Cisco IOS XE Flexible NetFlow フロー サンプリングを使用したトラフィック分析の CPU オーバーヘッドの軽減

このドキュメントには、Flexible NetFlow のトラフィック分析による CPU オーバーヘッドを軽減するためのサンプリングの設定について、およびその方法に関する説明が記載されています。

NetFlow は、ルータを通過するパケットの統計情報が得られる Cisco IOS XE テクノロジーです。NetFlow は、IP ネットワークから IP 運用データを取得するための規格です。NetFlow は、ネットワークとセキュリティの監視、ネットワーク計画、トラフィック分析、および IP アカウンティングをサポートするためのデータを提供します。

Flexible NetFlow は、実際の要件に合わせてトラフィック分析パラメータをカスタマイズする機能を追加することで、以前の NetFlow よりも改善されています。Flexible NetFlow では、トラフィック分析のための非常に複雑な構成を作成したり、再利用可能な構成コンポーネントを使用してデータをエクスポートすることが容易になります。

機能情報の検索

ご使用のソフトウェア リリースによっては、このモジュールに記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Flexible NetFlow の機能情報」（P.10）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

目次

フロー サンプリングを使用するための前提条件

Flexible NetFlow を設定する前に、次の前提条件を満たしておく必要があります。

- 「Cisco IOS XE Flexible NetFlow Overview」モジュールに記載された内容をよく理解していること。
- ネットワーク デバイスで、Flexible NetFlow がサポートされた Cisco IOS リリースが稼動していること。Flexible NetFlow をサポートした Cisco IOS ソフトウェア リリースのリストについては、「Cisco IOS Flexible NetFlow Features Roadmap」を参照してください。

IPv4 トラフィック

- ネットワーク デバイスが IPv4 ルーティング用に設定されていること。

Flexible NetFlow サンプラについて

Flexible NetFlow サンプラを設定する前に、次の概念を理解しておく必要があります。

フロー サンプラ

フロー サンプラは、ルータのコンフィギュレーションで別のコンポーネントとして作成されます。フロー サンプラは、分析用に選択されるパケットの数を制限することで、Flexible NetFlow を実行しているデバイス上の負荷を減らすために使用されます。サンプラでは、ランダムまたは確定的サンプリング手法（モード）を使用します。

- 確定的：サンプルを取得するたびに、同じサンプリング位置が使用されます。
- ランダム：サンプルを取得するたびに、ランダムに選択されたサンプリング位置が使用されます。

フロー サンプリングでは、ルータのパフォーマンスに対するモニタリング精度が交換されます。サンプラをフロー モニタに適用すると、フロー モニタが分析する必要のあるパケット数が減少するため、ルータでフロー モニタを実行するためのオーバーヘッド負荷が低下します。フロー モニタで分析されるパケット数が減少すると、フロー モニタのキャッシュに格納される情報の精度が、それに応じて低下します。

ip flow monitor コマンドを使用してインターフェイスに適用する場合、サンプラとフロー モニタを組み合わせます。

Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドを軽減するためのフロー サンプリングの設定方法

フロー サンプリングを使用すると、分析対象のパケット数が減少し、Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドが軽減されます。

（注） 次の作業では、これらのタスクで使用される Flexible NetFlow コマンドに必要なキーワードおよび引数のみについて説明します。これらの Flexible NetFlow コマンドで使用可能なその他のキーワードと引数については、『*Cisco IOS Flexible NetFlow Command Reference*』を参照してください。

Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドを軽減するためにフロー サンプリングを設定するには、次の作業を実行します。

- 「フロー モニタの設定」（P.3）（必須）
- 「フロー サンプリングの設定およびイネーブル化」（P.4）（必須）
- 「フロー サンプラ設定のステータスと統計情報の表示」（P.6）（任意）

フロー モニタの設定

サンプラはフロー モニタと連携してインターフェイスに適用されます。サンプリングをイネーブルにするには、フロー モニタを作成して、分析するトラフィック タイプを設定する必要があります。フロー モニタを設定するには、次の必須タスクを実行します。

フロー モニタ

各フロー モニタには、専用のキャッシュが割り当てられています。フロー モニタごとに、キャッシュ エントリの内容およびレイアウトを定義するレコードが必要です。レコード フォーマットは、事前定義済みのレコード フォーマットのいずれかにすることもできますが、上級のユーザであれば Flexible NetFlow フロー レコード コンフィギュレーション モードで **collect** および **match** コマンドを使用して独自のレコード フォーマットを作成することもできます。

