



メディア モニタリング設定ガイド

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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. 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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



目次

[最初にお読みください 1](#)

[Cisco Mediatrace の設定 3](#)

[機能情報の確認 3](#)

[Cisco Mediatrace の設定に関する情報 4](#)

[Cisco Mediatrace の概要 4](#)

[Cisco Mediatrace を使用して収集できるメトリック 4](#)

[Cisco Mediatrace の設定の概要 8](#)

[制限事項 9](#)

[Cisco Mediatrace の設定方法 9](#)

[Cisco Mediatrace の有効化 9](#)

[トラブルシューティングのヒント 10](#)

[Mediatrace イニシエータでの Cisco Mediatrace ビデオ プロファイルの設定 11](#)

[トラブルシューティングのヒント 13](#)

[Cisco Mediatrace のシステム プロファイルの設定 13](#)

[トラブルシューティングのヒント 14](#)

[Cisco Mediatrace のパス指定子プロファイルの設定 15](#)

[トラブルシューティングのヒント 16](#)

[Cisco Mediatrace のフロー指定子プロファイルの設定 16](#)

[トラブルシューティングのヒント 18](#)

[Cisco Mediatrace のセッション パラメータ プロファイルの設定 18](#)

[トラブルシューティングのヒント 20](#)

[Cisco Mediatrace セッションの設定 20](#)

[トラブルシューティングのヒント 22](#)

[Cisco Mediatrace セッションのスケジュール設定 23](#)

[トラブルシューティングのヒント 24](#)

[Cisco Mediatrace セッションのクリア 24](#)

[トラブルシューティングのヒント 25](#)

Cisco Mediatrace ポーリングの実行	25
トラブルシューティングのヒント	27
例	27
Cisco Mediatrace セッションのトラブルシューティングとモニタリング	29
Cisco Mediatrace の設定例	36
例 : Mediatrace の基本設定	36
次の作業	37
その他の参考資料	38
Cisco Mediatrace の機能情報	39
Cisco Performance Monitor の設定	43
機能情報の確認	43
Cisco Performance Monitor に関する情報	44
Cisco Performance Monitor の概要	44
Cisco Performance Monitor の設定の前提条件	44
Cisco Performance Monitor の構成コンポーネント	45
Cisco Performance Monitor を使用してモニタできるデータ	46
Cisco Performance Monitor の SNMP MIB サポート	47
Catalyst 6500 プラットフォームに関する制限事項	48
Cisco Performance Monitor の設定、トラブルシューティング、およびメンテナンスの 方法	50
Cisco Performance Monitor のフロー エクスポートの設定	50
トラブルシューティングのヒント	53
Cisco Performance Monitor のフロー レコードの設定	53
トラブルシューティングのヒント	56
Cisco Performance Monitor のフロー モニタの設定	57
トラブルシューティングのヒント	59
Cisco Performance Monitor のフロー クラスの設定	59
トラブルシューティングのヒント	61
既存のフロー モニタを使用した Cisco Performance Monitor のフロー ポリシーの設 定	61
トラブルシューティングのヒント	67

既存のフロー モニタを使用しない Cisco Performance Monitor のフロー ポリシーの設定	67
トラブルシューティングのヒント	73
既存のフロー ポリシーを使用して Cisco Performance Monitor ポリシーをインターフェイスに適用する方法	73
トラブルシューティングのヒント	74
既存のフロー ポリシーを使用せずに Cisco Performance Monitor ポリシーをインターフェイスに適用する方法	75
Cisco Performance Monitor のデータ収集の確認	82
Performance Monitor のキャッシュとクライアントの表示	90
Cisco Performance Monitor クラスのクロック レートの表示	93
フロー モニタの現在のステータスの表示	94
フロー モニタの設定の確認	95
インターフェイスで Cisco IOS Flexible NetFlow および Cisco Performance Monitor が有効になっていることの確認	96
フロー モニタ キャッシュの表示	97
フロー エクスポートの現在のステータスの表示	99
フロー エクスポートの設定の確認	100
デバッグの有効化	101
Cisco Performance Monitor の設定例	102
例：損失 RTP パケットおよび RTP ジッターのモニタリング	102
次の作業	103
その他の参考資料	104
Cisco Performance Monitor の機能情報	106



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

Cisco IOS XE リリース 3.7.0E (Catalyst スイッチング用) 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、コンバインドリリースの1つのバージョン - Cisco IOS XE 16 - に統合されました。この1つのリリースでスイッチングおよびルーティングポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。



(注)

技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかを示されます。



第 2 章

Cisco Mediatrace の設定

この章には、Cisco Mediatrace の設定に関する情報と説明が記載されています。

Cisco Mediatrace を使用すると、データ ストリームに関するネットワーク パフォーマンス低下の問題の切り分けを行ってトラブルシューティングできます。任意のタイプのフローをモニタするために使用できますが、主にビデオフローで使用されます。また、メディア フローパスに沿った、フロー以外に関連する監視にも使用できます。

- [機能情報の確認, 3 ページ](#)
- [Cisco Mediatrace の設定に関する情報, 4 ページ](#)
- [Cisco Mediatrace の設定方法, 9 ページ](#)
- [Cisco Mediatrace の設定例, 36 ページ](#)
- [次の作業, 37 ページ](#)
- [その他の参考資料, 38 ページ](#)
- [Cisco Mediatrace の機能情報, 39 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。

Cisco Mediatrace の設定に関する情報

Cisco Mediatrace の概要

Cisco Mediatrace は、IP フローのパスをネットワーク管理者が検出できるようにしてパフォーマンスの低下の問題を切り分けてトラブルシューティングを行う場合や、パス上のノードでモニタリング機能を動的に有効にする際や、ネットワークホップバイホップベースで情報を収集するのに役立ちます。この情報には、特に、フロー統計情報の他、着信および発信インターフェイス、CPU、ならびにメモリの使用率情報、さらに IP ルートまたは Cisco Mediatrace のモニタリング状態の変更が含まれます。

この情報は、次の 2 つのうちのいずれかの方法で取得できます。

- `exec` コマンドを発行して、メディアフロー上のホップからの統計情報のオンデマンド収集を実行します。この単発の操作では、メディアフロー上のホップが検出され、指定された他の一連の情報と共に表示されます。
- 特定の日の特定の時刻に定期モニタリングセッションが開始されるように Cisco Mediatrace を設定します。セッションを設定して、収集対象のメトリックおよびデータの収集頻度を指定することができます。パス上のホップの検出は操作の一部として自動的に実行されます。

指定したメトリックが収集されたら、それらのメトリックに関するレポートを表示できます。

Cisco Mediatrace は、Cisco Medianet 製品ファミリーの一部です。Medianet を他のシスコ製品と併せて使用する場合の設計、設定、およびトラブルシューティングの詳細については、クイックスタートガイドや導入ガイドも含めて、Cisco Medianet ナレッジベースポータル

(<http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html>) を参照してください。

Cisco Mediatrace を使用して収集できるメトリック

Mediatrace を使用して、次のカテゴリのメトリックを収集できます。

- 各レスポンドの共通メトリック
- システムメトリック：TCP プロファイル (System Metrics: TCP Profile)
- システムメトリック：RTP プロファイル (System Metrics: RTP Profile)
- システムメトリック：INTF プロファイル (System Metrics: INTF Profile)
- システムメトリック：CPU プロファイル (System Metrics: CPU Profile)
- システムメトリック：メモリ プロファイル (System Metrics: MEMORY Profile)
- アプリケーションヘルスメトリック：Mediatrace ヘルスプロファイル (App-Health Metrics: MEDIATRACE-HEALTH Profile)
- イニシエータからの Mediatrace 要求サマリに関するメトリック (Metrics for Mediatrace Request Summary from Initiator)

これらのカテゴリそれぞれに含まれる個々のメトリックを、以下の該当セクションに示します。

イニシエータからの Mediatrace 要求サマリに関するメトリック (Metrics for Mediatrace Request Summary from Initiator)

- 要求タイムスタンプ (Request Timestamp)
- リクエストのステータス (Request Status)
- 応答ホップの数 (Number of Hops Responded)
- 有効データを含むホップの数 (Number of Hops with Valid Data)
- エラーを含むホップの数 (Number of Hops with Error)
- データ レコードがないホップの数 (Number of hops with no data record)
- 前回のルート変更のタイムスタンプ (Last Route Change Timestamp)
- ルート インデックス (Route Index)

各レスポндаの共通メトリック

- メトリック収集ステータス (Metrics Collection Status)
- 到達可能性アドレス (Reachability address)
- 入力インターフェイス (Ingress Interface)
- 出力インターフェイス (Egress Interface)
- Mediatrace IP TTL
- ホスト名 (Hostname)
- Mediatrace ホップ数 (Mediatrace Hop Count)

パフォーマンス モニタ メトリック : TCP プロファイル (Perf-Monitor Metrics: TCP Profile)

- フロー サンプリング開始タイムスタンプ (Flow Sampling Start Timestamp)
- 測定の信頼性の喪失 (Loss of measurement confidence)
- 発生したメディア停止イベント (Media Stop Event Occurred)
- IP パケット ドロップ数 (IP Packet Drop Count)
- IP バイト数 (IP Byte Count)
- IP パケット数 (IP Packet Count)
- IP バイト レート (IP Byte Rate)
- IP DSCP
- IP TTL

- IP プロトコル (IP Protocol)
- メディア バイト数 (Media Byte Count)
- TCP 接続ラウンドトリップ遅延 (TCP Connect Round Trip Delay)
- TCP 損失イベント数 (TCP Lost Event Count)

パフォーマンス モニタ メトリック : RTP プロファイル (Perf-Monitor Metrics: RTP Profile)

- フロー サンプリング開始タイムスタンプ (Flow Sampling Start Timestamp)
- 測定の信頼性の喪失 (Loss of measurement confidence)
- 発生したメディア停止イベント (Media Stop Event Occurred)
- IP パケット ドロップ数 (IP Packet Drop Count)
- IP バイト数 (IP Byte Count)
- IP パケット数 (IP Packet Count)
- IP バイト レート (IP Byte Rate)
- パケット ドロップの理由 (Packet Drop Reason)
- IP DSCP
- IP TTL
- IP プロトコル (IP Protocol)
- メディア バイト レート (平均) (Media Byte Rate Average)
- メディア バイト数 (Media Byte Count)
- メディア パケット数 (Media Packet Count)
- RTP 到着間ジッター (平均) (RTP Interarrival Jitter Average)
- RTP パケット損失 (RTP Packets Lost)
- 予想 RTP パケット (pkts) (RTP Packets Expected (pkts)) :
- RTP パケット損失イベント数 (RTP Packet Lost Event Count) :
- RTP 損失率 (RTP Loss Percent)

システム メトリック : INTF プロファイル (System Metrics: INTF Profile)

- 収集タイムスタンプ (Collection timestamp)
- オクテット入力 (入力) (Octet input at Ingress)
- オクテット出力 (出力) (Octet output at Egress)
- エラーを含む受信パケット (入力) (Packets received with errors at Ingress)

- エラーを含むパケット（出力）（Packets with errors at Egress）
- 廃棄されたパケット（入力）（Packets discarded at Ingress）
- 廃棄されたパケット（出力）（Packets discarded at Egress）
- 入力インターフェイス速度（Ingress interface speed）
- 出力インターフェイス速度（Egress interface speed）

システム メトリック：CPU プロファイル（System Metrics: CPU Profile）

- CPU 使用率（1 分間）（CPU Utilization (1min)）
- CPU 使用率（5 分間）（CPU Utilization (5min)）
- 収集タイムスタンプ（Collection timestamp）

システム メトリック：メモリ プロファイル（System Metrics: MEMORY Profile）

- プロセッサ メモリ使用率（%）（Processor memory utilization %）
- 収集タイムスタンプ（Collection timestamp）

アプリケーションヘルス メトリック：Mediatrace ヘルス プロファイル（App-Health Metrics: MEDIATRACE-HEALTH Profile）

- 受信された要求（Requests Received）
- 前回の要求受信時刻（Time Last Request Received）
- 前回の要求のイニシエータ（Initiator of Last Request）
- ドロップされた要求（Requests Dropped）
- サポートされている最大同時セッション数（Max Concurrent Sessions supported）
- 現在アクティブなセッション（Sessions currently active）
- 切断されたセッション（Sessions Teared down）
- タイムアウトが発生したセッション（Sessions Timed out）
- 受信されたホップ情報要求（Hop Info Requests Received）
- 受信された Performance Monitor 要求（Performance Monitor Requests Received）
- 失敗した Performance Monitor 要求（Performance Monitor Requests failed）
- 受信された静的ポリシー要求（Static Policy Requests Received）
- 失敗した静的ポリシー要求（Static Policy Requests Failed）
- 受信されたシステム データ要求（System Data Requests Received）
- 失敗したシステム データ要求（System Data Requests Failed）

- 受信されたアプリケーションヘルス要求 (Application Health Requests Received)
- ローカルルート変更イベント (Local route change events)
- 前回のルート変更イベントの時刻 (Time of last route change event)
- 受信された不明な要求の数 (Number of unknown requests received)

Cisco Mediatrace の設定の概要

Cisco Mediatrace では、次のいずれかの方法で情報を取得できます。

- 事前にスケジュールされた定期モニタリングセッション。
- Mediatrace ポーリングとして知られる、オンデマンドでの単発の統計情報の収集。

Mediatrace セッションまたはポーリングを実装する前に、フロー情報の収集先の各ネットワークノードで Mediatrace を有効にしておく必要があります。Mediatrace セッションまたはポーリングを設定、開始、および制御するために使用するネットワークノードで Mediatrace Initiator をイネーブルにする必要があります。情報の収集先の各ネットワークノードで、Mediatrace Responder を有効にする必要があります。

Cisco Mediatrace セッションを設定するには、事前にパッケージ化されている次の2つのタイプのプロファイルのいずれかをセッションと関連付けることにより、セッションパラメータを設定できます。

- ビデオモニタリングプロファイル
- システムデータプロファイル

また、次のタイプのプロファイルを設定してセッションと関連付けることにより、独自のパラメータを Cisco Mediatrace セッションに設定できます。

- パス指定子プロファイル
- フロー指定子プロファイル
- セッションパラメータプロファイル

したがって、次のセクションでは、Cisco Mediatrace セッションを設定するために以下の作業を実行する方法について説明します。

- 1 Mediatrace の有効化
- 2 ビデオモニタリングプロファイルのセットアップ
- 3 システムデータプロファイルのセットアップ
- 4 パス指定子プロファイルのセットアップ
- 5 フロー指定子プロファイルのセットアップ
- 6 セッションパラメータプロファイルのセットアップ

7 プロファイルと Mediatrace セッションとの関連付ける

8 Mediatrace セッションのスケジュール設定

また、次のセクションでは、特定のパスのホップからデータをオンデマンドで取得する Mediatrace ポーリングを実行する方法についても説明します。

さらに、次のセクションでは、以下の作業を実行して Mediatrace セッションを管理する方法について説明します。

- 未完了の Cisco Mediatrace セッションのクリア
- Cisco Mediatrace セッションのトラブルシューティング

制限事項

- Mediatrace は IPv6 をサポートしていません。
- Resource Reservation Protocol (RSVP) は、同じインターフェイス上では着信 Path メッセージを転送しません（つまり、Path メッセージの送信元のインターフェイス経由では転送されないということです）。その場合、「出力インターフェイスが入力インターフェイスと同じです（ingress interface = egress interface）」というエラーメッセージが表示されます。ただし、Performance Routing (PfR) 境界ルータの場合は、着信インターフェイスで Path メッセージが送信されます。

Cisco Mediatrace の設定方法

Cisco Mediatrace の有効化

Cisco Mediatrace を使用してモニタするノードごとに、少なくとも 1 つの Cisco Mediatrace レスポンドを有効にする必要があります。また、Mediatrace セッションまたはポーリングを開始するすべてのノードについて、Cisco Mediatrace イニシエータを有効にする必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatraceinitiator {source-ip ip-address | source-interfaceinterface-name} [force][max-sessionsnumber]**
4. **mediatraceresponder[max-sessionsnumber]**
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	enable 例 : <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <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	mediatraceinitiator {source-ip ip-address source-interface interface-name} [force][max-sessions number] 例 : <pre>Router(config)# mediatrace initiator source-ip 10.10.1.1 max-sessions 4</pre>	Cisco Mediatrace またはイニシエータを有効にします。次のキーワードを使用することもできます。 <ul style="list-style-type: none"> ip-address : 常に到達可能な IP アドレス。 interface-name : イニシエータに接続する任意のローカル インターフェイス。 max-sessions : Cisco Mediatrace セッションの数を設定します。
ステップ 4	mediatraceresponder[max-sessions number] 例 : <pre>Router(config)# mediatrace responder max-sessions 4</pre>	Cisco Mediatrace レスポンダを有効にします。次のキーワードを使用することもできます。 <ul style="list-style-type: none"> max-sessions : Cisco Mediatrace セッションの数を設定します。
ステップ 5	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 モードに戻ります。

トラブルシューティングのヒント

show mediatrace responder app-health コマンドを使用して、レスポンダがイベント、要求、および Cisco Mediatrace に関連するその他の統計情報を正しく収集しているかどうかを確認します。

このコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Mediatrace イニシエータでの Cisco Mediatrace ビデオ プロファイルの設定

Cisco Mediatrace には、事前にパッケージ化されたビデオ モニタリング プロファイルが用意されています。このパッケージには、ビデオ メディア モニタリング セッションを開始するために必要なすべてのパラメータ設定が含まれています。また、Mediatrace イニシエータに独自のビデオ モニタリング プロファイルを設定することもできます。

新しいビデオ メディア モニタリング セッションを開始するため、それらのプロファイルの 1 つを関連付けて Cisco Mediatrace セッションを設定することができます。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatraceprofileperf-monitorname**
4. **admin-params**
5. **sampling-intervalseconds**
6. **exit**
7. **metric-list{tcp|rtpt}**
8. **clock-rate{type-number | type-name} rate**
9. **max-dropoutnumber**
10. **max-reordernumber**
11. **min-sequentialnumber**
12. **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。 • 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	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 3	mediatraceprofileperf-monitorname 例 : <pre>Router(config)# mediatrace profile perf-monitor vprofile-2</pre>	パフォーマンス プロファイル コンフィギュレーション モードを開始して、事前にパッケージ化されている Cisco Mediatrace ビデオ モニタリング プロファイルのパラメータを設定できるようにします。
ステップ 4	admin-params 例 : <pre>Router(config-mt-prof-perf)# admin-params</pre>	管理者パラメータ コンフィギュレーション モードを開始して、ビデオモニタリング管理者パラメータを設定できるようにします。
ステップ 5	sampling-intervalseconds 例 : <pre>Router(config-mt-prof-perf-params)# sampling-interval 40</pre>	ビデオモニタリングメトリックのサンプリング間隔（秒）を指定します。
ステップ 6	exit 例 : <pre>Router(config-mt-prof-perf-params)# exit</pre>	現在のコンフィギュレーションモードを終了し、パフォーマンス プロファイル コンフィギュレーション モードに戻ります。
ステップ 7	metric-list{tcp rtplib} 例 : <pre>Router(config-mt-prof-perf)# metric-list rtp</pre>	モニタ対象のメトリックが TCP と RTP のどちらに関するものであるかを指定します。
ステップ 8	clock-rate{type-number type-name} rate 例 : <pre>Router(config-mt-prof-perf-rtp-params)# clock-rate 64</pre>	（任意）RTP ビデオ モニタリング メトリックのサンプリングに使用するクロックレートを指定します。各ペイロードタイプには、関連付けられている特定のクロックレートがあります。それらは、タイプ番号とタイプ名のいずれかを使用して指定できます。ペイロードタイプ名で利用できる値の詳細については、『Cisco Media Monitoring Command Reference』を参照してください。
ステップ 9	max-dropoutnumber 例 : <pre>Router(config-mt-prof-perf-rtp-params)# max-dropout 2</pre>	（任意）RTP ビデオ モニタリング メトリックのサンプリング時に許可されるドロップアウトの最大数を指定します。ドロップアウトは、シーケンス番号が現在のパケットよりも古いものとして無視されるパケットの数を指定します。

