スパニング ツリー プロトコルの問題点と設計上の考慮事項

目次

概要

このドキュメントでは、Catalyst OS（CatOS）と Cisco IOS(R) ソフトウェアが稼働する Cisco Catalyst スイッチのブリッジングに関して安全なネットワークを実装するのに有効な推奨策のリストを提供しています。 本書では、スパニング ツリー プロトコル（STP）が失敗する可能性が

あるいくつかの一般的な原因と、問題の原因を特定するために確認する必要のある情報について説明します。 本書では、スパニング ツリーに関する問題を最小限に抑え、トラブルシューティングが容易な種類の設計も示します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

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。

背景説明

この文書では、STP の基本的な動作については説明しません。 STP の動作の仕組みを学習するには、次のドキュメントを参照してください。

- Catalyst スイッチでのスパニング ツリー プロトコル (STP) についての説明と設定方法

このドキュメントでは、IEEE 802.1w で定義されている Rapid STP (RSTP) は取り上げていません。 さらに、IEEE 802.1s で定義されている Multiple Spanning Tree (MST) も取り上げていません。 RSTP と MST の詳細は、下記のドキュメントを参照してください。

- マルチ スパニング ツリー プロトコル (802.1s) について
- 高速スパニングツリー プロトコル (802.1w) について

Cisco IOS ソフトウェアが稼働する Catalyst スイッチのためのさらに具体的な STP トラブルシューティングのドキュメントは、『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』を参照してください。

スパニングツリー プロトコルの障害

スパニング ツリー アルゴリズム (STA) の基本的な機能は、ブリッジ ネットワークで冗長リンクによって発生するループを遮断することです。 STP は Open System Interconnection (OSI; オープン システム インターコネクション) モデルのレイヤ 2 で動作します。 STP では、ブリッジ間で交換されるブリッジ プロトコル データ ユニット (BPDU) という手段により、最終的にトラフィックの転送やブロッキングを行うポートが選出されます。 特定の状況でこのプロトコルに障害が発生する場合があり、ネットワークの設計次第では、結果的な状況のトラブルシューティングが非常に困難になる可能性があります。 この特定の範囲では、トラブルシューティングの最も重要な部分は、問題が発生する前に実行します。

通常、STA の障害によりブリッジング ループが発生することになります。 スパニング ツリーの問題に関して Cisco テクニカルサポートにお問い合せいただく大多数のお客様からは不具合 (バグ) が示唆されますが、これが原因であることはほとんどありません。 ソフトウェアが問題であったとしても、STP 環境でのブリッジング ループは、ブロックするべきであるにもかかわらずトラフィックを転送しているポートにより発生しています。

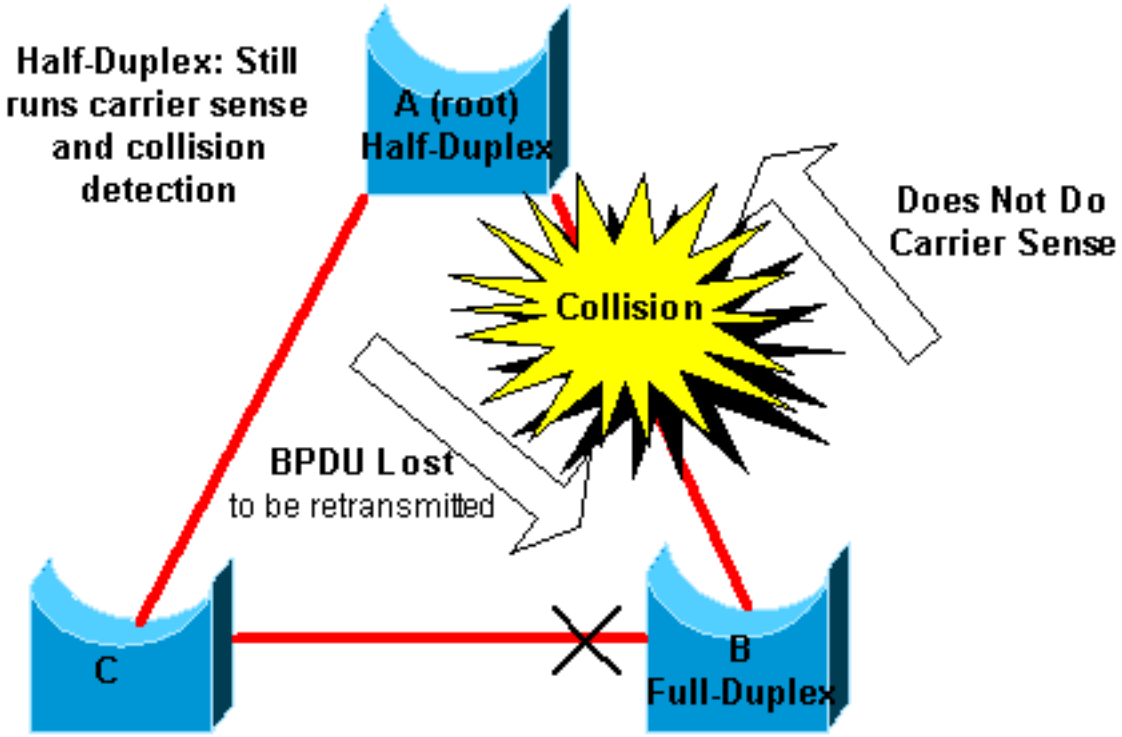
スパニング ツリー コンバージェンス

スパニングツリーが最初にどのように コンバージするか説明する例を参照するために[スパニング ツリー ビデオを](#)参照して下さい。 [この例では、BPDU が過剰に喪失されることによりブロッキングされたポートが転送モードに移行して、結果的に STA 障害が発生する理由についても説明されています。](#)

これ以降、STA の障害につながるさまざまな状況について説明します。 これらの障害のほとんどは BPDU の大量の喪失に関係するものです。 この喪失により、ブロッキングされているポートが転送モードに移行してしまいます。

デュプレックスのミスマッチ

ポイントツーポイント リンクにおける二重モードのミスマッチは、非常によく見られるコンフィギュレーション エラーです。 リンクの一端でデュプレックス モードをフル (全二重) に設定していて、他端を自動ネゴシエーション モードのままにしてあると、そのリンクは半二重になります。 (デュプレックス モードがフルに設定されたポートでは、以降のネゴシエーションは行われません。)



ポートで BPDU を送出するブリッジのデュプレックス モードが半二重に設定されている場合に、リンクの他端のピア ポートではデュプレックス モードが全二重になっているというのが、最悪のシナリオです。 上記の例では、ブリッジ A と B を結ぶリンク上での二重モードのミスマッチから、容易にブリッジ ループが発生します。 ブリッジ B は全二重に設定されているため、リンク アクセスの前にキャリア検知は行われません。 ブリッジ B は、ブリッジ A がリンクを使用中であっても、フレームの送出を開始します。 この状況は A のための問題です; ブリッジがフレームの別の伝達を試みる前に A を検出する、衝突を実行しますバックオフ アルゴリズムを繋いで下さい。 B から A へのトラフィックがある程度多いと、A から送出される各パケット (これには BPDU が含まれます) では遅延やコリジョンが発生して、結果的には廃棄されます。 STP の観点からは、A からの BPDU がこれ以上ブリッジ B で受信されないため、ブリッジ B はルート (root) ブリッジを喪失しています。 これにより、B ではブリッジ C に接続されたポートのブロックが解除され、ループが形成されます。

