STP問題のトラブルシューティング&；設計上の考慮事項

内容

関連情報

はじめに

このドキュメントでは、Cisco IOS®ソフトウェアを実行するCisco Catalystスイッチのブリッジングについて、安全なネットワークを実装するための推奨事項について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

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

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

背景説明

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。また、スパニングツリーに関連する問題を最小限に抑え、トラブルシューティングを容易にする設計の種類も示します。

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 STP の理解と設定

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、『CatalystスイッチでのSTPに関する問題のトラブルシューティング』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。このプロトコルは特定の状況で失敗する可能性があり、ネットワークの設計によっては、結果が非常に困難になる可能性のある状況をトラブルシューティングする場合があります。この特定の領域では、問題が発生する前に、トラブルシューティングプロセスの最も重要な部分を実行します。

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。ソフトウェアに問題がある場合でも、STP環境のブリッジングループは、トラフィックをブロックして転送する可能性のあるポートから発生します。

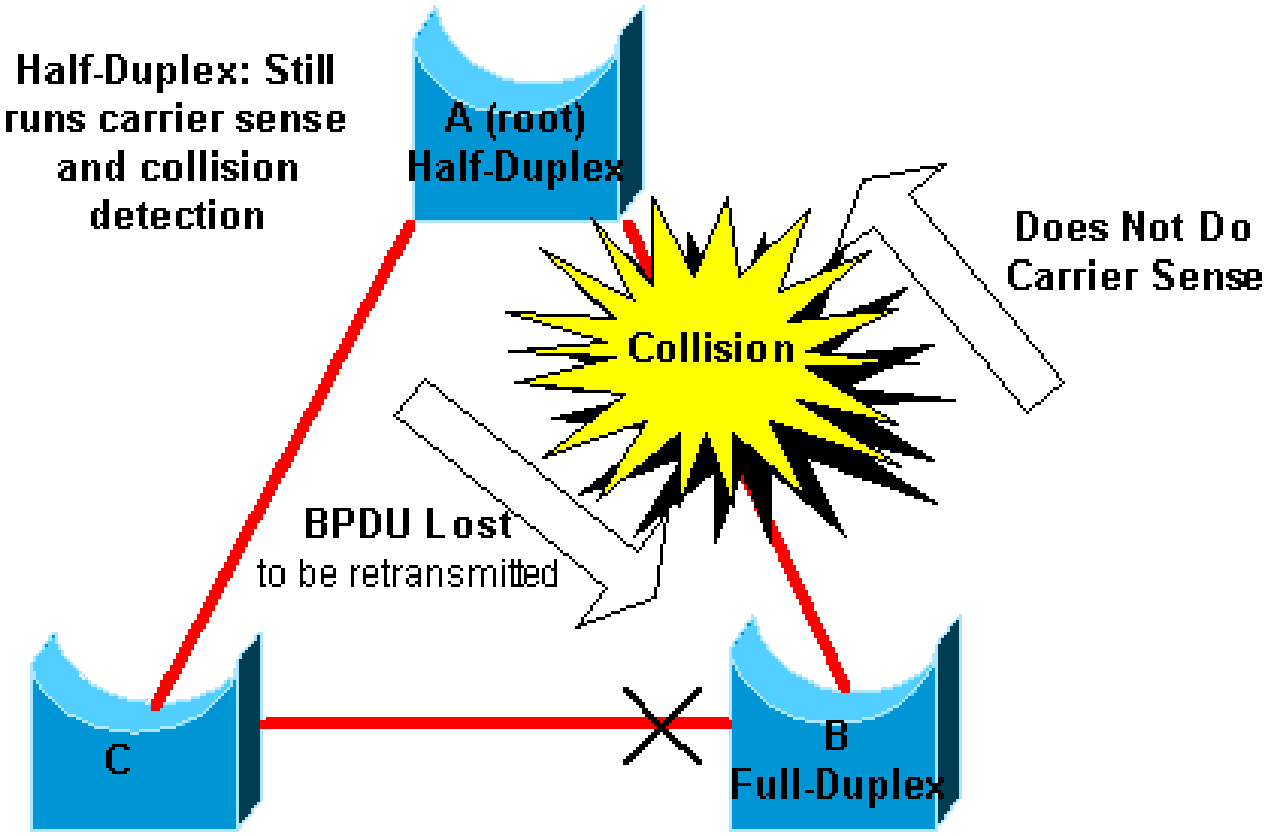
スパニング ツリー コンバージェンス

スパニング ツリーが最初にコンバージする仕組みを説明している例を見るには、スパニング ツリーに関するビデオ を参照してください。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。