	コマンドまたはアクション	目的
ステップ 10	max-reordernumber 例 : <pre>Router(config-mt-prof-perf-rtp-params)# max-reorder 4</pre>	(任意) RTP ビデオ モニタリング メトリックのサンプリング時に許可される順序変更の最大数を指定します。順序変更は、シーケンス番号が現在のパケットよりも新しいものとして無視されるパケットの数を指定します。
ステップ 11	min-sequentialnumber 例 : <pre>Router(config-mt-prof-perf-rtp-params)# min-sequential 2</pre>	(任意) RTP フローの分類に使用される連続パケットの最小数を指定します。
ステップ 12	end 例 : <pre>Router(config-mt-prof-perf-rtp-params)# 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モードに戻ります。

トラブルシューティングのヒント

show mediatrace profile perf-monitor コマンドを使用して、事前にパッケージ化されているビデオ モニタリング プロファイルのパラメータ値が正しく設定されていることを確認します。

このコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace のシステム プロファイルの設定

Cisco Mediatrace には、事前にパッケージ化されたシステム データ モニタリング プロファイルが用意されています。このパッケージには、システム データ モニタリング セッションを開始するために必要なすべてのパラメータ設定が含まれています。また、独自のシステム データ モニタリング プロファイルを設定することもできます。新しいシステム データ モニタリング セッションを開始するため、それらのプロファイルの 1 つを関連付けて Cisco Mediatrace セッションを設定することができます。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatraceprofilesystemname**
4. **metric-list {intf | cpu | memory}**
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	enable 例 : <pre>Router> enable</pre>	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 : <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	mediatraceprofilesystemname 例 : <pre>Router(config)# mediatrace profile system system-2</pre>	システム プロファイル コンフィギュレーション モードを開始して、Cisco Mediatrace のシステム プロファイルのパラメータを設定できるようにします。
ステップ 4	metric-list {intf cpu memory} 例 : <pre>Router(config-sys)# metric-list memory</pre>	モニタ対象のメトリックが、インターフェイス、CPU、メモリのいずれに関するものであるかを指定します。
ステップ 5	end 例 : <pre>Router(config-sys)# 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 モードに戻ります。

トラブルシューティングのヒント

show mediatrace profile system コマンドを使用して、事前にパッケージ化されているシステム データ プロファイルのパラメータ値が正しく設定されていることを確認します。

このコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace のパス指定子プロファイルの設定

Cisco Mediatrace セッションの設定では、パス指定子プロファイルを指定する必要があります。このプロファイルは、トラブルシューティングのためにモニタされるネットワーク ホップの検出に使用されるパラメータを定義します。オプションの **disc-proto** キーワードで指定する RSVP トランスポートプロトコルは、このホップ検出を実行するために使用されます。フロー指定子のパラメータ値は、トレース対象のメディア フローの値と一致している必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatracepath-specifiername [disc-proto rsvp] {gsidgsid | destinationipip-addressportnnnn}**
4. **sourceipip-addressportnnnn**
5. **l2-paramsgatewayip-addressvlanvlan-id**
6. **gsidgsid**
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	enable 例 : <pre>Router> enable</pre>	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 : <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	mediatracepath-specifiername [disc-proto rsvp] {gsidgsid destinationipip-addressportnnnn} 例 : <pre>Router(config)# mediatrace path-specifier path-4 disc-proto rsvp destination ip 10.1.1.1 port 400</pre>	パス指定子コンフィギュレーションモードを開始して、Cisco Mediatrace のパス指定子プロファイルのパラメータを設定できるようにします。このコマンドでは、パスの名前、宛先アドレス、およびポートを指定する必要があります。

	コマンドまたはアクション	目的
ステップ 4	sourceip-addressportnnnn 例 : <pre>Router(config-mt-path)# source ip 10.1.1.2 port 600</pre>	モニタ対象のメトリックの送信元 IP アドレスを指定します。
ステップ 5	l2-paramsgatewayip-addressvlanvlan-id 例 : <pre>Router(config-mt-path)# l2-params gateway 10.10.10.4 vlan 22</pre>	レベル 2 ゲートウェイの仮想 LAN の IP アドレスと ID を指定します。 (注) このコマンドは、Catalyst プラットフォームのみで使用できます。
ステップ 6	gsidgsid 例 : <pre>Router(config-mt-path)# gsid 60606060</pre>	モニタ対象のフローのメタデータ グローバル セッション ID を指定します。
ステップ 7	end 例 : <pre>Router(config-mt-path)# 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 モードに戻ります。

トラブルシューティングのヒント

show mediatrace path-specifier コマンドを使用して、パス指定子プロファイルのパラメータ値が正しく設定されていることを確認します。

このコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace のフロー指定子プロファイルの設定

Cisco Mediatrace セッションの設定では、フロー指定子プロファイルを指定する必要があります。このプロファイルは、フローを識別するための送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコルを定義します。プロファイルは、後で実際の Cisco Mediatrace セッションを設定するときに関連付けることができます。

RTP メディア フローについては、UDP をプロトコルとして選択します。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatraceflow-specifiername**
4. **source-ipip-address [source-portport]**
5. **dest-ipip-address [dest-portport]**
6. **gsidgsid**
7. **ip-protocol{tcp|udp}**
8. **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 : <pre>Router> enable</pre>	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 : <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	mediatraceflow-specifiername 例 : <pre>Router(config)# mediatrace flow-specifier flow-6</pre>	フロー指定子コンフィギュレーションモードを開始して、Cisco Mediatrace のフロー指定子プロファイルのパラメータを設定できるようにします。
ステップ 4	source-ipip-address [source-portport] 例 : <pre>Router(config-mt-flowspec)# source-ip 10.1.1.2 source-port 600</pre>	(任意) モニタ対象のメトリックの送信元 IP アドレスを指定します。
ステップ 5	dest-ipip-address [dest-portport] 例 : <pre>Router(config-mt-flowspec)# dest-ip 10.1.1.2 dest-port 600</pre>	モニタ対象のメトリックの宛先 IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	gsid <i>gsid</i> 例 : <pre>Router(config-mt-flowspec)# gsid 60606060</pre>	モニタ対象のフローのメタデータ グローバルセッション ID を指定します。
ステップ 7	ip-protocol {tcp udp} 例 : <pre>Router(config-mt-flowspec)# ip-protocol tcp</pre>	モニタ対象のメトリックが TCP と UDP のどちらに関するものであるかを指定します。
ステップ 8	end 例 : <pre>Router(config-mt-flowspec)# 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 モードに戻ります。

トラブルシューティングのヒント

show mediatrace flow-specifier コマンドを使用して、フロー指定子プロファイルのパラメータ値が正しく設定されていることを確認します。

このコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace のセッションパラメータ プロファイルの設定

Cisco Mediatrace セッションの設定では、セッションパラメータプロファイルを指定する必要があります。このプロファイルは、Cisco Mediatrace セッションの特性を定義し、Cisco Mediatrace セッションの動作を円滑化するのに役立ちます。プロファイルは、後で実際の Cisco Mediatrace セッションを設定するときに関連付けることができます。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatrace`session-params`*name***
4. **`response-timeout`*seconds***
5. **`frequency` {*frequency* | **on-demand**} **`inactivity-timeout`*seconds*****
6. **`history`*buckets***
7. **`route-change`*reaction-time**seconds***
8. **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 : <pre>Router> enable</pre>	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 : <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	mediatrace<code>session-params</code><i>name</i> 例 : <pre>Router(config-mt-sesparam)# mediatrace session-params qos-2</pre>	セッションパラメータ コンフィギュレーション モードを開始して、Cisco Mediatrace のセッションパラメータ プロファイルのパラメータを設定できるようにします。
ステップ 4	<code>response-timeout</code><i>seconds</i> 例 : <pre>Router(config-mt-sesparam)# response-timeout 8</pre>	イニシエータがレスポンスからの応答を待機する時間（秒）を指定します。
ステップ 5	<code>frequency</code> {<i>frequency</i> on-demand} <code>inactivity-timeout</code><i>seconds</i> 例 : <pre>Router(config-mt-sesparam)# frequency 4 inactivity-timeout 2</pre> 	セッションパラメータ メトリックのサンプリング間隔（秒）、およびレスポンスからのアクティビティがない場合にイニシエータがアクティブ状態を維持する時間（秒）を指定します。

	コマンドまたはアクション	目的
ステップ 6	historybuckets 例 : <pre>Router(config-mt-sesparam)# history 2</pre>	保持する履歴データセットの数を指定します（最大値は 10）。
ステップ 7	route-changereaction-timesecs 例 : <pre>Router(config-mt-sesparam)# route-change reaction-time 8</pre>	追加のルート変更に対するレスポンスの反応をイニシエータが待機する時間（秒）を指定します。範囲は秒単位です。
ステップ 8	end 例 : <pre>Router(config-mt-sesparam)# 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 モードに戻ります。

トラブルシューティングのヒント

show mediatrace session-param コマンドを使用して、セッション パラメータ プロファイルのパラメータ値が正しく設定されていることを確認します。

このコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace セッションの設定

Cisco Mediatrace セッションの設定は、さまざまなプロファイルをセッションに関連付けます。Cisco Mediatrace セッションに関連付けできるプロファイルは各タイプで 1 つだけです。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatrace***session-number*
4. **trace-route**
5. **path-specifier** {[**forward**] *path-name* | **reverse***path-name* }
6. **session-params***name*
7. **profile***systemname*
8. **profileperf-monitor***nameflow-specifierflow-specifier-name*
9. **profilesnmp***name*
10. **profilecustom***name*
11. **last-node** {**auto** | **address***address*}
12. **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。 • 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	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	mediatrace <i>session-number</i> 例 : Router(config)# mediatrace 157	セッション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	trace-route 例 : Router(config-mt-session)# trace-route	Cisco Mediatrace セッションのトレースルートの実行を有効にします。デフォルトでは、トレースルートは有効になっています。トレースルートの実行を停止にするには、このコマンドの no 形式を使用します。
ステップ 5	path-specifier {[forward] <i>path-name</i> reverse <i>path-name</i> } 例 : Router(config-mt-session)# path-specifier path-4	パス指定子プロファイルを Cisco Mediatrace セッションに関連付けます。

	コマンドまたはアクション	目的
ステップ 6	session-paramsname 例 : <pre>Router(config-mt-session)# session-params session-6</pre>	セッションパラメータプロファイルを Cisco Mediatrace セッションに関連付けます。
ステップ 7	profilesysteemname 例 : <pre>Router(config-mt-session)# profile system sys-2</pre>	システムプロファイルを Cisco Mediatrace セッションに関連付けます。
ステップ 8	profileperf-monitornameflow-specifierflow-specifier-name 例 : <pre>Router(config-mt-session)# profile perf-monitor monitor-6 flow-specifier flow-4</pre>	パフォーマンスモニタプロファイルおよびフロー指定子を Cisco Mediatrace セッションに関連付けます。
ステップ 9	profilesnmppname 例 : <pre>Router(config-mt-session)# profile snmp snmp-2</pre>	SNMP プロファイルを Cisco Mediatrace セッションに関連付けます。
ステップ 10	profilecustomname 例 : <pre>Router(config-mt-session)# profile custom cp-2</pre>	SNMP プロファイルを Cisco Mediatrace セッションに関連付けます。
ステップ 11	last-node {auto addressaddress} 例 : <pre>Router(config-mt-session)# last-node address 10.1.1.1</pre>	Cisco Mediatrace セッションの最後のノードを設定します。
ステップ 12	end 例 : <pre>Router(config-mt-session)# 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 モードに戻ります。

トラブルシューティングのヒント

show mediatrace session コマンドを使用して、特定のセッションまたはすべてのセッションのパラメータ設定を表示します。

show mediatrace responder app-health コマンドおよび **show mediatrace responder sessions** コマンドを使用して、モニタ中のノードのステータスを判別します。

必要なすべてのデータが Cisco Mediatrace で収集されない場合は、**debug mediatrace** コマンドを使用します。

これらのコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace セッションのスケジュール設定

Cisco Mediatrace セッションを設定したら、必要なときにデータの収集が開始されるようにスケジュールを設定することができます。Cisco Mediatrace セッションがパフォーマンス モニタリング メトリックの収集を目的とするものである場合は、セッションの開始時に Performance Monitor の有効化が試行されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **mediatrace schedule sessionID** [*life* {**forever** | *secs*}] [**start-time** {*hh:mm:ss*}[*monthday*|*daymonth*] | **pending** | **now** | **after***hh:mm:ss*] [**ageoutsecs**] [**recurring**]
4. **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 : <pre>Router> enable</pre>	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 : <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	mediatrace schedule sessionID [<i>life</i> { forever <i>secs</i> }] [start-time { <i>hh:mm:ss</i> }[<i>monthday</i> <i>daymonth</i>] pending now after <i>hh:mm:ss</i>] [ageoutsecs] [recurring] 例 : <pre>Router(config)# mediatrace schedule 22</pre>	セッションの実行日時を指定します。次の設定を使用します。 • <i>sessionID</i> : 実行するセッション。 • <i>life</i> : セッションの継続時間（秒数と forever のいずれか）。

	コマンドまたはアクション	目的
	<pre>life 40 start-time 10:00:00 AUG 20 recurring</pre>	<ul style="list-style-type: none"> • start-time : セッションの開始時刻（指定の日時、イベントの保留、即時、指定の日時の後のいずれか）。 • ageout : イニシエータでタイムアウトが発生してセッション設定が削除されるまでの時間。 • recurring : セッションが指定時刻に繰り返し実行されます。
ステップ 4	end 例 : <pre>Router(config-mt-sched)# 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モードに戻ります。

トラブルシューティングのヒント

show mediatrace session コマンドを使用して、特定のセッションまたはすべてのセッションのパラメータに意図したとおりの値が設定されていることを確認します。

show mediatrace responder app-health コマンドおよび **show mediatrace responder sessions** コマンドを使用して、モニタ中のノードのステータスを判別します。

必要なすべてのデータが Cisco Mediatrace で収集されない場合は、**debug mediatrace** コマンドを使用します。

これらのコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace セッションのクリア

以下の説明に従って **clearmediatraceincomplete-sessions** コマンドを使用して、イニシエータで完了していない Mediatrace セッションをクリアすることができます。また、このコマンドは、Cisco Mediatrace で設定したすべての Performance Monitor の設定をクリアします。**config** コマンドで作成したセッションについては、**nomediatraceschedule** コマンドを使用します。クリーンアップを実行すると、「セッションが切断されました (session teardown)」というメッセージが RSVP に対して出力され、続けて、ローカルの Mediatrace セッション データベースのクリーンアップが実行されます。

手順の概要

1. **enable**
2. **clearmediatraceincomplete-sessions**
3. **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 : <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <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	clearmediatraceincomplete-sessions 例 : <pre>Router# clear mediatrace incomplete-sessions</pre>	未完了の Mediatrace セッションをクリアします。
ステップ 3	end 例 : <pre>Router# 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 モードに戻ります。

トラブルシューティングのヒント

Cisco Mediatrace セッションのステータスをチェックするには、**show mediatrace responder sessions** コマンドを使用します。

これらのコマンドの詳細については、[Cisco Mediatrace セッションのトラブルシューティングとモニタリング](#)、(29 ページ) を参照してください。

Cisco Mediatrace ポーリングの実行

Cisco Mediatrace ポーリングは、特定のパスのホップからオンデマンドでデータを取得するために使用します。いくつかの使用例を以下に示します。

- 事前設定済みのセッションを使用してデータを取得する場合。この場合、他のパラメータをインラインで指定する必要はありません。事前設定済みのセッションでは、オンデマンドを頻度のタイプとして設定する必要があります。

- 特定のパスのホップからシステム データ、ホップ、またはビデオ モニタリング情報を取得する場合。設定モード特権がない場合、パスを事前設定済みパス指定子またはインラインパス仕様として指定することができます。ただし、デフォルトでは、Cisco Mediatrace は、パスのノードからパッシブモニタリングメトリックが報告されるように設定しようとし、次に、設定可能な時間待機した後に再びデータを収集しようとしています。
- Performance Monitor コマンドを使用して既に Performance Monitor ポリシーが設定されているメディア パスのノードからデータを取得するため、**configless** キーワードを使用することができます。この方法を使用してデータを取得する場合に留意すべきいくつかの重要な点として、次のようなものがあります。
 - デフォルトのパフォーマンス モニタリング プロファイルまたは関連付けられているパフォーマンス モニタリング プロファイルに設定されているサンプリング間隔が適用されます。静的ポリシーのサンプリング間隔が関連付けられているパフォーマンスモニタリング プロファイルのサンプリング間隔と一致しない場合、データは返されません。
 - レスポンダ ノードで Performance Monitor ポリシーが設定されていない場合、Cisco Mediatrace レスポンダは Performance Monitor を設定しようとせず、単にエラーをイニシエータに報告します。

手順の概要

1. **enable**
2. **mediatracepoll**{no-traceroute | sessionnumber | [timeoutvalue]path-specifier{namepath-name | gsidgsid | {[disc-protorsvp]destinationipip-address [portnnnnn] | sourceipip-address[portnnnnn] destinationipip-address[portnnnnn] [ip-protocol]{tcp | udp}}} {app-health | hops | l2-paramsgatewayip-address | system [profilesystem-profile-name] | [configless] perf-monitor [profileprofile-name]} {flow-specifiername | source-ipipaddress [source-portnnnnn] dest-ipipaddress [dest-portnnnnn] ip-protocol {tcp | udp}}}
3. **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。 • パスワードを入力します（要求された場合）。
ステップ 2	mediatracepoll {no-traceroute sessionnumber [timeoutvalue]path-specifier{namepath-name gsidgsid {[disc-protorsvp]destinationipip-address [portnnnnn] sourceipip-address[portnnnnn] destinationipip-address[portnnnnn] [ip-protocol]{tcp udp}}} {app-health hops	特定のパスのホップからオンデマンドでデータを取得します。次のいずれかのタイプの情報を使用して、ホップを指定できます。 • セッション定義またはその構成パラメータ

	コマンドまたはアクション	目的
	l2-paramsgateway <i>ip-address</i> system [profile <i>system-profile-name</i> [configless] perf-monitor [profile <i>profile-name</i>] {flow-specifier <i>name</i> source-ip <i>ipaddress</i> [source-port <i>nnnnn</i> dest-ip <i>ipaddress</i> [dest-port <i>nnnnn</i>] ip-protocol { tcp udp } } } } <p>例 :</p> <p>例 :</p> <pre>Router# mediatrace poll session 22</pre>	<ul style="list-style-type: none"> システム定義プロファイルまたはその構成パラメータ パス指定子プロファイル定義とパフォーマンスモニタリングプロファイル定義の組み合わせ、またはそれらの構成パラメータの組み合わせ <p>(注) l2-paramsgateway キーワードは、Catalyst プラットフォームのみで使用できます。</p>
ステップ 3	end <p>例 :</p> <pre>Router# 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 モードに戻ります。

トラブルシューティングのヒント

必要なすべてのデータが Cisco Mediatrace で収集されない場合は、次のようにします。

- **show mediatrace session** コマンドを使用して、特定のセッションまたはすべてのセッションのパラメータに意図したとおりの値が設定されていることを確認します。
- **show mediatrace responder app-health** コマンドおよび **show mediatrace responder sessions** コマンドを使用して、モニタ中のノードのステータスを判別します。
- **debug mediatrace** コマンドを使用して、エラー メッセージを表示します。

例



ヒント

ポーリングの出力例については、[Cisco Mediatrace の設定例](#)、(36 ページ) を参照してください。

例えば、送信元 IP アドレス、送信元ポート、および宛先ポートが不明な場合にデフォルトのシステム メトリックを取得するには、次のようにします。Cisco Mediatrace は、最適なローカル IP アドレスを送信元 IP アドレスとして使用して、RSVP を使用しているホップを検出します。

mediatracepollpathdestip-addresssystem

例えば、送信元ポート番号と宛先ポートが不明な場合にデフォルトのシステム メトリックを取得するには、次のようにします。指定した送信元と宛先の間のホップが RSVP によって検出されます。

mediatracepollpathsourceip-addressdestip-addresssystem

例えば、送信元ポート番号と宛先ポートがわかっている場合にデフォルトのシステム メトリックを取得するには、次のようにします。この情報が RSVP で使用されてホップが検出されます。

mediatracepollpathsource-ipip-addresssource-portnnndest-ipip-addressdest-portnnnip-protocoludpsystem

