CHAPTER 48

NetFlow データ収集

（注） この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_book.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

NetFlow の前提条件

なし。

NetFlow の制約事項

一般的な NetFlow の制約事項

- CEF テーブル（NetFlow テーブルではない）は、レイヤ 3 スイッチングをハードウェアに実装します。
- NetFlow は、ブリッジド IP トラフィックをサポートしています。
- NetFlow はマルチキャスト IP トラフィックをサポートします。
- NetFlow は **mls ip nat netflow-frag-l4-zero** コマンドをサポートしています。このコマンドは、特定のフロー マスク要件を削除し、NDE 機能と NAT 機能の間の NetFlow マスクの競合を解決します。**mls ip nat netflow-frag-l4-zero** が設定されている場合、PFC は、NAT が適用される前の初期のフラグメント化されたパケットの L4 情報をクリアします。
- デフォルトでは、以降のフラグメントの NAT が最初のフラグメントのレイヤ 4 情報に依存するため、NAT オーバーロードは RP 上でソフトウェアにより初期フラグメントを処理します。初期フラグメントがハードウェアでスイッチングされないようにするため、NAT NetFlow のものとは別のフロー マスクを必要とする 2 個の ACL エントリが NAT の内部インターフェイスに追加されます。初期フラグメントは NAT の内部インターフェイスのフラグメント ACL エントリの 1 つに一致し、別のフロー マスクを使用するため、NetFlow ショートカットに一致せず、ハードウェアでスイッチングされません。NAT の内部インターフェイスに追加された 2 個の追加の ACL エントリは、大きい ACL が NAT の内部インターフェイスに設定されている場合、マージによる巨大化の原因になります。

  mls ip nat netflow-frag-l4-zero コマンドを設定し、フラグメント化されたパケットに関する NetFlow 検索キーからレイヤ 4 ポート情報をゼロに設定できます。その後パケットは、処理のために RP に正しく送信されます。レイヤ 4 ゼロ モードでは、フラグメント化されたパケット（初期フラグメントを含む）は、レイヤ 4 ポート情報がゼロでない NetFlow エントリと一致しません。このモードでは、NAT の 2 つの追加フラグメント エントリは必要ではありません。

  これにより、大規模な ACL が NAT の内部インターフェイスで設定されている場合にマージの失敗の可能性を軽減し、NAT でフラグメント エントリに対する non-interface-full フロー マスクが必要であることが原因で発生する、NAT と NDE などのその他の機能のフロー マスクの矛盾を避けることができます。

  （注） このモードでは、NDE が full または interface-full フロー マスクを使用する場合、フラグメント化されたパケットは正しくカウントされません。同様に、初期フラグメントは、full-flow マスクを使用するマイクロフロー ポリシングを使用した正しいバケットにカウントされません。

- 統計情報は、NetFlow テーブルが満杯になるとスイッチングされるフローには使用できません。
- NetFlow テーブルの使用率が、次の表に示す推奨レベルの使用率を超過すると、統計情報を保存するための十分な領域が不足する確率が高くなります。表 48-1 に、推奨の最大使用率を示します。

表 48-1　NetFlow テーブルの使用率

PFC	推奨される NetFlow テーブルの使用率	NetFlow テーブルの合計容量
PFC3CXL	235,520（230 K）エントリ	262,144（256 K）エントリ
PFC3C	117,760（115 K）エントリ	131,072（128 K）エントリ
PFC3BXL	235,520（230 K）エントリ	262,144（256 K）エントリ
PFC3B	117,760（115 K）エントリ	131,072（128 K）エントリ

次の制限事項は、送信元および宛先の物理インターフェイスおよび MAC アドレスの NetFlow バージョン 9 サポートに適用されます。

- このサポートは、DHCP、IEEE 802.1x ポート ベースの認証、または IP ソース ガードが設定されている場合、コンパイルされた IP デバイス トラッキング データを使用します。
- このサポートは、IP デバイス トラッキング データ容量に制限されます。
- IP デバイスのトラッキング データに特定の IP アドレスのデータまたはエクスポートされた VLAN のデータが含まれていない場合、MAC アドレスまたは物理ポートのエクスポート データはゼロ値になります。
- ホストが ARP 要求を送信しない、または ARP スヌーピングが要求を逃した場合は、MAC アドレスのエクスポート データはゼロ値になります。
- 場合によって、IP デバイスのトラッキング データがスーパーバイザ エンジンとモジュール間の同期から外れた場合に、エクスポートに使用できるデータが正確でないことがあります。
- フロー マスクに送信元および宛先 IP アドレスおよび入力インターフェイスが含まれていない場合、MAC アドレスと物理ポートのエクスポート データはゼロ値になります。
- サポートは、トンネル、プライベート VLAN、アンナンバード インターフェイスにデータを提供しません。

