TX: 10 MB
		`[edit system syslog]`
		`archive {`
		`  size size;`
		`}`
		`file filename {`
		`  archive {`
		`  size size;`
		`  }`
		`}`
			"Especificación del tamaño, el número y las propiedades de archivado del archivo de registro" en la página 1341

Formato de marca de tiempo	Mes, fecha, hora, minuto, segundo Por ejemplo: `Aug 21 12:36:30`	`[edit system syslog]` `time-format format;`	"Incluir el año o milisegundo en marcas de tiempo" en la página 1348

Usuarios que pueden leer archivos de registro	usuario y usuarios con permiso Junos OS `rootmaintenance`	`[edit system syslog]`
		`archive {`
		`  world-readable;`
		`}`
		`file filename {`
		`  archive {`
		`  world-readable;`
		`  }`
		`}`
			"Especificación del tamaño, el número y las propiedades de archivado del archivo de registro" en la página 1341

Mensajes de registro del sistema predeterminados específicos de la plataforma

Los siguientes mensajes se generan de forma predeterminada en enrutadores específicos. Para ver cualquiera de estos tipos de mensajes, debe configurar al menos un destino para los mensajes, tal como se describe en Configuración mínima del registro del sistema de Junos OS."Configuración mínima de registro del sistema de Junos OS" en la página 1336

- Para registrar el mensaje de proceso del kernel en un enrutador serie M, MX o T, incluya la instrucción en el nivel jerárquico apropiado:`kernel info`

```
[edit system syslog]
(console | file filename | host destination | user username) {
    kernel info;
}
```

- En una matriz de enrutamiento compuesta por un enrutador de matriz de transmisión y enrutadores T640, el motor de enrutamiento primario de cada enrutador T640 reenvía todos los mensajes con una gravedad superior y superior al motor de enrutamiento principal del enrutador de matriz de transmisión.`info` Esto es equivalente a la siguiente instrucción de configuración incluida en el enrutador TX Matrix:

```
[edit system syslog]
host scc-master {
    any info;
}
```

- A partir de Junos OS versión 15.1X49-D10 y Junos OS versión 17.3R1, del mismo modo en una matriz de enrutamiento compuesta por un enrutador TX Matrix Plus con enrutadores T1600 o T4000 conectados, el motor de enrutamiento principal en cada LCC T1600 o T4000 reenvía al motor de enrutamiento primario en el enrutador TX Matrix Plus todos los mensajes con una gravedad de y superior.`info` Esto es equivalente a la siguiente instrucción de configuración incluida en el enrutador TX Matrix Plus:

> **NOTA**: Desde la perspectiva de la interfaz de usuario, la matriz de enrutamiento aparece como un único enrutador. El enrutador TX Matrix Plus controla todos los enrutadores T1600 o T4000 conectados a él en la matriz de enrutamiento.

```
[edit system syslog]
host sfc0-master {
    any info;
}
```

Interpretar mensajes generados en formato estándar

La sintaxis de un mensaje de formato estándar generado por un proceso o una biblioteca de subrutinas de Junos OS depende de si incluye la siguiente información de prioridad:

- Cuando la instrucción se incluye en el nivel de jerarquía [] o [], un mensaje de registro del sistema tiene la sintaxis siguiente:`explicit-priority` *filenamehostname*

```
timestamp        message-source: %facility-severity-TAG: message-text
```

- Cuando se dirige a la consola o a los usuarios, o cuando no se incluye la instrucción para archivos o hosts remotos, un mensaje de registro del sistema tiene la siguiente sintaxis:`explicit-priority`

```
timestamp        message-source: TAG: message-text
```

Tabla 128 en la página 1327 Describe los campos de mensaje.

Tabla 128: Campos en mensajes de formato estándar

Campo	Description
timestamp	Hora a la que se registró el mensaje.

Tabla 128: Campos en mensajes de formato estándar *(Continued)*

Campo	Description
message-source	Identificador del proceso o componente que genera el mensaje y la plataforma de enrutamiento en la que se registró el mensaje. Para Junos OS, este campo incluye dos o más subcampos: nombre de host, proceso e ID de proceso (PID). Para Junos OS Evolved, este campo incluye un nombre de host con un nombre de nodo adjunto, un nombre de proceso y un PID. Si la instrucción está configurada en el nivel jerárquico [edit system syslog] en un dispositivo Junos OS Evolved, el nombre del nodo no se anexa al nombre de host, sino que se antepone al nombre del proceso.`alternate-format` El formato de mensaje alternativo para Junos OS Evolved garantiza el mismo formato de nombre de host que los mensajes de Junos OS. Si el proceso no informa de su PID, no se muestra el PID. Los subcampos del origen del mensaje se muestran con el siguiente formato: *`hostname  process[process-ID]`*
facility	Código que especifica la utilidad a la que pertenece el mensaje de registro del sistema. Para obtener una asignación de códigos a nombres de instalaciones, consulte la tabla: Códigos de instalaciones indicados en la información de prioridad al incluir información de prioridad en los mensajes de registro del sistema."Incluir información de prioridad en los mensajes de registro del sistema" en la página 1343
severity	Código numérico que representa el nivel de gravedad asignado al mensaje de registro del sistema. Para obtener una asignación de códigos a nombres de gravedad, consulte la tabla: Códigos numéricos para los niveles de gravedad notificados en Información de prioridad al incluir información de prioridad en los mensajes de registro del sistema."Incluir información de prioridad en los mensajes de registro del sistema" en la página 1343
TAG	Cadena de texto que identifica de forma exclusiva el mensaje, en mayúsculas y utilizando el carácter de subrayado (_) para separar las palabras. El nombre de la etiqueta comienza con un prefijo que indica el proceso o la biblioteca del software generador. Las entradas de esta referencia están ordenadas alfabéticamente por este prefijo. No todos los procesos en una plataforma de enrutamiento utilizan etiquetas, por lo que este campo no siempre aparece.
message-text	Texto del mensaje.

Administrar el registro del sistema operativo host y los archivos principales

in this section

- Ver archivos de registro en el sistema operativo host | 1330
- Copiar archivos de registro del sistema host al conmutador | 1330
- Ver archivos principales en el sistema operativo host | 1330
- Copie los archivos principales del sistema host al conmutador | 1331
- Limpiar archivos temporales en el sistema operativo host | 1332

En los conmutadores Junos OS con un SO host, Junos OS puede generar mensajes de registro del sistema (también denominados *mensajes syslog*) para registrar los eventos que se producen en el conmutador, incluidos los siguientes:

- Operaciones rutinarias, como un inicio de sesión de usuario en la base de datos de configuración.
- Condiciones de error y fallo.
- Condiciones de emergencia o críticas, como el apagado del interruptor debido a una temperatura excesiva.

En los conmutadores de la serie OCX:

- Los mensajes de registro del sistema se registran en el archivo en el sistema operativo host en los siguientes escenarios:**/var/log/dcpfe.log**
  - Cuando se inicializa el demonio de reenvío.
  - Los mensajes se etiquetan como emergencia (LOG_EMERG). También se envía una copia del mensaje al directorio del conmutador.**/var/log**
- Los mensajes de los procesos están disponibles en el sistema host en el directorio.**/var/log** Los mensajes de registro del sistema del proceso de administración del chasis del host se registran en el archivo del directorio.**lcmd.log/var/log**

En conmutadores QFX con un SO host:

- Junos OS y el sistema operativo host registran mensajes de registro para eventos del sistema y del proceso, y generan archivos de núcleo cuando se producen determinados fallos del sistema.

- Estos archivos se almacenan en directorios como /var/log para los mensajes de registro, y /var/tmp o /var/crash para los archivos principales, según el tipo de sistema operativo host que se ejecute en el conmutador.

Para fines de diagnóstico, puede acceder a estos archivos de registro y núcleo del sistema SO host desde la CLI de Junos OS en el conmutador. También puede limpiar los directorios donde el sistema operativo host almacena registros temporales y otros archivos.

En este tema se incluyen las siguientes secciones:

Ver archivos de registro en el sistema operativo host

Para ver una lista de los archivos de registro creados en el sistema operativo host, escriba el siguiente comando:

```
user@switch> show app-engine logs
```

Copiar archivos de registro del sistema host al conmutador

Para copiar los archivos de registro del sistema operativo host al conmutador, ingrese el siguiente comando:

```
user@switch> request app-engine file-copy log from-jhost source to-vjunos destination
```

Por ejemplo, para copiar el archivo de registro en el conmutador, escriba el siguiente comando:*lcmd*

```
user@switch> request app-engine file-copy log from-jhost lcmd.log  to-vjunos /var/tmp
```

Ver archivos principales en el sistema operativo host

Para ver la lista de archivos principales generados y almacenados en el sistema operativo host, ingrese el siguiente comando:

```
user@switch> show app-engine crash
```

La lista podría verse como esta salida de ejemplo:

```
Compute cluster: default-cluster
  Compute node: default-node
```

```
    Crash Info
    ==========
    total 13480
    -rw-r--r-- 1 root root  178046 Feb 14 23:08 localhost.lcmd.26653.1455520135.core.tgz
    -rw-r--r-- 1 root root 4330343 Feb 15 00:45 localhost.dcpfe.7155.1455525926.core.tgz
    -rw-r--r-- 1 root root 4285901 Feb 15 01:49 localhost.dcpfe.25876.1455529782.core.tgz
    -rw-r--r-- 1 root root 4288508 Feb 15 02:39 localhost.dcpfe.713.1455532774.core.tgz
    -rw-r--r-- 1 root root  264079 Feb 15 17:02 localhost.lcmd.1144.1455584540.core.tgz
```

Copie los archivos principales del sistema host al conmutador

Para copiar archivos principales del SO host al conmutador, ingrese el siguiente comando:

```
user@switch> request app-engine file-copy crash from-jhost source to-vjunos destination-dir-or-file-path
```

Cuando la ruta de Junos OS de destino es un directorio, se utiliza el nombre de archivo de origen de forma predeterminada. Para cambiar el nombre del archivo en el destino, escriba el argumento de destino como una ruta de acceso completa, incluido el nombre de archivo deseado.

Por ejemplo, para copiar el archivo de almacenamiento principal en el conmutador, escriba el siguiente comando:*localhost.lcmd.26653.1455520135.core.tgz*

```
user@switch> request app-engine file-copy crash from-jhost
localhost.lcmd.26653.1455520135.core.tgz to-vjunos /var/tmp
```

Para ver los resultados en el conmutador, ingrese el siguiente comando:

```
user@switch> show system core-dumps
re0:
--------------------------------------------------------------------------
-rw-r--r--  1 root  field     178046 Feb 15 17:15 /var/tmp/
localhost.lcmd.26653.1455520135.core.tgz
total files: 1
```

Limpiar archivos temporales en el sistema operativo host

Para eliminar los archivos temporales creados en el sistema operativo host, ingrese el siguiente comando:

```
user@switch> request app-engine cleanup
```

Por ejemplo, la siguiente salida de ejemplo en un conmutador con un sistema operativo host Linux muestra la limpieza de archivos temporales almacenados en /var/tmp:

```
Compute cluster: default-cluster

  Compute node: default-node

   Cleanup (/var/tmp)
   =======
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
15.1X49-D10	A partir de Junos OS versión 15.1X49-D10 y Junos OS versión 17.3R1, del mismo modo en una matriz de enrutamiento compuesta por un enrutador TX Matrix Plus con enrutadores T1600 o T4000 conectados, el motor de enrutamiento principal en cada LCC T1600 o T4000 reenvía al motor de enrutamiento primario en el enrutador TX Matrix Plus todos los mensajes con una gravedad de y superior.`info`

Registro del sistema en un sistema de chasis único

in this section

- Descripción general de la configuración del registro del sistema de chasis único | 1333
- Instrucciones de configuración del registro del sistema de Junos OS | 1335
- Configuración mínima de registro del sistema de Junos OS | 1336
- Ejemplo: Configurar mensajes de registro del sistema | 1337
- Mensajes de registro en formato de datos estructurados | 1341
- Especificar el tamaño, el número y las propiedades de archivado del archivo de registro | 1341
- Incluir información de prioridad en los mensajes de registro del sistema | 1343
- Códigos de instalación de registro del sistema y códigos numéricos consignados en la información de prioridad | 1345
- Incluir el año o milisegundo en las marcas de tiempo | 1348
- Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados | 1349
- Junos System registra operadores de expresiones regulares para la instrucción match | 1352
- Deshabilitar el registro del sistema de una instalación | 1353
- Ejemplos: Configurar el registro del sistema | 1354
- Ejemplos: Asignar una instalación alternativa | 1356

Descripción general de la configuración del registro del sistema de chasis único

La utilidad de registro del sistema Junos es similar a la utilidad UNIX `.syslogd` En esta sección se describe cómo configurar el registro del sistema para un sistema de chasis único que ejecuta Junos OS.

La configuración del registro del sistema para el software Junos-FIPS y para los dispositivos de Juniper Networks en un entorno Common Criteria es la misma que para Junos OS. Para obtener más información, consulte la Guía de configuración segura para Common Criteria y Junos-FIPS.

Para obtener información acerca de cómo configurar el registro del sistema para una matriz de enrutamiento compuesta por un enrutador de matriz de transmisión y enrutadores T640, consulte Configuración del registro del sistema para un enrutador de matriz de TX."Configuración del registro del sistema para un enrutador TX Matrix" en la página 1358

Cada mensaje de registro del sistema pertenece a una instalación, que agrupa mensajes relacionados. A cada mensaje también se le asigna previamente un nivel de gravedad, que indica la gravedad con la que el evento desencadenante afecta a las funciones del enrutador. Siempre debe especificar la facilidad y la gravedad de los mensajes que se van a incluir en el registro. Para obtener más información, consulte Especificación de la facilidad y la gravedad de los mensajes que se incluirán en el registro."Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro" en la página 1380

Los mensajes se dirigen a uno o varios destinos incluyendo la instrucción adecuada en el nivel jerárquico :`[edit system syslog]`

- A un archivo con nombre en un sistema de archivos local, incluyendo la instrucción.`file` Consulte Dirigir mensajes de registro del sistema a un archivo de registro."Dirija los mensajes de registro del sistema a un archivo de registro" en la página 1383

- A la sesión de terminal de uno o más usuarios específicos (o todos los usuarios) cuando han iniciado sesión en el enrutador, incluyendo la instrucción.`user` Consulte Dirigir mensajes de registro del sistema a un terminal de usuario."Dirigir mensajes de registro del sistema a un terminal de usuario" en la página 1384

- A la consola del enrutador, incluyendo la instrucción.`console` Consulte Dirigir mensajes de registro del sistema a la consola."Dirija los mensajes de registro del sistema a la consola" en la página 1385

- A un equipo remoto que ejecuta la utilidad, incluyendo la instrucción.**syslogd**`host` Consulte Dirigir mensajes de registro del sistema a un equipo remoto.

De forma predeterminada, los mensajes se registran en un formato estándar, que se basa en un formato de registro del sistema UNIX; para obtener información detallada acerca del formato de los mensajes, consulte el Explorador de registros del sistema.https://apps.juniper.net/syslog-explorer/ Puede modificar el contenido y el formato de los mensajes registrados de las siguientes maneras:

- Puede registrar mensajes en un archivo en formato de datos estructurados en lugar del formato estándar de Junos. El formato de datos estructurados proporciona más información sin agregar una longitud significativa y facilita que las aplicaciones automatizadas extraigan información del mensaje. Para obtener más información, consulte Registro de mensajes en formato de datos estructurados."Mensajes de registro en formato de datos estructurados" en la página 1341

- La facilidad y el nivel de gravedad de un mensaje se denominan conjuntamente su prioridad. De forma predeterminada, el formato estándar de Junos para mensajes no incluye información de prioridad (el formato de datos estructurados incluye un código de prioridad de forma predeterminada). Para incluir información de prioridad en mensajes de formato estándar dirigidos a un archivo o a un destino remoto, incluya la instrucción.`explicit-priority` Para obtener más información, consulte Inclusión de información de prioridad en los mensajes de registro del sistema."Incluir información de prioridad en los mensajes de registro del sistema" en la página 1343

- De forma predeterminada, el formato estándar de Junos para los mensajes especifica el mes, la fecha, la hora, el minuto y el segundo en que se registró el mensaje. Puede modificar la marca de tiempo en

los mensajes de registro del sistema de formato estándar para incluir el año, el milisegundo o ambos. (El formato de datos estructurados especifica el año y el milisegundo de forma predeterminada). Para obtener más información, consulte Incluir el año o el milisegundo en las marcas de tiempo."Incluir el año o milisegundo en las marcas de tiempo" en la página 1348

- Al dirigir mensajes a un equipo remoto, puede especificar la dirección IP que se informa en los mensajes como su origen. También puede configurar funciones que faciliten separar los mensajes generados por Junos OS de los mensajes generados en determinados dispositivos. Para obtener más información, consulte Dirigir mensajes de registro del sistema a un equipo remoto.
- Las instalaciones predefinidas agrupan mensajes relacionados, pero también puede utilizar expresiones regulares para especificar con mayor exactitud qué mensajes de una instalación se registran en un archivo, un terminal de usuario o un destino remoto. Para obtener más información, vea Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados."Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

NOTA: Durante una comprobación de confirmación, las advertencias sobre la configuración (por ejemplo, no coinciden en los tamaños de los archivos de seguimiento o el número de archivos de seguimiento) no se muestran en la consola.**traceoptions** Sin embargo, estas advertencias se registran en los mensajes de registro del sistema cuando se confirma la nueva configuración.

Instrucciones de configuración del registro del sistema de Junos OS

Para configurar el conmutador para que registre mensajes del sistema, incluya la instrucción en el nivel de jerarquía:`syslog[edit system]`

```
[edit system]
syslog {
    archive <files number> <size size> <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites (ftp-url <password password>)> <files number> <size size> <start-
time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
```

```
            brief;
        }
    }
    host hostname {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string
        match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
    user (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

Configuración mínima de registro del sistema de Junos OS

Para grabar o ver mensajes de registro del sistema, debe incluir la instrucción en el nivel jerárquico .`syslog[edit system]` Especifique al menos un destino para los mensajes, como se describe en .Tabla 129 en la página 1336 Para obtener más información acerca de las instrucciones de configuración, consulte Información general sobre la configuración del registro del sistema de chasis único."Descripción general de la configuración del registro del sistema de chasis único" en la página 1333

Tabla 129: Instrucciones de configuración mínima para el registro del sistema

Destino	Instrucciones de configuración mínima

Archivo	`[edit system syslog]`
	`file filename {`
	`  facility severity;`
	`}`

Tabla 129: Instrucciones de configuración mínima para el registro del sistema *(Continued)*

Destino	Instrucciones de configuración mínima

Sesión de terminal de uno, varios o todos los usuarios	`[edit system syslog]`
	`user (`*`username`* `| *) {`
	`  `*`facility severity`*`;`
	`}`

Consola de enrutador o conmutador	`[edit system syslog]`
	`console {`
	`  `*`facility severity`*`;`
	`}`

Equipo remoto u otro motor de enrutamiento en el enrutador o conmutador	`[edit system syslog]`
	`host (`*`hostname`* `| other-routing-engine) {`
	`  `*`facility severity`*`;`
	`}`

Ejemplo: Configurar mensajes de registro del sistema

in this section

- Requisitos | **1338**
- Descripción general | **1338**
- Configuración | **1338**

El sistema QFabric supervisa los eventos que se producen en sus dispositivos componentes y distribuye mensajes de registro del sistema sobre esos eventos a todos los servidores de mensajes de registro (hosts) del sistema externo que están configurados. Los dispositivos de componentes pueden incluir dispositivos de nodo, dispositivos de interconexión, dispositivos de director y el chasis virtual. Los

mensajes se almacenan para su visualización sólo en la base de datos del sistema QFabric. Para ver los mensajes, ejecute el comando.`show log`

En este ejemplo se describe cómo configurar los mensajes de registro del sistema en el sistema QFabric.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 12.2
- Sistema QFabric
- Servidores externos que se pueden configurar como hosts de mensajes de registro del sistema

Descripción general

Los dispositivos componentes que generan eventos de mensajes de registro del sistema pueden incluir dispositivos de nodo, dispositivos de interconexión, dispositivos director y los conmutadores del plano de control. El siguiente ejemplo de configuración incluye estos componentes en el sistema QFabric:

- Software de director que se ejecuta en el grupo Director
- Interruptores del plano de control
- dispositivo de interconexión
- Dispositivos de múltiples nodos

Configuración

in this section

- Procedimiento | **1339**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red y, a continuación, copie y pegue los comandos en la CLI en el nivel de jerarquía.`[edit]`

```
set system syslog host 10.1.1.12 any error
set system syslog file qflogs
set system syslog file qflogs structured-data brief
set system syslog file qflogs archive size 1g
```

Procedimiento paso a paso

El ejemplo siguiente requiere que navegue por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar mensajes del sistema desde el dispositivo QFabric Director:

1. Especifique un host, cualquier instalación y el nivel de gravedad.`error`

   ```
   [edit system syslog]
   user@switch# set host 10.1.1.12 any error
   ```

   NOTA: Puede configurar más de un servidor de mensajes de registro del sistema (host). El sistema QFabric envía los mensajes a cada servidor configurado.

2. (Opcional) Especifique un nombre de archivo para capturar los mensajes de registro.

   NOTA: En el sistema QFabric, un archivo syslog denominado se configura implícitamente con niveles de facilidad y gravedad de y un tamaño de archivo de 100 MB.**messages**`any` `any` Por lo

tanto, no puede especificar el nombre de archivo en la configuración y la finalización automática de comandos no funciona para ese nombre de archivo.**messages**

```
[edit system syslog]
user@switch# set file qflogs structured-data brief
user@switch# set file qflogs
```

3. (Opcional) Configure el tamaño máximo del archivo de almacenamiento de mensajes de registro del sistema. En este ejemplo se especifica un tamaño de archivo de 1 GB.

```
[edit system syslog]
user@switch# set file qflogs archive size 1g
```

Resultados

Desde el modo de configuración, confírmela con el comando `show system`. Si el resultado no muestra la configuración deseada, repita las instrucciones en este ejemplo para corregir la configuración.

```
[edit]
user@switch# show system
syslog {
    file qflogs {
    }
    host 10.1.1.12 {
        any error;
    }
}
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

SEE ALSO

> *syslog (sistema QFabric)*
>
> *muestra el registro*

Mensajes de registro en formato de datos estructurados

Puede registrar mensajes en un archivo en formato de datos estructurados en lugar del formato estándar de Junos OS. El formato de datos estructurados proporciona más información sin agregar una longitud significativa y facilita que las aplicaciones automatizadas extraigan información de un mensaje.

El formato de datos estructurados cumple con el estándar de Internet RFC 5424, *el protocolo Syslog*, que está en https://tools.ietf.org/html/rfc5424. La RFC establece un formato de mensaje estándar independientemente del origen o del protocolo de transporte de los mensajes registrados.

Para enviar mensajes a un archivo en formato de datos estructurados, incluya la instrucción en el nivel de jerarquía:`structured-data`[`edit system syslog file` *`filename`*]

```
[edit system syslog file filename]
facility severity;
structured-data {
    brief;
}
```

La instrucción opcional suprime el texto en inglés que aparece de forma predeterminada al final de un mensaje para describir el error o evento.`brief`

El formato estructurado se utiliza para todos los mensajes registrados en el archivo generados por un proceso de Junos o una biblioteca de software.

> **NOTA**: Si incluye una o ambas instrucciones y junto con la instrucción, se omiten.`explicit-priority``time-format``structured-data` Estas instrucciones se aplican al formato de registro del sistema Junos OS estándar, no al formato de datos estructurados.

Especificar el tamaño, el número y las propiedades de archivado del archivo de registro

Para evitar que los archivos de registro crezcan demasiado, de forma predeterminada, la utilidad de registro del sistema de Junos OS escribe mensajes en una secuencia de archivos de un tamaño definido. Los archivos de la secuencia se denominan archivos *de almacenamiento* para distinguirlos del archivo *activo* en el que se escriben mensajes actualmente. El tamaño máximo predeterminado depende del tipo de plataforma:

- 128 kilobytes (KB) para conmutadores de la serie EX

- 1 megabyte (MB) para enrutadores serie M, MX y serie T
- 10 MB para enrutadores TX Matrix o TX Matrix Plus
- 1 MB para la serie QFX

Cuando un archivo de registro activo llamado alcanza el tamaño máximo, la utilidad de registro cierra el archivo, lo comprime y asigna un nombre al archivo comprimido.***logfilelogfile*.0.gz** A continuación, la utilidad de registro se abre y escribe en un nuevo archivo activo denominado .***logfile*** Este proceso también se conoce como rotación de archivos. Cuando el nuevo alcanza el tamaño máximo configurado, se cambia el nombre de , y el nuevo se cierra, se comprime y se le cambia el nombre . ***logfilelogfile*.0.gz*logfile*.1.gz*logfilelogfile*.0.gz** De forma predeterminada, la utilidad de registro crea hasta 10 archivos de almacenamiento de esta manera. Cuando se alcanza el número máximo de archivos comprimidos y cuando el tamaño del archivo activo alcanza el tamaño máximo configurado, el contenido del último archivo archivado se sobrescribe con el archivo activo actual. De forma predeterminada, la utilidad de registro también limita los usuarios que pueden leer archivos de registro al usuario y a los usuarios que tienen permiso de Junos OS .`rootmaintenance`

Junos OS proporciona una instrucción de configuración que configura la frecuencia de rotación de los archivos de registro del sistema configurando el intervalo de tiempo para comprobar el tamaño del archivo de registro.`log-rotate-frequency` La frecuencia se puede establecer en un valor de 1 minuto a 59 minutos. La frecuencia predeterminada es de 15 minutos.

Para configurar la frecuencia de rotación del registro, incluya la instrucción en el nivel de jerarquía.`log-rotate-frequency[edit system syslog]`

Puede incluir la instrucción para cambiar el tamaño máximo de cada archivo, cuántos archivos de almacenamiento se crean y quién puede leer los archivos de registro.`archive`

Para configurar valores que se apliquen a todos los archivos de registro, incluya la instrucción en el nivel de jerarquía:`archive[edit system syslog]`

```
archive  <files number> <size size> <world-readable | no-world-readable>;
```

Para configurar valores que se apliquen a un archivo de registro específico, incluya la instrucción en el nivel de jerarquía:`archive[edit system syslog file filename]`

```
archive <archive-sites (ftp-url  <password password>)> <files number> <size size> <start-
time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable> ;
```

`archive-sites site-name` Especifica una lista de sitios de archivado que desea usar para almacenar archivos. El valor es cualquier dirección URL FTP válida a un destino.`site-name` Si se configura más de un nombre de sitio, se crea una lista de sitios de archivado para los archivos de registro del sistema. Cuando se archiva un archivo, el enrutador o conmutador intenta transferir el archivo a la primera URL de la lista,

moviéndose al siguiente sitio sólo si la transferencia no se realiza correctamente. El archivo de registro se almacena en el sitio de archivado con el nombre de archivo de registro especificado. Para obtener información acerca de cómo especificar URL FTP válidas, consulte Formato para especificar nombres de archivo y URL en comandos de la CLI de Junos OS.https://www.juniper.net/documentation/en_US/junos15.1/topics/concept/junos-software-formats-filenames-urls.html

`binary-data` Marque el archivo como que contiene datos binarios. Esto permite el archivado adecuado de archivos binarios, como archivos WTMP (registros de inicio de sesión para sistemas basados en UNIX). Para restaurar la configuración predeterminada, incluya la instrucción.`no-binary-data`

`files` *`number`* Especifica el número de archivos que se van a crear antes de sobrescribir el archivo más antiguo. El valor puede ser del 1 al 1000.

`size` *`size`* Especifica el tamaño máximo de cada archivo. El valor puede ser de 64 KB (64k) a 1 gigabyte (1g); Para representar megabytes, utilice la letra después del entero.`m` No hay espacio entre los dígitos y la letra , o unidades.`kmg`

Define la fecha y la hora en la zona horaria local para una transferencia única del archivo de registro activo al primer sitio accesible de la lista de sitios especificada por la instrucción.`start-time "`*`YYYY-MM-DD.hh:mm`*`"archive-sites`

`transfer-interval` *`interval`* Define la cantidad de tiempo que el archivo de registro actual permanece abierto (incluso si no ha alcanzado el tamaño máximo posible) y recibe nuevas estadísticas antes de cerrarlo y transferirlo a un sitio de archivo. Este valor de intervalo puede ser de 5 a 2880 minutos.

`world-readable` Permite a todos los usuarios leer los archivos de registro. Para restaurar los permisos predeterminados, incluya la instrucción.`no-world-readable`

Incluir información de prioridad en los mensajes de registro del sistema

La facilidad y el nivel de gravedad de un mensaje se denominan conjuntamente su *prioridad*. De forma predeterminada, los mensajes registrados en el formato estándar de Junos OS no incluyen información sobre la prioridad. Para incluir información de prioridad en mensajes de formato estándar dirigidos a un archivo, incluya la instrucción en el nivel de jerarquía:`explicit-priority`[`edit system syslog file` *`filename`*]

```
[edit system syslog file filename]
facility severity;
explicit-priority;
```

NOTA: Los mensajes registrados en formato de datos estructurados incluyen información de prioridad de forma predeterminada. Si incluye la instrucción en el nivel de jerarquía junto con la instrucción, la instrucción se omite y los mensajes se registran en formato de datos estructurados.`structured-data`[`edit system syslog file filename`]`explicit-priority`explicit-priority

Para obtener información acerca de la instrucción, vea Registrar mensajes en formato de datos estructurados.`structured-data`"Mensajes de registro en formato de datos estructurados" en la página 1341

Para incluir información de prioridad en mensajes dirigidos a un equipo remoto u otro motor de enrutamiento, incluya la instrucción en el nivel de jerarquía:`explicit-priority`[`edit system syslog host (hostname | other-routing-engine)`]

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
explicit-priority;
```

NOTA: La opción no se aplica a la serie QFX.`other-routing-engine`

La prioridad registrada en un mensaje siempre indica el nombre original de la instalación local. Si la instrucción se incluye para mensajes dirigidos a un destino remoto, la utilidad de registro del sistema de Junos OS seguirá utilizando el nombre de instalación alternativo para los propios mensajes cuando los dirige al destino remoto.`facility-override` Para obtener más información, consulte Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto."Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1388

Cuando se incluye la instrucción, la utilidad de registro de Junos OS antepone códigos para el nombre de la instalación y el nivel de gravedad al nombre de la etiqueta del mensaje, si el mensaje tiene uno:`explicit-priority`

```
FACILITY-severity[-TAG]
```

(La etiqueta es un identificador único asignado a algunos mensajes de registro del sistema Junos OS).

En el ejemplo siguiente, el mensaje pertenece a la instalación y se le asigna gravedad (6):`CHASSISD_PARSE_COMPLETEdaemoninfo`

```
Aug 21 12:36:30 router1 chassisd[522]: %DAEMON-6-CHASSISD_PARSE_COMPLETE: Using new configuration
```

Cuando no se incluye la instrucción, la prioridad no aparece en el mensaje:`explicit-priority`

```
Aug 21 12:36:30 router1 chassisd[522]: CHASSISD_PARSE_COMPLETE: Using new configuration
```

Códigos de instalación de registro del sistema y códigos numéricos consignados en la información de prioridad

Tabla 130 en la página 1345 enumera los códigos de instalación que pueden aparecer en los mensajes de registro del sistema y los asigna a nombres de instalaciones.

> **NOTA**: Si la segunda columna de no incluye el nombre de instalación de Junos OS para un código, la función no `Tabla 130` se puede incluir en una instrucción en el nivel jerárquico .[edit system syslog] Junos OS puede usar las funciones de (y otras que no aparecen en la lista) al informar sobre operaciones internas.Tabla 130 en la página 1345

Tabla 130: Códigos de instalaciones consignados en la información de prioridad

Código	Nombre de la instalación de Junos	Tipo de evento o error
`AUTH`	`authorization`	Intentos de autenticación y autorización
`AUTHPRIV`		Intentos de autenticación y autorización que solo pueden ver los superusuarios
`CHANGE`	`change-log`	Cambios en la configuración de Junos OS
`CONFLICT`	`conflict-log`	La configuración especificada no es válida en el tipo de enrutador

Tabla 130: Códigos de instalaciones consignados en la información de prioridad *(Continued)*

Código	Nombre de la instalación de Junos	Tipo de evento o error
CONSOLE		Mensajes escritos por la salida de la consola del kernel r**/dev/console**
CRON		Acciones realizadas o errores encontrados por el proceso cron
DAEMON	daemon	Acciones realizadas o errores encontrados por los procesos del sistema
DFC	dfc	Acciones realizadas o errores encontrados por el proceso de captura dinámica de flujo
FIREWALL	firewall	Acciones de filtrado de paquetes realizadas por un filtro de firewall
FTP	ftp	Acciones realizadas o errores encontrados por el proceso FTP
INTERACT	interactive-commands	Comandos emitidos en el símbolo del sistema de la CLI de Junos OS o invocados por una aplicación cliente, como un protocolo XML de Junos o un cliente NETCONF
KERN	kernel	Acciones realizadas o errores encontrados por el kernel de Junos
NTP		Acciones realizadas o errores encontrados por el protocolo de tiempo de red (NTP)
PFE	pfe	Acciones realizadas o errores encontrados por el motor de reenvío de paquetes
SYSLOG		Acciones realizadas o errores encontrados por la utilidad de registro del sistema de Junos
USER	user	Acciones realizadas o errores encontrados por los procesos del espacio de usuario

Tabla 131 en la página 1347 enumera los códigos numéricos de gravedad que pueden aparecer en los mensajes de registro del sistema y los asigna a niveles de gravedad.

Tabla 131: Códigos numéricos para los niveles de gravedad notificados en la información de prioridad

Código numérico	Nivel de gravedad	Description
0	emergency	Fallo del sistema u otra condición que hace que el e de funcionar
1	alert	Condiciones que requieren corrección inmediata, c de datos del sistema dañada
2	critical	Condiciones críticas, como errores graves
3	error	Condiciones de error que generalmente tienen con menos graves que los errores en los niveles de eme alerta y críticos
4	warning	Condiciones que justifican el monitoreo
5	notice	Condiciones que no son errores, pero que pueden j tratamiento especial
6	info	Eventos o condiciones de no error de interés
7	debug	Mensajes de depuración de software (solo aparecer representante de soporte técnico le ha indicado qu este nivel de gravedad)

Incluir el año o milisegundo en las marcas de tiempo

De forma predeterminada, la marca de tiempo registrada en un mensaje de registro del sistema de formato estándar especifica el mes, la fecha, la hora, el minuto y el segundo en que se registró el mensaje, como en el ejemplo siguiente:

```
Aug 21 12:36:30
```

Para incluir el año, el milisegundo o ambos en la marca de tiempo, incluya la instrucción en los niveles de jerarquía o :`time-format`[`edit system syslog`][`edit security log`]

```
[edit system syslog]
time-format (year | millisecond | year millisecond);
```

Sin embargo, la marca de tiempo para los mensajes traceoption se especifica en milisegundos de forma predeterminada y es independiente de la instrucción.[`edit system syslog time-format`]

La marca de tiempo modificada se utiliza en mensajes dirigidos a cada destino configurado por una instrucción , o en el nivel de jerarquía, pero no a destinos configurados por una instrucción.`file``console``user`[`edit system syslog`]`host`

> **NOTA**: De forma predeterminada, en una consola de FreeBSD, la información de tiempo adicional no está disponible en los mensajes de registro del sistema dirigidos a cada destino configurado por una instrucción.`host` Sin embargo, en una implementación específica de Junos OS que utilice la consola de FreeBSD, la información de tiempo adicional está disponible en los mensajes de registro del sistema dirigidos a cada destino.

En el ejemplo siguiente se muestra el formato de una marca de tiempo que incluye el milisegundo (401) y el año (2006):

```
Aug 21 12:36:30.401 2006
```

> **NOTA**: Los mensajes registrados en formato de datos estructurados incluyen el año y el milisegundo de forma predeterminada. Si incluye la instrucción de datos estructurados en el nivel de jerarquía junto con la instrucción, la instrucción se omite y los mensajes se registran en formato de datos estructurados.[`edit system syslog file` *`filename`*]`time-format`[`time-format`]

Para obtener información acerca de la instrucción, vea Registrar mensajes en formato de datos estructurados.`structured-data`"Mensajes de registro en formato de datos estructurados" en la página 1341

Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados

Las instalaciones predefinidas agrupan mensajes relacionados, pero también puede hacer coincidir los mensajes con cadenas y expresiones regulares para refinar qué mensajes de una instalación se registran en un archivo, un terminal de usuario o un destino remoto.

Las instrucciones y configuración permiten hacer coincidir los mensajes de registro del sistema con una cadena o una expresión regular, respectivamente.`match-stringsmatch` Puede incluir estas instrucciones en los siguientes niveles jerárquicos:

- `[edit system syslog file filename]` (para un archivo)
- `[edit system syslog user (username | *)]` (para una sesión de usuario específica o para todas las sesiones de usuario en un terminal)
- `[edit system syslog host (hostname | other-routing-engine)]` (para un destino remoto)

Para evaluar los mensajes con respecto a una expresión regular y registrar únicamente los mensajes coincidentes en el destino dado, incluya la instrucción y especifique la expresión regular:`match`

```
match "regular-expression";
```

A partir de Junos OS versión 16.1, puede utilizar comparaciones de cadenas simples para filtrar mensajes de forma más eficaz, ya que requiere menos CPU que hacer coincidir con expresiones regulares complejas. Para especificar la cadena de texto que debe aparecer en un mensaje para que el mensaje se registre en un destino, incluya la instrucción y especifique la cadena o lista de cadenas coincidentes:`match-strings`

```
match-strings string-name;
```

```
match-strings [string1 string2];
```

Las instrucciones y seleccionan mensajes con la facilidad y la gravedad configuradas que coinciden con la cadena o expresión regular dadas.`match-stringsmatch` La instrucción realiza una comparación de cadena simple y, como resultado, consume menos CPU que usar la instrucción para hacer coincidir con expresiones regulares complejas.`match-stringsmatch` Si configura las instrucciones y para el mismo destino, Junos OS evaluará primero la condición; si el mensaje incluye alguna de las subcadenas configuradas, se registrará el mensaje y no se evaluará la condición.`matchmatch-stringsmatch-stringsmatch` Si no se cumple la condición, el sistema evalúa el mensaje con respecto a la expresión regular de la instrucción de configuración.`match-stringsmatch`

Al especificar expresiones regulares para la instrucción, utilice la notación definida en POSIX Standard 1003.2 para expresiones regulares UNIX extendidas (modernas).`match` Explicar la sintaxis de expresión regular está fuera del alcance de este documento, pero los estándares POSIX están disponibles en el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, http://www.ieee.org).http://www.ieee.org

Tabla 132 en la página 1350 Especifica qué carácter o caracteres coinciden con algunos de los operadores de expresiones regulares que puede utilizar en la instrucción Match. En las descripciones, el término término se refiere a un solo carácter alfanumérico o un conjunto de caracteres encerrados entre corchetes, paréntesis o llaves.

NOTA: La instrucción no distingue entre mayúsculas y minúsculas.`match`

Tabla 132: Operadores de expresión regular para la instrucción match

Operador	Partidos
. (punto)	Una instancia de cualquier carácter excepto el espacio.
* (asterisco)	Cero o más instancias del término inmediatamente anterior.
+ (signo más)	Una o más instancias del término inmediatamente anterior.
? (signo de interrogación)	Cero o una instancia del término inmediatamente anterior.
| (tubería)	Uno de los términos que aparece a cada lado del operador de tubería.
! (signo de exclamación)	Cualquier cadena excepto la especificada por la expresión, cuando el signo de exclamación aparece al principio de la expresión. El uso del signo de exclamación es específico de Junos OS.

Tabla 132: Operadores de expresión regular para la instrucción match *(Continued)*

Operador	Partidos
^ (intercalación)	Inicio de una línea, cuando el símbolo de intercalación aparece fuera de los corchetes. Una instancia de cualquier carácter que no lo siga entre corchetes, cuando el símbolo de intercalación es el primer carácter entre corchetes.
$ (signo de dólar)	Fin de una línea.
[ ] (corchetes pareados)	Una instancia de uno de los caracteres alfanuméricos adjuntos. Para indicar un rango de caracteres, utilice un guión (-) para separar los caracteres iniciales y finales del rango. Por ejemplo, [a-z0-9] coincide con cualquier letra o número.
( ) (paréntesis pareados)	Una instancia del valor evaluado del término adjunto. Los paréntesis se utilizan para indicar el orden de evaluación en la expresión regular.

Uso de cadenas y expresiones regulares

Filtre los mensajes que pertenecen a la instalación, dirigiendo aquellos que incluyen la cadena al terminal del usuario raíz:`interactive-commandsconfigure`

```
[edit system syslog]
user root {
    interactive-commands any;
    match-strings configure;
}
```

Mensajes como los siguientes aparecen en el terminal del usuario cuando un usuario emite un comando para entrar en el modo de configuración:`rootconfigure`

```
timestamp router-name mgd[PID]: UI_CMDLINE_READ_LINE: User 'user', command 'configure private'
```

Filtre los mensajes que pertenecen a la instalación y tienen una gravedad de o superior, dirigiéndolos al archivo .`daemonerror`**/var/log/process-errors** Omita los mensajes generados por el proceso SNMP (snmpd), dirigiéndolos en su lugar al archivo :**/var/log/snmpd-errors**

```
[edit system syslog]
file process-errors {
```

```
    daemon error;
    match "!(.*snmpd.*)";
}
file snmpd-errors {
    daemon error;
    match-strings snmpd;
}
```

Junos System registra operadores de expresiones regulares para la instrucción match

Tabla 133: Operadores de expresión regular para la instrucción match

Operador	Partidos
. (punto)	Una instancia de cualquier carácter excepto el espacio.
* (asterisco)	Cero o más instancias del término inmediatamente anterior.
+ (signo más)	Una o más instancias del término inmediatamente anterior.
? (signo de interrogación)	Cero o una instancia del término inmediatamente anterior.
| (tubería)	Uno de los términos que aparecen a cada lado del operador de tubería.
! (signo de exclamación)	Cualquier cadena excepto la especificada por la expresión, cuando signo de exclamación aparece al principio de la expresión. El uso d signo de exclamación es específico de Junos OS.
^ (intercalación)	El principio de una línea, cuando el símbolo de intercalación apare fuera de los corchetes. Una instancia de cualquier carácter que no lo siga entre corchetes cuando el símbolo de intercalación es el primer carácter entre corchetes.

