Risoluzione dei problemi di flap delle porte sugli switch Catalyst serie 9000

Sommario

Introduzione

In questo documento viene descritto come identificare, raccogliere log utili e risolvere i problemi che possono verificarsi con i port flap sugli switch Catalyst 9000.

Contributo di Leonardo Pena Davila

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, sono stati usati tutti gli switch Catalyst serie 9000.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il link flap è una situazione in cui l'interfaccia fisica dello switch continua a funzionare in senso verticale e verticale. La causa comune è in genere correlata a un cavo non valido, non supportato o non standard, a un Small Form-Factor Pluggable (SFP) o ad altri problemi di sincronizzazione del collegamento. I link flap possono essere intermittenti o permanenti.

Poiché i link flap tendono a rappresentare un'interferenza fisica, in questo documento viene spiegato come diagnosticare, raccogliere log utili e risolvere i problemi che possono verificarsi con i link flap sugli switch Catalyst 9000.

Risoluzione dei problemi

Se si dispone di accesso fisico allo switch per assicurarsi che i moduli di rete, i cavi e gli SFP siano installati correttamente, è possibile verificare quanto segue:

Installazione di moduli di rete

Nella tabella vengono descritte le best practice da adottare per installare un modulo di rete in uno switch Catalyst serie 9000:

Piattaforma	URL
Switch Catalyst serie 9200	Switch Catalyst serie 9200 - Guida all'installazion dell'hardware
Switch Catalyst serie 9300	Switch Catalyst serie 9300 - Guida all'installazion dell'hardware
Switch Catalyst serie 9400	Switch Catalyst serie 9400 - Guida all'installazion dell'hardware
Switch Catalyst serie 9500	Switch Catalyst serie 9500 - Guida all'installazion dell'hardware
Switch Catalyst serie 9600	Switch Catalyst serie 9600 - Guida alle installazio hardware

Verifica del cavo e di entrambi i lati della connessione

Nelle tabelle vengono descritti alcuni dei possibili problemi dei cavi che possono causare link flap.

Causa	Azione di ripristino
Cavo difettoso	Sostituire il cavo sospetto con un cavo sicuramente funzionante. Cerca pin rot persi nei connettori
Collegamenti allentati	Controllare che non vi siano collegamenti allentati. A volte un cavo sembra es inserito correttamente, ma non lo è. Scollegare il cavo e reinserirlo
Patch panel	Eliminare i collegamenti difettosi del patch panel. Se possibile, escludere il pa panel
SFP non valido o errato (specifico per fibra)	Sostituire l'SFP sospetto con l'SFP riconosciuto valido. Verificare il supporto hardware e software per questo tipo di SFP
Porta o porta del modulo	Spostare il cavo su una porta sicuramente funzionante per risolvere i problem

non valida	una porta o di un modulo sospetto
Dispositivo endpoint non valido o precedente	Sostituisci telefono, altoparlante, altro endpoint con un dispositivo funzionante recente
Modalità sospensione dispositivo	Si tratta di un "flap previsto". Prestare attenzione all'indicatore orario del riscon della porta per determinare se si verifica rapidamente o in modo intermittente la causa è un'impostazione di sospensione

Verifica della compatibilità di SFP e SFP+

La gamma di interfacce Cisco collegabili a sistema avviato offre numerose opzioni in termini di velocità, protocolli, portata e supporti di trasmissione supportati.

Èpossibile utilizzare qualsiasi combinazione di moduli SFP o SFP + ricetrasmettitori supportata dagli switch Catalyst serie 9000. Le uniche restrizioni sono che ciascuna porta deve corrispondere alle specifiche di lunghezza d'onda sull'altra estremità del cavo e che il cavo non deve superare la lunghezza del cavo stabilita per comunicazioni affidabili.

