

# Resolución de problemas de inestabilidad de puertos en switches Catalyst serie 9000

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Troubleshoot](#)

[Instalación de módulos de red](#)

[Verificación del cable y ambos lados de la conexión](#)

[Verifique la compatibilidad de SFP y SFP+](#)

[Identificación de inestabilidades de puerto](#)

[Comandos Interface Show](#)

[Verificación del estado del cable con Time Domain Reflector \(TDR\)](#)

[Directrices de TDR](#)

[Monitorado óptico digital \(DOM\)](#)

[Cómo habilitar DOM](#)

[Mensajes de Syslog de supervisión óptica digital](#)

[Óptica de Cisco y corrección de errores de reenvío \(FEC\)](#)

[Comandos de Debug](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo identificar, recolectar registros útiles y resolver problemas que pueden ocurrir con las inestabilidades de puerto en los switches Catalyst 9000.

Gentileza de Leonardo Pena Davila

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información de este documento se basa en todos los switches Catalyst serie 9000.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Una inestabilidad de puerto, generalmente conocida como inestabilidad de link, es una situación en la que una interfaz física en el switch sube y baja continuamente. La causa más común suele estar relacionada con un cable no estándar, no compatible o no estándar, con Small Form-Factor Pluggable (SFP) o con otros problemas de sincronización de enlaces. La causa de las aletas de link puede ser intermitente o permanente.

Dado que las inestabilidad de link tienden a ser una interferencia física, este documento explica los pasos para diagnosticar, recopilar registros útiles y resolver problemas que pueden ocurrir con las inestabilidad de puerto en los switches Catalyst 9000.

## Troubleshoot

Hay varias cosas que puede comprobar si tiene acceso físico al switch para asegurarse de que los módulos de red, los cables y los SFP estén correctamente instalados:

### Instalación de módulos de red

La tabla describe las prácticas recomendadas para instalar un módulo de red en un switch Catalyst serie 9000:

Platform	URL
Catalyst 9200 Series Switches	<a href="#">Guía de instalación de hardware de los switches Catalyst serie 9200</a>
Catalyst 9300 Series Switches	<a href="#">Guía de instalación de hardware de los switches Catalyst serie 9300</a>
Catalyst 9400 Series Switches	<a href="#">Guía de Instalación de Hardware de Catalyst 9400 Series Switches</a>
Catalyst 9500 Series Switches	<a href="#">Guía de instalación de hardware de los switches Catalyst serie 9500</a>
Catalyst 9600 Series Switches	<a href="#">Guía de instalación de hardware de switches Catalyst serie 9600</a>

### Verificación del cable y ambos lados de la conexión

Estas tablas describen algunos de los posibles problemas de cable que pueden causar inestabilidad de link.

Causa	Acción de recuperación
Cable en malas condiciones	Cambie el cable que supuestamente está en malas condiciones por un cable buenas condiciones. Busque pines rotos o perdidos en los conectores
Conexiones débiles	Verifique conexiones débiles. A veces, un cable parece estar correctamente colocado, pero no lo está. Desenchufe el cable y vuelva a insertarlo
Patch Panels	Elimine las conexiones del patch panel con fallas. Si es posible, desvíe el patch panel para descartarlo
SFP incorrecto o	Intercambie SFP sospechoso con SFP de funcionalidad comprobada. Verifique

incorrecto (específico de fibra)	soporte de hardware y software para este tipo de SFP
Puerto o puerto de módulo incorrecto	Mover el cable a un puerto conocido en buenas condiciones para resolver problemas con un puerto o un módulo que supuestamente está en malas condiciones
Dispositivo de terminal antiguo o defectuoso	Cambie el teléfono, el altavoz u otro terminal por otro que funcione correctamente o un dispositivo más reciente.
Modo de suspensión del dispositivo	Esta es una "inestabilidad esperada". Preste atención a la marca de tiempo de inestabilidad del puerto para determinar si ocurre rápidamente o de manera intermitente y si la causa es una configuración de suspensión

## Verifique la compatibilidad de SFP y SFP+

La cartera Cisco de las interfaces conectables en funcionamiento ofrece un amplio conjunto de opciones en términos de velocidades, protocolos, alcances y medios de transmisión soportados.

Puede utilizar cualquier combinación de módulos transmisores SFP o SFP+ que admita su dispositivo de switches Catalyst serie 9000. Las únicas restricciones son que cada puerto debe coincidir con las especificaciones de longitud de onda en el otro extremo del cable y que el cable no debe exceder la longitud de cable estipulada para comunicaciones confiables.

Utilice únicamente módulos transceptores SFP de Cisco en su dispositivo Cisco. Cada módulo transceptor SFP o SFP+ admite la función Cisco Quality Identification (ID), que permite que un switch o router de Cisco identifique y valide que Cisco ha certificado y probado el módulo transceptor.