フロー マスクの矛盾

一部の機能は、NetFlow テーブルを使用します。表 48-2 に、各機能のフロー マスク要件を示します。

表 48-2　フロー マスクに対する機能要件

（注） 「Min」は、フロー マスク要件が柔軟であることを示します。より詳細なフロー マスクも動作します。たとえば、「interface-source min」は、interface-source-destination も使用できることを示します。

「Exact」は、フロー マスク要件が柔軟でないことを示します。

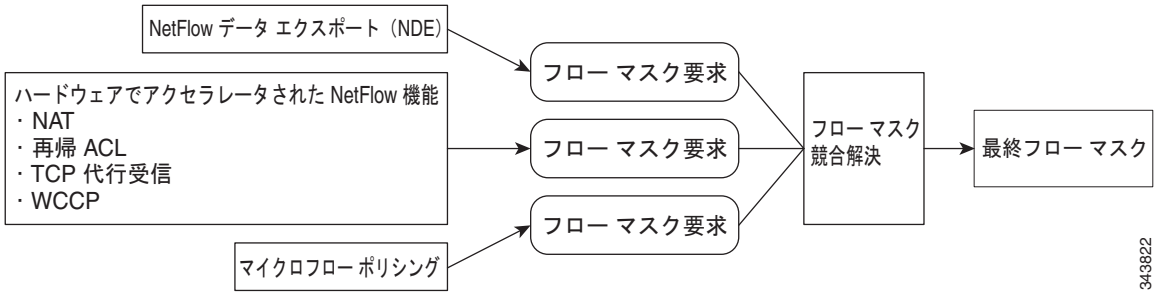
機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
再帰 ACL							Exact	
TCP 代行受信						Min		
Web キャッシュ リダイレクト（WCCP）							Exact	
サーバ ロード バランシング（SLB）						Min		
ネットワーク アドレス変換（NAT）								
• **mls ip nat netflow-frag-l4-zero** なし							Exact	Exact
• **mls ip nat netflow-frag-l4-zero** あり							Exact	
NetFlow データ エクスポート（NDE）								
• **mls flow ip interface-source** あり		Min						
• **mls flow ip interface-destination** あり				Min				
• **mls flow ip interface-destination-source** あり					Min			

表 48-2　フロー マスクに対する機能要件 （続き）

（注）「Min」は、フロー マスク要件が柔軟であることを示します。より詳細なフロー マスクも動作します。たとえば、「interface-source min」は、interface-source-destination も使用できることを示します。

「Exact」は、フロー マスク要件が柔軟でないことを示します。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
• **mls flow ip interface-full** あり							Min	
NetFlow サンプリング							Min	
NetFlow アグリゲーション				Min				
マイクロフロー ポリシング								
• **police flow mask full-flow** あり							Exact	
• **police flow mask src-only** あり	Exact							
• **police flow mask dest-only** あり			Exact					



NetFlow データ エクスポート、ハードウェアでアクセラレートされた NetFlow 機能、およびマイクロフロー ポリサーは、フロー マスクを要求する 3 つの機能カテゴリです。すべてを同時に設定することはできますが、それぞれが要求するフロー マスクによっては、設定が許可される場合とそうでない場合があります。通常、ハードウェアでアクセラレータされた NetFlow 機能のうち 1 つのみがインターフェイスで設定されます。ハードウェアでアクセラレータされた複数の NetFlow 機能が設定されている場合、その中には、フローがこれら複数の機能の影響を受ける場合、ハードウェアでアクセラレートされない可能性があります。

