キャンパス スイッチ ネットワークで VLAN 内および VLAN 間の接続が低速になる一般的な原因

目次

概要

このドキュメントでは、ネットワークの速度低下の原因となる可能性がある最も一般的な問題について説明します。 このドキュメントは、一般的なネットワークの速度低下の症状を分類し、問題を診断して解決するための方法について概説します。

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。

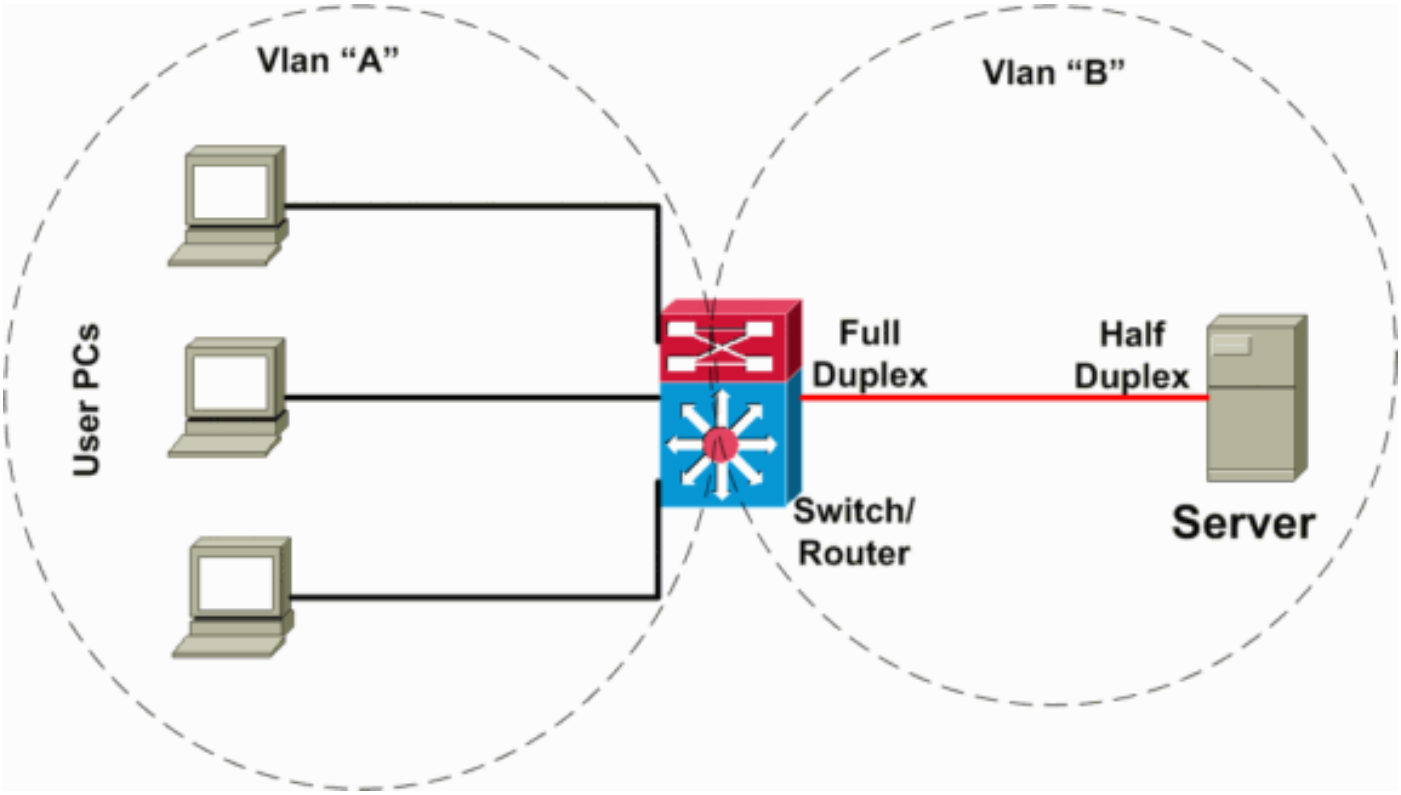
表記法

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。

VLAN 内および VLAN 間の接続速度が低下する一般的な原因

VLAN で接続速度が低下する症状は、さまざまなネットワーク層での複数の要因によって発生する可能性があります。 一般に、ネットワーク速度の問題は下位レベルで発生するものですが、上位レベルで観察される症状が「VLAN 速度の低下」という表現に包括されてしまう場合もあります。 問題を明確に区別するために、このドキュメントでは、:「コリジョン ドメインの速度低下」、「ブロードキャスト ドメインの速度低下」(または VLAN の速度低下)、および「VLAN 間転送の速度低下」という新しい用語を定義します。 これらの用語については、後のセクション「原因となる 3 つのカテゴリ」で定義します。

