Risoluzione dei problemi di incoerenza tra PVID e tipi nello Spanning Tree

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi di due incoerenze Spanning Tree Protocol (STP), un ID VLAN della porta (PVID) e un tipo di VLAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei concetti relativi all'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.

Premesse

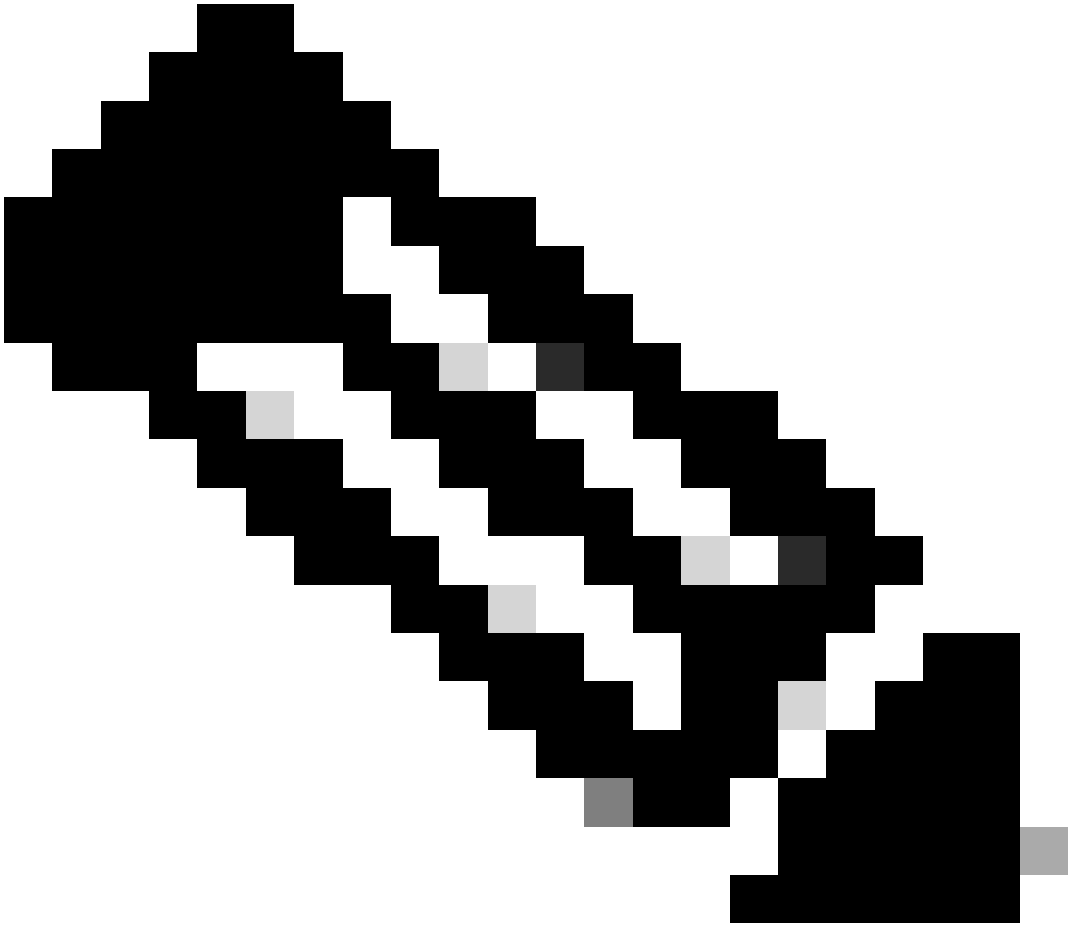
Nelle reti di layer 2 (L2), due dispositivi possono comunicare su un unico percorso. La ridondanza è supportata dal protocollo STP (Spanning-Tree Protocol), che rileva e blocca i percorsi ridondanti ed evita quindi i loop di inoltro. Alcune configurazioni errate possono causare errori STP e causare l'interruzione della rete. Per evitare tempi di inattività, sono stati implementati alcuni miglioramenti in modo che STP rilevi alcuni casi di configurazione errata e la porta corrispondente viene messa in uno stato incoerente.

Possono esistere diversi tipi di incoerenze STP:

- Incoerenza del loop - Viene rilevata dalla feature di protezione del loop. Per ulteriori informazioni, consultare il documento sulla configurazione di STP con Loop Guard e rilevamento dell'inclinazione della BPDU.
- Incoerenza radice (Root inconsistency) - Viene rilevata dalla funzione Root Guard. Per ulteriori informazioni, consultare il documento sul miglioramento dello Spanning Tree Protocol con Root Guard.
- Incoerenza di EtherChannel: rilevata dalla funzionalità di rilevamento della coerenza di EtherChannel. Per ulteriori informazioni, fare riferimento a Rilevamento delle incoerenze EtherChannel.
- Incoerenza dell'ID VLAN della porta (PVID) - Un'unità dati BPDU (Bridge Protocol Data Unit) per VLAN (PVST+) viene ricevuta su una VLAN diversa da quella di origine: (`Mancata corrispondenza dell'ID della porta VLAN` o `*PVID_Inc`).
- Incoerenza tra i tipi: PVST+ BPDU viene ricevuto su un trunk non 802.1Q.

Teoria delle incoerenze tra tipi e PVID

Gli switch Cisco Catalyst implementano la tecnologia PVST che utilizza i trunk ISL (Inter-Switch Link). Con il supporto di IEEE 802.1Q e ISL trunking, era necessaria una soluzione per l'interoperabilità tra PVST e IEEE 802.1Q, che prevedeva un singolo spanning tree per tutte le VLAN. Per soddisfare questo requisito è stata introdotta la funzionalità PVST+.



Nota: Dal punto di vista STP, IEEE 802.1D non riconosce le VLAN e IEEE 802.1Q riconosce le VLAN, ma usa un'unica istanza STP per tutte le VLAN. In altre parole, se la porta è bloccata, significa che è bloccata per tutte le VLAN su tale porta.

