



NetFlow コンフィギュレーションガイド

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティングシステムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、<http://www.cisco.com/go/trademarks> でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



目次

最初にお読みください。 1

「NetFlow および NetFlow データ エクスポートの設定」 3

機能情報の確認 3

NetFlow 集約キャッシュの設定の前提条件 4

NetFlow 集約キャッシュの設定の制限事項 4

NetFlow データ エクスポートの制約事項 4

NetFlow 集約キャッシュの設定に関する情報 5

NetFlow 集約キャッシュ 5

NetFlow 集約キャッシュの利点 5

NetFlow 集約キャッシュ方式 5

NetFlow 集約方式のフィールド 6

NetFlow AS 集約方式 9

NetFlow AS-ToS 集約方式 11

NetFlow 宛先プレフィックス集約方式 13

NetFlow 宛先プレフィックス-ToS 集約方式 15

NetFlow プレフィックス集約方式 17

NetFlow プレフィックス-ポート集約方式 19

NetFlow プレフィックス-ToS 集約方式 22

NetFlow プロトコル ポート集約方式 24

NetFlow プロトコル-ポート-ToS 集約方式 26

NetFlow 送信元プレフィックス集約方式 28

NetFlow 送信元プレフィックス-ToS 集約方式 30

NetFlow 集約キャッシュの NetFlow データ エクスポート フォーマット バージョン 9
および 8 の概要 32

NetFlow 集約キャッシュの設定方法 33

NetFlow 集約キャッシュの設定 33

集約キャッシュの設定の確認 36

NetFlow 集約キャッシュの設定例	39
AS 集約キャッシュの設定例	39
宛先プレフィックス集約キャッシュの設定例	39
プレフィックス集約キャッシュの設定例	40
プロトコル ポート集約キャッシュの設定例	40
送信元プレフィックス集約キャッシュの設定例	40
AS-ToS 集約キャッシュの設定例	41
プレフィックス-ToS 集約キャッシュの設定例	41
プレフィックス集約方式の最小マスクの設定例	41
宛先プレフィックス集約方式の最小マスクの設定例	42
送信元プレフィックス集約方式の最小マスクの設定例	42
集約キャッシュに対する NetFlow バージョン 9 データ エクスポートの設定例	42
その他の参考資料	43
NetFlow 集約キャッシュの設定に関する機能情報	44
用語集	45
NetFlow および NetFlow データ エクスポートの設定	47
機能情報の確認	47
NetFlow および NetFlow データ エクスポートの設定の前提条件	48
NetFlow および NetFlow データ エクスポートの設定の制限事項	48
NetFlow および NetFlow データ エクスポートの設定に関する情報	49
NetFlow データ キャプチャ	49
NetFlow フローのキー フィールド	50
NetFlow キャッシュ管理およびデータ エクスポート	50
NetFlow エクスポート フォーマット バージョン 9	52
NetFlow エクスポート フォーマット バージョン 9 の概要	52
NetFlow エクスポート バージョンのフォーマット	52
NetFlow エクスポート パケット ヘッダーのフォーマット	53
NetFlow フロー レコードおよびエクスポート フォーマットのコンテンツ情報	55
NetFlow データ エクスポート フォーマットの選択	57
NetFlow バージョン 9 データ エクスポート フォーマット	58
出力 NetFlow アカウンティングの利点 : NetFlow アカウンティングの簡素化	59

NetFlow サブインターフェイス サポートの利点：データ収集の微調整	61
NetFlow 複数エクスポート先の利点	61
NetFlow および NetFlow データ エクスポートの設定方法	62
NetFlow の設定	62
NetFlow が動作可能であることの確認と NetFlow 統計情報の表示	63
バージョン9 エクスポート フォーマットを使用する NetFlow データ エクスポートの設定	66
NetFlow データ エクスポートが動作可能であることの確認	69
ルータ上の NetFlow 統計情報の消去	70
NetFlow メイン キャッシュ パラメータのカスタマイズ	71
ルーティング デバイスでの NetFlow キャッシュ エントリの管理	71
NetFlow キャッシュのサイズ	72
NetFlow および NetFlow データ エクスポートの設定例	75
出力 NetFlow アカウンティングの設定例	75
NetFlow サブインターフェイス サポートの設定例	76
サブインターフェイスでの入力（受信）トラフィックに対する NetFlow サブインターフェイス サポート例	76
サブインターフェイスでの出力（送信）トラフィックに対する NetFlow サブインターフェイス サポート例	76
NetFlow 複数エクスポート先の設定例	77
その他の参考資料	77
NetFlow および NetFlow データ エクスポートを設定するための機能情報	79
用語集	81
トラックへのネットワーク トラフィックの NetFlow サンプリングを使用した選択	83
機能情報の確認	84
NetFlow サンプリングを使用したトラックへのネットワーク トラフィックの選択の前提条件	84
NetFlow サンプリングを使用したトラックへのネットワーク トラフィックの選択の制限事項	84
NetFlow サンプリングを使用したトラックへのネットワーク トラフィックの選択	85
NetFlow トラフィックのサンプリング	85
ランダム サンプル NetFlow サンプリング モード	85

ランダム サンプル NetFlow : NetFlow サンプラー	86
NetFlow サンプリングの設定方法	86
NetFlow データ エクスポートの影響を軽減するランダム サンプル NetFlow の設定	86
NetFlow サンプラー マップの定義	86
インターフェイスへの NetFlow サンプラー マップの適用	88
ランダム サンプル NetFlow の設定の確認	89
トラブルシューティングのヒント	91
NetFlow サンプリングの設定例	91
ランダム サンプル NetFlow の設定による NetFlow データ エクスポートの影響の軽減例	91
NetFlow サンプラー マップの定義例	91
NetFlow サンプラー マップのインターフェイスへの適用例	91
その他の参考資料	92
NetFlow サンプリングを使用したトラックへのネットワーク トラフィックの選択の機能情報	94
用語集	96



第 1 章

最初にお読みください。

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE リリース 3.7.0E (Catalyst スイッチ用) および Cisco IOS XE リリース 3.17S (アクセスおよびエッジルーティング用) の2つのリリースは、1つのバージョンの統合されたリリース (Cisco IOS XE 16) へと発展しています。これにより、スイッチングおよびルーティングポートフォリオの幅広い範囲のアクセスおよびエッジ製品に1つのリリースで対応できます。



(注)

技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。



第 2 章

「NetFlow および NetFlow データ エクスポートの設定」

このモジュールでは、NetFlow 集約キャッシュの設定とその手順について説明します。NetFlow のメインキャッシュは、NetFlow によってキャプチャされたデータを格納するために使用されるデフォルト キャッシュです。集約キャッシュと呼ばれる 1 つまたは複数の追加キャッシュを保持することによって、NetFlow 集約機能によるルータでの NetFlow データ エクスポート ストリームの制限付き集約が可能になります。選択した集約方式によって、リモートホストにエクスポートされるデータの種類の種類が決定します。

NetFlow は、ルータを通過するパケットの統計情報を提供する Cisco IOS XE アプリケーションであり、ネットワーク アカウンティングおよびセキュリティの新たな主要テクノロジーになりつつあります。

- [機能情報の確認, 3 ページ](#)
- [NetFlow 集約キャッシュの設定の前提条件, 4 ページ](#)
- [NetFlow 集約キャッシュの設定の制限事項, 4 ページ](#)
- [NetFlow 集約キャッシュの設定に関する情報, 5 ページ](#)
- [NetFlow 集約キャッシュの設定方法, 33 ページ](#)
- [NetFlow 集約キャッシュの設定例, 39 ページ](#)
- [その他の参考資料, 43 ページ](#)
- [NetFlow 集約キャッシュの設定に関する機能情報, 44 ページ](#)
- [用語集, 45 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、[Bug Search Tool](#) およびご使用の

プラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NetFlow 集約キャッシュの設定の前提条件

NetFlow をイネーブルにするには、次の作業を行う必要があります。

- IP ルーティング用にルータを設定する。
- ルータ、およびNetFlowを設定するインターフェイスで、シスコエクスプレスフォーワーディング、高速スイッチングのいずれかがイネーブルであることを確認する。
- NetFlow はメモリおよびCPU リソースを余分に消費するので、ルータで必要とされるリソースを確認する。

集約からの自律システム (AS) 情報が必要であるときに、エクスポートフォーマットのバージョンを設定していない場合は、エクスポート コマンドに **peer-as** または **origin-as** キーワードを必ず指定してください。

集約キャッシュ コンフィギュレーション モードから **enabled** キーワードを入力して、各 NetFlow 集約キャッシュを明示的にイネーブルにする必要があります。

マスキングを最小限にするには、ルータベースの集約をイネーブルにします。

NetFlow 集約キャッシュの設定の制限事項

パフォーマンス上の影響

ip flow egress コマンドを使用して出力 NetFlow アカウンティングを設定すると、アカウンティング関連の追加計算がルータのトラフィック転送パスで発生するので、ネットワーク パフォーマンスが低下する場合があります。

NetFlow データ エクスポートの制約事項

NetFlow バージョン 9 データ エクスポートの制約事項

- 下位互換性：バージョン 9 には、バージョン 5 およびバージョン 8 との下位互換性はありません。バージョン 5 またはバージョン 8 が必要である場合は、そのバージョンを設定する必要があります。

- エクスポートの帯域幅：バージョン 9 のエクスポートではより多くの帯域幅を使用します（テンプレートフローセットのため）。帯域幅使用量の増加は、テンプレートフローセットが送信される頻度によって異なります。デフォルトでは、帯域幅のコストの約 4 パーセントを占める 20 パケットごとにテンプレートが再送信されます。必要に応じて、**ipflow-exporttemplaterefresh-ratepackets** コマンドを使用することにより、再送信レートを下げることができます。
- パフォーマンス上の影響：有効なテンプレートフローセットを生成し、維持するには追加処理が必要であるため、バージョン 9 では全体的なパフォーマンスがわずかに低下します。

NetFlow 集約キャッシュの設定に関する情報

NetFlow 集約キャッシュ

NetFlow 集約キャッシュの利点

エクスポートデータの集約は通常、管理ワークステーションの NetFlow 収集ツールによって実行されます。ルータベースの集約により、ルータで NetFlow エクスポート レコードの制限付き集約を実行することができます。このように、データが NetFlow データ収集システムにエクスポートされる前に、ルータで NetFlow エクスポート データを要約することができます。これには、次のような利点があります。

- ルータとワークステーション間に必要な帯域幅が減少する。
- 必要な収集ワークステーション数が減少する。
- 1 秒あたり高フローのルータでパフォーマンスとスケーラビリティが向上する。

NetFlow 集約キャッシュ方式

Cisco IOS XE NetFlow 集約によって、フィールドがさまざまに組み合わせられた 1 つまたは複数の追加キャッシュが保持されます。これらのフィールドの組み合わせによって、どのフローがグループ化されるかが決まります。これらの追加キャッシュを集約キャッシュと呼びます。集約キャッシュを構成するフィールドの組み合わせを方式と呼びます。

各集約キャッシュには、個別のキャッシュ サイズ、キャッシュ エージェント タイムアウト パラメータ、エクスポート宛先 IP アドレス、およびエクスポート宛先ユーザ データグラム プロトコル (UDP) ポートを設定できます。通常のフロー エージェント プロセスは、メイン キャッシュで実行される場合と同様にアクティブな集約キャッシュごとに実行されます。オンデマンドのエージェントもサポートされています。各集約キャッシュではフィールドがさまざまに組み合わせられており、それによってどのデータ フローをグループ化するかが決定します。デフォルトの集約キャッシュ サイズは 4096 バイトです。

ipflow-aggregationcache コマンドの引数を使用して、キャッシュ集約方式を設定します。NetFlow では、次に示す 5 つの非タイプオブサービス (ToS) ベースのキャッシュ集約方式がサポートされています。

- 自律システム (AS) 集約方式
- 宛先プレフィックス集約方式
- プレフィックス集約方式
- プロトコルポート集約方式
- 送信元プレフィックス集約方式

NetFlow タイプオブサービスベースのルータ集約機能により、集約キャッシュのフィールドの 1 つとしてタイプオブサービス (ToS) が含まれる追加のキャッシュ集約方式がサポートされるようになりました。次に、6 つの ToS ベース集約方式を示します。

- AS-ToS 集約方式
- 宛先プレフィックス-ToS 集約方式
- プレフィックス-ポート集約方式
- プレフィックス-ToS 集約方式
- プロトコル-ポート-ToS 集約方式
- 送信元プレフィックス-ToS 集約方式



(注)

その他のエクスポートフォーマット (バージョン 9 など) もサポートされています。バージョン 9 を使用する場合、フォーマットは図のフォーマットと異なります。バージョン 9 エクスポート形式の詳細については、「NetFlow および NetFlow データ エクスポートの設定」の章を参照してください。

NetFlow 集約方式のフィールド

各キャッシュ集約方式には、他のキャッシュ集約方式とは異なるフィールドの組み合わせがあります。フィールドの組み合わせによって、メインキャッシュのフローが期限切れになったときにどのデータフローをグループ化し、収集するかが決定します。フローとは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、送信元ポートと宛先ポート、タイプオブサービス、およびフローがモニタされる同一インターフェイスなど、共通のフィールドを持つパケットの集合です。ルータでフロー集約を管理するには、データを調べるフィールドをグループ化して収集する集約キャッシュ方式を設定する必要があります。次の 2 つのテーブルに、非 ToS ベースおよび ToS ベースのキャッシュ集約方式でグループ化されて収集される NetFlow フィールドを示します。

次のテーブルに、非 ToS ベース集約方式に使用される NetFlow フィールドを示します。

表 1: 非 ToS ベース集約方式に使用される NetFlow フィールド

フィールド	AS	プロトコル ポート	送信元プレ フィックス	宛先プレ フィックス	プレフィック ス
送信元プレ フィックス			X		X
送信元プレ フィックス マ スク			X		X
宛先プレ フィックス				X	X
宛先プレ フィックス マ スク				X	X
送信元アプリ ケーション ポート		X			
宛先アプリ ケーション ポート		X			
入力インター フェイス	X		X		X
出力インター フェイス	X			X	X
IP プロトコル		X			
送信元 AS	X		X		X
宛先 AS	X			X	X
最初のタイム スタンプ	X	X	X	X	X
最後のタイム スタンプ	X	X	X	X	X
フローの数 ¹	X	X	X	X	X

フィールド	AS	プロトコル ポート	送信元プレ フィックス	宛先プレ フィックス	プレフィック ス
パケット数	X	X	X	X	X
バイト数	X	X	X	X	X

¹ Cisco ASR 1000 シリーズルータの場合、この値は常に 0 になります。これは、Cisco ASR 1000 シリーズルータでは、メイン キャッシュ フロー レコードからエージングアウトしたデータを抽出するのではなく、メイン キャッシュの処理とは無関係に各パケットを確認することによって集約キャッシュが管理されるためです。

次のテーブルに、ToS ベース集約方式に使用される NetFlow フィールドを示します。

表 2: **TOs** ベース集約方式に使用される **NetFlow** フィールド

フィールド	AS-ToS	プロトコル ポート-ToS	送信元プレ フィックス -ToS	宛先プレ フィックス -ToS	プレフィッ クス-ToS	プレフィッ クス-ポート
送信元プレ フィックス			X		X	X
送信元プレ フィックス マスク			X		X	X
宛先プレ フィックス				X	X	X
宛先プレ フィックス マスク				X	X	X
送信元アプ リケーショ ン ポート		X				X
宛先アプ リケーショ ン ポート		X				X
入力イン ターフェイ ス	X	X	X		X	X

フィールド	AS-ToS	プロトコル ポート-ToS	送信元プレ フィックス -ToS	宛先プレ フィックス -ToS	プレフィッ クス-ToS	プレフィッ クス-ポート
出力インターフェイス	X	X		X	X	X
IP プロトコル		X				X
送信元 AS	X		X		X	
宛先 AS	X			X	X	
ToS	X	X	X	X	X	X
最初のタイムスタンプ	X	X	X	X	X	X
最後のタイムスタンプ	X	X	X	X	X	X
フローの数 ²	X	X	X	X	X	X
パケット数	X	X	X	X	X	X
バイト数	X	X	X	X	X	X

- ² Cisco ASR 1000 シリーズ ルータの場合、この値は常に 0 になります。これは、Cisco ASR 1000 シリーズ ルータでは、メイン キャッシュ フロー レコードからエージングアウトしたデータを抽出するのではなく、メイン キャッシュの処理とは無関係に各パケットを確認することによって集約キャッシュが管理されるためです。

NetFlow AS 集約方式

NetFlow AS 集約方式では、NetFlow エクスポート データの量が実質的に減少し、AS 間のトラフィック フロー データが生成されます。この方式では、同一の送信元ボーダー ゲートウェイ プロトコル (BGP) AS、宛先 BGP AS、入力インターフェイス、および出力インターフェイスを持つデータ フローがグループ化されます。

集約された NetFlow データ エクスポート レコードでは、次の情報が報告されます。

- 送信元および宛先 BGP AS
- 集約レコードによって要約されたパケットの数
- 集約レコードによって要約されたフローの数

- 集約レコードによって要約されたバイトの数
- 送信元インターフェイス
- 宛先インターフェイス
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

次の に、AS 集約方式のデータ エクスポート フォーマットを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 1: AS 集約方式のデータ エクスポート フォーマット

0	Flows	
4	Packets	
8	Bytes	
12	First time stamp	
16	Last time stamp	
20	Source AS	Destination AS
24	Source interface	Destination interface

次のテーブルに、AS 集約方式で使用するデータ エクスポート レコードのフィールドの定義を示します。

表 3: AS 集約方式のデータ エクスポート レコード フィールドの定義

フィールド	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間

フィールド	定義
送信元 AS	送信元 IP アドレスの自律システム（ピアまたはオリジン）
宛先 AS	宛先 IP アドレスの自律システム（ピアまたはオリジン）
送信元インターフェイス	入力インターフェイスの SNMP インデックス
宛先インターフェイス	出力インターフェイスの SNMP インデックス

NetFlow AS-ToS 集約方式

NetFlow AS-ToS 集約方式では、送信元 BGP AS、宛先 BGP AS、送信元と宛先のインターフェイス、および ToS バイトが同一のフローがグループ化されます。AS-ToS 集約方式に基づいて集約された NetFlow エクスポート レコードによって、次の情報が報告されます。

- 送信元 BGP AS
- 宛先 BGP AS
- ToS バイト
- 集約レコードによって要約されたフローの数
- この集約レコードによって要約されたバイトの数
- この集約レコードによって要約されたパケットの数
- 送信元と宛先のインターフェイス
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

この集約方式は特に、AS 間のトラフィック フロー データを生成するため、および NetFlow エクスポート データの量を実質的に減少させるために役立ちます。次の図に、AS-ToS 集約方式のデー

タ エクスポート フォーマットを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 2: **AS-ToS** 集約方式のデータ エクスポート フォーマット

