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

目次

概要

このドキュメントでは、Cisco IOS® ソフトウェアを使用してスパニングツリー プロトコル（STP）の問題をトラブルシューティングする際の注意事項について説明します。 Catalyst 6500/6000 にのみ適用される特定のコマンドがあります。 ただし、Cisco IOS ソフトウェアが稼働する Cisco Catalyst スイッチに、原則のほとんどを適用できます。

での問題に対してトラブル シューティングを行う場合、その問題は概ね次の 3 つに集約されます。

- フォワーディング ループ
- 頻繁な STP Topology Change（TC; トポロジ変更）による過度のフラッディング
- コンバージェンス時間に関する問題

ある特定のパケットが複数回転送されているかどうかをトラッキングする（たとえば、IP Time to Live（TTL; 存続可能時間）を使用してネットワーク内を長時間循環しているトラフィックを廃棄する）メカニズムがブリッジングにはないので、同一レイヤ 2（L2）ドメイン内にある 2 つのデバイス間には、1 つのパスしか存在できません。

STP の目的は、STP アルゴリズムに基づいて冗長ポートをブロックして、冗長な物理トポロジをツリー型のトポロジに変えることです。 フォワーディング ループ（STP ループなど）は、冗長トポロジ内にブロックされるポートがない場合に発生します。フォワーディング ループが発生すると、トラフィックは際限なくネットワーク内を循環します。

いったん、フォワーディング ループが発生すると、そのフォワーディング ループのパスに沿って、最も低い帯域幅のリンクで輻輳が起こりやすくなります（リンクがすべて同じ帯域幅である場合、そのすべてのリンクで輻輳が起こります）。 この輻輳によりパケットの損失が発生し、さらに、影響を受ける L2 ドメイン内でのネットワークのダウンという状況につながります。

過度のフラッディングがある場合、それほどはっきりと症状として現れないかもしれません。 しかし、いつくかの低速リンクは、フラッディング トラフィックによって輻輳し、これらのリンクの背後のデバイスやユーザには、通信速度低下などの影響が現れたり、接続性が完全に失われたりすることもあります。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 各種スパニングツリーのタイプとその設定方法。 詳細は、「STP と IEEE 802.1s MST の設定」を参照してください。
- 各種スパニングツリーの機能とその設定方法。 詳細は、「STP 機能の設定」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- スーパーバイザ 2 エンジン搭載の Catalyst 6500
- Cisco IOS ソフトウェア リリース 12.1(13)E

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。

STP が正常に機能しない原因

STP には、動作環境に関して特定の前提条件があります。 このドキュメントに関連する前提条件は、次のとおりです。

- 2 つのブリッジ間の各リンクは双方向である。 つまり、A と B の間のリンクがアップ状態である限り、A が B に直接接続されている場合であれば、A は B の送ったデータを受信し、B は A の送ったデータを受信します。
- STP を実行している各ブリッジは、STP パケットとも呼ばれる STP Bridge Protocol Data Units（BPDU; ブリッジ プロトコル データ ユニット）の受信、処理および送信を恒常的に行うことができる。

上記の前提条件は、一見論理的で当たり前のように思われますが、この前提条件が満たされない

ような状況があります。 これらの状況のほとんどは種類のハードウェア上の問題を含みます; ただし、ソフトの欠陥はまた STP 失敗の原因となるかもしれません。 STP 障害の大多数は、各種ハードウェアの障害、誤設定、または不適切なケーブル接続によるものですが、件数は少ないながらも、ソフトウェアの障害によるものもあります。 また、スイッチの間に不必要な接続が追加された場合にも STP の障害が発生する場合があります。 それらの追加接続によって、VLAN がダウン状態になります。 この問題を解決するには、スイッチ間の不必要な接続をすべて削除します。

前述の前提条件のうち、1 つでも満たされていないと、1 台あるいは複数のブリッジで BPDU の受信や処理がされなくなる場合があります。 このことは、そのブリッジがネットワーク トポロジを検出できなくなることを意味します。 正しいネットワーク トポロジを検出できないと、スイッチはループをブロックできません。 したがって、フラッディング トラフィックがそのループが発生しているトポロジを循環し、すべての帯域幅を消費します。その結果、ネットワークがダウンします。

スイッチが BPDU を受信できなくなる原因の例としては、トランシーバまたは Gigabit Interface Converters (GBIC; ギガビット インターフェイス コンバータ) の故障、配線の問題、あるいはポート、ラインカードまたはスーパーバイザ エンジンでのハードウェア障害があります。 多くの STP 障害の原因になっています。 このような条件では、1 台のブリッジが BPDU を送信しても、下流側のブリッジではこれが受信されません。 また STP 処理も、スイッチが受信した BPDU を処理できないために CPU に負荷がかかり過ぎて (使用率が 99 % 以上になって) 中断することもあります。 BPDU も一方のブリッジから他方のブリッジへのパスを通る間に破損する可能性があり、これにより STP の正常な動作も妨げられます。

フォワーディング ループ以外にも、ブロックされるポートがないときに、ある特定のパケットだけが間違ってブロッキング ポートを経由して転送される場合があります。 このようなケースは、ソフトウェアの問題によるものがほとんどです。 このような動作により、「スロー ループ」が発生することがあります。 スロー ループとは、いくつかのパケットがループしているが、リンクが輻輳していないために、大多数のトラフィックはまだネットワーク上を流れていることを意味します。

このドキュメントの後のセクションでは、STP に関連する最も一般的な問題に対するトラブル シューティングのガイドラインを説明します。

フォワーディング ループに関するトラブルシューティング

フォワーディング ループは、その発生 (原因) と影響の両方において実に多種多様です。 STP に影響を与える問題は多岐に渡るので、このドキュメントでは、フォワーディング ループに関するトラブルシューティングの一般的なガイドラインだけを説明します。

