CHAPTER 1

# 概要

この章では、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの Network Analysis Module（NAM）と、その動作および管理方法について説明します。

（注） このインストレーション コンフィギュレーション ノートは、Cisco IOS ソフトウェアを所有しているユーザを対象としています。

この章で説明する内容は、次のとおりです。



## NAM の動作について

ここでは、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの Network Analysis Module（NAM）の動作について説明します。この項の構成は、次のとおりです。



NAM は NetFlow を分析および表示し、NetFlow バージョン 9 のレコードをサポートしています。NetFlow のリスニング モードでは現在、NetFlow バージョン 9 を使用したデータ ソースが表示されます。

NAM はまた、個々のイーサネット VLAN をモニタリングすることもできます。これにより、Catalyst 6500 シリーズ スーパーバイザ エンジンで提供されるサポートに対する拡張として機能できるようになります。

IETF に準拠したその他の任意のアプリケーションを使用して、キャパシティ計画、部門アカウンティング、およびリアルタイム アプリケーション プロトコル モニタリングのためのリンク、ホスト、プロトコル、応答時間の統計情報にアクセスできます。また、ネットワークのトラブルシューティングのために、フィルタを使用してバッファをキャプチャすることもできます。

NAM は、次のソースからのイーサネット VLAN トラフィックを分析できます。

- イーサネット、ファスト イーサネット、ギガビット イーサネット、トランク ポート、Fast EtherChannel SPAN または RSPAN 送信元ポート。

  SPAN と RSPAN の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』の「Configuring SPAN, RSPAN, and the Mini Protocol Analyzer」の章を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/span.html

- NetFlow データ エクスポート（NDE）。

  NDE の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/nde.html

表 1-1 に、NAM モニタリングに使用されるトラフィック ソースの概要を示します。

**表 1-1　NAM モニタリングのためのトラフィック ソースの概要**

| トラフィック ソース | LAN | | WAN | |
|---|---|---|---|---|
| | ポート | VLAN | ポート | VLAN |
| VACL キャプチャ | Yes | Yes | Yes | N/A |
| NetFlow データ エクスポート NDE（ローカル） | Yes | Yes | Yes | Yes |
| NetFlow データ エクスポート NDE（リモート） | Yes | Yes | Yes | Yes |
| SPAN | Yes | Yes | No | No |
| ERSPAN | Yes | Yes | No | No |

# NAM で SPAN を使用する方法について

スイッチド ポート アナライザ（SPAN）セッションは、モニタリング対象のネットワーク トラフィックを指定するパラメータで設定された、宛先ポートと一連の送信元ポートとの関連付けです。スイッチド ネットワーク内で複数の SPAN セッションを設定できます。

WS-SVC-NAM-1 プラットフォームには、SPAN セッションのための 1 つの宛先ポートが用意されています。WS-SVC-NAM-2 プラットフォームには、SPAN および VLAN アクセス コントロール リスト（VACL）セッションのための 2 つの可能な宛先ポートが用意されています。NAM への複数の SPAN セッションがサポートされますが、これらのセッションは異なるポートを宛先にする必要があります。SPAN のグラフィカル ユーザ インターフェイス（GUI）で使用される NAM 宛先ポートには、デフォルトで DATA PORT 1 および DATA PORT 2 という名前が付けられます。CLI では、SPAN ポートには表 1-2 に示す名前が付けられます。

**表 1-2　SPAN のポート名**

| モジュール | Cisco IOS ソフトウェア |
|---|---|
| WS-SVC-NAM-1 | データ ポート 1 |
| WS-SVC-NAM-2 | データ ポート 1 およびデータ ポート 2 |

これらの各ポートは独立しています。いずれかのポートからのトラフィックのみ、または両方のポートからのトラフィックが入力されるデータ ポート収集を作成できます。また、このような収集への入力を行う特定の VLAN に一致する、いずれかのポートからのパケットを含む VLAN ベースの収集も引き続き作成できます。

SPAN および Catalyst 6500 シリーズ スイッチ上での設定方法の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/span.html

SPAN および Cisco 7600 シリーズ ルータ上での設定方法の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/span.html

NAM は管理ポート上の Encapsulated Remote SPAN（ERSPAN）トラフィックをサポートしており、そのトラフィックをデータ ソースとして使用します。ERSPAN トラフィックでは、すべての収集タイプがサポートされます。