0	Flows		
4	Packets		
8	Bytes		
12	First time stamp		
16	Last time stamp		
20	Source AS	Destination AS	
24	Source interface	Destination interface	
28	ToS	PAD	Reserved

次のテーブルに、AS-ToS 集約方式で使用するデータ エクスポート レコードの用語の定義を示します。

表 4: **AS-ToS** 集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
送信元 AS	送信元 IP アドレスの自律システム（ピアまたはオリジン）
宛先 AS	宛先 IP アドレスの自律システム（ピアまたはオリジン）

用語	定義
送信元インターフェイス	入力インターフェイスの SNMP インデックス
宛先インターフェイス	出力インターフェイスの SNMP インデックス
ToS	タイプ オブ サービス バイト
PAD	ゼロ フィールド
予約済み	ゼロ フィールド

NetFlow 宛先プレフィックス集約方式

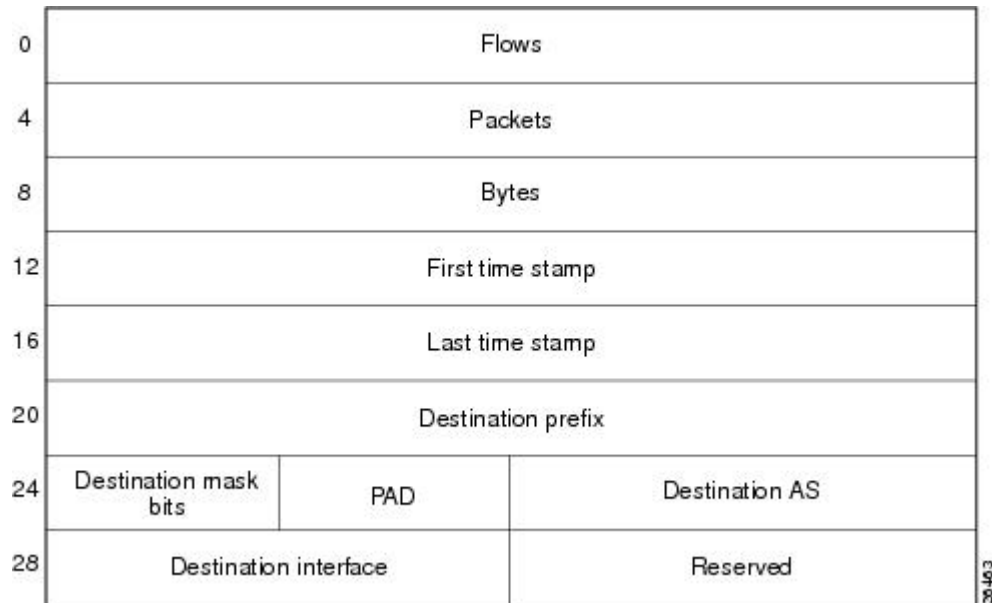
宛先プレフィックス集約方式では、NetFlow 対応デバイスを通過するネットワーク トラフィックの宛先を確認できるよう、データが生成されます。この方式では、同一の宛先プレフィックス、宛先プレフィックス マスク、宛先 BGP AS、および出力インターフェイスを持つデータ フローがグループ化されます。

集約された NetFlow データ エクスポート レコードでは、次の情報が報告されます。

- 宛先プレフィックス
- 宛先プレフィックス マスク
- 宛先 BGP AS
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 出力インターフェイス
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

次の図に、宛先プレフィックス集約方式のデータエクスポートフォーマットを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 3: 宛先プレフィックス集約データ エクスポート レコードのフォーマット



次のテーブルに、宛先プレフィックス集約方式で使用するデータエクスポートレコードの用語の定義を示します。

表 5: 宛先プレフィックス集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
宛先プレフィックス	宛先プレフィックス マスクを使って AND 検索された宛先 IP アドレス
宛先マスク ビット	宛先プレフィックス内のビット数

用語	定義
PAD	ゼロ フィールド
宛先 AS	宛先 IP アドレスの自律システム（ピアまたはオリジン）
宛先インターフェイス	出力インターフェイスの SNMP インデックス
予約済み	ゼロ フィールド

NetFlow 宛先プレフィックス-ToS 集約方式

NetFlow 宛先プレフィックス-ToS 集約方式では、同一の宛先プレフィックス、宛先プレフィックス マスク、宛先 BGP AS、ToS バイト、および出力インターフェイスを持つフローがグループ化されます。集約された NetFlow エクスポート レコードによって、次の情報が報告されます。

- 宛先 IP アドレス
- 宛先プレフィックス マスク
- 宛先 AS
- ToS バイト
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 出力インターフェイス
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

この集約方式は特に、NetFlow 対応デバイスを通過するネットワーク トラフィックの宛先を確認できるデータをキャプチャするために役立ちます。次の図に、宛先プレフィックス-ToS 集約方式

のデータ エクスポート フォーマットを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 4：宛先プレフィックス-**ToS** 集約方式のデータ エクスポート フォーマット

0	Flows		
4	Packets		
8	Bytes		
12	First time stamp		
16	Last time stamp		
20	Destination prefix		
24	Destination mask bits	ToS	Destination AS
28	Destination interface		Reserved

次のテーブルに、宛先プレフィックス-ToS 集約方式で使用するデータ エクスポート レコードの用語の定義を示します。

表 6：宛先プレフィックス-**ToS** 集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
宛先プレフィックス	宛先プレフィックス マスクを使って AND 検索された宛先 IP アドレス
宛先マスク ビット	宛先プレフィックス内のビット数

用語	定義
ToS	タイプ オブ サービス バイト
宛先 AS	宛先 IP アドレスの自律システム（ピアまたはオリジン）
宛先インターフェイス	出力インターフェイスの SNMP インデックス
予約済み	ゼロ フィールド

NetFlow プレフィックス集約方式

NetFlow プレフィックス集約方式では、NetFlow 対応デバイスを通過するネットワークトラフィックの送信元と宛先を確認できるよう、データが生成されます。この方式では、同一の送信元プレフィックス、宛先プレフィックス、送信元プレフィックスマスク、宛先プレフィックスマスク、送信元 BGP AS、宛先 BGP AS、入力インターフェイス、および出力インターフェイスを持つデータフローがグループ化されます。以下の図を参照してください。

集約された NetFlow データ エクスポート レコードでは、次の情報が報告されます。

- 送信元と宛先のプレフィックス
- 送信元と宛先のプレフィックス マスク
- 送信元および宛先 BGP AS
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 入力および出力インターフェイス
- 最初のパケットが交換されるときタイムスタンプと最後のパケットが交換されるときタイムスタンプ

次の図に、プレフィックス集約方式のデータエクスポートフォーマットを示します。集約方式で
使用されるデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 5: プレフィックス集約方式のデータ エクスポート フォーマット

0	Flows		
4	Packets		
8	Bytes		
12	First time stamp		
16	Last time stamp		
20	Source prefix		
24	Destination prefix		
28	Destination mask bits	Source mask bits	Reserved
32	Source AS		Destination AS
36	Source interface		Destination interface

次のテーブルに、プレフィックス集約方式で使用するデータエクスポートレコードの用語の定義を示します。

表 7: プレフィックス集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間

用語	定義
送信元プレフィックス	送信元プレフィックス マスクを使って AND 検索された送信元 IP アドレス、または集約されたフローの送信元 IP アドレスに属するプレフィックス
宛先プレフィックス	宛先プレフィックス マスクを使って AND 検索された宛先 IP アドレス
宛先マスク ビット	宛先プレフィックス内のビット数
送信元マスク ビット	送信元プレフィックス内のビット数
予約済み	ゼロ フィールド
送信元 AS	送信元 IP アドレスの自律システム（ピアまたはオリジン）
宛先 AS	宛先 IP アドレスの自律システム（ピアまたはオリジン）
送信元インターフェイス	入力インターフェイスの SNMP インデックス
宛先インターフェイス	出力インターフェイスの SNMP インデックス

NetFlow プレフィックス-ポート集約方式

NetFlow プレフィックス-ポート集約方式では、共通の送信元プレフィックス、送信元マスク、宛先プレフィックス、宛先マスク、該当する場合は送信元ポートと宛先ポート、入力インターフェイス、出力インターフェイス、プロトコル、および ToS バイトを持つフローがグループ化されます。集約された NetFlow エクスポート レコードによって、次の情報が報告されます。

- 送信元プレフィックス
- 送信元プレフィックス マスク
- 宛先プレフィックス
- 宛先プレフィックス マスク
- 送信元ポート
- 宛先ポート
- 送信元インターフェイス
- 宛先インターフェイス

- プロトコル
- ToS バイト
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

この集約方式は特に、NetFlow 対応デバイスを通過するネットワーク トラフィックの送信元と宛先を確認できるデータをキャプチャするために役立ちます。次の図に、プレフィックス集約方式のデータ エクスポート レコードを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 6: プレフィックス-ポート集約方式のデータ エクスポート レコード

0	Flows			
4	Packets			
8	Bytes			
12	First time stamp			
16	Last time stamp			
20	Source prefix			
24	Destination prefix			
28	Destination mask bits	Source mask bits	ToS	Protocol
32	Source port		Destination port	
36	Source interface		Destination interface	

次のテーブルに、プレフィックス-ポート集約方式で使用するデータ エクスポート レコードの用語の定義を示します。

表 8: プレフィックス-ポート集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
送信元プレフィックス	送信元プレフィックス マスクを使って AND 検索された送信元 IP アドレス、または集約されたフローの送信元 IP アドレスに属するプレフィックス
宛先プレフィックス	宛先プレフィックス マスクを使って AND 検索された宛先 IP アドレス
宛先マスク ビット	宛先プレフィックス内のビット数
送信元マスク ビット	送信元プレフィックス内のビット数
ToS	タイプ オブ サービス バイト
プロトコル	IP プロトコル バイト
送信元ポート	該当する場合は、送信元のユーザデータグラム プロトコル (UDP) または TCP ポート番号
宛先ポート	宛先ユーザ データグラム プロトコル (UDP) または TCP ポート番号
送信元インターフェイス	入力インターフェイスの SNMP インデックス
宛先インターフェイス	出力インターフェイスの SNMP インデックス

NetFlow プレフィックス-ToS 集約方式

NetFlow プレフィックス-ToS 集約方式では、共通の送信元プレフィックス、送信元マスク、宛先プレフィックス、宛先マスク、送信元 BGP AS、宛先 BGP AS、入力インターフェイス、出力インターフェイス、および ToS バイトを持つフローがグループ化されます。集約された NetFlow エクスポート レコードによって、次の情報が報告されます。

- 送信元プレフィックス
- 送信元プレフィックス マスク
- 宛先プレフィックス
- 宛先プレフィックス マスク
- 送信元 AS
- 宛先 AS
- 送信元インターフェイス
- 宛先インターフェイス
- ToS バイト
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

この集約方式は特に、NetFlow 対応デバイスを通過するネットワーク トラフィックの送信元と宛先を確認できるよう、データをキャプチャするために役立ちます。次の図に、プレフィックス-ToS

集約方式のデータ エクスポート フォーマットを示します。集約方式で使用されるデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 7: プレフィックス-*ToS* 集約方式のデータ エクスポート フォーマット

0	Flows			
4	Packets			
8	Bytes			
12	First time stamp			
16	Last time stamp			
20	Source prefix			
24	Destination prefix			
28	Destination mask bits	Source mask bits	ToS	PAD
32	Source AS		Destination AS	
36	Source interface		Destination interface	

次のテーブルに、プレフィックス-ToS 集約方式で使用されるデータ エクスポート レコードの用語の定義を示します。

表 9: プレフィックス-*ToS* 集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間

用語	定義
送信元プレフィックス	送信元プレフィックス マスクを使って AND 検索された送信元 IP アドレス、または集約されたフローの送信元 IP アドレスに属するプレフィックス
宛先プレフィックス	宛先プレフィックス マスクを使って AND 検索された宛先 IP アドレス
宛先マスク ビット	宛先プレフィックス内のビット数
送信元マスク ビット	送信元プレフィックス内のビット数
ToS	タイプ オブ サービス バイト
Pad	ゼロ フィールド
送信元 AS	送信元 IP アドレスの自律システム（ピアまたはオリジン）
宛先 AS	宛先 IP アドレスの自律システム（ピアまたはオリジン）
送信元インターフェイス	入力インターフェイスの SNMP インデックス
宛先インターフェイス	出力インターフェイスの SNMP インデックス

NetFlow プロトコル ポート集約方式

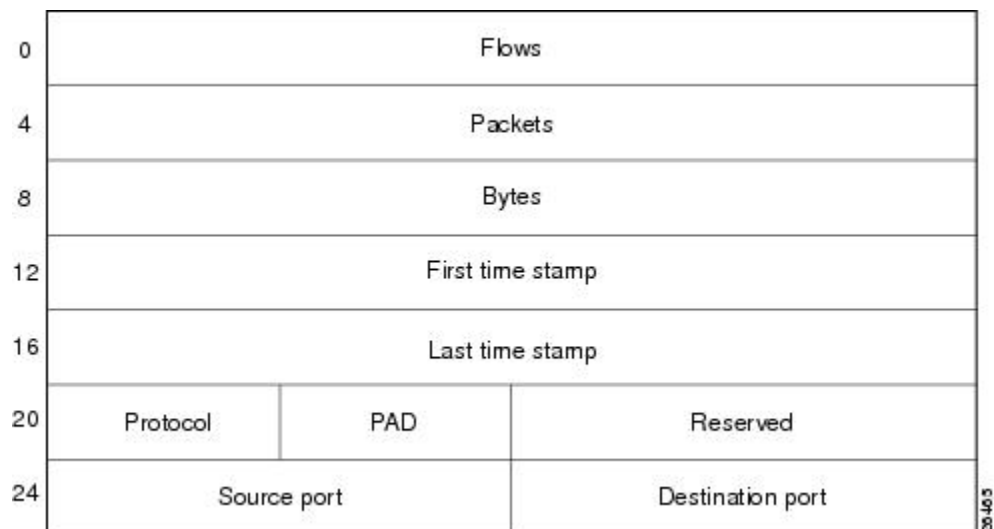
NetFlow プロトコル ポート集約方式では、トラフィック タイプ別にネットワーク使用量を確認できるよう、データがキャプチャされます。この方式では、同一の IP プロトコル、送信元ポート番号、および（該当する場合は）宛先ポート番号を持つデータ フローがグループ化されます。

集約された NetFlow データ エクスポート レコードでは、次の情報が報告されます。

- 送信元と宛先のポート番号
- IP プロトコル（6 = TCP、17 = UDP など）
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

次の図に、プロトコル ポート集約方式のデータ エクスポート フォーマットを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。

図 8: プロトコル ポート集約方式のデータ エクスポート フォーマット



次のテーブルに、プロトコル ポート集約方式で使用するデータ エクスポート レコードの用語の定義を示します。

表 10: プロトコル ポート集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
プロトコル	IP プロトコル バイト
PAD	ゼロ フィールド
予約済み	ゼロ フィールド

用語	定義
送信元ポート	該当する場合は、送信元のユーザデータグラム プロトコル (UDP) または TCP ポート番号
宛先ポート	宛先ユーザ データグラム プロトコル (UDP) または TCP ポート番号

NetFlow プロトコル-ポート-ToS 集約方式

NetFlow プロトコル-ポート-ToS 集約方式では、共通の IP プロトコル、ToS バイト、送信元と（該当する場合は）宛先のポート番号、および送信元と宛先のインターフェイスを持つフローがグループ化されます。集約された NetFlow エクスポート レコードによって、次の情報が報告されます。

- 送信元アプリケーション ポート番号
- 宛先ポート番号
- 送信元と宛先のインターフェイス
- IP プロトコル
- ToS バイト
- 集約レコードによって要約されたフローの数
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

この集約方式は特に、トラフィック タイプ別にネットワーク使用量を確認できるよう、データをキャプチャするために役立ちます。次の図に、プロトコル-ポート-ToS 集約方式のデータ エクス

ポートフォーマットを示します。集約方式で使用するデータエクスポートの用語の定義については、次のテーブルを参照してください。

図 9：プロトコル-ポート-*ToS* 集約方式のデータ エクスポート フォーマット

0	Flows		
4	Packets		
8	Bytes		
12	First time stamp		
16	Last time stamp		
20	Protocol	ToS	Reserved
24	Source port		Destination port
28	Source interface		Destination interface

次のテーブルに、プロトコル-ポート-ToS 集約方式で使用するデータ エクスポート レコードの用語の定義を示します。

表 11：プロトコル-ポート-*ToS* 集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
プロトコル	IP プロトコル バイト
ToS	タイプ オブ サービス バイト
予約済み	ゼロ フィールド

用語	定義
送信元ポート	該当する場合は、送信元のユーザデータグラム プロトコル（UDP）または TCP ポート番号
宛先ポート	宛先ユーザ データグラム プロトコル（UDP） または TCP ポート番号
送信元インターフェイス	入力インターフェイスの SNMP インデックス
宛先インターフェイス	出力インターフェイスの SNMP インデックス

NetFlow 送信元プレフィックス集約方式

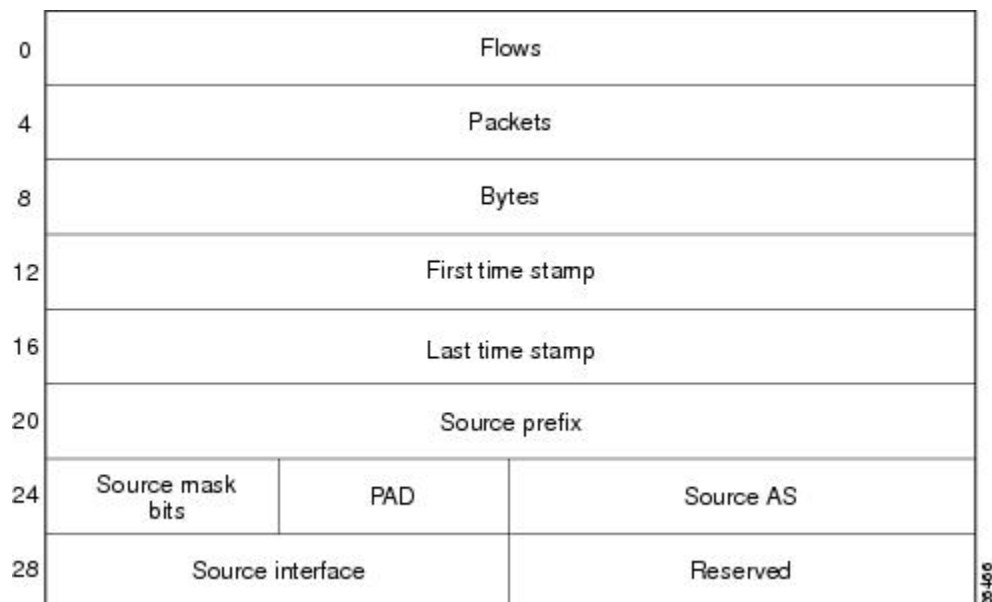
NetFlow 送信元プレフィックス集約方式では、NetFlow 対応デバイスを通過するネットワーク
トラフィックの送信元を確認できるよう、データがキャプチャされます。この方式では、同一の送
信元プレフィックス、送信元プレフィックス マスク、送信元 BGP AS、および入力インターフェ
イスを持つデータ フローがグループ化されます。