トラブルシューティングを始める前に、次の情報を入手する必要があります。

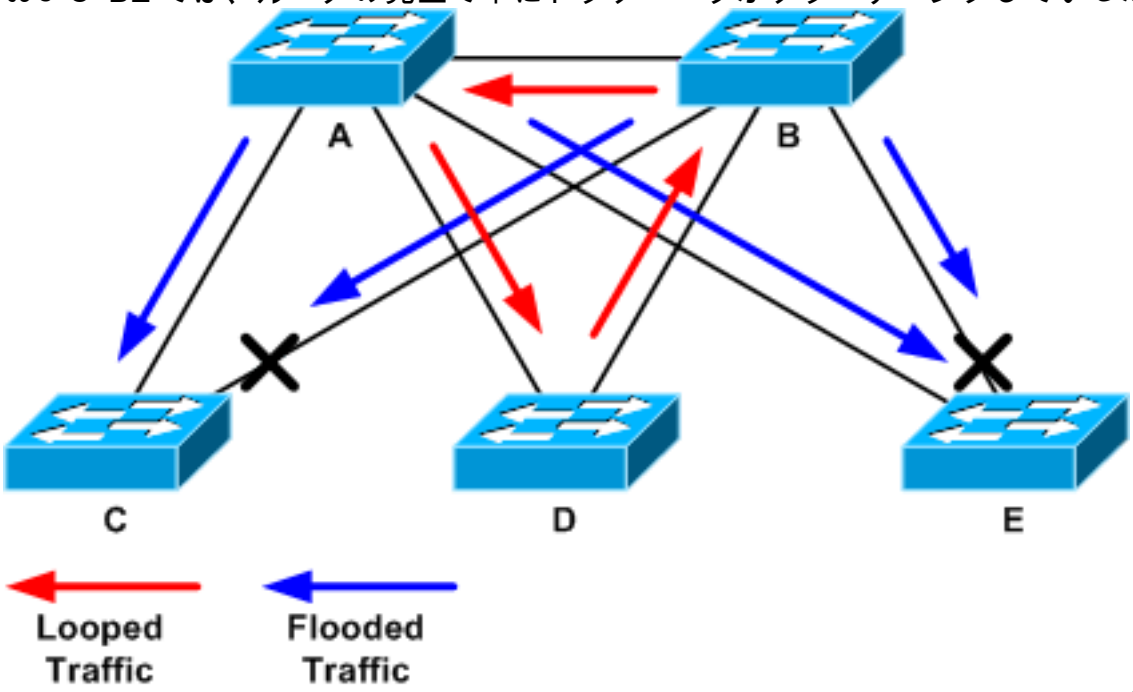
- すべてのスイッチとブリッジの詳細が示された実際のトポロジ図
- それらに対応する (相互接続されている) ポート番号
- どのスイッチがルートおよびバックアップ ルートか、デフォルト以外のコストや優先度がどのリンクに設定されているか、ブロッキング ポートがどこにあるかなどの STP 設定の詳細

一般に、トラブルシューティングには次のステップが必要です (状況によっては、いくつかの手順は行う必要がない場合があります)。

1. ループを識別します。ネットワーク内でフォワーディング ループが発生した場合、通常は次のような症状が見られます。ループの影響を受けるネットワーク領域との両方向の接続、

およびそのネットワーク領域を介した接続が失われる。ループの影響を受けるセグメントまたは VLAN と接続されたルータの CPU 使用率が高くなり、ルーティング プロトコルの近接ルータのフラッピングや Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）のアクティブ ルータのフラッピングなど、さまざまな症状が現れる。リンク使用率が高くなる（多くの場合 100 %）。スイッチ バックプレーンの使用率が高くなる（ベースライン使用率と比較して）。ネットワーク内でパケットがループしていることを示す Syslog メッセージが表示される（HSRP 重複 IP アドレスを示すメッセージなど）。アドレスの再学習が常に行われていることを示す Syslog メッセージや、MAC アドレスのフラッピング メッセージが表示される。多くのインターフェイス上で廃棄される出力数が増加する。**注:** 上記の症状のうち、いずれか 1 つだけが該当する場合は、別の問題を示している可能性があります（またはまったく問題にならないこともあります）。 しかし、上記のうち、多くの症状が同時に見られる場合は、そのネットワーク内でフォワーディング ループが発生している可能性が十分考えられます。**注:** フォワーディング ループが発生しているかどうかを確認する最も速い方法は、スイッチのバックプレーン トラフィックの使用率を確認することです。`cat# **show catalyst6000 traffic-meter traffic meter = 13%** Never cleared **peak = 14%** reached at 12:08:57 CET Fri Oct 4 2002` **注:** Cisco IOS ソフトウェアが稼働する Catalyst 4000 では、現在このコマンドはサポートされていません。現在のトラフィック レベルが通常のレベルを大幅に上回っている、またはベースラインが確認できない場合は、最近ピーク レベルに達していないか、およびピーク レベルが現在のトラフィック レベルに近いかどうかを確認してください。 たとえば、ピークのトラフィック レベルが 15 % で、そのレベルに達したのがわずか 2 分前であり、現在のトラフィック レベルが 14 % であったとすると、このような状況は、スイッチに異常に高い負荷がかかっていることを意味します。トラフィックが通常のレベルである場合は、ループが発生していないか、このデバイスがループとは関係がないことのいずれかを意味します。 ただし、スロー ループに関係している可能性は残ります。
2. ループが発生しているトポロジ（範囲）を検出します。ネットワークの停止原因がフォワーディング ループであることが特定されたら、そのループを停止させネットワーク機能を回復させることが、最優先の処理です。 ループを停止させるには、ループに関係するポートを特定する必要があります。 特定するには、リンク使用率（1 秒あたりのパケット数）が最も高いポートを調べます。 Cisco IOS ソフトウェアの show interface コマンドを実行すると、各インターフェイスの使用率が表示されます。分析を迅速に行うために、リンク使用率の情報とインターフェイス名だけを表示させるには、Cisco IOS ソフトウェアの正規表現を使用して出力フィルタリングを行います。 **show interface を**発行して下さい **| include line|\ /sec** パケット/秒統計情報およびインターフェイス名だけ表示する コマンド:`cat# **show interface | include line|\/sec** GigabitEthernet2/1 is up, line protocol is down 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec GigabitEthernet2/2 is up, line protocol is down 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec **GigabitEthernet2/3 is up, line protocol is up 5 minute input rate 99765230 bits/sec, 24912 packets/sec** 5 minute output rate 0 bits/sec, 0 packets/sec **GigabitEthernet2/4 is up, line protocol is up** 5 minute input rate 1000 bits/sec, 27 packets/sec **5 minute output rate 101002134 bits/sec, 25043 packets/sec** GigabitEthernet2/5 is administratively down, line protocol is down 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec GigabitEthernet2/6 is administratively down, line protocol is down 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec GigabitEthernet2/7 is up, line protocol is down 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec **GigabitEthernet2/8 is up, line protocol is up** 5 minute input rate 2000 bits/sec, 41 packets/sec **5 minute output rate 99552940 bits/sec, 24892 packets/sec** リンク使用率が最も高いインターフェイスに特に注意してください。 この例では、これらはインターフェイス g2/3、g2/4 および g2/8 です; それらはおそらくループに関連するポートです。

