Cisco ASR 9000 シリーズ ルータ へのビデオ モニタリング サービスの実装

ここでは、Cisco IOS XR ソフトウェアを実行する Cisco ASR 9000 シリーズ アグリゲーション サービス ルータで、ビデオ モニタリング サービスを実装する方法について説明します。

ビデオ モニタリング サービスは、ルータ上のフロー単位の統計情報を測定してアプリケーション トラフィックの品質（主にビデオ）をモニタします。この機能では、フローのスケーラブルかつ効率的なインライン モニタリング機能を提供します。

Cisco ASR 9000 シリーズ ルータ　上でのマルチキャスト ルーティング設定機能の履歴

リリース	変更内容
リリース 3.9.0	ビデオ モニタリング機能が導入されました。
リリース 3.9.1	ビデオ モニタリング サービスおよびその他の関連する変更の高帯域幅フローのサポートに関連するシナリオが含まれていました。
リリース 4.0.1	ビデオ フロー モニタリングのトラップおよびクローン機能のサポートが含まれていました。

内容

ビデオ モニタリングの実装の前提条件

ビデオ モニタリングの実装には、次の前提条件が必要です。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

- 高度なビデオ サービスのパッケージをインストールおよびアクティブ化する必要があります。オプション パッケージをインストールする方法の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』を参照してください。
- マルチキャスト ルーティング ソフトウェアのパッケージをインストールおよびアクティブ化し、マルチキャストルーティングをシステムでイネーブルにする必要があります。ビデオ モニタリングはマルチキャスト対応のインターフェイスでサポートされています。マルチキャスト ルーティングの詳細については、「*Implementing Layer 3 Multicast Routing on Cisco ASR 9000 Series Routers*」の章を参照してください。

ビデオ モニタリングの実装に関する情報

このマニュアルで説明するビデオ モニタリング機能を実装するには、次の概念を理解している必要があります。

- 「ビデオ モニタリングの概要」（P.MCC-188）
- 「ビデオ モニタリングでサポートされている主な機能」（P.MCC-189）
- 「ビデオ モニタリングの用語」（P.MCC-192）

ビデオ モニタリングの概要

低品質のビデオ環境は、サービス コストと収益低下の観点から、サービス プロバイダー間の主な不安の原因になっています。ヘルプ デスク時間、NOC（Network Operation Center）のトラブルシューティングのリソース、および出張サービスのサービス コストを削減するには、ビデオ トラフィックのモニタリング機能が必要です。Cisco ASR9000 ルータでは、ビデオ フローの問題はビデオ モニタリングにより簡単に診断できます。

パケット損失は、ビデオ品質低下の一般的な原因の 1 つです。圧縮されたビデオ フローでは、その影響はより顕著です。サービス プロバイダーの IP ネットワーク経由で転送されるビデオ トラフィックは、圧縮率の高いビデオ（MPEG または同様の符号化がされたビデオ）がほとんどです。圧縮の方法が原因で、トラフィックは非常に損失の影響を受けやすくなっています。ビデオは独立したフレーム（I フレーム）を使用して数秒ごとに符号化され、後続のフレームは I フレームからのデルタとして処理されます。損失が I フレームにある場合、3 ms のトラフィック（約 1 つの IP パケット）が損失すると、最大 1.2 秒間表示品質が低下する可能性があります。

ジッターは、エンド デバイスでのバッファ プロビジョニングに注意を要する重要なフロー特性です。画面にメディアを表示するセット トップ ボックス（STB）は、ビデオをリアルタイムにデコードする必要があります。STB は、画像をスムーズにデコードして表示できるように、受信するビデオ ストリームをバッファリングします。ネットワーク ジッターが大きくなると、STB でバッファ アンダーランまたはバッファ オーバーランを引き起こす可能性があります。ジッターの大きさによっては、画面に表示のアーティファクトや「ブラック スクリーン」を発生させてしまいます。

送信のエンドツーエンド遅延は、ブロードキャスト専用アプリケーションにとって大きな問題ではありません。ただし、ビデオ アプリケーションはよりインタラクティブになっているため、エンドツーエンド遅延は重要な Quality of Experience（QoE）要素になります。データ損失は QoE 低下の主な一因です。

QoE が低下する 3 つの主な原因は、次のとおりです。

- パケット損失
- ジッター
- 遅延

ビデオ モニタリングは、ビデオ品質の向上、そして QoE の向上に非常に重要な役割を担います。ビデオ モニタリングがルータで実装されると、ネットワーク オペレータはフローごとにビデオ転送パフォーマンスを測定および追跡できます。ビデオ パケットはルータを通過します。パケット ヘッダーを使用し、ビデオの品質に影響を与えるネットワーク パフォーマンスの基準となるメトリックを計算できます。同じフローに対して複数のルータでこの情報を比較することで、ネットワークで発生しているビデオの問題と影響を受けるフローをエンドツーエンドで明確に理解できます。

ビデオ フロー（より一般的には、あらゆるストリーミング フロー）の問題はビデオ モニタリングにより診断できます。ビデオ モニタリングの目的は、ネットワークにより生じる、QoE を低下させる可能性がある摂動や異常を検出することです。つまり、ストリーミングされている（ビデオ）トラフィックの転送パフォーマンスを測定します。符号化エラーや音声とビデオのずれなどのエラーも QoE を低下させます。ただし、これらはネットワークではなく符号化デバイスで発生します。このため、これらのエラーはモニタされません。

ビデオ モニタリングでサポートされている主な機能

データ プレーンからの直接測定

ビデオ モニタリングは、ビデオ品質を向上するうえで非常に重要な役割を担い、QoE が向上します。Cisco ASR 9000 シリーズ ルータ に実装されたビデオ モニタリングでは、ネットワーク オペレータはフロー単位でリアルタイムにビデオ転送パフォーマンスを測定および追跡できます。従来のトラフィック モニタリング ソリューション（サンプリングするフローをコントロール プレーン、またはルータ上の専用のブレードなどの別のハードウェアに送信する必要があるソリューション）と異なり、Cisco ASR 9000 シリーズ ルータのビデオ モニタリングはデータ プレーン自体でモニタリング操作を実行します。このため、ビデオ モニタリングにより、リアル タイムに転送パケットを分析し、ビデオの品質に影響を与えるネットワーク パフォーマンスの基準を提供するメトリックを計算することができます。