**Sugerencia:** Consulte este enlace para verificar la [Matriz de Compatibilidad de Óptica a Dispositivo de Cisco](#)

## Identificación de inestabilidades de puerto

Use el comando `show logging` para identificar un evento de inestabilidad de link. Este ejemplo muestra un mensaje de registro del sistema de switch parcial para un evento de inestabilidad de link con la interfaz TenGigabitEthernet1/0/40:

```
Switch#show logging | include changed
Aug 17 21:06:08.431 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/40, changed state to down
Aug 17 21:06:39.058 UTC: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to
down
Aug 17 21:06:41.968 UTC: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to up
Aug 17 21:06:42.969 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/40, changed state to up
Aug 17 21:07:20.041 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/40, changed state to down
Aug 17 21:07:21.041 UTC: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to
down
Aug 17 21:07:36.534 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/40, changed state to up
Aug 17 21:08:06.598 UTC: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to up
Aug 17 21:08:07.628 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/40, changed state to down
Aug 17 21:08:08.628 UTC: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to
```

```

down
Aug 17 21:08:10.943 UTC: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/40, changed state to up
Aug 17 21:08:11.944 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet1/0/40, changed state to up

```

**Sugerencia:** Si analiza los registros de mensajes del sistema, debe prestar atención a la **marca de tiempo** de la inestabilidad del puerto, ya que le permite comparar eventos simultáneos en ese puerto específico y validar si se espera o no la aparición de inestabilidad de link (por ejemplo: la configuración de suspensión u otra causa "normal" no necesariamente es un problema).

## Comandos Interface Show

El comando **show interface** le brinda mucha información que ayuda a identificar un posible problema de Capa 1 que causa un evento de inestabilidad de link:

```

Switch#show interfaces tenGigabitEthernet 1/0/40
TenGigabitEthernet1/0/40 is up, line protocol is up (connected)
Hardware is Ten Gigabit Ethernet, address is 00a5.bf9c.29a8 (bia 00a5.bf9c.29a8)
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 10Gb/s, link type is auto, media type is SFP-10GBase-SR  <-- SFP plugged into
the port
  input flow-control is on, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:03, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    670 packets input, 78317 bytes, 0 no buffer
    Received 540 broadcasts (540 multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 540 multicast, 0 pause input
    0 input packets with dribble condition detected
    1766 packets output, 146082 bytes, 0 underruns
0 Output 0 broadcasts (0 multicasts) 0 output errors, 0 collisions, 0 interface resets 0 unknown
protocol drops 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier, 0 pause
output 0 output buffer failures, 0 output buffers swapped out

```

Esta tabla enumera algunos de los contadores del comando **show interface**:

Contador	Problemas y causas comunes que aumentan los contadores de errores
CRC	Un número elevado de CRC suele ser el resultado de colisiones, pero también puede indicar un problema físico (como cableado, SFP, interfaz incorrecta o NIC) o una discordancia dúplex.
Errores de Entrada	Estos incluyen los recuentos ignorados, de fragmentos de tramas minúsculos y gigante falta de buffer, de CRC y de exceso. Otros errores relacionados con la entrada también pueden hacer que aumente el recuento de errores de entrada.

errores de salida Este problema se debe al bajo tamaño de la cola de salida o a la sobresuscripción.

Caídas totales de resultados Las caídas de salida son generalmente el resultado de la sobresuscripción de la interfaz causada por muchos a uno o una transferencia de 10Gbps a 1Gps. Los búferes de interfaz son un recurso limitado y sólo pueden absorber una ráfaga hasta un punto después del cual los paquetes comienzan a descartarse. Los búferes se pueden ajustar para dar un poco de amortiguación, pero no puede garantizar un escenario de caída de salida cero.

Caídas de protocolo desconocidas Las caídas de protocolo desconocidas normalmente se descartan porque la interfaz de salida no se recibe estos paquetes no está configurada para este tipo de protocolo, o puede ser un cualquier protocolo que el switch no reconozca. Por ejemplo, si tiene dos switches conectados y inhabilita el CDP en una interfaz de switch, esto resulta en caídas de protocolo desconocidas en esa interfaz. Los paquetes CDP ya no se reconocen, y se descartan.

El comando **history** permite que una interfaz mantenga el historial de uso en un formato gráfico similar al historial de la CPU. Este historial se puede mantener como bit por segundo (bps) o como paquetes por segundo (pps), como puede ver en este ejemplo:

```
Switch(config-if)#history ?  
  bps Maintain history in bits/second  
  pps Maintain history in packets/second
```

Junto con la velocidad, el usuario puede monitorear varios contadores de interfaz:

```
Switch(config-if)#history [bps|pps] ?  
  all Include all counters  
  babbles Include ethernet output babbles - Babbl  
  crcs Include CRCs - CRCs  
  deferred Include ethernet output deferred - Defer  
  dribbles Include dribbles - Dribl  
  excessive-collisions Include ethernet excessive output collisions -  
  ExCol  
  flushes Include flushes - Flush  
  frame-errors Include frame errors - FrErr  
  giants Include giants - Giant  
  ignored Include ignored - Ignor  
  input-broadcasts Include input broadcasts - iBcst  
  input-drops Include input drops - iDrop  
  input-errors Include input errors - iErr  
  interface-resets Include interface resets - IRset  
  late-collisions Include ethernet late output collisions - LtCol  
  lost-carrier Include ethernet output lost carrier - LstCr  
  multi-collisions Include ethernet multiple output collisions -  
  MlCol  
  multicast Include ethernet input multicast - MlCst  
  no-carrier Include ethernet output no-carrier - NoCarr  
  output-broadcasts Include output broadcasts - oBcst  
  output-buffer-failures Include output buffer failures - oBufF
```

```

output-buffers-swapped-out Include output buffers swapped out - oBSwO
output-drops Include output drops - oDrop
output-errors Include output errors - oErr
output-no-buffer Include output no buffer - oNoBf
overruns Include overruns - OvrRn
pause-input Include ethernet input pause - PsIn
pause-output Include ethernet output pause - PsOut
runts Include runts - Runts
single-collisions Include ethernet single output collisions - SnCol
throttles Include throttles - Thr1
underruns Include underruns - UndRn
unknown-protocol-drops Include unknown protocol drops - Unkno
watchdog Include ethernet output watchdog - Wtchdg
<cr> <cr>
SW_1(config-if)#

