

スパニングツリーのPVIDの不一致とタイプの不一致のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[PVIDの不一致とタイプの不一致の背景理論](#)

[トラブルシュート](#)

[関連情報](#)

はじめに

このドキュメントでは、2つのスパニングツリープロトコル(STP)の不一致(ポートVLAN ID(PVID)とタイプ)をトラブルシューティングする方法について説明します。

前提条件

要件

STPの概念に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコテクニカルティップスの表記法』を参照してください。

背景説明

レイヤ 2 (L2) ネットワークでは、2 つのデバイス間で可能なパスは 1 つだけです。冗長性はスパニングツリー プロトコル (STP) でサポートされ、STP により冗長なパスが検出されてブロックされ、フォワーディング ループが防止されます。ある種の設定ミスが STP の障害につながって、ネットワークの停止を引き起こす場合があります。ダウンタイムを防ぐために、いくつかの機能拡張が実装され、STP が特定のケースの設定ミスを検出するようになり、関連するポートが「inconsistent」状態になりました。

STP の不一致には、いくつかの種類があります。

- ループの不一致 — ループ ガード機能によって検出されます。詳細については、『[ループガードとBPDUスキュー検出を使用したSTPの設定](#)』を参照してください。
- ルートの不一致 — ルート ガード機能によって検出されます。詳細については、『[ルートガードによるスパニングツリープロトコルの強化](#)』を参照してください。
- EtherChannel の不一致 — EtherChannel の不一致検出機能によって検出されます。詳細については、「EtherChannel の不一致検出について」を参照してください。
- Port VLAN ID(PVID)の不一致 — Per VLAN Spanning Tree(PVST+)Bridge Protocol Data Unit(BPDU)が、発信元とは異なるVLANで受信されます(Port VLAN ID Mismatch or *PVID_Inc)。
- タイプの不一致 — PVST+ BPDUが802.1Q以外のトランクで受信されます。

PVID の不一致とタイプの不一致の背景理論

Cisco Catalystスイッチには、Inter-Switch Link (ISL ; スイッチ間リンク) トランクを使用する PVSTが実装されています。IEEE 802.1Q および ISL トランキングのサポートに伴い、PVST とすべての VLAN に対して単一のスパニングツリーを使用する IEEE 802.1Q の概念を相互運用するための方法が必要でした。PVST+ 機能は、この要件を満たすために導入されました。



注：STPの観点からは、IEEE 802.1DはVLAN対応ではなく、IEEE 802.1QはVLAN対応ですが、すべてのVLANに対して単一のSTPインスタンスを使用します。つまり、ポートがブロッキングされている場合、そのポート上のすべてのVLANに対してブロッキングされています。

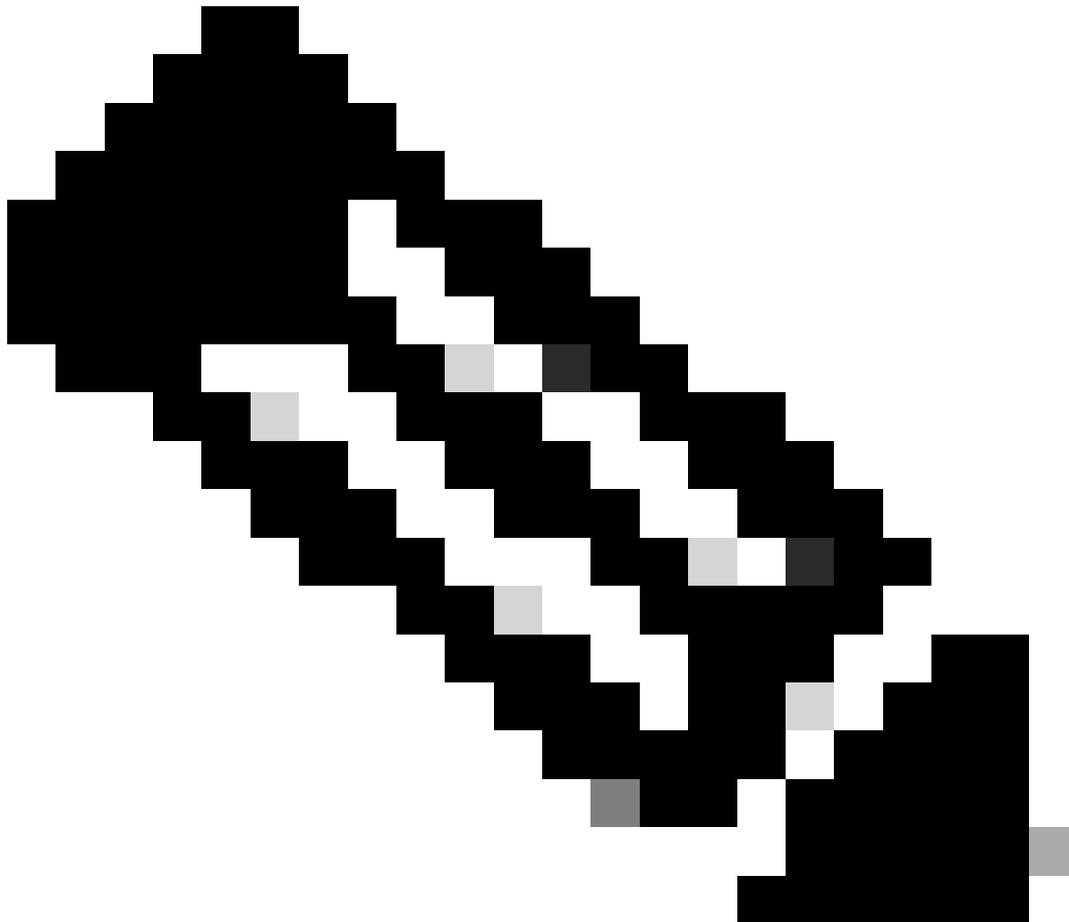
フォワーディングについても同じことが言えます。

以下は、IEEE 802.1Q トランク上のネイティブ VLAN が VLAN 1 の場合に、PVST+ が IEEE 802.1Q または IEEE 802.1D とどのように相互運用されるかを示しています。

