Network Analysis Module Traffic Analyzer Release 3.6 ユーザ ガイド

March 2007

Text Part Number: OL-11519-01-J

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。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。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、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、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、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

このドキュメントで使用しているインターネット プロトコル（IP）アドレスは、実在のアドレスではありません。ドキュメント中で示される例、コマンドの画面出力、および図は、いずれも視覚的な説明のみを目的としています。実在する IP アドレスが例示されていた場合、それらは意図して使用したものではありません。

Network Analysis Module Traffic Analyzer Release 3.6 ユーザ ガイド
Copyright © 2007 Cisco Systems, Inc.
All rights reserved.

CONTENTS

このマニュアルについて xiii

対象読者 xiv

表記法 xiv

技術情報の入手方法 xv

Cisco.com xv

Product Documentation DVD（英語版） xv

マニュアルの発注方法（英語版） xv

シスコシステムズマニュアルセンター xvi

シスコ製品のセキュリティの概要 xvii

シスコ製品のセキュリティ問題の報告 xvii

テクニカル サポート xviii

Cisco Technical Support & Documentation Web **サイト** xviii

Japan TAC Web **サイト** xviii

サービス リクエストの発行 xix

サービス リクエストのシビラティの定義 xix

その他の資料および情報の入手方法 xx

CHAPTER 1 **NAM Traffic Analyzer の概要** 1-1

NAM Traffic Analyzer **について** 1-1

ユーザ インターフェイス コンポーネントの詳細 1-3

共通のナビゲーションおよび制御要素 1-4

はじめに 1-6

CHAPTER 2 **ユーザおよびシステム管理** 2-1

ユーザ管理 2-2

パスワードの回復 2-2

スイッチまたはルータに定義されている NAM **ユーザ アカウントの変更** 2-3

User Administration GUI 2-3

新しいユーザの作成 2-3

ユーザの編集 2-4

ユーザの削除 2-5

TACACS+ **認証および認可の設定** 2-5

NAM 認証と認可をサポートする TACACS+ サーバの設定 2-7
Cisco ACS TACACS+ サーバの設定 2-7
Current User Sessions テーブルの表示 2-9
システム管理 2-10
システム リソース 2-10
ネットワーク パラメータの設定と表示 2-11
NAM SNMP システム グループの設定と表示 2-12
NAM コミュニティ ストリングの使用 2-13
NAM コミュニティ ストリングの作成 2-13
NAM コミュニティ ストリングの削除 2-14
NAM のシステム時刻 2-14
NAM のシステム時刻とスイッチまたはルータの同期 2-15
NTP サーバによる NAM のシステム時刻の設定 2-15
E メールの設定 2-15
FTP の設定 2-16
キャプチャ データ ストレージ 2-17
NFS ストレージの場所の作成 2-17
NFS ストレージの場所の編集 2-19
iSCSI ストレージの場所の作成 2-20
iSCSI ストレージの場所の編集 2-21
Web パブリケーション 2-21
診断 2-23
システム アラートの表示 2-23
監査証跡の表示 2-23
設定情報の監視とキャプチャ 2-25
テクニカル サポートの表示 2-26

CHAPTER 3 アプリケーションのセットアップ 3-1
スイッチ パラメータ 3-2
スイッチ情報の表示 3-2
NBAR プロトコル検出のセットアップ 3-3
ポート統計情報（Mini-RMON）のイネーブル化およびディセーブル化 3-4
Port Stats (Mini-RMON) Details の表示 3-5
スイッチ ログインの設定 3-6
ルータ パラメータ 3-7
ルータ システム情報の適用 3-7
データ ソースのセットアップ 3-8
SPAN セッション 3-9
SPAN セッションの作成 3-10

SPAN セッションの編集 3-12
SPAN セッションの削除 3-13
NetFlow インターフェイスについて 3-13
NetFlow フロー レコードについて 3-14
デバイスの NetFlow 設定 3-15
WAN インターフェイスの VACL 設定 3-17
LAN VLAN での VACL 設定 3-18
NetFlow デバイスの管理 3-19
デバイスの作成 3-19
デバイスの編集 3-20
デバイスの削除 3-20
デバイスのテスト 3-21
カスタム データ ソースの作成 3-21
NetFlow デバイスの選択 3-22
インターフェイスの選択 3-22
リスニング モードの使用方法 3-24
ルータのコミュニティ ストリングのテスト 3-26
インターフェイスのセットアップ 3-27
MPLS データ ソース 3-27
MPLS VPN ラベルの自動検出 3-28
レイヤ 3 VRF データ ソースのセットアップ 3-28
レイヤ 2 仮想回線データ ソースのセットアップ 3-29
MPLS ラベル データ ソースのセットアップ 3-31
VRF/VC 設定ファイルの作成 3-32
VRF/VC 設定ファイルのインポート 3-33
VRF/VC 設定ファイルのエクスポート 3-33
インポート ログ 3-33
監視のセットアップ 3-34
コア データの監視 3-34
Mini-RMON 収集のイネーブル化 3-36
音声データの監視 3-36
応答時間データの監視 3-37
応答時間のデータ収集の作成 3-38
応答時間のデータ収集の編集 3-38
応答時間のデータ収集の削除 3-39
DiffServ データの監視 3-39
DiffServ プロファイルのセットアップ 3-40
DiffServ プロファイルの作成 3-40

DiffServ プロファイルの編集 3-41
DiffServ プロファイルの削除 3-41
URL 収集データの監視 3-41
URL 収集のイネーブル化 3-42
URL 収集の変更 3-43
URL 収集のディセーブル化 3-44
プロトコル ディレクトリのセットアップ 3-45
個々のアプリケーション 3-45
新しいプロトコルの作成 3-46
プロトコルの編集 3-47
プロトコルの削除 3-48
アプリケーション グループのセットアップ 3-49
アプリケーション グループの作成 3-49
アプリケーション グループの編集 3-50
アプリケーション グループの削除 3-50
自動認識プロトコルのセットアップ 3-50
URL ベースのアプリケーションのセットアップ 3-52
URL ベースのアプリケーションの作成 3-52
URL ベースのアプリケーションの編集 3-54
URL ベースのアプリケーションの削除 3-55
アラームしきい値の設定 3-56
NAM の MIB しきい値の設定 3-56
NAM の MIB 変数の選択 3-57
NAM の MIB パラメータの選択 3-57
NAM の MIB しきい値の編集 3-59
NAM の MIB しきい値の削除 3-60
音声しきい値の設定 3-60
上流 RTP ストリームのしきい値の設定 3-61
NAM Syslog のセットアップ 3-61
スイッチしきい値の設定 3-63
スイッチしきい値の作成 3-63
スイッチしきい値の編集 3-65
スイッチしきい値の削除 3-65
NAM のトラップ宛先の設定 3-66
NAM のトラップ宛先の作成 3-66
NAM のトラップ宛先の編集 3-66
NAM のトラップ宛先の削除 3-67
NAM アラーム メールの設定 3-67

