NAM の導入

ここでは、ネットワークに NAM を導入する方法に関する使用例について説明します。Cisco Prime ネットワーク解析モジュール ソフトウェア の使用シナリオのほか、ネットワークのパフォーマンス管理についても詳しく説明します。

サポートされる NAM プラットフォーム上で実行されるリリース バージョンを確認するには、『*NAM Compatibility Matrix*』を参照してください。

使用例は、対処すべき特定のニーズや解決すべき問題に焦点を当てています。いずれのシナリオにおいても、「Cisco Prime NAM の導入」で説明した導入に関する考慮事項を踏まえたうえで、NAM のさまざまな機能を通じて目的の実現または問題の解決がなされています。こうした使用例を示す目的は、実際的な事例を紹介することにあります。これらの例は、ベスト プラクティスおよび効果的な NAM 展開の方法について説明し、いくつかのカテゴリにグループ化されます。

この章は、次の項で構成されています。

- 「データセンターへの導入」
- 「キャンパス環境への導入」
- 「ブランチへの導入」
- 「一般的な使用シナリオ」
- 「モニタリング アプリケーションおよびレポート アプリケーションと NAM の統合」

（注） この項で表示されるグラフィックの一部は画面に表示されるものとは異なる場合があります。これらの図は、例用です。

データセンターへの導入

- 「Nexus 1000V スイッチ環境のモニタリング」（P.21）
- 「トラフィックのリアルタイム モニタリングとリアルタイム分析」（P.12）
- 「TCP インタラクティブ アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「UDP リアルタイム アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「NAM を使用した QoS/DiffServ（DSCP）のモニタリング」（P.14）
- 「Cisco WAAS のモニタリングとその影響の測定」（P.8）

キャンパス環境への導入

- 「トラフィックのリアルタイム モニタリングとリアルタイム分析」（P.12）
- 「TCP インタラクティブ アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「UDP リアルタイム アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「NAM を使用した QoS/DiffServ（DSCP）のモニタリング」（P.14）
- 「NAM を使用した VoIP 品質のモニタリング」（P.3）

ブランチへの導入

- 「ブランチでの可視化」（P.7）
- 「トラフィックのリアルタイム モニタリングとリアルタイム分析」（P.12）
- 「TCP インタラクティブ アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「UDP リアルタイム アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「NAM を使用した QoS/DiffServ（DSCP）のモニタリング」（P.14）
- 「Cisco WAAS のモニタリングとその影響の測定」（P.8）
- 「NAM を使用した VoIP 品質のモニタリング」（P.3）

一般的な使用シナリオ

次の使用例は、ネットワークのいずれの構成要素にも適用可能です。

- 「サイトによる所在地または組織に合わせた導入」（P.5）
- 「NAM による履歴傾向分析（[Interactive Report] から実行）」（P.18）
- 「NAM による問題の特定」（P.25）
- 「カスタム アプリケーションの作成」（P.5）
- 「NAM の自動検出機能」（P.5）
- 「NAM によるスマート グリッドの可視化」（P.25）

モニタリング アプリケーションおよびレポート アプリケーションと NAM の統合

- 「NAM と LMS の統合」（P.7）
- 「NAM とサードパーティ レポート ツールの統合」（P.6）

配置例

- 「NAM を使用した VoIP 品質のモニタリング」（P.3）
- 「NAM の自動検出機能」（P.5）
- 「カスタム アプリケーションの作成」（P.5）
- 「サイトによる所在地または組織に合わせた導入」（P.5）
- 「NAM とサードパーティ レポート ツールの統合」（P.6）
- 「NAM と LMS の統合」（P.7）
- 「ブランチでの可視化」（P.7）
- 「Cisco WAAS のモニタリングとその影響の測定」（P.8）

NAM を使用した VoIP 品質のモニタリング

Cisco NAM では、音声品質分析の機能が大幅に向上しました。現在このソフトウェアでは、業界標準の MOS アルゴリズムを使用することで、音声品質の正確な測定が可能になっています。コール品質の測定値は 1 分ごとに計算され、グラフィカル ユーザ インターフェイスを介して確認することができます。ただし、NAM GUI に表示される音声関連の画面は旧リリースから大幅に変更されています。具体的には、有用な情報が迅速かつ自動的に表示されるようになり、詳細情報を表示するためのナビケーション操作も簡単になりました。

導入：音声品質の分析用に導入する NAM は、発信側の電話から着信側の電話へ伝送される VoIP パケットをモニタできる必要があります。ネットワーク内のブランチ エッジでは、ブランチを出入りするすべてのコールを可視化することができます。同様にキャンパス エッジでは、キャンパスの境界を通過するコールをモニタすることができます。特にモニタリングの対象が特定の電話やネットワークの特定領域である場合、このような目的に使用する NAM は通常、ディストリビューション レイヤに導入するのが適しています。たとえば、新しいマルチプロトコル ラベル スイッチング（MPLS）リンクをパイロットに設定し、X 社の本社の建物のうち 3 つがそのパイロットに含まれるとします。この場合、その建物内のユーザが使用するディストリビューション Catalyst 6500 に NAM を導入すれば、これら 3 つの建物について音声品質をモニタすることができます。

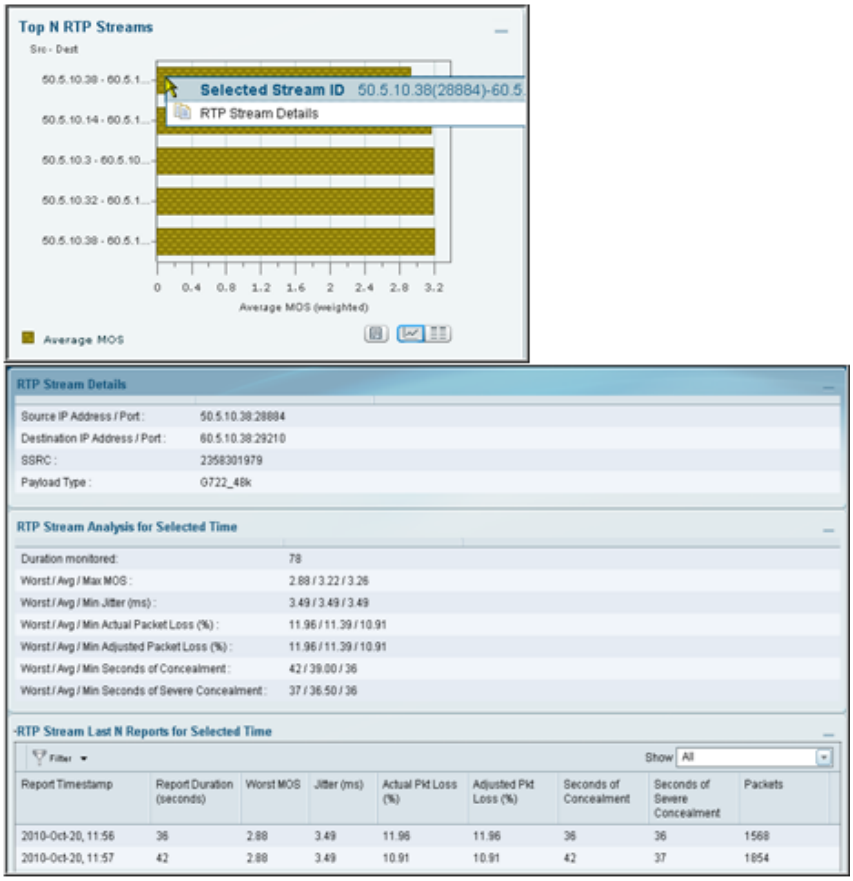
（注） データセンターは、コールの通過頻度が低いため、通常 RTP ストリーム分析を行う場所には適していません。ただし、電話と Cisco Unified Communications Manager との間のシグナリング メッセージをモニタする場所としてはデータセンターが適しています。NAM ではシグナリング メッセージのデコードを行うことにより、コール履歴、発信者名、電話番号などコールに関するさまざまな詳細情報の追跡が行われます。

次の手順に従ってネットワークをモニタすることにより、高いコール品質を維持することができます。品質に関する問題が生じた場合は、即座にその問題点を特定し、トラブルシューティングを行ってください。

ステップ 1　メニューから [Analyze] > [Media] を選択し [RTP Streams] を表示します。このチャートは、モニタしているすべての RTP ストリームの現在の音声品質を表したものです。MOS 値の範囲は 1 ～ 5 で、1 は低品質、5 は高品質を表します（[Poor]、[Fair]、[Good]、[Excellent] というカテゴリ分類については、凡例を参照）。次の図では、上位 N の RTP 送信元エンドポイントおよび RTP 宛先エンドポイントが表示されています。コールの中には、品質が非常に低いものも含まれているのがわかります。

ステップ 2　MOS が低いコールを特定するため、[Top N RTP Streams] をスクロール ダウンし、チャートをクリックして RTP ストリームの詳細をドリルダウンします。図 7-1 を見ると、リストの最上位に表示されている MOS は 2.88 という低い値であることがわかります。さらに、同じ行（たとえば、行 1）に表示されている別のメトリックを確認すると、ジッタが 3.49 でパケット損失率が 11 であり、MOS 値が低くなっていることに注意してください。こうした情報から、コール品質が低い根本的な原因がジッターにあること、あるいはネットワーク内のいずれかの場所で発生したパケット損失にあることがわかります。

図 7-1　MOS に基づく 上位 N の RTP ストリーム



ステップ 3　エンドポイントの IP アドレスがわかれば、ネットワーク トポロジを見ることで、サブネット 50.5.10.38 がネットワーク内のどの場所に存在するかを特定できます。この使用例において、このサブネットがメイン キャンパスの建物 3 にあるとすると、建物 3 のディストリビューション スイッチに NAM が配置されていることになります。