```

Al igual que con el historial de la CPU, hay gráficos de los últimos 60 segundos, los últimos 60 minutos y las últimas 72 horas. Se mantienen gráficos separados para los histogramas de entrada y salida:

```

Switch#sh interfaces gigabitEthernet 1/0/2 history ?
 60min   Display 60 minute histograms only
 60sec   Display 60 second histograms only
 72hour  Display 72 hour histograms only
 all     Display all three histogram intervals
 both    Display both input and output histograms
 input   Display input histograms only
 output  Display output histograms only
 |       Output modifiers

```

```

show interfaces tenGigabitEthernet 1/0/9 history 60sec

```

```

10
 9
 8
 7
 6
 5
 4
 3
 2
 1
0....5....1....1....2....2....3....3....4....4....5....5....6
0 5 0 5 0 5 0 5 0 5 0
TenGigabitEthernet1/0/9 input rate(mbits/sec) (last 60 seconds)

```

```

10
 9
 8
 7
 6

```

```

5
4
3
2
1
0....5....1....1....2....2....3....3....4....4....5....5....6
0 5 0 5 0 5 0 5 0 5 0
TenGigabitEthernet1/0/9 output rate(mbits/sec) (last 60 seconds)

```

Utilice el comando **show controllers ethernet-controller{interface{interface-number}}** para mostrar las estadísticas de contadores de tráfico por interfaz (**Transmitir** y **Recibir**) y de contadores de errores leídas desde el hardware. Utilice la palabra clave **phy** para mostrar los registros internos de la interfaz o la palabra clave **port-info** para mostrar información sobre el ASIC del puerto.

Este es un ejemplo del resultado de **show controllers ethernet-controller** para una interfaz específica:

```

Switch#show controllers ethernet-controller tenGigabitEthernet 2/0/1
Transmit                               TenGigabitEthernet2/0/1                               Receive
 61572 Total bytes                          282909 Total bytes
   0 Unicast frames                          600 Unicast frames
   0 Unicast bytes                          38400 Unicast bytes
  308 Multicast frames                       3163 Multicast frames
61572 Multicast bytes                       244509 Multicast bytes
   0 Broadcast frames                        0 Broadcast frames
   0 Broadcast bytes                         0 Broadcast bytes
   0 System FCS error frames                 0 IpgViolation frames
   0 MacUnderrun frames                      0 MacOverrun frames
   0 Pause frames                           0 Pause frames
   0 Cos 0 Pause frames                      0 Cos 0 Pause frames
   0 Cos 1 Pause frames                      0 Cos 1 Pause frames
   0 Cos 2 Pause frames                      0 Cos 2 Pause frames
   0 Cos 3 Pause frames                      0 Cos 3 Pause frames
   0 Cos 4 Pause frames                      0 Cos 4 Pause frames
   0 Cos 5 Pause frames                      0 Cos 5 Pause frames
   0 Cos 6 Pause frames                      0 Cos 6 Pause frames
   0 Cos 7 Pause frames                      0 Cos 7 Pause frames
   0 Oam frames                              0 OamProcessed frames
   0 Oam frames                              0 OamDropped frames
 193 Minimum size frames                    3646 Minimum size frames
   0 65 to 127 byte frames                   1 65 to 127 byte frames
   0 128 to 255 byte frames                  0 128 to 255 byte frames
 115 256 to 511 byte frames                 116 256 to 511 byte frames
   0 512 to 1023 byte frames                 0 512 to 1023 byte frames
   0 1024 to 1518 byte frames                0 1024 to 1518 byte frames
   0 1519 to 2047 byte frames                0 1519 to 2047 byte frames
   0 2048 to 4095 byte frames                0 2048 to 4095 byte frames
   0 4096 to 8191 byte frames                0 4096 to 8191 byte frames
   0 8192 to 16383 byte frames               0 8192 to 16383 byte frames
   0 16384 to 32767 byte frame               0 16384 to 32767 byte frame
   0 > 32768 byte frames                    0 > 32768 byte frames
   0 Late collision frames                   0 SymbolErr frames           <-- Usually
indicates Layer 1 issues. Large amounts of symbol errors can indicate a bad device, cable, or
hardware.
   0 Excess Defer frames                     0 Collision fragments       <-- If this
counter increments, this is an indication that the ports are configured at half-duplex.
   0 Good (1 coll) frames                    0 ValidUnderSize frames

```

```

0 Good (>1 coll) frames          0 InvalidOverSize frames
0 Deferred frames                0 ValidOverSize frames
0 Gold frames dropped            0 FcsErr frames          <-- Are the result
of collisions at half-duplex, a duplex mismatch, bad hardware (NIC, cable, or port)
0 Gold frames truncated
0 Gold frames successful
0 1 collision frames
0 2 collision frames
0 3 collision frames
0 4 collision frames
0 5 collision frames
0 6 collision frames
0 7 collision frames
0 8 collision frames
0 9 collision frames
0 10 collision frames
0 11 collision frames
0 12 collision frames
0 13 collision frames
0 14 collision frames
0 15 collision frames
0 Excess collision frames

```

LAST UPDATE 22622 msec AGO

Sugerencia: También puede utilizar el comando **show interfaces {interface{interface-number}} controller** para mostrar las estadísticas de transmisión y recepción de *lectura por interfaz del hardware*.