次のシナリオ (次のネットワーク ダイアグラムを参照) では、サーバーとクライアントの VLAN の間で、VLAN 間ルーティングを実行するレイヤ 3 (L3) スイッチが存在します。 この障害のシナリオでは、1 台のサーバがスイッチに接続されており、ポートのデュプレックス モードはサーバ側では半二重、スイッチ側では全二重にそれぞれ設定されています。 このような設定ミスによって、パケットの損失と速度の低下が発生し、サーバが接続されているリンクのトラフィック レートが高いほど、パケット損失が増加します。 このサーバと通信するクライアントにとっては、同じ VLAN 上の他のデバイスやクライアントとの通信には問題がないので、VLAN 間の転送に問題があって速度が低下しているように見えます。 問題は、異なる VLAN 上にあるサーバと通信するときにだけ発生します。 したがって、問題は単一のコリジョン ドメインで発生しているにもかかわらず、VLAN 間転送の速度低下のように見えます。



原因となる 3 つのカテゴリ

速度低下の原因は、次の 3 つのカテゴリに分類できます。

コリジョン ドメイン接続の速度低下

コリジョン ドメインは、半二重ポートに設定された接続デバイスが相互に、またはハブに接続された構成であると定義されます。 デバイスがスイッチのポートに接続され、全二重モードが設定されている場合、このようなポイントツーポイント接続でコリジョンは発生しません。 その場合でも、別の理由によってこのようなセグメントで速度低下が発生する可能性があります。

ブロードキャスト ドメイン接続の速度低下（VLAN の速度低下）

ブロードキャスト ドメイン接続の速度低下は、VLAN 全体（つまり、同じ VLAN 上のすべてのデバイス）で速度が低下する場合に発生します。

VLAN 間接続の速度低下（VLAN 間転送の速度低下）

VLAN 間接続の速度低下（VLAN 間転送の速度低下）は、ローカルの VLAN の速度は低下していなくても、トラフィックを代替の VLAN に転送する必要があり、これが予想されるレートで転送されない場合に発生します。

ネットワーク速度が低下する原因

パケット損失

多くの場合、上位レイヤのプロトコル（アプリケーション）が、ある操作を完了するまでに通常より長い時間を要した場合に、ネットワーク速度が低下していると見なされます。 このような速度低下の原因として、ネットワーク上でのパケットの損失があります。パケットの損失が発生すると、TCP やアプリケーションなどの上位レベルのプロトコルがタイムアウトして、再送信が開始されます。

ハードウェアでの転送の問題

別のタイプの速度低下として、ネットワーク機器が原因で、転送（レイヤ 2（L2）または L3）速度が低下する場合があります。 これは、正常な（設計上の）動作からの逸脱および、低速のパス転送へのスイッチングが原因で起こります。 具体的な例としては、スイッチの Multilayer Switching（MLS; マルチレイヤ スイッチング）がハードウェアによって VLAN 間の L3 パケットを転送することになっているにもかかわらず、設定ミスによって、MLS が正しく機能せず、ルータによって転送がソフトウェアで行われてしまい、VLAN 間の転送レートが大幅に低下する場合などがあります。

原因のトラブルシューティング

コリジョン ドメインの問題のトラブルシューティング

VLAN の速度が低下した場合には、まずコリジョン ドメインの問題を切り分ける必要があります。 同じコリジョン ドメインのユーザだけに接続の問題が発生しているのか、それとも複数のドメインで発生しているのかを明らかにします。 そのためには、同じコリジョン ドメイン上のユーザ PC 間でデータ転送を行い、他のコリジョン ドメインのパフォーマンス、またはそのコリジョン ドメイン自体で予想されるパフォーマンスと比較します。

そのコリジョン ドメインだけで問題が発生していて、同じ VLAN 内の他のコリジョン ドメインのパフォーマンスが正常な場合は、スイッチのポート カウンタを調べて、どのような問題がこのセグメントで発生しているかを特定します。 ほとんどの場合、デュプレックス モードのミスマッチのような単純な原因によって発生しています。 または、それほど多くはありませんが、セグメントの過負荷または加入過多により発生する場合もあります。 単一セグメントの問題のトラブルシューティングの詳細については、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。

異なるコリジョン ドメイン（ただし、同じ VLAN 上）のユーザで同じパフォーマンスの問題が発生している場合も、発信元と宛先の間にある 1 つまたは複数のイーサネット セグメントにおける二重モードのミスマッチが原因である可能性があります。 頻繁に発生するのは、次のようなシナリオです。 手動で VLAN のすべてのポートを全二重に設定してあるにもかかわらず（デフォルトの設定は「自動」）、ポートに接続しているユーザ（のネットワーク インターフェイス カード（NIC））がオートネゴシエーションの手順を実行しているような場合です。 その結果、すべてのポートでデュプレックスのミスマッチが発生し、各ポート（コリジョン ドメイン）のパフォーマンスが低下します。 したがって、VLAN 全体（ブロードキャスト ドメイン）にパフォーマンスの問題があるように見えますが、各ポートのコリジョン ドメインに対するデュプレックスの問題として分類されます。