これらの各機能はフロー マスクを要求します。最終的なフロー マスクは他の機能によって異なります。

機能の設定例

（注）
- 「Min」は、フロー マスク要件が柔軟であることを示します。より詳細なフロー マスクも動作します。たとえば、「interface-source min」は、interface-source-destination も使用できることを示します。

- 「Exact」は、フロー マスク要件が柔軟でないことを示します。
- 表 48-2（P.48-3）の情報を使用して、機能間の競合を確認できます。

NAT の「非インターフェイス Full」は NDE の「インターフェイス Full」と競合しますが、NAT の「インターフェイス Full」は NDE の「インターフェイス Full」と競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
ネットワーク アドレス変換（NAT） **mls ip nat netflow-frag-l4-zero** なし							Exact	Exact
NetFlow データ エクスポート（NDE） **mls flow ip interface-full** あり							Min	

NAT の「インターフェイス Full」は NDE の「インターフェイス Full」と競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
ネットワーク アドレス変換（NAT） **mls ip nat netflow-frag-l4-zero** あり							Exact	
NetFlow データ エクスポート（NDE） **mls flow ip interface-full** あり							Min	

NAT の「インターフェイス Full」は NDE の「インターフェイス送信元」と競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
ネットワーク アドレス変換（NAT） **mls ip nat netflow-frag-l4-zero** あり							Exact	
NetFlow データ エクスポート（NDE） **mls flow ip interface-source** あり		Min						

WCCP は NDE の「インターフェイス宛先 送信元」と競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
Web キャッシュ リダイレクト（WCCP）							Exact	
NetFlow データ エクスポート（NDE） **mls flow ip interface-destination-source** あり					Min			

WCCP は NDE の「インターフェイス Full」と競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
Web キャッシュ リダイレクト（WCCP）							Exact	
NetFlow データ エクスポート（NDE） **mls flow ip interface-full** あり							Min	

NDE の「インターフェイス Full」はマイクロフロー ポリシングの「宛先」と競合します。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
NetFlow データ エクスポート（NDE） **mls flow ip interface-full** あり							Min	
マイクロフロー ポリシング **police flow mask dest-only** あり			Exact					

NDE の「インターフェイス Full」はマイクロフロー ポリシングの「インターフェイス Full」と競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
NetFlow データ エクスポート（NDE） **mls flow ip interface-full** あり							Min	
マイクロフロー ポリシング **police flow mask full-flow** あり							Exact	

WCCP、NAT の「インターフェイス Full」と NDE の「インターフェイス Full」は競合しません。

機能	送信元	インターフェイス 送信元	宛先	インターフェイス 宛先	インターフェイス 宛先 送信元	Full	インターフェイス Full	非インターフェイス Full
Web キャッシュ リダイレクト（WCCP）							Exact	
ネットワーク アドレス変換（NAT） **mls ip nat netflow-frag-l4-zero** あり							Exact	
NetFlow データ エクスポート（NDE） **mls flow ip interface-full** あり							Min	

NetFlow について

NetFlow の概要

NetFlow 機能は、スイッチを通って流れるパケットに関するトラフィック統計情報を収集し、NetFlow テーブルに統計情報を保存します。ルート プロセッサ（RP）上の NetFlow テーブルは、ソフトウェアでルーティングされるフローの統計情報をキャプチャし、PFC（および各 DFC）上の NetFlow テーブルは、ハードウェアでルーティングされるフローの統計情報をキャプチャします。

一部の機能は、NetFlow テーブルを使用します。ネットワーク アドレス変換（NAT）などの機能は、NetFlow を使用して、転送結果を変更します。他の機能（Quality of Service（QoS）マイクロフロー ポリシングなど）は、NetFlow テーブルの統計情報を使用して、QoS ポリシーを適用します。NDE 機能は、（NetFlow コレクタと呼ばれる）外部デバイスに統計情報をエクスポートする機能を提供します。

NetFlow は、ルーテッド トラフィックとブリッジド トラフィックの両方の統計情報を収集するように設定できます。

大量の統計情報を収集してエクスポートすると、スイッチ プロセッサ（SP）および RP の CPU 使用率に多大な影響を与えることがあるため、NetFlow には、統計情報量を制御するためのオプションが用意されています。これらのオプションには、次のようなものがあります。