デュプレックスのミスマッチがある場合、CatOS および Cisco IOS ソフトウェアが稼働する Catalyst スイッチのスイッチ コンソールに下記のエラー メッセージが表示されます。

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

Cisco IOS ソフトウェア

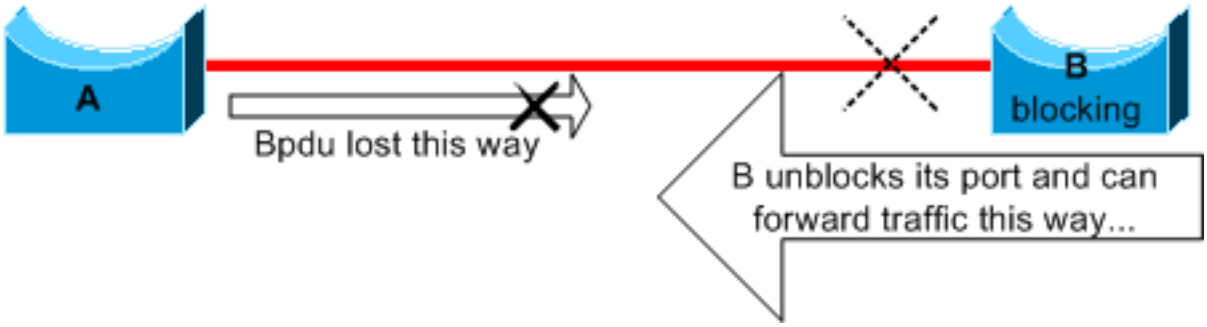
```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

デュプレックスの設定を調べて、一致していない場合は、設定を適切に行ってください。

デュプレックスのミスマッチをトラブルシューティングする方法についての詳細は、ドキュメント『イーサネット 10/100/1000 Mb 半二重/全二重オートネゴシエーションの設定とトラブルシューティング』を参照してください。

単方向リンク

単方向リンクはブリッジング ループの一般的な原因です。 光ファイバ リンクでは、検出されないまま潜在している障害により単方向リンクが引き起こされる場合がよくあります。 他の原因にはトランシーバの問題があります。 リンクをアップ状態のままにして、一方通行の通信をもたらすものは何であろうと、STP の観点では非常に危険です。 次の例で明確になります。



ここでは、A と B の間のリンクが単方向になっているものとします。 このリンクで B から A にトラフィックが転送されている間、A から B へのトラフィックは廃棄されます。このリンクが単方向になるまでは、ブリッジ B ではブロッキングが行われていたものとします。 ところが、ポートがブロッキングできるのは、より優先度の高いブリッジから BPDU を受信する場合です。 この場合、A から到着するすべての BPDU は廃棄されるため、ブリッジ B では、A に対する自身のポートを転送ステートに移行させて、トラフィックを転送する結果になります。 これによってループが形成されます。 スタートアップでこの障害があると、STP のコンバージは正しく行われません。 二重モード の ミスマッチの場合には、再度ブートするは一時的に助けます; しかしこの場合、ブリッジの再度ブートするは絶対に効果をもたらしません。

単方向リンクを転送ループの作成の前に検出するために、Cisco は単方向リンク検出（UDLD）プロトコルを設計し、設定しました。 この機能はレイヤ2 の不適当なケーブル接続か単方向リンクを検出する、いくつかのポートを無効にすることによって自動的に生じるループを切断できます。 ブリッジ環境では、可能な限り UDLD を実行します。

UDLD の使用についての詳細は、ドキュメント『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。

パケットの破損

同種の障害は、パケットの破損によっても発生する場合があります。 リンクで物理的エラーが頻繁に発生すると、連続した BPDU がある程度喪失されるか可能性があります。 この喪失により、ブロッキング ポートが転送モードに移行してしまう可能性があります。 STP のデフォルト パラメータはかなり余裕を持って設定されているため、これは頻繁に発生するものではありません。 ブロッキング ポートでは、50 秒間 BPDU の喪失が続かない限り、転送モードに移行することはありません。 BPDU の転送が 1 つでも成功すると、このループはクリアされます。 通常、この問題が発生するのは、STP のパラメータが不注意に調整された場合です。 この調整の例としては、max-age の削減があります。

パケットの破損の原因には、デュプレックスのミスマッチ、不良ケーブル、不正なケーブル長が考えられます。 CatOS と Cisco IOS ソフトウェアのエラー カウンタ出力についての説明は、ドキュメント『トラブルシューティング：スイッチ ポートおよびインターフェイスの問題』を参照してください。

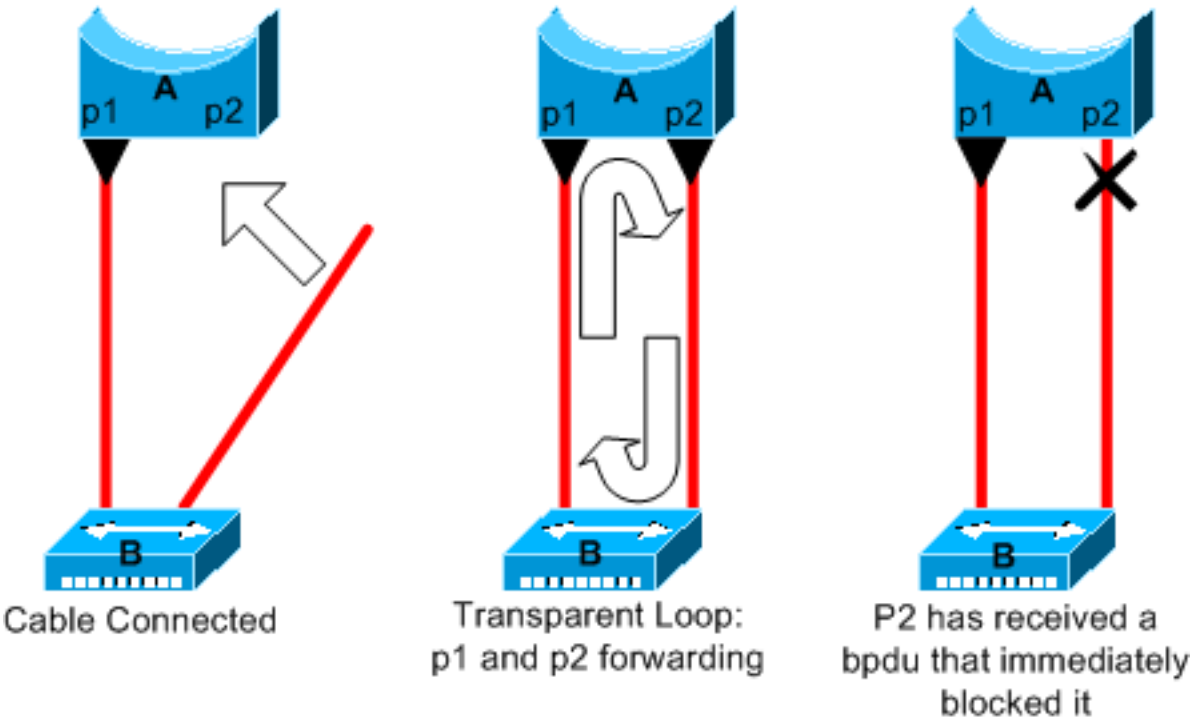
リソース エラー

専門的な Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）によりスイッチング機能のほとんどがハードウェアで実行されるハイエンドのスイッチでも、STP はソフトウェアで実装されています。 理由の如何にかかわらず、ブリッジでの CPU の過剰使用状態が発生している場合、リソースが BPDU の転送には不適切になっている可能性があります。 一般的に、STA（スパニング ツリー アルゴリズム）はプロセッサ バウンドの処理ではありませんが、他のプロセスよりも優先度が高くなっています。 このドキュメントの「リソース エラーの調査」セクションでは、特定のプラットフォームで処理できる STP のインスタンスの数についてのガイドラインを紹介しています。

PortFast の設定エラー

PortFast は、通常、ホストに接続するポートやインターフェイスだけをイネーブルにする機能です。 このポートでリンクがアップすると、ブリッジでは STA（スパニング ツリー アルゴリズム）の最初の数ステージがスキップされ、直接、転送モードに移行します。

注意： 他のスイッチやハブ、あるいはルータに接続されているスイッチのポートやインターフェイスで PortFast 機能を使用しないでください。 使用した場合は、ネットワーク ループが発生する可能性があります。