- VLAN 1 の STP BPDU が IEEE STP MAC アドレス (0180.c200.0000) に送信される (タグなし)
- VLAN 1 の STP BPDU は PVST+ MAC アドレスにも送信される (タグなし)
- 非VLAN 1のSTP BPDUはPVST+ MACアドレス(共有スパニングツリープロトコル (SSTP)MACアドレス0100.0ccc.cccdとも呼ばれる)に送信され、対応するIEEE 802.1Q VLANタグが付けられます。

IEEE 802.1Q トランク上のネイティブ VLAN が VLAN 1 でない場合：

- VLAN 1 の STP BPDU が PVST+ MAC アドレスに送信される (対応する IEEE 802.1Q VLAN のタグ付き)
 - VLAN 1 の STP BPDU は IEEE 802.1Q トランクのネイティブ VLAN 上の IEEE STP MAC アドレスにも送信される (タグなし)
 - VLAN 1 以外の STP BPDU が PVST+ MAC アドレスに送信される (対応する IEEE 802.1Q VLAN のタグ付き)
-



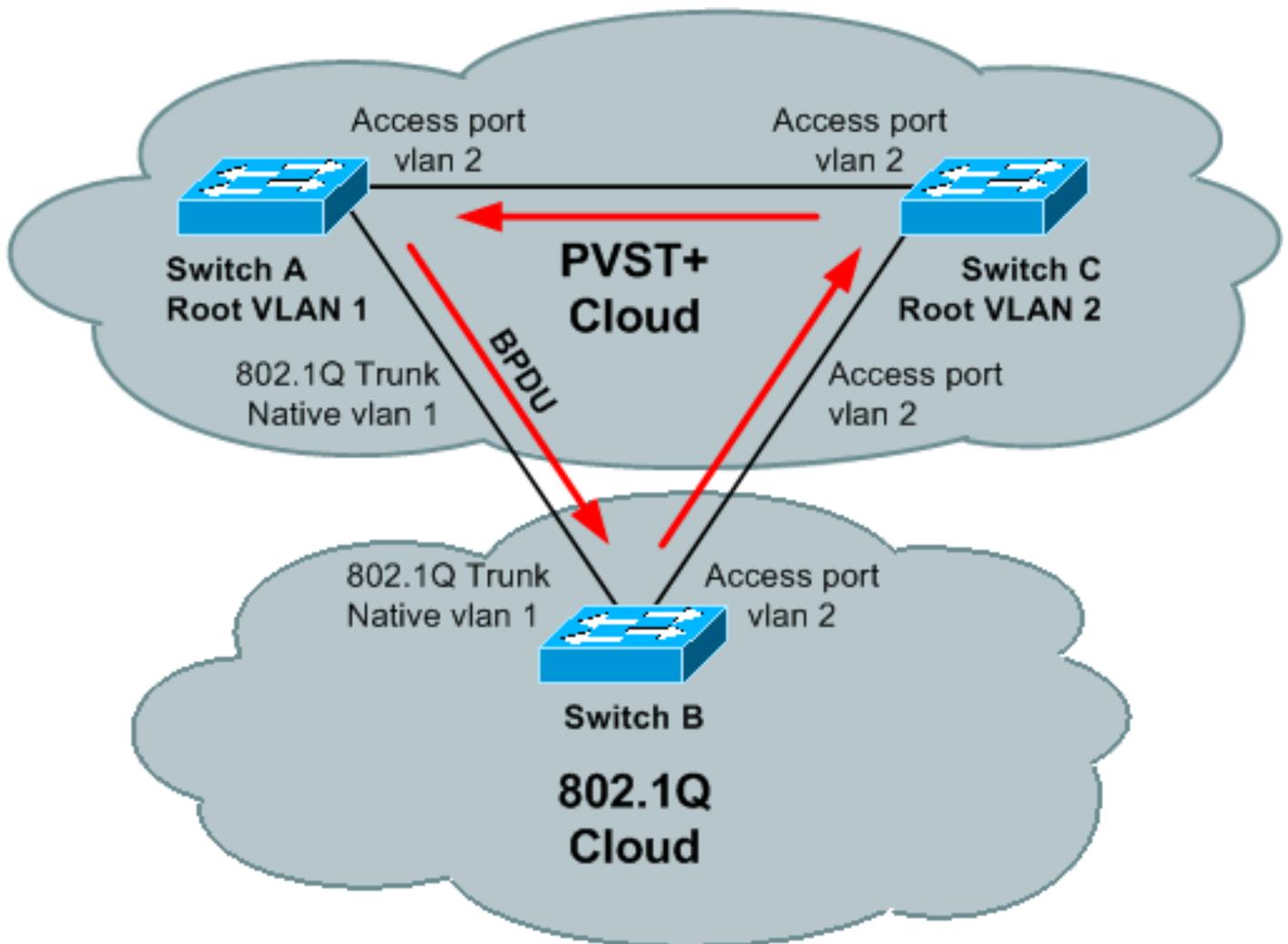
注：ネイティブVLAN STP BPDUはタグなしで送信されます。

このようにして、PVST+ の VLAN 1 STP は IEEE 802.1D または 802.1Q の STP とマージされ、一方、別の VLAN は IEEE 802.1D または 802.1Q ブリッジのクラウドを介してトンネル化されます。たとえば、IEEE 802.1D または 802.1Q のクラウドは、1 以外の PVST+ VLAN への「ワイヤ」に似ています。