グローバル プリファレンスの設定 3-68

CHAPTER 4 データの監視 4-1

データ収集およびデータ ソースの概要 4-2

複数の収集の設定 4-3

プロトコル自動検出 4-5

NDE フロー マスクおよび V8 集約キャッシュ 4-5

Monitor Overview チャートの表示 4-6

データ ソースの持続性 4-8

アプリケーション グループの表示 4-9

Application Groups Current Rates テーブルの表示 4-9

Application Group テーブルの詳細の表示 4-10

Application Group テーブルのリアルタイム データの表示 4-11

Application Group テーブルのレポートの表示 4-11

Application Group TopN Chart の表示 4-11

Application Groups Cumulative Data テーブルの表示 4-12

個別のアプリケーション データの表示 4-14

Applications Current Rates テーブルの表示 4-14

Applications テーブルの詳細の表示 4-15

Application テーブルのアプリケーション プロトコル データのキャプチャ 4-15

Application テーブルのリアルタイム データの表示 4-16

Applications テーブルのレポートの表示 4-16

Applications TopN Chart の表示 4-16

Applications Cumulative Data テーブルの表示 4-17

Applications テーブルの詳細の表示 4-18

収集された URL の表示 4-19

収集された URL の表示 4-19

URL 収集リストのフィルタリング 4-20

収集された URL からの URL ベースのアプリケーションの作成 4-20

音声データの表示 4-22

音声プロトコルの概要の表示 4-22

Aggregate Statistics テーブルのプロトコル詳細の表示 4-23

既知の電話機の表示 4-24

Known Phones テーブルの電話機詳細の表示 4-24

アクティブ コールの表示 4-30

Active Calls テーブルの通話詳細の表示 4-31

RTP ストリーム トラフィックの表示 4-31

ホスト データの監視 4-32

Network Hosts Current Rates テーブルの表示 4-32
ネットワーク ホストの詳細の表示 4-33
Network Host テーブルのネットワーク ホスト データのキャプチャ 4-35
Hosts テーブルのリアルタイム トラフィック統計情報の表示 4-35
Network Hosts テーブルのレポートの表示 4-35
Network Hosts TopN Chart の表示 4-36
Network Hosts Cumulative Data テーブルの表示 4-37
MAC Stations Current Rates テーブルの表示 4-37
MAC Stations TopN Chart の表示 4-38
MAC Stations Cumulative Data テーブルの表示 4-40
会話データの表示 4-41
Network Host Conversations Current Rates テーブルの表示 4-41
ネットワーク ホスト会話の詳細の表示 4-42
Network Host Conversations テーブルからのネットワーク ホスト会話データのキャプチャ 4-43
Network Host Conversations テーブルのリアルタイム トラフィック統計情報の表示 4-43
Network Host Conversations テーブルのレポートの表示 4-43
Network Host Conversations TopN Chart の表示 4-44
Network Host Conversations Cumulative Data テーブルの表示 4-45
ネットワーク ホスト会話の詳細の表示 4-45
MAC Station Conversations Current Rates テーブルの表示 4-46
MAC Station Conversations TopN Chart の表示 4-46
MAC Station Conversations Cumulative Data テーブルの表示 4-48
VLAN データの表示 4-49
VLAN Traffic Statistics Current Rates テーブルの表示 4-49
VLAN Traffic Statistics Current Rates テーブルのレポートの表示 4-50
VLAN Traffic Statistics TopN Chart の表示 4-50
VLAN Traffic Statistics Cumulative Data テーブルの表示 4-51
VLAN Priority (COS) Statistics Current Rates テーブルの表示 4-52
VLAN Priority (COS) Statistics TopN Chart の表示 4-53
VLAN Priority (COS) Statistics Cumulative Data テーブルの表示 4-54
DiffServ データの表示 4-55
DiffServ Traffic Statistics Current Rates テーブルの表示 4-55
DiffServ Traffic Statistics テーブルのリアルタイム トラフィック統計情報の表示 4-56
DiffServ Traffic Statistics テーブルのレポートの表示 4-57
DiffServ Traffic TopN Chart の表示 4-57
DiffServ Traffic Statistics Cumulative Data テーブルの表示 4-58

DiffServ Application Statistics Current Rates テーブルの表示 4-58
Application Statistics テーブルのアプリケーション会話の詳細の表示 4-59
DiffServ Application Statistics テーブルのリアルタイム トラフィック統計情報の表示 4-59
DiffServ Application Statistics テーブルのレポートの表示 4-60
DiffServ Application Statistics TopN Chart の表示 4-60
DiffServ Application Statistics Cumulative Data テーブルの表示 4-61
DiffServ Host Statistics Current Rates テーブルの表示 4-62
DiffServ Host Statistics テーブルのホスト会話の詳細の表示 4-63
DiffServ Host Statistics テーブルのリアルタイム データの表示 4-63
DiffServ Host Statistics テーブルのレポートの表示 4-64
DiffServ Host Statistics TopN Chart の表示 4-64
DiffServ Host Statistics Cumulative Data テーブルの表示 4-65
応答時間データの監視 4-67
レガシー アプリケーション応答時間の監視 4-67
NAM 3.6 アプリケーション応答時間の測定 4-67
サーバ アプリケーション応答時間 4-69
サーバ アプリケーション応答時間の表示 4-69
Application Response Time TopN Chart の表示 4-70
サーバ ネットワーク応答時間 4-71
サーバ ネットワーク応答時間の詳細の表示 4-72
Server Network Response Time TopN Chart の表示 4-73
サーバ / クライアント アプリケーション応答時間 4-74
サーバ / クライアント アプリケーション応答時間の表示 4-74
Client/Server Application Response Time TopN Chart の表示 4-77
サーバ / クライアント ネットワーク応答時間 4-78
サーバ / クライアント ネットワーク応答時間の表示 4-78
Client/Server Network Response Time TopN Chart の表示 4-80
ポート / インターフェイス統計情報データの表示 4-81
Port Stats Current Rates テーブルの表示 4-81
Interface Stats Current Rates テーブルの表示 4-82
ポート / インターフェイスの詳細の表示 4-83
Port/Interface Stats テーブルのリアルタイム トラフィック データの表示 4-83
Port/Interface Stats テーブルのレポートの表示 4-84
Port Stats TopN Chart の表示 4-84
Interface Stats TopN Chart の表示 4-86
Port Stats Cumulative Data テーブルの表示 4-87

Interface Stats Cumulative Data テーブルの表示 4-88
インターフェイスの詳細の表示 4-89
システム状態の表示 4-90
Switch Health 4-90
Switch Health 4-90
Switch Information 4-91
Crossbar Switching Fabric 4-93
Ternary Content Addressable Memory 情報 4-94
Router Health 4-95
Router Health 4-95
Router Information 4-96
NBAR の表示 4-98
NBAR Current Rates テーブルの表示 4-98
NBAR TopN Chart の表示 4-99
NBAR Cumulative Data テーブルの表示 4-100
MPLS トラフィック統計情報の表示 4-101
すべてのラベルの表示 4-101
MPLS タグによるトラフィック統計情報 4-101
カスタム RMON データ ソース 4-101
MPLS タグによるアプリケーションの監視 4-102
MPLS タグによるホストの監視 4-102
MPLS タグによるホスト会話の監視 4-102
VRF および VC 統計情報の表示 4-102

CHAPTER 5 レポートの作成と表示 5-1
基本レポート 5-2
基本レポートの作成 5-4
アプリケーション レポートの作成 5-5
アプリケーション グループ レポートの作成 5-7
ホスト レポートの作成 5-7
会話レポートの作成 5-9
VLAN レポートの作成 5-10
DiffServ レポートの作成 5-11
応答時間レポートの作成 5-12
スイッチ ポート レポートの作成 5-13
スイッチ状態レポートの作成 5-14
ルータ インターフェイス レポートの作成 5-15
MPLS レポートの作成 5-16
基本レポートの表示 5-17

レポートの詳細の表示 5-18
システム イベント ログの表示 5-19
レポートのイネーブル化 5-20
レポートのディセーブル化 5-20
レポート名の変更 5-20
レポートの削除 5-20
カスタム レポート 5-21
カスタム レポートの作成 5-21
新しいフォルダの作成 5-22
カスタム レポートの編集 5-22
カスタム レポートの削除 5-22
カスタム レポートの表示 5-22
カスタム レポートの別のフォルダへの移動 5-23
スケジュールされたエクスポート 5-24
レポートのエクスポートのスケジューリング 5-24
レポートのエクスポートの編集 5-26

CHAPTER 6 パケット データのキャプチャとデコード 6-1
バッファ 6-2
キャプチャ設定の構成 6-3
アドレス フィルタを使用したキャプチャ 6-8
プロトコル フィルタを使用したキャプチャ 6-9
ポート フィルタを使用したキャプチャ 6-10
カスタム フィルタを使用したキャプチャ 6-10
自動キャプチャ（アラームによってトリガーされるキャプチャ）の使用 6-10
パケット デコード情報の表示 6-11
Packet Decoder でのパケットの表示 6-12
Packet Decoder に表示されるパケットのフィルタリング 6-13
詳細なプロトコル デコード情報の表示 6-14
ファイル 6-15
キャプチャ ファイルの分析 6-16
キャプチャ ファイルのデコード 6-17
キャプチャ ファイルの名前の変更とマージ 6-17
キャプチャ ファイルの名前の変更 6-17
キャプチャ ファイルのマージ 6-18
キャプチャ ファイルのダウンロード 6-18
キャプチャ ファイルの削除 6-19
すべてのキャプチャ ファイルの削除 6-19

カスタム キャプチャ フィルタ 6-21
カスタム キャプチャ フィルタの作成 6-21
カスタム キャプチャ フィルタ式作成のヒント 6-23
カスタム キャプチャ フィルタの編集 6-24
カスタム キャプチャ フィルタの削除 6-24
カスタム表示フィルタ 6-25
カスタム表示フィルタの作成 6-25
カスタム デコード フィルタ式作成のヒント 6-27
カスタム表示フィルタの編集 6-28
カスタム表示フィルタの削除 6-28