集約された NetFlow データ エクスポート レコードでは、次の情報が報告されます。

- 送信元プレフィックス
- 送信元プレフィックス マスク
- 送信元 BGP AS
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 入力インターフェイス
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタ
イムスタンプ

次の図に、送信元プレフィックス集約方式のデータエクスポートフォーマットを示します。集約方式で使用するデータエクスポートの用語の定義については、次のテーブルを参照してください。

図 10：送信元プレフィックス集約方式のデータ エクスポート フォーマット



次のテーブルに、送信元プレフィックス集約方式で使用するデータエクスポートレコードの用語の定義を示します。

表 12：送信元プレフィックス集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間
送信元プレフィックス	送信元プレフィックスマスクを使って AND 検索された送信元 IP アドレス、または集約されたフローの送信元 IP アドレスに属するプレフィックス

用語	定義
送信元マスク ビット	送信元プレフィックス内のビット数
PAD	ゼロ フィールド
送信元 AS	送信元 IP アドレスの自律システム（ピアまたはオリジン）
送信元インターフェイス	入力インターフェイスの SNMP インデックス
予約済み	ゼロ フィールド

NetFlow 送信元プレフィックス-ToS 集約方式

NetFlow 送信元プレフィックス-ToS 集約方式では、共通の送信元プレフィックス、送信元プレフィックス マスク、送信元 BGP AS、ToS バイト、および入力インターフェイスを持つフローがグループ化されます。集約された NetFlow エクスポート レコードによって、次の情報が報告されます。

- 送信元プレフィックス
- 送信元プレフィックス マスク
- 送信元 AS
- ToS バイト
- 集約レコードによって要約されたバイトの数
- 集約レコードによって要約されたパケットの数
- 入力インターフェイス
- 最初のパケットが交換されたときのタイムスタンプと最後のパケットが交換されたときのタイムスタンプ

この集約方式は特に、NetFlow 対応デバイスを通過するネットワーク トラフィックの送信元を確認できるよう、データをキャプチャするために役立ちます。次の図に、送信元プレフィックス-ToS 集約方式のデータ エクスポート フォーマットを示します。集約方式で使用するデータ エクスポートの用語の定義については、次のテーブルを参照してください。



- (注) ルータのフローに送信元 IP アドレスのプレフィックスがない場合、NetFlow では /32 エントリが作成されるのではなく、マスク ビット 0 の 0.0.0.0 が使用されます。これによって、送信元アドレスをランダムに使用する DoS 攻撃による集約キャッシュのスラッシングを防止できます。この動作は、宛先プレフィックス-ToS、プレフィックス-ToS、およびプレフィックス-ポート集約方式の宛先に対しても実行されます。

図 11：送信元プレフィックス-ToS 集約方式のデータ エクスポート フォーマット

0	Flows		
4	Packets		
8	Bytes		
12	First time stamp		
16	Last time stamp		
20	Source prefix		
24	Source mask bits	ToS	Source AS
28	Source interface		Reserved

次のテーブルに、送信元プレフィックス-ToS 集約方式で使用するデータ エクスポート レコードの用語の定義を示します。

表 13：送信元プレフィックス-ToS 集約方式のデータ エクスポート レコードの用語の定義

用語	定義
フロー	集約されたメイン キャッシュ フローの数
Packets	集約されたフロー内のパケットの数
Bytes	集約されたフロー内のバイトの数
最初のタイム スタンプ	最初のパケットが交換されたときのシステム稼働時間
最後のタイム スタンプ	最後のパケットが交換されたときのシステム稼働時間

用語	定義
送信元プレフィックス	送信元プレフィックス マスクを使って AND 検索された送信元 IP アドレス、または集約されたフローの送信元 IP アドレスに属するプレフィックス
送信元マスク ビット	送信元プレフィックス内のビット数
ToS	タイプ オブ サービス バイト
送信元 AS	送信元 IP アドレスの自律システム（ピアまたはオリジン）
送信元インターフェイス	入力インターフェイスの SNMP インデックス
予約済み	ゼロ フィールド

NetFlow 集約キャッシュの NetFlow データ エクスポート フォーマット バージョン 9 および 8 の概要

NetFlow 集約キャッシュに使用できるエクスポート フォーマットは、バージョン 9 エクスポート フォーマットとバージョン 8 エクスポート フォーマットです。

- バージョン 9：新規のフィールドとレコードタイプのサポートに必要な汎用性を備えた、柔軟で拡張性のあるフォーマット。このフォーマットは、マルチキャスト、マルチプロトコル ラベルスイッチング（MPLS）、およびボーダー ゲートウェイ プロトコル（BGP）ネクスト ホップなど、NetFlow をサポートする新しいテクノロジーに対応します。バージョン 9 エクスポート フォーマットの利用により、メイン キャッシュと集約キャッシュに同じバージョンを使用できます。また、このフォーマットには拡張性があるため、今後導入される機能に同じエクスポート フォーマットを使用できます。
- バージョン 8：集約キャッシュからのデータ エクスポートをサポートするために追加されたフォーマット。エクスポート データ グラムには、特定の集約キャッシュ方式に対して有効である通常のバージョン 5 エクスポート データのサブセットが含まれています。データ エクスポートを設定するときは、バージョン 8 が集約キャッシュのデフォルト エクスポート バージョンになります。

バージョン 9 エクスポート フォーマットは柔軟で拡張性があり、新規のフィールドおよびレコードタイプのサポートに必要な汎用性を備えています。メイン キャッシュと集約キャッシュの両方にバージョン 9 エクスポート フォーマットを使用できます。

バージョン 8 エクスポート フォーマットは、集約キャッシュからのデータ エクスポートをサポートするために追加されました。このフォーマットの利用により、キャッシュ集約方式に対して有

効なバージョン5エクスポートデータのサブセットをエクスポートデータグラムに含めることができます。

詳細については、「[NetFlow Data Export; NetFlow データ エクスポート](#)」を参照してください。

NetFlow 集約キャッシュの設定方法

NetFlow 集約キャッシュの設定

NetFlow をイネーブルにして、NetFlow 集約キャッシュを設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `ipflow-aggregationcache {as | as-tos | destination-prefix | destination-prefix-tos | prefix | prefix-port | prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-prefix-tos}`
4. `cacheentriesnumber`
5. `cachetimeoutactiveminutes`
6. `cachetimeoutinactiveseconds`
7. `exportdestination {{ip-address | hostname} udp-port}`
8. 別のエクスポート先を設定するには、ステップ7を繰り返します。
9. `exportversion [9]`
10. `enabled`
11. `exit`
12. `interfaceinterface-typeinterface-number`
13. `ipflow {ingress | egress}`
14. `exit`
15. 他のインターフェイスで NetFlow をイネーブルにするには、ステップ12～14を繰り返します。
16. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	イネーブル化 例： <code>Device> enable</code>	特権 EXEC モードをイネーブルにします。 • 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
ステップ 2	configureterminal 例 : <pre>Device# configure terminal</pre>	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	ipflow-aggregationcache {as as-tos destination-prefix destination-prefix-tos prefix prefix-port prefix-tos protocol-port protocol-port-tos source-prefix source-prefix-tos} 例 : 例 : <pre>Device(config)# ip flow-aggregation cache destination-prefix</pre>	集約キャッシュ方式を指定して、集約キャッシュ コンフィギュレーション モードをイネーブルにします。 <ul style="list-style-type: none"> • as キーワードを入力すると、AS 集約キャッシュが設定されます。 • as-tos キーワードを入力すると、AS ToS 集約キャッシュが設定されます。 • destination-prefix キーワードを入力すると、宛先プレフィックス集約キャッシュが設定されます。 • destination-prefix-tos キーワードを入力すると、宛先プレフィックス ToS 集約キャッシュが設定されます。 • prefix キーワードを入力すると、プレフィックス集約キャッシュが設定されます。 • prefix-port キーワードを入力すると、プレフィックス ポート集約キャッシュが設定されます。 • prefix-tos キーワードを入力すると、プレフィックス ToS 集約キャッシュが設定されます。 • protocol-port キーワードを入力すると、プロトコル ポート集約キャッシュが設定されます。 • protocol-port-tos キーワードを入力すると、プロトコルポート ToS 集約キャッシュが設定されます。 • source-prefix キーワードを入力すると、送信元プレフィックス集約キャッシュが設定されます。 • source-prefix-tos キーワードを入力すると、送信元プレフィックス ToS 集約キャッシュが設定されます。
ステップ 4	cacheentriesnumber 例 : <pre>Device(config-flow-cache)# cache entries 2048</pre>	(任意) 集約キャッシュ運用パラメータを設定します。 <ul style="list-style-type: none"> • entries number のキーワードと引数のペアは、集約キャッシュで可能なキャッシュ エントリの数を示します。範囲は 1024 ~ 2000000 です。デフォルトは 4096 です。

	コマンドまたはアクション	目的
ステップ 5	cachetimeoutactiveminutes 例 : <pre>Device(config-flow-cache)# cache timeout active 15</pre>	(任意) 集約キャッシュ運用パラメータを設定します。 <ul style="list-style-type: none"> • timeout キーワードを入力すると、集約キャッシュ内のセッションが終了します。 • active minutes のキーワードと引数のペアは、エントリがアクティブである分数を示します。範囲は 1 ～ 60 分です。デフォルトは 30 分です。
ステップ 6	cachetimeoutinactiveseconds 例 : <pre>Device(config-flow-cache)# cache timeout inactive 300</pre>	(任意) 集約キャッシュ運用パラメータを設定します。 <ul style="list-style-type: none"> • timeout キーワードを入力すると、集約キャッシュ内のセッションが終了します。 • inactive seconds のキーワードと引数のペアは、集約キャッシュ内の非アクティブなエントリがタイムアウトになるまでの秒数を示します。値の範囲は 10 ～ 600 秒です。デフォルトは 15 秒です。
ステップ 7	exportdestination <i>{{ip-address hostname} udp-port}</i> 例 : <pre>Device(config-flow-cache)# export destination 172.30.0.1 991</pre>	(任意) NetFlow 集約キャッシュからの情報のエクスポートをイネーブルにします。 <ul style="list-style-type: none"> • <i>ip-address hostname</i> 引数は、宛先 IP アドレスまたはホスト名です。 • <i>port</i> 引数は宛先 UDP ポートです。
ステップ 8	別のエクスポート先を設定するには、ステップ 7 を繰り返します。	(任意) NetFlow 集約キャッシュごとに最大 2 つのエクスポート先を設定できます。
ステップ 9	exportversion [9] 例 : <pre>Device(config-flow-cache)# export version 9</pre>	(任意) データ エクスポート フォーマットのバージョンを指定します。 <ul style="list-style-type: none"> • version 9 キーワードは、エクスポート パケットにバージョン 9 フォーマットが使用されることを示します。
ステップ 10	enabled 例 : <pre>Device(config-flow-cache)# enabled</pre>	集約キャッシュをイネーブルにします。
ステップ 11	exit 例 : <pre>Device(config-if)# exit</pre>	NetFlow 集約キャッシュ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 12	interface <i>interface-type</i> interface-number 例 : Device(config)# interface fastethernet 0/0/0	NetFlow をイネーブルに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 13	ipflow {ingress egress} 例 : Device(config-if)# ip flow ingress	インターフェイスで NetFlow をイネーブルにします。 • ingress : インターフェイスで受信中のトラフィックをキャプチャします。 • egress : インターフェイスで送信中のトラフィックをキャプチャします。
ステップ 14	exit 例 : Device(config-if)# exit	(任意) 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、グローバル コンフィギュレーション モードに戻ります。 (注) 別のインターフェイスで NetFlow をイネーブルにする場合だけ、このコマンドを使用します。
ステップ 15	他のインターフェイスで NetFlow をイネーブルにするには、ステップ 12 ~ 14 を繰り返します。	(任意) :
ステップ 16	end 例 : Device(config-if)# end	現在の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。

集約キャッシュの設定の確認

集約キャッシュの設定を確認するには、次のコマンドを使用します。これらのコマンドによって、次のことが可能になります。

- NetFlow 集約キャッシュが動作可能であることを確認する。
- 集約キャッシュの NetFlow データ エクスポートが動作可能であることを確認する。
- 集約キャッシュ統計情報を表示する。

手順の概要

1. イネーブル化
2. `showipcacheflowaggregation {as | as-tos | destination-prefix | destination-prefix-tos | prefix | prefix-port | prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-prefix-tos}`
3. `showipflowexport`
4. `end`

手順の詳細

ステップ 1 イネーブル化

このコマンドを使用して、特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

例：

```
Device>enable
```

```
Device#
```

ステップ 2 `showipcacheflowaggregation {as | as-tos | destination-prefix | destination-prefix-tos | prefix | prefix-port | prefix-tos | protocol-port | protocol-port-tos | source-prefix | source-prefix-tos}`

`showipcacheflowaggregationdestination-prefix` コマンドを使用して、宛先プレフィックス集約キャッシュの設定を確認します。次に例を示します。

例：

```
Device# show ip cache flow aggregation destination-prefix
IP Flow Switching Cache, 139272 bytes
  5 active, 2043 inactive, 9 added
  841 ager polls, 0 flow alloc failures
  Active flows timeout in 15 minutes
  Inactive flows timeout in 300 seconds
IP Sub Flow Cache, 11144 bytes
  5 active, 507 inactive, 9 added, 9 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
Dst If      Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Null        0.0.0.0              /0    0      5     13   52    138.9
Et0/0.1     172.16.6.0           /24   0      1      1   56      0.0
Et1/0.1     172.16.7.0           /24   0      3     31K 1314   187.3
Et0/0.1     172.16.1.0           /24   0     16    104K 1398   188.4
Et1/0.1     172.16.10.0          /24   0      9     99K 1412   183.3
```

`showipcacheverboseflowaggregationsource-prefix` コマンドを使用して、送信元プレフィックス集約キャッシュの設定を確認します。次に例を示します。

例：

```
Device# show ip cache verbose flow aggregation source-prefix
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  51 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
```

```

Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  4 active, 1020 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If      Src Prefix      Msk AS      Flows  Pkts B/Pk  Active
FEt1/0/0.1  172.16.10.0    /24 0         4    35K 1391   67.9
FEt0/0/0.1  172.16.6.0     /24 0         2     5   88    60.6
FEt1/0/0.1  172.16.7.0     /24 0         2   3515 1423   58.6
FEt0/0/0.1  172.16.1.0     /24 0         2    20K 1416   71.9

```

showipcacheverboseflowaggregationprotocol-port コマンドを使用して、プロトコル ポート集約キャッシュの設定を確認します。次に例を示します。

例：

```

Device# show ip cache verbose flow aggregation protocol-port
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  158 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
0x01      0x0000      0x0000      6      52K      1405          104.3
0x11      0x0208      0x0208      1        3         52           56.9
0x01      0x0000      0x0800      2      846      1500          59.8
0x01      0x0000      0x0B01      2       10         56           63.0

```

ステップ3 showipflowexport

showipflowexport コマンドを使用して、集約キャッシュに対する NetFlow データ エクスポートが動作可能であることを確認します。次に例を示します。

例：

```

Device# show ip flow export
Flow export v1 is disabled for main cache
Version 9 flow records
Cache for protocol-port aggregation:
  Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
  Exporting using source IP address 172.16.6.2
Cache for source-prefix aggregation:
  Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
  Exporting using source IP address 172.16.6.2
Cache for destination-prefix aggregation:
  Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
  Exporting using source IP address 172.16.6.2
40 flows exported in 20 udp datagrams
0 flows failed due to lack of export packet
20 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures

```

ステップ4 end

このコマンドを使用して、特権 EXEC モードを終了します。

例：

```
Device# end
```

NetFlow 集約キャッシュの設定例

AS 集約キャッシュの設定例

次に、キャッシュ サイズが 2046、非アクティブ タイムアウトが 200 秒、キャッシュ アクティブ タイムアウトが 45 分、エクスポート宛先 IP アドレスが 10.42.42.1、および宛先ポートが 9992 の AS 集約キャッシュを設定する例を示します。

```
configure terminal
!
ip flow-aggregation cache as
  cache entries 2046
  cache timeout inactive 200
  cache timeout active 45
  export destination 10.42.42.1 9992
  enabled
!
interface FastEthernet0/0/0
  ip flow ingress
!
end
```

宛先プレフィックス集約キャッシュの設定例

次に、キャッシュ サイズが 2046、非アクティブ タイムアウトが 200 秒、キャッシュ アクティブ タイムアウトが 45 分、エクスポート宛先 IP アドレスが 10.42.42.1、および宛先ポートが 9992 の宛先プレフィックス集約キャッシュを設定する例を示します。

```
configure terminal
!
ip flow-aggregation cache destination-prefix
  cache entries 2046
  cache timeout inactive 200
  cache timeout active 45
  export destination 10.42.42.1 9992
  enabled
!
interface FastEthernet0/0/0
  ip flow ingress
!
end
```

プレフィックス集約キャッシュの設定例

次に、キャッシュ サイズが 2046、非アクティブ タイムアウトが 200 秒、キャッシュ アクティブ タイムアウトが 45 分、エクスポート宛先 IP アドレスが 10.42.42.1、および宛先ポートが 9992 のプレフィックス集約キャッシュを設定する例を示します。

```
configure terminal
!
ip flow-aggregation cache prefix
  cache entries 2046
  cache timeout inactive 200
  cache timeout active 45
  export destination 10.42.42.1 9992
  enabled
!
interface FastEthernet0/0/0
  ip flow ingress
!
end
```

プロトコル ポート集約キャッシュの設定例

次に、キャッシュ サイズが 2046、非アクティブ タイムアウトが 200 秒、キャッシュ アクティブ タイムアウトが 45 分、エクスポート宛先 IP アドレスが 10.42.42.1、および宛先ポートが 9992 のプロトコル ポート集約キャッシュを設定する例を示します。

```
configure terminal
!
ip flow-aggregation cache protocol-port
  cache entries 2046
  cache timeout inactive 200
  cache timeout active 45
  export destination 10.42.42.1 9992
  enabled
!
interface FastEthernet0/0/0
  ip flow ingress
!
end
```

送信元プレフィックス集約キャッシュの設定例

次に、キャッシュ サイズが 2046、非アクティブ タイムアウトが 200 秒、キャッシュ アクティブ タイムアウトが 45 分、エクスポート宛先 IP アドレスが 10.42.42.1、および宛先ポートが 9992 の送信元プレフィックス集約キャッシュを設定する例を示します。

```
configure terminal
!
ip flow-aggregation cache source-prefix
  cache entries 2046
```

```
cache timeout inactive 200
cache timeout active 45
export destination 10.42.42.1 9992
enabled
!
interface FastEthernet0/0/0
ip flow ingress
!
end
```