制約事項

フロー モニタで **record** コマンドのパラメータを変更する前に、**no ip flow monitor** コマンドを使用して、すべてのインターフェイスから適用済みのフロー モニタを削除する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name* | **netflow-original** | **netflow ipv4** *record* [**peer**]}
6. **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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**flow monitor** *monitor-name* **例：** `Router(config)# flow monitor FLOW-MONITOR-1`	フロー モニタを作成し、Flexible NetFlow 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。 • このコマンドでは、既存のフロー モニタを変更することもできます。
ステップ 4	**description** *description* **例：** `Router(config-flow-monitor)# description Used for basic traffic analysis`	（任意）フロー モニタの説明を作成します。
ステップ 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4**} *record* [**peer**]} **例：** `Router(config-flow-monitor)# record netflow ipv4 original-input`	フロー モニタのレコードを指定します。
ステップ 6	**end** **例：** `Router(config-flow-monitor)# end`	Flexible NetFlow フロー モニタ 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。

フロー サンプリングの設定およびイネーブル化

フロー サンプラを設定してイネーブルにするには、次の必須タスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sampler** *sampler-name*
4. **description** *description*
5. **mode** {**deterministic** | **random**} **1 out-of** *window-size*
6. **exit**
7. **interface** *type number*

8. **ip flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**}
9. **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	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**sampler** *sampler-name* **例：** `Router(config)# sampler SAMPLER-1`	サンプラを作成し、サンプラ コンフィギュレーション モードを開始します。 • このコマンドでは、既存のサンプラを変更することもできます。
ステップ 4	**description** *description* **例：** `Router(config-sampler)# description Sample at 50%`	（任意）フロー サンプラの説明を作成します。
ステップ 5	**mode** {**deterministic** | **random**} **1 out-of** *window-size* **例：** `Router(config-sampler)# mode random 1 out-of 2`	サンプラ モードおよびフロー サンプラのウィンドウ サイズを指定します。 • *window-size* 引数の範囲は、2 ～ 32,768 です。
ステップ 6	**exit** **例：** `Router(config-sampler)# exit`	サンプラ 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。
ステップ 7	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0/0`	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 8	**ip flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**} **例：** `Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input`	作成したフロー モニタおよびフロー サンプラをインターフェイスに割り当てて、サンプリングをイネーブルにします。
ステップ 9	**end** **例：** `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

フロー サンプラ設定のステータスと統計情報の表示

設定済みでイネーブル化したフロー サンプラのステータスおよび統計情報を表示するには、次の任意の作業を実行します。

手順の概要

1. **enable**
2. **show sampler** *sampler-name*

手順の詳細

ステップ 1 **enable**

enable コマンドによって、特権 EXEC モードを開始します（プロンプトが表示されたらパスワードを入力します）。

```
Router> enable

Router#
```

ステップ 2 **show sampler** *sampler-name*

show sampler コマンドでは、指定するサンプラの現在のステータスを表示します。

```
Router# show sampler SAMPLER-1

Sampler SAMPLER-1:
  ID:             2
  Description:    Sample at 50%
  Type:           random
  Rate:           1 out of 2
  Samples:        2482
  Requests:       4964
  Users (1):
    flow monitor FLOW-MONITOR-1 (ip,Et0/0,I  2482 out of 4964
```

Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドを軽減するためにフロー サンプリングを使用する設定例

ここでは、次の設定例について説明します。

例：IPv4 トラフィックの確定的サンプラの設定およびイネーブル化

次の例では、IPv4 出力トラフィックの確定的サンプリングを設定し、イネーブルにする方法を示します。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-output
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
!
interface FastEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 output
!
```

次の例では、IPv4 入力トラフィックの確定的サンプリングを設定し、イネーブルにする方法を示します。

このサンプルは、グローバル コンフィギュレーション モードから開始します。

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
!
interface FastEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!
```

例：インターフェイスでフロー モニタがすでにイネーブルの場合にフロー モニタにサンプラを追加する

次の例では、サンプラなしでインターフェイスでイネーブルになっているフロー モニタにサンプラを追加する場合の動作を示します。

```
Router(config)# interface FastEthernet 0/0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input

% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

次の例では、フロー モニタをサンプラと一緒にイネーブルにできるようにするために、インターフェイスからいったん削除する方法を示します。

```
Router(config)# interface FastEthernet 0/0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