例えば、送信元ポート番号と宛先ポートが不明な場合にデフォルトの RTP メトリック セットを取得するには、次のようにします。Cisco Mediatrace は、パスの送信元 IP アドレスと宛先 IP アドレスを使用して、Performance Monitor のデータをフィルタリングすると共にホップを検出します。

mediatracepollpathsourceip-addressdestip-addressperf-monitor

例えば、デフォルトの RTP メトリック セットを取得するには、次のようにします。Cisco Mediatrace は、パス パラメータを使用してホップを検出し、インライン フロー指定子プロファイルを Performance Monitor データのフィルタとして使用します。

mediatracepollpathsourceip-addressdestip-addressperf-monitorsource-ipip-addresssource-portnnndest-ipip-addressdest-portnnnip-protocoludp

例えば、デフォルトの TCP メトリック セットを取得するには、次のようにします。Cisco Mediatrace は、パス パラメータを使用してホップを検出し、インライン フロー指定子プロファイルを Performance Monitor データのフィルタとして使用します。

mediatracepollpathsourceip-addressdestip-addressperf-monitorsource-ipip-addresssource-portnnndest-ipip-addressdest-portnnnip-protocoltcp

例えば、デフォルトの RTP メトリック セットを取得するには、次のようにします。Cisco Mediatrace は、最適なローカル IP アドレスを送信元 IP アドレスとして使用してパス上のホップを検出し、インライン フロー指定子プロファイルを Performance Monitor データのフィルタとして使用します。

mediatracepollpathdestip-addressperf-monitorsource-ipip-addresssource-portnnndest-ipip-addressdest-portnnnip-protocoludp

例えば、デフォルトの TCP メトリック セットを取得するには、次のようにします。Cisco Mediatrace は、最適なローカル IP アドレスを送信元 IP アドレスとして使用してパス上のホップを検出し、インライン フロー指定子プロファイルを Performance Monitor データのフィルタとして使用します。

mediatracepollpathdestip-addressperf-monitorsource-ipip-addresssource-portnnndest-ipip-addressdest-portnnnip-protocoltcp

例えば、ホップで既に設定されている静的ポリシーからデフォルトの RTP メトリック セットを取得するには、次のようにします。このコマンドを使用しても Performance Monitor が設定されることはありません。Cisco Mediatrace は、パス パラメータを使用してホップを検出し、インライン フロー指定子プロファイルを Performance Monitor データのフィルタとして使用します。

mediatracepollpathsourceip-addressdestip-addressconfigperf-monitorflow-specifiersourceip-addressportnnndestip-addressportnnnip-protocoludp

ポーリングの出力例

この例は、次のホップ ポーリング コマンドの出力を示しています。

```
mediatrace poll path-specifier source 10.10.130.2 destination 10.10.132.2 hops
Started the data fetch operation.
Waiting for data from hops.
This may take several seconds to complete...
```

```

Data received for hop 1
Data received for hop 2
Data fetch complete.
Results:
Data Collection Summary:
  Request Timestamp: 22:47:56.788 PST Fri Oct 29 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 2
  Number of hops with valid data report: 2
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
  Number of Mediatrace hops in the path: 2
  Mediatrace Hop Number: 1 (host=responder1, ttl=254)
    Reachability Address: 10.10.12.3
    Ingress Interface: Gi0/1
    Egress Interface: Gi0/2
  Mediatrace Hop Number: 2 (host=responder2, ttl=253)
    Reachability Address: 10.10.34.3
    Ingress Interface: Gi0/1
    Egress Interface: Gi0/2

```

Cisco Mediatrace セッションのトラブルシューティングとモニタリング

ここで説明する **show** コマンドを使用して、Cisco Mediatrace セッションのトラブルシューティングとモニタリングを実行します。



ヒント

出力例については、この章の「例」セクションを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **showmediatraceprofileperf-monitor***[name]*
4. **showmediatraceprofiles***system**[name]*
5. **showmediatraceflow-specifier** *[name]*
6. **showmediatracepath-specifier** *[name]*
7. **showmediatraceinitiator**
8. **showmediatrace***session-params**[name]*
9. **showmediatrace***session**[config|data|stats| hops]* *[brief| ID]*
10. **showmediatrace***responderapp-health*
11. **showmediatrace***responder**sessions**[global-session-id|brief|details]*
12. **debugmediatrace***{event | trace | error}* *[initiator | responder|session-id]*
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	enable 例 : <pre>Router> enable</pre>	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 : <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	showmediatraceprofileperf-monitor[name] 例 : <pre>Router(config)# show mediatrace profile perf-monitor vprofile-4</pre>	事前にパッケージ化されているすべてのビデオ モニタリング プロファイルまたは指定されたプロファイルに設定されているパラメータを表示します。
ステップ 4	showmediatraceprofilesysteem[name] 例 : <pre>Router(config)# show mediatrace profile system system-8</pre>	事前にパッケージ化されているすべてのシステム データ プロファイルまたは指定されたプロファイルに設定されているパラメータを表示します。
ステップ 5	showmediatraceflow-specifier [name] 例 : <pre>Router(config)# show mediatrace flow-specifier flow-2</pre>	すべてのフロー指定子プロファイルまたは指定されたフロー指定子プロファイルに設定されているパラメータを表示します。
ステップ 6	showmediatracepath-specifier [name] 例 : <pre>Router(config)# show mediatrace path-specifier path-6</pre>	すべてのパス指定子プロファイルまたは指定されたパス指定子プロファイルに設定されているパラメータを表示します。
ステップ 7	showmediatraceinitiator 例 : <pre>Router(config)# show mediatrace initiator</pre>	イニシエータプロファイルに設定されているパラメータを表示します。
ステップ 8	showmediatrace-session-params[name] 例 : <pre>Router(config)# show mediatrace session-params sysparams-2</pre>	頻度や応答タイムアウトなど、セッションのモニタリング パラメータを表示します。 事前にパッケージ化されているすべてのシステム データ プロファイルまたは指定されたプロファイルに設定されているパラメータ。

	コマンドまたはアクション	目的
ステップ 9	showmediatrace session[config data stats hops] [brief ID] 例 : Router(config)# show mediatrace session data 1002	<p>すべてのセッションプロファイルまたは指定されたセッションプロファイルに設定されているパラメータを表示します。次のキーワードを使用して、該当の情報を表示します。</p> <ul style="list-style-type: none"> • config : セッションの設定。 • data : イニシエータで収集されたすべてのデータ レコードと、まだキャッシュに残っているすべてのデータ レコード。 • stats : このサービスパスまたはセッションの統計情報。 • hops : 以前のサービス パス（可能な場合）および検出された現在のサービスパス。また、前回のルート変更の場所と日時も表示されます。 • brief : ID、送信元および宛先のアドレスとポート、ならびにそれらに関連付けられている役割（イニシエータまたはレスポнда）のみを含むセッションのリスト。 • ID : セッション ID および何らかの状態情報。
ステップ 10	showmediatrace responder app-health 例 : Router(config)# show mediatrace responder app-health	<p>レスポндаの現在のステータスを表示します。</p>
ステップ 11	showmediatrace responder sessions[global-session-id brief details] 例 : Router(config)# show mediatrace responder sessions	<p>ローカルレスポндаのすべてのアクティブなセッションまたは特定のアクティブなセッションに関する情報を表示します。次のキーワードを使用して、対応する情報を表示します。</p> <ul style="list-style-type: none"> • global-session-id : 情報を表示するセッションの ID。 • brief : パスの宛先および送信元のアドレスとポート、それらの役割（イニシエータまたはレスポнда）、ならびに何らかの状態情報のみを表示します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • details : すべての情報を表示します。
ステップ 12	debugmediatrace{event trace error} [initiator responder session-id] 例 : <pre>Router(config)# debug mediatrace event 24</pre>	特定のパス、特定のセッション、またはすべてのイニシエータ機能とレスポンド機能について、デバッグを有効にします。次のオプションを使用できます。 <ul style="list-style-type: none"> • event : イベント情報のみを表示します。 • trace : トレース情報のみを表示します。 • error : エラーのみを表示します。 • initiator : イニシエータのみの情報を表示します。 • responder : レスポンドのみの情報を表示します。 • session-id : セッションのみの情報を表示します。
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 モードに戻ります。

例



(注) 以下の show コマンドの完全な説明については、『Cisco Media Monitoring Command Reference』を参照してください。

例えば、ビデオ モニタリング プロファイルを表示するには、次のようにします。

```
Router# show mediatrace profile perf-monitor
Perf-monitor Profile: vprof-4
Metric List: rtp
RTP Admin Parameter:
  Max Dropout: 5
  Max Reorder: 5
  Min Sequential: 5
Admin Parameter:
  Sampling Interval (sec): 30
```

例えば、システム データ プロファイルを表示するには、次のようにします。

```
Router# show mediatrace profile
```

system

```
System Profile: sys-1
Metric List: intf
```

例えば、フロー指定子プロファイルを表示するには、次のようにします。

```
Router# show mediatrace
      flow-specifier flow-1
Flow Specifier: flow-1
  Source address/port:
  Destination address/port:
  Protocol: udp
```

例えば、パス指定子プロファイルを表示するには、次のようにします。

```
Router# show mediatrace
      path-specifier flow-1
Path Configuration: psl
  Destination address/port: 10.10.10.1
  Source address/port: 10.10.10.4
  Gateway address/vlan:
  Discovery protocol: rsvp
```

例えば、イニシエータ プロファイルを表示するには、次のようにします。

```
Router# show mediatrace
      initiator
Version: Mediatrace 1.0
Mediatrace Initiator status: enabled
Source IP: 1.1.1.1
Number of Maximum Allowed Active Session: 127
Number of Configured Session: 1
Number of Active Session      : 0
Number of Pending Session     : 0
Number of Inactive Session    : 1
Note: the number of active session may be higher than max active session
      because the max active session count was changed recently.
```

例えば、セッションプロファイルを表示するには、次のようにします。

```
Router# show mediatrace session-params
Session Parameters: s-1
  Response timeout (sec): 60
  Frequency: On Demand
  Inactivity timeout (sec): 300
  History statistics:
    Number of history buckets kept: 3
  Route change:
    Reaction time (sec): 5
```

例えば、Mediatrace セッションの統計情報を表示するには、次のようにします。

```
Router# show mediatrace session stats 2
Session Index: 2
Global Session Id: 86197709
Session Operation State: Active
Operation time to live: Forever
Data Collection Summary:
  Request Timestamp: 23:55:04.228 PST Fri Oct 29 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 2
  Number of hops with valid data report: 2
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
  Last Route Change Timestamp:
  Route Index: 0
  Number of Mediatrace hops in the path: 2
  Mediatrace Hop Number: 1 (host=responder1, ttl=254)
  Metrics Collection Status: Success
```

```

Reachability Address: 10.10.12.3
Ingress Interface: Gi0/1
Egress Interface: Gi0/2

```



(注) ホップ 1 の残りのデータは、次に示すホップ 2 のデータと同様です。

```

Mediatrace Hop Number: 2 (host=responder2, ttl=253)
Metrics Collection Status: Success
Reachability Address: 10.10.34.3
Ingress Interface: Gi0/1
Egress Interface: Gi0/2
Metrics Collected:
  Collection timestamp: 23:55:04.237 PST Fri Oct 29 2010
  Octet input at Ingress (KB): 929381.572
  Octet output at Egress (MB): 1541.008502
  Pkts rcvd with err at Ingress (pkts): 0
  Pkts errored at Egress (pkts): 0
  Pkts discarded at Ingress (pkts): 0
  Pkts discarded at Egress (pkts): 0
  Ingress i/f speed (mbps): 1000.000000
  Egress i/f speed (mbps): 1000.000000

```

例えば、Mediatrace セッションの設定情報を表示するには、次のようにします。

```

Router# show mediatrace session config 2
Global Session Id: 93642270
-----
Session Details:
  Path-Specifier: ps1
  Session Params: sp1
  Collectable Metrics Profile: intf1
  Flow Specifier:
Schedule:
  Operation frequency (seconds): 30 (not considered if randomly scheduled)
  Next Scheduled Start Time: Start Time already passed
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
History Statistics:
  Number of history Buckets kept: 10

```

例えば、Mediatrace セッションのホップを表示するには、次のようにします。

```

show mediatrace session hops 2
Session Index: 2
Global Session Id: 93642270
Session Operation State: Active
Data Collection Summary:
  Request Timestamp: 13:40:32.515 PST Fri Jun 18 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 3
  Number of hops with valid data report: 3
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
  Last Route Change Timestamp:
  Route Index: 0
    Number of Mediatrace hops in the path: 3
    Mediatrace Hop Number: 1 (host=responder1, ttl=254)
      Ingress Interface: Gi0/1
      Egress Interface: Gi1/0
    Mediatrace Hop Number: 2 (host=responder2, ttl=253)
      Ingress Interface: Gi0/1
      Egress Interface: Gi1/0
    Mediatrace Hop Number: 3 (host=responder3, ttl=252)

```



```
Ingress Interface: Gi0/1
Egress Interface: Gi0/2
```

例えば、Mediatrace セッションのデータを表示するには、次のようにします。

```
Router# show mediatrace session data 2
Session Index: 2
Global Session Id: 35325453
Session Operation State: Active
Bucket index: 1
Data Collection Summary:
  Request Timestamp: 13:02:47.969 PST Fri Jun 18 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 3
  Number of hops with valid data report: 3
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
  Last Route Change Timestamp:
  Route Index: 0
    Number of Mediatrace hops in the path: 3
    Mediatrace Hop Number: 1 (host=responder1, ttl=254)
      Metrics Collection Status: Success
      Ingress Interface: Gi0/1
      Egress Interface: Gi1/0
      Metrics Collected:
        Collection timestamp: 13:04:57.781 PST Fri Jun 18 2010
        Octet input at Ingress (KB): 10982.720
        Octet output at Egress (KB): 11189.176
      Pkts rcvd with err at Ingress (pkts): 0
      Pkts errored at Egress (pkts): 0
      Pkts discarded at Ingress (pkts): 0
      Pkts discarded at Egress (pkts): 0
      Ingress i/f speed (mbps): 1000.000000
      Egress i/f speed (mbps): 1000.000000
    Mediatrace Hop Number: 2 (host=responder2, ttl=253)
      Metrics Collection Status: Success
      Ingress Interface: Gi0/1
      Egress Interface: Gi1/0
      Metrics Collected:
        Collection timestamp: 13:04:57.792 PST Fri Jun 18 2010
        Octet input at Ingress (MB): 1805.552836
        Octet output at Egress (MB): 1788.468650
        Pkts rcvd with err at Ingress (pkts): 0
        Pkts errored at Egress (pkts): 0
        Pkts discarded at Ingress (pkts): 0
        Pkts discarded at Egress (pkts): 0
        Ingress i/f speed (mbps): 1000.000000
        Egress i/f speed (mbps): 1000.000000
```

例えば、Mediatrace レスポンダのアプリケーション ヘルス情報を表示するには、次のようにします。

```
Router# show mediatrace responder app-health
Mediatrace App-Health Stats:
  Number of all requests received: 0
  Time of the last request received:
  Initiator ID of the last request received: 0
  Requests dropped due to queue full: 0
  Responder current max sessions: 45
  Responder current active sessions: 0
  Session down or tear down requests received: 0
  Session timed out and removed: 0
  HOPS requests received: 0
  VM dynamic polling requests received: 0
  VM dynamic polling failed: 0
  VM configless polling requests received: 0
  VM configless polling failed: 0
  SYSTEM data polling requests received: 0
  SYSTEM data polling requests failed: 0
  APP-HEALTH polling requests received: 0
  Route Change or Interface Change notices received: 0
```

```
Last time Route Change or Interface Change:
Unknown requests received: 0
```

例えば、Mediatrace レスポンダの簡潔なセッション情報を表示するには、次のようにします。

```
Router# show mediatrace responder sessions brief
Local Responder configured session list:
Current configured max sessions: 45
Current number of active sessions: 0
session-id initiator-name      src-ip      src-port    dst-ip      dst-port det-1
2    host-18      10.10.10.2    200    10.10.10.8    200
```

Cisco Mediatrace の設定例

例：Mediatrace の基本設定

この例のトポロジには、次のものが含まれています。

- Mediatrace イニシエータ (10.10.12.2) 1 つ
- 以下の間のレスポンダ 2 つ
 - メディア送信元 (10.10.130.2)
 - 宛先 (10.10.132.2)

この例では、送信元（アドレス 10.10.130.2、ポート 1000）から宛先（アドレス 10.10.132.2、ポート 2000）への RTP トラフィック ストリームがあります。

Mediatrace レスポンダの基本設定は、次のとおりです。

```
mediatrace responder
snmp-server community public RO
```

Mediatrace イニシエータの基本設定は、次のとおりです。

```
mediatrace initiator source-ip 10.10.12.2
mediatrace profile system intfl
mediatrace profile perf-monitor rtpl
mediatrace path-specifier path1 destination ip 10.10.132.2 port 2000
  source ip 10.10.130.2 port 1000
mediatrace flow-specifier flow1
  source-ip 10.10.130.2 source-port 1000
  dest-ip 10.10.132.2 dest-port 2000
mediatrace session-params spl
  response-timeout 10
  frequency 60 inactivity-timeout 180
mediatrace 1
  path-specifier path1
  session-params spl
  profile perf-monitor rtpl flow-specifier flow1
mediatrace schedule 1 life forever start-time now
mediatrace 2
  path-specifier path1
  session-params spl
  profile system intfl
mediatrace schedule 2 life forever start-time now
```

サンプルのリバース Mediatrace 設定は、次のとおりです。

```
Device# show mediatrace initiator
Mediatrace Initiator Software Version: 3.0
Mediatrace Protocol Version: 1
Mediatrace Initiator status: enabled

Source IP: 10.10.1.1
Source IPv6:

Number of Maximum Allowed Active Session: 8
Number of Configured Session: 3
Number of Active Session      : 2
Number of Pending Session     : 0
Number of Inactive Session    : 1
Number of Total Proxy Session : 1
Number of Active Proxy Session : 1
Number of Pending Proxy Session : 0
Number of Inactive Proxy Session : 0

Note: the number of active session may be higher than max active session
      because the max active session count was changed recently.

Device# show run
Device# show running-config | show mediatrace
mediatrace responder
mediatrace initiator source-ip 10.10.1.1
mediatrace profile perf-monitor MT_PERF_RTP
mediatrace path-specifier MT_PATH destination ip 10.11.1.10 port 21064
  source ip 10.10.1.11 port 28938
mediatrace path-specifier MT_PATH2 destination ip 10.10.10.10 port 16514
  source ip 10.10.1.10 port 16558
mediatrace flow-specifier MT_FLOW
  source-ip 10.10.1.11 source-port 28938
  dest-ip 10.10.1.50 dest-port 21064
mediatrace flow-specifier MT_FLOW2
  source-ip 10.1.1.50 source-port 21064
  dest-ip 10.1.1.11 dest-port 28938
mediatrace session-params MT_PARAMS
  response-timeout 50
  frequency 60 inactivity-timeout 180
  history data-sets-kept 10
mediatrace reverse 155
  path-specifier forward/reverse MT_PATH/MT_PATH2
  session-params MT_PARAMS
  profile perf-monitor MT_PERF_RTP flow-specifier MT_FLOW2
mediatrace schedule 155 life forever start-time now
mediatrace 157
  path-specifier MT_PATH
  session-params MT_PARAMS
  profile perf-monitor MT_PERF_RTP flow-specifier MT_FLOW
mediatrace schedule 157 life forever start-time now
```

次の作業

Medianet 製品ファミリの製品設定の詳細については、このガイドの他の章または『*Cisco Media Monitoring Configuration Guide*』を参照してください。

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 Mediatrace およびその他の Cisco Medianet 製品の設計、設定、ならびにトラブルシューティングに関する資料（クイック スタート ガイドや導入ガイドなど）。	Cisco Medianet ナレッジベース ポータルサイト (http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html) を参照してください。
IP アドレッシング コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『Cisco Media Monitoring Command Reference』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能がサポートする新しい 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。	--

RFC

RFC ¹	タイトル
RFC 2205	Resource Reservation Protocol (RSVP) http://www.ietf.org/rfc/rfc2205.txt

¹ これらの参考資料は、IP アドレッシングおよび IP ルーティングに関連する項目で利用できる多くの RFC の例です。RFC の完全なリストについては、IETF RFC のサイト (<http://www.ietf.org/rfc.html>) を参照してください。

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>

Cisco Mediatrace の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 1 : Cisco Mediatrace の機能情報

機能名	リリース	機能情報
Cisco Mediatrace 1.0	15.1(3)T 12.2(58)SE 15.1(4)M1 15.0(1)SY 15.1(1)SY 15.1(1)SY1 15.2(1)S Cisco IOS XE Release 3.5S 15.1(2)SY	