AS-ToS 集約キャッシュの設定例

次に、キャッシュ アクティブ タイムアウトが 20 分、エクスポート先 IP アドレスが 10.2.2.2、および宛先ポートが 9991 の AS-ToS 集約キャッシュの設定例を示します。

```
configure terminal

!

ip flow-aggregation cache as-tos
cache timeout active 20
export destination 10.2.2.2 9991
enabled
!
interface FastEthernet0/0/0
ip flow ingress
!
end
```

プレフィックス-ToS 集約キャッシュの設定例

次に、エクスポート先 IP アドレスが 10.4.4.4 および宛先ポートが 9995 のプレフィックス-ToS 集約キャッシュの設定例を示します。

```
configure terminal

!

ip flow-aggregation cache prefix-tos
export destination 10.4.4.4 9995
enabled
!
interface FastEthernet0/0/0
ip flow ingress
!
end
```

プレフィックス集約方式の最小マスクの設定例

次に、プレフィックス集約方式の最小マスクの設定例を示します。

```
configure terminal

!

ip flow-aggregation cache prefix
mask source minimum 24
mask destination minimum 28
enabled
```

```

!
interface FastEthernet0/0/0
 ip flow ingress
!
end

```

宛先プレフィックス集約方式の最小マスクの設定例

次に、宛先プレフィックス集約方式の最小マスクの設定例を示します。

```

configure terminal

!

ip flow-aggregation cache destination-prefix
 mask destination minimum 32
 enabled
!
interface FastEthernet0/0/0
 ip flow ingress
!
end

```

送信元プレフィックス集約方式の最小マスクの設定例

次に、送信元プレフィックス集約方式の最小マスクの設定例を示します。

```

configure terminal

!

ip flow-aggregation cache source-prefix
 mask source minimum 30
 enabled
!
interface FastEthernet0/0/0
 ip flow ingress
!
end

```

集約キャッシュに対する NetFlow バージョン 9 データ エクスポートの設定例

次に、AS 集約キャッシュ方式に対する NetFlow バージョン 9 データ エクスポートの設定例を示します。

```

configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export template refresh-rate 10
 export version 9
 export template timeout-rate 60
 enabled
!
interface Ethernet0/0
 ip flow ingress

```


!
end

その他の参考資料

関連資料

関連項目	マニュアル タイトル
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』
NetFlow コマンド	『Cisco IOS NetFlow Command Reference』
NetFlow の概要	「 <i>Cisco IOS NetFlow Overview</i> 」
NBAR の概要	<i>NBAR</i> を使用したネットワーク トラフィックの分類
NBAR の設定	「 <i>Configuring NBAR Using the MQC</i> 」
プロトコルディスカバリを使用した NBAR の設定	<i>Protocol Discovery</i> のイネーブル化
ネットワーク トラフィック データのキャプチャとエクスポート	<i>NetFlow</i> および <i>NetFlow</i> データ エクスポートの設定
CNS NetFlow Collection Engine のインストール、開始、および設定に関する情報	Cisco CNS NetFlow Collection Engine のマニュアル

標準および RFC

標準/RFC	タイトル
RFC 5103	『Bidirectional Flow Export Using IP Flow Information Export (IPFIX)』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカルサポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

NetFlow 集約キャッシュの設定に関する機能情報

表 14: NetFlow 集約キャッシュの設定に関する機能情報

機能名	リリース	機能の設定情報
NetFlow ToS-Based Router Aggregation	Cisco IOS XE Release 2.1	<p>NetFlow ToS ベース ルータ集約機能を使用すると、NetFlow エクスポートデータのルータベースのタイプ オブ サービス (ToS) 集約を制限できます。エクスポート データの集約により、収集装置にエクスポート可能な NetFlow エクスポート データが要約されます。その結果、NetFlow エクスポート データの帯域幅要件が減少し、NetFlow データ収集装置のプラットフォーム要件も減少します。</p> <p>この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。</p> <p>この機能により、ipflow-aggregationcache、showipcacheverboseflowaggregation、showipflowexport の各コマンドが変更されました。</p>

機能名	リリース	機能の設定情報
NetFlow Minimum Prefix Mask for Router-Based Aggregation	Cisco IOS XE Release 2.1	<p>NetFlow ルータベース集約の最小プレフィックス マスク機能を利用すると、プレフィックス集約方式、宛先プレフィックス集約方式、および送信元プレフィックス集約方式に最小のマスク サイズを設定できます。</p> <p>この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに導入されました。</p> <p>この機能により、ipflow-aggregationcache、maskdestination、masksource、showipcacheflowaggregation の各コマンドが変更されました。</p>

用語集

BGP : Border Gateway Protocol。Exterior Gateway Protocol (EGP) に置き換わるドメイン間ルーティングプロトコル。BGP システムは到着可能性情報を他の BGP システムと交換します。RFC 1163 によって定義されています。

BGP/MPLS/VPN : IP バックボーンを介して複数のリモートカスタマー サイトが接続できるように、マルチプロトコル ラベル スイッチング (MPLS) およびボーダー ゲートウェイ プロトコル (BGP) を使用したバーチャルプライベート ネットワーク (VPN) ソリューション。詳細については、RFC 2547 を参照してください。

CE ルータ : カスタマー エッジ (CE) ルータ。カスタマー ネットワークの一部であり、プロバイダー エッジ (PE) ルータのインターフェイスとなるルータ。

カスタマー ネットワーク : エンド カスタマーの管理下にあるネットワーク。RFC 1918 に定義されているとおり、カスタマー ネットワークにはプライベート アドレスを使用できます。カスタマー ネットワークは、論理的に個々に、またプライベート ネットワークからも隔離されています。カスタマー ネットワークは C ネットワークとも呼ばれます。

出力 PE : トラフィックがバックボーンから宛先のバーチャルプライベート ネットワーク (VPN) サイトに移動するときに経由するプロバイダー エッジ ルータ。

フロー : 送信元 IP アドレス、宛先 IP アドレス、送信元ポートと宛先ポート、タイプ オブ サービス、およびフローがモニタされるインターフェイスがすべて同一のパケットの集合。入力フローは入力インターフェイスに関連付けられ、出力フローは出力インターフェイスに関連付けられます。

入力 PE：トラフィックがバーチャルプライベート ネットワーク（VPN）サイトからバックボーン（プロバイダー ネットワーク）に移動するときに経由するプロバイダー エッジ ルータ。

ラベル：データ（パケットまたはセル）の転送方法をスイッチング ノードに指示する短い固定長の識別情報。

MPLS：マルチプロトコル ラベル スwitching。通常の方法でルーティングされたパスに沿ったパケット転送（MPLS ホップバイホップ転送とも呼ばれる）の新たな業界標準。

CE ルータ：プロバイダーエッジルータ。カスタマーエッジ（CE）ルータとのインターフェイスを取るプロバイダー ネットワークのエッジのルータ。

プロバイダー ネットワーク：サービス プロバイダーの管理下にあり、カスタマー サイト間の転送を可能にするバックボーンネットワーク。プロバイダー ネットワークは、P ネットワークとも呼ばれます。

VPN：バーチャル プライベート ネットワーク トンネリングを使用し、公衆 TCP/IP ネットワークを通じて IP トラフィックを安全に転送することを可能にするルータ構成。

VRF：プライベート ネットワーク（VPN）Routing/Forwarding（ルーティング/転送）インスタンス。VRF は、MPLS VPN テクノロジーの主要な要素です。VRF は、PE だけに存在します。VRF には VPN ルートが入力されます。VRF により、1 つの PE で複数のルーティング テーブルを使用することが可能です。VPN 内の各 PE で、VPN あたりに 1 つの VRF が必要です。



第 3 章

NetFlow および NetFlow データ エクスポートの設定

このモジュールでは、ネットワーク トラフィック データをキャプチャしてエクスポートするための NetFlow の設定とその手順について説明します。NetFlow のキャプチャとエクスポートは、NetFlow がイネーブルになっている各インターネットワーキングデバイスで個別に実行します。NetFlow がネットワーク内の各ルータで動作可能である必要はありません。NetFlow は、ルータを通過するパケットの統計情報を提供する Cisco IOS XE アプリケーションであり、ネットワーク アカウンティングおよびセキュリティの新たな主要テクノロジーになりつつあります。

- [機能情報の確認, 47 ページ](#)
- [NetFlow および NetFlow データ エクスポートの設定の前提条件, 48 ページ](#)
- [NetFlow および NetFlow データ エクスポートの設定の制限事項, 48 ページ](#)
- [NetFlow および NetFlow データ エクスポートの設定に関する情報, 49 ページ](#)
- [NetFlow および NetFlow データ エクスポートの設定方法, 62 ページ](#)
- [NetFlow および NetFlow データ エクスポートの設定例, 75 ページ](#)
- [その他の参考資料, 77 ページ](#)
- [NetFlow および NetFlow データ エクスポートを設定するための機能情報, 79 ページ](#)
- [用語集, 81 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、[Bug Search Tool](#) およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NetFlow および NetFlow データ エクスポートの設定の前提条件

NetFlow をイネーブルにするには、次の作業を行う必要があります。

- IP ルーティング用にルータを設定する。
- ルータ、および NetFlow を設定するインターフェイスでシスコ エクスプレス フォワーディング (CEF)、分散 CEF、高速スイッチングのいずれかがイネーブルであることを確認する。
- NetFlow はメモリおよび CPU リソースを余分に消費するので、ルータで必要とされるリソースを確認する。

NetFlow および NetFlow データ エクスポートの設定の制限事項

NetFlow キャッシュのプリセットサイズ

NetFlow は、メモリを余分に消費します。メモリの制約がある場合は、エントリ数が減るように NetFlow のサイズをプリセットすることもできます。デフォルトのキャッシュ サイズはプラットフォームによって異なります。

Cisco IOS XE Release 2.1 以降のリリースの出力 NetFlow アカウンティング

出力 NetFlow アカウンティング機能では、IP トラフィックの NetFlow 統計情報だけがキャプチャされます。マルチプロトコル ラベル スwitching (MPLS) 統計情報はキャプチャされません。出力 NetFlow アカウンティング機能をプロバイダー エッジ (PE) ルータで使用するにより、MPLS パケットとしてルータに到着し、ラベルのディスポジションが実行された出力 IP パケットに関する IP トラフィック フロー情報をキャプチャできます。

出力 NetFlow アカウンティングでは、アカウンティング関連の追加計算がルータのトラフィック 転送パスで発生するので、ネットワーク パフォーマンスが低下する場合があります。

ローカルに生成されたトラフィック（出力 NetFlow アカウンティング機能が設定されているルータによって生成されるトラフィック）は、出力 NetFlow アカウンティング機能のフロートラフィックとしてカウントされません。



(注) IPv4 パケットは、ルータを出るときに出力 NetFlow によってキャプチャされます。

NetFlow バージョン 9 データ エクスポートの制約事項

- 下位互換性：バージョン 9 には、バージョン 5 およびバージョン 8 との下位互換性はありません。
- エクスポートの帯域幅：バージョン 9 のエクスポートではより多くの帯域幅を使用します（テンプレートフローセットのため）。バージョン 5 と比較した場合の帯域幅使用量の増加は、テンプレートフローセットが送信される頻度によって異なります。デフォルトでは、帯域幅のコストの約 4 パーセントを占める 20 パケットごとにテンプレートが再送信されます。必要に応じて、**ip flow-export template refresh-rate packets** コマンドを使用することにより、再送信レートを下げることができます。
- パフォーマンス上の影響：有効なテンプレートフローセットを生成し、維持するには追加処理が必要であるため、バージョン 9 では全体的なパフォーマンスがわずかに低下します。
- 管理インターフェイス：NetFlow データ エクスポートは、管理インターフェイス ポートからはサポートされていません。

ポリシーベース ルーティングと NetFlow データ エクスポート

ローカル ポリシーが設定されると、アグリゲーション サービス ルータ（ASR）は挿入されたパケットを確認して、そのパケットにポリシーベース ルーティング（PBR）を適用します。NetFlow データ エクスポート（NDE）パケットが Cisco Express Forwarding ルックアップ中にデータ パスに挿入された場合、PBR ローカル ポリシーは NDE パケットに適用されません。この場合、ASR の NDE 機能は PBR では動作しません。

NetFlow および NetFlow データ エクスポートの設定に関する情報

NetFlow データ キャプチャ

NetFlow では、入力と出力の両方の IP パケットに対してパケットフローが識別されます。接続確立のプロトコルは含まれません。NetFlow は、既存のネットワーク（端末、アプリケーション ソフトウェア、LAN スイッチなどのネットワーク デバイスを含む）に対して完全に透過的です。また、NetFlow のキャプチャおよびエクスポートは、各インターネットワーキング デバイス上で独立して実行されます。したがって、NetFlow は、ネットワーク内の各ルータ上で動作可能である必要はありません。

NetFlow は、ほとんどのインターフェイス タイプおよびレイヤ 2 カプセル化にわたって IP トラフィックおよび IP カプセル化トラフィックに対してサポートされています。

NetFlow 統計情報を表示およびクリアできます。NetFlow 統計情報は、IP パケット サイズ分布、IP フロー スwitching キャッシュ情報、およびフロー情報で構成されます。

NetFlow フローのキー フィールド

ネットワークフローは、所定の送信元から宛先までの単方向のパケットストリームとして識別されます。送信元と宛先はいずれもネットワーク層のIPアドレスと、トランスポート層の送信元および宛先ポート番号によって定義されます。具体的には、フローは次のキー フィールドの組み合わせで識別されます。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート番号
- 宛先ポート番号
- レイヤ3 プロトコル タイプ
- タイプ オブ サービス (ToS)
- 入力論理インターフェイス

これらの7つのキー フィールドにより、一意のフローを定義します。パケットのキー フィールドが1つでも別のパケットと異なる場合は、それぞれ別のフローに属するものと見なされます。フローに含まれるその他のアカウントフィールド (NetFlow エクスポート バージョン 5 フロー フォーマットの自律システム番号など) は、設定しているエクスポート レコード バージョンによって異なります。フローは NetFlow キャッシュに格納されます。

NetFlow キャッシュ管理およびデータ エクスポート

NetFlow の主要コンポーネントは、IP フロー情報を格納する NetFlow キャッシュまたはデータ ソースと、NetFlow データをネットワーク管理コレクタ (NetFlow Collection Engine など) に送信する NetFlow エクスポートまたはトランスポート メカニズムです。NetFlow は、アクティブフローごとに NetFlow キャッシュ エントリ (フロー レコード) を作成することによって動作します。フロー レコードは、アクティブフローごとに NetFlow キャッシュ内に保持されます。NetFlow キャッシュ内の各フロー レコードには、後から NetFlow Collection Engine などの収集装置にエクスポートできるフィールドが含まれています。

NetFlow は非常に効率性が高く、ルータで交換されるトラフィックの約 1.5 パーセントがエクスポートデータとなります。NetFlow では、すべてのパケットが計上され (サンプルモード以外)、ルータまたはスイッチに到達したすべてのネットワーク トラフィックが高い要約率で詳細に表示されます。

NetFlow 対応スイッチングのスケラビリティとパフォーマンスを高めるには高度なフロー キャッシュ管理が必要であり、特に同時の短期フローを大量に処理する密度と使用頻度の高いエッジ ルータにとって重要です。NetFlow キャッシュ管理ソフトウェアには、パケットが既存フローの一部であるかどうか、または新規のフロー キャッシュ エントリを生成すべきかどうかを効率的に判断するための高度なアルゴリズムが揃っています。また、このアルゴリズムでは、NetFlow

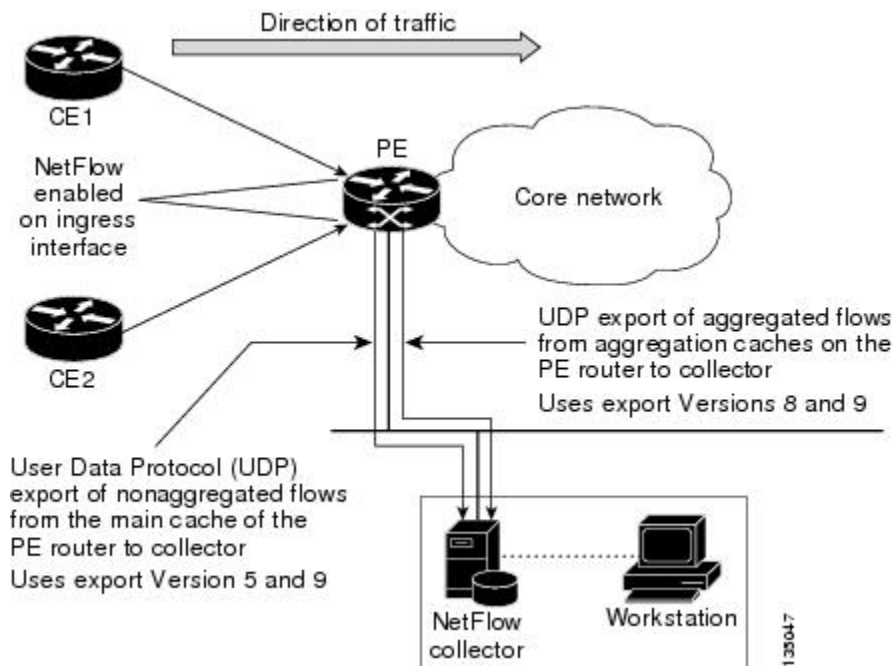
キャッシュに存在するフローごとのアカウントリング測定を動的に更新して、キャッシュ エージング/フローの期限切れを決定する能力があります。

期限切れの NetFlow キャッシュ エントリについては、次のルールが適用されます。

- 指定の時間、アイドル状態であったフローは期限切れとなり、キャッシュから削除されます。
- 長時間存続していたフローは期限切れとなり、キャッシュから削除されます（デフォルトでは、フローの存続可能時間は 30 分です。基礎をなすパケット カンバセーションが中断されることはありません）。
- キャッシュがいっぱいになると、フロー グループの積極的なエージングを同時に行うため、多数のヒューリスティックが適用されます。

期限切れとなったフローは「NetFlow エクスポート」データグラムにグループ化されて、NetFlow 対応デバイスからのエクスポートが可能になります。NetFlow 機能は、インターフェイス単位で設定します。NetFlow エクスポート機能を設定するには、Cisco NetFlow またはサードパーティ製のフロー コレクタの IP アドレスとアプリケーション ポート番号を指定する必要があります。フロー コレクタとは、NetFlow エクスポート データのフィルタリングおよび集約機能を行うデバイスです。次の図に、メイン キャッシュ および 集約 キャッシュ から コレクタ への NetFlow データ エクスポートの例を示します。