3. ループを遮断します。ループを遮断するには、関係するポートをシャットダウンするか接続解除します。 ループを停止させるだけでなく、そのループの根本的な原因も発見して、その原因を修正することが非常に重要です。 ループを遮断する作業は、比較的簡単です。**注**: それに続く原因 分析を助けるために、シャットダウンされて必要としませんし、すべてのポートをすぐに切りません; その代り、それらを一つずつ停止して下さい。 ポートのシャットダウンは、一般的に、ディストリビュータまたはコア スイッチなどのループの影響を受けている集約ポイントで行うのがよいとされています。 ポートすべてをすぐにシャットダウンし、順次に有効に するか、または再接続すれば、それははたらかないかもしれません; ループはおこるポートが再接続する直後に停止し、開始しないかもしれません。 そのため、障害を特定のポートに関連付けることが難しくなります。**注:** ループを遮断するためにスイッチをリブートする前に情報を収集しておくことをお勧めします。 そうしなければ、その後の原因究明のための分析が非常に難しくなります。各ポートをディセーブルにしたり、接続解除した後は、スイッチのバックプレーンの使用率が通常のレベルに戻っているかどうかを確認してください。**注:** 自分にループが発生していなくても、ループが原因で到着するトラフィックによるフラッディングが発生しているポートがあることを念頭においてください。 そのようなフラッディング ポートをシャットダウンすると、バックプレーン使用率は若干低下しますが、ループは停止しません。次 の 例 トポロジーでは、ループはスイッチA の間に、B および D あります。 従って、リンク AB、AD および BD は支えています。 これらのリンクのどれかをシャットダウンすれば、ループは停止します。 リンク AC、AE、BC および BE では、ループの発生で単にトラフィックがフラッディングしているだけです。



ループの影響を受けているポートをシャットダウンすると、バックプレーン使用率は正常値まで低下します。 どのポートをシャットダウンしたときに、バックプレーン使用率 (および他のポートの使用率) が正常のレベルに戻ったかに注意することが非常に重要です。この時点で、ループは停止し、ネットワークオペレーションは改良する必要があります; ただしループのオリジナル原因がおそらく固定ではなかったので、まだ顕著ないくつかの問題があるかもしれません。

4. ループの原因を発見し、その原因に対する処置を行います。ループが停止したら、ループが発生した原因を特定する必要があります。 ループの発生原因は多種多様であるため、発生原因の特定は、このプロセスのなかで最も難しい作業です。 またこの作業は、どのケースにも有効な手順として、正確に定型化することが難しい作業でもあります。 ただし、次に示すような一般的なガイドラインがあります。トポロジ図を調査して、冗長パスを見つけま

す。 このトポロジ図には、前のステップで発見された、ループの影響を受けているポートが含まれており、パケットが同じスイッチに戻ってくることが示されています（ループが発生している間パケットが辿るパス）。 前のトポロジの例では、このパスは AD-DB-BA です。冗長パス上にある各スイッチに対して、次の問題を確認します。このスイッチは正しい STP ルートを認識しているか。L2 ネットワーク内にあるすべてのスイッチは、共通の STP ルートで一致している必要があります。 ブリッジが常にある特定の VLAN または STP インスタンスに対して異なる ID を表示するときは、問題の症状がはっきりと現れているときです。 show spanning-tree vlan vlan-id コマンドを実行すると、所定の VLAN に対するルートブリッジ ID が表示されます。cat# **show spanning-tree vlan 333** MST03 Spanning tree enabled protocol mstp **Root ID Priority 32771 Address 0050.14bb.6000** Cost 20000 Port 136 (GigabitEthernet3/8) Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32771 (priority 32768 sys-id-ext 3) Address 00d0.003f.8800 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Prio.Nbr Status ---------------- ---- --- --------- -------- ---------------------- Gi3/8 Root FWD 20000 128.136 P2p Po1 Desg FWD 20000 128.833 P2p この VLAN 番号は、ポートから見つけることができます。ループに関係するポートは前述のステップで判明しているからです。 問題のポートがトランクである場合、そのトランク上のすべての VLAN が関係していることが度々あります。 これが事実ループは単一 VLAN で起こったようである場合、（たとえば）でなければ **show interfaces を**発行することを試みることができます **|** Supervisor 1 が VLAN ごとのスイッチングの統計情報を提供しないので） **L2|line|broadcast** コマンドを**含んで下さい**（Catalyst 6500/6000 シリーズ スイッチのスーパバイザ 2 およびそれ以降エンジンでだけ。 VLANインターフェイスだけを検知 して下さい。 通常、交換パケットの量が最も多い VLAN でループが発生しています。cat# **show int | include L2|line|broadcast Vlan1 is up, line protocol is up L2 Switched: ucast: 653704527 pkt, 124614363025 bytes - mcast: 23036247 pkt, 1748707536 bytes Received 23201637 broadcasts, 0 runts, 0 giants, 0 throttles** Vlan10 is up, line protocol is up L2 Switched: ucast: 2510912 pkt, 137067402 bytes - mcast: 41608705 pkt, 1931758378 bytes Received 1321246 broadcasts, 0 runts, 0 giants, 0 throttles Vlan11 is up, line protocol is up L2 Switched: ucast: 73125 pkt, 2242976 bytes - mcast: 3191097 pkt, 173652249 bytes Received 1440503 broadcasts, 0 runts, 0 giants, 0 throttles Vlan100 is up, line protocol is up L2 Switched: ucast: 458110 pkt, 21858256 bytes - mcast: 64534391 pkt, 2977052824 bytes Received 1176671 broadcasts, 0 runts, 0 giants, 0 throttles Vlan101 is up, line protocol is up L2 Switched: ucast: 70649 pkt, 2124024 bytes - mcast: 2175964 pkt, 108413700 bytes Received 1104890 broadcasts, 0 runts, 0 giants, 0 throttles 上記の例では、VLAN 1 に最も多くの数のブロード キャストおよび L2 交換トラフィックがあることがわかります。ルート ポートは正しく識別されているか。ルート ポートは、ルート ブリッジへのコストが最小となるポートです（低速のポートの方がコストが高くなるため、ホップ数が少なくてもコストが大きいパスになることがあります）。所定の VLAN に対して、どのポートがルートとみなされるかを判断するには、show spanning-tree vlan vlan コマンドを発行します。cat# **show spanning-tree vlan 333** MST03 Spanning tree enabled protocol mstp Root ID Priority 32771 Address 0050.14bb.6000 Cost 20000 **Port 136 (GigabitEthernet3/8)** Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32771 (priority 32768 sys-id-ext 3) Address 00d0.003f.8800 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Prio.Nbr Status ---------------- ---- --- --------- -------- ---------------- -------- Gi3/8 Root FWD 20000 128.136 P2p Po1 Desg FWD 20000 128.833 P2pルート ポートおよびブロッキングを行うはずのポートで BPDU が定常的に受信されているか。BPDU はルート ブリッジによって hello 間隔（デフォルトでは 2 秒）ごとに送信されます。 ルート以外のブリッジは、ルートから送られる BPDU の受信、処理、修正および伝搬を行います。 show spanning-tree interface interface detail コマンドを発行すると、BPDU が受信されているかどうかを確認できます。cat# **show spanning-tree interface g3/2 detail** Port 130 (GigabitEthernet3/2) of MST00 is backup blocking Port path cost 20000, Port priority 128, Port Identifier 128.130. Designated root has priority 0, address 0007.4f1c.e847 Designated bridge has priority 32768, address 00d0.003f.8800 Designated port id is 128.129, designated path cost 2000019 Timers: message age 4, forward delay 0, hold 0 **Number of transitions to**