Tabla 133: Operadores de expresión regular para la instrucción match *(Continued)*

Operador	Partidos
$ (signo de dólar)	El final de una línea.
[ ] (entre corchetes)	Una instancia de uno de los caracteres alfanuméricos adjuntos. Pa indicar un intervalo de caracteres, utilice un guión ( ) para separar caracteres iniciales y finales del intervalo.- Por ejemplo, coincide cualquier letra o número.`[a-z0-9]`
( ) (paréntesis pareados)	Una instancia del valor evaluado del término adjunto. Los parénte se utilizan para indicar el orden de evaluación en la expresión regu

Deshabilitar el registro del sistema de una instalación

Para deshabilitar el registro de mensajes que pertenecen a una instalación determinada, incluya la instrucción en la configuración.*`facility`* `none` Esta instrucción es útil cuando, por ejemplo, desea registrar mensajes que tienen el mismo nivel de gravedad y pertenecen a todas las instalaciones, excepto a unas pocas. En lugar de incluir una instrucción para cada instalación que desee registrar, puede incluir la instrucción y, a continuación, una instrucción para cada instalación que no desee registrar.`any` *`severityfacility`* `none` Por ejemplo, a continuación se registran todos los mensajes del nivel o superior en la consola, excepto los mensajes de las instalaciones y `.errordaemonkernel` Los mensajes de esas instalaciones se registran en el archivo en su lugar:**>/var/log/internals**

```
[edit system syslog]
console {
    any error;
    daemon none;
    kernel none;
}
file internals {
    daemon info;
    kernel info;
}
```

Ejemplos: Configurar el registro del sistema

En el ejemplo siguiente se muestra cómo configurar el registro de mensajes sobre todos los comandos introducidos por los usuarios en el símbolo del sistema de la CLI o invocados por aplicaciones cliente como el protocolo XML de Junos OS o las aplicaciones cliente NETCONF, y todos los intentos de autenticación o autorización, tanto al archivo como al terminal de cualquier usuario que haya iniciado sesión:**cli-commands**

```
[edit system]
syslog {
    file cli-commands {
        interactive-commands info;
        authorization info;
    }
    user * {
        interactive-commands info;
        authorization info;
    }
}
```

En el ejemplo siguiente se muestra cómo configurar el registro de todos los cambios en el estado de alarmas en el archivo :**/var/log/alarms**

```
[edit system]
syslog {
    file alarms {
        kernel warning;
    }
}
```

En el ejemplo siguiente se muestra cómo configurar el control de mensajes de varios tipos, como se describe en los comentarios. La información se registra en dos archivos, en el terminal de usuario , en una máquina remota y en la consola:`alex`

```
[edit system]
syslog {
    /* write all security-related messages to file /var/log/security */
    file security {
        authorization info;
        interactive-commands info;
```

```
    }
    /* write messages about potential problems to file /var/log/messages: */
    /* messages from "authorization" facility at level "notice" and above, */
    /* messages from all other facilities at level "warning" and above */
    file messages {
        authorization notice;
        any warning;
    }
    /* write all messages at level "critical" and above to terminal of user "alex" if */
    /* that user is logged in */
    user alex {
        any critical;
    }
    /* write all messages from the "daemon" facility at level "info" and above, and */
    /* messages from all other facilities at level "warning" and above, to the */
    /* machine monitor.mycompany.com */
    host monitor.mycompany.com {
        daemon info;
        any warning;
    }
    /* write all messages at level "error" and above to the system console */
    console {
        any error;
    }
}
```

En el ejemplo siguiente se muestra cómo configurar el control de los mensajes generados cuando los usuarios emiten comandos de la CLI de Junos OS especificando la función en los siguientes niveles de gravedad:`interactive-commands`

- `info`: registra un mensaje cuando los usuarios emiten algún comando en el indicador del modo operativo o de configuración de la CLI. En el ejemplo se escriben los mensajes en el archivo **./var/log/user-actions**
- : registra un mensaje cuando los usuarios emiten los comandos del modo de configuración y `.noticerollbackcommit` En el ejemplo se escriben los mensajes en el terminal de usuario `.philip`
- `warning`: registra un mensaje cuando los usuarios emiten un comando que reinicia un proceso de software. En el ejemplo se escriben los mensajes en la consola.

```
[edit system]
syslog {
    file user-actions {
```

```
        interactive-commands info;
    }
    user philip {
        interactive-commands notice;
    }
    console {
        interactive-commands warning;
    }
}
```

Ejemplos: Asignar una instalación alternativa

Registre todos los mensajes generados en la plataforma de enrutamiento local en el nivel de error o superior a la instalación en la máquina remota llamada :`local0monitor.mycompany.com`

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

Configure plataformas de enrutamiento ubicadas en California y plataformas de enrutamiento ubicadas en Nueva York para enviar mensajes a una única máquina remota llamada .`central-logger.mycompany.com` A los mensajes de California se les asigna una instalación alternativa y los mensajes de Nueva York se asignan a una instalación alternativa.`local0local2`

- Configure las plataformas de enrutamiento de California para agregar mensajes en la instalación:`local0`

```
[edit system syslog]
host central-logger.mycompany.com {
    change-log info;
    facility-override local0;
}
```

- Configure las plataformas de enrutamiento de Nueva York para agregar mensajes en la instalación:`local2`

```
[edit system syslog]
host central-logger.mycompany.com {
    change-log info;
    facility-override local2;
}
```

A continuación, puede configurar la utilidad de registro del sistema para escribir mensajes desde la instalación en el archivo y los mensajes de la instalación en el archivo .`central-loggerlocal0california-configlocal2new-york-config`

Registro del sistema para un enrutador TX Matrix o TX Matrix Plus

in this section

- Configuración del registro del sistema para un enrutador TX Matrix | **1358**
- Configuración del registro del sistema para un enrutador TX Matrix Plus | **1360**
- Configuración del reenvío de mensajes al enrutador de matriz de transmisión | **1362**
- Configuración del reenvío de mensajes al enrutador TX Matrix Plus | **1363**
- Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix | **1365**
- Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix Plus | **1368**
- Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix | **1371**
- Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix Plus | **1373**
- Configuración del registro del sistema de manera diferente en cada enrutador T640 en una matriz de enrutamiento | **1375**
- Configuración del registro del sistema de manera diferente en cada enrutador T1600 o T4000 en una matriz de enrutamiento | **1377**

Configuración del registro del sistema para un enrutador TX Matrix

Para configurar el registro del sistema para todos los enrutadores de una matriz de enrutamiento compuesta por un enrutador de matriz de transmisión y enrutadores T640, incluya la instrucción en el nivel de jerarquía en el enrutador de matriz de transmisión.`syslog`[`edit system`] La instrucción se aplica a todos los enrutadores de la matriz de enrutamiento.`syslog`

```
[edit system]
syslog {
    archive <files number> <size size <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url  <password password>}> <files number> <size size> <start-
time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | scc-master) {
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
        source-address source-address;
        port port number;
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
     (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

Cuando se incluyen en la configuración del enrutador TX Matrix, las siguientes instrucciones de configuración tienen el mismo efecto que en un sistema de chasis único, excepto que se aplican a todos los enrutadores de la matriz de enrutamiento:

- `archive`: define el tamaño y el número de archivos de registro en cada plataforma de la matriz de enrutamiento. Consulte Especificación del tamaño, el número y las propiedades de archivado del archivo de registro."Especificar el tamaño, el número y las propiedades de archivado del archivo de registro" en la página 1341

- `console`: dirige los mensajes especificados a la consola de cada plataforma de la matriz de enrutamiento. Consulte Dirigir mensajes de registro del sistema a la consola."Dirija los mensajes de registro del sistema a la consola" en la página 1385

- `file`: dirige los mensajes especificados a un archivo con el mismo nombre en cada plataforma de la matriz de enrutamiento. Consulte Dirigir mensajes de registro del sistema a un archivo de registro."Dirija los mensajes de registro del sistema a un archivo de registro" en la página 1383

- `match`: limita el conjunto de mensajes registrados en un destino a aquellos que contienen (o no contienen) una cadena de texto que coincide con una expresión regular. Consulte Uso de cadenas y expresiones regulares para refinar el conjunto de mensajes registrados."Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

  La instrucción separada en el nivel de jerarquía se aplica a los mensajes reenviados desde los enrutadores T640 al enrutador TX Matrix.`match`[`edit system syslog host scc-master`] Consulte Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix."Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix" en la página 1371

- `port`: especifica el número de puerto del servidor syslog remoto.

- : establece la dirección IP del enrutador que se informará en los mensajes de registro del sistema como origen de mensajes, cuando los mensajes se dirigen a los equipos remotos especificados en todas las instrucciones en el nivel jerárquico, para cada plataforma de la matriz de enrutamiento.`source-address`*hostname*[`edit system syslog`] En una matriz de enrutamiento compuesta por un enrutador TX Matrix y enrutadores T640, los enrutadores T640 no informan la dirección en mensajes dirigidos al otro motor de enrutamiento en cada enrutador o al enrutador TX Matrix. Consulte Especificación de una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto."Especificar una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1387

- `structured-data`: escribe mensajes en un archivo en formato de datos estructurados. Consulte Registro de mensajes en formato de datos estructurados."Mensajes de registro en formato de datos estructurados" en la página 1341

- `time-format`: agrega el milisegundo, el año o ambos a la marca de tiempo en cada mensaje de formato estándar. Consulte Incluir el año o milisegundo en las marcas de tiempo."Incluir el año o milisegundo en las marcas de tiempo" en la página 1348

- `user`: dirige los mensajes especificados a la sesión de terminal de uno o más usuarios especificados en cada plataforma de la matriz de enrutamiento en la que han iniciado sesión. Consulte Dirigir mensajes de registro del sistema a un terminal de usuario."Dirigir mensajes de registro del sistema a un terminal de usuario" en la página 1384

El efecto de las otras instrucciones difiere un poco para una matriz de enrutamiento que para un sistema de chasis único.

Configuración del registro del sistema para un enrutador TX Matrix Plus

Desde la perspectiva de la interfaz de usuario, la matriz de enrutamiento aparece como un único enrutador. El enrutador TX Matrix Plus (también llamado SFC de chasis de estructura de conmutador) controla todos los enrutadores T1600 o T4000 (también llamados LCC de chasis de tarjeta de línea) en la matriz de enrutamiento.

Para configurar el registro del sistema para todos los enrutadores en una matriz de enrutamiento compuesta por un enrutador TX Matrix Plus con LCC T1600 o T4000 conectadas, incluya la instrucción en el nivel de jerarquía en el SFC.`syslog[edit system]` La instrucción se aplica a todos los enrutadores de la matriz de enrutamiento.`syslog`

```
[edit system]
syslog {
    archive <files number> <size size <world-readable | no-world-readable>;
    console {
        facility severity;
    }
    file filename {
        facility severity;
        archive <archive-sites {ftp-url  <password password>}> <files number> <size size> <start-
time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
        explicit-priority;
        match "regular-expression";
        structured-data {
            brief;
        }
    }
    host (hostname | other-routing-engine | sfc0-master) {
```

```
        facility severity;
        explicit-priority;
        facility-override facility;
        log-prefix string;
        match "regular-expression";
    }
    source-address source-address;
    time-format (year | millisecond | year millisecond);
     (username | *) {
        facility severity;
        match "regular-expression";
    }
}
```

Cuando se incluyen en la configuración del enrutador TX Matrix Plus, las siguientes instrucciones de configuración tienen el mismo efecto que en un sistema de chasis único, excepto que se aplican a todos los enrutadores de la matriz de enrutamiento.

- `archive`: define el tamaño y el número de archivos de registro en cada enrutador de la matriz de enrutamiento. Consulte Especificación del tamaño, el número y las propiedades de archivado del archivo de registro."Especificar el tamaño, el número y las propiedades de archivado del archivo de registro" en la página 1341

- `console`: dirige los mensajes especificados a la consola de cada enrutador de la matriz de enrutamiento. Consulte Dirigir mensajes de registro del sistema a la consola."Dirija los mensajes de registro del sistema a la consola" en la página 1385

- `file`: dirige los mensajes especificados a un archivo con el mismo nombre en cada enrutador de la matriz de enrutamiento. Consulte Dirigir mensajes de registro del sistema a un archivo de registro."Dirija los mensajes de registro del sistema a un archivo de registro" en la página 1383

- `match`: limita el conjunto de mensajes registrados en un destino a aquellos que contienen (o no contienen) una cadena de texto que coincide con una expresión regular. Consulte Uso de cadenas y expresiones regulares para refinar el conjunto de mensajes registrados."Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

  La instrucción independiente en el nivel de jerarquía se aplica a los mensajes reenviados desde las LCC T1600 o T4000 al SFC.`match`[`edit system syslog host sfc0-master`] Consulte Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix Plus."Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix Plus" en la página 1373

- : establece la dirección IP del enrutador como origen de mensajes en los mensajes de registro del sistema cuando los mensajes se dirigen a los equipos remotos especificados en todas las instrucciones en el nivel jerárquico, para cada enrutador de la matriz de enrutamiento.`source-addresshost` *`hostname`*[`edit system syslog`] En una matriz de enrutamiento compuesta por un enrutador TX

Matrix Plus con LCC T1600 o T4000 conectadas, los enrutadores T1600 o T4000 no informan la dirección en mensajes dirigidos al otro motor de enrutamiento en cada enrutador o al enrutador TX Matrix Plus. Consulte Especificación de una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto."Especificar una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1387

- `structured-data`: escribe mensajes en un archivo en formato de datos estructurados. Consulte Registro de mensajes en formato de datos estructurados."Mensajes de registro en formato de datos estructurados" en la página 1341
- `time-format`: agrega el milisegundo, el año o ambos a la marca de tiempo en cada mensaje de formato estándar. Consulte Incluir el año o milisegundo en las marcas de tiempo."Incluir el año o milisegundo en las marcas de tiempo" en la página 1348
- `user`: dirige los mensajes especificados a la sesión de terminal de uno o más usuarios especificados en cada enrutador de la matriz de enrutamiento en la que han iniciado sesión. Consulte Dirigir mensajes de registro del sistema a un terminal de usuario."Dirigir mensajes de registro del sistema a un terminal de usuario" en la página 1384

El efecto de las otras instrucciones difiere un poco para una matriz de enrutamiento que para un sistema de chasis único.

Configuración del reenvío de mensajes al enrutador de matriz de transmisión

De forma predeterminada, el motor de enrutamiento primario de cada enrutador T640 reenvía al motor de enrutamiento primario del enrutador TX Matrix todos los mensajes de todas las instalaciones con un nivel de gravedad superior o superior .`info` Para cambiar la instalación, el nivel de gravedad o ambos, incluya la instrucción en el nivel de jerarquía en el enrutador TX Matrix:`host scc-master[edit system syslog]`

```
[edit system syslog]
host scc-master {
    facility severity;
}
```

Para deshabilitar el reenvío de mensajes, establezca la función en y el nivel de gravedad en :`anynone`

```
[edit system syslog]
host scc-master {
```

```
    any none;
}
```

En cualquier caso, la configuración se aplica a todos los enrutadores T640 de la matriz de enrutamiento.

Para capturar los mensajes reenviados por los enrutadores T640 (así como los mensajes generados en el enrutador TX Matrix), también debe configurar el registro del sistema en el enrutador TX Matrix. Dirija los mensajes a uno o más destinos incluyendo las instrucciones apropiadas en el nivel de jerarquía en el enrutador TX Matrix:`[edit system syslog]`

- A un archivo, como se describe en Dirigir mensajes de registro del sistema a un archivo de registro."Dirija los mensajes de registro del sistema a un archivo de registro" en la página 1383
- A la sesión de terminal de uno o más usuarios específicos (o todos los usuarios), como se describe en Dirigir mensajes de registro del sistema a un terminal de usuario."Dirigir mensajes de registro del sistema a un terminal de usuario" en la página 1384
- A la consola, como se describe en Dirigir mensajes de registro del sistema a la consola."Dirija los mensajes de registro del sistema a la consola" en la página 1385
- A un equipo remoto que ejecuta la utilidad syslogd o al otro motor de enrutamiento. Para obtener más información, consulte Dirigir mensajes a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión."Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión" en la página 1394

Como se indicó anteriormente, las instrucciones de configuración incluidas en el enrutador TX Matrix también configuran los mismos destinos en cada enrutador T640 de la matriz de enrutamiento.

Al especificar el nivel de gravedad para los mensajes locales (en el nivel de jerarquía) y los mensajes reenviados (en el nivel de jerarquía), puede establecer el mismo nivel de gravedad para ambos, establecer un nivel de gravedad más bajo para los mensajes locales o establecer un nivel de gravedad más alto para los mensajes locales.`[edit system syslog (file | host | console | user)][edit system syslog host scc-master]` En los ejemplos siguientes se describen las consecuencias de cada configuración. (Para simplificar, los ejemplos usan la facilidad en todos los casos.`any` También puede especificar diferentes gravedades para diferentes instalaciones, con consecuencias más complejas).

Configuración del reenvío de mensajes al enrutador TX Matrix Plus

Desde la perspectiva de la interfaz de usuario, la matriz de enrutamiento aparece como un único enrutador. El enrutador TX Matrix Plus (también llamado SFC de chasis de estructura de conmutador) controla todos los enrutadores T1600 o T4000 (también llamados LCC de chasis de tarjeta de línea) en la matriz de enrutamiento.

De forma predeterminada, el motor de enrutamiento principal de cada LCC T1600 o T4000 conectada reenvía al motor de enrutamiento primario del SFC todos los mensajes de todas las instalaciones con un nivel de gravedad superior o superior .`info` Para cambiar la instalación, el nivel de gravedad o ambos, incluya la instrucción en el nivel de jerarquía en el SFC:`host sfc0-master[edit system syslog]`

```
[edit system syslog]
host sfc0-master {
    facility severity;
}
```

Para deshabilitar el reenvío de mensajes, establezca la función en y el nivel de gravedad en :`anynone`

```
[edit system syslog]
host sfc0-master {
    any none;
}
```

En cualquier caso, la configuración se aplica a todas las LCC conectadas en la matriz de enrutamiento.

Para capturar los mensajes reenviados por las LCC T1600 o T4000 (así como los mensajes generados en el propio SFC), también debe configurar el registro del sistema en el SFC. Dirija los mensajes a uno o más destinos incluyendo las instrucciones apropiadas en el nivel jerárquico del SFC:`[edit system syslog]`

- A un archivo, como se describe en Dirigir mensajes de registro del sistema a un archivo de registro."Dirija los mensajes de registro del sistema a un archivo de registro" en la página 1383
- A la sesión de terminal de uno o más usuarios específicos (o todos los usuarios), como se describe en Dirigir mensajes de registro del sistema a un terminal de usuario."Dirigir mensajes de registro del sistema a un terminal de usuario" en la página 1384
- A la consola, como se describe en Dirigir mensajes de registro del sistema a la consola."Dirija los mensajes de registro del sistema a la consola" en la página 1385
- A un equipo remoto que ejecuta la utilidad syslogd o al otro motor de enrutamiento. Para obtener más información, consulte Dirigir mensajes a un destino remoto desde la matriz de enrutamiento basada en un enrutador de transmisión Matrix Plus."Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en un enrutador TX Matrix Plus" en la página 1395

Como se indicó anteriormente, las instrucciones de configuración incluidas en el SFC también configuran los mismos destinos en cada LCC conectada.

Al especificar el nivel de gravedad para los mensajes locales (en el nivel de jerarquía) y los mensajes reenviados (en el nivel de jerarquía), puede establecer el mismo nivel de gravedad para ambos, establecer un nivel de gravedad más bajo para los mensajes locales o establecer un nivel de gravedad

más alto para los mensajes locales.`[edit system syslog (file | host | console | user)][edit system syslog host sfc0-master]` En los ejemplos siguientes se describen las consecuencias de cada configuración. (Para simplificar, los ejemplos usan la facilidad en todos los casos.`any` También puede especificar diferentes gravedades para diferentes instalaciones, con consecuencias más complejas).

Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix

in this section

- Mensajes registrados cuando los niveles de gravedad local y reenviado son los mismos | **1365**
- Mensajes registrados cuando el nivel de gravedad local es menor | **1366**
- Mensajes registrados cuando el nivel de gravedad local es mayor | **1367**

En este tema se describe el impacto de los diferentes niveles de gravedad locales y reenviados configurados para los mensajes de registro del sistema en un enrutador TX Matrix:

Mensajes registrados cuando los niveles de gravedad local y reenviado son los mismos

Cuando el nivel de gravedad es el mismo para los mensajes locales y reenviados, el registro en el enrutador TX Matrix contiene todos los mensajes de los registros de los enrutadores T640. Por ejemplo, puede especificar la gravedad del archivo, que es el nivel de gravedad predeterminado para los mensajes reenviados por los enrutadores T640:`info`**/var/log/messages**

```
[edit system syslog]
file messages {
    any info;
}
```

Tabla 134 en la página 1366 especifica qué mensajes se incluyen en los registros de los enrutadores T640 y del enrutador TX Matrix.

Tabla 134: Ejemplo: El nivel de gravedad local y reenviado son información

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador T640	Local	`info`
Enrutador de matriz de transmisión	Local	`info`
	Reenviado desde enrutadores T640	`info`

Mensajes registrados cuando el nivel de gravedad local es menor

Cuando el nivel de gravedad es menor para los mensajes locales que para los mensajes reenviados, el registro en el enrutador TX Matrix incluye menos mensajes reenviados que cuando las gravedades son las mismas. Los mensajes generados localmente se siguen registrando en el nivel de gravedad más bajo, por lo que su número en cada registro es el mismo que cuando las gravedades son las mismas.

Por ejemplo, en un enrutador TX Matrix, puede especificar la gravedad del archivo y la gravedad de los mensajes reenviados:`notice`**/var/log/messages**`critical`

```
[edit system syslog]
file messages {
    any notice;
}
host scc-master {
    any critical;
}
```

Tabla 135 en la página 1366 especifica qué mensajes de una matriz de enrutamiento se incluyen en los registros de los enrutadores T640 y TX. Los enrutadores T640 reenvían solo aquellos mensajes con gravedad o superior, por lo que el registro en el enrutador TX Matrix no incluye los mensajes con gravedad , o que los enrutadores T640 registran localmente.`criticalerrorwarningnotice`

Tabla 135: Ejemplo: Se nota la gravedad local, la gravedad reenviada es crítica

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador T640	Local	`notice`

Tabla 135: Ejemplo: Se nota la gravedad local, la gravedad reenviada es crítica *(Continued)*

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador de matriz de transmisión	Local	`notice`
	Reenviado desde enrutadores T640	`critical`

Mensajes registrados cuando el nivel de gravedad local es mayor

Cuando el nivel de gravedad es mayor para los mensajes locales que para los mensajes reenviados, el registro en el enrutador TX Matrix incluye menos mensajes reenviados que cuando las gravedades son las mismas y todos los registros locales contienen menos mensajes en general.

Por ejemplo, puede especificar la gravedad del archivo y la gravedad de los mensajes reenviados:`critical`**/var/log/messages**`notice`

```
[edit system syslog]
file messages {
    any critical;
}
host scc-master {
    any notice;
}
```

Tabla 136 en la página 1367 especifica qué mensajes se incluyen en los registros de los enrutadores T640 y del enrutador TX Matrix. Aunque los enrutadores T640 reenvían mensajes con gravedad o superior, el enrutador TX Matrix descarta cualquiera de esos mensajes con gravedad inferior a (no registra los mensajes reenviados con gravedad , , o).`noticecriticalerrorwarningnotice` Ninguno de los registros incluye mensajes con gravedad o inferior.`error`

Tabla 136: Ejemplo: La gravedad local es crítica, la gravedad reenviada se nota

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador T640	Local	`critical`

Tabla 136: Ejemplo: La gravedad local es crítica, la gravedad reenviada se nota *(Continued)*

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador de matriz de transmisión	Local	`critical`
	Reenviado desde enrutadores T640	`critical`

Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix Plus

in this section

- Mensajes registrados cuando los niveles de gravedad local y reenviado son los mismos | **1368**
- Mensajes registrados cuando el nivel de gravedad local es menor | **1369**
- Mensajes registrados cuando el nivel de gravedad local es mayor | **1370**

En este tema se describe el impacto de los diferentes niveles de gravedad locales y reenviados configurados para los mensajes de registro del sistema en un enrutador TX Matrix Plus:

Mensajes registrados cuando los niveles de gravedad local y reenviado son los mismos

Cuando el nivel de gravedad es el mismo para los mensajes locales y reenviados, el registro en el enrutador TX Matrix Plus contiene todos los mensajes de los registros de los enrutadores T1600 en la matriz de enrutamiento. Por ejemplo, puede especificar la gravedad del archivo, que es el nivel de gravedad predeterminado para los mensajes reenviados por los enrutadores T1600:`info`**/var/log/messages**

```
[edit system syslog]
file messages {
    any info;
}
```

Tabla 137 en la página 1369 especifica qué mensajes de una matriz de enrutamiento basada en un enrutador TX Matrix Plus se incluyen en los registros de los enrutadores T1600 y TX Matrix Plus:

Tabla 137: Ejemplo: El nivel de gravedad local y reenviado son información

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador T1600	Local	`info`
enrutador de transmisión Matrix Plus	Local	`info`
	Reenviado desde enrutadores T1600	`info`

Mensajes registrados cuando el nivel de gravedad local es menor

Cuando el nivel de gravedad es menor para los mensajes locales que para los mensajes reenviados, el registro en el enrutador de TX Matrix Plus incluye menos mensajes reenviados que cuando las gravedades son las mismas. Los mensajes generados localmente se siguen registrando en el nivel de gravedad más bajo, por lo que su número en cada registro es el mismo que cuando las gravedades son las mismas.

Por ejemplo, en un enrutador TX Matrix Plus, puede especificar la gravedad del archivo y la gravedad de los mensajes reenviados:`notice`**/var/log/messages**`critical`

```
[edit system syslog]
file messages {
    any notice;
}
host sfc0-master {
    any critical;
}
```

Tabla 138 en la página 1370 especifica qué mensajes de una matriz de enrutamiento se incluyen en los registros de los enrutadores T1600 y TX Matrix Plus. Los enrutadores T1600 reenvían solo aquellos mensajes con gravedad o superior, por lo que el registro en el enrutador TX Matrix Plus no incluye los mensajes con gravedad , o que los enrutadores T1600 registran localmente.`criticalerrorwarningnotice`

Tabla 138: Ejemplo: Se nota la gravedad local, la gravedad reenviada es crítica

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador T1600	Local	`notice`
enrutador de transmisión Matrix Plus	Local	`notice`
	Reenviado desde enrutadores T1600	`critical`

Mensajes registrados cuando el nivel de gravedad local es mayor

Cuando el nivel de gravedad es mayor para los mensajes locales que para los mensajes reenviados, el registro en el enrutador TX Matrix Plus incluye menos mensajes reenviados que cuando las gravedades son las mismas, y todos los registros locales contienen menos mensajes en general.

Por ejemplo, puede especificar la gravedad del archivo y la gravedad de los mensajes reenviados:`critical`**/var/log/messages**`notice`

```
[edit system syslog]
file messages {
    any critical;
}
host sfc0-master {
    any notice;
}
```

Tabla 139 en la página 1371 especifica qué mensajes se incluyen en los registros de los enrutadores T1600 y TX Matrix Plus. Aunque los enrutadores T1600 reenvían mensajes con gravedad o superior, el enrutador TX Matrix Plus descarta cualquiera de esos mensajes con gravedad inferior a (no registra los mensajes reenviados con gravedad , , o).`notice``critical``error``warning``notice` Ninguno de los registros incluye mensajes con gravedad o inferior.`error`

Tabla 139: Ejemplo: La gravedad local es crítica, la gravedad reenviada se nota

Ubicación del registro	Origen de los mensajes	Gravedad más baja incluida
Enrutador T1600	Local	`critical`
enrutador de transmisión Matrix Plus	Local	`critical`
	Reenviado desde enrutadores T1600	`critical`

Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix

in this section

- Incluir información de prioridad en los mensajes reenviados | **1372**
- Agregar una cadena de texto a mensajes reenviados | **1373**
- Usar expresiones regulares para refinar el conjunto de mensajes reenviados | **1373**

Para configurar funciones opcionales adicionales al especificar cómo los enrutadores T640 reenvían mensajes al enrutador TX Matrix, incluya instrucciones en el nivel de jerarquía.`[edit system syslog host scc-master]` Para incluir información de prioridad (instalación y nivel de gravedad) en cada mensaje reenviado, incluya la instrucción.`explicit-priority` Para insertar una cadena de texto en cada mensaje reenviado, incluya la instrucción.`log-prefix` Para usar la coincidencia de expresiones regulares para especificar con mayor exactitud qué mensajes de una instalación se reenvían, incluya la instrucción.`match`

```
[edit system syslog]
host scc-master {
    facility severity;
    explicit-priority;
    log-prefix string;
```

```
    match "regular-expression";
}
```

También puede incluir la instrucción en el nivel jerárquico , pero no se recomienda hacerlo.`facility-override`[`edit system syslog host scc-master`] No es necesario utilizar funciones alternativas para los mensajes reenviados al enrutador TX Matrix, ya que ejecuta la utilidad de registro del sistema Junos y puede interpretar las funciones específicas de Junos OS. Para obtener más información acerca de las instalaciones alternativas, consulte Cambiar el nombre de la instalación alternativa para los mensajes de registro del sistema dirigidos a un destino remoto."Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1388

Incluir información de prioridad en los mensajes reenviados

Cuando se incluye la instrucción en el nivel jerárquico, los mensajes reenviados al enrutador TX Matrix incluyen información de prioridad.`explicit-priority`[`edit system syslog host scc-master`] Para que la información aparezca en un archivo de registro en el enrutador TX Matrix, también debe incluir la instrucción en el nivel de jerarquía para el archivo en el enrutador TX Matrix.`explicit-priority`[`edit system syslog file` *`filename`*] Como consecuencia, el archivo de registro con el mismo nombre en cada plataforma de la matriz de enrutamiento también incluye información de prioridad para los mensajes generados localmente.

Para incluir información de prioridad en mensajes dirigidos a un equipo remoto desde todos los enrutadores de la matriz de enrutamiento, incluya también la instrucción en el nivel de jerarquía del equipo remoto.`explicit-priority`[`edit system syslog host` *`hostname`*] Para obtener más información, consulte Dirigir mensajes a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión."Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión" en la página 1394

En el ejemplo siguiente, el archivo en todos los enrutadores incluye información de prioridad para mensajes con gravedad y superior de todas las instalaciones.**/var/log/messages**`notice` El registro en el enrutador TX Matrix también incluye mensajes con esas características reenviados desde los enrutadores T640.

```
[edit system syslog]
host scc-master {
    any notice;
    explicit-priority;
}
file messages {
    any notice;
    explicit-priority;
}
```

Agregar una cadena de texto a mensajes reenviados

Cuando se incluye la instrucción en el nivel de jerarquía, la cadena que se define aparece en cada mensaje reenviado al enrutador de matriz de transmisión.`log-prefix`[`edit system syslog host scc-master`] Para obtener más información, consulte Agregar una cadena de texto a mensajes de registro del sistema dirigidos a un destino remoto."Agregar una cadena de texto a los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1387

Usar expresiones regulares para refinar el conjunto de mensajes reenviados

Cuando se incluye la instrucción en el nivel de jerarquía, la expresión regular que especifique controla qué mensajes de los enrutadores T640 se reenvían al enrutador de matriz de TX.`match`[`edit system syslog host scc-master`] La expresión regular no se aplica a los mensajes del enrutador T640 dirigidos a destinos distintos del enrutador TX Matrix. Para obtener más información acerca de la coincidencia de expresiones regulares, vea Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados."Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

Configuración de funciones opcionales para mensajes reenviados en un enrutador TX Matrix Plus

in this section

- Incluir información de prioridad en los mensajes reenviados | **1374**
- Agregar una cadena de texto a mensajes reenviados | **1375**
- Usar expresiones regulares para refinar el conjunto de mensajes reenviados | **1375**

Desde la perspectiva de la interfaz de usuario, la matriz de enrutamiento aparece como un único enrutador. El enrutador TX Matrix Plus (también llamado SFC de chasis de estructura de conmutador) controla todos los enrutadores T1600 o T4000 (también llamados LCC de chasis de tarjeta de línea) en la matriz de enrutamiento.

Para configurar funciones opcionales adicionales al especificar cómo las LCC T1600 o T4000 conectadas reenvían mensajes al SFC, incluya instrucciones en el nivel jerárquico .[`edit system syslog host sfc0-master`] Para incluir información de prioridad (instalación y nivel de gravedad) en cada mensaje reenviado, incluya la instrucción.`explicit-priority` Para insertar una cadena de texto en cada mensaje reenviado, incluya la

instrucción.`log-prefix` Para usar la coincidencia de expresiones regulares para especificar con mayor exactitud qué mensajes de una instalación se reenvían, incluya la instrucción.`match`

```
[edit system syslog]
host sfc0-master {
    facility severity;
    explicit-priority;
    log-prefix string;
    match "regular-expression;
}
```

También puede incluir la instrucción en el nivel jerárquico , pero no se recomienda hacerlo.`facility-override`[`edit system syslog host sfc0-master`] No es necesario utilizar recursos alternativos para los mensajes reenviados al SFC, ya que ejecuta la utilidad de registro del sistema Junos y puede interpretar los recursos específicos de Junos OS. Para obtener más información acerca de las instalaciones alternativas, consulte Cambiar el nombre de la instalación alternativa para los mensajes de registro del sistema dirigidos a un destino remoto."Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1388

Incluir información de prioridad en los mensajes reenviados

Cuando se incluye la instrucción en el nivel de jerarquía, los mensajes reenviados al enrutador TX Matrix Plus (o al SFC) incluyen información de prioridad.`explicit-priority`[`edit system syslog host sfc0-master`] Para que la información aparezca en un archivo de registro en el SFC, también debe incluir la instrucción en el nivel de jerarquía para el archivo en el SFC.`explicit-priority`[`edit system syslog file filename`] Como consecuencia, el archivo de registro con el mismo nombre en cada plataforma de la matriz de enrutamiento también incluye información de prioridad para los mensajes generados localmente.

Para incluir información de prioridad en mensajes dirigidos a un equipo remoto desde todos los enrutadores de la matriz de enrutamiento, incluya también la instrucción en el nivel de jerarquía del equipo remoto.`explicit-priority`[`edit system syslog host hostname`] Para obtener más información, consulte Dirigir mensajes a un destino remoto desde la matriz de enrutamiento basada en un enrutador de transmisión Matrix Plus."Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en un enrutador TX Matrix Plus" en la página 1395

En el ejemplo siguiente, el archivo en todos los enrutadores incluye información de prioridad para mensajes con gravedad y superior de todas las instalaciones.**/var/log/messages**`notice` El registro en el SFC del enrutador TX Matrix Plus también incluye mensajes con esas características reenviados desde las LCC T1600 o T4000 conectadas.

```
[edit system syslog]
host sfc0-master {
```

```
    any notice;
    explicit-priority;
}
file messages {
    any notice;
    explicit-priority;
}
```

Agregar una cadena de texto a mensajes reenviados

Cuando se incluye la instrucción en el nivel de jerarquía, la cadena que se define aparece en cada mensaje reenviado al enrutador TX Matrix Plus.`log-prefix`[`edit system syslog host sfc0-master`] Para obtener más información, consulte Agregar una cadena de texto a mensajes de registro del sistema dirigidos a un destino remoto."Agregar una cadena de texto a los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1387

Usar expresiones regulares para refinar el conjunto de mensajes reenviados

Cuando se incluye la instrucción en el nivel de jerarquía, la expresión regular que especifique controla qué mensajes de las LCC T1600 o T4000 conectadas se reenvían al SFC de TX Matrix Plus.`match`[`edit system syslog host sfc0-master`] La expresión regular no se aplica a los mensajes de las LCC conectadas que se dirigen a destinos distintos del SFC. Para obtener más información acerca de la coincidencia de expresiones regulares, vea Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados."Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

Configuración del registro del sistema de manera diferente en cada enrutador T640 en una matriz de enrutamiento

Se recomienda que todos los enrutadores de una matriz de enrutamiento compuesta por un enrutador de matriz de transmisión y enrutadores T640 utilicen la misma configuración, lo que implica que incluya instrucciones de configuración de registro del sistema únicamente en el enrutador de matriz de transmisión. Sin embargo, en raras circunstancias, puede optar por registrar mensajes diferentes en diferentes enrutadores. Por ejemplo, si un enrutador de la matriz de enrutamiento tiene problemas con la autenticación, un representante de soporte técnico de Juniper Networks podría indicarle que registre los mensajes de la instalación con gravedad en ese enrutador.`authorizationdebug`

Para configurar los enrutadores por separado, incluya instrucciones de configuración en los grupos apropiados en el nivel de jerarquía del enrutador de matriz de TX:[`edit groups`]

- Para configurar los valores que se aplican al enrutador TX Matrix pero no a los enrutadores T640, inclúyalos en los grupos de configuración y .`re0re1`
- Para configurar los valores que se aplican a enrutadores T640 concretos, inclúyalos en los grupos de configuración y, donde es el número de índice del chasis de tarjeta de línea (LCC) del enrutador.`lcc`*n*`-re0lcc`*n*`-re1`*n*

Cuando utilice grupos de configuración, no emita comandos de modo de configuración de CLI para cambiar instrucciones en el nivel de jerarquía en el enrutador TX Matrix.`[edit system syslog]` Si lo hace, las instrucciones resultantes sobrescriben las instrucciones definidas en los grupos de configuración y se aplican también a los enrutadores T640. (Además, le recomendamos que no emita comandos de modo de configuración CLI en los enrutadores T640 en ningún momento).

En el ejemplo siguiente se muestra cómo configurar los archivos en tres enrutadores para incluir diferentes conjuntos de mensajes:**/var/log/messages**

- En el enrutador TX Matrix, mensajes locales con gravedad y superior de todas las instalaciones.`info` El archivo no incluye mensajes de los enrutadores T640, porque la instrucción deshabilita el reenvío de mensajes.`host scc-master`
- En el enrutador T640 designado , mensajes de la instalación con gravedad y superior.`LCC0authorizationinfo`
- En el router T640 designado , mensajes con gravedad de todas las instalaciones.`LCC1notice`

```
[edit groups]
re0 {
    system {
        syslog {
            file messages {
                any info;
            }
            host scc-master {
                any none;
            }
        }
    }
}
re1 {
    ... same statements as for re0 ...
}
lcc0-re0 {
    system {
        syslog {
```

```
            file messages {
                authorization info;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
    system {
        syslog {
            file messages {
                any notice;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc1-re0 ...
}
```

Configuración del registro del sistema de manera diferente en cada enrutador T1600 o T4000 en una matriz de enrutamiento

Se recomienda que todos los enrutadores de una matriz de enrutamiento compuesta por un enrutador TX Matrix Plus con enrutadores T1600 o T4000 utilicen la misma configuración, lo que implica que incluya instrucciones de configuración de registro del sistema únicamente en el enrutador de transmisión Matrix Plus. Sin embargo, en raras circunstancias, puede optar por registrar mensajes diferentes en diferentes enrutadores. Por ejemplo, si un enrutador de la matriz de enrutamiento tiene problemas con la autenticación, un representante de soporte técnico de Juniper Networks podría indicarle que registre los mensajes de la instalación con gravedad en ese enrutador.`authorizationdebug`

Para configurar los enrutadores por separado, incluya instrucciones de configuración en los grupos apropiados en el nivel de jerarquía del enrutador TX Matrix Plus:`[edit groups]`

- Para configurar los valores que se aplican al enrutador TX Matrix Plus pero no a los enrutadores T1600 o T4000, inclúyalos en los grupos de configuración y .`re0re1`

- Para configurar las opciones que se aplican a enrutadores T1600 o T4000 concretos, inclúyalas en los grupos de configuración y , donde es el número de índice del chasis de tarjeta de línea (LCC) del enrutador.`lcc`*n*`-re0``lcc`*n*`-re1`*n*

Cuando utilice grupos de configuración, no emita comandos de modo de configuración de CLI para cambiar instrucciones en el nivel de jerarquía en el enrutador TX Matrix Plus.`[edit system syslog]` Si lo hace, las instrucciones resultantes sobrescribirán las instrucciones definidas en los grupos de configuración y se aplicarán también a los enrutadores T1600 o T4000. (Además, le recomendamos que no emita comandos de modo de configuración CLI en los enrutadores T1600 o T4000 en ningún momento).

Para obtener más información acerca de los grupos de configuración de una matriz de enrutamiento, consulte el capítulo sobre grupos de configuración en la Guía del usuario de la CLI de Junos OS .

En el ejemplo siguiente se muestra cómo configurar los archivos en tres enrutadores para incluir diferentes conjuntos de mensajes:**/var/log/messages**

- En el enrutador TX Matrix Plus, mensajes locales con gravedad y superior de todas las instalaciones.`info` El archivo no incluye mensajes de los enrutadores T1600 o T4000, porque la instrucción deshabilita el reenvío de mensajes.`host sfc0-master`

- En el enrutador T1600 o T4000 designado , mensajes de la instalación con gravedad y superior.`LCC0authorizationinfo`

- En el enrutador T1600 o T4000 designado , mensajes con gravedad de todas las instalaciones.`LCC1notice`

```
[edit groups]
re0 {
    system {
        syslog {
            file messages {
                any info;
            }
            host sfc0-master {
                any none;
            }
        }
    }
}
re1 {
    ... same statements as for re0 ...
}
lcc0-re0 {
```

```
    system {
        syslog {
            file messages {
                authorization info;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc0-re0 ...
}
lcc1-re0 {
    system {
        syslog {
            file messages {
                any notice;
            }
        }
    }
}
lcc0-re1 {
    ... same statements as for lcc1-re0 ...
}
```

Dirija los mensajes de registro del sistema a un destino remoto

in this section

- Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro | **1380**
- Dirija los mensajes de registro del sistema a un archivo de registro | **1383**
- Dirigir mensajes de registro del sistema a un terminal de usuario | **1384**
- Dirija los mensajes de registro del sistema a la consola | **1385**
- Dirija los mensajes de registro del sistema a un equipo remoto o a otro motor de enrutamiento | **1385**

- Especificar una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto | **1387**
- Agregar una cadena de texto a los mensajes de registro del sistema dirigidos a un destino remoto | **1387**
- Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto | **1388**
- Funciones predeterminadas para los mensajes de registro del sistema dirigidos a un destino remoto | **1391**
- Facilidades alternativas para mensajes de registro del sistema dirigidos a un destino remoto | **1391**
- Ejemplos: Asignar una función alternativa al sistema Mensajes de registro dirigidos a un destino remoto | **1393**
- Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión | **1394**
- Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en un enrutador TX Matrix Plus | **1395**

Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro

Cada mensaje de registro del sistema pertenece a una instalación, que agrupa mensajes generados por la misma fuente (como un proceso de software) o que se refieren a una condición o actividad similar (como intentos de autenticación). A cada mensaje también se le asigna previamente un nivel de gravedad, que indica la *gravedad* con la que el evento desencadenante afecta a las funciones de la plataforma de enrutamiento.

Cuando se configura el registro para una instalación y un destino, se especifica un nivel de gravedad para cada instalación. Los mensajes de la instalación que están clasificados en ese nivel y superior se registran en el siguiente destino:

```
[edit system syslog]
(console | file filename | host destination | user username) {
    facility severity ;
}
```

Para obtener más información acerca de los destinos, consulte Dirigir mensajes de registro del sistema a "un terminal de usuario y Dirigir mensajes de registro del sistema a" en la página 1384la consola."Dirija los mensajes de registro del sistema a la consola" en la página 1385

Para registrar mensajes que pertenecen a más de una instalación en un destino determinado, especifique cada instalación y la gravedad asociada como una instrucción independiente dentro del conjunto de instrucciones para el destino.

Tabla 140 en la página 1381 enumera los recursos de registro del sistema de Junos OS que puede especificar en las instrucciones de configuración en el nivel jerárquico `.[edit system syslog]`

Tabla 140: Funciones de registro del sistema Junos OS

Instalación	Tipo de evento o error
`any`	Todos (mensajes de todas las instalaciones)
`authorization`	Intentos de autenticación y autorización
`change-log`	Cambios en la configuración de Junos OS
`conflict-log`	La configuración especificada no es válida en el tipo de enrutador
`daemon`	Acciones realizadas o errores encontrados por los procesos del sistema
`dfc`	Eventos relacionados con la captura dinámica de flujo
`explicit-priority`	Incluir prioridad y facilidad en los mensajes de registro del sistema
`external`	Acciones realizadas o errores encontrados por las aplicaciones externas locales
`firewall`	Acciones de filtrado de paquetes realizadas por un filtro de firewall
`ftp`	Acciones realizadas o errores encontrados por el proceso FTP
`interactive-commands`	Comandos emitidos en el símbolo del sistema de la interfaz de línea de comandos (CLI) de Junos OS o por una aplicación cliente, como un protocolo XML de Junos o un cliente XML de NETCONF
`kernel`	Acciones realizadas o errores encontrados por el kernel de Junos OS

Tabla 140: Funciones de registro del sistema Junos OS *(Continued)*

Instalación	Tipo de evento o error
`ntp`	Acciones realizadas o errores encontrados por los procesos del protocolo de tiempo de red
`pfe`	Acciones realizadas o errores encontrados por el motor de reenvío de paquetes
`security`	Eventos o errores relacionados con la seguridad
`user`	Acciones realizadas o errores encontrados por los procesos del espacio de usuario

enumera los niveles de gravedad que puede especificar en las instrucciones de configuración en el nivel jerárquico .Tabla 141 en la página 1382`[edit system syslog]` Los niveles a través están en orden de mayor gravedad (mayor efecto sobre el funcionamiento) a más bajo.`emergency` `info`

A diferencia de los otros niveles de gravedad, el nivel deshabilita el registro de una instalación en lugar de indicar la gravedad con la que un evento desencadenante afecta a las funciones de enrutamiento.`none` Para obtener más información, consulte Deshabilitar el registro del sistema de una instalación."Deshabilitar el registro del sistema de una instalación" en la página 1353

Tabla 141: Niveles de gravedad de los mensajes de registro del sistema

valor	Nivel de gravedad	Description
NA	`none`	Deshabilita el registro de la instalación asociada a un destino
0	`emergency`	Fallo del sistema u otra condición que hace que el enrutador deje de funcionar
1	`alert`	Condiciones que requieren corrección inmediata, como una base de datos del sistema dañada
2	`critical`	Condiciones críticas, como errores graves

Tabla 141: Niveles de gravedad de los mensajes de registro del sistema *(Continued)*

valor	Nivel de gravedad	Description
3	`error`	Condiciones de error que generalmente tienen consecuencias menos graves que los errores en los niveles de emergencia, alerta y críticos
4	`warning`	Condiciones que justifican el monitoreo
5	`notice`	Condiciones que no son errores, pero que pueden justificar un tratamiento especial
6	`info`	Eventos o condiciones de no error de interés
7	`any`	Incluye todos los niveles de gravedad

Dirija los mensajes de registro del sistema a un archivo de registro

Para dirigir los mensajes de registro del sistema a un archivo del directorio del motor de enrutamiento local, incluya la instrucción en el nivel de jerarquía:**/var/log**`file[edit system syslog]`

```
[edit system syslog]
file filename {
    facility severity;
    archive <archive-sites (ftp-url  <password password>)> <files number> <size size> <start-
time "YYYY-MM-DD.hh:mm"> <transfer-interval minutes> <world-readable | no-world-readable>;
    explicit-priority;
    match "regular-expression";
    structured-data {
        brief;
    }
}
```

Para obtener la lista de instalaciones y niveles de gravedad, consulte Especificación de la facilidad y la gravedad de los mensajes que se incluirán en el registro."Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro" en la página 1380

Para evitar que los archivos de registro crezcan demasiado, la utilidad de registro del sistema de Junos OS escribe mensajes de forma predeterminada en una secuencia de archivos de un tamaño definido. Al incluir la instrucción, puede configurar el número de archivos, su tamaño máximo y quién puede leerlos, ya sea para todos los archivos de registro o para un archivo de registro determinado.`archive` Para obtener más información, consulte Especificación del tamaño, número y propiedades de archivado del archivo de registro."Especificar el tamaño, el número y las propiedades de archivado del archivo de registro" en la página 1341

Para obtener información acerca de las siguientes instrucciones, consulte las secciones indicadas:

- —Consulte Inclusión de información de prioridad en los mensajes de registro del sistema`explicit-priority`"Incluir información de prioridad en los mensajes de registro del sistema" en la página 1343
- : consulte Uso de cadenas y expresiones regulares para refinar el conjunto de mensajes registrados`match`"Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349
- —Consulte Registro de mensajes en formato de datos estructurados`structured-data`"Mensajes de registro en formato de datos estructurados" en la página 1341

Dirigir mensajes de registro del sistema a un terminal de usuario

Para dirigir los mensajes de registro del sistema a la sesión de terminal de uno o más usuarios específicos (o todos los usuarios) cuando inician sesión en el motor de enrutamiento local, incluya la instrucción en el nivel de jerarquía:`user[edit system syslog]`

```
[edit system syslog]
user (username | *) {
    facility severity;
    match "regular-expression";
}
```

Especifique uno o más nombres de usuario de Junos OS, separando varios valores con espacios, o utilice el asterisco () para indicar todos los usuarios que han iniciado sesión en el motor de enrutamiento local.`*`

Para obtener la lista de los recursos de registro y los niveles de gravedad, consulte Especificación de la utilidad y la gravedad de los mensajes que se incluirán en el registro."Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro" en la página 1380 Para obtener información acerca de la

instrucción, vea Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados.`match`"Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

Dirija los mensajes de registro del sistema a la consola

Para dirigir los mensajes de registro del sistema a la consola del motor de enrutamiento local, incluya la instrucción en el nivel de jerarquía:`console`[`edit system syslog`]

```
[edit system syslog]
console {
    facility severity;
}
```

Para obtener la lista de los recursos de registro y los niveles de gravedad, consulte Especificación de la utilidad y la gravedad de los mensajes que se incluirán en el registro."Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro" en la página 1380

Dirija los mensajes de registro del sistema a un equipo remoto o a otro motor de enrutamiento

Para dirigir los mensajes de registro del sistema a un equipo remoto o al otro motor de enrutamiento, incluya la instrucción en el nivel de jerarquía:`host`[`edit system syslog`]

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
```

```
}
source-address source-address;
```

Para dirigir los mensajes de registro del sistema a un equipo remoto, incluya la instrucción para especificar la dirección IP versión 4 (IPv4), la dirección IP versión 6 (IPv6) o el nombre de host completo.`host` *hostname* El equipo remoto debe ejecutar la utilidad estándar `.syslogd` No recomendamos dirigir los mensajes a otro dispositivo de Juniper Networks. En cada mensaje de registro del sistema dirigido al equipo remoto, el nombre de host del motor de enrutamiento local aparece después de la marca de tiempo para indicar que es el origen del mensaje.

Para dirigir los mensajes de registro del sistema al otro motor de enrutamiento en un dispositivo con dos motores de enrutamiento instalados y operativos, incluya la instrucción.`host other-routing-engine` La instrucción no es automáticamente recíproca, por lo que debe incluirla en cada configuración de motor de enrutamiento si desea que los motores de enrutamiento dirijan mensajes entre sí. En cada mensaje dirigido al otro motor de enrutamiento, la cadena o aparece después de la marca de tiempo para indicar el origen del mensaje.`re0re1`

Para obtener la lista de los recursos de registro y los niveles de gravedad que se deben configurar en la instrucción, consulte Especificación de la facilidad y la gravedad de los mensajes que se incluirán en el registro.`host`"Especifique la utilidad y la gravedad de los mensajes que se incluirán en el registro" en la página 1380

Para registrar información sobre el nivel de instalación y gravedad en cada mensaje, incluya la instrucción.`explicit-priority` Para obtener más información, consulte Inclusión de información de prioridad en los mensajes de registro del sistema."Incluir información de prioridad en los mensajes de registro del sistema" en la página 1343

Para obtener información acerca de la instrucción, vea Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados.`match`"Usar cadenas y expresiones regulares para refinar el conjunto de mensajes registrados" en la página 1349

Al dirigir mensajes a equipos remotos, puede incluir la instrucción para especificar la dirección IP del dispositivo que se informa en los mensajes como su origen.`source-address` En cada instrucción, incluya la instrucción para asignar una función alternativa y la instrucción para agregar una cadena a cada mensaje.`hostfacility-overridelog-prefix` Puede incluir la instrucción para habilitar el reenvío de mensajes de registro del sistema estructurados a un servidor de registro del sistema remoto en el formato de mensaje de registro del sistema IETF `.structured-data`

Especificar una dirección de origen alternativa para los mensajes de registro del sistema dirigidos a un destino remoto

Para especificar el enrutador de origen que se notificará en los mensajes de *registro del sistema* cuando los mensajes se dirijan a un equipo remoto, incluya la instrucción en el nivel de jerarquía:`source-address`[`edit system syslog`]

```
[edit system syslog]
source-address source-address;
```

es una dirección IPv4 o IPv6 válida configurada en una de las interfaces del enrutador.*`source-address`* La dirección se indica en los mensajes dirigidos a todos los equipos remotos especificados en instrucciones en el nivel de jerarquía, pero no en mensajes dirigidos al otro motor de enrutamiento.`host` *`hostname`*[`edit system syslog`]

Agregar una cadena de texto a los mensajes de registro del sistema dirigidos a un destino remoto

Para agregar una cadena de texto a cada mensaje de registro del sistema dirigido a un equipo remoto o al otro motor de enrutamiento, incluya la instrucción en el nivel de jerarquía:`log-prefix`[`edit system syslog host`]

```
[edit system syslog host (hostname | other-routing-engine)]
facility severity;
log-prefix string;
```

La cadena puede contener cualquier carácter alfanumérico o especial, excepto el signo igual (=) y los dos puntos (:). Tampoco puede incluir el carácter espacial; No escriba la cadena entre comillas (" ") en un intento de incluir espacios en ella.

