

CatalystスイッチでのSTP問題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](#)

[STP障害の原因](#)

[転送ループのトラブルシューティング](#)

[1. ループの識別](#)

[2. ループのトポロジ \(範囲 \) の検出](#)

[3. ループの解除](#)

[4. ループの原因の発見と修正](#)

[5. 冗長性の復元](#)

[トポロジ変更の調査](#)

[フラグメンテーションの原因の特定](#)

[TCの発生源の特定](#)

[過度の TC を防ぐための処置](#)

[コンバージェンス時間関連の問題のトラブルシューティング](#)

[STP debugコマンドの使用](#)

[フォワーディングループからのネットワークの保護](#)

[1. すべてのスイッチ間リンクで単方向リンク検出\(UDLD\)を有効にする](#)

[2. すべてのスイッチでループガードを有効にする](#)

[3. すべてのエンドステーションポートでPortFastを有効にする](#)

[4. 両側 \(サポートされている場合 \) とNon-SilentOptionでEtherChannelをDesirableModeに設定する](#)

[5. スイッチ間リンクでオートネゴシエーションを無効にしない \(サポートされている場合 \)](#)

[6. STPタイマーを調整する際には注意が必要です](#)

[7. サービス拒絶攻撃を受ける可能性がある場合は、ルートガードでネットワークSTP境界を保護します](#)

[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た未承認のネットワークデバイス \(ハブ、スイッチ、ブリッジングルータなど \) によるSTPの影響を防止します](#)

[9. 管理VLANでのユーザトラフィックの回避](#)

[10. 予測可能な \(ハードコードされた \) STPルートとバックアップSTPルートの配置](#)

[関連情報](#)

はじめに

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方法について説明します。

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。詳細については、『[STPおよび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いています。

- 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

ドキュメント表記の詳細については、『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

Catalyst 6500/6000だけに適用される特定のコマンドもありますが、ほとんどの原則は、Cisco IOSソフトウェアを実行する任意のCisco Catalystスイッチに適用できます。

ほとんどのSTPの問題には、次の3つの問題があります。

- フォワーディング ループ.
- STPトポロジ変更(TC)が頻繁に発生することによる過剰なフラッディング。
- コンバージェンス時間に関する問題.

ブリッジには、特定の packets が複数回転送されたのか（IP Time to Live [TTL]など）、またはネットワーク内を長時間循環するトラフィックを廃棄するのに使用されているのかを追跡するメカニズムがないためです。同じレイヤ2(L2)ドメイン内の2つのデバイス間に存在できるパスは1つだけです。

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、冗長な物理トポロジをツリー状のトポロジに解決することです。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。

フォワーディングループが開始すると、そのパスに沿って最低帯域幅のリンクが輻輳します。すべてのリンクが同じ帯域幅の場合、すべてのリンクが輻輳します。この輻輳によりパケット損失が発生し、影響を受けるL2ドメインでネットワークのダウン状態が発生します。

過度のフラッディングがあると、症状はそれほど明らかではありません。低速リンクは、フラッディングされたトラフィックによって輻輳する可能性があり、輻輳したリンクの背後にあるデバイスやユーザでは、遅延が発生したり、接続が完全に失われたりする可能性があります。

STP障害の原因

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がBに直接接続している場合、AはBが送信した内容を受信し、BはAが送信した内容を、リンクがB間でアップしている限り受信します。
- STPを実行する各ブリッジは、STPパケットとも呼ばれるSTPブリッジプロトコルデータユニット(BPDU)を定期的に受信、処理、および送信できます。

これらの前提条件は、一見論理的で当たり前のように思われますが、満たされない状況もあります。これらの状況のほとんどは、ハードウェアの問題に関連していますが、ソフトウェアの不具合が原因でSTP障害が発生する場合があります。さまざまなハードウェア障害、誤設定、接続の問題がSTP障害の大部分を引き起こしているのに対し、ソフトウェア障害は少数です。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。

