



NetFlow の設定

この章では、Cisco NX-OS デバイス上で NetFlow 機能を設定する方法について説明します。

この章は、次の内容で構成されています。

- [NetFlow について \(1 ページ\)](#)
- [NetFlow の前提条件 \(5 ページ\)](#)
- [NetFlow に関する注意事項および制約事項 \(5 ページ\)](#)
- [NetFlow の設定 \(9 ページ\)](#)
- [NetFlow 設定の確認 \(20 ページ\)](#)
- [NetFlow のモニタリング \(21 ページ\)](#)
- [NetFlow の表示例 \(21 ページ\)](#)
- [NetFlow のコンフィギュレーション例 \(22 ページ\)](#)

NetFlow について

NetFlow は入力 IP パケットについてパケットフローを識別し、各パケットフローに基づいて統計情報を提供します。NetFlow のためにパケットやネットワークデバイスを変更する必要はありません。

NetFlow ではフローを使用して、アカウントリング、ネットワークモニタリング、およびネットワーク プランニングに関連する統計情報を提供します。フローは送信元インターフェイス (VLAN 向け) に届く単方向のパケットストリームで、キーの値は同じです。キーは、パケット内のフィールドを識別する値です。フローを作成するには、フローレコードを使用して、フロー固有のキーを定義します。

Cisco NX-OS は、ネットワーク異常とセキュリティ問題の高度な検出を有効にする Flexible NetFlow 機能をサポートします。フレキシブル NetFlow 機能を使用すると、大量の定義済みフィールドの集合からキーを選択することで、そのアプリケーションに最適なフローレコードを定義できます。

1 つのフローと見なされるパケットでは、すべてのキー値が一致している必要があります。フローは、設定したエクスポートレコードバージョンに基づいて、関係のある他のフィールドを集めることもあります。フローは NetFlow キャッシュに格納されます。

フロー用に NetFlow が収集したデータをエクスポートするには、フロー エクスポートを使用し、このデータを Cisco Stealthwatch などのリモート NetFlow コレクタにエクスポートします。Cisco NX-OS は次の状況で、NetFlow エクスポート用のユーザデータグラムプロトコル (UDP) データグラムの一部としてフローをエクスポートします。

- フローはフロータイムアウト値に従って定期的にエクスポートされます。設定されていない場合、デフォルトは 10 秒です。
- ユーザがフローの強制的エクスポートを行った。

フローレコードによってフロー用に収集するデータのサイズが決まります。フローモニター、フローレコードおよびフローエクスポートを NetFlow キャッシュ情報と結合します。

Cisco NX-OS は NetFlow 統計を集計し、インターフェイスまたはサブインターフェイス上のすべてのパケットを分析します。

デュアルレイヤ NetFlow の実装

他の Cisco Nexus プラットフォームとは異なり、Cisco Nexus 9000 シリーズスイッチは、NetFlow 処理を次の 2 つのレイヤに分離します。

- 第 1 レイヤは、ラインレートトラフィックのパケット単位の可視性をサポートします。パケットをサンプリングして統計的に分析する必要はありません。代わりに、パケットをラインレートで処理および集約できます。
- 2 番目のレイヤは、大規模なフローの収集を可能にします。フローを失うことなく何十万ものフローを維持でき、定期的に外部コレクタにエクスポートします。

フローレコード

フローレコードでは、パケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。キーと関連フィールドを任意の組み合わせで指定して、フローレコードを定義できます。Cisco NX-OS は、様々なキーセットをサポートしています。フローレコードでは、フロー単位で収集するカウンタのタイプも定義します。32 ビットまたは 64 ビットのパケットカウンタまたはバイトカウンタを設定できます。

キーフィールドは、**match** キーワードで指定されます。対象フィールドとカウンタは **collect** キーワードで指定されます。

Cisco NX-OS では、フローレコードの作成時に次の **match** フィールドをデフォルトとして使用できます。

- match interface input
- match flow direction

フロー エクスポート

フローエクスポートでは、NetFlow エクスポート パケットに関して、ネットワーク層およびトランスポート層の詳細を指定します。フロー エクスポートで設定できる情報は次のとおりです。

- エクスポート宛先 IP アドレス
- 送信元インターフェイス
- UDP ポート番号 (NetFlow コレクタが NetFlow パケットをリスニングするところ) : デフォルト値は 9995 です。



(注) NetFlow エクスポート パケットでは、送信元インターフェイスに割り当てられた IP アドレスを使用します。送信元インターフェイスを設定しない場合、フローエクスポートはエクスポートする予定のフローをドロップします。

