概要

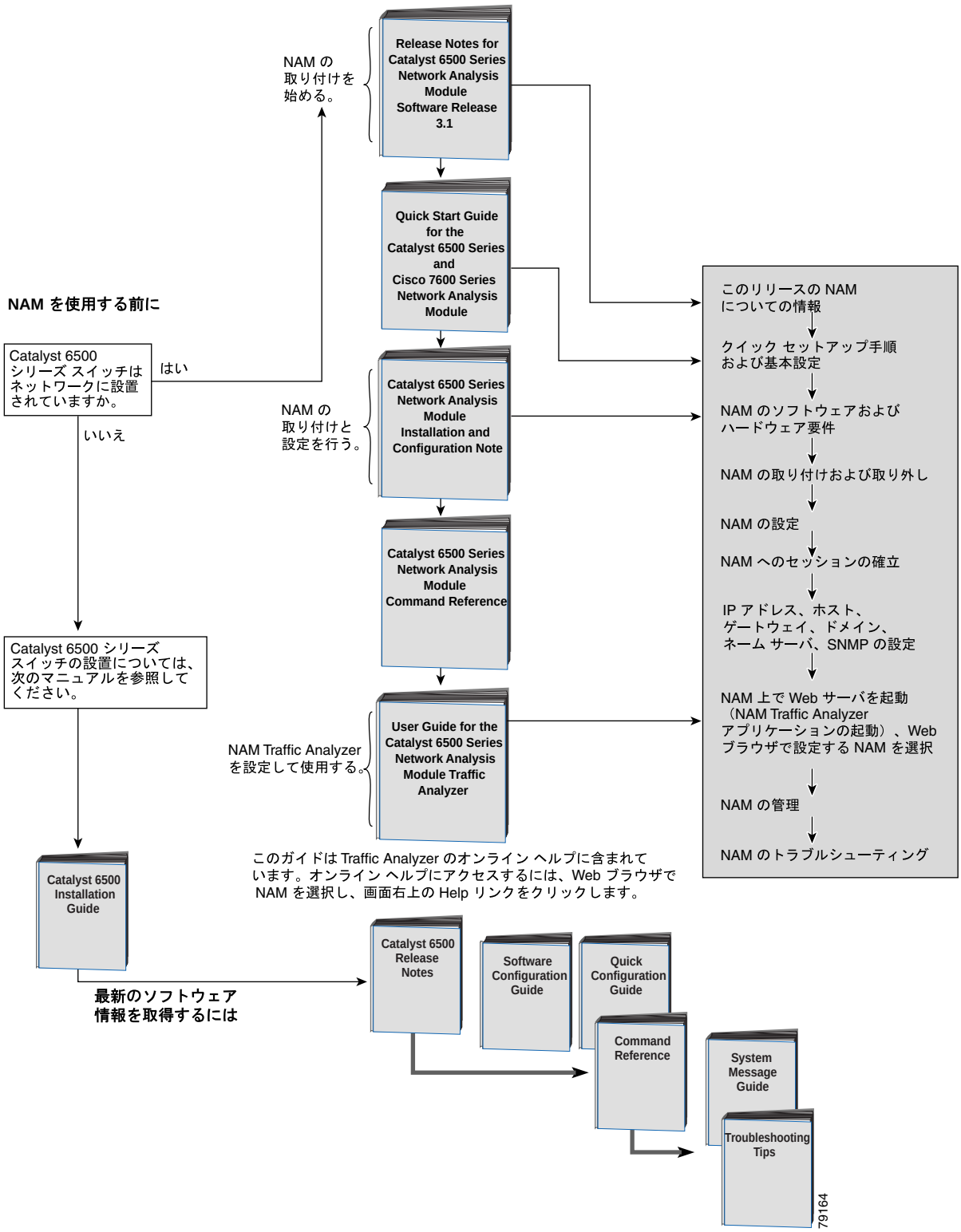
ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ Network Analysis Module（NAM; ネットワーク解析モジュール）の機能および管理方法について説明します。