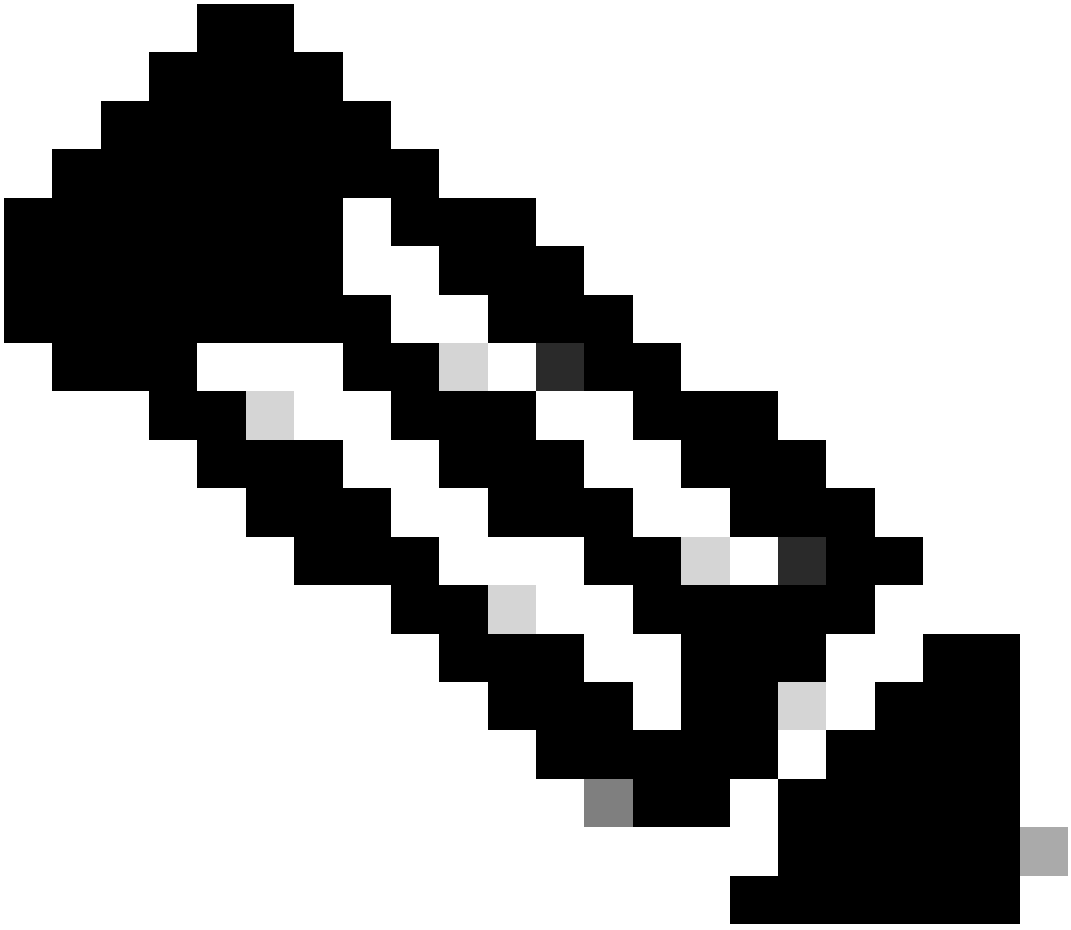
Lo stesso vale per l'inoltro.

Nell'elenco viene mostrata l'interoperabilità di PVST+ con IEEE 802.1Q o IEEE 802.1D, se la VLAN nativa su un trunk IEEE 802.1Q è la VLAN 1:

- Le BPDU VLAN 1 STP vengono inviate all'indirizzo MAC STP IEEE (0180.c200.0000), senza tag.
- Le BPDU VLAN 1 STP vengono inviate anche all'indirizzo MAC PVST+, senza tag.
- Le BPDU non VLAN 1 STP vengono inviate all'indirizzo MAC PVST+ (detto anche indirizzo MAC SSTP (Shared Spanning Tree Protocol), ossia 0100.0ccc.cccd), e sono contrassegnate con un tag VLAN IEEE 802.1Q corrispondente.

Se la VLAN nativa su un trunk IEEE 802.1Q non è la VLAN 1:

- Le BPDU VLAN 1 STP vengono inviate all'indirizzo MAC PVST+ e sono contrassegnate con un tag VLAN IEEE 802.1Q corrispondente.
- Le BPDU VLAN 1 STP vengono inviate anche all'indirizzo MAC STP IEEE sulla VLAN nativa del trunk IEEE 802.1Q, senza tag.
- Le BPDU non VLAN 1 STP vengono inviate all'indirizzo MAC PVST+ e sono contrassegnate con un tag VLAN IEEE 802.1Q corrispondente.



Nota: Le BPDU STP della VLAN nativa vengono inviate senza tag.

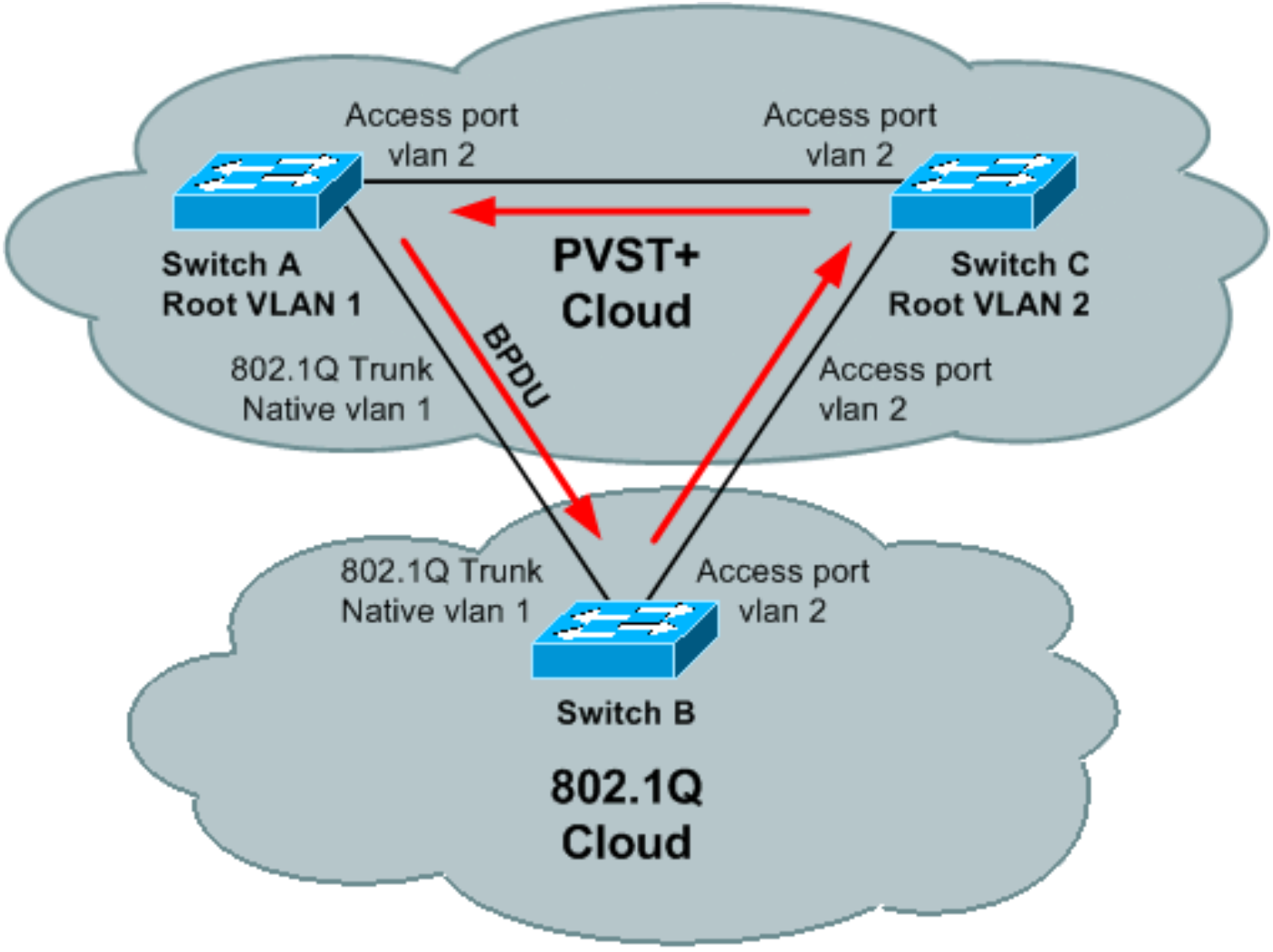
In questo modo, la VLAN 1 STP di PVST+ si unisce con STP di IEEE 802.1D o 802.1Q, mentre le altre VLAN sono tunneling attraverso il cloud di bridge IEEE 802.1D o 802.1Q.