CHAPTER 7 アラームの表示 7-1
NAM ログの表示 7-2
スイッチ ログの表示 7-3

APPENDIX A トラブルシューティング A-1
NAM の一般的な問題 A-2
ユーザ名およびパスワードの問題 A-3
ログインの問題 A-5
SPAN に関連する問題 A-7
パケットのキャプチャの問題 A-8
アラームとインターフェイス統計情報またはポート統計情報の問題 A-10
NetFlow および NBAR の監視の問題 A-11
レポートの問題 A-15
イメージのアップグレードおよびパッチの問題 A-16
Web ブラウザの応答時間および表示の問題 A-17
NAM とスイッチの日付と時刻の同期の問題 A-18
診断エラー メッセージの問題 A-18
ホスト名解決の問題 A-19
データ不一致の問題 A-20
HTTPS および セキュリティ証明書の問題 A-21
SNMP の問題 A-22
プロトコル サポートの問題 A-23
音声監視の問題 A-24

APPENDIX B サポートされている MIB オブジェクト B-1
サポートされている MIB B-1

INDEX 索引

このマニュアルについて

Revised: February 13, 2007, OL-11519-01-J

このマニュアルでは、Network Analysis Module Traffic Analyzer の使用方法について説明します。このユーザ ガイドには、次の章および付録があります。

- 第 1 章「NAM Traffic Analyzer の概要」では、NAM Traffic Analyzer の概要を示します。GUI について説明し、NAM Traffic Analyzer のさまざまなコンポーネントの使用方法について情報を提供します。
- 第 2 章「ユーザおよびシステム管理」では、ユーザ管理タスクおよびシステム管理タスクの実行と、テクニカル サポートを受けるために必要な診断情報の生成について説明します。
- 第 3 章「アプリケーションのセットアップ」では、NAM Traffic Analyzer アプリケーションのセットアップについて説明します。
- 第 4 章「データの監視」では、さまざまなタイプのデータを表示および監視するためのオプションについて説明します。
- 第 5 章「レポートの作成と表示」では、NAM Traffic Analyzer のレポート機能について説明します。レポート機能を使用すると、NAM が監視するネットワーク トラフィックに関する短期から中期の履歴データを保存および取得できます。
- 第 6 章「パケット データのキャプチャとデコード」では、パケット データのキャプチャ、フィルタリング、デコード用に複数のバッファを設定する方法、ファイル コントロール システムでデータを管理する方法、およびパケットの内容を表示する方法について説明します。
- 第 7 章「アラームの表示」では、アラームの設定方法について説明します。アラームを使用すると、上昇データのしきい値または下降データのしきい値、あるいはその両方に基づいてあらかじめ定義された条件に対して警告を出すことができます。NAM MIB、NAM 音声監視のしきい値、およびスイッチしきい値を設定できます。
- 付録 A 「トラブルシューティング」では、NAM Traffic Analyzer の使用時に発生する一般的な問題をトラブルシューティングする方法について説明します。
- 付録 B「サポートされている MIB オブジェクト」では、NAM Traffic Analyzer でサポートされる MIB オブジェクトについて説明します。

対象読者

このマニュアルは、Network Analysis Modules（NAM）をセットアップおよび設定するネットワーク管理者を対象としています。NAM は、トラフィックを監視し、ネットワーク セグメントで発生する問題を診断するために使用します。ネットワーク管理者は、次の内容について理解している必要があります。

- インターネットワーキングで使用される基本概念および用語
- ネットワーク トポロジおよびプロトコル
- UNIX の基本コマンドまたは Windows の基本操作

表記法

このマニュアルは、次の表記法を使用しています。

項目	表記法
コマンドおよびキーワード	太字
ユーザが値を指定する変数	イタリック体
セッション情報およびシステム情報の表示出力	`screen` フォント
ユーザが入力する情報	太字の **`screen`** フォント
ユーザが入力する変数	イタリック体の *`screen`* フォント
メニュー項目およびボタン名	太字
本文中のメニュー項目の選択	**Option > Network Preferences**
表中のメニュー項目の選択	Option > Network Preferences

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

シスコの Web サイトの各国語版には、次の URL からアクセスしてください。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納した、包括的なライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関する複数のバージョンのマニュアルにアクセスし、技術情報を HTML で参照できます。また、この DVD を使用すると、シスコの Web サイトで参照できるのと同じマニュアルに、インターネットに接続せずにアクセスできます。一部の製品については、PDF 版のマニュアルもご利用いただけます。

Product Documentation DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、次の URL の Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD=）を発注できます。

http://www.cisco.com/go/marketplace/

マニュアルの発注方法（英語版）

2005 年 6 月 30 日以降、Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないとみなされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。
無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術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、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンラインサービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『iQ Magazine』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

  デジタル版には、次の URL からアクセスできます。

  http://ciscoiq.texterity.com/ciscoiq/sample/

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

NAM Traffic Analyzer の概要

次の項で、NAM Traffic Analyzer のさまざまなコンポーネントの使用方法について説明します。

- NAM Traffic Analyzer について（P.1-1）
- ユーザ インターフェイス コンポーネントの詳細（P.1-3）
- 共通のナビゲーションおよび制御要素（P.1-4）
- はじめに（P.1-6）

NAM Traffic Analyzer について

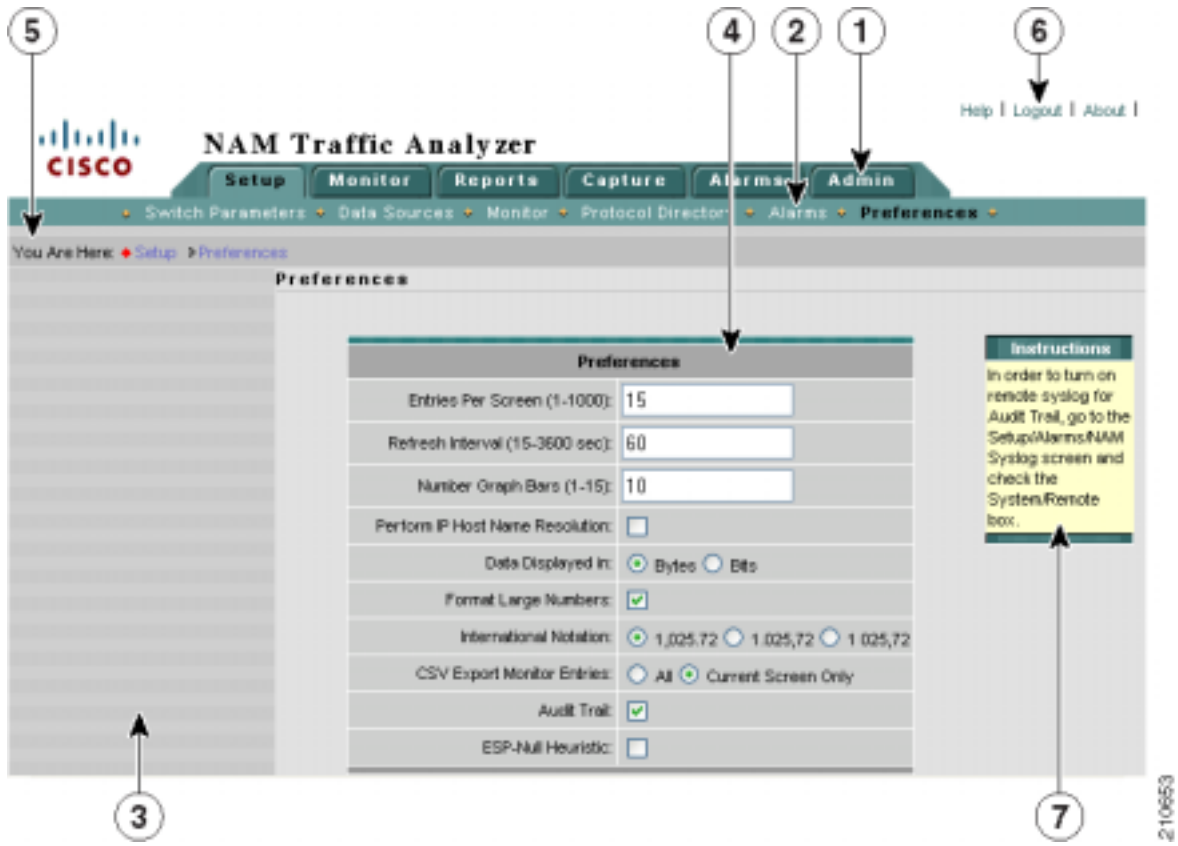
Network Analysis Module（NAM）は、Catalyst 6000 と Catalyst 6500 シリーズのスイッチと Cisco 3660、3700 シリーズ、2800 シリーズ、3800 シリーズのルータに組み込まれたインターフェイス カード、および 2600 のセレクト モデルです。NAM は、Remote Monitoring（RMON; リモート モニタリング）、RMON Extensions for Switched Networks（SMON; スイッチド ネットワーク用 RMON 拡張）、およびその他の Management Information Base（MIB; 管理情報ベース）を使用して、ネットワーク トラフィックを監視および分析します。