Usare solo i Cisco SFP transceiver Module sul dispositivo Cisco. Ogni modulo ricetrasmettitore SFP o SFP+ supporta la funzione ID (Quality Identification) Cisco che consente a uno switch o a un router Cisco di identificare e convalidare la certificazione e il test del modulo ricetrasmettitore da parte di Cisco.

> **Suggerimento**: per verificare la matrice di compatibilità tra dispositivi ottici Cisco, fare riferimento a questo collegamento

Identificazione degli flap delle porte

Utilizzare il **show logging**per identificare un evento link flap. Nell'esempio viene mostrato un messaggio di registro di sistema dello switch parziale per un evento di link flap con l'interfaccia 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
```

Suggerimento: se si analizzano i log dei messaggi di sistema, è necessario prestare attenzione all'**indicatore orario** del link flap, in quanto consente di confrontare eventi simultanei su quella porta specifica e di verificare se è previsto o meno il link flap (ad esempio, impostazioni di sospensione o altre cause "normali" non necessariamente un problema).

Comandi Show dell'interfaccia

Il comando **show interface** fornisce molte informazioni che aiutano a identificare un possibile problema del layer 1 che causa un evento di link flap:

```
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
```

In questa tabella vengono elencati alcuni contatori del comando **show interface**:

Contatore	Problemi e cause comuni che aumentano i contatori di errori
CRC	Un numero elevato di CRC è in genere il risultato di collisioni, ma può anche indicare u problema fisico (ad esempio un cablaggio, un SFP, un'interfaccia errata o una scheda o una mancata corrispondenza del duplex.
Input errors	include il conteggio di runt frame, giant frame, no buffer, CRC, frame, overrun e pacche ignorati. Il conteggio degli errori di input può inoltre aumentare a causa di altri errori co all'input.
output errors	Questo problema è dovuto alle dimensioni ridotte della coda di output o a una sottoscri eccessiva.
Totale perdite di	Le perdite di output sono generalmente il risultato di una sovrascrittura dell'interfaccia

output	causata da molti a uno o da un trasferimento da 10 Gbps a 1 Gps. I buffer di interfaccia sono una risorsa limitata e possono assorbire una frammentazione solo fino a un punto dopo il quale i pacchetti iniziano a cadere. I buffer possono essere regolati in modo da fornire un'attenuazione, ma non è possibile garantire uno scenario di perdita di output p zero.
Interruzioni di protocollo sconosciute	Le interruzioni di protocollo sconosciute vengono in genere ignorate perché l'interfaccia vengono ricevuti i pacchetti non è configurata per questo tipo di protocollo oppure può essere un protocollo non riconosciuto dallo switch. Ad esempio, se si hanno due switch connessi e si disabilita il CDP su un'interfaccia dello switch, il protocollo dell'interfaccia scartato. I pacchetti CDP non vengono più riconosciuti e vengono quindi eliminati.

Il comando **history** consente a un'interfaccia di mantenere la cronologia di utilizzo in un formato grafico simile alla cronologia della CPU. La cronologia può essere mantenuta come bit al secondo (bps) o come pacchetti al secondo (pps), come mostrato nell'esempio seguente:

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

Oltre alla velocità, l'utente può monitorare vari contatori di interfaccia:

```
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)#
```

Come per la cronologia della CPU, sono disponibili grafici per gli ultimi 60 secondi, gli ultimi 60 minuti e le ultime 72 ore. Vengono mantenuti grafici separati per gli istogrammi di input e di output:

```
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)
```

Usare il **comando show controller ethernet-controller{interface{*numero-interfaccia*}}** per visualizzare le statistiche dei contatori del traffico per interfaccia (**trasmissione** e **ricezione**) e dei contatori degli errori letti dall'hardware. Utilizzare la parola chiave **phy** per visualizzare i registri interni dell'interfaccia o la parola chiave **port-info** per visualizzare le informazioni sull'ASIC della porta.

Questo è un esempio di output del **comando show controller ethernet-controller** per un'interfaccia specifica:

```
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 msecs AGO
```

> **Suggerimento: è inoltre possibile utilizzare il** comando **show interfaces {interface{*interface-number*} controller** per visualizzare le statistiche di **trasmissione** e **ricezione** lette dall'hardware per **interfaccia**.

Usare i **flap dell'interfaccia show platform pm{interface{*numero-interfaccia*}}** per visualizzare il numero di volte in cui un'interfaccia si è guastata:

Questo è un esempio di output dei **flap di interfaccia pm della piattaforma show{interface{*numero-interfaccia*}}**per un'interfaccia specifica:

```
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
```

Utilizzare il comando **show idprom{interface{*numero-interfaccia*}}** senza parole chiave per visualizzare le informazioni IDPROM per l'interfaccia specifica. Da utilizzare con la parola chiave **detail** per visualizzare informazioni IDPROM esadecimali dettagliate.

Questo è un esempio di output del comando **show idprom{interface{*numero-interfaccia*}}** per un'interfaccia specifica. I valori **High** e **Low** Warning|Alarm **threshold** elencati in questo output del comando sono i normali parametri operativi del ricetrasmettitore ottico. Questi valori possono essere verificati dalla scheda tecnica per l'ottica specifica. Fare riferimento alla [scheda tecnica di Cisco Optics]

```
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
```

Suggerimento:verificare che la versione hardware e software del dispositivo sia compatibile con la matrice di compatibilità tra dispositivi ottici Cisco SFP/SFP+ installata

Nella tabella seguente vengono elencati i vari comandi che è possibile usare per risolvere i problemi dei link flap:

Comando	Scopo
mostra errori contatori interfacce	Visualizza i contatori degli errori dell'interfa
funzionalità show interfaces	Visualizza le funzionalità dell'interfaccia specifica
show interface transceiver **(specifico per fibra/SFP)**	Visualizza informazioni sui ricetrasmettitori con il monitoraggio ottico digitale (DOM) ab
show interface link	Visualizza informazioni a livello di collegam
show interface {interface{*interface-number*} piattaforma	Visualizza le informazioni sulla piattaforma interfaccia
show controller ethernet-controller {interface{*interface-number*}} port-info	Visualizza informazioni aggiuntive sulla por
show controller ethernet-controller {interface{*interface-number*}} collegamento dettagli	Visualizza lo stato del collegamento
show errdisable flap-value	Visualizza il numero di flap che possono verificarsi prima dello stato err-disabled.
clear counters	Utilizzare questo comando per azzerare i contatori del traffico e degli errori in modo verificare se il problema è solo temporane i contatori continuano ad aumentare.
clear controller ethernet-controller	Utilizzare questo comando per cancellare i contatori hardware di trasmissione e ricezi

Verificare lo stato del cavo con Time Domain Reflector (TDR)

La funzione Time Domain Reflectometer (TDR) consente di determinare se un cavo è APERTO o CORTO quando è guasto. Con TDR è possibile controllare lo stato dei cavi in rame per le porte sugli switch Catalyst serie 9000. Il TDR rileva un errore del cavo con un segnale inviato attraverso il cavo e legge il segnale riflesso. Il segnale può essere riflesso in tutto o in parte a causa di difetti del cavo

Utilizzare il comando test cable-diagnostics tdr {interface**{*interface-number*} }**per avviare il test TDR, quindi utilizzare il comando **show cable-diagnostics tdr**{*interfaceinterface-number*}.

Suggerimento: per ulteriori informazioni, fare riferimento a Controllo dello stato e della connettività delle porte

L'esempio mostra il risultato del test TDR per l'interfaccia 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
```

> **Suggerimento**: sugli switch Catalyst serie 9300, vengono rilevati solo questi tipi di errore dei cavi: **OPEN**, **SHORT** e **IMPEDANCE MISMATCH.** Se il cavo è terminato correttamente, viene visualizzato lo stato **Normale** (Normal) a scopo illustrativo.