これらの前提条件の1つが満たされない場合、1つ以上のブリッジがBPDUを受信または処理できません。これは、ブリッジがネットワークトポロジを検出しないことを意味します。正しいトポロジを認識していないと、スイッチはループをブロックできません。したがって、フラッディングされたトラフィックはループしたトポロジを循環し、すべての帯域幅を消費して、ネットワークをダウンさせます。

スイッチがBPDUを受信できない原因の例としては、トランシーバやGigabit Interface Converter (GBIC ; ギガビットインターフェイスコンバータ) の不良、ケーブルの問題、ポート、ラインカード、またはスーパーバイザエンジンのハードウェア障害などがあります。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。STP処理は、スイッチが受信したBPDUを処理できないため、CPUの過負荷 (99%以上) によって中断される可能性もあります。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。

フォワーディンググループ以外に、ブロックされているポートがない場合、トラフィックをブロックしているポートを経由して特定のパケットだけが誤って転送される状況があります。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。このような動作は、低速ループを引き起こす可能性があります。これは、一部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、トラフィックの大部分が引き続きネットワークを通過していることを意味します。

転送ループのトラブルシューティング

フォワーディンググループは、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開始する前に、次の情報が必要です。

- 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。
- 対応するポート番号（相互接続）。
- STP設定の詳細。たとえば、どのスイッチがルートおよびバックアップルートであるか、デフォルト以外のコストまたはプライオリティがどのリンクに設定されているか、トラフィックをブロックしているポートの位置がどれであるかなどの詳細。

1. ループの識別

ネットワーク内でフォワーディンググループが発生すると、通常は次のような症状が現れます。

- 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
- 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）。
- ネットワークでのパケットループを示すsyslogメッセージ（HSRP重複IPアドレスのメッセージなど）。
- 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で廃棄される出力の数が増加します。

これらの理由のいずれかが単独で異なる問題を示している可能性があります（または、まったく問題がない可能性があります）。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グループが発生している可能性が十分考えられます。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。

```
<#root>
```

```
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ソフトウェアを搭載したCatalyst 4000は、現在このコマンドをサポートしていません。

現在のトラフィックレベルが過剰であるか、またはベースラインレベルが不明な場合は、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、ピーク時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、スイッチの負荷が異常に高くな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. ループのトポロジ (範囲) の検出

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。

ループを停止するには、ループに参加しているポートを把握する必要があります。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確認します。show interfaceCisco IOSソフトウェア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。

使用率の情報とインターフェイス名だけを表示する (簡単に分析するため) には、Cisco IOSソフトウェアで一般的な式の出力をフィルタします。show interfaceを発行します。| include line|Vseccommandコマンドを使用すると、パケット/秒の統計情報とインターフェイス名のみを表示できます。

```
<#root>
```

```
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注意してください。この例では、インターフェイス g2/3、g2/4、およびg2/8がループに参加するポートです。