（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、Catalyst オペレーティング システムと Cisco IOS ソフトウェアのユーザにも適用されます。各オペレーティング システムに関する手順については、それぞれのオペレーティング システムのセクションで個別に明記します。

具体的な内容は次のとおりです。

はじめに

NAM の使用を開始する前に、以下のロードマップを参照してください。



NAM の機能

ここでは、Catalyst 6500 シリーズ スイッチ、Catalyst 6000 シリーズ スイッチ、または Cisco 7600 シリーズ ルータ NAM の機能を説明します。具体的な内容は次のとおりです。

- NAM における SPAN の使い方（p.1-4）
- NAM における VACL の使い方（p.1-5）
- NAM における NDE の使い方（p.1-6）

NAM は、Remote Monitoring（RMON; リモート モニタリング）、スイッチド ネットワーク用の RMON 拡張機能（SMON）、および MIB（Management Information Base; 管理情報ベース）を使用してネットワーク トラフィックのモニタと解析を行います。詳細は、「サポート対象の MIB オブジェクト」（p.5-18）を参照してください。

NAM はリモート デバイスの NetFlow をモニタ、解析および表示し、次の RMON グループをサポートします。

- RFC 2819 で定義されている RMON グループ
- RFC 2021 で定義されている RMON2 グループ
- RFC 3287 で定義されている DSMON グループ
- RFC 3273 で定義されている高キャパシティ RMON グループ（メディア独立型グループをのぞく）
- RFC 2613 で定義されている SMON グループ
- Application Response Time MIB で定義されているすべてのグループ
- NetFlow バージョン 9 のレコード。NetFlow リスニング モードのデータ ソースは NetFlow バージョン 9 を使って表示されます。

NAM には、個々のイーサネット VLAN（仮想 LAN）をモニタする機能もあります。この機能によって Catalyst 6500 シリーズ スーパバイザ エンジンが提供する基本的な RMON サポートが拡張されます。

他の Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）準拠 RMON アプリケーションを使用することにより、リンク、ホスト、プロトコル、および応答時間に関する統計情報にアクセスできます。これらの情報は、キャパシティ プランニング、部門別アカウンティング、およびリアルタイムでのアプリケーション プロトコルのモニタリングに役立ちます。さらに、フィルタおよびキャプチャ バッファを使用してネットワークのトラブルシューティングを行うこともできます。

NAM は次のソースからのイーサネット VLAN トラフィックを解析できます。

- イーサネット、ファースト イーサネット、ギガビット イーサネット、トランク ポート、または Fast EtherChannel Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）または RSPAN 送信元ポート。

  SPAN および RSPAN の詳細は、『*Catalyst 6500 Series Switch Software Configuration Guide*』の「Configuring SPAN and RSPAN」を参照してください。
- NetFlow Data Export（NDE; NetFlow データ エクスポート）。

  NDE の詳細は、『*Catalyst 6500 Series Switch Software Configuration Guide*』を参照してください。

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

表 1-1　NAM モニタの対象となるトラフィック ソース

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	可	可	可	不可
NDE（ローカル）	可	可	可	可
NDE（リモート）	可	可	可	可
SPAN	可	可	不可	不可
ERSPAN	可	可	不可	不可

NAM における SPAN の使い方

SPAN セッションでは、パラメータを設定してモニタ対象のネットワーク トラフィックを指定し、宛先ポートを送信元ポートのセットに関連付けます。スイッチド ネットワークには複数の 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 セッションの宛先ポートが 1 つあります。WS-SVC-NAM-2 プラットフォームには SPAN および VACL セッションの宛先ポートが 2 つある可能性があります。NAM への複数 SPAN セッションがサポートされていますが、ポートの宛先は別々にする必要があります。SPAN の GUI（グラフィカル ユーザ インターフェイス）で使用するデフォルトの NAM 宛先ポート名は DATA PORT 1 および DATA PORT 2 です。CLI（コマンドライン インターフェイス）の SPAN ポート名を表 1-2 に示します。