この例では、デバイス A はポート p1 で転送を行っているブリッジです。 ポート p2 には PortFast が設定されています。 デバイス B はハブです。 2 番目のケーブルを A に接続したとたんに、ポート p2 が転送モードになり、p1 と p2 間にループが形成されます。 p1 か p2 で、これら 2 つのポートのいずれかをブロッキング モードにする BPDU が受信されると、このループは停止します。 ところが、この種の過渡的なループには問題があります。 このループ上のトラフィックが密集していると、ブリッジではループを停止させる BPDU の転送がうまく行かない場合があります。 この問題により、極端な場合はコンバージェンスがかなり遅れて、ネットワークがダウンする可能性があります。

CatOS および Cisco IOS ソフトウェアが稼働するスイッチでの PortFast の正しい使用についての詳細は、ドキュメント『PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復』を参照してください。

PortFast が設定されていても、ポートやインターフェイスで STP が構成されていることには変わりはありません。 PortFast が設定されたポートやインターフェイスに、現在アクティブなルート ブリッジ（root bridge）の優先順位よりもブリッジの優先順位が低いスイッチが接続されている場合、そのスイッチがルート ブリッジに選出されることはありません。 ルート ブリッジがこのように変わると、アクティブな STP トポロジに悪影響が及ぶ場合があり、ネットワークの最適性が阻害される可能性があります。 この状況になるのを防ぐため、CatOS および Cisco IOS ソフトウェアが稼働するほとんどの Catalyst スイッチには BPDU ガードと呼ばれる機能が備わっています。 BPDU ガードでは、PortFast が設定されたポートやインターフェイスで BPDU が受信されると、そのポートやインターフェイスをディセーブルにします。

CatOS および Cisco IOS ソフトウェアが稼働するスイッチでの BPDU ガードの使用についての詳細は、ドキュメント『スパニングツリー PortFast BPDU ガード機能拡張』を参照してください。

不適切な STP パラメータ調整と直径（diameter）の問題

max-age パラメータの値がアグレッシブで転送遅延があると、STP トポロジがきわめて不安定になる場合があります。 このような場合、一部の BPDU の喪失によりループが発生する可能性があります。 あまり知られていない別の問題に、ブリッジ ネットワークの直径（diameter）に関連するものがあります。 STP タイマーの控えめなデフォルト値では、ネットワークの最大の直径が

7 に想定されています。 この最大のネットワークの直径により、ネットワーク内でブリッジが互いに取り得る距離が制限されています。 この場合、各ブリッジが取り得る相互の隔たりは、最大で 7 ホップになります。 この制限の部分は、BPDU で搬送される age フィールドによるものです。

BPDU がルート ブリッジからツリーの末葉部分に伝播される場合、その BPDU がブリッジを通過するたびに age フィールドが加算されます。 最終的に、age フィールドが最大 age を超過すると、そのブリッジで BPDU が廃棄されます。 ルートから遠すぎるブリッジがネットワークにあると、この問題が発生する可能性があります。 この問題により、スパニング ツリーのコンバージェンスが影響を受けます。

STP タイマーのデフォルト値からの変更を計画している場合は、格別な注意を払ってください。この方法でコンバージェンスを速めようとすると危険があります。 STP タイマーを変更すると、ネットワークの直径と STP の安定性に影響があります。 ブリッジの優先順位を変更してルート ブリッジを選択でき、ポート コストと優先順位パラメータを変更して冗長性とロード バランシングを制御できます。

Cisco Catalyst ソフトウェアでは、最も重要な STP パラメータを微調整する次のマクロが提供されています。

- setspantreeroot[secondary] マクロ コマンドでは、ブリッジの優先順位を下げることにより、ルート（または代替ルート）になります。 このコマンドには追加オプションを使用でき、ネットワークの直径を指定することにより、STP タイマーの調整が行われます。 正しく実行されたとしても、タイマーの調整によってコンバージェンスの時間が顕著に改善されるわけではなく、ネットワークが不安定になるリスクがあります。 さらに、この種の調整では、ネットワークにデバイスが追加されるたびにアップデートが必要です。 ネットワーク エンジニアによく知られている、控えめなデフォルト値を維持してください。
- CatOS の set spantree uplinkfast コマンド、あるいは、Cisco IOS ソフトウェアの spanning-tree uplinkfast コマンドでは、スイッチの優先順位を増加することにより、そのスイッチがルートにはなれないようにします。 コマンドはアップリンク障害の場合に STP コンバージェンス時間を増加します。 いくつかのコア スイッチへの二重接続とディストリビューション スイッチのこのコマンドを使用して下さい。 ドキュメント『UplinkFast 機能の説明と設定』を参照してください。