デュプレックスの不一致

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。リンクの一方の側でデュプレックスモードを全二重に手動で設定し、もう一方の側をオートネゴシエーションモードのままにすると、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。前の例では、ブリッジAとBの間のリンクでデュプレックスのミスマッチが発生すると、簡単にブリッジングループが発生することがあります。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がすでにリンクを使用している場合でも、フレームの送信を開始します。この状況は A にとっては問題です。つまり、ブリッジ A では、ブリッジで次のフレームの転送が試行される前に、コリジョンが検出されてバックオフ アルゴリズムが実行されます。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には、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、次のエラーメッセージが表示されることがあります。

Cisco IOS ソフトウェア

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half duplex), with TBA050714
```

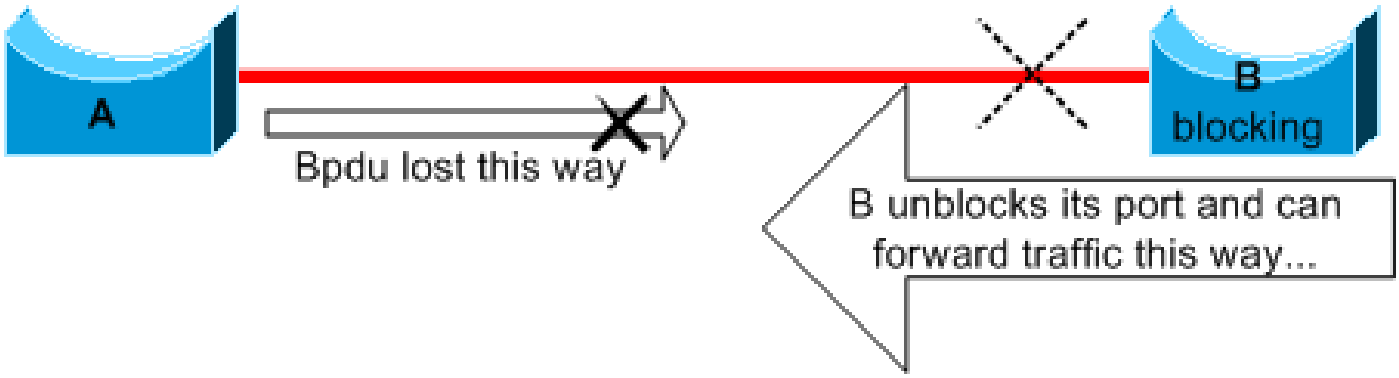
デュプレックスの設定を調べて、一致していない場合は、設定を適切に行ってください。

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確認』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。デュプレックスのミスマッチの場合、一時的にはリブートが有効ですが、この場合は、ブリッジのリブートはまったく効果がありません。

転送ループが発生する前に単方向リンクを検出するために、シスコは 単方向リンク検出（UDLD）プロトコルを設計および実装しています。 この機能は、一部のポートを無効にすることで、レイヤ 2 上の不適切なケーブル配線や単方向リンクを検出し、結果として生じるループを自動的に切断することができます。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『UDLDプロトコル機能の設定』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。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。