ローカル ストレージとリモート アクセス

ビデオ モニタリングでは、ネットワーク オペレータがユーザ インターフェイスからアクセスできるように、ワイヤ速度でパケット損失およびジッターを測定し、収集した情報をルータに保存します。さらに、複数のルータで測定および保存されたパフォーマンス メトリックは、リモートの運用センターから標準 SNMP 経由でアクセスできます。これらのメトリックは、構成および分析が可能なビデオ フローのエンドツーエンドの明確な情報を提供します。

予防的および対処的な使用

Cisco ASR 9000 シリーズ ルータのビデオ モニタリングは、サービス プロバイダーの対処的および予防的な使用に対応します。新しい顧客にサービス カバレッジを拡大する前に、ビデオ サービスの品質を確認するために使用できます。また、ビデオ モニタリングは分析の強力なツールとなり、顧客の電話内容をトラブルシューティングするために使用できます。ネットワーク オペレータは、パケット損失、ジッター、フロー レート、フロー数の変化など、さまざまなイベントのアラームを発生するようにビデオ モニタリングを設定できます。このアラームは、有効な任意の値または範囲でトリガーされるように設定できます。

ビデオ モニタリング上のフロー

ビデオ モニタリングは、一意のフローを区別するために 4 つのパケット ヘッダー フィールド（送信元 IP アドレス、宛先 IP アドレス、送信元 UDP ポート、および宛先 UDP ポート。つまり、プロトコル ID は常に UDP）を使用します。

マルチキャストと ユニキャスト

現在のリリースでは、ビデオ モニタリングは、IP ヘッダーに IPv4 マルチキャスト宛先アドレスを持つフローをモニタします。ユニキャスト宛先アドレスを持つフローはモニタしません。

フロー レートのタイプとプロトコル レイヤ

ビデオ モニタリングは、IP レイヤで CBR（固定ビット レート）フローをモニタします。つまり、ビデオ モニタリングでは、IPv4 パケット内の UDP データグラムにカプセル化されている CBR 符号化されたメディア ストリーム（たとえば、MPEG-2）をモニタできます。ビデオ モニタリングでは、ユーザはメディア パケットの数とサイズに加えて、IP レイヤでのパケット レート、またはメディア レイヤでのビット レートを設定できます。

メトリック

ビデオ モニタリングは、IP-UDP レベルで MDI（Media Delivery Index、RFC 4445）定義に則ったパケット損失およびジッターのメトリックの両方をサポートします。MDI メトリックは MLR（メディア損失レート）および DF（遅延係数）です。ビデオ モニタリングは、MDI MLR の拡張である MRV（メディア レート変動）を使用します。つまり、MLR は損失だけをキャプチャしますが、MRV は、損失と過多の両方をキャプチャします。ビデオ モニタリング DF は MDI 定義と同様、モニタしている MDI ジッターに加えて、1 回の公称パケット到着時間間隔を表します。ビデオ モニタリングは、主な 2 つのメトリックとともに、パケット数、バイト数、パケット レート、ビット レート、パケット サイズ、IP ヘッダーの TTL（存続可能時間）フィールド、フロー数、発生したアラーム、およびさまざまなイベントのタイムスタンプをサポートします。

（注） MDI ジッターという用語は、ビデオ モニタリングで測定された DF メトリックの正確性を示すために使用されます。MDI ジッターは、公称到着基準時間と実際のパケット到着時間を比較することで測定されます。一方、単純なパケット間ジッターは連続する 2 つのパケットの到着時間の差で測定されます。前者は、後者よりも CBR フローのパフォーマンスを正確にキャプチャします。

フロー数

現在のリリースでは、Cisco ASR9000 シリーズ ルータのビデオ モニタリングは NP（ネットワーク プロセッサ）あたり最大 1024 のフローをサポートします。各ライン カードまたは各システムの最大フロー数は、ライン カードの NP の数およびシステムのライン カードの数によって異なります。シャーシあたりのフロー収容数は、シャーシの NP の数によって異なります。

たとえば、4 個のライン カードを使用する Cisco ASR 9000 シリーズ ルータ ボックスがあり、各ライン カードに 8 個の NP がある場合、シャーシあたりのフロー収容数は各シャーシ最大 1K × 8 × 4 = 32K になります。

ハイ アベイラビリティ機能

Cisco ASR 9000 シリーズ ルータのビデオ モニタリングは、さまざまなレベルでハイ アベイラビリティをサポートします。ビデオ モニタリングは、プロセスの OIR（活性挿抜）、ライン カードの OIR、RSP（ルート スイッチ プロセッサ）のフェールオーバーと、ルータのリロードをサポートします。設定は、すべてのハイ アベイラビリティのシナリオで、永続的です。モニタされた統計情報データは、プロセスの OIR および RSP のフェールオーバーにおいても維持されます。

インターフェイスのタイプおよび方向

ビデオ モニタリングをアクティブにするには、インターフェイスでビデオ モニタリング サービス ポリシーを設定する必要があります。ビデオ モニタリング ポリシーを適用できるインターフェイスには 4 種類あり、メイン インターフェイス、サブインターフェイス、イーサネット バンドル インターフェイス、イーサネット バンドル サブインターフェイスです。ビデオ モニタリングはレイヤ 3 インターフェイスだけをサポートし、レイヤ 2 インターフェイス（つまり、L2VPN ブリッジ ドメイン上の L2 転送インターフェイス）はサポートしません。ビデオ モニタリングは、インターフェイスの入力方向にだけ設定できます。