例：フロー モニタからのサンプラの削除

次の例では、サンプラのキーワードおよび引数なしで再び flow monitor コマンドを入力して、インターフェイス上のフロー モニタからサンプラを削除する場合の動作を示します。

```
Router(config)# interface FastEthernet 0/0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input

% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.
```

次の例では、サンプラなしでイネーブルにできるように、サンプラと一緒にイネーブルになっているフロー モニタをインターフェイスから削除する方法を示します。

```
Router(config)# interface FastEthernet 0/0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

関連情報

QoS（Quality of Service）と帯域幅モニタリング、アプリケーションおよびユーザ フロー モニタリングとプロファイリング、セキュリティ分析など、特定の目的に対する Flexible NetFlow の高度な設定の詳細については、「Customizing Cisco IOS XE Flexible NetFlow Flow Records and Flow Monitors」モジュールを参照してください。

Flexible NetFlow に対して事前定義済みのレコードを設定する場合は、「Configuring Cisco IOS XE Flexible NetFlow with Predefined Records」モジュールを参照してください。

Flexible NetFlow に対してデータ エクスポートを設定する場合は、「Configuring Data Export for Cisco IOS XE Flexible NetFlow with Flow Exporters」モジュールを参照してください。

参考資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Flexible NetFlow の概要	「Cisco IOS XE Flexible NetFlow Overview」
Flexible NetFlow の機能ロードマップ	「Cisco IOS Flexible NetFlow Features Roadmap」
Flexible NetFlow での以前の NetFlow のエミュレート	「Getting Started with Configuring Cisco IOS XE Flexible NetFlow」
Flexible NetFlow データをエクスポートするためのフロー エクスポータの設定	「Configuring Data Export for Cisco IOS XE Flexible NetFlow with Flow Exporters」
Flexible NetFlow のカスタマイズ	「Customizing Cisco IOS XE Flexible NetFlow Flow Records and Flow Monitors」
事前定義済みレコードを使用した Flexible NetFlow の設定	「Configuring Cisco IOS XE Flexible NetFlow with Predefined Records」
Flexible NetFlow のコンフィギュレーション コマンド	『*Cisco IOS Flexible NetFlow Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに対する MIB を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 3954	『*Cisco Systems NetFlow Services Export Version 9*』

シスコのテクニカル サポート

説明	リンク
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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

Flexible NetFlow の機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Flexible NetFlow の機能情報

機能名	リリース	機能情報
Flexible NetFlow	Cisco IOS XE Release 3.1S	Flexible NetFlow が導入されました。 Flexible NetFlow 機能については、次の項で説明します。 • 「フロー サンプリングを使用するための前提条件」（P.2） • 「Flexible NetFlow サンプラについて」（P.2） • 「Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドを軽減するためのフロー サンプリングの設定方法」（P.3） • 「Flexible NetFlow によるトラフィック分析の CPU オーバーヘッドを軽減するためにフロー サンプリングを使用する設定例」（P.6） 次のコマンドが導入または変更されました。**cache**（Flexible NetFlow）、**clear flow exporter**、**clear flow monitor**、**clear sampler**、**collect counter**、**collect flow**、**collect interface**、**collect ipv4**、**collect ipv4 destination**、**collect ipv4 fragmentation**、**collect ipv4 section**、**collect ipv4 source**、**collect ipv4 total-length**、**collect ipv4 ttl**、**collect routing**、**collect timestamp sys-uptime**、**collect transport**、**collect transport icmp ipv4**、**collect transport tcp**、**collect transport udp**、**debug flow exporter**、**debug flow monitor**、**debug flow record**、**debug sampler**、**description**（Flexible NetFlow）、**destination**、**dscp**（Flexible NetFlow）、**exporter**、**flow exporter**、**flow monitor**、**flow record**、**ip flow monitor**、**match flow**、**match interface**（Flexible NetFlow）、**match ipv4**、**match ipv4 destination**、**match ipv4 fragmentation**、**match ipv4 section**、**match ipv4 source**、**match ipv4 total-length**、**match ipv4 ttl**、**match routing**、**match transport**、**match transport icmp ipv4**、**match transport tcp**、**match transport udp**、**mode**（Flexible NetFlow）、**option**（Flexible NetFlow）、**record**、**sampler**、**show flow exporter**、**show flow interface**、**show flow monitor**、**show flow record**、**show sampler**、**source**（Flexible NetFlow）、**statistics packet**、**template data timeout**、**transport**（Flexible NetFlow）。