Cisco NX-OS は、タイムアウトが発生するたびにデータを NetFlow コレクタへエクスポートします。キャッシュをフラッシュし、フローを強制的にエクスポートするには、フラッシュキャッシュ タイムアウトを設定できます (**flow timeout** コマンドを使用)。

エクスポート形式

Cisco NX-OS は、バージョン 9 のエクスポート形式をサポートします。この形式は、古いバージョン 5 のエクスポート形式よりも効率的なネットワーク使用率をサポートし、IPv6 およびレイヤ 2 フィールドをサポートします。さらに、バージョン 9 エクスポート形式は、NetFlow コレクタで完全な 32 ビット SNMP ifIndex 値をサポートします。

レイヤ 2 NetFlow キー

フレキシブル NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。レイヤ 2 のキーは次のとおりです。

- 送信元および宛先 MAC アドレス
- 送信元 VLAN ID
- イーサネット フレームのイーサネット タイプ

受信方向については、次のインターフェイスに対してレイヤ 2 NetFlow を適用できます。

- アクセス モードのスイッチ ポート
- トランク モードのスイッチ ポート
- レイヤ 2 のポート チャンネル



- (注) Layer 2 NetFlow を VLAN、送信インターフェイス、またはレイヤ 3 インターフェイス (VLAN インターフェイスなど) に適用できます。

フロー モニタ

フロー モニタは、フロー レコードおよびフロー エクスポートを参照します。フロー モニタはインターフェイスに適用します。

NetFlow 出カインターフェイス

FM-E および FM-E2 モジュールを搭載した Cisco Nexus 9300-FX および Cisco Nexus 9500 プラットフォーム スイッチの NetFlow 出カインターフェイスには、次の機能があります。

- **show flow cache** コマンドの NetFlow は `output_if_id` を表示し、出カインターフェイスを 9700-FX ラインカードを備えた Cisco Nexus 9300-FX および 9500 プラットフォーム スイッチのコレクタにエクスポートします。
- Cisco Nexus 9300-FX プラットフォーム スイッチの NetFlow 出カインターフェイスは、IPv4 と IPv6 の両方のトラフィック フローをサポートします。Cisco Nexus 9500 プラットフォーム スイッチの NetFlow 出カインターフェイスは、IPv4 トラフィック フローでのみサポートされ、IPv6 トラフィック フローではサポートされません。**show flow cache** コマンドは、`output_if_id` を `0x0` として表示します。またこの機能は、コントロールプレーントラフィックや ICMP 要求/応答メッセージなど、スイッチ宛でのトラフィック以外のトラフィックでもサポートされます。
- NetFlow は、宛先インターフェイスとしてネクストホップを持つ IPv4/IPv6 着信トラフィック フローのコレクタへの出カインターフェイスのエクスポートをサポートします。InputInt および OutputInt の NetFlow エクスポート形式は、NetFlow コレクタで完全な 32 ビット SNMP ifIndex 値をサポートします。
- NetFlow 出カインターフェイスは、MPLS、VXLAN、GRE などのトンネルトラフィック フローではサポートされません。
- NetFlow 出カインターフェイスの例の詳細については、[NetFlow の表示例 \(21 ページ\)](#) を参照してください。

高可用性

Cisco NX-OS は NetFlow のステートフル リスタートをサポートします。リブート後、Cisco NX-OS は実行コンフィギュレーションを適用します。

フロー キャッシュは再起動で保持されず、再起動中にソフトウェアに送信されるパケットは処理されません。

NetFlow の前提条件

NetFlow の前提条件は、次のとおりです。

- 使用しているデバイスで必要とされるリソースを正しく理解していること。NetFlow はメモリと CPU リソースを消費するからです。

NetFlow に関する注意事項および制約事項



- (注) スケールの情報については、リリース特定の『Cisco Nexus 9000 Series NX-OS Verified Scalability Guide』を参照してください。

NetFlow に関する設定時の注意事項および制約事項は、次のとおりです。

- 次の注意事項は、-EX および -FX ラインカード搭載のすべての Cisco Nexus 9500 プラットフォーム スイッチに適用されます。

-FX ポートがすでに適用されている NetFlow 設定のトランクである場合、-EX ポートをトランクとして設定しても、サポートされていない -EX NetFlow 設定は -FX ポート トランクから削除されません。たとえば、3 つ以上の異なる IPv4 フロー モニタを -FX ポート トランクに適用し、-EX ポートが同じトランクに追加された場合、-EX ポートの制限のみであるため、2 つのモニタを超えるトランクの設定は自動的に削除されません。この設定では、-EX トランク ポートの 2 つのモニタを超えるフローはレポートされないため、-EX ポートと -FX ポートの両方が同じトランクに存在する可能性があるモジュラ スイッチでは、プロトコルごとに 2 つのモニタ (v4/v6/CE) のみを使用することを推奨します。
- NetFlow は、-EX、-FX、および -GX 混合シャーシの Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。-EX、-FX、および -GX 混合シャーシの Cisco Nexus 9500 プラットフォーム スイッチでは、SPAN を NetFlow と同時に使用できます。Cisco Nexus 9500-GX プラットフォーム スイッチは、sFlow 機能を組み合わせた SPAN をサポートしていません。
- Cisco NX-OS リリース 9.3 (4) 以降では、次の RTP / NetFlow モニタリング制限が存在します。