図 12: メイン キャッシュ および 集約 キャッシュ からの NetFlow データ エクスポート



NetFlow エクスポート フォーマット バージョン 9

ここでは、NetFlow データ エクスポート フォーマットのバージョン 9 についてさらに詳しく説明します。

NetFlow エクスポート フォーマット バージョン 9 の概要

NetFlow では、エクスポート形式バージョン 9 フォーマットの UDP データグラムにデータがエクスポートされます。

バージョン 9 は、新規のフィールドとレコードタイプのサポートに必要な汎用性を備えた、柔軟で拡張性のあるフォーマットです。バージョン 9 エクスポート フォーマットの利用により、メインキャッシュと集約キャッシュに同じバージョンを使用できます。また、このフォーマットには拡張性があるため、今後導入される機能に同じエクスポート フォーマットを使用できます。

NetFlow エクスポート バージョンのフォーマット

どのエクスポートバージョンでも、NetFlow エクスポート データグラムはヘッダーとフロー レコードのシーケンスで構成されます。ヘッダーには、シーケンス番号、レコードカウント、システム動作時間などの情報が含まれています。フロー レコードには、IP アドレス、ポート、ルーティング情報などのフロー情報が含まれます。

NetFlow バージョン 9 エクスポート フォーマットは、最新の NetFlow エクスポート フォーマットです。NetFlow Version 9 エクスポート フォーマットの識別機能は、テンプレートがベースとなります。テンプレートにより、レコードフォーマットが拡張可能になります。この機能を使用することで、基本的なフローレコードフォーマットを同時に変更することなく、将来的に NetFlow を拡張することができます。

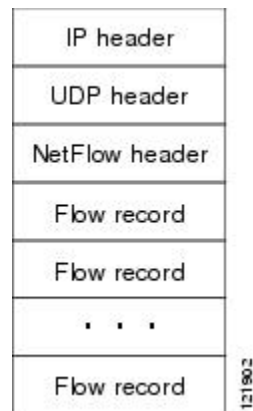
NetFlow バージョン 9 エクスポート フォーマットでテンプレートを使用すると、他にも次のような主要な利点があります。

- レイヤ 2～7 の情報、ルーティング情報、IP バージョン 6 (IPv6)、IP バージョン 4 (IPv4)、およびマルチキャスト情報といった、ルータまたはスイッチのほとんどの情報をエクスポートできます。この新しい情報により、新たなエクスポートデータの活用とネットワーク動作の表示が可能になります。
- NetFlow のコレクタを提供したり、サービスを表示したりするアプリケーションを作成するサードパーティ ビジネス パートナーは、新規の NetFlow エクスポート フィールドが追加されるたびにアプリケーションを再コンパイルする必要はありません。代わりに、既知のテンプレートフォーマットを記述する外部のデータ ファイルを使用することができます。
- 現在の実装を中断することなく、より短時間で NetFlow に新しい機能を追加できます。

IETF IP、Information Export (IPFIX) ワーキング グループ (WG)、および IETF パケット サンプリング (PSAMP) WG の動作は、NetFlow バージョン 9 のエクスポート フォーマットに基づきます。

次の図に、NetFlow の固定形式のエクスポート バージョン 7 に使用される一般的なデータグラムを示します。

図 13: NetFlow の固定フォーマットのエクスポート バージョン 7

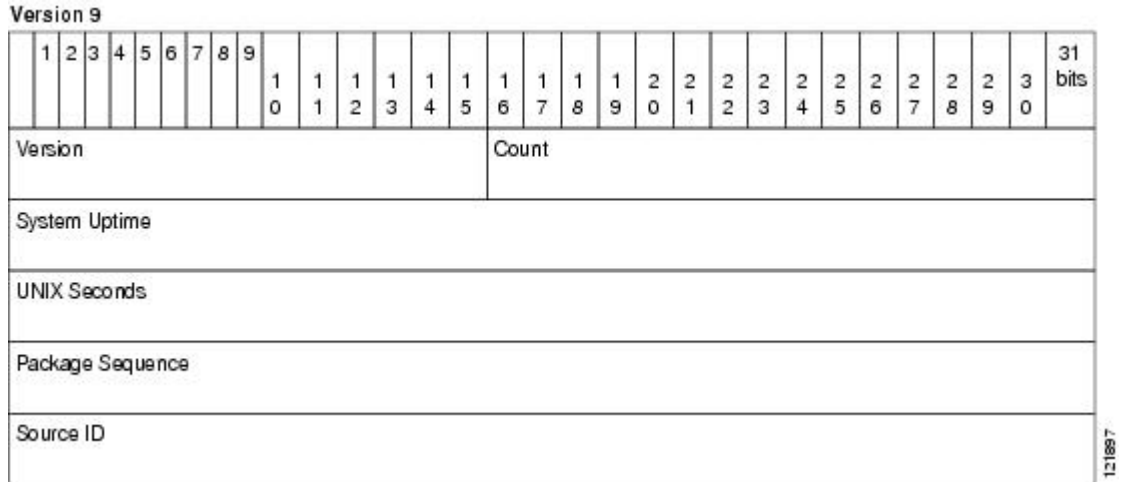


NetFlow エクスポート パケット ヘッダーのフォーマット

5 つのすべてのエクスポート バージョンで、データグラムはヘッダーと 1 つまたは複数のフローレコードによって構成されます。ヘッダーの最初のフィールドには、エクスポート データグラムのバージョン番号が定義されます。通常、すべてのフォーマット バージョンに対応する受信アプリケーションでは、任意のフォーマット バージョンからの最大限のデータグラムを格納するのに十分な大きさのバッファが割り当てられ、ヘッダーを使用してデータグラムの解釈方法が判断されます。ヘッダーの 2 番目のフィールドには、データグラム内のレコード数が定義されます（このデータグラムによって表される期限切れフローの数を示します）。NetFlow エクスポート バージョン 9 のデータグラム ヘッダーには、データグラムの損失を確認するために NetFlow コレクタで使用する「シーケンス番号」のフィールドも含まれます。

図 3 に、NetFlow バージョン 9 エクスポート パケット ヘッダー フォーマットを示します。

図 14 : NetFlow バージョン 9 エクスポート パケット ヘッダーのフォーマット



次のテーブルに、NetFlow バージョン 9 エクスポート パケット ヘッダーのフィールド名と説明を示します。

表 15 : NetFlow バージョン 9 エクスポート パケット ヘッダーのフィールド名および説明

フィールド名	説明
Version	このパケットでエクスポートされる NetFlow レコードのバージョン。バージョン 9 の場合、この値は 0x0009 になります。
Count	このパケット内に含まれる FlowSet レコード（テンプレートおよびデータ）の数。
System Uptime	このデバイスが最初に起動されてからの経過時間（ミリ秒）。
UNIX Seconds	0000 協定世界時（UTC）1970 以降の秒数。
パッケージ シーケンス	このエクスポートデバイスにより送信されたすべてのエクスポートパケットのインクリメンタル シーケンス カウンタ。この値は累積値であり、ミスされたエクスポートパケットがあるか調べるために使用できます。

フィールド名	説明
送信元 ID	Source ID フィールドは 32 ビットの値であり、特定のデバイスからエクスポートされた各フローの固有性を保証するために使用されますこのフィールドの形式はベンダー固有です。シスコの実装においては、最初の 2 つのバイトは将来の拡張用に予約されており、常に 0 です。バイト 3 は、エクスポート側デバイスのルーティングエンジンに関する固有性を提供します。バイト 4 は、エクスポート側デバイスの特定のラインカードまたは Versatile Interface Processor に関する固有性を提供します。コレクタデバイスは、送信元 IP アドレスと送信元 ID フィールドを組み合わせて使用して、着信した NetFlow エクスポート パケットを特定デバイス上の NetFlow の固有インスタンスと関連付ける必要があります。

NetFlow フロー レコードおよびエクスポート フォーマットのコンテンツ情報

ここでは、シスコのエクスポート フォーマット フロー レコードの詳細を示します。次のテーブルに、バージョン 9 に使用できるフロー レコードフォーマットのフィールドを示します。（Y は、そのフィールドが使用できることを示します。N は、そのフィールドが使用できないことを示します）。

表 16: フォーマット バージョン 9 の NetFlow フロー レコード フォーマットのフィールド

フィールド	バージョン 9
送信元 IP アドレス	Y
宛先 IP アドレス	Y
送信元 TCP/UDP アプリケーション ポート	Y
宛先 TCP/UDP アプリケーション ポート	Y
ネクスト ホップ ルータ IP アドレス	Y
入力物理インターフェイス インデックス	Y
出力物理インターフェイス インデックス	Y
このフローのパケット数	Y

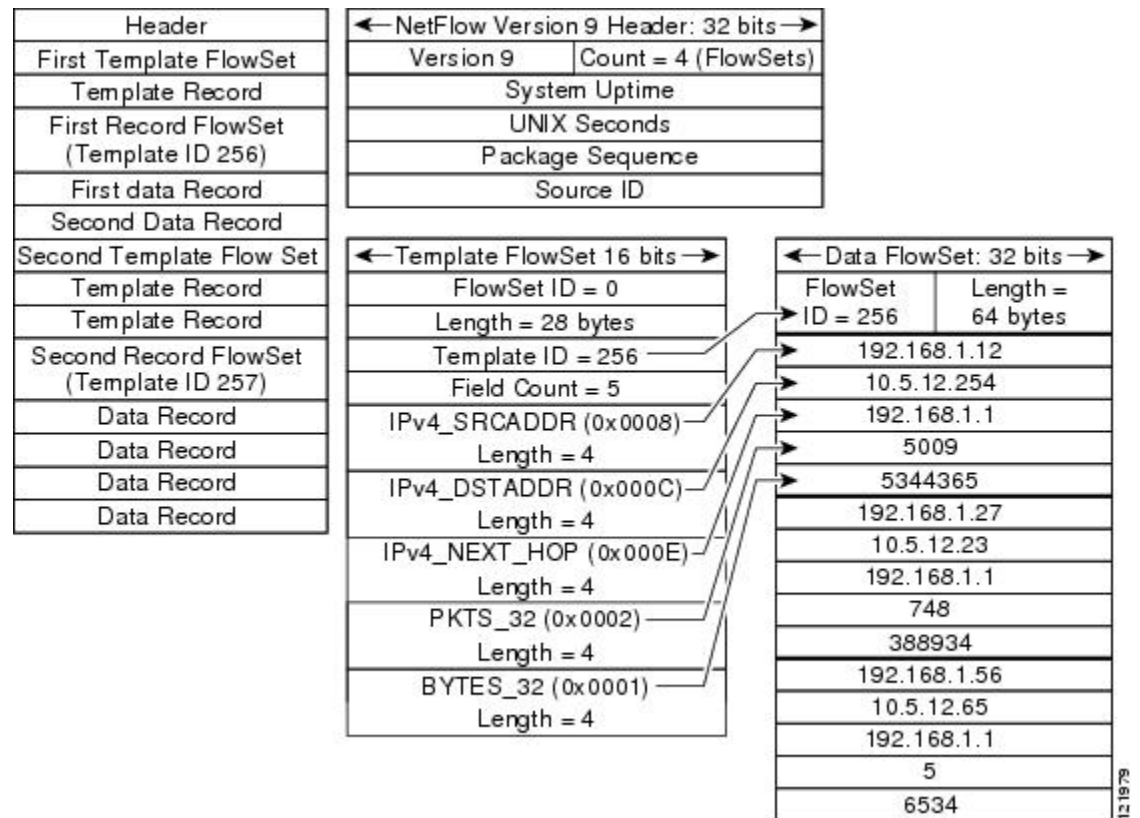
フィールド	バージョン 9
このフローのバイト数	Y
フロー タイムスタンプの開始	Y
フロー タイムスタンプの終了	Y
IP プロトコル (例 : TCP=6、UDP=17)	Y
タイプ オブ サービス (ToS) バイト	Y
TCP フラグ (TCP フラグの累積 OR)	Y
送信元 AS 番号	Y
宛先 AS 番号	Y
送信元サブネット マスク	Y
宛先サブネット マスク	Y
フラグ (複数のフローのうち、どのフローが無効であるかを示します)	Y
その他のフロー フィールド ³	Y

³ バージョン 9 エクスポート フォーマットで利用できるその他のフロー フィールドのリストについては、図 5 を参照してください。

次の図に、バージョン 9 エクスポート フォーマットの一般的なフロー レコードを示します。NetFlow バージョン 9 エクスポート レコード フォーマットは、従来の NetFlow の固定フォーマット エクスポート レコードとは異なります。NetFlow バージョン 9 では、テンプレートにより NetFlow データが説明され、フロー セットに実際のデータが含まれます。このため、柔軟なエク

サポートが実現します。バージョン 9 の現在のフィールドの詳細については、『[NetFlow Version 9 Flow-Record Format](#)』を参照してください。

図 15: NetFlow バージョン 9 エクスポート パケットの例



すべてのエクスポートバージョンについて、最近期限切れとなったフローの数があらかじめ決められた最大数に達するか、1 秒おきのいずれか先に発生するタイミングで NetFlow データ エクスポート パケットを送信する宛先 (NetFlow Collection Engine を実行するワークステーションなど) を指定します。

バージョン 9 のフローレコード形式、データタイプ、およびエクスポートデータフィールドと、該当する場合はプラットフォーム固有の情報については、『[NetFlow Solutions Service Guide](#)』の付録 2 を参照してください。

NetFlow データ エクスポート フォーマットの選択

NetFlow では、エクスポート形式バージョン 9 の UDP データグラムにデータがエクスポートされます。マルチキャスト、DoS、IPv6 などの各種テクノロジーからデータをエクスポートする必要があります。バージョン 9 エクスポートフォーマットでは、メインキャッシュと集約キャッシュからのエクスポートがサポートされます。

NetFlow バージョン 9 データ エクスポート フォーマット

NetFlow バージョン 9 データ エクスポートでは、シスコ エクスプレス フォワーディング スイッチングおよび高速スイッチングがサポートされます。

NetFlow バージョン 9 は、ネットワーク ノードからコレクタに NetFlow レコードを送信するための柔軟で拡張性のある手段です。NetFlow バージョン 9 には定義可能なレコードタイプが用意されています。また、自己記述型で、NetFlow Collection Engine の設定を容易にします。

バージョン 9 エクスポートを使用すると、設定した間隔で NetFlow Collection Engine（以前の NetFlow FlowCollector）に送信できる新規のフォーマットをルータに定義できます。必要な機能をイネーブルにすると、それらの機能に対応するフィールド値が NetFlow Collection Engine に送信されます。

NetFlow Collection Engine を提供したり、NetFlow のサービスを表示したりするアプリケーションを製造するサードパーティ ビジネス パートナーは、新規の NetFlow テクノロジーが追加されるたびにアプリケーションを再コンパイルする必要はありません。その代わりに、NetFlow v9 エクスポート フォーマット機能を利用することで、既知のテンプレート フォーマットとフィールドタイプが記述された外部のデータ ファイルを使用できます。

NetFlow バージョン 9 については、次の点を考慮してください。

- レコード フォーマットはテンプレートによって定義されます。
- テンプレートの記述は、ルータから NetFlow Collection Engine に伝達されます。
- フロー レコードは最小限のテンプレート情報とともにルータから NetFlow Collection Engine に送信されるので、NetFlow Collection Engine でレコードを適切なテンプレートに関連付けることができます。
- バージョン 9 は基礎をなすトランスポート（UDP、TCP、Stream Control Transmission Protocol (SCTP) など）とは無関係です。

NetFlow バージョン 9 テンプレートベース フロー レコード フォーマット

NetFlow Version 9 エクスポート フォーマットの主要機能は、テンプレートがベースとなります。テンプレートには、NetFlow レコード フォーマットと、レコード内のフィールドの属性（タイプや長さなど）が記述されます。ルータで各テンプレートに ID が割り当てられ、テンプレートの記述と一緒に NetFlow Collection Engine に伝達されます。テンプレート ID は、ルータから NetFlow Collection Engine へのその後のすべての通信に使用されます。

NetFlow バージョン 9 エクスポート フロー レコード

NetFlow の基本出力はフロー レコードです。NetFlow バージョン 9 エクスポート フォーマットでは、テンプレートに定義されているものと同じフィールドのシーケンスの後に、フロー レコードが続きます。NetFlow フロー レコードが属するテンプレートは、テンプレートに属する NetFlow フロー レコードのグループの前に付加されるテンプレート ID によって決定します。既存の NetFlow フローレコード フォーマットの詳細については、『NetFlow Services Solutions Guide』を参照してください。

NetFlow バージョン 9 エクスポート パケット

NetFlow バージョン 9 のエクスポート パケットは、パケット ヘッダーとフローセットで構成されます。パケット ヘッダーによって新規バージョンが識別され、バージョン 9 のパケット ヘッダーの詳細についてのその他の詳細は [NetFlow バージョン 9 データ エクスポート フォーマット](#)、(58 ページ) 図 3 で説明します。フローセットには、テンプレート フローセットとデータ フローセットの 2 種類があります。テンプレート フローセットには、データ フローセット (またはフロー レコード) に含まれるフィールドが記述されます。各データ フローセットには、同じテンプレート ID を持つ 1 つまたは複数のフローの値または統計情報が含まれます。NetFlow Collection Engine でテンプレート フローセットが受信されると、フローセットとエクスポート元アドレスが格納されるので、フローセット ID と送信元の組み合わせに一致する後続のデータ フローセットをテンプレート フローセットのフィールド定義にしたがって解析できます。バージョン 9 では、NetFlow Collection Engine Version 4.0 がサポートされます。バージョン 9 のエクスポート パケットの例については、[NetFlow バージョン 9 データ エクスポート フォーマット](#)、(58 ページ) を参照してください。

出力 NetFlow アカウンティングの利点：NetFlow アカウンティングの簡素化

次の例に示すように、出力 NetFlow アカウンティング機能の利用により、NetFlow の設定が簡素化されます。

次の図では、着信および発信 (入力および出力) の両方のフロー統計情報がサーバに必要です。サーバはルータ B に接続されています。図の「雲」は、ネットワークのコアを示し、MPLS VPN が含まれます。

矢印で示されているすべてのトラフィックを計上する必要があります。実線の矢印は IP トラフィックを示し、点線の矢印は MPLS VPN を示しています。

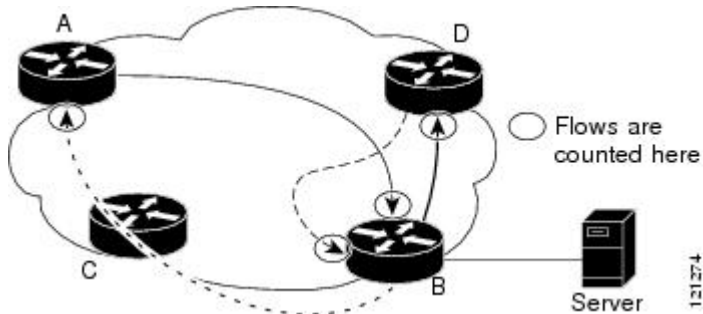
次の最初の図には、出力 NetFlow アカウンティング機能が導入される前に、フロー トラフィックがどのように追跡されていたかを示します。次の 2 番目の図には、出力 NetFlow アカウンティング機能が導入された後に、フロー トラフィックがどのように追跡されているかを示します。出力 NetFlow アカウンティング機能によって設定作業が簡素化され、この例ではサーバに関する着信フローおよび発信フローの統計情報の収集と追跡が容易になります。