3. ループの解除

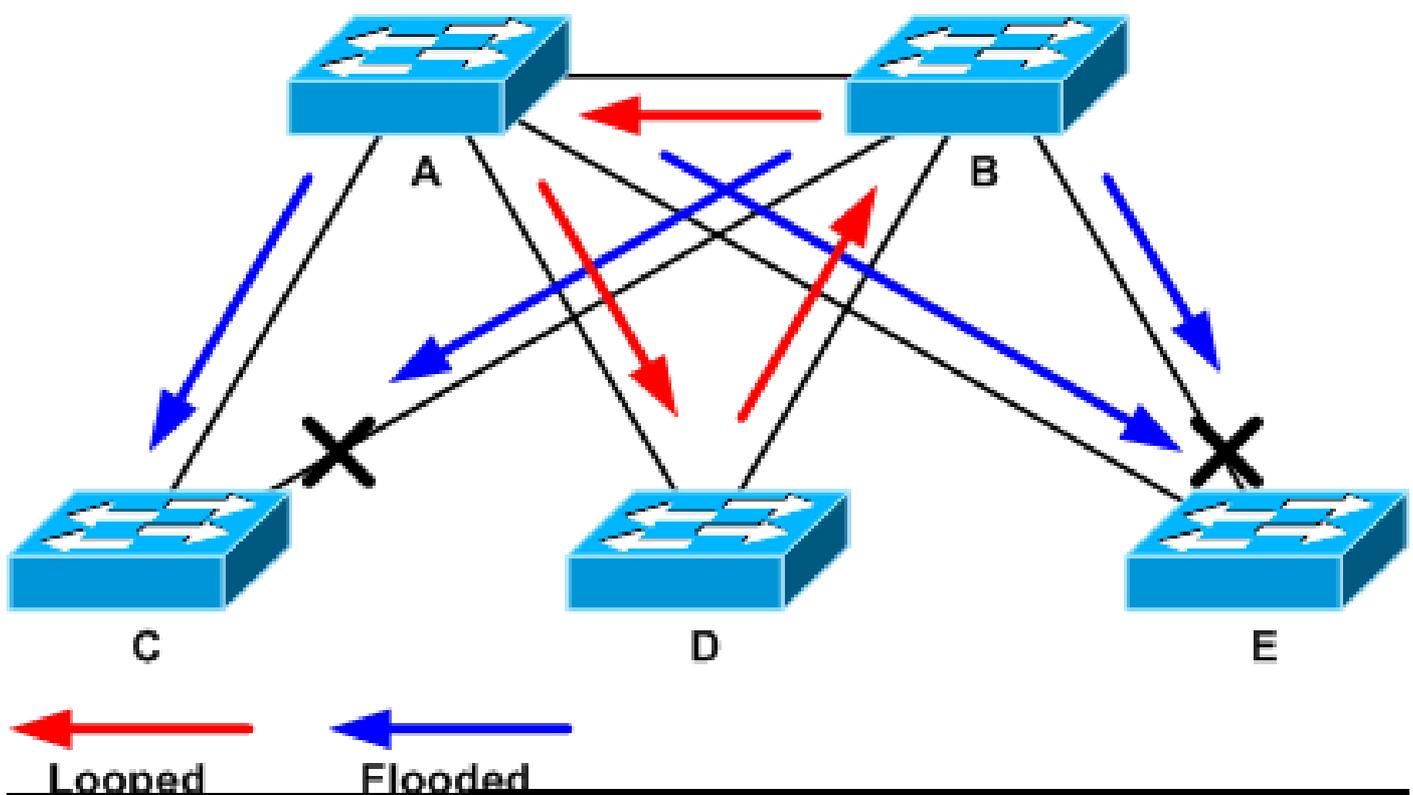
ループを遮断するには、関係するポートをシャットダウンするか接続解除します。ループを停止するだけでなく、ループの根本原因を見つけて修正することも特に重要です。ループを解消する方が比較的簡単です

 注：すべてのポートを同時にシャットダウンしたり、取り外したりする必要はありません。一度に1つずつシャットダウンできます。デистриビューションスイッチやコアスイッチなど、ループの影響を受ける集約ポイントでポートをシャットダウンすることをお勧めします。すべてのポートを一度にシャットダウンし、それらを1つずつイネーブルにしたり、再接続したりすると、機能しません。ループが停止し、障害のあるポートが再接続された直後にはループを開始できなくなります。したがって、障害を特定のポートに関連付けることは困難です。

注：ループを解消するために、スイッチをリブートする前に情報を収集することを推奨します。それ以外の場合、その後の根本原因分析は困難です。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：ポートはループを維持しませんが、ループに到達したトラフィックはフラッディングします。このようなフラッディングポートをシャットダウンしても、バックプレーン使用率はわずかに低下するだけで、ループは停止しません。

次のトポロジ例では、ループはスイッチA、B、およびDの間にあります。したがって、リンクAB、AD、およびBDが維持されます。これらのリンクのいずれかをシャットダウンすると、ループが停止します。リンクAC、AE、BC、およびBEは、ループを伴って到着するトラフィックを単にフラッディングしているだけです。