La utilidad de registro del sistema de Junos OS anexa automáticamente dos puntos y un espacio a la cadena especificada cuando se escriben los mensajes de registro del sistema en el registro. La cadena se inserta después del identificador del motor de enrutamiento que generó el mensaje.

En el ejemplo siguiente se muestra cómo agregar la cadena M120 a todos los mensajes para indicar que el enrutador es un enrutador M120 y dirigir los mensajes al equipo remoto hardware-logger.mycompany.com:

```
[edit system syslog]
host hardware-logger.mycompany.com {
    any info;
    log-prefix M120;
}
```

Cuando estas instrucciones de configuración se incluyen en un enrutador M120 denominado origin1, aparece un mensaje en el hardware-logger.mycompany.com de inicio de sesión del sistema similar al siguiente:

```
Mar 9 17:33:23 origin1 M120: mgd[477]: UI_CMDLINE_READ_LINE: user ‘root’, command ‘run show
version’
```

Cambiar el nombre alternativo de la instalación para los mensajes de registro del sistema dirigidos a un destino remoto

Algunas funciones asignadas a los mensajes registrados en el enrutador o conmutador local tienen nombres específicos de Junos OS (consulte "Funciones de registro del sistema de Junos OS" en la página 1319). En la configuración recomendada, un equipo remoto designado en el nivel de jerarquía no es un enrutador o conmutador de Juniper Networks, por lo que su utilidad syslogd no puede interpretar los nombres específicos de Junos OS.`[edit system syslog host hostname]` Para habilitar la utilidad syslogd estándar para gestionar los mensajes de estas instalaciones cuando los mensajes se dirigen a un equipo remoto, se utiliza un nombre de instalación estándar en lugar del nombre de instalación específico de Junos OS.`local`*X*

Funciones predeterminadas para mensajes de registro del sistema dirigidos a un destino remoto muestra el nombre de instalación alternativo predeterminado junto al nombre de instalación específico de Junos OS para el que se utiliza."Funciones predeterminadas para los mensajes de registro del sistema dirigidos a un destino remoto" en la página 1391

La utilidad syslogd en una máquina remota maneja todos los mensajes que pertenecen a una instalación de la misma manera, independientemente de la fuente del mensaje (el enrutador o conmutador de Juniper Networks o la propia máquina remota). Por ejemplo, las siguientes instrucciones en la

configuración del enrutador llamadas mensajes directos desde la instalación a la máquina remota monitor.mycompany.com:`local-routerauthorization`

```
[edit system syslog]
host monitor.mycompany.com {
    authorization info;
}
```

La instalación alternativa predeterminada para la instalación local también es `.authorizationauthorization` Si la utilidad syslogd activado está configurada para escribir mensajes pertenecientes a la instalación en el archivo , el archivo contiene los mensajes generados cuando los usuarios inician sesión y los mensajes generados cuando los usuarios inician sesión en `.monitorauthorization`**/var/log/auth-attempts**`local-routermonitor` Aunque el nombre del equipo de origen aparece en cada mensaje de registro del sistema, la mezcla de mensajes de varios equipos puede dificultar el análisis del contenido del archivo.`auth-attempts`

Para facilitar la separación de los mensajes de cada origen, puede asignar una función alternativa a todos los mensajes generados el cuando se dirigen a `.local-routermonitor` A continuación, puede configurar la utilidad syslogd para escribir mensajes con la instalación alternativa en un archivo diferente de los mensajes generados en sí mismo.`monitormonitor`

Para cambiar la función utilizada para todos los mensajes dirigidos a un equipo remoto, incluya la instrucción en el nivel de jerarquía:`facility-override`[`edit system syslog host` *`hostname`*]

```
[edit system syslog host hostname]
facility severity;
facility-override facility;
```

En general, tiene sentido especificar una instalación alternativa que aún no esté en uso en la máquina remota, como una de las instalaciones.`local`*X* En el equipo remoto, también debe configurar la utilidad syslogd para manejar los mensajes de la manera deseada.

Facilidades para la instrucción facility-override enumera las instalaciones que puede especificar en la instrucción."Dirija los mensajes de registro del sistema a un destino remoto" en la página 1379`facility-override`

No se recomienda incluir la instrucción en el nivel jerárquico `.facility-override`[`edit system syslog host other-routing-engine`] No es necesario utilizar nombres de instalaciones alternativos al dirigir mensajes al otro motor de enrutamiento, ya que su utilidad de registro del sistema Junos OS puede interpretar los nombres específicos de Junos OS.

En el ejemplo siguiente se muestra cómo registrar todos los mensajes generados en el enrutador local en el nivel de error o superior en la función local0 en el equipo remoto llamado monitor.mycompany.com:

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

En el ejemplo siguiente se muestra cómo configurar enrutadores ubicados en California y enrutadores ubicados en Nueva York para enviar mensajes a un único equipo remoto denominado central-logger.mycompany.com. Los mensajes de California se asignan a la instalación alternativa local0 y los mensajes de Nueva York se asignan a la instalación alternativa local2.

- Configure los enrutadores de California para agregar mensajes en la instalación local0:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local0;
  }
  ```

- Configure los enrutadores de Nueva York para agregar mensajes en la instalación local2:

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local2;
  }
  ```

En el registrador central, puede configurar la utilidad de registro del sistema para escribir mensajes desde la instalación local0 en el archivo y los mensajes desde la instalación local2 en el archivo **.change-lognew-york-config**

Funciones predeterminadas para los mensajes de registro del sistema dirigidos a un destino remoto

Tabla 142 en la página 1391 muestra el nombre de instalación alternativo predeterminado junto al nombre de instalación específico de Junos OS para el que se utiliza. Para las instalaciones que no aparecen en la lista, el nombre alternativo predeterminado es el mismo que el nombre de la instalación local.

Tabla 142: Funciones predeterminadas para mensajes dirigidos a un destino remoto

Instalación local específica de Junos OS	Función predeterminada cuando se dirige a un destino remoto
registro de cambios	local6
registro de conflictos	local5
dfc	local1
Firewall	local3
comandos interactivos	local7
Pfe	local4

Facilidades alternativas para mensajes de registro del sistema dirigidos a un destino remoto

Tabla 143 en la página 1392 enumera las funciones que puede especificar en la instrucción.`facility-override`

Tabla 143: Facilidades para la declaración de anulación de instalaciones

Instalación	Description
`authorization`	Intentos de autenticación y autorización
`daemon`	Acciones realizadas o errores encontrados por los procesos del sistema
`ftp`	Acciones realizadas o errores encontrados por el proceso FTP
`kernel`	Acciones realizadas o errores encontrados por el kernel de Junos OS
`local0`	Instalación local número 0
`local1`	Instalación local número 1
`local2`	Instalación local número 2
`local3`	Instalación local número 3
`local4`	Instalación local número 4
`local5`	Instalación local número 5
`local6`	Instalación local número 6
`local7`	Instalación local número 7
`user`	Acciones realizadas o errores encontrados por los procesos del espacio de usuario

No se recomienda incluir la instrucción en el nivel jerárquico `.facility-override[edit system syslog host other-routing-engine]` No es necesario utilizar nombres de instalaciones alternativos al dirigir mensajes al otro motor de enrutamiento, ya que su utilidad de registro del sistema Junos OS puede interpretar los nombres específicos de Junos OS.

Ejemplos: Asignar una función alternativa al sistema Mensajes de registro dirigidos a un destino remoto

Registre todos los mensajes generados en la plataforma de enrutamiento local en el nivel de error o superior a la instalación en la máquina remota llamada :`local0monitor.mycompany.com`

```
[edit system syslog]
host monitor.mycompany.com {
    any error;
    facility-override local0;
}
```

Configure plataformas de enrutamiento ubicadas en California y plataformas de enrutamiento ubicadas en Nueva York para enviar mensajes a una única máquina remota llamada central-logger.mycompany.com. A los mensajes de California se les asigna la instalación alternativa local0 y los mensajes de Nueva York se asignan a la instalación alternativa local2.

- Configure las plataformas de enrutamiento de California para agregar mensajes en la instalación:`local0`

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local0;
  }
  ```

- Configure las plataformas de enrutamiento de Nueva York para agregar mensajes en la instalación:`local2`

  ```
  [edit system syslog]
  host central-logger.mycompany.com {
      change-log info;
      facility-override local2;
  }
  ```

A continuación, puede configurar la utilidad de registro del sistema para escribir mensajes desde la instalación en el archivo y los mensajes de la instalación en el archivo .`central-logger`,`local0`**california-config**`local2`**new-york-config**

Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en el enrutador de matriz de transmisión

Puede configurar una matriz de enrutamiento compuesta por un enrutador de matriz de transmisión y enrutadores T640 para dirigir los mensajes de registro del sistema a una máquina remota o al otro motor de enrutamiento en cada enrutador, al igual que en un sistema de chasis único. Incluya la instrucción en el nivel de jerarquía en el enrutador TX Matrix:`host`[`edit system syslog`]

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

El enrutador TX Matrix dirige los mensajes a una máquina remota u otro motor de enrutamiento de la misma manera que un sistema de chasis único, y las instrucciones opcionales (, , , , y) también tienen el mismo efecto que en un sistema de chasis único.`explicit-priority``facility-override``log-prefix``match``source-address`

Para que el enrutador de matriz de transmisión incluya información de prioridad cuando dirige mensajes que se originaron en un enrutador T640 al destino remoto, también debe incluir la instrucción en el nivel de jerarquía.`explicit-priority`[`edit system syslog host scc-master`]

La instrucción no interactúa con el reenvío de mensajes desde los enrutadores T640 al enrutador TX Matrix.`other-routing-engine` Por ejemplo, si incluye la instrucción en la configuración del motor de enrutamiento en la ranura 0 (), el motor de enrutamiento de cada enrutador T640 envía mensajes únicamente al motor de enrutamiento de su plataforma.`re0``re0``re1` Tampoco envía mensajes directamente al motor de enrutamiento en el enrutador TX Matrix.`re1`

Debido a que la configuración en el enrutador TX Matrix se aplica a los enrutadores T640, cualquier enrutador T640 que tenga interfaces para acceso directo a Internet también dirige mensajes a la máquina remota. Las consecuencias incluyen las siguientes:

- Si los enrutadores T640 están configurados para reenviar mensajes al enrutador TX Matrix (como en la configuración predeterminada), la máquina remota recibe dos copias de algunos mensajes: uno directamente desde el enrutador T640 y el otro desde el enrutador TX Matrix. Los mensajes que se duplican dependen de si la gravedad es la misma para el registro local y para los mensajes reenviados. Para obtener más información, consulte Configuración del reenvío de mensajes al enrutador TX

Matrix."Configuración del reenvío de mensajes al enrutador de matriz de transmisión" en la página 1362

- Si la instrucción está configurada en el nivel de jerarquía, todos los enrutadores de la matriz de enrutamiento notifican la misma dirección de origen en los mensajes dirigidos al equipo remoto.`source-address`[`edit system syslog`] Esto es apropiado, porque la matriz de enrutamiento funciona como un único enrutador.
- Si se incluye la instrucción, los mensajes de todos los enrutadores de la matriz de enrutamiento incluyen la misma cadena de texto.`log-prefix` No puede utilizar la cadena para distinguir entre los enrutadores de la matriz de enrutamiento.

Mensajes directos a un destino remoto desde la matriz de enrutamiento basada en un enrutador TX Matrix Plus

Desde la perspectiva de la interfaz de usuario, la matriz de enrutamiento aparece como un único enrutador. El enrutador TX Matrix Plus (también llamado SFC de chasis de estructura de conmutación) controla todos los enrutadores T1600 o T4000, también llamados LCC de chasis de tarjeta ine) en la matriz de enrutamiento.

Puede configurar una matriz de enrutamiento compuesta por un enrutador TX Matrix Plus con LCC T1600 o T4000 conectadas para dirigir los mensajes de registro del sistema a una máquina remota o al otro motor de enrutamiento en cada enrutador de enrutamiento, al igual que en un sistema de chasis único. Incluya la instrucción en el nivel jerárquico en el SFC:`host`[`edit system syslog`]

```
[edit system syslog]
host (hostname | other-routing-engine) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
```

El enrutador TX Matrix Plus dirige los mensajes a una máquina remota o al otro motor de enrutamiento de la misma manera que un sistema de chasis único, y las instrucciones opcionales (, , , , y) también tienen el mismo efecto que en un sistema de chasis único.`explicit-priority``facility-override``log-prefix``match``source-address`

Para que el enrutador TX Matrix Plus incluya información de prioridad cuando dirige mensajes que se originaron en una LCC T1600 o T4000 conectada al destino remoto, también debe incluir la instrucción en el nivel de jerarquía.`explicit-priority`[`edit system syslog host sfc0-master`]

La instrucción no interactúa con el reenvío de mensajes desde las LCC T1600 o T4000 conectadas al SFC.`other-routing-engine` Por ejemplo, si incluye la instrucción en la configuración del motor de enrutamiento en la ranura 0 (), el motor de enrutamiento de cada LCC T1600 o T4000 conectada envía mensajes únicamente al motor de enrutamiento de su enrutador.`re0``re0``re1` Tampoco envía mensajes directamente al motor de enrutamiento en el SFC.`re1`

Dado que la configuración del SFC se aplica a las LCC T1600 o T4000 conectadas, cualquier LCC que tenga interfaces para el acceso directo a Internet también dirige los mensajes a la máquina remota. Las consecuencias incluyen las siguientes:

- Si las LCC están configuradas para reenviar mensajes al SFC (como en la configuración predeterminada), el equipo remoto recibe dos copias de algunos mensajes: uno directamente desde la LCC T1600 o T4000 y el otro desde el SFC. Los mensajes que se duplican dependen de si la gravedad es la misma para el registro local y para los mensajes reenviados. Para obtener más información, consulte Configuración del reenvío de mensajes al enrutador TX Matrix Plus."Configuración del reenvío de mensajes al enrutador TX Matrix Plus" en la página 1363

- Si la instrucción está configurada en el nivel de jerarquía, todos los enrutadores de la matriz de enrutamiento notifican la misma dirección de origen en los mensajes dirigidos al equipo remoto.`source-address`[`edit system syslog`] Esto es apropiado, ya que la matriz de enrutamiento funciona como un único enrutador de enrutamiento.

- Si se incluye la instrucción, los mensajes de todos los enrutadores de la matriz de enrutamiento incluyen la misma cadena de texto.`log-prefix` No puede utilizar la cadena para distinguir entre los enrutadores de la matriz de enrutamiento.

Mostrar archivos de registro del sistema

in this section

- Mostrar un archivo de registro desde un sistema de chasis único | **1397**
- Contenido de muestra del archivo de registro | **1397**
- Mostrar un archivo de registro desde una matriz de enrutamiento | **1400**
- Mostrar archivos de registro MD5 | **1401**

Mostrar un archivo de registro desde un sistema de chasis único

Para mostrar un archivo de registro almacenado en un sistema de chasis único, ingrese al modo operativo de la CLI de Junos OS y ejecute uno de los siguientes comandos:

```
user@host> show log log-filename
user@host> file show log-file-pathname
```

De forma predeterminada, los comandos muestran el archivo almacenado en el motor de enrutamiento local. Para mostrar el archivo almacenado en un motor de enrutamiento determinado, anteponga el nombre del archivo o ruta de acceso con la cadena o y dos puntos.`re0re1` Los ejemplos siguientes muestran el archivo almacenado en el motor de enrutamiento en la ranura 1:**/var/log/messages**

```
user@host> show log re1:messages
 user@host> file show re1:/var/log/messages
```

Para obtener información acerca de los campos de un mensaje de registro, consulte Interpretación de mensajes generados en formato estándar por un proceso o biblioteca de Junos OS, Interpretación de mensajes generados en formato estándar por servicios en una PIC e Interpretación de mensajes generados en formato de datos estructurados.https://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-interpreting-msg-by-junos-process.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-interpreting-msg-by-services-on-pic.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-interpreting-msg-generated-structured-data-format.html Para obtener ejemplos, consulte Contenido de ejemplo de archivo de registro."Contenido de muestra del archivo de registro" en la página 1397

Contenido de muestra del archivo de registro

Este tema contiene contenido de ejemplo del directorio /var/log. Puede mostrar el contenido del archivo almacenado en el motor de enrutamiento local. **/var/log/messages** (El directorio es la ubicación predeterminada para los archivos de registro, por lo que no es necesario incluirlo en el nombre de archivo.**/var/log** El archivo es un destino configurado con frecuencia para los mensajes de registro del sistema).**messages**

NOTA: En Junos OS evolucionado, el archivo solo se escribe en el motor de enrutamiento principal.**messages** Los mensajes del motor de enrutamiento de copia de seguridad se encuentran en el archivo del motor de enrutamiento principal.**messages**

```
user@host> show log messages Apr 11 10:27:25 router1 mgd[3606]: UI_DBASE_LOGIN_EVENT: User
'barbara' entering configuration mode
 Apr 11 10:32:22 router1 mgd[3606]: UI_DBASE_LOGOUT_EVENT: User 'barbara' exiting configuration
mode
Apr 11 11:36:15 router1 mgd[3606]: UI_COMMIT: User 'root' performed commit: no comment
 Apr 11 11:46:37 router1 mib2d[2905]: SNMP_TRAP_LINK_DOWN: ifIndex 82, ifAdminStatus up(1),
ifOperStatus down(2), ifName at-1/0/0
```

Puede mostrar el contenido del archivo , que se ha configurado previamente para incluir mensajes de la instalación.**/var/log/processes**`daemon` Al emitir el comando, debe especificar la ruta de acceso completa del archivo:`file show`

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
 Feb 22 20:35:07 router1 snmpd[359]: SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler:
cleared all throttled traps
 Feb 23 07:34:56 router1 snmpd[359]: SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm
start
 Feb 23 07:38:19 router1 snmpd[359]: SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold
start
```

Puede mostrar el contenido del archivo cuando la instrucción se incluye en el nivel de jerarquía []:**/var/log/processes** `explicit-priorityedit system syslog file processes`

```
user@host> file show /var/log/processes Feb 22 08:58:24 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
 Feb 22 20:35:07 router1 snmpd[359]:
%DAEMON-6-SNMPD_THROTTLE_QUEUE_DRAINED: trap_throttle_timer_handler: cleared all throttled traps
Feb 23 07:34:56 router1 snmpd[359]:
%DAEMON-3-SNMPD_TRAP_WARM_START: trap_generate_warm: SNMP trap: warm start
Feb 23 07:38:19 router1 snmpd[359]:
%DAEMON-2-SNMPD_TRAP_COLD_START: trap_generate_cold: SNMP trap: cold start
```

Compatibilidad con mensajes de advertencia para el uso excesivo de rendimiento:

El dispositivo SRX4100 admite hasta 20 Gbps y 7 Mpps de rendimiento de firewall de combinación de Internet (IMIX). Cuando el rendimiento de IMIX supera los 20 Gbps y 7 Mpps en un dispositivo SRX4100, se registran los mensajes de registro nuevos. Estos mensajes de registro le recuerdan que hay un uso excesivo del rendimiento. Puede ver los siguientes mensajes de registro de ejemplo al ejecutar el comando.`show log messages`

```
user@host> show log messages
Apr 25 14:01:12 user Throughput exceed 20Gbps and 7Mpps in 35% of last 15 minutes, above the
time threshold 10%!
Apr 25 14:16:12 user Throughput exceed 20Gbps and 7Mpps in 95% of last 15 minutes, above the
time threshold 10%!
```

Como recordatorio del uso excesivo del rendimiento, cada 15 minutos el sistema calcula cuántos minutos ha superado los 20 Gbps y 7 Mpps. El sistema activa un mensaje de registro si el rendimiento ha superado más de 1 minuto, 30 segundos (10%) de los últimos 15 minutos. Por ejemplo, supongamos que ve el siguiente mensaje de registro:

```
Throughput exceed 20 Gbps and 7 Mpps in 35% of last 15 minutes, above the time threshold 10%!
```

Significa que su rendimiento ha superado los 20 Gbps y 7 Mpps durante 5 minutos, 15 segundos de los últimos 15 minutos (35 % de 15 minutos) que activaron el mensaje de registro.

Para desactivar este mensaje de registro, se recomienda reducir el nivel de transferencia de datos por debajo de 20 Gbps y 7 Mpps o instalar la licencia de actualización de rendimiento mejorado.

NOTA: Esta función requiere una licencia. Consulte la Guía de licencias de Juniper para obtener información general sobre la administración de licencias.https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/licensing/licensing.html Consulte las hojas de datos del producto en Puertas de enlace de servicios de la serie SRX para obtener más información, o comuníquese con su equipo de cuentas de Juniper o con su socio de Juniper.https://www.juniper.net/us/en/products-services/security/srx-series/

Mostrar un archivo de registro desde una matriz de enrutamiento

Una forma de mostrar un archivo de registro almacenado en el motor de enrutamiento local de cualquiera de las plataformas individuales en una matriz de enrutamiento (nodos de enrutamiento T640 o plataforma TX Matrix) es iniciar sesión en un motor de enrutamiento de la plataforma, entrar en el modo operativo de la CLI de Junos OS y emitir el comando o descrito en Visualización de un archivo de registro desde un sistema de chasis único.show log`file show`"Mostrar un archivo de registro desde un sistema de chasis único" en la página 1397

Para mostrar un archivo de registro almacenado en un nodo de enrutamiento T640 durante una sesión de terminal en la plataforma TX Matrix, emita el comando o y agregue un prefijo que especifique el número de índice LCC del nodo de enrutamiento T640 como lccn, seguido de dos puntos.`show logfile show` El índice puede ser de 0 (cero) a 3:

```
user@host> show log lccn:log-filename
user@host> file show lccn:log-file-pathname
```

De forma predeterminada, los comandos y muestran el archivo de registro especificado almacenado en el motor de enrutamiento principal en el nodo de enrutamiento T640.`show logfile show` Para mostrar el registro desde un motor de enrutamiento determinado, anteponga el nombre del archivo o ruta de acceso con la cadena lccn-primary, , o , seguida de dos puntos.`lccn-re0lccn-re1` Todos los ejemplos siguientes muestran el archivo almacenado en el motor de enrutamiento principal (en la ranura 0) en el nodo de enrutamiento LCC2:**/var/log/messages**

```
user@host> show log lcc2:messages
 user@host> show log lcc2-master:messages
 user@host> show log lcc2-re0:messages
user@host> file show lcc2:/var/log/messages
```

Si los nodos de enrutamiento T640 reenvían mensajes a la plataforma TX Matrix (como en la configuración predeterminada), otra forma de ver los mensajes generados en un nodo de enrutamiento T640 durante una sesión de terminal en la plataforma TX Matrix es simplemente mostrar un archivo de registro local. Sin embargo, los mensajes se entremezclan con mensajes de otros nodos de enrutamiento T640 y de la propia plataforma TX Matrix. Para obtener más información acerca del reenvío de mensajes, consulte Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix."Impacto de los diferentes niveles de gravedad locales y reenviados en los mensajes de registro del sistema en un enrutador TX Matrix" en la página 1365

Para obtener información acerca de los campos de un mensaje de registro, consulte Interpretación de mensajes generados en formato de datos estructurados, Interpretación de mensajes generados en formato estándar por servicios en una PIC e Interpretación de mensajes generados en formato estándar

porun proceso o biblioteca de Junos OS.https://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-interpreting-msg-generated-structured-data-format.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-interpreting-msg-by-services-on-pic.htmlhttps://www.juniper.net/documentation/en_US/junos/topics/reference/general/syslog-interpreting-msg-by-junos-process.html Para obtener ejemplos, consulte Contenido de ejemplo de archivo de registro."Contenido de muestra del archivo de registro" en la página 1397

Mostrar archivos de registro MD5

Junos OS and Junos OS Evolved BGP supports authentication for protocol exchanges. When you configure TCP Message Digest 5 (MD5) authentication for BGP protocol on the neighboring routing devices to verify the authenticity of BGP packets, the following log warning messages stored in **/var/log/messages/** are displayed:

En Junos OS,

Cuando MD5 se configura en un dispositivo local pero no en un dispositivo par,

```
Apr 16 21:49:52  R1_re kernel: tcp_auth_ok: Packet from 2.2.2.2:52848 missing MD5 digest
```

Cuando MD5 se configura en un par pero no en un dispositivo local,

```
Apr 16 21:51:30  R1_re kernel: tcp_auth_ok: Packet from 2.2.2.2:54049 unexpectedly has MD5 digest
```

Cuando MD5 está configurado en ambos enrutadores y hay una no coincidencia de contraseña de autenticación, se muestra el siguiente registro:

```
Apr 16 21:51:58  R1_re kernel: tcp_auth_ok: Packet from 2.2.2.2:54049 wrong MD5 digest
```

En Junos OS Evolved,

Cuando la autenticación TCP MD5 está configurada en un dispositivo local pero no en el par dispositivo, los mensajes de registro no están disponibles.

Cuando la autenticación TCP MD5 está configurada en el par pero no en el dispositivo local, los mensajes de registro no están disponibles.

Cuando MD5 está configurado en ambos enrutadores y hay una no coincidencia de contraseña de autenticación, se muestra el siguiente registro:

```
Apr 16 21:41:22  vScapa1-RE0-re0 kernel: %KERN-6-TCP: MD5 Hash failed for (2.2.2.2, 39213)-
>(1.1.1.1, 179)
```

Configurar el registro del sistema para dispositivos de seguridad

in this section

- Descripción general del registro del sistema para dispositivos de seguridad | **1403**
- Formato binario para registros de seguridad | **1405**
- Registro e informes en la caja | **1406**
- Supervisar informes | **1414**
- Configurar archivos de registro de seguridad binaria en caja | **1426**
- Configurar archivos de registro de seguridad binaria fuera de la caja | **1428**
- Configurar archivos de registro de seguridad de Protobuf en caja en modo de evento | **1430**
- Configurar archivos de registro de seguridad de Protobuf en caja en modo de secuencia | **1431**
- Configurar archivos de registro de seguridad de Protobuf fuera de la caja | **1433**
- Enviar mensajes de registro del sistema a un archivo | **1434**
- Configurar el sistema para enviar todos los mensajes de registro a través de eventd | **1435**

Descripción general del registro del sistema para dispositivos de seguridad

in this section

- Registros del plano de control y del plano de datos | **1403**
- Servidor de registro del sistema redundante | **1404**

Junos OS admite la configuración y supervisión de mensajes de registro del sistema (también denominados *mensajes syslog*). Puede configurar archivos para registrar mensajes del sistema y también asignar atributos, como niveles de gravedad, a los mensajes. Las solicitudes de reinicio se registran en los archivos de registro del sistema, que puede ver con el comando.`show log`

Esta sección contiene los siguientes temas:

Registros del plano de control y del plano de datos

Junos OS genera mensajes de registro independientes para registrar los eventos que se producen en los planos de control y datos del sistema.

- Los registros del plano de control, también denominados registros del sistema, incluyen eventos que se producen en la plataforma de enrutamiento. El sistema envía eventos del plano de control al proceso en el motor de enrutamiento, que luego maneja los eventos mediante políticas de Junos OS, generando mensajes de registro del sistema o ambos.`eventd` Puede elegir enviar los registros del plano de control a un archivo, terminal de usuario, consola de plataforma de enrutamiento o máquina remota. Para generar registros del plano de control, utilice la instrucción en el nivel de jerarquía.`syslog[system]`

- Los registros del plano de datos, también denominados registros de seguridad, incluyen principalmente eventos de seguridad que se controlan dentro del plano de datos. Los registros de seguridad pueden estar en formato de texto o binario, y pueden guardarse localmente (modo de evento) o enviarse a un servidor externo (modo de secuencia). El formato binario es necesario para el modo de transmisión y se recomienda conservar espacio de registro en el modo de evento.

  Tenga en cuenta lo siguiente:

  - Los registros de seguridad se pueden guardar localmente (en caja) o externamente (fuera de la caja), pero no ambos.

- SRX1400, SRX1500, SRX3400, SRX3600, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600 y SRX5800 dispositivos utilizan de forma predeterminada el modo de transmisión. Para especificar el formato binario y un servidor externo, consulte Configuración de archivos de registro de seguridad binaria fuera de la caja."Configurar archivos de registro de seguridad binaria fuera de la caja" en la página 1428

  > **NOTA**: Es posible que se eliminen los registros si configura el registro en modo de evento en estos dispositivos.

  A partir de Junos OS versión 15.1X49-D100, el modo predeterminado para SRX1500 dispositivo es el modo de transmisión. Antes de Junos OS versión 15.1X49-D100, el modo predeterminado para SRX1500 dispositivo era el modo de evento.

- Además de las versiones 18.4R1, 18,4R2, 19.1 y 19.2R1 de Junos OS, en todas las demás versiones a partir de Junos OS versión 18.3R3, el modo de registro predeterminado para los dispositivos SRX300, SRX320, SRX340, SRX345, SRX550 y SRX550M es el modo de transmisión. Los eventos del plano de datos se escriben en los archivos de registro del sistema de manera similar a los eventos del plano de control. Para especificar el formato binario de los registros de seguridad, consulte Configuración de archivos de registro de seguridad binarios fuera de la caja."Configurar archivos de registro de seguridad binaria fuera de la caja" en la página 1428

A partir de la versión 20.2R1 de Junos OS, admitimos el escape en el reenvío de registros de flujo y la generación de informes en caja para evitar errores de análisis. El modo de transmisión admite el escape y los formatos cuando los registros no se envían a procesar.`sd-syslogbinary eventd` Para los registros enviados al proceso, recomendamos no habilitar una opción, ya que el proceso ha habilitado el escape para el registro de estructura.`eventdescapeeventd` El modo Evento solo admite escape en formato.`binary` De forma predeterminada, la opción está desactivada.`escape` Debe habilitar la opción mediante el comando.`escapeset security log escape`

Servidor de registro del sistema redundante

El tráfico de registro del sistema de seguridad destinado a servidores remotos se envía a través de los puertos de interfaz de red, que admiten dos destinos de registro del sistema simultáneos. Cada destino de registro del sistema debe configurarse por separado. Cuando se configuran dos direcciones de destino de registro del sistema, se envían registros idénticos a ambos destinos. Aunque se pueden configurar dos destinos en cualquier dispositivo que admita la característica, agregar un segundo destino es útil principalmente como copia de seguridad redundante para implementaciones de clústeres de chasis independientes y activas/configuradas para copias de seguridad.

Está disponible la siguiente información de servidor redundante:

- Instalación: `cron`

- Description: Proceso de programación de cron
- Nivel de gravedad (de mayor a menor gravedad): `debug`
- Description: Mensajes de depuración de software

Formato binario para registros de seguridad

Junos OS genera mensajes de registro independientes para registrar los eventos que se producen en el plano de control y en el plano de datos del sistema. El plano de control supervisa los eventos que se producen en la plataforma de enrutamiento. Estos eventos se registran en los mensajes de registro del sistema. Para generar mensajes de registro del sistema, utilice la instrucción en el nivel de jerarquía.`syslog[system]`

Los mensajes de registro del plano de datos, denominados mensajes de registro de seguridad, registran los eventos de seguridad que el sistema controla directamente dentro del plano de datos. Para generar mensajes de registro de seguridad, utilice la instrucción en el nivel jerárquico `.log[security]`

Los mensajes de registro del sistema se mantienen en archivos de registro en formatos basados en texto, como BSD Syslog, Structured Syslog y WebTrends Enhanced Log Format (WELF).

Los mensajes de registro de seguridad también se pueden mantener en formatos basados en texto. Sin embargo, dado que el registro de seguridad puede producir grandes cantidades de datos, los archivos de registro basados en texto pueden consumir rápidamente recursos de almacenamiento y CPU. En función de la implementación del registro de seguridad, un archivo de registro en formato binario puede proporcionar un uso más eficaz del almacenamiento en caja o fuera de la caja y una mejor utilización de la CPU. El formato binario para los mensajes de registro de seguridad está disponible en todos los firewalls de la serie SRX.

Cuando se configura en modo de evento, los mensajes de registro de seguridad generados en el plano de datos se dirigen al plano de control y se almacenan localmente en el dispositivo. Los mensajes de registro de seguridad almacenados en formato binario se mantienen en un archivo de registro independiente del que se usa para mantener los mensajes de registro del sistema. No se puede acceder a los eventos almacenados en un archivo de registro binario con comandos avanzados de secuencias de comandos de registro destinados a archivos de registro basados en texto. Un comando operativo de CLI independiente admite la decodificación, conversión y visualización de archivos de registro binarios almacenados localmente en el dispositivo.

Cuando se configuran en modo de secuencia, los mensajes de registro de seguridad generados en el plano de datos se transmiten a un dispositivo remoto. Cuando estos mensajes se almacenan en formato binario, se transmiten directamente a un servidor de recopilación de registros externo en un formato binario específico de Juniper. Los archivos de registro binarios almacenados externamente solo se pueden leer con Juniper Secure Analytics (JSA) o Security Threat Response Manager (STRM).

A partir de Junos OS versión 17.4R2 y posteriores, en dispositivos serie SRX300, SRX320, SRX340, SRX345 e instancias de firewall virtual vSRX, cuando el dispositivo está configurado en modo de secuencia, puede configurar un máximo de ocho hosts de registro del sistema. En Junos OS versión 17.4R2 y versiones anteriores, solo puede configurar tres hosts de registro del sistema en el modo de secuencia. Si configura más de tres hosts de registro del sistema, aparecerá el siguiente mensaje de error.**error: configuration check-out failed**

Para obtener información acerca de cómo configurar registros de seguridad binarios en caja (modo de evento), consulte Configuración de archivos de registro de seguridad binaria en caja."Configurar archivos de registro de seguridad binaria en caja" en la página 1426 Para obtener información acerca de cómo configurar registros de seguridad binarios fuera de la caja (modo de secuencia), consulte Configuración de archivos de registro de seguridad binaria fuera de la caja."Configurar archivos de registro de seguridad binaria fuera de la caja" en la página 1428

Registro e informes en la caja

in this section

- Descripción general | **1406**
- Funciones de informes integradas | **1411**
- Selección de tablas | **1413**
- Duración de la tabla | **1413**
- Modo denso de tabla | **1414**
- Escenario de clúster de chasis | **1414**

En este tema se describe la funcionalidad de la CLI de registro e informes internos, así como los aspectos de diseño de los informes integrados para los dispositivos SRX.

Descripción general

El registro de tráfico en caja en unidades de estado sólido (SSD) admite ocho servidores de registro o archivos externos.

Se agrega un archivo XML todo en uno que contiene toda la información de los registros de tráfico. El archivo XML también genera todos los archivos de encabezado de registro y los documentos relacionados con el registro de tráfico.

Un nuevo proceso (demonio) denominado *demonio de administración de registros locales (llmd*) se admite en las tarjetas de procesamiento de servicios 0 (SPCs0) para controlar el registro de tráfico en caja. El tráfico producido por el flujo en SPC se enumera en los registros de tráfico. El llmd guarda estos registros en el SSD local. Los registros de tráfico se guardan en cuatro formatos diferentes. Consulte para obtener información sobre los formatos de registro.Tabla 144 en la página 1407

Tabla 144: Formatos de registro

Formato de registro	Description	Predeterminado
Syslog	• Formato de registro tradicional para guardar registros.	Sí
SD-syslog	• Formato de archivo de registro del sistema estructurado. • La mayoría descriptiva y larga, por lo tanto, ocupa más espacio para almacenar. • Lleva más tiempo transferir los registros guardados en este formato debido al tamaño.	-
Welf	• WebTrends Enhanced Log File Format es un formato de intercambio de archivos de registro estándar de la industria. • Compatible con Firewall Suite 2.0 y versiones posteriores, Firewall Reporting Center 1.0 y versiones posteriores, y Security Reporting Center 2.0 y versiones posteriores.	-
Binario	• Formato propietario de Juniper. • Menos descriptivo entre todos los demás formatos de registro y ocupa el menor espacio en comparación con otros formatos de registro.	-
protobuf	• El mecanismo extensible de Google para serializar datos estructurados, neutral en cuanto al idioma y la plataforma de Google. • Se utiliza un método diferente para codificar los datos. • El tamaño del archivo es pequeño en comparación con syslog y sd-syslog.	

El mecanismo de informes en caja es una mejora de la funcionalidad de registro existente. La funcionalidad de registro existente se modifica para recopilar registros de tráfico del sistema, analizar los registros y generar informes de estos registros en forma de tablas mediante la CLI. La función de informes en caja está destinada a proporcionar una interfaz simple y fácil de usar para ver los registros de seguridad. Los informes en caja son páginas J-Web fáciles de usar de varios eventos de seguridad en forma de tablas y gráficos. Los informes permiten a la administración de seguridad de TI identificar la información de seguridad de un vistazo y decidir rápidamente las acciones a tomar. Se realiza un análisis exhaustivo de los registros (según los tipos de sesión) para funciones como pantalla, IDP, seguridad de contenido e IPSec.

Puede definir filtros para los datos de registro sobre los que se informa en función de los siguientes criterios:

> **NOTA**: Las condiciones superior, detallada e intervalenta no se pueden utilizar al mismo tiempo.

- `top <number>`: esta opción le permite generar informes para eventos de seguridad principales como se especifica en el comando. Por ejemplo: los 5 principales ataques IPS o las 6 URL principales detectadas a través de Content Security.
- `in-detail <number>`: esta opción le permite generar contenido de registro detallado.
- `in-interval <time-period>`: esta opción permite generar los eventos registrados entre determinados intervalos de tiempo.
- `summary`—Esta opción permite generar el resumen de los eventos. De esta manera, puede ajustar el informe a sus necesidades y mostrar solo los datos que desea usar.

El número máximo en el intervalo que muestra el recuento en intervalos es 30. Si se especifica una gran duración, los contadores se ensamblan para garantizar que el intervalo de entrada máximo sea inferior a 30.

Tanto en detalle como en resumen tienen la opción "todos", ya que diferentes tablas tienen atributos diferentes (como la tabla de sesión no tiene el atributo "motivo" pero Content Security sí), la opción "todos" no tiene ningún filtro excepto el tiempo de inicio y el tiempo de finalización. Si hay algún otro filtro que no sea la hora de inicio y la hora de finalización, se muestra un error.

Por ejemplo: root@host> mostrar el informe del registro de seguridad en detalle todos los motivos de la razón1

```
error: "query condition error"
```

Los registros del firewall de la aplicación para la visibilidad de aplicaciones y usuarios enumerarán las aplicaciones y las aplicaciones anidadas. Cuando los registros de estas características enumeran

aplicaciones anidadas, las aplicaciones anidadas se enumeran en J-Web. Cuando los registros enumeran las aplicaciones anidadas como no aplicables o desconocidas, solo las aplicaciones se enumeran en J-Web.

Utilice los siguientes comandos de CLI para ver las aplicaciones y los usuarios de todas las aplicaciones y la lista de aplicaciones anidadas:

- Para las principales aplicaciones anidadas por recuento:`show security log report top session-close top-number <number> group-by application order-by count with user`
- Para las principales aplicaciones anidadas por volumen:`show security log report top session-close top-number <number> group-by application order-by volume with user`
- Para el usuario superior por recuento con aplicación anidada:`show security log report top session-close top-number <number> group-by user order-by count with application`

La función de informes en caja está habilitada de forma predeterminada cuando se cargan las configuraciones predeterminadas de fábrica en el firewall de la serie SRX con Junos OS versión 15.1X49-D100 o posterior.

Si está actualizando el firewall de la serie SRX desde una versión de Junos OS anterior a Junos OS 15.1X49-D100, el firewall de la serie SRX hereda la configuración existente y la función de informes integrados está deshabilitada de forma predeterminada. Debe configurar el comando y el comando para habilitar la función de informes en caja en el dispositivo que se actualiza.`set security log reportset security log mode stream`

A partir de Junos OS versión 19.3R1 , la configuración predeterminada de fábrica no incluye la configuración de informes en caja para aumentar la vida útil de la unidad de estado sólido (SSD). Puede habilitar la función de informes en caja configurando el comando de la CLI en la jerarquía.`set security log report[edit security log]`

Consulte la Guía del usuario de J-Web para dispositivos de la serie SRX para realizar esta tarea en la interfaz de usuario de J-Web .https://www.juniper.net/documentation/us/en/software/jweb-srx21.2/jweb-srx/index.html

A partir de Junos OS versión 21.3R1, los registros de informes en caja se almacenan en el sistema de archivos de memoria (MFS) si no hay ningún SSD externo. El número máximo de registros que puede guardar en MFS es menor que el que puede guardar en un SSD externo. Esto evita el agotamiento y la falla de la memoria. Los registros guardados en MFS no se conservan después del reinicio del dispositivo o un corte de energía. Consulte para conocer el número de registros registrados en los informes integrados y externos.Tabla 145 en la página 1410

Tabla 145: Número de registros

Modo de informe	Sesión	Pantalla	DPI	Seguridad de contenido	IPsec-VPN	CIELO
Fuera de la caja	1200,000	120,000	120,000	120,000	40 000	120,000
En caja	500 000	50 000	50 000	50 000	20,000	50 000

NOTA: Debe configurar la política de seguridad para la sesión mediante el comando para enumerar todas las aplicaciones y aplicaciones anidadas en Seguimiento de aplicaciones en J-Web mediante la función de informes en caja.`set security policies from-zone zone-name to-zone zone-name policy` *`policy-name`* `then log session-close` Consulte para obtener más información (Políticas de seguridad) para obtener más información.*log (Security Policies)*

Después de grabar el mensaje de registro, el registro se almacena en un archivo de registro que luego se almacena en la tabla de base de datos del RE para su posterior análisis (en dispositivos SRX300, SRX320, SRX340, SRX345 y SRX550M) o en la tarjeta SSD para su posterior análisis (en dispositivos SRX1500, SRX4100 y SRX4200).

NOTA: Esta función admite la recepción de la mayoría de los informes principales según el recuento o el volumen de la sesión o el tipo de registro, captura los eventos que ocurren en cada segundo dentro de un intervalo de tiempo especificado y captura el contenido del registro para una condición de CLI especificada. Para generar informes se utilizan varias condiciones de la CLI, como "resumen", arriba", "en detalle" e "en intervalo". Solo puede generar un informe a la vez mediante la CLI. No se pueden usar todas las condiciones de CLI al mismo tiempo. Solo puede generar un informe a la vez mediante la CLI.

Los beneficios de esta característica son:

- Los informes se almacenan localmente en el firewall de la serie SRX y no se requieren dispositivos o herramientas independientes para el almacenamiento de registros e informes.
- Los informes en caja son páginas J-Web fáciles de usar de varios eventos de seguridad en forma de tablas y gráficos.
- Proporciona una interfaz simple y fácil de usar para ver los registros de seguridad.

- Los informes generados permiten al equipo de gestión de seguridad de TI identificar la información de seguridad de un vistazo y decidir rápidamente las acciones a tomar.

La función de informes en caja admite:

- Generación de informes basados en los requerimientos. Por ejemplo: recuento o volumen de la sesión, tipos de registros para actividades como IDP, seguridad de contenido, VPN IPsec.
- Capturar eventos en tiempo real dentro de un rango de tiempo especificado.
- Captura de todas las actividades de red en un formato lógico, organizado y fácil de entender basado en varias condiciones especificadas por CLI.

Funciones de informes integradas

La función de informes en caja admite:

- **Sqlite3 support as a library**—sqlite3 no era compatible antes de Junos OS versión 15.1X49-D100. A partir de Junos OS versión 15.1X49-D100, los demonios que se ejecutan en el RE, así como otros módulos potenciales, utilizan una base de datos de registros SQL (SQLite versión 3) para almacenar registros en firewalls de la serie SRX.

  En Junos OS versión 19.4R1, actualizamos la base de datos de registro en caja para mejorar el rendimiento de las consultas.

- **Running llmd in both Junos OS and Linux OS**: el demonio de reenvío (flowd) decodifica el índice de la base de datos a partir de registros binarios y envía tanto el índice como el registro al demonio de administración de registros local (llmd).

  En los dispositivos SRX300, SRX320, SRX340, SRX345 y SRX550M, llmd se ejecuta en Junos OS. En dispositivos SRX1500, SRX4100 y SRX4200, llmd se ejecuta en Linux. Por lo tanto, para admitir que llmd se ejecute tanto en Junos OS como en Linux OS, el directorio de código llmd se mueve del lado de Linux al lado de Junos OS.

- **Storing of logs into specified table of the sqlite3 database by llmd**— Se introduce un nuevo demonio syslog para recopilar registros locales en firewalls de la serie SRX y guardarlos en la base de datos.

  A partir de Junos OS versión 19.3R1, Junos OS almacena registros en varias tablas en lugar de una sola tabla en un archivo de base de datos. Cada tabla contiene la marca de tiempo de los registros más antiguos y más recientes. Cuando inicia una consulta basada en la hora de inicio y finalización, llmd busca la tabla más reciente para generar informes.

  Por ejemplo, si hay 5 millones de registros en una tabla de un archivo de base de datos generado en las últimas 10 horas, y si desea tomar un informe, debe dedicar más de media hora. A partir de la versión 19.3R1 de Junos OS, una tabla se divide en varias tablas y cada tabla tiene 0,5 millones de registros. Para generar el mismo informe, basta con una información de tabla.

Le recomendamos que consulte con un tiempo más corto para un mejor rendimiento.

- **Database table definition**—Para los registros de sesión, los tipos de datos son dirección de origen, dirección de destino, aplicación, usuario, etc. Para los registros relacionados con las características de seguridad, los tipos de datos son nombre de ataque, dirección URL, protocolo de perfil, etc. Por lo tanto, diferentes tablas están diseñadas para almacenar diferentes tipos de registros para ayudar a mejorar el rendimiento y ahorrar espacio en disco. El firewall de la serie SRX crea una tabla de base de datos para cada tipo de registro, cuando se registran los datos de registro.

  Cada tipo de tabla de base de datos tiene su número máximo de registro específico del dispositivo. Cuando el número de registro de tabla alcanza la limitación, los registros nuevos reemplazan a los registros más antiguos. Junos OS almacena el inicio de sesión en un firewall de la serie SRX en el que se pasa el tráfico activo.

  A partir de Junos OS versión 19.3R1, puede crear varias tablas en un archivo de base de datos para almacenar registros. Puede definir la capacidad de almacenar registros en una tabla.

  Si el límite del número de registro supera la capacidad de la tabla, Junos OS almacena los registros en la segunda tabla. Por ejemplo, si el límite de registros de la tabla 1 supera la capacidad de la tabla, Junos OS almacena los registros en la tabla 2.

  Si el límite del número de registro supera la última tabla del archivo 1, Junos OS almacena los registros en la tabla 1 del archivo 2. Por ejemplo, la tabla n es la última tabla del archivo 1. Cuando los registros superan la capacidad de la tabla, Junos OS almacena los registros en la tabla 1 del archivo 2.

  Para hacer efecto inmediato después de cambiar el número de tabla, utilice el comando operativo.`clear security log report`

- **Database table rotation**—Cada tipo de tabla de base de datos tiene su número máximo de registro específico del dispositivo. Cuando el número de registro de tabla alcanza la limitación, los registros nuevos reemplazan a los registros más antiguos.

  A continuación se describe la capacidad del tamaño del archivo de base de datos:Tabla 146 en la página 1412

  Tabla 146: Capacidad de tamaño de archivo de base de datos

Dispositivos	Sesión	Pantalla	DPI	Seguridad de contenido	IPsec-VPN	CIELO
SRX300, SRX320, SRX340, SRX345 y SRX550M	1.8G	0.18G	0,18G	0,18G	0.06G	0,18G

Tabla 146: Capacidad de tamaño de archivo de base de datos *(Continued)*

Dispositivos	Sesión	Pantalla	DPI	Seguridad de contenido	IPsec-VPN	CIELO
SRX1500	12G	2.25G	2,25G	2,25G	0.75G	2,25G
SRX4100 y SRX4200	15G	2,25G	2,25G	2,25G	0,75G	2,25G
SRX4600	22,5G	6G	6G	6G	0,75G	2,25G
Firewall virtual vSRX	1,8G	0,18G	0,18G	0,18G	0,06 G	0,18G

- **Calculating and displaying the reports that are triggered by CLI**: los informes de la base de datos se reciben de la CLI como interfaz. Con la CLI, puede calcular y mostrar los detalles de los informes.