その NAM に移動し、メニューから [Analyze] > [Managed Device] > [Interface] を選択します。このページには、すべてのインターフェイスと、各インターフェイスにおけるエラーまたは廃棄数がリスト表示されます。建物 3 からコアに接続するリンクを探します。そのインターフェイスがパケット損失の原因である可能性があります。そのインターフェイスに不具合があるかどうかを確認し、必要があればそれに対処します。

「トラフィックの分析」、「RTP Streams」（P.37）、および「音声シグナリングのしきい値の設定」（P.51）を参照してください。

NAM の自動検出機能

既存の NAM 4.x または NAM 6 を使用している場合は、SPAN セッションを設定する必要はありません。SPAN セッションは（デバイス上ではなく）NAM 上で自動的に作成されます。新しい NAM 5.x を使用している場合は、SPAN または NetFlow を設定する必要があります。

データ ソースが自動的に作成されるようにするためには、NAM にトラフィックを転送するデバイス上であらかじめ SPAN または NetFlow を設定しておく必要があります。「Prime NAM データ ソースの設定」（P.10）を参照してください。

カスタム アプリケーションの作成

NAM では、TCP/UDP ポート番号に基づいてアプリケーション/プロトコルが識別されます。そのため、カスタム ポートを使用するアプリケーションがある場合は、それらのアプリケーションがポートではなく名前で識別されるように NAM を設定することができます。

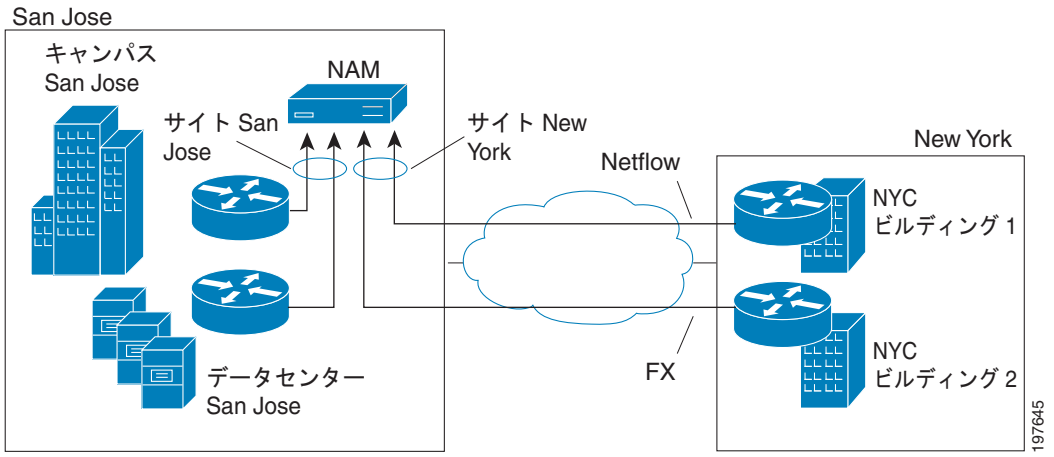
「アプリケーション トラフィックへのより深い可視性の作成」（P.68）を参照してください。

サイトによる所在地または組織に合わせた導入

Cisco Prime NAM は、サイトを定義するための機能を備えています。このサイトを利用すると、パフォーマンスに関する統計情報を集約しまとめることができます。サイトとはホスト（ネットワーク エンドポイント）の集合で、トラフィックのモニタリングや問題に関するトラブルシューティングが容易になるよういくつかのビューに分割されています。各サイトは、アドレス プレフィックスおよびアドレス マスクにより指定されたサブネットを複数まとめたものとして定義できるほか、リモート デバイスのデータ ソース（たとえばリモート WAE デバイスとセグメント情報）などその他の基準に基づいて定義することもできます。ネットワーク分析データのビューを特定の都市、建物、または建物の階に制限するには、サイト機能を使用できます。

図 7-2 は、ネットワーク内のさまざまな場所にある複数のデータ ソースを分析する集中型 NAM の導入形態を図示したものです。

図 7-2　サイト レベルでの集約



このような導入形態の場合には、SanJose-Campus、SanJose-Datacenter、NewYork-NetFlow-Bldg1、NewYork-WAAS-Bldg2 など複数のサイトを作成できます。サイトの設定に合致しないデータは、Default サイトに表示されます。これにより、モニタリングおよびトラブルシューティングに関するビューや情報が区分けされるため、目的の特定領域にドリルダウンできます。

また、サイトを定義する際には複数タイプのデータ ソースを指定することも可能です。その場合には、すべてのネットワーク トラフィックを集約して表示できます。

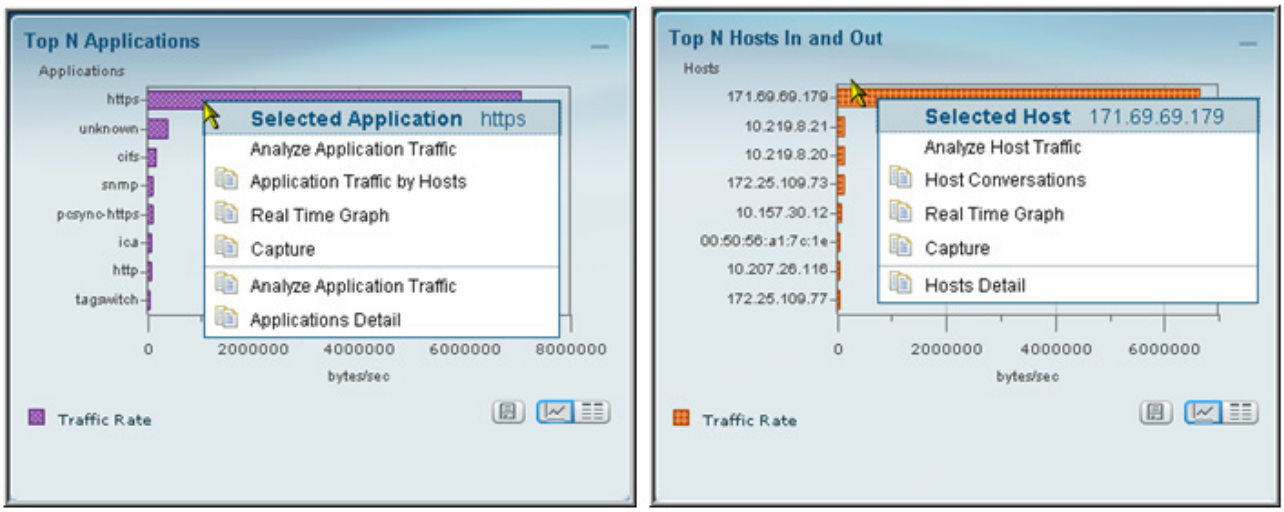
事前に定義されている「Unassigned Site」を使用すると、ユーザ定義サイトを設定しなくても容易に NAM を稼働できます。いずれのユーザ定義サイトにも属さないホストは、自動的に Unassigned Site の所属となります。

インタラクティブ ダッシュボードは、San Jose または New York サイトにドリル ダウンして上位のアプリケーション、ホスト、VLAN、DSCP、アプリケーション応答時間を調べるために使用できます。

ダッシュボードの各チャートからコンテキスト メニューにアクセスすれば、さらにドリルダウンして、アプリケーション、ホスト、カンバセーション、VLAN トラフィックに関する詳細など、さまざまなデータを分析できます。

図 7-3 は、上位 N のアプリケーションに関するチャートおよび上位 N のホストに関するチャートから、コンテキスト メニューを使ってドリルダウンする場面を表したものです。

図 7-3　アプリケーションおよびホストのドリルダウン



NAM とサードパーティ レポート ツールの統合

CA NetQoS SuperAgent には、アプリケーションの応答時間を集約する目的で、Prime NAM が統合されています。また Prime NAM は、ホスト、カンバセーション、RTP、および応答時間を集約できるよう、CompuWare Vantage および InfoVista 5View にも統合されています。

API（アプリケーション プログラミング インタフェース）とも呼ばれる NAM ノースバウンド インターフェイスの詳細を確認するには、『*NAM API Programmer's Guide*』についてシスコの営業担当者にお問い合わせください。API を使用すると、**Prime NAM** をプロビジョニングしたり、パフォーマンス データを抽出したりできます。

Prime NAM ノースバウンド API を使用して独自のスクリプトを作成することができますが、GUI の設定が必要です。

「[Response Time Summary] の使用方法」を参照してください。

NAM と LMS の統合

NAM GUI は、LMS（LAN 管理スイート）4.0 のダッシュボード上に配置することが可能で、LMS のグラフィカル ユーザ インターフェイスからアクセスできます。LMS については、http://www.cisco.com にある技術マニュアルを参照してください。

現在、この機能には次のような特長があります。

- LMS により構成されたネットワーク トポロジの一部として NAM を検出できる
- LMS に特化した NAM アラームを使用できる
- 複数の NAM に対しソフトウェアを LMS 経由で容易にアップデートできる
- ポータル レベルでの統合により、NAM GUI を LMS 内に組み込むことができる

また、LMS でサポートされているデバイスを確認することにより、FCAPS のどの機能がどのタイプの NAM で使用できるのかを判断することができます。

http://www.cisco.com/en/US/partner/products/ps11200/products_device_support_tables_list.html