Utilice el comando **show platform pm interface-flaps{interface{interface-number}}** para mostrar el número de veces que una interfaz se ha caído:

Este es un ejemplo del resultado de **show platform pm interface-flaps{interface{interface-number}}** para una interfaz específica:

```
Switch#show platform pm interface-flaps tenGigabitEthernet 2/0/1
```

Field	AdminFields	OperFields
Access Mode	Static	Static
Access Vlan Id	1	0
Voice Vlan Id	4096	0
VLAN Unassigned		0
ExAccess Vlan Id	32767	
Native Vlan Id	1	
Port Mode	dynamic	access
Encapsulation	802.1Q	Native
disl	auto	
Media	unknown	
DTP Nonegotiate	0	0
Port Protected	0	0
Unknown Unicast Blocked	0	0
Unknown Multicast Blocked	0	0
Vepa Enabled	0	0
App interface	0	0
Span Destination	0	
Duplex	auto	full

```

Default Duplex          auto
Speed                  auto          1000
Auto Speed Capable     1              1
No Negotiate           0              0
No Negotiate Capable   1024           1024
Flow Control Receive    ON             ON
Flow Control Send      Off            Off
Jumbo                  0              0
saved_holdqueue_out    0
saved_input_defqcount  2000
Jumbo Size             1500

```

```

Forwarding Vlans : none
Current Pruned Vlans : none
Previous Pruned Vlans : none

```

```
Sw LinkNeg State : LinkStateUp
```

```

No.of LinkDownEvents : 12 <-- Number of times the interface
flapped
XgxsResetOnLinkDown(10GE) :
Time Stamp Last Link Flapped(U) : Aug 19 14:58:00.154 <-- Last time the interface flapped
LastLinkDownDuration(sec) 192 <-- Time in seconds the interface
stayed down during the last flap event
LastLinkUpDuration(sec): 2277 <-- Time in seconds the interface
stayed up before the last flap event

```

Utilice el comando **show idprom{interface{interface-number}}** sin palabras clave para mostrar la información IDPROM de la interfaz específica. Utilícelo con la palabra clave **detail** para mostrar información detallada de IDPROM hexadecimal.

Este es un ejemplo del resultado de **show idprom{interface{interface-number}}** para una interfaz específica. Los valores **High** y **Low Warning|Alarm umbral** que se enumeran en este resultado del comando son los parámetros normales de funcionamiento del transceptor óptico. Estos valores se pueden verificar desde la hoja de datos para la óptica específica. Consulte la [ficha técnica de la óptica de Cisco](#)

```
Switch#show idprom interface Twe1/0/1
```

```

IDPROM for transceiver TwentyFiveGigE1/0/1 :
Description                = SFP or SFP+ optics (type 3)
Transceiver Type:          = GE CWDM 1550 (107)
Product Identifier (PID)   = CWDM-SFP-1550 <--
Vendor Revision            = A
Serial Number (SN)         = XXXXXXXXXX <-- Cisco Serial Number
Vendor Name                = CISCO-FINISAR
Vendor OUI (IEEE company ID) = 00.90.65 (36965)
CLEI code                  = CNTRV14FAB
Cisco part number          = 10-1879-03
Device State                = Enabled.
Date code (yy/mm/dd)       = 14/12/22
Connector type             = LC.
Encoding                    = 8B10B (1)
Nominal bitrate             = OTU-1 (2700 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified
The transceiver type is 107
Link reach for 9u fiber (km) = LR-2(80km) (80)
                             LR-3(80km) (80)
                             ZX(80km) (80)

```

Link reach for 9u fiber (m) = IR-2 (40km) (255)  
 LR-1 (40km) (255)  
 LR-2 (80km) (255)  
 LR-3 (80km) (255)  
 DX (40KM) (255)  
 HX (40km) (255)  
 ZX (80km) (255)  
 VX (100km) (255)

Link reach for 50u fiber (m) = SR (2km) (0)  
 IR-1 (15km) (0)  
 IR-2 (40km) (0)  
 LR-1 (40km) (0)  
 LR-2 (80km) (0)  
 LR-3 (80km) (0)  
 DX (40KM) (0)  
 HX (40km) (0)  
 ZX (80km) (0)  
 VX (100km) (0)  
 1xFC, 2xFC-SM (10km) (0)  
 ESCON-SM (20km) (0)

Link reach for 62.5u fiber (m) = SR (2km) (0)  
 IR-1 (15km) (0)  
 IR-2 (40km) (0)  
 LR-1 (40km) (0)  
 LR-2 (80km) (0)  
 LR-3 (80km) (0)  
 DX (40KM) (0)  
 HX (40km) (0)  
 ZX (80km) (0)  
 VX (100km) (0)  
 1xFC, 2xFC-SM (10km) (0)  
 ESCON-SM (20km) (0)

Nominal laser wavelength = 1550 nm.  
 DWDM wavelength fraction = 1550.0 nm.  
 Supported options = Tx disable  
 Tx fault signal  
 Loss of signal (standard implementation)

Supported enhanced options = Alarms for monitored parameters  
 Diagnostic monitoring = Digital diagnostics supported  
 Diagnostics are externally calibrated  
 Rx power measured is "Average power"

