

# Risoluzione dei problemi di link flap su Nexus 9000

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Comprendere le cause del link flap](#)

[Identifica link flap](#)

[Identificazione dell'inversione dei collegamenti di layer 1 o di protocollo](#)

[Esempio di inversione di livello 1](#)

[Esempio di LACP Triggered Flap](#)

[Risoluzione dei problemi di inversione dei collegamenti di layer 1](#)

[Problema di layer 1 su NX-OS 10.2.1 e versioni successive](#)

[TORTA link flap](#)

[Collega torta giù](#)

[TORTA ottica](#)

[Esempio di TORTA: link Flap causato dalla chiusura e riattivazione della porta sul lato peer](#)

[Esempio di TORTA: collegamento non attivo causato dalla chiusura della porta sul lato peer](#)

[Sostituzione di parti difettose](#)

[Problema di layer 1 su NX-OS 10.1.2 e versioni precedenti](#)

[Verifica della cronologia eventi porta-client](#)

[Verifica degli eventi ASIC](#)

[Controllo delle informazioni DOM \(Digital Optical Monitoring\) su entrambi i lati](#)

[Test di sostituzione e sostituzione dei componenti difettosi](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come risolvere il problema del link flap di layer 1 sugli switch Nexus 9000.

## Prerequisiti

### Requisiti

Cisco consiglia di familiarizzare con il sistema operativo Cisco Nexus (NX-OS) e l'architettura Nexus di base prima di procedere con le informazioni descritte in questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- N9K-C93180YC-FX
- nxos64-cs.10.2.6.M

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.

## Comprendere le cause del link flap

Il link flap è un problema di rete in cui un'interfaccia fisica di uno switch, ad esempio Nexus 9000, alterna in modo continuo l'attivazione e l'inattività. Questo comportamento di interruzione può compromettere le prestazioni della rete, destabilizzarla e interrompere la comunicazione, causando in tal modo notevoli inconvenienti. I link flap in genere derivano da livelli fisici difettosi o da problemi di sincronizzazione del protocollo.

- Flap Del Collegamento Attivato Dal Protocollo

I link flap attivati dal protocollo si verificano quando si verifica un problema con la sincronizzazione del protocollo. Questo potrebbe coinvolgere protocolli come il Link Aggregation Control Protocol (LACP), Virtual Port-Channel e altri. Il problema può essere causato da una configurazione errata del protocollo o dalla perdita di pacchetti, che a loro volta possono causare instabilità del collegamento. Un monitoraggio regolare e aggiornamenti software tempestivi possono aiutare a prevenire questo tipo di link flap.

- Problema fisico di layer 1

I link flap possono anche avere origine dal layer 1, lo strato fisico della rete. Questo spesso coinvolge componenti fisici come cavi e interfacce. Cavi danneggiati, allentati o obsoleti e interfacce non funzionanti correttamente possono causare il link al link flap. Ispezioni fisiche e interventi di manutenzione periodici, tra cui controlli dei cavi e test dell'interfaccia, possono aiutare a identificare e risolvere questi problemi prima che portino ai link flap.

In questo documento viene descritta la risoluzione dei problemi fisici di layer 1.

## Identifica link flap

I link flap possono essere facilmente identificati dai log. Nell'esempio viene visualizzato un evento di link flap sulla porta E1/5, in cui la porta si spegne e quindi torna su in un secondo momento.

<#root>

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel100: Ethernet1/5 is down
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
```

```

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Lin

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-SPEED: Interface Ethernet1/5, operational speed changed
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_DUPLEX: Interface Ethernet1/5, operational duplex mo
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_RX_FLOW_CONTROL: Interface Ethernet1/5, operational
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_TX_FLOW_CONTROL: Interface Ethernet1/5, operational
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-SPEED: Interface port-channel100, operational speed cha
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_DUPLEX: Interface port-channel100, operational duple
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_RX_FLOW_CONTROL: Interface port-channel100, operatio
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-IF_TX_FLOW_CONTROL: Interface port-channel100, operatio

2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_UP: port-channel100: Ethernet1/5 is up

2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operationa
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETHPORT-5-IF_UP: Interface Ethernet1/5 is up in mode access
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETHPORT-5-IF_UP: Interface port-channel100 is up in mode access

```

## Identificazione dell'inversione dei collegamenti di layer 1 o di protocollo

Ethernet Port Manager (Ethpm) è un processo che gestisce le interfacce Ethernet. La cronologia degli eventi Ethpm può essere utilizzata per identificare la causa di un link flap.

### Esempio di inversione di livello 1

In E1/5 si è verificato un errore di collegamento alle 05:28:35, con la transizione verso l'etpm attivata da ETH\_PORT\_FSM\_EV\_LINK\_DOWN. Ciò indica un link al layer 1.

<#root>