NAM Traffic Analyzer は、ブラウザベースで RMON1、RMON2、SMON、DSMON、および NAM の音声監視機能へのアクセスが可能な、NAM 組み込みのソフトウェアです。このソフトウェアを使用して、ネットワークのアベイラビリティおよび状態のトラブルシューティングおよび監視を行います。

(注) NM-NAM デバイスで使用できない監視機能があります。

NAM Traffic Analyzer ウィンドウ（図 1-1）は、NAM Traffic Analyzer のユーザ インターフェイスの例です。

図 1-1　NAM Traffic Analyzer ウィンドウ



1	主な機能にアクセスするタブ。タブは、ユーザ インターフェイスの各ウィンドウに表示されます（詳細ポップアップ ウィンドウを除く）。	**5**	現在の機能へのパスを示すコンテキスト行。この領域のリンクをクリックして、関連するウィンドウに戻ります。
2	各タブに関連するオプション。コンテキストに応じて、タブごとに機能が異なります。	**6**	グローバルな機能（オンライン ヘルプ、ログアウト、アプリケーションの詳細説明）にアクセスするツールバー。
3	現在の機能へのパスを示すコンテキスト バー。このバーのリンクをクリックして、対応するウィンドウに移動します。	**7**	この GUI ウィンドウの使用方法について役立つ情報を表示する指示ボックス。
4	グラフ、表、ダイアログボックス、チャートおよび指示ボックスが表示されるコンテンツ領域。		

（注） Traffic Analyzer のすべての時刻は、通常、24 時間制で表示されます。たとえば、3:00 p.m. は 15:00 と表示されます。

ユーザ インターフェイス コンポーネントの詳細

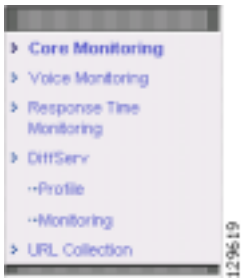
コンテキスト行

コンテキスト行には、操作の階層内での現在の位置が表示されます。この例では、Response Time Client/Server Table が表示されています。

次の項目をクリックできます。

- **Response Time** をクリックすると、Response Time Server Table に戻ります。
- **Monitor** をクリックすると、Monitor Overview ウィンドウに戻ります。

コンテンツ



コンテンツ（一部のウィンドウだけに存在）には、個々のタブのオプションに従属するオプションが表示されます。上の例は、**Setup** > **Monitor** をクリックすると表示されます。

ツールバー

ツールバーは、ユーザ インターフェイスの各ウィンドウの右上に表示されます。

- **Logout** をクリックすると、NAM Traffic Analyzer からログアウトします。
- **Help** をクリックすると、その状況に応じた情報（現在の機能に関する情報）が表示されます。ヘルプは、別のブラウザ ウィンドウに表示されます。
- **About** をクリックすると、NAM Traffic Analyzer に関する情報が表示されます。

共通のナビゲーションおよび制御要素

共通のナビゲーションおよび制御要素（表 1-1）に、ユーザ インターフェイスの共通のナビゲーションおよび制御要素を示します。

表 1-1　共通のナビゲーションおよび制御要素

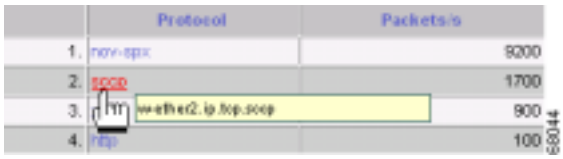
要素	説明
Start	アクションを開始します。
Stop	アクション（パケットのキャプチャなど）を中止します。
Pause	アクションを一時停止します。
Create	新しいレコード、ユーザ、キャプチャ、フィルタなどを作成します。
Delete	レコード、ユーザ、キャプチャ、フィルタなどを削除します。
Edit	レコード、ユーザ、キャプチャ、フィルタなどを編集します。
Go	特定の行番号から始まるレコード グループにジャンプします。
Prev	前のレコード グループを表示します。
Next	次のレコード グループを表示します。
Filter	さまざまな基準（IP アドレス対プロトコルなど）に基づいて情報を表示します。
Apply	変更を適用します。現在のウィンドウは表示されたままです。
Submit	変更を適用します。別のウィンドウに移動します。
Reset	ダイアログボックス内で行った変更をリセット（クリア）します。
Close	ウィンドウを閉じます。
Address ▽	カラム情報を降順にソートします。
Test	機能（ルータへの読み取りおよび書き込みアクセスなど）をテストします。
Report	選択した変数のレポートを作成します。
Real-Time	選択した変数のリアルタイム統計情報を表示します。
Capture	パケットをバッファにキャプチャします。

表 1-1　共通のナビゲーションおよび制御要素（続き）

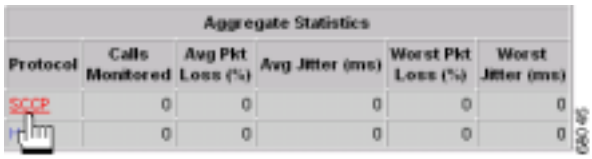
要素	説明
	画面上のデータを **.csv** テキスト ファイルにエクスポートします。1 ページにエクスポートするデータを増やすには、テーブルの 1 ページあたりの行数の設定を増やす必要があります。デフォルトの設定は、1 ページに 15 行です。
	画面上のデータを PDF ファイルにエクスポートします。
	画面上のデータを容易に印刷できるようにウィンドウを開きます。Web ブラウザから、Print コマンドを使用してウィンドウを印刷できます。1 ページに印刷するデータを増やすには、テーブルの 1 ページあたりの行数の設定を増やす必要があります。デフォルトの設定は、1 ページに 15 行です。
	オンライン ヘルプを起動します。

共通のナビゲーションおよび制御要素のほかに、次のナビゲーション補助機能を使用できます。

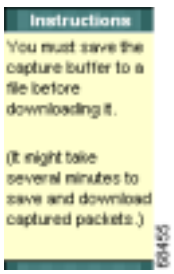
ポップアップ ヘルプ：リンク内の短縮されたプロトコル カプセル化情報を展開するには、リンクの上にマウスを移動します。完全なプロトコル カプセル化名が表示されます。



リンク：テキストの上にマウスを移動します。テキストの色が青から赤に変化した場合、およびカーソルが指の形に変化した場合、そのテキストはリンクです。



指示ボックス：一部のウィンドウでは、コンテンツ領域に操作内容が記述された指示ボックスが表示されます。



はじめに

NAM Traffic Analyzer を効果的に使用するには、決められた一連のタスクを実行する必要があります。

ステップ 1　Setup タブ（図 1-2）を使用して、NAM でのモニタリング収集を設定し、イネーブルにします。詳細については、第 3 章「アプリケーションのセットアップ」を参照してください。

図 1-2　Setup タブ

Setup タブには次のオプションがあります。

- Switch Parameters：NAM とスイッチとの間の接続を確認します。
- Router Parameters：ルータと通信するために NAM が使用するパラメータを設定します。

（注）　Router Parameters オプションは、NM-NAM デバイスに限って使用できます。

- Data Sources：監視のために、スイッチまたはルータからこの NAM に収集されるネットワーク トラフィックを指定します。NetFlow データ ソースの作成にも使用します。
- Monitor：収集および監視するトラフィック統計情報の種類を指定します。
- Protocol Directory：プロトコル グループおよび URL ベースのプロトコルを指定します。
- Alarms：アラーム条件およびしきい値を設定します。
- Preferences：すべての NAM Traffic Analyzer ユーザに適用されるグローバルなプリファレンスを規定します。このプリファレンスによって、データの表示形式が決まります。