- NetFlow フロー マスクは、測定するフローの細かさを決定します。非常に固有性の高いフロー マスクは、エクスポートするための多数の NetFlow テーブル エントリおよび大量の統計情報を生成します。固有性の低いフロー マスクは、トラフィック統計情報を少数の NetFlow テーブル エントリに集約し、生成する統計情報の量も少なくなります。
- インターフェイス単位の NetFlow により、レイヤ 3 インターフェイス上での NetFlow データ収集をイネーブルまたはディセーブルにできます。
- NetFlow フロー サンプリングは、フロー内のトラフィックのサブセットのデータをエクスポートしますが、これによってエクスポートされる統計情報量を大幅に減らすことができます。NetFlow フロー サンプリングが、収集される統計情報の量を減らすことはありません。
- NetFlow アグリゲーションにより、エクスポートする前に収集した統計情報が結合されます。集約により、エクスポートするレコードの量は減りますが、収集する統計情報の量は減りません。NetFlow アグリゲーションにより、SP の CPU 使用率が増え、コレクタが使用できるデータが減ります。NetFlow アグリゲーションは、NetFlow バージョン 8 を使用します。

NetFlow は 3 つの設定可能タイマーを定義し、テーブルから削除できる失効フローを識別します。NetFlow は、失効エントリを削除し、新しいエントリのためにテーブルのスペースをクリアします。

PFC での NetFlow

PFC の NetFlow テーブルは、ハードウェアでルーティングされるフローの統計情報をキャプチャします。フローとは、送信元と宛先の間での、パケットの単方向ストリームです。フロー マスクは、NetFlow が NetFlow テーブル エントリを照合（または作成）するために使用する着信パケットのフィールドを指定します。

すべてのフロー マスクは、定義に入力インターフェイスを含んでいます。したがって、NetFlow は常にインターフェイス単位をベースに統計情報を収集します。また、NetFlow はインターフェイス単位でイネーブルまたはディセーブルにできます。

PFC は次のフロー マスクをサポートします。

- interface-source：より固有性の低いフロー マスク。各送信元 IP アドレスからのインターフェイスの全入力フローの統計情報は、1 つのエントリに集約されます。
- interface-destination：より固有性の低いフロー マスク。各宛先 IP アドレスへのインターフェイスの全入力フローの統計情報は、1 つのエントリに集約されます。
- interface-destination-source：より固有性の高いフロー マスク。同じ送信元 IP アドレスと宛先 IP アドレスの間のインターフェイスの全入力フローの統計情報は、1 つのエントリに集約されます。
- interface-full：最も固有性の高いフロー マスク。PFC は、インターフェイスの IP フローごとにテーブル エントリを個別に作成し、維持します。interface-full エントリには送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポートが格納されます。

フロー マスクは、収集する統計情報の細かさを決定し、これによって NetFlow テーブルのサイズが制御されます。固有性の低いフロー マスクでは、結果的に NetFlow テーブルのエントリが少なくなり、最も固有性の高いフロー マスクでは、NetFlow エントリが最も多くなります。

たとえば、フロー マスクが interface-source に設定されている場合、NetFlow テーブルには、送信元 IP アドレスごとに 1 つのエントリが含まれます（NetFlow が 1 つのインターフェイス上だけでイネーブルになっている場合を想定）。各送信元からのすべてのフローの統計情報は、1 つのエントリに蓄積されます。ただし、フロー マスクが interface-full に設定されている場合、NetFlow テーブルでは、full flow につき 1 つのエントリが含まれます。送信元 IP アドレスごとに多くのエントリが存在する可能性があるため、NetFlow が大型になることがあります。NetFlow テーブルの容量については、「NetFlow の制約事項」（P.48-1）を参照してください。

RP での NetFlow

RP の NetFlow 機能は、ソフトウェアでルーティングされるフローの統計情報をキャプチャします。RP の NetFlow の設定についての詳細は、『*Cisco IOS NetFlow Configuration Guide*』を参照してください。