Selección de tablas

Cuando desee generar un informe a partir de varias tablas, llmd ordena las tablas según la marca de tiempo y selecciona las tablas según la hora de inicio y la hora de finalización solicitadas.

Por ejemplo, hay tres tablas: la tabla 1 (1 a 3), la tabla 2 (3 a 5) y la tabla 3 (6 a 8). 1 a 3, 3 a 6 y 6 a 8 denota la marca de tiempo de los registros más recientes y antiguos. Si solicita un informe del 4 al 6, Junos OS generará un informe a partir de la tabla 2 y la tabla 3.

Duración de la tabla

Puede decidir la duración de la tabla mediante el comando de configuración `.set security log report table-lifetime` Junos OS quita la tabla después de que el tiempo de identificación de la tabla supere la duración de la tabla. Por ejemplo, si configura la duración de la tabla como 2 y la fecha actual es 26-julio-2019, significa que el 24-julio-2019 se eliminarán los registros a las 00:00:00.

Si cambia la fecha y la hora manualmente en un dispositivo, la duración de la tabla cambia. Por ejemplo, si la hora de identificación de una tabla es 19 de julio de 2019 y configura la duración de la tabla como 10, Junos OS debería quitar la tabla el 29 de julio de 2019. Si cambia la fecha del dispositivo como 18-julio-2019, entonces la vida útil real de la tabla se convierte en 30-julio-2019.

Modo denso de tabla

En Junos OS versión 19.4R1, actualizamos el mecanismo predeterminado de almacenamiento y búsqueda en la base de datos de registro en caja para administrar los registros. Ahora puede personalizar el almacenamiento de registros y los resultados del mecanismo de búsqueda. Por ejemplo, si espera menos registros de tráfico, puede usar la configuración predeterminada con una hora de inicio y una hora de detención.

Sin embargo, si espera un gran número de registros de tráfico y mayores intervalos de tiempo para los que se generarán los registros, habilite el modo denso. Para habilitar el modo denso, utilice el comando de configuración.`set security log report table-mode dense`

Escenario de clúster de chasis

Para los informes internos en un clúster de chasis, los registros se almacenan en el disco local en el que el dispositivo está procesando el tráfico activo. Estos registros no se sincronizan con el par del clúster de chasis.

Cada nodo es responsable de almacenar registros cuando cada nodo procesa el tráfico activo. En caso de modo activo/pasivo, solo el nodo activo procesa el tráfico y los registros también se almacenan solo en el nodo activo. En caso de conmutación por error, el nuevo nodo activo procesa el tráfico y almacena los registros en su disco local. En caso de modo activo/activo, cada nodo procesa su propio tráfico y los registros se almacenan en los nodos respectivos.

SEE ALSO

Informe

Supervisar informes

in this section

- Informe de monitoreo de amenazas | **1415**
- Informe de monitoreo de tráfico | **1423**

Los informes en caja ofrecen un servicio integral de informes donde su equipo de administración de seguridad puede detectar un evento de seguridad cuando ocurre, acceder y revisar inmediatamente los detalles pertinentes sobre el evento y decidir rápidamente las medidas correctivas adecuadas. La función de informes J-Web proporciona informes de una o dos páginas que equivalen a una compilación de numerosas entradas de registro.

Esta sección contiene los siguientes temas:

Informe de monitoreo de amenazas

in this section

- Propósito | **1415**
- Acción | **1415**

Propósito

Utilice el Informe de amenazas para supervisar las estadísticas generales y los informes de actividad de las amenazas actuales a la red. Puede analizar los datos de registro en busca de información sobre el tipo de amenaza, los detalles de origen y destino, y la frecuencia de las amenazas. El informe calcula, muestra y actualiza las estadísticas, proporcionando presentaciones gráficas del estado actual de la red.

Acción

Para ver el informe de amenazas:

1. Haga clic en la parte inferior derecha del panel de control o seleccione en la interfaz de usuario de J-Web.**Threats ReportMonitor>Reports>Threats** Aparecerá el informe de amenazas.
2. Seleccione una de las siguientes pestañas:
   - **Statistics** pestaña. Consulte para obtener una descripción del contenido de la página.Tabla 4
   - **Activities** pestaña. Consulte para obtener una descripción del contenido de la página.Tabla 5

Tabla 147: Salida de la ficha Estadísticas en el informe Amenazas

Campo	Description
Panel de estadísticas generales	

Tabla 147: Salida de la ficha Estadísticas en el informe Amenazas *(Continued)*

Campo	Description

Categoría de amenaza	Una de las siguientes categorías de amenazas:
	• Tráfico
	• DPI
	• Seguridad de contenido
	  • Antivirus
	  • Antispam
	  • Filtro web: haga clic en la categoría Filtro web para mostrar los contadores de 39 subcategorías.
	  • Filtro de contenido
	• Evento de firewall
	• DNS

Severidad	Nivel de gravedad de la amenaza: • Emerg • Alerta • Crit • Err • Advertencia • Aviso • Información • Depuración
Golpes en las últimas 24 horas	Número de amenazas encontradas por categoría en las últimas 24 horas.

Tabla 147: Salida de la ficha Estadísticas en el informe Amenazas *(Continued)*

Campo	Description
Aciertos en la hora actual	Número de amenazas encontradas por categoría en la última hora.
Recuentos de amenazas en las últimas 24 horas	
Por gravedad	Gráfico que representa el número de amenazas recibidas cada hora durante las últimas 24 horas ordenadas por nivel de gravedad.
Por categoría	Gráfico que representa el número de amenazas recibidas cada hora durante las últimas 24 horas ordenadas por categoría.
Eje X	Lapso de veinticuatro horas con la hora actual ocupando la columna más a la derecha de la pantalla. El gráfico se desplaza hacia la izquierda cada hora.
Eje	Número de amenazas encontradas. El eje escala automáticamente en función del número de amenazas encontradas.
Amenazas más recientes	
Nombre de la amenaza	Nombres de las amenazas más recientes. En función de la categoría de amenaza, puede hacer clic en el nombre de la amenaza para ir a un sitio del motor de análisis y obtener una descripción de la amenaza.

Tabla 147: Salida de la ficha Estadísticas en el informe Amenazas *(Continued)*

Campo	Description

Categoría	Categoría de cada amenaza:
	• Tráfico
	• DPI
	• Seguridad de contenido
	  • Antivirus
	  • Antispam
	  • Filtro web
	  • Filtro de contenido
	• Evento de firewall
	• DNS

IP/puerto de origen	Dirección IP de origen (y número de puerto, si corresponde) de la amenaza.
IP/puerto de destino	Dirección IP de destino (y número de puerto, si corresponde) de la amenaza.
Protocolo	Nombre de protocolo de la amenaza.
Description	Identificación de amenazas según el tipo de categoría: • Antivirus: URL • Filtro web: categoría • Filtro de contenido: motivo • Antispam: correo electrónico del remitente
Acción	Medidas adoptadas en respuesta a la amenaza.
Tiempo de golpe	Hora en que se produjo la amenaza.

Tabla 147: Salida de la ficha Estadísticas en el informe Amenazas *(Continued)*

Campo	Description
Tendencia de amenazas en las últimas 24 horas	

Categoría	Gráfico circular que representa el recuento comparativo de amenazas por categoría:
	• Tráfico
	• DPI
	• Seguridad de contenido
	  • Antivirus
	  • Antispam
	  • Filtro web
	  • Filtro de contenido
	• Evento de firewall
	• DNS

Resumen de contadores de filtro web	
Categoría	El recuento de filtros web se desglosa en hasta 39 subcategorías. Al hacer clic en la lista de filtros web del panel Estadísticas generales, se abre el panel Resumen de contadores de filtros web.
Golpes en las últimas 24 horas	Número de amenazas por subcategoría en las últimas 24 horas.
Aciertos en la hora actual	Número de amenazas por subcategoría en la última hora.

Tabla 148: Salida de la ficha Actividades en el informe Amenazas

Campo	Función
Virus más recientes	
Nombre de la amenaza	Nombre de la amenaza de virus. Los virus pueden basarse en servicios, como Web, FTP o correo electrónico, o en función del nivel de gravedad.
Severidad	Nivel de gravedad de cada amenaza: • Emerg • Alerta • Crit • Err • Advertencia • Aviso • Información • Depuración
IP/puerto de origen	Dirección IP (y número de puerto, si procede) del origen de la amenaza.
IP/puerto de destino	Dirección IP (y número de puerto, si procede) del destino de la amenaza.
Protocolo	Nombre de protocolo de la amenaza.
Description	Identificación de amenazas según el tipo de categoría: • Antivirus: URL • Filtro web: categoría • Filtro de contenido: motivo • Antispam: correo electrónico del remitente

Tabla 148: Salida de la ficha Actividades en el informe Amenazas *(Continued)*

Campo	Función
Acción	Medidas adoptadas en respuesta a la amenaza.
Hora del último golpe	La última vez que ocurrió la amenaza.
Remitentes de correo electrónico no deseado más recientes	
Desde e-mail	Dirección de correo electrónico que fue la fuente del spam.
Severidad	Nivel de gravedad de la amenaza: • Emerg • Alerta • Crit • Err • Advertencia • Aviso • Información • Depuración
IP de origen	Dirección IP del origen de la amenaza.
Acción	Medidas adoptadas en respuesta a la amenaza.
Hora del último envío	Última vez que se envió el correo electrónico no deseado.
Solicitudes de URL bloqueadas recientemente	
dirección	Solicitud de URL bloqueada.

Tabla 148: Salida de la ficha Actividades en el informe Amenazas *(Continued)*

Campo	Función
IP/puerto de origen	Dirección IP (y número de puerto, si procede) de la fuente.
IP/puerto de destino	Dirección IP (y número de puerto, si procede) del destino.
Aciertos en la hora actual	Número de amenazas encontradas en la última hora.
Ataques de desplazados internos más recientes	
Ataque	
Severidad	Gravedad de cada amenaza: • Emerg • Alerta • Crit • Err • Advertencia • Aviso • Información • Depuración
IP/puerto de origen	Dirección IP (y número de puerto, si procede) de la fuente.
IP/puerto de destino	Dirección IP (y número de puerto, si procede) del destino.
Protocolo	Nombre de protocolo de la amenaza.
Acción	Medidas adoptadas en respuesta a la amenaza.

Tabla 148: Salida de la ficha Actividades en el informe Amenazas *(Continued)*

Campo	Función
Hora del último envío	La última vez que se envió la amenaza de IDP.

Informe de monitoreo de tráfico

in this section

- Propósito | **1423**
- Acción | **1423**

Propósito

Supervise el tráfico de red revisando los informes de las sesiones de flujo de las últimas 24 horas. Puede analizar los datos de registro para obtener estadísticas de conexión y uso de sesión mediante un protocolo de transporte.

Acción

Para ver el tráfico de red en las últimas 24 horas, seleccione en la interfaz de usuario de J-Web.**Monitor>Reports>Traffic** Consulte para obtener una descripción del informe.Tabla 6

Tabla 149: Salida del informe de tráfico

Campo	Description
Sesiones en las últimas 24 horas por protocolo	

Tabla 149: Salida del informe de tráfico *(Continued)*

Campo	Description
Nombre del protocolo	Nombre del protocolo. Para ver la actividad horaria por protocolo, haga clic en el nombre del protocolo y revise el "Gráfico de actividades del protocolo" en el panel inferior. • TCP • UDP • ICMP
Total de la sesión	Número total de sesiones para el protocolo en las últimas 24 horas.
Bytes entrantes (KB)	Número total de bytes entrantes en KB.
Bytes de salida (KB)	Número total de bytes salientes en KB.
Paquetes entrantes	Número total de paquetes entrantes.
Salida de paquetes	Número total de paquetes salientes.
Sesiones cerradas más recientes	
IP/puerto de origen	Dirección IP de origen (y número de puerto, si procede) de la sesión cerrada.
IP/puerto de destino	Dirección IP de destino (y número de puerto, si procede) de la sesión cerrada.
Protocolo	Protocolo de la sesión privada. • TCP • UDP • ICMP
Bytes entrantes (KB)	Número total de bytes entrantes en KB.

Tabla 149: Salida del informe de tráfico *(Continued)*

Campo	Description
Bytes de salida (KB)	Número total de bytes salientes en KB.
Paquetes entrantes	Número total de paquetes entrantes.
Salida de paquetes	Número total de paquetes salientes.
Timestamp	La hora a la que se cierra el período de sesiones.
Cuadro de Actividades de Protocolo	
Bytes de entrada/salida	Representación gráfica del tráfico como bytes entrantes y salientes por hora. El recuento de bytes es para el protocolo seleccionado en el panel Sesiones en las últimas 24 horas por protocolo. Si cambia la selección, este gráfico se actualizará inmediatamente.
Entrada/salida de paquetes	Representación gráfica del tráfico como paquetes entrantes y salientes por hora. El recuento de paquetes es para el protocolo seleccionado en el panel Sesiones en las últimas 24 horas por protocolo. Si cambia la selección, este gráfico se actualizará inmediatamente.
Sesiones	Representación gráfica del tráfico como el número de sesiones por hora. El recuento de sesiones es para el protocolo seleccionado en el panel Sesiones en las últimas 24 horas por protocolo. Si cambia la selección, este gráfico se actualizará inmediatamente.
Eje X	Una hora por columna durante 24 horas.
Eje	Recuento de bytes, paquetes o sesiones.
Tabla de sesión de protocolo	
Sesiones por protocolo	Representación gráfica del tráfico como el recuento de sesiones actuales por protocolo. Los protocolos que se muestran son TCP, UDP e ICMP.

Configurar archivos de registro de seguridad binaria en caja

Los firewalls de la serie SRX utilizan dos tipos de registros (registros del sistema y registros de seguridad) para registrar los eventos del sistema. Los registros del sistema registran eventos del plano de control, por ejemplo, cuando un usuario administrador inicia sesión. Los registros de seguridad, también conocidos como registros de tráfico, registran eventos del plano de datos relacionados con el manejo específico del tráfico. Por ejemplo, Junos OS genera un registro de seguridad si una política de seguridad deniega cierto tráfico debido a una infracción de política. Para obtener más información acerca de los registros del sistema, consulte "Descripción general del registro del sistema de Junos OS" en la página 1319. Para obtener más información acerca de los registros de seguridad, consulte Descripción del registro del sistema para dispositivos de seguridad."Descripción general del registro del sistema para dispositivos de seguridad" en la página 1403

Puede recopilar y guardar registros del sistema y de seguridad en formato binario, ya sea en caja (es decir, almacenados localmente en el firewall de la serie SRX) o fuera de la caja (transmitidos a un dispositivo remoto). El uso del formato binario garantiza que los archivos de registro se almacenen de manera eficiente, lo que a su vez mejora la utilización de la CPU.

Puede configurar archivos de seguridad en formato binario utilizando la instrucción en el nivel de jerarquía.`log[security]`

El registro en caja también se conoce como registro en modo de evento. Para el modo de transmisión y el registro de seguridad fuera de la caja, consulte Configuración de archivos de registro de seguridad binaria fuera de la caja."Configurar archivos de registro de seguridad binaria fuera de la caja" en la página 1428 Al configurar registros de seguridad en formato binario para el registro en modo de eventos, puede definir opcionalmente el nombre de archivo, la ruta de acceso del archivo y otras características, como se detalla en el siguiente procedimiento:

1. Especifique el modo y el formato de registro para el registro en caja.

```
[edit security]
user@host# set log mode event
user@host# set log format binary
```

> **NOTA**: Si configura el registro del sistema para enviar registros del sistema a un destino externo (es decir, fuera de la caja o en modo de secuencia), los registros de seguridad también se envían a ese destino, incluso si utiliza el registro de seguridad en modo de evento. Para obtener más información acerca del envío de registros del sistema a un destino externo, consulte Ejemplos:" Configuración del registro del sistema." en la página 1354

NOTA: Los modos de registro de seguridad fuera de la caja y en caja no se pueden habilitar simultáneamente.

2. (Opcional) Defina un nombre y una ruta de acceso para el archivo de registro.

NOTA: El nombre de archivo de registro de seguridad no es obligatorio. Si el nombre de archivo del registro de seguridad no está configurado, de forma predeterminada el archivo bin_messages se crea en el directorio /var/log.

```
[edit security]
user@host# set log file name security-binary-log
user@host# set log file path security/log-folder
```

3. (Opcional) Cambie el tamaño máximo del archivo de registro y el número máximo de archivos de registro que se pueden archivar.

NOTA: De forma predeterminada, el tamaño máximo del archivo de registro es de 3 MB y se pueden archivar un total de tres archivos de registro.

En los siguientes comandos de ejemplo, se establece un valor de 5 MB y 5 archivos archivados, respectivamente:

```
[edit security]
user@host# set log file size 5
user@host# set log file files 5
```

4. (Opcional) Configure el indicador hpl para habilitar seguimientos de diagnóstico para los archivos de registro de seguridad binaria. El prefijo smf_hpl identifica todos los seguimientos de registro binario.

```
[edit security]
user@host# set log traceoptions flag hpl
```

5. Para la directiva de seguridad de permisos predeterminados, los registros de tráfico se generan cuando finaliza una sesión.`RT_FLOW`

```
[edit security]
user@host# set policies from-zone trust to-zone untrust policy default-permit then log
session-close
```

6. (Opcional) Los registros de tráfico se generan cuando se inicia una sesión.`RT_FlOW`

```
[edit security]
user@host# set policies from-zone trust to-zone untrust policy default-permit then log
session-init
```

Vea el contenido del archivo de registro en modo de evento almacenado en el dispositivo mediante comando y use comando para borrar el contenido del archivo de registro de seguridad en modo de evento binario.`show security log file``clear security log file`

> **NOTA**: El comando muestra los mensajes de registro de seguridad en modo de evento si están en un formato basado en texto y el comando muestra los mensajes de registro de seguridad en modo de evento si están en formato binario (en caja).`show security log``show security log file` Juniper Secure Analytics (JSA) lee el registro binario externo.

Configurar archivos de registro de seguridad binaria fuera de la caja

Los firewalls de la serie SRX tienen dos tipos de registro: Registros del sistema y registros de seguridad. Los registros del sistema registran eventos del plano de control, por ejemplo, el inicio de sesión del administrador en el dispositivo. Para obtener más información acerca de los registros del sistema, consulte "Descripción general del registro del sistema de Junos OS" en la página 1319. Los registros de seguridad, también conocidos como registros de tráfico, registran eventos del plano de datos relacionados con el manejo específico del tráfico, por ejemplo, cuando una política de seguridad deniega cierto tráfico debido a alguna infracción de la política. Para obtener más información acerca de los registros de seguridad, consulte Descripción del registro del sistema para dispositivos de seguridad."Descripción general del registro del sistema para dispositivos de seguridad" en la página 1403

Los dos tipos de registro se pueden recopilar y guardar dentro o fuera de la caja. En el procedimiento siguiente se explica cómo configurar registros de seguridad en formato binario para el registro fuera de caja (modo de secuencia).

Puede configurar archivos de seguridad en formato binario utilizando la instrucción en el nivel de jerarquía.`log[security]`

El siguiente procedimiento especifica el formato binario para el registro de seguridad en modo de secuencia y define las características del nombre de archivo, la ruta de acceso y el archivo de registro. Para el modo de evento y el registro de seguridad en caja, consulte Configuración de archivos de registro de seguridad binaria en caja."Configurar archivos de registro de seguridad binaria en caja" en la página 1426

1. Especifique el modo de registro y el formato del archivo de registro. Para el registro en modo de transmisión fuera de la caja:

```
set security log mode stream
set security log stream test-stream format binary host 1.3.54.22
```

> **NOTA**: Los modos de registro de seguridad fuera de la caja y en caja no se pueden habilitar simultáneamente.

2. Para el registro de seguridad externo, especifique la dirección de origen, que identifica el firewall de la serie SRX que generó los mensajes de registro. La dirección de origen es obligatoria.

```
set security log source-address 2.3.45.66
```

3. Opcionalmente, defina un nombre de archivo de registro y una ruta de acceso.

> **NOTA**: El nombre de archivo de registro de seguridad no es obligatorio. Si el nombre de archivo del registro de seguridad no está configurado, de forma predeterminada el archivo bin_messages se crea en el directorio /var/log.

```
set security log file name security-binary-log
set security log file path security/log-folder
```

4. Opcionalmente, cambie el tamaño máximo del archivo de registro y el número máximo de archivos de registro que se pueden archivar. De forma predeterminada, el tamaño máximo del archivo de registro es de 3 MB y se pueden archivar un total de tres archivos de registro.

```
set security log file size 5
set security log file files 5
```

5. Opcionalmente, seleccione el indicador hpl para habilitar los seguimientos de diagnóstico para el registro binario. El prefijo smf_hpl identifica todos los seguimientos de registro binario.

```
set security log traceoptions flag hpl
```

6. Vea el contenido del archivo de registro en modo de evento almacenado en el dispositivo mediante Juniper Secure Analytics (JSA) o Security Threat Response Manager (STRM).

Configurar archivos de registro de seguridad de Protobuf en caja en modo de evento

Protocol Buffers (Protobuf) is a data format used to serialize structured security logs. You can configure the security log using protobuf format. Data plane use the Protobuf to encode the log and send the log to rtlog process. The rtlog process saves the log file based on the device configuration. By default, the log files are stored in **/var/log/*filename.pb*** directory. You can decode the file data using rtlog process.

Para configurar el formato Protobuf en modo de evento:

1. Especifique el modo y el formato de registro para el registro en caja.

```
[edit security]
user@host# set log mode event
user@host# set log format protobuf
```

2. Defina un nombre y una ruta de acceso para el archivo de registro.

```
[edit security]
user@host# set log file name file1.pb
user@host# set log file path /var/tmp
```

3. Cambie el tamaño máximo del archivo de registro y el número máximo de archivos de registro que se pueden archivar.

```
[edit security]
user@host# set log file size 5
user@host# set log file files 5
```

Vea el contenido del archivo de registro protobuf almacenado en el dispositivo mediante el comando.`show security log file file1.pb`

`user@host>` **show security log file file1.pb**

```
<14>1 2023-03-17T00:06:55 10.53.78.91 RT_LOG_SELF_TEST - SECINTEL_ACTION_LOG
[junos@2636.1.1.1.2.129 category="secintel" sub-category="CC" action="block" action-
detail="test" http-host="test" threat-severity="5" source-address="1.16.16.16" source-
port="16384" destination-address="2.16.16.16" destination-port="32768" protocol-id="17"
application="test" nested-application="test" feed-name="test" policy-name="test" profile-
name="test" username="Fake username" roles="test" session-id="1" source-zone-name="Fake src
zone" destination-zone-name="Fake dst zone" occur-count="3"]
<14>1 2023-03-17T00:06:55 10.53.78.91 RT_LOG_SELF_TEST - AAMW_ACTION_LOG [junos@2636.1.1.1.2.129
hostname="test" file-category="virus" verdict-number="5" malware-info="Test-File" action="block"
list-hit="test" file-hash-lookup="test" source-address="1.16.16.16" source-port="16384"
destination-address="2.16.16.16" destination-port="32768" protocol-id="17" application="test"
nested-application="test" policy-name="test" username="Fake username" roles="test" session-
id="1" source-zone-name="Fake src zone" destination-zone-name="Fake dst zone" sample-
sha256="da26ba1e13ce4702bd5154789ce1a699ba206c12021d9823380febd795f5b002" file-name="test_name"
url="www.test.com"]
...
```

Configurar archivos de registro de seguridad de Protobuf en caja en modo de secuencia

Data plane use the Protobuf to encode the log and send the log to `llmd` process. The `llmd` process saves the log file based on the device configuration. By default, the log files are stored in **/var/traffic-log/*filename.pb*** directory. You can decode the log file data using `uspinfo` process.

Para configurar el formato Protobuf en modo de secuencia para archivar:

1. Especifique el modo y el formato de registro para el registro en caja.

```
[edit security]
user@host# set log mode stream
user@host# set log stream s1 format protobuf
```

2. Defina un nombre para el archivo de registro.

```
[edit security]
user@host# set log stream s1 file name file2.pb
```

3. Cambie el tamaño máximo del archivo de registro que se puede archivar.

```
[edit security]
user@host# set log stream s1 file size 5
```

Vea el contenido del archivo de registro protobuf almacenado en el dispositivo mediante el comando.`show security log stream file file2.pb`

`user@host>` **show security log file file2.pb**

```
<14>1 2023-03-15T22:27:34 10.53.78.91 RT_FLOW - RT_FLOW_SESSION_CREATE [junos@2636.1.1.1.2.129
source-address="1.0.0.3" source-port="38800" destination-address="4.0.0.3" destination-port="80"
connection-tag="0" service-name="junos-http" nat-source-address="1.0.0.3" nat-source-
port="38800" nat-destination-address="4.0.0.3" nat-destination-port="80" nat-connection-tag="0"
src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-nat-rule-name="N/A"
protocol-id="6" policy-name="policy1" source-zone-name="trust" destination-zone-name="untrust"
session-id="69" username="N/A" roles="N/A" packet-incoming-interface="ge-0/0/0.0"
application="HTTP" nested-application="BING" encrypted="No" application-category="Web"
application-sub-category="miscellaneous" application-risk="2" application-characteristics="N/A"
src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-inspection="Off" tunnel-inspection-policy-set="root"
source-tenant="N/A" destination-service="N/A"]
<14>1 2023-03-15T22:27:57 10.53.78.91 RT_FLOW - RT_FLOW_SESSION_CLOSE [junos@2636.1.1.1.2.129
reason="TCP FIN" source-address="1.0.0.3" source-port="38800" destination-address="4.0.0.3"
destination-port="80" connection-tag="0" service-name="junos-http" nat-source-address="1.0.0.3"
nat-source-port="38800" nat-destination-address="4.0.0.3" nat-destination-port="80" nat-
connection-tag="0" src-nat-rule-type="N/A" src-nat-rule-name="N/A" dst-nat-rule-type="N/A" dst-
nat-rule-name="N/A" protocol-id="6" policy-name="policy1" source-zone-name="trust" destination-
zone-name="untrust" session-id="69" packets-from-client="11129" bytes-from-client="583566"
packets-from-server="154153" bytes-from-server="218074629" elapsed-time="23" application="HTTP"
```

```
nested-application="BING" username="N/A" roles="N/A" packet-incoming-interface="ge-0/0/0.0"
encrypted="No" application-category="Web" application-sub-category="miscellaneous" application-
risk="2" application-characteristics="N/A" secure-web-proxy-session-type="NA" peer-session-
id="0" peer-source-address="0.0.0.0" peer-source-port="0" peer-destination-address="0.0.0.0"
peer-destination-port="0" hostname="NA NA" src-vrf-grp="N/A" dst-vrf-grp="N/A" tunnel-
inspection="Off" tunnel-inspection-policy-set="root" session-flag="0" source-tenant="N/A"
destination-service="N/A" user-type="N/A"]
...
```

Configurar archivos de registro de seguridad de Protobuf fuera de la caja

El plano de datos utiliza el formato Protobuf en y el modo para codificar el registro y enviarlo al host.`streamstream-event` Los datos del registro de seguridad se envían al host utilizando un protocolo de transporte y un número de puerto diferentes. El host recibe el registro protobuf y lo guarda en un archivo. Copie , y los archivos al host.`hplc_collect.pyhplc_view.pysecurity_log.xmlprotobuflog.proto` El se utiliza para recopilar y guardar los archivos de registro en el host.`hplc_collect.py` El se utiliza para descodificar los datos del archivo en el host y puede ver los datos mediante `.protobuflog.protohplc_view.py` Los archivos se publican y se copian en el host.**/share/juniper** Los archivos y son compatibles con la última versión 3 de python.`hplc_collect.pyhplc_view.py`

Para configurar el formato Protobuf en modo stream-event para hospedar:

1. Especifique el modo de registro y el formato de secuencia de registro para el registro fuera de la caja. Es una combinación del modo de transmisión y de evento.`Stream-event`

   ```
   [edit security]
   user@host# set log mode stream-event
   user@host# set log stream s1 format protobuf
   ```

2. Para el registro de seguridad externo, especifique la dirección de origen, que identifica el firewall de la serie SRX que generó los mensajes de registro.

   ```
   [edit security]
   user@host# set log source-address 10.0.0.3
   ```

3. Defina un nombre y una ruta de acceso para el archivo de registro.

```
[edit security]
user@host# set log stream s1 file name proto-1og.pb
user@host# set log file path /var/tmp
```

4. Configure la secuencia de registro s1 con la configuración de host y puerto.

```
[edit security]
user@host# set log stream s1 host 4.0.0.3 port 514
user@host# set log stream s1 transport protocol udp
```

5. Cambie el tamaño máximo del archivo de registro y el número máximo de archivos de registro que se pueden archivar.

```
[edit security]
user@host# set log file size 5
user@host# set log file files 5
```

6. Configure el archivo log.trace para descodificar y ver el contenido del registro.

```
[edit security]
user@host# set log traceoptions file log.trace
```

Enviar mensajes de registro del sistema a un archivo

Puede dirigir los mensajes de registro del sistema a un archivo en la tarjeta CompactFlash (CF). El directorio predeterminado para los archivos de registro es `./var/log` Para especificar un directorio diferente en la tarjeta CF, incluya la ruta de acceso completa.

Cree un archivo denominado y envíe mensajes de registro de la clase en el nivel de gravedad al archivo.`securityauthorizationinfo`

Para establecer el nombre de archivo, la instalación y el nivel de gravedad:

```
{primary:node0}
user@host# set system syslog file security authorization info
```

Configurar el sistema para enviar todos los mensajes de registro a través de eventd

El proceso de configuración de registro se suele utilizar para Junos OS.`eventd` En esta configuración, los registros del plano de control y del plano de datos, o de seguridad, se reenvían desde el plano de datos al proceso del plano de control del motor de enrutamiento.`rtlogd` A continuación, el proceso reenvía los registros con formato syslog o sd-syslog al proceso o los registros con formato WELF al recopilador de registros WELF externo o remoto.`rtlogdeventd`

Para enviar todos los mensajes de registro a través de :`eventd`

1. Establezca el proceso para controlar los registros de seguridad y enviarlos a un servidor remoto.`eventd`

```
{primary:node0}
user@host# set security log mode event
```

2. Configure el servidor que recibirá los mensajes de registro del sistema.

```
{primary:node0}
user@host# set system syslog host hostname any any
```

donde es el nombre de host completo o la dirección IP del servidor que recibirá los registros.*hostname*

> **NOTA**: Para enviar registros duplicados a un segundo servidor remoto, repita el comando con un nuevo nombre de host completo o una nueva dirección IP de un segundo servidor.
>
> Si su implementación es un clúster de chasis activo/activo, también puede configurar el registro de seguridad en el nodo activo que se enviará a servidores remotos independientes para lograr la redundancia de registro.

Para cambiar el nombre o redirigir una de las configuraciones de registro, debe eliminarla y volver a crearla. Para eliminar una configuración:

```
{primary:node0}
user@host# delete security log mode event
```

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
15.1X49-D100	A partir de Junos OS versión 15.1X49-D100, el modo predeterminado para SRX1500 dispositivo es el modo de transmisión. Antes de Junos OS versión 15.1X49-D100, el modo predeterminado para SRX1500 dispositivo era el modo de evento.
17.4R2	A partir de Junos OS versión 17.4R2 y posteriores, en dispositivos serie SRX300, SRX320, SRX340, SRX345 e instancias de firewall virtual vSRX, cuando el dispositivo está configurado en modo de secuencia, puede configurar un máximo de ocho hosts de registro del sistema. En Junos OS versión 17.4R2 y versiones anteriores, solo puede configurar tres hosts de registro del sistema en el modo de secuencia. Si configura más de tres hosts de registro del sistema, aparecerá el siguiente mensaje de error.**error: configuration check-out failed**
Junos OS Release 15.1X49-D100	La función de informes en caja está habilitada de forma predeterminada cuando se cargan las configuraciones predeterminadas de fábrica en el firewall de la serie SRX con Junos OS versión 15.1X49-D100 o posterior.
Junos OS Release 19.3R1	A partir de Junos OS versión 19.3R1, SRX300, SRX320, SRX340, SRX345, SRX550 y SRX550M dispositivos utilizan de forma predeterminada el modo de transmisión.
Junos OS Release 19.3R1	A partir de Junos OS versión 19.3R1 , la configuración predeterminada de fábrica no incluye la configuración de informes en caja para aumentar la vida útil de la unidad de estado sólido (SSD).

Configurar Syslog a través de TLS

summary

Obtenga información sobre cómo configurar el dispositivo para transportar mensajes de registro del sistema (también conocidos como mensajes syslog) de forma segura a través del protocolo Seguridad de la capa de transporte (TLS).

in this section

- Registros del plano de control | **1437**
- Registros del plano de datos | **1442**

Registros del plano de control

in this section

- Ejemplo: Configurar Syslog a través de TLS | 1437

Control plane logs, also called system logs, include events that occur on the routing platform. The system sends control plane events to the eventd process on the Routing Engine, which then handles the events by using Junos OS policies, by generating system log messages, or by doing both. You can choose to send control plane logs to a file, user terminal, routing platform console, or remote machine. To generate control plane logs, use the `syslog` statement at the `[system]` hierarchy level.

Ejemplo: Configurar Syslog a través de TLS

in this section

- Requisitos | 1437
- Descripción general | 1438
- Configuración | 1438

En este ejemplo se muestra cómo configurar un dispositivo de Juniper Networks para transportar mensajes syslog (registros del plano de control) de forma segura a través de TLS.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- Junos OS versión 21.2R1 o posterior
- Junos OS Evolved versión 23.4R1 o posterior
- Dispositivo con Junos OS o Junos OS evolucionado (cliente syslog)
- Servidor Syslog

Descripción general

Utilice el protocolo TLS para habilitar el transporte seguro de mensajes de registro del sistema (registros del plano de control) desde el cliente syslog al servidor syslog. TLS utiliza certificados para autenticar y cifrar la comunicación.

- Autenticación del servidor (o TLS unidireccional): el cliente verifica la identidad del servidor y confía en el servidor.
- Autenticación mutua: tanto el servidor como el cliente confían el uno en el otro.

Puede elegir entre autenticación de servidor o autenticación mutua dependiendo de su red. Para acceder rápidamente a la información que necesita, haga clic en los vínculos de la Tabla 1.Tabla 150 en la página 1438

Tabla 150: Modos de autenticación TLS

Modo de autenticación	Procedimiento	Sección donde se encuentra la información
Autenticación del servidor	Configurar PKI Configurar el dispositivo	"Autenticación del servidor" en la página 1440

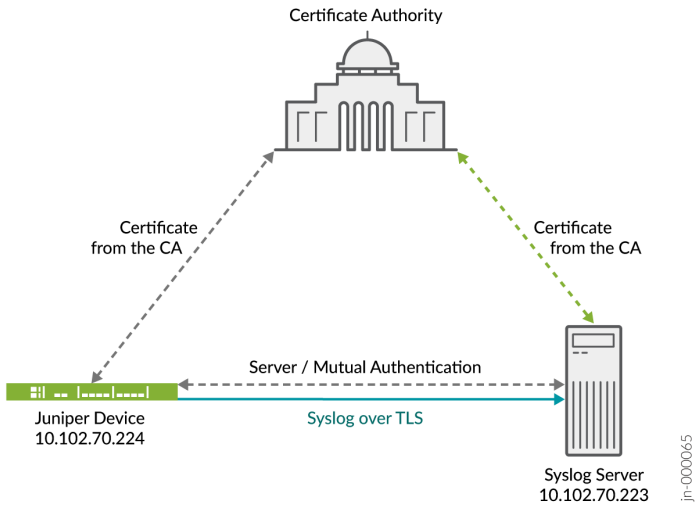
Configuración

in this section

- Descripción general de la configuración de la infraestructura de clave pública (PKI) | **1439**
- Configurar la autenticación del servidor en el dispositivo | **1440**
- Resultados | **1441**
- Verificación | **1442**

En el siguiente ejemplo, usamos el protocolo TLS para transportar de forma segura mensajes syslog (registros del plano de control) desde el dispositivo Juniper al servidor syslog remoto. La figura 1 muestra la topología básica utilizada en este ejemplo.

Figura 46: Syslog a través de TLS



Descripción general de la configuración de la infraestructura de clave pública (PKI)

Para configurar PKI en el dispositivo:

1. Cree un perfil de entidad de certificación (CA) y asocie un identificador de CA al perfil de CA. Consulte Ejemplo: Configuración de un perfil de CA.

2. (Opcional) Cree una comprobación de revocación para especificar un método para validar el certificado. Puede usar listas de revocación de certificados (CRL) o el Protocolo de estado de certificado en línea (OCSP). Consulte Revocación de certificados.https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-revoking-digital-certificates.html

3. (Opcional) Cree un grupo de CA de confianza y agregue el perfil de CA al grupo de confianza. Consulte Configuración de un grupo de CA de confianza.https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-certificate-authority-profiles.html#id-configuring-a-trusted-ca-group

4. Cargue el certificado de CA en el dispositivo. Puede cargar el certificado manualmente. Consulte Ejemplo: Cargar certificados locales y de CA manualmente. En función del entorno de implementación, puede usar el Protocolo de administración de certificados versión 2 (CMPv2) o el Protocolo simple de inscripción de certificados (SCEP) para la inscripción de certificados en línea. Consulte Inscripción de un certificado de CA en línea mediante SCEP y Descripción de la inscripción de certificados con CMPv2.https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-enrolling-a-ca-certificate-online-using-scephttps://www.juniper.net/documentation/us/en/software/junos/vpn-

ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-understanding-certificate-enrollment-with-cmpv2

5. (Opcional para autenticación mutua) Cargue el certificado local en el dispositivo. Puede cargar el certificado local manualmente. En función del entorno de implementación, puede usar CMPv2 o SCEP para la inscripción de certificados en línea. Consulte Inscripción de un certificado local en línea mediante SCEP y Descripción de la inscripción de certificados con CMPv2.https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-example-enrolling-a-local-certificate-online-using-scephttps://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-configuring-ca-and-local-certificates.html#id-understanding-certificate-enrollment-with-cmpv2

6. Compruebe que los certificados se cargan correctamente. Utilice el comando request security pki ca-certificate verify para comprobar si el certificado de CA se ha cargado correctamente.https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/ref/command/request-security-pki-ca-certificate-verify-ca-profile.html Utilice el comando request security pki local-certificate verify para comprobar que el certificado local se ha cargado correctamente.https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/ref/command/request-security-pki-local-certificate-verify-certificate-id.html

Configurar la autenticación del servidor en el dispositivo

Procedimiento paso a paso

El siguiente procedimiento requiere que navegue por varios niveles en la jerarquía de configuración. Para obtener información acerca de cómo navegar por la CLI, consulte Uso del editor de CLI en modo de configuración.https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/cli-editor-configuration-mode-quick-reference-using.html

Para configurar el dispositivo:

1. Especifique el servidor syslog que recibe los mensajes de registro del sistema. Puede especificar la dirección IP del servidor syslog o un nombre de host completo. En este ejemplo, utilice 10.102.70.233 como dirección IP del servidor syslog.

```
[edit]
user@host# set system syslog host 10.102.70.233 any any
```

2. Especifique el número de puerto del servidor syslog.

```
[edit]
user@host# set system syslog host 10.102.70.233 port 10514
```

3. Especifique el protocolo de transporte syslog para el dispositivo. En este ejemplo, use TLS como protocolo de transporte.

```
[edit]
user@host# set system syslog host 10.102.70.223 transport tls
```

4. Especifique el nombre del grupo de entidades emisoras de certificados (CA) de confianza o especifique el nombre del perfil de CA que se va a utilizar. En este ejemplo, utilice example-ca como perfil de CA.

```
[edit]
user@host# set system syslog host 10.102.70.223 tlsdetails trusted-ca-group ca-profiles
example-ca
```

5. Configure el dispositivo para enviar todos los mensajes de registro.

```
[edit]
user@host# set system syslog file messages any any
```

6. Confirme la configuración.

```
[edit]
user@host# commit
```

Resultados

En el modo de configuración, confirme la configuración mediante el comando.`show system syslog`

```
[edit]
user@host# run show system syslog
host 10.102.70.223
{
    port 10514;
    transport tls;
    tlsdetails {
       local-certificate example-cert;
       trusted-ca-group trusted-ca-group-name {
            ca-profiles example-ca};
```

```
        }

      }
  }
```

Verificación

Para comprobar que la configuración funciona correctamente, escriba el comando en el servidor syslog.`show log`

SEE ALSO

tlsdetails

Registros del plano de datos

in this section

- Ejemplo: Configurar el protocolo TLS Syslog en firewalls de la serie SRX | **1442**

Data plane logs, also called security logs, include security events that are handled inside the data plane. Security logs can be in text or binary format, and you can save them locally (event mode) or configure your device to send the logs to an external server (stream mode). You require binary format for stream mode. We recommend binary format to conserve log space in event mode.

Ejemplo: Configurar el protocolo TLS Syslog en firewalls de la serie SRX

in this section

- Requisitos | **1443**
- Descripción general | **1443**
- Configuración | **1443**
- Verificación | **1447**

En este ejemplo se muestra cómo configurar el protocolo syslog de Seguridad de la capa de transporte (TLS) en firewalls de la serie SRX para recibir eventos syslog cifrados de dispositivos de red que admiten el reenvío de eventos syslog TLS.

Requisitos

Antes de comenzar, habilite las capacidades de cifrado o descifrado y comprobación de certificados de servidor.

Descripción general

El protocolo syslog TLS permite que un origen de registro reciba eventos syslog cifrados de dispositivos de red que admiten el reenvío de eventos syslog TLS. El origen del registro crea un puerto de escucha para eventos syslog TLS entrantes y genera un archivo de certificado para los dispositivos de red.

En este ejemplo, se configura un recopilador syslog asociado a un perfil SSL-I. Cada perfil SSL-I permite al usuario especificar cosas como el conjunto de cifrados preferidos y los certificados de CA de confianza. Puede configurar varios perfiles SSL-I y asociar los perfiles con diferentes servidores recopiladores.

Configuración

in this section

- Procedimiento | **1443**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente esta sección del ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
set security log mode stream
set security log format sd-syslog
set security log source-interface ge-0/0/1.0
set security log transport protocol tls
```

```
set security log transport tls-profile ssl-i-tls
set security log stream server1 format sd-syslog
set security log stream server1 category all
set security log stream server1 host 192.0.2.100
set services ssl initiation profile ssl-i-tls protocol-version all
set services ssl initiation profile ssl-i-tls trusted-ca all
set services ssl initiation profile ssl-i-tls actions ignore-server-auth-failure
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacer eso, consulte Uso del editor de CLI en el modo de configuración de la Guía del usuario de CLI.