ステップ 2　Admin タブ（図 1-3）を使用して、NAM Traffic Analyzer アカウントを作成、編集または削除します。これらのタスクを実行するために必要な権限を備えている必要があります。

詳細については、第 2 章「ユーザおよびシステム管理」を参照してください。

図 1-3　Admin タブ

Admin タブには次のオプションがあります。

- Users：NAM Traffic Analyzer ユーザおよび TACACS+ 認証と認可を追加、削除および編集します。
- System：システム パラメータ、ネットワーク パラメータ、および NAM コミュニティ ストリング設定を規定します。
- Diagnostics：NAM の問題のトラブルシューティングに使用する情報を生成します。

ステップ 3　Monitor タブ（図 1-4）、Reports タブ（図 1-5）、Capture タブ（図 1-6）、および Alarms タブ（図 1-7）を任意の順序で使用して、リアルタイム データ表示の設定、特定の基準を使用したデータのキャプチャ、通知の設定を行います。

Monitor タブ

Monitor タブには、キャプチャ バッファおよびアラームを除く、NAM での特定のモニタリング収集を設定するツールが用意されています。たとえば、会話収集、プロトコル収集、音声収集などがあります。詳細については、第 4 章「データの監視」を参照してください。

図 1-4　Monitor タブ

Monitor タブには次のオプションがあります。

- Overview：最もアクティブなアプリケーション、最もアクティブなホスト、プロトコル スイートおよびサーバ応答時間を含む、いくつかの種類の統計情報が表示されます。
- Apps：アプリケーション プロトコルに基づいて、パケットおよびバイトの分布が表示されます。
- Voice/Video：NAM でイネーブルになっている音声プロトコルから収集されたトラブルシューティング データが表示されます（SCCP、SIP、H.323 および MGCP を含む）。
- Hosts：ネットワーク ホストごとに、RMON1 および RMON2 ホスト テーブルのアクティブなホスト収集の結果が表示されます。
- Conversations：ネットワーク ホストのペアごとに収集された会話データが表示されます。
- VLAN：VLAN の ID またはプライオリティに基づいて、NAM で収集された VLAN データが表示されます。

（注）　VLAN データは、NM-NAM デバイスでは使用できません。

- DiffServ：NAM で収集された Differentiated Services（DiffServ）データに基づいて、パケットおよびバイトの分布が表示されます。
- Response Time：クライアントサーバ アプリケーションの応答時間が表示されます。
- Switch：スイッチ ポートごとに収集されたさまざまなデータが表示されます。
- Router：ルータ インターフェイスの統計情報、状態、および NBAR が表示されます。

(注)　NM-NAM デバイスには、収集されたさまざまなデータをルータ インターフェイス単位で表示する Interface Stats オプションがあります。

- MPLS：MPLS タグごとにトラフィック統計情報が表示されます。

(注)　MPLS データは、NM-NAM デバイスでは使用できません。

Reports タブ

レポート機能（図 1-5）を使用すると、NAM が監視するネットワーク トラフィックに関する短期から中期の履歴データを保存および取得できます。詳細については、第 5 章「レポートの作成と表示」を参照してください。

図 1-5　Reports タブ

Reports タブには次のオプションがあります。

- Basic Reports：レポートを設定および表示します。
- Custom Reports：複数の基本レポートを設定および表示します。
- Scheduled Export：レポートが自動的に生成およびエクスポートされるように設定します。

Capture タブ

Capture タブ（図 1-6）には、キャプチャ バッファ データを設定および表示するウィンドウがあります。詳細については、第 6 章「パケット データのキャプチャとデコード」を参照してください。

図 1-6　Capture タブ

Capture タブには次のオプションがあります。

- Buffers：キャプチャ バッファ（キャプチャ フィルタを含む）の設定および管理、キャプチャの開始および停止、キャプチャしたパケットの表示およびデコードを行います。
- Files：キャプチャ バッファ内のパケットをファイルに保存し、ファイルをデコードおよびダウンロードします。
- Custom Filters：カスタマイズしたキャプチャ フィルタおよび表示フィルタを作成します。

Alarms タブ

Alarms タブ（図 1-7）には、Setup タブで規定したしきい値によって生成されたアラームを表示するメカニズムが用意されています。詳細については、第 7 章「アラームの表示」を参照してください。

図 1-7　Alarms タブ

Alarms タブには次のオプションがあります。

- NAM：NAM MIB しきい値および NAM 音声監視しきい値に関するすべてのしきい値イベントが表示されます。
- Switch：スイッチの Mini-RMON MIB からの RMON logTable が表示されます。

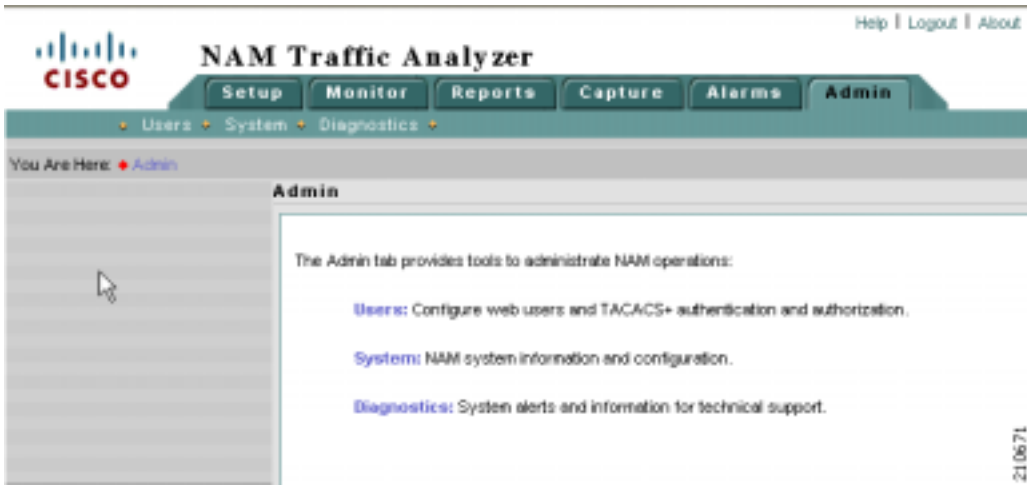
（注）　Switch オプションは、NM-NAM デバイスでは使用できません。

CHAPTER 2

ユーザおよびシステム管理

この章では、ユーザおよびシステム管理タスクの実行と、テクニカル サポートを得るために必要な診断情報の生成について説明します。図 2-1 は、トップレベルの Admin ウィンドウを示しています。

図 2-1　トップレベルの Admin ウィンドウ



この章には、次の項があります。

- ユーザ管理（P.2-2）
- システム管理（P.2-10）
- 診断（P.2-23）

ユーザ管理

NAM インターフェイス カードをスイッチまたはルータに組み込むとき、NAM CLI を使用して HTTP サーバをイネーブルにし、最初に NAM Traffic Analyzer にアクセスするユーザ名とパスワードを設定します。

最初のユーザ アカウントの設定後は、追加のアカウントを作成し、さまざまなアクセス権のレベルをユーザごとに個別にイネーブルまたはディセーブルにできます。これは、RMON 収集の設定、システム パラメータの設定、RMON データの表示など、各ユーザが実行できるタスクに対応する特権を割り当てることで行います。

表 2-1 に、ユーザの特権と、それぞれの特権の説明を示します。

表 2-1　ユーザの特権

特権	アクセス レベル
Account Mgmt	ユーザによるユーザ アカウントの作成、削除、編集が可能です。
System Config	ユーザによる IP アドレス、ゲートウェイ、HTTP ポートなどの基本的な NAM システム パラメータの編集が可能です。
Capture	ユーザによるパケットのキャプチャの実行およびキャプチャ バッファの管理が可能です。 NAM Traffic Analyzer のプロトコル デコードを使用します。
Alarm Config	ユーザによるスイッチ、ルータおよび NAM のアラームの作成、削除、編集が可能です。
Collection Config	ユーザによる次の作成、削除、編集が可能です。 • 収集とレポート • プロトコル ディレクトリ エントリ • プロトコル グループ • URL ベースのアプリケーション
Collection View	ユーザによるモニタリング データとレポートの表示（すべてのユーザに権限あり）が可能です。