機能名	リリース	機能情報
		<p>この機能を使用すると、データストリームに関するネットワーク パフォーマンス低下の問題の切り分けを行って、トラブルシューティングを実行できます。</p> <p>この機能により、次のコマンドが導入または変更されました。</p> <p>admin-params、clearmediatrace、incomplete-sessions、clock-rate (RTP パラメータ)、dest-ip (フロー)、frequency (セッション パラメータ)、history (セッション パラメータ)、ip-protocol (フロー)、max-dropout、max-reorder、mediatrace、mediatraceinitiator、mediatraceresponder、mediatracepath-specifier、mediatracepoll、mediatraceprofileperf-monitor、mediatraceprofilesysteem、mediatracesschedule、mediatracessession-params、metric-list (モニタリング プロファイル)、metric-list (システム プロファイル)、min-sequential、path-specifier、profileperf-monitor、profilesysteem、response-timeout (セッション パラメータ)、route-changereaction-time、sampling-interval、session-params、showmediatraceflow-specifier、showmediatraceinitiator、showmediatracepath-specifier、showmediatraceprofilesysteem、showmediatraceprofileperf-monitor、showmediatraceresponderapp-health、</p>

機能名	リリース	機能情報
		showmediatracerespondersessions 、 showmediatracession 、 showmediatracession-params 、 source-ip （フロー）、 sourceip （パス）。



第 3 章

Cisco Performance Monitor の設定

このドキュメントには、Cisco Performance Monitor の設定に関する情報と説明が記載されています。

- 機能情報の確認, 43 ページ
- Cisco Performance Monitor に関する情報, 44 ページ
- Cisco Performance Monitor の設定、トラブルシューティング、およびメンテナンスの方法, 50 ページ
- Cisco Performance Monitor の設定例, 102 ページ
- 次の作業, 103 ページ
- その他の参考資料, 104 ページ
- Cisco Performance Monitor の機能情報, 106 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。

Cisco Performance Monitor に関する情報

Cisco Performance Monitor の概要

Cisco Performance Monitor では、ネットワーク内のパケットフローをモニタすることで、対象のアプリケーションのパフォーマンスに重大な影響が現れる前に、そのフローに影響をおよぼす可能性がある問題点を認識できます。高品質で対話型のビデオトラフィックはネットワークの問題点の影響を非常に受けやすいため、ビデオトラフィックに対しては特にパフォーマンスモニタリングの重要性は高くなります。他のアプリケーションに影響を与えることがほとんどない軽度の問題であっても、ビデオの品質には大きな影響をおよぼす可能性があります。

Cisco Performance Monitor は Cisco NetFlow や Cisco Flexible NetFlow と同様のソフトウェア コンポーネントとコマンドを使用するので、それらの製品について熟知していると、Cisco Performance Monitor の設定方法について理解するのに役立ちます。これらの製品は、ルータを通過するパケットの統計情報を提供し、IP ネットワークから IP 運用データを取得するための定番製品です。これらは、ネットワークとセキュリティのモニタリング、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。Cisco NetFlow および Cisco Flexible NetFlow の詳細については、「その他の参考資料」に記載されているドキュメントを参照してください。

Performance Monitor およびその他の Cisco Medianet 製品の設計、設定、ならびにトラブルシューティングの詳細については、クイック スタート ガイドや導入ガイドも含めて、Cisco Medianet ナレッジベース ポータルサイト (<http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html>) を参照してください。

Cisco Performance Monitor の設定の前提条件

Cisco Performance Monitor 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。

IPv4 トラフィック

- ネットワーキング デバイスが IPv4 ルーティング用に設定されていること。
- 使用しているルータおよび Flexible NetFlow を有効にするすべてのインターフェイスで Cisco Express Forwarding または分散型 Cisco Express Forwarding が有効になっていること。

IPv6 トラフィック

- Cisco Express Forwarding が、ルータ、および Cisco Performance Monitor を有効にするインターフェイスで有効になっている必要があります。Cisco Express Forwarding は **ipv6 cef** コマンドを使用して有効にすることができます。

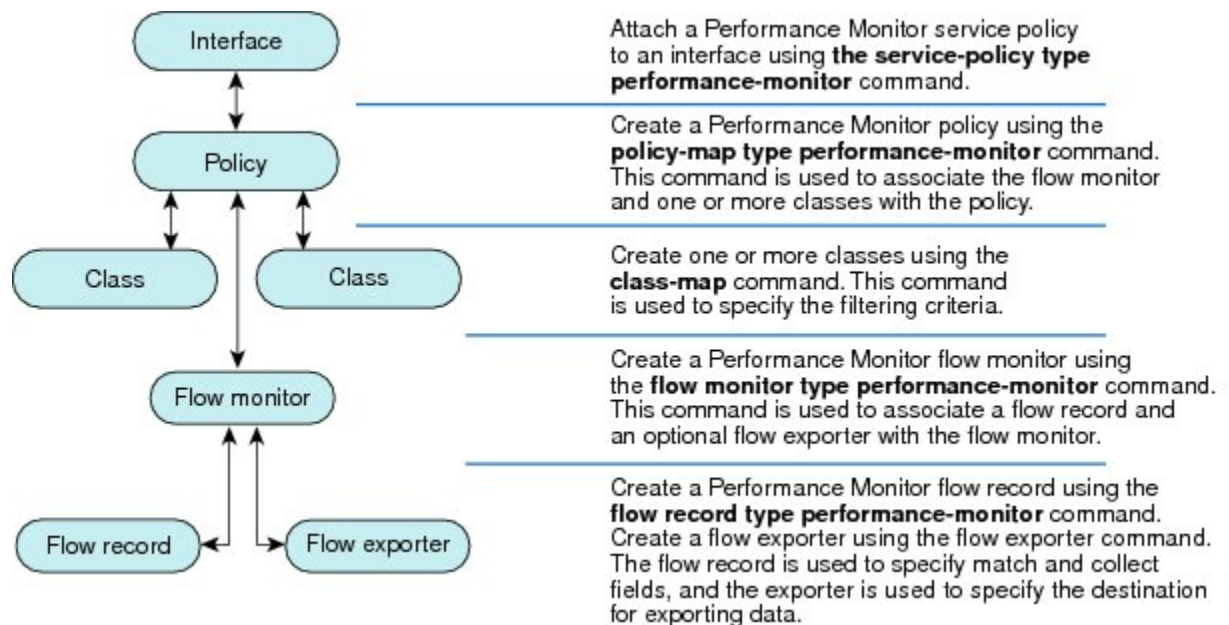
Cisco Performance Monitor の構成コンポーネント

Cisco Performance Monitor を設定するには、Flexible NetFlow で通常設定するのと同じ基本要素の多くを設定します。

- インターフェイス
- ポリシー (Policy)
- クラス
- フロー モニタ
- フロー レコード
- フロー エクスポート

次の図に、それらの要素がどのように関連しているかを示します。図の最下部にある要素を最初に設定します。

図 1 : Cisco Performance Monitor のコンポーネント



上記のように、ポリシーには1つ以上のクラスが含まれます。各クラスにはそのクラスに関連付けられているフロー モニタがあり、各フロー モニタにはフロー レコードとフロー モニタに関連付けられているオプションのフロー エクスポートがあります。これらの要素は、次の順序で設定します。

- 1 フロー レコードを設定して、モニタする非キー フィールドとキー フィールドを指定します。これは、**match** コマンドおよび**collect** コマンドを使用して設定します。また、オプションで、

フロー エクスポートを設定してエクスポート先を指定することもできます。Cisco Performance Monitor では、**performance-monitor** タイプのフロー レコードを設定する必要があります。

- 2 フロー レコードおよびフローエクスポートを含むフロー モニタを設定します。Cisco Performance Monitor では、**performance-monitor** タイプのフロー モニタを設定する必要があります。
- 3 **class-map** コマンドを使用して、クラスを設定してフィルタリング基準を指定します。
- 4 **policy-map** コマンドを使用して、ポリシーを設定して 1 つ以上のクラスと 1 つ以上の **performance-monitor** タイプのフロー モニタを含めます。Cisco Performance Monitor では、**performance-monitor** タイプのポリシーを設定する必要があります。
- 5 **service-policy type performance-monitor** コマンドを使用して、**performance-monitor** タイプのポリシーを該当のインターフェイスに関連付けます。

Cisco Performance Monitor を使用してモニタできるデータ

collect コマンドまたは **match** コマンドを使用して、対応する非キー フィールドについてフロー レコードを設定することにより、以下の情報をモニタできます。



ヒント

これらの統計情報の詳細については、『*Cisco Media Monitoring Command Reference*』で **show performance monitor status** コマンドを参照してください。

- IP パケット数 (IP Packet Count)
- IP TTL
- IP TTL (最小) (IP TTL minimum)
- IP TTL (最大) (IP TTL maximum)
- インターフェイス マッピングへのフロー (Flow to Interface Mapping)
- IP フローの宛先アドレスとポート、送信元アドレスとポート、およびプロトコル
- RTP 同期ソース (SSRC) (RTP Synchronization Source (SSRC))
- IP オクテット数 (IP Octets Count)
- メディア ストリーム パケット数 (Media Stream Packet Count)
- メディア ストリーム オクテット数 (Media Stream Octet Count)
- メディア バイト レート (Media Byte Rate)
- メディア バイト数 (Media Byte Count)
- メディア パケット レート (Media Packet Rate)
- メディア パケット損失数 (Media Packet Loss Count)
- メディア パケット損失レート (Media Packet Loss Rate)

- 予想パケット数 (Packets Expected Count)
- 測定レート (Measured Rate)
- メディア損失イベント数 (Media Loss Event Count)
- ラウンドトリップ時間 (RTT)
- 到着間ジッター (RFC3550) (最大) (Interarrival Jitter (RFC3550) max)
- 到着間ジッター (RFC3550) (最小 2) (Interarrival Jitter (RFC3550) min 2)
- 到着間ジッター (RFC3550) (平均) (Interarrival Jitter (RFC3550) mean)
- メディア レート変動 (Media Rate Variation)
- モニタ イベント (Monitor Event)
- メディア エラー (Media Error)
- メディア停止 (Media Stop)
- IP バイト数 (IP Byte Count)
- IP バイト レート (IP Byte Rate)
- IP Source Mask
- IP Destination Mask
- モニタリング インターバルのエポック (Epoch of A Monitoring Interval)
- パケット転送ステータス (Packet Forwarding Status)
- Packet Drops
- DSCP および IPv6 トラフィック クラス (DSCP and IPv6 Traffic Class)

Cisco Performance Monitor の SNMP MIB サポート

Cisco Performance Monitor は、メディア ストリームをモニタするため、業界標準の Simple Network Management Protocol (SNMP) の使用をサポートします。このサポート機能は、次に示すシスコ独自の SNMP Management Information Base (MIB) モジュールの追加と共に実装されます。

- CISCO-FLOW-MONITOR-TC-MIB : 以下の MIB モジュールに共通するテキスト規則を定義します。
- CISCO-FLOW-MONITOR-MIB : システムでサポートされているフロー モニタを表すフレームワーク、システムで学習されたフロー、それらのフローに関して収集されるフロー メトリックを定義します。
- CISCO-RTP-METRICS-MIB : RTCP Receiver Report パケット (RFC 3550) によって表されるメトリックと同様の、RTP ストリームに関して収集される品質メトリックを表すオブジェクトを定義します。

- **CISCO-IP-CBR-METRICS-MIB** : 固定ビット レート (CBR) をもつ IP ストリームに関して収集される品質メトリックを表すオブジェクトを定義します。

これらの MIB の詳細について、また、特定のプラットフォーム、Cisco IOS リリース、およびフィチャー セットの MIB を検索してダウンロードするには、Cisco MIB Locator (<http://www.cisco.com/go/mibs>) を使用してください。

また、この機能には、新しいコマンドライン インターフェイス (CLI) コマンド 2 つと、変更された CLI コマンド 1 つも含まれています。これらのコマンドは、次のとおりです。

- **snmp-serverhost** : 受信者へのフロー モニタリング SNMP 通知の配信を有効にします。
- **snmp-serverenabletrapsflowmon** : フロー モニタリング SNMP 通知を有効にします。デフォルトでは、フロー モニタリング SNMP 通知は無効になっています。
- **snmpmibflowmonalarmhistory** : フロー モニタリングのアラーム履歴ログで保持するエントリの最大数を設定します。

これらのコマンドの詳細については、『Cisco IOS Master Command List』を参照してください。

Catalyst 6500 プラットフォームに関する制限事項

Cisco Performance Monitor には Catalyst 6000 プラットフォームに関する次の制限事項があります。

- モニタできるインターフェイスのタイプについて、いくつかの制限事項があります。以下の 2 つの表に、Catalyst 6500 プラットフォームにおける入力モニタリングと出力モニタリングでサポートされているインターフェイスのタイプを示します。

表 2: 入力インターフェイスのサポート

インターフェイス タイプ	サポート
レイヤ 3 ルーテッド ポート	あり
レイヤ 3 サブインターフェイス (a)	なし
レイヤ 3 ポート チャンネル	あり
レイヤ 3 ポートチャンネルサブインターフェイス (a)	なし
レイヤ 3 SVI (b)	一部 (以下の箇条書きの 3 番目の項目を参照)
L3 トンネル	なし
レイヤ 2 物理 (スイッチド) ポート	あり
レイヤ 2 ポート チャンネル	あり

インターフェイス タイプ	サポート
レイヤ 2 VLAN	あり

表 3: 出力インターフェイスのサポート

インターフェイス タイプ	サポート
レイヤ 3 ルーテッド ポート	あり
レイヤ 3 サブインターフェイス (a)	あり
レイヤ 3 ポート チャンネル	あり
レイヤ 3 ポートチャンネルサブインターフェイス (a)	あり
レイヤ 3 SVI (b)	あり
L3 トンネル	なし
レイヤ 2 物理 (スイッチド) ポート	なし
レイヤ 2 ポート チャンネル	なし
レイヤ 2 VLAN	あり

- VRF でのパフォーマンス モニタリングはサポートされていません。
- マルチキャストフローのパフォーマンスのモニタリングは、入力方向でサポートされています。
- VLAN インターフェイスのトランク ポートからのルーテッドトラフィックは、トラフィックの送信元 VLAN インターフェイスを特定できないため、モニタできません。「Routed traffic from trunk ports will not be monitored by ingress policy on VLAN interface (トランク ポートからのルーテッドトラフィックは、VLAN インターフェイスの入力ポリシーにより、モニタされません)」という syslog メッセージが表示されます。

回避策として、トランク インターフェイスでパフォーマンス モニタリング ポリシーを設定できます。このモニタリングを利用すると、CPU 使用率が増加することになります。

- match all タイプのクラス マップを使用することはできません。サポートされているのは、match any タイプの検索のみです。match all タイプのクラス マップを使用するようにパフォーマンス モニタリングを設定した場合、パケットの複製が CPU に送られます。その結果、match-all クラスが正常に適用されると、再びパケットが CPU で分類されて、必要に応じてドロップされます。そのため、CPU 使用率が予想よりも高くなります。

- VLAN インターフェイスの出力のパフォーマンス モニタリング ポリシーでは、VLAN 内でブリッジされるトラフィックはモニタされません。これは、ハードウェアの制限によるものです。回避策は、VLAN インターフェイスの出力だけでなく入力でもポリシーを適用することです。VLAN インターフェイスの入力のポリシーでは、ブリッジされたパケットがモニタされます。
 - 出力ポリシーによって複製されるパケットについては、ソフトウェアによるレート制限のみが可能です。それらのパケットについてハードウェアベースの保護を使用することはできません。したがって、多くのフローをモニタする場合のシナリオでは、CPU 割り込み使用率が高くなる可能性があります。
 - 出力パフォーマンス モニタリングでは、Catalyst 6500 プラットフォームの再循環メカニズムを利用します。その結果、フレーム スイッチングの遅延が数マイクロ秒増加します。
 - 高速（CEF）パスを使用してスイッチングされるパケットについては、パフォーマンス モニタリングはサポートされていません。
 - 合法的傍受およびパフォーマンス モニタリングでは、パケットの複製と同じメカニズムを利用します。合法的傍受機能は、パフォーマンス モニタリングよりも優先されます。したがって、パフォーマンス モニタリングは、合法的傍受機能が有効になっている場合には機能しません。そのようなことが発生すると、syslog メッセージが作成されます。
 - パフォーマンス モニタリングでは、最適化 ACL ロギング、VACL キャプチャ、IPv6 コピーなどの他の機能と同じメカニズムを利用します。最初に有効にされた機能が優先されます。その他の機能はブロックされて設定できなくなり、syslog メッセージが作成されます。
- 反応（メディア停止を含む）がパフォーマンス モニタリング ポリシーで設定されている場合にトラフィックが不安定になると、syslog メッセージはバッファに記録され、コンソール画面には出力されません。

Cisco Performance Monitor の設定、トラブルシューティング、およびメンテナンスの方法



（注）これらの作業で使用する Flexible NetFlow のコマンド、キーワード、および引数の多くは、以前のリリースでも利用できます。これらの既存の Flexible NetFlow コマンド、キーワード、および引数の詳細については、『Cisco IOS Flexible NetFlow Command Reference』を参照してください。

Cisco Performance Monitor のフロー エクスポートの設定

フロー エクスポートは、Cisco Performance Monitor で収集されるデータを NetFlow Collection Engine などのリモートシステムへ送信するために使用されます。エクスポートでは、転送プロトコルと

して User Datagram Protocol (UDP) が使用され、バージョン 9 エクスポート フォーマットが使用されます。

詳細な分析や保管を目的として、Cisco Performance Monitor によって収集されるデータをリモートシステムにエクスポートするためにフロー モニタ用のフロー エクスポートを設定するには、次のオプション作業を実行します。Cisco Performance Monitor では、フロー エクスポートは Cisco IOS Flexible NetFlow の場合と同様の方法で設定します。詳細については、『*Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters*』を参照してください。



(注) フローエクスポートごとに、1つ宛先のみがサポートされます。複数の宛先にデータをエクスポートする場合は、複数のフロー エクスポートを設定してフロー モニタに割り当てる必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **flowexporterexporter-name**
4. **descriptiondescription**
5. **destination {ip-address | hostname} [vrfvrf-name]**
6. **export-protocolnetflow-v9**
7. **dscpdscp**
8. **sourceinterface-typeinterface-number**
9. **option {exporter-stats | interface-table | sampler-table} [timeoutseconds]**
10. **output-features**
11. **templatedattimeoutseconds**
12. **transportudpudp-port**
13. **ttlseconds**
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	enable 例 : <pre>Router> enable</pre>	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 : <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。

	コマンドまたはアクション	目的
ステップ 3	flowexporter <i>exporter-name</i> 例 : <pre>Router(config)# flow exporter EXPORTER-1</pre>	フロー エクスポートを作成し、Flexible NetFlow 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。 • このコマンドでは、既存のフローエクスポートを変更することもできます。
ステップ 4	description <i>description</i> 例 : <pre>Router(config-flow-exporter)# description Exports to the datacenter</pre>	(任意) 設定および showflowexporter コマンドの出力に表示されるエクスポートの説明を設定します。
ステップ 5	destination { <i>ip-address</i> <i>hostname</i> } [<i>vrfvrf-name</i>] 例 : <pre>Router(config-flow-exporter)# destination 172.16.10.2</pre>	エクスポートでデータを送信する宛先システムの IP アドレスまたはホスト名を指定します。
ステップ 6	export-protocol <i>netflow-v9</i> 例 : <pre>Router(config-flow-exporter)# export-protocol netflow-v9</pre>	エクスポートで使用する NetFlow エクスポート プロトコルのバージョンを指定します。デフォルト値 (netflow-v9) のみがサポートされています。
ステップ 7	dscp <i>dscp</i> 例 : <pre>Router(config-flow-exporter)# dscp 63</pre>	(任意) エクスポートによって送信されるデータグラムの Diffserv コードポイント (DSCP) パラメータを設定します。 • <i>dscp</i> 引数の範囲は 0 ～ 63 です。デフォルト : 0。
ステップ 8	source <i>interface-typeinterface-number</i> 例 : <pre>Router(config-flow-exporter)# source ethernet 0/0</pre>	(任意) エクスポートで、エクスポートされたデータグラムの送信元 IP アドレスとして IP アドレスを使用するローカル インターフェイスを指定します。
ステップ 9	option { exporter-stats interface-table sampler-table } [<i>timeoutseconds</i>] 例 : <pre>Router(config-flow-exporter)# option exporter-stats timeout 120</pre>	(任意) エクスポートのオプションデータパラメータを設定します。 • 3 つのオプションを同時に設定できます。 • <i>seconds</i> 引数の範囲は、1 ～ 86,400 です。デフォルト値 : 600。