STP を正常に動作させるには、PVST+ ブリッジを IEEE 802.1D または 802.1Q ブリッジに接続する際に特定のルールを守る必要があります。主なルールは、PVST+ ブリッジは、IEEE 802.1Q または 802.1D ブリッジのクラウドに接続しているすべてのブリッジ上のネイティブ VLAN と一致する IEEE 802.1Q トランクを使用して、IEEE 802.1D または 802.1Q ブリッジに接続する必要がありますというものです。

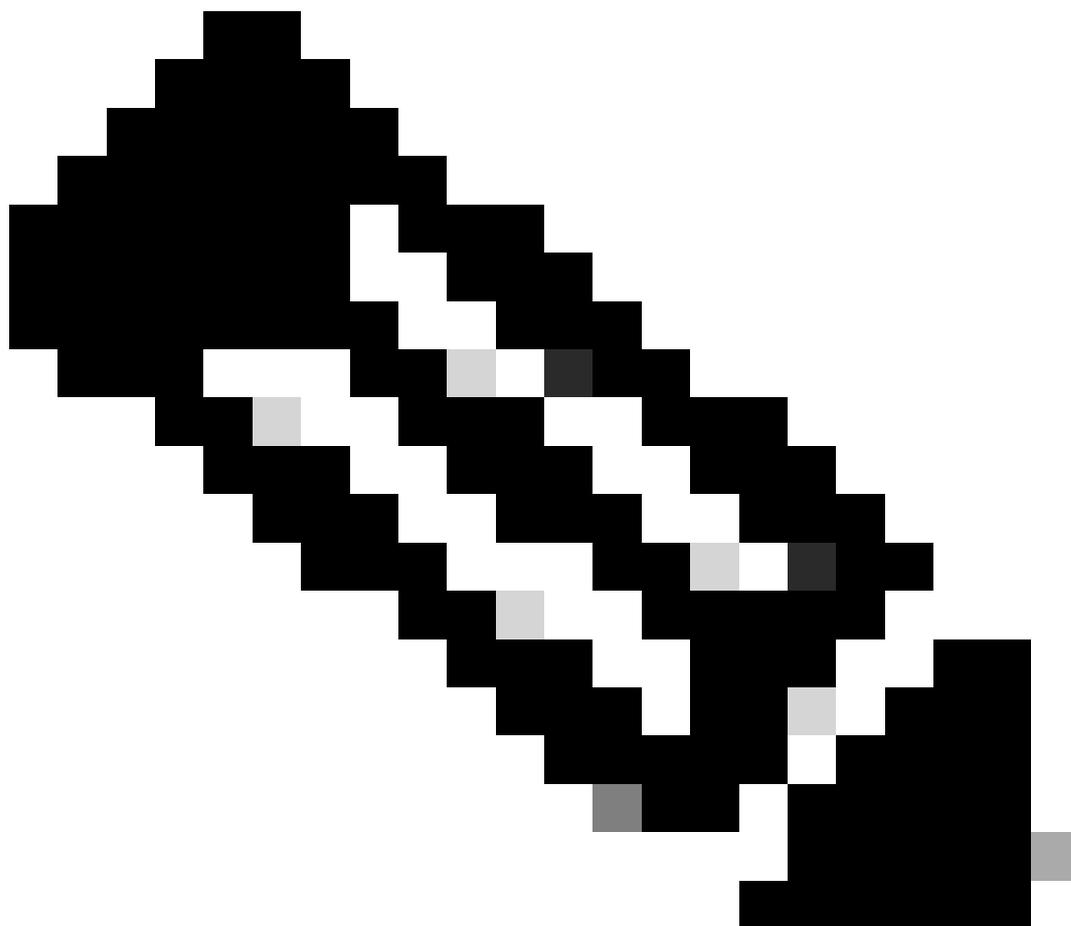
PVST+ BPDU には VLAN 番号が含まれており、PVST+ ブリッジはこの番号を使用して、以前のルールが守られているかどうかを検出します。Catalyst スイッチが設定ミスを検出した場合、対応するポートが「PVID-inconsistent」または「type-inconsistent」状態になり、対応するポート上で対応する VLAN のトラフィックがブロックされます。これらの状態は、設定ミスや配線ミスによる転送ループを防止します。