ERSPAN は SPAN の拡張であり、ここではパケットが総称ルーティング カプセル化（GRE）パケットにカプセル化され、ERSPAN 宛先に送信されます。ERSPAN の送信元と宛先は通常、PFC5 以降のリリースの Supervisor Engine 720 です。ERSPAN トラフィックは、IP または GRE を使用して、ルータ間で送信されるパケットをカプセル化します。その後、カプセル化が解除されたトラフィックは NAM データ ポートに送信することができます。

# NAM で VACL を使用する方法について

VLAN アクセス コントロール リストは、WAN インターフェイスまたは VLAN からのトラフィックを NAM 上のデータ ポートに転送できます。VACL では、SPAN の使用に代わる方法が提供されます。VACL は、IP および IPX プロトコルのレイヤ 3 アドレスに基づくアクセス コントロールを提供できます。サポートされないプロトコルのアクセス コントロールは、MAC アドレス経由で実行されます。MAC VACL は、IP または IPX アドレスのアクセス コントロールには使用できません。

VACL には、次の 2 つのタイプがあります。1 つは、すべてのブリッジまたはルーティングされた VLAN パケットをキャプチャします。もう 1 つは、すべてのブリッジまたはルーティングされた VLAN パケットの選択されたサブセットをキャプチャします。

VACL は、VLAN 内でブリッジされるか、あるいは VLAN または（12.1(13)E 以降のリリースの場合は）WAN インターフェイスとの間でルーティングされたすべてのパケットに対するアクセス コントロールを提供できます。ルータ インターフェイス上でのみ設定され、ルーティングされたパケットにのみ適用される通常の Cisco IOS 標準または拡張 ACL とは異なり、VACL はすべてのパケットに適用できるため、任意の VLAN または WAN インターフェイスに適用できます。VACL はハードウェアで処理されます。

VACL は、Cisco IOS アクセス コントロール リスト（ACL）を使用します。VACL は、ハードウェアでサポートされていない Cisco IOS ACL フィールドをすべて無視します。パケットの分類には、標準および拡張 Cisco IOS ACL が使用されます。分類されたパケットには、アクセス コントロール（セキュリティ）、暗号化、ポリシーベース ルーティングなどのさまざまな機能を適用できます。標準および拡張 Cisco IOS ACL は、ルータ インターフェイス上でのみ設定され、ルーティングされたパケットに適用されます。

VLAN 上で VACL を設定すると、その VLAN に送信されてきた（ルーティングまたはブリッジングされた）すべてのパケットが、VACL チェックの対象になります。パケットは、スイッチ ポート経由で、またはルーティングされた後はルータ ポート経由で VLAN に入ることができます。Cisco IOS ACL とは異なり、VACL は方向（入力または出力）では定義されません。

VACL には、アクセス コントロール エントリ（ACE）の順序リストが設定されています。各 ACE には、パケットの内容に対応する多数のフィールドがあります。各フィールドに、関連するビットを示す関連ビット マスクを指定します。各 ACE は、一致が発生した場合に、システムがそのパケットをどのように処理するかが記述されたアクションに関連付けられています。この動作は、機能によって異なります。Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータは、IP、IPX、および MAC レイヤ トラフィックの 3 つのタイプの ACE をハードウェアでサポートしています。WAN インターフェイスに適用される VACL は、IP トラフィックのみをサポートしています。

VACL を設定して VLAN に適用すると、VLAN に着信するすべてのパケットが、この VACL と照合されます。VACL を VLAN に適用し、ACL を VLAN 内のルーティング対象インターフェイスに適用すると、VLAN に着信するパケットは最初に VACL と照合されます。そこで許可されると、次に入力 ACL と照合され、それからルーティング対象インターフェイスで処理されます。別の VLAN にルーティングされるパケットは、最初に、ルーティング対象インターフェイスに適用される出力 ACL と照合されます。そこで許可されると、宛先 VLAN 用に設定された VACL が適用されます。VACL が特定のパケット タイプ用に設定されていて、VACL と該当タイプのパケットとが一致しない場合、デフォルト動作では、パケットが拒否されます。

VACL を設定する場合は、次の点に注意してください。

- VACL とコンテキストベース アクセス コントロール（CBAC）を同じインターフェイス上に設定することはできません。
- TCP インターセプトおよび再帰 ACL は、同じインターフェイス上の VACL アクションより優先されます。
- インターネット グループ管理プロトコル（IGMP）パケットは VACL に対して確認されません。