RTP モニタリング機能は、スイッチのすべてのインターフェイスで RTP フローのモニタをイネーブルにし、**show flow rtp detail** コマンド出力で報告します。RTP フローは、16384 ~ 32767 の範囲内の送信元ポートを持つ UDP フローです。RTP モニタリングがイネーブルになっているスイッチ インターフェイスに NetFlow モニタが接続されている場合、そのインターフェイス上のすべてのトラフィック/フロー (RTP フローを含む) が **show flow cache** コマンドの出力で報告されます。RTP フローは、**show flow rtp detail** コマンドの出力に表示されなくなります。接続されたモニタが削除されると、RTP フローが **show flow rtp detail** コマンド出力で再度報告されます。

この制限は、次のスイッチに影響します。

- Cisco Nexus 9336C-FX2
 - Cisco Nexus 93240YC-FX2
 - Cisco Nexus 9348GC-FXP
 - Cisco Nexus 93180YC-FX
 - Cisco Nexus 93108TC-FX
 - Cisco Nexus 9316D-GX
 - Cisco Nexus 93600CD-GX
 - Cisco Nexus 9364C-GX
 - 9636C-RX ラインカードを搭載した Cisco Nexus 9504、9508 および 9516 スイッチ
- Cisco NX-OS リリース 9.3(3) 以降、NetFlow に関する次の無停止インサービス ソフトウェア アップグレード (ND ISSU) の制限がすべての Cisco Nexus 9000 シリーズスイッチに適用されます。
- ND ISSU の実行中、2 分間のエクスポート損失が予想されます。
 - ND ISSU 中は、管理インターフェイスの送信元ポートを持つエクスポートはサポートされません。エクスポート損失は、管理インターフェイスが起動するまで予想されません。
- **record netflow ipv4 original-input**、**record netflow ipv4 original-output**、および **record netflow layer2-switched input** コマンドは、Cisco NX-OS リリース 9.3(1) ではサポートされていません。
- Cisco NX-OS リリース 9.2(2) 以降、Cisco Nexus 9300-FX スイッチは NetFlow データ エクスポート (NDE) の OUTPUT_SNMP フィールドの収集をサポートしています。他の Cisco Nexus 9000 プラットフォームスイッチまたは Cisco Nexus ラインカードは、OUTPUT_SNMP フィールドの収集をサポートしていません。
- Cisco Nexus 9300-FX プラットフォーム スイッチに対して、レイヤ 2 NetFlow に対してすでに設定されているポート チャネルにメンバを追加すると、NetFlow の設定が削除され、ポート チャネルのレイヤ 2 設定が追加されます。
- NetFlow はトンネルインターフェイスではサポートされていません。
- NetFlow は、CPU で送信されるパケットではサポートされません。
- 入力 NetFlow のみがサポートされます。出力 NetFlow はサポートされていません。
- フローキャッシュは、レイヤ 2、IPv4、IPv6 などのフロータイプごとにクリアできます。フロー モニタごとにクリアすることはできません。
- フロー収集は ARP トラフィックに対して実行されません。

- NetFlow データエクスポート (NDE) では、送信元インターフェイスを設定する必要があります。送信元インターフェイスを設定しない場合、フローエクスポートはエクスポートする予定のフローをドロップします。
- レイヤ 2 スイッチドフロー モニタは、レイヤ 2 インターフェイスにのみ適用されます。IP および IPv6 フロー モニタは、VLAN、SVI、レイヤ 3 ルーテッドインターフェイス、またはサブインターフェイスに適用できます。
- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスへ変更するか、レイヤ 3 インターフェイスをレイヤ 2 インターフェイスへ変更すると、ソフトウェアで、インターフェイスからレイヤ 2 の NetFlow 設定が削除されます。
- 同じフロー モニタを VLAN およびレイヤ 3 インターフェイス (物理レイヤ 3 インターフェイス、SVI インターフェイス、またはレイヤ 3 サブインターフェイスなど) と共有することはできません。ACL は異なるため共有できないため、VLAN とレイヤ 3 インターフェイスを区別する必要があります。これらは 2 つの異なるプロファイルとして扱う必要があります。
- ロールバック中、ハードウェアでプログラムされているレコードを変更しようとする、ロールバックは失敗します。
- Cisco NX-OS リリース 9.2(1) 以降：
 - FEX レイヤ 3 ポートの NetFlow は Cisco Nexus 9300 EX と 9300 FX プラットフォームスイッチでサポートされています。
 - Cisco Nexus 9300-EX プラットフォームスイッチで NetFlow CE がサポートされています。