	コマンドまたはアクション	目的
ステップ 10	output-features 例 : <pre>Router(config-flow-exporter)# output-features</pre>	(任意) Quality of Service (QoS) と暗号化を使用してエクスポート パケットを送信できるようにします。
ステップ 11	templatedatatimeoutseconds 例 : <pre>Router(config-flow-exporter)# template data timeout 120</pre>	(任意) タイムアウトに基づくテンプレートの再送を設定します。 • <i>seconds</i> 引数の範囲は、1 ～ 86400 です (86400 秒 = 24 時間)。
ステップ 12	transportudpudp-port 例 : <pre>Router(config-flow-exporter)# transport udp 650</pre>	UDP をトランスポート プロトコルとして設定し、エクスポートされるデータグラムを宛先システムがリスニングする UDP ポートを指定します。 • <i>udp-port</i> 引数の範囲は 1 ～ 65536 です。
ステップ 13	ttlseconds 例 : <pre>Router(config-flow-exporter)# ttl 15</pre>	(任意) エクスポートによって送信されるデータグラムの存続可能時間 (TTL) 値を設定します。 • <i>seconds</i> 引数の範囲は、1 ～ 255 です。
ステップ 14	end 例 : <pre>Router(config-flow-exporter)# end</pre>	フロー エクスポート 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。

トラブルシューティングのヒント

フロー エクスポートの設定とステータスをチェックするには、**showflowexporter** コマンドを使用します。

Cisco Performance Monitor のフロー レコードの設定

Cisco Performance Monitor のフロー レコードの設定に関する基本概念と手法は、Flexible NetFlow のフローレコードの場合と同じです。フローレコードは、収集されたデータを集約して表示する方法を指定します。唯一の大きな違いは、Cisco Performance Monitor の場合、コマンドに **type performance-monitor** が含まれていることです。

手順の概要

1. enable
2. configureterminal
3. flowrecordtypeperformance-monitorrecord-name
4. matchipv4{destination{address | prefix[minimum-mask mask]}| protocol| source{address | prefix[minimum-mask mask]}}
5. matchtransport{destination-port| rtp [ssrc]| source-port}
6. collectapplicationmedia{bytes{rate| counter}| packets{rate| counter}| events}
7. collectcounter{bytes[long| rate]| packets[dropped[long| long]}}
8. collectinterface{input| output}
9. collectipv4{destination mask[minimum-mask mask]| dscp| source mask[minimum-mask mask] | ttl[minimum | maximum]}
10. collectmonitorevent
11. collectroutingforwarding-status[reason]
12. collecttimestampinternal
13. collecttransport{event packet-loss counter | packets{expected counter| lost{counter| rate}}| round-trip-time| rtp jitter{minimum| mean| maximum}}
14. collectflowdirection
15. 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 : <pre>Router> enable</pre>	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 : <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	flowrecordtypeperformance-monitorrecord-name 例 : <pre>Router(config)# flow record type performance-monitor record-8</pre>	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。 • このコマンドでは、既存のフロー レコードを変更することもできます。
ステップ 4	matchipv4{destination{address prefix[minimum-mask mask]} protocol source{address prefix[minimum-mask mask]}}	1 つ以上の IPv4 フィールドをキー フィールドとして使用することを指定します。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Router(config-flow-record)# match ipv4 destination address</pre>	
ステップ 5	<p>matchtransport{destination-port rtp [ssrc] source-port}</p> <p>例 :</p> <pre>Router(config-flow-record)# match transport destination-port</pre>	Real-time Transport Protocol (RTP) パケット ヘッダーの Synchronization Source (SSRC) フィールドを含め、1 つ以上のトランスポート層フィールドをキー フィールドとして使用することを指定します。
ステップ 6	<p>collectapplicationmedia{bytes{rate counter} packets{rate counter} events}</p> <p>例 :</p> <pre>Router(config-flow-record)# collect application media events</pre>	アプリケーションメディアのバイト、パケット、またはイベントを非キーフィールドとして使用することを指定します。アプリケーションイベントは、フローの反応ステートメントで指定されているいずれかのしきい値をモニタリングインターバルで少なくとも1回超えることがあった場合や、メディアパケットが検出されなかった場合に発生します。
ステップ 7	<p>collectcounter{bytes[long rate] packets[dropped[long] long]}</p> <p>例 :</p> <pre>Router(config-flow-record)# collect counter bytes long</pre>	非キーフィールドとして使用するバイトまたはパケットの数を指定します。
ステップ 8	<p>collectinterface{input output}</p> <p>例 :</p> <pre>Router(config-flow-record)# collect interface input</pre>	入力インターフェイスまたは出力インターフェイスを非キーフィールドとして使用することを指定します。
ステップ 9	<p>collectipv4{destination mask[minimum-mask mask]} dscp source mask[minimum-mask mask] ttl[minimum maximum]}</p> <p>例 :</p> <pre>Router(config-flow-record)# collect ipv4 dscp</pre>	IPv4 DiffServ コード ポイント (DCSP) フィールドまたは IPv4 存続可能時間 (TTL) フィールドを非キーフィールドとして使用することを指定します。

	コマンドまたはアクション	目的
ステップ 10	collectmonitorevent 例 : <pre>Router(config-flow-record)# collect monitor event</pre>	モニタ イベント フィールドを非キー フィールドとして使用することを指定します。モニタ イベントは、メディア アプリケーション パケットが検出されない場合に発生します
ステップ 11	collectroutingforwarding-status[reason] 例 : <pre>Router(config-flow-record)# collect routing forwarding-status</pre>	1 つ以上のルーティング属性を非キー フィールドとして使用することを指定します。
ステップ 12	collecttimestampinternal 例 : <pre>Router(config-flow-record)# collect timestamp internal</pre>	フローで最初または最後に検出されたパケットのシステム タイムスタンプを非キー フィールドとして使用することを指定します。
ステップ 13	collecttransport{event packet-loss counter packets{expected counter lost{counter rate}} round-trip-time rtp jitter{minimum mean maximum}} 例 : <pre>Router(config-flow-record)# collect transport packets expected counter</pre>	1 つ以上のトランスポート層フィールドを非キーフィールドとして使用することを指定します。これらのフィールドには、次のメトリックが含まれます。 <ul style="list-style-type: none"> • パケット損失カウンタ • 予想パケット カウンタ • ジッター
ステップ 14	collectflowdirection 例 : <pre>Router(config-flow-record)# collect flow direction</pre>	フロー方向フィールドを非キーフィールドとして使用することを指定します。
ステップ 15	end 例 : <pre>Router(config-flow-record)# end</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、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

フロー レコードの設定とステータスをチェックするには、**showflowrecordtypeperformance-monitor** コマンドを使用します。

Cisco Performance Monitor のフロー モニタの設定

Cisco Performance Monitor のフロー モニタの設定に関する基本概念は、Flexible NetFlow のフロー モニタの場合と同じです。各フロー モニタには、別々のキャッシュが割り当てられ、キャッシュ エントリの内容とレイアウトを定義するレコードが必要です。

フロー モニタを設定する場合は、次のいずれかを使用する必要があります:

- 設定済みの既存のフロー レコード
- 次のいずれかのデフォルトの事前定義済みレコード
 - デフォルトの RTP レコード (**default-rtp**)
 - デフォルトの TCP レコード (**default-tcp**)
 - Flexible NetFlow の「NetFlow IPv4 original input」



(注)

フロー レコードを変更するには、関連付けられているすべてのフロー モニタから削除する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **flowmonitortypeperformance-monitor***monitor-name*
4. **description***description*
5. **cache**{*entries*|*timeout*|*type*}
6. **statistics**{*packet*}
7. **exporter***exporter-name*
8. **record** {*record-name*|**default-rtp**|**default-tcp**|**netflow ipv4 original-input**}
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 : Device> enable	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 : Device# 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	flowmonitortypeperformance-monitormonitor-name 例 : Device(config)# flow monitor type performance-monitor FLOW-MONITOR-2	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。 • 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	descriptiondescription 例 : Device(config-flow-monitor)# description Used for monitoring IPv4 traffic	(任意) フロー モニタの説明を作成します。
ステップ 5	cache{entries timeout type} 例 : Device(config-flow-monitor)# cache timeout 20	(任意) フロー モニタのキャッシュを作成します。
ステップ 6	statistics{packet} 例 : Device(config-flow-monitor)# statistics	(任意) フロー モニタの統計情報を収集するかどうかを指定します。
ステップ 7	exporterexporter-name 例 : Device(config-flow-monitor)# exporter export-4	フロー モニタのフロー エクスポートを指定します。
ステップ 8	record {record-name default-rtp default-tcp netflow ipv4 original-input} 例 : Device(config-flow-monitor)# record default-rtp	フロー モニタのフロー レコードを指定します。
ステップ 9	end 例 : Device(config-flow-monitor)# end	フロー モニタ 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。

トラブルシューティングのヒント

フロー モニタの設定とステータスをチェックするには、**showflowmonitortypeperformance-monitor** コマンドおよび **showrunning-configflowmonitor** コマンドを使用します。

Cisco Performance Monitor のフロー クラスの設定

Cisco Performance Monitor のクラスの設定に関する基本概念と手法は、他のタイプのクラスの場合と同じです。クラスは、モニタリング対象のフロー トラフィックを決定するフィルタを指定します。フィルタは、さまざまな **match** コマンドをクラス マップ モードで使用して設定します。

まだフロー モニタを設定していない場合は、次のいずれかを実行できます。



(注) ネスト形式のクラス マップはサポートされていません。つまり、**class-map** コマンドはクラス マップ コンフィギュレーション モード (**config-cmap**) では使用できません。

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map***class-name*
4. **description***description*
5. **match** {*access-group* {*access-group* | **name** *access-group-name*} | **any** | **class-map** *class-map-name* | **cos** *cos-value* | **destination-address** *macaddress* | **discard-class** *class-number* | **dscp** *dscp-value* | **flow** {**direction** | **sampler**} | **fr-de** | **fr-dlci** *dlci-number* | **input-interface** *interface-name* | **ip** {**rtp** *starting-port-number* *port-range* | **precedence** | **dscp**} | **mpls** **experimental** *topmost-number* | **notmatch-criterion** | **packetlength** {**max** *maximum-length-value* [**min** *minimum-length-value*] | **min** *minimum-length-value* [**max** *maximum-length-value*]} | **precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*} | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **source-address** *macaddress-destination* | **vlan** {*vlan-id* | *vlan-range* | *vlan-combination*}}
6. **rename** *class-name*
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	enable 例 : Device> enable	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 : Device# 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	class-mapclass-name 例 : Device(config)# class-map class-4	ポリシーに含めるクラスを指定します。ポリシーに含める各クラスについて、このコマンドを繰り返し実行します。
ステップ 4	descriptiondescription 例 : Device(config-cmap)# description match any packets	(任意) フロークラスの説明を作成します。
ステップ 5	match {access-group {access-group nameaccess-group-name} any class-mapclass-map-name coscos-value destination-addressmacaddress discard-classclass-number dscpdscp-value flow {direction sampler} fr-de fr-dlciidci-number input-interfaceinterface-name ip {rtpstarting-port-numberport-range precedence dscp} mplsexperimentaltopmostnumber notmatch-criterion packetlength {maxmaximum-length-value [minminimum-length-value] minminimum-length-value [maxmaximum-length-value]} precedence {precedence-criteria1 precedence-criteria2 precedence-criteria3 precedence-criteria4} protocolprotocol-name qos-groupqos-group-value source-addressmacaddress-destination vlan {vlan-id vlan-range vlan-combination}} 例 : Device(config-cmap)# match any	分類基準を指定します。 詳細および例については、『Cisco Media Monitoring Command Reference』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 6	rename <i>class-name</i> 例 : Device(config-cmap)# rename class-4	フロー クラスの新しい名前を指定します。
ステップ 7	end 例 : Device(config-cmap)# 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。

トラブルシューティングのヒント

フロー クラスの設定とステータスをチェックするには、**show policy-map type performance-monitor** コマンドまたは **show class-map** コマンドを使用します。

既存のフロー モニタを使用した Cisco Performance Monitor のフロー ポリシーの設定

Cisco Performance Monitor のクラスの設定に関する基本概念と手法は、他のタイプのクラスの場合と同じです。クラスは、どのフロー モニタを含めるかを指定します。唯一の大きな違いは、Cisco Performance Monitor の場合、**policy-map** コマンドに **type performance-monitor** が含まれていることです。

フロー モニタをまだ設定していない場合や、既存のフロー モニタを新しいクラスに使用しない場合は、**flow monitor inline** オプションを使用し、どのフロー レコードおよびフロー エクスポートを含めるかを指定して、フロー モニタを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type performance-monitor***policy-name*
4. **parameter-map type performance-monitor system-default-aor**
5. **class** {*class-name* | **class-default**}
6. **flow monitor***monitor-name*
7. **monitor metric ip-cbr**
8. **ratelayer3**{*byte-rate* {**bps** | **kbits** | **mbps** | **gbps**} | **packet**}
9. **exit**
10. **monitormetricrtp**
11. **clock-rate**{*type-number* | *type-name* | **default**}*rate*
12. **max-dropout***number*
13. **max-reorder***number*
14. **min-sequential***number*
15. **ssrcmaximum***number*
16. **exit**
17. **monitorparameters**
18. **flows***number*
19. **intervalduration***number*
20. **history***number*
21. **timeout***number*
22. **exit**
23. **reactID** {**media-stop** | **mrp** | **rtp-jitter-average** | **transport-packets-lost-rate**}
24. **action** {**snmp** | **syslog**}
25. **alarmseverity**{**alert** | **critical** | **emergency** | **error** | **info**}
26. **alarmtype**{**discrete** | **grouped**{*countnumber* | *percentnumber*}
27. **thresholdvalue**{*gnumber* | *gtnumber* | *lnumber* | *ltnumber* | *rangerng-start**rng-end*}
28. **description***description*
29. **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 : Device> enable	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	configure terminal 例 : Device# 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	policy-map type performance-monitor <i>policy-name</i> 例 : Device(config)# policy-map type performance-monitor FLOW-MONITOR-4	ポリシーを作成し、ポリシー 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、既存のポリシーを変更することもできます。
ステップ 4	parameter-map type performance-monitor system-default-aor 例 : Device(config-pmap)# parameter-map type performance-monitor system-default-aor	Performance Monitor のパラメータ マップを作成します。使用可能な唯一のマップは system-default-aor マップです。
ステップ 5	class {class-name class-default} 例 : Device(config-pmap)# class class-4	ポリシーに含めるクラスを指定します。ポリシーに含める各クラスについて、このコマンドを繰り返し実行します。
ステップ 6	flow monitor <i>monitor-name</i> 例 : Device(config-pmap-c)# flow monitor FLOW-MONITOR-4	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。既存のフロー モニタを使用しない場合は、 既存のフロー モニタを使用しない Cisco Performance Monitor のフロー ポリシーの設定 、(67 ページ) の説明に従って、 inline オプションを使用して新しいフロー モニタを設定できます。
ステップ 7	monitor metric ip-cbr 例 : Device(config-pmap-c)# monitor metric ip-cbr	(任意) IP-CBR モニタ メトリック 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	ratelayer3 { <i>byte-rate</i> { bps kbps mbps gbps } packet } 例 : Device(config-pmap-c-mipcbr)# rate layer3 248 mbps	(任意) メトリックのモニタリングのレート指定します。 • byte-rate : データ レート (単位 : Bps、kBps、mBps、または gBps) 。指定できる範囲は 1 ～ 65535 です。 • packet : パケット レート (単位 : pps) 。

	コマンドまたはアクション	目的
ステップ 9	exit 例 : Device(config-pmap-c-mipcbr)# exit	ポリシー クラス コンフィギュレーション モードに戻ります。
ステップ 10	monitormetricrtp 例 : Device(config-pmap-c)# monitor metric rtp	RTP モニタ メトリック コンフィギュレーション モードを開始します。
ステップ 11	clock-rate { <i>type-number</i> <i>type-name</i> default } <i>rate</i> 例 : Device(config-pmap-c-mrtp)# clock-rate 8 9600	RTP ビデオ モニタリング メトリック のサンプリング に使用するクロック レートを指定します。 クロック タイプ の番号 と名前 の詳細 については、『 <i>Cisco Media Monitoring Command Reference</i> 』を参照してください。 <i>rate</i> の範囲は 1 ～ 192 kHz です。
ステップ 12	max-dropoutnumber 例 : Device(config-pmap-c-mrtp)# max-dropout 2	RTP ビデオ モニタリング メトリック のサンプリング 時に許可されるドロップアウトの最大数を指定します。
ステップ 13	max-reordernumber 例 : Device(config-pmap-c-mrtp)# max-reorder 4	RTP ビデオ モニタリング メトリック のサンプリング 時に許可される順序変更の最大数を指定します。
ステップ 14	min-sequentialnumber 例 : Device(config-pmap-c-mrtp)# min-sequential 2	ストリームを RTP フローとして識別するために必要な連続パケットの最小数を指定します。
ステップ 15	ssrcmaximumnumber 例 : Device(config-pmap-c-mrtp)# ssrc maximum 20	同じフロー内でモニタできる SSRC の最大数を指定します。 フローは、プロトコル、送信元と宛先のアドレス、および送信元と宛先のポートによって定義されます。

	コマンドまたはアクション	目的
ステップ 16	exit 例 : Device(config-pmap-c-mrtp)# exit	ポリシー クラス コンフィギュレーション モードに戻ります。
ステップ 17	monitorparameters 例 : Device(config-pmap-c)# monitor parameters	モニタ パラメータ コンフィギュレーション モードを開始します。
ステップ 18	flowsnumber 例 : Device(config-pmap-c-mparam)# flows 40	各モニタ キャッシュのフローの最大数を指定します。
ステップ 19	intervaldurationnumber 例 : Device(config-pmap-c-mparam)# interval duration 40	ビデオ モニタリング メトリックのサンプリング間隔 (秒) を指定します。
ステップ 20	historynumber 例 : Device(config-pmap-c-mparam)# history 4	収集されるビデオ モニタリング メトリックの履歴バケットの数を指定します。
ステップ 21	timeoutnumber 例 : Device(config-pmap-c-mparam)# timeout 20	停止したフローがデータベースから削除されるまでのインターバルの数を指定します。
ステップ 22	exit 例 : Device(config-pmap-c-mparam)# exit	ポリシー クラス コンフィギュレーション モードに戻ります。
ステップ 23	reactID {media-stop mrv rtp-jitter-average transport-packets-lost-rate}	次のメトリックのしきい値を超えた場合の反応を指定できるモードを開始します。 • ID : 反応設定の ID。有効値の範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Device(config-pmap-c)# react 41 rtp-jitter-average</pre>	<ul style="list-style-type: none"> • media-stop : フローのトラフィックが検出されません。 • mrvt : 実際のレートと予想レートの差を予想レートで割ることによって算出されるレート。 • rtp-jitter-average : 平均ジッター。 • transport-packets-lost-rate : 損失パケット数を予想パケット数で割ることによって算出されるレート。
ステップ 24	<p>action {snmp syslog}</p> <p>例 :</p> <pre>Device(config-pmap-c-react)# action syslog</pre>	しきい値を超えた場合の報告方法を指定します。
ステップ 25	<p>alarmseverity {alert critical emergency error info}</p> <p>例 :</p> <pre>Device(config-pmap-c-react)# alarm severity critical</pre>	報告されるアラームのレベルを指定します。デフォルト設定は、 info です。
ステップ 26	<p>alarmtype {discrete grouped {countnumber percentnumber}}</p> <p>例 :</p> <pre>Device(config-pmap-c-react)# alarm type discrete</pre>	報告が必要なアラームと見なされるレベルのタイプを指定します。デフォルト設定は、 discrete です。
ステップ 27	<p>thresholdvalue {gnumber gtnumber lenumber ltnumber rangerng-startrng-end}</p> <p>例 :</p> <pre>Device(config-pmap-c-react)# threshold value ge 20</pre>	<p>報告が必要なアラームと見なされるしきい値のタイプを指定します。</p> <p>値が指定されておらず、アプリケーション名がキー フィールドとして設定されている場合は、デフォルトのマップで検出されるしきい値が使用されます。値が指定されておらず、また、アプリケーション名がキー フィールドとして設定されていない場合、しきい値にはデフォルト値が使用されます。</p> <p>同じポリシーとクラスに対して複数の反応コマンドが設定されているが、しきい値が指定されているのは1つの反応設定のみである場合は、設定されている反応の値が優先され、残りのしきい値は無視されます。</p> <p>同じポリシーとクラスに対して複数の反応コマンドが設定されており、しきい値が1つも設定されていない場合は、</p>

