

Probleemoplossing voor poortflaps op Catalyst 9000 Series Switches

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Problemen oplossen](#)

[Installatie van netwerkmodules](#)

[Controleer de kabel en beide zijden van de verbinding](#)

[Controleer SFP- en SFP+ compatibiliteit](#)

[Poortflappen identificeren](#)

[Opdrachten voor interfaceweergave](#)

[Controleer de kabelstatus met Time Domain Reflector \(TDR\)](#)

[TDR-richtlijnen](#)

[Digitale optische bewaking \(DOM\)](#)

[DOM inschakelen](#)

[Syslog-berichten voor digitale optische bewaking](#)

[Cisco Optica en voorwaartse foutcorrectie \(FEC\)](#)

[Debug opdrachten](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u nuttige logbestanden kunt identificeren, verzamelen en problemen kunt oplossen die zich met poortflaps op Catalyst 9000 switches kunnen voordoen.

Bijgedragen door Leonardo Pena Davila

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op alle Catalyst 9000 Series switches.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een port flap, meestal een link flap genoemd, is een situatie waarin een fysieke interface op de switch voortdurend omhoog en omlaag gaat. De veel voorkomende oorzaak is meestal gerelateerd aan slechte, niet-ondersteunde of niet-standaard kabel of Small Form-Factor Pluggable (SFP) of andere problemen met linksynchronisatie. De oorzaak van de linkflappen kan intermitterend of permanent zijn.

Aangezien linkflaps meestal een fysieke interferentie zijn, legt dit document de stappen uit om te diagnosticeren, nuttige logbestanden te verzamelen en problemen op te lossen die kunnen optreden met poortflaps op Catalyst 9000 switches.

Problemen oplossen

Er zijn een aantal dingen die u kunt controleren als u fysieke toegang tot de switch hebt om er zeker van te zijn dat de netwerkmodules, kabels en SFP correct zijn geïnstalleerd:

Installatie van netwerkmodules

De tabel beschrijft de best practices voor de installatie van een netwerkmodule in een Catalyst 9000 Series switch:

Platform	URL
Catalyst 9200 Series switches	Catalyst 9200 Series hardwaregids voor Switches
Catalyst 9300 Series switches	Catalyst 9300 Series Switches installatiegids voor hardware
Catalyst 9400 Series switches	Catalyst 9400 Series hardwaregids voor Switches
Catalyst 9500 Series switches	Catalyst 9500 Series hardwaregids voor Switches
Catalyst 9600 Series switches	Catalyst 9600 Series Switches installatiegids voor hardware

Controleer de kabel en beide zijden van de verbinding

In deze tabellen worden enkele mogelijke kabelproblemen beschreven die linkflappen kunnen veroorzaken.

Oorzaak	Terugvorderingsactie
Slechte kabel	Verwissel de slechte kabel met een goed werkende kabel. Zoek gebroken of verloren pinnen op connectors
Losse aansluitingen	Controleer op losse aansluitingen. Soms lijkt een kabel goed te zitten, maar doet niet zo. Haal de kabel uit de aansluiting en plaats deze opnieuw
Patchpanelen	Verhelp slechte aansluitingen op het patchpaneel. Omzeil zo mogelijk het patchpaneel om uit te sluiten dat dit de oorzaak van het probleem is
Slechte of verkeerde SFP (glasvezelspecifiek)	Wissel verdachte SFP met bekende goede SFP. Controleer de hardware- en softwareondersteuning voor dit type SFP

Slechte poort of module	Verplaats de kabel naar een goed werkende poort om problemen met een poort of module te troubleshooten
Slecht of Oud-endpointapparaat	Wisseltelefoon, luidspreker, ander eindpunt met bekend goed apparaat of nieuw apparaat
Apparaatslaapstand	Dit is een "verwachtingsflap". Let op het tijdstempel van de havenflap om te bepalen of het snel of met tussenpozen gebeurt en of een slaapstand de oorzaak is

Controleer SFP- en SFP+ compatibiliteit

De Cisco-portfolio van hot pluggable interfaces biedt een uitgebreide reeks keuzes in termen van snelheden, protocollen, bereiken en ondersteunde transmissiemedia.

U kunt elke combinatie van SFP- of SFP+ transceivermodules gebruiken die door uw Catalyst 9000 Series switches-apparaat wordt ondersteund. De enige beperkingen zijn dat elke haven de golflengtespecificaties op het andere eind van de kabel moet aanpassen en dat de kabel de vastgestelde kabellengte voor betrouwbare mededelingen niet moet overschrijden.