不一致の検出の必要性を説明するために、スイッチAとCではPVST+ STPを実行し、スイッチBでは802.1Q STPを実行する次のトポロジを検討します。



VLAN 1 のルートの BPDU が VLAN 2 のルートの BPDU よりも良好である場合、VLAN 2 トポロジではポートはブロックされません。VLAN 2 の BPDU がトポロジを「完全に囲む」ことはありません。B では PVST+ の VLAN 1 STP とマージされた 1 つの STP しか実行しないため、B-C リンク上では VLAN 1 BPDU に置き換えられます。このため、フォワーディング ループがあります。幸い、スイッチ A は VLAN 2 の PVST+ BPDU を (スイッチ B によってフラッディングされる SSTP アドレスに) スイッチ C に送信します。スイッチ C は、ポート C-B を type-inconsistent 状態にすること

ができ、これによりループが防止されます。



注：一部のコマンド出力では、*-inconsistent STP状態は「broken」と呼ばれます。

STP の不一致が検出されると、スイッチは次の syslog メッセージを送信します。

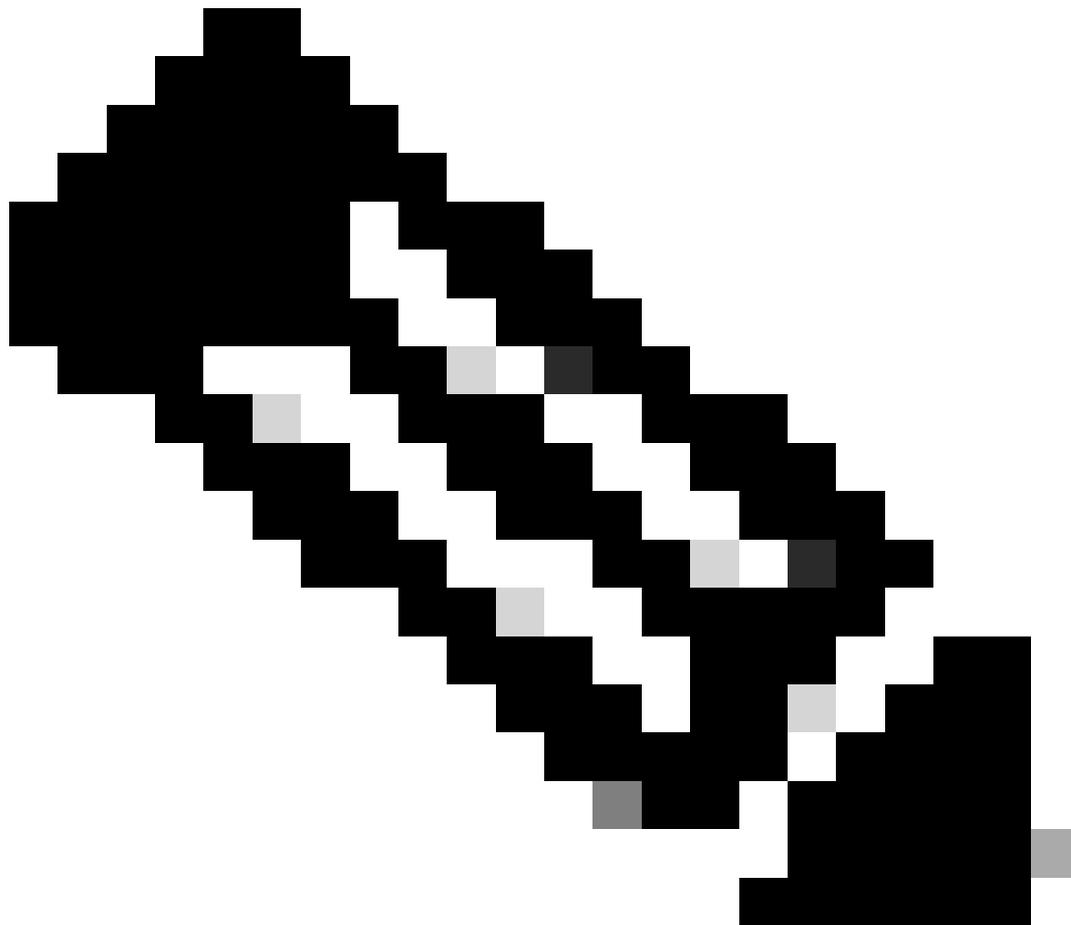
```
%SPANTREE-2-RECV_1Q_NON_TRUNK: Received IEEE 802.1Q BPDU on non trunk  
FastEthernet0/1 on vlan 1.
```

```
%SPANTREE-2-BLOCK_PORT_TYPE: Blocking FastEthernet0/1 on vlan 1.  
Inconsistent port type.
```

```
%SPANTREE-2-RX_1QPVIDERR: Rcvd 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
```

この例では、VLAN 1 が BPDU の受信側で、VLAN 10 が BPDU の発信元です。不一致が検出さ

れると、このBPDUが受信されたポートで両方のVLANがブロックされます。



注：メッセージは、使用しているCisco IOS®ソフトウェアリリースのタイプとバージョンによって異なる場合があります。

ポートが不一致のBPDUを受信しなくなった場合、*-inconsistentステートはクリアされ、STPは通常のSTP動作に基づいてポートの状態を変更します。変更を示すために syslog メッセージが送信されます。

