

スパニングツリーの PVID とタイプの不一致のトラブルシューティング

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[PVID の不一致とタイプの不一致の背景理論](#)

[トラブルシューティング](#)

[関連情報](#)

概要

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。ダウンタイムを避けるために、いくつかの拡張が実装された結果、STP は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」状態に置かれるようになりました。

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 スキュー検出機能によるスパニングツリー プロトコルの拡張機能](#)」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、「[スパニングツリー プロトコル ルート ガード機能拡張](#)」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。(VLAN ID が *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。

このドキュメントでは、最後の 2 つの不一致 (PVID とタイプ) の原因のトラブルシューティング方法について説明します。その他の不一致のトラブルシューティング方法については、前述のドキュメントを参照してください。

前提条件

要件

このドキュメントの読者は、STP の概念について理解している必要があります。

使用するコンポーネント

このドキュメントは、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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[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。

PVID の不一致とタイプの不一致の背景理論

Cisco Catalyst スイッチは、Inter-Switch Link (ISL) トランクを使用して PVST を実装しています。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ン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 の観点では、IEEE 802.1D は VLAN 対応でなく、IEEE 802.1Q は VLAN 対応ですが、IEEE 802.1Q はすべての 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)
- VLAN 1 以外の STP BPDU が PVST+ MAC アドレス (別名 Shared Spanning Tree Protocol (SSTP) MAC アドレス。0100.0ccc.cccd) に送信される (対応する IEEE 802.1Q VLAN のタグ付き)

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

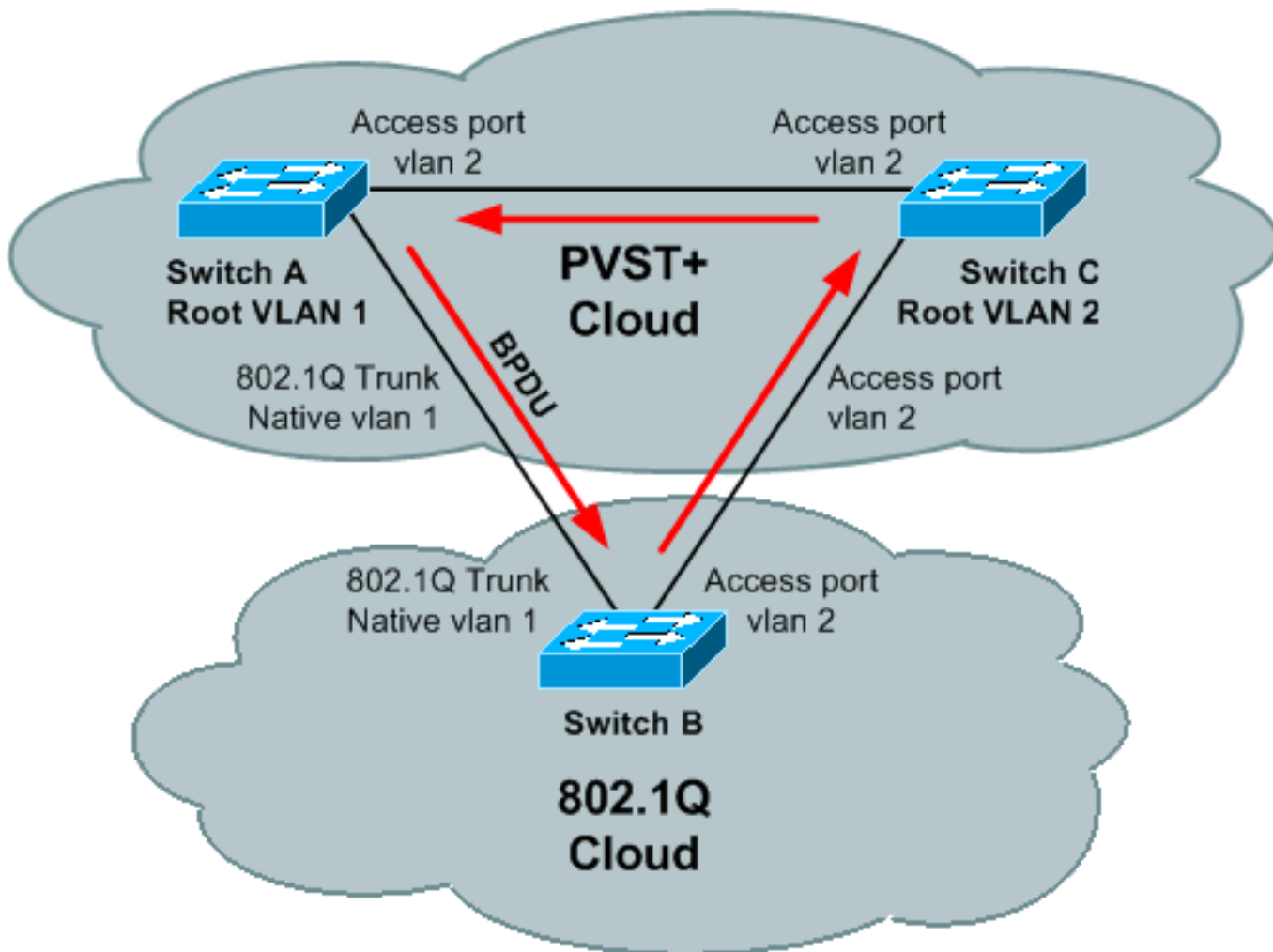
- VLAN 1 の STP BPDU が PVST+ MAC アドレスに送信される (対応する IEEE 802.1Q VLAN のタグ付き)
- VLAN 1 の STP BPDU は IEEE 802.1Q トランクのネイティブ VLAN 上の IEEE STP MAC アドレスにも送信される (タグなし)
- VLAN 1 以外の STP BPDU が PVST+ MAC アドレスに送信される (対応する IEEE 802.1Q VLAN のタグ付き) 注: ネイティブ VLAN の STP BPDU はタグなしで送信されます。

