



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の概要 \(1 ページ\)](#)

ポートベースのトラフィック制御の概要

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。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

ストーム制御に関する情報

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。

トラフィック アクティビティの測定方法

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らない限り、スイッチ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。

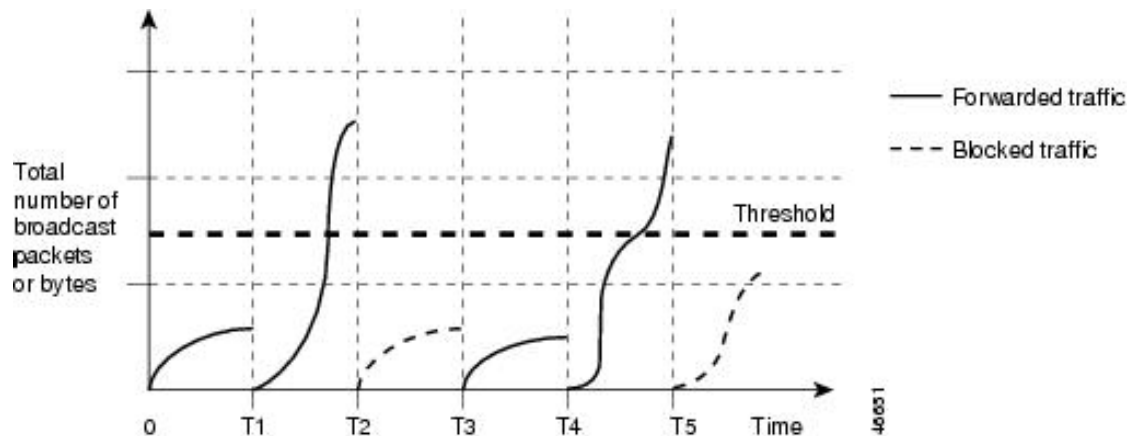


- (注) マルチキャストトラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット (BPDU) および Cisco Discovery Protocol フレームなどの制御トラフィック以外のマルチキャストトラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

トラフィック パターン

図 1: ブロードキャストストーム制御の例

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。



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ると、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。

ストーム制御の設定方法

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> 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： デバイス# 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 <i>interface-id</i> 例： デバイス(config)# interface gigabitethernet1/0/1	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	storm-control { broadcast multicast unicast } level { <i>level</i> [<i>level-low</i>] bps <i>bps</i> [<i>bps-low</i>] pps <i>pps</i> [<i>pps-low</i>]} 例： デバイス(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。 キーワードの意味は次のとおりです。 • <i>level</i> 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。 • (任意) <i>level-low</i> 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

	コマンドまたはアクション	目的
		<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • bps <i>bps</i> 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) <i>bps-low</i> 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 <i>pps</i> 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をブロックします。指定できる範囲は0.0～10000000000.0です。 • (任意) <i>pps-low</i> 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。

	コマンドまたはアクション	目的
		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： デバイス (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。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。 <ul style="list-style-type: none"> • 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： デバイス (config-if) # end	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： デバイス # 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。
ステップ 8	copy running-config startup-config 例： デバイス # copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

保護ポートに関する情報

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、同一スイッチ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、スイッチ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

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。

スイッチスタックは論理的には1つのスイッチを表しているため、レイヤ2トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチスタックの保護ポート間では転送されません。

保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

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 チャン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 チャンネル グループ内のすべてのポートでイネーブルになります。

保護ポートの設定方法

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport protected**
5. **end**
6. **show interfaces *interface-id* switchport**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	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）。

	コマンドまたはアクション	目的
	デバイス> <code>enable</code>	
ステップ 2	configure terminal 例： デバイス# <code>configure terminal</code>	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： デバイス (config)# <code>interface gigabitethernet 1/0/1</code>	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 protected 例： デバイス (config-if)# <code>switchport protected</code>	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： デバイス (config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id switchport 例： デバイス# <code>show interfaces gigabitethernet 1/0/1 switchport</code>	入力を確認します。
ステップ 7	show running-config 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 8	copy running-config startup-config 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

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
<code>show interfaces [interface-id] switchport</code>	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、ブロッキングおよびポート保護の設定を含めて表示

ポート ブロッキングに関する情報

ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 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 ブロッキングの設定方法

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。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport block multicast`
5. `switchport block unicast`

6. **end**
7. **show interfaces interface-id switchport**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> 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： デバイス# 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： デバイス(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： デバイス(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： デバイス(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： デバイス(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show interfaces interface-id switchport 例：	入力を確認します。

	コマンドまたはアクション	目的
	デバイス# <code>show interfaces gigabitethernet 1/0/1 switchport</code>	
ステップ 8	show running-config 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 9	copy running-config startup-config 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

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
<code>show interfaces [interface-id] switchport</code>	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、ブロッキングおよびポート保護の設定を含めて表示

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

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <p>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。</p>	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。