表 1-2　SPAN のポート名

モジュール	Cisco IOS ソフトウェア	Catalyst オペレーティング システム ソフトウェア
NAM-1	data-port 1	*モジュール番号* : 3
NAM-2	data-port 1 および data-port 2	*モジュール番号* : 7 または *モジュール番号* : 8

ポートはそれぞれ独立しています。1 つのポートのトラフィックだけを読み込んでデータポート集合を作成することも、両方のポートからトラフィックを読み込んでデータポート集合を作成することもできます。また、VLAN ベースの集合も作成できます。その場合は、集合を読み込んだ VLAN に対応するポートのパケットを使用します。

SPAN の詳細および SPAN を Catalyst 6000 および 6500 シリーズ スイッチに設定する方法については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sy/swcg/span.htm#1032978

SPAN の詳細および SPAN を Cisco 7600 シリーズ ルータに設定する方法については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/swcg/span.htm

NAM は管理ポートの Encapsulated Remote SPAN（ERSPAN）トラフィックをサポートし、このトラフィックをデータ ソースとして使用します。ERSPAN トラフィックのすべての集合タイプがサポートされます。

ERSPAN は SPAN の拡張版で、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）パケットにカプセル化されたパケットが ERSPAN の宛先に送信されます。通常、ERSPAN の発信元および宛先は 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 を使用してルータで送信するパケットをカプセル化し、NAM データ ポートにはカプセル化解除されたトラフィックが送信されます。

NAM における VACL の使い方

VLAN Access Control List（VACL; VLAN アクセス コントロール リスト）とは、WAN インターフェイスまたは VLAN から NAM のデータ ポートにトラフィックを転送する方法です。VACL には SPAN を使用する方法もあります。VACL は IP および IPX プロトコルのレイヤ 3 アドレスに基づいてアクセスを制御することもできます。サポートされていないプロトコルは、MAC アドレスからアクセスが制御されます。MAC VACL を使って IP または IPX アドレスをアクセス制御することはできません。

VACL には、すべてのブリッジド VLAN パケットまたはルーテッド VLAN パケットをキャプチャするタイプと、すべてのブリッジド VLAN パケットまたはルーテッド VLAN パケットのサブセットを指定してキャプチャするタイプの 2 種類があります。Catalyst オペレーティング システムの VACL を使った場合、VLAN パケットしかキャプチャできません。これは、スイッチ上の VLAN に最初からルーティングまたはブリッジされているためです。

VACL は、VLAN 内でブリッジされているすべてのパケット、VLAN または WAN インターフェイスにルーティングされているすべてのパケット、あるいは VLAN または WAN インターフェイスからルーティングされているすべてのパケットにアクセス制御を提供できます。ただし WAN インターフェイスについてはリリース 12.1(13)E 以降しか対応していません。通常の Cisco IOS 規格や拡張 ACL はルータ インターフェイス専用に設定されており、ルーティングされたパケットにだけ適用されますが、VACL はすべてのパケットに適用でき、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 Access Control List（ACL; アクセス コントロール リスト）を使用します。VACL は、ハードウェアでサポートされない Cisco IOS ACL フィールドを無視します。標準および拡張 Cisco IOS ACL は、パケットを分類するために使用します。分類されたパケットは、アクセス コントロール（セキュリティ）、暗号化、Policy-Based Routing（PBR; ポリシー ベース ルーティング）などの機能の対象になります。標準および拡張 Cisco IOS ACL はルータ インターフェイス専用に設定され、ルーティングされたパケットに適用されます。

VLAN 上に VACL が設定されると、VLAN に届くすべてのパケットは、ルーティングされたものであれブリッジされたものであれ、VACL でチェックします。パケットはスイッチ ポートから VLAN に届く場合と、ルーティング後にルータ ポートから届く場合があります。Cisco IOS ACL とは異なり、VACL には入力や出力の方向が定義されていません。