フロー レートと DF 精度

Cisco ASR 9000 シリーズ ルータのビデオ モニタリングは、1 ms の精度の DF メトリック パフォーマンスを提供します。さらに、ビデオ モニタリングは、最大 100 Mbps のフロー レートの標準画質（SD）ビデオ トラフィック（圧縮率の高いビデオ トラフィック）をサポートします。

入力ユーザ インターフェイス

ビデオ モニタリングは、MQC（モジュラ QoS 設定）構文に則る従来の CLI（コマンド ライン インターフェイス）入力による設定をサポートします。アクセス コントロール リスト（ACL）、クラス マップ、およびポリシー マップを設定することで、ビデオ モニタリングを設定できます。ビデオ モニタリングは、インターフェイスにサービス ポリシーを適用することでアクティブ化できます。その場でのポリシーの変更はサポートされていません。設定されたサービス ポリシーは、一度インターフェイスに適用されると、インターフェイスから適用を解除した後でのみ変更できます。

出力ユーザ インターフェイス

ビデオ モニタリングでは、モニタされた統計情報を取得するためのさまざま show コマンドおよび clear コマンドを使用できます。ビデオ モニタリング コマンドの詳細については、『*Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference*』の「*Video Monitoring Commands on Cisco ASR 9000 Series Routers*」モジュールを参照してください。

ポリシー マップの一部として、ビデオ モニタリングにおいてさまざまな条件で syslog メッセージを生成するように、TCA（しきい値超過アラート）を設定できます。**show** コマンドを使用するか SNMP プル経由で、スタンディング アラームを取得することもできます。XML は、ビデオ モニタリングでサポートされています。

クラス マップとポリシー マップの数

ビデオ モニタリングを使用するには、クラス マップと、データ プレーンでどのフローをモニタするかを決定するフィルタとして機能するポリシー マップを設定する必要があります。ビデオ モニタリングは、ポリシーマップあたり最大 1024 のクラス マップ、およびシステムあたり最大 1024 のクラス マップをサポートしています。システムでは最大 256 のポリシー マップがサポートされています。

ビデオ モニタリングのトラップとクローン

トラップとクローンは基本的なパフォーマンス モニタリング サービス機能の拡張であり、選択されたフロー数のパケットをフィルタリング（トラップ）および複製（クローン）し、ネットワーク上のリモート デバイスに送信することで、ビデオ画質のよりきめ細かな分析を実現します。クローンされたパケットは、パフォーマンス トラフィックのクローン プロファイルで指定されているインターフェイスへのマルチキャスト転送プロセスによって複製されます。リモート デバイスは、MPEG 層レベルのデータをより詳細に分析できます。このデバイスはデバッグ ツールとモニタリング ツールの両方に使用できます。また、このデバイスは、同じルータのサービス エンジン ブレードとして機能させることができます。

ビデオ モニタリングの用語

ビデオ モニタリング サービスを Cisco ASR 9000 シリーズ ルータに実装および設定するには、ビデオ モニタリングの用語と概念を理解している必要があります。

インターバル期間とインターバル アップデート

ビデオ モニタリングは、ユーザによって設定された、インターバル期間と呼ばれる期間のデータ プレーン上のすべてのパケットを継続的に解析します。統計情報は、各インターバル期間の最後に定期的にエクスポートされます。このエクスポートされた統計情報は、インターバル アップデートと呼ばれます。ビデオ モニタリング フローのステータスおよびその遷移は、すべてこれらのインターバル アップデートを参照して説明されます。これらのインターバル アップデートに関して、エクスポートされたすべてのビデオ モニタリング フローの統計情報も保存されます。

インターバル期間は、重要なビデオ モニタリング パラメータです。ビデオ モニタリング設定によって、エクスポートの頻度、保存されるエクスポートの数、非アクティブ フローを削除する時間などの機能に対するインターバル期間が固定されます。（停止したフローおよびパフォーマンスが低下したフローに対する）アラームの発生を含むすべてのビデオ モニタリング機能は、インターバル アップデートの内容に基づいています。

ビデオ モニタリング フロー

ビデオ モニタリング フローは、ヘッダー フィールドが、設定されたクラス マップ（および関連するアクセス コントロール リスト）と一致するパケット ストリームのインスタンスです。固有のフローはビデオ モニタリング サービス ポリシーが適用されているインターフェイスに対してローカルです。ビデオ モニタリング フローは一連の保存されたインターバル アップデートで構成されます。1 回のモニタリング間隔の後にビデオ モニタリング上で作成される固有のフローは、新規フローと呼ばれます。このため、1 回のモニタリング間隔よりも短い長さのパケット ストリームは、ビデオ モニタリング フローとしてエクスポートされず、保存もされません。

フローの停止

ルータが 1 回分のインターバル アップデート以上の期間でモニタされているフロー上でのパケットの受信を停止した場合、モニタされているフローは停止したと見なされます。

フローの再開

停止されたビデオ モニタリング フローがパケットの受信を開始する場合、正常なインターバル アップデートが次のモニタリング間隔でエクスポートされます。再開されたフローには、1 回以上のゼロ インターバルに続いて正常なインターバル アップデートがあります。

フローのスイッチオーバー

イーサネット バンドル インターフェイス、またはイーサネット バンドル サブインターフェイス上のビデオ モニタリング フローは、物理メンバ インターフェイス間で移動する場合があります。つまり、パケット ストリームが 1 つのインターフェイス上でフローを停止し、別のインターフェイス上でフローを開始します。これをフローのスイッチオーバーといいます。このような場合に、両方のインターフェイスが同じライン カード上にある場合、ビデオ モニタリングはスイッチオーバー前のフローとスイッチオーバー後のフローを同一のフローとして処理します。それ以外の場合は 2 つの異なるフローとして処理します。

フローの削除

停止されたビデオ モニタリング フローが（モニタリング間隔の数から）設定されたタイムアウトの間、ゼロのインターバルをエクスポートし続けると、フローはデッドと見なされ、削除するためにマーキングされます。マーキングされたすべてのフローの実際の削除は、定期的な（150 秒ごと）スイープ機能により、少し遅れて実行されます。エクスポートされたすべての統計情報（ゼロ インターバルを含む一連のインターバル アップデート）は、一度削除されるとストレージから完全に削除されます。