forwarding state: 0 Link type is point-to-point by default, Internal Loop guard is enabled by default on the port BPDU: sent 3, **received 53** cat# **show spanning-tree interface g3/2 detail** Port 130 (GigabitEthernet3/2) of MST00 is backup blocking Port path cost 20000, Port priority 128, Port Identifier 128.130. Designated root has priority 0, address 0007.4f1c.e847 Designated bridge has priority 32768, address 00d0.003f.8800 Designated port id is 128.129, designated path cost 2000019 Timers: message age 5, forward delay 0, hold 0 Number of transitions to forwarding state: 0 Link type is point-to-point by default, Internal Loop guard is enabled by default on the port BPDU: sent 3, **received 54** **注:** このコマンドの 2 回の出力の間に、1 つの BPDU が受信されています (カウンタが 53 から 54 になっています)。表示されるカウンタは、STP プロセスによって実際に維持されるカウンタです。 このことは、受信カウンタが増加した場合、BPDU が物理ポートによって受信されただけでなく、STP プロセスによっても受信されたことを意味します。received BPDU カウンタが代替ルート ポートまたはバックアップ ポートとなるはずのポート上で増加しない場合は、そのポートで何らかのマルチキャストが受信されているかどうかを確認します (BPDU はマルチキャストとして送信されます)。 次のように、show interface interface counters コマンドを発行します。cat# **show interface g3/2 counters** Port InOctets InUcastPkts **InMcastPkts** InBcastPkts Gi3/2 14873036 2 **89387** 0 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Gi3/2 114365997 83776 732086 19 cat# **show interface g3/2 counters** Port InOctets InUcastPkts **InMcastPkts** InBcastPkts Gi3/2 14873677 2 **89391** 0 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Gi3/2 114366106 83776 732087 19 (STP ポートの役割についての簡単な説明は、『ループ ガードと BPDU スキュー検出機能を使用したスパニングツリー プロトコルの拡張』の「STP ポートの役割の要約」のセクションにあります。) BPDU が受信されない場合は、そのポートでエラーがカウントされていないかどうかを確認します。 次のように、show interface interface counters errors コマンドを発行します。 cat# **show interface g4/3 counters errors** Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards Gi4/3 0 0 0 0 0 0 Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen Runts Giants Gi4/3 0 0 0 0 0 0 0 BPDU が物理ポートによって受信されてはいるものの、STP プロセスに達してしない可能性があります。 上記 2 つの例で使用したコマンドを実行して、マルチキャストがある程度受信され、かつエラーが増加していないことが示された場合は、BPDU が STP プロセスの段階で廃棄されていないかどうかを確認します。 次のように、Catalyst 6500 上で remote command switch test spanning-tree process-stats コマンドを発行します。cat# **remote command switch test spanning-tree process-stats** ------------------TX STATS------------------ transmission rate/sec = 2 paks transmitted = 5011226 paks transmitted (opt) = 0 opt chunk alloc failures = 0 max opt chunk allocated = 0 ------------------RX STATS------------------ **receive rate/sec = 1** paks received at stp isr = 3947627 paks queued at stp isr = 3947627 **paks dropped at stp isr = 0 drop rate/sec = 0** paks dequeued at stp proc = 3947627 paks waiting in queue = 0 queue depth = 7(max) 12288(total) --------------PROCESSING STATS-------------- queue wait time (in ms) = 0(avg) 540(max) processing time (in ms) = 0(avg) 4(max) proc switch count = 100 add vlan ports = 20 time since last clearing = 2087269 sec この例で使用されたコマンドにより、STP プロセスの統計情報が表示されます。 廃棄カウンタの数が増加していないことを確認するとともに、受信パケットが増加していることを確認することが重要です。受信カウンタの数が増加していないにもかかわらず、物理ポートでマルチキャストを受信している場合は、パケットがそのスイッチのインバンド インターフェイス (CPU のインターフェイス) によって受信されているかを確認します。 **remote コマンド switch を示します ibc を**発行して下さい | Catalyst 6500/6000 の **| rx_input** コマンド:cat# **remote command switch show ibc | i rx_input** rx_inputs=**5626468**, rx_cumbytes=859971138 cat# **remote command switch show ibc | i rx_input** rx_inputs=**5626471**, rx_cumbytes=859971539 この例では、2 回の出力の間に 23 個のパケットがインバンド ポートにより受信されたことを示しています。**注:** この 23 のパケットはだけでなく、BPDUパケットです; これはインバンド ポートによって受信されるすべてのパケットのための Global カウンターです。ローカル スイッチやポート上で BPDU が廃棄されている形跡がない場合は、リンクの反対側のスイッチに移動して、そのスイッチが BPDU を送信しているかどうかを確認する必要があります。BPDU がルートではない指定ポートに規則的

に送信されているか。ポートの役割によれば、ポートから BPDU が送信されているにもかかわらず、隣接ルータでこれが受信されていない場合は、BPDU が実際に送信されているかどうかを確認します。 次のように、show spanning-tree interface interface detail コマンドを発行します。`cat# **show spanning-tree interface g3/1 detail** Port 129 (GigabitEthernet3/1) of MST00 is **designated** forwarding Port path cost 20000, Port priority 128, Port Identifier 128.129. Designated root has priority 0, address 0007.4f1c.e847 Designated bridge has priority 32768, address 00d0.003f.8800 Designated port id is 128.129, designated path cost 2000019 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 0 Link type is point-to-point by default, Internal Loop guard is enabled by default on the port **BPDU: sent 1774**, received 1 cat# **show spanning-tree interface g3/1 detail** Port 129 (GigabitEthernet3/1) of MST00 is **designated** forwarding Port path cost 20000, Port priority 128, Port Identifier 128.129. Designated root has priority 0, address 0007.4f1c.e847 Designated bridge has priority 32768, address 00d0.003f.8800 Designated port id is 128.129, designated path cost 2000019 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 0 Link type is point-to-point by default, Internal Loop guard is enabled by default on the port **BPDU: sent 1776**, received 1` この例では、2 回の出力の間に 2 つの BPDU が送信されています。**注:** STPプロセスは `BPDU` 維持します: カウンター。 このカウンタにより、物理ポートに向けた BPDU が実際に送信されたことが示されています。 送信済みマルチキャスト パケット用のポート カウンタが増加していないかどうかを確認します。 次のように、show interface interface counters コマンドを発行します。 この確認は、BPDU が送信されたかどうかを判別するのに役立ちます。`cat# **show interface g3/1 counters** Port InOctets InUcastPkts InMcastPkts InBcastPkts Gi3/1 127985312 83776 812319 19 Port OutOctets OutUcastPkts **OutMcastPkts** OutBcastPkts Gi3/1 131825915 3442 **872342** 386 cat# **show interface g3/1 counters** Port InOctets InUcastPkts InMcastPkts InBcastPkts Gi3/1 127985312 83776 812319 19 Port OutOctets OutUcastPkts **OutMcastPkts** OutBcastPkts Gi3/1 131826447 3442 **872346** 386` これらのすべてのステップを実行すれば、BPDU が受信、送信または処理されなかったスイッチやリンクを発見できます。まれに、STP がポートの正確な状態を計算したにもかかわらず、コントロール プレーンの障害によって、この状態を転送ハードウェアに設定できないことがあります。 ブロックされる必要があるポートがハードウェア レベルでブロックされていない場合は、ループが発生する可能性があります。 ご使用のネットワークでこのような問題が疑われるときは、シスコ テクニカルサポートにお問い合せください。