VACL には、順番の決まった Access Control Entry（ACE; アクセス コントロール エントリ）のリストがあります。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。フィールドには関連付けたビット マスクを含めることができ、どのビットが関連しているかがわかります。ACE にはアクションが関連付けられており、一致した場合にシステムからパケットに対して行う内容が指定されています。アクションは機能に依存しています。Catalyst 6000 シリーズ スイッチ、6500 シリーズ スイッチ、および Cisco 7600 シリーズ ルータのハードウェアは次の 3 種類の ACE をサポートします。IP、IPX、MAC レイヤ トラフィックです。WAN インターフェイスに適用される VACL は IP トラフィックだけをサポートします。

VACL を設定して VLAN に適用した場合、VLAN に届くすべてのパケットを VACL でチェックします。VACL を VLAN に適用し、ACL を VLAN のルーテッド インターフェイスに適用した場合、VLAN に届くパケットはまず VACL でチェックされます。結果が permit であれば、次に入力 ACL でチェックされ、その後ルーテッド インターフェイスで処理されます。このパケットが別の VLAN にルーティングされた場合、まずルーテッド インターフェイスに適用された出力 ACL でチェックされ、結果が permit であれば、宛先 VLAN に設定された VACL が適用されます。VACL がパケット タイプに設定され、そのタイプのパケットと VACL が一致しなければ、デフォルトのアクションは deny です。

VACL を設定する場合は、次の項目に注意してください。

- VACL および Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）を同じインターフェイスに設定することはできません。
- TCP 代行受信とリフレクシブ ACL が同じインターフェイスに設定されている場合、VACL のアクションが優先されます。
- Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）パケットは VACL でチェックされません。

Cisco IOS ソフトウェアで VACL を設定する方法の詳細は『*Network Analysis Module for Catalyst 6500 Series and Cisco 7600 Series Command Reference*』を参照してください。Catalyst オペレーティング システムでセキュリティ ACL を設定する方法の詳細は、『*Catalyst 6500 Series Software Configuration Guide*』および『*Catalyst 6500 Series Command Reference*』を参照してください。

NAM における NDE の使い方

NDE は、NAM のポート トラフィックがモニタできるリモート デバイスです。NAM の NDE データ ソースを使用するには、NAM の UDP ポート 3000 に NDE パケットをエクスポートするようにリモート デバイスを設定します。デバイスはインターフェイスごとに設定する必要があります。Web アプリケーション ユーザ インターフェイスに、NDE デバイスを指定するための画面が追加されています（NDE デバイスは IP アドレスで区別できます）。デフォルトでは、スイッチのローカル スーパバイザ エンジンは常に NDE デバイスとして使用できます。

IP アドレスとコミュニティ ストリングを指定すると、追加の NDE デバイスが定義できます。コミュニティ ストリングは省略可能です。コミュニティ ストリングは、インターフェイス用に便利なテキスト形式の文字列をリモート デバイスにアップロードして、NetFlow レコードでモニタするために使用します。

NAM の NDE データ ソースについては、NAM Traffic Analyzer のオンライン ヘルプで **Contents > Setting Up the Application > Setting Up Data Sources > Understanding NetFlow Interfaces** の順に選択してください。

NAM の管理

NAM を管理するには、NAM に組み込まれた Web ベースの NAM Traffic Analyzer アプリケーション（NAM から Web ブラウザを起動）、または CiscoWorks 2000 にバンドルされているような Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）管理アプリケーションを使用します。

NAM Traffic Analyzer を使用すると、Web ブラウザを通じて NAM のデータ / 音声トラフィック管理機能およびモニタ機能にアクセスできます。NAM Traffic Analyzer を使用するには、CLI を使用して NAM の基本設定を行う必要があります。その後は、1 つのコマンドで NAM Traffic Analyzer を起動できるようになります。

NAM Traffic Analyzer を使用して、次の作業を行うことができます。

- さまざまな統計情報の履歴レポートの設定および表示
- SPAN リソースの設定
- 収集の設定
- 統計情報のモニタ
- 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

