Probleemoplossing bij Spanning Tree PVID- en type-inconsistenties

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met twee STP-inconsistenties (Spanning Tree Protocol), poort-VLAN-id (PVID) en type.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van STP-concepten.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- of hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

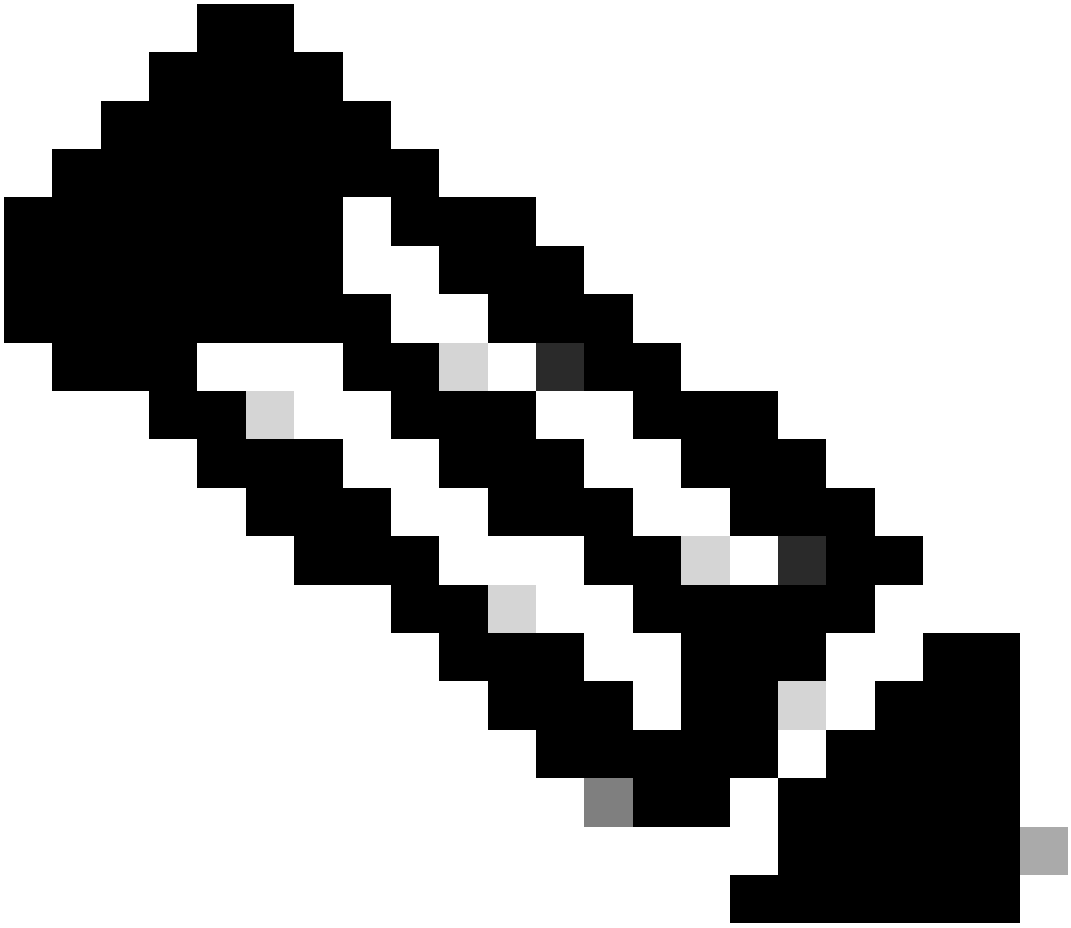
Bij L2-netserken (Layer 2) netwerken kan er slechts één pad bestaan tussen twee apparaten. Spanning-Tree Protocol (STP) ondersteunt redundantie en detecteert en blokkeert redundante paden om zo de vorming van doorstuurlussen te voorkomen. Bepaalde onjuiste configuraties kunnen resulteren in STP-fouten en netwerkuitval veroorzaken. Om downtime te voorkomen zijn bepaalde verbeteringen geïmplementeerd zodat STP bepaalde gevallen van verkeerde configuratie detecteert en de betreffende poort in een "inconsistente" staat wordt gezet.

Er kunnen verschillende soorten STV-inconsistenties zijn:

- Lus-inconsistentie—Dit wordt gedetecteerd door de functie Lijn bewaken. Raadpleeg STP configureren met behulp van Loop Guard en BPDU Skew Detection voor meer informatie.
- Root inconsistentie—Dit wordt gedetecteerd door de Root Guard-functie. Raadpleeg Spanning Tree Protocol met Root Guard voor meer informatie.
- EtherChannel-inconsistentie—Dit wordt gedetecteerd door de EtherChannel-consistentiedetectiefunctie. Raadpleeg Inconsistentiedetectie in EtherChannel voor meer informatie.
- Inconsistentie-A per-VLAN Spanning Tree (PVST+) Bridge Protocol Data Unit (BPDU) wordt ontvangen op een ander VLAN dan dat het gegenereerd is: (`Port VLAN ID` Mismatchor`*PVID_Inc`).
- Type inconsistentie—Een PVST+ BPDU wordt ontvangen op een niet-802.1Q trunk.

Theorie achter PVID- en type-inconsistenties

Cisco Catalyst switches implementeren PVST die Inter-Switch Link (ISL)-trunks gebruiken. Dankzij de ondersteuning van IEEE 802.1Q- en ISL-trunking was er een manier nodig voor samenwerking tussen PVST en het IEEE 802.1Q-concept van één overspanningsstructuur voor alle VLAN's. De PVST+-functie is geïntroduceerd om aan deze eis te voldoen.



Opmerking: vanuit het STP-standpunt is IEEE 802.1D niet VLAN-bewust en IEEE 802.1Q is VLAN-bewust, maar maakt gebruik van één STP-instantie voor alle VLAN's. Namelijk als de haven toen blokkeert het voor alle VLANs op die haven blokkeert.