Transceiver temperature operating range = -5 C to 75 C (commercial)  
 Minimum operating temperature = 0 C  
 Maximum operating temperature = 70 C  
**High temperature alarm threshold** = +90.000 C  
**High temperature warning threshold** = +85.000 C  
**Low temperature warning threshold** = +0.000 C  
**Low temperature alarm threshold** = -4.000 C  
**High voltage alarm threshold** = 3600.0 mVolts  
**High voltage warning threshold** = 3500.0 mVolts  
**Low voltage warning threshold** = 3100.0 mVolts  
**Low voltage alarm threshold** = 3000.0 mVolts  
 High laser bias current alarm threshold = 84.000 mAmps  
 High laser bias current warning threshold = 70.000 mAmps  
 Low laser bias current warning threshold = 4.000 mAmps  
 Low laser bias current alarm threshold = 2.000 mAmps  
**High transmit power alarm threshold** = 7.4 dBm  
**High transmit power warning threshold** = 4.0 dBm  
**Low transmit power warning threshold** = -1.7 dBm  
**Low transmit power alarm threshold** = -8.2 dBm  
**High receive power alarm threshold** = -3.0 dBm  
**Low receive power alarm threshold** = -33.0 dBm  
**High receive power warning threshold** = -7.0 dBm  
**Low receive power warning threshold** = -28.2 dBm

External Calibration: bias current slope = 1.000  
External Calibration: bias current offset = 0

**Sugerencia:** asegúrese de que la versión de hardware y software del dispositivo es compatible con la [matriz de compatibilidad de óptica a dispositivo de Cisco](#) instalada en SFP/SFP+

Esta tabla enumera los diversos comandos que se pueden utilizar para resolver problemas de inestabilidad de link:

### Comando

show interfaces counters errors

show interfaces capabilities

show interface transceivers (**fibre/SFP specific**)

show interface link

show interface {interface{*interface-number*}} platform

show controllers ethernet-controller {interface{*interface-number*}} port-info

show controllers ethernet-controller {interface{*interface-number*}} link status detail

show errdisable flap-values

clear counters

clear controllers ethernet-controller

### Propósito

Muestra los contadores de errores de la interfaz

Muestra las capacidades de la interfaz específica

Muestra información acerca de los transceptores ópticos que tienen habilitada supervisión óptica digital (DOM)

Muestra información de nivel de vínculo

Muestra información de la plataforma de interfaz

Muestra información adicional del puerto

Muestra el estado del vínculo

Muestra el número de flaps permitidos ante estado errdisable.

Utilice este comando para poner a cero los contadores de tráfico y de errores, de modo que pueda ver si el problema es sólo temporal si los contadores siguen aumentando.

Utilice este comando para borrar los contadores de transmisión y recepción de hardware.

## Verificación del estado del cable con Time Domain Reflector (TDR)

La función Time Domain Reflectometer (TDR) permite determinar si un cable está ABIERTO o CORTO cuando tiene un fallo. Con TDR, puede verificar el estado de los cables de cobre para los puertos de los switches Catalyst serie 9000. El TDR detecta un fallo de cable con una señal que se envía a través del cable y lee la señal que se refleja hacia atrás. Toda o parte de la señal puede reflejarse de nuevo debido a defectos en el cable

Use el test cable-diagnostics tdr {interface{*interface-number*}} para iniciar la prueba de TDR y, a continuación, use el comando **show cable-diagnostics tdr**{interface-interface-number}.

**Consejo:** Consulte [Verificación del Estado del Puerto y la Conectividad](#) para obtener más detalles

El ejemplo muestra un resultado de la prueba TDR para la interfaz Tw2/0/10:

```
Switch#show cable-diagnostics tdr interface tw2/0/10
```

TDR test last run on: November 05 02:28:43

Interface Speed Local pair Pair length Remote pair Pair status

-----

Tw2/0/10 1000M Pair A 1 +/- 5 meters Pair A Impedance Mismatch

Pair B 1 +/- 5 meters Pair B Impedance Mismatch

Pair C 1 +/- 5 meters Pair C Open

Pair D 3 +/- 5 meters Pair D Open

**Sugerencia:** En los switches Catalyst serie 9300, solo se detectan estos tipos de fallas de cable: **OPEN**, **SHORT** e **IMPEDANCE MISMATCH**. El estado **Normal** se muestra en caso de que el cable se termine correctamente y esto se hace con fines ilustrativos.

## Directrices de TDR

Estas directrices se aplican al uso de TDR:

- No cambie la configuración del puerto mientras se esté ejecutando la prueba TDR.
- Si conecta un puerto durante una prueba de TDR a un puerto habilitado para Auto-MDIX, el resultado de TDR puede ser inválido.
- Si conecta un puerto durante una prueba TDR a un puerto 100BASE-T como el del dispositivo, los pares no utilizados (4-5 y 7-8) se notifican como defectuosos porque el extremo remoto no termina estos pares.
- Debido a las características del cable, debe ejecutar la prueba de TDR varias veces para obtener resultados precisos.
- No cambie el estado del puerto (por ejemplo, quite el cable en el extremo cercano o lejano) porque los resultados pueden ser imprecisos.
- El TDR funciona mejor si el cable de prueba se desconecta del puerto remoto. De lo contrario, puede resultar difícil interpretar los resultados correctamente.
- TDR funciona a través de cuatro cables. En función de las condiciones del cable, el estado puede mostrar que un par está ABIERTO o EN CORTO, mientras que el resto de pares de cables se muestran como defectuosos. Esta operación es aceptable porque puede declarar un cable defectuoso siempre que un par de cables sea OPEN o SHORT.
- El objetivo de TDR es determinar la deficiencia del funcionamiento de un cable en lugar de localizar un cable defectuoso.
- Cuando el TDR localice un cable defectuoso, podrá utilizar una herramienta de diagnóstico de cables fuera de línea para diagnosticar mejor el problema.
- Los resultados de TDR pueden diferir entre ejecuciones en diferentes modelos de switches de Catalyst 9300 Series Switches debido a la diferencia de resolución de las implementaciones de TDR. Cuando esto ocurra, debe consultar la herramienta de diagnóstico del cable fuera de línea.