```

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Lin

2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann

```

```
N9K-C93180YC-FX# show system internal ethpm event-history interface e1/5
```

```

[143] 2024-01-21T05:26:02.100255000+00:00 [-] FSM:<Ethernet1/5> Transition:
Previous state: [ETH_PORT_FSM_ST_WAIT_BUNDLE_MEMBER_BRINGUP]
Triggered event: [ETH_PORT_FSM_EV_FIRST_BRINGUP_BUNDLE_MEMBER_DONE]
Next state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]
[144]

```

```
2024-01-21T05:27:35.
```

```
783495000+00:00 [-] FSM:<Ethernet1/5> Transition:
```

Previous state: [ETH\_PORT\_FSM\_ST\_BUNDLE\_MEMBER\_UP]

Triggered event: [ETH\_PORT\_FSM\_EV\_LINK\_DOWN]

Next state: [FSM\_ST\_NO\_CHANGE]

## Esempio di LACP Triggered Flap

E1/8 entra in uno stato di inizializzazione verso il basso alle 07:40:07, con la transizione etpm attivata da ETH\_PORT\_FSM\_EV\_EXTERNAL\_REINIT\_NO\_FLAP\_REQ. Indica un link flap attivato dal protocollo LACP (Link Aggregation Control Protocol).

<#root>

```
2024 Jan 21 07:37:20 N9K-C93180YC-FX %ETHPORT-5-IF_UP: Interface port-channel200 is up in Layer3
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel200: first operationa
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel200: Ethernet1/8 is dow
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel200,bandwidt
```

```
2024 Jan 21 07:40:07 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_INITIALIZING: Interface Ethernet1/8 is down (In
```

<#root>

```
N9K-C93180YC-FX# show system internal ethpm event-history interface e1/8
```

```
[218] 2024-01-21T07:37:20.551880000+00:00 [-] FSM:<Ethernet1/8> Transition:
Previous state: [ETH_PORT_FSM_ST_WAIT_BUNDLE_MEMBER_BRINGUP]
Triggered event: [ETH_PORT_FSM_EV_FIRST_BRINGUP_BUNDLE_MEMBER_DONE]
Next state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]
```

[219]

```
2024-01-21T07:40:07.104339000
```

```
+00:00 [-] FSM:<Ethernet1/8> Transition:
Previous state: [ETH_PORT_FSM_ST_BUNDLE_MEMBER_UP]
Triggered event:
```

```
[ETH_PORT_FSM_EV_EXTERNAL_REINIT_NO_FLAP_REQ]
```

```
Next state: [FSM_ST_NO_CHANGE]
```

## Risoluzione dei problemi di inversione dei collegamenti di layer 1

Cisco offre una vasta gamma di moduli ottici per supportare una vasta gamma di velocità, supporti e distanze. Prima di collegare un collegamento a Nexus 9000, verificare che l'SFP e il cavo siano compatibili con il software e l'hardware correnti. È possibile verificare questa condizione

eseguendo le operazioni seguenti:

[Matrice di compatibilità tra dispositivi ottici Cisco](#)

[Matrice di interoperabilità ottica-ottica Cisco](#)

## Problema di layer 1 su NX-OS 10.2.1 e versioni successive

A partire da NX-OS 10.2.1, il Platform Insights Engine (PIE) è supportato su tutte le piattaforme CloudScale ToR ed EoR. PIE è un'applicazione di analisi della root cause in tempo reale e on-switch.

Tre TORTE possono essere utili per risolvere il problema del link flap sul layer 1.

### TORTA link flap

Il link flap PIE analizza gli eventi di link flap pubblicati dai driver dello spazio utente (USD) e determina la causa principale di un link flap. Il PIE pubblica l'analisi della causa principale al broker. Gli eventi di link flap vengono pubblicati da USD (client PIE) quando un link flap. Gli USD raccolgono tutti i dati rilevanti dall'ASIC e dall'USD necessari per l'analisi della causa principale e pubblicano i dati al broker. Il link flap PIE analizza i dati e arriva alla causa principale più probabile per il link flap.

### Collega torta giù

Il collegamento TORTA verso il basso individua la causa principale del mancato collegamento. USD raccoglie dati su un'interfaccia configurata per essere attiva, ma lo stato operativo dell'interfaccia non è attivo. Questi dati vengono pubblicati nell'applicazione PIE. Il link-down PIE sottoscrive questi eventi, riceve i dati dal broker e analizza i dati per trovare la causa principale.

### TORTA ottica

Optics PIE è un motore di monitoraggio continuo che esegue un'analisi delle serie temporali dei dati DOM raccolti a intervalli regolari. Tenendo traccia di vari parametri nel DOM in un periodo, la PIE arriva a una metrica per descrivere lo stato delle ottiche per ciascuna porta ottica. La metrica è un'intuizione sullo stato di tendenza di un ricetrasmittitore ottico.

Per ulteriori informazioni, fare riferimento a questo documento PIE:

[Cisco Nexus serie 9000 NX-OS Platform Insights Engine Guide, versione 10.2\(x\)](#)

Esempio di TORTA: link Flap causato dalla chiusura e riattivazione della porta sul lato peer

<#root>

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel100: Ethernet1/5 is down
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
```

```
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Lin
2024 Jan 21 05:27:35 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
2024 Jan 21 05:27:58 N9K-C93180YC-FX %ETHPORT-5-SPEED: Interface Ethernet1/5, operational speed changed
<snip>
2024 Jan 21 05:28:02 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_UP: port-channel100: Ethernet1/5 is up
```

```
N9K-C93180YC-FX# show pie interface ethernet 1/5 link-flap-rca
```

```
2024-01-21 05:27:35
```

```
Event Id: 00000068 Ethernet1/5 Source Id: 436209664 RCA Code: 41 >>>PIE event time
```

```
Reason: Link flapped/down due to Local Fault, check peer
```

```
>>>PIE link flap reason
```

```
N9K-C93180YC-FX# show pie interface ethernet 1/5 transceiver-insights
```

```
2024-01-21 05:30:12 Event Id: 00000080 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
```

```
2024-01-21 05:28:12 Event Id: 00000072 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
```