注 すべての -EX タイプのプラットフォームスイッチ (Cisco Nexus 9700-FX ラインカードを含む) では、CE NetFlow は非 IPv4 および IPv6 トラフィック フローの CE フローレコードのみをキャプチャします。-FX および -FX2 タイプのプラットフォームスイッチとラインカードでは、**mac packet-classify** がインターフェイスに適用されている限り、IP フローの CE フロー データをキャプチャできます。

- Cisco Nexus 9300-EX プラットフォームスイッチの場合、VLAN または SVI に適用されたフロー モニタは、スイッチドトラフィックとルーテッドトラフィックの両方のフローを収集できます。Cisco Nexus 9300-FX プラットフォームスイッチの場合、NetFlow VLAN はスイッチドトラフィックに対してのみサポートされ、NetFlow SVI はルーテッドトラフィックに対してのみサポートされます。
- Cisco Nexus 9300-EX プラットフォームスイッチは、同じインターフェイスで NetFlow と SPAN を同時にサポートします。この機能は、SPAN および sFlow の代わりに使用できません。

- Cisco Nexus 9300-EX/FX プラットフォーム スイッチ、および EX/FX モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、SPAN と sFlow の両方を同時に有効にすることはできません。一方がアクティブな場合、もう一方は有効にできません。ただし、Cisco Nexus 9300-EX/FX/FX2 および -EX モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、NetFlow と SPAN の両方を同時に有効にすることができ、sFlow と SPAN を使用する代わりに実行可能です。



注 Cisco Nexus 9300-FX2 プラットフォーム スイッチは、sFlow と SPAN の共存をサポートします。

- Cisco Nexus 9300-EX プラットフォーム スイッチでは、同じフロー モニタを VLAN と SVI に同時に接続することはできません。
- Cisco Nexus 9300-EX プラットフォーム スイッチには専用の TCAM があり、カービングは必要ありません。
- ing-netflow リージョンの TCAM カービング設定は、-FX ラインカードでは実行できます。-EX ラインカードでは、デフォルトの ing-netflow リージョン TCAM カービングが 1024 であり、それ以外の場合は設定できません。-EX および -FX ラインカードのポートの場合、ing-netflow リージョンの推奨最大値は 1024 です。
- ToS フィールドは、Cisco Nexus 9300-EX プラットフォーム スイッチではエクスポートされません。
- IP ToS に基づくレコード一致は、IPv6 フロー モニタではサポートされません。ToS 値は、トラフィックが保持する値に関係なく、コレクタで 0x0 として収集されます。

この制限は、次のプラットフォーム スイッチ ファミリに適用されます。

- Cisco Nexus 9300-EX
 - Cisco Nexus 9300-FX
 - Cisco Nexus 9300-FX2
 - Cisco Nexus 9300-FX3
 - Cisco Nexus 9300-GX
 - -EX または FX ライン カード搭載の Cisco Nexus 9500
- Cisco Nexus 3232C および 3264Q スイッチは、NetFlow をサポートしていません。
 - Cisco NX-OS リリース 10.1(2) 以降、Netflow は N9K-X9716D-GX ライン カードでサポートされます。
 - この機能をサポートするプラットフォームでのみ NetFlow を有効にします。
 - Cisco NX-OS リリース 10.2(1)F 以降、レイヤ 2 インターフェイス上のレイヤ 3 NetFlow は、Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FX3、9300-GX、および 9300-GX2 プラットフォーム、9500-EX LC および 9500-FX LC でサポートされます。

- レイヤ 3 フロー モニタまたはレイヤ 2 フロー モニタのいずれかをレイヤ 2 インターフェイスに接続できます（両方は接続できません）。
- フロー モニタがすでにレイヤ 3 インターフェイスに接続されている場合、同じフロー モニタをレイヤ 2 インターフェイスに接続することはできません。
- レイヤ 3 フロー モニタがレイヤ 2 インターフェイスに適用されている場合、**mac-packet-classify** コマンドはサポートされません。



(注) 確認済みの NetFlow のスケール数については、『[Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#)』を参照してください。