- 間接的なリンク障害が発生した場合は、CatOS の set spantree backbonefast enable コマンド、あるいは、Cisco IOS ソフトウェアの spanning-tree backbonefast コマンドでスイッチの STP コンバージェンス時間を増加できます。 BackboneFast は Cisco 固有の機能です。 ドキュメント『Catalyst スイッチ上の Backbone Fast の概要と設定』を参照してください。

STP タイマーについての詳細、および、どうしても必要な場合に STP タイマーを調整するルールについての詳細は、ドキュメント『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。

ソフトウェア エラー

「概要」で説明しているように、STP は Cisco 製品で実装された最初の機能の 1 つです。 この機能には非常に高い安定性を期待できます。 現在、すでに判明している何らかのきわめて限定的な場合に STP に障害を発生させるのは、EtherChannel のような、STP よりも新しい機能との相互作用だけです。 多数のさまざまな要素によりソフトウェアの不具合が引き起こされる可能性があり、多数のさまざまな影響が及ぶ可能性があります。 不具合により引き起こされる可能性のある問題を適切に説明する方法はありません。 一般的にソフトウェアのエラーにより引き起こされる最も危険な状況は、一部の BPDU を無視すると、ブロッキング ポートが転送モードに移行す

ることです。

障害のトラブルシューティング

残念ながら、STP の問題をトラブルシューティングするシステマティックな手順はありません。しかしながら、このセクションでは使用できる対策をいくつかまとめてあります。 このセクションの手順のほとんどは、一般的なブリッジング ループのトラブルシューティングに適用されるものです。 接続の喪失につながる STP の他の障害を判別する従来からのアプローチを利用することもできます。 たとえば、問題が発生したトラフィックがたどるパスを探索できます。

注: これらのトラブルシューティング手順のほとんどは、ブリッジ ネットワークの各種デバイスに接続できることを前提としています。 この接続性とは、コンソール アクセスがあることを意味しています。 たとえば、ブリッジング ループが発生している間は、おそらく Telnet 接続はできません。

Ciscoデバイスからの **show-tech support コマンド**の出力がある場合、潜在的な問題および 修正を表示するのに Cisco CLI アナライザ（登録ユーザのみ）を使用できます。

ネットワーク ダイアグラムの使用

ブリッジング ループのトラブルシューティングを開始する前に、少なくとも、下記の項目について知っている必要があります。

- ブリッジング ネットワークのトポロジ
- ルート ブリッジの口ケーション
- ブロッキングされたポートと冗長リンクの口ケーション

この知識が必要なのは、少なくとも、次の 2 つの理由によります。

- ネットワークで何を修復するのかを知るためには、ネットワークが正常に動作している場合にはどのように見えるのかを知っている必要があります。
- トラブルシューティング手順のほとんどは、単に **show** コマンドを使用して、エラー状況の判別を試みることになります。 ネットワークの知識は、キーとなるデバイスの重要なポートに焦点を当てる上で有効です。

ブリッジ ループの識別

かつては、ブロードキャスト ストームがネットワークに深刻な影響を与える可能性がありました。 今日では、ハードウェア レベルでの転送を提供する高速リンクやデバイスの登場により、サーバ等の単一デバイスから送信されるブロードキャストがネットワークに対して深刻な影響を与えることは少なくなりました。 ブリッジング ループを判別する最適な方法は、飽和状態のリンクでトラフィックをキャプチャして、類似したパケットが複数回検出されることをチェックすることです。 これに対して実用上は、接続性の問題が特定ブリッジ ドメイン内のすべてのユーザに同時に発生していると、ブリッジング ループが発生していると考えられます。

デバイス上のポートの使用状況をチェックし、異常な値がないかを確認します。 このドキュメントの「ポートの使用状況のチェック」セクションを参照してください。

CatOS が稼働する Catalyst スイッチでは、**showsystem** コマンドで全体的なバックプレーンの使用状況を容易にチェックできます。 このコマンドでは、スイッチ バックプレーンの現在の使用状況が提供され、ピークの使用状況とピーク使用状況の日付も指定されます。 尋常ではないピーク

使用状況がある場合、このデバイスでブリッジング ループが発生していた可能性があることが示されています。

接続の迅速な復旧と今後のための準備

ループをクリアするためにポートをディセーブルにする

ブリッジ ネットワークでは、ブリッジング ループはきわめて厳しい状況です。 通常、管理者にはループの原因を探っている時間はなく、できるだけ速く接続を復旧することが望まれます。 この状況から抜ける簡単な方法は、ネットワークで冗長性を提供している各ポートを手動でディセーブルにすることです。 ネットワークで最も影響を受けている箇所を判別できる場合、そのエリアのポートのディセーブル化を開始します。 あるいは、可能ならば、ブロッキングしているポートを最初からディセーブルにします。 ポートを無効にするたびに、ネットワークの接続を復元するかどうか確認して下さい。 無効ポートがループを停止する識別によって、またこのポートが見つけられる冗長パスを特定します。 そのポートが本来ブロッキング モードであるべきポートだった場合は、おそらくそこが障害の発生したリンクです。