NetFlow 機能

インターフェイス単位の NetFlow

インターフェイス単位の NetFlow は、インターフェイス単位で PFC NetFlow データ収集をイネーブルにします。

インターフェイス単位の NetFlow 機能をサポートするソフトウェア リリースにアップグレードするとき、システムは自動的にインターフェイス単位の NetFlow をイネーブルにし、各レイヤ 3 インターフェイス上で **ip flow ingress** コマンドを設定します。この一度だけのアクションは、アップグレード後の最初のリロードの際に行われ、グローバル NetFlow 対応コマンドとの下位互換性を維持します。リロード後には、レイヤ 3 インターフェイス上で **no ip flow ingress** コマンドを設定し、選択的に PFC および RP NetFlow データ収集をディセーブルにできます。

インターフェイス単位の NetFlow 機能は、レイヤ 3 インターフェイス上の IPv4 ユニキャスト フローだけに適用されます。非 IIPv4 プロトコルのフロー（IPv6 および MPLS）は、この機能では制御されません。

NetFlow アグリゲーション

NetFlow は、ハードウェア（PFC）またはソフトウェア（RP）で転送されるパケットの集約をサポートします。これらの機能の詳細については、『*Cisco IOS NetFlow Configuration Guide*』を参照してください。

- NetFlow アグリゲーション スキーム
- NetFlow アグリゲーションの設定
- RP の NetFlow でサポートされる ToS ベースのルータ アグリゲーション

マルチキャスト IP の NetFlow

NetFlow は、ハードウェア（PFC）またはソフトウェア（RP）で転送されるマルチキャスト IP パケットをサポートします。

NetFlow マルチキャストでは、入力アカウンティングおよび出力アカウンティングが提供されます。入力アカウンティングでは、NetFlow が送信元あたり 1 つのフローを作成し、そこにパケット レプリケーションの発生数についての情報を含めます。出力アカウンティングでは、NetFlow が各発信インターフェイスに対して 1 つのフローを作成します。

任意で、NetFlow マルチキャストは、リバース パス失敗（RPF）チェックに失敗したマルチキャスト パケットの統計情報を保持します。

（注）　mls netflow コマンドをグローバルにディセーブルにすると、非 RPF マルチキャスト トラフィックがソフトウェア内でドロップされ、新しい非 RPF Netflow エントリは作成されません。

NetFlow のデフォルト設定

機能	デフォルト値
NetFlow	イネーブル
ルーティングされた IP トラフィックの NetFlow	ディセーブル
入力ブリッジド IP トラフィックの NetFlow	ディセーブル
NetFlow サンプリング	ディセーブル
NetFlow アグリゲーション	ディセーブル
インターフェイス単位の NDE	イネーブル
ACL 拒否トラフィックの除外	ディセーブル（NetFlow は ACL 拒否トラフィックに対してエントリを作成）

NetFlow の設定方法

ここでは、NetFlow の設定手順について説明します。

- 「PFC での NetFlow の設定」（P.48-10）
- 「NetFlow 機能の設定」（P.48-14）

PFC での NetFlow の設定

- 「PFC の NetFlow のイネーブル化」（P.48-11）
- 「MAC アドレスおよび物理インターフェイスのデータ収集のイネーブル化」（P.48-11）
- 「最小 IP MLS フロー マスクの設定」（P.48-12）
- 「MLS エージング タイムの設定」（P.48-12）

- 「PFC Netflow 情報の表示」（P.48-14）

PFC の NetFlow のイネーブル化

PFC で NetFlow 統計情報収集をグローバルにイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# mls netflow`	PFC の NetFlow をイネーブルにします。

PFC で NetFlow 統計情報の収集をディセーブルにする例を示します（デフォルト設定はイネーブル）。

```
Router(config)# no mls netflow
```

MAC アドレスおよび物理インターフェイスのデータ収集のイネーブル化

NetFlow バージョン 9、リリース 15.1SY 以降のリリースでは、レイヤ 2 およびレイヤ 3 ハードウェアスイッチド ユニキャスト IPv4 トラフィックのフローの一部として、送信元および宛先の物理インターフェイスと、送信元および宛先 MAC アドレスをサポートします。次の制約事項を参照してください。

NetFlow MAC アドレスまたは物理インターフェイスのデータ収集をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip flow-capture {mac-addresses | physical-port}`	NetFlow MAC アドレスまたは物理インターフェイスのデータ収集をイネーブルにします。

次に、NetFlow MAC アドレス データ収集をイネーブルにする例を示します。

```
Router(config)# ip flow-capture mac-addresses
```

次に、NetFlow 物理インターフェイス データ収集をイネーブルにする例を示します。

```
Router(config)# ip flow-capture physical-port
```

インターフェイスで NetFlow MAC アドレスまたは物理インターフェイスのデータ エクスポートをイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config-if)# ip flow ingress layer2-information`	NetFlow MAC アドレスまたは物理インターフェイスのデータ収集のエクスポートをイネーブルにします。

次に、NetFlow MAC アドレスまたは物理インターフェイスのデータ エクスポートをイネーブルにする例を示します。

```
Router(config-if)# ip flow ingress layer2-information
```

最小 IP MLS フロー マスクの設定

PFC で NetFlow テーブルに対するフロー マスクの最小特性を設定できます。設定した他の機能がより固有性の高いフロー マスクを必要とする場合、実際のフロー マスクは **mls flow** コマンドで設定したレベルよりも固有性が高くなります（「フロー マスクの矛盾」（P.48-3）を参照）。

最小 IPv4 フロー マスクを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# mls flow ip {interface-source | interface-destination | interface-destination-source | interface-full}`	IPv4 パケットに最小フロー マスクを設定します。

次に、最小フロー マスクを設定する例を示します。

```
Router(config)# mls flow ip interface-destination
```

IP MLS フロー マスクの設定を表示するには、次の作業を行います。

コマンド	目的
`Router# show mls netflow flowmask`	フロー マスクの設定を表示します。

次に、MLS フロー マスクの設定を表示する例を示します。

```
Router# show mls netflow flowmask
current ip flowmask for unicast: if-dst
Router#
```

MLS エージング タイムの設定

MLS エージング タイム（デフォルトは 300 秒）は、すべての NetFlow テーブル エントリに適用されます。normal エージング タイムは、32 ～ 4092 秒の範囲で設定できます。フローは、設定されたインターバルより 4 秒早く、または 4 秒遅く経過する場合があります。フローは、平均して設定値の 2 秒以内に経過します。

ルーティングの変更またはリンク ステートの変化など、エージング以外のイベントによって MLS エントリが削除される場合があります。

（注）　MLS エントリの数が推奨使用率（「NetFlow の制約事項」（P.48-1）を参照）を超えると、一部のフローで隣接統計情報しか使用できなくなる場合があります。

NetFlow テーブル サイズが推奨利用率を超えないように維持するには、**mls aging** コマンドを使用する際、次のパラメータをイネーブルにします。

- **normal**：非アクティブ タイマーを設定します。タイマーに設定した期間内にフローでパケットが受信されなかった場合、フロー エントリはテーブルから削除されます。
- **fast aging**：わずかな数のパケットしかスイッチングせず、その後、再び使用されることのないフローに対して作成されるエントリを、効率的に期限切れにするためのプロセスを設定します。**fast aging** パラメータは、**time** キーワード値を使用して、各フローについて最低でも **threshold** キー

ワード値で指定される数のパケットがスイッチングされているかどうかを調べます。time で指定される時間内に threshold で指定される数のパケットをスイッチングしていないフローについては、このエントリが期限切れになります。

- **long**：指定した時間にわたってアクティブになっていたエントリを、エントリが使用中であっても削除するように設定します。long エージングは、不正確な統計情報の原因となるカウンタ ラップアラウンドを防止するために使用します。

fast aging によって削除される一般的なテーブル エントリは、Domain Name Server（DNS; ドメイン ネーム サーバ）または Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバとやりとりするフローに対するエントリです。

MLS fast エージング タイムをイネーブルにする必要がある場合、最初は 128 秒に設定してください。NetFlow テーブル サイズが増え続け、推奨利用率を超えた場合は、テーブル サイズが推奨利用率未満になるまで設定値を下げます。テーブルが増え続け、推奨利用率を超えた場合は、normal MLS エージング タイムを短くします。

MLS エージング タイムを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **mls aging** {**fast** [**threshold** {*1-128*} | **time** {*1-128*}] | **long** *64-1920* | **normal** *32-4092*}	NetFlow テーブル エントリの MLS エージング タイムを設定します。

次に、MLS エージング タイムを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls aging fast threshold 64 time 30
```

MLS エージング タイムの設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show mls netflow aging**	MLS エージング タイムの設定を表示します。

次に、MLS エージング タイムの設定を表示する例を示します。