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

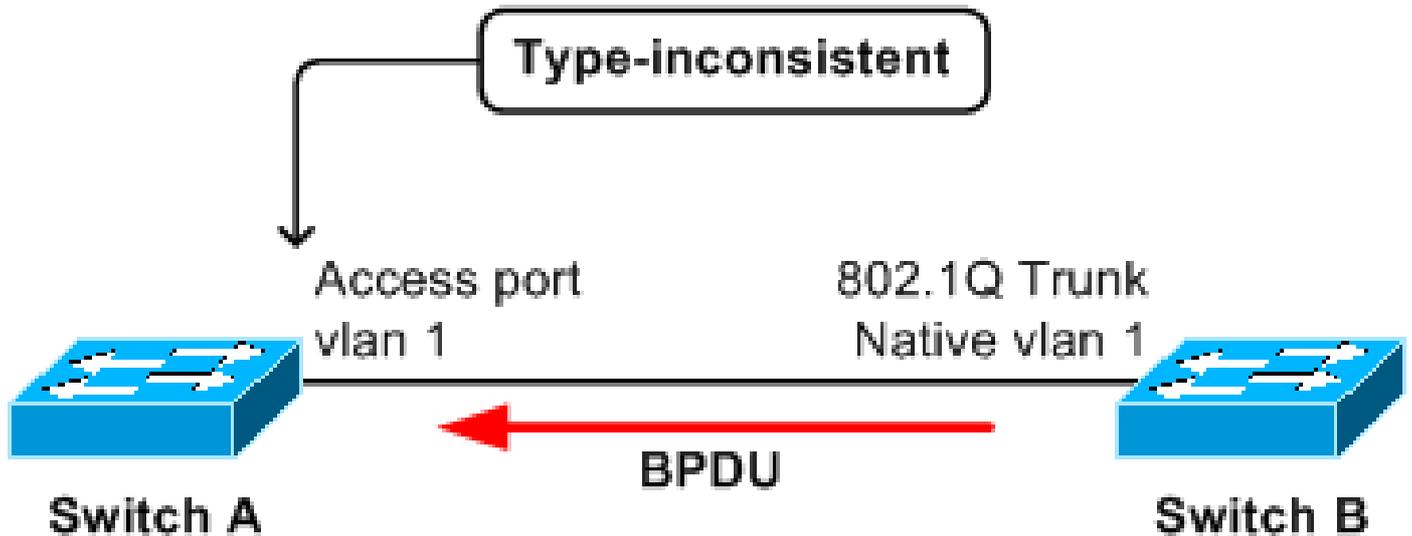
PVST+動作の詳細については、『[PVST+からrapid-PVSTへのスパンニングツリー移行の設定例](#)』を参照してください。

トラブルシューティング

不一致ポートのリストを表示するために、最新の Cisco IOS ベースの STP 実装では、show spanning-tree inconsistentports コマンドをサポートしています。

ほとんどの場合、ポート上で検出される STP の不一致の原因は明白です。

- アクセスポートが IEEE 802.1Q タグ付きの SSTP BPDU を受信する場合。

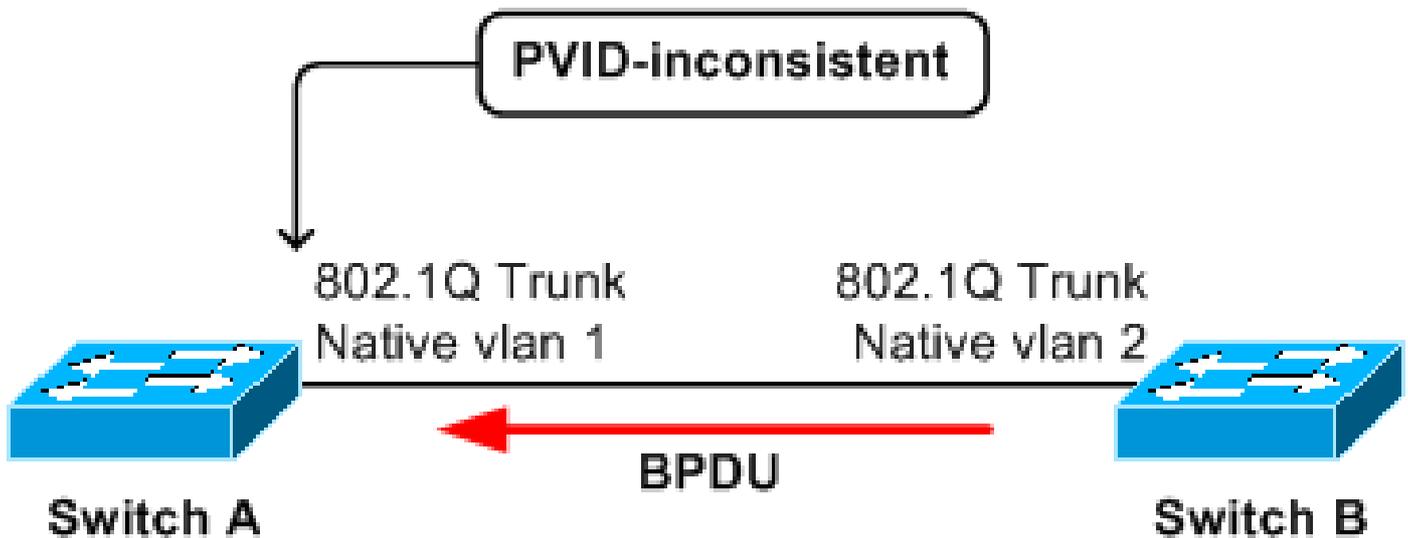


このシナリオでは、ブリッジ A 上のアクセスポートが、ブリッジ B から VLAN 1 以外の VLAN の STP からのタグ付き PVST+ BPDU を受信しています。A のポートは type-inconsistent ステートになる可能性があります。