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。これにより、設定ミスや誤った配線が原因でフォワーディング ループが発生するのを防ぎます。

不一致の検出が必要であることを示すために、次のトポロジについて考えてみます。ここでは、スイッチ A と C は PVST+ STP を実行し、スイッチ B は 802.1Q STP を実行しています。



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 がトポロジ周囲を「完全に囲む」ことはありません。B は PVST+ の VLAN 1 STP とマージされる 1 つの STP しか実行しないため、B-C リンク上では VLAN 1 の BPDU と置き換えられます。このため、フォワーディング ループがあります。幸いにも、スイッチ A はスイッチ C (Switch C の方のスイッチ B) によってあふれる VLAN 2 の PVST+ BPDU を送信します (SSTP アドレスにループを防ぐ型矛盾した状態にポート CB を入れます)。

注: コマンドの出力によっては、*-inconsistent STP 状態は「broken」とも呼ばれます。”

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。不一致が検出された場合、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 リリースまたは Catalyst OS (CatOS) オペレーティング システムの種類とバージョンにより異なります。

注: 一致しない BPDU の受信をポートが停止すると、*-inconsistent 状態はクリアされ、STP は通常の STP 動作に従っ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.
```

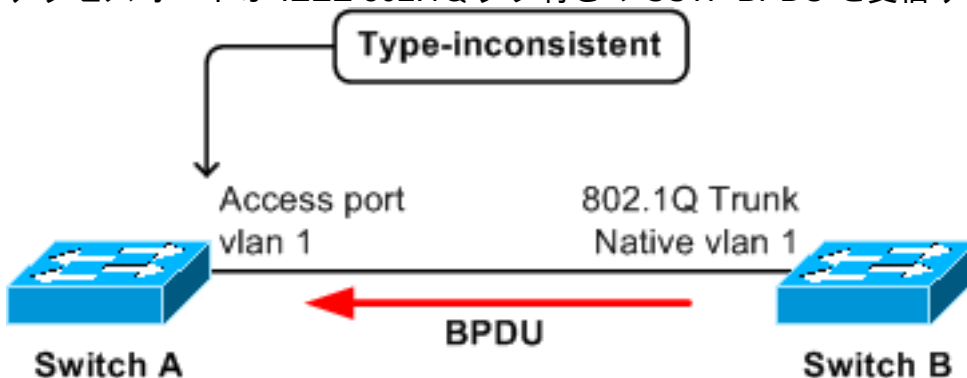
PVST+ 動作の詳細については、「[IEEE 802.1Q VLAN 間のブリッジ](#)」を参照してください。

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。

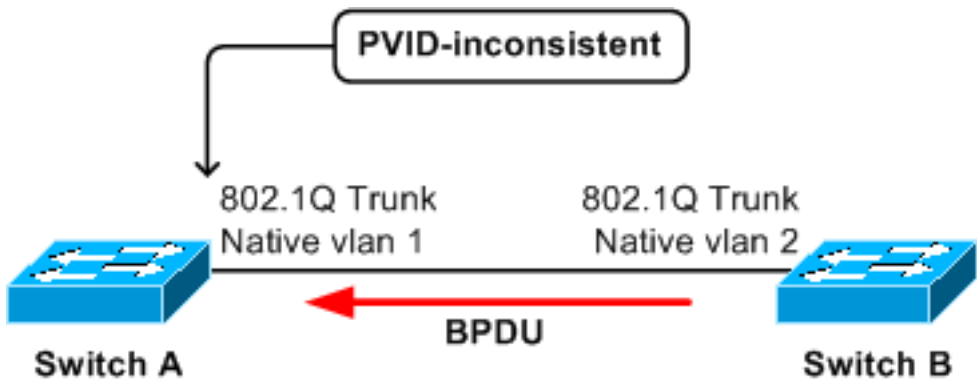
ほとんどの場合、ポート上で検出される STP の不一致の原因は明白です。

- 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 上のポートは、type-inconsistent 状態に置かれます。注: スイッチは直接接続されている必要はありません。1 台以上の IEEE 802.1D または IEEE 802.1Q スイッチ—またはハブ—を介して接続されている場合、効果は同じです。