出力 NetFlow アカウンティング機能が導入される前は、入力フローしか追跡できなかったため、ルータ B からの入力フローおよび出力フローを追跡するには、次の NetFlow 設定を行う必要がありました。

- ルータ A からルータ B への入力 IP トラフィックを追跡するために、ルータ B のインターフェイスで NetFlow をイネーブルにする。
- ルータ B からルータ D への入力 IP トラフィックを追跡するために、ルータ D のインターフェイスで NetFlow をイネーブルにする。
- ルータ B からルータ A への MPLS VPN の入力トラフィックを追跡するために、ルータ A のインターフェイスで NetFlow をイネーブルにする。

- ルータ D からルータ B への MPLS VPN の入力トラフィックを追跡するために、ルータ B のインターフェイスで NetFlow をイネーブルにする。

図 16 : 入力だけの NetFlow の例



上記の図で使用しているような設定でサーバのフロー統計情報を取得するには、3 つの各ルータからの NetFlow 統計情報を 1 つにまとめる必要があります。

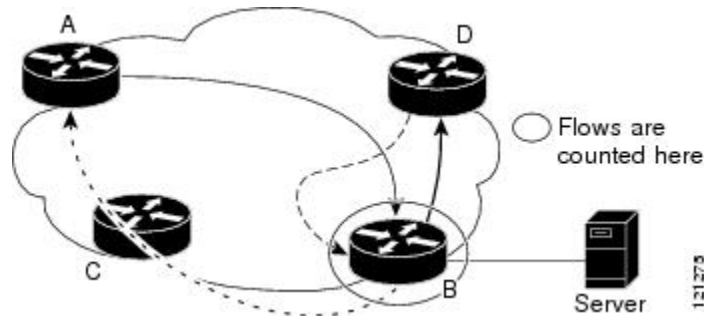
これに対し、次の図の例では、NetFlow、出力 NetFlow アカウンティング機能、および MPLS 出力 NetFlow アカウンティング機能を使用してルータ B に関する入力フローおよび出力フローの統計情報をキャプチャすることで、サーバに関する必要なフロー統計情報を取得しています。

次の図では、次の NetFlow 設定がルータ B に適用されます。

- ルータ A からルータ B への入力 IP トラフィックを追跡するために、ルータ B のインターフェイスで NetFlow をイネーブルにする。
- ルータ B からルータ D への出力 IP トラフィックを追跡するために、ルータ B のインターフェイスで出力 NetFlow アカウンティング機能をイネーブルにする。
- ルータ B からルータ D への MPLS VPN の入力トラフィックを追跡するために、ルータ B のインターフェイスで NetFlow をイネーブルにする。
- ルータ B からルータ A への MPLS VPN の入力トラフィックを追跡するために、ルータ B のインターフェイスで NetFlow をイネーブルにする。

ルータ B で NetFlow を設定した後は、ルータ B で **show ip cache flow** コマンドまたは **show ip cache verbose flow** コマンドを入力することによって、サーバに関するすべての NetFlow 統計情報を表示できます。

図 17：出力 NetFlow アカウンティングの例



NetFlow サブインターフェイス サポートの利点：データ収集の微調整

NetFlow はサブインターフェイス単位で設定できます。ネットワークに何千ものサブインターフェイスが存在する場合に、ほんのいくつかのサブインターフェイスからだけエクスポートレコードを収集するには、そのようにサブインターフェイス単位で設定できます。その結果、NetFlow データ エクスポートの帯域幅要件が減少し、NetFlow データ収集装置のプラットフォーム要件も減少します。

選択したサブインターフェイスに NetFlow を設定することには、次の利点があります。

- ルーティング デバイスと NetFlow 管理ワークステーション間に必要な帯域幅が減少する。
- NetFlow ワークステーションの要件が減少する。つまり、処理用のワークステーションに送信されるフローの数が減少します。

NetFlow 複数エクスポート先の利点

NetFlow 複数エクスポート先機能の利用により、NetFlow データに複数の宛先を設定できます。この機能をイネーブルにすると、NetFlow データのまったく同じ 2 つのストリームが宛先ホストに送信されます。現在、最大で 2 つのエクスポート先を設定できます。

NetFlow 複数エクスポート先機能により、冗長データストリームが提供されるので、完全な NetFlow データを受信できる可能性が増します。同じエクスポート データが複数の NetFlow コレクタに送信されるので、パケットの損失が減少します。

NetFlow および NetFlow データ エクスポートの設定方法

NetFlow の設定

手順の概要

1. イネーブル化
2. `configureterminal`
3. `interfaceinterface-typeinterface-number`
4. `ipflow {ingress | egress}`
5. `exit`
6. 他のインターフェイスで NetFlow をイネーブルにするには、ステップ 3～5 を繰り返します。
7. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： <code>Router> enable</code>	(必須) 特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>configureterminal</code> 例： <code>Router# configure terminal</code>	(必須) 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	<code>interfaceinterface-typeinterface-number</code> 例： <code>Router(config)# interface fastethernet 0/0/0</code>	(必須) NetFlow をイネーブルに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	<code>ipflow {ingress egress}</code> 例： <code>Router(config-if)# ip flow ingress</code>	(必須) インターフェイスで NetFlow をイネーブルにします。 • ingress : インターフェイスで受信中のトラフィックをキャプチャします。 • egress : インターフェイスで送信中のトラフィックをキャプチャします。

	コマンドまたはアクション	目的
		これは、 出力 NetFlow アカウンティングの利点：NetFlow アカウンティングの簡素化 、(59 ページ) で説明している出力 NetFlow アカウンティング機能です。
ステップ 5	exit 例： <pre>Router(config-if)# exit</pre>	(任意) 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、グローバル コンフィギュレーション モードに戻ります。 (注) 別のインターフェイスで NetFlow をイネーブルにする場合だけ、このコマンドを使用します。
ステップ 6	他のインターフェイスで NetFlow をイネーブルにするには、ステップ 3 ～ 5 を繰り返します。	(任意) :
ステップ 7	end 例： <pre>Router(config-if)# end</pre>	(必須) 現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

NetFlow が動作可能であることの確認と NetFlow 統計情報の表示

NetFlow が動作可能であることを確認し、NetFlow の統計情報を表示するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. `showipcacheflow`
3. `showipcacheverboseflow`
4. `end`

手順の詳細

ステップ 1 イネーブル化

このコマンドを使用して、特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

例：

```
Router> enable
```

Router#

ステップ2 showipcacheflow

このコマンドを使用して、NetFlow が動作可能であることを確認し、NetFlow 統計情報の要約を表示します。次に、このコマンドの出力例を示します。

例：

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
    .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 aged polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol      Total      Flows      Packets Bytes   Packets Active(Sec) Idle(Sec)
-----      -
Flows         /Sec      /Flow  /Pkt   /Sec    /Flow    /Flow
TCP-FTP       108        0.0        1133   40      2.4     1799.6    0.9
TCP-FTPD      108        0.0        1133   40      2.4     1799.6    0.9
TCP-WWW       54         0.0        1133   40      1.2     1799.6    0.8
TCP-SMTP      54         0.0        1133   40      1.2     1799.6    0.8
TCP-BGP       27         0.0        1133   40      0.6     1799.6    0.7
TCP-NNTP      27         0.0        1133   40      0.6     1799.6    0.7
TCP-other     297        0.0        1133   40      6.8     1799.7    0.8
UDP-TFTP      27         0.0        1133   28      0.6     1799.6    1.0
UDP-other     108        0.0       1417   28      3.1     1799.6    0.9
ICMP          135        0.0        1133   427     3.1     1799.6    0.8
Total:        945        0.0       1166   91      22.4    1799.6    0.8
SrcIf         SrcIPAddress  DstIf         DstIPAddress  Pr SrcP DstP  Pkts
-----
FEt0/0/0     192.168.67.6  FEt1/0/0.1    172.16.10.200  01 0000 0C01  51
FEt0/0/0     10.10.18.1    Null          172.16.11.5    11 0043 0043  51
FEt0/0/0     10.10.18.1    Null          172.16.11.5    11 0045 0045  51
FEt0/0/0     10.234.53.1   FEt1/0/0.1    172.16.10.2    01 0000 0800  51
FEt0/0/0     10.10.19.1    Null          172.16.11.6    11 0044 0044  51
FEt0/0/0     10.10.19.1    Null          172.16.11.6    11 00A2 00A2  51
FEt0/0/0     192.168.87.200 FEt1/0/0.1    172.16.10.2    06 0014 0014  50
FEt0/0/0     192.168.87.200 FEt1/0/0.1    172.16.10.2    06 0015 0015  52
.
.
FEt0/0/0     172.16.1.84   FEt1/0.1      172.16.10.19   06 0087 0087  50
FEt0/0/0     172.16.1.84   FEt1/0.1      172.16.10.19   06 0050 0050  51
FEt0/0/0     172.16.1.85   FEt1/0.1      172.16.10.20   06 0089 0089  49
FEt0/0/0     172.16.1.85   FEt1/0.1      172.16.10.20   06 0050 0050  50
FEt0/0/0     10.251.10.1   FEt1/0.1      172.16.10.2    01 0000 0800  51
FEt0/0/0     10.162.37.71  Null          172.16.11.3    06 027C 027C  49
Router#
```

ステップ3 showipcacheverboseflow

このコマンドを使用して、NetFlow が動作可能であることを確認し、NetFlow 統計情報の詳細な要約を表示します。次に、このコマンドの出力例を示します。

例：

```
Router# show ip cache verbose flow
```

```

ToS
IP packet size distribution (1130681 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
    .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
    .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2992518 aged polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active (Sec) /Flow	Idle (Sec) /Flow
TCP-FTP	108	0.0	1133	40	2.4	1799.6	0.9
TCP-FTPD	108	0.0	1133	40	2.4	1799.6	0.9
TCP-WWW	54	0.0	1133	40	1.2	1799.6	0.8
TCP-SMTP	54	0.0	1133	40	1.2	1799.6	0.8
TCP-BGP	27	0.0	1133	40	0.6	1799.6	0.7
TCP-NNTP	27	0.0	1133	40	0.6	1799.6	0.7
TCP-other	297	0.0	1133	40	6.6	1799.7	0.8
UDP-TFTP	27	0.0	1133	28	0.6	1799.6	1.0
UDP-other	108	0.0	1417	28	3.0	1799.6	0.9
ICMP	135	0.0	1133	427	3.0	1799.6	0.8
Total:	945	0.0	1166	91	21.9	1799.6	0.8

```

SrcIf      SrcIPAddress      DstIf      DstIPAddress      Pr TOS Flgs Pkts
Port Msk AS      Port Msk AS      NextHop      B/Pk Active
FEt0/0/0    192.168.67.6      FEt1/0.1      172.16.10.200    01 00 10 799
0000 /0 0      0C01 /0 0      0.0.0.0      28 1258.1
FEt0/0/0    10.10.18.1        Null          172.16.11.5      11 00 10 799
0043 /0 0      0043 /0 0      0.0.0.0      28 1258.0
FEt0/0/0    10.10.18.1        Null          172.16.11.5      11 00 10 799
0045 /0 0      0045 /0 0      0.0.0.0      28 1258.0
FEt0/0/0    10.234.53.1       FEt1/0.1      172.16.10.2      01 00 10 799
0000 /0 0      0800 /0 0      0.0.0.0      28 1258.1
FEt0/0/0    10.10.19.1        Null          172.16.11.6      11 00 10 799
0044 /0 0      0044 /0 0      0.0.0.0      28 1258.1
.
.
FEt0/0/0    172.16.1.84       FEt1/0/0.1    172.16.10.19     06 00 00 799
0087 /0 0      0087 /0 0      0.0.0.0      40 1258.1
FEt0/0/0    172.16.1.84       FEt1/0/0.1    172.16.10.19     06 00 00 799
0050 /0 0      0050 /0 0      0.0.0.0      40 1258.0
FEt0/0/0    172.16.1.85       FEt1/0/0.1    172.16.10.20     06 00 00 798
0089 /0 0      0089 /0 0      0.0.0.0      40 1256.5
FEt0/0/0    172.16.1.85       FEt1/0/0.1    172.16.10.20     06 00 00 799
0050 /0 0      0050 /0 0      0.0.0.0      40 1258.0
FEt0/0/0    10.251.10.1       FEt1/0/0.1    172.16.10.2      01 00 10 799
0000 /0 0      0800 /0 0      0.0.0.0      1500 1258.1
FEt0/0/0    10.162.37.71      Null          172.16.11.3      06 00 00 798
027C /0 0      027C /0 0      0.0.0.0      40 1256.4
Router#

```

ステップ 4 end

このコマンドを使用して、特権 EXEC モードを終了します。

例：

```
Router# end
```

バージョン 9 エクスポート フォーマットを使用する NetFlow データ エクスポートの設定

バージョン 9 エクスポート フォーマットを使用して NetFlow データ エクスポートを設定するには、次の任意の作業手順を実行します。



(注) この作業は、Stream Control Transmission Protocol (SCTP) を使用した信頼性のある NetFlow データ エクスポートの設定手順は含まれていません。SCTP を使用した信頼性のある NetFlow データ エクスポートの設定とその手順については、『NetFlow Reliable Export with SCTP』モジュールを参照してください。

はじめる前に

この作業には、NetFlow の設定手順は含まれていません。NetFlow データ エクスポートを使用してトラフィック データをエクスポートするには、ルータの少なくとも 1 つのインターフェイスで NetFlow をイネーブルにすることによって NetFlow を設定する必要があります。NetFlow の設定の詳細については、[NetFlow の設定](#)を参照してください。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `ip flow-export destination {ip-address | hostname} udp-port`
4. 追加の NetFlow エクスポート先を設定するには、ステップ 3 を繰り返します。
5. `ipflow-exportsourceinterface-typeinterface-number`
6. `ipflow-exportversion9[origin-as|peer-as] [bgp-nexthop]`
7. `ipflow-exportinterface-names`
8. `ipflow-exporttemplaterefresh-ratepackets`
9. `ipflow-exporttemplatettimeout-rateminutes`
10. `ipflow-exporttemplateoptionsexport-stats`
11. `ipflow-exporttemplateoptionsrefresh-ratepackets`
12. `ipflow-exporttemplateoptionstimeout-rateminutes`
13. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
	例 : <pre>Router> enable</pre>	<ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例 : <pre>Router# configure terminal</pre>	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	ip flow-export destination {ip-address hostname} udp-port 例 : <pre>Router(config)# ip flow-export destination 172.16.10.2 99</pre>	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンしている UDP ポートを指定します。
ステップ 4	追加の NetFlow エクスポート先を設定するには、ステップ 3 を繰り返します。	（任意）NetFlow に最大 2 つのエクスポート先を設定できます。
ステップ 5	ipflow-exportsourceinterface-typeinterface-number 例 : <pre>Router(config)# ip flow-export source ethernet 0/0</pre>	（任意）インターフェイスからの IP アドレスを指定します。IP アドレスは、宛先ホストに NetFlow データ エクスポートによって送信される UDP データ グラムの送信元 IP アドレスとして使用されます。
ステップ 6	ipflow-exportversion9[origin-as peer-as] [bgp-nexthop] 例 : <pre>Router(config)# ip flow-export version 9</pre>	（任意）NetFlow キャッシュ エントリ内の情報のエクスポートをイネーブルにします。 <ul style="list-style-type: none"> • version 9 キーワードは、エクスポート パケットにバージョン 9 フォーマットが使用されることを示します。 • origin-as キーワードは、エクスポート統計情報に、送信元と宛先の起点自律システムが含まれることを示します。 • peer-as キーワードは、エクスポート統計情報に送信元と宛先のピア自律システムが含まれることを示します。 • bgp-nexthop キーワードは、エクスポート統計情報に BGP ネクスト ホップ関連の情報が含まれることを示します。

	コマンドまたはアクション	目的
		<p>注意 Cisco 12000 シリーズ インターネット ルータにこのコマンドを入力すると、NetFlow で RP と LC シスコ エクスプレス フォワーディング テーブルがリロードされる数秒間だけ、パケットの転送が停止します。アクティブ ネットワークへのサービスの中断を回避するには、変更時間帯にこのコマンドを適用するか、ルータのリブート時にコマンドが実行されるように startup-config ファイルに追加します。</p>
ステップ 7	ipflow-exportinterface-names 例 : <pre>Router(config)# ip flow-export interface-names</pre>	NetFlow キャッシュ エントリが宛先システムにエクスポートされるときに、フローからインターフェイス名が含まれるように NetFlow データ エクスポートを設定します。
ステップ 8	ipflow-exporttemplaterefresh-ratepackets 例 : <pre>Router(config)# ip flow-export template refresh-rate 15</pre> 例 :	<p>(任意) NetFlow キャッシュ エントリ内の情報のエクスポートをイネーブルにします。</p> <ul style="list-style-type: none"> • template キーワードは、テンプレート固有の設定を指定します。 • refresh-rate packets のキーワードと引数のペアは、テンプレートが再送信される前にエクスポートされるパケットの数を指定します。1～600 個のパケットを指定できます。デフォルトは 20 です。
ステップ 9	ipflow-exporttemplatetimeout-rateminutes 例 : <pre>Router(config)# ip flow-export template timeout-rate 90</pre>	<p>(任意) NetFlow キャッシュ エントリ内の情報のエクスポートをイネーブルにします。</p> <ul style="list-style-type: none"> • template キーワードは、timeout-rate キーワードがテンプレートに適用されることを示します。 • timeout-rate minutes のキーワードと引数のペアは、テンプレートが再送信されるまでの経過時間を指定します。1～3600 分を指定できます。デフォルトは 30 です。
ステップ 10	ipflow-exporttemplateoptionsexport-stats 例 : <pre>Router(config)# ip flow-export template options export-stats</pre>	<p>(任意) NetFlow キャッシュ エントリ内の情報のエクスポートをイネーブルにします。</p> <ul style="list-style-type: none"> • template キーワードは、テンプレート固有の設定を指定します。 • options キーワードは、テンプレートオプションを指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • export-stats キーワードは、エクスポート統計情報にエクスポートされたフローの合計数とエクスポートされたパケットの合計数が含まれることを示します。
ステップ 11	ipflow-exporttemplateoptionsrefresh-ratepackets 例 : <pre>Router(config)# ip flow-export template options refresh-rate 25</pre>	(任意) NetFlow キャッシュ エントリ内の情報のエクスポートをイネーブルにします。 <ul style="list-style-type: none"> • template キーワードは、テンプレート固有の設定を指定します。 • options キーワードは、テンプレートオプションを指定します。 • refresh-rate packets のキーワードと引数のペアは、テンプレートが再送信される前にエクスポートされるパケットの数を指定します。1～600個のパケットを指定できます。デフォルトは 20 です。
ステップ 12	ipflow-exporttemplateoptionstimeout-rateminutes 例 : <pre>Router(config)# ip flow-export template options timeout-rate 120</pre>	(任意) NetFlow キャッシュ エントリ内の情報のエクスポートをイネーブルにします。 <ul style="list-style-type: none"> • template キーワードは、テンプレート固有の設定を指定します。 • options キーワードは、テンプレートオプションを指定します。 • timeout-rate minutes のキーワードと引数のペアは、テンプレートが再送信されるまでの経過時間を指定します。1～3600 分を指定できます。デフォルトは 30 です。
ステップ 13	end 例 : <pre>Router(config)# end</pre>	現在のコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