ブランチでの可視化

ブランチで可視化する方法には次の 3 つの選択肢があります。

1. Cisco Integrated Service Router Generation 1 で稼働する専用の NME-NAM-120S を使用する。
2. Cisco Integrated Service Router Generation 2 環境の SM SRE 7xx または SM SRE 9xx で稼働している、アプリケーションとしての NAM。
3. ISR G2 で使用可能な Cisco IOS 機能の 1 つであり、アプリケーションの応答やトラフィックについての統計情報をカプセル化するパフォーマンス エージェント（PA）を使用する。基盤となる Netflow v9 は、データセンター（DC）またはキャンパスの中央の NAM にエクスポートできます。PA は WAAS Express（同じく IOS 機能の 1 つ）を補完する役割があり、これらを併用することで WAN 最適化の前後におけるエンドツーエンドの可視化が実現します。従来の方法でブランチに WAAS を導入していた場合は、トラフィックの送信元を 2 つ（NetFlow と WAAS フロー エージェント）使用していたのに対して、ここで使用するトラフィックの送信元は 1 つだけです。シナリオ「Cisco WAAS のモニタリングとその影響の測定」（P.8）を参照してください。

これらの選択肢のうち最初の 2 つには大きな違いはありません。いずれを選択した場合でも、ローカル ブランチの可視化およびブランチ間の可視化を実現できるほか、ブランチを出入りするすべてのトラフィックをキャプチャできます。

これらのブランチ NAM モジュールは、リモート サイトの数が少ない環境に導入するか、または強化された 1 つのブランチに導入するのが適切です。3 番めの選択肢を選んだ場合、実現されるのはローカル ブランチの可視化のみですが、複数のリモート サイト（たとえば 100 箇所 /1000 箇所規模のリモート サイト）に NAM モジュールを導入した場合よりもスケーラブルです。ネットワークのモニタリングおよびトラブルシューティングに関する要件によっては、強化されたブランチには NAM モジュールおよび PA を導入し小規模のブランチには PA を導入するなど、異なる選択肢を併用するという方法も考えられます。このモデルでは、DC にある中央 NAM により、DC からブランチへのエンドツーエンドの可視化が実現されているほか、スーパー ブランチ（強化されたブランチ）においてブランチ間のトラフィックをキャプチャすることができるようになっています。

NME-NAM-120S または SM-SRE に NAM を設置する詳しい方法については、Cisco.com にあるインストレーション ガイドを参照してください。PA を設定する詳しい方法については、第 3 章「Cisco Prime NAM のセットアップ」を参照してください。リリースの詳細については、www.cisco.com にある『*Cisco Prime Release Notes*』を参照してください。

Cisco WAAS のモニタリングとその影響の測定

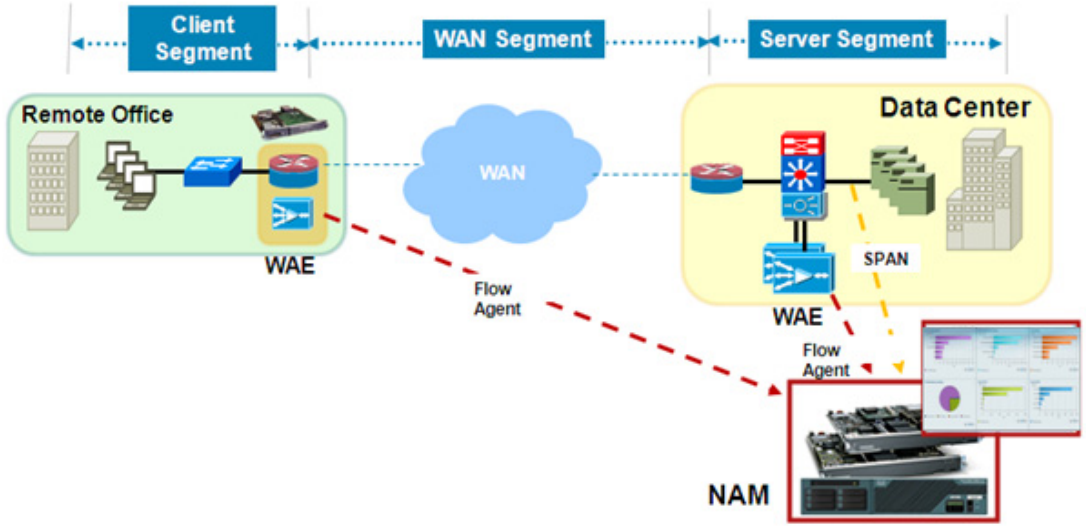
Cisco Wide Area Application Services（WAAS）は包括的な WAN 最適化ソリューションで、WAN 経由でのアプリケーションの高速化、ブランチ オフィスへのビデオ配信、およびブランチ オフィスにおける IT サービスのローカル ホスティングを行うことができます。IT 部門では、Cisco WAAS を使用することにより、LAN と同様のアプリケーション パフォーマンスを維持しながらアプリケーションやストレージをデータセンターに一元化することができるほか、ブランチ オフィスにおけるデバイスの設置面積を減らしつつローカルにホストされた IT サービスを提供することができます。

WAAS を導入する IT 担当者にとって、WAN の最適化がもたらすメリットを数値的に測定しそれをレポートすることは、課せられた使命の 1 つです。もし正確な測定が可能であればその効果は大きく、投資回収率を示すことや、ソリューションに元々期待されていた改善の成果が実際に達成されているかどうかを評価することなどが可能となり、結果的に導入を拡大する際には、情報のモニタリング、トラブルシューティング、およびプランニング用として引き続き WAAS を使用できるようにもなります。

NAM では、データ ソースとして WAE デバイスまたはパフォーマンス エージェント（PA）を使用することにより、WAAS 用に最適化されたフローをモニタできます。この機能を使用すれば、NAM では、WAAS によって作成されるブランチ、WAN、データセンターという 3 つの異なるセグメントについて最適化関連のメトリックを可視化できます。

WAAS を導入するに際しては、Cisco NAM アプライアンスまたは NAM-2X ブレードをデータセンターのエッジに配置することが推奨されます。NAM では、ネットワーク内のこの場所から、SPAN テクノロジーを使用してローカル メトリックを測定することができます。リモート ブランチ セグメントに関する情報については、フロー エージェントによりリモート WAE デバイスからエクスポートされたデータ、または ISR G2 ブランチ ルータの PA および WAAS Express に基づいて測定されます。NME-NAM が使用できる場合は、リモート ブランチ サイトに NME-NAM を導入すると非常に有効です。この NME-NAM により、サイトにおける WAAS が有効になる前のユーザ エクスペリエンスを実現することが可能で、WAAS が有効になった後のユーザ エクスペリエンスとそれを比較できます。図 7-4 を参照してください。

図 7-4　複数のデータ ソースに基づいた Cisco NAM による分析



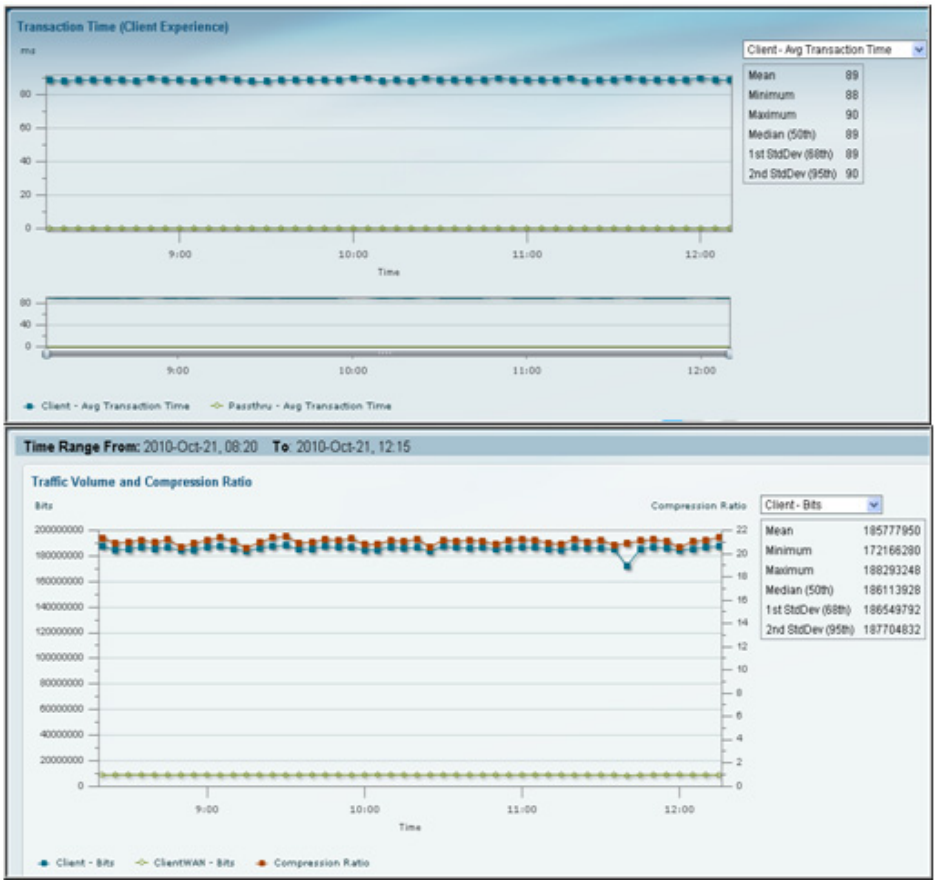
このソリューションを導入する手順は次のとおりです。

ステップ 1　データセンターに導入された NAM 2x20 から、[Analyze] > [WAN Optimization] > [Top Talker Detail] を選択して、WAAS が有効になる前のアプリケーションの応答時間を測定します。トップ トーカー表示には、最適化のための可能な候補である上位のアプリケーション、ネットワーク リンク、クライアント、およびサーバの使用率、同時接続および平均トランザクション時間などのデータが含まれます。