## Monitorado óptico digital (DOM)

La supervisión óptica digital (DOM) es un estándar del sector diseñado para definir una interfaz digital que permita acceder a parámetros en tiempo real como:

- Temperatura
- Voltaje de alimentación del transceptor
- Corriente de desviación del láser
- Alimentación Tx óptica

- Potencia de Rx óptica

## Cómo habilitar DOM

La tabla enumera los comandos que puede utilizar para activar/desactivar DOM para todos los tipos de transceptores en el sistema:

Pasos	Comando o acción	Propósito
Paso 1	<b>enable</b> <b>Ejemplo:</b> switch>enable	Habilita el modo EXEC físico Ingrese su contraseña si se le pide que lo haga
Paso 2	<b>configure terminal</b> <b>Ejemplo:</b> switch#configure terminal transceiver type all	Ingresa en el modo de configuración global
Paso 3	<b>Ejemplo:</b> switch(config)#transceiver type all control	Ingresa al modo de configuración de tipo de transceptor
Paso 4	<b>Ejemplo:</b> switch(config)#monitoring	Permite supervisar todos los transceptores ópticos.

Utilice el comando **show interfaces {interface{interface-number}} transceiver detail** para mostrar la información del transceptor:

```
Switch#show interfaces hundredGigE 1/0/25 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are calibrated.

High Alarm  High Warn  Low Warn  Low Alarm
      Temperature      Threshold  Threshold  Threshold  Threshold
Port (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)
-----
Hu1/0/25 28.8 75.0 70.0 0.0 -5.0

      High Alarm  High Warn  Low Warn  Low Alarm
      Voltage      Threshold  Threshold  Threshold  Threshold
Port (Volts) (Volts) (Volts) (Volts) (Volts)
-----
Hu1/0/25 3.28 3.63 3.46 3.13 2.97

      High Alarm  High Warn  Low Warn  Low Alarm
      Current      Threshold  Threshold  Threshold  Threshold
Port Lane (milliamperes) (mA) (mA) (mA) (mA)
-----
Hu1/0/25 N/A 6.2 10.0 8.5 3.0 2.6

Optical      High Alarm  High Warn  Low Warn  Low Alarm
      Transmit Power Threshold  Threshold  Threshold  Threshold
Port Lane (dBm) (dBm) (dBm) (dBm) (dBm)
-----
Hu1/0/25 N/A -2.2 1.7 -1.3 -7.3 -11.3
```

Optical		High Alarm	High Warn	Low Warn	Low Alarm
Port Lane	(dBm)	Receive Power	Threshold	Threshold	Threshold
Hu1/0/25	N/A	-16.7	2.0	-1.0	-9.9

**Sugerencia:** para determinar si un transceptor óptico funciona en los niveles de señal adecuados, consulte la [ficha técnica de la óptica de Cisco](#)

## Mensajes de Syslog de supervisión óptica digital

Esta sección describe los mensajes de syslog de violación de umbral más relevantes:

### Niveles de temperatura de cables ópticos SFP

- **Explicación:** Este mensaje de registro se genera cuando la temperatura es baja o excede los valores normales de operación óptica:

```
%SFF8472-3-THRESHOLD_VIOLATION: Te7/3: Temperature high alarm; Operating value: 88.7 C, Threshold value: 74.0 C.
```

```
%SFF8472-3-THRESHOLD_VIOLATION: Fo1/1/1: Temperature low alarm; Operating value: 0.0 C, Threshold value: 35.0 C.
```

### Niveles de voltaje de la óptica SFP

- **Explicación:** Este mensaje de registro se genera cuando el voltaje es bajo o excede los valores normales de funcionamiento óptico:

```
%SFF8472-3-THRESHOLD_VIOLATION: Gi1/1/3: Voltage high warning; Operating value: 3.50 V, Threshold value: 3.50 V.
```

```
%SFF8472-5-THRESHOLD_VIOLATION: Gi1/1: Voltage low alarm; Operating value: 2.70 V, Threshold value: 2.97 V.
```

### Niveles de luz de la óptica SFP

- **Explicación:** Este mensaje de registro se genera cuando la potencia de la luz es baja o excede los valores de operación óptica:

```
%SFF8472-3-THRESHOLD_VIOLATION: Gi1/0/1: Rx power high warning; Operating value: -2.7 dBm, Threshold value: -3.0 dBm.
```

```
%SFF8472-5-THRESHOLD_VIOLATION: Te1/1: Rx power low warning; Operating value: -13.8 dBm, Threshold value: -9.9 dBm.
```

**Sugerencia:** para obtener más información sobre DOM, consulte [Supervisión óptica digital](#)

## Óptica de Cisco y corrección de errores de reenvío (FEC)

FEC es una técnica utilizada para detectar y corregir un determinado número de errores en un flujo de bits y anexa bits redundantes y código de comprobación de errores al bloque de mensajes

antes de la transmisión. Como fabricante de módulos, Cisco se encarga de diseñar nuestros transceptores para que cumplan con las especificaciones. Cuando el transceptor óptico funciona en una plataforma host de Cisco, la FEC se habilita de forma predeterminada en función del tipo de módulo óptico que detecte el software host (consulte esta [tabla descargable](#)). En la gran mayoría de los casos, la implementación de la FEC viene dictada por el estándar del sector que admite el tipo de óptica.