ビデオ モニタリングの実装

ビデオ モニタリングの設定は、関連するクラスマップ、ポリシー マップの設定、およびインターフェイスへのビデオ モニタリング ポリシーのバインディングを含む 4 段階の手順です。

- 「IPv4 アクセス リストの作成」（P.MCC-193）
- 「クラスマップの設定」（P.MCC-195）
- 「ポリシーマップの設定」（P.MCC-197）
- 「インターフェイスへのサービス ポリシーの設定」（P.MCC-206）
- 「インターフェイスへのトラップおよびクローンの設定」（P.MCC-208）

IPv4 アクセス リストの作成

この手順は、通常の IPv4 アクセス リストの作成および設定と似ています。ここでは、簡単な参照用に、ビデオ モニタリング用の ACL の設定例を示します。詳細については、『*Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services*』設定ガイドの「*Implementing Access lists and Prefix lists*」の章を参照してください。

ここでは、標準 IPv4 アクセス リストを設定します。

標準アクセス リストでは、照合操作に送信元アドレスを使用します。

（注） ビデオ モニタリング ポリシーでは、ACL 設定において明示的な **deny** 文を許可していません。また、log または log-input は、ACL 設定ではサポートされていません。

手順の概要

1. **configure**
2. **ipv4 access-list** *name*
3. [*sequence-number*] **remark** *remark*
4. [*sequence-number*] **permit udp source** [*source-port*] **destination** [*destination-port*]
5. 必要に応じてステップ 4 を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。
6. **end**
   または
   commit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv4 access-list** *name* **例：** `RP/0/RSP0/CPU0:router# ipv4 access-list acl_1`	IPv4 アクセス リスト コンフィギュレーション モードを開始し、アクセス リスト acl_1 を設定します。
ステップ 3	[*sequence-number*] **remark** *remark* **例：** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out`	（任意）名前付きアクセス リストにおいて、以降の **permit** ステートメントに関するコメントを入力できます。 • 注釈は最大 255 文字まで可能で、これより長い文字は切り捨てられます。 • 注釈は、**permit** ステートメントの前後に設定できますが、設定する場所は一貫性を保つ必要があります。
ステップ 4	[*sequence-number*] **permit udp source** [*source-port*] **destination** [*destination-port*] **例：** `RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit udp 172.16.0.0/24 eq 5000 host 225.0.0.1 eq 5000`	次の条件で送信元および宛先ポートを指定できます。 • ビデオ モニタリングは udp だけをサポートします。 • パケットの送信元となるネットワークまたはホスト番号を指定するには、*source* キーワードを使用します。 • 送信元に適用されるワイルドカード ビットを指定するには、オプションの *source-wildcard* 引数を使用します。 • パケットの宛先となるネットワークまたはホスト番号を指定するには、*destination* キーワードを使用します。 • 宛先に適用されるワイルドカード ビットを指定するには、オプションの *destination-wildcard* 引数を使用します。

	コマンドまたはアクション	目的
ステップ 5	必要に応じてステップ 4 を繰り返し、シーケンス番号順にステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。	アクセス リストの変更を可能にします。

ステップ 6	**end**
	または
	commit
	
	例：
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# end`
	または
	`RP/0/RSP0/CPU0:router(config-ipv4-acl)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		– **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		– **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		– **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

クラスマップの設定

ここでは、フロー分類子を設定します。これは、個々のフローに一致するフロー識別子の場合もあれば、複数のフローと一致する集約フィルタとなる場合もあります。

手順の概要

1. **configure**
2. **class-map type traffic** *class-map-name*
3. **match access-group ipv4** *acl-name*
4. **end-class-map**
5. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**class-map type traffic** *class-map-name* **例：** `RP/0/RSP0/CPU0:router(config)# class-map type traffic class1`	クラスマップ モードを開始します。クラスマップのタイプは常に traffic として入力する必要があります。
ステップ 3	**match access-group ipv4** *acl-name* **例：** `RP/0/RSP0/CPU0:router(config-cmap)# match access-group ipv4 acl1`	このクラスに一致させる ACL を入力します。各クラスに一致させることができる ACL は 1 つだけです。
ステップ 4	**end-class-map** **例：** `RP/0/RSP0/CPU0:router(config-cmap)# end-class-map`	クラスマップの設定を完了します。
ステップ 5	**end** または **commit** **例：** `RP/0/RSP0/CPU0:router(config-cmap)# commit`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:` – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ポリシーマップの設定

ビデオ モニタリングのポリシー マップは performance-traffic タイプです。ビデオ モニタリング ポリシーマップでは、1 つのレベルの階層のみサポートされています。これは、階層型ポリシー マップ設定がビデオ モニタリングでサポートされないことを意味します。

ビデオ モニタリングのポリシー マップ設定は、次の 3 つから構成されます。

- フロー パラメータの設定：インターバル期間、必要な履歴間隔、タイムアウトなど、モニタされるフローのさまざまな特性を指定します。
- メトリック パラメータの設定：モニタされるフローについて、計算が必要なメトリックを指定します。
- 反応パラメータの設定：指定するパラメータに基づいて、フローに対してアラートが生成されます。

設定の階層は、policy -> class -> flow です。これは、上記で指定されたすべてのパラメータが、特定のクラスと一致する、ポリシーマップのすべてのフローに適用されることを意味します。指定されたクラスに一致するフローへのフロー パラメータと反応パラメータの指定は任意ですが、メトリック パラメータの指定は必須です。