ステップ 2　DC およびブランチの WAE からの WAAS フローについて、WAAS クライアント サイドおよび WAAS サーバ サイドを定義します。

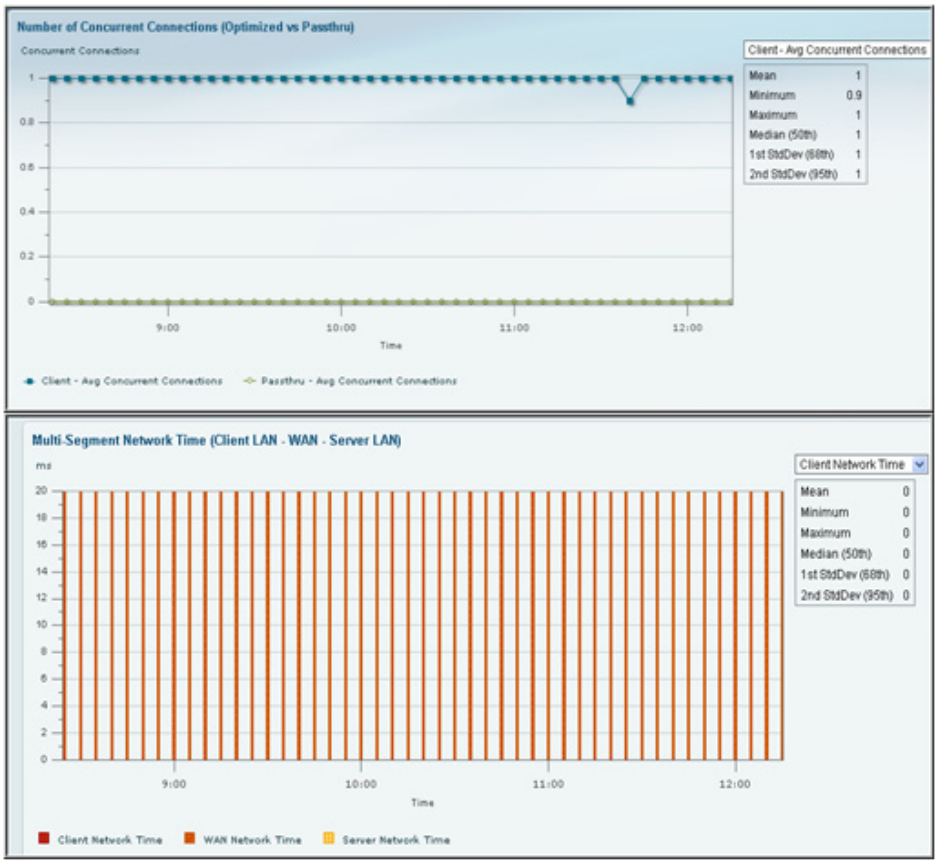
ステップ 3　NAM のインタラクティブ ダッシュボードを使用して、分析されたデータを表示します。図 7-5 に表示されているのは、[Client Transaction Time]、[Traffic Volume and Compression Ratio]、[Number of Concurrent Connections (Optimized vs.Passthru)]、[Multi-Segment Network Time (Client LAN - WAN - Server LAN)] の各画面です。最初のグラフからわかるように、最適化されていないトラフィックはすべて、[Passthru] として表示されます。

図 7-5　アプリケーションのパフォーマンス分析（最適化後）



上記のスクリーン ショットからは、WAAS が有効になるとブランチにおけるユーザ エクスペリエンスが大幅に改善される様子がわかります。こうしたレポートは、WAN の最適化テクノロジーへの投資が妥当であることを示し、従業員の生産性向上やリモート サイトからのユーザ エクスペリエンスの改善という観点で見た場合の投資回収率を明示するうえで非常に有効です。

図 7-6



ステップ 4　データセンターに配置された NAM から見た場合、応答時間の測定に対する情報のソースは 2 つあります。SPAN からはデータセンターでの測定値およびブランチからのエクスポート データを取得できます。一方、WAAS フローまたは PA からはブランチでの測定値を取得できます。データセンターの NAM では、これら 2 つの情報ソースを使用することにより、各ブランチについての現在の応答時間を継続的にモニタすることが可能であり、これを利用すれば IT 担当者はユーザ エクスペリエンスを適切な範囲に維持することができます。正常とは異なる応答時間が検出された場合は、問題のトラブルシューティングに関する情報を伝えるためのアラートが適切な担当者に送信されるよう NAM を設定することができます。

（注）　上記のシナリオにおいて、NAM 2x20 を WAVE-574 および WAE-674 上の NAM 仮想ブレードに置き換えても、同じタイプのレポートを取得できます。

モニタリング

- 「トラフィックのリアルタイム モニタリングとリアルタイム分析」（P.12）
- 「NAM を使用した QoS/DiffServ（DSCP）のモニタリング」（P.14）
- 「NAM による履歴傾向分析（[Interactive Report] から実行）」（P.18）

- 「TCP インタラクティブ アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「UDP リアルタイム アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価」（P.21）
- 「Nexus 1000V スイッチ環境のモニタリング」（P.21）

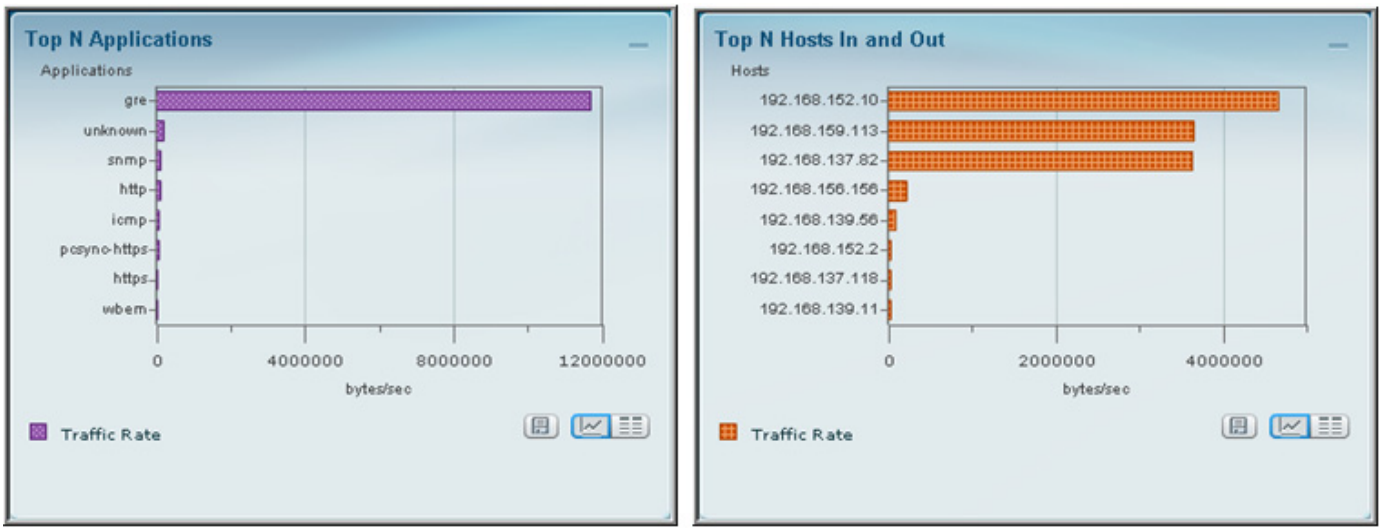
トラフィックのリアルタイム モニタリングとリアルタイム分析

ネットワーク オペレーション センター（NOC）には、キャンパス ネットワークおよび 2 つのブランチ オフィスをモニタし、それらのネットワーク内で検出された異常を追跡するという役割があります。

次に説明するのは、キャンパス エッジの Cisco Catalyst 6500 シリーズ スイッチに配置された NAM-2 ブレードを管理する手順です。ローカル SPAN およびリモート NetFlow トラフィックが、この NAM によってモニタリングされています。ここでは、これらのデータ ソースに基づいて複数のサイトがすでに定義されているとします。

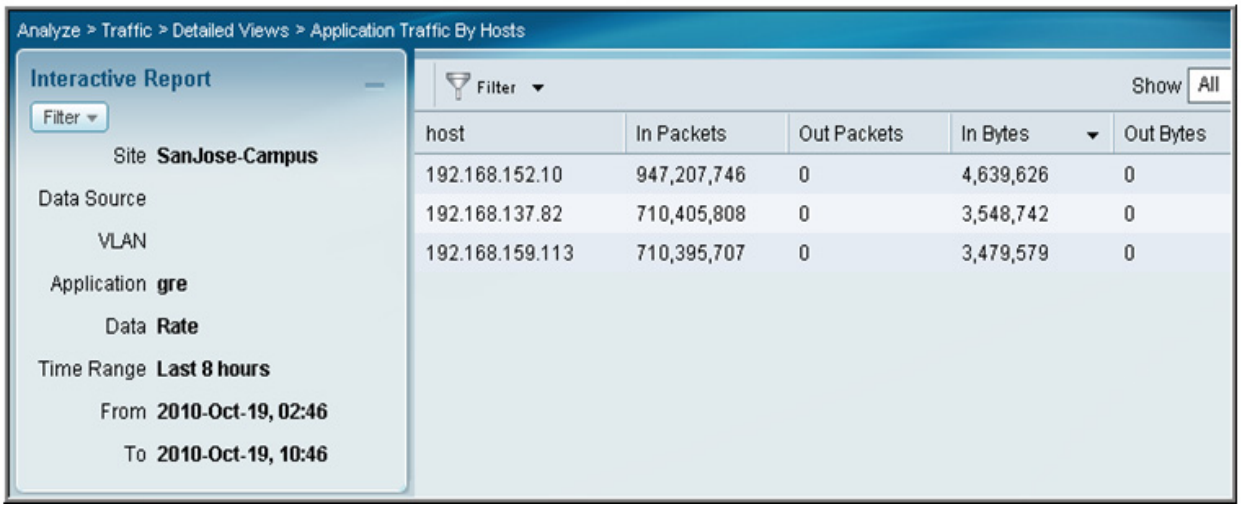
ステップ 1　[Traffic Summary] ダッシュボード（[Monitor] > [Overview] > [Traffic Summary]）で、画面の左側にある [Interactive Report] および [Filter] ボタンを使用して、特定サイトに関するデータのみをダッシュボード上に表示します。これにより、そのサイトに関する上位のアプリケーション、ホスト、VLAN、および DSCP を確認できます。ここでは、帯域幅を決定する最上位のホストに注目します（図 7-7 を参照）。