Para ciertas especificaciones personalizadas, las implementaciones de FEC varían. Consulte el documento [Comprensión de FEC y su Implementación en Cisco Optics](#) para obtener información detallada.

El ejemplo muestra cómo configurar FEC y algunas de las opciones disponibles:

```
switch(config-if)#fec?  
  auto Enable FEC Auto-Neg  
  cl108 Enable clause108 with 25G  
  cl174 Enable clause74 with 25G  
  off Turn FEC off
```

Use the **show interface** command to verify FEC configuration:

```
TwentyFiveGigE1/0/13 is up, line protocol is up (connected)  
Hardware is Twenty Five Gigabit Ethernet, address is 3473.2d93.bc8d (bia 3473.2d93.bc8d)  
MTU 9170 bytes, BW 25000000 Kbit/sec, DLY 10 usec,  
reliability 255/255, txload 1/255, rxload 1/255  
Encapsulation ARPA, loopback not set  
Keepalive set (10 sec)  
Full-duplex, 25Gb/s, link type is force-up, media type is SFP-25GBase-SR  
  Fec is auto < -- The configured setting for FEC is displayed here  
input flow-control is on, output flow-control is off  
ARP type: ARPA, ARP Timeout 04:00:00  
--snip--
```

**Nota:** ambos lados de un link deben tener la misma FEC encoding algoritmo habilitado para que el link aparezca.

## Comandos de Debug

Esta tabla enumera los diversos comandos que se pueden utilizar para debug Port Flaps

**Precaución:** Utilice los comandos debug con precaución. Tenga en cuenta que muchos **comandos debug** tienen un impacto en la red activa y solo se recomiendan para su uso en un entorno de laboratorio cuando se reproduce el problema.

;

Comando	Propósito
debug pm	Depuración de Port Manager
debug pm port	Eventos relacionados con los puertos
debug platform pm	Información de depuración del administrador de puertos de plataforma NGWC
debug platform pm l2-control	NGWC L2 Control Infra debug

debug platform pm link-status	Eventos de detección de link de interfaz
debug platform pm pm-vectors	Funciones vectoriales del administrador de puertos
debug condition interface <interface name>	Habilitar debugs selectivamente para una interfaz específica
debug interface state	Estados y transiciones

Este es un ejemplo parcial de salida de ejemplo de la *depuración* comandos enumerados en la tabla:

```
SW_2#sh debugging
PM (platform):
L2 Control Infra debugging is on <-- debug platform pm l2-control
PM Link Status debugging is on <-- debug platform pm link-status
PM Vectors debugging is on <-- debug platform pm pm-vectors
Packet Infra debugs:

Ip Address Port
-----|-----

Port Manager:
Port events debugging is on <-- debug pm port

Condition 1: interface Te1/0/2 (1 flags triggered)
Flags: Te1/0/2

----- Sample output -----

*Aug 25 20:01:05.791: link up/down event : link-down on Te1/0/2
*Aug 25 20:01:05.791: pm_port 1/2: during state access, got event 5(link_down) <-- Link down
event (day/time)
*Aug 25 20:01:05.791: @@@ pm_port 1/2: access -> pagp
*Aug 25 20:01:05.792: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:05.792: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:05.792: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:05.792: IOS-FMAN-PM-DEBUG-PM-VECTORS: Vp Disable: pd=0x7F1E797914B0 dpidx=10
Te1/0/2
*Aug 25 20:01:05.792: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:05.792: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:05.792: Maintains count of VP per Interface:delete, pm_vp_counter[0]: 14,
pm_vp_counter[1]: 14
*Aug 25 20:01:05.792: *** port_modechange: 1/2 mode_none(10)
*Aug 25 20:01:05.792: @@@ pm_port 1/2: pagp -> dtp
*Aug 25 20:01:05.792: stop flap timer : Te1/0/2 pagp
*Aug 25 20:01:05.792: *** port_bndl_stop: 1/2 : inform yes
*Aug 25 20:01:05.792: @@@ pm_port 1/2: dtp -> present
*Aug 25 20:01:05.792: *** port_dtp_stop: 1/2
*Aug 25 20:01:05.792: stop flap timer : Te1/0/2 pagp
*Aug 25 20:01:05.792: stop flap timer : Te1/0/2 dtp
*Aug 25 20:01:05.792: stop flap timer : Te1/0/2 unknown
*Aug 25 20:01:05.792: *** port_linkchange: reason_link_change(3): link_down(0)1/2 <-- State
link change
*Aug 25 20:01:05.792: pm_port 1/2: idle during state present
*Aug 25 20:01:05.792: @@@ pm_port 1/2: present -> link_down <-- State of the link
*Aug 25 20:01:06.791: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/2,
changed state to down
*Aug 25 20:01:07.792: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to down
*Aug 25 20:01:11.098: IOS-FMAN-PM-DEBUG-LINK-STATUS: Received LINKCHANGE in xcvr message, if_id
```