5. 冗長性の復元を行います。ループを引き起こしているデバイスやリンクを特定できたら、このデバイスをネットワークから遮断するか、この問題を解決するための処置 (ファイバまたは GBIC の交換など) を行う必要があります。 ステップ 3 で接続解除した冗長リンクを復元する必要があります。ループを引き起こしているデバイスやリンクに対する操作は、なるべく少なくすることが重要です。これは、ループにつながる多くの条件は、常に変化しており、不定期に発生するもので、さらに不安定であるためです。 つまり、このような条件は、トラブルシューティングの間またはその直後には解消されていても、ある程度の時間が経過してから再発する場合があるということです。 またこのような状況がまったく再発しない可能性もあります。 シスコ テクニカル サポートによる詳しい調査を可能にするためには、このような状況を保全する必要があります。 スイッチをリセットする前に、このような状況に関する情報を収集することが重要です。 状況が解消されても、ループの根本的な原因を特定することが困難な場合が度々あります。 ループを引き起こしているデバイスやリンクを特定することが主要な目的ですが、同じような障害によってループが再発することがないようにする必要もあります。 この件に関する詳細は、このドキュメントの「フォワーディング ループからのネットワークの保護」のセクションを参照してください。

トラブルシューティング：過度のトポロジ変更が原因で発生するフラッディング

TC メカニズムの役割は、転送トポロジが変更された後に L2 転送テーブルを修正することです。 TC の発生後に、それまであるポートを介してアクセスできていた MAC アドレスが、別のポートを介さないとアクセスできなくなる場合があります。これによって接続不能になる事態を避けるために、TC メカニズムが必要になります。 TC は TC が発生する VLAN のすべてのスイッチのフォワーディングテーブル 経過時間を短縮します; 従って、アドレスが学び直されなければ、それはエージング アウト、パケット範囲に宛先MAC アドレスを確認するためにフラッディングはために発生します。

TC は、ポートの STP 状態が STP forwarding 状態に変わった場合、または forwarding 状態から別の状態に変わった場合に発生します。 特定のデスティネーション MAC アドレスが期限切れになってもあふれる TC が長くのために続くべきではなかった後。 アドレスは最初のパケットによって学び直されます MAC アドレスが期限切れになったホストから来る。 問題となるのは、TC が短い間隔で繰り返し発生した場合です。 スイッチの転送テーブルがすぐにエージングするため、フラッディングがほとんど絶え間なく発生します。

注: Rapid STP または Multiple STP (IEEE 802.1w および IEEE 802.1s) では、ポートの状態が forwarding に変わった場合だけでなく、役割が designated から root に変わった場合にも、TC が発生します。 802.1D ではエージング タイムが短縮されるのに対し、Rapid STP では L2 転送テーブルが即座にフラッシュされます。 転送テーブルが即座にフラッシュされると、接続は早く復元されますが、フラッディングは増加します。

適切に構成されたネットワークでは、TC はまれにしか発生しません。 スイッチ ポートのリンクがアップまたはダウンすると、ポートの STP 状態が forwarding に変わるか、または forwarding から別の状態に変わり、そのたびに TC が発生します。 ポートがフラッピングしていると、TC が繰り返し発生し、そのたびにフラッディングが発生します。

STP PortFast 機能が有効なポートでは、forwarding 状態に移行したり、forwarding 状態から別の状態に移行しても、TC は発生しません。 すべてのエンドデバイス ポート (プリンタ、PC、サーバなど) で PortFast を設定すれば、TC の量を抑えることができるため、この設定を行うことを強く推奨します。 TC の詳細については、『スパニングツリー プロトコル トポロジの変更』を参照してください。

ネットワーク上で TC が繰り返し発生する場合は、その TC の発生元を特定し、TC を減らすための処置を行って、フラッディングを最小限に抑える必要があります。

802.1d では、TC イベントに関する STP 情報は、BPDU の特別な種類である TC Notification (TCN; TC 通知) を通じて、各ブリッジに伝搬されます。 TCN BPDU を受信しているポートをたどっていけば、TC の発生元のデバイスを特定できます。

フラッディングの原因が STP TC かどうかの調査

フラッディングは通常、パフォーマンスの低下が観察されたり、輻輳が起こるはずのないリンクでパケットが廃棄されたり、ローカル セグメント上にない同一の宛先に対する複数のユニキャスト パケットがパケット アナライザで示されることから判断されます。

ユニキャスト フラッディングの詳細は、『752スイッチド キャンパス ネットワークにおけるユニキャスト フラッディング』を参照してください。

Cisco IOS ソフトウェアが稼働している Catalyst 6500/6000 では、フォワーディング エンジンのカウンタ (スーパーバイザ 2 エンジンの場合のみ) をチェックして、フラッディングの量を見積ることができます。 **remote コマンド switch を表示します EARL 統計情報を**発行して下さい **| i MISS_DA|**ST_FRコマンド:

```
cat# remote command switch show earl statistics | i MISS_DA|ST_FR ST_MISS_DA = 18 530308834
ST_FRMS = 97 969084354 cat# remote command switch show earl statistics | i MISS_DA|ST_FR
ST_MISS_DA = 4 530308838 ST_FRMS = 23 969084377
```

この例では、このコマンドが最後に実行されてからの変更が最初のカラムに、最後にリブートしてからの累積値が 2 番目のカラムに示されています。 フラッディングが発生したフレームの量が最初の行に示され、処理されたフレームの量が 2 番目の行に示されています。 この 2 つの値が近い場合、または最初の値が急速に増加している場合には、そのスイッチがトラフィックのフラッディングを発生させている可能性があります。 ただし、このカウンタは精度が低いので、フラッディングが発生していることを確認するその他の方法と必ず併用するようにしてください。 カウンタは、スイッチごとに 1 つ存在します。ポートごとや VLAN ごとではありません。 ときおりフラッディング パケットが発生するのは正常です。それは、宛先 MAC アドレスが転送テーブルにない場合には、スイッチによってフラッディングが行われるからです。 また、学習されていない宛先アドレスを持つパケットをスイッチが受信した場合にも、フラッディングが行われます。