ユーザの作成と編集の詳細については、P.2-3 の「新しいユーザの作成」および P.2-4 の「ユーザの編集」を参照してください。

パスワードの回復

スイッチまたはルータで CLI コマンドを使用して、パスワードを回復できます。適切な特権を持つユーザは、NAM CLI とパスワードを工場出荷時のデフォルト状態にリセットできます。Catalyst 6000 および 6500 シリーズ NAM の NAM パスワードのリセットの詳細については、『*Catalyst Network Analysis Module Installation and Configuration Note Release 3.5*』を参照してください。NM-NAM デバイスの NAM パスワードのリセットの詳細については、『*Network Analysis Module (NM-NAM) Feature Module*』を参照してください。NME-NAM デバイスの NAM パスワードのリセットの詳細については、『*Network Analysis Module (NME-NAM) Installation and Configuration Note*』を参照してください。

NAM Traffic Analyzer の管理者（admin）パスワードを忘れた場合は、次のいずれかの方法で回復できます。

- 別のユーザがアカウント管理権限を持っている場合は、パスワードを忘れたユーザを削除してから、Admin タブをクリックし、**Users** をクリックして、別のユーザとしてログインし、新しいユーザを作成します。

- パスワードを忘れたユーザ以外に他のローカル　ユーザが設定されていない場合は、NAM の **rmwebusers** CLI コマンドを使用します。次に、http または https をイネーブルにして NAM Traffic Analyzer ユーザの作成を要求します。

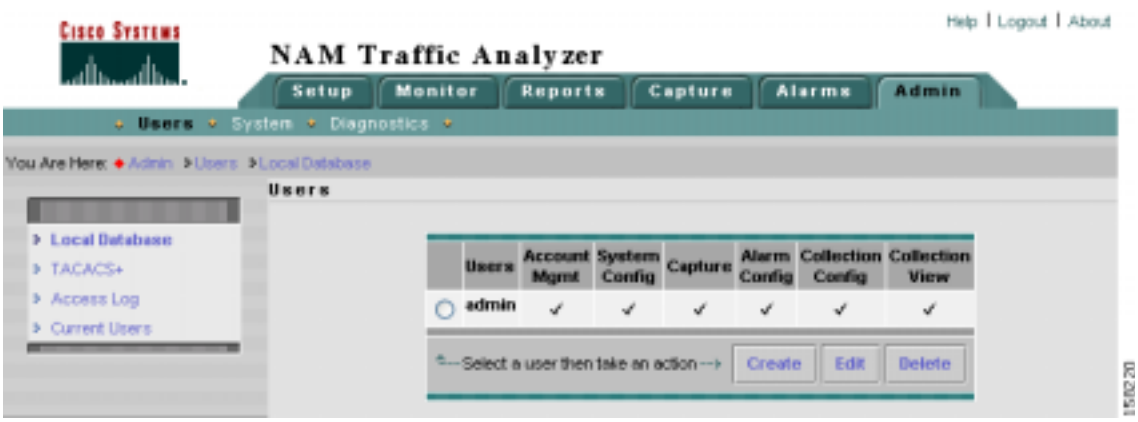
スイッチまたはルータに定義されている NAM ユーザ アカウントの変更

定義済みの root および guest NAM ユーザ アカウント（スイッチまたはルータの **session** コマンドあるいは NAM CLI への Telnet ログインでアクセス可能）は、静的で NAM Traffic Analyzer から独立しています。これらの静的アカウントは変更できません。また、他の CLI ベースのユーザを NAM Traffic Analyzer に追加することもできません。

User Administration GUI

User Administration GUI を使用して、ユーザを管理できます。図 2-2 は、トップレベルの User Admin GUI ウィンドウを示しています。

図 2-2　User Admin GUI



新しいユーザの作成

新しいユーザを作成するには、次の手順を実行します。

ステップ 1　**Admin** > **Users** を選択します。

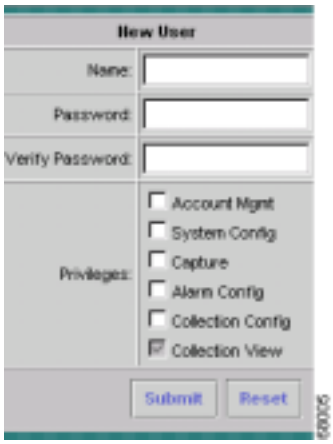
図 2-3 に示すとおり、GUI にローカル データベース内のユーザが表示されます。チェックマークは、一覧された機能に対して各ユーザが特権を持っていることを示しています。

図 2-3　Users テーブル

ステップ 2　**Create** をクリックします。

GUI に New User ダイアログボックス（図 2-4）が表示されます。

図 2-4　New User ダイアログボックス



ステップ 3　新しいユーザを作成するために必要な情報を入力し、新しいユーザに許可する特権を選択します。表 2-2 に、New User ダイアログボックスのフィールドを示します。ユーザの特権の説明については、表 2-1 を参照してください。

表 2-2　New User ダイアログボックス

フィールド	説明	使用法
Name	アカウント名	ユーザのアカウント名を入力します。
Password Verify Password	アカウント パスワード	—
Privileges	このアカウントに関連付ける特権	ユーザに付与する特権をすべて選択します。

（注）　ユーザ名とパスワードは 32 文字以下の英数字にします。

ステップ 4　ユーザを作成するには、**Submit** をクリックします。または、取り消すには、**Reset** をクリックします。

ユーザの編集

ユーザの設定を編集するには、次の手順を実行します。

ステップ 1　**Admin** > **Users** を選択します。

Users テーブルが表示されます。

ステップ 2　ユーザ名を選択します。

ステップ 3　**Edit** をクリックします。

ステップ 4　Modify Users ダイアログボックスで、必要な情報を変更します。各フィールドの説明については、New User ダイアログボックス（図 2-4）を参照してください。

変更を保存するには、**Submit** をクリックします。または、操作を取り消すには、**Reset** をクリックします。

ユーザの削除

ユーザを削除するには、次の手順を実行します。

ステップ 1　**Admin** > **Users** を選択します。

Users テーブルが表示されます。

ステップ 2　ユーザ名を選択します。

ステップ 3　**Delete** をクリックします。

（注）　ユーザのログイン中にユーザ　アカウントを削除した場合、そのユーザはログインしたままで、その特権も保持されます。セッションは、そのユーザがログアウトするまで有効です。セッション中にアカウントを削除、または権限を変更した場合、影響があるのはその後のセッションのみです。ログインしているユーザを強制的にログアウトするには、NAM を再起動します。

TACACS+ 認証および認可の設定

Terminal Access Controller Access Control System（TACACS）は、リモート アクセス認証、認可、およびイベント ロギングなどの関連サービスを提供する認証プロトコルです。TACACS では、ユーザ パスワードと特権は個別のスイッチまたはルータではなく中央データベースで管理されるため、スケーラビリティが得られます。

TACACS+ は、認証および認可に追加サポートを提供するシスコシステムズの拡張です。

ユーザが NAM Traffic Analyzer にログインすると、TACACS+ はユーザ名とパスワードが有効かどうかを判別し、付与されているアクセス特権を判別します。

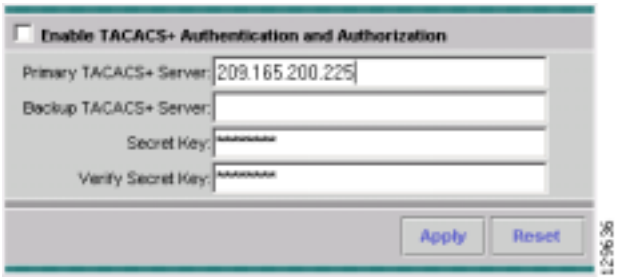
TACACS+ 認証および認可を規定するには、次の手順を実行します。

ステップ 1　**Admin** > **Users** を選択します。

ステップ 2　コンテンツ メニューで **TACACS+** をクリックします。

TACACS+ Authentication and Authorization ダイアログボックス（図 2-5）が表示されます。

図 2-5　TACACS+ Authentication and Authorization ダイアログボックス



ステップ 3　TACACS+ Authentication and Authorization ダイアログボックス（表 2-3）に示されている適切な情報を入力または選択します。

表 2-3　TACACS+ Authentication and Authorization ダイアログボックス

フィールド	使用法
Enable TACACS+ Authentication and Authorization	TACACS+ 認証および認可をイネーブルにするかどうかを決定します。 • イネーブルにする場合は、チェックボックスをオンにします。 • ディセーブルにする場合は、チェックボックスをオフにします。
Primary TACACS+ Server	プライマリ サーバの IP アドレスを入力します。
Backup TACACS+ Server	バックアップ サーバの IP アドレスを入力します（オプション）。 **（注）** プライマリ サーバが 30 秒以内に応答しない場合は、バックアップ サーバに接続されます。
Secret Key	TACACS+ のパスワードを入力します。
Verify Secret Key	TACACS+ のパスワードを再入力します。

ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、**Apply** をクリックします。
- 取り消すには、**Reset** をクリックします。

ヒント　TACACS+ の設定された NAM Traffic Analyzer にログインできない場合は、入力した TACACS+ サーバ名と秘密鍵が正しいことを確認してください。詳細については、P.A-3 の「ユーザ名およびパスワードの問題」を参照してください。

NAM 認証と認可をサポートする TACACS+ サーバの設定

Admin タブから TACACS+ オプションをイネーブルにするだけでなく、NAM Traffic Analyzer ユーザの認証および認可ができるように TACACS+ サーバを設定する必要があります。

（注） 設定方法は、使用する TACACS+ サーバの種類によって異なります。

Cisco ACS TACACS+ サーバの設定

Windows NT および 2000 システムの場合

Cisco ACS TACACS+ サーバを設定するには、次の手順を実行します。

ステップ 1　ACS サーバにログインします。

ステップ 2　**Network Configuration** をクリックします。

ステップ 3　**Add Entry** をクリックします。

ステップ 4　Network Access Server に、NAM ホスト名と IP アドレスを入力します。

ステップ 5　秘密鍵を入力します。

（注） 秘密鍵は、NAM で設定したものと同じにする必要があります。

ステップ 6　Authenticate Using フィールドで、**TACACS+** を選択します。

ステップ 7　**Submit/Restart** をクリックします。

NAM ユーザまたはユーザ グループの追加

NAM ユーザまたはユーザ グループを追加するには、次の手順を実行します。

ステップ 1　**User Setup** をクリックします。

ステップ 2　ユーザのログイン名を入力します。

ステップ 3　**Add/Edit** をクリックします。

ステップ 4　ユーザのデータを入力します。

ステップ 5　**User Setup** を選択します。

ステップ 6　ユーザのパスワードを入力します。

ステップ 7　必要に応じてユーザ グループを割り当てます。

ステップ 8　TACACS+ settings で、次を実行します。

a. **Shell** を選択します。
b. **IOS Command** を選択します。
c. **Permit** を選択します。
d. **Command** を選択します。
e. **web** と入力します。
f. Arguments フィールドに、次のように入力します。

```
permit capture
permit system
permit collection
permit account
permit alarm
permit view
```

ステップ 9　Unlisted Arguments で、**Deny** を選択します。

汎用 TACACS+ サーバの設定

汎用 TACACS+ サーバを設定するには、次の手順を実行します。

ステップ 1　リモート アクセス サーバとして NAM IP アドレスを指定します。

ステップ 2　NAM と通信する TACACS+ サーバの秘密鍵を設定します。

(注)　秘密鍵は、NAM で設定したものと同じにする必要があります。

ステップ 3　NAM へのアクセスを許可するユーザまたはグループごとに、次の TACACS+ パラメータを設定します。

パラメータ	入力
service	`shell`
cmd	`web`

cmd-arg	次のうちの 1 つまたは複数を入力します。
	`accountmgmt`
	`system`
	`capture`
	`alarm`
	`collection`
	`view`

password authentication method：Password Authentication Protocol（PAP）	`pap`

Current User Sessions テーブルの表示

Current User Sessions テーブルは、アプリケーションにログインしているユーザのレコードです。ユーザ セッションは、非アクティブになってから 30 分後にタイムアウトします。ユーザ セッションがタイムアウトすると、その行はテーブルから削除されます。

現在のユーザ セッション テーブルを表示するには、次の手順を実行します。

ステップ 1　**Admin** > **Users** を選択します。

ステップ 2　コンテンツで **Current Users** をクリックします。

Current User Sessions テーブル（表 2-4）が表示されます。

表 2-4　Current User Sessions テーブル

フィールド	説明
User ID	NAM へのログインに使用されたユーザ ID
From	ユーザがログインした接続元のマシン名
Login Time	ユーザがログインした時刻
Last Activity	最後のユーザ アクティビティのタイムスタンプ

システム管理

Admin タブの System オプションでは、次の機能にアクセスできます。

- システム リソース（P.2-10）
- ネットワーク パラメータの設定と表示（P.2-11）
- NAM SNMP システム グループの設定と表示（P.2-12）
- NAM のシステム時刻（P.2-14）
- E メールの設定（P.2-15）
- FTP の設定（P.2-16）
- キャプチャ データ ストレージ（P.2-17）
- Web パブリケーション（P.2-21）

システム リソース

Admin > **System** を選択し、System Overview ウィンドウ（図 2-6）を表示します。

図 2-6　System Overview ウィンドウ

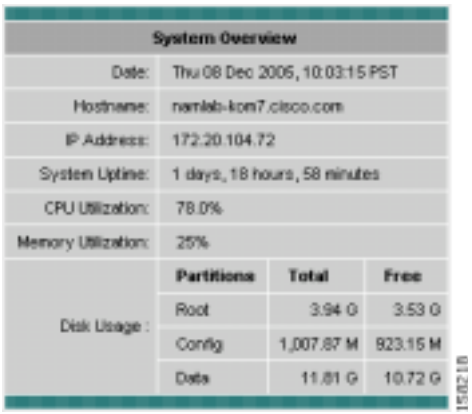


表 2-5 に、System Overview ウィンドウのフィールドを示します。

表 2-5　System Overview

フィールド	説明
Date	現在の日付と時刻（スイッチ、ルータ、または NTP サーバと同期している）
Hostname	NAM ホスト名
IP Address	NAM の IP アドレス
System Uptime	ホストが中断なしで稼動する時間の長さ
CPU Utilization	NAM によって消費される CPU リソースの比率
Memory Utilization	NAM によって消費されるメモリ リソースの比率
Disk Usage	ディスク パーティションと、それぞれの総容量および空き容量を表示

ネットワーク パラメータの設定と表示

ネットワーク パラメータを表示および設定するには、次の手順を実行します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **Network Parameters** をクリックします。

Network Parameters ダイアログボックス（図 2-7）が表示されます。

図 2-7　Network Parameters ダイアログボックス

ステップ 3　Network Parameters ダイアログボックス（表 2-6）で、情報を入力または変更します。

表 2-6　Network Parameters ダイアログボックス

フィールド	説明
IP Address	NAM の IP アドレス
IP Broadcast	NAM のブロードキャスト アドレス
Subnet Mask	NAM のサブネット マスク
IP Gateway	NAM の IP ゲートウェイ アドレス
Host Name	NAM のホスト名
Domain name	NAM のドメイン名
Nameservers	NAM のネーム サーバ アドレス

ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

NAM SNMP システム グループの設定と表示

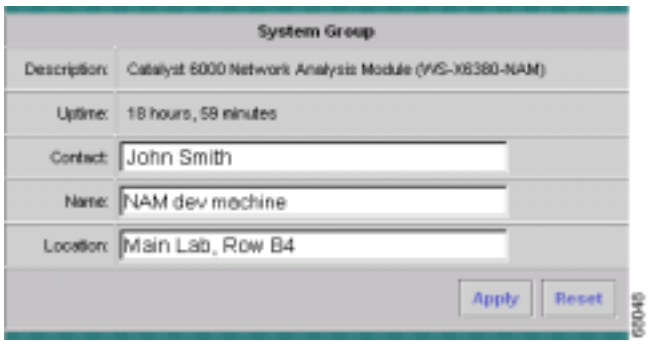
NAM SNMP システム グループを表示および設定するには、次の手順を実行します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **NAM SNMP** をクリックします。

ウィンドウの上部に、SNMP System Group ダイアログボックス（図 2-8）および NAM Community Strings ダイアログボックス（図 2-9）が表示されます。

図 2-8　SNMP System Group ダイアログボックス



ステップ 3　SNMP System Group ダイアログボックス（表 2-7）で、情報を入力または変更します。

表 2-7　SNMP System Group ダイアログボックス

フィールド	説明
Contact	NAM の担当者の名前
Name	NAM の名前
Location	NAM を搭載するスイッチまたはルータの物理的な場所

ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

NAM コミュニティ ストリングの使用

コミュニティ ストリングを使用することにより、他のアプリケーションが、SNMP get および set 要求の NAM への送信、コレクションの設定、データのポーリングなどを実行できるようになります。