NetFlow データ エクスポートが動作可能であることの確認

NetFlow データ エクスポートが動作可能であることを確認し、NetFlow データ エクスポートの統計情報を表示するには、次の任意の作業手順を実行します。

手順の概要

1. showipflowexport

手順の詳細

showipflowexport

このコマンドを使用して、メインキャッシュやその他すべてのイネーブルのキャッシュに関する統計情報を含む、NetFlow データ エクスポートの統計情報を表示します。次に、このコマンドの出力例を示します。

例：

```
Router# show ip flow export
Flow export v9 is enabled for main cache
Exporting flows to 172.16.10.2 (99)
Exporting using source interface Ethernet0/0
Version 9 flow records
0 flows exported in 0 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
```

ルータ上の NetFlow 統計情報の消去

ルータ上の NetFlow 統計情報を消去するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. clearipflowstats
3. end

手順の詳細

ステップ1 イネーブル化

このコマンドを使用して、特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

例：

```
Router> enable
Router#
```

ステップ 2 clearipflowstats

このコマンドを使用して、ルータ上の NetFlow 統計情報を消去します。次に例を示します。

例：

```
Router# clear ip flow stats
```

ステップ 3 end

このコマンドを使用して、特権 EXEC モードを終了します。

例：

```
Router# end
```

NetFlow メイン キャッシュ パラメータのカスタマイズ

NetFlow は、アクティブ フローごとに NetFlow キャッシュ エントリ（フロー レコード）を作成することによって動作します。フロー レコードは、すべてのアクティブ フローに対する NetFlow キャッシュ内に保持されます。NetFlow キャッシュ内の各フロー レコードには、後から NetFlow Collection Engine などの収集装置にエクスポートできるフィールドが含まれています。NetFlow では、フローへのデータの累積が可能です。各フローは、IP アドレス、インターフェイス、アプリケーション、および ToS などの固有の特性によって識別されます。

メインの NetFlow キャッシュに対するパラメータをカスタマイズするには、次の手順を実行します。

ルーティング デバイスでの NetFlow キャッシュ エントリの管理

ルーティング デバイスでは 1 秒に 1 回 NetFlow キャッシュがチェックされ、次のインスタンスでフローが期限切れとなります。

- フロー キャッシュが満杯になっている。
- フローが非アクティブになっている。デフォルトでは、15 秒以内に更新されなかったフローは非アクティブに分類されます。
- アクティブ フローが指定した分数だけモニタされている。デフォルトでは、アクティブ フローは 30 分モニタされた後、キャッシュからフラッシュされます。

ルーティングデバイスのデフォルトのタイマー設定は、非アクティブタイマーが15秒、アクティブタイマーが30分です。非アクティブタイマーには、10～600秒の範囲で時間間隔を独自に設定できます。アクティブタイマーに設定できる時間間隔の範囲は、1～60分です。

NetFlow キャッシュのサイズ

インターフェイスでNetFlowをイネーブルにした後、NetFlowにより、NetFlow キャッシュに多数のエントリを格納できるようにメモリが予約されます。通常、NetFlow キャッシュのサイズはNetFlow トラフィック レートのニーズを満たします。キャッシュのデフォルトサイズは64K フロー キャッシュです。各キャッシュ エントリに64 バイトのストレージが必要です。デフォルトのエントリ数が設定されたキャッシュには、約4MBのDRAMが必要です。必要に応じて、キャッシュに保持するエントリ数を増減することができます。大量のフロー トラフィックを処理する環境（インターネット コア ルータなど）には、131072（128K）のように値を大きくすることを推奨します。フロー トラフィックの情報を取得するには、**showipcacheflow** コマンドを使用します。

ipflow-cacheentries コマンドを使用すると、NetFlow キャッシュのサイズを1024～524,288 エントリの間で設定できます。**cacheentries** コマンドを使用すると（NetFlow 集約の設定後）、NetFlow 集約キャッシュのサイズを1024～2,000,000 エントリの間で設定できます。



注意

NetFlow キャッシュ エントリの値は変更しないことを推奨します。この機能は適切に使用しないと、ネットワークに問題が生じるおそれがあります。NetFlow キャッシュ エントリをデフォルト値に戻すには、**noipflow-cacheentries** グローバル コンフィギュレーション コマンドを使用します。



(注)

NetFlow をイネーブルにした後でNetFlow メイン キャッシュに関するパラメータを変更した場合は、ルータをリブートするか、NetFlow がイネーブルである各インターフェイスでNetFlow をディセーブルにしてから再びイネーブルにするまで、パラメータの変更は有効になりません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interfaceinterface-typeinterface-number**
4. **noipflow {ingress | egress}**
5. **exit**
6. NetFlow をイネーブルにした残りのインターフェイスに対して、手順 3 ～ 5 を繰り返します。
7. **ipflow-cacheentriesnumber**
8. **ipflow-cachetimeoutactiveminutes**
9. **ipflow-cachetimeoutinactiveseconds**
10. **interfaceinterface-typeinterface-number**
11. **ipflow {ingress | egress}**
12. **exit**
13. ステップ 3 ～ 5 で NetFlow をディセーブルにした残りのインターフェイスに対して、ステップ 10 ～ 12 を繰り返します。
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例 : Router> enable	(必須) 特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合) 。
ステップ 2	configureterminal 例 : Router# configure terminal	(必須) 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	interfaceinterface-typeinterface-number 例 : Router(config)# interface fastethernet 0/0/0	(NetFlow がインターフェイスですでにイネーブルである場合に必須。) NetFlow をディセーブルに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	noipflow {ingress egress} 例 : Router(config-if)# no ip flow ingress	(NetFlow がインターフェイスでイネーブルである場合に必須。) NetFlow をインターフェイス上でディセーブルにします。 • ingress : インターフェイスで受信中のトラフィックをキャプチャします。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • egress : インターフェイスで送信中のトラフィックをキャプチャします。
ステップ 5	exit 例 : <pre>Router(config-if)# exit</pre>	(任意) 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、グローバル コンフィギュレーション モードに戻ります。 (注) 別のインターフェイスで NetFlow をディセーブルにする場合だけ、このコマンドを使用します。
ステップ 6	NetFlow をイネーブルにした残りのインターフェイスに対して、手順 3～5 を繰り返します。	(NetFlow がその他のインターフェイスでイネーブルである場合に必須。) --
ステップ 7	ipflow-cacheentriesnumber 例 : <pre>Router(config)# ip flow-cache entries 131072</pre>	(任意) NetFlow キャッシュに保持されるエントリの数を変更します。 <ul style="list-style-type: none"> • number は、保持されるエントリの数です。有効範囲は 1024 ～ 2000000 です。デフォルト値は 200000 です。
ステップ 8	ipflow-cachetimeoutactiveminutes 例 : <pre>Router(config)# ip flow-cache timeout active 20</pre>	(任意) フローキャッシュのタイムアウトパラメータを指定します。 <ul style="list-style-type: none"> • active : アクティブフロー タイムアウトを指定します。 • minutes : アクティブフローがタイムアウトになるまでにキャッシュ内に保持される分数を指定します。指定できる範囲は 1 ～ 60 です。デフォルトは 30 です。
ステップ 9	ipflow-cachetimeoutinactiveseconds 例 : <pre>Router(config)# ip flow-cache timeout inactive 130</pre>	(任意) フローキャッシュのタイムアウトパラメータを指定します。 <ul style="list-style-type: none"> • inactive : 非アクティブフロー タイムアウトを指定します。 • seconds : タイムアウトになる前に非アクティブなフローがキャッシュに残される秒数を指定します。範囲は 10 ～ 600 です。デフォルトは 15 です。
ステップ 10	interfaceinterface-typeinterface-number 例 : <pre>Router(config)# interface fastethernet 0/0/0</pre>	(必須) NetFlow をイネーブルに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。

	コマンドまたはアクション	目的
ステップ 11	ipflow {ingress egress} 例 : <pre>Router(config-if)# ip flow ingress</pre>	(必須) インターフェイスで NetFlow をイネーブルにします。 <ul style="list-style-type: none"> • ingress : インターフェイスで受信中のトラフィックをキャプチャします。 • egress : インターフェイスで送信中のトラフィックをキャプチャします。
ステップ 12	exit 例 : <pre>Router(config-if)# exit</pre>	(任意) 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、グローバルコンフィギュレーションモードに戻ります。 (注) 別のインターフェイスで NetFlow をイネーブルにする場合だけ、このコマンドを使用します。
ステップ 13	ステップ 3 ~ 5 で NetFlow をディセーブルにした残りのインターフェイスに対して、ステップ 10 ~ 12 を繰り返します。	(他のインターフェイスで NetFlow をイネーブルにする必要がある場合に必須。) --
ステップ 14	end 例 : <pre>Router(config-if)# end</pre>	(必須) 現在のコンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

NetFlow および NetFlow データ エクスポートの設定例

出力 NetFlow アカウンティングの設定例

次に、[出力 NetFlow アカウンティングの利点 : NetFlow アカウンティングの簡素化](#)で説明されているとおりに出力 NetFlow アカウンティングを設定する例を示します。

```
configure terminal
!
interface ethernet 0/0
 ip flow egress
!
```

NetFlow サブインターフェイス サポートの設定例

サブインターフェイスでの入力（受信）トラフィックに対する **NetFlow** サブインターフェイス サポート

```
configure terminal
!
interface ethernet 0/0.1
 ip flow ingress
!
```

サブインターフェイスでの出力（送信）トラフィックに対する **NetFlow** サブインターフェイス サポート

```
configure terminal
!
interface ethernet 1/0.1
 ip flow egress
!
```



(注) NetFlowでは、多くのCPU処理時間と帯域幅を必要とする各インターフェイスのステータスも確認されます。複数のサブインターフェイスが設定されており、それらのすべてのサブインターフェイスにNetFlowデータキャプチャを設定する必要がある場合は、個々のサブインターフェイスではなく、メインのインターフェイスにNetFlowを設定することを推奨します。

サブインターフェイスでの入力（受信）トラフィックに対するNetFlowサブインターフェイス サポート例

```
configure terminal
!
interface fastethernet 0/0/0.1
 ip flow ingress
!
```

サブインターフェイスでの出力（送信）トラフィックに対するNetFlowサブインターフェイス サポート例

```
configure terminal
!
interface fastethernet 1/0/0.1
 ip flow egress
!
```



- (注) NetFlow では、多くの CPU 処理時間と帯域幅を必要とする各インターフェイスのステータスも確認されます。複数のサブインターフェイスが設定されており、それらのすべてのサブインターフェイスに NetFlow データ キャプチャを設定する必要がある場合は、個々のサブインターフェイスではなく、メインのインターフェイスに NetFlow を設定することを推奨します。