TC の発生元の特定

過度のフラッディングが発生している VLAN の VLAN 番号がわかっている場合は、STP カウンタをチェックして、TC の数が多いかどうか、TC の数が恒常的に増加しているかどうかを調べます。 次のように、show spanning-tree vlan vlan-id detail コマンドを発行します（この例では VLAN 1 が使用されています）。

```
cat# show spanning-tree vlan 1 detail VLAN0001 is executing the ieee compatible Spanning Tree
protocol Bridge Identifier has priority 32768, sysid 1, address 0007.0e8f.04c0 Configured hello
time 2, max age 20, forward delay 15 Current root has priority 0, address 0007.4f1c.e847 Root
port is 65 (GigabitEthernet2/1), cost of root path is 119 Topology change flag not set, detected
flag not set Number of topology changes 1 last change occurred 00:00:35 ago from
GigabitEthernet1/1 Times: hold 1, topology change 35, notification 2 hello 2, max age 20,
forward delay 15 Timers: hello 0, topology change 0, notification 0, aging 300
```

VLAN 番号がわからない場合は、パケット アナライザを使用するか、またはすべての VLAN の TC カウンタをチェックします。

過度の TC を防ぐための処置

number of topology changes カウンタを監視して、値が恒常的に増加しているかどうかを調べます。 次に、最後の TC を受信したポート（前の例では、GigabitEthernet 1/1 というポート）に接続されているブリッジに移動し、そのブリッジへの TC がどこから来たかを調べます。 STP PortFast が有効になっていない端末ポートが見つかるか、修正が必要なフラッピング リンクが見つかるまで、この処理を繰り返す必要があります。 依然として別の場所から TC が送られてくる場合には、この手順全体を繰り返す必要があります。 リンクがエンド ホストのものである場合は、PortFast 機能を設定して、TC が発生しないようにしてください。

注: Cisco IOS ソフトウェアの STP の実装では、TC のカウンタが増加するのは、TCN BPDU が VLAN 内のポートで受信された場合だけです。 TC フラグが設定された通常のコンフィギュレーション BPDU が受信されても、TC カウンタは増加しません。 したがって、フラッディングの原因として TC が疑われる場合は、その VLAN 内の STP ルート ブリッジから TC の発生元を突き止めていくのが、最善の方法です。 この方法が、TC の量および発生元に関して最も正確な情報が得られる方法です。

コンバージェンス時間に関する問題のトラブルシューティング

STP の実際の動作が、期待した動作とは異なる場合があります。 最もよく発生する 2 つの問題は、次のとおりです。

- STP コンバージェンスまたは再コンバージェンスに、予想以上に時間がかかる。
- 結果として作成されるトポロジが、期待したものと違う。

多くの場合、このような動作は次の原因で発生します。

- 実際のトポロジと文書に記載されているトポロジのミスマッチ
- 設定の誤り（たとえば、STP タイマーの設定の不統一、STP の直径の超過、PortFast の設定の誤りなど）
- コンバージェンス時または再コンバージェンス時にスイッチの CPU に過負荷がかかっている
- ソフトウェアの欠陥

前述のとおり、STP に影響を与える問題は多岐に渡るので、このドキュメントでは、トラブルシューティングの一般的なガイドラインだけを説明します。

コンバージェンスに予想以上に時間がかかる理由を突き止めるためには、一連の STP イベントを調べて、何がどのような順序で行われているかを調べます。 Cisco IOS ソフトウェアの STP 実装には（ポート不統一などの特別なイベントを除いて）特別なロギングはないので、発生している事象を調べるためには、Cisco IOS ソフトウェアの STP デバッグ機能を使用します。

Cisco IOS ソフトウェアが稼働している Catalyst 6500/6000 で STP を使用する場合は、Switch Processor（SP; スイッチ プロセッサ）（またはスーパーバイザ）で処理が行われます。したがって、SP でデバッグを有効にする必要があります。 Cisco IOS ソフトウェアのブリッジ グループでは、Route Processor（RP; ルート プロセッサ）で処理が行われます。したがって、RP（MSFC）でデバッグを有効にする必要があります。

STP デバッグ コマンド

多くの STP debug コマンドは、開発時に使用するためのコマンドです。 その出力を理解するには、Cisco IOS ソフトウェアの STP の実装に関する詳細な知識が必要になります。 いくつかのデバッグは、すぐに読める形で出力できます。これには、ポートの状態や役割の変化、TC などのイベント、受信または送信された BPDU のダンプなどが含まれます。 このセクションでは、すべてのデバッグを詳細に説明することはせず、最もよく使用されるデバッグを簡単に説明します。

注: debug コマンドを使用する際は、必要最小限のデバッグだけを有効にしてください。 リアルタイムでデバッグを行う必要がない場合は、出力はコンソールに表示させず、ログに記録するようにしてください。 過度のデバッグを行うと、CPU に過負荷がかかり、スイッチの動作が中断する場合があります。 デバッグの出力を、コンソールや Telnet セッションに表示させずに、ログに記録するには、logging console informational および no logging monitor コマンドをグローバル コンフィギュレーション モードで発行します。

Per VLAN Spanning-Tree（PVST）および Rapid-PVST の場合、一般的なイベントのログを見るには、debug spanning-tree event コマンドを発行します。 これは、STP で何が起こっているかを大まかに把握するための、最初のデバッグです。

Multiple Spanning-Tree（MST; 多重スパニングツリー）モードの場合は、debug spanning-tree event コマンドは動作しません。 そのため、debug spanning-tree mstp roles コマンドを発行して、ポートの役割の変化を調べます。

ポートの STP 状態の変化を調べるには、次のように、debug spanning-tree switch state コマンドと debug pm vp コマンドを発行します。

```
cat-sp# debug spanning-tree switch state Spanning Tree Port state changes debugging is on cat-
sp# debug pm vp Virtual port events debugging is on Nov 19 14:03:37: SP: pm_vp 3/1(333): during
```