ポリシーマップのメトリック パラメータの設定

ポリシー マップのメトリック パラメータには、次のものがあります。

- レイヤ 3 パケット レート、または
- メディア ビット レート（指定された UDP ペイロードのメディア パケット カウント数とサイズを含む）。

（注） レイヤ 3 パケット レートとメディア レートには、相互に排他的なコンフィギュレーション コマンドがあります。

それぞれの場合の設定について、この項で説明します。

レイヤ 3 パケット レート

手順の概要

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor metric ip-cbr**
5. **rate layer3 packet** *packet-rate* **pps**
6. **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** RP/0/RSP0/CPU0:router# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map type** *performance-traffic policy-map-name* **例：** RP/0/RSP0/CPU0:router(config)# **policy-map type** *performance-traffic policy1*	ポリシーマップ モードを開始します。ポリシーマップのタイプは常に performance traffic として入力する必要があります。
ステップ 3	**class type** *traffic class-name* **例：** RP/0/RSP0/CPU0:router(config-pmap)# **class type** *traffic class-name*	このポリシーに一致させるクラスマップを入力します。複数のクラスを 1 つのポリシーに指定できます。
ステップ 4	**monitor metric ip-cbr** **例：** RP/0/RSP0/CPU0:router(config- pmap-c)# **monitor metric ip-cbr**	IP-CBR メトリック モニタ サブモードを開始します。 **（注）** 現在、ip-cbr メトリック モニタリングのみビデオ モニタリングでサポートされます。

	コマンドまたはアクション	目的
ステップ 5	**rate layer3 packet** *packet-rate* **pps** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr) # **rate layer3 packet** *packet-rate* **pps**	IP レイヤ 3 パケット レートを pps 単位で指定します。
ステップ 6	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr) # **end** または RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr) # **commit**	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:` – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

メディア ビットレート

メディア ビットレートのメトリック パラメータは、メディア ビット レート、メディア パケット カウント、パケット サイズで構成されます。

レート メディア オプションを使用すると、1 個の UDP パケットに存在するメディア ペイロード パケット（MPEG-2 データグラム）の数と、各メディア ペイロードのサイズを指定できます。メディア ビット レートの指定は必須です。Cisco IOS XR ソフトウェア リリース 3.9.1 では、パケット カウントおよびパケット サイズのデフォルトはありません。このため、これらの値を設定する必要があります。

（注） メディア ビット レートが 1052800 bps、メディア パケット カウントが 7、メディア パケット サイズが 188 バイトに設定されている場合、メディア パケット レートはレイヤ 3 で 100 pps です。計算は次のとおりです。1052800 / (7 × 188 × 8) = 100 pps

手順の概要

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*

3. **class type** *traffic class-name*
4. **monitor metric ip-cbr**
5. **rate media** *bit-rate* **{bps|kbps|mbps|gbps}**
6. **media packet count in-layer3** *packet-count*
7. **media packet size** *packet-size*
8. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map type** *performance-traffic policy-map-name* **例：** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	ポリシーマップ モードを開始します。ポリシーマップのタイプは常に performance traffic として入力する必要があります。
ステップ 3	**class type** *traffic class-name* **例：** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	このポリシーに一致させるクラスマップを入力します。複数のクラスを 1 つのポリシーに指定できます。
ステップ 4	**monitor metric ip-cbr** **例：** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor metric ip-cbr`	IP-CBR メトリック モニタ サブモードを開始します。 **（注）** 現在、ip-cbr メトリック モニタリングのみビデオ モニタリングでサポートされます。
ステップ 5	**rate media** *bit-rate* **{bps|kbps|mbps|gbps}** **例：** `RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# rate media 100 mbps`	bps、kbps、mbps、または gbps 単位でフローのメディア ビット レートを指定します。ここで設定をコミットできます。オプション パラメータを指定することもできます。 **（注）** デフォルトのメディア ビットレートの単位は kbps です。
ステップ 6	**media packet count in-layer3** *packet-count* **例：** `RP/0/RSP0/CPU0:router(config-pmap-c-ipbr)# media packet count in-layer3 10`	IP ペイロードごとにメディア パケット数を指定します。

	コマンドまたはアクション	目的
ステップ 7	**media packet size packet-size** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **media packet size** *188*	IP ペイロードの各メディア パケットのサイズ（バイト単位）を指定します。
ステップ 8	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **end** または RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **commit**	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ポリシーマップのフロー パラメータの設定

ポリシー マップのフロー パラメータはオプションです。

ビデオ モニタリングでは、データ プレーンは、各間隔の最後にエクスポートされるメトリックとフローを継続的にモニタします。また、このインターバル期間と、各フロー（履歴）で格納する必要があるインターバルの数を任意に指定できます。各フローには、次のフロー パラメータを指定できます。

- **インターバル期間**：この時間間隔の最後にメトリックがエクスポートされます。これは 5 の倍数で指定します（10 ～ 300 秒の任意の値）。デフォルト値は 30 です。
- **履歴**：各フローで保存する必要があるフロー情報（フロー ID、メトリックなど）を含むインターバル数。これは、1 ～ 60 の任意の値を指定できます。デフォルト値は 10 です。
- **タイムアウト**：インターバル期間の倍数で指定されるタイムアウト。この期間を過ぎると、非アクティブなフローは削除用にマーキングされます。これは、2 ～ 60 の任意の値を指定できます。デフォルト値は 0 です。（注：タイムアウト値 0 には、フローをタイム アウトさせずにスタティック フローにするという特別な意味があります）。
- **各クラスの最大フロー**：ポリシーの各クラスでモニタする必要があるフローの最大数。これは、1 ～ 1024 の任意の値を指定できます。デフォルト値は 1024 です。