ループおよびフラッディングされたトラフィック

サポートポートをシャットダウンすると、バックプレーン使用率が正常値まで低下します。どのポートのシャットダウンによってバックプレーン使用率（および他のポートの使用率）が通常のレベルに戻ったかを知る必要があります。この時点でループが停止し、ネットワーク動作が改善されますが、ループの元の原因が修正されていないため、まだ他の問題があります。

4. ループの原因の発見と修正

ループが停止したら、ループの発生原因を特定する必要があります。理由はさまざまであるため、これはプロセスの難しい部分です。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。

ガイドライン：

- トポロジ図を調べて、冗長パスを見つけます。これには、前のステップで検出されたサポートポートが同じスイッチに戻る場合も含まれます（ループ中にパスパケットが通った場合）。前のトポロジの例では、このパスは AD-DB-BA です。
- 冗長パス上のすべてのスイッチについて、スイッチが正しいSTPルートを認識しているかどうかを確認します。

L2ネットワーク内のすべてのスイッチは、共通のSTPルートに合意する必要があります。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 コマンドを発行して、特定のVLANのルートブリッジIDを表示します。

```
<#root>
```

```
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。これが当てはまらない場合（たとえば、単一の VLAN でループが発生しているように見える場合）は、show interfaces | include L2|line|broadcastcommand (Catalyst 6500/6000 シリーズスイッチの Supervisor 2 以降のエンジンに対してのみ実行します。これは、Supervisor 1 では VLAN 単位のスイッチング統計情報が提供されないためです)。VLAN インターフェイスのみを確認します。多くの場合、ループが発生したのは、スイッチ導入パケットの数が最も多い VLAN です。

```
<#root>
```

```
cat#
```

```
show interface | 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。ルートポートが正しく識別されていることを確認します。

ルートポートは、ルートブリッジへのコストが最も低いポートである必要があります (低速ポートの方がコストが高いため、1つのパスがホップの点では短くてもコストの点では長い場合があります)。特定のVLANに対して、どのポートがルートとみなされているかを判断するには、show spanning-tree vlanコマンドを発行します。

```
<#root>
```

```
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

BPDUがルートポートとブロック対象のポートで定期的に受信されていることを確認します。

BPDUはevery hellointerval(デフォルトでは2秒)にルートブリッジから送信されます。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 コマンドを発行して、BPDUが受信されているかどうかを確認します。

```
<#root>
```

```
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：コマンドの2つの出力の間で1つのBPDUが受信されました（カウンタは53から54に変化しました）。

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。つまり、受信カウンタが増加した場合、BPDUが物理ポートで受信されただけでなく、STPプロセスでも受信されたこととなります。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で received BPDUカウンタが増加しない場合は、ポートがマルチキャスト（BPDUはマルチキャストとして送信される）を受信していないかどうかを確認します。次のように、show interface interface counters command コマンドを発行します。

<#root>

cat#

```
show interface g3/2 counters
```

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi3/2	14873036	2		

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		

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「[ループガードとBPDUスキュー検出によるSTPの拡張](#)」セクションにあります。BPDUが受信されない場合は、ポートでエラーがカウントされているかどうかを確認します。次のように、show interface interface counters errors command コマンドを発行します。

```
<#root>
```

```
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。前の2つの例で使用したコマンドによって、マルチキャストの一部が受信され、エラーがカウントされていないことが示された場合は、BPDUがSTPプロセスレベルで廃棄されているかどうかを確認してください。Catalyst 6500でremote command switch test spanning-tree process-statsコマンドを発行します。

```
<#root>
```

```
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
```

この例で使用されるコマンドは、STPプロセスの統計情報を表示します。ドロップカウンタが増

加していないこと、および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。受信パケットは増加しないが、物理ポートがマルチキャストを受信する場合は、パケットが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) で受信されていることを確認します。リモートコマンドスイッチshow ibcを発行します。 | Catalyst 6500/6000のi rx_inputcommand:

```
<#root>
```

```
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：これら23個のパケットはBPDUパケットだけではありません。これは、インバンドポートで受信されるすべてのパケットのグローバルカウンタです。

ローカルスイッチまたはポートでBPDUが廃棄されている形跡がない場合は、リンクの反対側にあるスイッチに移動して、そのスイッチからBPDUが送信され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定期的に送信されているかどうかを確認します。ポートの役割が一致する場合、ポートはBPDUを送信しますが、ネイバーはそれを受信しません。BPDUが送信されているかどうかを確認します。show spanning-tree interface interface detailコマンドを発行します。

```
<#root>
```

```
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つのBPDUが出力間で送信されます。

 注:STPプロセスはBPDU:sentcounterを維持します。これは、このカウンタが、BPDUが物理ポートに向けて送信され、送出されたことを意味します。送信済みマルチキャストパケットのポートカウンタが増加するかどうかを確認します。show interface interface counterscommandコマンドを発行します。これは、BPDUのトラフィックフローを判別するのに役立ちます。

```
<#root>
```

```
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。STPがポートの正しい状態を計算したが、コントロールプレーンの問題が原因で、転送ハードウェアにこの状態を設定できない可能性があります。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問題が発生していると考えられる場合は、[シスコのテクニカルサポート](#)にサポートを要請してください。

5. 冗長性の復元

ループを引き起こしているデバイスまたはリンクが見つかったら、そのデバイスをネットワークから切り離すか、問題を解決する必要があります（ファイバやGBICの交換など）。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。

ループを引き起こすデバイスやリンクを操作しないことが重要です。これは、ループを引き起こす多くの条件が一時的で、断続的で、不安定であるためです。つまり、調査の実行中または実行後に条件がクリアされた場合、その条件はしばらく発生しないか、まったく発生しません。[シスコテクニカルサポート](#)が詳しく調査できるように、状況を記録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。ある状態が解消された場合、ループの根本原因を特定することは不可能です。情報を収集する場合は、この問題によってループが再度発生していないことを確認します。詳細については、「[フォワーディングループからのネットワークの保護](#)」を参照してください。

トポロジ変更の調査

トポロジ変更(TC)メカニズムの役割は、トポロジの変更後にL2転送テーブルを修正することです。これは、以前は特定のポートを介してアクセスできていたMACアドレスが変更され、別のポートを介してアクセスできるようになるため、接続不能を回避するために必要です。TCは、TCが

発生しているVLAN内のすべてのスイッチで、転送テーブルの経過時間を短くする。そのため、アドレスが再学習されないと、エージングアウトしてフラッディングが発生し、パケットが確実に宛先MACアドレスに到達します。

TCは、ポートのSTPステートがSTPforwardingstateに変更されるか、STPforwardingstateから変更されることによってトリガーされます。TCの後、特定の宛先MACアドレスがエージングアウトしても、フラッディングが長く続くことはありません。このアドレスは、MACアドレスがエージングアウトされたホストから送信された最初のパケットによって再学習されます。TCが短い間隔で繰り返し発生すると、問題が発生する可能性があります。スイッチは転送テーブルを絶えずファストエージングしているため、フラッディングがほとんど絶え間なく発生する可能性があります。

 注：Rapid STP(RSTP)またはMultiple STP (IEEE 802.1wおよびIEEE 802.1s) を使用する場合、TCはポートの状態が forwardingに変更されること、およびロールが frodesignatedtorootに変更されることによってトリガーされます。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。転送テーブルを即時にフラッシュすると、接続の復元は高速になりますが、フラッディングが増加する可能性があります

TCは、適切に設定されたネットワークではまれなイベントです。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またはfromforwardingに変更された後、最終的に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のPortFast機能が有効になっているポートでは、TCがフォワーディング状態に移行したり、フォワーディング状態から戻ったりする際に、TCが発生することはありません。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を設定すると、TCの量が少なくなるため、設定することを強く推奨します。

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を受信するポートをたどると、TCを発信したデバイスを確認できます。