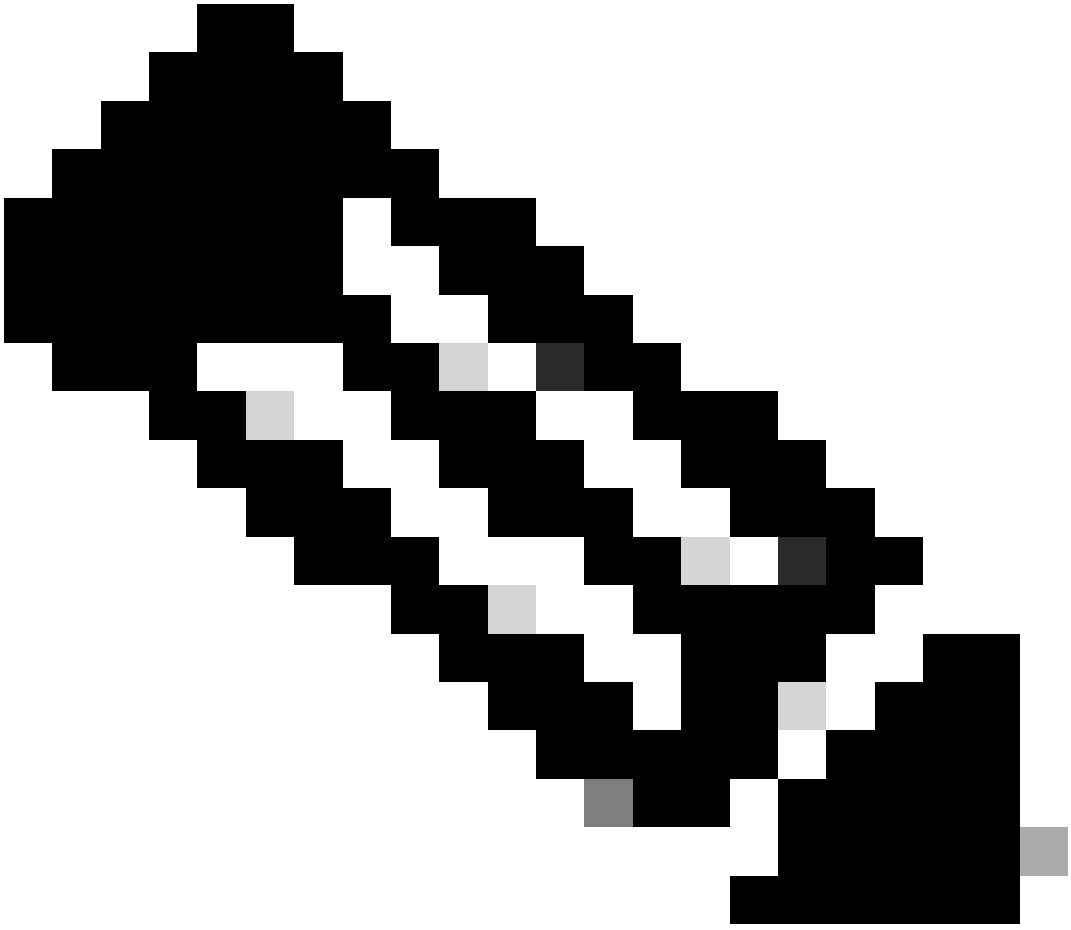
Het zelfde is waar voor het door:sturen.

Deze lijst toont hoe PVST+ met IEEE 802.1Q of IEEE 802.1D interopereert, als het native VLAN op een IEEE 802.1Q-trunk VLAN 1 is:

- VLAN 1 STP BPDU's worden naar het IEEE STP MAC-adres (0180.c200.0000) verzonden, zonder label.
- VLAN 1 STP BPDUs worden ook verzonden naar het adres van PVST+ MAC, untagged.
- Niet-VLAN 1 STP BPDUs worden verzonden naar het PVST+ MAC-adres (ook wel het Shared Spanning Tree Protocol (SSTP) MAC-adres, 0100.0cc.cccd genoemd), getagd met een corresponderende IEEE 802.1Q VLAN-tag.

Als het native VLAN op een IEEE 802.1Q-trunk niet VLAN 1 is:

- VLAN 1 STP BPDU’s worden naar het PVST+ MAC-adres verzonden, getagd met een corresponderende IEEE 802.1Q VLAN-tag.
- VLAN 1 STP BPDU’s worden ook verzonden naar het IEEE STP MAC-adres op het native VLAN van de IEEE 802.1Q-trunk, zonder tags.
- Niet-VLAN 1 STP BPDU's worden naar het PVST+ MAC-adres verzonden, getagd met een corresponderende IEEE 802.1Q VLAN-tag.



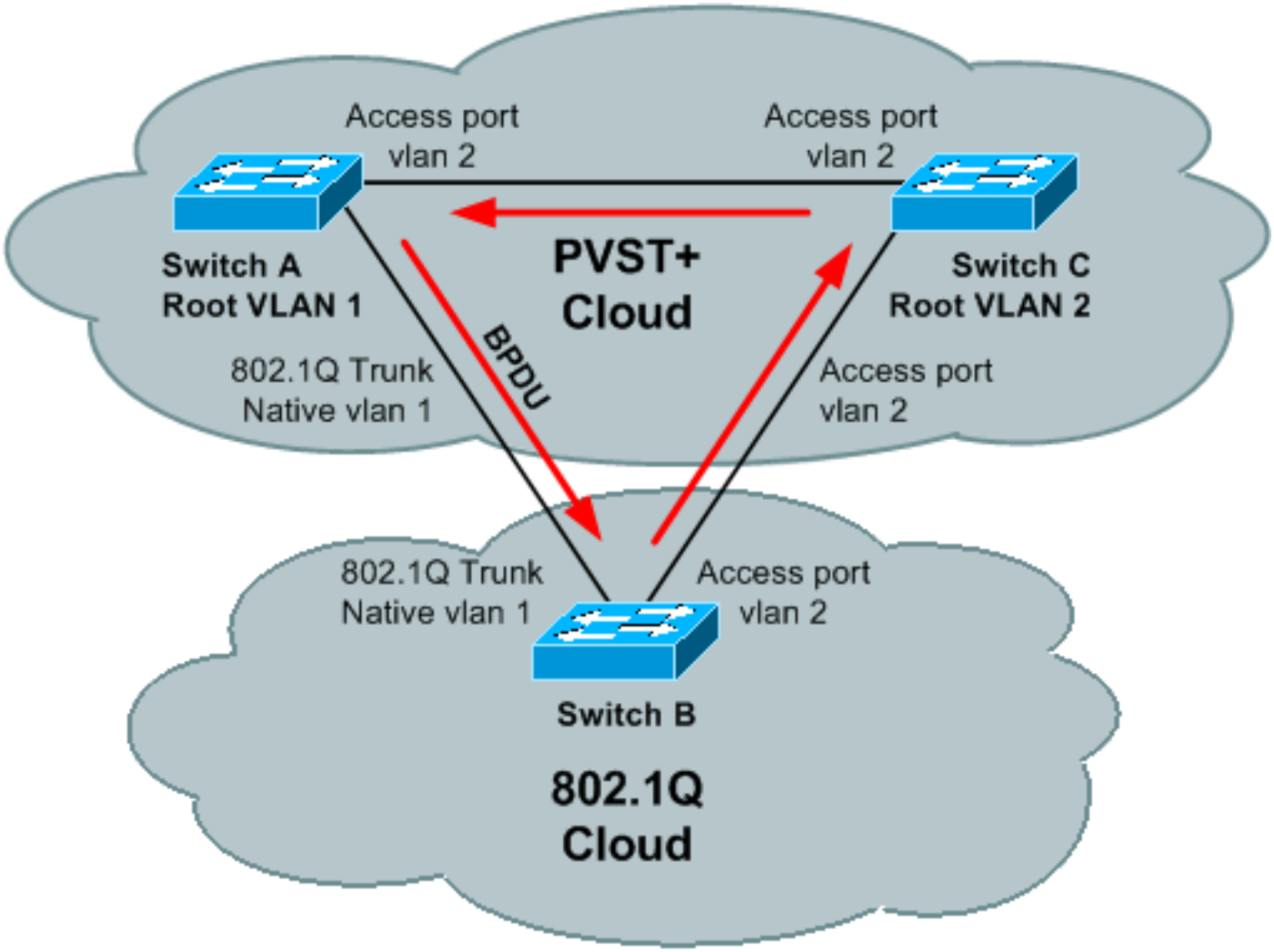
Opmerking: native VLAN STP BPDU's worden zonder tags verzonden.