Linee guida TDR

Le presenti linee guida si applicano all'uso di TDR:

- Non modificare la configurazione della porta durante l'esecuzione del test TDR.
- Se si collega una porta durante un test TDR a una porta abilitata per Auto-MDIX, il risultato TDR potrebbe non essere valido.
- Se si collega una porta durante un test TDR a una porta 100BASE-T come quella del dispositivo, le coppie inutilizzate (4-5 e 7-8) vengono segnalate come guaste perché l'estremità remota non termina queste coppie.
- A causa delle caratteristiche dei cavi, è necessario eseguire il test TDR più volte per ottenere risultati accurati.
- Non modificare lo stato della porta (ad esempio, rimuovere il cavo dall'estremità vicina o remota) perché i risultati potrebbero essere imprecisi.
- TDR funziona meglio se il cavo di prova è scollegato dalla porta remota. In caso contrario, può risultare difficile interpretare correttamente i risultati.
- Il TDR funziona su quattro fili. In base alle condizioni del cavo, lo stato può indicare che una coppia è OPEN o SHORT, mentre tutte le altre coppie di fili sono visualizzate come guaste. Questa operazione è accettabile in quanto è possibile dichiarare un errore di cavo a condizione che una coppia di fili sia OPEN o SHORT.
- L'intento del TDR è determinare il cattivo funzionamento di un cavo, piuttosto che individuare un cavo difettoso.
- Quando TDR individua un cavo difettoso, è comunque possibile utilizzare uno strumento di diagnosi dei cavi offline per diagnosticare meglio il problema.
- I risultati TDR possono variare a seconda del modello di switch Catalyst serie 9300 a causa della differenza di risoluzione delle implementazioni TDR. In questo caso, è necessario fare riferimento a uno strumento di diagnosi dei cavi non in linea.

Monitoraggio ottico digitale (DOM)

Digital Optical Monitoring (DOM) è uno standard industriale, progettato per definire un'interfaccia digitale per accedere a parametri in tempo reale, quali:

- Temperatura
- Tensione di alimentazione del ricetrasmettitore
- Corrente di polarizzazione del laser
- Alimentazione Tx ottica
- Alimentazione Rx ottica

Come abilitare DOM

Nella tabella sono elencati i comandi che è possibile utilizzare per attivare/disattivare DOM per

tutti i ricetrasmettitori del sistema:

Passi	Comando o azione	Scopo
Passaggio 1	**attivare** **Esempio:** switch>abilita	Abilita la modalità di esecuzione fisica Se richiesto, immettere la password
Passaggio 2	**configurare il terminale** **Esempio:** switch#configure terminal	Entra nella modalità di configurazione globale
Passaggio 3	ricetrasmettitore tipo all **Esempio:** switch(config)#transceiver type all	Attiva la modalità di configurazione del tipo Ricetrasmettitore
Passaggio 4	monitoraggio **Esempio:** switch(config)#monitoring	Consente il monitoraggio di tutti i ricetrasmettitori ottici.

Utilizzare il comando **show interfaces** {interface{*interface-number*} **transceiver detail** per visualizzare le informazioni sul ricetrasmettitore:

```
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)
--------- ---- --------------- ---------- --------- --------- ---------
Hu1/0/25 N/A -16.7 2.0 -1.0 -9.9 -13.9
```

Suggerimento: per determinare se un ricetrasmettitore ottico funziona ai livelli di segnale appropriati, fare riferimento alle specifiche Cisco Optics

Messaggi del syslog di monitoraggio ottico digitale

In questa sezione vengono descritti i messaggi syslog più rilevanti per la violazione di soglia:

Livelli di temperatura delle ottiche SFP

- **Spiegazione:** Questo messaggio log viene generato quando la temperatura è bassa o supera i normali valori operativi dell'ottica:

```
%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.
```