NetFlow の設定

NetFlow を設定する手順は、次のとおりです。

手順

- ステップ 1** NetFlow 機能を有効にします。
- ステップ 2** フローにキーおよびフィールドを指定することによって、フロー レコードを定義します。
- ステップ 3** エクスポートフォーマット、プロトコル、宛先、およびその他のパラメータを指定することによって、任意でフロー エクスポートを定義します。
- ステップ 4** フロー レコードおよびフロー エクスポートに基づいて、フロー モニタを定義します。
- ステップ 5** 送信元インターフェイス、サブインターフェイス、または VLAN インターフェイスにフロー モニタを適用します。

NetFlow 機能の有効化

フローを設定するには、先に NetFlow をグローバルで有効しておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</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。

	コマンドまたはアクション	目的
ステップ 2	[no] feature netflow 例： <code>switch(config)# feature netflow</code>	NetFlow 機能を有効にします。デフォルトではディセーブルになっています。 (注) N9K-T2 EoR を搭載した Cisco Nexus 9500 プラットフォームスイッチは、NetFlow をサポートしていません。
ステップ 3	(任意) copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	実行設定を、スタートアップ設定にコピーします。

フローレコードの作成

フローレコードを作成し、照合するためのキー、および収集するための非キーフィールドをフロー内に追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル コンフィギュレーションモードを開始します。
ステップ 2	flow record name 例： <code>switch(config)# flow record Test</code> <code>switch(config-flow-record)#</code>	フローレコードを作成し、フローレコードコンフィギュレーションモードを開始します。フローレコード名には最大 63 文字の英数字を入力できます。
ステップ 3	(任意) description string 例： <code>switch(config-flow-record)# description IPv4Flow</code>	最大 63 文字で、フローレコードの説明を示します。
ステップ 4	(任意) match type 例： <code>switch(config-flow-record)# match transport destination-port</code>	一致キーを指定します。詳細については、 match パラメータの指定 (11 ページ) を参照してください。

	コマンドまたはアクション	目的
		(注) レイヤ4ポートデータをエクスポートするには、 match transport destination-port および match ip protocol コマンドが必要です。
ステップ 5	(任意) collect type 例： switch(config-flow-record)# collect counter packets	コレクションフィールドを指定します。詳細については、 collect パラメータの指定 (12 ページ) を参照してください。
ステップ 6	(任意) show flow record [name] [record-name] {netflow-original netflow protocol-port netflow {ipv4 ipv6} {original-input original-output}} 例： switch(config-flow-record)# show flow record netflow protocol-port	NetFlow のフローレコード情報を表示します。フローレコード名には最大 63 文字の英数字を入力できます。
ステップ 7	(任意) copy running-config startup-config 例： switch(config-flow-record)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

match パラメータの指定

フローレコードごとに、次の match パラメータを 1 つ以上設定する必要があります。

コマンド	目的
match datalink {mac source-address mac destination-address ethertype vlan} 例： switch(config-flow-record)# match datalink ethertype	レイヤ2属性をキーとして指定します。

コマンド	目的
<p>match ip {protocol tos}</p> <p>例:</p> <pre>switch(config-flow-record)# match ip protocol</pre>	<p>IP プロトコルまたは ToS フィールドをキーとして指定します。</p> <p>(注) レイヤ 4 ポートデータをエクスポートするには、match transport destination-port および match ip protocol コマンドが必要です。</p> <p>データは show hardware flow ip コマンドの出力に収集されて表示されますが、両方のコマンドを設定するまで収集とエクスポートは行われません。</p>
<p>match ipv4 {destination address source address}</p> <p>例:</p> <pre>switch(config-flow-record)# match ipv4 destination address</pre>	<p>IPv4 送信元または宛先アドレスをキーとして指定します。</p>
<p>match ipv6 {destination address source address flow-label options}</p> <p>例:</p> <pre>switch(config-flow-record)# match ipv6 flow-label</pre>	<p>IPv6 キーを指定します。</p>
<p>match transport {destination-port source-port}</p> <p>例:</p> <pre>switch(config-flow-record)# match transport destination-port</pre>	<p>トランスポート送信元または宛先ポートをキーとして指定します。</p> <p>(注) レイヤ 4 ポートデータをエクスポートするには、match transport destination-port および match ip protocol コマンドが必要です。</p> <p>データは show hardware flow ip コマンドの出力に収集されて表示されますが、両方のコマンドを設定するまで収集とエクスポートは行われません。</p>

collect パラメータの指定

フロー レコードごとに、次の collect パラメータを 1 つ以上設定する必要があります。

コマンド	目的
collect counter {bytes packets} [long] 例: <pre>switch(config-flow-record)# collect counter packets</pre>	フローからパケットベースまたはバイトカウンタを収集します。任意で、64ビットカウンタを使用することを指定できます。
collect ip version 例: <pre>switch(config-flow-record)# collect ip version</pre>	フローの IP バージョンを収集します。
collect timestamp sys-uptime {first last} 例: <pre>switch(config-flow-record)# collect timestamp sys-uptime last</pre>	フローの先頭または最終パケットに関するシステム稼働時間を収集します。
collect transport tcp flags 例: <pre>switch(config-flow-record)# collect transport tcp flags</pre>	フローのパケットに対応する TCP トランスポート層フラグを収集します。