Op deze manier wordt VLAN 1 STP van PVST+ samengevoegd met STP van IEEE 802.1D of 802.1Q, terwijl andere VLAN’s worden getunneld door de cloud van IEEE 802.1D- of 802.1Q-bruggen. Zo ziet de IEEE 802.1D- of 802.1Q-cloud er bijvoorbeeld hetzelfde uit als een "bedrading" voor andere PVST+ VLAN’s dan 1.

Neem voor een juiste werking van STP bepaalde regels in acht wanneer u PVST+-bruggen aansluit op IEEE 802.1D- of 802.1Q-bruggen. De belangrijkste regel is dat PVST+-bruggen via een IEEE 802.1Q-trunk met IEEE 802.1D- of 802.1Q-bruggen verbonden moeten zijn met een consistent Native VLAN op alle bruggen die verbinding maken met de cloud van IEEE 802.1Q- of 802.1D-bruggen.

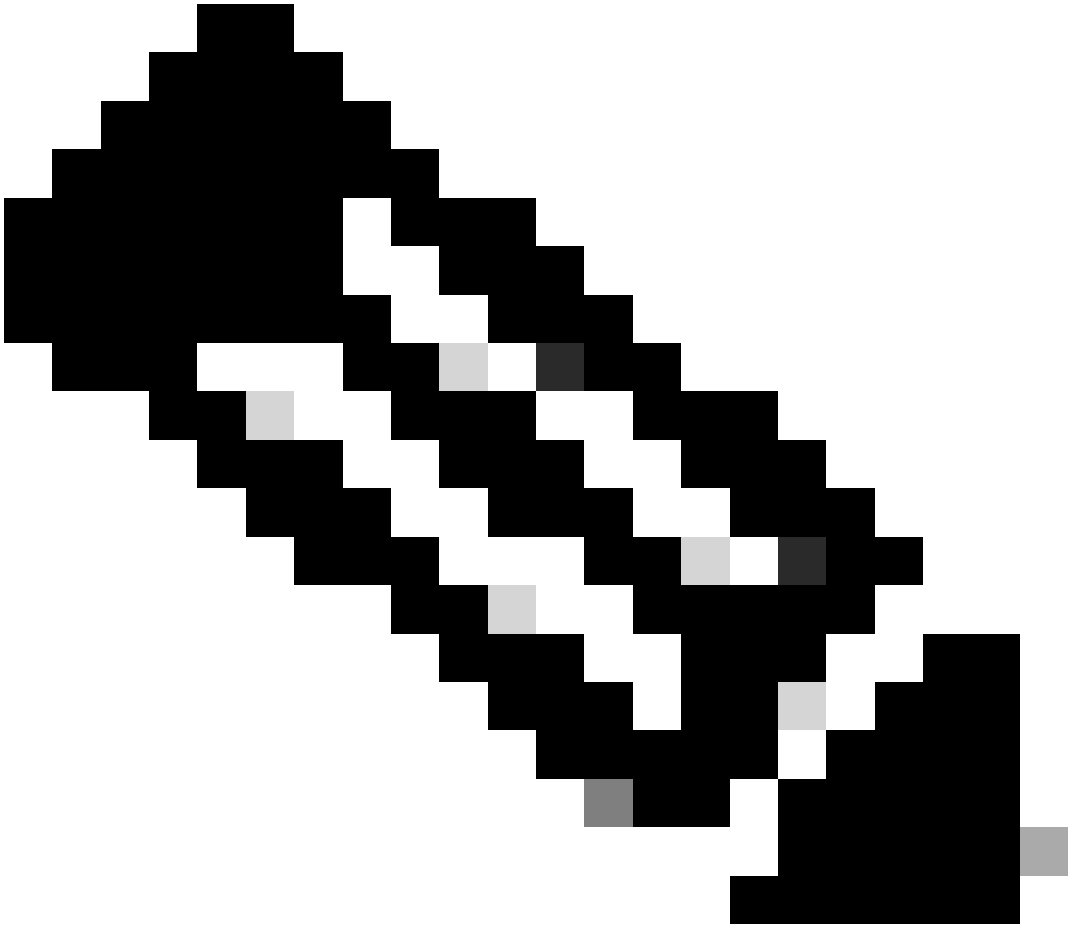
PVST+ BPDU bevat een VLAN-nummer waarmee PVST+-bruggen kunnen detecteren of de vorige regel niet wordt nageleefd. Wanneer een Catalyst switch een foutieve configuratie detecteert, worden de bijbehorende poorten in een status "PVID-inconsistent" of "type-inconsistent" gezet, die effectief het verkeer in het corresponderende VLAN op een corresponderende poort blokkeert. Deze staten verhinderen het door:sturen van lijnen die door misconfiguratie worden veroorzaakt of verkeerd geprogrammeerd waren.