考慮する必要のあるもう 1 つの状況は、特定の NIC に関するパフォーマンスの問題です。 パフォーマンスに問題のある NIC が共有セグメントに接続されている場合には、セグメント全体の速度が低下する可能性があります。特に、その NIC が接続されているサーバが他のセグメントや VLAN にもサービスを提供している場合には、パフォーマンスに影響が出る可能性があります。トラブルシューティングの際に判断を誤る可能性があるので、こうしたケースがあることを覚えておいてください。 この場合もやはり、問題を絞り込むための最善の方法は、同じセグメント（問題の疑いがある NIC が接続されているセグメント）上の 2 つのホストの間でデータを転送してみることです。NIC だけがそのポートに接続されている場合は、問題の切り分けは難しくなります。このような場合には、このホストで別の NIC を試してみるか、または疑わしいホストを別のポートに接続してみて、ポートと NIC が正しく設定されていることを確認します。

それでも問題が解決しない場合は、スイッチ ポートのトラブルシューティングを試みてください。 詳細は、『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。

最も困難なケースは、Cisco スイッチに接続されている NIC の一部またはすべてが互換性のない場合です。 この場合は、スイッチにパフォーマンスの問題が存在するように見えます。 Cisco スイッチと NIC の互換性をチェックするには、『Cisco Catalyst スイッチと NIC との互換性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。

最初の 2 つのケース（コリジョン ドメインの速度低下と VLAN の速度低下のトラブルシューティング）については、これらの原因に関係するドメインが異なるため、区別する必要があります。コリジョン ドメインの速度低下の場合は、問題はスイッチの外側（またはスイッチ ポートかスイッチのエッジ）か、またはスイッチ外部にあります。 この場合、そのセグメントだけに問題がある可能性があります（加入過多のセグメント、セグメントの長さの超過、セグメントの物理的な問題、またはハブやリピータの問題など）。 VLAN の速度低下の場合、問題がある可能性が最も高いのはスイッチ（1 つまたは複数のスイッチ）の内部です。 問題を正しく診断できないと、間違った場所で問題を探すことで時間を無駄にする可能性があります。

ケースを診断した後で、次の項目をチェックしてください。

共有セグメントの場合：

- セグメントが過負荷または加入過多かどうかを確認
- セグメントが正常かどうかを確認（ケーブルの長さが正しいかどうか、減衰が基準以内かどうか、メディアが物理的に破損していないかどうかなど）
- ネットワーク ポートおよびセグメントに接続されているすべての NIC 設定の互換性を確認
- NIC が正常に動作しているかどうか（および、最新のドライバを使用しているかどうか）を確認
- ネットワーク ポートでエラーが増加し続けているかどうかを確認
- ネットワーク ポートが過負荷かどうかを確認（特にサーバ ポートの場合）

ポイントツーポイント共有セグメントまたはコリジョンが発生しない（全二重）セグメントの場合：

- ポートと NIC が互換性のある設定であることを確認する。
- セグメントが正常であることを確認
- NIC が正常であることを確認
- ネットワーク ポートのエラーまたは加入過多を確認

VLAN 内（ブロードキャスト ドメイン）の速度低下のトラブルシューティング

前のセクションで説明したデュプレックスのミスマッチの問題またはコリジョン ドメインの問題が存在しないことを確認したら、次に VLAN 内の速度低下のトラブルシューティングを行います。 速度低下の場所を切り分けるための次のステップでは、同一 VLAN（ただし、異なるポート、；つまり異なるコリジョン ドメイン）のホスト間でデータ転送を行い、代替 VLAN で行った同じテストのパフォーマンスと比較します。