state forwarding, got event 4(remove) **Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): forwarding -> notforwarding port 3/1 (was forwarding) goes down in vlan 333** Nov 19 14:03:37: SP: *** vp_fwdchange: single: notfwd: 3/1(333) Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): notforwarding -> present Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/1(333) Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): present -> not_present Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/1(333) **Nov 19 14:03:37: SP: pm_vp 3/2(333): during state notforwarding, got event 4(remove) Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): notforwarding -> present Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/2(333) Port 3/2 (was not forwarding) in vlan 333 goes down** Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): present -> not_present Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/2(333) Nov 19 14:03:53: SP: pm_vp 3/1(333): during state not_present, got event 0(add) Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): not_present -> present Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/1(333) **Nov 19 14:03:53: SP: pm_vp 3/1(333): during state present, got event 8(linkup) Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): present -> notforwarding Nov 19 14:03:53: SP: STP SW: Gi3/1 new blocking req for 0 vlans Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/1(333) Port 3/1 link goes up and blocking in vlan 333** Nov 19 14:03:53: SP: pm_vp 3/2(333): during state not_present, got event 0(add) Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): not_present -> present Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/2(333) **Nov 19 14:03:53: SP: pm_vp 3/2(333): during state present, got event 8(linkup) Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): present -> notforwarding Nov 19 14:03:53: SP: STP SW: Gi3/2 new blocking req for 0 vlans Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/2(333) Port 3/2 goes up and blocking in vlan 333 Nov 19 14:04:08: SP: STP SW: Gi3/1 new learning req for 1 vlans Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 0 vlans Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 1 vlans Nov 19 14:04:23: SP: pm_vp 3/1(333): during state notforwarding, got event 14(forward_notnotify) Nov 19 14:04:23: SP: @@@ pm_vp 3/1(333): notforwarding -> forwarding Nov 19 14:04:23: SP: *** vp_list_fwdchange: forward: 3/1(333) Port 3/1 goes via learning to forwarding in vlan 333**

STP が特定の動作を行う理由を調べる場合には、スイッチが受信または送信した BPDU を見ると、多くの場合役に立ちます。

cat-sp# **debug spanning-tree bpdu receive** Spanning Tree BPDU Received debugging is on Nov 6 11:44:27: SP: STP: VLAN1 rx BPDU: config protocol = ieee, packet from GigabitEthernet2/1 , linktype IEEE_SPANNING , enctype 2, encsize 17 Nov 6 11:44:27: SP: STP: enc 01 80 C2 00 00 00 00 06 52 5F 0E 50 00 26 42 42 03 Nov 6 11:44:27: SP: STP: Data 0000000000000000074F1CE847000000138048000 6525F0E4 08010010014000 2000F00 Nov 6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013 80480006525F0E40 8010 0100 1400 0200 0F00

このデバッグは PVST、Rapid-PVST および MST モードのためにはたらきます; しかしそれは BPDU のコンテンツをデコードしません。 しかし、BPDU が受信されていることは確認できます。

PVST および Rapid-PVST で BPDU のコンテンツを表示するには、次のように、debug spanning-tree switch rx decode コマンドと debug spanning-tree switch rx process コマンドを発行します。 MST で BPDU のコンテンツを表示するには、debug spanning-tree mstp bpdu-rx コマンドを発行します。

cat-sp# **debug spanning-tree switch rx decode** Spanning Tree Switch Shim decode received packets debugging is on cat-sp# **debug spanning-tree switch rx process** Spanning Tree Switch Shim process receive bpdu debugging is on Nov 6 12:23:20: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026 Nov 6 12:23:20: SP: encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1 Nov 6 12:23:20: SP: 42 42 03 SPAN Nov 6 12:23:20: SP: CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013 Nov 6 12:23:20: SP: B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00 Nov 6 12:23:22: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026 Nov 6 12:23:22: SP: encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1 Nov 6 12:23:22: SP: 42 42 03 SPAN Nov 6 12:23:22: SP: CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013 Nov 6 12:23:22: SP: B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00

MST モードの場合は、次の debug コマンドを使用すると、詳細な BPDU のデコードを有効にできます。

cat-sp# **debug spanning-tree mstp bpdu-rx** Multiple Spanning Tree Received BPDUs debugging is on Nov 19 14:37:43: SP: MST:BPDU DUMP [**rcvd_bpdu Gi3/2** Repeated] Nov 19 14:37:43: SP: MST: Proto:0 Version:3 Type:2 Role: DesgFlags[F] Nov 19 14:37:43: SP: MST: Port_id:32897 cost:2000019 Nov

```
19 14:37:43: SP: MST: root_id :0007.4f1c.e847 Prio:0 Nov 19 14:37:43: SP: MST: br_id
:00d0.003f.8800 Prio:32768 Nov 19 14:37:43: SP: MST: age:2 max_age:20 hello:2 fwdelay:15 Nov 19
14:37:43: SP: MST: V3_len:90 PathCost:30000 region:STATIC rev:1 Nov 19 14:37:43: SP: MST:
ist_m_id :0005.74 Nov 19 14:37:43: SP: MST:BPDU DUMP [rcvd_bpdu Gi3/2 Repeated] Nov 19 14:37:43:
SP: MST: Proto:0 Version:3 Type:2 Role: DesgFlags[ F ] Nov 19 14:37:43: SP: MST: Port_id:32897
cost:2000019 Nov 19 14:37:43: SP: MST: root_id :0007.4f1c.e847 Prio:0 Nov 19 14:37:43: SP: MST:
br_id :00d0.003f.8800 Prio:32768 Nov 19 14:37:43: SP: MST: age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST: V3_len:90 PathCost:30000 region:STATIC rev:1 Nov 19 14:37:43: SP: MST:
ist_m_id :0005.7428.1440 Prio:32768 Hops:18 Num Mrec: 1 Nov 19 14:37:43: SP: MST: stci=3 Flags[
F ] Hop:19 Role:Desg [Repeated] Nov 19 14:37:43: SP: MST: br_id:00d0.003f.8800 Prio:32771
Port_id:32897 Cost:2000028.1440 Prio:32768 Hops:18 Num Mrec: 1 Nov 19 14:37:43: SP: MST: stci=3
Flags[ F ] Hop:19 Role:Desg [Repeated] Nov 19 14:37:43: SP: MST: br_id:00d0.003f.8800 Prio:32771
Port_id:32897 Cost:20000
```

注: Cisco IOS ソフトウェア リリース 12.1.13E 以降では、STP の条件付デバッグがサポートされています。 これにより、受信または送信された BPDU をポートごとまたは VLAN ごとにデバッグできます。

debug condition vlan vlan_num または debug condition interface interface コマンドを発行して、デバッグ出力の範囲を特定のインターフェイスまたは VLAN に限定します。

フォワーディング ループからのネットワークの保護

STP が特定の障害を正しく処理できない問題に対処するために、シスコでは多くの機能や機能拡張を開発し、フォワーディング ループからネットワークを保護しています。

STP のトラブルシューティングは、特定の障害が発生した原因の絞り込みおよび特定に役立ちますが、フォワーディング ループからネットワークを保護するための唯一の方法は、それらの機能拡張を実装することです。