- 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。

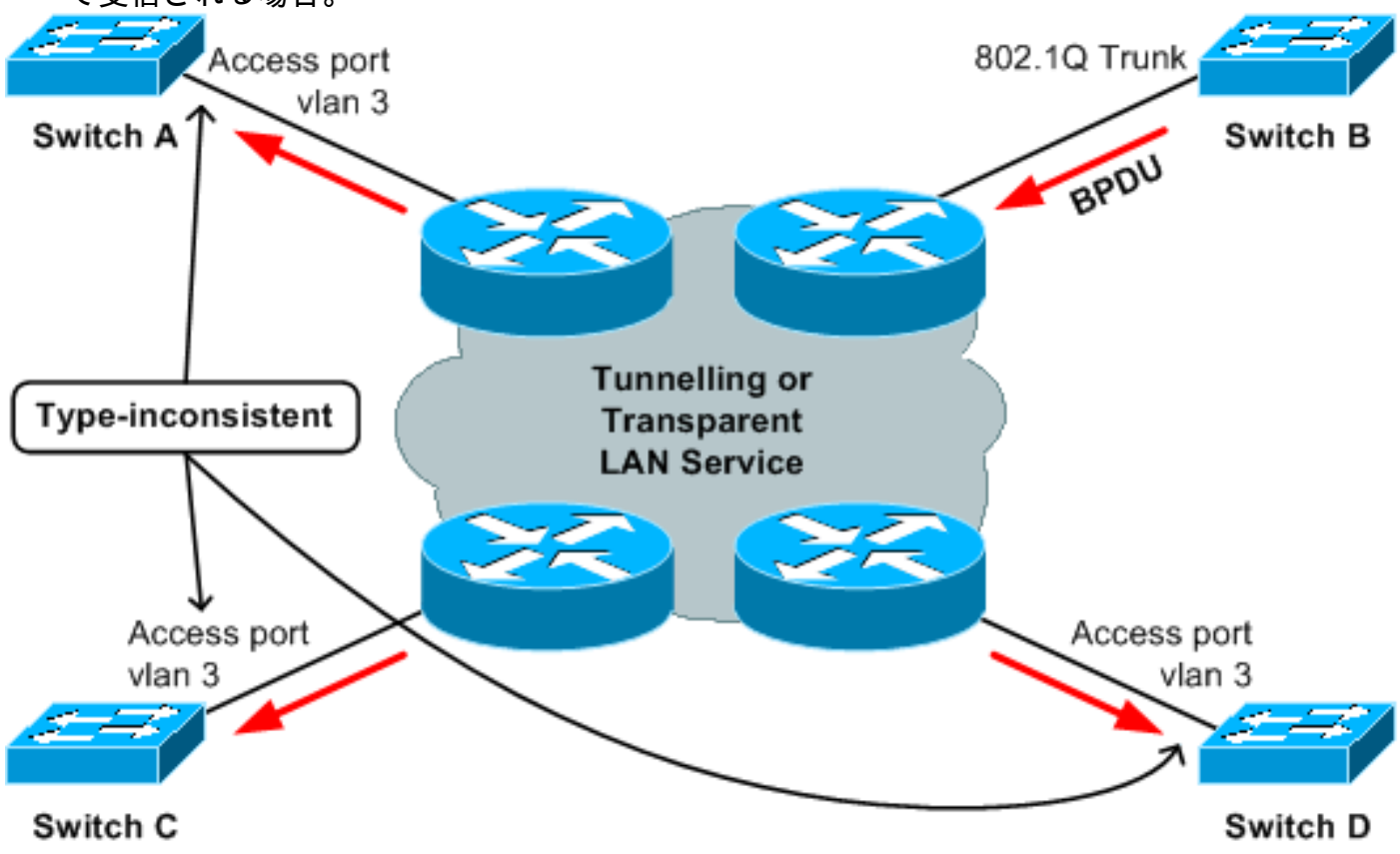


このシナリオでは、A上のトランクポートは、VLAN 2のSTPからVLAN 2のタグの付いたPVST+ BPDUを受信しています。これにより、A上のポートがVLAN 1とVLAN 2の両方でブロックされます。ポイントツーポイントリンクの両端のデバイスがCisco Catalystスイッチである場合、通常は、ローカルとリモートの両方のポートの設定を調べることで設定の不一致が明らかになります。

- 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。

原因の特定がそれほど簡単でない場合もあります。

- 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

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、トランク上にデバイスが多いと、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. ソース Mac アドレスとBPDU の送信元ブリッジ ID を確立します。これは、問題が発生している間に行われている必要があります。
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 には、通常は、パケット アナライザを使用するか、デバッグを有効にして受信された BPDU のダンプを表示するという 2 つの選択肢があります。

デバッグを使用した STP BPDU のダンプの詳細については、「[Cisco IOS システム ソフトウェアが稼働する Catalyst スイッチでの STP に関するトラブルシューティング](#)」の「[STP デバッグ コマンド](#)」セクション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 が分かると、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 address BPDU_mac_address コマンド (Cisco IOS ベースのスイッチの場合) または show cam mac_address コマンド (CatOS ベースのスイッチの場合) を発行しても、通常、エントリは見つかりません。

「問題の」MAC アドレスを検索する 1 つの方法として、クラウドに接続されているすべてのスイッチからの show spanning-tree コマンド (Cisco IOS の場合) または show spantree (CatOS の場合) コマンドの出力を収集します。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。