VLAN の速度低下に対しては、次の原因が考えられます。

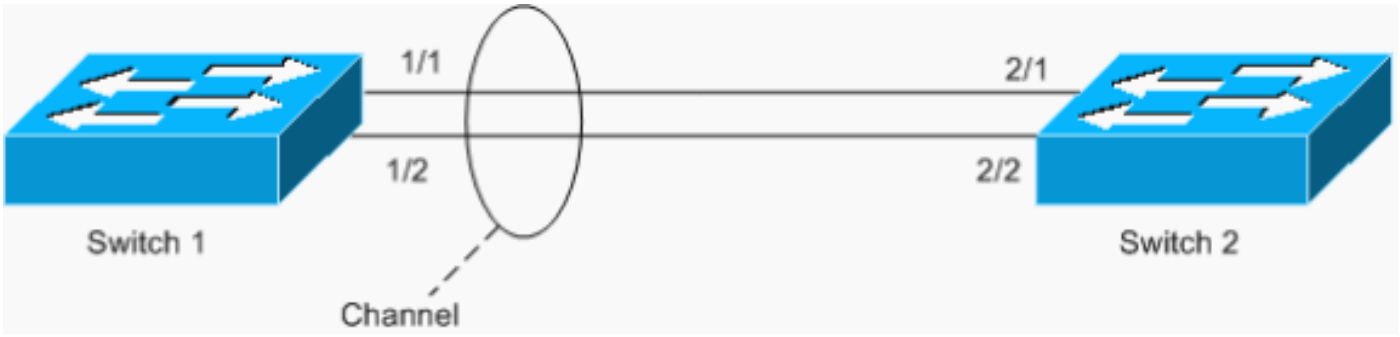
- トラフィック ループ
- VLAN の過負荷または加入過多
- スイッチのインバンド パスにおける輻輳
- スイッチ管理プロセッサでの CPU 使用率の高さ
- カットスルー スイッチでの入力エラー
- 1 ソフトウェアまたはハードウェアの設定ミス
- 1 ソフトウェアの不具合
- 1 ハードウェアの問題

intraVLAN 内接続に速度低下をもたらすこれらの 3 つの原因は、このドキュメントの対象外で、シスコ テクニカルサポートのエンジニアによるトラブルシューティングが必要になる場合があります。 上記の考えられる原因のうち最初の 5 つが除外されたら、シスコ テクニカルサポートでサービス リクエストをオープンすることが必要な場合もあります。

トラフィック ループ

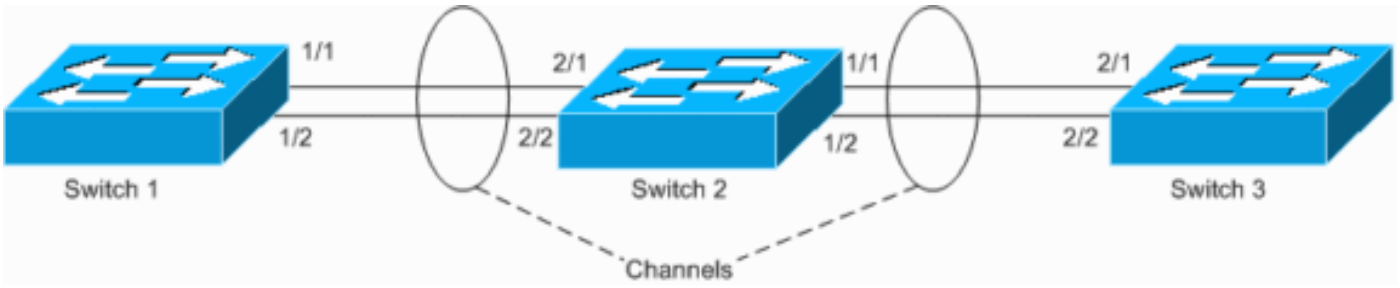
トラフィック ループは、VLAN の速度低下の最も一般的な原因です。 ループとともに、ループが発生していることを示す他の症状を確認する必要があります。 Spanning Tree Protocol（STP; スパニング ツリー プロトコル）ループのトラブルシューティングについては、『スパニング ツリー プロトコルの問題点と設計上の考慮事項』を参照してください。 ギガビット対応のバックプレーンを備えた強力なスイッチ（Cisco Catalyst 6500/6000 など）は、管理 CPU のパフォーマンスを低下させずに一部の（STP）ループに対処できますが、パケットがループすると、NIC の入力バッファおよびスイッチの受信/送信（Rx/Tx）バッファがオーバーフローし、他のデバイスへの接続時にパフォーマンスが低下する可能性があります。

ループのもう 1 つの例は、次のシナリオで示されているような、非対称に設定された EtherChannel の場合です。



この例では、ポート 1/1 と 1/2 はチャネル内にありますが、ポート 2/1 と 2/2 はチャネル内にはありません。

スイッチ 1 に設定されたチャネル (強制チャネル) があり、スイッチ 2 に対応する ポートのためのチャネル設定がありません。 フラッディング トラフィック (マルチキャスト、ブロードキャスト、および不明なユニキャスト) がスイッチ 1 からスイッチ 2 に流れた場合には、スイッチ 2 はそれをチャネルにループ バックします。 トラフィックは連続してループされず、1 回反映されるだけなので、これは完全なループではありません。 これはループ全体の半分です。 このような設定ミスが 2 つあると、次の例に示すように完全なループが作成される場合があります。