Para configurar el protocolo syslog TLS:

1. Establezca el modo de registro en stream.

```
[edit security]
user@host# set log mode stream
```

2. Especifique el formato de registro del sistema estructurado (sd-syslog) para el registro remoto de mensajes de seguridad.

```
[edit security]
user@host# set log format sd-syslog
```

3. Establezca el número de interfaz de origen del host.

```
[edit security]
user@host# set log source-interface ge-0/0/1.0
```

4. Especifique TLS como protocolo de transporte del registro de seguridad que se utilizará para registrar los datos.

```
[edit security]
user@host# set log transport protocol tls
```

5. Especifique el nombre del perfil TLS.

```
[edit security]
user@host# set log transport tls-profile ssl-i-tls
```

6. Establezca la secuencia de registro para que utilice el formato syslog estructurado para enviar registros al servidor 1.

```
[edit security]
user@host# set log stream server1 format sd-syslog
```

7. Establezca la categoría de registro del servidor 1 en todos.

```
[edit security]
user@host# set log stream server1 category all
```

8. Especifique los parámetros de host del servidor introduciendo el nombre del servidor o la dirección IP.

```
[edit security]
user@host# set log stream server1 host 192.0.2.100
```

9. Defina la versión del protocolo para el perfil de acceso de iniciación SSL.

```
[edit services]
user@host# set ssl initiation profile ssl-i-tls protocol-version all
```

10. Adjunte todos los grupos de perfiles de CA al perfil de iniciación de SSL para usarlos al solicitar un certificado del mismo nivel.

```
[edit services]
user@host# set ssl initiation profile ssl-i-tls trusted-ca all
```

11. Configure el perfil de acceso de iniciación SSL para omitir el error de autenticación del servidor.

```
[edit services]
user@host# set ssl initiation profile ssl-i-tls actions ignore-server-auth-failure
```

Resultados

En el modo de configuración, compruebe la configuración mediante el comando.`show security log` Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

```
[edit]
user@host# show security log
    mode stream;
        format sd-syslog;
        source-interface ge-0/0/1.0;
        transport {
            protocol tls;
            tls-profile ssl-i-tls;
        }
        stream server1 {
            format sd-syslog;
            category all;
            host {
            192.0.2.100;
            }
        }
    }
```

```
[edit]
user@host# run show configuration services ssl initiation
    profile ssl-i-tls {
        protocol-version all;
        trusted-ca all;
        actions {
            ignore-server-auth-failure;
        }
    }
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Verificación

Para comprobar que la configuración funciona correctamente, escriba el comando en el servidor syslog.`show log`

Supervisar mensajes de registro

in this section

- Supervisar mensajes de registro del sistema | **1447**

Supervisar mensajes de registro del sistema

in this section

- Propósito | **1447**
- Acción | **1448**
- Significado | **1448**

Propósito

Muestra mensajes de registro del sistema sobre la serie QFX. Si busca en un archivo de registro del sistema cualquier entrada relacionada con la interfaz que le interese, puede investigar más a fondo un problema con una interfaz en el conmutador.

Acción

Para ver los mensajes de registro del sistema:

```
user@switch1> show log messages
```

Salida de muestra

nombre-comando

```
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:01 switch1 newsyslog[2283]: logfile turned over due to size>128K
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent for Fan 1
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent for Fan 2
Nov  4 11:30:06  switch1 chassism[952]: CM ENV Monitor: set fan speed is 65 percent for Fan 3
...
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor: jroute daemon
memory usage (Management process): new instance detected (variable:
sysApplElmtRunMemory.5.6.2293)
Nov  4 11:52:53  switch1 snmpd[944]: SNMPD_HEALTH_MON_INSTANCE: Health Monitor: jroute daemon
memory usage (Command-line interface): new instance detected (variable:
sysApplElmtRunMemory.5.8.2292)
...
Nov  4 12:10:24  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command 'exit '
Nov  4 12:10:27  switch1 mgd[2293]: UI_DBASE_LOGOUT_EVENT: User 'jsmith' exiting configuration
mode
Nov  4 12:10:31  switch1 mgd[2293]: UI_CMDLINE_READ_LINE: User 'jsmith', command 'show log
messages
```

Significado

El resultado de ejemplo muestra las siguientes entradas en el archivo:**messages**

- Se creó un nuevo archivo de registro cuando el archivo anterior alcanzó el tamaño máximo de 128 kilobytes (KB).
- La velocidad del ventilador para los ventiladores 1, 2 y 3 se establece en 65 por ciento.
- Se detecta actividad de supervisión de estado.

- Los comandos de CLI fueron introducidos por el usuario jsmith.

SEE ALSO

> *Borrar registro*
>
> *muestra el registro*
>
> Syslog

11

PART IN COVERPAGE

Administración de red y solución de problemas

Monitoreo y solución de problemas | 1451

Solución de problemas del rendimiento del sistema con la metodología de monitoreo de recursos | 1503

Configuración de las opciones de depuración y rastreo de rutas de datos | 1515

Uso de MPLS para diagnosticar LSP, VPN y circuitos de capa 2 | 1534

Uso de la captura de paquetes para analizar el tráfico de red | 1538

Solución de problemas de dispositivos de seguridad | 1568

Monitoreo y solución de problemas

summary

En esta sección se describen las funciones de supervisión de red y solución de problemas de Junos OS.

in this section

- Ping Hosts | **1451**
- Supervisar el tráfico a través del enrutador o conmutador | **1453**
- Descripción general de la memoria direccionable de contenido ternario dinámico | **1458**
- Resolución de problemas de resolución de nombres DNS en directivas de seguridad del sistema lógico (solo administradores principales) | **1474**
- Solución de problemas de la interfaz de servicios de vínculo | **1475**
- Solución de problemas de las políticas de seguridad | **1488**
- Registrar mensajes de error utilizados para solucionar problemas relacionados con ISSU | **1493**

Ping Hosts

in this section

- Propósito | **1452**
- Acción | **1452**
- Significado | **1452**

Propósito

Utilice el comando de la CLI para comprobar que se puede acceder a un host a través de la red.`ping` Este comando es útil para diagnosticar problemas de conectividad de host y red. El dispositivo envía una serie de solicitudes de eco (ping) del Protocolo de mensajes de control de Internet (ICMP) a un host especificado y recibe respuestas de eco ICMP.

Acción

Para usar el comando para enviar cuatro solicitudes (recuento de ping) al host3:`ping`

```
ping host count number
```

Salida de muestra

nombre-comando

```
ping host3 count 4
user@switch> ping host3 count 4
PING host3.site.net (192.0.2.111): 56 data bytes
64 bytes from 192.0.2.111: icmp_seq=0 ttl=122 time=0.661 ms
64 bytes from 192.0.2.111: icmp_seq=1 ttl=122 time=0.619 ms
64 bytes from 192.0.2.111: icmp_seq=2 ttl=122 time=0.621 ms
64 bytes from 192.0.2.111: icmp_seq=3 ttl=122 time=0.634 ms

--- host3.site.net ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.619/0.634/0.661/0.017 ms
```

Significado

- Los resultados muestran la siguiente información:`ping`
  - Tamaño del paquete de respuesta ping (en bytes).
  - Dirección IP del host desde el que se envió la respuesta.
  - Número de secuencia del paquete de respuesta ping. Puede usar este valor para hacer coincidir la respuesta ping con la solicitud ping correspondiente.

- Valor de recuento de saltos de tiempo de vida (ttl) del paquete de respuesta de ping.
- Tiempo total entre el envío del paquete de solicitud de ping y la recepción del paquete de respuesta de ping, en milisegundos. Este valor también se denomina tiempo de ida y vuelta.
- Número de solicitudes de ping (sondeos) enviadas al host.
- Número de respuestas de ping recibidas del host.
- Porcentaje de pérdida de paquetes.
- Estadísticas de ida y vuelta: desviación mínima, media, máxima y estándar del tiempo de ida y vuelta.

Supervisar el tráfico a través del enrutador o conmutador

in this section

- Mostrar estadísticas en tiempo real sobre todas las interfaces del enrutador o conmutador | **1453**
- Mostrar estadísticas en tiempo real sobre una interfaz en el enrutador o conmutador | **1455**

Para diagnosticar un problema, muestre estadísticas en tiempo real sobre el tráfico que pasa a través de las interfaces físicas en el enrutador o conmutador.

Para mostrar estadísticas en tiempo real sobre interfaces físicas, realice estas tareas:

Mostrar estadísticas en tiempo real sobre todas las interfaces del enrutador o conmutador

in this section

- Propósito | **1454**
- Acción | **1454**
- Significado | **1455**

Propósito

Muestra estadísticas en tiempo real sobre el tráfico que pasa por todas las interfaces del enrutador o conmutador.

Acción

Para mostrar estadísticas en tiempo real sobre el tráfico que pasa por todas las interfaces del enrutador o conmutador:

```
user@host> monitor interface traffic
```

Salida de muestra

nombre-comando

```
user@host> monitor interface traffic
host name                 Seconds: 15                  Time: 12:31:09
Interface    Link  Input packets        (pps)     Output packets        (pps)
 so-1/0/0    Down              0          (0)                  0          (0)
 so-1/1/0    Down              0          (0)                  0          (0)
 so-1/1/1    Down              0          (0)                  0          (0)
 so-1/1/2    Down              0          (0)                  0          (0)
 so-1/1/3    Down              0          (0)                  0          (0)
 t3-1/2/0    Down              0          (0)                  0          (0)
 t3-1/2/1    Down              0          (0)                  0          (0)
 t3-1/2/2    Down              0          (0)                  0          (0)
 t3-1/2/3    Down              0          (0)                  0          (0)
 so-2/0/0      Up         211035          (1)              36778          (0)
 so-2/0/1      Up         192753          (1)              36782          (0)
 so-2/0/2      Up         211020          (1)              36779          (0)
 so-2/0/3      Up         211029          (1)              36776          (0)
 so-2/1/0      Up         189378          (1)              36349          (0)
 so-2/1/1    Down              0          (0)              18747          (0)
 so-2/1/2    Down              0          (0)              16078          (0)
 so-2/1/3      Up              0          (0)              80338          (0)
 at-2/3/0      Up              0          (0)                  0          (0)
 at-2/3/1    Down              0          (0)                  0          (0)
Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D
```

Significado

La salida de ejemplo muestra datos de tráfico para interfaces activas y la cantidad que cada campo ha cambiado desde que se inició el comando o desde que se borraron los contadores con la clave.`C` En este ejemplo, el comando se ha estado ejecutando durante 15 segundos desde que se emitió el comando o desde la última vez que los contadores volvieron a cero.`monitor interface`

Mostrar estadísticas en tiempo real sobre una interfaz en el enrutador o conmutador

in this section

- Propósito | **1455**
- Acción | **1455**
- Significado | **1456**

Propósito

Muestra estadísticas en tiempo real sobre el tráfico que pasa a través de una interfaz en el enrutador o conmutador.

Acción

Para mostrar el tráfico que pasa a través de una interfaz en el enrutador o conmutador, utilice el siguiente comando del modo operativo de la CLI de Junos OS:

```
user@host> monitor interface  interface-name
```

Salida de muestra

nombre-comando

```
user@host> monitor interface so-0/0/1
Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
R1
Interface: so-0/0/1, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: OC3 Traffic statistics:
  Input bytes:                    5856541 (88 bps)
```

```
  Output bytes:                   6271468 (96 bps)
  Input packets:                   157629 (0 pps)
  Output packets:                  157024 (0 pps)
Encapsulation statistics:
  Input keepalives:                 42353
  Output keepalives:                42320
  LCP state: Opened
Error statistics:
  Input errors:                         0
  Input drops:                          0
  Input framing errors:                 0
  Input runts:                          0
  Input giants:                         0
  Policed discards:                     0
  L3 incompletes:                       0
  L2 channel errors:                    0
  L2 mismatch timeouts:                 0
  Carrier transitions:                  1
  Output errors:                        0
  Output drops:                         0
  Aged packets:                         0
Active alarms : None
Active defects: None
SONET error counts/seconds:
  LOS count                             1
  LOF count                             1
  SEF count                             1
  ES-S                                 77
  SES-S                                77
SONET statistics:
  BIP-B1                                0
  BIP-B2                                0
  REI-L                                 0
  BIP-B3                                0
  REI-P                                 0
Received SONET overhead:  F1        : 0x00  J0        : 0xZ
```

Significado

La salida de ejemplo muestra los paquetes de entrada y salida para una interfaz SONET determinada ().`so-0/0/1` La información puede incluir errores comunes de interfaz, como alarmas SONET/SDH y T3, loopbacks detectados y aumentos en los errores de trama. Para obtener más información, consulte Lista

de comprobación para el seguimiento de condiciones de error.*Lista de comprobación para condiciones de error de seguimiento*

Para controlar el resultado del comando mientras se está ejecutando, utilice las teclas que se muestran en .Tabla 1

Tabla 151: Teclas de control de salida para el comando de interfaz de monitor

Acción	Clave
Mostrar información sobre la siguiente interfaz. El comando se desplaza por las interfaces físicas o lógicas en el mismo orden en que las muestra el comando.`monitor interfaceshow interfaces terse`	`N`
Mostrar información sobre una interfaz diferente. El comando le pedirá el nombre de una interfaz específica.	`I`
Congele la pantalla, deteniendo la visualización de estadísticas actualizadas.	`F`
Descongele la visualización y reanude la visualización de estadísticas actualizadas.	`T`
Borre (cero) los contadores delta actuales desde que se inició.`monitor interface` No borra el contador acumulativo.	`C`
Detenga el comando.`monitor interface`	`Q`

Consulte el Explorador de CLI para obtener más información sobre el uso de condiciones de coincidencia con el comando.https://www.juniper.net/documentation/content-applications/cli-explorer/junos/`monitor traffic`

Descripción general de la memoria direccionable de contenido ternario dinámico

in this section

- Aplicaciones que utilizan infraestructura TCAM dinámica | 1458
- Características que utilizan el recurso TCAM | 1459
- Monitoreo del uso de recursos TCAM | 1463
- Ejemplo: Monitoreo y solución de problemas del recurso TCAM | 1464
- Monitoreo y resolución de problemas del recurso TCAM en enrutadores de la serie ACX | 1471
- Escalado de servicios en enrutadores ACX5048 y ACX5096 | 1473

En los enrutadores de la serie ACX, la memoria direccionable de contenido ternario (TCAM) es utilizada por varias aplicaciones como firewall, administración de fallas de conectividad, PTPoE, RFC 2544, etc. El motor de reenvío de paquetes (PFE) de los enrutadores de la serie ACX utiliza TCAM con límites de espacio TCAM definidos. La asignación de recursos TCAM para varias aplicaciones de filtro se distribuye estáticamente. Esta asignación estática conduce a una utilización ineficiente de los recursos TCAM cuando es posible que todas las aplicaciones de filtro no utilicen este recurso TCAM simultáneamente.

La asignación dinámica del espacio TCAM en los enrutadores ACX asigna eficientemente los recursos TCAM disponibles para varias aplicaciones de filtro. En el modelo TCAM dinámico, varias aplicaciones de filtro (como inet-firewall, bridge-firewall, cfm-filters, etc.) pueden utilizar de manera óptima los recursos TCAM disponibles cuando sea necesario. La asignación dinámica de recursos TCAM se basa en el uso y se asigna dinámicamente para las aplicaciones de filtro según sea necesario. Cuando una aplicación de filtro ya no utiliza el espacio TCAM, el recurso se libera y está disponible para su uso por otras aplicaciones. Este modelo dinámico de TCAM atiende a una mayor escala de utilización de recursos de TCAM en función de la demanda de la aplicación.

Aplicaciones que utilizan infraestructura TCAM dinámica

Las siguientes categorías de aplicaciones de filtro utilizan la infraestructura TCAM dinámica:

- Filtro de firewall: todas las configuraciones de firewall
- Filtro implícito: demonios del motor de enrutamiento (RE) que usan filtros para lograr su funcionalidad. Por ejemplo, gestión de fallos de conectividad, validación IP MAC, etc.

- Filtros dinámicos: aplicaciones que utilizan filtros para lograr la funcionalidad en el nivel PFE. Por ejemplo, clasificador fijo de nivel de interfaz lógica, RFC 2544, etc. Los demonios RE no sabrán acerca de estos filtros.
- Filtros de inicio del sistema: filtros que requieren entradas a nivel del sistema o un conjunto fijo de entradas en la secuencia de arranque del enrutador. Por ejemplo, captura de protocolo de control de capa 2 y capa 3, aplicador de ARP predeterminado, etc.

> **NOTA**: El filtro System-init que tiene las aplicaciones para la captura de protocolos de control de capa 2 y capa 3 es esencial para la funcionalidad general del sistema. Las aplicaciones de este grupo de control consumen un espacio TCAM fijo y mínimo del espacio TCAM general. El filtro system-init no utilizará la infraestructura TCAM dinámica y se creará cuando se inicialice el enrutador durante la secuencia de arranque.

Características que utilizan el recurso TCAM

Las aplicaciones que utilizan el recurso TCAM se denominan tcam-app en este documento. Por ejemplo, inet-firewall, puente-firewall, administración de errores de conectividad, administración de fallas de enlace, etc. son todas tcam-apps diferentes.

Tabla 152 en la página 1459 describe la lista de tcam-apps que utilizan recursos TCAM.

Tabla 152: Características que utilizan el recurso TCAM

Aplicaciones TCAM/ Usuarios de TCAM	Característica/funcionalidad	Etapa TCAM
bd-dtag-validate	Validación de doble etiquetado de dominio de puente **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Salida
bd-tpid-swap	Mapa VLAN de dominio de puente con operación tpid de intercambio	Salida
cfm-bd-filter	Administración de errores de conectividad filtros implícitos de dominio de puente	Ingreso
cfm-filter	Filtros implícitos de administración de errores de conectividad	Ingreso

Tabla 152: Características que utilizan el recurso TCAM *(Continued)*

Aplicaciones TCAM/ Usuarios de TCAM	Característica/funcionalidad	Etapa TCAM
cfm-vpls-filter	Administración de errores de conectividad filtros vpls implícitos **NOTA**: Esta función solo se admite en enrutadores ACX5048 y ACX5096.	Ingreso
cfm-vpls-ifl-filter	Administración de errores de conectividad vpls filtros de interfaz lógica implícitos **NOTA**: Esta función solo se admite en enrutadores ACX5048 y ACX5096.	Ingreso
cos-fc	Clasificador fijo de nivel de interfaz lógica	Pre-ingreso
fw-ccc-in	Firewall de entrada de la familia de conexión cruzada de circuitos	Ingreso
fw-family-out	Firewall de salida a nivel familiar	Salida
fw-fbf	Reenvío basado en filtros de firewall	Pre-ingreso
fw-fbf-inet6	Reenvío basado en filtros de firewall para la familia inet6	Pre-ingreso
fw-ifl-in	Firewall de ingreso a nivel de interfaz lógica	Ingreso
fw-ifl-out	Firewall de salida a nivel de interfaz lógica	Salida
fw-inet-ftf	Firewall de entrada de la familia Inet en una tabla de reenvío	Ingreso
fw-inet6-ftf	Firewall de entrada de la familia Inet6 en una tabla de reenvío	Ingreso
fw-inet-in	Firewall de entrada de la familia Inet	Ingreso

Tabla 152: Características que utilizan el recurso TCAM *(Continued)*

Aplicaciones TCAM/ Usuarios de TCAM	Característica/funcionalidad	Etapa TCAM
fw-inet-rpf	Comprobación de fallo del firewall de entrada de la familia Inet en RPF	Ingreso
fw-inet6-in	Firewall de entrada de la familia Inet6	Ingreso
fw-inet6-family-out	Firewall de salida a nivel de familia Inet6	Salida
fw-inet6-rpf	Firewall de entrada de la familia Inet6 en una comprobación de fallo de RPF	Ingreso
fw-inet-pm	Firewall de la familia Inet con acción de espejo de puerto **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Ingreso
fw-l2-in	Firewall de entrada de familia de puentes en la interfaz de capa 2	Ingreso
fw-mpls-in	Firewall de entrada de la familia MPLS	Ingreso
fw-semantics	Semántica de uso compartido de firewall para firewall configurado por CLI	Pre-ingreso
fw-vpls-in	Firewall de entrada de la familia VPLS en la interfaz VPLS	Ingreso
ifd-src-mac-fil	Filtro MAC de origen a nivel de interfaz física	Pre-ingreso
ifl-statistics-in	Estadísticas de interfaz de nivel lógico en la entrada	Ingreso
ifl-statistics-out	Estadísticas de interfaz de nivel lógico a la salida	Salida
ing-out-iff	Aplicación de entrada en nombre del filtro de familia de salida para log y syslog	Ingreso

Tabla 152: Características que utilizan el recurso TCAM *(Continued)*

Aplicaciones TCAM/ Usuarios de TCAM	Característica/funcionalidad	Etapa TCAM
ip-mac-val	Validación IP MAC	Pre-ingreso
ip-mac-val-bcast	Validación IP MAC para difusión	Pre-ingreso
ipsec-reverse-fil	Filtros inversos para el servicio IPsec **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Ingreso
irb-cos-rw	Reescritura de IRB CoS	Salida
lfm-802.3ah-in	Administración de fallos de vínculo (IEEE 802.3ah) en la entrada **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Ingreso
lfm-802.3ah-out	Administración de errores de vínculo (IEEE 802.3ah) a la salida	Salida
lo0-inet-fil	Looback interfaz inet filter	Ingreso
lo0-inet6-fil	Filtro inet6 de interfaz Looback	Ingreso
mac-drop-cnt	Las estadísticas de caídas por MAC validan y obtienen filtros MAC	Ingreso
mrouter-port-in	Puerto de enrutador de multidifusión para espionaje	Ingreso
napt-reverse-fil	Filtros inversos para el servicio de traducción de puertos de direcciones de red (NAPT) **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Ingreso

Tabla 152: Características que utilizan el recurso TCAM *(Continued)*

Aplicaciones TCAM/ Usuarios de TCAM	Característica/funcionalidad	Etapa TCAM
no-local-switching	Puente sin conmutación local	Ingreso
ptpoe	Trampas punto a punto a través de Ethernet **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Ingreso
ptpoe-cos-rw	Reescritura de CoS para PTPoE **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Salida
rfc2544-layer2-in	RFC2544 para el servicio de capa 2 en la entrada	Pre-ingreso
rfc2544-layer2-out	RFC2544 para el servicio de capa 2 a la salida **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Salida
service-filter-in	Filtro de servicio al ingresar **NOTA**: Esta función no se admite en enrutadores ACX5048 y ACX5096.	Ingreso

Monitoreo del uso de recursos TCAM

Puede utilizar los comandos show y clear para supervisar y solucionar problemas de uso de recursos TCAM dinámicos.

Tabla 153 en la página 1464 resume los comandos de la interfaz de línea de comandos (CLI) que puede usar para supervisar y solucionar problemas de uso de recursos TCAM dinámicos.

Tabla 153: Mostrar y borrar comandos para supervisar y solucionar problemas de TCAM dinámico

Tarea	Comando
Mostrar las aplicaciones compartidas y las aplicaciones relacionadas para una aplicación en particular	Mostrar la aplicación PFE TCAM
Mostrar el uso de recursos TCAM para una aplicación y las etapas (salida, entrada y preentrada)	Mostrar el uso de TFE TCAM (ACX5448) Mostrar resumen de HW del filtro PFEhttps://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/ref/command/show-pfe-filter.html
Mostrar los errores de uso de recursos TCAM para aplicaciones y etapas (salida, entrada y preentrada)	Mostrar errores de TFE TCAM
Borra las estadísticas de errores de uso de recursos TCAM para aplicaciones y etapas (salida, entrada y preentrada)	Borrar errores de TCAM de PFE

Ejemplo: Monitoreo y solución de problemas del recurso TCAM

En esta sección se describe un caso de uso en el que puede supervisar y solucionar problemas de recursos de TCAM mediante comandos show. En este caso de uso, ha configurado servicios de capa 2 y las aplicaciones relacionadas con el servicio de capa 2 utilizan recursos TCAM. El enfoque dinámico, como se muestra en este ejemplo, le brinda la flexibilidad completa para administrar los recursos de TCAM según sea necesario.

El requisito de servicio es el siguiente:

- Cada dominio de puente tiene una interfaz UNI y una interfaz NNI
- Cada interfaz UNI tiene:
  - Un controlador de nivel de interfaz lógica para vigilar el tráfico a 10 Mbps.
  - Clasificador multicampo con cuatro términos para asignar clase de reenvío y prioridad de pérdida.
- Cada interfaz UNI configura CFM UP MEP en el nivel 4.
- Cada interfaz NNI configura CFM DOWN MEP en el nivel 2

Consideremos un escenario en el que hay 100 servicios configurados en el enrutador. Con esta escala, todas las aplicaciones se configuran correctamente y el estado muestra el estado.**OK**

1. Visualización del uso de recursos TCAM para todas las etapas.

   Para ver el uso de recursos TCAM para todas las etapas (salida, entrada y preentrada), utilice el comando.`show pfe tcam usage all-tcam-stages detail` En enrutadores ACX5448, utilice el comando para ver el recurso TCAM usgae.`show pfe filter hw summary`

```
user@host> show pfe tcam usage all-tcam-stages detail
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage

Tcam Resource Stage: Ingress
----------------------------
Free [hw-grps: 2 out of 8]
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Used  Allocated  Available     Errors
Tcam-Entries    800       1024        224          0
Counters        800       1024        224          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
cfm-filter                500      500        0          3     OK
cfm-bd-filter             300      300        0          2     OK

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    500        512         12          0
Counters        500       1024        524          0
Policers          0       1024       1024          0

App tcam usage:
----------------
```

```
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-l2-in                  500      500        0          2     OK
  fw-semantics              0        X        X          1     OK

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    200        512        312          0
Counters        200        512        312          0
Policers        100        512        412          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-ifl-in                 200      200      100          1     OK

Tcam Resource Stage: Egress
---------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage
```

2. Configure servicios adicionales de capa 2 en el enrutador.

   Por ejemplo, agregue 20 servicios más en el enrutador, aumentando así el número total de servicios a 120. Después de agregar más servicios, puede comprobar el estado de la configuración comprobando el mensaje syslog mediante el comando o ejecutando el comando.`show log messagesshow pfe tcam errors`

   A continuación se muestra un ejemplo de salida de mensaje syslog que muestra la escasez de recursos TCAM para filtros de familia de conmutación Ethernet para configuraciones más recientes ejecutando el comando CLI .`show log messages`

```
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error
(dfw):acx_dfw_check_phy_slice_availability :Insufficient phy slices to accomodate grp:13/
IN_IFF_BRIDGE mode:1/DOUBLE
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_check_resource_availability :Could
not write filter: f-bridge-ge-0/0/0.103-i, insufficient TCAM resources
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error
(dfw):acx_dfw_update_filter_in_hw :acx_dfw_check_resource_availability failed for filter:f-
bridge-ge-0/0/0.103-i
```

```
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_create_hw_instance :Status:1005
Could not program dfw(f-bridge-ge-0/0/0.103-i) type(IN_IFF_BRIDGE)! [1005]
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_bind_shim :[1005] Could not create
dfw(f-bridge-ge-0/0/0.103-i) type(IN_IFF_BRIDGE)
[Sat Jul 11 16:10:33.794 LOG: Err] ACX Error (dfw):acx_dfw_bind :[1000] bind failed for
filter f-bridge-ge-0/0/0.103-i
```

Si utiliza el comando de la CLI para comprobar el estado de la configuración, el resultado será el siguiente:`show pfe tcam errors all-tcam-stages detail`

```
user@host> show pfe tcam errors all-tcam-stages detail
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage

Tcam Resource Stage: Ingress
----------------------------
Free [hw-grps: 2 out of 8]
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Used  Allocated  Available     Errors
Tcam-Entries    960       1024         64          0
Counters        960       1024         64          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
cfm-filter                600      600        0          3     OK
cfm-bd-filter             360      360        0          2     OK

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    510        512          2         18
Counters        510       1024        514          0
Policers          0       1024       1024          0

App tcam usage:
```

```
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-l2-in                  510      510        0          2 FAILED
  fw-semantics              0        X        X          1     OK

App error statistics:
----------------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-l2-in                   18        0        0          2 FAILED
  fw-semantics              0        X        X          1     OK

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    240        512        272          0
Counters        240        512        272          0
Policers        120        512        392          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-ifl-in                 240      240      120          1     OK

Tcam Resource Stage: Egress
---------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage
```

El resultado indica que la aplicación se está quedando sin recursos TCAM y pasa al estado ERROR.**fw-l2-in** Aunque hay dos segmentos TCAM disponibles en la etapa de entrada, la aplicación no puede utilizar el espacio TCAM disponible debido a su modo (DOUBLE), lo que provoca un error en la escasez de recursos.**fw-l2-in**

3. Arreglar las aplicaciones que han fallado debido a la escasez de recursos TCAM.

   La aplicación falló debido a que se agregó más cantidad de servicios en los enrutadores, lo que resultó en una escasez de recursos TCAM.**fw-l2-in** Aunque otras aplicaciones parecen funcionar bien, se recomienda desactivar o quitar los servicios recién agregados para que la aplicación pase a un

estado OK.**fw-l2-in** Después de quitar o desactivar los servicios recién agregados, debe ejecutar los comandos y para comprobar que no hay más aplicaciones en estado de error.`show pfe tcam usageshow pfe tcam error`

Para ver el uso de recursos TCAM para todas las etapas (salida, entrada y preentrada), utilice el comando.`show pfe tcam usage all-tcam-stages detail` Para enrutadores ACX5448, utilice el comando para ver el uso de recursos TCAM.`show pfe filter hw summary`

```
user@host> show pfe tcam usage all-tcam-stages detail
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage

Tcam Resource Stage: Ingress
----------------------------
Free [hw-grps: 2 out of 8]
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Used  Allocated  Available     Errors
Tcam-Entries    800       1024        224          0
Counters        800       1024        224          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-------------------------------------------------------------------
cfm-filter                500      500        0          3     OK
cfm-bd-filter             300      300        0          2     OK

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    500        512         12         18
Counters        500       1024        524          0
Policers          0       1024       1024          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
```

```
  Related-App-Name ..
-----------------------------------------------------------------
fw-l2-in                  500      500        0          2     OK
  fw-semantics              0        X        X          1     OK

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
               Used  Allocated  Available     Errors
Tcam-Entries    200        512        312          0
Counters        200        512        312          0
Policers        100        512        412          0

App tcam usage:
----------------
App-Name              Entries Counters Policers Precedence  State
  Related-App-Name ..
-----------------------------------------------------------------
fw-ifl-in                 200      200      100          1     OK

Tcam Resource Stage: Egress
---------------------------
Free [hw-grps: 3 out of 3]
No dynamic tcam usage
```

Para ver los errores de uso de recursos TCAM para todas las etapas (salida, entrada y preingreso), use el comando.`show pfe tcam errors all-tcam-stages`

```
user@host> show pfe tcam errors all-tcam-stages detail
Slot 0

Tcam Resource Stage: Pre-Ingress
--------------------------------
No tcam usage

Tcam Resource Stage: Ingress
----------------------------
Group: 11, Mode: SINGLE, Hw grps used: 3, Tcam apps: 2
               Errors   Resource-Shortage
Tcam-Entries        0                   0
Counters            0                   0
Policers            0                   0

Group: 8, Mode: DOUBLE, Hw grps used: 2, Tcam apps: 1
```

```
                Errors   Resource-Shortage
Tcam-Entries       18                   0
Counters            0                   0
Policers            0                   0

Group: 14, Mode: SINGLE, Hw grps used: 1, Tcam apps: 1
                Errors   Resource-Shortage
Tcam-Entries        0                   0
Counters            0                   0
Policers            0                   0

Tcam Resource Stage: Egress
---------------------------
No tcam usage
```

Puede ver que todas las aplicaciones que utilizan los recursos TCAM están en estado e indica que el hardware se ha configurado correctamente.**OK**

NOTA: Como se muestra en el ejemplo, deberá ejecutar los comandos y en cada paso para asegurarse de que las configuraciones son válidas y de que las aplicaciones que usan el recurso TCAM están en buen estado.`show pfe tcam errorsshow pfe tcam usage` Para enrutadores ACX5448, use el comando para ver el uso de recursos TCAM.`show pfe filter hw summary`

Monitoreo y resolución de problemas del recurso TCAM en enrutadores de la serie ACX

La asignación dinámica del espacio de memoria direccionable de contenido ternario (TCAM) en la serie ACX asigna eficientemente los recursos TCAM disponibles para diversas aplicaciones de filtro. En el modelo TCAM dinámico, varias aplicaciones de filtro (como inet-firewall, bridge-firewall, cfm-filters, etc.) pueden utilizar de manera óptima los recursos TCAM disponibles cuando sea necesario. La asignación dinámica de recursos TCAM se basa en el uso y se asigna dinámicamente para las aplicaciones de filtro según sea necesario. Cuando una aplicación de filtro ya no utiliza el espacio TCAM, el recurso se libera y está disponible para su uso por otras aplicaciones. Este modelo dinámico de TCAM atiende a una mayor escala de utilización de recursos de TCAM en función de la demanda de la aplicación. Puede utilizar los comandos show and clear para supervisar y solucionar problemas de uso dinámico de recursos TCAM en los enrutadores de la serie ACX.

NOTA: Las aplicaciones que utilizan el recurso TCAM se denominan tcam-app en este documento.

Descripción general de la memoria direccionable de contenido ternario dinámico muestra la tarea y los comandos para supervisar y solucionar problemas de recursos TCAM en enrutadores de la serie ACX

Tabla 154: Comandos para supervisar y solucionar problemas de recursos TCAM en la serie ACX

Cómo	Comando
Ver las aplicaciones compartidas y relacionadas para una aplicación en particular.	`show pfe tcam app (list-shared-apps | list-related-apps)`
Vea el número de aplicaciones en todas las etapas de tcam.	`show pfe tcam usage all-tcam-stages`
Vea el número de aplicaciones que utilizan el recurso TCAM en una etapa especificada.	`show pfe tcam usage tcam-stage (ingress | egress | pre-egress)`
Vea el recurso TCAM utilizado por una aplicación en detalle.	`show pfe tcam usage app <application-name> detail`
Ver el recurso TCAM utilizado por una aplicación en una etapa especificada.	`show pfe tcam usage tcam-stage (ingress | egress | pre-egress) app <application-name>`
Conozca la cantidad de recursos TCAM consumidos por una tcam-app	`show pfe tcam usage app <application-name>`
Vea los errores de uso de recursos TCAM para todas las etapas.	`show pfe tcam errors all-tcam-stages detail`
Ver los errores de uso de recursos TCAM para una etapa	`show pfe tcam errors tcam-stage (ingress | egress | pre-egress)`
Ver los errores de uso de recursos TCAM para una aplicación.	`show pfe tcam errors app <application-name>`

Tabla 154: Comandos para supervisar y solucionar problemas de recursos TCAM en la serie ACX *(Continued)*

Cómo	Comando
Ver los errores de uso de recursos TCAM para una aplicación junto con su otra aplicación compartida.	`show pfe tcam errors app <application-name> shared-usage`
Borre las estadísticas de errores de uso de recursos TCAM para todas las etapas.	`clear pfe tcam-errors all-tcam-stages`
Borre las estadísticas de error de uso de recursos TCAM para una etapa especificada	`clear pfe tcam-errors tcam-stage (ingress | egress | pre-egress)`
Borre las estadísticas de error de uso de recursos TCAM para una aplicación.	`clear pfe tcam-errors app <application-name>`

Para obtener más información sobre el TCAM dinámico en la serie ACX, consulte Descripción general de la memoria direccionable de contenido ternario dinámico."Descripción general de la memoria direccionable de contenido ternario dinámico" en la página 1458

Escalado de servicios en enrutadores ACX5048 y ACX5096

En enrutadores ACX5048 y ACX5096, un servicio típico (como ELINE, ELAN e IP VPN) que se implementa puede requerir aplicaciones (como policías, filtros de firewall, administración de errores de conectividad IEEE 802.1ag, RFC2544) que utilicen la infraestructura TCAM dinámica.

> **NOTA**: Las aplicaciones de servicio que usan recursos TCAM están limitadas por la disponibilidad de recursos TCAM. Por lo tanto, la escala del servicio depende del consumo del recurso TCAM por parte de dichas aplicaciones.

Puede encontrar un caso de uso de ejemplo para monitorear y solucionar problemas de escala de servicio en enrutadores ACX5048 y ACX5096 en la sección Descripción general de la memoria direccionable de contenido ternario dinámico ."Descripción general de la memoria direccionable de contenido ternario dinámico" en la página 1458

Resolución de problemas de resolución de nombres DNS en directivas de seguridad del sistema lógico (solo administradores principales)

in this section

- Problema | 1474
- Causa | 1474
- Solución | 1474

Problema

Description

Es posible que la dirección de un nombre de host en una entrada de la libreta de direcciones que se usa en una directiva de seguridad no se resuelva correctamente.

Causa

Normalmente, las entradas de la libreta de direcciones que contienen nombres de host dinámicos se actualizan automáticamente para los firewalls de la serie SRX. El campo TTL asociado a una entrada DNS indica la hora a partir de la cual la entrada debe actualizarse en la caché de directivas. Una vez que expira el valor TTL, el firewall de la serie SRX actualiza automáticamente la entrada DNS para una entrada de libreta de direcciones.

Sin embargo, si el firewall de la serie SRX no puede obtener una respuesta del servidor DNS (por ejemplo, la solicitud DNS o el paquete de respuesta se pierde en la red o el servidor DNS no puede enviar una respuesta), es posible que la dirección de un nombre de host en una entrada de libreta de direcciones no se resuelva correctamente. Esto puede hacer que el tráfico se caiga ya que no se encuentra ninguna política de seguridad o coincidencia de sesión.

Solución

El administrador principal puede usar el comando para mostrar información de caché DNS en el firewall de la serie SRX.`show security dns-cache` Si es necesario actualizar la información de caché DNS, el administrador principal puede usar el comando.`clear security dns-cache`

NOTA: Estos comandos solo están disponibles para el administrador principal en dispositivos configurados para sistemas lógicos. Este comando no está disponible en sistemas lógicos de usuario ni en dispositivos que no están configurados para sistemas lógicos.

SEE ALSO

Descripción de las directivas de seguridad de sistemas lógicos

Solución de problemas de la interfaz de servicios de vínculo

in this section

- Determinar qué componentes de CoS se aplican a los vínculos constituyentes | **1475**
- Determinar qué causa la fluctuación y la latencia en el paquete multivínculo | **1479**
- Determinar si LFI y equilibrio de carga funcionan correctamente | **1479**
- Determinar por qué se dejan caer paquetes en un PVC entre un dispositivo de Juniper Networks y un dispositivo de terceros | **1488**

Para resolver problemas de configuración en una interfaz de servicios de vínculo:

Determinar qué componentes de CoS se aplican a los vínculos constituyentes

in this section

- Problema | **1476**
- Solución | **1476**

Problema

Description

Está configurando un paquete multivínculo, pero también tiene tráfico sin encapsulación MLPPP que pasa a través de vínculos constituyentes del paquete multivínculo. ¿Aplica todos los componentes de CoS a los enlaces constituyentes o es suficiente aplicarlos al paquete multivínculo?

Solución

Puede aplicar una asignación de programador al paquete multivínculo y a sus vínculos constituyentes. Aunque puede aplicar varios componentes de CoS con la asignación del programador, configure solo los que sean necesarios. Le recomendamos que mantenga la configuración de los enlaces constituyentes simple para evitar retrasos innecesarios en la transmisión.

Tabla 5 muestra los componentes de CoS que se aplicarán en un paquete multivínculo y sus vínculos constituyentes.

Tabla 155: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Clasificador	Sí	No	La clasificación CoS tiene lugar en el lado entrante de la interfaz, no en el lado de transmisión, por lo que no se necesitan clasificadores en los enlaces constituyentes.
Clase de reenvío	Sí	No	La clase de reenvío se asocia a una cola y la cola se aplica a la interfaz mediante una asignación de programador. La asignación de cola está predeterminada en los vínculos constituyentes. Todos los paquetes de Q2 del paquete multivínculo se asignan a Q2 del enlace constituyente, y los paquetes de todas las demás colas se ponen en cola en Q0 del enlace constituyente.

Tabla 155: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes *(Continued)*

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Mapa del programador	Sí	Sí	Aplique las asignaciones del programador en el paquete multivínculo y el vínculo constituyente de la siguiente manera: • Velocidad de transmisión: asegúrese de que el orden relativo de la velocidad de transmisión configurada en Q0 y Q2 sea el mismo en los vínculos constituyentes que en el paquete multivínculo. • Prioridad del programador: asegúrese de que el orden relativo de la prioridad del programador configurada en Q0 y Q2 sea el mismo en los vínculos constituyentes que en el paquete multivínculo. • Tamaño del búfer: dado que todos los paquetes que no son LFI del paquete multivínculo transitan en Q0 de los vínculos constituyentes, asegúrese de que el tamaño del búfer en Q0 de los enlaces constituyentes sea lo suficientemente grande. • Perfil de colocación RED: configure un perfil de colocación ROJA solo en el paquete multivínculo. La configuración del perfil de gota RED en los enlaces constituyentes aplica un mecanismo de contrapresión que cambia el tamaño del búfer e introduce variación. Dado que este comportamiento puede provocar caídas de fragmentos en los vínculos constituyentes, asegúrese de dejar el perfil de colocación ROJO en la configuración predeterminada de los vínculos constituyentes.

Tabla 155: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes *(Continued)*

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Velocidad de conformación para un programador por unidad o un programador de nivel de interfaz	No	Sí	Dado que la programación por unidad se aplica solo en el punto final, aplique esta velocidad de conformación solo a los vínculos constituyentes. Cualquier configuración aplicada anteriormente se sobrescribe con la configuración del vínculo constituyente.
Velocidad de transmisión exacta o modelado a nivel de cola	Sí	No	La forma a nivel de interfaz aplicada en los vínculos constituyentes anula cualquier forma en la cola. Por lo tanto, aplique la forma exacta de la velocidad de transmisión solo en el paquete multivínculo.
Reescritura de reglas	Sí	No	Los bits de reescritura se copian del paquete en los fragmentos automáticamente durante la fragmentación. Por lo tanto, lo que se configura en el paquete multivínculo se lleva en los fragmentos a los enlaces constituyentes.
Grupo de canales virtuales	Sí	No	Los grupos de canales virtuales se identifican mediante reglas de filtro de firewall que se aplican a los paquetes solo antes del paquete multivínculo. Por lo tanto, no es necesario aplicar la configuración del grupo de canales virtuales a los vínculos constituyentes.

SEE ALSO

Guía del usuario de clase de servicio (dispositivos de seguridad)

Determinar qué causa la fluctuación y la latencia en el paquete multivínculo

in this section

- Problema | 1479
- Solución | 1479

Problema

Description

Para probar la fluctuación y la latencia, se envían tres flujos de paquetes IP. Todos los paquetes tienen la misma configuración de prioridad de IP. Después de configurar LFI y CRTP, la latencia aumentó incluso en un vínculo no congestionado. ¿Cómo puede reducir la fluctuación y la latencia?

Solución

Para reducir la fluctuación y la latencia, haga lo siguiente:

1. Asegúrese de que ha configurado una velocidad de conformación en cada enlace constituyente.
2. Asegúrese de que no ha configurado una velocidad de conformación en la interfaz de servicios de vínculo.
3. Asegúrese de que el valor de la velocidad de conformación configurada sea igual al ancho de banda de la interfaz física.
4. Si las velocidades de conformación están configuradas correctamente y la fluctuación persiste, comuníquese con el Centro de asistencia técnica de Juniper Networks (JTAC).

Determinar si LFI y equilibrio de carga funcionan correctamente

in this section

- Problema | 1480
- Solución | 1480

Problema

Description

En este caso, tiene una sola red que admite varios servicios. La red transmite datos y tráfico de voz sensible a los retrasos. Después de configurar MLPPP y LFI, asegúrese de que los paquetes de voz se transmiten a través de la red con muy poco retraso y fluctuación. ¿Cómo puede saber si los paquetes de voz se tratan como paquetes LFI y si el equilibrio de carga se realiza correctamente?

Solución

Cuando LFI está habilitado, los paquetes de datos (no LFI) se encapsulan con un encabezado MLPPP y se fragmentan en paquetes de un tamaño especificado. Los paquetes de voz sensibles al retardo (LFI) están encapsulados en PPP e intercalados entre fragmentos de paquetes de datos. Las colas y el equilibrio de carga se realizan de manera diferente para los paquetes LFI y no LFI.

Para comprobar que LFI se realiza correctamente, determine que los paquetes estén fragmentados y encapsulados según lo configurado. Después de saber si un paquete se trata como un paquete LFI o un paquete que no es LFI, puede confirmar si el equilibrio de carga se realiza correctamente.

: supongamos que dos dispositivos de Juniper Networks, R0 y R1, están conectados por un paquete multivínculo que agrega dos vínculos serie y `.Solution Scenariolsq-0/0/0.0se-1/0/0se-1/0/1` En R0 y R1, MLPPP y LFI se habilitan en la interfaz de servicios de vínculo y el umbral de fragmentación se establece en 128 bytes.

En este ejemplo, usamos un generador de paquetes para generar flujos de voz y datos. Puede utilizar la función de captura de paquetes para capturar y analizar los paquetes en la interfaz entrante.

Los dos flujos de datos siguientes se enviaron en el paquete multivínculo:

- 100 paquetes de datos de 200 bytes (mayores que el umbral de fragmentación)
- 500 paquetes de datos de 60 bytes (más pequeños que el umbral de fragmentación)

Las dos secuencias de voz siguientes se enviaron en el paquete multivínculo:

- 100 paquetes de voz de 200 bytes desde el puerto fuente 100
- 300 paquetes de voz de 200 bytes desde el puerto fuente 200

Para confirmar que la LFI y el equilibrio de carga se realizan correctamente:

> **NOTA**: En este ejemplo, solo se muestran y describen las partes significativas de la salida del comando.

1. Compruebe la fragmentación de paquetes. Desde el modo operativo, escriba el comando para comprobar que los paquetes grandes están fragmentados correctamente.`show interfaces lsq-0/0/0`

```
user@R0#> show interfaces lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Last flapped   : 2006-08-01 10:45:13 PDT (2w0d 06:06 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

  Logical interface lsq-0/0/0.0 (Index 69) (SNMP ifIndex 42)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
    Bandwidth: 16mbps
    Statistics         Frames      fps       Bytes        bps
    Bundle:
      Fragments:
        Input :             0        0           0          0
        Output:          1100        0      118800          0
      Packets:
        Input :             0        0           0          0
        Output:          1000        0      112000          0
   ...
    Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 9.9.9/24, Local: 9.9.9.10
```

`Meaning`: el resultado muestra un resumen de los paquetes que transitan por el dispositivo en el paquete multivínculo. Compruebe la siguiente información en el paquete multivínculo:

- El número total de paquetes en tránsito = 1000
- El número total de fragmentos en tránsito=1100
- El número de paquetes de datos fragmentados =100

El número total de paquetes enviados (600 + 400) en el paquete multivínculo coincide con el número de paquetes en tránsito (1000), lo que indica que no se descartó ningún paquete.

El número de fragmentos en tránsito supera en 100 el número de paquetes en tránsito, lo que indica que 100 paquetes de datos grandes se fragmentaron correctamente.

`Corrective Action`: si los paquetes no están fragmentados correctamente, compruebe la configuración del umbral de fragmentación. Los paquetes menores que el umbral de fragmentación especificado no se fragmentan.

2. Verifique la encapsulación del paquete. Para averiguar si un paquete se trata como un paquete LFI o no LFI, determine su tipo de encapsulación. Los paquetes LFI están encapsulados PPP y los paquetes que no son LFI se encapsulan con PPP y MLPPP. Las encapsulaciones PPP y MLPPP tienen diferentes sobrecargas, lo que resulta en paquetes de diferentes tamaños. Puede comparar tamaños de paquetes para determinar el tipo de encapsulación.

   Un pequeño paquete de datos no fragmentado contiene un encabezado PPP y un solo encabezado MLPPP. En un paquete de datos fragmentado de gran tamaño, el primer fragmento contiene un encabezado PPP y un encabezado MLPPP, pero los fragmentos consecutivos contienen solo un encabezado MLPPP.

   Las encapsulaciones PPP y MLPPP agregan el siguiente número de bytes a un paquete:

   - La encapsulación PPP agrega 7 bytes:

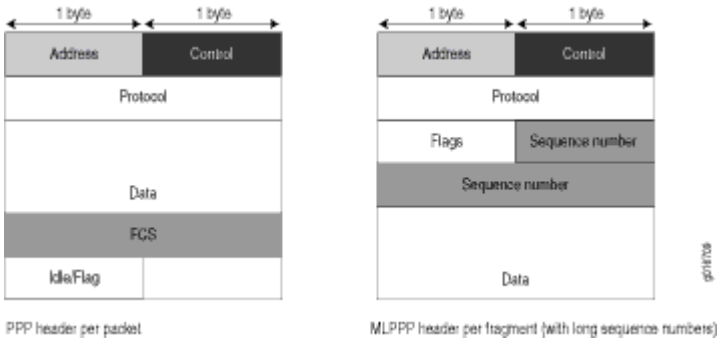
     4 bytes de encabezado + 2 bytes de secuencia de comprobación de tramas (FCS) + 1 byte que está inactivo o contiene una marca

   - La encapsulación MLPPP agrega entre 6 y 8 bytes:

     4 bytes de encabezado PPP+2 a 4 bytes de encabezado multivínculo

   Figura 1 muestra la sobrecarga agregada a los encabezados PPP y MLPPP.

Figura 47: Encabezados PPP y MLPPP



Para los paquetes CRTP, la sobrecarga de encapsulación y el tamaño del paquete son incluso menores que para un paquete LFI. Para obtener más información, consulte Ejemplo: Configuración del protocolo de transporte comprimido en tiempo real.

Tabla 6 muestra la sobrecarga de encapsulación de un paquete de datos y un paquete de voz de 70 bytes cada uno. Después de la encapsulación, el tamaño del paquete de datos es mayor que el tamaño del paquete de voz.

Tabla 156: Sobrecarga de encapsulación PPP y MLPPP

Tipo de paquete	Encapsulación	Tamaño inicial del paquete	Sobrecarga de encapsulación	Tamaño del paquete después de la encapsulación
Paquete de voz (LFI)	PPP	70 bytes	4 + 2 + 1 = 7 bytes	77 bytes
Fragmento de datos (no LFI) con secuencia corta	MLPPP	70 bytes	4 + 2 + 1 + 4 + 2 = 13 bytes	83 bytes
Fragmento de datos (no LFI) con secuencia larga	MLPPP	70 bytes	4 + 2 + 1 + 4 + 4 = 15 bytes	85 bytes

Desde el modo operativo, escriba el comando para mostrar el tamaño del paquete transmitido en cada cola.`show interfaces queue` Divida el número de bytes transmitidos por el número de paquetes para obtener el tamaño de los paquetes y determinar el tipo de encapsulación.

3. Verifique el equilibrio de carga. Desde el modo operativo, introduzca el comando en el paquete multivínculo y sus enlaces constituyentes para confirmar si el equilibrio de carga se realiza en consecuencia en los paquetes.`show interfaces queue`

```
user@R0> show interfaces queue lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                600                   0 pps
    Bytes                :              44800                   0 bps
  Transmitted:
    Packets              :                600                   0 pps
```

```
    Bytes                :              44800                  0 bps
    Tail-dropped packets :                  0                  0 pps
    RED-dropped packets  :                  0                  0 pps
    …
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                  0 pps
    Bytes                :                  0                  0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                400                  0 pps
    Bytes                :              61344                  0 bps
  Transmitted:
    Packets              :                400                  0 pps
    Bytes                :              61344                  0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                  0                  0 pps
    Bytes                :                  0                  0 bps
 …
```

```
user@R0> show interfaces queue se-1/0/0
Physical interface: se-1/0/0, Enabled, Physical link is Up
  Interface index: 141, SNMP ifIndex: 35
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
  Transmitted:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
   ...
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                 0 pps
    Bytes                :                  0                 0 bps
  …
```

```
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                100                 0 pps
    Bytes                :              15272                 0 bps
  Transmitted:
    Packets              :                100                 0 pps
    Bytes                :              15272                 0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                 19                 0 pps
    Bytes                :                247                 0 bps
  Transmitted:
    Packets              :                 19                 0 pps
    Bytes                :                247                 0 bps
    …
```

```
user@R0> show interfaces queue se-1/0/1
Physical interface: se-1/0/1, Enabled, Physical link is Up
  Interface index: 142, SNMP ifIndex: 38
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
  Transmitted:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
    …
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                 0 pps
    Bytes                :                  0                 0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                300                 0 pps
    Bytes                :              45672                 0 bps
  Transmitted:
    Packets              :                300                 0 pps
```