図 7-7　上位のアプリケーションおよびホスト



ステップ 2　上位のアプリケーションに関するグラフをクリックし、GRE アプリケーションを使用するすべてのホストが表示されるようにドリルダウンします。このアプリケーションのトラフィックは、3 つのホストによって生成されているのがわかります（図 7-8 を参照）。

図 7-8　アプリケーションのトラフィックに関する統計情報（ホスト別）



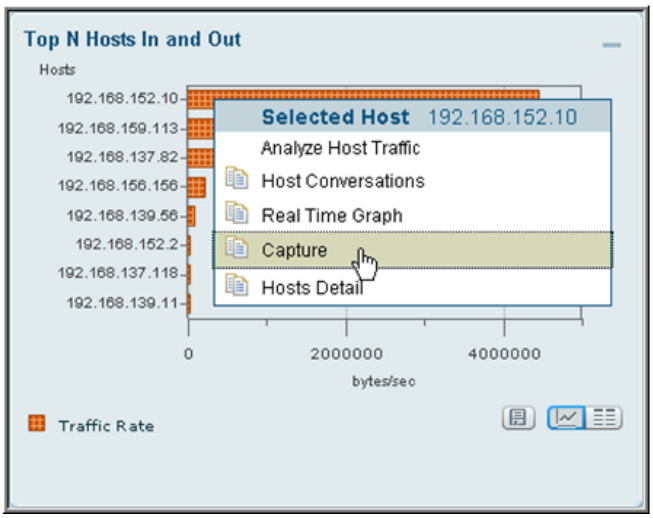
ステップ 3　[Top N Hosts In and Out] に戻り（[Traffic Summary] > [Top N Hosts In and Out]）、ホストをクリックします（図 7-8 の例では「192.168.152.10」）。

ステップ 4　[Analyze] > [Traffic] > [Host] を選択し、このホストおよびアプリケーションによってこのトラフィックが生成されてきた期間を確認します。[Time Range] の値は、左側の [Interactive Report] および [Filter] ボタンを使用して変更することができます。パターンや傾向を把握するためには、期間を短縮または拡大することが必要な場合もあります。

図 7-9　アプリケーションのトラフィックに関する統計情報（ホスト別）

ステップ 5　電子メールによるアラート、トラップ、および syslog に対しては、これらのパターンを基にしてしきい値を設定することができます。アラートは、パケット キャプチャを開始する際にも使用できます。必要に応じて、コンテキスト メニュー（色が付いたバーをクリックすると表示される）からパケット キャプチャを開始するためのオプションを選択することもできます（図 7-10 を参照）。

図 7-10　ワンクリックによるパケット キャプチャ



NAM はキャンパス エッジに導入されていますが、その他コア、ディストリビューション（NAM-2X またはアプライアンス）、ブランチ オフィス（NME-NAM）などの場所に導入した場合でも、同様の情報が得られます。

この使用例からは、リアルタイム分析が持ついくつかの長所を知ることができます。アプリケーションおよびカンバセーションをリアルタイムに分析できるだけでなく、目的のストリームをキャプチャすることもできます。

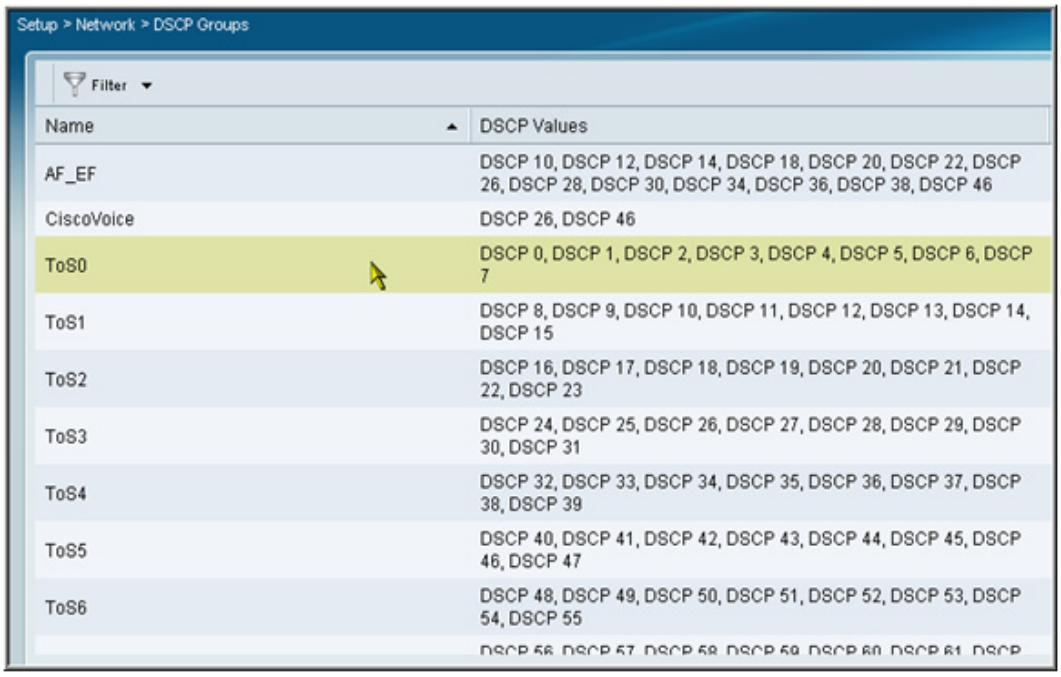
NAM を使用した QoS/DiffServ（DSCP）のモニタリング

DiffServ では、QoS によってトラフィックがどのように分類されているかを確認できるほか、マーキングが正しくないトラフィックや不正トラフィックを検出することもできます。NAM では、タイプ オブ サービス（ToS）のビット設定に基づいて、アプリケーション/プロトコルが識別されます。管理者は、DSCP グループを設定することも、用意されている DSCP グループを使用することもできます（図 7-11 を参照）。音声テンプレートを使用すると、音声トラフィックが正しくマーキングされているかどうかをモニタすることができます。図 7-13 には、すべての DSCP 値に対する DiffServ アプリケーションの統計情報が表示されています。これを見ると、リスト内に RTP および Session Initiation Protocol（SIP）が表示されているのがわかります。これは、この 2 つがそれぞれのパス全体を通じて正しくマーキングされていないことを示しています。

以下のシナリオでは、QoS が導入されています。これにより、VoIP トラフィックが優先されるため、ネットワーク全体の音声品質が向上します。NAM は、データセンターおよびブランチに導入されており、DSCP をモニタし QoS ポリシーを検証するのに利用されています。

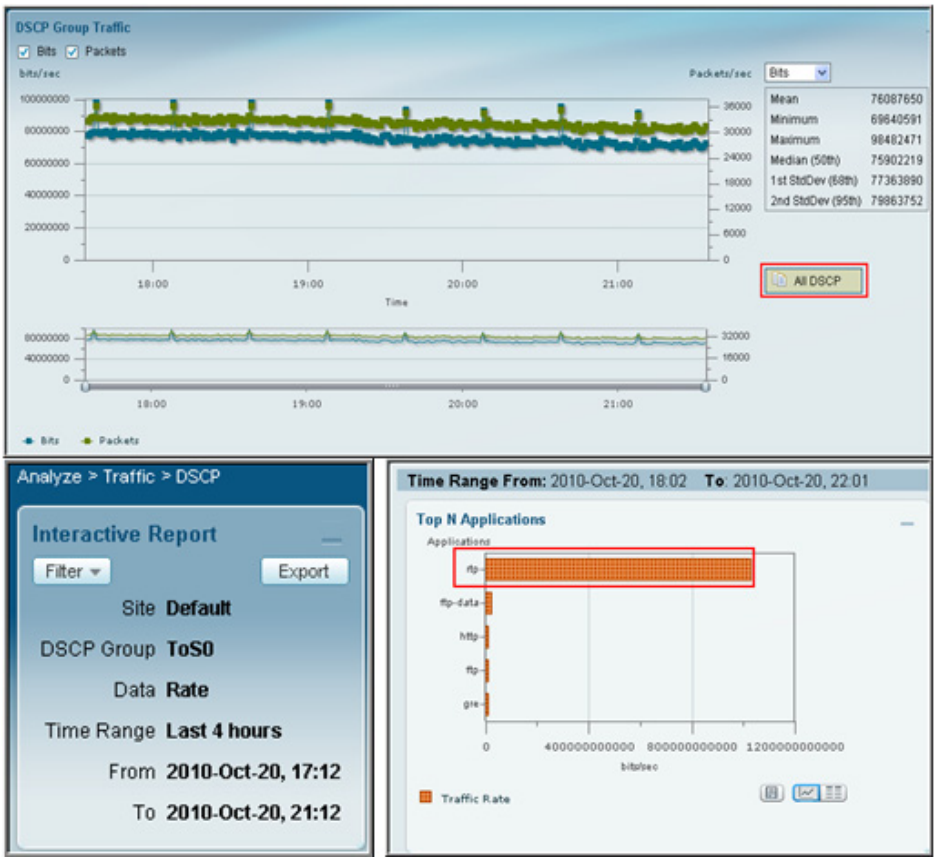
ステップ 1　[Setup] > [Media] > [DSCP Groups] を選択して、デフォルトのグループを表示します。

