

Risoluzione dei problemi dei loop di livello 2

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Comandi usati](#)

[Teoria della risoluzione dei problemi](#)

[Applicazione](#)

[Prevenzione](#)

Introduzione

Questo documento descrive le informazioni per identificare l'origine dei loop di livello 2 e fornire salvaguardie per prevenirli in futuro.

Prerequisiti

È consigliabile conoscere i concetti relativi all'utilizzo di STP.

Componenti usati

Quanto riportato in questo documento non è limitato a versioni software o hardware specifiche.

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.

Comandi usati

- `show interfaces | include è attivo` | frequenza di input
- `show cdp neighbors <interface>`
- `show spanning-tree`
- `show logging` (visualizza registri)

Teoria della risoluzione dei problemi

Indipendentemente dalla topologia, dal punto di partenza (lo switch a cui si è connessi per primo), l'approccio per tenere traccia della causa del problema è lo stesso.

Usare il comando show interface fornito in precedenza. Ci stiamo concentrando sull'interfaccia o sulle interfacce con alte velocità di ingresso.

Elevati tassi di output sono un sintomo,... non una causa.

Una volta identificate le interfacce ad alta velocità in ingresso, usare il protocollo CDP adiacente per controllare i collegamenti degli switch connessi. Se si trova una porta host, provare a chiuderla per risolvere il problema.

Per gli switch interconnessi a doppio collegamento, usare i comandi dello Spanning Tree per confermare gli stati di blocco e inoltro. Ciò consente di identificare una porta/uno switch non funzionante.

Notifiche di modifica della topologia (TCN) - Ignorare queste notifiche durante l'utilizzo dei loop.

Gli switch meno recenti non dispongono di COPP o non sono in grado di gestire l'elaborazione BPDU, il che produce TCN casuali.

Se si ritiene che la porta sia la causa del problema, spegnerla e attendere almeno 30 secondi. Se il problema persiste, procedere e "non chiudere" l'interfaccia.

Applicazione

```
DistroSwitch#show interfaces | include is up|input rate
GigabitEthernet1/0/1 is up, line protocol is up
 5 minute input rate 1482600 bits/sec, 2739 packets/sec
GigabitEthernet1/0/2 is up, line protocol is up
 5 minute input rate 291658000 bits/sec, 366176 packets/sec <-----
TenGigabitEthernet1/1/1 is up, line protocol is up
 5 minute input rate 1339000 bits/sec, 2614 packets/sec
```

```
DistroSwitch#show cdp neighbors gigabitEthernet 1/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
 S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
 D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID Local Intrfce Holdtme Capability Platform Port ID
access Gig 1/0/2 158 S I C9300-48P Gig 2/0/2 <-----
```

<#root>

```
DistroSwitch#show logging
```

```
*May 3 18:33:45.885: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port G
*May 3 18:33:58.841: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
```

```
*May 3 18:34:13.842: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port G
*May 3 18:34:28.839: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:43.840: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
*May 3 18:34:58.839: %SW_MATM-4-MACFLAP_NOTIF: Host 0cd0.f8dc.dc47 in vlan 1 is flapping between port T
```

```
access#show spanning-tree vlan 1
Spanning tree instance(s) for vlan 1 does not exist.
```

Prevenzione

Procedure ottimali STP

BPDU Guard: disabilita le interfacce se ottengono BPDU Guard anziché inoltrarlo

Root Guard: in genere, per i dispositivi di distro che si trovano di fronte all'accesso, non è necessario visualizzare mai un BPDU superiore o inferiore sull'interfaccia a cui deve essere applicato.

Loop Guard: in genere per tutti gli switch a livello globale. Se uno switch riceve una BPDU su un'interfaccia, tiene traccia di tale interfaccia per verificare se continua a ricevere le BPDU ogni

Due secondi dopo. In caso contrario, il ciclo non è coerente.