Gebruik alleen Cisco SFP-transceivermodules op uw Cisco-apparaat. Elke SFP- of SFP+ transceivermodule ondersteunt de Cisco Quality Identification (ID)-functie die een Cisco-switch of -router in staat stelt om te identificeren en te valideren dat de transceivermodule door Cisco is gecertificeerd en getest.

Tip: raadpleeg deze link om de [Cisco Optics-to-Device Compatibility Matrix](#) te controleren

Poortflappen identificeren

Gebruik de `show logging` opdracht om een linkflap-gebeurtenis te identificeren. In dit voorbeeld wordt een logboekbericht getoond van een partiële switch voor een link flap-gebeurtenis met de interface TenGigabit Ethernet1/0/40:

```
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
```

Tip: Als u de systeemberichtlogboeken analyseert, moet u aandacht besteden aan de

tijdstempel van de poortflap, omdat het u in staat stelt om gelijktijdige gebeurtenissen op die specifieke poort te vergelijken en te valideren of de link flap voorkomen wordt verwacht (bijvoorbeeld: slaapstand of andere "normale" kwestie niet noodzakelijk een probleem).

Opdrachten voor interfaceweergave

Het bevel van de **showinterface** geeft u heel wat informatie die helpt om een mogelijke Layer 1 kwestie te identificeren die een gebeurtenis van de verbindingsflap veroorzaakt:

```
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
```

Deze lijst maakt een lijst van enkele tellers van het bevel van de **showinterface**:

Teller	Problemen en gemeenschappelijke oorzaken die foutentellers vergroten
CRC	Een groot aantal CRC's is gewoonlijk het resultaat van botsingen maar kan ook wijzen een fysiek probleem (zoals bekabeling, SFP, slechte interface of NIC) of een duplexmismatch.
Input errors	Dit omvat de tellingen voor Runts, Giants, no buffer, CRC, frame, overrun en ignored. Andere input-gerelateerde fouten kunnen er ook toe leiden dat het aantal invoerfouten toeneemt.
output errors	Dit probleem is te wijten aan de lage grootte van de outputrij of wanneer er overtekening
Totale output dalingen	Output druppels zijn over het algemeen het resultaat van interface-overtekening die do velen aan één of 10 Gbps aan 1 Gbps overdracht wordt veroorzaakt. De buffers van de interface zijn een beperkt middel en kunnen een uitbarsting tot een punt slechts absorber

waarna beginnen de pakketten te dalen. Buffers kunnen worden afgestemd om wat kus te geven, maar het kan geen nuloutput drop scenario garanderen.

Onbekende protocoldruppels worden normaal gesproken verbroken omdat de interface deze pakketten worden ontvangen niet voor dit type protocol is geconfigureerd of omdat een willekeurig protocol kan zijn dat de switch niet herkent. Als u bijvoorbeeld twee switch-interfaces hebt aangesloten en u CDP uitschakelt op één switch-interface, resulteert dit in onbekende protocoldruppels op die interface. De CDP-pakketten worden niet meer herkend en worden afgewezen.

Met de opdracht **history** kan een interface gebruiksgeschiedenis in een grafische indeling behouden die vergelijkbaar is met de CPU-geschiedenis. Deze geschiedenis kan worden gehandhaafd als bit per seconde (bps) of pakketten per seconde (pps) zoals u in dit voorbeeld kunt zien:

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

Samen met de snelheid kan de gebruiker verschillende interfacetellers bewaken:

```
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 - Thrtl
underruns Include underruns - UndRn
unknown-protocol-drops Include unknown protocol drops - Unkno
watchdog Include ethernet output watchdog - Wtchdg
<cr> <cr>
SW_1(config-if)#

```

Net als bij de CPU-geschiedenis zijn er grafieken van de afgelopen 60 seconden, de laatste 60 minuten en de laatste 72 uur. Er worden afzonderlijke grafieken bijgehouden voor invoer- en uitvoerhistogrammen:

```

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)

```

Gebruik de **show controllers ethernetcontroller{interface{interface-nummer}}** om per-interface (**Transmissie** en **Ontvang**) te tonen van de verkeerstellers en fouten tellerstatistieken die van de hardware worden gelezen. Gebruik het **phy**-trefwoord om de interne interfaceregisters of het **port-info**-trefwoord weer te geven om informatie over de poort ASIC weer te geven.