次に、フォワーディング ループからネットワークを保護する方法を示します。

1. スイッチとスイッチをつなぐすべてのリンクで、UniDirectional Link Detection (UDLD; 単方向リンク検出) を有効にします。 UDLD の詳細については、『単方向リンク検出プロトコル機能の説明と設定』を参照してください。
2. すべてのスイッチでループ ガードを有効にします。 ループ ガードの詳細については、『ループ ガードと BPDU スキュー検出機能を使用したスパニングツリー プロトコルの拡張』を参照してください。UDLD とループガードを有効にすると、フォワーディング ループを発生させる原因の大部分が取り除かれます。 フォワーディング ループが作成される代わりに、問題のリンク (または障害が発生したハードウェアに依存するすべてのリンク) がシャットダウンまたはブロックされます。**注:** この 2 つ機能は重複しているように見えますが、それぞれ固有の機能が備わっています。 したがって、両方の機能を同時に使用すれば、最も高度な保護が行われます。 UDLD とループ ガードの詳細な比較については、『ループ ガードと単方向リンク検出』を参照してください。アグレッシブ UDLD を使用すべきか、通常の UDLD を使用すべきかについては、さまざまな意見があります。 注意する必要があるのは、アグレッシブ UDLD にしても、通常モードの UDLD に比べてループに対する保護が強化されるわけではない、ということです。 アグレッシブ UDLD では、ポートスタックのシナリオ (リンクはアップ状態だが、関連するトラフィックのブラックホールがない状態) が検出されます。 この追加機能の欠点は、一貫した障害が存在しないと、アグレッシブ UDLD によってリンクが無効にされてしまう可能性があることです。 UDLD の hello 間隔の修正は、アグレッシブ UDLD 機能とよく混同されます。 これは正しくありません。 タイマーは、どちらの UDLD モードでも修正できます。**注:** まれに、アグレッシブ UDLD によってすべてのアップリンク ポートがシャットダウンされ、スイッチが実質的にネットワークに

接続されていない状態になることがあります。 これは、たとえば、両方のアップストリーム スイッチの CPU に非常に高い負荷がかかっており、アグレッシブ モードの UDLD が使用されている場合に発生することがあります。 したがって、スイッチでアウトオブバンド管理が有効でない場合には、エラーディセーブルタイムアウトを設定することを推奨します。

3. すべての端末ポートで PortFast を有効にします。ネットワークのパフォーマンスに影響を与える可能性のある TC およびそれに続くフラッディングの量を制限するためには、PortFast を有効にする必要があります。 端末に接続するポートとだけこのコマンドを使用して下さい。 さもなければ、偶然トポロジループによりデータパケット ループを引き起こし、スイッチおよびネットワークオペレーションを中断する場合があります。**注意：** **spanning-tree portfast コマンドを**使用しないとき注意して下さい。 このコマンドはポート細目 portfast コマンドだけを取除きます。 このコマンドは暗黙のうちにグローバル コンフィギュレーション モードの**スパニングツリーポートファスト default コマンドを**定義すれば、そしてポートがトランク ポートでなければ portfast を有効に します。 portfast をグローバルに設定しない場合、**spanning-tree portfast コマンドはスパニングツリーポートファスト disable コマンド**と同等ではないです。
4. 両端で EtherChannel を desirable モードに設定し（サポートされている場合）、non-silent オプションを設定します。desirable モードにすると、Port Aggregation Protocol（PAgP; ポート集約プロトコル）によって、実行時のチャネル ピア間の一貫性が保たれます。 これによって、特にチャネルの再設定時（チャネルへのリンクの追加時や削除時、リンク障害の検出時など）に、ループの発生を防止する能力が一段と強化されます。 内蔵の Channel Misconfiguration Guard（チャネルの設定ミス ガード）もあります。これはデフォルトで有効であり、チャネルの設定ミスや他の状況が原因でフォワーディング ループが発生することを防ぎます。 この機能の詳細については、『EtherChannel の不一致検出について』を参照してください。
5. スイッチとスイッチをつなぐリンクの自動ネゴシエーションは、無効にしないでください（サポートされている場合）。自動ネゴシエーション メカニズムは、リモート障害情報を伝達できます。これは、リモート側での障害を最も早く検出できる方法です。 リモート側で障害が検出された場合、リンクが引き続きパルスを受信していても、ローカル側はリンクをダウンさせます。 UDLD のような高レベル 検知機構と比較されて、オート ネゴシエーションは非常にファースト（マイクロ秒の内で）しかし UDLD のエンドツーエンド カバレッジに欠けています（全体の datapath のような: _cpu —転送論理を— port1 — port2 —フォワーディング論理— CPU vs port1 — port2）。 障害検出機能については、アグレッシブ UDLD モードの機能と自動ネゴシエーションの機能はよく似ています。 リンクの両端でネゴシエーションがサポートされている場合には、アグレッシブモードの UDLD を有効にする必要はありません。
6. STP タイマーの調整は慎重に行ってください。STP タイマーは、タイマー相互およびネットワーク トポロジに依存しています。 タイマーを不注意に変更すると、STP が正しく動作しなくなることがあります。 STP タイマーの詳細については、『スパニングツリー プロトコル（STP）タイマーの理解と調整』を参照してください。
7. サービス拒絶攻撃を受ける可能性がある場合は、ネットワーク STP 境界をルート ガードで保護してください。ルート ガードと BPDU ガードを使用すると、外部の操作から STP を保護できます。 このような攻撃を受ける可能性がある場合には、ルート ガードと BPDU ガードを使用してネットワークを保護する必要があります。 ルート ガードおよび BPDU ガードの詳細は、次のドキュメントを参照してください。スパニングツリー プロトコル ルート ガード機能拡張スパニングツリー PortFast BPDU ガード機能拡張
8. PortFast 対応ポートで BPDU ガードを有効にして、そのポートに接続されている権限のないネットワーク デバイス（ハブ、スイッチ、ブリッジ ルータなど）によって STP が操作さ

れることを防ぎます。ルート ガードが適切に設定されていれば、外部からの STP の操作はすでに防がれています。 BPDU ガードを有効にすると、（優良な BPDU だけでなく）どのような BPDU を受信してもポートがシャットダウンされます。 BPDU ガードは、syslog メッセージを作成してからポートをシャットダウンするので、このような事象を調査する必要がある場合に便利です。 2 つの PortFast 対応ポートが、直接またはハブを経由して接続されている場合は、短期間しか続かないループは、ルート ガードでも BPDU ガードでも防ぐことはできないことに注意してください。

9. 管理 VLAN でのユーザ トラフィックを防ぎます。 管理 VLAN は、ネットワーク全体ではなく、ビルディング ブロックに限定します。管理 VLAN のブロードキャスト パケットは、スイッチ管理インターフェイスで受信されます。 過度のブロードキャストが発生した場合（ブロードキャスト ストームやアプリケーションの誤動作などが発生した場合）、スイッチの CPU に過負荷がかかって、STP の動作に悪影響を与える可能性があります。
10. STP ルートとバックアップ STP ルートの配置を、予測できるようにしておきます（ハードコードします）。STP ルートとバックアップ STP ルートを設定して、どのような状況で障害が発生してもコンバージェンスが予測どおりに行われ、トポロジが適切に構築されるようにしておく必要があります。 STP の優先順位をデフォルト値のままにして、どのルート スイッチが選択されるか予測できない状態にはしないでください。

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とドキュメント - Cisco Systems