セキュリティを強化するには、NAM Traffic Analyzer を使用して、NAM がリモート TACACS+ サーバを使用するように設定します。TACACS+ サーバを使用して Web ベース ユーザの認証および許可を行うことができます。また、NAM 上のローカル データベースを使用してセキュリティを確保することもできます。

Cisco NetScout nGenius Real-Time Monitor（RTM）などの SNMP 管理アプリケーションを使用して、NAM を管理することもできます。Cisco NetScout nGenius RTM は Cisco Works 2000 LAN Management Solution（LMS）のコンポーネントです。RTM の詳しい使用方法については、CiscoWorks のマニュアルまたは次の URL を参照してください。

http://www.Cisco.com/univercd/cc/td/doc/product/lan/cat6000/fam_mod/rel2_1_2/ol_2428.htm

RMON および SNMP エージェント サポートを使用するには、CLI を使用して NAM を設定します。

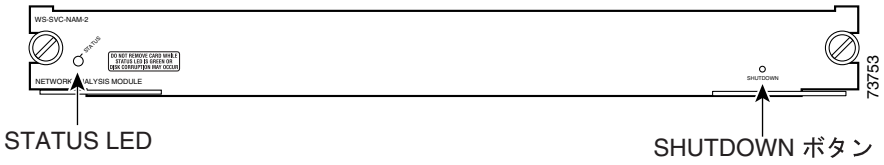
すでにスイッチ上で NAM を設定し稼働させていて、NAM の使用手順を熟知している場合は、**ip http server enable** CLI コマンドを入力してブラウザで NAM Traffic Analyzer を起動し、NAM Traffic Analyzer の使用を開始できます。

NAM Traffic Analyzer の詳しい使用方法については、『*User Guide for the Network Analysis Module Traffic Analyzer*』Release 3.3 を参照してください。

前面パネル

NAM の前面パネル（図 1-1）には、STATUS LED と SHUTDOWN ボタンが 1 つずつあります。

図 1-1　Network Analysis Module



STATUS LED

STATUS LED は、NAM の動作状態を表します（表 1-3 を参照）。

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パスしました。NAM は動作可能です。
レッド	個別ポート テスト以外の診断テストに失敗しました。
オレンジ	次の 3 つの条件のいずれかを表します。 • NAM は起動およびセルフテスト診断シーケンスの実行中です。 • NAM はディセーブルです。 • NAM はシャットダウン ステートです。
消灯	NAM の電源がオフです。

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可能性があります。

NAM ハードディスクの損傷を防ぐには、NAM を正しくシャットダウンした後にシャーシから NAM を取り外すか、または電源を切断する必要があります。このシャットダウン手順は通常、スーパバイザ エンジン CLI プロンプトまたは NAM CLI プロンプトでコマンドを入力して開始します。

（注）　破損したディスクを復旧するには、**--install** オプションを使ってアプリケーション イメージをアップグレードします。「Catalyst オペレーティング システム ソフトウェアを使用した NAM アプリケーション ソフトウェアのアップグレード」（p.19）を参照してください。

NAM がこれらのコマンドに正常に応答しない場合は、前面パネルの SHUTDOWN ボタンを使用してシャットダウン手順を開始します。

シャットダウン手順の完了には、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 が消灯します。

仕様

表 1-4 に、NAM の仕様を示します。

表 1-4　WS-SVC-NAM-1 および WS-SVC-NAM-2 の仕様

仕様	説明
寸法（高さ × 幅 × 奥行）	1.2 × 14.4 × 16 インチ（3.0 × 35.6 × 40.6 cm）
重量	最小：3 ポンド（1.36 kg） 最大：5 ポンド（2.27 kg）
環境条件	
動作時の温度	32 ～ 104°F（0 ～ 40°C）
非動作時の温度	–40 ～ 158°F（–40 ～ 70°C）
湿度	10 ～ 90%（結露しないこと）
周囲湿度 （結露しないこと）非動作時および保管時	5 ～ 95%
高度	海抜 10,000 フィート（3,050 m）以下