Dit is een voorbeeld van output van de **show controllers ethernetcontroller** voor een specifieke interface:

```

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

Tip: U kunt ook de opdracht van de show interfaces {interface{interface-number}} controller gebruiken om de per-interface verzend en ontvang statistieken die van de hardware worden gelezen weer te geven.

Gebruik het **showplatform pm interface-flaps{interface{interface-nummer}}** om het aantal keren weer te geven dat een interface minder geworden is:

Dit is een voorbeeld van output van het **showplatform pm interface-flaps{interface{interface-nummer}}** voor een specifieke interface:

```
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

```

Gebruik de **show idprom{interface{interface-nummer}}** opdracht zonder trefwoorden om de IDPROM-informatie voor de specifieke interface weer te geven. Gebruik dit woord met het **detailwoord** om gedetailleerde hexadecimale IDPROM-informatie weer te geven.

Dit is een voorbeeld van uitvoer van de **show idprom{interface{interface-nummer}}** voor een specifieke interface. De waarden voor **hoge en lage waarschuwing|alarmdrempels** die in deze opdrachtoutput worden vermeld, zijn de normale optische transceiverparameters. Deze waarden kunnen worden geverifieerd aan de hand van het gegevensblad voor de specifieke optische stof. Raadpleeg het [Cisco Optics-gegevensblad](#)

```
Switch#show idprom interface Twel1/0/1
```

```

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

Tip:Zorg ervoor dat de hardware- en softwareversie van het apparaat compatibel is met de SFP/SFP+ geïnstalleerde [Cisco Optics-to-Device Compatibility Matrix](#)

Deze tabel geeft een overzicht van de verschillende opdrachten die kunnen worden gebruikt voor probleemoplossing bij koppelingen:

Opdracht

toon interfaces tellerfouten

toon interfacemogelijkheden

toon interfacetransceivers (**glasvezel/SFP-specifiek**)

interfacekaart weergeven

toon interface {interface{*interface-number*} platform

toon controllers ethernetcontroller {interface{*interface-number*} poort-info

toon controllers Ethernet-controller {interface{*interface-number*}} details van de verbindingstatus

waarden van de flap-waarde voor uitschakelen weergeven

clear counters

duidelijke controllers Ethernet-controller

Doel

Toont de interfacefouttellers

Toont de mogelijkheden van de specifieke interface

Hier wordt informatie weergegeven over de optische transceivers waarvoor digitale optische bewaking (DOM) is ingeschakeld

Informatie over koppelingsniveau weergegeven

Informatie over interfaceplatform weergegeven

Hier wordt aanvullende poortinformatie weergegeven

Toont koppelingsstatus

Toont het aantal flaps die toegestaan zijn om te voorkomen voor te komen vóór de erreless status.

Gebruik deze opdracht om het verkeer en de foutentellers op nul te zetten, zodat u kunt vaststellen of het probleem alleen tijdelijk is of dat de fouten blijven toenemen.

Gebruik deze opdracht om de hardware-temperaturen voor verzending en ontvangst te verwijderen

Controleer de kabelstatus met Time Domain Reflector (TDR)

Met de functie Time Domain Reflectometer (TDR) kunt u bepalen of een kabel OPEN of SHORT is wanneer er een fout is. Met TDR kunt u de status van koperkabels controleren voor de poorten op de Catalyst 9000 Series Switches . TDR detecteert een kabelfout met een signaal dat door de kabel wordt verzonden en leest het signaal dat terug wordt weerspiegeld. Het signaal of een deel ervan kan teruggekaatst worden ten gevolge van defecten in de kabel

Gebruik de test kabel-diagnostiek `tdr {interface{interface-number}}` om de TDR test te beginnen, gebruik dan de **show kabel-diagnostiek tdr{*interface-number*}**.

Tip: Raadpleeg de [status en connectiviteit van de controlepoort](#) voor meer informatie