	コマンドまたはアクション	目的
		最も小さい反応 ID が割り当てられている設定にデフォルトのしきい値が適用されます。
ステップ 28	description <i>description</i> 例 : Device(config-cmap-c-react)# description rtp-jitter-average above 40	(任意) 反応の説明を作成します。
ステップ 29	end 例 : Device(config-pmap-c-react)# 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。

トラブルシューティングのヒント

フロー ポリシーの設定とステータスをチェックするには、**show policy-map type performance-monitor** コマンドを使用します。

既存のフロー モニタを使用しない Cisco Performance Monitor のフロー ポリシーの設定

Cisco Performance Monitor のクラスの設定に関する基本概念と手法は、他のタイプのクラスの場合と同じです。クラスは、どのフロー モニタを含めるかを指定します。唯一の大きな違いは、Cisco Performance Monitor の場合、**policy-map** コマンドに **typeperformance-monitor** が含まれていることです。

フロー モニタをまだ設定していない場合や、既存のフロー モニタを新しいクラスに使用しない場合は、クラス コンフィギュレーションモードで、どのフロー レコードおよびフロー エクスポートを含めるかを指定して、フロー モニタを設定できます。

手順の概要

1. **enable**
2. **configureterminal**
3. **policy-map***typeperformance-monitorpolicy-nameclassclass-name*
4. **class** *{class-name | class-default}*
5. **flowmonitorinline**
6. **record** *{record-name|default-rtp|default-tcp}*
7. **exporter***exporter-name*
8. **exit**
9. **monitor metric** *ip-cbr*
10. **ratelayer3** *{byte-rate {bps | kbps | mbps | gbps} | packet}*
11. **exit**
12. **monitormetricrtp**
13. **clock-rate** *{type-number| type-name} rate*
14. **max-dropout***number*
15. **max-reorder***number*
16. **min-sequential***number*
17. **ssrcmaximum***number*
18. **exit**
19. **monitorparameters**
20. **flows***number*
21. **intervalduration***number*
22. **history***number*
23. **timeout***number*
24. **exit**
25. **react***ID {media-stop | mrv | rtp-jitter-average | transport-packets-lost-rate}*
26. **action** *{snmp | syslog}*
27. **alarmseverity** *{alert|critical|emergency|error| info}*
28. **alarmtype** *{discrete|grouped{countnumber | percentnumber}}*
29. **thresholdvalue** *{gnumber | gtnumber | lenumber | ltnumber | rangerng-startrng-end}*
30. **description***description*
31. **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 : <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <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	policy-map type performance-monitor policy-name class class-name 例 : <pre>Router(config)# policy-map type performance-monitor FLOW-MONITOR-4</pre>	ポリシーを作成し、ポリシー コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> このコマンドでは、既存のポリシーを変更することもできます。
ステップ 4	class {class-name class-default} 例 : <pre>Router(config-pmap)# class class-4</pre>	ポリシーに含めるクラスを指定します。 ポリシーに含める各クラスについて、このコマンドを繰り返し実行します。
ステップ 5	flowmonitor inline 例 : <pre>Router(config-pmap-c)# flow monitor inline</pre>	インライン モードを開始し、新しいフロー モニタを設定できるようにします。
ステップ 6	record {record-name default-rtp default-tcp} 例 : <pre>Router(config-pmap-c-flowmon)# record default-tcp</pre>	フロー モニタに関連付けるフロー レコードを指定します。
ステップ 7	exporter exporter-name 例 : <pre>Router(config-pmap-c-flowmon)# exporter exporter-4</pre>	フロー エクスポートに関連付けるフロー レコードを指定します。
ステップ 8	exit 例 : <pre>Router(config-pmap-c-flowmon)# exit</pre>	ポリシー クラス 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 9	monitor metric ip-cbr 例 : <pre>Router(config-pmap-c)# monitor metric ip-cbr</pre>	(任意) IP-CBR モニタ メトリック コンフィギュレーション モードを開始します。
ステップ 10	ratelayer3 { <i>byte-rate</i> { bps kbps mbps gbps } packet } 例 : <pre>Router(config-pmap-c-mipcbr)# rate layer3 248 mbps</pre>	(任意) メトリックのモニタリングのレート指定します。 <ul style="list-style-type: none"> • byte-rate : データ レート (単位 : Bps、kBps、mBps、または GBps)。指定できる範囲は 1 ～ 65535 です。 • packet : パケット レート (単位 : pps)。
ステップ 11	exit 例 : <pre>Router(config-pmap-c-mipcbr)# exit</pre>	ポリシークラスコンフィギュレーションモードに戻ります。
ステップ 12	monitormetricrtp 例 : <pre>Router(config-pmap-c)# monitor metric rtp</pre>	RTP モニタ メトリック 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	clock-rate { <i>type-number</i> <i>type-name</i> } <i>rate</i> 例 : <pre>Router(config-pmap-c-mrtp)# clock-rate 8 9600</pre>	RTP ビデオモニタリングメトリックのサンプリングに使用するクロック レートを指定します。 クロック タイプの番号と名前の詳細については、『 <i>Cisco Media Monitoring Command Reference</i> 』を参照してください。 <i>rate</i> の範囲は 1 ～ 192 kHz です。
ステップ 14	max-dropoutnumber 例 : <pre>Router(config-pmap-c-mrtp)# max-dropout 2</pre>	RTP ビデオモニタリングメトリックのサンプリング時に許可されるドロップアウトの最大数を指定します。
ステップ 15	max-reordernumber 例 : <pre>Router(config-pmap-c-mrtp)# max-reorder 4</pre>	RTP ビデオモニタリングメトリックのサンプリング時に許可される順序変更の最大数を指定します。

	コマンドまたはアクション	目的
ステップ 16	min-sequentialnumber 例 : <pre>Router(config-pmap-c-mrtp)# min-sequential 2</pre>	ストリームを RTP フローとして識別するために必要な連続パケットの最小数を指定します。
ステップ 17	ssrcmaximumnumber 例 : <pre>Router(config-pmap-c-mrtp)# ssrc maximum 20</pre>	同じフロー内でモニタできる SSRC の最大数を指定します。フローは、プロトコル、送信元と宛先のアドレス、および送信元と宛先のポートによって定義されます。
ステップ 18	exit 例 : <pre>Router(config-pmap-c-mrtp)# exit</pre>	ポリシークラスコンフィギュレーションモードに戻ります。
ステップ 19	monitorparameters 例 : <pre>Router(config-pmap-c)# monitor parameters</pre>	モニタパラメータコンフィギュレーションモードを開始します。
ステップ 20	flowsnumber 例 : <pre>Router(config-pmap-c-mparam)# flows 40</pre>	各モニタ キャッシュのフローの最大数を指定します。
ステップ 21	intervaldurationnumber 例 : <pre>Router(config-pmap-c-mparam)# interval duration 40</pre>	モニタリング メトリックを収集するためのインターバルの長さ（秒）を指定します。
ステップ 22	historynumber 例 : <pre>Router(config-pmap-c-mparam)# history 4</pre>	収集されたビデオモニタリングメトリックについて表示する履歴インターバルの数を指定します。
ステップ 23	timeoutnumber 例 : <pre>Router(config-pmap-c-mparam)# timeout 20</pre>	停止したフローがデータベースから削除されるまでのインターバルの数を指定します。

	コマンドまたはアクション	目的
ステップ 24	exit 例 : <pre>Router(config-pmap-c-mparam)# exit</pre>	ポリシークラスコンフィギュレーションモードに戻ります。
ステップ 25	react <i>ID</i> { media-stop mrsv rtp-jitter-average transport-packets-lost-rate } 例 : <pre>Router(config-pmap-c)# react 41 rtp-jitter-average</pre>	次のメトリックのしきい値を超えた場合の反応を指定できるモードを開始します。 <ul style="list-style-type: none"> • ID : 反応設定の ID。有効値の範囲は 1 ～ 65535 です。 • media-stop : フローのトラフィックが検出されません。 • mrsv : 実際のレートと予想レートの差を予想レートで割ることによって算出されるレート。 • rtp-jitter-average : 平均ジッター。 • transport-packets-lost-rate : 損失パケット数を予想パケット数で割ることによって算出されるレート。
ステップ 26	action { snmp syslog } 例 : <pre>Router(config-pmap-c-react)# action syslog</pre>	しきい値を超えた場合の報告方法を指定します。
ステップ 27	alarmseverity { alert critical emergency error info } 例 : <pre>Router(config-pmap-c-react)# alarm severity critical</pre>	報告されるアラームのレベルを指定します。デフォルト設定は、 info です。
ステップ 28	alarmtype { discrete grouped { countnumber percentnumber } 例 : <pre>Router(config-pmap-c-react)# alarm severity critical</pre>	報告が必要なアラームと見なされるレベルのタイプを指定します。デフォルト設定は、 discrete です。
ステップ 29	thresholdvalue { gnumber gtnumber lnumber ltnumber rangerng-starttrng-end } 例 : <pre>Router(config-pmap-c-react)# threshold value ge</pre>	報告が必要なアラームと見なされるしきい値のタイプを指定します。

	コマンドまたはアクション	目的
ステップ 30	description <i>description</i> 例 : <pre>Router(config-cmap-c-react)# description rtp-jitter-average above 40</pre>	(任意) 反応の説明を作成します。
ステップ 31	end 例 : <pre>Router(config-pmap-c-react)# 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 モードに戻ります。

トラブルシューティングのヒント

フローポリシーの設定とステータスをチェックするには、**show policy-map type performance-monitor** コマンドを使用します。

既存のフロー ポリシーを使用して Cisco Performance Monitor ポリシーをインターフェイスに適用する方法

Cisco Performance Monitor ポリシーをアクティブにする前に、そのポリシーを 1 つ以上のインターフェイスに適用する必要があります。Cisco Performance Monitor をアクティブにするには、次の必須作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***type**number*
4. **service-policy***type***performance-monitor** {**input** | **output**} *policy-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	enable 例 : <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <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	interfacetype <i>number</i> 例 : <pre>Router(config)# interface ethernet 0/0</pre>	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	service-policy <i>type</i> performance-monitor { input output } <i>policy-name</i> 例 : 例 : <pre>Router(config-if)# service-policy type performance-monitor input mypolicy-map-4</pre> 例 :	インターフェイスまたは仮想回線（VC）のサービス ポリシーとして使用されるポリシー マップを入力インターフェイスまたは VC（あるいは出力のインターフェイスまたは VC）に付加します。 <ul style="list-style-type: none"> input : 指定したポリシーマップを入力インターフェイスまたは入力 VC に付加します。 output : 指定したポリシーマップを出力インターフェイスまたは出力 VC に付加します。 policy-name : 対応付けるサービス ポリシー マップ（policy-map コマンドで作成）の名前。名前には最大 40 文字までの英数字を指定できます。
ステップ 5	end 例 : <pre>Router(config-if)# 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 モードに戻ります。

トラブルシューティングのヒント

サービス ポリシーの設定とステータスをチェックするには、次のコマンドを使用します。

- **showperformancemonitorhistory**

- `showperformancemonitorstatus`
- `showpolicy-mapypreperformance-monitorinterface`

既存のフローポリシーを使用せずに Cisco Performance Monitor ポリシーをインターフェイスに適用する方法

Cisco Performance Monitor ポリシーをアクティブにする前に、そのポリシーを 1 つ以上のインターフェイスに適用する必要があります。Cisco Performance Monitor をアクティブにするには、次の必須作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***type**number*
4. **service-policy***type***performance-monitor***inline* { **input** | **output** }
5. **match** { *access-group* { *access-group* | **name** *access-group-name* } | **any** | **class-map** *class-map-name* | **cos** *cos-value* | **destination-address** *mac address* | **discard-class** *class-number* | **dscp** *dscp-value* | **flow** { **direction** | **sampler** } | **fr-de** | **fr-dlci** *dlci-number* | **input-interface** *interface-name* | **ip** { **rtp** *starting-port-number* *port-range* | **precedence** | **dscp** } | **mpls** **experimental** *topmost-number* | **notmatch-criterion** | **packetlength** { **max** *maximum-length-value* [**min** *minimum-length-value*] | **min** *minimum-length-value* [**max** *maximum-length-value*] } | **precedence** { *precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4* } | **protocol** *protocol-name* | **qos-group** *qos-group-value* | **source-address** *macaddress-destination* | **vlan** { *vlan-id* | *vlan-range* | *vlan-combination* } }
6. **flowmonitor** { *monitor-name* | **inline** }
7. **record** { *record-name* | **default-rtp** | **default-tcp** }
8. **exporter** *exporter-name*
9. **exit**
10. **monitor metric** *ip-cbr*
11. **rate** *layer3* { *byte-rate* { **bps** | **kbps** | **mbps** | **gbps** } | **packet** }
12. **exit**
13. **monitor metric** *rtp*
14. **clock-rate** { *type-number* | *type-name* } *rate*
15. **max-dropout** *number*
16. **max-reorder** *number*
17. **min-sequential** *number*
18. **ssrc** *maximum-number*
19. **exit**
20. **monitor parameters**
21. **flows** *number*
22. **interval** *duration-number*
23. **history** *number*
24. **timeout** *number*
25. **exit**
26. **react** *ID* { **media-stop** | **mrvt** | **rtp-jitter-average** | **transport-packets-lost-rate** }
27. **action** { **snmp** | **syslog** }
28. **alarm** *severity* { **alert** | **critical** | **emergency** | **error** | **info** }
29. **alarm** *type* { **discrete** | **grouped** { *count-number* | *percent-number* } }
30. **threshold** *value* { *g-number* | *gt-number* | *l-number* | *lt-number* | *range* *rng-start* *rng-end* }
31. **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 : <pre>Router> enable</pre>	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 : <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	interface <i>type</i> <i>number</i> 例 : <pre>Router(config)# interface ethernet 0/0</pre>	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	service-policy <i>type</i> performance-monitor <i>inline</i> {input output} 例 : 例 : <pre>Router(config-if)# service-policy type performance-monitor inline input</pre>	インターフェイスまたは仮想回線 (VC) のサービス ポリシーとして使用されるポリシー マップを入力 of インターフェイスまたは VC（あるいは出力 of インターフェイスまたは VC）に付加します。 • input : 指定したポリシー マップを入力インターフェイスまたは入力 VC に付加します。 • output : 指定したポリシー マップを出力インターフェイスまたは出力 VC に付加します。
ステップ 5	match {access-group <i>{access-group name</i> <i>access-group-name</i> } any class-map <i>class-map-name</i> cos <i>cos-value</i> destination-address <i>mac address</i> discard-class <i>class-number</i> dscp <i>dscp-value</i> flow {direction sampler} fr-de <i>fr-dlci</i> <i>dlci-number</i> input-interface <i>interface-name</i> ip {rtp <i>starting-port-number</i> <i>port-range</i> precedence dscp mpls <i>experimental</i> <i>topmost</i> <i>number</i> notmatch-criterion packetlength {max <i>maximum-length-value</i> [min <i>minimum-length-value</i> min <i>minimum-length-value</i> [max <i>maximum-length-value</i>]} precedence {precedence-criteria1 precedence-criteria2 precedence-criteria3 precedence-criteria4} protocol <i>protocol-name</i> qos-group <i>qos-group-value</i> 	分類基準を指定します。 詳細および例については、『Cisco Media Monitoring Command Reference』を参照してください。

既存のフローポリシーを使用せずに Cisco Performance Monitor ポリシーをインターフェイスに適用する方法

	コマンドまたはアクション	目的
	source-address <i>macaddress-destination</i> vlan { <i>vlan-id</i> <i>vlan-range</i> <i>vlan-combination</i> } 例 : Router(config-if-spolicy-inline)# match any	
ステップ 6	flowmonitor { <i>monitor-name</i> inline } 例 : Router(config-if-spolicy-inline)# flow monitor inline	フロー ポリシーと関連付ける既存のフロー モニタを指定します。既存のフロー モニタを使用しない場合は、 inline オプションを使用して新しいフロー モニタを設定できます。 必要な場合は、 inline オプションを使用してフロー レコードおよびフロー エクスポートを指定することもできます。
ステップ 7	record { <i>record-name</i> default-rtp default-tcp } 例 : Router(config-spolicy-inline-flowmon)# record default-tcp	(任意) 既存のフロー モニタを使用せず、代わりに inline オプションを使用する場合は、このコマンドを使用してフロー レコードを設定します。
ステップ 8	exporter <i>exporter-name</i> 例 : Router(config-spolicy-inline-flowmon)# exporter exporter-4	(任意) 既存のフロー モニタを使用せず、代わりに inline オプションを使用する場合は、このコマンドを使用してフロー エクスポートを設定します。
ステップ 9	exit 例 : Router(config-spolicy-inline-flowmon)# exit	サービス ポリシー インライン コンフィギュレーション モードに戻ります。
ステップ 10	monitor metric ip-cbr 例 : Router(config-if-spolicy-inline)# monitor metric ip-cbr	IP-CBR モニタ メトリック コンフィギュレーション モードを開始します。
ステップ 11	ratelayer3 { <i>byte-rate</i> { bps kbps mbps gbps } packet } 例 : Router(config-spolicy-inline-mipcbr)# rate layer3 248 mbps	メトリック モニタリング レートを指定します。 <ul style="list-style-type: none"> • byte-rate : データ レート (単位 : Bps、kBps、mBps、または gBps)。指定できる範囲は 1 ～ 65535 です。 • packet : パケット レート (単位 : pps)。

	コマンドまたはアクション	目的
ステップ 12	exit 例 : <pre>Router(config-spolicy-inline-mipcbr)# exit</pre>	サービス ポリシー インライン コンフィギュレーション モードに戻ります。
ステップ 13	monitormetricrtp 例 : <pre>Router(config-if-spolicy-inline)# monitor metric rtp</pre>	RTP モニタ メトリック コンフィギュレーション モードを開始します。
ステップ 14	clock-rate { <i>type-number</i> <i>type-name</i> } <i>rate</i> 例 : <pre>Router(config-spolicy-inline-mrtp)# clock-rate 8 9600</pre>	RTP ビデオ モニタリング メトリックのサンプリングに使用するクロック レートを指定します。 クロック タイプの番号と名前の詳細については、『 <i>Cisco Media Monitoring Command Reference</i> 』を参照してください。 <i>rate</i> の範囲は 1 ～ 192 kHz です。
ステップ 15	max-dropoutnumber 例 : <pre>Router(config-spolicy-inline-mrtp)# max-dropout 2</pre>	RTP ビデオ モニタリング メトリックのサンプリング時に許可されるドロップアウトの最大数を指定します。
ステップ 16	max-reordernumber 例 : <pre>Router(config-spolicy-inline-mrtp)# max-reorder 4</pre>	RTP ビデオ モニタリング メトリックのサンプリング時に許可される順序変更の最大数を指定します。
ステップ 17	min-sequentialnumber 例 : <pre>Router(config-spolicy-inline-mrtp)# min-sequential 2</pre>	ストリームを RTP フローとして識別するために必要な連続パケットの最小数を指定します。
ステップ 18	ssrcmaximumnumber 例 : <pre>Router(config-spolicy-inline-mrtp)# ssrc maximum 20</pre>	同じフロー内でモニタできる SSRC の最大数を指定します。フローは、プロトコル、送信元と宛先のアドレス、および送信元と宛先のポートによって定義されます。