注：スイッチを直接接続する必要はありません。スイッチが1つ以上のIEEE 802.1DまたはIEEE 802.1Qスイッチ、あるいはハブを経由して接続されている場合も、同様の結果になります。

-
- IEEE 802.1Q トランキング ポートが、BPDU の受信先の VLAN と一致しない VLAN TLV (タイプ、長さ、値) を持つ IEEE 802.1Q タグなしの SSTP BPDU を受信する場合。



このシナリオでは、A上のトランクポートは、VLAN 2のSTPからVLAN 2のタグの付いたPVST+ BPDUを受信しています。これにより、A上のポートがVLAN 1とVLAN 2の両方でブロックされます。

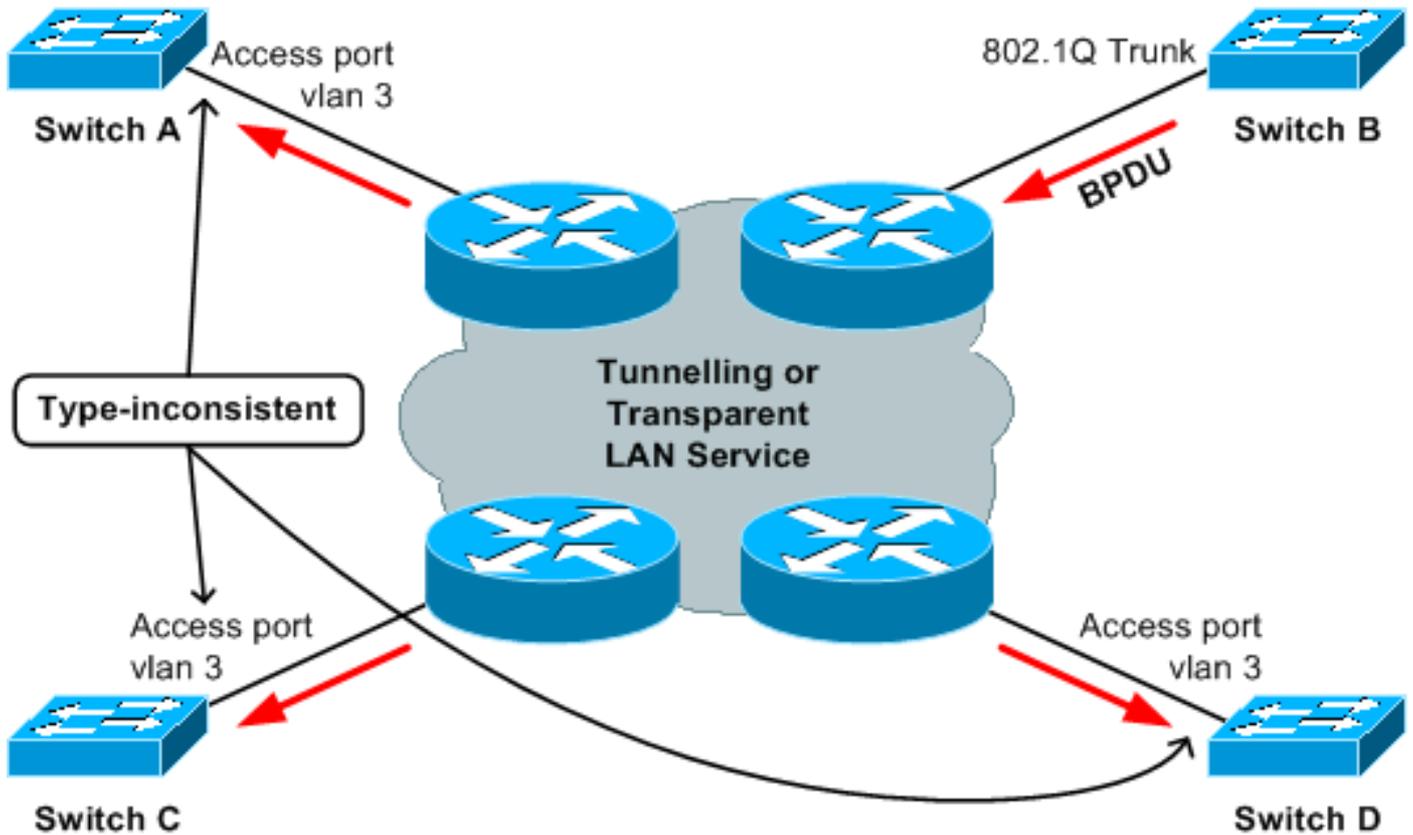
ポイントツーポイントリンクの両端のデバイスがCisco Catalystスイッチである場合、通常は、ローカルとリモートの両方のポートの設定を調べることで設定の不一致が明らかになります。

- ポートの一方の側がIEEE 802.1Q トランキング用に設定され、もう一方の側がアクセスポートである場合。
- 両方の側でIEEE 802.1Q トランクが設定されているが、ネイティブ VLAN が異なる場合。

これらの場合は、設定の不一致を修正して、STPの不一致を解決します。

場合によっては、原因の特定がより困難になります。

- BPDUが、複数のデバイスで共有されるメディアから受信される場合。
- BPDUが、クラウドに接続されたPVST+スイッチを伴うIEEE 802.1Dまたは802.1Q STPモデルを実装するスイッチクラウドから受信される場合。
- BPDUが、いくつかのトンネル（Data Link Switch Plus (DLSw+)クラウド、L2プロトコルトンネリング、EoMPLS、Virtual Path Links (VPL)、LAN Emulation (LANE) など）を経て受信される場合。