図 7-11　デフォルトの DSCP グループ



ステップ 2　[Analyze] > [Traffic] > [DSCP] を選択して、分類に誤りがあるトラフィックを検索します。図 7-12 では、RTP プロトコルが ToS0 に分類されているのがわかります。

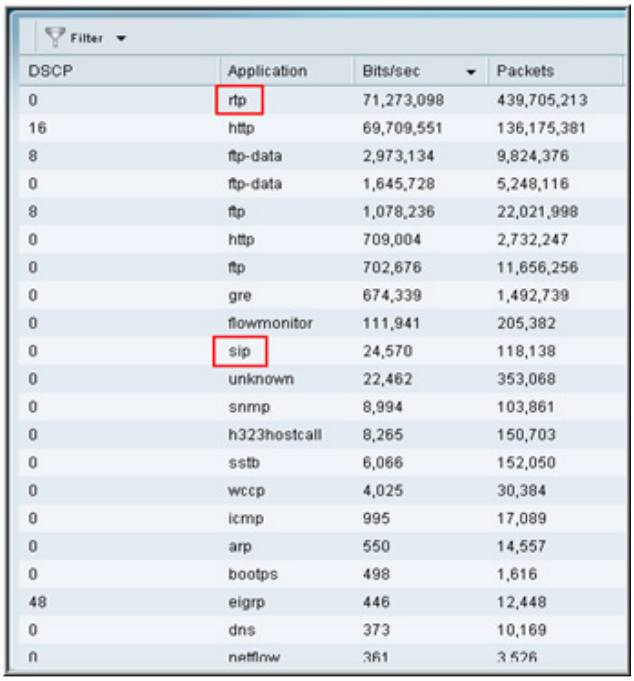
図 7-12　DSCP グループ：ToS0



ステップ 3　[**All DSCP**] ボタンをクリックして、すべての DSCP およびアプリケーションを表示します。

ステップ 4　図 7-13 では、RTP と SIP が枠で囲まれています。これらのプロトコルは DSCP 0 に分類されていますが、音声トラフィックに関する標準的な分類は DSCP 46 および DSCP 24 であるため、DSCP 0 という分類は正しくありません。これは、音声トラフィックが一部、ネットワーク上で誤って分類されていることを示しています。またブランチ NAM を表示することで、音声トラフィックの分類が誤っていないかどうかを検証することもできます。

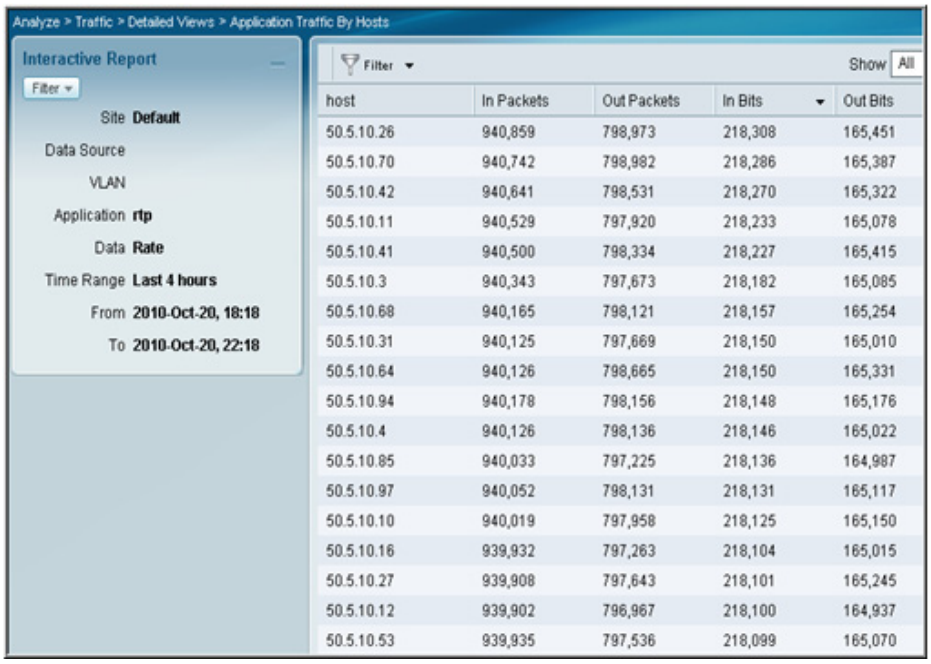
図 7-13　全 DSCP テーブル


Filter

DSCP	Application	Bits/sec	Packets
0	rtp	71,273,098	439,705,213
16	http	69,709,551	136,175,381
8	ftp-data	2,973,134	9,824,376
0	ftp-data	1,645,728	5,248,116
8	ftp	1,078,236	22,021,998
0	http	709,004	2,732,247
0	ftp	702,676	11,656,256
0	gre	674,339	1,492,739
0	flowmonitor	111,941	205,382
0	sip	24,570	118,138
0	unknown	22,462	353,068
0	snmp	8,994	103,861
0	h323hostcall	8,265	150,703
0	sstb	6,066	152,050
0	wccp	4,025	30,384
0	icmp	995	17,089
0	arp	550	14,557
0	bootps	498	1,616
48	eigrp	446	12,448
0	dns	373	10,169
0	netflow	361	3,526

ステップ 5　RTP のグラフをクリックし、[Application Traffic by Host] を選択して、これらのプロトコルを使用するクライアントを表示します。これにより、これらのクライアントからの RTP トラフィックまたは SIP トラフィックが正しくマーキングされていない原因について、トラブルシューティングを行うことができます。図 7-14 に示したように、NAM にはこれらのプロトコルを使用する電話の IP アドレスが表示されます。これにより、クライアント間のルータおよびスイッチに実装されている QoS ポリシーを確認することができます。

図 7-14　RTP ホスト テーブル



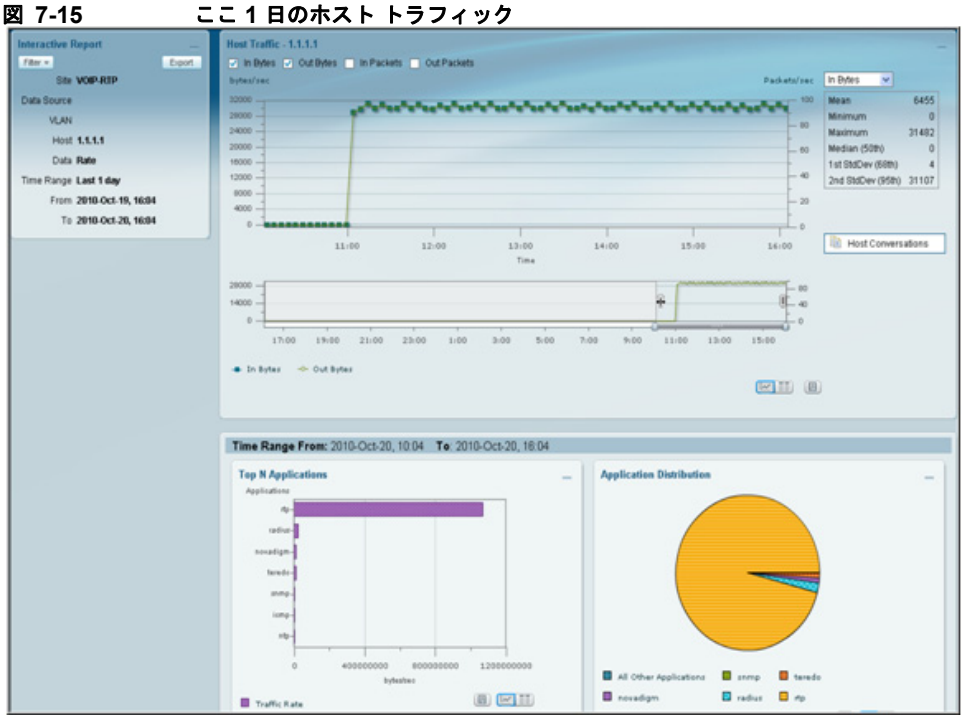
NAM による履歴傾向分析（[Interactive Report] から実行）

履歴傾向分析は、ネットワークのパフォーマンス管理における重要な要素です。リアルタイム分析ではイベントに関する情報を把握できますが、履歴傾向分析ではイベントが時系列で可視化されます。この時系列により、ネットワーク トラフィックの挙動の変化、異常な動作、ピーク時および閑散時におけるネットワークの使用率など、ネットワークのさまざまな側面について有益な情報を把握することができます。また、将来におけるネットワークのアップグレード、アプリケーションの導入、ハードウェアの増設などを計画する場合にも有用です。NAM の履歴傾向分析機能については、注意すべき点がいくつかあります。

- [Interactive Report] > [**Filter**] ボタン（NAM ウィンドウの左側にある）をクリックし、[Time Range] の値を変更することにより、短期の傾向を見ることも長期の傾向を見ることもできます。インタラクティブ レポートはエクスポートすることができるほか、この先必要なとき即座に参照できるようにフィルタ設定を保存することもできます。エクスポートされたデータは、電子メールを介して CSV 形式または PDF 形式で送信することができます。

- 図 7-15 には、ここ 1 日のホスト トラフィックが表示されています。中央のグラフから 10:00 ～ 16:00 の時間帯に相当する部分を拡大することで、このホストで使用されているその他のアプリケーションを確認することができます。