Om de behoefte aan inconsistentiedetectie te illustreren, overweeg deze topologie, waar switches A en C PVST+ STP in werking stellen en switch B 802.1Q STP in werking stelt:



Als BPDU van de wortel in VLAN 1 beter is dan BPDU van de wortel in VLAN 2 dan is er geen blokkerende haven in VLAN 2 topologie. BPDU van VLAN 2 maakt nooit een "volledige cirkel" rond de topologie; het wordt vervangen door VLAN 1 BPDU op de verbinding B-C, omdat B slechts één STP in werking stelt die met VLAN 1 STP van PVST+ wordt samengevoegd. Er is dus een voorwaartse lus. Gelukkig, switch A verzendt PVST+ BPDUs van VLAN 2 (naar het adres

SSTP dat door switch B) wordt overstroomd naar switch C. Switch C kan haven C-B in een type-inconsistente staat zetten, die de lijn verhindert.

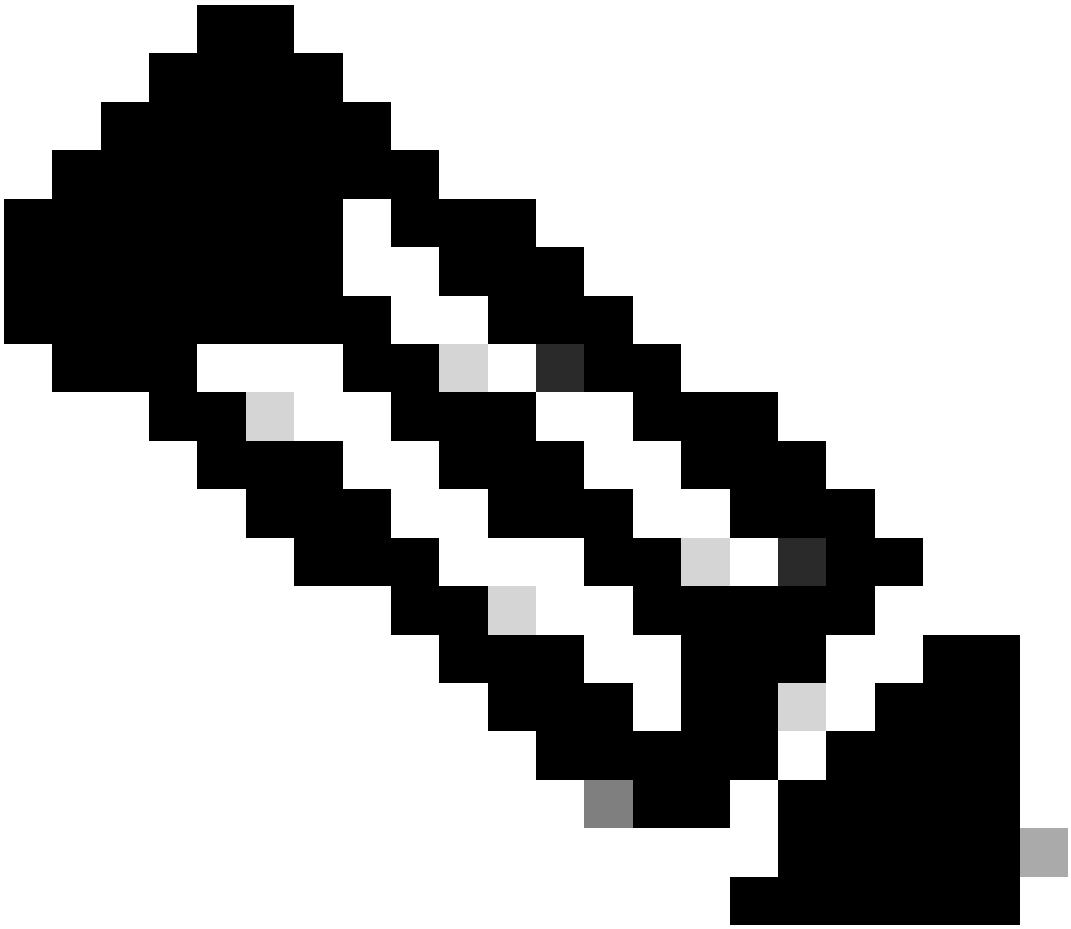


Opmerking: in sommige opdrachtoutput wordt de *-inconsistente STP-status "broken" genoemd.

Wanneer STP-inconsistentie wordt gedetecteerd, verzenden switches deze syslogberichten:

```
%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
```

In dat voorbeeld, is VLAN 1 waar BPDU werd ontvangen, en VLAN 10 is waar BPDU is voortgekomen. Wanneer inconsistentie wordt gedetecteerd, worden beide VLAN's geblokkeerd op de poort waar deze BPDU wordt ontvangen.



Opmerking: berichten kunnen variëren op basis van het type en de versie van de Cisco IOS®-softwarerelease die in gebruik zijn.

Bericht, als de haven niet meer inconsistente BPDUs ontvangt, wordt de *-inconsistente staat ontruimd en STP verandert de havenstaat die op normale verrichting STP wordt gebaseerd. Er wordt een syslogbericht verzonden om de wijziging aan te geven:

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

Raadpleeg voor meer informatie over PVST+-werking Spanning Tree van PVST+ naar Rapid-