手順の概要

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor parameters**
5. **{interval duration** *duration*| **flows** *number of flows* | **history** *intervals* | **timeout** *duration***}**
6. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map type** *performance-traffic policy-map-name* **例：** `RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1`	ポリシーマップ モードを開始します。ポリシーマップのタイプは常に performance traffic として入力する必要があります。
ステップ 3	**class type** *traffic class-name* **例：** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name`	このポリシーに一致させるクラスマップを入力します。複数のクラスを 1 つのポリシーに指定できます。
ステップ 4	**monitor parameters** **例：** `RP/0/RSP0/CPU0:router(config- pmap-c)# monitor parameters`	フロー モニタ サブ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 5	**{interval duration** *duration*| **flows** *number of flows*	**history** *intervals*	**timeout** *duration}* **例：** RP/0/RSP0/CPU0:router(config-pmap-c-fparm)# **interval duration** *10*	• フローごとにインターバル期間を指定するには、**interval duration** オプションを選択します。範囲は 10 ～ 300 で、5 の倍数である必要があります。デフォルト値は 30 です。 • フローごとに保存するインターバル データの最大数を指定するには、**history** オプションを選択します。これは、1 ～ 60 の任意の値を指定できます。デフォルト値は 10 です。 • インターバル期間の倍数でタイムアウトを指定するには、**timeout** オプションを選択します。この期間を過ぎると、非アクティブなフローは削除用にマーキングされます。範囲は 2 ～ 60 です。デフォルト値は 0 で、スタティック フローを示します。 • クラスごとにモニタできるフローの最大数を指定するには、**flows** オプションを選択します。範囲は 1 ～ 1024 です。デフォルト値は 1024 です。
ステップ 6	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **end** または RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **commit**	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:` – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ポリシーマップの反応パラメータの設定

ポリシー マップの反応パラメータはオプションです。

反応パラメータは、ユーザにとって直接の基準となるフロー品質を示すパラメータです。フローは継続的にモニタされ、インターバル期間の最後に、特定のパラメータに対してユーザが指定したしきい値を超過したかどうかを確認するために統計情報が検査されます。超過している場合、syslog アラームがコンソールに生成されます。アラームが設定されている場合、この条件に対する追加の syslog 通知は発行されません。

- メディア レート変動（MRV）：フローの MRV 統計情報がユーザ指定のしきい値を超えると、ビデオ モニタリングが反応しアラームを生成します。
- 遅延係数：フローの遅延係数統計情報がユーザ指定のしきい値を超えると、ビデオ モニタリングが反応しアラームを生成します。
- メディア停止：フローが停止すると、ビデオ モニタリングが反応しアラームを生成します。これは、フローに対して 1 回分のモニタリング間隔の間にパケットを受信していないことを示します。
- パケットレート：フローのパケット レートがユーザ指定のしきい値を超えると、ビデオ モニタリングが反応しアラームを生成します。
- フローカウント：各クラスのフロー カウントがユーザ指定のしきい値を超えると、ビデオ モニタリングが反応しアラームを生成します。

手順の概要

1. **configure**
2. **policy-map type performance-traffic** *policy-map-name*
3. **class type traffic** *class-name*
4. **react** *react-id* {**mrv | delay-factor | media-stop | packet-rate | flow-count**}
5. **threshold type immediate**
6. **threshold value {ge | gt | le | lt | range}** *limit*
7. **action syslog**
8. **alarm severity {error | critical | alert | emergency}**
9. **alarm type {discrete | grouped }**
10. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** RP/0/RSP0/CPU0:router# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**policy-map type** *performance-traffic policy-map-name* **例：** RP/0/RSP0/CPU0:router(config)# **policy-map type** *performance-traffic policy1*	ポリシーマップ モードを開始します。ポリシーマップのタイプは常に performance traffic として入力する必要があります。
ステップ 3	**class type** *traffic class-name* **例：** RP/0/RSP0/CPU0:router(config-pmap)# **class type** *traffic class-name*	このポリシーに一致させるクラスマップを入力します。複数のクラスを 1 つのポリシーに指定できます。
ステップ 4	**react** *react-id* **{mrv | delay-factor | packet-rate | flow-count | media-stop}** **例：** RP/0/RSP0/CPU0:router(config- pmap-c)# **react** 1 **mrv**	反応パラメータ設定サブモードを開始します。ここで指定する反応 ID は、各クラスで一意である必要があります。
ステップ 5	**threshold type immediate** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-react)# **threshold type immediate**	しきい値に対してトリガー タイプを指定します。現在、使用可能なしきい値タイプは immediate です。
ステップ 6	**threshold value {ge | gt | le | lt | range}** *limit* **例：** RP/0/RSP0/CPU0:router(config-pmap-c-react)# **threshold value ge** 50	しきい値に対してトリガー値の範囲を指定します。
ステップ 7	**action syslog** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-react)# **action syslog**	**action** キーワードでは、しきい値の制限を超えた場合に実行するアクションを指定します。現在、syslog アクションが使用できる唯一のオプションです。
ステップ 8	**alarm severity {error | critical | alert | emergency}** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-react)# **alarm severity critical**	syslog のアラームの重大度を指定します。

	コマンドまたはアクション	目的
ステップ 9	**alarm type {discrete | grouped }** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-react)# **alarm type discrete**	アラーム タイプを指定します。個別のアラームがしきい値を超えたすべてのフローに発行されます。特定の数または割合のフローがしきい値を超えた場合は、グループ化されたアラームが発行されます。
ステップ 10	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **end** または RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# **commit**	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

この設定手順については、次の事項に注意してください。

- **media-stop** 反応パラメータに対して、**threshold-type** および **threshold-value** オプションを適用できません。
- **flow-count** 反応パラメータに対して、**alarm-type** オプションを適用できません。

インターフェイスへのサービス ポリシーの設定

ビデオ モニタリング サービスをイネーブルにするには、設定されたポリシーマップを入力方向のインターフェイスに適用する必要があります。

イーサネット バンドル インターフェイスの場合、サービス ポリシーを物理メンバ インターフェイスには適用せず、バンドル親インターフェイスのみに適用することができます。イーサネット バンドル サブインターフェイスの場合、サービス ポリシーはサブインターフェイスのみに適用できます。VLAN サブインターフェイスの場合、サービス ポリシーをメイン インターフェイスに適用できません。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **service-policy type performance-traffic input** *policy-map-name*
4. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例**： RP/0/RSP0/CPU0:router# configure	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type interface-path-id* **例**： RP/0/RSP0/CPU0:router(config)# **interface** *type interface-path-id*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • type 引数には、インターフェイス タイプを指定します。インターフェイス タイプの詳細については、疑問符（?）オンライン ヘルプ機能を使用してください。 • インスタンスの引数には物理インターフェイス インスタンスまたは仮想インスタンスを指定します。 • 物理インターフェイス インスタンスの表記方法は rack/slot/module/port です。表記の一部として、値を区切るスラッシュ（/）が必要です。 • 仮想インターフェイス インスタンスの番号範囲は、インターフェイス タイプによって異なります。