フロー エクスポートの作成

フロー エクスポートの設定では、フローに対するエクスポート パラメータを定義し、リモート NetFlow Collector への到達可能性情報を指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例: <pre>switch# configure terminal switch(config)#</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 2	flow exporter name 例: <pre>switch(config)# flow exporter flow-exporter-one switch(config-flow-exporter)#</pre>	フローエクスポートを作成し、フローエクスポート コンフィギュレーション モードを開始します。フローエクスポート名を最大 63 文字の英数字で入力できます。
ステップ 3	destination {ipv4-address ipv6-address} [use-vrf name] 例: <pre>switch(config-flow-exporter)# destination 192.0.2.1</pre>	このフローエクスポートの宛先 IPv4 または IPv6 アドレスを設定します。任意で、NetFlow Collector に到達するために使用する VRF を設定できます。

	コマンドまたはアクション	目的
		VRF 名には最大 32 文字の英数字を入力できます。
ステップ 4	source <i>interface-type name/port</i> 例： <pre>switch(config-flow-exporter)# source ethernet 2/1</pre>	設定された宛先で NetFlow Collector に到達するために使用するインターフェイスを指定します。
ステップ 5	(任意) description <i>string</i> 例： <pre>switch(config-flow-exporter)# description exportversion9</pre>	このフローエクスポートについて説明します。説明には最大 63 文字の英数字を入力できます。
ステップ 6	(任意) dscp <i>value</i> 例： <pre>switch(config-flow-exporter)# dscp 0</pre>	DSCP (DiffServ コードポイント) 値を指定します。範囲は 0 ~ 63 です。
ステップ 7	(任意) transport udp port 例： <pre>switch(config-flow-exporter)# transport udp 200</pre>	NetFlow Collector に到達するために使用する UDP ポートを指定します。範囲は 0 ~ 65535 です。 (注) UDP ポートを指定しない場合は、9995 がデフォルトとして選択されます。
ステップ 8	version 9 例： <pre>switch(config-flow-exporter)# version 9 switch(config-flow-exporter-version-9)#</pre>	NetFlow エクスポート バージョンを指定します。フローエクスポートのバージョン 9 コンフィギュレーションサブモードを開始するには、バージョン 9 を選択します。
ステップ 9	(任意) option {exporter-stats interface-table} timeout seconds 例： <pre>switch(config-flow-exporter-version-9)# option exporter-stats timeout 1200</pre>	フローエクスポートの統計情報再送信タイマーを設定します。値の範囲は 1 ~ 86400 秒です。
ステップ 10	(任意) template data timeout seconds 例： <pre>switch(config-flow-exporter-version-9)# template data timeout 1200</pre>	テンプレートデータ再送信タイマーを設定します。値の範囲は 1 ~ 86400 秒です。
ステップ 11	(任意) copy running-config startup-config 例：	実行設定を、スタートアップ設定にコピーします。

	コマンドまたはアクション	目的
	switch(config-flow-exporter-version-9) # copy running-config startup-config	

フロー モニタの作成

フロー モニタを作成して、フロー レコードおよびフロー エクスポートと関連付けることができます。1つのモニタに属しているすべてのフローは、様々なフィールド上で照合するために関連するフローレコードを使用します。データは指定されたフローエクスポートにエクスポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	flow monitor name 例： switch(config)# flow monitor flow-monitor-one switch(config-flow-monitor)#	フロー モニタを作成し、フロー モニタ コンフィギュレーション モードを開始します。フロー モニタ名を最大 63 文字の英数字で入力できます。
ステップ 3	(任意) description string 例： switch(config-flow-monitor) # description IPv4Monitor	このフローモニタについて説明します。説明には最大 63 文字の英数字を入力できます。
ステップ 4	(任意) exporter name 例： switch(config-flow-monitor) # export v9	フロー エクスポートとこのフロー モニタを関連付けます。エクスポート名には最大 63 文字の英数字を入力できます。
ステップ 5	record name [netflow-original netflow protocol-port netflow {ipv4 ipv6} {original-input original-output}] 例： switch(config-flow-monitor) # record IPv4Flow	フロー レコードを指定したフロー モニタと関連付けます。レコード名には最大 63 文字の英数字を入力できます。 (注) record netflow ipv4 original-input 、 record netflow ipv4 original-output 、 record netflow layer2-switched input は、Cisco NX-OS リリース 9.3(1) ではサポートされていません。