```
    Bytes                :              45672                 0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                 18                 0 pps
    Bytes                :                234                 0 bps
  Transmitted:
    Packets              :                 18                 0 pps
    Bytes                :                234                 0 bps
```

: el resultado de estos comandos muestra los paquetes transmitidos y en cola en cada cola de la interfaz de servicios de vínculo y sus vínculos constituyentes. muestra un resumen de estos valores.`Meaning`Tabla 7 (Dado que el número de paquetes transmitidos es igual al número de paquetes en cola en todos los vínculos, esta tabla muestra sólo los paquetes en cola).

Tabla 157: Número de paquetes transmitidos en una cola

Paquetes en cola	Paquete lsq-0/0/0.0	Enlace constituyente se-1/0/0	Enlace constituyente se-1/0/1	Explicación
Paquetes en Q0	600	350	350	El número total de paquetes que transitan por los vínculos constituyentes (350+350 = 700) superó el número de paquetes en cola (600) en el paquete multivínculo.
Paquetes en Q2	400	100	300	El número total de paquetes que transitan por los vínculos constituyentes es igual al número de paquetes del paquete.
Paquetes en Q3	0	19	18	Los paquetes que transitan Q3 de los enlaces constituyentes son para mensajes keepalive intercambiados entre enlaces constituyentes. Por lo tanto, no se contaron paquetes en Q3 del paquete.

En el paquete multivínculo, compruebe lo siguiente:

- El número de paquetes en cola coincide con el número transmitido. Si los números coinciden, no se descartó ningún paquete. Si se ponían en cola más paquetes de los que se transmitían, los paquetes se descartaban porque el búfer era demasiado pequeño. El tamaño del búfer en los vínculos constituyentes controla la congestión en la etapa de salida. Para corregir este problema, aumente el tamaño del búfer en los vínculos constituyentes.

- El número de paquetes que transitan Q0 (600) coincide con el número de paquetes de datos grandes y pequeños recibidos (100+500) en el paquete multivínculo. Si los números coinciden, todos los paquetes de datos transitaron correctamente Q0.

- El número de paquetes que transitan Q2 en el paquete multivínculo (400) coincide con el número de paquetes de voz recibidos en el paquete multivínculo. Si los números coinciden, todos los paquetes LFI de voz transitaron correctamente Q2.

En los vínculos constituyentes, compruebe lo siguiente:

- El número total de paquetes que transitan Q0 (350+350) coincide con el número de paquetes de datos y fragmentos de datos (500+200). Si los números coinciden, todos los paquetes de datos después de la fragmentación transitaron correctamente Q0 de los enlaces constituyentes.

  Los paquetes transitaron por ambos enlaces constituyentes, lo que indica que el equilibrio de carga se realizó correctamente en paquetes que no eran LFI.

- El número total de paquetes que transitan Q2 (300+100) en los enlaces constituyentes coincide con el número de paquetes de voz recibidos (400) en el paquete multivínculo. Si los números coinciden, todos los paquetes LFI de voz transitaron correctamente Q2.

  Paquetes LFI desde el puerto de origen transitados y paquetes LFI desde el puerto de origen transitados.`100se-1/0/0200se-1/0/1` Por lo tanto, todos los paquetes LFI (Q2) se cifraron en función del puerto de origen y transitaron correctamente ambos enlaces constituyentes.

`Corrective Action`: si los paquetes transitaron solo un vínculo, siga estos pasos para resolver el problema:

1. Determine si el vínculo físico está (operativo) o (no disponible).`updown` Un vínculo no disponible indica un problema con el PIM, el puerto de interfaz o la conexión física (errores de capa de enlace). Si el vínculo está operativo, vaya al paso siguiente.

2. Compruebe que los clasificadores estén definidos correctamente para los paquetes que no son LFI. Asegúrese de que los paquetes que no sean LFI no estén configurados para ponerse en cola en Q2. Todos los paquetes en cola para Q2 se tratan como paquetes LFI.

3. Compruebe que al menos uno de los siguientes valores es diferente en los paquetes LFI: dirección de origen, dirección de destino, protocolo IP, puerto de origen o puerto de destino. Si se configuran los mismos valores para todos los paquetes LFI, todos los paquetes se cifran al mismo flujo y transitan por el mismo vínculo.

4. Utilice los resultados para verificar el equilibrio de carga.

Determinar por qué se dejan caer paquetes en un PVC entre un dispositivo de Juniper Networks y un dispositivo de terceros

in this section

- Problema | **1488**
- Solución | **1488**

Problema

Description

Está configurando un circuito virtual permanente (PVC) entre interfaces T1, E1, T3 o E3 en un dispositivo de Juniper Networks y un dispositivo de terceros, y los paquetes se descartan y se produce un error en el ping.

Solución

Si el dispositivo de terceros no tiene la misma compatibilidad con FRF.12 que el dispositivo de Juniper Networks o admite FRF.12 de otra manera, la interfaz del dispositivo de Juniper Networks en el PVC podría descartar un paquete fragmentado que contenga encabezados FRF.12 y contarlo como un "descarte vigilado".

Como solución alternativa, configure paquetes multivínculo en ambos pares y configure umbrales de fragmentación en los paquetes multivínculo.

Solución de problemas de las políticas de seguridad

in this section

- Sincronización de políticas entre el motor de enrutamiento y el motor de reenvío de paquetes | **1489**
- Comprobación de un error de confirmación de política de seguridad | **1490**
- Comprobación de una confirmación de política de seguridad | **1491**

- Depurar búsqueda de directivas | 1492

Sincronización de políticas entre el motor de enrutamiento y el motor de reenvío de paquetes

in this section

- Problema | 1489
- Solución | 1490

Problema

Description

Las políticas de seguridad se almacenan en el motor de enrutamiento y en el motor de reenvío de paquetes. Las políticas de seguridad se insertan desde el motor de enrutamiento al motor de reenvío de paquetes cuando se confirman las configuraciones. Si las políticas de seguridad del motor de enrutamiento no están sincronizadas con el motor de reenvío de paquetes, se produce un error en la confirmación de una configuración. Se pueden generar archivos de volcado de núcleo si se intenta la confirmación repetidamente. La falta de sincronización puede deberse a:

- Un mensaje de política del motor de enrutamiento al motor de reenvío de paquetes se pierde en tránsito.
- Un error con el motor de enrutamiento, como un UID de directiva reutilizado.

Entorno

Las directivas del motor de enrutamiento y del motor de reenvío de paquetes deben estar sincronizadas para que se confirme la configuración. Sin embargo, en determinadas circunstancias, es posible que las directivas del motor de enrutamiento y del motor de reenvío de paquetes no estén sincronizadas, lo que provoca un error en la confirmación.

Síntomas

Cuando se modifican las configuraciones de directiva y las directivas no están sincronizadas, aparece el siguiente mensaje de error: `error: Warning: policy might be out of sync between RE and PFE <SPU-name(s)> Please request security policies check/resync.`

Solución

Use el comando para mostrar el valor de suma de comprobación de la directiva de seguridad y use el comando para sincronizar la configuración de las directivas de seguridad en el motor de enrutamiento y el motor de reenvío de paquetes, si las directivas de seguridad no están sincronizadas.`show security policies checksumrequest security policies resync`

SEE ALSO

show security policies checksum

request security policies check

request security policies resync

Comprobación de un error de confirmación de política de seguridad

in this section

- Problema | **1490**
- Solución | **1491**

Problema

Description

La mayoría de los errores de configuración de directivas se producen durante una confirmación o un tiempo de ejecución.

Los errores de confirmación se notifican directamente en la CLI cuando se ejecuta el comando de la CLI en modo de configuración.**commit-check** Estos errores son errores de configuración y no puede confirmar la configuración sin corregirlos.

Solución

Para corregir estos errores, haga lo siguiente:

1. Revise los datos de configuración.
2. Abra el archivo /var/log/nsd_chk_only. Este archivo se sobrescribe cada vez que se realiza una comprobación de confirmación y contiene información detallada sobre el error.

Comprobación de una confirmación de política de seguridad

in this section

Problema | 1491
Solución | 1491

Problema

Description

Al realizar una confirmación de configuración de directiva, si observa que el comportamiento del sistema es incorrecto, siga estos pasos para solucionar este problema:

Solución

1. Comandos operativos : ejecute los comandos operativos para las políticas de seguridad y compruebe que la información que se muestra en el resultado es coherente con lo que esperaba.**show** De lo contrario, la configuración debe cambiarse adecuadamente.
2. Traceoptions: defina el comando en la configuración de la política.`traceoptions` Los indicadores bajo esta jerarquía se pueden seleccionar según el análisis del usuario de la salida del comando.`show` Si no puede determinar qué indicador usar, la opción de indicador se puede usar para capturar todos los registros de seguimiento.`all`

```
user@host# set security policies traceoptions <flag all>
```

También puede configurar un nombre de archivo opcional para capturar los registros.

```
user@host# set security policies traceoptions <filename>
```

Si especificó un nombre de archivo en las opciones de seguimiento, puede buscar el archivo de registro en /var/log/<filename> para determinar si se ha notificado algún error en el archivo. (Si no especificó un nombre de archivo, el nombre de archivo predeterminado es eventual). Los mensajes de error indican el lugar del error y la razón apropiada.

Después de configurar las opciones de seguimiento, debe volver a confirmar el cambio de configuración que provocó el comportamiento incorrecto del sistema.

Depurar búsqueda de directivas

in this section

- Problema | **1492**
- Solución | **1492**

Problema

Description

Si tiene la configuración correcta, pero parte del tráfico se ha interrumpido o permitido incorrectamente, puede habilitar el indicador en las traceoptions de las políticas de seguridad.`lookup` La marca registra los seguimientos relacionados con la búsqueda en el archivo de seguimiento.`lookup`

Solución

```
user@host# set security policies traceoptions <flag lookup>
```

Registrar mensajes de error utilizados para solucionar problemas relacionados con ISSU

in this section

- Errores de proceso del chasis | 1493
- Descripción del control de errores comunes para ISSU | 1494
- Errores relacionados con soporte técnico de ISSU | 1498
- Error en las comprobaciones de validación inicial | 1498
- Errores relacionados con la instalación | 1500
- Errores de conmutación por error del grupo de redundancia | 1501
- Errores de sincronización de estado del kernel | 1502

Los siguientes problemas pueden producirse durante una actualización de ISSU. Puede identificar los errores mediante los detalles de los registros. Para obtener información detallada acerca de mensajes de registro del sistema específicos, consulte Explorador de registros del sistema.

Errores de proceso del chasis

in this section

- Problema | 1493
- Solución | 1493

Problema

Description

Errores relacionados con el chasis.

Solución

Utilice los mensajes de error para comprender los problemas relacionados con el chasisd.

Cuando se inicia ISSU, se envía una solicitud al chasis para comprobar si hay algún problema relacionado con el ISSU desde la perspectiva del chasis. Si hay un problema, se crea un mensaje de registro.

Descripción del control de errores comunes para ISSU

in this section

- Problema | **1494**
- Solución | **1494**

Problema

Description

Es posible que encuentre algunos problemas en el curso de una ISSU. En esta sección se proporcionan detalles sobre cómo manejarlos.

Solución

Cualquier error encontrado durante una ISSU da como resultado la creación de mensajes de registro e ISSU sigue funcionando sin afectar al tráfico. Si es necesario revertir a versiones anteriores, el evento se registra o el ISSU se detiene, para no crear versiones no coincidentes en ambos nodos del clúster de chasis. Tabla 158 en la página 1494 Proporciona algunas de las condiciones de error comunes y sus soluciones. Los mensajes de ejemplo que se usan en el provienen del dispositivo SRX1500 y también son aplicables a todos los firewalls de la serie SRX compatibles.Tabla 158 en la página 1494

Tabla 158: Errores y soluciones relacionados con ISSU

Condiciones de error	Soluciones
Intentar iniciar una ISSU cuando la instancia anterior de una ISSU ya está en curso	Se muestra el siguiente mensaje: `warning: ISSU in progress` Puede anular el proceso actual de ISSU e iniciar el ISSU de nuevo con el comando.`request chassis cluster in-service-upgrade abort`

Tabla 158: Errores y soluciones relacionados con ISSU *(Continued)*

Condiciones de error	Soluciones

Error de reinicio en el nodo secundario	No se produce ningún tiempo de inactividad del servicio, ya que el nodo principal sigue proporcionando los servicios necesarios. Se muestran mensajes detallados de la consola en los que se solicita que borre manualmente los estados de ISSU existentes y restaure el clúster de chasis.
	
	`error: [Oct  6 12:30:16]: Reboot secondary node failed (error-code: 4.1)`
	
	`error: [Oct  6 12:30:16]: ISSU Aborted! Backup node maybe in inconsistent state, Please restore backup node`
	`[Oct  6 12:30:16]: ISSU aborted. But, both nodes are in ISSU window.`
	`Please do the following:`
	`1. Rollback the node with the newer image using rollback command`
	`Note: use the 'node' option in the rollback command`
	`otherwise, images on both nodes will be rolled back`
	`2. Make sure that both nodes (will) have the same image`
	`3. Ensure the node with older image is primary for all RGs`
	`4. Abort ISSU on both nodes`
	`5. Reboot the rolled back node`
	
	A partir de Junos OS versión 17.4R1, el temporizador de espera para el reinicio inicial del nodo secundario durante el proceso ISSU se amplía de 15 minutos (900 segundos) a 45 minutos (2700 segundos) en clústeres de chasis en dispositivos SRX1500, SRX4100, SRX4200 y SRX4600.

Tabla 158: Errores y soluciones relacionados con ISSU *(Continued)*

Condiciones de error	Soluciones

El nodo secundario no pudo completar la sincronización en frío	Se agota el tiempo de espera del nodo principal si el nodo secundario no puede completar la sincronización en frío. Se muestran mensajes de consola detallados que borran manualmente los estados de ISSU existentes y restauran el clúster de chasis. No se produce ningún tiempo de inactividad del servicio en este escenario.
	
	`[Oct  3 14:00:46]: timeout waiting for secondary node node1 to sync(error-code: 6.1)`
	`Chassis control process started, pid 36707`
	
	`error: [Oct  3 14:00:46]: ISSU Aborted! Backup node has been upgraded, Please restore backup node`
	`[Oct  3 14:00:46]: ISSU aborted. But, both nodes are in ISSU window.`
	`Please do the following:`
	`1. Rollback the node with the newer image using rollback command`
	`Note: use the 'node' option in the rollback command`
	`otherwise, images on both nodes will be rolled back`
	`2. Make sure that both nodes (will) have the same image`
	`3. Ensure the node with older image is primary for all RGs`
	`4. Abort ISSU on both nodes`
	`5. Reboot the rolled back node`

Tabla 158: Errores y soluciones relacionados con ISSU *(Continued)*

Condiciones de error	Soluciones

Error de conmutación por error de secundaria recién actualizada	No se produce ningún tiempo de inactividad del servicio, ya que el nodo principal sigue proporcionando los servicios necesarios. Se muestran mensajes detallados de la consola en los que se solicita que borre manualmente los estados de ISSU existentes y restaure el clúster de chasis.
	
	`[Aug 27 15:28:17]: Secondary node0 ready for failover.`
	`[Aug 27 15:28:17]: Failing over all redundancy-groups to node0`
	`ISSU: Preparing for Switchover`
	`error: remote rg1 priority zero, abort failover.`
	`[Aug 27 15:28:17]: failover all RGs to node node0 failed (error-code: 7.1)`
	`error: [Aug 27 15:28:17]: ISSU Aborted!`
	`[Aug 27 15:28:17]: ISSU aborted. But, both nodes are in ISSU window.`
	`Please do the following:`
	`1. Rollback the node with the newer image using rollback command`
	`Note: use the 'node' option in the rollback command`
	`otherwise, images on both nodes will be rolled back`
	`2. Make sure that both nodes (will) have the same image`
	`3. Ensure the node with older image is primary for all RGs`
	`4. Abort ISSU on both nodes`
	`5. Reboot the rolled back node`
	`{primary:node1}`

Error de actualización en la estación principal	No se produce ningún tiempo de inactividad del servicio, ya que el nodo secundario conmuta por error como principal y continúa proporcionando los servicios necesarios.

Error de reinicio en el nodo principal	Antes del reinicio del nodo principal, ya que los dispositivos están fuera de la configuración de ISSU, no se muestran mensajes de error relacionados con ISSU. Se muestra el siguiente mensaje de error de reinicio si se detecta algún otro error:
	
	`Reboot failure on Before the reboot of primary node, devices will be out of ISSU setup and no primary node error messages will be displayed.`
	`Primary node`

Errores relacionados con soporte técnico de ISSU

in this section

- Problema | 1498
- Solución | 1498

Problema

Description

Se produce un error de instalación debido a software no compatible y a una configuración de características no compatible.

Solución

Utilice los siguientes mensajes de error para comprender los problemas relacionados con la compatibilidad:

```
WARNING: Current configuration not compatible with /var/tmp/junos-srx5000-11.4X3.2-domestic.tgz
Exiting in-service-upgrade window
Exiting in-service-upgrade window
```

Error en las comprobaciones de validación inicial

in this section

- Problema | 1499
- Solución | 1499

Problema

Description

Las comprobaciones de validación iniciales fallan.

Solución

Las comprobaciones de validación fallan si la imagen no está presente o si el archivo de imagen está dañado. Los siguientes mensajes de error se muestran cuando las comprobaciones de validación iniciales fallan cuando la imagen no está presente y se anula el ISSU:

Cuando la imagen no está presente

```
user@host> ...0120914_srx_12q1_major2.2-539764-domestic.tgz reboot
Chassis ISSU Started
Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade
Initiating in-service-upgrade
Fetching package...
error: File does not exist: /var/tmp/junos-srx1k3k-12.1I20120914_srx_12q1_major2.2-539764-
domestic.tgz
error: Couldn't retrieve package /var/tmp/junos-srx1k3k-12.1I20120914_srx_12q1_major2.2-539764-
domestic.tgz
Exiting in-service-upgrade window
Exiting in-service-upgrade window
Chassis ISSU Aborted
Chassis ISSU Aborted
Chassis ISSU Aborted
ISSU: IDLE
ISSU aborted; exiting ISSU window.
```

Cuando el archivo de imagen está dañado

Si el archivo de imagen está dañado, se muestra el siguiente resultado:

```
user@host> ...junos-srx1k3k-11.4X9-domestic.tgz_1 reboot
Chassis ISSU Started
node1:
--------------------------------------------------------------------------
```

```
Chassis ISSU Started
ISSU: Validating Image
Initiating in-service-upgrade

node1:
--------------------------------------------------------------------------
Initiating in-service-upgrade
ERROR: Cannot use /var/tmp/junos-srx1k3k-11.4X9-domestic.tgz_1:
gzip: stdin: invalid compressed data--format violated
tar: Child returned status 1
tar: Error exit delayed from previous errors
ERROR: It may have been corrupted during download.
ERROR: Please try again, making sure to use a binary transfer.
Exiting in-service-upgrade window

node1:
--------------------------------------------------------------------------
Exiting in-service-upgrade window
Chassis ISSU Aborted
Chassis ISSU Aborted

node1:
--------------------------------------------------------------------------
Chassis ISSU Aborted
ISSU: IDLE
ISSU aborted; exiting ISSU window.

{primary:node0}
```

El nodo principal valida la configuración del dispositivo para garantizar que se pueda confirmar con la nueva versión del software. Si algo sale mal, la ISSU se anula y se muestran mensajes de error.

Errores relacionados con la instalación

in this section

- Problema | **1501**
- Solución | **1501**

Problema

Description

El archivo de imagen de instalación no existe o el sitio remoto es inaccesible.

Solución

Utilice los siguientes mensajes de error para comprender los problemas relacionados con la instalación:

```
error: File does not exist: /var/tmp/junos-srx5000-11.4X3.2-domest
error: Couldn't retrieve package /var/tmp/junos-srx5000-11.4X3.2-domest
```

ISSU descarga la imagen de instalación como se especifica en el comando ISSU como argumento. El archivo de imagen puede ser un archivo local o ubicado en un sitio remoto. Si el archivo no existe o el sitio remoto es inaccesible, se informa de un error.

Errores de conmutación por error del grupo de redundancia

in this section

- Problema | **1501**
- Solución | **1501**

Problema

Description

Problema con un error del grupo de redundancia automática (RG).

Solución

Utilice los siguientes mensajes de error para comprender el problema:

```
failover all RG 1+ groups to node 0
error: Command failed.  None of the redundancy-groups has been failed over.
```

```
Some redundancy-groups on node1 are already in manual failover mode.
Please execute 'failover reset all' first..
```

Errores de sincronización de estado del kernel

in this section

- Problema | **1502**
- Solución | **1502**

Problema

Description

Errores relacionados con ksyncd.

Solución

Use los siguientes mensajes de error para comprender los problemas relacionados con ksyncd:

```
Failed to get kernel-replication error information from Standby Routing Engine.
mgd_slave_peer_has_errors() returns error at line 4414 in mgd_package_issu.
```

ISSU comprueba si hay errores de ksyncd en el nodo secundario (nodo 1) y muestra el mensaje de error si hay algún problema y anula la actualización.

Tabla de historial de cambios

La compatibilidad de la función depende de la plataforma y la versión que utilice. Utilice Feature Explorer a fin de determinar si una función es compatible con la plataforma.

release heading in release-history	desc heading in release-history
17.4R1	A partir de Junos OS versión 17.4R1, el temporizador de espera para el reinicio inicial del nodo secundario durante el proceso ISSU se amplía de 15 minutos (900 segundos) a 45 minutos (2700 segundos) en clústeres de chasis en dispositivos SRX1500, SRX4100, SRX4200 y SRX4600.

Solución de problemas del rendimiento del sistema con la metodología de monitoreo de recursos

in this section

- Descripción general del cálculo del uso de la supervisión de recursos | 1503
- Diagnóstico y depuración del rendimiento del sistema mediante la configuración de la supervisión del uso de recursos de memoria en enrutadores de la serie MX | 1506
- Solucionar problemas de la discrepancia de los valores de jnxNatObjects para MS-DPC y MS-MIC | 1510
- Objetos administrados para la memoria Ukernel para un motor de reenvío de paquetes en una ranura FPC | 1512
- Objetos administrados para datos estadísticos de memoria del motor de reenvío de paquetes | 1512
- Objetos administrados para el próximo salto, Jtree y memoria de filtro de firewall para un motor de reenvío de paquetes en una ranura FPC | 1513
- jnxPfeMemoryErrorsTable | 1513
- pfeMemoryErrors | 1514

Descripción general del cálculo del uso de la supervisión de recursos

in this section

- Monitoreo de recursos y cálculo del uso para tarjetas de línea basadas en Trio | 1504
- Monitoreo de recursos y cálculo de uso para tarjetas de línea basadas en I-Chip | 1504

Puede configurar la capacidad de supervisión de recursos mediante las consultas MIB de CLI y SNMP. Puede emplear esta utilidad para aprovisionar suficiente espacio libre (límites de espacio de memoria establecidos para la aplicación o el enrutador virtual) para supervisar el estado y la eficiencia operativa de los DPC y MPC. También puede analizar y ver el uso o consumo de memoria para el tipo de memoria jtree y para páginas contiguas, palabras dobles y páginas de memoria libre. La memoria jtree en todos los motores de reenvío de paquetes del enrutador de la serie MX tiene dos segmentos: Un segmento almacena principalmente tablas de enrutamiento e información relacionada, y el otro segmento

almacena principalmente información relacionada con el filtro de firewall. Como la asignación de más memoria para tablas de enrutamiento o filtros de firewall puede interrumpir las operaciones de reenvío de un motor de reenvío de paquetes, la CLI de Junos OS muestra una advertencia para reiniciar todos los FPC afectados cuando confirme una configuración que incluya la instrucción route mejorada en memoria.

Las siguientes secciones describen las ecuaciones de cálculo y la interpretación de las diferentes regiones de memoria para tarjetas de línea basadas en I-chip y en Trio:

Monitoreo de recursos y cálculo del uso para tarjetas de línea basadas en Trio

En las tarjetas de línea basadas en Trio, los bloques de memoria para los filtros de salto siguiente y firewall se asignan por separado. Además, hay una memoria de expansión, que se utiliza cuando la memoria asignada para el filtro de firewall o salto siguiente se consume por completo. Tanto el filtro del próximo salto como el del firewall pueden asignar memoria desde la memoria de expansión. La región de memoria de encapsulación es específica de las tarjetas de línea basadas en I-chip y no es aplicable a las tarjetas de línea basadas en Trio. Por lo tanto, para las tarjetas de línea basadas en Trio, el porcentaje de espacio libre en memoria se puede interpretar de la siguiente manera:

% Free (NH) = (1- (Used NH memory + Used Expansion memory) / (Total NH memory+Total Expansion memory)) × 100

% Free (Firewall or Filter) = (1-(Used FW memory+Used Expansion memory) / (Total FW memory+Total Expansion memory)) × 100

La memoria de encapsulación es específica del chip I y no es aplicable a las tarjetas de línea basadas en Trio.

% Free (Encap memory) = Not applicable

Monitoreo de recursos y cálculo de uso para tarjetas de línea basadas en I-Chip

Las tarjetas de línea basadas en I-chip contienen 32 MB de memoria RAM estática (SRAM) asociada con el bloque de búsqueda de ruta y 16 MB de memoria SRAM asociada con el bloque WAN de salida.

La memoria de búsqueda de ruta es un único grupo de 32 MB de memoria que se divide en dos segmentos de 16 MB cada uno. En una configuración estándar, el segmento 0 se usa para NH y prefijos, y el segmento 1 se usa para firewall o filtro. Esta asignación se puede modificar mediante la opción mejorada de memoria de ruta en el nivel de jerarquía [edit chassis]. En una configuración general, a la aplicación NH se le puede asignar memoria desde cualquiera de los dos segmentos. Por lo tanto, el porcentaje de memoria libre para NH se calcula en 32 MB de memoria. Actualmente, a las aplicaciones de firewall sólo se les asigna memoria del segmento 1. Como resultado, el porcentaje de memoria libre que se debe supervisar para el firewall comienza desde la memoria disponible de 16 MB en el segmento 1 solamente.

Para las tarjetas de línea basadas en I-chip, el porcentaje de espacio libre en la memoria se puede interpretar de la siguiente manera:

```
% Free (NH) = (32-(Used NH memory+Used FW memory+Used Other application)) / 32×100
```

```
% Free (Firewall or Filter)=(16-(Used NH memory+Used FW memory+Used Other application)) / 16×100
```

El tamaño de memoria para la SRAM de WAN de salida (Iwo) es de 16 MB y almacena los descriptores de capa 2 que contienen la información de encapsulación. Esta entidad es un recurso crítico y necesita ser monitoreada. Este espacio de memoria se muestra en la salida del comando show como "Encap mem". El porcentaje de memoria libre para la región de encapsulación se calcula de la siguiente manera:

% Free (Encapsulation memory) = (16-(Iwo memory used (L2 descriptors +other applications))) / 16×100

El nivel de marca de agua configurado para la memoria del próximo salto también es eficaz para la memoria de encapsulación. Por lo tanto, si el porcentaje de memoria libre para la región de encapsulación cae por debajo de la marca de agua configurada, se generan registros.

Si el porcentaje de memoria libre es menor que la marca de agua de memoria libre de un tipo de memoria específico, se registra el siguiente mensaje de error en el syslog:

```
“Resource Monitor: FPC <slot no> PFE <pfe inst> <“JNH memory” or “FW/ Filter memory”> is below set watermark
<configured watermark>”.
```

Puede configurar operaciones de seguimiento de supervisión de recursos mediante la instrucción en el nivel de jerarquía.`traceoptions file <`*`filename`*`> flag `*`flag`*` level `*`level`*` size `*`bytes`*`[edit system services resource-monitor]` De forma predeterminada, los mensajes se escriben en **./var/log/rsmonlog** Los registros de errores asociados con el error de comunicación del socket (entre el motor de enrutamiento y el motor de reenvío de paquetes) son útiles para diagnosticar los problemas en la comunicación entre el motor de enrutamiento y el motor de reenvío de paquetes.

Desde la perspectiva ucraniana, MPC5E contiene solo una instancia de motor de reenvío de paquetes. La salida del comando show chassis fabric plane muestra el estado de las conexiones del plano de fabric al motor de reenvío de paquetes. Dado que existen dos motores de reenvío de paquetes, verá PFE-0 y PFE-1 en la salida.

```
user@host# run show chassis fabric plane
Fabric management PLANE state
Plane 0
  Plane state: ACTIVE
      FPC 0
          PFE 0 :Links ok
          PFE 1 :Links ok
```

Dado que solo existe una instancia de motor de reenvío de paquetes para MPC5E, el resultado del comando fpc show system resource-monitor muestra solo una fila correspondiente a la instancia 0 del motor de reenvío de paquetes.

```
user@host# run show system resource-monitor fpc
FPC Resource Usage Summary

Free Heap Mem Watermark         : 20  %
Free NH Mem Watermark           : 20  %
Free Filter Mem Watermark       : 20  %

* - Watermark reached

                    Heap                      ENCAP mem       NH mem          FW mem
   Slot #         % Free    PFE #           % Free       % Free          % Free
        0            94              0                    NA           83              99
```

La marca de agua configurada se conserva en los procedimientos GRES e ISSU unificados.

Diagnóstico y depuración del rendimiento del sistema mediante la configuración de la supervisión del uso de recursos de memoria en enrutadores de la serie MX

Junos OS admite una capacidad de supervisión de recursos mediante las consultas MIB de CLI y SNMP. Puede emplear esta utilidad para aprovisionar suficiente espacio libre (límites de espacio de memoria establecidos para la aplicación o el enrutador virtual) para garantizar la estabilidad del sistema, especialmente el estado y la eficiencia operativa de las tarjetas de línea basadas en I-chip y los FPC basados en Trio en enrutadores de la serie MX. Cuando la utilización de la memoria, ya sea la memoria ukernel o la memoria ASIC, alcanza un cierto umbral, las operaciones del sistema comprometen la salud y la estabilidad del manejo del tráfico de la tarjeta de línea y tal compensación en el rendimiento del sistema puede ser perjudicial para admitir tráfico y protocolos en vivo.

Para configurar las propiedades de la funcionalidad de utilización de recursos de memoria:

1. Especifique que desea configurar el mecanismo de supervisión para el uso de diferentes regiones de recursos de memoria.

```
[edit]
user@host# edit system services resource-monitor
```

Esta función está habilitada de forma predeterminada y no se puede deshabilitar manualmente.

2. Especifique el valor de umbral alto, por encima del cual se generan las advertencias o los registros de errores, para todas las regiones de memoria, como montón o ukernel, salto siguiente y encapsulación, y memoria de filtro de firewall.

```
[edit system services resource-monitor]
user@host# set high-threshold value
```

3. Especifique el porcentaje de espacio libre de memoria utilizado para supervisar los próximos saltos con un valor de marca de agua.

```
[edit system services resource-monitor]
user@host# set free-nh-memory-watermark percentage
```

4. Especifique el porcentaje de espacio de memoria libre utilizado para ukernel o memoria de montón que se va a supervisar con un valor de marca de agua.

```
[edit system services resource-monitor]
user@host# set free-heap-memory- watermark percentage
```

5. Especifique el porcentaje de espacio libre de memoria utilizado para la memoria del firewall y del filtro que se va a supervisar con un valor de marca de agua.

```
[edit system services resource-monitor]
user@host# set free-filter-memory-memory- watermark percentage
```

NOTA:

El valor predeterminado y el valor configurado del valor de marca de agua para el porcentaje de memoria libre del próximo salto también se aplican a la memoria de encapsulación. Los valores de marca de agua predeterminados para el porcentaje de memoria libre de ukernel o montón, memoria del próximo salto y memoria de filtro de firewall son del 20 por ciento.

6. Deshabilite la generación de mensajes de registro de errores cuando el uso de recursos de memoria supere los niveles de umbral o punto de control. De forma predeterminada, los mensajes se escriben en /var/log/rsmonlog.

```
[edit system services resource-monitor]
user@host# set no-logging
```

7. Defina la categoría de recursos que desea supervisar y analizar para garantizar la estabilidad del sistema, especialmente el estado y la eficiencia operativa de las tarjetas de línea basadas en I-chip y las FPC basadas en Trio en enrutadores de la serie MX. La categoría de recursos incluye estadísticas detalladas de utilización de CPU, velocidad de sesión y recuento de sesiones. Utilice las estadísticas de categoría de recursos para comprender en qué medida los nuevos objetos o aplicaciones de ataque afectan al rendimiento.

```
[edit system services resource-monitor]
user@host# edit resource-category jtree
```

> **NOTA**: La memoria jtree en todos los motores de reenvío de paquetes del enrutador de la serie MX tiene dos segmentos: Un segmento almacena principalmente tablas de enrutamiento e información relacionada, y el otro segmento almacena principalmente información relacionada con el filtro de firewall. Junos OS proporciona la instrucción de memoria mejorada para reasignar la memoria jtree para rutas, filtros de firewall y VPN de capa 3.

8. Configure el tipo de recurso como páginas contiguas para las que desea habilitar el mecanismo de supervisión para proporcionar suficiente margen para garantizar un rendimiento eficaz del sistema y la capacidad de gestión del tráfico. Especifique el valor de umbral alto y bajo, superando el cual se generan advertencias o registros de errores, para el tipo o región de memoria especificados, que es una página contigua en este caso.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type contiguous-pages high-threshold percentage
user@host# set resource-type contiguous-pages low-threshold percentage
```

9. Configure el tipo de recurso como palabras dobles libres (dwords) para el que desea habilitar el mecanismo de supervisión para proporcionar suficiente margen para garantizar un rendimiento eficaz del sistema y la capacidad de gestión del tráfico. Especifique el valor de umbral alto y bajo,

superando el cual se generan advertencias o registros de errores, para el tipo o región de memoria especificados, que es dwords libre en este caso.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type free-dwords high-threshold percentage
user@host# set resource-type free-dwords low-threshold percentage
```

10. Configure el tipo de recurso como páginas de memoria libre para las que desea habilitar el mecanismo de supervisión para proporcionar suficiente margen para garantizar un rendimiento eficaz del sistema y la capacidad de gestión del tráfico. Especifique el valor de umbral alto y bajo, superando el cual se generan advertencias o registros de errores, para el tipo o región de memoria especificados, que son páginas de memoria libre en este caso.

```
[edit system services resource-monitor resource-category jtree]
user@host# set resource-type free-pages high-threshold percentage
user@host# set resource-type free-pages low-threshold percentage
```

11. Vea el uso de recursos de memoria en los motores de reenvío de paquetes de una FPC mediante el comando.`show system resource-monitor fpc` La memoria de filtro indica la memoria del contador de filtro utilizada para los contadores de filtro de firewall. El asterisco (*) que se muestra junto a cada una de las regiones de memoria indica aquellas para las que se está superando actualmente el umbral configurado.

```
user@host# run show system resource-monitor fpc
FPC Resource Usage Summary

Free Heap Mem Watermark         : 20  %
Free NH Mem Watermark           : 20  %
Free Filter Mem Watermark       : 20  %

* - Watermark reached

                    Heap                      ENCAP mem       NH mem          FW mem
   Slot #         % Free    PFE #           % Free       % Free          % Free
        0            94              0                    NA           83              99
```

Solucionar problemas de la discrepancia de los valores de jnxNatObjects para MS-DPC y MS-MIC

in this section

- Problema | 1510
- Resolución | 1510

Problema

Description

Cuando MS-DPC y MS-MIC se implementan en una red y el tipo de traducción de direcciones de red (NAT) está configurado como , el resultado del comando para jnxNatObjects muestra valores diferentes para MS-DPC y MS-MIC.`napt-44snmp mib walk`

Resolución

Configurar SNMP para que coincida con los valores de jnxNatObjects para MS-DPC y MS-MIC

Para configurar SNMP para que coincida con los valores de jnxNatObjects para MS-DPC y MS-MIC:

1. Ejecute el comando de modo de configuración.`set services service-set` *`service-set-name`* `nat-options snmp-value-match-msmic` En el ejemplo de configuración siguiente se muestra cómo configurar SNMP para que coincida con los valores de objetos específicos de MS-MIC de la tabla MIB jnxNatObjects con los valores de objetos de MS-DPC.

```
[edit]
user@host# set services service-set Mobile nat-options snmp-value-match-msmic
```

2. Emita el comando para confirmar los cambios.`commit`

```
[edit]
user@host# commit
commit complete
```

3. (Opcional) Ejecute el comando para comprobar que los valores de los objetos específicos de MS-MIC de la tabla MIB jnxNatObjects coinciden con los valores de los objetos de MS-DPC.`show snmp mib walk jnxNatObjects` Por ejemplo, el resultado siguiente muestra que los valores de los objetos específicos de MS-MIC y los objetos de MS-DPC coinciden.

```
[edit]
user@host# run show snmp mib walk jnxNatObjects
jnxNatSrcXlatedAddrType.6.77.111.98.105.108.101 = 1
jnxNatSrcPoolType.6.77.111.98.105.108.101 = 13
jnxNatSrcNumPortAvail.6.77.111.98.105.108.101 = 64512
jnxNatSrcNumPortInuse.6.77.111.98.105.108.101 = 0
jnxNatSrcNumAddressAvail.6.77.111.98.105.108.101 = 1
jnxNatSrcNumAddressInUse.6.77.111.98.105.108.101 = 0
jnxNatSrcNumSessions.6.77.111.98.105.108.101 = 0
jnxNatRuleType.9.77.111.98.105.108.101.58.116.49 = 13
jnxNatRuleTransHits.9.77.111.98.105.108.101.58.116.49 = 0
jnxNatPoolType.6.77.111.98.105.108.101 = 13
jnxNatPoolTransHits.6.77.111.98.105.108.101 = 0
```

NOTA: Puede utilizar el comando de modo de configuración para deshabilitar esta característica.`delete services service-set` *`service-set-name`* `nat-options snmp-value-match-msmic`

SEE ALSO

Configuración de reglas de servicio

snmp-value-match-msmic

Objetos administrados para la memoria Ukernel para un motor de reenvío de paquetes en una ranura FPC

El , cuyo identificador de objeto es , contiene el que recupera las estadísticas globales de ukernel o memoria de montón para la ranura del motor de reenvío de paquetes especificada.`jnxPfeMemoryUkernTable{jnxPfeMemory 1}JnxPfeMemoryUkernEntry` Cada , cuyo identificador de objeto es , contiene los objetos enumerados en la tabla siguiente.`JnxPfeMemoryUkernEntry{jnxPfeMemoryUkernTable 1}` El denota el uso de memoria, como la memoria total disponible y el porcentaje de memoria utilizada.`jnxPfeMemoryUkernEntry`

Tabla 159: jnxPfeMemoryUKernTable

Objeto	ID de objeto	Description
`jnxPfeMemoryUkernFreePercent`	`jnxPfeMemoryUkernEntry 3`	Denota el porcentaje de memoria libre del motor de reenvío de paquetes dentro del montón ucraniano.

Objetos administrados para datos estadísticos de memoria del motor de reenvío de paquetes

La tabla, cuyo identificador de objeto es , contiene los objetos enumerados en jnxPfeMemory`{jnxPfeMib 2}`Tabla 160 en la página 1512

Tabla 160: Tabla jnxPfeMemory

Objeto	ID de objeto	Description
`jnxPfeMemoryUkernTable`	`jnxPfeMemory 1`	Proporciona estadísticas globales de memoria ucraniana para la ranura del motor de reenvío de paquetes especificada.
`jnxPfeMemoryForwardingTable`	`jnxPfeMemory 2`	Proporciona estadísticas globales de utilización de memoria de próximo salto (para tarjetas de línea basadas en Trio) o Jtree (para tarjetas de línea basadas en I-chip) y estadísticas de utilización de memoria de filtro de firewall para la ranura del motor de reenvío de paquetes especificada.

Objetos administrados para el próximo salto, Jtree y memoria de filtro de firewall para un motor de reenvío de paquetes en una ranura FPC

El , cuyo identificador de objeto es , contiene que recupera la memoria del salto siguiente para las tarjetas de línea basadas en Trio, la memoria jtree para las tarjetas de línea basadas en I-chip y las estadísticas de memoria de firewall o filtro para la ranura del motor de reenvío de paquetes especificada para las tarjetas de línea basadas en I-chip y Trio.`jnxPfeMemoryForwardingTable{jnxPfeMemory 2}JnxPfeMemoryForwardingEntry` Cada , cuyo identificador de objeto es , contiene los objetos enumerados en la tabla siguiente.`jnxPfeMemoryForwardingEntry{jnxPfeMemoryForwardingTable 1}`

El representa la instancia ASIC, la memoria ASIC utilizada y la memoria libre ASIC. `jnxPfeMemoryForwardingEntry` La memoria jtree en todos los motores de reenvío de paquetes del enrutador de la serie MX tiene dos segmentos: Un segmento almacena principalmente tablas de enrutamiento e información relacionada, y el otro segmento almacena principalmente información relacionada con el filtro de firewall. Como la asignación de más memoria para tablas de enrutamiento o filtros de firewall puede interrumpir las operaciones de reenvío de un motor de reenvío de paquetes, la CLI de Junos OS muestra una advertencia para reiniciar todos los FPC afectados cuando confirme una configuración que incluya la instrucción route mejorada en memoria. La configuración no se hace efectiva hasta que reinicie el FPC o DPC (en enrutadores de la serie MX).

Tabla 161: jnxPfeMemoryForwardingTable

Objeto	ID de objeto	Description
`jnxPfeMemoryForwardingChipSlot`	`jnxPfeMemoryForwardingEntry 1`	Indica el número de instancia ASIC en el complejo Motor de reenvío de paquetes.
`jnxPfeMemoryType`	`jnxPfeMemoryForwardingEntry 2`	Indica el tipo de memoria del motor de reenvío de paquetes, donde nh = 1, fw = 2, encap = 3.
`jnxPfeMemoryForwardingPercentFree`	`jnxPfeMemoryForwardingEntry 3`	Indica el porcentaje de memoria libre para cada tipo de memoria.

jnxPfeMemoryErrorsTable

La MIB del motor de reenvío de paquetes específico para la empresa de Juniper Networks, cuyo identificador de objeto es , admite una nueva tabla MIB, , para mostrar los contadores de errores de

memoria del motor de reenvío de paquetes.{jnxPfeMibRoot 1}jnxPfeMemoryErrorsTable El , cuyo identificador de objeto es , contiene el .jnxPfeMemoryErrorsTablejnxPfeNotification 3JnxPfeMemoryErrorsEntry Cada , cuyo identificador de objeto es , contiene los objetos enumerados en la tabla siguiente.JnxPfeMemoryErrorsEntry{ jnxPfeMemoryErrorsTable 1 }

Tabla 162: jnxPfeMemoryErrorsTable

Objeto	ID de objeto	Description
jnxPfeFpcSlot	jnxPfeMemoryErrorsEntry 1	Significa el número de ranura FPC para este conjunto de notificaciones PFE
jnxPfeSlot	jnxPfeMemoryErrorsEntry 2	Indica el número de ranura PFE para este conjunto de errores.
jnxPfeParityErrors	jnxPfeMemoryErrorsEntry 3	Significa el recuento de errores de paridad
jnxPfeEccErrors	jnxPfeMemoryErrorsEntry 4	Significa el recuento de errores del código de comprobación de errores (ECC)

pfeMemoryErrors

El , cuyo identificador de objeto es , contiene el atributo.pfeMemoryErrorsNotificationPrefix{jnxPfeNotification 0}pfeMemoryErrors El objeto pfeMemoryErrors, cuyo identificador contiene los objetos y . {pfeMemoryErrorsNotificationPrefix 1}jnxPfeParityErrorsjnxPfeEccErrors

Tabla 163: pfeMemoryErrors

Objeto	ID de objeto	Description
pfeMemoryErrors	pfeMemoryErrorsNotificationPrefix 1	Se envía una notificación pfeMemoryErrors cuando aumenta el valor de jnxPfeParityErrors o jnxPfeEccErrors.

Configuración de las opciones de depuración y rastreo de rutas de datos

in this section

- Descripción de la depuración de rutas de datos para dispositivos de la serie SRX | 1515
- Captura de paquetes desde el modo operativo | 1516
- Descripción de la depuración de seguridad mediante opciones de seguimiento | 1517
- Descripción de la depuración de flujos mediante opciones de seguimiento | 1518
- Depurar la ruta de datos (procedimiento de la CLI) | 1518
- Configuración de opciones de seguimiento de depuración de flujo (procedimiento de CLI) | 1519
- Configuración de opciones de seguimiento de seguridad (procedimiento de CLI) | 1520
- Visualización de archivos de registro y seguimiento | 1522
- Mostrar resultados para las opciones de seguimiento de seguridad | 1523
- Visualización de operaciones de seguimiento de multidifusión | 1524
- Visualización de una lista de dispositivos | 1525
- Ejemplo: Configuración de la depuración de extremo a extremo en un dispositivo de la serie SRX | 1527

Descripción de la depuración de rutas de datos para dispositivos de la serie SRX

La depuración de rutas de datos, o depuración de extremo a extremo, proporciona rastreo y depuración en varias unidades de procesamiento a lo largo de la ruta de procesamiento de paquetes. El filtro de paquetes se puede ejecutar con un impacto mínimo en el sistema de producción.

Si su objetivo es recopilar capturas de paquetes, le recomendamos encarecidamente que aproveche la captura de paquetes en modo operativo introducida en Junos OS versión 19.3R1. Consulte "Captura de paquetes desde el modo operativo" en la página 1516.

En un firewall de la serie SRX, un paquete pasa por una serie de eventos que involucran diferentes componentes, desde el procesamiento de entrada hasta el de salida.

Con la característica de depuración de rutas de datos, puede rastrear y depurar (capturar paquetes) en diferentes puntos de datos a lo largo de la ruta de procesamiento. Los eventos disponibles en la ruta de

procesamiento de paquetes son: Entrada NP, subproceso de equilibrio de carga (LBT), jexec, subproceso de pedido de paquetes (POT) y salida NP. También puede habilitar el seguimiento de módulo de flujo si se establece el indicador de seguimiento de flujo de seguridad para un módulo determinado.

En cada evento, puede especificar cualquiera de las cuatro acciones (recuento, volcado de paquetes, resumen de paquetes y seguimiento). La depuración de rutas de datos proporciona filtros para definir qué paquetes capturar y solo se realiza un seguimiento de los paquetes coincidentes. El filtro de paquetes puede filtrar paquetes según la interfaz lógica, el protocolo, el prefijo de la dirección IP de origen, el puerto de origen, el prefijo de la dirección IP de destino y el puerto de destino.

La depuración de rutas de datos se admite en SRX4600, SRX5400, SRX5600 y SRX5800.

Para habilitar la depuración de extremo a extremo, debe realizar los pasos siguientes:

1. Defina el archivo de captura y especifique el tamaño máximo de captura.
2. Defina el filtro de paquetes para rastrear solo un determinado tipo de tráfico según el requisito.
3. Defina el perfil de acción especificando la ubicación en la ruta de procesamiento desde donde capturar los paquetes (por ejemplo, entrada LBT o NP).
4. Habilite la depuración de rutas de datos.
5. Capturar tráfico.
6. Deshabilite la depuración de rutas de datos.
7. Ver o analizar el informe.

El comportamiento de filtrado de paquetes para las opciones de puerto e interfaz es el siguiente:

- El filtro de paquetes rastrea el tráfico IPv4 e IPv6 si solo se especifica.**port**
- El filtro de paquetes rastrea el tráfico IPv4, IPV6 y no IP si solo se especifica.**interface**

Captura de paquetes desde el modo operativo

La depuración de rutas de datos o de extremo a extremo proporciona rastreo y depuración en varias unidades de procesamiento a lo largo de la ruta de procesamiento de paquetes. La captura de paquetes es una de las funciones de depuración de rutas de datos. Puede ejecutar la captura de paquetes desde el modo operativo con un impacto mínimo en el sistema de producción sin confirmar las configuraciones.

Puede capturar los paquetes mediante filtros para definir qué paquetes capturar. El filtro de paquetes puede filtrar paquetes según la interfaz lógica, el protocolo, el prefijo de la dirección IP de origen, el puerto de origen, el prefijo de la dirección IP de destino y el puerto de destino. Puede modificar el nombre de archivo, el tipo de archivo, el tamaño de archivo y el tamaño de captura de la salida de

captura de paquetes. También puede extender los filtros en dos filtros e intercambiar los valores de los filtros.

La captura de paquetes desde el modo operativo se admite en SRX4600, SRX5400, SRX5600 y SRX5800.

Para capturar paquetes desde el modo operativo, debe realizar los pasos siguientes:

1. Desde el modo operativo, defina el filtro de paquetes para rastrear el tipo de tráfico en función de sus requisitos mediante el comando de la CLI.`request packet-capture start` Consulte para conocer las opciones de filtro de captura de paquetes disponibles.*request packet-capture start*
2. Capture los paquetes necesarios.
3. Puede usar el comando de la CLI para detener la captura de paquetes o, después de recopilar el número solicitado de paquetes, la captura de paquetes se detiene automáticamente.`request packet-capture stop`
4. Vea o analice el informe de datos del paquete capturado.

Las limitaciones de capturar paquetes desde el modo operativo son:

1. La captura de paquetes en modo de configuración y la captura de paquetes en modo operativo no pueden coexistir.
2. La captura de paquetes en modo operativo es una operación única y el sistema no almacena el historial de este comando.
3. Debe utilizar la captura de paquetes en modo operativo con una tasa baja de flujo de tráfico.

SEE ALSO

> *request packet-capture start*
>
> *request packet-capture stop*

Descripción de la depuración de seguridad mediante opciones de seguimiento

La función de seguimiento de Junos OS permite a las aplicaciones escribir información de depuración de seguridad en un archivo. La información que aparece en este archivo se basa en los criterios establecidos. Puede utilizar esta información para analizar problemas de aplicaciones de seguridad.

La función trace funciona de forma distribuida, con cada subproceso escribiendo en su propio búfer de seguimiento. Estos búferes de rastreo se recopilan en un punto, se ordenan y se escriben en archivos de

seguimiento. Los mensajes de rastreo se entregan mediante el protocolo de comunicaciones entre procesos (IPC). Un mensaje de seguimiento tiene una prioridad menor que la de los paquetes de protocolo de control, como BGP, OSPF e IKE, por lo que la entrega no se considera tan confiable.

Descripción de la depuración de flujos mediante opciones de seguimiento

Para las opciones de seguimiento de flujo, puede definir un filtro de paquetes mediante combinaciones de , , , , , y .**destination-portdestination-prefixinterfaceprotocolsource-portsource-prefix** Si se establece el indicador de seguimiento de flujo de seguridad para un módulo determinado, el paquete que coincide con el filtro de paquetes específico desencadena el seguimiento de flujo y escribe información de depuración en el archivo de seguimiento.

Depurar la ruta de datos (procedimiento de la CLI)

La depuración de rutas de datos se admite en SRX5400, SRX5600 y SRX5800.

Para configurar el dispositivo para la depuración de rutas de datos:

1. Especifique el siguiente comando de solicitud para establecer la depuración de la ruta de acceso de datos para las varias unidades de procesamiento a lo largo de la ruta de procesamiento de paquetes:

```
[edit]
user@host# set security datapath-debug
```

2. Especifique las opciones de seguimiento para la depuración de rutas de datos mediante el siguiente comando:

```
[edit]
user@host# set security datapath-debug traceoptions
```

3. Con el comando request security packet-filter, puede establecer el filtro de paquetes para especificar los paquetes relacionados para realizar la acción de depuración de ruta de datos. Se admiten un máximo de cuatro filtros al mismo tiempo. Por ejemplo, el siguiente comando establece el primer filtro de paquetes:

```
[edit]
user@host# set security datapath-debug packet-filter name
```

4. Con el comando request security action-profile, puede establecer la acción para la coincidencia de paquetes para un filtro especificado. Solo se admite el perfil de acción predeterminado, que es la opción de seguimiento para la entrada ezchip del procesador de red, la salida ezchip, spu.lbt y spu.pot:

```
[edit]
user@host# set security datapath-debug packet-filter name action-profile
```

Configuración de opciones de seguimiento de depuración de flujo (procedimiento de CLI)

En los ejemplos siguientes se muestran las opciones que puede definir mediante `.security flow traceoptions`

- Para hacer coincidir el puerto de destino imap para el filtro de paquetes filter1, utilice la instrucción siguiente:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 destination-port imap
```

- Para establecer la dirección del prefijo IPv4 de destino 1.2.3.4 para el filtro de paquetes filter1, utilice la instrucción siguiente:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 destination-prefix 1.2.3.4
```

- Para establecer la interfaz lógica fxp0 para el filtro de paquetes filter1, utilice la instrucción siguiente:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 interface fxp0
```

- Para que coincida con el protocolo IP TCP para el filtro de paquetes filter1, utilice la instrucción siguiente:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 protocol tcp
```

- Para hacer coincidir el puerto de origen HTTP para el filtro de paquetes filter1, utilice la instrucción siguiente:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 source-port http
```

- Para establecer la dirección del prefijo IPv4 5.6.7.8 para el filtro de paquetes filter1, utilice la instrucción siguiente:

```
[edit]
user@host# set security flow traceoptions packet-filter filter1 source-prefix 5.6.7.8
```

Configuración de opciones de seguimiento de seguridad (procedimiento de CLI)

Utilice las siguientes instrucciones de configuración para configurar las opciones de seguimiento de seguridad en el editor de configuración de la CLI.