このような設定ミスがあると、トラフィックが誤ってスイッチングされるため MAC アドレスが正しくないポートで学習されて、パケットの損失が発生する危険があります。 たとえば、 (上の図のように) Hot Standby Router Protocol (HSRP; ホット スタンバイ ルータ プロトコル) を使用するルータが、スイッチ 1 に接続されているものとします。 ルータがパケットをブロードキャストすると、その MAC がスイッチ 2 によってループ バックされて、チャネルからスイッチ 1 によって学習され、ルータから再びユニキャスト パケットが送信されるまでその状態が続きます。

VLAN の過負荷または加入過多

VLAN のどこかにボトルネック (加入過多のセグメント) があるかどうかに注意し、その場所を特定します。 VLAN が過負荷になっていることを示す最初の徴候は、ポートの Rx バッファまたは Tx バッファが加入過多になることです。 いずれかのポートで outdiscard または indiscard が表示される場合は、そのポートが過負荷になっていないかを確認します。 (InDiscard の増加は、Rx バッファがいっぱいであることだけを示すわけではありません)。 Catalyst OS (CatOS) では、**show mac mod/port** または **show top [N]** コマンドが役に立ちます。 Cisco IOS® ソフトウェア (ネイティブ) では、**show interfaces slot#/port# counters errors** コマンドにより廃棄を確認できます。 VLAN の過負荷または加入過多のシナリオとトラフィック ループのシナリオは一緒に発生することがよくありますが、個別に存在することもあります。

最も頻繁に見られるのは、トラフィックの集約帯域幅を少なく見積もり過ぎたために、バックボーン ポートで発生する過負荷です。 この問題を回避する最善の方法は、ポートがボトルネックになっているデバイスの間に EtherChannel を設定することです。 そのネットワーク セグメントがすでにチャネルの場合には、さらに多くのポートをチャネル グループに追加して、チャネルのキャパシティを増やします。

また、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の極性の問題についても認識する必要があります。 この問題は、ルータによってトラフィックがロード バランスされたネットワークで発生しますが、CEF のアルゴリズムが均質であるために、すべてのトラフィックが分極化され、次のホップでは、ロード バランスされなくなります。 ただしこの問題は、ロード バランスされた L3 リンクという特定のトポロジが必要になるため、頻繁には発生しません。 Cisco Express Forwarding（CEF）に関するおよびロード バランシング詳細については、ハイブリッド モードのSupervisor 2を搭載する Catalyst 6000スイッチでのユニキャストIPルーティングCEFのトラブルシューティングを参照して下さい。

VLAN が過負荷になるもう 1 つの原因は、非対称ルーティングの問題です。 このタイプの設定を行うと、極端に大量のトラフィックが発生するため、VLAN におけるフラッディングの原因になる場合があります。 詳細については、ドキュメント『*: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*』の「*原因 1： 非対称ルーティング」のセクションを参照してください。*

場合によっては、ネットワーク デバイス自体がボトルネックになることがあります。 たとえば、3 ギガビット バックプレーンのスイッチに 4 ギガビットのトラフィックを送り込もうとすると、大量のトラフィックが失われることになります。 ネットワーク スイッチのアーキテクチャに関する説明は、このドキュメントの対象範囲外です。 ただし、ネットワーク スイッチのキャパシティを検討するときは、次の点に注意してください。

- バックプレーンのキャパシティ
- 行頭ブロッキングの問題
- ブロッキングおよび非ブロッキング スイッチ/ポートのアーキテクチャ

スイッチのインバンド パスにおける輻輳

スイッチのインバンド パスにおける輻輳によって、ネットワークでスパニング ツリー ループやその他のタイプの不安定な状態が発生する可能性があります。 シスコ スイッチのインバンド ポートは、いずれも管理プロセッサに管理トラフィック（Cisco Discovery Protocol および Port Aggregation Protocol（PAgP; ポート集約プロトコル）などのトラフィック）のインターフェイスを提供する仮想ポートです。 インバンド ポートが仮想と見なされるのは、一部のアーキテクチャではユーザはこのポートを見ることができず、インバンド機能がポートの通常の動作と結合されているためです。 たとえば、Catalyst 4000、Catalyst 5000、および Catalyst 6500/6000 シリーズ スイッチ（CatOS が稼働）の SC0 インターフェイスは、インバンド ポートのサブセットです。 インターフェイス SC0 が提供するのは、設定されている VLAN 内の管理プロセッサに対する IP スタックだけです。一方、インバンド ポートは、設定されている任意の VLAN の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）および他の多くの管理プロトコル（Cisco Discovery Protocol、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）、Cisco Group Management Protocol（CGMP）、Dynamic Trunking Protocol（DTP; ダイナミック トランキング プロトコル）など）に対して、管理プロセッサへのアクセスを提供します。