図 7-15　ここ 1 日のホスト トラフィック

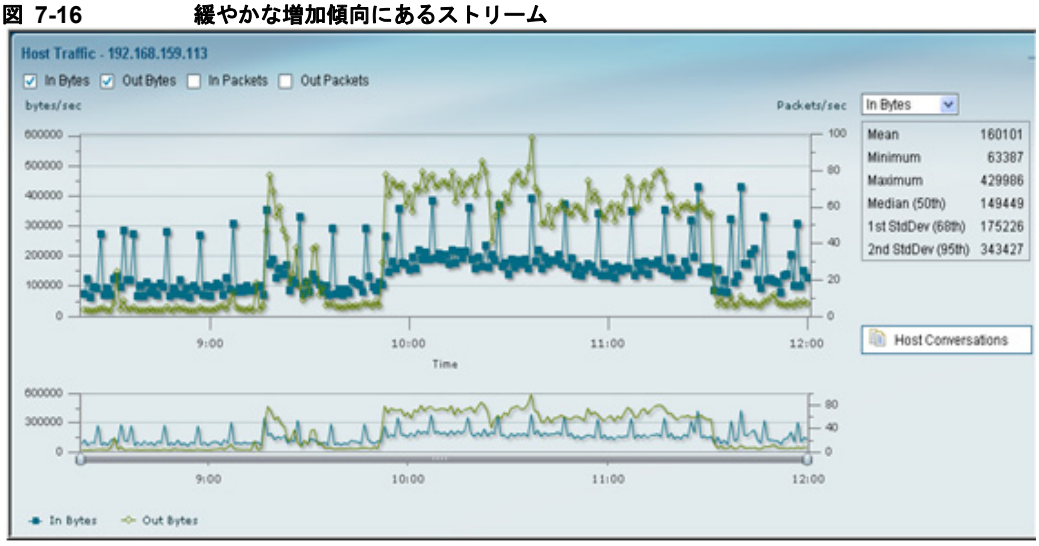


以下の導入シナリオでは、6 ヵ月以内に増設される新しいブランチに必要な容量を予測するため、規模がほぼ同じ既存のブランチ オフィスの使用率を分析します。既存のブランチにあるブランチ ルータ（ISR）に NME-NAM を導入する手順は次のとおりです。

ステップ 1　ブランチとデータセンターの間におけるトラフィック レートのキャプチャを開始します。[Interactive Report] > [Filter] > [Time Range] > [Custom] を選択（月を指定するための日付を入力）して、前月のトラフィックを表示します。

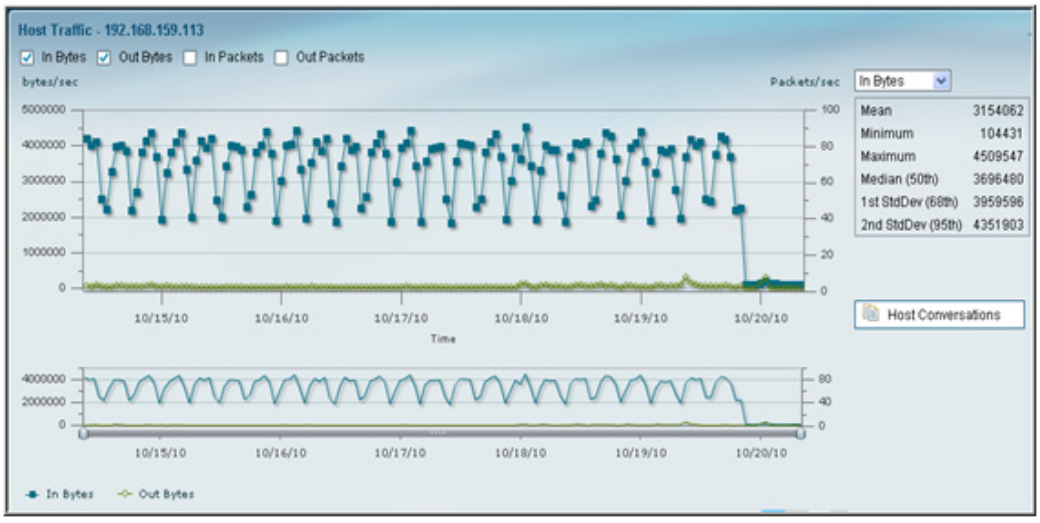
ステップ 2　今日のカンバセーション レポートを開き、緩やかな増加傾向にはあるもののその増加率を確認することができないようなストリームを見つけます（図 7-16 を参照）。

図 7-16　緩やかな増加傾向にあるストリーム



ステップ 3　[Interactive Report] で [Time Range] の値を動的に変更し、1 ヵ月という粒度での傾向を分析します。このパターンからは周期的な増加が認められますが、極大値はいずれも 4.5 KBps と 5.x KBps との間に留まっています（図 7-17 を参照）。このことから、新しいサイトで必要となる ISP リンクは従来とほぼ同じものであり、標準の T1 回線であれば新しいリモート オフィスに必要なレベルを十分満たしていると結論付けることができます。

図 7-17　1 ヵ月という粒度で表示された傾向



履歴傾向分析は、ネットワークの計画やベースライン化を進めるうえで有効な予備作業です。たとえば、ビジネスに不可欠なアプリケーションやサーバをモニタしその傾向を分析すれば、これらの傾向からは、日常的に行われるさまざま意思決定にとって有用な情報を得ることができます。

TCP インタラクティブ アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価

アプリケーション パフォーマンスの応答時間分析には、最大で 45 個のメトリックが使用されます。これらのうち多数のメトリックを基にしてしきい値を設定することが可能で、それらのしきい値を超過した場合はアラートが送信されるようにすることもできます。重要なアプリケーションやサーバに対しては、[Average Server Response Time]、[Average Transaction Time]、または [Average Network Time] と [Average Server Network Time] を使用して、しきい値を設定することが推奨されます。これらのしきい値を使用すると、アプリケーション パフォーマンスに関する問題点の所在を特定できるほか、その問題点がサーバにあるのかネットワークにあるのかを明確にすることができます。アラームに従って NAM にアクセスすると、サーバへアクセスしているアプリケーションおよびクライアントを表示できるほか、デバイスおよびインターフェイスの使用率をモニタしているトラフィック パスのデバイスを確認することもできます。

「アプリケーション応答時間」（P.22）を参照してください。

「しきい値の定義」（P.44）を参照してください。

UDP リアルタイム アプリケーションを対象とした NAM によるアプリケーションレベルでのパフォーマンス モニタリングの評価

NAM では RTP ストリームがモニタされます。電話コールが終了すると、エンドポイントではその情報の計算が行われた後、コール マネージャに送信されます。そのパス上に NAM があれば、送信された情報はその NAM によって傍受されます。

NAM では、RTP ストリームのほか、エンドポイントから送信されたボイスコール統計情報のモニタリングおよび分析が行われます。エンドポイントから送信されたボイスコール統計情報と RTP ストリームとに基づいて、電話番号とエンドポイントの IP アドレスとが関連付けられます。MOS、ジッター、およびパケット損失については、RTP ストリームの分析に基づいてアラートが送信されます。

「音声 Signaling/RTP ストリーム モニタリング」（P.5）を参照してください。

「トラフィックの分析」（P.7）、「RTP Streams」（P.37）を参照してください。

表 3-40、「[Voice Monitor Setup] ウィンドウ」を参照してください。

Nexus 1000V スイッチ環境のモニタリング

ネットワークやアプリケーションが仮想化環境へ移行すると、その環境内部の詳しい情報を取得するための手段を確保することが課題となります。NAM VSB は、Cisco Nexus 1010 仮想化アプライアンスと統合することにより、そうした手段として使用することできます。NAM VSB を使用すると、仮想スイッチング レイヤの動作を可視化できるほか、仮想マシン（VM）を監視して VM についての統計情報を取得することができます。図 7-18 を参照してください。

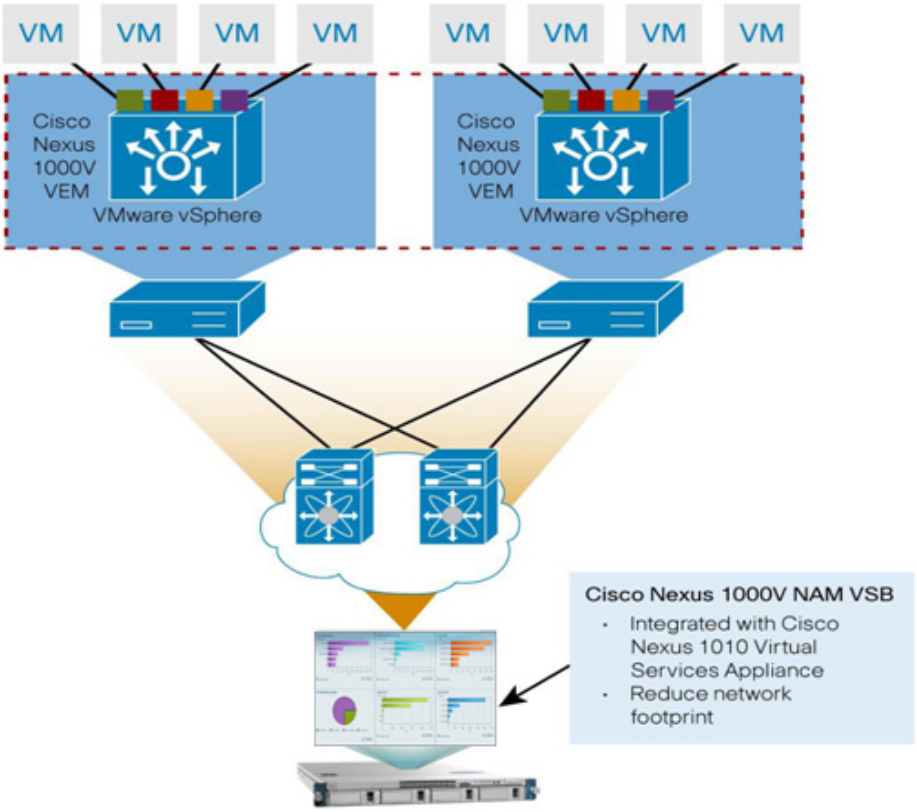
Nexus 1000V スイッチを、Prime NAM ソフトウェアが実行されている他の NAM プラットフォームによりモニタすることもできます。