```
Router# show mls netflow aging
enable timeout packet threshold
------ ------- ----------------
normal aging true 300 N/A
fast aging true 32 100
long aging true 900 N/A
```

ACL 拒否の除外の設定

デフォルトでは、NetFlow テーブル エントリは、ACL 拒否フローに対して作成されます。これらのフローは、NetFlow テーブルをオーバーフローさせることがあります。NetFlow テーブルから ACL 拒否フローを除外するには、次の作業を行います。

コマンド	目的
Router# **mls exclude acl-deny**	NetFlow テーブルから ACL 拒否フローを除外します。

次に、NetFlow テーブルから ACL 拒否フローを除外する例を示します。

```
Router(config)# mls exclude acl-deny
```

PFC Netflow 情報の表示

PFC での NetFlow についての情報を表示するには、次の作業を行います。

コマンド	目的
`Router(config)# show mls netflow {aggregation | aging | creation | flowmask | ip | ipv6 | mpls | table-contention | usage}`	PFC での NetFlow についての情報を表示します。

NetFlow 機能の設定

NetFlow 機能は、一般的にハードウェア（PFC）またはソフトウェア（RP）で転送されるパケットに適用されます。機能を PFC に適用するには、PFC で NetFlow がイネーブルになっている必要があります。

ここでは、NetFlow 機能の設定手順について説明します。

- 「レイヤ 3 インターフェイスでの NetFlow の設定」（P.48-14）
- 「入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化」（P.48-15）
- 「NetFlow アグリゲーションの設定」（P.48-16）
- 「マルチキャスト IP トラフィックに対する NetFlow の設定」（P.48-17）

レイヤ 3 インターフェイスでの NetFlow の設定

インターフェイス単位の NDE 機能により、ハードウェア（PFC）またはソフトウェア（RP）で転送されるパケットに対して、インターフェイス単位をベースとした NetFlow 収集をイネーブルまたはディセーブルにできます。この機能は、デフォルトでイネーブルにされています。

レイヤ 3 インターフェイスの NetFlow をイネーブルまたはディセーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {vlan vlan_ID} | {type slot/port} | {port-channel port_channel_number}`	設定するレイヤ 3 インターフェイスを選択します。
ステップ 2	`Router(config-if)# ip flow ingress`	指定したインターフェイスの NetFlow をイネーブルにします。NetFlow は、ハードウェア（PFC）またはソフトウェア（RP）で転送されるパケットの統計情報を収集します。
ステップ 3	`Router(config-if)# no ip flow ingress`	指定したインターフェイスの NetFlow をディセーブルにします。NetFlow は、ハードウェア（PFC）またはソフトウェア（RP）で転送されるパケットの統計情報の収集を停止します。

PFC でのインターフェイス単位の NetFlow をサポートするソフトウェア イメージに初めてアップグレードするとき、システムは NetFlow をイネーブルにするように各レイヤ 3 インターフェイスを自動的に設定します（これにより、グローバル **mls netflow** コマンドとの下位互換性を維持します）。この一度だけのアクションは、アップグレード後に初めてシステムが再起動されたときに行われます。このアクションのあと、NetFlow データ収集をディセーブルまたはイネーブルにするように、レイヤ 3 インターフェイスを設定できます。

入力ブリッジド IP トラフィックに対する NetFlow のイネーブル化

NetFlow は、入力ブリッジド IP トラフィックをサポートしています。

（注）

- 入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにすると、NetFlow フロー サンプリング機能によってこの統計情報を使用できます（「NetFlow サンプリング」（P.49-9）を参照）。
- VLAN でブリッジド IP トラフィックに対して NetFlow をイネーブルにするには、対応する VLAN インターフェイスを作成し、**no shutdown** コマンドを入力する必要があります。必要に応じて、**no shutdown** コマンドのあとに **shutdown** コマンドを入力できます。
- レイヤ 3 VLAN の場合、入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにすると、指定した VLAN 上のレイヤ 3 フローに対する NetFlow もイネーブルになります。
- エクスポートされたブリッジド フローには、入力および出力 VLAN 情報が含まれ、物理ポート情報は含まれません。

VLAN 上の入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip flow ingress layer2-switched vlan` *vlan_ID*`[-`*vlan_ID*`] [, `*vlan_ID*`[-`*vlan_ID*`]]`	指定の VLAN 上での入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにします。 （注）　VLAN 上での入力ブリッジド IP トラフィックに対して NetFlow を使用するには、**mls netflow** コマンドを使用して、PFC 上で NetFlow をイネーブルにする必要があります。

次に、VLAN 200 上の入力ブリッジド IP トラフィックに対して NetFlow をイネーブルにする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip flow ingress layer2-switched vlan 200
```