Ad esempio, il cloud IEEE 802.1D o 802.1Q ha un aspetto simile a quello di un cavo delle VLAN PVST+, ma non a quello di 1.

Per il corretto funzionamento di STP, osservare alcune regole quando si connettono bridge PVST+ a bridge IEEE 802.1D o 802.1Q. La regola principale è che i bridge PVST+ devono connettersi a bridge IEEE 802.1D o 802.1Q tramite un trunk IEEE 802.1Q con una VLAN nativa coerente su tutti i bridge che si connettono al cloud di bridge IEEE 802.1Q o 802.1D.

La PVST+ BPDU contiene un numero VLAN che consente ai bridge PVST+ di rilevare se la regola precedente non viene rispettata. Quando uno switch Catalyst rileva una configurazione errata, le porte corrispondenti vengono messe in uno stato di incoerenza PVID o di tipo incoerente, che blocca efficacemente il traffico sulla VLAN corrispondente su una porta corrispondente. Questi stati impediscono l'inoltro di loop causati da una configurazione errata o da cavi non corretti.

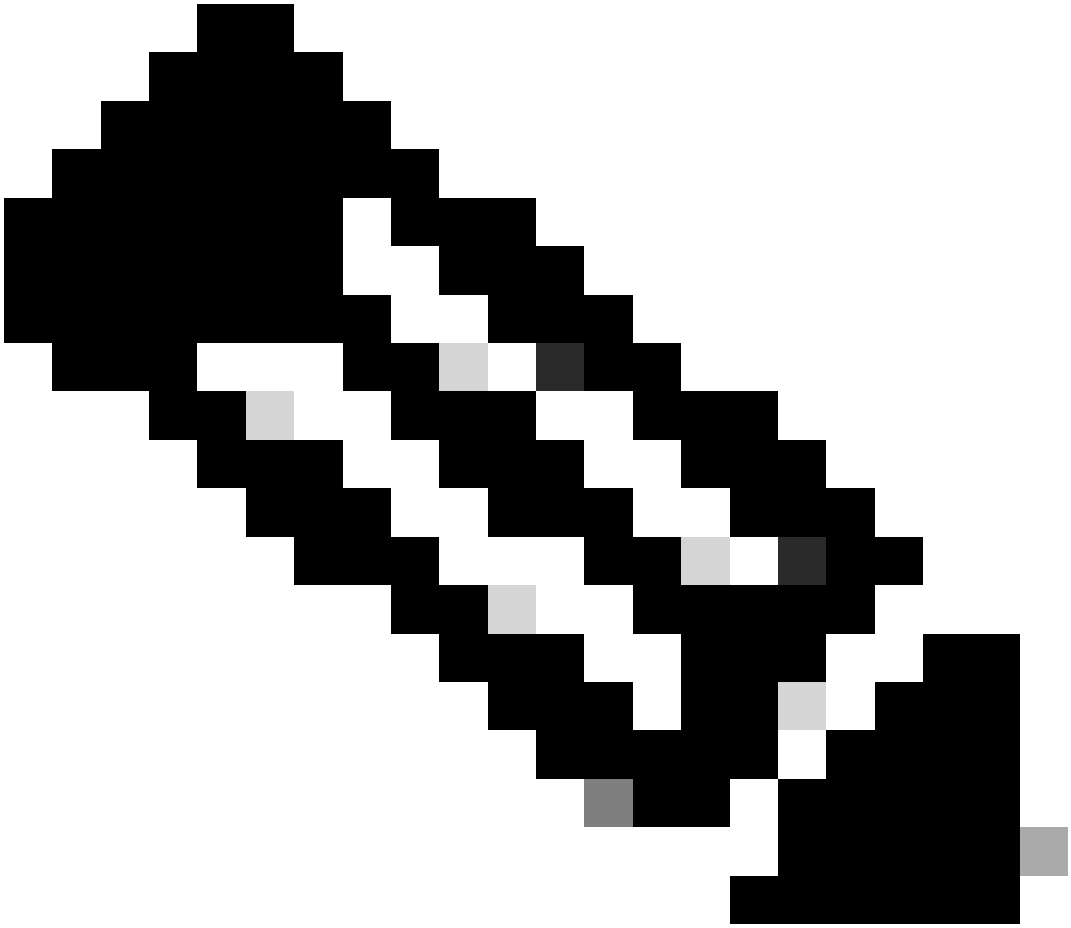
Per illustrare la necessità del rilevamento delle incoerenze, prendere in considerazione questa topologia, in cui gli switch A e C eseguono PVST+ STP e lo switch B esegue 802.1Q STP:



Se il valore BPDU della radice nella VLAN 1 è migliore del valore BPDU della radice nella VLAN 2, non vi è alcuna porta di blocco nella topologia della VLAN 2. La BPDU della VLAN 2 non fa mai un cerchio completo attorno alla topologia; viene sostituita dalla VLAN 1 BPDU sul collegamento B-C, in quanto B esegue solo un STP unito alla VLAN 1 STP di PVST+.