Esempio di TORTA: collegamento non attivo causato dalla chiusura della porta sul lato peer

```
<#root>
```

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-FOP_CHANGED: port-channel100: first operational
```

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETH_PORT_CHANNEL-5-PORT_DOWN: port-channel100: Ethernet1/5 is down
```

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
```

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_BANDWIDTH_CHANGE: Interface port-channel100,bandwidth
```

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_LINK_FAILURE: Interface Ethernet1/5 is down (Lin
```

```
2024 Jan 21 05:48:38 N9K-C93180YC-FX %ETHPORT-5-IF_DOWN_PORT_CHANNEL_MEMBERS_DOWN: Interface port-chann
```

```
N9K-C93180YC-FX# show pie interface ethernet 1/5 link-down-rca
```

```
2024-01-21 05:48:48
```

```
Event Id: 00000197 Ethernet1/5 Source Id: 436209664 RCA Code: 16 >>>PIE event time
```

```
Reason: No PCS alignment detected. Please check Fec, speed, Autoneg configurations with peer
```

```
>>>Physical layer failed
```

```
N9K-C93180YC-FX# show pie interface ethernet 1/5 transceiver-insights
```

```
2024-01-21 05:50:12 Event Id: 00000199 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
```

```
2024-01-21 05:48:12 Event Id: 00000187 Event Class: xcvr DOM DB Event Interface: Ethernet1/5 Health Met
```

## Sostituzione di parti difettose

In base all'output PIE, si consiglia di sostituire il componente potenzialmente difettoso e continuare il monitoraggio. Se il link flap persiste, è necessario eseguire un test di swap per restringere la parte difettosa. Un test di scambio può essere eseguito modificando un componente alla volta e mantenendo tutti gli altri elementi invariati. Infine, il collegamento si stabilizza dopo lo swapping del componente guasto.

## Problema di layer 1 su NX-OS 10.1.2 e versioni precedenti

Per le versioni del software NX-OS precedenti alla versione 10.2(1), il supporto PIE non è disponibile. Per controllare il link flap di layer 1 sono necessari diversi passaggi manuali.

### Verifica della cronologia eventi porta-client

Elenca tutti gli eventi di collegamento nel modulo allegato. Il tempo di rimbalzo si riferisce alla durata dell'attesa di un'interfaccia prima di notificare al supervisore l'interruzione di un collegamento. Durante questo periodo, l'interfaccia attende di verificare se il collegamento è di nuovo attivo. Questa opzione viene usata per determinare se il collegamento è stato interrotto o se si è verificato un leggero flap.

<#root>

```
N9K-C93180YC-FX# attach module 1
```

```
module-1# show system internal port-client link-event
```

```
***** Port Client Link Events Log *****
```

```
-----  
Time PortNo Speed Event Stsinfo  
-----
```

```
Jan 21 05:48:38 2024 00122142 Ethernet1/5 ---- DOWN Link down debounce timer stopped and link is down
```

```
Jan 21 05:48:37 2024 00993003 Ethernet1/5 ---- DOWN Link down debounce timer started(0x40e50006)
```