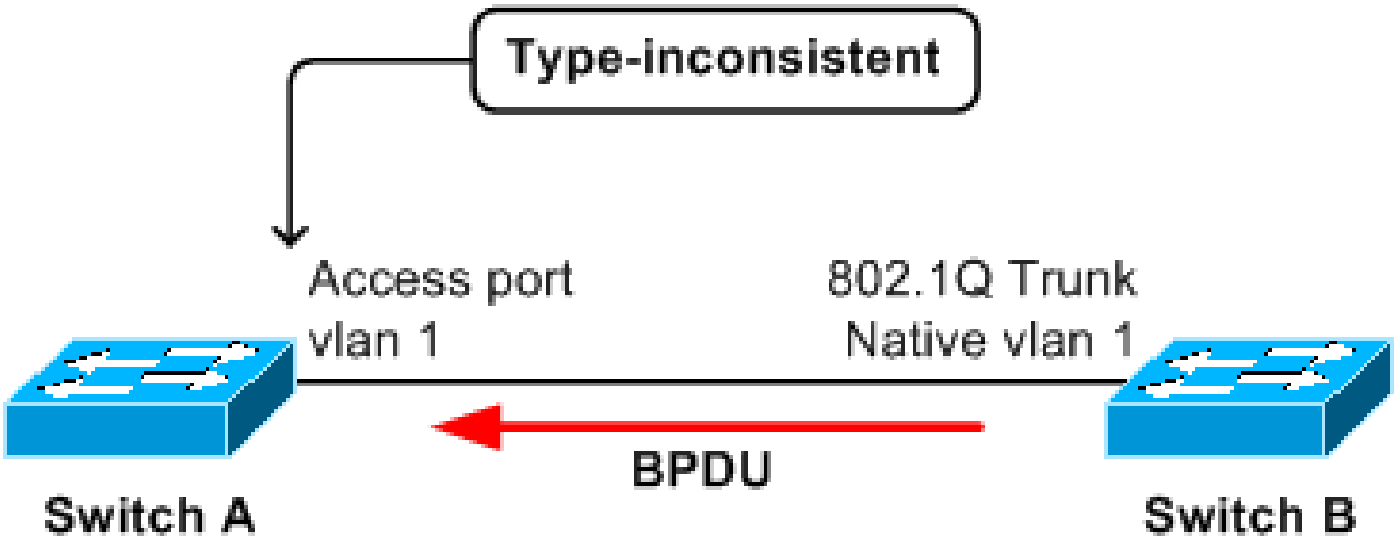
PVST Migration Configuration Voorbeeld.

Problemen oplossen

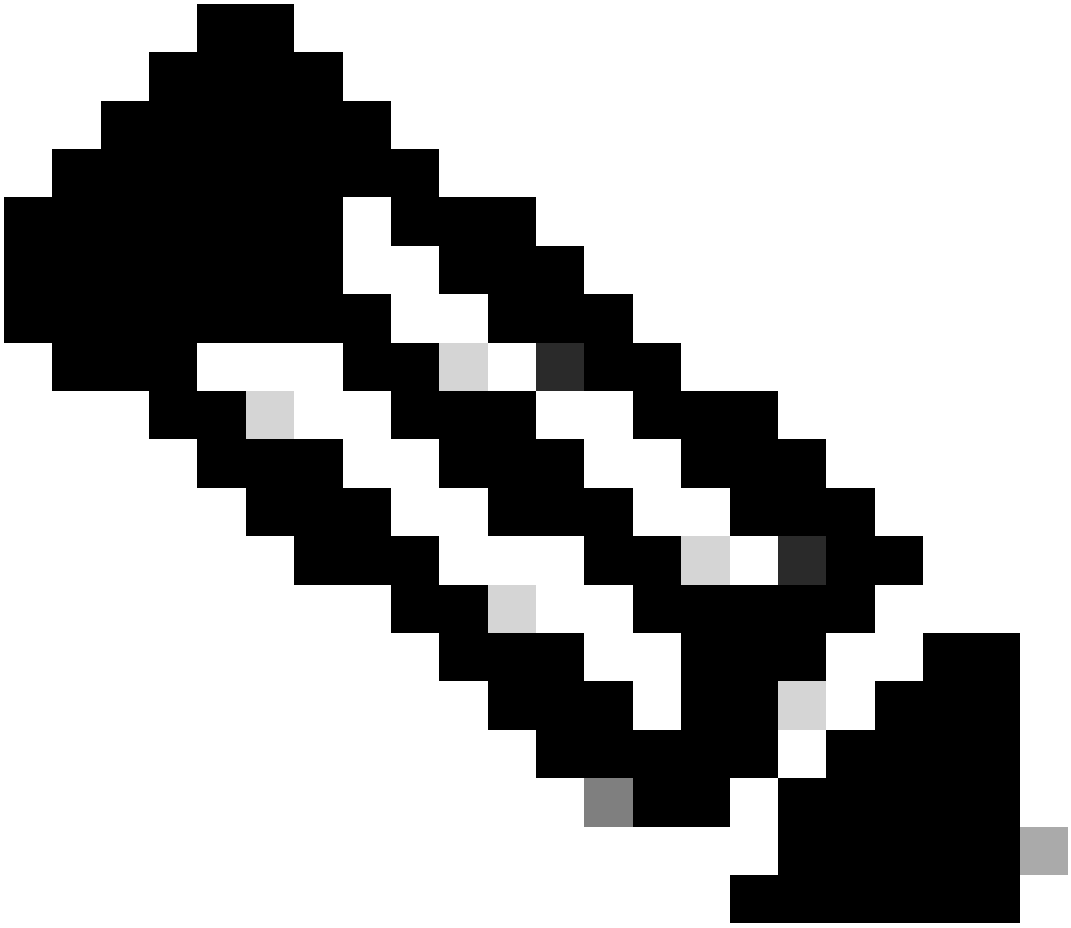
Om de lijst met inconsistente poorten te zien, ondersteunt recente Cisco IOS-gebaseerde STP-implementatie de opdracht show Spanning-Tree inconsistente poorten.

In de meeste gevallen is de reden voor de detectie van STV-inconsistentie op de poort duidelijk:

- Access port ontvangt een IEEE 802.1Q-getagd SSTP BPDU.