インバンド ポートが（アプリケーションの設定ミスやユーザ トラフィックなどのために）過負荷状態になると、定期的なメッセージや「hello」を受信することで状態を安定させるプロトコルの場合は、不安定になる可能性があります。 この状態が原因で、一時的なループやインターフェイスのフラッピング、およびその他の問題が発生し、このタイプの速度低下が発生する場合があります。

スイッチでインバンド ポートの輻輳を発生させるのは困難ですが、悪意を持って作成された Denial of Service（DoS; サービス拒絶攻撃）であれば成功する可能性があります。 インバンド ポートでレートを制限したり、トラフィックを削減したりする手段はありません。 解決するには

、スイッチの管理者が介入して調査する必要があります。 通常、インバンド ポートには輻輳に対して高い耐性があります。 インバンド ポートに Rx 方向または Tx 方向で異常が発生したりスタックすることは、ほとんどありません。 これは、ハードウェアが停止することを意味し、スイッチ全体に影響があります。 この状態は認識するのが難しく、通常は、シスコ テクニカル サポートのエンジニアが診断を行います。 症状としては、スイッチが突然何も「聞こえなく」なり、Cisco Discovery Protocol ネイバーのアップデートなどの制御トラフィックの受信を停止します。これは、Rx インバンドの問題を示しています（ただし、Cisco Discovery Protocol ネイバーが 1 つでも認識される場合は、インバンドは機能しています）。 同様に、接続されているすべてのスイッチで 1 つのスイッチからの Cisco Discovery Protocol（および他のすべての管理プロトコル）が失われた場合は、そのスイッチのインバンド インターフェイスに関連した Tx の問題を示しています。

スイッチ管理プロセッサでの CPU 使用率の高さ

インバンド パスが過負荷になると、スイッチの CPU 使用率が高くなる可能性があります。 また、CPU はその不必要なトラフィックをすべて処理しなければならないので、状況はさらに悪化します。 CPU の高使用率が過負荷状態のインバンド パスまたはそれに代わる問題によるものである場合は、上の「スイッチのインバンド パスにおける輻輳」セクションで説明したように、管理プロトコルに影響することがあります。

一般に、管理 CPU はすべてのスイッチにおいて脆弱なポイントと考える必要があります。 スイッチを正しく設定することで、CPU 使用率の高さにより発生する問題のリスクを抑えることができます。

Catalyst 4000 シリーズ スイッチの スーパーバイザ エンジン I と II のアーキテクチャは、管理 CPU がスイッチング オーバーヘッドに含まれる設計になっています。 次のことに留意してください。

- CPU は、新しいパス（Supervisor Engine I と II はパスベースです）がスイッチに入るたびに、スイッチ ファブリックをプログラムします。 インバンド ポートが過負荷の場合は、新しいパスは廃棄されます。 その結果、トラフィックがポート間でスイッチされるときに、上位レイヤのプロトコルでパケットの損失（サイレント破棄）と速度低下が発生します（上記の「スイッチのインバンド パスにおける輻輳」セクションを参照）。
- スーパーバイザ エンジン I および II では、スイッチングは一部 CPU で実行されるため、CPU の使用率が高いと、Catalyst 4000 のスイッチング機能が影響を受ける可能性があります。 Supervisor Engine I および II で CPU 使用率が高い場合は、スイッチングのオーバーヘッド自体が原因である可能性があります。

Catalyst 4500/4000 シリーズの Supervisor Engine II+、III、および IV は、トラフィックによる影響をきわめて受けにくいですが、Cisco IOS ソフトウェア ベースの Supervisor Engine における MAC アドレスの学習については、依然として管理 CPU により完全にソフトウェアで行われています。 そのため、CPU の使用率の高さがこのプロセスに影響を与え、速度低下につながる可能性があります。 Supervisor Engine I および II と同様に、Supervisor Engine II+、III、IV の場合でも、大量の MAC アドレス学習または再学習によって、CPU の使用率が高くなる可能性があります。

Catalyst 3500XL および 2900XL シリーズ スイッチの場合も、MAC の学習に CPU が関係するため、高速でアドレスの再学習が行われる処理によって CPU のパフォーマンスが影響を受けます。

また、MAC アドレスの学習プロセスは（完全にハードウェアで実装される場合であっても）、スイッチング プロセスと比較すると低速なプロセスです。 MAC アドレスの再学習の割合が高い状