Cisco IOS ソフトウェアで VACL を設定する方法の詳細については、『*Network Analysis Module for Catalyst 6500 Series and Cisco 7600 Series Command Reference*』を参照してください。

# NAM で NDE を使用する方法について

NAM は、NAM 内のデータ属性が設定された一連の記述子またはクエリーに基づき、集約されたデータの継続的なストリーミングのためのフォーマットとして NetFlow を使用します。NetFlow データ エクスポート（NDE）は、NAM 上のポート トラフィックをモニタリングできるようにするためのリモート デバイスです。NAM は、トラフィック分析のために、ローカルまたはリモートのスイッチやルータから NDE を収集できます。

NAM の NDE データ ソースを使用するには、このリモート デバイスを、NDE パケットを NAM 上の UDP ポート 3000 にエクスポートするように設定する必要があります。このデバイスの設定は、インターフェイスごとに必要になる場合があります。

IETF 標準の基盤である NetFlow v9 フォーマットの特徴は、それがテンプレートをベースにしている点にあります。テンプレートは、レコード フォーマットの設計を拡張可能なものにします。NetFlow サービスが将来拡張されても、基本フロー レコード フォーマットを変更し続ける必要がありません。

NetFlow の詳細については、http://www.cisco.com/go/netflow か、または『*Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.2SX*』の「Configuring NetFlow Data Export」の章を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/nde.html

NDE クエリーの作成および管理の詳細については、『*Cisco Network Analysis Module API Programmer Guide, 5.1*』を参照してください。

# NAM で WAAS を使用する方法について

Cisco Wide Area Application Services（WAAS）ソフトウェアは、ワイドエリア ネットワーク（WAN）環境で稼働する TCP ベースのアプリケーションのパフォーマンスを最適化し、ブランチのセキュリティを保持および強化します。WAAS ソリューションは、協調して動作してネットワークを介した WAN トラフィックを最適化する、Wide Area Application Engines（WAE）と呼ばれる一連のデバイスで構成されます。

クライアント アプリケーションとサーバ アプリケーションが相互に通信しようとしたとき、ネットワーク デバイスが、クライアント アプリケーションや送信先サーバに代わって動作するために、そのトラフィックを傍受し、WAE へとリダイレクトします。

WAE フロー エージェントが、WAAS WAE の WAN インターフェイスと LAN インターフェイス両方の通過するパケット ストリームに関する情報を提供します。対象となるトラフィックには、特定のサーバやエクスポートされるトランザクションのタイプが含まれます。NAM は、WAAS フロー エージェントからエクスポートされたデータを処理し、アプリケーションの応答時間の計算を実行して、そのデータをユーザによってセットアップされたレポートに入力します。

WAE は、トラフィックを検証し、組み込みのアプリケーション ポリシーを使用して、トラフィックを最適化するか、それとも最適化せずにネットワークを通過させるかを決定します。

自分のネットワークでの WAE とアプリケーション ポリシーの設定とモニタリングは、WAAS Central Manager GUI を使用して一元的に行えます。WAAS Central Manager GUI では、新しいアプリケーション ポリシーを作成して、WAAS システムがカスタム アプリケーションやあまり一般的でないアプリケーションを最適化するようにすることも可能です。

WAAS データ ソースと WAAS デバイスの管理の詳細については、『*Cisco Prime Network Analysis Module Installation and Configuration Note, 5.1 for WAAS VB*』を参照してください。

# NAM の管理

NAM は、組み込みの（Web ブラウザを NAM に転送する）Web ベースの NAM アプリケーションか、または簡易ネットワーク管理プロトコル（SNMP）管理アプリケーション（CiscoWorks2000 にバンドルされたアプリケーションなど）から管理できます。

NAM は、Web ブラウザを経由した NAM データや音声トラフィックのための管理およびモニタリング機能へのアクセスを提供します。NAM GUI を使用するには、CLI を使用して、NAM 上でいくつかの基本的な設定作業を実行する必要があります。それにより、1 つのコマンドで NAM を起動できます。