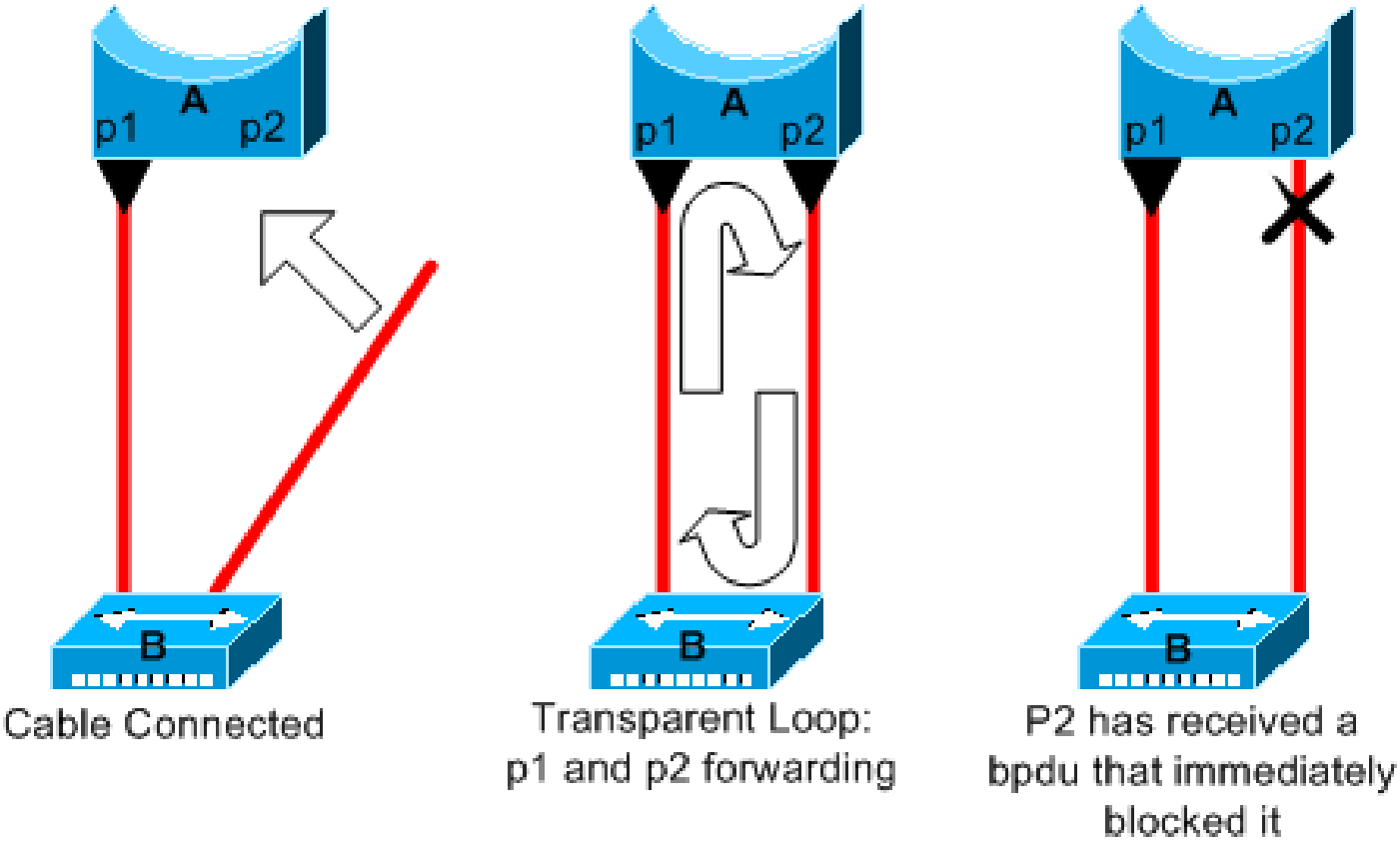
リソース エラー

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。何らかの理由でブリッジのCPUが過剰に使用されている場合は、BPDUの送信にリソースが不十分にな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、ハブ、またはルータに接続するスイッチポートまたはインターフェイスでは、PortFast機能を使用しないでください。それ以外の場合は、ネットワークループを作成できます。



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。

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。この状況を回避するために、Cisco IOSソフトウェアを実行するほとんどのCatalystスイッチには、BPDU Guardという名前の機能があります。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。

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ガード機能拡張について』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。この方法で再コンバージェンスを高速化しようとすると危険です。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。

- spanning-tree vlan number root { primary | secondary }コマンドは、ブリッジプライオリティを下げてルート（または代替ルート）にします。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。

- Cisco IOSソフトウェアのspanning-tree uplinkfastコマンドでは、スイッチのプライオリティ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。このコマンドにより、アップリンク障害が発生した場合の STP コンバージェンス時間が増加します。このコマンドは、一部のコア スイッチへのデュアル接続を備えたディストリビューション スイッチで使用します。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、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