Livelli di tensione delle ottiche SFP

- **Spiegazione:** Questo messaggio log viene generato quando la tensione è bassa o supera i normali valori di funzionamento dell'ottica:

```
%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.
```

Livelli di luce delle ottiche SFP

- **Spiegazione:** Questo messaggio log viene generato quando la potenza della luce è bassa o supera i valori di funzionamento dell'ottica:

```
%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.
```

Suggerimento: per ulteriori informazioni su DOM, vedere Monitoraggio ottico digitale

Cisco Optics e Forward Error Correction (FEC)

La tecnologia FEC è utilizzata per rilevare e correggere un certo numero di errori in un flusso di bit e aggiunge bit ridondanti e codice di controllo degli errori al blocco di messaggi prima della trasmissione. In qualità di produttore di moduli, Cisco si preoccupa di progettare i ricetrasmettitori in modo che siano conformi alle specifiche. Quando il ricetrasmettitore ottico viene utilizzato in una piattaforma host Cisco, la funzione FEC è abilitata per impostazione predefinita in base al tipo di modulo ottico rilevato dal software host (vedere questa tabella scaricabile). Nella maggior parte dei casi, l'implementazione della tecnologia FEC è dettata dagli standard di settore supportati dal

tipo di ottica.

Per alcune specifiche personalizzate, le implementazioni FEC variano. Per informazioni dettagliate, fare riferimento a Descrizione di FEC e della sua implementazione nel documento Cisco Optics.

Nell'esempio viene mostrato come configurare FEC e alcune delle opzioni disponibili:

```
switch(config-if)#fec?
  auto Enable FEC Auto-Neg
  cl108 Enable clause108 with 25G
  cl74 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**: entrambi i lati di un collegamento devono avere la stessa FEC encoding algoritmo abilitato per l'attivazione del collegamento.

Comandi debug

In questa tabella vengono elencati i vari comandi che è possibile utilizzare per eseguire il debug degli flap delle porte

> **Attenzione**: usare con cautela i comandi di debug. Tenere presente che molti **comandi di debug** hanno un impatto sulla rete in tempo reale e si consiglia di utilizzarli in un ambiente lab quando il problema viene riprodotto. ;

Comando	Scopo
debug pm	Debug di Port Manager
porta pm di debug	Eventi correlati alle porte
piattaforma di debug pm	Informazioni di debug su NGWC Platform Port Manager
debug platform pm l2-control	Debug dell'infrastruttura di controllo NGWC L2
debug platform pm - stato-collegamento	Eventi rilevamento collegamento interfaccia
debug platform pm-vector	Funzioni vettoriali di Port Manager
debug condition interface <nome interfaccia>	Abilitazione selettiva dei debug per un'interfaccia

	specifica
debug interface state	Transizioni stati

Questo è un esempio di output di esempio parziale della d*debug* comandi elencati nella tabella:

```
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
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 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
```

Informazioni correlate

Matrice di compatibilità tra dispositivi ottici Cisco

Scheda tecnica di Cisco SFP Module per applicazioni Gigabit Ethernet

25GE e 100GE - White paper sull'aumento della velocità nelle aziende con protezione degli investimenti

Data sheet della soluzione Cisco CWDM SFP

Supporto per l'innovazione: in che modo Cisco TAC sta trasformando la documentazione e semplificando il self-service

Documentazione e supporto tecnico – Cisco Systems

ID bug Cisco	Descrizione
ID bug Cisco CSCvu13029	Intermittent Link Flaps su switch mGig Cat9300 su endpoint con supporto r
ID bug Cisco CSCvt50788	Problemi di interoperabilità Cat9400 mGig con altri dispositivi mGig provoc link flap
ID bug Cisco CSCvu92432	CAT9400: flap dell'interfaccia Mgig con access point Mgig
ID bug Cisco CSCve65787	Supporto Autoneg per xcvr Cu 100G/40G/25G

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).