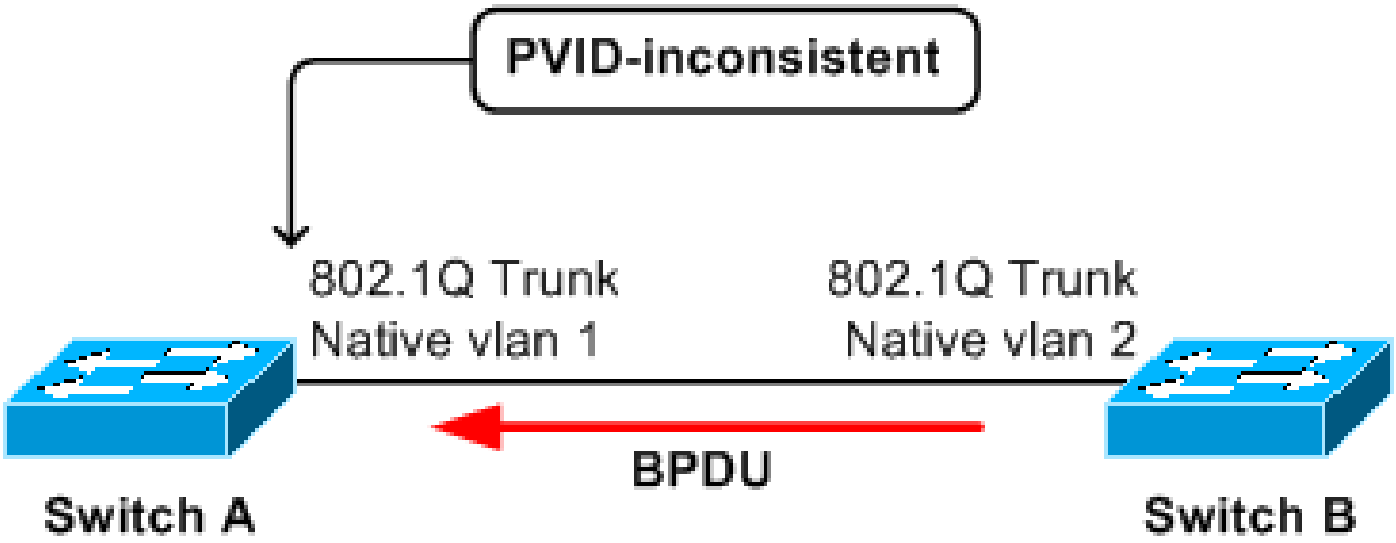


In dit scenario, ontvangt de toegangshaven op brug A, van brug B, een geëtiketteerde PVST+ BPDU van STP van VLAN buiten 1. De poort op A kan in een type-inconsistente staat gezet worden.



Opmerking: de switches hoeven niet rechtstreeks te worden verbonden. Als ze via een of meer IEEE 802.1D- of IEEE 802.1Q-switches worden verbonden, of zelfs via hubs, is het effect hetzelfde.

- De IEEE 802.1Q-trunkingpoort ontvangt een niet-gelabelde SSTP BPDU met een VLAN-type, lengte, waarde (TLV) dat niet overeenkomt met het VLAN waar de BPDU is ontvangen.



In dit scenario ontvangt de trunkpoort op A een PVST+ BPDU van STP van VLAN 2 met een tag van VLAN 2. Hierdoor wordt de poort op A geactiveerd die in zowel VLAN 1 als VLAN 2 moet worden geblokkeerd.

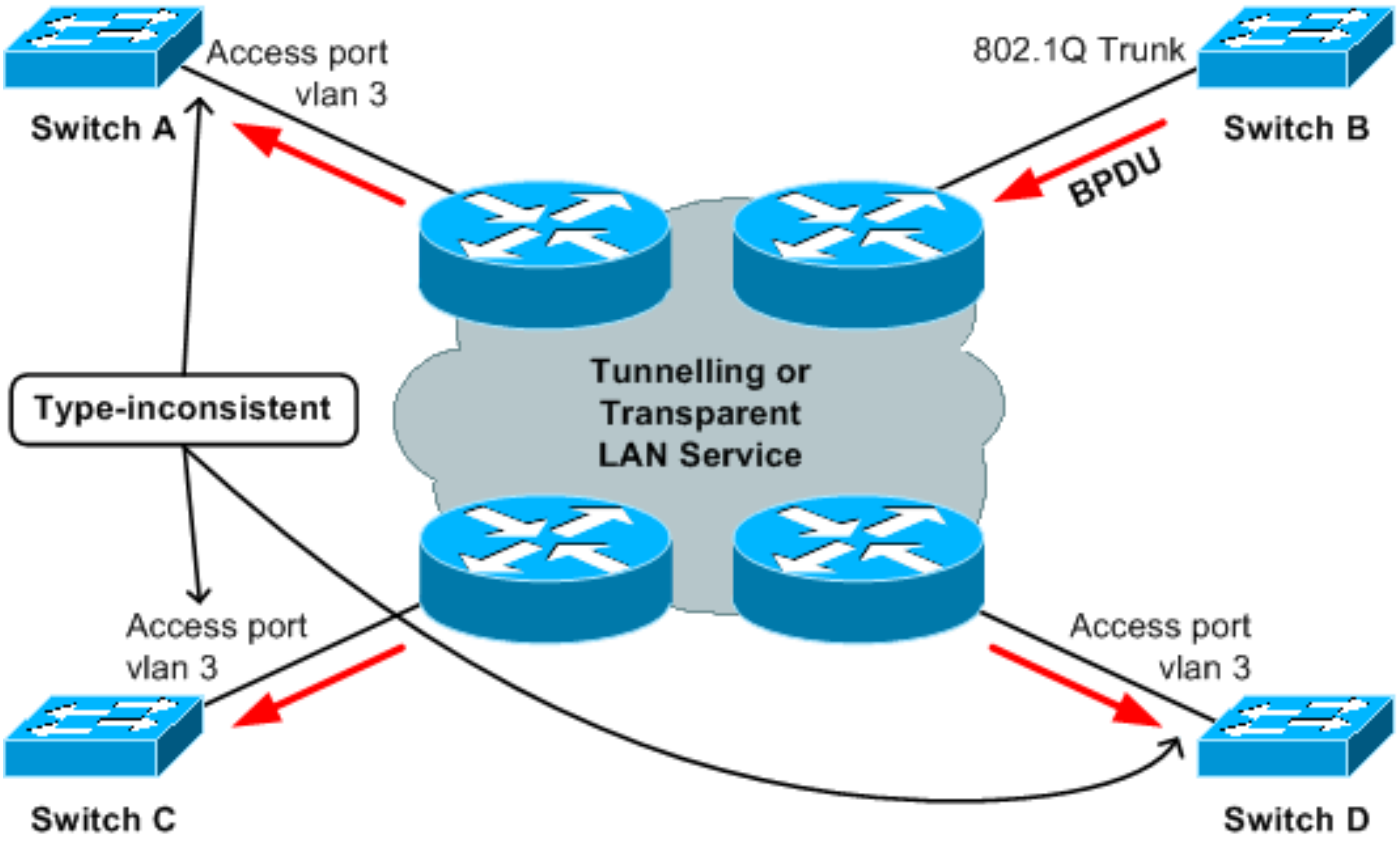
Als apparaten aan beide uiteinden van een point-to-point link Cisco Catalyst-switches zijn, wordt door een onderzoek van de lokale en externe poortconfiguratie doorgaans de configuratiewanverhouding blootgelegd:

- De poort is aan de ene kant geconfigureerd voor IEEE 802.1Q trunking, maar aan de andere kant is de toegangspoort.
- De IEEE 802.1Q-trunks bevinden zich aan beide zijden, maar de native VLAN's zijn verschillend.