このシナリオでは、次の 2 つの選択肢があります。

- アプリケーションを仮想化環境に配置し、Nexus 1000V スイッチによりネットワーク接続を実現する。この環境のモニタリングには、Nexus 1010 仮想サービス アプライアンス上にインストールした NAM VSB を使用する。
- NAM-2 をデータセンターに導入し、仮想化環境用として Nexus 1000V スイッチを使用して、仮想スイッチ トラフィックをモニタする。

（注）　Nexus 1000V スイッチおよび NAM がすでにネットワーク内に導入されている場合は、そのいずれかの NAM により ERSPAN データ ソースまたは NetFlow データ ソースを指定することができます。1000V スイッチと NAM は、同一の物理スイッチに直接接続する必要があります。

図 7-18　Cisco Nexus 1000V NAM 仮想サービス ブレードの導入



Nexus 1000V 環境をモニタする手順は次のとおりです。

ステップ 1　Nexus 1010 仮想サービス アプライアンス上に NAM VSB をインストールして設定するか、または NAM-2 に対し Nexus スイッチをインストールして設定します。Cisco.com にある NAM の設置および設定に関するガイドを参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html

ステップ 2　NAM VSB の場合：

1. NAM にデータを提供する Cisco 1000V スイッチ仮想スーパーバイザ モジュール（VSM）上で ERSPAN または NetFlow が設定されていることを確認します。
2. NAM に応じて、ERSPAN データ ソースまたは NetFlow データ ソースを設定します。
3. ERSPAN および NetFlow に対し、NAM で適用可能なすべてのモニタリング パラメータを有効にします。図 7-19 は、アプリケーション、ホスト、プロトコル、サーバの応答時間などについて上位 N の情報が表示される [Traffic Summary] ウィンドウです。ナビゲーション操作により、リストに表示されているカテゴリごとに詳細情報を表示することができます。

4. ウィンドウの左側にある [Interactive Report] を使用して、アプリケーションの応答時間、ホスト、およびカンバセーション トラフィック パターンの傾向分析に関するレポートを設定します。

図 7-19　NAM モニタ（全体）

5. 物理インターフェイスおよび仮想インターフェイスについてのテーブルには、VM 間のトラフィックに関する使用率が表示されます（図 7-20）。各仮想インターフェイスが接続する VM はただ 1 つであるため、このデータを見れば、いずれの VM がスイッチ リソースを使用しているのかを知ることができます。さらに、ホストおよびカンバセーションについてのテーブルでは、リソースが使用されている要因を特定することができます。

図 7-20　NAM モニタ（管理対象デバイスのインターフェイス）

Interfaces Statistics

Filter

Interface	In % Utilization	Out % Utilizati	In Packets/s	Out Packets/s	In Bytes/s	Out Bytes/s	In Non-Unicas	Out Non-Unicast/	In Discards/s	Out Discards/s
Vethernet16	0	0	4,295.15	0.11	283,736.22	10.14	0.00	0.11	0	0
Ethernet4/2	0	0	1,412.16	4.72	85,597.59	1,238.02	1.65	0.02	0.13	0
port-channel2	0	0	1,412.15	4.73	85,597.19	1,238.45	1.64	0.02	0.13	0
Ethernet3/2	0	0	1,227.22	188.72	74,142.62	12,131.28	1.52	0.02	0	0
port-channel1	0	0	1,227.21	188.72	74,142.49	12,131.64	1.52	0.02	0	0
Vethernet4	0	0	479.77	0.19	76,942.69	18.86	0	0.11	0	0
Ethernet5/2	0	0	190.93	1,226.46	11,961.08	74,595.41	1.52	0.02	0	0
port-channel3	0	0	190.93	1,226.44	11,959.96	74,593.44	1.52	0.02	0	0
mgmt0	0	0	5.47	2.22	0	442.07	0	0	0	0
Vethernet17	0	0	0.50	1.80	189.53	577.32	0.01	1.30	0	0

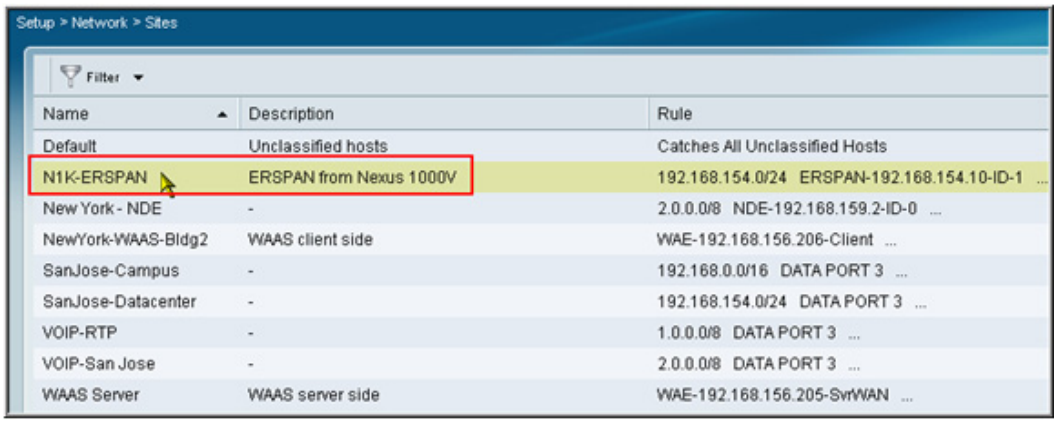
（注） NAM VSB により、機能はほぼ同様に補完されます。ただし、NAM VSB では、ERSPAN データ ソースと NetFlow データ ソース以外のデータ ソースはサポートされておらず、音声モニタリングおよびパケット キャプチャは実行されません。

ステップ 3　他の NAM プラットフォーム（NAM-2X）の場合：

1. NAM-2X に対して ERSPAN または NetFlow が指定されるように Nexus 1000V スイッチを設定します。

2. [Setup] > [Traffic] > [NAM Data Sources] を選択して、NAM にデータを提供する Cisco 1000V スイッチ仮想スーパーバイザ モジュール（VSM）上で ERSPAN または NetFlow が設定されていることを確認します。
3. [Setup] > [Network] > [Sites] を選択して、このデータ ソースのサイトを作成します（図 7-21）。

図 7-21　NAM サイト



4. [Monitor] > [Overview] > [Traffic Summary]（図 7-22）、および [Monitor] > [Overview] > [Response Time Summary] を選択します。

図 7-22　Nexus 1000V トラフィックの概要

トラブルシューティング

- 「NAM による問題の特定」（P.25）
- 「NAM によるスマート グリッドの可視化」（P.25）
- 「トラフィックのリアルタイム モニタリングとリアルタイム分析」（P.12）

NAM による問題の特定

アラームの詳細情報（Cisco Prime ネットワーク解析モジュール ソフトウェア から **[Monitor] > [Overview] > [Alarm Summary]** を選択すると表示される）を使用すると、違反のあったしきい値についてドリルダウンすることができます。またこのアラームを電子メールで受信することもできます（[Setup] > [Alarms] > [E-mail]）。次に示すのはアラームの具体例です。

```
2010 SEPT 28 9:17:0:Application:Exceeded rising value(1000);packets;60653;Site(San Jose),
Application(http)
```

このアラームを受信した場合は、NAM GUI にアクセスして、San Jose サイトのアプリケーションを表示し、しきい値を超えるような値の上昇が発生した原因を特定します。まず [Analyze] > [Traffic] > [Application] をクリックします。左側にある [Interactive Report] ウィンドウで、[Site] の値を「San Jose」、[Application] の値を「HTTP」、[Time Range] の値を、アラートを受信したときの期間にそれぞれ変更します。これにより、このプロトコルを使用しているすべてのホストが表示されます。上位のホストを表示し、このアプリケーションにアクセスしている不正なホストがないかどうかを確認します。[Analyze] > [Traffic] > [Host] を選択すると、やり取りの多いカンバセーション（したがってこのアプリケーションに対するトラフィックが増加する原因となるカンバセーション）を表示することができます。

アラームがアプリケーションの応答時間に関するものである場合は、[Monitor] > [Response Time Summary] または [Analyze] > [Response Time] > [Application] を選択すれば、このアプリケーションにアクセスしているホストについてドリルダウンすることができます。アプリケーション サーバを特定し、ホストされているその他のアプリケーションおよびそのサーバにアクセスしているすべてのクライアントを表示します。

[Monitor] 下の「[Response Time Summary] の使用方法」（P.3）を参照してください。

[Analyze] 下の「応答時間の測定」（P.18）を参照してください。

NAM によるスマート グリッドの可視化

NAM は、IEC 60870 プロトコル（電力会社で使用される主要プロトコルの 1 つ）をそのまま認識することはできません。NAM は 1 つの専用ポートとして使用されるため、カスタムのプロトコルを追加する必要があります。[Setup] > [Classification] > [Application Configuration] を選択すると、そのアプリケーションを使用しているすべてのホストが表示されます。NAM は Telnet アプリケーションと見なされます。