- Para deshabilitar el seguimiento remoto, escriba la instrucción siguiente:

```
[edit]
user@host# set security traceoptions no-remote-trace
```

- Para escribir mensajes de seguimiento en un archivo local, escriba la instrucción siguiente. El sistema guarda el archivo de seguimiento en eldirectorio. **/var/log/**

```
[edit]
user@host# set security traceoptions use-local-files
```

- Para especificar un nombre para el archivo de seguimiento, escriba la instrucción siguiente. Los valores válidos oscilan entre 1 y 1024 caracteres. El nombre no puede incluir espacios, /, ni % de caracteres. El nombre de archivo predeterminado es seguridad.

```
[edit]
user@host# set security traceoptions file filename
```

- Para especificar el número máximo de archivos de seguimiento que se pueden acumular, escriba la instrucción siguiente. Los valores válidos oscilan entre 2 y 1000. El valor predeterminado es 3.

```
[edit]
user@host# set security traceoptions file files 3
```

- Para especificar los criterios de coincidencia que desea que utilice el sistema al registrar información en el archivo, escriba la instrucción siguiente. Escriba una expresión regular. Se aceptan caracteres comodín (*).

```
[edit]
user@host# set security traceoptions file match *thread
```

- Para permitir que cualquier usuario lea el archivo de seguimiento, escriba la instrucción. `world-readable` De lo contrario, escriba la instrucción.`no-world-readable`

```
[edit]
user@host# set security traceoptions file world-readable
user@host# set security traceoptions file no-world-readable
```

- Para especificar el tamaño máximo al que puede crecer el archivo de seguimiento, escriba la instrucción siguiente. Una vez que el archivo alcanza el tamaño especificado, se comprime y se le cambia el nombre a 0.gz, el siguiente archivo se denomina 1.gz y así sucesivamente.*filenamefilename* Los valores válidos oscilan entre 10240 y 1.073.741.824.

```
[edit]
user@host# set security traceoptions file size 10240
```

- Para activar las opciones de seguimiento y realizar más de una operación de seguimiento, establezca los siguientes indicadores.

```
[edit]
user@host# set security traceoptions flag all
user@host# set security traceoptions flag compilation
user@host#  set security traceoptions flag configuration
user@host# set security traceoptions flag routing-socket
```

- Para especificar los grupos a los que se aplican o no estas opciones de seguimiento, escriba las instrucciones siguientes:

```
[edit]
user@host# set security traceoptions apply-groups value
user@host# set security traceoptions apply-groups-except value
```

Visualización de archivos de registro y seguimiento

Ingrese el comando para mostrar adiciones en tiempo real a los registros del sistema y archivos de seguimiento:`monitor start`

```
user@host> monitor start filename
```

Cuando el dispositivo agrega un registro al archivo especificado por , el registro se muestra en la pantalla.*filename* Por ejemplo, si ha configurado un archivo de registro del sistema denominado (incluyendo la instrucción en el nivel de jerarquía []), puede escribir el comando para mostrar los registros agregados al registro del sistema.`system-logsyslogedit systemmonitor start system-log`

Para mostrar una lista de los archivos que se están supervisando, escriba el comando.`monitor list` Para detener la visualización de los registros de un archivo especificado, escriba el comando.`monitor stop` *filename*

Mostrar resultados para las opciones de seguimiento de seguridad

in this section

- Propósito | 1523
- Acción | 1523

Propósito

Muestra la salida para las opciones de seguimiento de seguridad.

Acción

Utilice el comando para mostrar el resultado de los archivos de seguimiento.`show security traceoptions` Por ejemplo:

```
[edit]
user@host # show security traceoptions file usp_trace
user@host # show security traceoptions flag all
user@host # show security traceoptions rate-limit 888
```

El resultado de este ejemplo es el siguiente:

```
Apr 11 16:06:42 21:13:15.750395:CID-906489336:FPC-01:PIC-01:THREAD_ID-01:PFE:now update
0x3607edf8df8in 0x3607e8d0
Apr 11 16:06:42 21:13:15.874058:CID-1529687608:FPC-01:PIC-01:THREAD_ID-01:CTRL:Enter
Function[util_ssam_handler]
Apr 11 16:06:42 21:13:15.874485:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default1: Rate limit
changed to 888
Apr 11 16:06:42 21:13:15.874538:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default1: Destination ID
set to 1
Apr 11 16:06:42 21:13:15.874651:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default2: Rate limit
changed to 888
Apr 11 16:06:42 21:13:15.874832:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default2: Destination ID
set to 1
Apr 11 16:06:42 21:13:15.874942:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default3: Rate limit
changed to 888
```

```
Apr 11 16:06:42 21:13:15.874997:CID-00:FPC-01:PIC-01:THREAD_ID-01:CTRL:default3: Destination ID
set to 1
```

Visualización de operaciones de seguimiento de multidifusión

Para supervisar y mostrar las operaciones de seguimiento de multidifusión, escriba el comando:`mtrace monitor`

```
user@host> mtrace monitor
```

```
Mtrace query at Apr 21 16:00:54 by 192.1.30.2, resp to 224.0.1.32, qid 2a83aa packet from
192.1.30.2 to 224.0.0.2 from 192.1.30.2 to 192.1.4.1 via group 224.1.1.1 (mxhop=60)  Mtrace
query at Apr 21 16:00:57 by 192.1.30.2, resp to 224.0.1.32, qid 25dc17 packet from 192.1.30.2 to
224.0.0.2 from 192.1.30.2 to 192.1.4.1 via group 224.1.1.1 (mxhop=60)  Mtrace query at Apr 21
16:01:00 by 192.1.30.2, resp to same, qid 20e046 packet from 192.1.30.2 to 224.0.0.2 from
192.1.30.2 to 192.1.4.1 via group 224.1.1.1 (mxhop=60)  Mtrace query at Apr 21 16:01:10 by
192.1.30.2, resp to same, qid 1d25ad packet from 192.1.30.2 to 224.0.0.2 from 192.1.30.2 to
192.1.4.1 via group 224.1.1.1 (mxhop=60)
```

En este ejemplo solo se muestran las consultas.`mtrace` Sin embargo, cuando el dispositivo captura una respuesta, la pantalla es similar, pero también aparece la respuesta completa (exactamente como aparece en la salida del comando).`mtracemtracemtrace from-source`

Tabla 164 en la página 1524 Resume los campos de salida de la pantalla.

Tabla 164: Resumen de salida del comando CLI mtrace monitor

Campo	Description
Mtrace *operation-type* at *time-of-day*	• *operation-type*—Tipo de operación de rastreo de multidifusión: `query` o `response`. • *time-of-day*: fecha y hora en que se capturó la consulta o respuesta de seguimiento de multidifusión.
by	Dirección IP del host que emite la consulta.

Tabla 164: Resumen de salida del comando CLI mtrace monitor *(Continued)*

Campo	Description
`resp to address`	*address*—Dirección de destino de la respuesta.
`qid qid`	*qid*: número de ID de consulta.
`packet from source to destination`	• *source*: dirección IP del origen de la consulta o respuesta. • *destination*—Dirección IP del destino de la consulta o respuesta.
`from source to destination`	• *source*—Dirección IP del origen de multidifusión. • *destination*: dirección IP del destino de la multidifusión.
`via group address`	*address*: dirección del grupo que se está rastreando.
`mxhop=number`	*number*—Ajuste del salto máximo.

Visualización de una lista de dispositivos

Para mostrar una lista de dispositivos entre el dispositivo y un host de destino especificado, escriba el comando con la siguiente sintaxis:`traceroute`

```
user@host> traceroute host <interface interface-name> <as-number-lookup> <bypass-routing>
<gateway address> <inet | inet6> <no-resolve> <routing-instance routing-instance-name>
<source source-address> <tos number> <ttl number> <wait seconds>
```

Tabla 165 Describe las opciones de comando.traceroute

Tabla 165: Opciones de comando de traceroute de CLI

La opción	Description
host	Envía paquetes de traceroute al nombre de host o a la dirección IP que especifique.
`interface` *interface-name*	(Opcional) Envía los paquetes traceroute a la interfaz que especifique. Si no incluye esta opción, los paquetes traceroute se envían en todas las interfaces.
`as-number-lookup`	(Opcional) Muestra el número de sistema autónomo (AS) de cada salto intermedio entre el dispositivo y el host de destino.
`bypass-routing`	(Opcional) Omite las tablas de enrutamiento y envía los paquetes traceroute solo a hosts en interfaces conectadas directamente. Si el host no está en una interfaz conectada directamente, se devuelve un mensaje de error. Utilice esta opción para mostrar una ruta a un sistema local a través de una interfaz que no tiene ninguna ruta a través de ella.
`gateway` *address*	(Opcional) Utiliza la puerta de enlace que especifique para enrutar.
`inet`	(Opcional) Fuerza los paquetes traceroute a un destino IPv4.
`inet6`	(Opcional) Fuerza los paquetes traceroute a un destino IPv6.
`no-resolve`	(Opcional) Suprime la visualización de los nombres de host de los saltos a lo largo de la ruta de acceso.
`routing-instance` *routing-instance-name*	(Opcional) Utiliza la instancia de enrutamiento especificada para traceroute.
`source` *address*	(Opcional) Utiliza la dirección de origen que especifique en el paquete traceroute.
`tos` *number*	(Opcional) Establece el valor del tipo de servicio (TOS) en el encabezado IP del paquete traceroute. Especifique un valor de a `.0255`

Tabla 165: Opciones de comando de traceroute de CLI *(Continued)*

La opción	Description
`ttl` *`number`*	(Opcional) Establece el valor de tiempo de vida (TTL) para el paquete traceroute. Especifique un recuento de saltos desde `.0128`
`wait` *`seconds`*	(Opcional) Establece el tiempo máximo de espera de una respuesta.

Para salir del comando, presione Ctrl-C.`traceroute`

A continuación se muestra un ejemplo de salida de un comando:`traceroute`

```
user@host> traceroute host2
```

```
traceroute to 173.24.232.66 (172.24.230.41), 30 hops max, 40 byte packets  1  173.18.42.253
(173.18.42.253)  0.482 ms  0.346 ms  0.318 ms  2  host4.site1.net (173.18.253.5)  0.401 ms
0.435 ms  0.359 ms  3  host5.site1.net (173.18.253.5)  0.401 ms  0.360 ms  0.357 ms  4
173.24.232.65 (173.24.232.65)  0.420 ms  0.456 ms  0.378 ms  5  173.24.232.66 (173.24.232.66)
0.830 ms  0.779 ms  0.834 ms
```

Los campos de la pantalla son los mismos que los que muestra la herramienta de diagnóstico J-Web traceroute.

Ejemplo: Configuración de la depuración de extremo a extremo en un dispositivo de la serie SRX

in this section

- Requisitos | **1528**
- Descripción general | **1528**
- Configuración | **1529**
- Habilitar la depuración de rutas de datos | **1531**
- Verificación | **1532**

En este ejemplo se muestra cómo configurar y habilitar la depuración de extremo a extremo en un firewall de la serie SRX con un SRX5K-MPC.

Requisitos

En este ejemplo, se utilizan los siguientes componentes de hardware y software:

- SRX5600 dispositivo con un SRX5K-MPC instalado con transceptor CFP de Ethernet de 100 Gigabit
- Junos OS versión 12.1X47-D15 o posterior para firewalls serie SRX

Antes de empezar:

- Consulte "Descripción de la depuración de rutas de datos para dispositivos" en la página 1515 de la serie SRX.

No se necesita ninguna configuración especial más allá de la inicialización del dispositivo antes de configurar esta función.

Descripción general

La depuración de rutas de datos mejora las capacidades de solución de problemas al proporcionar rastreo y depuración en varias unidades de procesamiento a lo largo de la ruta de procesamiento de paquetes. Con la característica de depuración de rutas de datos, puede rastrear y depurar (capturar paquetes) en diferentes puntos de datos a lo largo de la ruta de procesamiento. En cada evento, puede especificar una acción (recuento, volcado de paquetes, resumen de paquetes y seguimiento) y puede establecer filtros para definir qué paquetes capturar.

En este ejemplo, se define un filtro de tráfico y, a continuación, se aplica un perfil de acción. El perfil de acciones especifica una variedad de acciones en la unidad de procesamiento. La entrada y la salida se especifican como ubicaciones en la ruta de procesamiento para capturar los datos del tráfico entrante y saliente.

A continuación, habilite la depuración de rutas de datos en modo operativo y, por último, vea el informe de captura de datos.

> **NOTA**: La depuración de rutas de datos se admite en SRX1400, SRX3400, SRX3600, SRX5400, SRX5600 y SRX5800.

Configuración

in this section

- Procedimiento | 1529

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
set security datapath-debug traceoptions file e2e.trace size 10m
set security datapath-debug capture-file e2e.pcap format pcap
set security datapath-debug maximum-capture-size 1500
set security datapath-debug capture-file files 10
set security datapath-debug action-profile profile-1 preserve-trace-order
set security datapath-debug action-profile profile-1 record-pic-history
set security datapath-debug action-profile profile-1 event np-ingress trace
set security datapath-debug action-profile profile-1 event np-ingress count
set security datapath-debug action-profile profile-1 event np-ingress packet-summary
set security datapath-debug action-profile profile-1 event np-egress trace
set security datapath-debug action-profile profile-1 event np-egress count
set security datapath-debug action-profile profile-1 event np-egress packet-summary
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar la depuración de rutas de datos:

1. Edite la opción de depuración de rutas de datos de seguridad para las varias unidades de procesamiento a lo largo de la ruta de procesamiento de paquetes:

```
[edit]
user@host# edit security datapath-debug
```

2. Habilite el archivo de captura, el formato de archivo, el tamaño del archivo y el número de archivos.

```
[edit security datapath-debug]
user@host# set traceoptions file e2e.trace size 10m
user@host# set capture-file e2e.pcap format pcap;
user@host# set maximum-capture-size 1500
user@host# set capture-file files 10
```

3. Configure el perfil de acción, el tipo de evento y las acciones para el perfil de acción.

```
[edit security datapath-debug]
user@host# set action-profile profile-1 preserve-trace-order
user@host# set action-profile profile-1 record-pic-history
user@host# set action-profile profile-1 event np-ingress trace
user@host# set action-profile profile-1 event np-ingress count
user@host# set action-profile profile-1 event np-ingress packet-summary
user@host# set action-profile profile-1 event np-egress trace
user@host# set action-profile profile-1 event np-egress count
user@host# set action-profile profile-1 event np-egress packet-summary
```

Resultados

Desde el modo de configuración, confírmela con el comando `show security datapath-debug`. Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

```
traceoptions {
    file e2e.trace size 10m;
}
capture-file e2e.pcap format pcap;
maximum-capture-size 1500;
capture-file files 10;
action-profile {
```

```
    profile-1 {
        preserve-trace-order;
        record-pic-history;
        event np-ingress {
            trace;
            packet-summary;
            packet-dump;
        }
        event np-egress {
            trace;
            packet-summary;
            packet-dump;
        }
    }
}
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Habilitar la depuración de rutas de datos

in this section

- Procedimiento | **1531**

Procedimiento

Procedimiento paso a paso

Después de configurar la depuración de rutas de datos, debe iniciar el proceso en el dispositivo desde el modo operativo.

1. Habilite la depuración de rutas de datos.

```
user@host> request security datapath-debug capture start
```

```
datapath-debug capture started on file datapcap
```

2. Antes de comprobar la configuración y ver los informes, debe deshabilitar la depuración de rutas de datos.

```
user@host> request security datapath-debug capture stop
```

```
datapath-debug capture succesfully stopped, use show security datapath-debug capture to view
```

> **NOTA**: Debe detener el proceso de depuración una vez que haya terminado de capturar los datos. Si intenta abrir los archivos capturados sin detener el proceso de depuración, los archivos obtenidos no se pueden abrir a través de ningún software de terceros (por ejemplo, tcpdump y wireshark).

Verificación

in this section

- Comprobación de los detalles de la captura de paquetes de depuración de rutas de datos | **1532**

Confirme que la configuración funcione correctamente.

Comprobación de los detalles de la captura de paquetes de depuración de rutas de datos

Propósito

Verifique los datos capturados habilitando la configuración de depuración de rutas de datos.

Acción

Desde el modo operativo, ingrese el comando `show security datapath-debug capture`.

```
Packet 8, len 152: (C2/F2/P0/SEQ:57935:np-ingress)
00 10 db ff 10 02 00 30 48 83 8d 4f 08 00 45 00
00 54 00 00 40 00 40 01 9f c7 c8 07 05 69 c8 08
05 69 08 00 91 1f 8f 03 2a a2 ae 66 85 53 8c 7d
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37
Packet 9, len 152: (C2/F2/P0/SEQ:57935:np-egress)
00 30 48 8d 1a bf 00 10 db ff 10 03 08 00 45 00
00 54 00 00 40 00 3f 01 a0 c7 c8 07 05 69 c8 08
05 69 08 00 91 1f 8f 03 2a a2 ae 66 85 53 8c 7d
02 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15
16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
36 37....
```

Para abreviar, la salida del comando se trunca para mostrar solo unos pocos ejemplos.`show` Las muestras adicionales han sido reemplazadas por puntos suspensivos (...).

Para ver los resultados, desde el modo operativo de la CLI, acceda al shell de UNIX local y navegue hasta el directorio **./var/log/<*file-name*>** El resultado se puede leer mediante la utilidad.`tcpdump`

```
user@host>start shell
%tcpdump -nr/var/log/e2e.pcap
```

```
21:50:04.288767 C0/F3 event:1(np-ingress) SEQ:1 IP 192.168.14.2 > 192.168.13.2: ICMP echo
request, id 57627, seq 0, length 64
21:50:04.292590 C0/F3 event:2(np-egress) SEQ:1 IP 192.168.14.2 > 192.168.13.2: ICMP echo
request, id 57627, seq 0, length 64
1:50:04.295164 C0/F3 event:1(np-ingress) SEQ:2 IP 192.168.13.2 > 192.168.14.2: ICMP echo reply,
id 57627, seq 0, length 64
21:50:04.295284 C0/F3 event:2(np-egress) SEQ:2 IP 192.168.13.2 > 192.168.14.2: ICMP echo reply,
id 57627, seq 0, length 64
```

NOTA: Si ha terminado de solucionar problemas de la depuración de rutas de datos, elimine todas (sin limitarse a las opciones de seguimiento de flujo) y la configuración completa de depuración de rutas de datos, incluida la configuración de depuración de rutas de datos para la captura de paquetes (volcado de paquetes), que debe iniciarse o detenerse manualmente.`traceoptions` Si alguna parte de la configuración de depuración permanece activa, seguirá utilizando los recursos del dispositivo (CPU/memoria).

Uso de MPLS para diagnosticar LSP, VPN y circuitos de capa 2

in this section

- Descripción general de la comprobación de conexión MPLS | **1534**

Descripción general de la comprobación de conexión MPLS

in this section

- MPLS habilitado | **1537**
- Dirección de circuito cerrado | **1537**
- Dirección de origen para sondeos | **1538**
- Uso del comando ping | **1538**

Utilice la herramienta de diagnóstico MPLS de ping J-Web o los comandos de CLI , , y para diagnosticar el estado de las rutas conmutadas por etiquetas (LSP), las redes privadas virtuales (VPN) de capa 2 y capa 3, y los circuitos de capa 2.`ping mplsping mpls l2circuitping mpls l2vpnping mpls l3vpn`

En función de cómo responde a los sondeos el nodo de salida de LSP o VPN del extremo remoto de la conexión, puede determinar la conectividad del LSP o VPN.

Cada sonda es una solicitud de eco enviada al punto de salida de LSP o VPN como un paquete MPLS con una carga UDP. Si el nodo saliente recibe la solicitud de eco, comprueba el contenido de la sonda y devuelve un valor en la carga UDP del paquete de respuesta. Si el dispositivo recibe el paquete de respuesta, notifica una respuesta de ping correcta.

Las respuestas que tardan más de 2 segundos se identifican como sondeos fallidos.

resume las opciones para usar la herramienta de diagnóstico MPLS ping J-Web o el comando CLI para mostrar información sobre las conexiones MPLS en VPN y LSP.Tabla 166 en la página 1535`ping mpls`

Tabla 166: Opciones para comprobar conexiones MPLS

Herramienta MPLS J-Web Ping	comando ping mpls	Propósito	Información adicional
Ping RSVP-signaled LSP	`ping mpls rsvp`	Comprueba la operatividad de un LSP configurado por el Protocolo de reserva de recursos (RSVP). El dispositivo hace ping a un LSP determinado utilizando el nombre de LSP configurado.	Cuando un LSP con señal RSVP tiene varias rutas, el dispositivo envía las solicitudes de ping a la ruta que está activa actualmente.
Ping LDP-signaled LSP	`ping mpls ldp`	Comprueba la operatividad de un LSP configurado por el protocolo de distribución de etiquetas (LDP). El dispositivo hace ping a un LSP determinado utilizando el prefijo y la longitud de la clase de equivalencia de reenvío (FEC).	Cuando un LSP con señal LDP tiene varias puertas de enlace, el dispositivo envía las solicitudes de ping a través de la primera puerta de enlace. Las solicitudes de ping enviadas a los LSP señalados por LDP solo usan la instancia de enrutamiento maestra.

Tabla 166: Opciones para comprobar conexiones MPLS *(Continued)*

Herramienta MPLS J-Web Ping	comando ping mpls	Propósito	Información adicional
Ping LSP to Layer 3 VPN prefix	`ping mpls l3vpn`	Comprueba el funcionamiento de las conexiones relacionadas con una VPN de capa 3. El dispositivo prueba si hay un prefijo presente en la tabla de enrutamiento y reenvío VPN (VRF) de un dispositivo perimetral de proveedor (PE) mediante un prefijo de destino VPN de capa 3.	El dispositivo no prueba la conexión entre un dispositivo PE y un enrutador perimetral del cliente (CE).
Locate LSP using interface name	`ping mpls l2vpn interface`	Comprueba la operatividad de las conexiones relacionadas con una VPN de capa 2. El dispositivo dirige la solicitud saliente y sondea la interfaz especificada.	–
Instance to which this connection belongs	`ping mpls l2vpn instance`	Comprueba la operatividad de las conexiones relacionadas con una VPN de capa 2. El dispositivo hace ping en una combinación del nombre de instancia de enrutamiento VPN de capa 2, el identificador de sitio local y el identificador de sitio remoto, para probar la integridad del circuito VPN de capa 2 (especificado por los identificadores) entre los enrutadores de PE entrantes y salientes.	–
Locate LSP from interface name	`ping mpls l2circuit interface`	Comprueba la operatividad de las conexiones de circuito de capa 2. El dispositivo dirige la solicitud saliente y sondea la interfaz especificada.	–

Tabla 166: Opciones para comprobar conexiones MPLS *(Continued)*

Herramienta MPLS J-Web Ping	comando ping mpls	Propósito	Información adicional
Locate LSP from virtual circuit information	`ping mpls l2circuit virtual-circuit`	Comprueba la operatividad de las conexiones de circuito de capa 2. El dispositivo hace ping en una combinación del prefijo IPv4 y el identificador de circuito virtual en el enrutador de PE saliente, probando la integridad del circuito de capa 2 entre los enrutadores de PE entrantes y salientes.	–
Ping end point of LSP	`ping mpls lsp-end-point`	Comprueba la operatividad de un extremo de LSP. El dispositivo hace ping a un extremo LSP mediante un prefijo FEC LDP o una dirección de extremo LSP RSVP.	–

Antes de utilizar la función ping MPLS, asegúrese de que la interfaz receptora del extremo remoto VPN o LSP tenga habilitada MPLS y de que la interfaz de circuito cerrado del nodo saliente esté configurada como `.127.0.0.1` La dirección de origen de las sondas MPLS debe ser una dirección válida en el dispositivo de la serie J.

Esta sección incluye los siguientes temas:

MPLS habilitado

Para procesar las solicitudes MPLS de ping, el extremo remoto de la VPN o LSP debe configurarse adecuadamente. Debe habilitar MPLS en la interfaz de recepción del nodo saliente para la VPN o el LSP. Si MPLS no está habilitado, el extremo remoto descarta los paquetes de solicitud entrantes y devuelve un mensaje de "host ICMP inalcanzable" al dispositivo de la serie J.

Dirección de circuito cerrado

La dirección de bucle invertido () en el nodo de salida debe configurarse como `.lo0127.0.0.1` Si esta dirección de interfaz no está configurada correctamente, el nodo saliente no tiene esta entrada de reenvío. Descarta los paquetes de solicitud entrantes y devuelve un mensaje de "host inalcanzable" al dispositivo de la serie J.

Dirección de origen para sondeos

La dirección IP de origen que especifique para un conjunto de sondeos debe ser una dirección configurada en una de las interfaces de dispositivo de la serie J. Si no es una dirección de dispositivo válida de la serie J, la solicitud de ping falla con el mensaje de error "No se puede asignar la dirección solicitada".

Uso del comando ping

Solo puede realizar determinadas tareas a través de la CLI. Utilice el comando de la CLI para comprobar que se puede acceder a un host a través de la red.`ping` Este comando es útil para diagnosticar problemas de conectividad de host y red. El dispositivo envía una serie de solicitudes de eco (ping) ICMP a un host especificado y recibe respuestas de eco ICMP.

SEE ALSO

- Señal
- ping mpls ldp
- ping mpls lsp-end-point
- ping mpls L2circuit
- ping mpls L2VPN
- ping mpls L3VPN
- ping mpls rsvp

Uso de la captura de paquetes para analizar el tráfico de red

in this section

- Descripción general de la captura de paquetes | **1539**
- Ejemplo: Habilitar la captura de paquetes en un dispositivo | **1542**
- Ejemplo: Configurar la captura de paquetes en una interfaz | **1547**
- Ejemplo: Configurar un filtro de firewall para la captura de paquetes | **1550**

- Ejemplo: Configurar la captura de paquetes para la depuración de rutas de datos | 1553
- Deshabilitar la captura de paquetes | 1558
- Modificar la encapsulación en interfaces con la captura de paquetes configurada | 1558
- Eliminar archivos de captura de paquetes | 1560
- Mostrar encabezados de paquetes | 1561

Descripción general de la captura de paquetes

in this section

- Captura de paquetes en interfaces de dispositivos | 1540
- Filtros de firewall para la captura de paquetes | 1541
- Archivos de captura de paquetes | 1541
- Análisis de archivos de captura de paquetes | 1542

La captura de paquetes es una herramienta que le ayuda a analizar el tráfico de red y solucionar problemas de red. La herramienta de captura de paquetes captura paquetes de datos en tiempo real que viajan a través de la red para monitoreo y registro.

NOTA: La captura de paquetes se admite en interfaces físicas, interfaces reth e interfaces de túnel, como gr, ip, st0 y lsq-/ls.

Los paquetes se capturan como datos binarios, sin modificaciones. Puede leer la información del paquete sin conexión con un analizador de paquetes como Wireshark o tcpdump. Si necesita capturar rápidamente paquetes destinados o que se originan en el motor de enrutamiento y analizarlos en línea, puede usar la herramienta de diagnóstico de captura de paquetes J-Web.

NOTA: La herramienta de captura de paquetes no admite la captura de paquetes IPv6.

Puede utilizar el editor de configuración de J-Web o el editor de configuración de CLI para configurar la captura de paquetes.

Los administradores de red y los ingenieros de seguridad utilizan la captura de paquetes para realizar las siguientes tareas:

- Supervise el tráfico de red y analice los patrones de tráfico.
- Identificar y solucionar problemas de red.
- Detecte brechas de seguridad en la red, como intrusiones no autorizadas, actividad de spyware o análisis de ping.

La captura de paquetes funciona como un muestreo de tráfico en el dispositivo, excepto que captura paquetes enteros, incluido el encabezado de capa 2, y guarda el contenido en un archivo en formato libpcap. La captura de paquetes también captura fragmentos IP.

No puede habilitar la captura de paquetes y el muestreo de tráfico en el dispositivo al mismo tiempo. A diferencia del muestreo de tráfico, no hay operaciones de rastreo para la captura de paquetes.

NOTA: Puede habilitar la captura de paquetes y *la duplicación de puertos* simultáneamente en un dispositivo.

Esta sección contiene los siguientes temas:

Captura de paquetes en interfaces de dispositivos

La captura de paquetes es compatible con las interfaces T1, T3, E1, E3, serie, Gigabit Ethernet, ADSL, G.SHDSL, PPPoE y RDSI.

Para capturar paquetes en una interfaz RDSI, configure la captura de paquetes en la interfaz del marcador. Para capturar paquetes en una interfaz PPPoE, configure la captura de paquetes en la interfaz lógica PPPoE.

La captura de paquetes admite PPP, Cisco HDLC, Frame Relay y otras encapsulaciones ATM. La captura de paquetes también admite las encapsulaciones PPP multivínculo (MLPPP), Multilink Frame Relay de extremo a extremo (MLFR) y Multilink Frame Relay UNI/NNI (MFR).

Puede capturar todos los paquetes IPv4 que fluyen en una interfaz en la dirección de entrada o salida. Sin embargo, en el tráfico que omite el módulo de software de flujo (paquetes de protocolo como ARP, OSPF y PIM), los paquetes generados por el motor de enrutamiento no se capturan a menos que haya configurado y aplicado un filtro de firewall en la interfaz en la dirección de salida.

Las interfaces de túnel solo admiten la captura de paquetes en la dirección de salida.

Utilice el editor de configuración de J-Web o el editor de configuración de CLI para especificar el tamaño máximo del paquete, el nombre de archivo que se utilizará para almacenar los paquetes capturados, el tamaño máximo de archivo, el número máximo de archivos de captura de paquetes y los permisos de archivo.

> **NOTA**: Para los paquetes capturados en interfaces T1, T3, E1, E3, serie e ISDN en la dirección de salida (salida), el tamaño del paquete capturado puede ser 1 byte menor que el tamaño máximo de paquete configurado debido al bit de prioridad de pérdida de paquetes (PLP).

Para modificar la encapsulación en una interfaz con la captura de paquetes configurada, debe deshabilitar la captura de paquetes.

Filtros de firewall para la captura de paquetes

Cuando se habilita la captura de paquetes en un dispositivo, se capturan y almacenan todos los paquetes que fluyen en la dirección especificada en la configuración de captura de paquetes (entrante, saliente o ambos). La configuración de una interfaz para capturar todos los paquetes puede degradar el rendimiento del dispositivo. Puede controlar el número de paquetes capturados en una interfaz con filtros de firewall y especificar varios criterios para capturar paquetes para flujos de tráfico específicos.

También debe configurar y aplicar los filtros de firewall adecuados en la interfaz si necesita capturar paquetes generados por el dispositivo host, ya que el muestreo de interfaz no captura paquetes que se originan en el dispositivo host.

Archivos de captura de paquetes

Cuando la captura de paquetes está habilitada en una interfaz, todo el paquete, incluido el encabezado de capa 2, se captura y almacena en un archivo. Puede especificar el tamaño máximo del paquete a capturar, hasta 1500 bytes. La captura de paquetes crea un archivo para cada interfaz física.

La creación y el almacenamiento de archivos se llevan a cabo de la siguiente manera. Supongamos que asigna al archivo de captura de paquetes el nombre .**pcap-file** La captura de paquetes crea múltiples archivos (uno por interfaz física), sufijando cada archivo con el nombre de la interfaz física; por ejemplo, para la interfaz Gigabit Ethernet .**pcap-file.fe-0.0.1fe-0.0.1** Cuando el archivo denominado alcanza el tamaño máximo, se cambia el nombre del archivo .**pcap-file.fe-0.0.1pcap-file.fe-0.0.1.0** Cuando el archivo denominado vuelva a alcanzar el tamaño máximo, se cambiará el nombre al archivo denominado y se le cambiará el nombre .**pcap-file.fe-0.0.1pcap-file.fe-0.0.1.0pcap-file.fe-0.0.1.1pcap-file.fe-0.0.1pcap-file.fe-0.0.1.0** Este proceso continúa hasta que se supera el número máximo de archivos y se sobrescribe el archivo más antiguo. El archivo es siempre el archivo más reciente.**pcap-file.fe-0.0.1**

Los archivos de captura de paquetes no se quitan incluso después de deshabilitar la captura de paquetes en una interfaz.

Análisis de archivos de captura de paquetes

Los archivos de captura de paquetes se almacenan en formato libpcap en el directorio./`var/tmp` Puede especificar privilegios de usuario o administrador para los archivos.

Los archivos de captura de paquetes se pueden abrir y analizar sin conexión con tcpdump o cualquier analizador de paquetes que reconozca el formato libpcap. También puede utilizar FTP o el Protocolo de control de sesión (SCP) para transferir los archivos de captura de paquetes a un dispositivo externo.

> **NOTA**: Desactive la captura de paquetes antes de abrir el archivo para analizarlo o transferirlo a un dispositivo externo con FTP o SCP. La desactivación de la captura de paquetes garantiza que el búfer de archivos interno se vacíe y que todos los paquetes capturados se escriban en el archivo.

Ejemplo: Habilitar la captura de paquetes en un dispositivo

in this section

- Requisitos | **1542**
- Descripción general | **1543**
- Configuración | **1543**
- Verificación | **1545**

En este ejemplo se muestra cómo habilitar la captura de paquetes en un dispositivo, analizar el tráfico de red y solucionar problemas de red.

Requisitos

Antes de empezar:

- Establecer conectividad básica.

- Configure las interfaces de red. Consulte la Guía del usuario de interfaces para dispositivos de seguridad.

Descripción general

En este ejemplo, el tamaño máximo de captura de paquetes en cada archivo se establece en 500 bytes. El intervalo va de 68 a 1500 y el valor predeterminado es de 68 bytes. Especifique el nombre de archivo de destino para el archivo de captura de paquetes como archivo pcap. A continuación, especifique el número máximo de archivos que desea capturar como 100. El intervalo es de 2 a 10.000 y el valor predeterminado es 10 archivos. Establecer el tamaño máximo de cada archivo en 1024 bytes. El intervalo es de 1.024 a 104.857.600 y el valor predeterminado es 512.000 bytes. Por último, especifique que todos los usuarios tengan permiso para leer los archivos de captura de paquetes.

Configuración

in this section

- Procedimiento | **1543**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
set forwarding-options packet-capture maximum-capture-size 500
set forwarding-options packet-capture file filename pcap-file files 100 size 1024 world-readable
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte *Uso del editor de CLI en el modo de configuración*.

Para habilitar la captura de paquetes en un dispositivo:

1. Establezca el tamaño máximo de captura de paquetes.

```
[edit]
user@host# edit forwarding-options
user@host# set packet-capture maximum-capture-size 500
```

2. Especifique el nombre de archivo de destino.

```
[edit forwarding-options]
user@host# set packet-capture file filename pcap-file
```

3. Especifique el número máximo de archivos que desea capturar.

```
[edit forwarding-options]
user@host# set packet-capture file files 100
```

4. Especifique el tamaño máximo de cada archivo.

```
[edit forwarding-options]
user@host# set packet-capture file size 1024
```

5. Especifique que todos los usuarios tengan permiso para leer el archivo.

```
[edit forwarding-options]
user@host# set packet-capture file world-readable
```

Resultados

Desde el modo de configuración, confírmela con el comando `run show forwarding-options`. Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

```
[edit]
user@host# run show forwarding-options
packet-capture {
    file filename pcap-file files 100 size 1k world-readable;
```

```
    maximum-capture-size 500;
}
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Verificación

in this section

- Verificación de la configuración de captura de paquetes | **1545**
- Verificación de paquetes capturados | **1545**

Confirme que la configuración funcione correctamente.

Verificación de la configuración de captura de paquetes

Propósito

Compruebe que la captura de paquetes esté configurada en el dispositivo.

Acción

En el modo de configuración, escriba el comando `run show forwarding-options`. Compruebe que el resultado muestra la configuración de archivo prevista para capturar paquetes.

Verificación de paquetes capturados

Propósito

Compruebe que el archivo de captura de paquetes está almacenado en el directorio y que los paquetes se pueden analizar sin conexión.`/var/tmp`

Acción

1. Desactive la captura de paquetes.

   Mediante FTP, transfiera un archivo de captura de paquetes (por ejemplo,) a un servidor donde haya instalado herramientas de análisis de paquetes (por ejemplo,).`126b.fe-0.0.1tools-server`

1. Desde el modo de configuración, conéctese mediante FTP.`tools-server`

```
[edit]
user@host# run ftp tools-server
Connected to tools-server.mydomain.net
220 tools-server.mydomain.net FTP server (Version 6.00LS) ready
Name (tools-server:user):remoteuser
331 Password required for remoteuser.
Password:
230 User remoteuser logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

2. Desplácese hasta el directorio donde se almacenan los archivos de captura de paquetes en el dispositivo.

```
ftp> lcd /var/tmp
Local directory now /cf/var/tmp
```

3. Copie el archivo de captura de paquetes que desea analizar en el servidor, por ejemplo .`126b.fe-0.0.1`

```
ftp> put 126b.fe-0.0.1
local: 126b.fe-0.0.1 remote: 126b.fe-0.0.1
200 PORT command successful.
150 Opening BINARY mode data connection for '126b.fe-0.0.1'.
100%   1476       00:00 ETA
226 Transfer complete.
1476 bytes sent in 0.01 seconds (142.42 KB/s)
```

4. Vuelva al modo de configuración.

```
ftp> bye
221 Goodbye.
[edit]
user@host#
```

2. Abra el archivo de captura de paquetes en el servidor con tcpdump o cualquier analizador de paquetes que admita el formato libpcap y revise la salida.

```
root@server% tcpdump -r 126b.fe-0.0.1 -xevvvv
```

```
01:12:36.279769 Out 0:5:85:c4:e3:d1 > 0:5:85:c8:f6:d1, ethertype IPv4 (0x0800), length 98: (tos
0x0, ttl  64, id 33133, offset 0, flags [none], proto: ICMP (1), length: 84) 14.1.1.1 >
15.1.1.1: ICMP echo request seq 0, length 64
                         0005 85c8 f6d1 0005 85c4 e3d1 0800 4500
                         0054 816d 0000 4001 da38 0e01 0101 0f01
                         0101 0800 3c5a 981e 0000 8b5d 4543 51e6
                         0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
                         aaaa aaaa 0000 0000 0000 0000 0000 0000
                         0000 0000 0000 0000 0000 0000 0000 0000
                         0000
01:12:36.279793 Out 0:5:85:c8:f6:d1 > 0:5:85:c4:e3:d1, ethertype IPv4 (0x0800), length 98: (tos
0x0, ttl  63, id 41227, offset 0, flags [none], proto: ICMP (1), length: 84) 15.1.1.1 >
14.1.1.1: ICMP echo reply seq 0, length 64
                         0005 85c4 e3d1 0005 85c8 f6d1 0800 4500
                         0054 a10b 0000 3f01 bb9a 0f01 0101 0e01
                         0101 0000 445a 981e 0000 8b5d 4543 51e6
                         0100 aaaa aaaa aaaa aaaa aaaa aaaa aaaa
                         aaaa aaaa 0000 0000 0000 0000 0000 0000
                         0000 0000 0000 0000 0000 0000 0000 0000
                         0000
root@server%
```

Ejemplo: Configurar la captura de paquetes en una interfaz

in this section

- Requisitos | **1548**
- Descripción general | **1548**
- Configuración | **1548**
- Verificación | **1549**

En este ejemplo se muestra cómo configurar la captura de paquetes en una interfaz para analizar el tráfico.

Requisitos

Antes de empezar:

- Establecer conectividad básica.
- Configure las interfaces de red. Consulte la Guía del usuario de interfaces para dispositivos de seguridad.

Descripción general

En este ejemplo, se crea una interfaz denominada fe-0/0/1 y, a continuación, se configura la dirección del tráfico para el que se habilita la captura de paquetes en la interfaz lógica como entrante y saliente.

> **NOTA**: En el tráfico que omite el módulo de software de flujo (paquetes de protocolo como ARP, OSPF y PIM), los paquetes generados por el motor de enrutamiento no se capturan a menos que haya configurado y aplicado un filtro de firewall en la interfaz en la dirección de salida.

Configuración

in this section

- Procedimiento | **1548**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
edit interfaces fe-0/0/1
set unit 0 family inet sampling input output
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte *Uso del editor de CLI en el modo de configuración*.

Para configurar la captura de paquetes en una interfaz:

1. Cree una interfaz.

```
[edit]
user@host# edit interfaces fe-0/0/1
```

2. Configure la dirección del tráfico.

```
[edit interfaces fe-0/0/1]
user@host# set unit 0 family inet sampling input output
```

3. Cuando termine de configurar el dispositivo, confirme la configuración.

```
[edit]
user@host# commit
```

Verificación

in this section

- Verificación de la configuración de captura de paquetes | 1549

Verificación de la configuración de captura de paquetes

Propósito

Confirme que la configuración funcione correctamente.

Compruebe que la captura de paquetes esté configurada en la interfaz.

Acción

En el modo de configuración, escriba el comando `run show interfaces fe-0/0/1`.

Ejemplo: Configurar un filtro de firewall para la captura de paquetes

in this section

- Requisitos | **1550**
- Descripción general | **1550**
- Configuración | **1551**
- Verificación | **1553**

En este ejemplo se muestra cómo configurar un filtro de firewall para la captura de paquetes y aplicarlo a una interfaz lógica.

Requisitos

Antes de empezar:

- Establecer conectividad básica.
- Configure las interfaces de red. Consulte la Guía del usuario de interfaces para dispositivos de seguridad.

Descripción general

in this section

- Topología | **1551**

En este ejemplo, se establece un filtro de firewall denominado dest-all y un nombre de término denominado dest-term para capturar paquetes desde una dirección de destino específica, que es 192.168.1.1/32. Defina la condición de coincidencia para aceptar los paquetes de muestra. Finalmente, aplique el filtro dest-all a todos los paquetes salientes en la interfaz fe-0/0/1.

NOTA: Si aplica un filtro de firewall en la interfaz de circuito cerrado, afecta a todo el tráfico hacia y desde el motor de enrutamiento. Si el filtro de firewall tiene una acción, se muestrean los paquetes hacia y desde el motor de enrutamiento.`sample` Si la captura de paquetes está habilitada, los paquetes hacia y desde el motor de enrutamiento se capturan en los archivos creados para las interfaces de entrada y salida.

Topología

Configuración

in this section

- Procedimiento | **1551**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
set firewall filter dest-all term dest-term from destination-address 192.168.1.1/32
set firewall filter dest-all term dest-term then sample accept
edit interfaces
set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración en la Guía del usuario de CLI de Junos OS .*Usar el editor de CLI en el modo de configuración*

Para configurar un filtro de firewall para la captura de paquetes y aplicarlo a una interfaz lógica:

1. Especifique el filtro del firewall y su dirección de destino.

```
[edit]
user@host# edit firewall
user@host# set filter dest-all term dest-term from destination-address 192.168.1.1/32
```

2. Defina la condición de coincidencia y su acción.

```
[edit firewall]
user@host# set filter dest-all term dest-term then sample accept
```

3. Aplique el filtro a todos los paquetes salientes.

```
[edit interfaces]
user@host# set interfaces fe-0/0/1 unit 0 family inet filter output dest-all
```

Resultados

Desde el modo de configuración, confírmela con el comando `run show firewall filter dest-all`. Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

```
[edit]
user@host# run show firewall filter dest-all
term dest-term {
    from {
        destination-address 192.168.1.1/32;
    }
    then {
        sample;
        accept;
    }
}
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Verificación

in this section

- Comprobación del filtro de firewall para la configuración de captura de paquetes | 1553

Comprobación del filtro de firewall para la configuración de captura de paquetes

Propósito

Confirme que la configuración funcione correctamente.