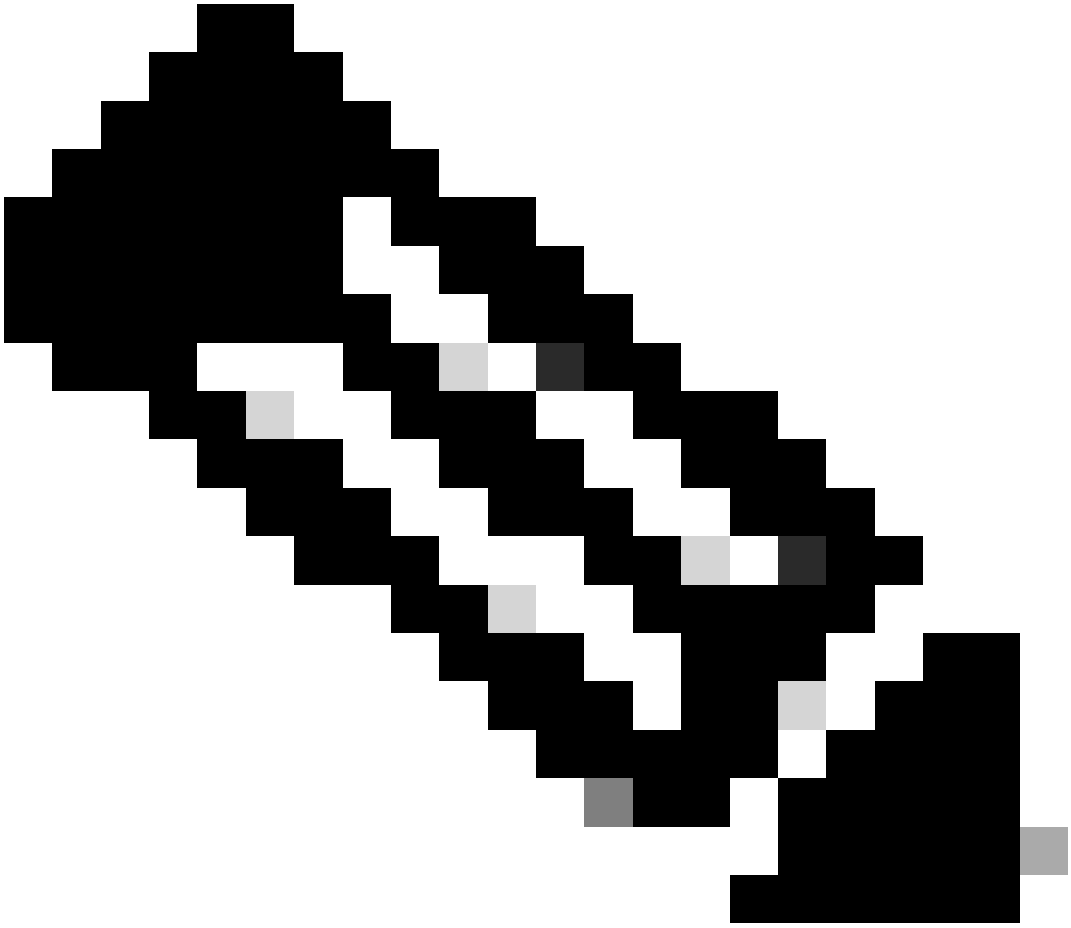
「概要」で説明しているように、STP は Cisco 製品で実装された最初の機能の 1 つです。この機能には非常に高い安定性を期待できます。現在、すでに判明している何らかのきわめて限定的な場合に STP に障害を発生させるのは、EtherChannel のような、STP よりも新しい機能との相互作用だけです。多数のさまざまな要素によりソフトウェアの不具合が引き起こされる可能性があり、多数のさまざまな影響が及ぶ可能性があります。不具合により引き起こされる可能性のある問題を適切に説明する方法はありません。ソフトウェアエラーから発生する最も危険な状況は、一部のBPDUを無視した場合、またはブロッキン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

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：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さまざまなデバイスへの接続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、リモート接続を確立できない可能性があります。

ご使用のCiscoデバイスの、 **show tech-support** コマンドの出力データがあれば、Cisco CLI Analyzerを使用できます。



注：シスコの内部ツールおよび情報にアクセスできるのは、シスコの登録ユーザーのみです。

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 ブリッジのロケーション

- ブロッキングされたポートと冗長リンクのロケーション

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、エラー状態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。

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、可能であれば、ブロッキング状態にある可能性のあるポートを最初にディセーブルにします。ポートを 1 つ無効化するたびに、ネットワークの接続が復旧したかどうかをチェックします。 どのポートを無効化したときにループが解消するかを特定することにより、どのポートが位置する冗長パスに障害が存在していたかがわかります。このポートがブロッキング状態の場合は、障害が発生したリンクが見つかったと考えられます。