ブロッキングされているポートをホスティングするデバイスでの STP イベントのログ

問題の発生源を正確には判別できない場合、あるいは、問題を定常的に把握できない場合、障害が発生しているネットワークのブリッジやスイッチで STP イベントの口ギングをイネーブルにします。 設定するためにデバイスの数を制限したいと思う場合少なくともこれをブロック化ポートをホストする口グオン デバイス 有効に して下さい; ブロック化ポートの遷移はループを作成するものがです。

- Cisco IOS ソフトウェア上の問題 STP デバッグ情報を有効に する EXEC コマンド **debug spanning-tree events**。 デバイス バッファ内のこのデバッグ情報をキャプチャするには、一般的なコンフィギュレーション モード コマンド loggingbuffered を発行します。
- CatOS- は **set logging level spantree 7 default コマンド** デバッグ レベルに STP に関連しているイベントのデフォルトレベルを上げます。 setloggingbuffer500 コマンドを使用して、確実にスイッチ バッファ内の最大数のメッセージが口ギングされるようにします。

デバッグ出力の syslog デバイスへの転送を試みることもできます。 残念ながら、ブリッジング ループが発生すると、syslog サーバへの接続が維持されることはほとんどありません。

ポートのチェック

最初に検査する重要なポートはブロッキング ポートです。 このセクションでは、他のポートでの検索対象のリストが紹介されており、CatOS および Cisco IOS ソフトウェアが稼働するスイッチで発行するコマンドが簡単に説明されています。

ブロックされたポートが BPDU を受信しているかどうかのチェック

特にブロッキングされているポートとルート (root) ポートで、時おり BPDU が受信されることを確認します。 ポートでのパケットや BPDU の受信障害を引き起こす可能性のある問題は複数あります。

- Cisco IOS ソフトウェア リリース 12.0 またはそれ以降ソフトウェアの Cisco IOS に、**show spanning-tree** *ブリッジグループ#*コマンドの出力 BPDU あります。 このフィールドには、各インターフェイスで受信された BPDU の数が示されています。 このコマンドをさらに 1 ~ 2

回発行して、デバイスで BPDU が受信されているか判別します。showspanning-tree コマンドの出力に BPDU フィールドがない場合は、debug spanning-tree コマンドで STP デバッグをイネーブルにして、BPDU の受信を確認できます。
- 特定のポートが受信すること CatOS **show mac** *モジュール/port コマンドは*マルチキャストパケットの数を告げます。 *しかし、使用できる最も簡単なコマンドは* showspantreestatisticsmodule#/port# vlan# コマンドです。 このコマンドでは、特定の VLAN 上の特定のポートで受信されたコンフィギュレーション BPDU の実際の数が表示されます。トランキングが設定されていると、1 つのポートが複数の VLAN に属している可能性があります。 このドキュメントの「もう 1 つの CatOS コマンド」セクションを参照してください。

デュプレックスのミスマッチを確認する

デュプレックスのミスマッチを探すには、ポイントツーポイント リンクの両端をチェックする必要があります。

- Cisco IOS ソフトウェア上の問題特定のポートの速度 および デュプレックス ステータスをチェックする **show interfaces** [*インターフェイス interface-number*] **status コマンド**。
- **show port** *module#/port#* コマンドの出力 CatOS 一番最初の行はポートコンフィギュレーションに従って速度 および デュプレックスを与えます。

ポートの使用状況のチェック

トラフィックの負荷が過剰なインターフェイスでは、有効な BPDU の転送が失敗する場合があります。 リンクの負荷が過剰な場合にも、ブリッジング ループが形成される可能性があります。

- Cisco IOS ソフトウェア使用 インターフェイスの利用を判別するコマンド **show interfaces**。load や packets input/output のような複数のフィールドが、この判別には有効です。 **show interfaces** コマンド出力の説明は、ドキュメント『トラブルシューティング：スイッチ ポートおよびインターフェイスの問題』を参照してください。
- CatOS **show mac** *module#/port#* コマンドはポートが受信し、送信するパケットについての統計情報を表示するものです。 showtop コマンドでは、30 秒間に渡るポートの使用状況の評価が自動的に行われ、結果が表示されます。 このコマンドでは、パーセンテージによる帯域幅の使用状況で結果が分類されますが、結果の分類には別のオプションも利用可能です。 さらに、showsystem コマンドでもバックプレーン使用状況が表示されますが、このコマンドでは特定のポートに対する指定は行われません。