Compruebe que el filtro de firewall para la captura de paquetes esté configurado.

Acción

En el modo de configuración, escriba el comando `run show firewall filter dest-all`. Compruebe que el resultado muestra la configuración prevista del filtro de firewall para capturar los paquetes enviados a la dirección de destino.

Ejemplo: Configurar la captura de paquetes para la depuración de rutas de datos

in this section

- Requisitos | 1554
- Descripción general | 1554
- Configuración | 1554
- Verificación | 1557

En este ejemplo se muestra cómo configurar la captura de paquetes para supervisar el tráfico que pasa por el dispositivo. La captura de paquetes luego vuelca los paquetes en un formato de archivo PCAP que puede ser examinado posteriormente por la utilidad tcpdump.

Requisitos

Antes de comenzar, consulte "Depurar la ruta de datos (procedimiento de la CLI)." en la página 1518

Descripción general

Se define un filtro para filtrar el tráfico; A continuación, se aplica un perfil de acción al tráfico filtrado. El perfil de acciones especifica una variedad de acciones en la unidad de procesamiento. Una de las acciones admitidas es el volcado de paquetes, que envía el paquete al motor de enrutamiento y lo almacena en forma propietaria para leerlo con el comando.`show security datapath-debug capture`

> **NOTA**: La depuración de rutas de datos se admite en SRX1400, SRX3400, SRX3600, SRX5400, SRX5600 y SRX5800.

Configuración

in this section

- Procedimiento | **1554**

Procedimiento

Configuración rápida de CLI

Para configurar rápidamente este ejemplo, copie los siguientes comandos, péguelos en un archivo de texto, elimine los saltos de línea, cambie los detalles necesarios para que coincidan con su configuración de red, copie y pegue los comandos en la CLI en el nivel de jerarquía `[edit]` y, luego, ingrese `commit` desde el modo de configuración.

```
set security datapath-debug capture-file my-capture
set security datapath-debug capture-file format pcap
set security datapath-debug capture-file size 1m
set security datapath-debug capture-file files 5
set security datapath-debug maximum-capture-size 400
set security datapath-debug action-profile do-capture event np-ingress packet-dump
set security datapath-debug packet-filter my-filter action-profile do-capture
set security datapath-debug packet-filter my-filter source-prefix 1.2.3.4/32
```

Procedimiento paso a paso

En el ejemplo siguiente, debe explorar por varios niveles en la jerarquía de configuración. Para obtener instrucciones sobre cómo hacerlo, consulte Uso del editor de CLI en modo de configuración enla Guía del usuario de CLI de Junos OS.*Usar el editor de CLI en el modo de configuración*

Para configurar la captura de paquetes:

1. Edite la opción security datapath-debug para las varias unidades de procesamiento a lo largo de la ruta de procesamiento de paquetes:

```
[edit]
user@host# edit security datapath-debug
```

2. Habilite el archivo de captura, el formato de archivo, el tamaño del archivo y el número de archivos. El número de tamaño limita el tamaño del archivo de captura. Una vez alcanzado el tamaño límite, si se especifica el número de archivo, el archivo de captura se rotará a filename , donde se incrementará automáticamente hasta que alcance el índice especificado y, a continuación, vuelva a cero.*xx* Si no se especifica ningún índice de archivos, los paquetes se descartarán después de alcanzar el límite de tamaño. El tamaño predeterminado es 512 kilobytes.

```
[edit security datapath-debug]
user@host# set capture-file my-capture format pcap size 1m files 5
[edit security datapath-debug]
user@host# set maximum-capture-size 400
```

3. Habilite el perfil de acción y establezca el evento. Establezca el perfil de acción como do-capture y el tipo de evento como np-ingress:

```
[edit security datapath-debug]
user@host# edit action-profile do-capture
[edit security datapath-debug action-profile do-capture]
user@host# edit event np-ingress
```

4. Habilite el volcado de paquetes para el perfil de acción:

```
[edit security datapath-debug action-profile do-capture event np-ingress]
user@host# set packet-dump
```

5. Habilite las opciones de filtro, acción y filtro de paquetes. El filtro de paquetes se establece en mi-filtro, el perfil de acción se establece en do-capture y la opción de filtro se establece en source-prefix 1.2.3.4/32.

```
[edit security datapath-debug]
user@host# set security datapath-debug packet-filter my-filter action-profile do-capture
```

```
[edit security datapath-debug]
user@host#  set security datapath-debug packet-filter my-filter source-prefix 1.2.3.4/32
```

Resultados

Desde el modo de configuración, confírmela con el comando `show security datapath-debug`. Si el resultado no muestra la configuración deseada, repita las instrucciones de configuración en este ejemplo para corregirla.

```
security {
    datapath-debug {
        capture-file {
            my-capture
            format pcap
            size 1m
            files 5;
        }
    }
    maximum-capture-size 100;
    action-profile do-capture {
        event np-ingress {
             packet-dump
         }
      }
    packet-filter my-filter {
         source-prefix 1.2.3.4/32
        action-profile do-capture
     }
 }
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Verificación

in this section

- Verificación de la captura de paquetes | 1557
- Comprobación de la captura de depuración de rutas de datos | 1557
- Contador de depuración de comprobación de rutas de datos | 1558

Confirme que la configuración funcione correctamente.

Verificación de la captura de paquetes

Propósito

Compruebe si la captura de paquetes funciona.

Acción

Desde el modo operativo, escriba el comando para iniciar la captura de paquetes y escriba el comando para detener la captura de paquetes.`request security datapath-debug capture startrequest security datapath-debug capture stop`

Para ver los resultados, desde el modo operativo de la CLI, acceda al shell de UNIX local y navegue hasta el directorio /var/log/my-capture. El resultado se puede leer mediante la utilidad tcpdump.

Comprobación de la captura de depuración de rutas de datos

Propósito

Compruebe los detalles del archivo de captura de depuración de rutas de datos.

Acción

Desde el modo operativo, ingrese el comando `show security datapath-debug capture`.

```
user@host>show security datapath-debug capture
```

ADVERTENCIA: Cuando haya terminado de solucionar problemas, asegúrese de eliminar o desactivar todas las configuraciones de traceoptions (no limitadas a flow traceoptions) y la estrofa completa de configuración de datapath-debug de seguridad. Si alguna configuración de depuración permanece activa, seguirá utilizando los recursos de CPU y memoria del dispositivo.

Contador de depuración de comprobación de rutas de datos

Propósito

Compruebe los detalles del contador de depuración de rutas de datos.

Acción

Desde el modo operativo, ingrese el comando `show security datapath-debug counter`.

Deshabilitar la captura de paquetes

Debe deshabilitar la captura de paquetes antes de abrir el archivo de captura de paquetes para analizarlo o transferirlo a un dispositivo externo. La desactivación de la captura de paquetes garantiza que el búfer de archivos interno se vacíe y que todos los paquetes capturados se escriban en el archivo.

Para deshabilitar la captura de paquetes, ingrese desde el modo de configuración:

```
[edit forwarding-options]
user@host# set packet-capture disable
```

Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Modificar la encapsulación en interfaces con la captura de paquetes configurada

Antes de modificar la encapsulación en una interfaz de dispositivo configurada para la captura de paquetes, debe deshabilitar la captura de paquetes y cambiar el nombre del archivo de captura de paquetes más reciente. De lo contrario, la captura de paquetes guarda los paquetes con diferentes

encapsulaciones en el mismo archivo de captura de paquetes. Los archivos de paquetes que contienen paquetes con diferentes encapsulaciones no son útiles, porque las herramientas de análisis de paquetes como tcpdump no pueden analizar dichos archivos.

Después de modificar la encapsulación, puede volver a habilitar la captura de paquetes de forma segura en el dispositivo.

Para cambiar la encapsulación en interfaces con captura de paquetes configurada:

1. Desactive la captura de paquetes (consulte "Deshabilitar captura de paquetes" en la página 1558).
2. Ingrese desde el modo de configuración.`commit`
3. Cambie el nombre del último archivo de captura de paquetes en el que va a cambiar la encapsulación con la extensión.`.chdsl`

   a) Desde el modo operativo, acceda al shell local de UNIX.

   ```
   user@host> start shell
   %
   ```

   b) Desplácese hasta el directorio donde se almacenan los archivos de captura de paquetes.

   ```
   % cd /var/tmp
   %
   ```

   c) Cambie el nombre del último archivo de captura de paquetes para la interfaz en la que está cambiando la encapsulación; por ejemplo `.fe.0.0.0`

   ```
   % mv pcap-file.fe.0.0.0 pcap-file.fe.0.0.0.chdsl
   %
   ```

   d) Vuelva al modo operativo.

   ```
   % exit
   user@host>
   ```

4. Cambie la encapsulación en la interfaz mediante la interfaz de usuario de J-Web o el editor de configuración de CLI.
5. Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.
6. Vuelva a habilitar la captura de paquetes (consulte Ejemplo:" Habilitar la captura de paquetes en un dispositivo)." en la página 1542

7. Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Eliminar archivos de captura de paquetes

La eliminación de archivos de captura de paquetes del directorio /var/tmp solo elimina temporalmente los archivos de captura de paquetes. Los archivos de captura de paquetes para la interfaz se crean automáticamente de nuevo la próxima vez que se confirma un cambio en la configuración de captura de paquetes o como parte de una rotación de archivos de captura de paquetes.

Para eliminar un archivo de captura de paquetes:

1. Desactive la captura de paquetes (consulte "Deshabilitar captura de paquetes" en la página 1558).
2. Elimine el archivo de captura de paquetes de la interfaz.
   a) Desde el modo operativo, acceda al shell local de UNIX.

```
user@host> start shell
%
```

   b) Desplácese hasta el directorio donde se almacenan los archivos de captura de paquetes.

```
% cd /var/tmp
%
```

   c) Elimine el archivo de captura de paquetes para la interfaz; por ejemplo `.pcap-file.fe.0.0.0`

```
% rm pcap-file.fe.0.0.0
%
```

   d) Vuelva al modo operativo.

```
% exit
user@host>
```

3. Vuelva a habilitar la captura de paquetes (consulte Ejemplo:" Habilitar la captura de paquetes en un dispositivo)." en la página 1542
4. Cuando termine de configurar el dispositivo, ingrese `commit` en el modo de configuración.

Mostrar encabezados de paquetes

Escriba el comando para mostrar los encabezados de los paquetes transmitidos a través de interfaces de red con la siguiente sintaxis:`monitor traffic`

> **NOTA**: El uso del comando puede degradar el rendimiento del sistema.`monitor traffic` Se recomienda usar opciones de filtrado, como y , para minimizar el impacto en el rendimiento de paquetes en el sistema.`countmatching`

```
user@host> monitor traffic <absolute-sequence> <count number> <interface interface-name> <layer2-headers> <matching "expression"> <no-domain-names> <no-promiscuous> <no-resolve> <no-timestamp> <print-ascii> <print-hex> <size bytes> <brief | detail | extensive>
```

Describe las opciones de comando.Tabla 167 en la página 1561`monitor traffic`

Tabla 167: Opciones de comando de monitoreo de tráfico de CLI

La opción	Description
`absolute-sequence`	(Opcional) Muestra los números de secuencia TCP absolutos.
`count number`	(Opcional) Muestra el número especificado de encabezados de paquete. Especifique un valor de a `.0100,000` El comando se cierra y sale del símbolo del sistema después de alcanzar este número.
`interface interface-name`	(Opcional) Muestra los encabezados de los paquetes para el tráfico en la interfaz especificada. Si no se especifica una interfaz, se supervisa la interfaz con el número más bajo.
`layer2-headers`	(Opcional) Muestra el encabezado del paquete de capa de vínculo en cada línea.
`matching "expression"`	(Opcional) Muestra encabezados de paquetes que coinciden con una expresión entre comillas (" "). Mediante condiciones de coincidencia de lista, operadores lógicos y operadores aritméticos, binarios y relacionales que puede utilizar en la expresión.Tabla 168 en la página 1563Tabla 170 en la página 1566

Tabla 167: Opciones de comando de monitoreo de tráfico de CLI *(Continued)*

La opción	Description
`no-domain-names`	(Opcional) Suprime la presentación de la parte del nombre de dominio del nombre de host.
`no-promiscuous`	(Opcional) Especifica que se coloque la interfaz supervisada en modo promiscuo.*not* En el modo promiscuo, la interfaz lee todos los paquetes que le llegan. En el modo no promiscuo, la interfaz lee sólo los paquetes dirigidos a ella.
`no-resolve`	(Opcional) Suprime la presentación de nombres de host.
`no-timestamp`	(Opcional) Suprime la visualización de las marcas de tiempo de los encabezados de los paquetes.
`print-ascii`	(Opcional) Muestra cada encabezado de paquete en formato ASCII.
`print-hex`	(Opcional) Muestra cada encabezado de paquete, excepto los encabezados de capa de vínculo, en formato hexadecimal.
`size` *bytes*	(Opcional) Muestra el número de bytes para cada paquete que especifique. Si el encabezado de un paquete supera este tamaño, el encabezado del paquete mostrado se trunca. El valor predeterminado es .`96`
`brief`	(Opcional) Muestra información mínima del encabezado del paquete. Este es el valor predeterminado.
`detail`	(Opcional) Muestra la información del encabezado del paquete con detalles moderados. Para algunos protocolos, también debe usar la opción para ver información detallada.`size`
`extensive`	(Opcional) Muestra el nivel más extenso de información de encabezado de paquete. Para algunos protocolos, también debe usar la opción para ver información extensa.`size`

Para salir del comando y volver al símbolo del sistema, presione Ctrl-C.`monitor traffic`

Para limitar la información del encabezado del paquete que muestra el comando, incluya la opción.`monitor trafficmatching "expression"` Una expresión consta de una o más condiciones de coincidencia enumeradas en , entre comillas (" ").Tabla 168 en la página 1563 Puede combinar condiciones de coincidencia mediante los operadores lógicos enumerados en (mostrados en orden de mayor a menor prioridad).Tabla 169 en la página 1566

Por ejemplo, para mostrar encabezados de paquetes TCP o UDP, escriba:

```
user@host> monitor traffic matching “tcp || udp”
```

Para comparar los siguientes tipos de expresiones, utilice los operadores relacionales enumerados en (enumerados de mayor a menor prioridad):Tabla 170 en la página 1566

- Aritmética: expresiones que utilizan los operadores aritméticos enumerados en .Tabla 170 en la página 1566
- Binario: expresiones que utilizan los operadores binarios enumerados en .Tabla 170 en la página 1566
- Descriptor de acceso de datos de paquetes: expresiones que utilizan la sintaxis siguiente:

  ```
  protocol [byte-offset <size>]
  ```

  Reemplazar por cualquier protocolo en .*protocol*Tabla 168 en la página 1563 Reemplace con el desplazamiento de bytes, desde el principio del encabezado del paquete, para usarlo en la comparación.*byte-offset* El parámetro opcional representa el número de bytes examinados en el encabezado del paquete: 1, 2 o 4 bytes.*size*

  Por ejemplo, el siguiente comando muestra todo el tráfico de multidifusión:

  ```
  user@host> monitor traffic matching “ether[0] & 1 !=0”
  ```

Tabla 168: Monitoreo de tráfico de CLI Condiciones de coincidencia

Condición de coincidencia	Description
Tipo de entidad	

Tabla 168: Monitoreo de tráfico de CLI Condiciones de coincidencia *(Continued)*

Condición de coincidencia	Description
`host [address | hostname]`	Hace coincidir los encabezados de los paquetes que contienen la dirección o el nombre de host especificados. Puede anteponer cualquiera de las siguientes condiciones de coincidencia de protocolo, seguidas de un espacio, a :`host` , , o cualquiera de las condiciones de coincidencia direccional.`arpiprarp`
`network address`	Hace coincidir los encabezados de los paquetes con las direcciones de origen o destino que contienen la dirección de red especificada.
`network address mask mask`	Hace coincidir los encabezados de los paquetes que contienen la dirección de red especificada y la máscara de subred.
`port [port-number | port-name]`	Hace coincidir los encabezados de los paquetes que contienen el número o nombre de puerto TCP o UDP de origen o destino especificados.
Direccional	
`destination`	Hace coincidir los encabezados de los paquetes que contienen el destino especificado. Las condiciones de coincidencia direccional se pueden anteponer a cualquier condición de coincidencia de tipo de entidad, seguida de un espacio.
`source`	Hace coincidir los encabezados de paquete que contienen el origen especificado.
`source and destination`	Hace coincidir los encabezados de los paquetes que contienen el destino de origen especificado.*and*
`source or destination`	Hace coincidir los encabezados de los paquetes que contienen el destino de origen especificado.*or*
Longitud del paquete	
`less bytes`	Hace coincidir paquetes con longitudes menores o iguales al valor especificado, en bytes.

Tabla 168: Monitoreo de tráfico de CLI Condiciones de coincidencia *(Continued)*

Condición de coincidencia	Description
`greater` *bytes*	Hace coincidir paquetes con longitudes mayores o iguales que el valor especificado, en bytes.
Protocolo	
`arp`	Hace coincidir todos los paquetes ARP.
`ether`	Hace coincidir todas las tramas Ethernet.
`ether [broadcast | multicast]`	Hace coincidir las tramas de difusión o multidifusión de Ethernet. Esta condición de coincidencia puede anteponerse con o `.sourcedestination`
`ether protocol [`*address* `| (\arp | \ip | \rarp)`	Hace coincidir las tramas Ethernet con la dirección o el tipo de protocolo especificados. Los argumentos, , y también son condiciones de coincidencia independientes, por lo que deben ir precedidos de una barra diagonal inversa (\) cuando se usan en la condición de coincidencia.`arpiprarpether protocol`
`icmp`	Hace coincidir todos los paquetes del ICMP
`ip`	Hace coincidir todos los paquetes IP.
`ip [broadcast | multicast]`	Hace coincidir los paquetes de difusión o de multidifusión IP.
`ip protocol [`*address* `| (\icmp | igrp | \tcp | \udp)]`	Hace coincidir los paquetes IP con la dirección o el tipo de protocolo especificados. Los argumentos, , y también son condiciones de coincidencia independientes, por lo que deben ir precedidos de una barra diagonal inversa (\) cuando se usan en la condición de coincidencia.`icmptcpudpip protocol`
`isis`	Hace coincidir todos los mensajes de enrutamiento IS-IS.
`rarp`	Hace coincidir todos los paquetes RARP.

Tabla 168: Monitoreo de tráfico de CLI Condiciones de coincidencia *(Continued)*

Condición de coincidencia	Description
`tcp`	Hace coincidir todos los paquetes TCP.
`udp`	Hace coincidir todos los paquetes UDP.

Tabla 169: Monitoreo de tráfico de CLI Operadores lógicos

Operador lógico	Description
`!`	NOT lógica. Si la primera condición no coincide, se evalúa la siguiente.
`&&`	Lógica Y. Si la primera condición coincide, se evalúa la siguiente. Si la primera condición no coincide, se omite la siguiente.
`||`	Lógica O. Si la primera condición coincide, se omite la siguiente. Si la primera condición no coincide, se evalúa la siguiente.
`()`	Agrupe los operadores para anular el orden de precedencia predeterminado. Los paréntesis son caracteres especiales, cada uno de los cuales debe ir precedido de una barra diagonal inversa (\).

Tabla 170: Monitoreo de tráfico de CLI Operadores aritméticos, binarios y relacionales

Operador	Description
Operador aritmético	
`+`	Operador de suma.
`-`	Operador de sustracción.
`/`	Operador de división.

Tabla 170: Monitoreo de tráfico de CLI Operadores aritméticos, binarios y relacionales *(Continued)*

Operador	Description
Operador binario	
&	Operación a nivel de bits Y.
*	Operación a nivel de bits exclusiva O.
|	Operación a nivel de bits inclusiva O.
Operador relacional	
<=	Se produce una coincidencia si la primera expresión es menor o igual que la segunda.
>=	Se produce una coincidencia si la primera expresión es mayor o igual que la segunda.
<	Se produce una coincidencia si la primera expresión es menor que la segunda.
>	Se produce una coincidencia si la primera expresión es mayor que la segunda.
=	Se produce una coincidencia si la primera expresión es igual a la segunda.
!=	Se produce una coincidencia si la primera expresión no es igual a la segunda.

A continuación se muestra un ejemplo de salida del comando:`monitor traffic`

```
user@host> monitor traffic count 4 matching “arp” detail
```

```
Listening on fe-0/0/0, capture size 96 bytes  15:04:16.276780  In arp who-has 193.1.1.1 tell
host1.site2.net 15:04:16.376848  In arp who-has host2.site2.net tell host1.site2.net
15:04:16.376887  In arp who-has 193.1.1.2 tell host1.site2.net 15:04:16.601923  In arp who-has
193.1.1.3 tell host1.site2.net
```

Solución de problemas de dispositivos de seguridad

in this section

- Resolución de problemas de resolución de nombres DNS en directivas de seguridad del sistema lógico (solo administradores principales) | 1568
- Solución de problemas de la interfaz de servicios de vínculo | 1569
- Solución de problemas de las políticas de seguridad | 1583

Resolución de problemas de resolución de nombres DNS en directivas de seguridad del sistema lógico (solo administradores principales)

in this section

- Problema | 1568
- Causa | 1568
- Solución | 1569

Problema

Description

Es posible que la dirección de un nombre de host en una entrada de la libreta de direcciones que se usa en una directiva de seguridad no se resuelva correctamente.

Causa

Normalmente, las entradas de la libreta de direcciones que contienen nombres de host dinámicos se actualizan automáticamente para los firewalls de la serie SRX. El campo TTL asociado a una entrada DNS indica la hora a partir de la cual la entrada debe actualizarse en la caché de directivas. Una vez que

expira el valor TTL, el firewall de la serie SRX actualiza automáticamente la entrada DNS para una entrada de libreta de direcciones.

Sin embargo, si el firewall de la serie SRX no puede obtener una respuesta del servidor DNS (por ejemplo, la solicitud DNS o el paquete de respuesta se pierde en la red o el servidor DNS no puede enviar una respuesta), es posible que la dirección de un nombre de host en una entrada de libreta de direcciones no se resuelva correctamente. Esto puede hacer que el tráfico se caiga ya que no se encuentra ninguna política de seguridad o coincidencia de sesión.

Solución

El administrador principal puede usar el comando para mostrar información de caché DNS en el firewall de la serie SRX.`show security dns-cache` Si es necesario actualizar la información de caché DNS, el administrador principal puede usar el comando.`clear security dns-cache`

> **NOTA**: Estos comandos solo están disponibles para el administrador principal en dispositivos configurados para sistemas lógicos. Este comando no está disponible en sistemas lógicos de usuario ni en dispositivos que no están configurados para sistemas lógicos.

SEE ALSO

- Descripción de las directivas de seguridad de sistemas lógicos

Solución de problemas de la interfaz de servicios de vínculo

in this section

- Determinar qué componentes de CoS se aplican a los vínculos constituyentes | **1570**
- Determinar qué causa la fluctuación y la latencia en el paquete multivínculo | **1574**
- Determinar si LFI y equilibrio de carga funcionan correctamente | **1574**
- Determinar por qué se dejan caer paquetes en un PVC entre un dispositivo de Juniper Networks y un dispositivo de terceros | **1583**

Para resolver problemas de configuración en una interfaz de servicios de vínculo:

Determinar qué componentes de CoS se aplican a los vínculos constituyentes

in this section

Problema | 1570
Solución | 1570

Problema

Description

Está configurando un paquete multivínculo, pero también tiene tráfico sin encapsulación MLPPP que pasa a través de vínculos constituyentes del paquete multivínculo. ¿Aplica todos los componentes de CoS a los enlaces constituyentes o es suficiente aplicarlos al paquete multivínculo?

Solución

Puede aplicar una asignación de programador al paquete multivínculo y a sus vínculos constituyentes. Aunque puede aplicar varios componentes de CoS con la asignación del programador, configure solo los que sean necesarios. Le recomendamos que mantenga la configuración de los enlaces constituyentes simple para evitar retrasos innecesarios en la transmisión.

Tabla 1 muestra los componentes de CoS que se aplicarán en un paquete multivínculo y sus vínculos constituyentes.

Tabla 171: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Clasificador	Sí	No	La clasificación CoS tiene lugar en el lado entrante de la interfaz, no en el lado de transmisión, por lo que no se necesitan clasificadores en los enlaces constituyentes.

Tabla 171: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes *(Continued)*

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Clase de reenvío	Sí	No	La clase de reenvío se asocia a una cola y la cola se aplica a la interfaz mediante una asignación de programador. La asignación de cola está predeterminada en los vínculos constituyentes. Todos los paquetes de Q2 del paquete multivínculo se asignan a Q2 del enlace constituyente, y los paquetes de todas las demás colas se ponen en cola en Q0 del enlace constituyente.

Tabla 171: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes *(Continued)*

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Mapa del programador	Sí	Sí	Aplique las asignaciones del programador en el paquete multivínculo y el vínculo constituyente de la siguiente manera: • Velocidad de transmisión: asegúrese de que el orden relativo de la velocidad de transmisión configurada en Q0 y Q2 sea el mismo en los vínculos constituyentes que en el paquete multivínculo. • Prioridad del programador: asegúrese de que el orden relativo de la prioridad del programador configurada en Q0 y Q2 sea el mismo en los vínculos constituyentes que en el paquete multivínculo. • Tamaño del búfer: dado que todos los paquetes que no son LFI del paquete multivínculo transitan en Q0 de los vínculos constituyentes, asegúrese de que el tamaño del búfer en Q0 de los enlaces constituyentes sea lo suficientemente grande. • Perfil de colocación RED: configure un perfil de colocación ROJA solo en el paquete multivínculo. La configuración del perfil de gota RED en los enlaces constituyentes aplica un mecanismo de contrapresión que cambia el tamaño del búfer e introduce variación. Dado que este comportamiento puede provocar caídas de fragmentos en los vínculos constituyentes, asegúrese de dejar el perfil de colocación ROJO en la configuración predeterminada de los vínculos constituyentes.

Tabla 171: Componentes de CoS aplicados en paquetes multivínculo y enlaces constituyentes *(Continued)*

Componente Cos	Paquete Multilink	Enlaces constituyentes	Explicación
Velocidad de conformación para un programador por unidad o un programador de nivel de interfaz	No	Sí	Dado que la programación por unidad se aplica solo en el punto final, aplique esta velocidad de conformación solo a los vínculos constituyentes. Cualquier configuración aplicada anteriormente se sobrescribe con la configuración del vínculo constituyente.
Velocidad de transmisión exacta o modelado a nivel de cola	Sí	No	La forma a nivel de interfaz aplicada en los vínculos constituyentes anula cualquier forma en la cola. Por lo tanto, aplique la forma exacta de la velocidad de transmisión solo en el paquete multivínculo.
Reescritura de reglas	Sí	No	Los bits de reescritura se copian del paquete en los fragmentos automáticamente durante la fragmentación. Por lo tanto, lo que se configura en el paquete multivínculo se lleva en los fragmentos a los enlaces constituyentes.
Grupo de canales virtuales	Sí	No	Los grupos de canales virtuales se identifican mediante reglas de filtro de firewall que se aplican a los paquetes solo antes del paquete multivínculo. Por lo tanto, no es necesario aplicar la configuración del grupo de canales virtuales a los vínculos constituyentes.

SEE ALSO

Guía del usuario de clase de servicio (dispositivos de seguridad)

Determinar qué causa la fluctuación y la latencia en el paquete multivínculo

in this section

- Problema | 1574
- Solución | 1574

Problema

Description

Para probar la fluctuación y la latencia, se envían tres flujos de paquetes IP. Todos los paquetes tienen la misma configuración de prioridad de IP. Después de configurar LFI y CRTP, la latencia aumentó incluso en un vínculo no congestionado. ¿Cómo puede reducir la fluctuación y la latencia?

Solución

Para reducir la fluctuación y la latencia, haga lo siguiente:

1. Asegúrese de que ha configurado una velocidad de conformación en cada enlace constituyente.
2. Asegúrese de que no ha configurado una velocidad de conformación en la interfaz de servicios de vínculo.
3. Asegúrese de que el valor de la velocidad de conformación configurada sea igual al ancho de banda de la interfaz física.
4. Si las velocidades de conformación están configuradas correctamente y la fluctuación persiste, comuníquese con el Centro de asistencia técnica de Juniper Networks (JTAC).

Determinar si LFI y equilibrio de carga funcionan correctamente

in this section

- Problema | 1575
- Solución | 1575

Problema

Description

En este caso, tiene una sola red que admite varios servicios. La red transmite datos y tráfico de voz sensible a los retrasos. Después de configurar MLPPP y LFI, asegúrese de que los paquetes de voz se transmiten a través de la red con muy poco retraso y fluctuación. ¿Cómo puede saber si los paquetes de voz se tratan como paquetes LFI y si el equilibrio de carga se realiza correctamente?

Solución

Cuando LFI está habilitado, los paquetes de datos (no LFI) se encapsulan con un encabezado MLPPP y se fragmentan en paquetes de un tamaño especificado. Los paquetes de voz sensibles al retardo (LFI) están encapsulados en PPP e intercalados entre fragmentos de paquetes de datos. Las colas y el equilibrio de carga se realizan de manera diferente para los paquetes LFI y no LFI.

Para comprobar que LFI se realiza correctamente, determine que los paquetes estén fragmentados y encapsulados según lo configurado. Después de saber si un paquete se trata como un paquete LFI o un paquete que no es LFI, puede confirmar si el equilibrio de carga se realiza correctamente.

: supongamos que dos dispositivos de Juniper Networks, R0 y R1, están conectados por un paquete multivínculo que agrega dos vínculos serie y `.Solution Scenariolsq-0/0/0.0se-1/0/0se-1/0/1` En R0 y R1, MLPPP y LFI se habilitan en la interfaz de servicios de vínculo y el umbral de fragmentación se establece en 128 bytes.

En este ejemplo, usamos un generador de paquetes para generar flujos de voz y datos. Puede utilizar la función de captura de paquetes para capturar y analizar los paquetes en la interfaz entrante.

Los dos flujos de datos siguientes se enviaron en el paquete multivínculo:

- 100 paquetes de datos de 200 bytes (mayores que el umbral de fragmentación)
- 500 paquetes de datos de 60 bytes (más pequeños que el umbral de fragmentación)

Las dos secuencias de voz siguientes se enviaron en el paquete multivínculo:

- 100 paquetes de voz de 200 bytes desde el puerto fuente 100
- 300 paquetes de voz de 200 bytes desde el puerto fuente 200

Para confirmar que la LFI y el equilibrio de carga se realizan correctamente:

> **NOTA**: En este ejemplo, solo se muestran y describen las partes significativas de la salida del comando.

1. Compruebe la fragmentación de paquetes. Desde el modo operativo, escriba el comando para comprobar que los paquetes grandes están fragmentados correctamente.`show interfaces lsq-0/0/0`

```
user@R0#> show interfaces lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Last flapped   : 2006-08-01 10:45:13 PDT (2w0d 06:06 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

  Logical interface lsq-0/0/0.0 (Index 69) (SNMP ifIndex 42)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
    Bandwidth: 16mbps
    Statistics         Frames      fps       Bytes        bps
    Bundle:
      Fragments:
        Input :             0        0           0          0
        Output:          1100        0      118800          0
      Packets:
        Input :             0        0           0          0
        Output:          1000        0      112000          0
   ...
    Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 9.9.9/24, Local: 9.9.9.10
```

`Meaning`: el resultado muestra un resumen de los paquetes que transitan por el dispositivo en el paquete multivínculo. Compruebe la siguiente información en el paquete multivínculo:

- El número total de paquetes en tránsito = 1000
- El número total de fragmentos en tránsito=1100
- El número de paquetes de datos fragmentados =100

El número total de paquetes enviados (600 + 400) en el paquete multivínculo coincide con el número de paquetes en tránsito (1000), lo que indica que no se descartó ningún paquete.

El número de fragmentos en tránsito supera en 100 el número de paquetes en tránsito, lo que indica que 100 paquetes de datos grandes se fragmentaron correctamente.

`Corrective Action`: si los paquetes no están fragmentados correctamente, compruebe la configuración del umbral de fragmentación. Los paquetes menores que el umbral de fragmentación especificado no se fragmentan.

2. Verifique la encapsulación del paquete. Para averiguar si un paquete se trata como un paquete LFI o no LFI, determine su tipo de encapsulación. Los paquetes LFI están encapsulados PPP y los paquetes que no son LFI se encapsulan con PPP y MLPPP. Las encapsulaciones PPP y MLPPP tienen diferentes sobrecargas, lo que resulta en paquetes de diferentes tamaños. Puede comparar tamaños de paquetes para determinar el tipo de encapsulación.

   Un pequeño paquete de datos no fragmentado contiene un encabezado PPP y un solo encabezado MLPPP. En un paquete de datos fragmentado de gran tamaño, el primer fragmento contiene un encabezado PPP y un encabezado MLPPP, pero los fragmentos consecutivos contienen solo un encabezado MLPPP.

   Las encapsulaciones PPP y MLPPP agregan el siguiente número de bytes a un paquete:

   - La encapsulación PPP agrega 7 bytes:

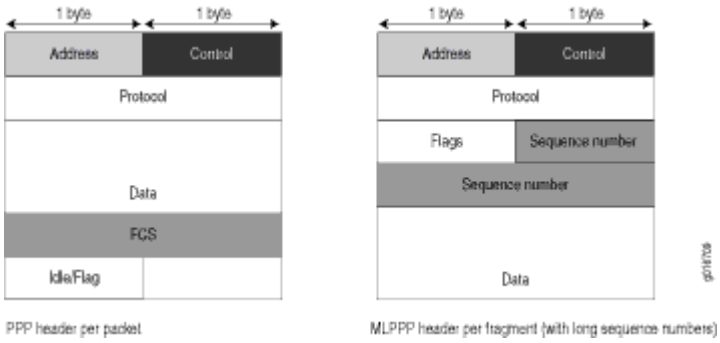
     4 bytes de encabezado + 2 bytes de secuencia de comprobación de tramas (FCS) + 1 byte que está inactivo o contiene una marca

   - La encapsulación MLPPP agrega entre 6 y 8 bytes:

     4 bytes de encabezado PPP+2 a 4 bytes de encabezado multivínculo

   Figura 1 muestra la sobrecarga agregada a los encabezados PPP y MLPPP.

Figura 48: Encabezados PPP y MLPPP



Para los paquetes CRTP, la sobrecarga de encapsulación y el tamaño del paquete son incluso menores que para un paquete LFI. Para obtener más información, consulte Ejemplo: Configuración del protocolo de transporte comprimido en tiempo real.

Tabla 2 muestra la sobrecarga de encapsulación de un paquete de datos y un paquete de voz de 70 bytes cada uno. Después de la encapsulación, el tamaño del paquete de datos es mayor que el tamaño del paquete de voz.

Tabla 172: Sobrecarga de encapsulación PPP y MLPPP

Tipo de paquete	Encapsulación	Tamaño inicial del paquete	Sobrecarga de encapsulación	Tamaño del paquete después de la encapsulación
Paquete de voz (LFI)	PPP	70 bytes	4 + 2 + 1 = 7 bytes	77 bytes
Fragmento de datos (no LFI) con secuencia corta	MLPPP	70 bytes	4 + 2 + 1 + 4 + 2 = 13 bytes	83 bytes
Fragmento de datos (no LFI) con secuencia larga	MLPPP	70 bytes	4 + 2 + 1 + 4 + 4 = 15 bytes	85 bytes

Desde el modo operativo, escriba el comando para mostrar el tamaño del paquete transmitido en cada cola.`show interfaces queue` Divida el número de bytes transmitidos por el número de paquetes para obtener el tamaño de los paquetes y determinar el tipo de encapsulación.

3. Verifique el equilibrio de carga. Desde el modo operativo, introduzca el comando en el paquete multivínculo y sus enlaces constituyentes para confirmar si el equilibrio de carga se realiza en consecuencia en los paquetes.`show interfaces queue`

```
user@R0> show interfaces queue lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                600                  0 pps
    Bytes                :              44800                  0 bps
  Transmitted:
    Packets              :                600                  0 pps
```

```
    Bytes                :              44800                  0 bps
    Tail-dropped packets :                  0                  0 pps
    RED-dropped packets  :                  0                  0 pps
    …
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                  0 pps
    Bytes                :                  0                  0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                400                  0 pps
    Bytes                :              61344                  0 bps
  Transmitted:
    Packets              :                400                  0 pps
    Bytes                :              61344                  0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                  0                  0 pps
    Bytes                :                  0                  0 bps
 …
```

```
user@R0> show interfaces queue se-1/0/0
Physical interface: se-1/0/0, Enabled, Physical link is Up
  Interface index: 141, SNMP ifIndex: 35
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
  Transmitted:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
   ...
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                 0 pps
    Bytes                :                  0                 0 bps
  …
```

```
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                100                 0 pps
    Bytes                :              15272                 0 bps
  Transmitted:
    Packets              :                100                 0 pps
    Bytes                :              15272                 0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                 19                 0 pps
    Bytes                :                247                 0 bps
  Transmitted:
    Packets              :                 19                 0 pps
    Bytes                :                247                 0 bps
    …
```

```
user@R0> show interfaces queue se-1/0/1
Physical interface: se-1/0/1, Enabled, Physical link is Up
  Interface index: 142, SNMP ifIndex: 38
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
  Transmitted:
    Packets              :                350                 0 pps
    Bytes                :              24350                 0 bps
    …
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets              :                  0                 0 pps
    Bytes                :                  0                 0 bps
  …
Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets              :                300                 0 pps
    Bytes                :              45672                 0 bps
  Transmitted:
    Packets              :                300                 0 pps
```

```
    Bytes                :              45672                 0 bps
    …
Queue: 3, Forwarding classes: NC
  Queued:
    Packets              :                 18                 0 pps
    Bytes                :                234                 0 bps
  Transmitted:
    Packets              :                 18                 0 pps
    Bytes                :                234                 0 bps
```

: el resultado de estos comandos muestra los paquetes transmitidos y en cola en cada cola de la interfaz de servicios de vínculo y sus vínculos constituyentes. muestra un resumen de estos valores.`Meaning`Tabla 3 (Dado que el número de paquetes transmitidos es igual al número de paquetes en cola en todos los vínculos, esta tabla muestra sólo los paquetes en cola).

Tabla 173: Número de paquetes transmitidos en una cola

Paquetes en cola	Paquete lsq-0/0/0.0	Enlace constituyente se-1/0/0	Enlace constituyente se-1/0/1	Explicación
Paquetes en Q0	600	350	350	El número total de paquetes que transitan por los vínculos constituyentes (350+350 = 700) superó el número de paquetes en cola (600) en el paquete multivínculo.
Paquetes en Q2	400	100	300	El número total de paquetes que transitan por los vínculos constituyentes es igual al número de paquetes del paquete.
Paquetes en Q3	0	19	18	Los paquetes que transitan Q3 de los enlaces constituyentes son para mensajes keepalive intercambiados entre enlaces constituyentes. Por lo tanto, no se contaron paquetes en Q3 del paquete.

En el paquete multivínculo, compruebe lo siguiente:

- El número de paquetes en cola coincide con el número transmitido. Si los números coinciden, no se descartó ningún paquete. Si se ponían en cola más paquetes de los que se transmitían, los paquetes se descartaban porque el búfer era demasiado pequeño. El tamaño del búfer en los vínculos constituyentes controla la congestión en la etapa de salida. Para corregir este problema, aumente el tamaño del búfer en los vínculos constituyentes.

- El número de paquetes que transitan Q0 (600) coincide con el número de paquetes de datos grandes y pequeños recibidos (100+500) en el paquete multivínculo. Si los números coinciden, todos los paquetes de datos transitaron correctamente Q0.

- El número de paquetes que transitan Q2 en el paquete multivínculo (400) coincide con el número de paquetes de voz recibidos en el paquete multivínculo. Si los números coinciden, todos los paquetes LFI de voz transitaron correctamente Q2.

En los vínculos constituyentes, compruebe lo siguiente:

- El número total de paquetes que transitan Q0 (350+350) coincide con el número de paquetes de datos y fragmentos de datos (500+200). Si los números coinciden, todos los paquetes de datos después de la fragmentación transitaron correctamente Q0 de los enlaces constituyentes.

  Los paquetes transitaron por ambos enlaces constituyentes, lo que indica que el equilibrio de carga se realizó correctamente en paquetes que no eran LFI.

- El número total de paquetes que transitan Q2 (300+100) en los enlaces constituyentes coincide con el número de paquetes de voz recibidos (400) en el paquete multivínculo. Si los números coinciden, todos los paquetes LFI de voz transitaron correctamente Q2.

  Paquetes LFI desde el puerto de origen transitados y paquetes LFI desde el puerto de origen transitados.`100se-1/0/0200se-1/0/1` Por lo tanto, todos los paquetes LFI (Q2) se cifraron en función del puerto de origen y transitaron correctamente ambos enlaces constituyentes.

`Corrective Action`: si los paquetes transitaron solo un vínculo, siga estos pasos para resolver el problema:

1. Determine si el vínculo físico está (operativo) o (no disponible).`updown` Un vínculo no disponible indica un problema con el PIM, el puerto de interfaz o la conexión física (errores de capa de enlace). Si el vínculo está operativo, vaya al paso siguiente.

2. Compruebe que los clasificadores estén definidos correctamente para los paquetes que no son LFI. Asegúrese de que los paquetes que no sean LFI no estén configurados para ponerse en cola en Q2. Todos los paquetes en cola para Q2 se tratan como paquetes LFI.

3. Compruebe que al menos uno de los siguientes valores es diferente en los paquetes LFI: dirección de origen, dirección de destino, protocolo IP, puerto de origen o puerto de destino. Si se configuran los mismos valores para todos los paquetes LFI, todos los paquetes se cifran al mismo flujo y transitan por el mismo vínculo.

4. Utilice los resultados para verificar el equilibrio de carga.

Determinar por qué se dejan caer paquetes en un PVC entre un dispositivo de Juniper Networks y un dispositivo de terceros

in this section

- Problema | 1583
- Solución | 1583

Problema

Description

Está configurando un circuito virtual permanente (PVC) entre interfaces T1, E1, T3 o E3 en un dispositivo de Juniper Networks y un dispositivo de terceros, y los paquetes se descartan y se produce un error en el ping.

Solución

Si el dispositivo de terceros no tiene la misma compatibilidad con FRF.12 que el dispositivo de Juniper Networks o admite FRF.12 de otra manera, la interfaz del dispositivo de Juniper Networks en el PVC podría descartar un paquete fragmentado que contenga encabezados FRF.12 y contarlo como un "descarte vigilado".

Como solución alternativa, configure paquetes multivínculo en ambos pares y configure umbrales de fragmentación en los paquetes multivínculo.

Solución de problemas de las políticas de seguridad

in this section

- Sincronización de políticas entre el motor de enrutamiento y el motor de reenvío de paquetes | 1584
- Comprobación de un error de confirmación de política de seguridad | 1585
- Comprobación de una confirmación de política de seguridad | 1586

- Depurar búsqueda de directivas | 1587

Sincronización de políticas entre el motor de enrutamiento y el motor de reenvío de paquetes

in this section

- Problema | 1584
- Solución | 1585

Problema

Description

Las políticas de seguridad se almacenan en el motor de enrutamiento y en el motor de reenvío de paquetes. Las políticas de seguridad se insertan desde el motor de enrutamiento al motor de reenvío de paquetes cuando se confirman las configuraciones. Si las políticas de seguridad del motor de enrutamiento no están sincronizadas con el motor de reenvío de paquetes, se produce un error en la confirmación de una configuración. Se pueden generar archivos de volcado de núcleo si se intenta la confirmación repetidamente. La falta de sincronización puede deberse a:

- Un mensaje de política del motor de enrutamiento al motor de reenvío de paquetes se pierde en tránsito.
- Un error con el motor de enrutamiento, como un UID de directiva reutilizado.

Entorno

Las directivas del motor de enrutamiento y del motor de reenvío de paquetes deben estar sincronizadas para que se confirme la configuración. Sin embargo, en determinadas circunstancias, es posible que las directivas del motor de enrutamiento y del motor de reenvío de paquetes no estén sincronizadas, lo que provoca un error en la confirmación.

Síntomas

Cuando se modifican las configuraciones de directiva y las directivas no están sincronizadas, aparece el siguiente mensaje de error: `error: Warning: policy might be out of sync between RE and PFE <SPU-name(s)> Please request security policies check/resync.`

Solución

Use el comando para mostrar el valor de suma de comprobación de la directiva de seguridad y use el comando para sincronizar la configuración de las directivas de seguridad en el motor de enrutamiento y el motor de reenvío de paquetes, si las directivas de seguridad no están sincronizadas.`show security policies checksumrequest security policies resync`

SEE ALSO

> *show security policies checksum*
>
> *request security policies check*
>
> *request security policies resync*

Comprobación de un error de confirmación de política de seguridad

in this section

- Problema | **1585**
- Solución | **1586**

Problema

Description

La mayoría de los errores de configuración de directivas se producen durante una confirmación o un tiempo de ejecución.

Los errores de confirmación se notifican directamente en la CLI cuando se ejecuta el comando de la CLI en modo de configuración.**commit-check** Estos errores son errores de configuración y no puede confirmar la configuración sin corregirlos.

Solución

Para corregir estos errores, haga lo siguiente:

1. Revise los datos de configuración.
2. Abra el archivo /var/log/nsd_chk_only. Este archivo se sobrescribe cada vez que se realiza una comprobación de confirmación y contiene información detallada sobre el error.

Comprobación de una confirmación de política de seguridad

in this section

- Problema | **1586**
- Solución | **1586**

Problema

Description

Al realizar una confirmación de configuración de directiva, si observa que el comportamiento del sistema es incorrecto, siga estos pasos para solucionar este problema:

Solución

1. Comandos operativos : ejecute los comandos operativos para las políticas de seguridad y compruebe que la información que se muestra en el resultado es coherente con lo que esperaba.**show** De lo contrario, la configuración debe cambiarse adecuadamente.
2. Traceoptions: defina el comando en la configuración de la política.`traceoptions` Los indicadores bajo esta jerarquía se pueden seleccionar según el análisis del usuario de la salida del comando.`show` Si no puede determinar qué indicador usar, la opción de indicador se puede usar para capturar todos los registros de seguimiento.`all`

```
user@host# set security policies traceoptions <flag all>
```

También puede configurar un nombre de archivo opcional para capturar los registros.

```
user@host# set security policies traceoptions <filename>
```

Si especificó un nombre de archivo en las opciones de seguimiento, puede buscar el archivo de registro en /var/log/<filename> para determinar si se ha notificado algún error en el archivo. (Si no especificó un nombre de archivo, el nombre de archivo predeterminado es eventual). Los mensajes de error indican el lugar del error y la razón apropiada.

Después de configurar las opciones de seguimiento, debe volver a confirmar el cambio de configuración que provocó el comportamiento incorrecto del sistema.

Depurar búsqueda de directivas

in this section

- Problema | **1587**
- Solución | **1587**

Problema

Description

Si tiene la configuración correcta, pero parte del tráfico se ha interrumpido o permitido incorrectamente, puede habilitar el indicador en las traceoptions de las políticas de seguridad.`lookup` La marca registra los seguimientos relacionados con la búsqueda en el archivo de seguimiento.`lookup`

Solución

```
user@host# set security policies traceoptions <flag lookup>
```

12

PART IN COVERPAGE

Instrucciones de configuración y comandos operativos

Descripción general de referencia de la CLI de Junos

Hemos consolidado todos los comandos e instrucciones de configuración de la CLI de Junos en un solo lugar. Obtenga información sobre la sintaxis y las opciones que componen las instrucciones y los comandos, y comprenda los contextos en los que usará estos elementos de CLI en sus configuraciones y operaciones de red.

- Referencia de la CLI de Junos

Haga clic en los vínculos para acceder a Junos OS y a los temas de resumen de comandos y declaración de configuración de Junos OS evolucionado.

- Instrucciones de configuración
- Comandos operativos