Esiste pertanto un loop di inoltro. Fortunatamente, lo switch A invia pacchetti PVST+ BPDU della VLAN 2 (all'indirizzo SSTP inondato dallo switch B) verso lo switch C. Lo switch C può mettere la

porta C-B in uno stato di incoerenza del tipo, che impedisce il loop.

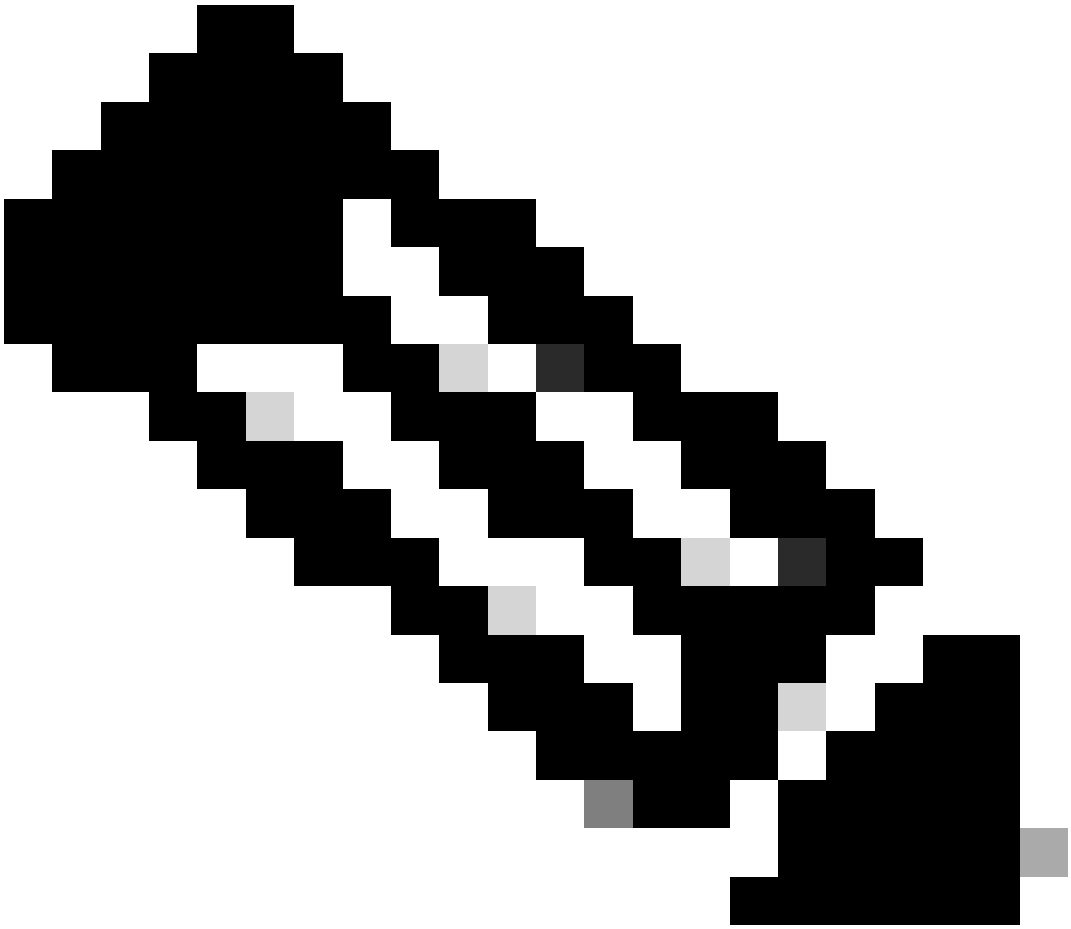


> Nota: In alcuni output del comando, lo stato STP non coerente viene indicato come interrotto.

Quando viene rilevata un'incoerenza STP, gli switch inviano questi messaggi syslog:

```
%SPANTREE-2-RECV_1Q_NON_TRUNK: Received IEEE 802.1Q BPDU on non trunk
FastEthernet0/1 on vlan 1.
%SPANTREE-2-BLOCK_PORT_TYPE: Blocking FastEthernet0/1 on vlan 1.
Inconsistent port type.

%SPANTREE-2-RX_1QPVIDERR: Rcved pvid_inc BPDU on 1Q port 3/25 vlan 1
%SPANTREE-2-RX_BLKPORTPVID: Block 3/25 on rcving vlan 1 for inc peer vlan 10
%SPANTREE-2-TX_BLKPORTPVID: Block 3/25 on xmtting vlan 10 for inc peer vlan
```

Nell'esempio, la VLAN 1 è la destinazione della BPDU e la VLAN 10 la destinazione della BPDU. Quando viene rilevata un'incoerenza, entrambe le VLAN sono bloccate sulla porta a cui viene ricevuta la BPDU.



Nota: I messaggi possono variare in base al tipo e alla versione della versione del software Cisco IOS® in uso.

Se la porta non riceve più BPDU incoerenti, lo stato *-incoerente viene cancellato e l'opzione STP modifica lo stato della porta in base al normale funzionamento dell'opzione STP. Viene inviato un messaggio syslog per indicare la modifica:

```
%SPANTREE-SP-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on vlan 1.
Port consistency restored.
```

Per ulteriori informazioni sul funzionamento di PVST+, fare riferimento all'esempio di