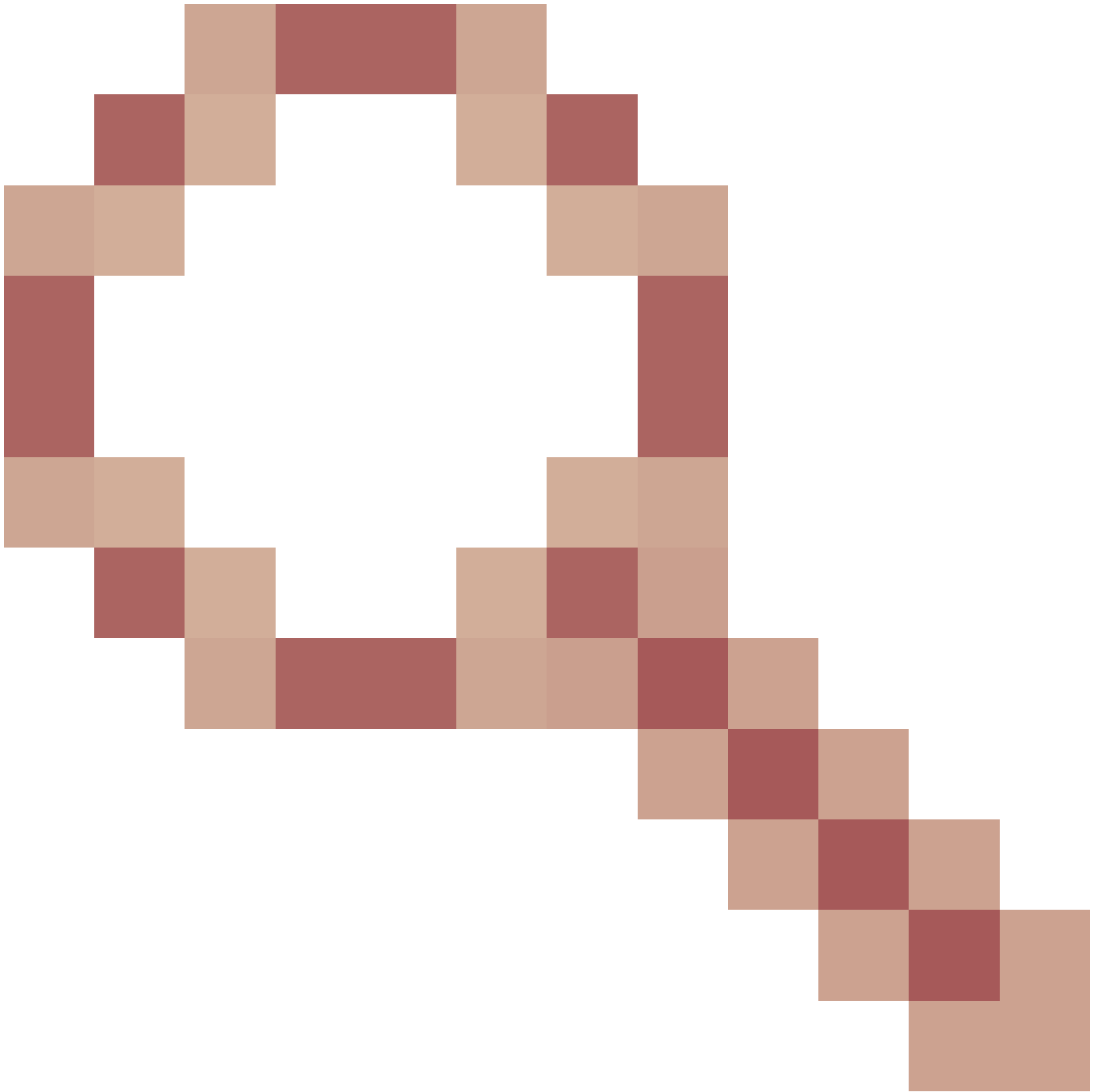
Filtro BPDU - Disabilita STP. BPDU non inviati né elaborati al momento della ricezione. In comune con i provider di servizi, non necessariamente con le reti aziendali

NON CONSIGLIARE TUTTE LE FUNZIONI STP - ad esempio bpdupfilter tronca bpduguard

UDLD Aggressivo

Controllo temporale: impostato su 1%, non superiore o inferiore - Cisco bug

[IDCSCvt85758](#)



CoPP e QoS per scenari specifici sono utili ma non comuni.

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).