NAM GUI では、次の作業を実行できます。

- 1 つのウィンドウ内に複数の図を表示するダッシュボード スタイルのレイアウトへのアクセス
- さまざまなトラフィック統計情報に関する履歴データの設定および表示
- SPAN リソースの設定
- 収集の設定
- 統計情報のモニタリング
- パケットのキャプチャおよびデコード
- アラームの設定および表示

セキュリティを向上させるために、リモート TACACS+ サーバを使用するように NAM を設定できます。TACACS+ サーバは、Web ベースのユーザのための認証および認可を提供します。また、セキュリティのために NAM 上のローカル データベースを使用することもできます。

SNMP エージェントのサポートを使用するために、CLI を使用して NAM を設定できます。

すでに設定され、スイッチ内で動作している NAM があり、かつ NAM に精通している場合は、**ip http server enable** CLI コマンドを入力してから、ブラウザで NAM GUI を起動することによって NAM の使用を開始できます。

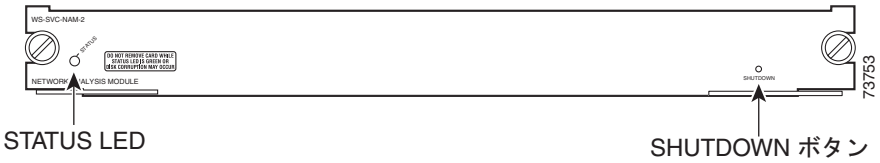
NAM GUI の使用の詳細については、『*User Guide for the Cisco Prime Network Analysis Module*』を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/5.1user/guide/nam51_ug.html

# 前面パネルの説明

NAM の前面パネル（図 1-1 を参照）には、STATUS LED と SHUTDOWN ボタンが含まれています。

**図 1-1　NAM の前面パネル**




## STATUS LED

STATUS LED は、NAM の動作状態を示します。表 1-3 に、この LED の動作を示します。

**表 1-3　STATUS LED の説明**

| 色 | 説明 |
|---|---|
| グリーン | すべての診断テストに合格しました。NAM が稼働しています。 |
| レッド | 個別ポート テスト以外の診断に失敗しました。 |
| オレンジ | 次の 3 つの状態のいずれかを示します。<br>• NAM はブートおよびセルフテスト診断シーケンスを実行しています。<br>• NAM は無効になっています。<br>• NAM はシャットダウン状態にあります。 |
| オフ | NAM に電源が入っていません。 |

## SHUTDOWN ボタン

**注意**　NAM が完全にシャットダウンし、STATUS LED がオレンジ色になるまで、スイッチから NAM を取り外さないでください。NAM が完全にシャットダウンする前にスイッチから NAM を取り外すと、ディスクが破損するおそれがあります。

NAM のハード ディスクが破損しないように、シャーシから NAM を取り外したり、電源を切断したりする前に NAM を正しくシャットダウンする必要があります。このシャットダウン手順は通常、スーパーバイザ エンジンの CLI プロンプトまたは NAM CLI プロンプトで入力されるコマンドによって開始されます。

**（注）**　ディスクの破損が発生した場合は、**--install** オプションを使用してアプリケーション イメージを再度アップグレードすることによってディスクを復旧できます。

NAM がこれらのコマンドに正しく応答できなかった場合は、前面パネルの SHUTDOWN ボタンを押してシャットダウン手順を開始してください。

シャットダウン手順には数分かかることがあります。NAM がシャットダウンすると、STATUS LED は消えます。

# 仕様

表 1-4 に NAM の仕様を示します。これらの仕様は、次のモジュールに適用されます。

- WS-SVC-NAM-1
- WS-SVC-NAM-1-250S
- WS-SVC-NAM-2
- WS-SVC-NAM-2-250S

**表 1-4　Network Analysis Module の仕様**

| 仕様 | 説明 |
|---|---|
| サイズ（高さ x 幅 x 奥行） | 3.0 x 35.6 x 40.6 cm（1.2 x 14.4 x 16 インチ） |
| 重量 | 最小：3 ポンド（1.36 kg）<br>最大：5 ポンド（2.27 kg） |
| 環境条件： | |
| 動作温度 | 32 ～ 104 °F（0 ～ 40 °C） |
| 温度（非動作時） | –40 ～ 158 °F（–40 ～ 70 °C） |
| 湿度 | 10 ～ 90%（結露しないこと） |
| 湿度：非動作時および保管時（結露しないこと） | 5 ～ 95% |
| 高度 | 海面～ 10,000 フィート（3050 m） |