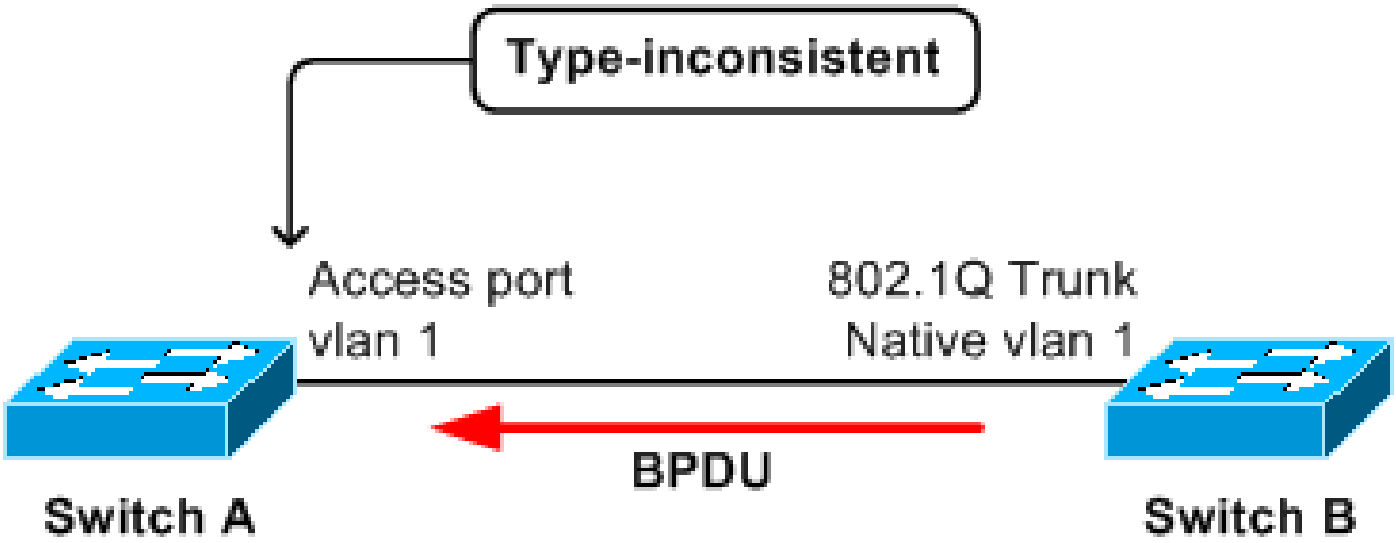
configurazione della migrazione da PVST+ a Rapid-PVST.

Risoluzione dei problemi

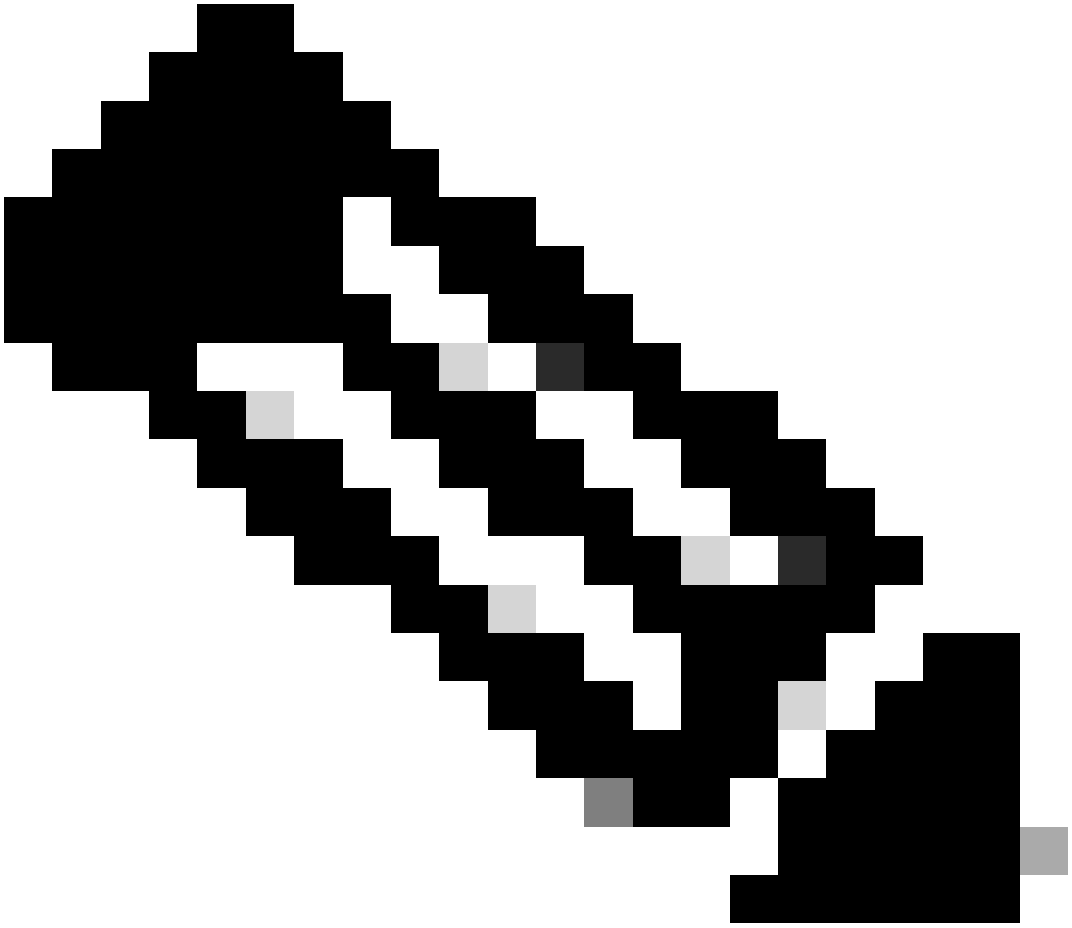
Per visualizzare un elenco delle porte incoerenti, la recente implementazione di STP basato su Cisco IOS supporta il comando show spanning-tree inconsistentports.

Nella maggior parte dei casi, il motivo per cui è stata rilevata un'incoerenza STP sul porto è evidente:

- La porta di accesso riceve una BPDU SSTP con tag IEEE 802.1Q.