態が続く場合には、原因を探して除去する必要があります。 ネットワークでのスパニング ツリー ループは、このような MAC アドレスの再学習の原因になる可能性があります。 MAC アドレスの再学習（または MAC アドレス フラッピング）は、ポートベースの VLAN を実装するサードパーティのスイッチによって発生することもあります。これは、MAC アドレスが VLAN タグと関連付けられていないことを意味します。 この種類のスイッチを特定の設定でシスコのスイッチに接続すると、VLAN 間で MAC が漏洩してしまう場合があります。 その結果、MAC アドレスの再学習の割合が高くなり、パフォーマンスが低下する可能性があります。

カットスルー スイッチでの入力エラー

カットスルー入力エラー パケットの伝搬は「コリジョン ドメイン接続の速度低下」に関連しますが、エラー パケットが別のセグメントに転送されるため、セグメント間のスイッチングに問題があるように見えます。 カットスルー スイッチ（Catalyst 8500 シリーズ Campus Switch Routers（CSR; キャンパス スイッチ ルータ）や Catalyst 4000 シリーズ用の Catalyst 2948G-L3 または L3 スイッチング モジュールなど）では、スイッチがパケットを宛先ポートに転送するのに十分な情報をパケットの L2/L3 ヘッダーから取得すると、すぐにパケット/フレームのスイッチングが開始されます。 そのため、入力ポートと出力ポートの間でパケットがスイッチされている場合には、パケットの先頭が出力ポートからすでに転送されているのに、パケットの残りの部分はまだ入力ポートで受信中という状態になります。 ここで、入力セグメントが正常ではなく、Cyclic Redundancy Check（CRC; 巡回冗長検査）エラーまたはラントが発生した場合、どのようになるでしょうか。 スイッチはフレームを最後まで受信して初めてこのことを認識しますが、そのときには、フレームの大部分は出力ポートから転送済です。 残りのエラーのあるフレームは、転送しても意味がないため廃棄され、出力ポートでは「アンダーラン」エラー、入力ポートでは対応するエラー カウンタが増分されます。 複数の入力ポートに異常があり、それらのサーバが出力ポートに存在する場合、実際には何も問題がなくてもサーバ セグメントに問題があるように見えます。

カットスルー L3 スイッチの場合は、アンダーランを監視して、発生した場合は、すべての入力ポートでエラーをチェックする必要があります。

ソフトウェアまたはハードウェアの設定ミス

設定ミスにより、VLAN の速度が低下する可能性があります。 このような悪影響は、加入過多または過負荷の状態の VLAN によって発生する場合もありますが、最も多いのは不適切な設計や設計上の見落しに起因するものです。 たとえば、トラフィックの制限方式が正しく設定されていないセグメント（VLAN）では、マルチキャスト トラフィック（たとえば、ビデオや音声のストリーム）によって簡単に過負荷な状態が発生してしまいます。 このようなマルチキャスト トラフィックはデータ転送にも影響を与えるため、VLAN 全体のすべてのユーザにパケット損失（および、マルチキャスト ストリームを受信する予定のないユーザにセグメントのフラッディング）をもたらす可能性があります。

ソフトウェアの不具合とハードウェアの問題

ソフトウェアの不具合とハードウェアの問題は、トラブルシューティングの難しい逸脱をもたらすので、判別が困難です。 問題の原因がソフトウェアの不具合またはハードウェアの問題であると考えられる場合は、シスコ テクニカルサポートのエンジニアに連絡して、問題の調査を依頼して下さい。

VLAN 間の接続速度の低下に関するトラブルシューティング

VLAN 間接続の速度低下についてトラブルシューティングする前に、このドキュメントの「コリ

ジョン ドメインの問題のトラブルシューティング」および「VLAN 内（ブロードキャスト ドメイン）の速度低下のトラブルシューティング」セクションで解説されている問題を調査して、除外してください。

ほとんどの場合、VLAN 間接続の速度低下はユーザの設定ミスが原因です。 たとえば、MLS または Multicast Multilayer Switching（MMLS; マルチキャスト マルチレイヤ スイッチング）の設定が正しくない場合には、パケットの転送がルータの CPU によって行われます。この場合、パスは低速になります。 設定ミスを防ぎ、必要な場合に効率よくトラブルシューティングするには、使用している L3 転送デバイスで使われているメカニズムについて理解しておく必要があります。ほとんどの場合、L3 転送メカニズムは、ルーティングおよび Address Resolution Protocol（ARP; アドレス レゾリューション プロトコル）テーブルのコンパイルと、抽出されたパケットの転送情報のハードウェアへのプログラミング（ショートカット）に基づくものです。ショートカットをプログラミングするプロセスに障害があると、ソフトウェアでのパケット転送（低速のパス）、不正な転送（正しくないポートへの転送）、またはトラフィックのブラック ホールが発生します。