	コマンドまたはアクション	目的
ステップ 6	(任意) copy running-config startup-config 例 : <pre>switch(config-flow-monitor)# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

インターフェイスへのフロー モニタの適用

フロー モニタは入力インターフェイスに適用できます。出力 NetFlow はサポートされていません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</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 2	interface vlan <i>vlan-id</i> 例 : <pre>switch(config)# interface vlan 10 switch(config-if)#</pre>	VLAN インターフェイスを設定し、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 3	ip flow monitor {ipv4 ipv6 layer-2-switched} input 例 : <pre>switch(config-if)# ip flow monitor ipv4 input</pre>	入力パケットのインターフェイスに、IPv4、IPv6、またはレイヤ 2 スイッチ フロー モニタを関連付けます。
ステップ 4	(任意) copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

VLAN 上でのブリッジ型 NetFlow の設定

VLAN のレイヤ 2 スイッチド パケットでレイヤ 3 データを収集するために、VLAN にフロー モニタを適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	vlan configuration <i>vlan-id</i> 例： switch(config)# vlan configuration 30 switch(config-vlan-config)#	VLAN コンフィギュレーション モードを開始します。VLAN ID の範囲は 1 ~ 3967 または 4048 ~ 4093 です。 (注) VLAN コンフィギュレーション モードでは、作成とは無関係に VLAN を設定できます。これは、VTP クライアントのサポートに必要です。
ステップ 3	{ip ipv6} flow monitor <i>name</i> 例： switch(config-vlan-config)# ip flow monitor testmonitor	入力パケットのフロー モニタを VLAN に関連付けます。フロー モニタ名を最大 63 文字の英数字で入力できます。
ステップ 4	(任意) copy running-config startup-config 例： switch(config-vlan-config)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

レイヤ 2 NetFlow キーの設定

フレキシブル NetFlow レコード内でレイヤ 2 キーを定義できます。このレコードを使用して、レイヤ 2 インターフェイスのフローをキャプチャできます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	flow record <i>name</i> 例：	フローレコードコンフィギュレーションモードを開始します。フローレコードの設定の詳細については、 フローレ

	コマンドまたはアクション	目的
	<pre>switch(config)# flow record L2_record switch(config-flow-record)#</pre>	コードの作成 (10 ページ) を参照してください。
ステップ 3	<p>match datalink {mac source-address mac destination-address ethertype vlan}</p> <p>例 :</p> <pre>switch(config-flow-record)# match datalink ethertype</pre>	レイヤ 2 属性をキーとして指定します。
ステップ 4	<p>exit</p> <p>例 :</p> <pre>switch(config-flow-record)# exit switch(config)#</pre>	フローレコードコンフィギュレーションモードを終了します。
ステップ 5	<p>interface {ethernet slot/port port-channel number}</p> <p>例 :</p> <pre>switch(config)# interface Ethernet 6/3 switch(config-if#)</pre>	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。インターフェイス タイプは、物理的なイーサネットポートまたはポートチャネルを指定できます。
ステップ 6	<p>switchport</p> <p>例 :</p> <pre>switch(config-if)# switchport</pre>	インターフェイスをレイヤ 2 の物理インターフェイスに変更します。スイッチポートの設定に関する詳細については、「Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド」を参照してください。
ステップ 7	<p>mac packet-classify</p> <p>例 :</p> <pre>switch(config-if)# mac packet-classify</pre>	<p>パケットの MAC 分類を強制します。</p> <p>このコマンドの使用に関する詳細については、「Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド」を参照してください。</p> <p>(注) フローを検出するためにこのコマンドを使用する必要があります。</p>
ステップ 8	<p>layer2-switched flow monitor flow-name input</p> <p>例 :</p> <pre>switch(config-if)# layer2-switched flow monitor L2_monitor input</pre>	フローモニタをスイッチポートの入力パケットに関連付けます。フローモニタ名を最大 63 文字の英数字で入力できます。

	コマンドまたはアクション	目的
ステップ 9	(任意) show flow record netflow layer2-switched input 例： switch(config-if)# show flow record netflow layer2-switched input	レイヤ2 NetFlow のデフォルト レコードの情報を表示します。
ステップ 10	(任意) copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