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 イベントのロギングをイネーブルにします。設定するデバイスの数を制限する場合は、少なくとも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このロギングを有効にします。ブロッキングされたポートが転送モードに移行することが、ループが形成される原因です。

- Cisco IOSソフトウェアの場合：execコマンド **debug spanning-tree events** を発行して、STPデバッグ情報をイネーブルにします。general config modeコマンド **logging buffered** を発行して、デバイスバッファ内のこのデバッグ情報をキャプチャします。

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、さまざまなポートで検索するコマンドのリストを示し、Cisco IOSソフトウェアが稼働するスイッチに対して発行するコマンドの簡単な説明を示します。

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Cisco IOSソフトウェアリリース12.0以降では、 **show spanning-tree vlan <vlan-id> detail** コマンドの出力にBPDUフィールドがあります。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。もう1つのオプションは、**debug spanning-tree bpdu**コマンドでSTPデバッグを有効にして、BPDUの受信を確認することです。

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： **show interfaces [interface-number] status** コマンドを発行して、特定のポートの速度とデュプレックスのステータスをチェックします。

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 **show interfaces** コマンドを使用して、インターフェイスの使用率を確認します。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。

パケットの破損のチェック

- Cisco IOSソフトウェア： **show interfaces** コマンドの`input errors`カウンタでエラーの増分を探します。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。

の説明については、『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 **show interfaces** command output.

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 ソフトウェアの場合：**show processes cpu コマンドを発行します**。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。

スイッチに対して**show spanning-tree summary totals** コマンドを発行すると、このコマンドによって、VLANごとの論理ポートまたは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。この総計は、異なる VLAN 向け STP のすべてのインスタンスを通した、すべての論理ポートの合計を表します。この数値が、各スーパバイザ エンジン タイプでサポートされている最大数を超えないようにしてください。

注：スイッチの論理ポートの合計を計算する式は次のとおりです。

(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 nor

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。

Platform	Cisco IOS ソフトウェアでの STP の制限
Catalyst 6500/6000 Supervisor Engine 720	Cisco IOSリリース12.2SXFのリリースノートとリビルド
Catalyst 4500/4000	Catalyst 4500シリーズスイッチ、Cisco IOS、12.1EWのリリースノート
Catalyst 3750	Catalyst 3750スイッチソフトウェアコンフィギュレーションガイド、リリース12.1(19)EA1

不要な機能のディセーブル化

トラブルシューティングを行う際には、ネットワークで現在何が問題なのかを特定します。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、複数の異なるリンクを1つのリンクに論理的にバンドルするためにSTPを必要とする機能です。この機能をトラブルシューティングプロセス中に無効にすることは意味があります。一般的な規則として、設定をできるだけシンプルにすると、問題のトラブルシューティングプロセスが容易になります。