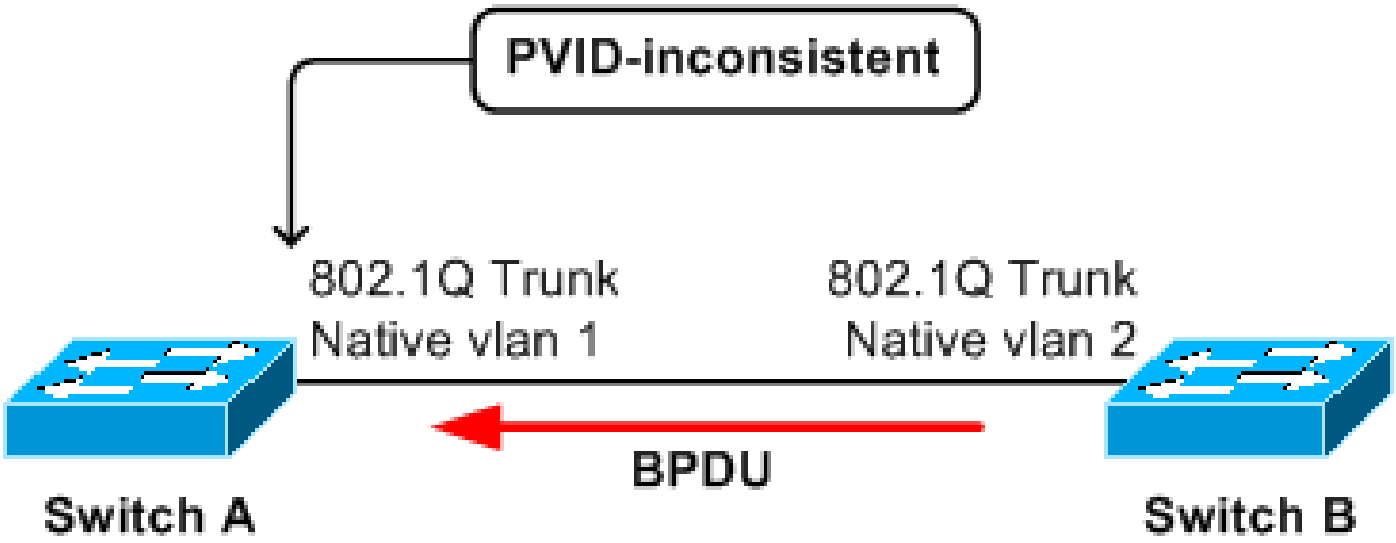


In questo scenario, la porta di accesso sul bridge A riceve, dal bridge B, una PVST+ BPDU con tag da STP di una VLAN diversa da 1. La porta sul bridge A può essere messa in stato di incoerenza di tipo.



Nota: Non è necessario che gli switch siano collegati direttamente; se sono connessi tramite uno o più switch IEEE 802.1D o IEEE 802.1Q, o anche hub, l'effetto è lo stesso.

- La porta trunking IEEE 802.1Q riceve una BPDU SSTP non codificata con un tipo, una lunghezza e un valore VLAN (TLV) che non corrisponde alla VLAN su cui è stata ricevuta la BPDU.



In questo scenario, la porta trunk su A riceve una PVST+ BPDU da STP della VLAN 2 con un tag della VLAN 2. Questo attiva il blocco della porta su A sia sulla VLAN 1 che sulla VLAN 2.

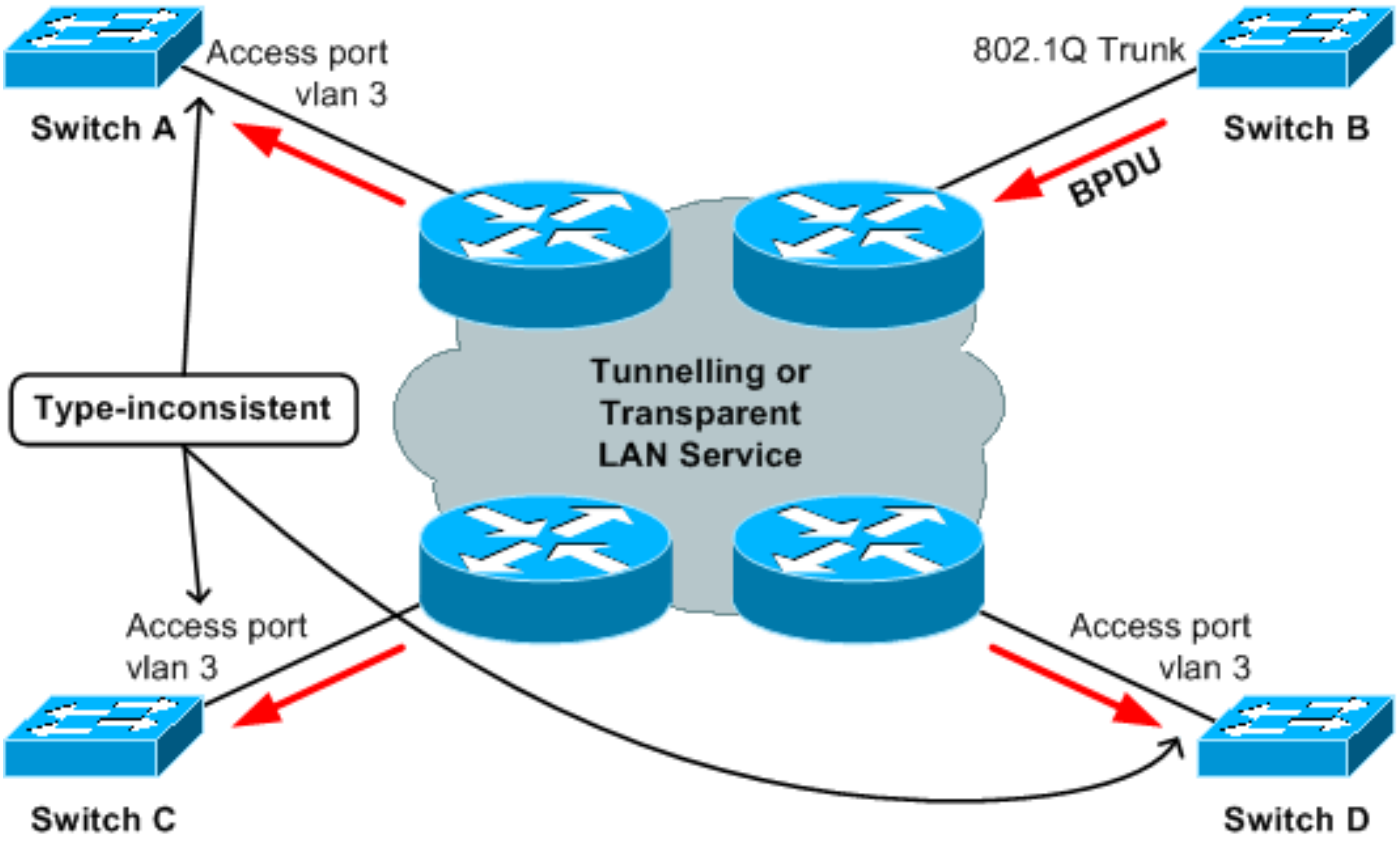
Se i dispositivi su entrambe le estremità di un collegamento point-to-point sono switch Cisco Catalyst, un esame della configurazione delle porte locale e remota in genere rivela una mancata corrispondenza della configurazione:

- La porta è configurata per il trunking IEEE 802.1Q su un lato ma l'altro lato è la porta di accesso.
- I trunk IEEE 802.1Q sono su entrambi i lati, ma le VLAN native sono diverse.

In questi casi, correggere la mancata corrispondenza della configurazione per risolvere l'incoerenza STP.

In alcuni casi, è più difficile identificare il motivo:

- Viene ricevuta una BPDU da un supporto condiviso con più dispositivi.
- Viene ricevuta una BPDU dal cloud di switch che implementa un modello STP IEEE 802.1D o 802.1Q mentre gli switch PVST+ sono connessi al cloud.
- Una BPDU proviene da dietro un tunnel (ad esempio, Data Link Switch Plus [DLSw+] cloud, tunneling del protocollo L2, EoMPLS, Virtual Path Link [VPL], LAN Emulation [LANE] e altri).



