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

内容

概要

この文書は、スイッチド ネットワークにおけるユニキャスト パケット フラッディングの考えられる原因と影響について説明しています。

前提条件

要件

このドキュメントに特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。

表記法

ドキュメントの表記法の詳細は、「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。

問題の定義

LAN スイッチでは転送テーブル（レイヤ 2 テーブル、Content Addressable Memory（CAM）テーブル）の使用により、フレームの VLAN 番号と宛先 MAC アドレスに基づいてトラフィックが特定のポートに誘導されます。着信 VLAN にフレームの宛先 MAC アドレスに対応するエントリ

がない場合、その（ユニキャスト）フレームはそれぞれの VLAN 内のすべての転送ポートに送信されてしまうため、フラッディングを引き起こします。

限定されたフラッディングは通常のスイッチング プロセスの一部です。ただし、継続的にフラッディングが発生することによって、ネットワークのパフォーマンスが悪影響を受ける場合があります。この文書では、フラッディングによってどのような問題が引き起こされるかについて説明し、ある特定のトラフィックが継続的にフラッディングされる最も一般的な理由を示します。

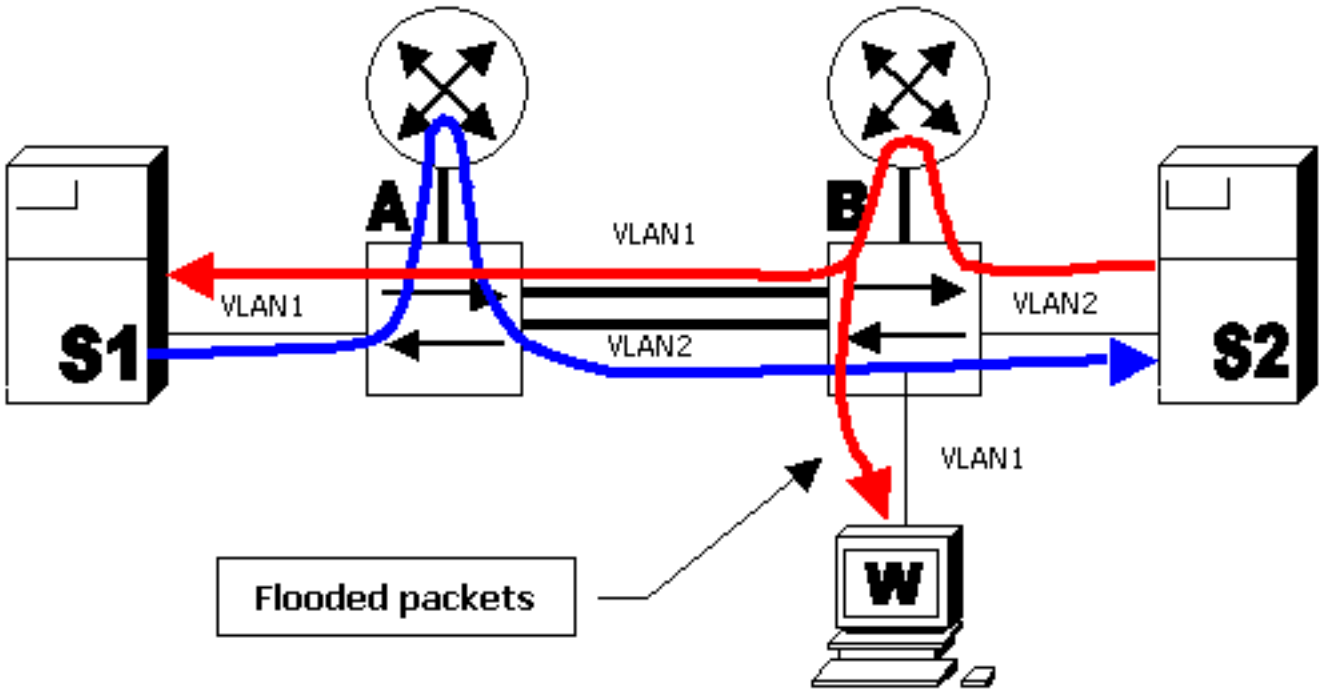
Catalyst 2900 XL、3500 XL、2940、2950、2970、3550、3750、4500/4000、5000、6500/6000 シリーズ スイッチなどの最近のスイッチでは、VLAN ごとに L2 転送テーブルが管理されていることに注意してください。

フラッディングの原因

フラッディングの根本的原因は、スイッチの L2 転送テーブルにパケットの宛先 MAC アドレスが登録されていないことにあります。このような場合、（パケットを受信したポートを除く）VLAN 内のすべての転送ポートからパケットが送信されてしまうため、フラッディングが発生します。 次のケース スタディでは、宛先 MAC アドレスがスイッチで認識されない一般的な原因を示します。

原因 1：非対称ルーティング

大量のトラフィックがフラッディングされると、帯域幅の低いリンクが飽和状態になり、ネットワークのパフォーマンスが低下したり、そのような帯域幅の低いリンクを経由して接続されているデバイスにまったく接続できなくなったりする危険性があります。次の図を検討してみます。



上記の図では、VLAN 1 のサーバ S1 が VLAN 2 のサーバ 2 へのバックアップ（バルク データ転送）を実行しています。サーバ S1 のデフォルト ゲートウェイはルータ A の VLAN 1 インターフェイスをポイントしています。サーバ S2 のデフォルト ゲートウェイは、ルータ B の VLAN 2 インターフェイスをポイントしています。S1 から S2 へのパケットは次のパスを通ります。

- S1--VLAN 1--スイッチ A--ルータ A--VLAN 2--スイッチ B--VLAN 2--S2（青い線）

S2 から S1 に送信されるパケットは、次のパスを通ります。

- S2--VLAN 2--スイッチ B--ルータ B--VLAN 1--スイッチ A--VLAN 1 へのフラッディング--S1（赤い線）

このような配置では、スイッチ A が VLAN 2 内で S2 MAC アドレスから送信されたトラフィックを「見る」ことがないことに注意してください（ルータ B によって送信元 MAC アドレスが書き換えられており、パケットは VLAN 1 だけに到達するため）。 これは、スイッチ A が S2 MAC アドレスにパケットを送信するたびに、パケットが VLAN 2 にフラッディングされることを意味します。同じ状況がスイッチ B での S1 MAC アドレスについても起こります。

この動作は非対称ルーティングと呼ばれます。パケットは送信される方向によって異なるパスを通ります。フラッディングを引き起こす最大の原因は 2 つありますが、非対称ルーティングはそのうちの 1 つです。

ユニキャスト フラッディングの影響

上記の例に戻ると、S1とS2間のデータ転送のパケットは、主にスイッチAのVLAN 2とスイッチBのVLAN 1にフラッディングされます。これは、スイッチBのVLAN 1に接続されたすべてのポート（この例ではのワークステーションW）が55550000050)が55005005500000000000000000000000000000000000000000000000000000000000000000このトラフィック量によって、10 Mbps リンクは飽和状態になります。そのため、PC にまったく接続できなくなるか、またはパフォーマンスが著しく低下します。

このフラッディングは非対称ルーティングが原因であり、サーバ S1 がブロードキャスト パケット（Address Resolution Protocol（ARP）など）を送信すると、フラッディングを停止できる場合があります。 スイッチAはこのパケットをVLAN 1にフラッディングし、スイッチBはS1のMACアドレスを受信して学習します。スイッチはトラフィックを継続的に受信していないため、この転送エントリはエージングアウトし、フラッディングが再開されます。同じプロセスが S2 にも当てはまります。

非対称ルーティングによって生じるフラッディングを制限するには、いくつかの方法があります。詳細は、次のドキュメントを参照してください。

- Catalyst 2948G-L3 および 4908G-L3 スイッチのブリッジ グループでの非対称ルーティング
- 非対称ルーティングと HSRP（HSRP が稼働しているルータが接続されたネットワークでのユニキャスト トラフィックの過剰なフラッディング）

通常は、ルータの ARP タイムアウトとスイッチの転送テーブルのエージング タイムを近付ける方法をとります。それによって、ARP パケットがブロードキャストされます。その結果、L2 転送テーブルのエントリがエージング アウトする前に、再学習が行われるようになります。

この種の問題がよく見られるシナリオは、冗長レイヤ 3（L3）スイッチ（Mutilayer Switch Feature Card（MSFC）が搭載された Catalyst 6000 など）で、Hot Standby Router Protocol（HSRP）を使用したロード バランスを設定しているケースです。 このケースでは、1 台のスイッチが偶数番号の VLAN に対してアクティブになり、別の 1 台のスイッチが奇数番号の VLAN に対してアクティブになります。

原因 2：スパニングツリー プロトコル トポロジの変更

フラッディングが原因で生じるもう 1 つの一般的な問題は、スパニング ツリー プロトコルの Topology Change Notification（TCN; トポロジ変更通知）です。TCN は、転送トポロジが変更さ

れた後に、転送テーブルを訂正することを目的に設計されました。トポロジの変更後は、それまで特定のポートを通じてアクセスしていた宛先に別のポートからアクセスするようになります。これによって接続不能になる事態を避けるために、TCN が必要になります。TCN は転送テーブルのエージング タイムを短縮することによって機能します。そのため、アドレスが再学習されていなければ、エージング アウトすることになり、フラッディングが発生します。

TCN は、転送状態に移行したポート、または転送状態から別の状態に移行したポートによってトリガされます。TCN の発行後は、特定の宛先 MAC アドレスがエージング アウトしても、ほとんどの場合、そのアドレスは再学習されるため、しばらくの間はフラッディングは発生しません。問題となるのは、TCN が短い間隔で繰り返し発行される場合です。スイッチの転送テーブルがすぐにエージングするため、フラッディングがほとんど絶え間なく発生します。

一般に、適切に構成されたネットワークでは、TCN が発行されることはほとんどありません。スイッチのポートがアップまたはダウンするときに、ポートの STP の状態が「転送」に変わるか、または「転送」から別の状態に変わると、最終的に TCN が発行されます。ポートがフラッピングしていると、TCN が繰り返し発行され、そのたびにフラッディングが発生します。

STP PortFast 機能を有効にしたポートでは、転送状態に移行するか、転送状態から別の状態に移行しても、TCN は発行されません。すべてのエンドデバイス ポート (プリンタ、PC、サーバなど) で PortFast を設定すれば、TCN の量を低く抑えることができます。TCN の詳細については、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 トポロジの変更について

注：MSFC IOS には、VLAN 内で TCN が発行された場合に、VLAN インターフェイスを通じて ARP テーブルにエントリを再入力する最適化機能があります。この機能を使用すると、ARP 要求がブロードキャストされ、ホストからの ARP 応答によってホストの MAC アドレスが再学習されるため、TCN を原因とするフラッディングを抑制できます。

原因 3：転送テーブルのオーバーフロー

その他にフラッディングの原因として考えられるものに、スイッチの転送テーブルのオーバーフローがあります。この場合、転送テーブルのスペースが使用可能になるまで、新しいアドレスが学習されないため、そのようなアドレス宛てのパケットがフラッディングされます。転送テーブルのスペースが使用可能になると、新しいアドレスが学習されます。最近のスイッチは、ほとんどの場合、MAC アドレスを収容できる十分な大きさの転送テーブルを持つように設計されているため、転送テーブルがオーバーフローする可能性はゼロとは言えませんが、めったにありません。

転送テーブルの消耗は、ネットワーク攻撃によって、1 台のホストがそれぞれ異なる送信元 MAC アドレスを持つフレームを生成し続けるようになることによっても発生します。このような攻撃を受けると、転送テーブルのリソースが独占されてしまいます。転送テーブルが飽和状態になると、アドレスを新たに学習できなくなるため、他のトラフィックがフラッディングされます。この種の攻撃は、スイッチの転送テーブルを調べることで検出できます。大部分の MAC アドレスが同じポートまたはポートのグループを指しています。このような攻撃を防ぐには、ポート セキュリティ機能を使用して、信頼できないポートで学習される MAC アドレスの数を制限します。

Cisco IOS® または CatOS ソフトウェアが稼働する Catalyst スイッチのコンフィギュレーション ガイドには、「ポート セキュリティの設定」または「ポート ベースのトラフィック制御の設定」というセクションがあります。詳細については、シスコ スイッチ製品ページで、各スイッチのテクニカル ドキュメントを参照してください。

注：ユニキャストフラッディングが、ポートセキュリティ用に「制限」を条件として設定された

スイッチポートで発生すると、セキュリティ違反が発生します。

```
Router(config-if)#switchport port-security violation restrict
```

注：このようなセキュリティ違反が発生した場合は、「restrict」モードに設定された該当ポートは、十分な数のセキュアMACアドレスを削除して最大値を下回るまで、未知の送信元アドレスを持つパケットを廃棄する必要があります。これにより、SecurityViolationカウンタが増加します。

注：この動作の代わりに、スイッチポートが「シャットダウン」状態になった場合は、`Router(config-if)#switchport`す。

過剰なフラッディングの検出方法

ほとんどのスイッチでは、フラッディングを検出するための特別なコマンドは実装されていません。Cisco IOS システム ソフトウェア (ネイティブ) バージョン 12.1(14)E 以降、または Cisco CatOS システム ソフトウェア バージョン 7.5 以降が稼働する Catalyst 6500/6000 Supervisor Engine 2 以降のシリーズ スイッチには、「**ユニキャスト フラッド保護**」機能が実装されています。この機能を使用すると、VLAN ごとにユニキャスト フラッディングを監視して、フラッディングが一定量を超えた場合に指定したアクションを実行できます。このアクションには、syslog への記録、VLAN の制限、または VLAN のシャットダウンがありますが、フラッディングの検出には、syslog が最も役に立ちます。フラッディングが一定量を超え、syslog への記録がアクションとして指定されている場合は、次のようなメッセージが表示されます。

```
%UNICAST_FLOOD-4-DETECTED: Host 0000.0000.2100 on vlan 1 is flooding
to an unknown unicast destination at a rate greater than/equal to 1 Kfps
```

表示されている MAC アドレスは、このスイッチ上でパケットのフラッディングが発生している発信元 MAC です。スイッチは宛先 MAC アドレスを参照することにより転送を実行するため、通常は、どの宛先 MAC アドレスに対してフラッディングが発生しているかを確認する必要があります。 Catalyst 6500/6000スーパーバイザエンジン2以降のCisco IOS (ネイティブ) バージョン12.1(20)Eでは、フラッディングが発生しているMACアドレスを表示する機能が実装されます。

```
cat6000#sh mac-address-table unicast-flood
Unicast Flood Protection status: enabled

Configuration:
 vlan      Kfps         action       timeout
------+----------+-----------------+----------
   55          1             alert      none

Mac filters:
 No.   vlan   souce mac addr.           installed on           time left (mm:ss)
-----+------+----------------+-----------------------------+-----------------

Flood details:
 Vlan   souce mac addr.              destination mac addr.
------+---------------+-------------------------------------------------
   55   0000.2222.0000    0000.1111.0029, 0000.1111.0040, 0000.1111.0063
                          0000.1111.0018, 0000.1111.0090, 0000.1111.0046
                          0000.1111.006d
```

さらに、MAC アドレス 0000.2222.0000 から、destination mac addr セクションに表示されている MAC アドレスにトラフィックが送信されているかどうかを調べることができます。トラフィックが正当なものである場合は、宛先 MAC アドレスがスイッチで認識されない原因を確認する

必要があります。

パフォーマンスが低下したり、デバイスに接続できなくなったりしたときには、ワークステーション上でパケットのトレースをキャプチャすることによって、フラッディングが発生しているかどうかを検出できる場合があります。通常は、ワークステーションに関係のないユニキャスト パケットが、ポートで繰り返し検出されることはありません。 このような状況が起こっている場合は、フラッディングが発生している可能性があります。フラッディングの原因が異なれば、パケット トレースの状態もまた異なります。

原因が非対称ルーティングにある場合は、特定の MAC アドレス宛てのパケットが存在する可能性が高いため、宛先が応答した後もフラッディングは止まりません。原因が TCN にある場合は、フラッディング中に多数の異なるアドレスが含まれます。フラッディングはやがておさまりますが、後で再び始まります。

原因が L2 転送テーブルのオーバーフローにある場合は、おそらく非対称ルーティングと同じようなフラッディングが見られます。非対称ルーティングと異なるのは、不自然なパケットが多いという点、または異なる送信元 MAC アドレスを持つ正常なパケットが異常に大量に存在するという点です。

関連情報

- スイッチ製品に関するサポート ページ
- LAN スイッチング テクノロジーに関するサポート ページ
- テクニカルサポート - Cisco Systems