この例では、スイッチ B の設定が誤っており、SSTP BPDU をクラウドに送信しているため、スイッチ A、C、および D 上のポートが type-inconsistent 状態になります。ここでの問題は、「問題の」BPDU の発信元であるデバイスが、影響を受けているスイッチに直接接続されていないことであり、そのため、トランク上のデバイスが多い場合、すべてのデバイスのトラブルシューティングに時間がかかることがあります。

幸い、この問題には体系的なトラブルシューティング方法があります。

1. 送信元MACアドレスとBPDUの送信ブリッジIDを確立します。これは、問題が発生している間に行う必要があります
2. 「問題の」BPDU の発信元のブリッジを見つけます。これは後で行うことができ、必ずしも問題が発生したときでなくても構いません。

ステップ1では、通常、パケットアナライザを使用する方法と、受信したBPDUのダンプを表示するデバッグを有効にする方法の2つの方法があります。

デバッグを使用したSTP BPDUのダンプの詳細については、『[CatalystスイッチでのSTPに関する問題のトラブルシューティング](#)』の「[STPデバッグコマンドの使用](#)」の項を参照してください。

次に、受信された BPDU を示すデバッグ出力の例を示します。

```
*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

ソース MAC アドレスと送信元ブリッジ ID が分かったら、この MAC アドレスが属しているデバイスを検出する必要があります。スイッチは、通常、ソースの MAC アドレスを BPDU フレームから学習するわけではないため、これは複雑になる可能性があります。show mac-address-table addressBPDU_mac_address コマンド (Cisco IOS ベースのスイッチ用) を発行しても、通常はエントリが見つかりません。

「問題の」MAC アドレスを見つける1つの方法は、クラウドに接続されているすべてのスイッチから show spanning-tree コマンドの出力を収集することです。これらのコマンド出力には、各ブリッジのブリッジ ID に関する情報が含まれています。

<#root>

Boris#

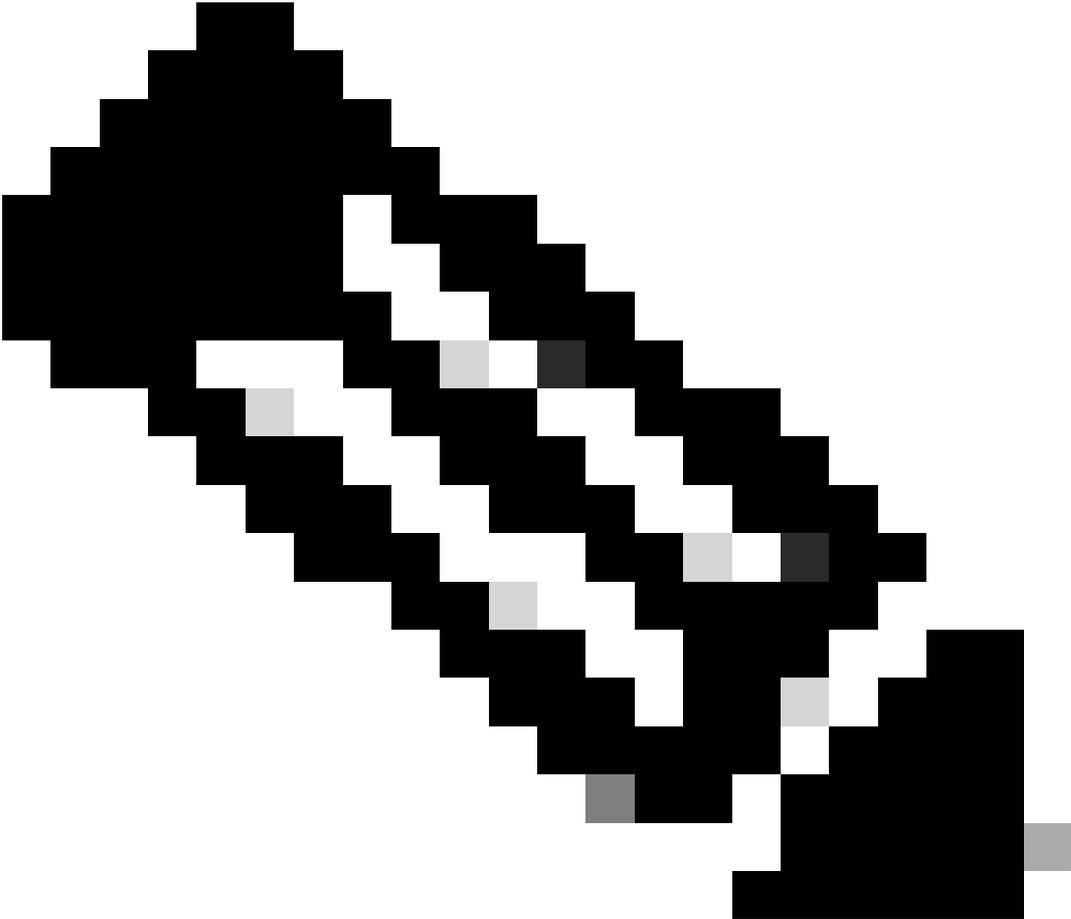
show spanning-tree

!--- 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.



注：モデル、ソフトウェアバージョン、および設定に基づいて、スイッチは複数のブリッジID MACアドレスを持つことができます。幸い、すべてのアドレスは通常、特定の範囲（たとえば、0001.1234.5600 ~ 0001.1234.5640）に含まれます。1つのブリッジID MACアドレスがわかっている場合は、送信したブリッジID MACアドレス（ステップ1で確認）が特定のブリッジID MACアドレスの範囲内にあるかどうかを確認できます。ネットワーク管理ツールを使用して、すべてのブリッジのブリッジIDを収集することもできます。

問題のBPDUを送信しているブリッジが見つかったら、クラウドに接続されているポートの設定を確認する必要があります。同じクラウドに接続されている他のスイッチとの整合性が（非トランキングおよびネイティブVLANではなく）保たれていることを確認します。

ブリッジが適切なBPDUを送信していても、トンネリングクラウド内で不適切に変更されている可能性があります。この場合、問題のBPDUがクラウドに着信し、他のブリッジの設定と一致していながら、同じBPDUがクラウドから発信される際に矛盾している（たとえば、BPDUが別のVLANのクラウドから発信される、タグ付きまたはタグなしの）ことを確認できます。このような場合、問題のBPDUの発信元MACアドレスが送信元ブリッジIDと同じブリッジに属しているか

どうかを確認すると役立ちます。同じブリッジに属していない場合は、そのBPDUの送信元MACアドレスを所有しているブリッジを検索して、その設定を確認できます。

BPDUの送信元MACアドレスを所有するスイッチを見つけるには、show moduleコマンド出力を（Catalyst 4000および6000に対して）検査する以外は、同じ方法を使用できます（ブリッジIDを見つける）。他のCatalystスイッチの場合は、show interfaceコマンドの出力を調べて、ポートに属しているMACアドレスを確認できます。