```
Jan 21 05:45:14 2024 00432606 Ethernet1/5 10G UP SUCCESS(0x0)
```

### Verifica degli eventi ASIC

Questi eventi forniscono informazioni dettagliate su ogni evento di collegamento.

<#root>

```
N9K-C93180YC-FX# attach module 1
module-1# show hardware internal tah link-events fp-port 5
```

```
324) Jan 21 05:48:37 2024 uSec 992843: Fp 5 : tahusd_isr.c #8469
Port Down with an ASIC interrupt
----- ASIC MAC/PCS/Serdes REGS (Mac Channel 0) -----
```

Link flapped due to Local Fault, check peer

>>>Local Fault means the local

device detected the issue on the receive path.

>>>

Remote Fault means a Local Fault is detected across the link.

```
Intr Regs 00:0x0000, 01:0x0000, 02:0x0000, 03:0x0010, 07:0x0000, 11:0x0000, 15:0x0000
sts2.bercount : 0x0f00 sts2.errorblocks : 0x0000
bercounthi : 0x0000 erroredblockhi : 0x0000
counters0.syncloss : 0x0001 counters0.blockloss: 0x0001
counters1.highber : 0x0000 counters1.vlderr : 0x0000
counters2.unkerr : 0x0012 counters2.invlerr : 0x0000
```

Codice di errore	Spiegazione
sts2.bloccatierrati	Conta i blocchi errati (bit di ordine superiore).
sts2.conteggio	Conta le intestazioni di sincronizzazione errate (bit di ordine inferiore).
bercounthi	Conta le intestazioni di sincronizzazione errate (bit di ordine superiore).
blockoerrato	Conta i blocchi errati (bit di ordine superiore).
counters0.syncloss	Perdita sincronizzazione



counters0.blocklockloss	Blocca perdita di blocchi
counters1.highber	Valore BER elevato
counters1.vlderr	Errore valido
counters2.unkerr	Errore sconosciuto
contatori2.invlerr	Errore non valido

Controllo delle informazioni DOM (Digital Optical Monitoring) su entrambi i lati

In questo output sono disponibili diverse informazioni SFP (Small Form-Factor Pluggable). Se un valore non rientra nell'intervallo accettabile nella diagnostica SFP, l'SFP è considerato un componente potenzialmente danneggiato e deve essere sostituito. In questo esempio, tutto è in ordine.

<#root>

N9K-C93180YC-FX# show interface e1/5 transceiver details

```

Ethernet1/5
transceiver is present
type is 10Gbase-SR          >>>SFP type
name is CISCO-OPLINK       >>>SFP vendor
part number is TPP4XGDS0CCISE2G
revision is 02
serial number is OPMXXXXXXXX >>>SFP SN
nominal bitrate is 10300 MBit/sec >>>SFP bitrate
Link length supported for 50/125um OM2 fiber is 82 m
Link length supported for 62.5/125um fiber is 26 m
Link length supported for 50/125um OM3 fiber is 300 m
cisco id is 3
cisco extended id number is 4
cisco part number is 10-2415-03
cisco product id is SFP-10G-SR >>>SFP PID
cisco version id is V03

```

SFP Detail Diagnostics Information (internal calibration)

```

-----
          Current           Alarms           Warnings
          Measurement       High    Low    High    Low
-----

```

Temperature

36.52 C                    75.00 C -5.00 C 70.00 C 0.00 C

#### Voltage

3.28 V                    3.63 V   2.97 V   3.46 V   3.13 V

#### Current

6.61 mA                    12.00 mA   0.50 mA   11.50 mA   1.00 mA

#### Tx Power

-2.70 dBm                    1.99 dBm   -11.30 dBm   -1.00 dBm   -7.30 dBm

#### Rx Power

-2.40 dBm                    1.99 dBm   -13.97 dBm   -1.00 dBm   -9.91 dBm

Transmit Fault Count = 0

-----  
Note: ++ high-alarm; + high-warning; -- low-alarm; - low-warning  
peer side information is snipped.

### Test di sostituzione e sostituzione dei componenti difettosi

Se i controlli precedenti danno risultati soddisfacenti, è necessario eseguire un test di scambio per restringere la parte difettosa. Un test di scambio può essere eseguito modificando un componente alla volta e mantenendo tutti gli altri elementi invariati. Alla fine, il collegamento si stabilizza dopo che il componente guasto specifico è stato sostituito.

## Informazioni correlate

[Scheda tecnica di Nexus 9000](#)

[Guida alla configurazione delle interfacce Nexus 9000](#)

[Guida di Nexus 9000 NX-OS Platform Insights Engine](#)

## 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).