既存のフローポリシーを使用せずに Cisco Performance Monitor ポリシーをインターフェイスに適用する方法

	コマンドまたはアクション	目的
ステップ 19	exit 例 : Router(config-spolicy-inline-mrtp) # exit	サービス ポリシー インライン コンフィギュレーション モードに戻ります。
ステップ 20	monitorparameters 例 : Router(config-if-spolicy-inline) # monitor parameters	モニタ パラメータ コンフィギュレーション モードを開始します。
ステップ 21	flowsnumber 例 : Router(config-spolicy-inline-mparam) # flows 40	各モニタ キャッシュのフローの最大数を指定します。
ステップ 22	intervaldurationnumber 例 : Router(config-spolicy-inline-mparam) # interval duration 40	モニタリングメトリックを収集するためのインターバルの長さ（秒）を指定します。
ステップ 23	historynumber 例 : Router(config-spolicy-inline-mparam) # history 4	収集されたビデオ モニタリング メトリックについて表示する履歴インターバルの数を指定します。
ステップ 24	timeoutnumber 例 : Router(config-spolicy-inline-mparam) # timeout 20	停止したフローがデータベースから削除されるまでのインターバルの数を指定します。
ステップ 25	exit 例 : Router(config-spolicy-inline-mparam) # exit	サービス ポリシー インライン 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 26	react <i>ID</i> { media-stop mrvt rtp-jitter-average transport-packets-lost-rate } 例 : <pre>Router(config-if-spolicy-inline)# react 6 rtp-jitter-average</pre>	次のメトリックのしきい値を超えた場合の反応を指定できるモードを開始します。 <ul style="list-style-type: none"> • ID : 反応設定の ID。有効値の範囲は 1 ～ 65535 です。 • media-stop : フローのトラフィックが検出されません。 • mrvt : 実際のレートと予想レートの差を予想レートで割ることによって算出されるレート。 • rtp-jitter-average : 平均ジッター。 • transport-packets-lost-rate : 損失パケット数を予想パケット数で割ることによって算出されるレート。
ステップ 27	action { snmp syslog } 例 : <pre>Router(config-spolicy-inline-react)# action syslog</pre>	しきい値を超えた場合の報告方法を指定します。
ステップ 28	alarmseverity { alert critical emergency error info } 例 : <pre>Router(config-spolicy-inline-react)# alarm severity critical</pre>	報告されるアラームのレベルを指定します。
ステップ 29	alarmtype { discrete grouped { countnumber percentnumber }} 例 : <pre>Router(config-pspolicy-inline-react)# alarm severity critical</pre>	報告が必要なアラームと見なされるレベルのタイプを指定します。
ステップ 30	thresholdvalue { gnumber gtnumber lnumber ltnumber rangerng-starttrng-end } 例 : <pre>Router(config-spolicy-inline-react)# threshold value ge</pre>	報告が必要なアラームと見なされるしきい値のタイプを指定します。

	コマンドまたはアクション	目的
ステップ 31	end 例 : Router(config-spolicy-inline-react)# 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。

次の作業

サービス ポリシーの設定とステータスをチェックするには、**showperformancemonitorstatus** コマンドおよび **showperformancemonitorhistory** コマンドを使用します。

Cisco Performance Monitor のデータ収集の確認

Cisco Performance Monitor がデータを収集していることを確認するには、次のオプション作業を実行します。



(注)

フローが相互に関連付けられるので、同じポリシーが同じ入力インターフェイスと出力インターフェイスに適用されている場合に **show** コマンドを実行すると、その入力インターフェイスと出力インターフェイスについて単一のフローが表示され、フローのインターフェイス名と方向は表示されません。

データが収集されていない場合は、このセクションの残りの作業を完了させます。

はじめる前に

フロー モニタ キャッシュ内のフローを表示するには、オリジナルのフロー レコードで定義された基準に適合するトラフィックを受信するインターフェイスに、入力フロー モニタを適用する必要があります。

この場合、**filter = {ip {source-addrsource-prefix | any} {dst-addrdst-prefix | any} | {tcp | udp} {source-addrsource-prefix | any} {[eq|lt|gt|number|rangemin|max] ssrc {ssrc-number | any} | {dst-addrdst-prefix | any} eq|lt|gt|number|rangemin|max] ssrc {ssrc-number | any}}**

手順の概要

1. **enable**
2. **showpolicy-maptypeperformance-monitor[interfaceinterface-name][classclass-name][input|output]**
3. **showperformancemonitorstatus[interfaceinterfacename[filter] | policypolicy-map-nameclassclass-map-name[filter]] | filter**
4. **showperformancemonitorhistory[interval{all|number[startnumber]} | interfaceinterfacename[filter] | policypolicy-map-nameclassclass-map-name[filter]] | filter]**

手順の詳細

ステップ 1 **enable**

enable コマンドを使用して、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）。

例：

```
Device> enable
Device#
```

ステップ 2 **show policy-map type performance-monitor [interface interface-name] [class class-name] [input|output]**

このコマンドによって表示されるフィールドの説明については、『Cisco Media Monitoring Command Reference』を参照してください。

次に、あるフロー ポリシーの出力例を示します。

例：

```
Policy Map type performance-monitor PM-POLICY-4
Class PM-CLASS-4
  flow monitor PM-MONITOR-4
  record PM-RECORD-4
  exporter PM-EXPORTER-4
  monitor parameters
    interval duration 30
    timeout 10
    history 10
    flows 8000
  monitor metric rtp
    min-sequential 5
    max-dropout 5
    max-reorder 5
    clock-rate default 90000
    ssrc maximum 5
```

表 4： *policy-map type performance-monitor* のフィールドの説明

フィールド	説明
Policy Map type performance-monitor	Cisco Performance Monitor のフロー ポリシーの名前。
flow monitor	Cisco Performance Monitor のフロー モニタの名前。
record	Cisco Performance Monitor のフロー レコードの名前。
exporter	Cisco Performance Monitor のフロー エクスポートの名前。
monitor parameter	フロー ポリシーのパラメータ。
interval duration	ポリシーで設定されている収集間隔の時間。

フィールド	説明
timeout	ポリシーで設定されているデータ収集時の応答待機時間。
history	ポリシーで設定されている収集履歴の保持数。
flows	ポリシーで設定されているフローの収集数。
monitor metric rtp	フロー ポリシーの RTP メトリック。
min-sequential	RTP フローの分類に使用される連続パケットについて設定されている最小数。
max-dropout	現在のパケットよりもシーケンス番号が小さいものとして無視されるパケットについて設定されている最大数。
max-reorder	現在のパケットよりもシーケンス番号が大きいものとして無視されるパケットについて設定されている最大数。
clock-rate default	パケット到着遅延の計算に使用される RTP パケット タイムスタンプ クロック用に設定されているクロック レート。
ssrc maximum	同じフロー内でモニタできる SSRC について設定されている最大数。フローは、プロトコル、送信元と宛先のアドレス、および送信元と宛先のポートによって定義されます。範囲は 1 ～ 50 です。

ステップ 3 **showperformancemonitorstatus**[interfaceinterfacename[filter]] | **polycypolicy-map-nameclassclass-map-name[filter]]** | filter]

この場合、**filter** = {**ip** {**source-addrsource-prefix** | **any**} {**dst-addrdst-prefix** | **any**} | {**tcp** | **udp**} {**source-addrsource-prefix** | **any**} {**[eq|lt|gt]number|rangeminmax** | **ssrc** {**ssrc-number** | **any**} | {**dst-addrdst-prefix** | **any**} **eq|lt|gt]number|rangeminmax** | **ssrc** {**ssrc-number** | **any**}}

このコマンドは、指定された数の最新のインターバルの累積統計情報を表示します。インターバルの数は、**history** コマンドを使用して設定します。このコマンドのデフォルト設定は、最新 10 の収集インターバルです。収集インターバルの長さは、**intervalduration** コマンドを使用して指定します。

他のインターバルの統計情報を表示するには、次のステップの説明に従って、**performancemonitorhistory** コマンドを使用します。これらのコマンドの詳細については、『Cisco Media Monitoring Command Reference』を参照してください。

ステップ 4 **showperformancemonitorhistory**[interval{all|number[startnumber]} | interfaceinterfacename[filter] | policypolicy-map-nameclassclass-map-name[filter]} | filter]

この場合、**filter** = {**ip** {**source-addr**source-prefix | **any**} {**dst-addr**dst-prefix | **any**} | {**tcp** | **udp**} {**source-addr**source-prefix | **any**} {**eq**|**lt**|**gt**number|**range**minmax| **ssrc** {**ssrc-number** | **any**} | {**dst-addr**dst-prefix | **any**} **eq**|**lt**|**gt**number|**range**minmax| **ssrc** {**ssrc-number** | **any**}}

このコマンドは、最新のものを含めて、任意またはすべてのインターバルで Cisco Performance Monitor によって収集された統計情報を表示します。収集インターバルの長さは、**intervalduration** コマンドを使用して指定します。

このコマンドの詳細については、『Cisco Media Monitoring Command Reference』を参照してください。

次に、**showperformancemonitorhistory** コマンドの出力例を示します。

- (注) 同じポリシーが同じ入力インターフェイスと出力インターフェイスに適用されている場合、その入力インターフェイスと出力インターフェイスについて単一のフローが表示され、フローのインターフェイス名と方向は表示されません。

例：

```
Codes: * - field is not configurable under flow record
       NA - field is not applicable for configured parameters
Match: ipv4 source address = 21.21.21.1, ipv4 destination address = 1.1.1.1,
transport source-port = 10240, transport destination-port = 80, ip protocol = 6,
Policy: RTP_POL, Class: RTP_CLASS
```

```
start time                               14:57:34
=====
*history bucket number                   : 1
routing forwarding-status                 : Unknown
transport packets expected counter       : NA
transport packets lost counter           : NA
transport round-trip-time (msec)         : 4
transport round-trip-time sum (msec)     : 8
transport round-trip-time samples        : 2
transport event packet-loss counter      : 0
interface input                          : Null
interface output                         : Null
counter bytes                            : 8490
counter packets                          : 180
counter bytes rate                       : 94
counter client bytes                     : 80
counter server bytes                     : 200
counter client packets                   : 6
counter server packets                   : 6
transport tcp window-size minimum        : 1000
transport tcp window-size maximum        : 2000
transport tcp window-size average        : 1500
transport tcp maximum-segment-size       : 0
application media bytes counter          : 1270
application media bytes rate             : 14
application media packets counter        : 180
application media event                  : Stop
monitor event                            : false
```

```
[data set,id=257] Global session ID|Multi-party session ID|
[data] 11                               |22
```

表 5 : *show performance monitor status and show performance-monitor history* のフィールドの説明

フィールド	説明
history bucket number	収集された履歴データのバケットの数。

フィールド	説明
routing forwarding-status reason	

フィールド	説明
	<p>2 桁の最上位ビットがステータスを表し、残りの 6 ビットが理由コードを表す 8 ビットを使用して、転送状態が検出されます。</p> <p>ステータスは、Unknown (00)、Forwarded (10)、Dropped (10)、Consumed (11) のいずれかです。</p> <p>次に、各ステータス カテゴリの転送ステータス値を示します。</p> <p>Unknown</p> <ul style="list-style-type: none"> • 0 <p>Forwarded</p> <ul style="list-style-type: none"> • Unknown 64 • Forwarded Fragmented 65 • Forwarded not Fragmented 66 <p>Dropped</p> <ul style="list-style-type: none"> • Unknown 128 • Drop ACL Deny 129 • Drop ACL drop 130 • Drop Unroutable 131 • Drop Adjacency 132 • Drop Fragmentation & DF set 133 • Drop Bad header checksum 134 • Drop Bad total Length 135 • Drop Bad Header Length 136 • Drop bad TTL 137 • Drop Policer 138 • Drop WRED 139 • Drop RPF 140 • Drop For us 141 • Drop Bad output interface 142 • Drop Hardware 143 <p>Consumed</p>

フィールド	説明
	<ul style="list-style-type: none"> • Unknown 192 • Terminate Punt Adjacency 193 • Terminate Incomplete Adjacency 194 • Terminate For us 195
transport packets expected counter	予想パケット数。
transport packets lost counter	パケット損失数。
transport round-trip-time (msec)	ラウンド トリップを完了させるためにかかった時間（ミリ秒）。
transport round-trip-time sum (msec)	すべてのサンプリングのラウンド トリップを完了させるためにかかった合計時間（ミリ秒）。
transport round-trip-time samples	ラウンド トリップ時間の計算に使用されたサンプルの合計数。
transport event packet-loss counter	損失イベントの数（損失パケットの連続セットの数）。
interface input	着信インターフェイス インデックス。
interface output	発信インターフェイス インデックス。
counter bytes	すべてのフローで収集されたバイトの合計数。
counter packets	すべてのフローで送信された IP パケットの合計数。
counter bytes rate	すべてのフローのモニタリング インターバルでモニタリング システムによって 1 分間に処理されたパケットまたはビット（設定によって異なる）の平均数。
counter client bytes	クライアントの送信バイト数。
counter server bytes	サーバの送信バイト数。
counter client packets	クライアントの送信パケット数。
counter servers packets	サーバの送信パケット数。

フィールド	説明
transport tcp window-size-maximum	TCP ウィンドウの最大サイズ。
transport tcp window-size-minimum	TCP ウィンドウの最小サイズ。
transport tcp window-size-average	TCP ウィンドウの平均サイズ。
transport tcp maximum-segment-size	最大 TCP セグメント サイズ。
application media bytes counter	特定のメディア ストリームでメディア アプリケーションから受信された IP バイトの数。
application media bytes rate	モニタリングインターバルにおけるすべてのフローの平均メディア ビット レート (bps)。
application media packets counter	特定のメディア ストリームでメディア アプリケーションから受信された IP パケットの数。
application media event	ビット1は使用されません。ビット2は、メディア アプリケーション パケットが検出されなかったこと、つまり、メディア停止イベントが発生したことを示します。
monitor event	ビット1は、フローの反応ステートメントで指定されているいずれかのしきい値をモニタリング インターバルで少なくとも1回超えることがあったことを示します。ビット2は、測定の実験性の喪失が発生したことを示します。

Performance Monitor のキャッシュとクライアントの表示

Cisco Performance Monitor のキャッシュとクライアントを表示するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **showperformancemonitorcache[policypolicy-map-nameclassclass-map-name][interfaceinterfacename]**
3. **showperformancemonitorclientsdetailall**

手順の詳細

ステップ 1 enable

enable コマンドを使用して、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）。

例：

```
Device> enable
Device#
```

ステップ 2 showperformancemonitorcache[policypolicy-map-nameclassclass-map-name][interfaceinterfacename]

例：

```
MMON Metering Layer Stats:
  static pkt cnt: 3049
  static cce sb cnt: 57
  dynamic pkt cnt: 0
  Cache type: Permanent
  Cache size: 2000
  Current entries: 8
  High Watermark: 9
  Flows added: 9
  Updates sent ( 1800 secs) 0

IPV4 SRC ADDR  IPV4 DST ADDR  IP PROT  TRNS SRC PORT  TRNS DST PORT
ipv4 ttl ipv4 ttl min ipv4 ttl max  ipv4 dscp bytes long perm pktslong perm  user space vm
=====
10.1.1.1      10.1.2.3      17      4000      1967
0      0      0 0x00      80
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1      10.1.2.3      17      6000      1967
0      0      0 0x00      80
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1      10.1.2.3      17      4000      2000
0      0      0 0x00      44
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1      10.1.2.3      6      6000      3000
0      0      0 0x00      84
2 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
0x00000000
```

```

10.1.1.1      10.1.2.3      17      1967      6001
0              0              0 0x00              36
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1      10.1.2.3      17      1967      4001
0              0              0 0x00              36
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1      10.1.2.3      6      3001      6001
0              0              0 0x00              124
3 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1      10.1.2.3      17      2001      4001
0              0              0 0x00              44
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000

```

ステップ 3 showperformancemonitorclientsdetailall

例 :

```

Client name for ID 1 : Mediatrace-131419052
Type: Mediatrace
Age: 443 seconds
Monitor Object: MMON_DYN -class-map-69
Flow spec: (dvmc-acl#47) 10.10.130.2 1000 10.10.132.2 2000 17
monitor parameters
  interval duration 60
  timeout 2
  history 1
  flows 100
monitor metric rtp
  min-sequential 10
  max-dropout 5
  max-reorder 5
  clock-rate 112 90000
  clock-rate default 90000
  ssrc maximum 20
monitor metric ip-cbr
  rate layer3 packet 20
Flow record: dvmc_fnf_fdef_47
Key fields:
  ipv4 source address
  ipv4 destination address
  transport source-port
  transport destination-port
  ip protocol
Non-key fields:
  monitor event

```

```

application media event
routing forwarding-status
ip dscp
ip ttl
counter bytes rate
application media bytes rate
transport rtp jitter mean
transport packets lost counter
transport packets expected counter
transport event packet-loss counter
transport packets lost rate
timestamp interval
counter packets dropped
counter bytes
counter packets
application media bytes counter
application media packets counter
Monitor point: MMON_DYN_policy-map-70 GigabitEthernet0/3 output
Classification Statistic:
  matched packet: 545790
  matched byte: 64403220

```

Cisco Performance Monitor クラスのクロック レートの表示

1 つ以上のクラスのクロック レートを表示するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **showperformancemonitorclockrate[policypolicy-map-nameclassclass-map-name]**

手順の詳細

ステップ 1 enable

enable コマンドを使用して、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）。

例：

```

Device> enable
Device#

```

ステップ 2 showperformancemonitorclockrate[policypolicy-map-nameclassclass-map-name]

クラス名を指定しない場合は、すべてのチャネルの情報が表示されます。

例：

```

Device# show performance monitor clock rate policy all-apps class telepresence-CS4
Load for five secs: 6%/2%; one minute: 5%; five minutes: 5% Time source is NTP, 17:41:35.508 EST
Wed Feb 16 2011
RTP clock rate for Policy: all-apps, Class: telepresence-CS4
  Payload type      Clock rate(Hz)

```

```

pcmu      (0 )      8000
gsm       (3 )      8000
g723      (4 )      8000
dvi4      (5 )      8000
dvi4-2    (6 )     16000
lpc       (7 )      8000
pcma      (8 )      8000
g722      (9 )      8000
l16-2     (10 )     44100
l16       (11 )     44100
qcelp     (12 )      8000
cn        (13 )      8000
mpa       (14 )     90000
g728      (15 )      8000
dvi4-3    (16 )     11025
dvi4-4    (17 )     22050
g729      (18 )      8000
celb      (25 )     90000
jpeg      (26 )     90000
nv        (28 )     90000
h261      (31 )     90000
mpv       (32 )     90000
mp2t      (33 )     90000
h263      (34 )     90000
          (96 )     48000
          (112)     90000
default   90000

```

フロー モニタの現在のステータスの表示

フロー モニタの現在のステータスを表示するには、次のオプション作業を実行します。

はじめる前に

フロー モニタ キャッシュ内のフローを表示するには、オリジナルのフロー レコードで定義された基準に適合するトラフィックを受信するインターフェイスに、入力フロー モニタを適用する必要があります。

手順の概要

1. **enable**
2. **showflowmonitortypeperformance-monitor**

手順の詳細

ステップ 1 **enable**

enable コマンドを使用して、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）。

例：

```
Device> enable
Device#
```

ステップ 2 showflowmonitortypeperformance-monitor

showflowmonitortypeperformance-monitor コマンドでは、指定したフローモニタの現在のステータスが表示されます。

例：

```
Device# show flow monitor type performance-monitor
Flow Monitor type performance-monitor monitor-4:
  Description:          User defined
  Flow Record:          record-4
  Flow Exporter:        exporter-4
  No. of Inactive Users: 0
  No. of Active Users:  0
```

フロー モニタの設定の確認

入力したコンフィギュレーション コマンドを確認するには、次のオプション作業を実行します。

はじめる前に

フロー モニタ キャッシュ内のフローを表示するには、オリジナルのフロー レコードで定義された基準に適合するトラフィックを受信するインターフェイスに、入力フロー モニタを適用する必要があります。

手順の概要

1. **enable**
2. **showrunning-configflowmonitor**

手順の詳細

ステップ 1 enable

enable コマンドを使用して、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）。

例：

```
Device> enable
Device#
```

ステップ 2 showrunning-configflowmonitor

■ インターフェイスで Cisco IOS Flexible NetFlow および Cisco Performance Monitor が有効になっていることの確認

showrunning-configflowmonitor コマンドを使用して、指定したフロー モニタのコンフィギュレーション コマンドを表示します。

例：

```
Device# show running-config flow monitor
Current configuration:
!
flow monitor FLOW-MONITOR-1
description Used for basic IPv4 traffic analysis
record netflow ipv4 original-input
!
!
flow monitor FLOW-MONITOR-2
description Used for basic IPv6 traffic analysis
record netflow ipv6 original-input
!
```

インターフェイスで Cisco IOS Flexible NetFlow および Cisco Performance Monitor が有効になっていることの確認

インターフェイスで Flexible NetFlow および Cisco Performance Monitor が有効になっていることを確認するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **showflowinterfacetypenumber**