レイヤ2 インターフェイスでのレイヤ3 NetFlow の設定

レイヤ2 インターフェイスでレイヤ3 フロー情報をキャプチャするために、レイヤ2 インターフェイスでレイヤ3 フロー モニタを定義できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	flow record name 例： switch(config)# flow record L3_record switch(config-flow-record)#	フロー レコード コンフィギュレーション モードを開始します。フロー レコードの設定の詳細については、 フロー レコードの作成 (10 ページ) を参照してください。
ステップ 3	interface {ethernet slot/port port-channel number} 例： switch(config)# interface Ethernet 6/3 switch(config-if#)	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。インターフェイス タイプは、物理的なイーサネット ポートまたはポート チャネルを指定できます。
ステップ 4	switchport 例： switch(config-if)# switchport	インターフェイスをレイヤ2 モードに変更します。スイッチ ポートの設定に関する詳細については、「 Cisco Nexus 9000 シリーズ NX-OS レイヤ2 スイッチング 設定ガイド 」を参照してください。

	コマンドまたはアクション	目的
ステップ 5	ip flow monitor <i>flow-name</i> input 例： switch(config-if)# ip flow monitor v41 input	フロー モニタをスイッチ ポートの入力 パケットに関連付けます。フロー モニ タ名を最大 63 文字の英数字で入力でき ます。
ステップ 6	ipv6 flow monitor <i>flow-name</i> input 例： switch(config-if)# ipv6 flow monitor v61 input	IPv6 フロー モニタをスイッチ ポートの 入力パケットに関連付けます。フロー モニタ名を最大 63 文字の英数字で入力 できます。
ステップ 7	(任意) copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	実行設定を、スタートアップ設定にコ ピーします。

NetFlow タイムアウトの設定

任意で、システム内のすべてのフローに適用されるグローバルな NetFlow タイムアウトを設定
できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	flow timeout <i>seconds</i> 例： switch(config)# flow timeout 30	フラッシュ タイムアウト値を秒単位で 設定します。範囲は 5 ～ 60 秒です。デ フォルト値は 10 秒です。
ステップ 3	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	実行設定を、スタートアップ設定にコ ピーします。

NetFlow 設定の確認

NetFlow 設定を表示するには、次のタスクのうちのいずれかを実行します。

コマンド	目的
show flow cache [ipv4 ipv6 ce]	NetFlow IP フローに関する情報を表示します。
show flow exporter [name]	NetFlow のフローエクスポート情報と統計情報を表示します。フローエクスポート名を最大 63 文字の英数字で入力できます。
show flow interface [interface-type slot/port]	NetFlow インターフェイスに関する情報を表示します。
show flow record [name]	NetFlow のフローレコード情報を表示します。フローレコード名には最大 63 文字の英数字を入力できます。
show flow record netflow layer2-switched input	レイヤ 2 NetFlow コンフィギュレーションの情報を表示します。
show running-config netflow	現在デバイスにある NetFlow 設定を表示します。

NetFlow のモニタリング

NetFlow の統計情報を表示するには、**show flow exporter** コマンドを使用します。NetFlow エクスポートの統計情報を消去するには、**clear flow exporter** コマンドを使用します。

NetFlow の表示例

IPv4 の **show flow cache** コマンドの出力には、次のように表示されます。

```

show flow cache
IPV4 Entries
SIP          DIP          BD ID  S-Port  D-Port  Protocol  Byte Count  Packet Count  TCP
FLAGS  TOS  if_id      output_if_id  flowStart  flowEnd
10.10.30.4  30.33.1.2   1480   30000   17998   17         683751850   471553         0x0
          0x0  0x90105c8  0x1a005000   14096494  14153835
30.33.1.2   10.10.39.4  4145   30000   18998   17         43858456   30164         0x0
          0x0  0x1a005000  0x1a006600   14096477  14099491
10.10.29.4  30.33.1.2   1479   30000   17998   17         683751850   471553         0x0
          0x0  0x90105c7  0x1a005000   14096476  14153817
10.10.7.4   30.33.1.2   1457   30000   17998   17         683753300   471554         0x0
          0x0  0x90105b1  0x1a005000   14096481  14153822
30.33.1.2   10.10.42.4  4145   30000   18998   17         95289344   65536         0x0
          0x0  0x1a005000  0x1a006600   14112551  14119151
10.10.49.4  30.33.1.2   1499   30000   17998   17         683753300   471554         0x0
          0x0  0x90105db  0x1a005000   14096486  14153827

```

NetFlow のコンフィギュレーション例

この例では、IPv4 に対して NetFlow エクスポートを設定する方法を示します。

```
feature netflow
flow exporter ee
  destination 171.70.242.48 use-vrf management
  source mgmt0
  version 9
  template data timeout 20
flow record rr
  match ipv4 source address
  match ipv4 destination address
  collect counter bytes
  collect counter packets
flow monitor foo
  record rr
  exporter ee
interface Ethernet2/45
  ip flow monitor foo input
  ip address 10.20.1.1/24
  no shutdown
```