In deze gevallen, bevestig de configuratiewanverhouding om de inconsistentie op te lossen STP.

In sommige gevallen is het moeilijker de reden te achterhalen:

- Een BPDU wordt ontvangen van een gedeelde media met meerdere apparaten.
- Er wordt een BPDU ontvangen vanuit de switch-cloud, die een IEEE 802.1D- of 802.1Q STP-model implementeert terwijl PVST+-switches zijn verbonden met de cloud.
- Een BPDU komt van achter sommige tunnels (bijvoorbeeld Data Link Switch Plus [DLSw+] cloud, L2-protocoltunneling, EoMPLS, Virtual Path Links [VPLs], LAN Emulation [LANE] en anderen).



In dit voorbeeld is switch B verkeerd geconfigureerd en injecteert een SSTP BPDU in de cloud. Dit zorgt ervoor dat de poorten op de switches A, C en D inconsistent worden met het type. Het probleem is dat het apparaat dat de "beledigende" BPDU genereert niet rechtstreeks is verbonden met de getroffen switches. Aldus, met vele apparaten op de boomstam, kan het tijd verbruiken om elk van hen problemen op te lossen.

Gelukkig is er een systematische benadering voor het oplossen van dit probleem:

1. Vestig het adres van bronMAC en het verzenden van brug-ID van BPDU. Dit moet gebeuren terwijl de kwestie zich voordoet
2. Vind de brug die de "beledigende" BPDU voortbrengt. Dit kan op een later tijdstip worden gedaan, niet noodzakelijk wanneer de kwestie zich voordoet.

Voor Stap 1 zijn er normaal twee opties: gebruik een pakketanalyzer of schakel debug in om de dump van ontvangen BPDU's te zien.

Zie de sectie STP-debugopdrachten gebruiken in het gedeelte Problemen met de STP-oplossing op Catalyst-Switches voor meer informatie over het gebruik van een debug om STP BPDU's te dumpen.

Dit is een voorbeeld van debug-uitvoer die ontvangen BPDU toont:

```
*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
```

Zodra u het adres van bron-MAC kent en bridge-id verstuurt, moet u het apparaat vinden waar dit MAC-adres toe behoort. Dit kan worden gecompliceerd door het feit dat de switches typisch niet de adressen van MAC van een bron van BPDU kaders leren. Als u de opdracht show mac-address-table addressBPDU_mac_address uitgeeft (voor Cisco IOS-gebaseerde switches), wordt doorgaans geen ingang gevonden.

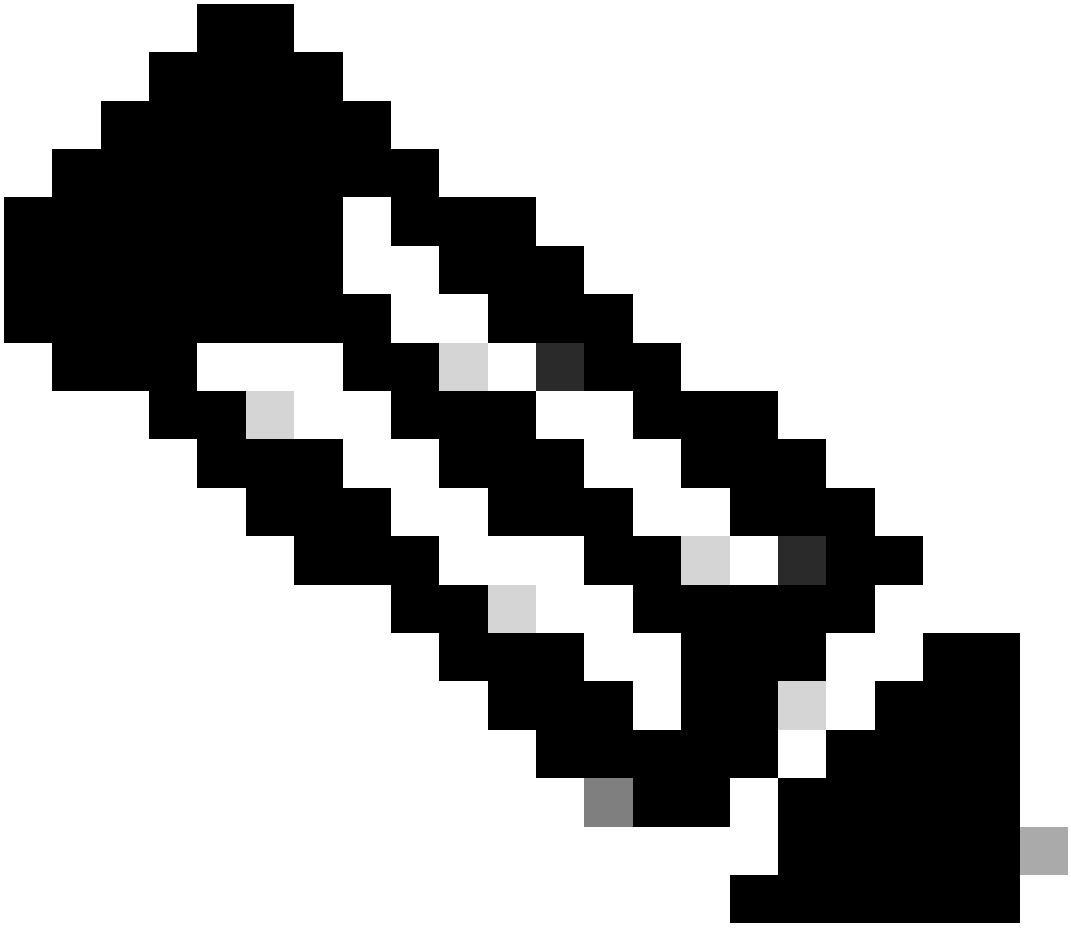
Een manier om het "beledigende" MAC-adres te vinden is om, van alle switches die zijn verbonden met de cloud, output te verzamelen van de show Spanning-Tree opdracht. Deze opdrachtoutput bevat informatie over de bridge-id van elke brug.