In questo esempio, lo switch B non è configurato correttamente e inserisce una BPDU SSTP nel cloud. In questo modo, le porte sugli switch A, C e D diventano incoerenti con il tipo.

Il problema è che il dispositivo da cui proviene la BPDU in conflitto non è collegato direttamente agli switch interessati.

Pertanto, con molti dispositivi sul trunk, la risoluzione di tutti i problemi può richiedere tempo.

Fortunatamente, esiste un approccio sistematico alla risoluzione di questo problema:

1. Stabilire l'indirizzo MAC di origine e l'ID bridge di invio della BPDU. Questa operazione deve essere eseguita mentre si verifica il problema.

2. Trovare il bridge da cui proviene la BPDU in conflitto. Questa operazione può essere eseguita in un secondo momento, non necessariamente quando si verifica il problema.

Per il passo 1, normalmente sono disponibili due opzioni: usare un analizzatore di pacchetti o abilitare il debug per visualizzare il dump delle BPDU ricevute.

Per ulteriori informazioni sull'uso del comando debug per eseguire il dump delle BPDU STP, consultare la sezione Use STP Debug Commands in Risoluzione dei problemi STP sugli switch Catalyst.

Questo è un esempio di output di debug che mostra la BPDU ricevuta:

```
*Mar 14 19:33:27: STP SW: PROC RX: 0100.0ccc.cccd<-0030.9617.4f08 type/len 0032
*Mar 14 19:33:27:     encap SNAP linktype sstp vlan 10 len 64 on v10 Fa0/14
```

```
*Mar 14 19:33:27:     AA AA 03 00000C 010B SSTP
*Mar 14 19:33:27:     CFG P:0000 V:00 T:00 F:00 R:8000 0050.0f2d.4000 00000000
*Mar 14 19:33:27:     B:8000 0050.0f2d.4000 80.99 A:0000 M:1400 H:0200 F:0F00
*Mar 14 19:33:27:     T:0000 L:0002 D:0001
```

Dopo aver conosciuto l'indirizzo MAC di origine e l'ID bridge di invio, è necessario trovare il dispositivo a cui appartiene l'indirizzo MAC. Questa situazione può essere complicata dal fatto che gli switch in genere non imparano gli indirizzi MAC di un'origine dai frame BPDU.

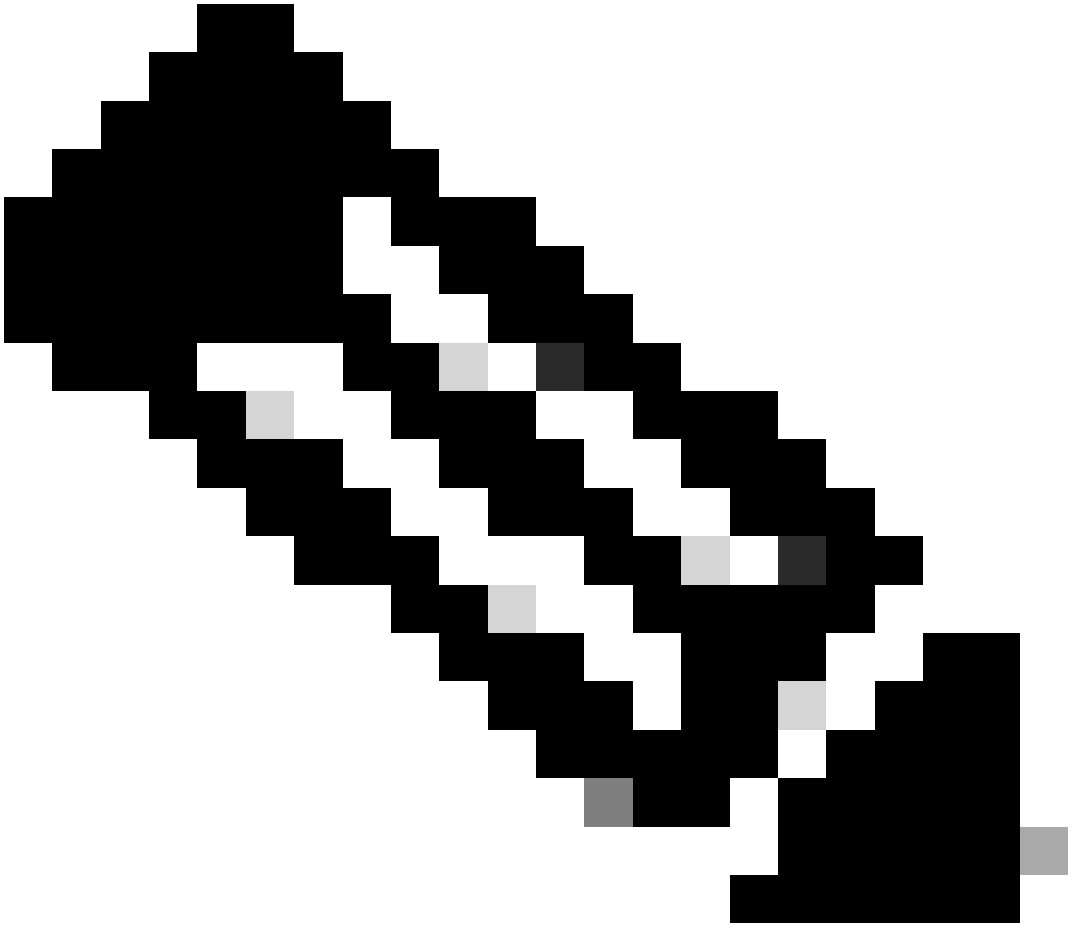
Se si esegue il comando show mac-address-table addressBPDU_mac_address (per gli switch con Cisco IOS), in genere non viene trovata alcuna voce.

Per trovare l'indirizzo MAC dannoso, è possibile raccogliere da tutti gli switch connessi al cloud l'output del comando show spanning-tree.

Questi output del comando includono informazioni sull'ID di ciascun bridge.

<#root>

```
Boris#

show spanning-tree


!--- Use with Cisco IOS.

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    0
             Address     0007.4f1c.e847
             Cost        131
             Port        136 (GigabitEthernet3/8)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00d0.003f.8800

!--- Output suppressed.
```



Nota: In base al modello, alla versione software e alla configurazione, uno switch può avere più indirizzi MAC di ID bridge. Fortunatamente, tutti gli indirizzi possono in genere essere compresi in un determinato intervallo, ad esempio da 0001.1234.5600 a 0001.1234.5640. Se si conosce un indirizzo MAC di ID bridge, è possibile controllare se l'indirizzo MAC di ID bridge inviato (individuato nel passaggio 1) rientra nell'intervallo di indirizzi MAC di ID bridge specificati. È inoltre possibile utilizzare gli strumenti di gestione della rete per raccogliere gli ID di tutti i bridge.