NetFlow アグリゲーションの設定

NetFlow アグリゲーションを設定するには、『*Cisco IOS NetFlow Configuration Guide*』を参照してください。

（注）
- NetFlow アグリゲーションを設定するとき、ハードウェア（PFC）またはソフトウェア（RP）で転送されるパケットに対して自動的に設定されます。
- PFC および DFC では、NetFlow ToS ベースのルータ アグリゲーションをサポートしません。

PFC または DFC の NetFlow アグリゲーション情報を表示するには、次の作業を行います。

コマンド	目的
`Router # show ip cache flow aggregation {as | destination-prefix | prefix | protocol-port | source-prefix) module slot_num`	NetFlow アグリゲーション キャッシュ情報を表示します。
`Router # show mls netflow aggregation flowmask`	NetFlow アグリゲーション フロー マスク情報を表示します。

（注）　PFC および DFC では、NetFlow ToS ベースのルータ アグリゲーションをサポートしません。

次に、NetFlow アグリゲーション キャッシュ情報を表示する例を示します。

```
Router# show ip cache flow aggregation destination-prefix module 1
IPFLOW_DST_PREFIX_AGGREGATION records and statistics for module :1
IP Flow Switching Cache, 278544 bytes
2 active, 4094 inactive, 6 added
236 ager polls, 0 flow alloc failures
Active flows timeout in 30 minutes
Inactive flows timeout in 15 seconds
Dst If Dst Prefix Msk AS Flows Pkts B/Pk Active
Gi7/9 9.1.0.0 /16 0 3003 12M 64 1699.8
Gi7/10 11.1.0.0 /16 0 3000 9873K 64 1699.8
Router#
```

次に、NetFlow アグリゲーション フロー マスク情報を表示する例を示します。

```
Router# show mls netflow aggregation flowmask
 Current flowmask set for netflow aggregation : Vlan Full Flow
 Netflow aggregations configured/enabled :
        AS Aggregation
        PROTOCOL-PORT Aggregation
        SOURCE-PREFIX Aggregation
        DESTINATION-PREFIX Aggregation
Router
```

マルチキャスト IP トラフィックに対する NetFlow の設定

マルチキャスト IP トラフィックに対して NetFlow を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip multicast netflow output-counters`	（任意）入力フローの出力バイト/パケット数の計算をイネーブルにします。
ステップ 2	`Router(config)# ip multicast netflow rpf-failure`	（任意）RPF チェックが失敗したマルチキャスト データの NetFlow をイネーブルにします。
ステップ 3	`Router(config)# interface {vlan vlan_ID} | {type slot/port} | {port-channel port_channel_number}`	設定するレイヤ 3 インターフェイスを選択します。
ステップ 4	`Router(config-if)# ip flow {ingress | egress}`	特定のインターフェイスでの（RP および PFC の）NetFlow マルチキャスト トラフィックをイネーブルにします。 • NetFlow マルチキャスト入力アカウンティングをイネーブルにするには、**ingress** を指定します。 • NetFlow マルチキャスト出力アカウンティングをイネーブルにするには、**egress** を指定します。

マルチキャスト トラフィックの NetFlow の設定についての詳細は、『*Cisco IOS NetFlow Configuration Guide*』の「Configuring NetFlow Multicast Accounting」を参照してください。

「Configuring NetFlow Multicast Accounting」では、マルチキャスト高速スイッチングまたはマルチキャスト ディストリビューティッド ファースト スイッチング（MDFS）を設定するのに必要な前提条件が指定されています。ただし、この前提条件は、15.1SY リリースで NetFlow マルチキャスト サポートを設定するときには適用されません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する