<#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.
```



Opmerking: op basis van het model, de softwareversie en de configuratie, kan een switch meerdere bridge-id MAC-adressen hebben. Gelukkig, kunnen alle adressen typisch in een bepaald bereik zijn (bijvoorbeeld van 0001.1234.5600 tot 0001.1234.5640). Als u één adres van MAC van brugID kent dan kunt u controleren of het verzonden adres van MAC van brug-ID (gevonden in Stap 1) binnen de waaier van bepaalde adressen van MAC van brug-ID valt. U kunt ook netwerkbeheertools gebruiken om de brug-ID's van alle bruggen te verzamelen.

Zodra u de brug hebt gevonden die de beledigende BPDU heeft verzonden, moet u de configuratie van de poort die aan de cloud is gekoppeld verifiëren: zorg ervoor dat deze consistent is (trunking in plaats van niet-trunking en Native VLAN) met andere switches die ook met dezelfde cloud zijn verbonden.

Het zou kunnen gebeuren dat de brug juiste BPDUs verzendt, maar zij worden verkeerd gewijzigd binnen de tunnelwolk. In dat geval kunt u zien dat de beledigende BPDU die in de cloud komt, consistent is met de configuratie van de andere bruggen, maar dezelfde BPDU wordt inconsistent wanneer hij de cloud verlaat (bijvoorbeeld de BPDU verlaat de cloud in een ander VLAN, of wordt

gelabeld of niet gelabeld). In een dergelijk geval kan het helpen om te controleren of het MAC-adres van de aanstootgevende BPDU tot dezelfde brug behoort als de verzendende brug-ID. Als dit niet het geval is dan kunt u proberen om van de brug de plaats te bepalen die het adres bron van MAC van BPDU bezit en zijn configuratie verifiëren.

Om de switch te vinden die het bron-MAC-adres van de BPDU bezit, kunt u dezelfde aanpak gebruiken (om de bridge-id te vinden), behalve nu wordt de opdrachtoutput van de showmodule geïnspecteerd (voor Catalyst 4000 en 6000). Voor andere Catalyst switches kunt u de uitvoer van de opdracht show interface onderzoeken om de MAC-adressen te zien die tot de poorten behoren.

<#root>

```
Cat4000-#
```

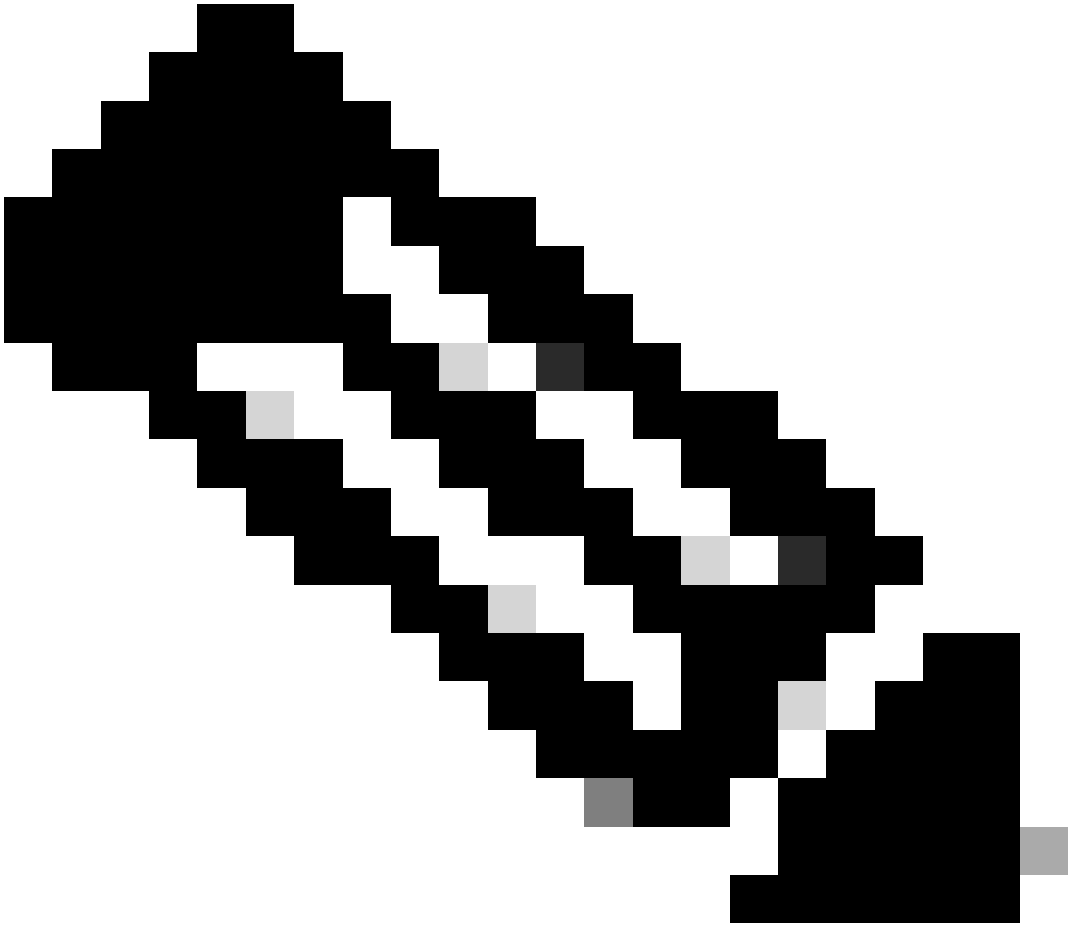
show module

```
!--- 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.
```



Opmerking: Als de cloud DLSw+ is, raadpleegt u Begrijpen en configureren van DLSw en 802.1Q

Gerelateerde informatie

- Productondersteuning voor LAN/Spanning Tree Protocol
- Technologische ondersteuning
- Cisco Technical Support en downloads

Over deze vertaling

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