NetFlow 複数エクスポート先の設定例

次の例は、Flexible NetFlow マルチ エクスポート先を設定する方法を示しています。

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export destination 172.16.10.2 9991
!
```



- (注) メイン キャッシュおよび各集約キャッシュに最大 2 つのエクスポート先を設定できます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
NetFlow コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『Cisco IOS NetFlow Command Reference』
NetFlow 入力フィルタの設定作業	「Using NetFlow Filtering or Sampling to Select the Network Traffic to Track」
ランダム サンプル NetFlow の設定作業	「Using NetFlow Filtering or Sampling to Select the Network Traffic to Track」
NetFlow 集約キャッシュの設定作業	NetFlow 集約キャッシュの設定
CNS NetFlow Collection Engine のインストール、開始、および設定に関する情報	Cisco CNS NetFlow Collection Engine のマニュアル
NetFlow フロー レコード形式の説明	『NetFlow Services Solutions Guide』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NetFlow および NetFlow データ エクスポートを設定するための機能情報

表 17: NetFlow および NetFlow データ エクスポートを設定するための機能情報

機能名	リリース	機能情報
Egress NetFlow Accounting	12.3(11)T 15.0(1)S	<p>出力 NetFlow アカウンティング機能の利用により、ルータを出る出力トラフィックの NetFlow 統計情報を収集することができます。NetFlow の以前のバージョンで収集できるのは、ルータに入る入力トラフィックの統計情報だけです。</p> <p>この機能により、ipflowegress コマンドおよび ipflow-egressinput-interface コマンドが導入されました。</p> <p>この機能により、flow-sampler、match、showipcacheflow、showipcacheverboseflow、および showipflowinterface の各コマンドが変更されました。</p>
NetFlow Multiple Export Destinations	12.0(19)S 12.2(2)T 12.2(14)S 15.0(1)S	<p>NetFlow 複数エクスポート先機能の使用により、NetFlow データに複数の宛先を設定できます。</p> <p>この機能により、ipflow-aggregationcache、ipflow-exportdestination、および showipflowexport の各コマンドが変更されました。</p>

機能名	リリース	機能情報
NetFlow Subinterface Support	12.0(22)S 12.2(14)S 12.2(15)T 12.2(33)SB	<p>NetFlow サブインターフェイスサポート機能は、サブインターフェイス単位での NetFlow のイネーブル化を可能します。</p> <p>この機能により、ipflowingress コマンドが導入されました。</p> <p>この機能により、showipinterface コマンドが変更されました。</p>
NetFlow v9 Export Format	12.0(24)S 12.2(18)S 12.2(27)SBC 12.2(18)SXF 12.3(1) 15.0(1)S	<p>NetFlow v9 エクスポートフォーマットは柔軟で拡張性があり、新規のフィールドおよびレコードタイプのサポートに必要な汎用性を備えています。このフォーマットは、マルチキャスト、MPLS、ネットワークアドレス変換 (NAT)、および BGP ネクストホップなど、NetFlow をサポートする新規のテクノロジーに対応します。</p> <p>この機能により、debugipflowexport、export、ipflow-export、および showipflowexport の各コマンドが変更されました。</p>
NetFlow データ エクスポートに追加されたインターフェイス名のサポート ⁴	12.4(2)T	<p>ipflow-export コマンドに interface-names キーワードを入力すると、NetFlow キャッシュエントリを宛先システムにエクスポートするときにフローからインターフェイス名が含まれるように、NetFlow データ エクスポートを設定できます。</p>

⁴ これはマイナーな拡張です。マイナーな拡張は、通常 Feature Navigator に記載されません。

用語集

AS：自律システム。共通のルーティング戦略を共有する、共通の管理の下にあるネットワークの集合。自律システムは、エリアで分割されます。自律システムには、インターネット割り当て番号局（IANA）によって、一意な 16 ビットの数字が割り当てられる必要があります。

シスコエクスプレス フォワーディング：大規模で動的なトラフィック パターンを持つネットワークのパフォーマンスと拡張性を最適化する、レイヤ 3 IP スイッチング テクノロジー。

BGP：Border Gateway Protocol。Exterior Gateway Protocol（EGP）に置き換わるドメイン間ルーティング プロトコル。BGP システムは到着可能性情報を他の BGP システムと交換します。RFC 1163 によって定義されています。

BGP ネクスト ホップ：特定の宛先に到達するためにルータで使用するネクスト ホップの IP アドレス。

エクスポート パケット：NetFlow サービスがイネーブルであるデバイス（ルータなど）によって作成されたパケットのタイプ。別のデバイス（NetFlow Collection Engine など）にアドレス指定されます。このパケットには、NetFlow 統計情報が含まれています。この他方のデバイスによってパケットが処理されます（IP フローの情報の解析、集約、および格納）。

高速スイッチング：ルート キャッシュを使用して、ルータを介したパケット交換を促進するシスコの機能。

フロー：送信元 IP アドレス、宛先 IP アドレス、プロトコル、送信元ポートと宛先ポート、タイプ オブ サービス、およびフローがモニタされるインターフェイスがすべて同一のパケットの集合。入力フローは入力インターフェイスに関連付けられ、出力フローは出力インターフェイスに関連付けられます。

NetFlow：ルータを通過するパケットの統計情報が得られる Cisco IOS アプリケーション。ネットワーク アカウンティングおよびセキュリティの新たな主要テクノロジーになりつつあります。

NetFlow 集約：NetFlow 機能の 1 機能であり、NetFlow Collection Engine などの NetFlow データ収集システムにデータがエクスポートされる前に、Cisco IOS ルータ上で NetFlow エクスポートデータを要約することができます。この機能により、NetFlow エクスポートデータの帯域幅要件が減少し、NetFlow データ収集装置のプラットフォーム要件も減少します。

NetFlow v9：NetFlow エクスポート フォーマットのバージョン 9。ネットワーク ノードからコレクタに NetFlow レコードを送信するための柔軟で拡張可能な手段です。NetFlow バージョン 9 には定義可能なレコードタイプが用意されています。また、自己記述型で、NetFlow Collection Engine の設定を容易にします。



第 4 章

トラックへのネットワーク トラフィックの NetFlow サンプルングを使用した選択

この章では、NetFlow サンプルングの使用によるトラックへのネットワーク トラフィックの選択とその手順について説明します。この章で説明するランダム サンプル NetFlow 機能を使用して、トラフィックの特定のサブセットからデータを収集できます。ランダム サンプル NetFlow 機能では、連続した n 個のパケット (n はユーザが設定可能なパラメータ) ごとにランダムに選択される 1 個のパケットだけを処理することにより、Cisco ルータ内のトラフィックのサブセットに関する NetFlow データが得られます。

NetFlow は、ルータを通過するパケットの統計情報を提供する Cisco IOS XE アプリケーションであり、ネットワーク アカウンティングおよびセキュリティの新たな主要テクノロジーになりつつあります。

- [機能情報の確認, 84 ページ](#)
- [NetFlow サンプルングを使用したトラックへのネットワーク トラフィックの選択の前提条件, 84 ページ](#)
- [NetFlow サンプルングを使用したトラックへのネットワーク トラフィックの選択の制限事項, 84 ページ](#)
- [NetFlow サンプルングを使用したトラックへのネットワーク トラフィックの選択, 85 ページ](#)
- [NetFlow サンプルングの設定方法, 86 ページ](#)
- [NetFlow サンプルングの設定例, 91 ページ](#)
- [その他の参考資料, 92 ページ](#)
- [NetFlow サンプルングを使用したトラックへのネットワーク トラフィックの選択の機能情報, 94 ページ](#)
- [用語集, 96 ページ](#)

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、[Bug Search Tool](#) およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NetFlowサンプリングを使用したトラックへのネットワークトラフィックの選択の前提条件

ランダム サンプル NetFlow 機能を設定する前に、次の作業を実行しておく必要があります。

- IP ルーティング用にルータを設定する。
- ルータおよびランダム サンプル NetFlow を設定するインターフェイスでシスコ エクスプレス フォワーディングを設定する。高速スイッチングはサポートされていません。
- NetFlow データをエクスポートする場合は、NetFlow バージョン 9 データ エクスポートを設定する（設定しなかった場合、NetFlow データは、キャッシュ内で表示できますが、エクスポートされません）。
- サンプラー オプションテンプレートを使用する場合、または NetFlow サンプラー ID を表示する場合は、NetFlow バージョン 9 を設定する。

NetFlowサンプリングを使用したトラックへのネットワークトラフィックの選択の制限事項

フル NetFlow がインターフェイス上でイネーブルになっている場合、フル NetFlow がランダム サンプル NetFlow よりも優先されます（したがって、ランダム サンプル NetFlow は無効になります）。つまり、インターフェイス上でランダム サンプル NetFlow をイネーブルにする前に、そのインターフェイス上のフル NetFlow をディセーブルにする必要があります。

物理インターフェイス上でランダム サンプル NetFlow をイネーブルにしても、サブインターフェイス上でランダム サンプル NetFlow が自動的にイネーブルになることはありません。サブインターフェイス上で明示的に設定する必要があります。また、ランダム サンプル NetFlow を物理インターフェイス（またはサブインターフェイス）上でディセーブルにしても、フル NetFlow がイネーブルになることはありません。この制約事項は、フル NetFlow への移行によって物理インター

フェイス（またはサブインターフェイス）に過剰な負荷がかかるのを防いでいます。フル NetFlow が必要な場合は、明示的にイネーブルにする必要があります。

サンプラー オプション テンプレートをを使用する場合は、NetFlow バージョン 9 を使用してください。

NetFlow サンプリングを使用したトラックへのネットワーク トラフィックの選択

NetFlow トラフィックのサンプリング

NetFlow では、Cisco ルータにおいてフロー単位の非常に細かいトラフィック統計情報が提供されます。フローとは、同じサブインターフェイス上でルータに到着し、送信元と宛先の IP アドレス、レイヤ 4 プロトコル、送信元と宛先の TCP/UDP ポート、および IP ヘッダー内のタイプ オブ サービス (ToS) バイトが同一である単方向のパケットのストリームです。ルータにより NetFlow 統計情報が NetFlow キャッシュに蓄積され、蓄積された情報は、外部デバイス (Cisco Networking Service (CNS) NetFlow Collection Engine など) にエクスポートしてさらに処理できます。

フル NetFlow では、イネーブルのサブインターフェイスに入ってくるすべてのトラフィックが記録されます。しかし、場合によっては、このトラフィックのサブセットに関してだけ、NetFlow データを収集することがあります。ランダム サンプル NetFlow 機能によって、着信トラフィックを NetFlow 処理に関係のあるトラフィックだけに制限することができます。ランダム サンプル NetFlow では、連続した n 個のパケットごとにランダムに選択された 1 個のパケットだけを処理することにより、Cisco ルータ内のトラフィックのサブセットが NetFlow データとして提供されます。



(注)

ランダム サンプル NetFlow は、サンプル NetFlow よりも統計的に正確です。NetFlow でパケットをサンプリングする機能は、サンプル NetFlow 機能によって最初に提供されました。サンプル NetFlow 機能で使用方法は、決定論的なサンプリングです。この方法では、インターフェイスごとに毎回 n 番目のパケットが NetFlow で処理するために選択されます。たとえば、サンプリング レートを 100 パケットごとに 1 つとして設定すると、1 番め、101 番め、201 番め、301 番めと続くパケットがサンプル NetFlow によってサンプリングされます。サンプル NetFlow では、ランダムなサンプリングはできません。そのため、トラフィックが一定のパターンで到着する場合は、統計情報が不正確になる可能性があります。

ランダム サンプル NetFlow サンプリング モード

サンプリング モードでは、NetFlow で処理するためのトラフィックのサブセットを選択するアルゴリズムが使用されます。ランダム サンプル NetFlow 機能を使用するランダム サンプリング モードでは、NetFlow 処理のために平均して n 個の連続するパケットから 1 つのパケットが選択され

るように、着信パケットがランダムに選択されます。たとえば、サンプリング レートを 100 パケットごとに 1 つとして設定すると、NetFlow によって 5 番目のパケットがサンプリングされ、その後に、120 番め、199 番め、302 番めというようにサンプリングされる可能性があります。この設定例では、全トラフィックの 1% に対する NetFlow データが得られます。n の値は設定可能なパラメータであり、指定できる範囲は 1 ~ 65535 個のパケットです。

ランダム サンプル NetFlow : NetFlow サンプラー

NetFlow サンプラー マップにより、NetFlow サンプルングの特性（サンプリング レートや NetFlow サンプラー名など）のセットが定義されます。各 NetFlow サンプラー マップは、物理インターフェイスだけでなく、1 つ以上のサブインターフェイスにも適用できます。最大で 8 つの NetFlow サンプラー マップを定義できます。

たとえば、ランダム サンプリング モードと 100 パケットにつき 1 つのサンプリング レートを特性として持つ mysampler1 という名前の NetFlow サンプラー マップを作成できます。この NetFlow サンプラー マップは、任意の数のサブインターフェイスに適用できます。適用された各サブインターフェイスでは、mysampler1 を参照して NetFlow サンプルングが実行されます。これらのサブインターフェイスからのトラフィックは（サンプリングの観点から）マージされます。これにより、サブインターフェイス単位の NetFlow サンプルングよりもさらに強い「ランダム性」が導入されますが、統計的には、関係する各サブインターフェイスに同じ 100 パケットにつき 1 つのサンプリング レートが与えられます。

ランダム サンプル NetFlow におけるサンプリングは、NetFlow サンプラによって行われます。NetFlow サンプラーは、物理インターフェイスまたはサブインターフェイスに適用されている NetFlow サンプラー マップのインスタンスとして定義されます。物理インターフェイス上でフル NetFlow が設定されると、その物理インターフェイスのすべてのサブインターフェイス上でランダム サンプル NetFlow がフル NetFlow に上書きされます。

NetFlow サンプルングの設定方法

NetFlow データ エクスポートの影響を軽減するランダム サンプル NetFlow の設定

ランダム サンプル NetFlow 機能の設定を行い、これを確認するには、次のタスクを実行します。

NetFlow サンプラー マップの定義

NetFlow サンプラー マップを定義するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. `configureterminal`
3. `flow-sampler-map`*sampler-map-name*
4. `moderandomone-out-of`*sampling-rate*
5. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例 : <pre>Router> enable</pre>	(必須) 特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	<code>configureterminal</code> 例 : <pre>Router# configure terminal</pre>	(必須) 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	<code>flow-sampler-map</code><i>sampler-map-name</i> 例 : <pre>Router(config)# flow-sampler-map mysampler1</pre>	(必須) NetFlow サンプラー マップを定義し、フロー サンプラー マップ コンフィギュレーション モードを開始します。 • <i>sampler-map-name</i> 引数は、定義される NetFlow サンプラー マップの名前です。
ステップ 4	<code>moderandomone-out-of</code><i>sampling-rate</i> 例 : <pre>Router(config-sampler)# mode random one-out-of 100</pre>	(必須) ランダム モードをイネーブルにし、NetFlow サンプラー のサンプリング レートを指定します。 • random キーワードは、サンプリングにランダム モードを使用することを指定します。 • one-out-of <i>sampling-rate</i> のキーワードと引数のペアは、サンプリングを行うサンプリング レート (<i>n</i> パケットごとに 1 つ) を指定します。 <i>n</i> には、1 ~ 65535 (パケット) を指定できます。
ステップ 5	<code>end</code> 例 : <pre>Router(config-sampler)# end</pre>	(必須) 現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

インターフェイスへの NetFlow サンプラー マップの適用

NetFlow サンプラー マップをインターフェイスに適用するには、次の手順を実行します。

NetFlow サンプラー マップを物理インターフェイス（またはサブインターフェイス）に適用して、NetFlow サンプラーを作成できます。

手順の概要

1. **イネーブル化**
2. **configureterminal**
3. **interfaceinterface-typeinterface-number**
4. **flow-samplersampler-map-name**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： Router> enable	(必須) 特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Router# configure terminal	(必須) 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	interfaceinterface-typeinterface-number 例： Router(config)# fastethernet 1/0/0.2	(必須) 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	flow-samplersampler-map-name 例： Router(config-if)# flow-sampler mysampler1	(必須) NetFlow サンプラー マップをインターフェイスに適用し、NetFlow サンプラーを作成します。 • <i>sampler-map-name</i> 引数は、インターフェイスに適用する NetFlow サンプラー マップの名前です。
ステップ 5	end 例： Router(config-if)# end	(必須) 現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ランダム サンプル NetFlow の設定の確認

ランダム サンプル NetFlow の設定を確認するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. `showflow-sampler`
3. `showipcacheverboseflow`
4. `showipflowexporttemplate`
5. `end`

手順の詳細

ステップ 1 イネーブル化

このコマンドを使用して、特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

例：

```
Router> enable
Router#
```

ステップ 2 `showflow-sampler`

このコマンドを使用して、1 つまたはすべてのランダム サンプル NetFlow サンプラーの属性（モード、サンプリングレート、サンプリングされたパケットの数など）を表示し、サンプラーの設定を確認します。次に例を示します。

例：

```
Router# show flow-sampler
Sampler : mysampler1, id : 1, packets matched : 10, mode : random sampling mode
sampling interval is : 100
Sampler : myflowsampler2, id : 2, packets matched : 5, mode : random sampling mode
sampling interval is : 200
```

特定の NetFlow サンプラーの属性を確認するには、`show flow-sampler sampler-map-name` コマンドを使用します。たとえば、mysampler1 という名前の NetFlow サンプラーに対しては次のように入力します。

例：

```
Router# show flow-sampler mysampler1
```

```
Sampler : mysampler1, id : 1, packets matched : 0, mode : random sampling mode
sampling interval is : 100
```

ステップ 3 showipcacheverboseflow

このコマンドを使用して、ランダム サンプル NetFlow が設定されているときのヘッダー内の追加の NetFlow フィールドを表示します。次に例を示します。

例：

```
Router# show ip cache verbose flow
...
SrcIf          SrcIPAddress      DstIf          DstIPAddress    Pr TOS Flgs Pkts
Port Msk AS      Port Msk AS      NextHop          B/Pk Active
BGP: BGP NextHop
Fet1/0/0      8.8.8.8          FEt0/0/0*      9.9.9.9         01 00 10      3
0000 /8 302      0800 /8 300      3.3.3.3         100      0.1
BGP: 2.2.2.2      Sampler: 1 Class: 1 FFlags: 01
```

この例では、サンプラー、クラス ID、および一般的なフラグが設定されているときの **show ip cache verbose flow** コマンドの NetFlow 出力を示しています。フローに関して表示される情報は、そのフローに設定されているフラグによって異なります。フローがサンプラーによってキャプチャされた場合は、出力にサンプラー ID が表示されます。フローが MQC によってマーク付けられた場合は、表示にクラス ID が含まれます。一般的なフラグが設定されている場合は、出力にそれらのフラグが含まれます。

show ip cache verbose flow コマンドの出力で表示される可能性のある NetFlow フラグ (FFlags) は、次のとおりです。

- FFlags: 01 (#define FLOW_FLAGS_OUTPUT 0x0001) : 出力フロー
- FFlags: 02 (#define FLOW_FLAGS_DROP 0x0002) : 廃棄されたフロー (ACL による廃棄など)
- FFlags: 08 (#define FLOW_FLAGS_IPV6 0x0008) : IPv6 フロー
- FFlags: 10 (#define FLOW_FLAGS_RSVD 0x0010) : 予備

IPv6 と RSVD の FFlags はあまり使用されません。FFlags がゼロの場合、その行は出力から省略されます。複数のフラグが定義されている場合は (論理和がとられる)、フラグの両方のセットが 16 進数形式で表示されます。

ステップ 4 showipflowexporttemplate

このコマンドを使用して、テンプレート固有の設定に関して NetFlow データ エクスポートの統計情報 (テンプレート タイムアウトやリフレッシュ レートなど) を表示します。次に例を示します。

例：

```
Router# show ip flow export template
Template Options Flag = 0
Total number of Templates added = 0
Total active Templates = 0
Flow Templates active = 0
Flow Templates added = 0
Option Templates active = 0
Option Templates added = 0
Template ager polls = 0
Option Template ager polls = 0
Main cache version 9 export is enabled
Template export information
```



```
Template timeout = 30
Template refresh rate = 20
Option export information
Option timeout = 30
Option refresh rate = 20
```

ステップ 5 end

このコマンドを使用して、特権 EXEC モードを終了します。

例：

```
Router# end
```

トラブルシューティングのヒント

NetFlow キャッシュにマルチキャストフロー レコードがない場合は、マルチキャストスイッチング カウンタをチェックしてプロセススイッチドパケットの存在を確認します（NetFlow では、ファーストスイッチドパケットまたは MDFS スイッチドパケットだけがエクスポートされます）。プロセススイッチドパケットが存在する場合は、MDFS ルーティングテーブルを調べて潜在的な問題を確認します。

NetFlow サンプリングの設定例

ランダム サンプル NetFlow の設定による NetFlow データ エクスポートの影響の軽減例

NetFlow サンプラー マップの定義例

mysampler1 という名前の NetFlow サンプラー マップを定義する例を示します。

```
configure terminal
!
flow-sampler-map mysampler1
mode random one-out-of 100
end
```

NetFlow サンプラー マップのインターフェイスへの適用例

次に、シスコ エクスプレス フォワーディング スwitching をイネーブルにし、mysampler1 という名前の NetFlow サンプラー マップをインターフェイス FastEthernet 1/0/0 に適用して、このインターフェイスで NetFlow サンプラーを作成する方法の例を示します。

```
configure terminal
```

```

!
ip cef
!
interface fastethernet 1/0/0
  flow-sampler mysampler1
end

```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
NetFlow コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『Cisco IOS NetFlow Command Reference』
ネットワーク トラフィックデータをキャプチャし、エクスポートするための NetFlow の設定作業	「NetFlow および NetFlow データ エクスポートの設定」
ランダム サンプル NetFlow の設定作業	「トラックへのネットワーク トラフィックの NetFlow サンプルングを使用した選択」
NetFlow 集約キャッシュの設定作業	「NetFlow 集約キャッシュの設定」
CNS NetFlow Collection Engine のインストール、開始、および設定に関する情報	Cisco CNS NetFlow Collection Engine のマニュアル

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	<p>選択したプラットフォーム、Cisco IOS XE Release、およびフィーチャセットの MIB を検索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。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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>	<p>http://www.cisco.com/en/US/support/index.html</p>

NetFlow サンプルングを使用したトラックへのネットワーク トラフィックの選択の機能情報

表 18 : NetFlow サンプルングを使用したトラックへのネットワーク トラフィックの選択の機能情報

機能名	リリース	機能の設定情報
ランダム サンプル NetFlow	Cisco IOS XE Release 2.1	

機能名	リリース	機能の設定情報
		<p>ランダム サンプル NetFlow では、連続した n 個のパケット (n はユーザが設定可能なパラメータ) ごとにランダムに選択される 1 個のパケットだけ进行处理することにより、Cisco ルータ内のトラフィックのサブセットに関する NetFlow データが得られます。パケットは、到着時にサンプリングされます (これらのパケットに対して NetFlow キャッシュ エントリが作成される前)。統計的なトラフィックのサンプリングによって、価値のある NetFlow データが得られるとともに、ルータ リソースの消費が大幅に削減されます (特に CPU リソース)。ランダム サンプル NetFlow の主な用途は、トラフィック エン지니어リング、容量プランニング、およびフル NetFlow でなくてもネットワーク トラフィックの正確なビューが得られるアプリケーションです。</p> <p>この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。</p> <p>この機能により、debugflow-sampler、flow-sampler、flow-sampler-map、ipflow-export、mode (flowsamplermapconfiguration)、showflow-sampler の各コマンドが追加または変更されました。</p>

用語集

ACL : アクセス コントロール リスト。ルータによって保持されるユーザおよびユーザ グループの参加者リストです。このリストは、多数のサービスについてルータに対するアクセスまたはルータからのアクセスを制御するために使用されます。

BGP : Border Gateway Protocol。Exterior Gateway Protocol (EGP) に代わるドメイン間ルーティングプロトコル。BGP システムは到着可能性情報を他の BGP システムと交換します。RFC 1163 によって定義されています。

CEF : Cisco Express Forwarding。大規模で動的なトラフィック パターンを使用してネットワークのパフォーマンスと拡張性を最適化する、レイヤ 3 IP スイッチング テクノロジー。

高速スイッチング : ルート キャッシュを使用して、ルータを介したパケット交換を促進するシステムの機能。

フロー : 任意の送信元と宛先の間の単方向のパケットのストリーム。送信元と宛先は、ネットワーク層の IP アドレスとトランスポートレイヤの送信元および宛先のポート番号によってそれぞれ定義されます。

MQC : モジュラ Quality of Service (QoS) コマンドラインインターフェイス (CLI)。トラフィック ポリシを作成し、それらをインターフェイスに付加することができる CLI 構造です。1 つのトラフィック ポリシーには、1 つのトラフィック クラスと 1 つ以上の QoS 機能が含まれます。トラフィック ポリシー内にある QoS 機能により、分類後のトラフィックの処理方法が決定されます。

NBAR : Network-Based Application Recognition。Cisco IOS ソフトウェアの分類エンジンです。伝送制御プロトコル (TCP) またはユーザ データグラム プロトコル (UDP) のポート番号を動的に割り当てる Web ベースのアプリケーションやクライアント/サーバアプリケーションなど、多種多様なアプリケーションを認識します。アプリケーションが認識された後は、そのアプリケーションの特定のサービスをネットワークで使用できます。NBAR は、Cisco Content Networking アーキテクチャの重要な要素であり、QoS 機能と連動して、ネットワーク帯域幅の効率的な利用を可能にします。

NetFlow : フロー単位で情報を管理する Cisco IOS XE セキュリティおよびアカウンティング機能。

NetFlow サンプラー : 少なくとも 1 つの物理インターフェイスまたはサブインターフェイスに適用されている NetFlow サンプラー マップ内で定義された特性のセット。

NetFlow サンプラー マップ : NetFlow サンプルング用の特性 (サンプルング レートなど) のセットの定義。

NetFlow v9 : NetFlow エクスポート フォーマットのバージョン 9。ネットワーク ノードからコレクタに NetFlow レコードを送信するための柔軟で拡張可能な手段です。NetFlow バージョン 9 には定義可能なレコードタイプが用意されています。また、自己記述型で、NetFlow Collection Engine の設定を容易にします。

ToS : タイプ オブ サービス (ToS)。特定のデータグラムに必要な Quality of Service を示す、IP ヘッダーの 2 番目のバイトです。



索引

N

- NetFlow アグリゲーション [41](#)
 - プレフィックス-ToS 集約方式 [41](#)
 - 設定 (例) [41](#)