```
<#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

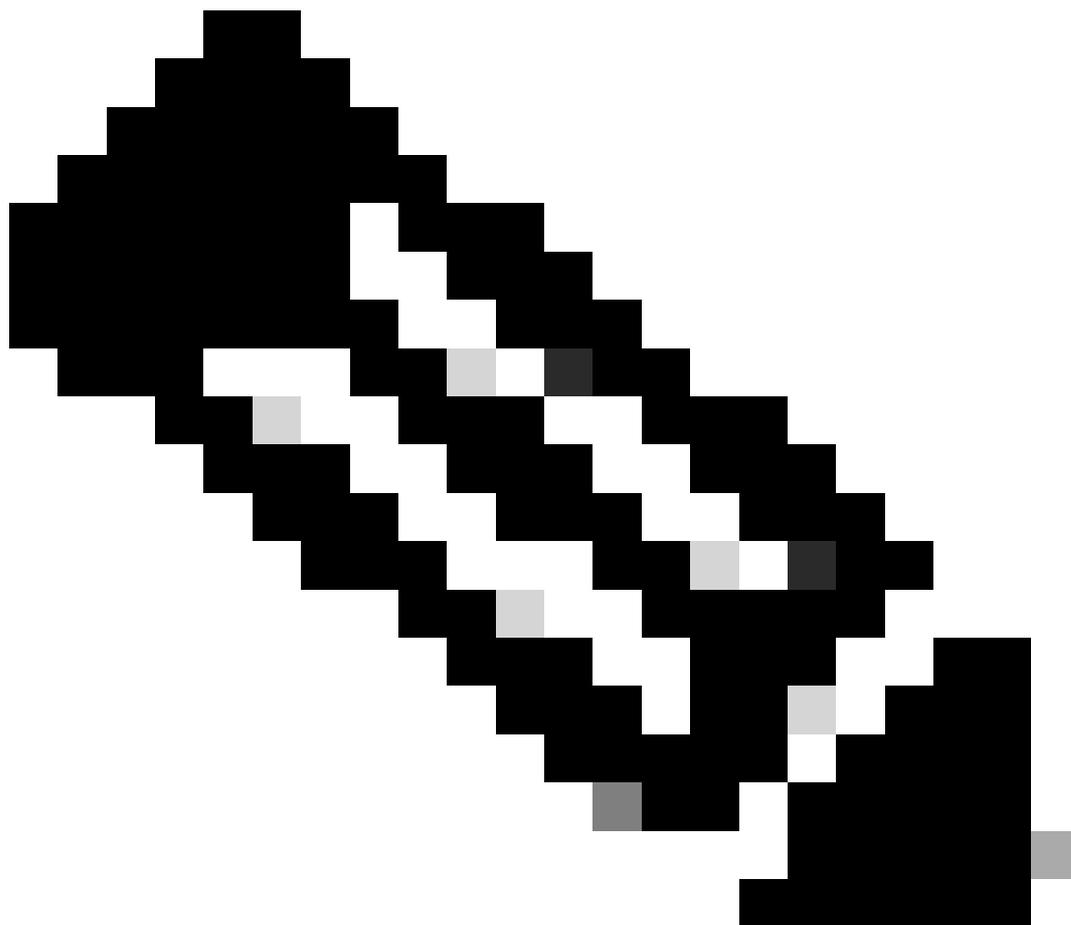
```
!--- Output suppressed.
```

```
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.
```



注：クラウドがDLSw+の場合は、『[DLSwと802.1Qの説明と設定](#)』を参照してください。

関連情報

- [LAN/スパニングツリープロトコル製品のサポート](#)
- [技術サポート](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。