	コマンドまたはアクション	目的
ステップ 3	**service-policy type performance-traffic input** *policy-name* **例：** RP/0/RSP0/CPU0:router(config-if)# **service-policy type performance-traffic input** *policy1*	入力方向のインターフェイスにポリシーを適用します。
ステップ 4	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-if)# **end** または RP/0/RSP0/CPU0:router(config-if)# **commit**	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

インターフェイスへのトラップおよびクローンの設定

トラップとクローンは既存のビデオ モニタリング サービスの拡張であるため、現在のコントロール プレーン インフラストラクチャを拡張することで、トラップとクローンの設定を収容できます。

フロー タプル情報（送信元および宛先 IP アドレス）を使用して、トラップをインストールできます。トラップでは、一致したパケットは最終的にリモート デバイスまたはローカル プローブで詳細に分析されます。

次の手順では、一般的なビデオ モニタリング シナリオでのトラップおよびクローン プロセスの操作方法を示します。

- 適切なパッケージ（マルチキャスト PIE およびビデオ PIE）をインストールしてビデオ モニタリングをイネーブルにし、ACL、クラス マップ、ポリシー マップを設定し、インターフェイスにポリシー マップをバインドする必要があります。

- フローの送信元と宛先を指定することで複製するフローを指定して、トラップとクローンを設定する必要があります。
- トラップは VidMon コントロール プレーンによってデータ プレーンにインストールされ、VidMon データ プレーンは指定されたフローのパケットのクローンを開始します。
- クローンされたパケットは、リモート モニタリング デバイスに転送され、詳細に分析されます。

（注） インストールされているトラップを確認するには、**show performance traffic clone profile** コマンドを使用します。ビデオ モニタリングのトラップおよびクローン機能は、マルチキャスト トラフィックに対してのみサポートされます。これはクローン インターフェイスのスタティック IGMP グループを使用して実装されます。クローン インターフェイスは、ローカル プローブに接続された専用ポートに設定できます。

手順の概要

1. **configure**
2. **performance traffic clone profile**
3. **performance traffic clone profile** *profile_name* **description**
4. **interface** *type interface-path-id*
5. **clone flow ipv4 source** <*source-ip*> **destination** <*destination-ip*>
6. **end** または **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**performance traffic clone profile** **例：** `RP/0/RSP0/CPU0:router(config)# performamce traffic clone profile`	パフォーマンス トラフィック クローン プロファイル モードを開始します。
ステップ 3	**performance traffic clone profile** *profile_name* **description** **例：** `RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# performamce traffic clone profile profile1 description`	クローン プロファイルの説明を設定します。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type interface-path-id* **例：** RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# **interface** *GigabitEthernet 0/0/0/1*	クローン プロファイルの出力インターフェイスを設定します。
ステップ 5	**clone flow ipv4 source** *<source-ip>* **destination** *<destination-ip>* **例：** RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# **clone flow ipv4** *23.1.1.1 224.2.2.2*	クローン プロファイルに、クローンする必要があるトラフィック フローを設定します。 **（注）** 複数のフローを 1 つのクローン プロファイルに関連付けることができます。同様に、1 つのフローを複数のクローン プロファイルに関連付けることができます。
ステップ 6	**end** または **commit** **例：** RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# **end** または RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# **commit**	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:` – **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。 – **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 – **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

ビデオ モニタリング 実装の設定例

ここでは、さまざまなシナリオの設定例を示します。

シナリオ 1

イーサネット バンドル インターフェイスに、マルチキャスト ビデオ トラフィックがフローごとに 300 pps で流れている 3 つの物理メンバがあります。

ビデオ モニタリングを使用してこのイーサネット バンドルのすべてのフローをモニタし、フローごとのトラフィック負荷の予想レートが 10 % を超える場合にクリティカル レベルのアラームを発行し、遅延係数が 4 ms を超える場合にエラーレベルのアラームを発行します。収集された統計情報を 10 秒ごとにレポートします。フローがアクティブである限り、レポートされた統計情報を 10 分間保存します。パケットを 30 秒間受信しなかった場合は、フロー統計情報を削除します。

例

```
ipv4 access-list sample-acl
 10 permit udp any any
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   interval duration 10
   history 60
   timeout 3
  !
  monitor metric ip-cbr
   rate layer3 packet 300 pps
  !
  react 100 mrv
   threshold type immediate
   threshold value gt 10.00
   action syslog
   alarm severity error
   alarm type discrete
  !
  react 101  delay-factor
   threshold type immediate
   threshold value gt 4.00
   action syslog
   alarm severity error
   alarm type discrete
  !
 !
 end-policy-map
!
interface Bundle-Ether10
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
interface TenGigE0/6/0/0
 bundle id 10 mode on
!
interface TenGigE0/6/0/1
 bundle id 10 mode on
!
interface TenGigE0/6/0/2
 bundle id 10 mode on
!
```

シナリオ 2

VLAN サブインターフェイスは、さまざまな UDP ポート番号と共通のマルチキャスト グループ アドレス 225.0.0.1 を持つ 100 個のビデオ ストリームを伝送しています。IP レイヤの予想パケット レートは不明ですが、メディア ビット レートは 1052800 bps であることがわかっています。メディア ペイロードには MPEG-2 符号化 CBR フローが含まれることがわかっており、デフォルトのパケット化が使用されています（つまり、1 個の UDP ペイロードに 7 個の MPEG パケットがあり、各パケットの長さは 188 バイトです）。