便利なコマンド

Cisco IOS ソフトウェア コマンド

- **show interfaces**
- **show spanning-tree**
- **show bridge**
- **show processes cpu**

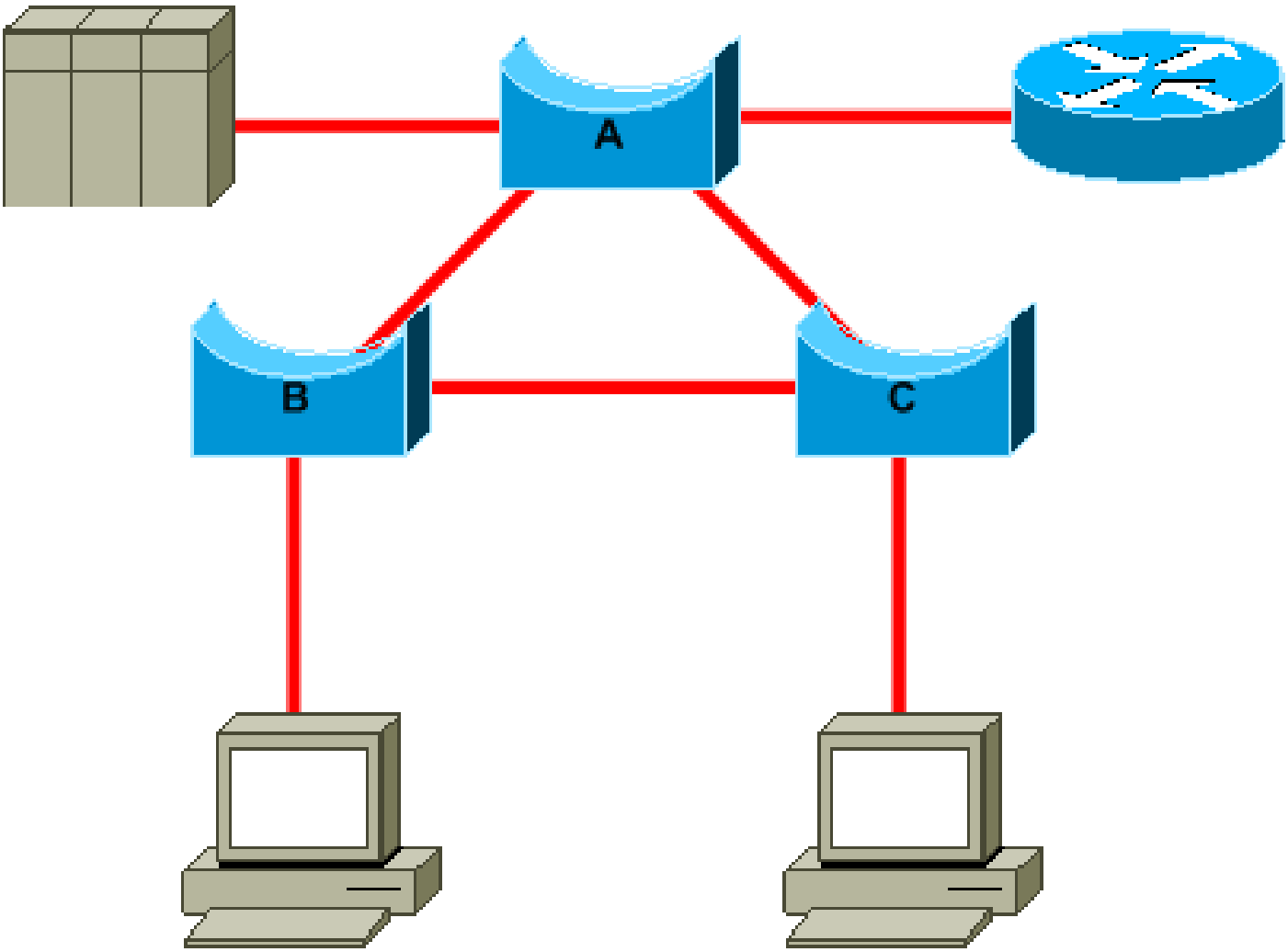
- **debug spanning-tree**

- **logging buffered**

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異なります。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がルートの場合、AからCへのリンクはブリッジAまたはブリッジCでブロックされます。この場合、スイッチBに接続するホストは、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、B と C に接続する両方のホストではルータとサーバに 2 ホップで到達可能です。この場合、平均距離は 2 ホップになります。

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。

注:VLANごとに、STPプライオリティパラメータの値を減らして、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ドします。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。

注：各VLANについて、安定したネットワークでブロックしている可能性のあるポートを把握してください。ブロックされたポートがループを解消する、ネットワーク内の各物理ループを明確に示すネットワークダイアグラムを作成します。

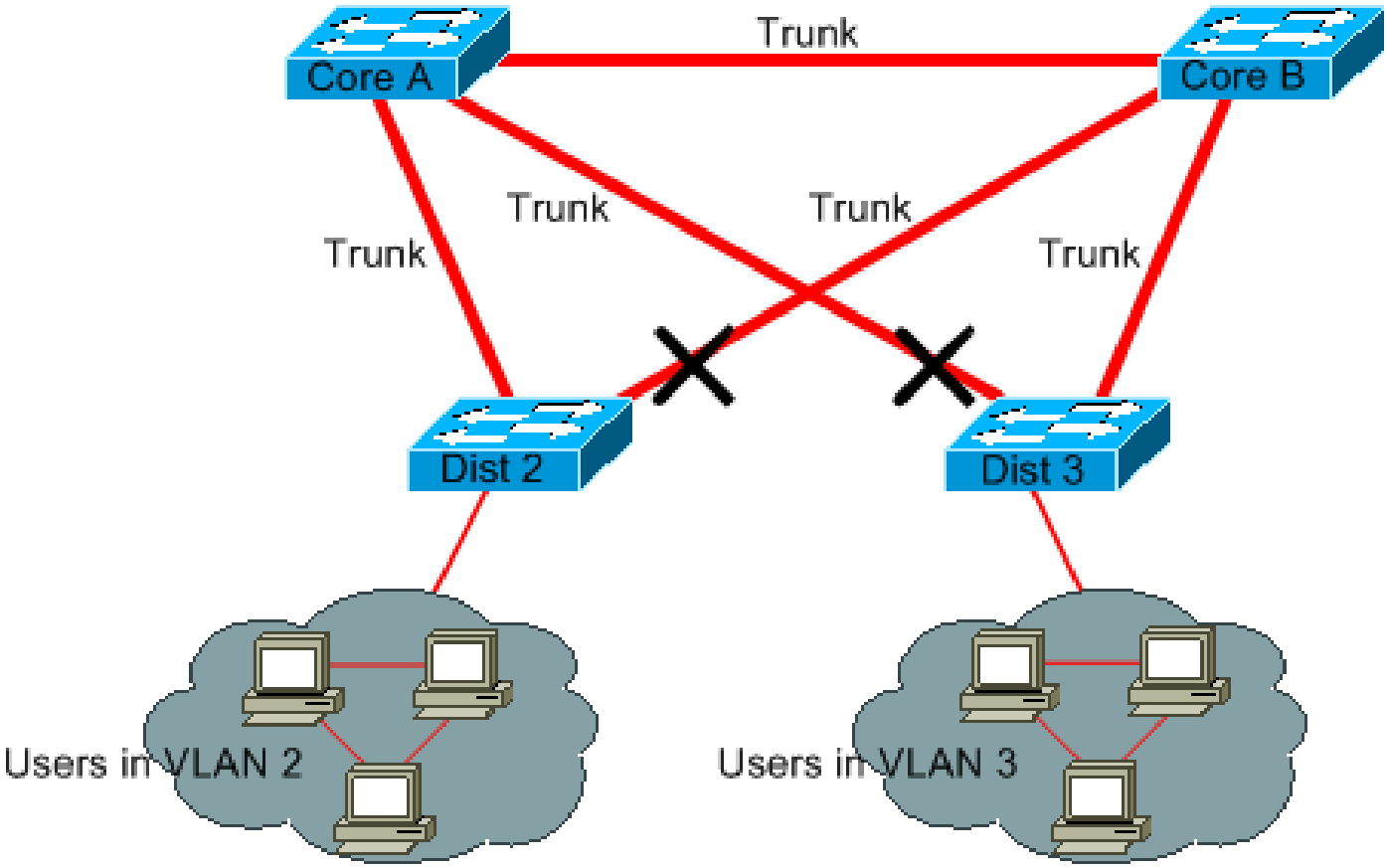
冗長リンクのロケーションがわかっていると、突発的に発生するブリッジング ループとその原因の判別に有効です。さらに、ブロッキングされたポートのロケーションがわかっていると、エラーが発生したロケーションが判別できます。

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。



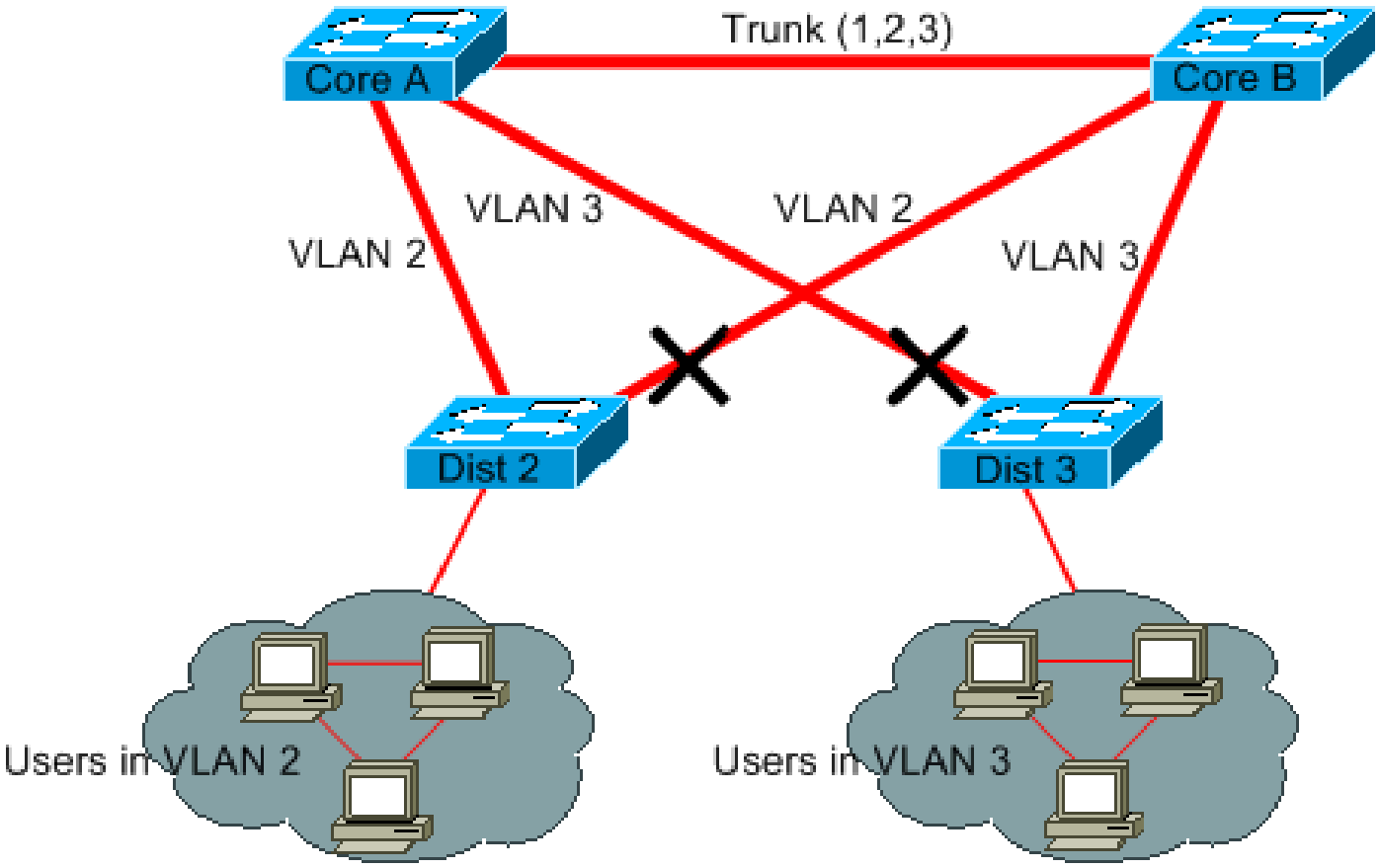
2 つのコア スイッチに、ディストリビューション スイッチが二重接続されています。ディストリビューション スイッチに接続されたユーザは、ネットワークで利用可能な複数の VLAN のサブセットに所属するだけです。この例では、Dist 2 に接続されたユーザはすべて VLAN 2 に所属しており、Dist 3 は VLAN 3 のユーザに接続しているだけです。デフォルトでは、トランクにより、VLAN Trunk Protocol（VTP）ドメイン内に定義されたすべての VLAN が搬送されます。VLAN 3 の不要なブロードキャスト トラフィックとマルチキャスト トラフィックを受信するのは Dist 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。その結果、Core AとCore Bの間に3つの冗長パスが作成されます。この冗長性により、ブロッキングされたポートが増えて、ループが発生する可能性が高くなります。

注：トランクから不要なVLANをプルーニングしてください。

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。

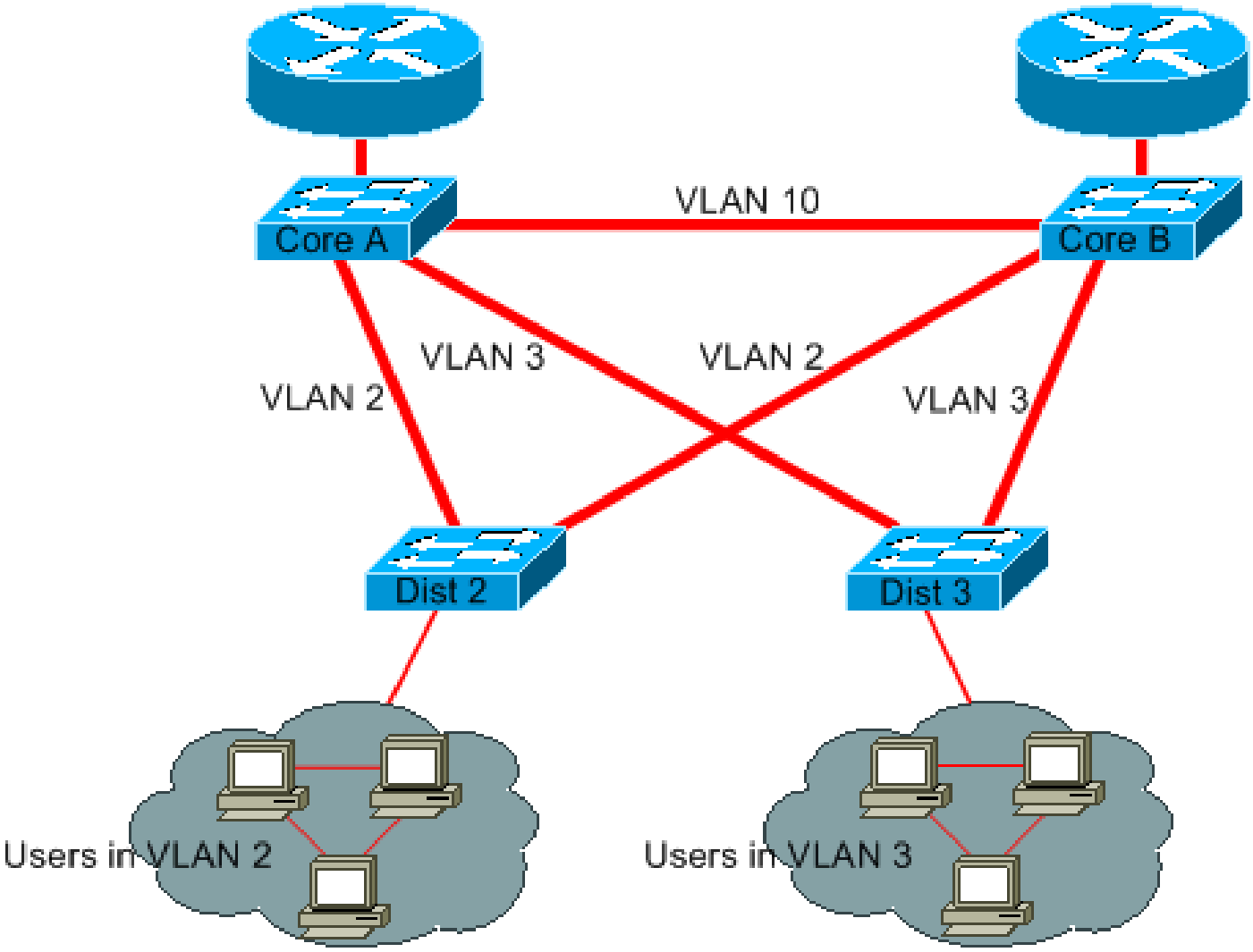
レイヤ 3 スイッチングの使用

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。

ハイエンドのシスコレイヤ3スイッチは、レイヤ2スイッチング機能と同じ速度でこの機能を実行できます。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な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を離れる速度は、VLAN内でブリッジングを行う速度と同じなので、速度の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 は一般的にはそれほどプロセッサに負荷がかかるものではなく、ほとんどの Cisco のスイッチでは、パケット スイッチングに CPU は関与しません。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。

以前のリリースでは、シスコの実装ではトランクからVLAN 1を削除する方法がありませんでした。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。

Cisco IOSソフトウェアリリース12.1(11b)Eからは、トランクからVLAN 1を削除できます。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

- **シスコサポートツールカタログ**
- **シスコのテクニカルサポートとダウンロード**

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