パケットの破損のチェック

- エラーのための Cisco IOS ソフトウェア外観は **show interfaces コマンド**の カウンターで増分します。 このエラー カウンタには、runts、giants、no buffer、CRC、frame、overrun および ignored counts があります。**show interfaces** コマンド出力の説明は、ドキュメント『トラブルシューティング：スイッチ ポートおよびインターフェイスの問題』を参照してください。
- CatOS コマンド **show port** *module#/port# は*`FCS-ErrXmit-ErrRcv-Err` およびフィールドが付いているいくつかの詳細を説明します。 showcountersmodule#/port# コマンドでは、統計情報がさらに詳細に提供されます。

もう 1 つの CatOS コマンド

showspantreestatisticsmodule#/port# vlan# コマンドでは、特定のポートに関するきわめて正確な情報が提供されます。 このコマンドを対象のポートで発行して、特に次のフィールドに注意を払ってください。

- TRANS カウンターは学習からの転送かにポートの移行何時間覚えています。 安定したトポロジでは、このカウンタは常に 1 を示しています。 ポートがダウンしてアップすると、このカウンタは 0 にリセットされます。 そのため、1 よりも大きい値は、このポートで発生した移行が STP 再計算の結果であることを示しています。 移行は直接のリンク障害の結果ではありません。
- カウンターその回数をこのリンクで切れる最大 存続期間トラッキングします。 基本的には、BPDU を待機するポートでは、max age まで待ち受けてから、代表ブリッジが失われたものと見なされます。 max age のデフォルトは 20 秒です。 このイベントが発生するたびに、このカウンタが加算されます。 この値が 0 ではない場合、この LAN の代表ブリッジが不安定であるか、BPDU の転送に問題を抱えていることが示されています。

リソース エラーの調査

CPU の高い使用率は、STA (スパニング ツリー アルゴリズム) が稼働するシステムでは危険である場合があります。 デバイスでの CPU リソースが適切であることをチェックするには、次の方法を使用します。

- Cisco IOS ソフトウェア上の問題 **show processes cpu コマンド**。 CPU 使用率が高すぎないことをチェックします。 CatOS や Cisco IOS ソフトウェアが稼働する Catalyst 4500/4000 シリーズ スイッチでは、ドキュメント『Catalyst 4000、2948G、2980G、および 4912G スイッチでの CPU 使用率の理解』を参照してください。
- CatOS 問題 CPU稼働率 情報を表示する **show proc cpu コマンド**。 CPU 使用率が高すぎないことをチェックします。

スーパーバイザ エンジンが処理できる STP のさまざまなインスタンス数には制限があります。 さまざまな VLAN で STP のすべてのインスタンスにまたがる論理ポートの総数が、各スーパーバイザ エンジンのタイプとメモリ構成でサポートされている最大数を超過していないことを確認してください。

CatOS が稼働するスイッチでは show spantree summary コマンド、または、Cisco IOS ソフトウェアが稼働するスイッチでは show spanning-tree summary totals コマンドを発行します。 これらのコマンドにより、VLAN ごとの論理ポートやインターフェイスの数が STP Active カラムに表示されます。 カラムの一番下に合計数が表示されます。 合計は異なる VLAN のための STP のすべての例を渡るすべての口ジカルポートの合計を表します。 この数が各スーパバイザ エンジンタイプのためにサポートされる最大数を超過しないことを確かめて下さい。

注: スイッチでの論理ポートの総数を計算する式を次に示します。

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Catalyst スイッチに適用される STP に関する制限の要約は、下記のドキュメントを参照してください。

プラットフォーム	CatOS での STP の制限	Cisco IOS ソフトウェアでの STP

		限
Catalyst 6500/6000 Supervisor Engine I および II	STP のトラブルシューティング	
Catalyst 6500/6000 Supervisor Engine 720	STP のトラブルシューティング	スパニング ツリーのトラブルシューティング
Catalyst 4500/4000	Spanning Tree	スパニング ツリーのトラブルシューティング
Catalyst 3750		STP の設定

不要な機能のディセーブル化

トラブルシューティングは、現在のネットワーク内で問題になっている箇所を特定することです。 できるだけ多くの機能をディセーブルにします。 ディセーブルにすることは、ネットワークのストラクチャを簡易化に有効で、問題の判別を容易にします。 たとえば、EtherChanneling は STP が論理的に単一 の リンクに複数の異なるリンクを組み込むように要求する機能です; トラブルシューティングの間のこの機能の無力は理にかなっています。 一般的なルールとして、コンフィギュレーションをできるだけ単純にすることにより、問題のトラブルシューティングが容易になります。

役に立つコマンド

Cisco IOS ソフトウェア コマンド

- show interfaces
- show spanning-tree
- show bridge
- show processes cpu
- debug spanning-tree
- logging buffered

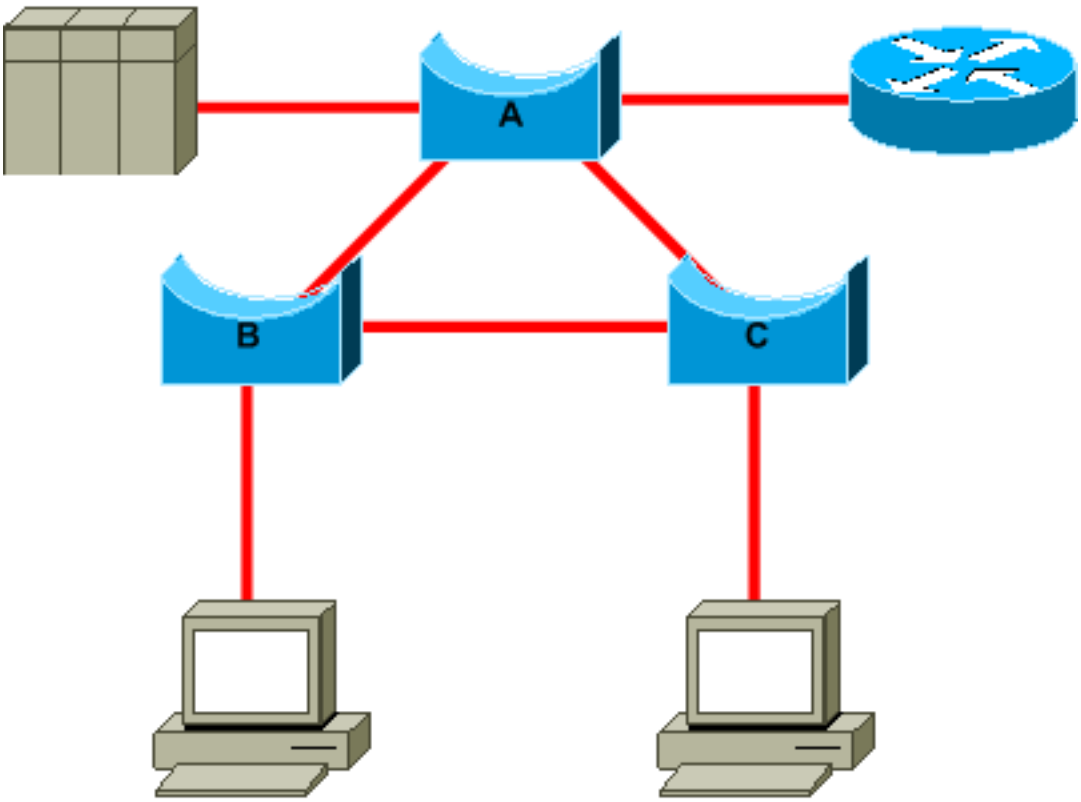
CatOS コマンド

- show port
- show mac
- show spantree
- show spantree statistics
- show spantree blockedports
- show spantree summary
- show top
- show proc cpu
- show system
- show counters
- set spantree root[secondary]
- set spantree uplinkfast
- set logging level
- set logging buffered

トラブルを回避するための STP の設計

ルート（root）の位置の確認

ルートが意図的に選定されていないことに起因し、トラブルシューティングの際、どのブリッジがルートなのかという情報が得られないことがしばしばあります。 ルートになるブリッジが STP によって決定されることは避ける必要があります。 ネットワーク設計を考慮し、それぞれの VLAN でどのブリッジをルートとすることがベストなのかを判断し、決定してください。 これはネットワークの設計によって決まります。 通常は、ネットワークの中心に位置する強力なブリッジを選択します。 ルート ブリッジをネットワークの中央にサーバとルータに直接接続して設置すると、一般的には、クライアントからサーバとルータへの平均距離が削減されます。



上記のダイアグラムには、次のことが示されています。

- ブリッジ B がルートである場合、A から C へのリンクはブリッジ A かブリッジ C でブロッキングされます。この場合、スイッチ B に接続するホストでは、サーバとルータに 2 ホップでアクセスできます。 ブリッジ C に接続するホストでは、サーバとルータに 3 ホップでアクセスできます。 この平均距離は 2.5 ホップになります。
- ブリッジ A がルートである場合、ルータおよびサーバは B および C で接続する両方のホストのための 2 つのホップで到達可能です。 このとき平均的な距離は 2 つのホップです。

この単純な例での論理を、より複雑なトポロジに転用します。

特記事項： 各 VLAN で、STP 優先順位パラメータの値を削減して、ルート ブリッジとバックアップ ルート ブリッジをハード コーディングします。 あるいは、setspantreeroot マクロを使用することもできます。

冗長箇所の特定

対象の冗長リンクの組織構成を計画します。 STP のプラグアンドプレイ機能のことは忘れてください。 ブロッキング対象ポートを判断するために、STP コスト パラメータを調整します。 設計が階層構造になっていて、ルート ブリッジが適切なロケーションにある場合、通常、この調整は不要です。

特記事項： 各 VLAN について、安定したネットワーク内のどのポートでブロッキングが行われるべきかを把握しておいてください。 ネットワーク内の各物理的ループ、および、それらのループを遮断するブロッキングされたポートを明確に示すネットワーク ダイアグラムを準備するようにしてください。

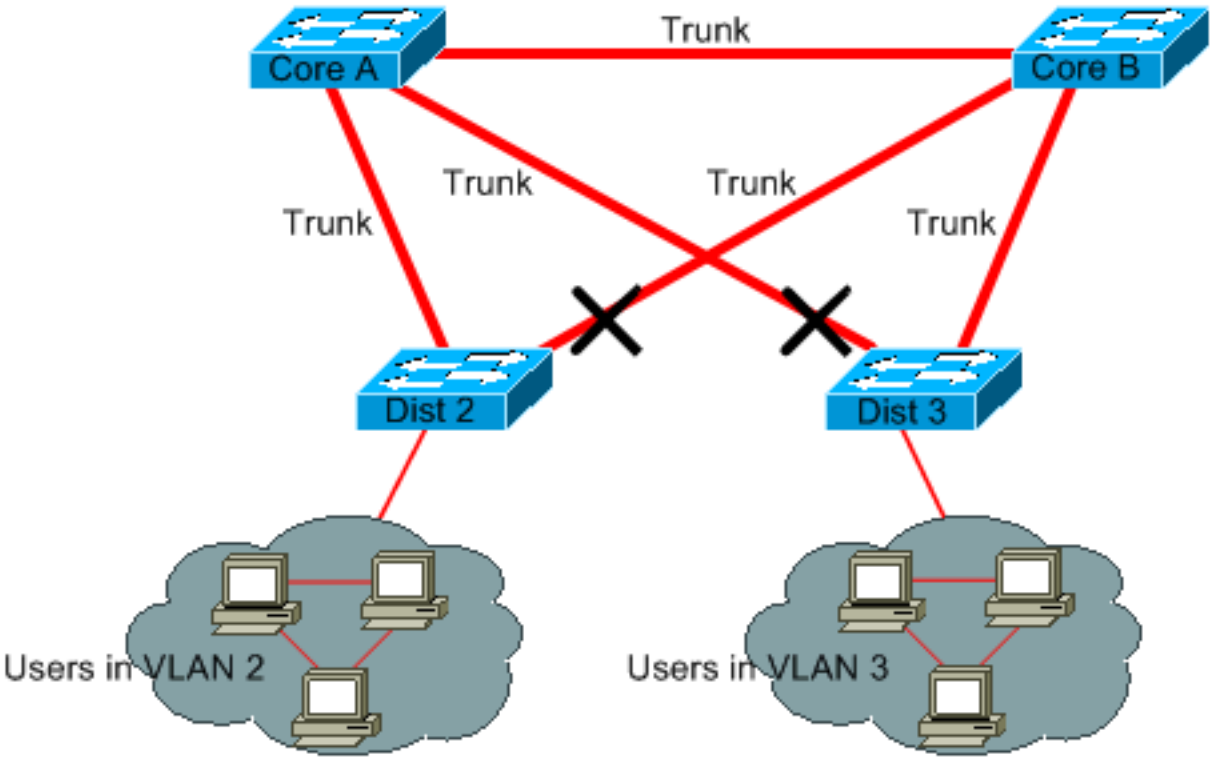
冗長リンクのロケーションがわかっていると、突発的に発生するブリッジング ループとその原因の判別に有効です。 さらに、ブロッキングされたポートのロケーションがわかっていると、エラーが発生したロケーションが判別できます。

ブロックキングされるポートの数の最小化

STP で行われる唯一の重要な動作は、ポートのブロッキングです。 ブロッキングが行われている単一のポートが誤って転送モードに移行すると、ネットワークの大きな部分がメルトダウンする可能性があります。 STP の使用に固有のリスクを制限するのに適切な方法は、ブロッキングされたポートの数をできるだけ削減することです。

使用していない VLAN のプルーニング

ブリッジ ネットワークでの 2 つのノード間に必要な冗長リンクは 2 つまでです。 ところが、次のような設定が一般的です。

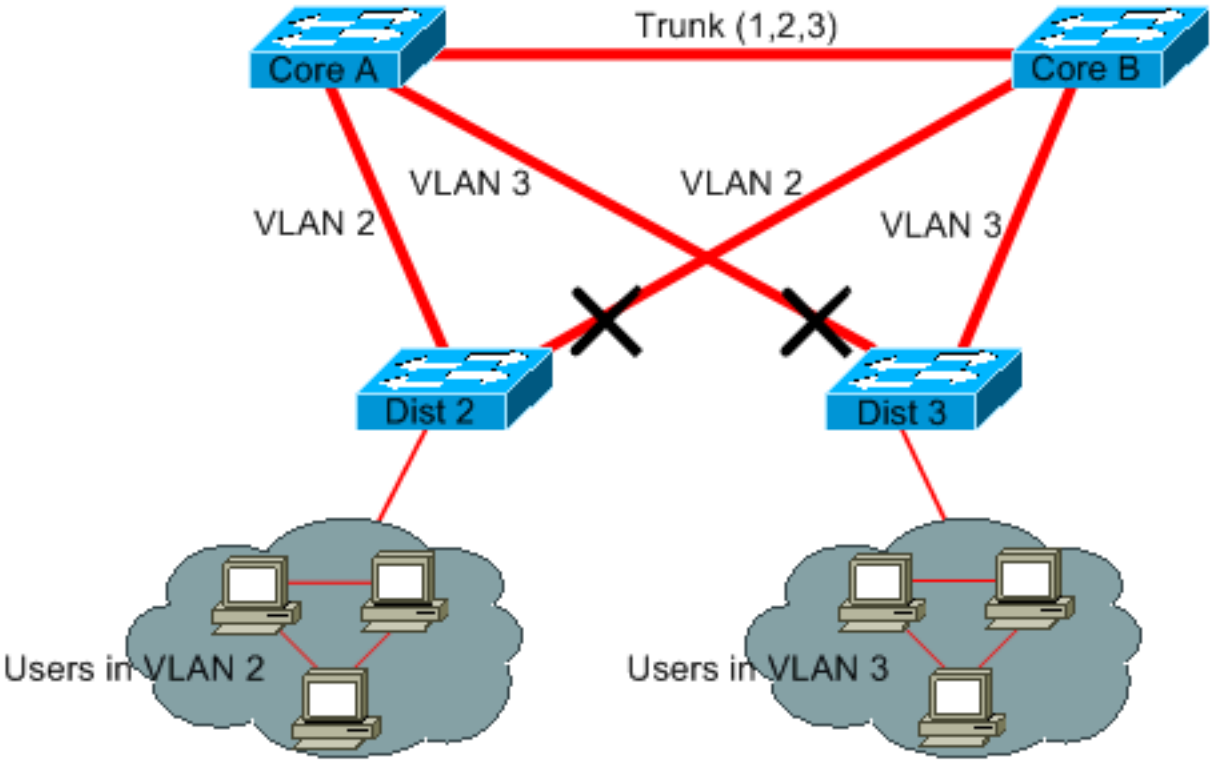


2 つのコア スイッチに、ディストリビューション スイッチが二重接続されています。 ディストリビューション スイッチに接続されたユーザは、ネットワークで利用可能な複数の VLAN のサブセットに所属するだけです。 この例では、Dist 2 で接続するユーザは VLAN 2 にすべてです; Dist 3 は VLAN 3.のユーザしか、トランク運びます VLANトランク プロトコル (VTP) ドメインで定義されるすべての VLAN をデフォルトで接続しません。 VLAN 3 の不要なブロードキャスト トラフィックとマルチキャスト トラフィックを受信するのは Dist 2 だけですが、そこでも、VLAN 3 のポートの 1 つに対してブロッキングが行われています。 結果はその間 3 つの冗長パス芯を取り、A の芯を取ります B.をです。 この冗長性はループのより多くのブロック化ポートおよびより高い確率という結果に終ります。