Dopo aver trovato il bridge che ha inviato la BPDU in conflitto, è necessario verificare la configurazione della porta collegata al cloud: verificare che sia coerente (con il trunking in contrapposizione alla VLAN nativa e non trunking) con altri switch connessi allo stesso cloud.

Potrebbe accadere che il bridge invii le BPDU corrette, ma queste vengono modificate in modo errato all'interno del cloud di tunneling. In questo caso, è possibile notare che la BPDU in conflitto che entra nel cloud è coerente con la configurazione degli altri bridge, ma la stessa BPDU diventa incoerente quando esce dal cloud (ad esempio, la BPDU esce dal cloud in una VLAN diversa o diventa con o senza tag). In questo caso, è possibile verificare se l'indirizzo MAC di origine della

BPDU in conflitto appartiene allo stesso bridge dell'ID bridge di invio.

In caso contrario, è possibile provare a individuare il bridge proprietario dell'indirizzo MAC di origine della BPDU e verificarne la configurazione.

Per individuare lo switch proprietario dell'indirizzo MAC di origine della BPDU, è possibile usare lo stesso approccio (per trovare l'ID del bridge), a eccezione del fatto che ora l'output del comando show module viene ispezionato (per Catalyst 4000 e 6000). Per altri switch Catalyst, è possibile esaminare l'output del comando show interface per visualizzare gli indirizzi MAC che appartengono alle porte.

<#root>

```
Cat4000-#
```

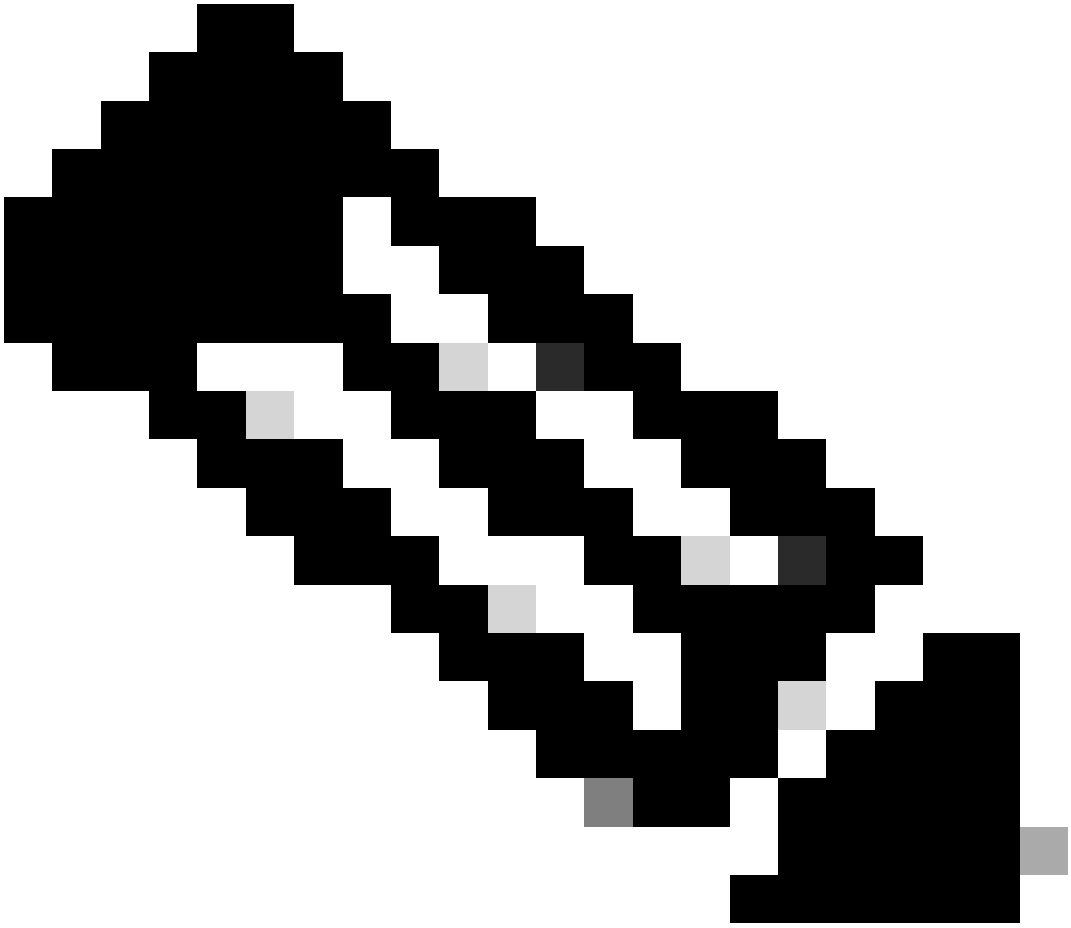
show module

```
!--- Use for Catalyst 4000,5000,6000

Mod  Ports Card Type                              Model              Serial No.
----+-----+-----------------------------------------+-----------------+-----------
 1      2  1000BaseX (GBIC) Supervisor(active)    WS-X4515           ZZZ00000001
 5     14  1000BaseT (RJ45), 1000BaseX (GBIC)     WS-X4412-2GB-T     ZZZ00000002

 M MAC addresses                    Hw  Fw           Sw               Status
--+--------------------------------+---+------------+----------------+---------
 1 000a.4172.ea40 to 000a.4172.ea41 1.2 12.1(12r)EW  12.1(14)E1, EARL Ok
 5 0001.4230.d800 to 0001.4230.d80d 1.0                                Ok

!--- Output suppressed.
```

```
cat3550#
```

show interface | i bia

```
  Hardware is Gigabit Ethernet, address is 0002.4b28.da80 (bia 0002.4b28.da80)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da83 (bia 0002.4b28.da83)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da86 (bia 0002.4b28.da86)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da88 (bia 0002.4b28.da88)
  Hardware is Gigabit Ethernet, address is 0002.4b28.da89 (bia 0002.4b28.da89)

!--- Output suppressed.
```



Nota: Se il cloud è DLSw+, fare riferimento alla sezione sulla descrizione e configurazione di DLSw e 802.1Q

Informazioni correlate

- Supporto dei prodotti LAN/Spanning Tree Protocol
- Supporto tecnologico
- Supporto tecnico Cisco e download

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).