```
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. Doris (enable) show spantree !--- Use with CatOS.
VLAN 1 Spanning tree mode RAPID-PVST+ Spanning tree type ieee Spanning tree enabled Designated
Root 00-07-4f-1c-e8-47 Designated Root Priority 0 Designated Root Cost 123 Designated Root Port
9/7 Root Max Age 20 sec Hello Time 2 sec Forward Delay 15 sec Bridge ID MAC ADDR 00-d0-03-ef-4c-
00 !--- Output suppressed.
```

注: モデル、ソフトウェア バージョン、および設定に応じて、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、特定の範囲に属します (0001.1234.5600 ~ 0001.1234.5640 など)。1 つのブリッジ ID MAC アドレスが分かっている場合、ステップ 1 で確認した送信元ブリッジ ID MAC アドレスが、特定のブリッジ ID MAC アドレスの範囲内にあるかどうか確認ができます。

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、クラウドに接続しているポートの設定を確認して、同じクラウドに接続している他のスイッチと一致している（非ランキングやネイティブ VLANではなくランキング）ことを確認します。

ブリッジは正しいBPDUを送信しているけれど、トンネリングクラウド内部で不適切に変更されている場合があります。この場合、「問題の」BPDUがクラウドに入るときは他のブリッジの設定と一致しているけれど、同じBPDUがクラウドを出るときは一致していない（たとえば、BPDUが異なるVLANでクラウドを出たり、タグ付きまたはタグなしになっている）ことを確認できません。このような場合は、「問題の」BPDUの送信元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ことが役立ちます。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検索するには、ブリッジIDを検索するのと同じ手順を実行します。ただし、ここでは、(Catalyst 4000、5000、6000に対して) **show module** コマンドの出力が検査されている点が異なります。Catalyst 2900 XL、3500 XL、2950、および3550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アドレスを確認する必要があります。

```
Cat4000-IOS# 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+ である場合は、「[DLSw と 802.1q の説明と設定](#)」を参照してください。

[関連情報](#)

- [LAN 製品に関するサポート ページ](#)
- [LAN スイッチングに関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)