特記事項： 不要な VLAN を現在のトランクからプルーニングします。

VTP のプルーニングは有効な手段ですが、この種のプラグアンドプレイ機能はネットワークのコアでは不要です。

次の例では、ディストリビューション スイッチをコアに接続するために使用されているのはアクセス VLAN だけです。



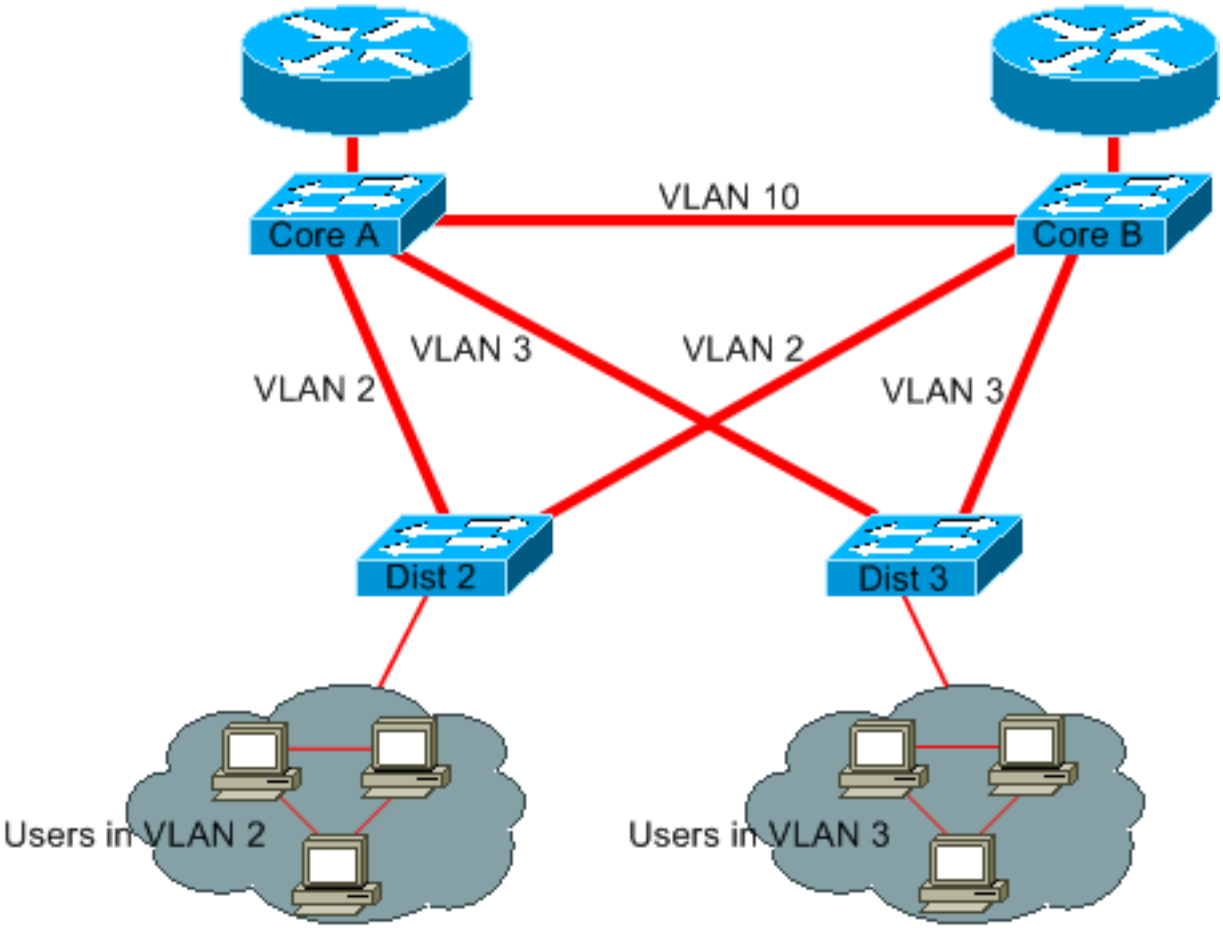
この設計では、ブロックされるポートは VLAN ごとに 1 つのみです。 さらに、この設計では、CoreA か CoreB をシャットダウンするだけで、すべての冗長リンクをワンステップで削除できます。

レイヤ 3 スイッチングの使用

レイヤ 3 スイッチングでは、スイッチングの速度近辺でルーティングが行われます。 ルータは主に次の 2 つの機能を担います。

- ルータでは転送テーブルが構築されます。 ルータは、一般的にルーティング プロトコルを手段としてピアとの情報交換を行います。
- ルータでは、パケットを受信して、宛先アドレスに基づいた適切なインターフェイスにパケットを転送します。

ハイエンドの Cisco レイヤ 3 スイッチは、この 2 番目の機能をレイヤ 2 スイッチング機能と同じスピードで実行できるようになりました。 ルーティング ホップを導入して、ネットワークの追加セグメンテーションを作成しても、速度への悪影響はありません。 次のダイアグラムでは、「使用していない VLAN のプルーニング」セクションの例に基づくものです。



ここでは、Core A と Core B がレイヤ 3 スイッチです。 VLAN 2 と VLAN 3 は Core A と Core B 間でブリッジングされておらず、STP ループが発生する可能性はありません。

- レイヤ 3 ルーティング プロトコルへの依存により、冗長性は維持されています。 この設計により、STP による再コンバージェンスよりも高速の再コンバージェンスが保証されます。
- ここでは、STP でブロッキングされた単一ポートはありません。 そのため、ブリッジング ループが発生する可能性はありません。
- レイヤ 3 スイッチングによって VLAN を通過するスピードは、VLAN 内部のブリッジ処理と同等のため、スピード ペナルティはありません。

この設計には、障壁が 1 つだけあります。 この種の設計に移行するには、通常、アドレッシング スキームのリワークが必要になります。

不要な場合の STP の維持

ブロッキングされたポートをすべてネットワークから排除できて、物理的な冗長性がなくなったとしても、STP をディセーブルにはしないでください。 STP は一般にあまりプロセッサ集約型ではないです; パケット交換はほとんどの Ciscoスイッチで CPU を含みません。 さらに、各リンクで送信される BPDU で、利用可能な帯域幅を著しく低下させてしまうものはほとんどありません。 しかしながら、STP が設定されていないブリッジ ネットワークでは、たとえば操作員がパッチパネルでエラーを犯した場合、瞬時にメルトダウンしてしまう可能性があります。 一般的に、ブリッジ ネットワークで STP をディセーブルにすることは、そのリスクに値しません。

管理 VLAN からのトラフィックの分離とネットワーク全体をスパニングする単一の VLAN の不設置

Cisco のスイッチには、通常、VLAN にバインドする単一の IP アドレスが備わっており、これは

管理 VLAN として周知のものです。 この VLAN では、スイッチは通常の IP ホストとして機能します。 具体的には、すべてのブロードキャストやマルチキャストのパケットが CPU に転送されます。 管理 VLAN でブロードキャストやマルチキャストのトラフィックのレートが高いと、CPU およびバイタルな BPDU を処理する CPU の能力に悪影響が及ぶ可能性があります。 そのため、管理 VLAN ではユーザ トラフィックを流さないようにしてください。

最近まで、Cisco の実装では、VLAN 1 をトランクから外す方法はありませんでした。 VLAN 1 は、通常、管理 VLAN として機能し、同じ IP サブセットですべてのスイッチにアクセス可能です。 この設定は便利な反面、VLAN 1 でのブリッジング ループがすべてのトランクに影響するために危険性があり、ネットワーク全体のダウンに至る可能性があります。 当然ながら、使用している VLAN にかかわらず、同じ問題が存在します。 高速のレイヤ 3 スイッチを使用して、ブリッジング ドメインのセグメント化を試みてください。

CatOS バージョン 5.4 と Cisco IOS ソフトウェア リリース 12.1(11b)E では、VLAN 1 をトランクから外すことができます。 それでも VLAN 1 は存在しますが、トラフィックのブロッキングが行われ、ループが発生する可能性が防止されます。

関連情報

- ツール & リソース : テクニカルサポート & ドキュメント
- テクニカル サポートとドキュメント – Cisco Systems