100 個を超えるフローはモニタしません。フローが停止してもフローをタイムアウトおよび削除しませんが、停止したフローの割合が 90 % を超える場合は、エラーレベルのアラームを発行します。

例

```
ipv4 access-list sample-acl
 10 permit udp any host 225.0.0.1
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   flows 100
!
  monitor metric ip-cbr
   rate media 1052800 bps
  !
  react 100 media-stop
   action syslog
   alarm severity error
   alarm type grouped percent 90
  !
 end-policy-map
!
interface GigabitEthernet0/0/0/0
 no shutdown
!
interface GigabitEthernet0/0/0/0.1
 encapsulation dot1q 500
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

monitor metric ip-cbr において、次の 2 行はデフォルトであるため、設定する必要がありません。

- media packet count in-layer3 7
- media packet size 188

ただし、これらのパラメータがデフォルト値と異なる場合は、設定する必要があります。

シナリオ 3

メイン インターフェイスには、3 つのマルチキャスト ストリーム グループがあり、1 番目のグループの UDP 宛先ポートは 1000、2 番目のグループは 2000、3 番目のグループは 3000 および 4000 です。これらの 3 つのストリーム グループはそれぞれ 100 pps、200 pps、300 pps で流れています。

各グループのフローの最大数を 300 フローに制限し、これらがプロビジョニングされたフロー容量の 90 % に達した場合は、エラー レベルのアラームを発行します。

例

```
ipv4 access-list sample-acl-1
 10 permit udp any any eq 1000
!
ipv4 access-list sample-acl-2
 10 permit udp any any eq 2000
!
ipv4 access-list sample-acl-3
 10 permit udp any any eq 3000
 20 permit udp any any eq 4000
!
class-map type traffic match-any sample-class-1
 match access-group ipv4 sample-acl-1
 end-class-map
!
class-map type traffic match-any sample-class-2
 match access-group ipv4 sample-acl-2
 end-class-map
!
class-map type traffic match-any sample-class-3
 match access-group ipv4 sample-acl-3
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class-1
  monitor parameters
   interval duration 10
   history 60
   timeout 3
   flows 300
  !
  monitor metric ip-cbr
   rate layer3 packet 100 pps
  !
  react 100 flow-count
   threshold type immediate
   threshold value gt 270
   action syslog
   alarm severity error
  !
class type traffic sample-class-2
  monitor parameters
   interval duration 10
   history 60
   timeout 3
   flows 300
  !
  monitor metric ip-cbr
   rate layer3 packet 200 pps
  !
  react 100 flow-count
   threshold type immediate
   threshold value gt 270
   action syslog
   alarm severity error
  !
class type traffic sample-class-1
  monitor parameters
   interval duration 10
   history 60
   timeout 3
   flows 300
```

```
  !
  monitor metric ip-cbr
   rate layer3 packet 300 pps
  !
  react 100 flow-count
   threshold type immediate
   threshold value gt 270
   action syslog
   alarm severity error
  !
 !
 end-policy-map
!
interface GigabitEthernet0/0/0/0
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

シナリオ 4

10GE メイン インターフェイスは、スポーツ スタジアム内の 6 台の HD カメラに直接接続されているデジタル コンテンツ マネージャ（DCM）から 6 つの高解像度（HD）ビデオ ストリームを受信します。各 HD ビデオ ストリームは圧縮解除され、帯域幅はレイヤ 2 で 1.611 Gbps（140625 pps に相当）になります。これら 6 つのストリームは、マルチキャスト グループ 225.0.0.1 ～ 225.0.0.6 で受信され、UDP ポート番号は 5000 です。

すべてのフローの遅延係数が 2 ms を超えるか、メディア損失比率が 5 % を超える場合は、クリティカル レベルのアラームを発行します。10 秒間隔で、最大量の履歴を保存します。このインターフェイスで 6 つを超えるフローはモニタしません。非アクティブ フローをタイムアウトしません。

例

```
ipv4 access-list sample-acl
 10 permit udp any eq 5000 225.0.0.0/24 eq 5000
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
 end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   interval duration 10
   history 60
   flows 6
  !
  monitor metric ip-cbr
   rate layer3 packet 140625 pps
  !
  react 100 mrv
   threshold type immediate
   threshold value gt 5.00
   action syslog
   alarm severity critical
   alarm type discrete
  !
  react 200 delay-factor
   threshold type immediate
   threshold value gt 2.00
   action syslog
   alarm severity critical
```

```
   alarm type discrete
  !
 end-policy-map
!
interface TenGigE0/2/0/0
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!
```

シナリオ 5

イーサネット インターフェイスは、マルチキャスト ビデオ トラフィックが流れている Cisco ASR 9000 シリーズ ルータに設定されています。ビデオ モニタリングを使用して、このイーサネット インターフェイスのすべてのビデオ フローのパフォーマンスをモニタします。ビデオ モニタリングのトラップおよびクローン機能を使用して、これらのフロー パケットをトラップし、指定した出力インターフェイスにクローン（複製）します。

指定した出力インターフェイスにクローンするフローを含むトラップおよびクローン プロファイルを設定します。プロファイルの説明を追加します。

例

```
Performance traffic clone profile profile1
   Description video flows monitored by vidmon
   Interface GigE 0/1/1/1
   flow ipv4 source 23.1.1.1 destination 231.2.2.2
```

その他の関連資料

ここでは、Cisco IOS XR ソフトウェア へのマルチキャスト ルーティングの実装に関する参考資料について説明します。

関連資料

関連項目	参照先
マルチキャスト コマンド リファレンス マニュアル	『*Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ マルチキャスト コマンド リファレンス*』
スタートアップ資料	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
モジュラの QoS コマンド リファレンス資料	『*Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference*』

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を検索およびダウンロードするには、http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml にある Cisco MIB Locator を使用し、[Cisco Access Products] メニューからプラットフォームを選択します。

RFC

RFC	タイトル
RFC4445	Proposed Media Delivery Index (MDI)

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport