ポート単位のトラフィック制御の設定

ポートベースのトラフィック制御

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポートレベルでパケットをフィルタまたはブロックするために使用するシスコデバイス上のレイヤ2機能の組み合わせです。次のポートベースのトラフィック制御機能がサポートされています。

- ストーム制御
- 保護ポート
- ポート ブロッキング

ポート ベースのトラフィック制御に関する情報

ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

測定されたトラフィックアクティビティ

ストーム コントロールは、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回るまで、デバイスはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

（注） マルチキャスト トラフィックのストーム制御しきい値に達した場合、ブリッジ プロトコル データ ユニット（BPDU）および Cisco Discovery Protocol フレームなどの制御トラフィック以外のマルチキャスト トラフィックはすべてブロックされます。ただし、デバイスでは Open Shortest Path First（OSPF）などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

ユニキャストのストーム制御は、既知のユニキャスト トラフィックと不明なユニキャスト トラフィックの組み合わせです。ユニキャストのストーム制御が設定され、設定値を超えると、ストームはハードウェア ポリサーを介して各タイプのトラフィックにヒットします。次に、設定されたストームが 10% の場合に、ユニキャスト トラフィックがフィルタリングされる例を示します。

- 着信トラフィックは、不明なユニキャスト 8% + 既知のユニキャスト 7% です。合計 15% のストームは、ハードウェア ポリサーによってハードウェアでフィルタリングされません。
- 着信トラフィックは不明なユニキャスト 11% + 既知のユニキャスト 7% です。合計 18% のストームが不明なユニキャスト トラフィック タイプにヒットし、ハードウェア ポリサーは 11% を超える不明なトラフィックをフィルタリングします。
- 着信トラフィックは不明なユニキャスト 11% + 既知のユニキャスト 11% です。合計 22% のストームが不明なユニキャスト トラフィックと既知のユニキャスト トラフィックにヒットし、ハードウェア ポリサーは両方のユニキャスト トラフィックをフィルタリングします。

（注） インターフェイスで **storm-control unicast** および **storm-control unknown unicast** コマンドの両方を設定しないでください。これら両方のコマンドを設定すると、不明なユニキャストストーム制御値がハードウェアで変更される可能性があります。

トラフィック パターン

T1 から T2、T4 から T5 のタイム インターバルで、転送するブロードキャスト トラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャスト トラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャスト トラフィックが再び転送されます。

ストーム制御抑制レベルと 1 秒間のインターバルを組み合わせて、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が 100% であれば、トラフィックに対する制限はありません。値を 0.0 にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。

（注） パケットは一定の間隔で届くわけではないので、トラフィック アクティビティを測定する 1 秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィックタイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

ハードウェアレートリミッタによるストーム制御

トラフィックストーム制御は、設定された間隔で着信トラフィックレベルをモニターします。ただし、ストームを識別するための統計情報カウンタに基づいているため、ストーム制御にかかる反応時間はやや遅くなります。ハードウェアレートリミッタを使用すると、アクションは ASIC レベルで実行され、その結果ストーム制御アクションは、トラフィックレートが設定されたしきい値レベルに達するとただちに開始されます。ハードウェアレートリミッタには、ブロードキャスト、マルチキャスト、ユニキャスト、および不明なユニキャストトラフィックのポリサーが実装されています。

保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一デバイス上のポート間でレイヤ 2 トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、デバイス上のポート間でユニキャスト、ブロードキャスト、またはマルチキャストトラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャスト トラフィックを転送しません。データ トラフィックはレイヤ 2 の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータ トラフィックは、レイヤ3デバイスを介して転送されなければなりません。
- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

デバイススタックは論理的には 1 つのデバイスを表しているため、レイヤ 2 トラフィックは、スタック内の同一デバイスか異なるデバイスかにかかわらず、デバイススタックの保護ポート間では転送されません。

保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャネルで保護ポートをイネーブルにした場合は、そのポート チャネル グループ内のすべてのポートでイネーブルになります。

デフォルトでは、保護ポートは定義されていません。

ポート ブロッキング

デフォルトでは、デバイスは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャスト トラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャスト トラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャスト パケットが他のポートにフラッディングされないようにします。

（注） マルチキャスト トラフィックでは、ポート ブロッキング機能は純粋なレイヤ 2 パケットだけをブロックします。ヘッダーに IPv4 または IPv6 の情報を含むマルチキャスト パケットはブロックされません。

ポート ベースのトラフィック制御の設定方法

ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィック タイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数 % の差異が生じる可能性があります。

（注） ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

始める前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御を EtherChannel で設定する場合、ストーム制御設定は EtherChannel 物理インターフェイスに伝播します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]} 例： `Device(config-if)# storm-control unicast level 87 65`	ブロードキャスト、マルチキャスト、またはユニキャスト ストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 • *level* には、ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第2位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00 ～ 100.00 です。

	コマンドまたはアクション	目的
		• （任意）*level-low* には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ～ 100.00 です。 しきい値に最大値（100%）を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャスト トラフィックがブロックされます。 • **bps** *bps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをビット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*bps-low* には、下限しきい値レベルをビット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ～ 10000000000.0 です。 • **pps** *pps* には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。上限しきい値に到達すると、ポートはトラフィック

	コマンドまたはアクション	目的
		をブロックします。指定できる範囲は 0.0 ～ 10000000000.0 です。 • （任意）*pps-low* には、下限しきい値レベルをパケット/秒で指定します（小数点第1位まで）。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は **0.0 ～** 10000000000.0 です。 BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号（k、m、gなど）を使用できます。
ステップ 5	**storm-control action** {**shutdown** | **trap**} 例： `Device(config-if)# storm-control action trap`	ストーム検出時に実行するアクションを指定します。ストームが検出されると、**shutdown** または **trap** アクションがすべてのトラフィックに適用されます。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 • ストーム中、ポートを errdisable の状態にするには、**shutdown** キーワードを選択します。 • ストームが検出された場合、SNMP トラップを生成するには、**trap** キーワードを選択します。
ステップ 6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**] 例： `Device# show storm-control gigabitethernet1/0/1 unicast`	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィック タイプを入力しない場合は、すべてのトラフィック タイプ（ブロードキャスト、マルチキャスト、ユニキャスト）の詳細が表示されます。

保護ポートの設定

始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport protected** 例： `Device(config-if)# switchport protected`	インターフェイスを保護ポートとして設定します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

保護ポートの監視

表 *1:* 保護ポートの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたはポートの管理ステータスまたは動作ステータスを、ブロッキングおよびポート保護の設定を含めて表示します。

インターフェイスでのフラッディング トラフィックのブロッキング

始める前に

インターフェイスは物理インターフェイスまたはEtherChannelグループのいずれも可能です。ポート チャネルのマルチキャストまたはユニキャスト トラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	**switchport block multicast** 例： `Device(config-if)# switchport block multicast`	ポートからの未知のマルチキャストの転送をブロックします。
ステップ5	**switchport block unicast** 例： `Device(config-if)# switchport block unicast`	ポートからの未知のユニキャストの転送をブロックします。
ステップ6	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ポート ブロッキングの監視

表 *2:* ポート ブロッキングの設定を表示するコマンド

コマンド	目的
show interfaces [*interface-id*] **switchport**	すべてのスイッチング（非ルーティング）ポートまたはポートの管理ステータスまたは動作ステータスを、ロッキングおよびポート保護の設定を含めて表示しま

ポートベースのトラフィック制御に関するその他の関連資料

関連資料

関連項目	マニュアル タイトル
ポート セキュリティ	『セキュリティ コンフィギュレーション ガイド』の「ポートセキュリティ」

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ポートベースのトラフィック制御の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	ポートベースのトラフィック制御	ポートベースのトラフィック制御は、特定トラフィック状態に応じてポート レベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。