フラッディングの原因の特定

フラッディングはパフォーマンスの低下が原因であること、輻輳が起こるはずのないリンクでパケットが廃棄されていること、およびパケットアナライザはローカルセグメント上にない同じ宛先に対する複数のユニキャストパケットを示していることを判別できます。ユニキャストフラッディングの詳細については、『[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。リモートコマンドスイッチshow earl statisticsを発行します。 | i

MISS_DA|ST_FRcommand:

<#root>

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コラムに、最後にリポートしてからの累積値が2番目のコ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。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は、スイッチがトラフィックをフラッディングし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。宛先MACアドレスが転送テーブルにない場合はスイッチが常にフラッディングする可能性があるため、フラッディングパケットが見られることは正常です。これは、スイッチが、まだ学習されていない宛先アドレスを持つパケットを受信する場合に発生する可能性があります。

TCの発生源の特定

過剰な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、定期的に増加しているかを確認します。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）。

<#root>

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 の変更カウンタを監視して、定期的に増加するかどうかを確認できます。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。TC が他のソースから来る場合は、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に属している場合は、PortFast 機能を設定して TC の発生を防ぐことができます。

 注: Cisco IOS ソフトウェアの STP 実装では、TCN BPDU が VLAN 内のポートで受信された場合にだけ、TC のカウンタが増加します。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 カウンタは増分されません。つまり、フラッピングの原因が TC であると疑われる場合は、その VLAN 内の STP ルートブリッジから TC の発生源を突き止めます。TC の数と発生源に関して最も正確な情報を得ることができます。

コンバージェンス時間関連の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。
- トポロジ結果が予想と異なる。

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。
- STP タイマーの設定の不整合、STP 直径の増加、PortFast の設定ミスなど、設定ミス。
- 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ため、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

かかる理由を理解するには、STPイベントのシーケンスを調べて、何が起きているのか、どのような順序で行われているかを確認します。Cisco IOSソフトウェアのSTP実装では、結果（ポートの不一致などの特定のイベントを除く）はログに記録されないため、Cisco IOSソフトウェアを使用してSTPをデバッグすると、より明確に表示できます。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の場合、ルートプロセッサ(RP)で処理が行われるので、RP(MSFC)でデバッグを有効にする必要があります。

STP debugコマンドの使用

多くの STPdebugcommandsは、開発技術者向けです。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場合、必要最小限のデバッグを有効にします。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セッションではなくログに出力するには、グローバルコンフィギュレーションモードでthelogging console informationおよびno logging monitorコマンドを発行します。一般的なイベントのログを見るには、Per VLAN Spanning-Tree(PVST)とRapid-PVSTに対してdebug spanning-tree eventcommandを発行します。これは、STPで発生した問題に関する情報を提供する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 eventcommandコマンドは動作しません。したがって、debug spanning-tree mstp rolescommandを発行して、ポートの役割の変更を確認します。ポートのSTP状態の変化を見るには、debug spanning-tree switch statecommandとdebug pm vpccommandを発行します。

```
<#root>
```

```
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。

```
<#root>
```

```
cat-sp#
```

```
debug spanning-tree bpd 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 000000000000000074F1CE8470000001380480006525F0E4
080100100140002000F00
```