In het voorbeeld wordt een TDR-testresultaat getoond voor interface 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
```

Tip: op Catalyst 9300 Series Switches worden alleen deze typen kabelfouten gedetecteerd - **OPEN, SHORT** en **IMPEDANCE MISMATCH**. De **normale** status wordt weergegeven als de kabel op de juiste manier wordt afgesloten. Dit wordt ter illustratie gedaan.

TDR-richtlijnen

Deze richtsnoeren zijn van toepassing op het gebruik van TDR:

- Verander de poortconfiguratie niet terwijl de TDR-test wordt uitgevoerd.
- Als u een poort tijdens een TDR-test aansluit op een Auto-MDIX enabled-poort, kan het TDR-resultaat ongeldig zijn.
- Als u een poort tijdens een TDR-test aansluit op een 100BASE-T poort zoals die op het apparaat, worden de ongebruikte paren (4-5 en 7-8) als defect gerapporteerd omdat het externe uiteinde deze paren niet afsluit.
- Wegens kabelkenmerken, moet u de TDR test meerdere malen uitvoeren om nauwkeurige resultaten te krijgen.
- Wijzig de poortstatus niet (verwijder bijvoorbeeld de kabel aan het nabije of verre eind) omdat de resultaten onnauwkeurig kunnen zijn.
- TDR werkt het beste als de testkabel is losgekoppeld van de externe poort. Anders kan het voor u moeilijk zijn de resultaten correct te interpreteren.
- TDR werkt via vier bedradingen. Gebaseerd op de kabelvoorwaarden, kan de status tonen dat één paar OPEN of KORT is terwijl alle andere draadparen defect tonen. Deze handeling is acceptabel omdat u een kabel defect kunt verklaren op voorwaarde dat één paar draden of OPEN of KORT is.
- De bedoeling van TDR is te bepalen hoe slecht een kabel werkt in plaats van een defecte kabel te vinden.
- Wanneer TDR een defecte kabel lokaliseert, kunt u nog steeds een offline kabeldiagnosetool gebruiken om het probleem beter te diagnosticeren.
- TDR-resultaten kunnen verschillen tussen looppas op verschillende switch-modellen van Catalyst 9300 Series Switches vanwege het resolutieverschil van TDR-implementaties. Wanneer dit gebeurt, moet u verwijzen naar een offline kabel diagnosetool.

Digitale optische bewaking (DOM)

Digital Optical Monitoring (DOM) is een industriebrede norm, bedoeld om een digitale interface te definiëren voor toegang tot realtime parameters zoals:

- Temperatuur
- Voedingsspanning voor transceiver
- Laserbias-stroom
- Optische TX-voeding
- Optische RX-voeding

DOM inschakelen

In de tabel staan de opdrachten die u kunt gebruiken om DOM in/uit te schakelen voor alle

transceivertypen in het systeem:

Werkwijze	Opdracht of handeling	Doel
Stap 1	toelaten Voorbeeld: switch>inschakelen	Schakelt de fysieke EXEC-modus in Voer uw wachtwoord in indien dit wordt gevraagd
Stap 2	configureer terminal Voorbeeld: switch #configure terminal transceivertype alles	Hiermee gaat u de globale configuratiemodus in
Stap 3	Voorbeeld: switch(configuratie)#transceiver type alles toezicht	Hiermee gaat u de configuratiemodus van het transceivertype in
Stap 4	Voorbeeld: switch (configuratie)#monitoring	Maakt bewaking van alle optische transceivers mogelijk.

Gebruik de **show interfaces {interface{interface-number} transceiver detail** opdracht om transceiver informatie te tonen:

```
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
      Receive Power  Threshold  Threshold  Threshold  Threshold
Port Lane (dBm) (dBm) (dBm) (dBm) (dBm)
-----
```

Tip: Raadpleeg het [Cisco Optics-gegevensblad](#) om te bepalen of een optische transceiver op de juiste signaalniveaus werkt

Syslog-berichten voor digitale optische bewaking

In deze sectie worden de meest relevante syslog-berichten voor drempelwaardeoverschrijding beschreven:

Temperatuurniveaus van SFP-optica

- **Uitleg:** Deze logberichten worden gegenereerd wanneer de temperatuur laag is of de normale optische bedrijfswaarden overschrijdt:

```
%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.
```

Spanningsniveaus voor SFP-glasvezelkabels

- **Uitleg:** Deze logberichten worden gegenereerd wanneer het voltage laag is of de normale optische bedrijfswaarden overschrijdt:

```
%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.
```

Lichtniveaus voor SFP-optica

- **Uitleg:** Deze logberichten worden gegenereerd wanneer de lichtstroom laag is of de optische bedrijfswaarden overschrijdt:

```
%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.
```

Tip: voor meer informatie over DOM zie [Digitale optische bewaking](#)

Cisco Optica en voorwaartse foutcorrectie (FEC)

FEC is een techniek die wordt gebruikt om een bepaald aantal fouten in een bitstream te detecteren en te corrigeren en voegt redundante bits en foutcontrolecodes toe aan het berichtblok vóór de transmissie. Als modulefabrikant zorgt Cisco ervoor dat onze transceivers worden ontworpen om aan de specificaties te voldoen. Wanneer de optische transceiver in een Cisco-hostplatform wordt gebruikt, wordt de FEC standaard ingeschakeld op basis van het type optische module dat door de hostsoftware wordt gedetecteerd (zie deze [downloadbare tabel](#)). In de

overgrote meerderheid van de gevallen wordt de FEC implementatie bepaald door de industriestandaard die het optische type ondersteunt.

Voor bepaalde douanespecificaties, variëren de implementaties van FEC. Raadpleeg [Inzicht in FEC en de implementatie ervan in Cisco Optics](#)-document voor meer informatie.

In het voorbeeld wordt getoond hoe FEC en een aantal van de beschikbare opties moeten worden geconfigureerd:

```
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--
```

Opmerking: beide zijden van een link moeten dezelfde FEC hebben encoding algoritme ingeschakeld voor de link.

Debug opdrachten

Deze tabel toont de verschillende opdrachten die kunnen worden gebruikt om poortflaps te debuggen

Waarschuwing: Gebruik de debug commando's voorzichtig. Houd er rekening mee dat veel **debug commando's** een impact hebben op het live netwerk en dat ze alleen aangeraden worden om te gebruiken in een lab omgeving wanneer het probleem gereproduceerd wordt.

;

Opdracht	Doel
debug pm	Poortbeheer, debuggen
debug pm-poort	Poortgerelateerde gebeurtenissen
debug platform pm	Debuginformatie voor NGWC Platform Port Mana
debug platform pm l2-control	debug van NGWC L2 Control Info
debug platform pm link-status	Gebeurtenissen voor interfacekaartdetectie
debug platform pm pm-vectoren	Poortbeheer Vectorfuncties

debug voorwaarde interface <naam interface>

Schakel debugs selectief in voor specifieke interface

debug interfacestatus

Statusovergangen

Dit is een voorbeeld van een deelsteekproef van de **debug** opdrachten die in de tabel worden vermeld:

```
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 Tel/0/2 (1 flags triggered)
```

```
Flags: Tel/0/2
```

```
----- Sample output -----
```

```
*Aug 25 20:01:05.791: link up/down event : link-down on Tel/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
```

```
Tel/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 : Tel/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 : Tel/0/2 pagp
```

```
*Aug 25 20:01:05.792: stop flap timer : Tel/0/2 dtp
```

```
*Aug 25 20:01:05.792: stop flap timer : Tel/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 Tel/0/2, link up <-- Link became up
```


***Aug 25 20:01:11.098: link up/down event: link-up on Tel1/0/2**

*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 : Tel1/0/2 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 Tel1/0/2 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 Tel1/0/2 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: Tel1/0/2 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 Tel1/0/2 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 : Tel1/0/2 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 Tel1/0/2 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(Tel1/0/2) and vlan:1

*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: VP ENABLE: vp_pvlan_port_mode:access for
Tel1/0/2

*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: VP Enable: vp_pvlan_native_vlanId:1 for
Tel1/0/2

*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 Tel1/0/2 in set all
vlans 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 Tel1/0/2

*Aug 25 20:01:11.101: IOS-FMAN-PM-DEBUG-PM-VECTORS: vp_pvlan port_mode:access native_vlan:1 for

Tel/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

Gerelateerde informatie

[Cisco-compatibiliteitstabel voor glasvezel-naar-apparaat](#)

[Cisco SFP-modules voor Gigabit Ethernet-toepassingen - gegevensblad](#)

[25 GE en 100 GE - Hogere snelheden in ondernemingen mogelijk maken met Investment Protection White Paper](#)

[Gegevensblad voor Cisco CWDM SFP-oplossing](#)

[Ondersteuning voor innovatie: hoe Cisco TAC documentatie transformeert en zelfservice vereenvoudigt](#)

[Technische ondersteuning en documentatie – Cisco Systems](#)

Cisco bug-ID

Cisco bug-id [CSCvu13029](#)

Cisco fout-id [CSCvt50788](#)

Cisco bug-id [CSCvu92432](#)

Cisco fout-id [CSCve65787](#)

Beschrijving

Intermittent Link Flaps op mGig Cat9300 switches naar mGig geschikt end Cat9400 mGig interop problemen met andere mGig apparaten veroorzaakt linkflappen

CAT9400: Mgig interface Flaps met Mgid AP's

Automatische ondersteuning voor 100G/40G/25G Cu XCVR

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.