通常、ショートカットプログラミングの障害または不完全なショートカットの作成（ソフトウェアでのパケット転送、不正な転送、またはトラフィックのブラック ホールの原因になります）は、ソフトウェアの不具合によるものです。 このようなケースが考えられる場合は、シスコ テクニカルサポートのエンジニアに調査を依頼してください。 それ以外の VLAN 間転送の速度低下の理由としては、ハードウェアの異常が考えられますが、このドキュメントではそのような原因は対象としていません。 ハードウェアで異常が発生すると、ハードウェアでショートカットが正常に作成されず、トラフィックは低速の（ソフトウェア）パスになったり、ブラック ホールに入ったりします。 ハードウェアの異常についても、シスコ テクニカルサポートに調査を依頼してください。

機器の設定には問題がないと考えられるのに、ハードウェアのスイッチングが行われない場合は、ソフトウェアの不具合またはハードウェアの異常が原因である可能性があります。 ただし、このような結論を下す前に、デバイスの機能に注意する必要があります。

ハードウェアの転送が中断するか、またはまったく行われない場合に、最もよくある状況を 2 つ示します。

- まず、ショートカットを格納するメモリに空きがない状況です。 メモリがいっぱいになると、通常、ソフトウェアはそれ以上ショートカットを作成しなくなります。（たとえば、NetFlow または Cisco Express Forwarding ベースの MLS は、新しいショートカットを格納する場所がなくなると非アクティブになり、ソフトウェア（低速のパス）に切り替わります。）
- 機器がハードウェア スイッチングを行うよう設計されていないのに、それがはっきりしていない。 たとえば、Catalyst 4000 シリーズの Supervisor Engine III 以降は、IP トラフィックだけをハードウェアで転送するように設計されています。 それ以外のタイプのトラフィックは CPU によってソフトウェアで処理されます。 もう 1 つの例は、CPU の介入を必要とする Access Control List（ACL; アクセス コントロール リスト）の設定です（たとえば、「ログ」オプションの指定）。 このルールに該当するトラフィックは、CPU によってソフトウェアで処理されます。

カットスルー スイッチでの入力エラー も、VLAN 間ルーティングの速度が低下する原因になる場合があります。 カットスルー スイッチの場合、L3 と L2 のトラフィックの転送に同じアーキテクチャ原理を使用するため、「VLAN 内（ブロードキャスト ドメイン）の速度低下のトラブルシューティング」セクションで説明したトラブルシューティング方法を L2 トラフィックにも適用できます。

VLAN 間ルーティングに影響を与えるもう 1 つのタイプの設定ミスは、エンドユーザ デバイス（PC やプリンタなど）での設定ミスです。 よく見られる状況は PC の設定ミスで、 たとえば、デフォルト ゲートウェイの設定ミス、無効な PC ARP テーブル、IGMP クライアントの誤動作などがあります。 よくあるケースとしては、ルータまたはルーティング機能を持つデバイスが複数あり、エンドユーザ PC の一部または全部が、誤ったデフォルト ゲートウェイを使用するように設定されている場合があります。 ネットワーク デバイスはすべて適切に設定されて正しく動作するにもかかわらず、この設定ミスのためにエンドユーザ デバイスがそれを使用しないので、これは最も厄介な状況になる可能性があります。

ネットワーク内のデバイスがどのようなタイプのハードウェア アクセラレーションも備えていない（そして NetFlow MLS に参加しない）通常のルータである場合、トラフィック転送のレートは CPU の速度とそのビジー状態に完全に依存します。 CPU の使用率が高い場合、転送レートが確実に影響を受けます。 ただし、L3 スイッチでは、CPU の使用率が高くなっても、転送レートが影響を受けるとは限りません。 CPU の使用率が高い場合には、ハードウェア ショートカットを作成（プログラム）する CPU の能力が影響を受けます。 ショートカットがハードウェアにすでにインストールされている場合には、CPU の使用率が高くても、ショートカットがエージングアウトするまで（有効期間タイマーがある場合）、または CPU によって削除されるまでは、トラフィック（プログラムされたショートカットに対するもの）はハードウェアでスイッチされます。 ただし、ルータが何らかのタイプのソフトウェア アクセラレーション（ファースト スイッチングや Cisco Express Forwarding スイッチングなど）を使用するように設定されている場合には、パケットの転送がソフトウェア ショートカットによって影響を受けることがあります。 つまり、ショートカットが壊れた場合、またはメカニズム自体が故障した場合には、転送レートの加速は行われず、代わりに、トラフィックが CPU にパントされるため、データ転送レートが低下します。

関連情報

- IP マルチレイヤ スイッチングのトラブルシューティング
- ハイブリッド モードの Supervisor 2 を搭載する Catalyst 6000 スイッチでのユニキャスト IP ルーティング CEF のトラブルシューティング（英語）
- Catalyst 3750/3560/3550 シリーズ スイッチによる VLAN 間ルーティングの設定
- スイッチ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