```
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モードでは機能しますが、BPDUの内容はデコードしません。しかし、BPDUが受信されていることは確認できます。BPDUの内容を表示するには、PVSTおよびRapid-PVSTのdebug spanning-tree switch rxプロセスコマンドとともにdebug spanning-tree switch rx decodecommandを発行します。MSTのBPDUの内容を確認するには、debug spanning-tree mstp bpd-rxcommandコマンドを発行します。

```
<#root>
```

```
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、次のdebugコマンドを使用して、詳細なBPDUのデコードを有効にできます。
。

<#root>

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 の条件付き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インターフェイス単位または VLAN 単位に制限します。

フォワーディンググループからのネットワークの保護

シスコは、STP が特定の障害を管理できない場合に、フォワーディンググループからネットワークを保護するために、多くの機能と拡張機能を開発しました。

STP のトラブルシューティングを行う際には、特定の障害の原因を切り分け、場合によっては見つけるのに役立ちます。また、フォワーディンググループからネットワークを保護するには、これらの機能拡張を実装することが唯一の方法です。

次に、フォワーディング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. すべてのスイッチ間リンクで単方向リンク検出(UDLD)を有効にする

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する

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機能](#)』を参照してください。

UDLD とループガードを有効にすると、フォワーディンググループの原因の大部分が排除されます。フォワーディンググループが発生する代わりに、障害のあるリンク (または障害のある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つの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を備えています。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。アグレッシブ UDLD では、通常モードの UDLD に比べて、ループに対する保護機能が強化されません。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 hello interval の変更は、アグレッシブ UDLD 機能と混同されることがよくあります。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の他の部分から分離されることがあります。たとえば、両方のアップストリームスイッチでCPU使用率が極端に高くなり、アグレッシブモードのUDLDが使用されている場合に、この状態が発生する可能性があります。したがって、スイッチにアウトオブバンド管理が設定されていない場合は、侵食できないタイムアウトを設定することを推奨します。

3. すべてのエンドステーションポートでPortFastを有効にする

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。このコマンドは、エンドステーションに接続するポートだけに使用します。そうしないと、予期しないトポロジグループによってデータパケットループが発生し、スイッチとネットワークの動作が中断する可能性があります。

 注意：no spanning-tree portfastコマンドを使用する場合は注意が必要です。このコマンドで削除されるのは、ポート固有のPortFastコマンドだけです。このコマンドは、グローバルコンフィギュレーションモードでspanning-tree portfast defaultコマンドを定義した場合、およびポートがトランクポートでない場合に、PortFastを暗黙的に有効にします。PortFastをグローバルに設定しない場合、no spanning-tree portfastコマンドはspanning-tree portfast disableコマンドと同等です。

4. 両側（サポートされている場合）でEtherChannelをDesirableモードに設定し、Non-Silent オプションを設定する

Desirableモードでは、ポート集約プロトコル(PAgP)を有効にして、チャネリングピア間でランタイムの一貫性を確保できません。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。組み込みのChannel Misconfiguration Guard（チャネル設定ミスガード）があります。これはデフォルトで有効であり、チャネルの設定ミスやその他の状況に起因するフォワーディングループを防止します。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. スイッチ間リンクでオートネゴシエーションを無効にしない（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ると、リンクにパルスが送られても、ローカル側がリンクをダウンさせます。UDLDなどの高レベルの検出メカニズムと比較すると、自動ネゴシエーションは（マイクロ秒以内で）非常に高速ですが、UDLDのエンドツーエンドのカバレッジは存在しません（データパス：CPU全体 - フォワーディングロジック - port1 - port2 - フォワーディングロジック - CPU対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タイマーを調整する際には注意が必要です

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。タイマーを任意に変更しても、STPが正しく動作しない。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\(STP\)タイマーの説明と調整](#)』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、ルートガードでネットワークSTP境界を保護します

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た未承認のネットワークデバイス (ハブ、スイッチ、ブリッジングルータなど) によるSTPの影響を防止します

ルートガードを正しく設定すると、外部からのSTPの影響を受けなくなります。BPDUガードが有効になっている場合は、BPDUを受信するポートがシャットダウンされます。BPDUガードは syslogメッセージを生成してポートをシャットダウンするため、これはインシデントの調査に役立ちます。ルートまたはBPDUガードが短いサイクルのループを防止しない場合は、2つの高速対応ポートが直接またはハブを介して接続されます。

9. 管理VLANでのユーザトラフィックの回避

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。過剰なブロードキャスト (ブロードキャストストームやアプリケーションの動作不良など) が発生すると、スイッチのCPUが過負荷になり、STPの動作が歪む可能性があります。

10. 予測可能な (ハードコードされた) STPルートとバックアップSTPルートの配置

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](#)

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。