## 10 (TenGigabitEthernet1/0/2)

```
*Aug 25 20:01:11.098: IOS-FMAN-PM-DEBUG-LINK-STATUS: if_id 0xA, if_name Te1/0/2, link up <--
Link became up
*Aug 25 20:01:11.098: link up/down event: link-up on Te1/0/2
*Aug 25 20:01:11.098: pm_port 1/2: during state link_down, got event 4(link_up)
*Aug 25 20:01:11.098: @@@ pm_port 1/2: link_down -> link_up
*Aug 25 20:01:11.098: flap count for link type : Te1/0/2 Linkcnt = 0
*Aug 25 20:01:11.099: pm_port 1/2: idle during state link_up
*Aug 25 20:01:11.099: @@@ pm_port 1/2: link_up -> link_authentication
*Aug 25 20:01:11.099: pm_port 1/2: during state link_authentication, got event 8(authen_disable)
*Aug 25 20:01:11.099: @@@ pm_port 1/2: link_authentication -> link_ready
*Aug 25 20:01:11.099: *** port_linkchange: reason_link_change(3): link_up(1)1/2
*Aug 25 20:01:11.099: pm_port 1/2: idle during state link_ready
*Aug 25 20:01:11.099: @@@ pm_port 1/2: link_ready -> dtp
*Aug 25 20:01:11.099: IOS-FMAN-PM-DEBUG-PM-VECTORS: Set pm vp mode attributes for Te1/0/2 vlan 1
*Aug 25 20:01:11.099: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.099: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.099: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.099: pm_port 1/2: during state dtp, got event 13(dtp_complete)
*Aug 25 20:01:11.099: @@@ pm_port 1/2: dtp -> dtp
*Aug 25 20:01:11.099: IOS-FMAN-PM-DEBUG-PM-VECTORS: Set pm vp mode attributes for Te1/0/2 vlan 1
*Aug 25 20:01:11.099: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.099: DTP flapping: flap count for dtp type: Te1/0/2 Dtpcnt = 0
*Aug 25 20:01:11.099: pm_port 1/2: during state dtp, got event 110(dtp_done)
*Aug 25 20:01:11.099: @@@ pm_port 1/2: dtp -> pre_pagp_may_suspend
*Aug 25 20:01:11.099: pm_port 1/2: idle during state pre_pagp_may_suspend
*Aug 25 20:01:11.099: @@@ pm_port 1/2: pre_pagp_may_suspend -> pagp_may_suspend
*Aug 25 20:01:11.099: pm_port 1/2: during state pagp_may_suspend, got event 33(pagp_continue)
*Aug 25 20:01:11.099: @@@ pm_port 1/2: pagp_may_suspend -> start_pagp
*Aug 25 20:01:11.099: pm_port 1/2: idle during state start_pagp
*Aug 25 20:01:11.099: @@@ pm_port 1/2: start_pagp -> pagp
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Set pm vp mode attributes for Te1/0/2 vlan 1
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: *** port_bndl_start: 1/2
*Aug 25 20:01:11.100: stop flap timer : Te1/0/2 pagp
*Aug 25 20:01:11.100: pm_port 1/2: during state pagp, got event 34(dont_bundle)
*Aug 25 20:01:11.100: @@@ pm_port 1/2: pagp -> pre_post_pagp
*Aug 25 20:01:11.100: pm_port 1/2: idle during state pre_post_pagp
*Aug 25 20:01:11.100: @@@ pm_port 1/2: pre_post_pagp -> post_pagp
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: pm_port 1/2: during state post_pagp, got event 14(dtp_access)
*Aug 25 20:01:11.100: @@@ pm_port 1/2: post_pagp -> access
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Set pm vp mode attributes for Te1/0/2 vlan 1
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.100: Maintains count of VP per Interface:add, pm_vp_counter[0]: 15,
pm_vp_counter[1]: 15
*Aug 25 20:01:11.100: IOS-FMAN-PM-DEBUG-PM-VECTORS: vlan vp enable for port(Te1/0/2) and vlan:1
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: VP ENABLE: vp_pvlan_port_mode:access for
Te1/0/2
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: VP Enable: vp_pvlan_native_vlanId:1 for
Te1/0/2
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.101: *** port_modechange: 1/2 mode_access(1)
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: The operational mode of Te1/0/2 in set all
```

```
vlan is 1
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: vp_pvlan port_mode:access vlan:1 for Te1/0/2
*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: vp_pvlan port_mode:access native_vlan:1 for
Te1/0/2
*Aug 25 20:01:11.102: IOS-FMAN-PM-DEBUG-PM-VECTORS: Success sending PM tdl message
*Aug 25 20:01:13.098: %LINK-3-UPDOWN: Interface TenGigabitEthernet1/0/2, changed state to up
*Aug 25 20:01:14.098: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet1/0/2,
changed state to up
```

## Información Relacionada

[Matriz de compatibilidad de óptica a dispositivo de Cisco](#)

[Ficha técnica de los módulos Cisco SFP para aplicaciones Gigabit Ethernet](#)

[Informe técnico sobre la protección de la inversión de 25 GE y 100 GE para lograr mayores velocidades en las empresas](#)

[Hoja de datos de la solución Cisco CWDM SFP](#)

[Apoyo a la innovación: cómo el Cisco TAC está transformando la documentación y simplificando el autoservicio](#)

[Soporte Técnico y Documentación - Cisco Systems](#)

### ID de falla de funcionamiento de Cisco

### Descripción

ID de bug de Cisco

Intermittent Link Flaps en switches mGig Cat9300 a terminales compatibles mGig

[CSCvu13029](#)

ID de bug de Cisco

Problemas de interoperabilidad Cat9400 mGig con otros dispositivos mGig causan inestabilidad de link

[CSCvt50788](#)

ID de bug de Cisco

CAT9400: Intermittentes de interfaz Mgig con AP Mgig

[CSCvu92432](#)

ID de bug de Cisco

Compatibilidad con autoneg para 100 G/40 G/25 G Cu xcvr

[CSCve65787](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).