手順の詳細

ステップ 1 **enable**

enable コマンドを使用して、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）。

例：

```
Router> enable
Router#
```

ステップ 2 **showflowinterfacetypenumber**

showflowinterface コマンドを使用して、インターフェイスで Flexible NetFlow および Cisco Performance Monitor が有効になっていることを確認します。

例：

```
Router# show flow interface ethernet 0/0
Interface Ethernet0/0
  FNF: monitor:      FLOW-MONITOR-1
        direction:   Input
        traffic(ip):  on
  FNF: monitor:      FLOW-MONITOR-2
        direction:   Input
        traffic(ipv6): on
```

フロー モニタ キャッシュの表示

フロー モニタ キャッシュのデータを表示するには、次のオプション作業を実行します。

はじめる前に

フロー モニタ キャッシュ内のフロー データを表示するには、NetFlow original レコードで定義された基準に適合するトラフィックを受信するインターフェイスに、入力フロー モニタを適用する必要があります。

手順の概要

1. **enable**
2. **showflowmonitorname *monitor-name* cache format record**

手順の詳細

ステップ 1 **enable**

enable コマンドを使用して、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）。

例：

```
Device> enable
Device#
```

ステップ 2 **showflowmonitorname *monitor-name* cache format record**

showflowmonitorname *monitor-name* cache format record コマンド文字列は、フロー モニタのキャッシュのステータス、統計情報、およびフロー データを表示します。

例：

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record
Cache type:      Normal
Cache size:      4096
```

```

Current entries:                        8
High Watermark:                        8
Flows added:                           24
Flows aged:                            16
  - Active timeout ( 1800 secs)        0
  - Inactive timeout ( 15 secs)        16
  - Event aged                          0
  - Watermark aged                      0
  - Emergency aged                      0
IPV4 SOURCE ADDRESS:                   10.251.10.1
IPV4 DESTINATION ADDRESS:               172.16.10.2
TRNS SOURCE PORT:                       0
TRNS DESTINATION PORT:                  2048
INTERFACE INPUT:                        Et0/0
FLOW SAMPLER ID:                        0
IP TOS:                                0x00
IP PROTOCOL:                            1
ip source as:                           0
ip destination as:                       0
ipv4 next hop address:                  172.16.7.2
ipv4 source mask:                       /0
ipv4 destination mask:                  /24
tcp flags:                              0x00
interface output:                       Et1/0
counter bytes:                           733500
counter packets:                         489
timestamp first:                         720892
timestamp last:                         975032
.
.
.
IPV4 SOURCE ADDRESS:                   172.16.6.1
IPV4 DESTINATION ADDRESS:               224.0.0.9
TRNS SOURCE PORT:                       520
TRNS DESTINATION PORT:                  520
INTERFACE INPUT:                        Et0/0
FLOW SAMPLER ID:                        0
IP TOS:                                0xC0
IP PROTOCOL:                            17
ip source as:                           0
ip destination as:                       0
ipv4 next hop address:                  0.0.0.0
ipv4 source mask:                       /24
ipv4 destination mask:                  /0
tcp flags:                              0x00
interface output:                       Null
counter bytes:                           52
counter packets:                         1
timestamp first:                         973804
timestamp last:                         973804
Device# show flow monitor name FLOW-MONITOR-2 cache format record
Cache type:                             Normal
Cache size:                             4096
Current entries:                         6
High Watermark:                         8
Flows added:                             1048
Flows aged:                              1042
  - Active timeout ( 1800 secs)          11
  - Inactive timeout ( 15 secs)          1031
  - Event aged                           0
  - Watermark aged                       0
  - Emergency aged                       0
IPV6 FLOW LABEL:                         0
IPV6 EXTENSION MAP:                      0x00000040
IPV6 SOURCE ADDRESS:                     2001:DB8:1:ABCD::1
IPV6 DESTINATION ADDRESS:                 2001:DB8:4:ABCD::2
TRNS SOURCE PORT:                         3000
TRNS DESTINATION PORT:                    55
INTERFACE INPUT:                          Et0/0
FLOW DIRECTION:                          Input
FLOW SAMPLER ID:                          0

```



```

IP PROTOCOL:          17
IP TOS:                0x00
ip source as:          0
ip destination as:     0
ipv6 next hop address: ::
ipv6 source mask:      /48
ipv6 destination mask: /0
tcp flags:             0x00
interface output:      Null
counter bytes:         521192
counter packets:       9307
timestamp first:       9899684
timestamp last:        11660744
.
.
.
IPV6 FLOW LABEL:       0
IPV6 EXTENSION MAP:    0x00000000
IPV6 SOURCE ADDRESS:   FE80::A8AA:BBFF:FEBB:CC03
IPV6 DESTINATION ADDRESS: FF02::9
TRNS SOURCE PORT:      521
TRNS DESTINATION PORT: 521
INTERFACE INPUT:       Et0/0
FLOW DIRECTION:        Input
FLOW SAMPLER ID:       0
IP PROTOCOL:          17
IP TOS:                0xE0
ip source as:          0
ip destination as:     0
ipv6 next hop address: ::
ipv6 source mask:      /10
ipv6 destination mask: /0
tcp flags:             0x00
interface output:      Null
counter bytes:         92
counter packets:       1
timestamp first:       11653832
timestamp last:        11653832

```

フロー エクスポートの現在のステータスの表示

フロー エクスポートの現在のステータスを表示するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **showflowexporter**[*exporter-name*]

手順の詳細

ステップ 1 enable

enable コマンドを使用して、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）。

例 :

```
Device> enable
Device#
```

ステップ 2 showflowexporter[exporter-name]

showflowexporter コマンドでは、指定したフロー エクスポートの現在のステータスが表示されます。

例 :

```
Device# show flow exporter EXPORTER-1
Flow Exporter EXPORTER-1:
  Description:           Exports to Chicago datacenter
  Transport Configuration:
    Destination IP address: 172.16.10.2
    Source IP address:     172.16.7.1
    Transport Protocol:    UDP
    Destination Port:      65
    Source Port:           56041
    DSCP:                  0x0
    TTL:                   255
```

フロー エクスポートの設定の確認

フロー エクスポートを設定するために入力したコンフィギュレーション コマンドを確認するには、次のオプション作業を実行します。

手順の概要

1. **enable**
2. **showrunning-configflowexporterexporter-name**

手順の詳細

ステップ 1 enable

enable コマンドを使用して、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）。

例 :

```
Device> enable
Device#
```

ステップ 2 showrunning-configflowexporterexporter-name

showrunning-configflowexporter コマンドを使用して、指定したフロー エクスポートのコンフィギュレーション コマンドを表示します。

例 :

```
Device# show running-config flow exporter EXPORTER-1
Building configuration...
!
flow exporter EXPORTER-1
  description Exports to datacenter
  destination 172.16.10.2
  transport udp 65
!
```

デバッグの有効化

Cisco Performance Monitor のデバッグを有効にするには、特権 EXEC モードで、次のオプション作業を実行します。

手順の概要

1. **debugperformancemonitor**{database | dynamic | event | export | flow-monitor | metering | provision | sibling | snmp | tca | timer}

手順の詳細

debugperformancemonitor{database | dynamic | event | export | flow-monitor | metering | provision | sibling | snmp | tca | timer}

debugperformancemonitor コマンドは、次のパフォーマンス モニタ コンポーネントのデバッグを有効にします。

- フロー データベース
- ダイナミック モニタリング
- パフォーマンス イベント
- エクスポート
- フロー モニタ
- 測定層
- プロビジョニング
- 兄弟管理
- SNMP
- TCA
- タイマー

次に、ダイナミック モニタリングを有効にする方法の例を示します。

例：

```
Device# debug performance monitor dynamic
```

Cisco Performance Monitor の設定例

例：損失 RTP パケットおよび RTP ジッターのモニタリング

この例では、**gig1** インターフェイスの損失 RTP パケットの数、RTP ジッターの量、およびその他の基本統計情報をモニタする設定を示します。また、この例では、次のいずれかのイベントがインターフェイスで発生した場合に syslog でエントリが作成されるように Cisco Performance Monitor が設定されています。

- 損失 RTP パケットの割合が 5～9% です。
- 損失 RTP パケットの割合が 10% を超えています。
- メディア停止イベントが発生しました。

```
! Set the filter spec for the flows to monitor.
access-list 101 ip permit host 10.10.2.20 any
! Use the flow record to define the flow keys and metric to collect.
flow record type performance-monitor video-monitor-record
match ipv4 source
match ipv4 destination
match transport source-port
match transport destination-port
match rtp ssrc
collect timestamp
collect counter byte
collect counter packet
collect mse
collect media-error
collect counter rtp interval-jitter
collect counter rtp packet lost
collect counter rtp lost event
! Set the exporting server. The export message format is based on FNFv.9.
flow export video-nms-server
export-protocol netflow-v9
destination cisco-video-management
transport udp 32001
! Set the flow filter in the class-map.
class-map match-all video-class
access-group ipv4 101
! Set the policy map with the type performance-monitor for video monitor.
policy-map type performance-monitor video-monitor
! Set the video monitor actions.
class video-class
! Specify where the metric data is being exported to.
export flow video-nms-server
flow monitor inline
```

```
record video-monitor-record
! Set the monitoring modeling parameters.
monitor parameters
! Set the measurement timeout to 10 secs.
interval duration 10
! Set the timeout to 10 minutes.
timeout 10
! Specify that 30 flow intervals can be kept in performance database.
history 30
priority 7
! Set rtp flow verification criteria.
monitor metric rtp
! Configure a RTP flow criteria: at least 10 packets in sequence.
min-sequential 10
! Ignore packets that are more than 5 packet ahead in terms of seq number. max-dropout
5
! Ignore packets that are more than 5 packets behind in terms of seq number.
max-reorder 5
! Set the clock rate frequency for rtp packet timestamp clock.
clock-rate 89000
! Set the maximum number of ssrc allowed within this class.
ssrc maximum 100
! Set TCA for alarm.
react 100 transport-packets-lost-rate
description critical TCA
! Set the threshold to greater than 10%.
threshold gt 10
! Set the threshold to the average number based on the last five intervals.
threshold type average 5
action syslog
alarm severity critical
react 110 transport-packets-lost-rate
description medium TCA
! Set the threshold to between 5% and 9% of packet lost.
threshold range gt 5 le 9
threshold type average 10
action syslog
alarm type grouped percent 30
react 3000 media-stop
action syslog
alarm severity critical
alarm type grouped percent 30

interface gig1
service-policy type performance-monitor video-mon in
```

次の作業

Medianet 製品ファミリの製品設定の詳細については、このガイドの他の章または『*Cisco Media Monitoring Configuration Guide*』を参照してください。

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
Performance Monitor およびその他の Cisco Medianet 製品の設計、設定、ならびにトラブルシューティングに関する資料（クイックスタートガイドや導入ガイドなど）。	Cisco Medianet ナレッジベース ポータルサイト (http://www.cisco.com/web/solutions/medianet/knowledgebase/index.html) を参照してください。
IP アドレッシング コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『Cisco Media Monitoring Command Reference』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Flexible NetFlow のコンフィギュレーション コマンド	『Cisco IOS Flexible NetFlow Command Reference』
Flexible NetFlow の概要	「Cisco IOS Flexible NetFlow Overview」
Flexible NetFlow の機能ロードマップ	「Cisco IOS Flexible NetFlow Features Roadmap」
Flexible NetFlow データをエクスポートするためのフロー エクスポートの設定	「Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters」
Flexible NetFlow のカスタマイズ	「Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors」
Flexible NetFlow のトラフィック監視によるオーバーヘッド軽減のためのフローサンプリング設定	「Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic」
事前定義済みレコードを使用した Flexible NetFlow の設定	「Configuring Cisco IOS Flexible NetFlow with Predefined Records」
Flexible NetFlow Top N Talkers を使用したネットワーク トラフィックの分析	「Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic」
Flexible NetFlow 用の IPv4 マルチキャスト統計情報サポートの設定	「Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow」

規格

規格	タイトル
なし	—

MIB

MIB	MIB のリンク
<ul style="list-style-type: none"> • CISCO-FLOW-MONITOR-TC-MIB • CISCO-FLOW-MONITOR-MIB • CISCO-RTP-METRICS-MIB • CISCO-IP-CBR-METRICS-MIB 	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
RFC 3954	<p>『Cisco Systems NetFlow Services Export Version 9』</p> <p>http://www.ietf.org/rfc/rfc3954.txt</p>
RFC 3550	<p>『RTP: A Transport Protocol for Real-Time Applications』</p> <p>http://www.ietf.org/rfc/rfc3550.txt</p>

シスコのテクニカル サポート

説明	リンク
<p>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。</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Cisco Performance Monitor の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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。

表 6 : Cisco Performance Monitor の機能情報

機能名	リリース	機能情報
Cisco Performance Monitor 1.0	15.1(3)T 12.2(58)SE 15.1(4)M1 15.0(1)SY Cisco IOS XE Release 3.5S 15.1(1)SG Cisco IOS XE Release 3.3 SG 15.1(2)SY	

機能名	リリース	機能情報
		<p>この機能を使用すると、ネットワーク内のパケットフローをモニタして、ご使用のアプリケーションのパフォーマンスに重大な影響が現れる前に、そのフローに影響を及ぼす可能性がある問題を認識できるようになります。</p> <p>この機能のサポートは、Cisco IOS XE Release 3.5S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ用に追加されました。</p> <p>Cisco IOS XE Release 3.3 SG および Cisco IOS release 15.1(1)SG の場合、特定のタイプのインターフェイスでは入力データまたは出力データのモニタリングに関する制限事項がいくつかあります。詳細については、「制限事項」を参照してください。</p> <p>他のすべてのリリースでは、この機能により、次のコマンドが導入または変更されました。</p> <p>action (ポリシー反応およびポリシー インライン反応)、 alarmseverity (ポリシー反応およびポリシー インライン反応)、 alarmtype (ポリシー反応およびポリシー インライン反応)、 class-map、clock-rate (ポリシー RTP)、 collectapplicationmedia、 clearperformance-monitorcounters、 collectcounter、 collectflowdirection、 collectinterface、collectipv4、 collectipv4destination、 collectipv4source、 collectipv4ttl、 collectmonitorevent、 collectrouting、</p>

機能名	リリース	機能情報
		collecttimestampinterval 、 collecttransporteventpacket-losscounter 、 collecttransportpackets 、 collecttransportrtppjitter 、 debugperformance-monitorcounters 、 debugperformance-monitorcounters 、 description (Performance Monitor) 、 destinationdscp (Flexible NetFlow) 、 export-protocol 、 exporter 、 flowmonitortypeperformance-monitor 、 flowrecordtypeperformance-monitor 、 flows 、 history (モニタリングパラメータ) 、 intervalduration 、 matchaccess-group 、 matchany 、 matchclass-map 、 matchcos 、 matchdestination-addressmac 、 matchdiscard-class 、 matchdscp 、 matchflow 、 matchfr-de 、 matchfr-dlci 、 matchinput-interface 、 matchipdscp 、 matchipprecedence 、 matchiprtp 、 matchipv4 、 matchipv4destination 、 matchipv4source 、 matchmplsexperimentaltopmost 、 matchnot 、 matchpacketlength (クラスマップ) 、 matchprecedence 、 matchprotocol 、 matchqos-group 、 matchsource-addressmac 、 matchtransportdestination-port 、 matchtransportrtppsrc 、 matchtransportsource-port 、 matchvlan 、 max-dropout (ポリシー RTP) 、 max-reorder (ポリシー RTP) 、 min-sequential (ポリシー RTP) 、 monitormetricip-cbr 、

機能名	リリース	機能情報
		monitormetricrtp 、 monitorparameters 、 option (Flexible NetFlow) 、 output-features 、 platformperformance-monitorrate-limit 、 policy-maptypeperformance-monitor 、 ratelayer3 、 react (ポリ シー) 、 record (Performance Monitor) 、 rename (ポリ シー) 、 service-policytypeperformance-monitor 、 showperformancemonitorhistory 、 showperformancemonitorstatus 、 showplatformhardwareadentryinterface 、 showplatformsoftwareccm 、 showplatformsoftwarefeature-managecam 、 showplatformsoftwarefeature-managecam 、 showpolicy-maptypeperformance-monitor 、 snmp-serverhost 、 snmp-serverenabletrapsflowmon 、 snmpmibflowmonalarmhistory 、 source (Flexible NetFlow) 、 ssrcmaximum 、 templatedatatimeout 、 thresholdvalue (ポリシー反応 およびポリシー インライン反 応) 、 timeout (モニタリング パラメータ) 、 transport (Flexible NetFlow) 、 ttl (Flexible NetFlow) 。

機能名	リリース	機能情報
Performance Monitor (フェーズ 2)	15.2(2)T Cisco IOS XE Release 3.5S	

機能名	リリース	機能情報
		<p>この機能を使用すると、IPv6 フィールドをモニタできるようになります。また、以前のリリースではサポートされていない Flexible NetFlow の他のすべての collect コマンドと match コマンドを使用できます。</p> <p>現在では、フローが相互に関連付けられるので、同じポリシーが同じ入力インターフェイスと出力インターフェイスに適用されている場合に show コマンドを実行すると、その入力インターフェイスと出力インターフェイスについて単一のフローが表示されます。</p> <p>この機能のサポートは、Cisco IOS XE Release 3.5S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ用に追加されました。</p> <p>この機能により、次のコマンドが導入または変更されました。</p> <p>collectdatalinkmac、 collectipv4fragmentation、 collectipv4section、 collectipv4total-length、 collectipv6、 collectipv6destination、 collectipv6extensionmap、 collectipv6fragmentation、 collectipv6hop-count、 collectipv6length、 collectipv6section、 collectipv6source、 collectroutingis-multicast、 collectroutingmulticast replication-factor、 collecttimestampsys-uptime、 collecttransport、 collecttransporticmpv4、 collecttransporticmpv6、</p>

機能名	リリース	機能情報
		collecttransporttcp、 collecttransportudp、 matchapplication name、 matchconnection transaction-id、 matchdatalinkdot1q vlan、 matchdatalinkmac、 matchdatalinkvlan、 matchinterface、 matchipv4fragmentation、 matchipv4section、 matchipv4total-length、 matchipv4ttl、 matchipv6、 matchipv6destination、 matchipv6extension map、 matchipv6fragmentation、 matchipv6hop-limit、 matchipv6length、 matchipv6section、 matchipv6source、 matchrouting、 matchroutingis-multicast、 matchroutingmulticastreplication-factor、 matchtransport、 matchtransporticmpipv4、 matchtransporticmpipv6、 matchtransporttcp、 matchtransportudp

機能名	リリース	機能情報
Performance Monitor (フェーズ 3)	15.2(3)T	<p>この機能を使用すると、複数のエクスポートを設定し、メタデータフィールドと新しいTCPメトリックをモニタできます。</p> <p>この機能により、次のコマンドが導入または変更されました。</p> <p>collect application、collect transport tcp bytes out-of-order、collect transport packets out-of-order、collect transport tcp maximum-segment-size、collect transport tcp window-size maximum、collect transport tcp window-size minimum、collect transport tcp window-size average、match application、match transport tcp bytes out-of-order、match transport packets out-of-order、match transport tcp maximum-segment-size、match transport tcp window-size maximum、match transport tcp window-size minimum、match transport tcp window-size average</p>
パフォーマンスモニタリング : IPv6 サポート	Cisco IOS XE Release 3.6S	<p>この機能を使用すると、モニタを IPv6 インターフェイスに接続できます。</p> <p>この機能のサポートは、Cisco IOS XE Release 3.6S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ用に追加されました。</p>

機能名	リリース	機能情報
パフォーマンスモニタリング : 誤った順序でのパケットのトラ ンスポート	Cisco IOS XE Release 3.6S	<p>この機能を使用すると、誤った順序で送信された TCP パケットの合計数をモニタできます。</p> <p>この機能のサポートは、Cisco IOS XE Release 3.6S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ用に追加されました。</p> <p>この機能により、次のコマンドが導入または変更されました。 collect transport tcp bytes out-of-order、collect transport packets out-of-order。</p>
Flexible NetFlow : IPFIX エクス ポート フォーマット	15.2(4)M	<p>IPFIX エクスポートプロトコルを使用したエクスポートパケットの送信を有効化します。</p> <p>NBAR から抽出されたフィールドのエクスポートは、IPFIX 経由でのみサポートされます。</p> <p>次のコマンドが導入されました。export-protocol</p>