NAM コミュニティ ストリングの作成

NAM コミュニティ ストリングを作成するには、次の手順を実行します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **NAM SNMP** をクリックします。

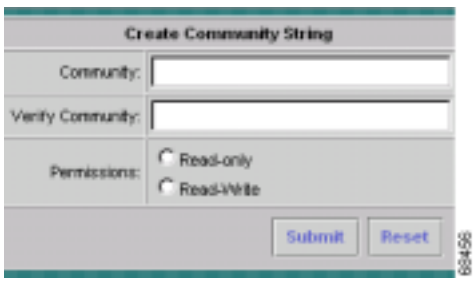
ウィンドウの上部に、NAM Community Strings ダイアログボックス（図 2-9）が表示されます。

図 2-9　NAM Community Strings ダイアログボックス

ステップ 3　エントリを選択して、**Create** をクリックします。

Create Community String ダイアログボックス（図 2-10）が表示されます。

図 2-10　Create Community String ダイアログボックス



ステップ 4　コミュニティ ストリングを入力します（意味のある名前を使用）。

ステップ 5　Verify Community フィールドに、コミュニティ ストリングを再入力します。

ステップ 6　次の基準を使用して、読み取り専用権限、または読み取り / 書き込み権限を割り当てます。

- 読み取り専用は、SNMP MIB 変数への読み取りアクセスのみ可能です（get）。
- 読み取り / 書き込みは、SNMP MIB 変数への完全な読み取りおよび書き込みアクセスが可能です（get と set）。

ステップ 7　次のいずれかを実行します。

- 変更するには、**Submit** をクリックします。
- 取り消すには、**Reset** をクリックします。

NAM コミュニティ ストリングの削除

NAM コミュニティ ストリングを削除するには、次の手順を実行します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **NAM SNMP** をクリックします。

ウィンドウの下部に、NAM Community Strings ダイアログボックス（図 2-9）が表示されます。

ステップ 3　エントリを選択して、**Delete** をクリックします。

注意　NAM コミュニティ ストリングを削除すると、SNMP エージェントの外部から NAM への SNMP 要求がブロックされます。

コミュニティ ストリングが削除されます。

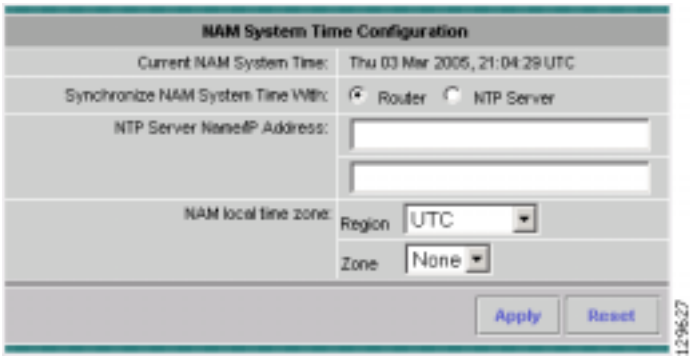
NAM のシステム時刻

NAM は、2 つのソース（スイッチまたはルータと、NTP サーバ）のいずれかから UTC（GMT）時刻を取得します。次のいずれかの方法で、NAM のシステム時刻を設定できます。

- NAM のシステム時刻とスイッチまたはルータの同期（P.2-15）
- NTP サーバによる NAM のシステム時刻の設定（P.2-15）

NAM システム時刻の設定後に、NAM System Time Configuration 画面を使用してローカル時間帯を設定できます。図 2-11 に NAM System Time Configuration 画面を示します。

図 2-11　NAM System Time Configuration 画面



NAM のシステム時刻とスイッチまたはルータの同期

ステップ 1　Switch オプション ボタンまたは Router オプション ボタンをクリックします。

ステップ 2　リストから地域とローカル時間帯を選択します。

ステップ 3　次のいずれかを実行します。

- 変更内容を保存するには、**Apply** をクリックします。
- 設定を元のままにするには、**Reset** をクリックします。

NTP サーバによる NAM のシステム時刻の設定

NTP サーバを使用して NAM のシステム時刻を設定するには、次の手順を実行します。

ステップ 1　NTP Server オプション ボタンを選択します。

ステップ 2　2 つまでの NTP サーバ名または IP アドレスを、NTP sever name/IP Address テキスト ボックスに入力します。

ステップ 3　リストから地域とローカル時間帯を選択します。

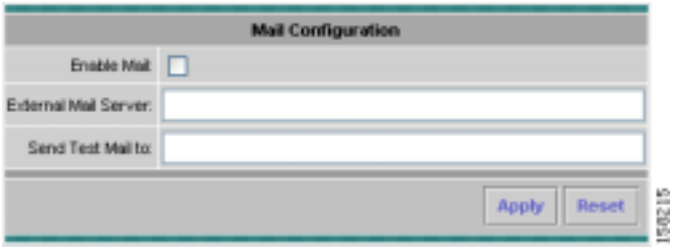
ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、**Apply** をクリックします。
- 設定を元のままにするには、**Reset** をクリックします。

E メールの設定

アラーム通知やレポートを電子メールで送信するように NAM を設定できます。図 2-12 に EMail Configuration ウィンドウを示します。レポートの E メール送信を設定する方法の詳細については、P.5-24 の「スケジュールされたエクスポート」の項の表 5-15、Scheduled Exports ウィンドウのオプションを参照してください。

図 2-12　EMail Configuration ウィンドウ



通知を E メールで送信するように NAM を設定する手順は、次のとおりです。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　**EMail Configuration** をクリックします。

Email Configuration ウィンドウ（図 2-12）が表示されます。表 2-8 に Email Configuration オプションを示します。

表 2-8　Email Configuration オプション

フィールド	説明
Enable Mail	レポートおよびアラーム通知の E メール送信をイネーブルにします。
External Mail Server	外部メール サーバの識別名。
Send Test Mail	最大 3 つまで、E メール受信者の E メール アドレスを一覧表示します。

ステップ 3　**Enable EMail** をオンにします。

ステップ 4　**外部メール サーバ**の識別名を入力します。

ステップ 5　変更内容を保存するには、**Apply** をクリックします。

FTP の設定

アラーム通知やレポートを FTP で送信するように NAM を設定できます。図 2-13 に FTP Configuration ウィンドウを示します。FTP を使用したレポートの転送を設定する方法の詳細については、P.5-24 の「スケジュールされたエクスポート」の項の表 5-15、Scheduled Exports ウィンドウのオプションを参照してください。

図 2-13　FTP Configuration ウィンドウ

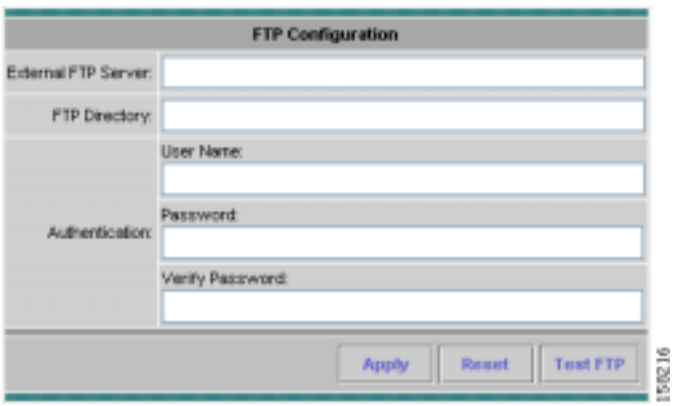


表 2-9 に、FTP の設定に使用するフィールドを示します。

表 2-9　FTP Configuration オプション

フィールド	説明
External FTP Server	FTP サーバのホスト名または IP アドレス
FTP Directory	FTP ファイルが格納されるディレクトリのフル パス名
Authentication	外部 FTP サーバの認証に使用されるユーザ名フィールドとパスワード フィールド

キャプチャ データ ストレージ

Capture Data Storage オプションを使用して、キャプチャ データを格納するリモート ファイル システムを設定できます。データのキャプチャを設定する前に、キャプチャ データ ストレージの場所を設定する必要があります。**Admin** > **Capture Data Storage** を選択し、Capture Data Storage ウィンドウ（図 2-14 ）を開きます。

図 2-14　Capture Data Storage ウィンドウ

この項の内容は、次のとおりです。

- NFS ストレージの場所の作成（P.2-17）
- NFS ストレージの場所の編集（P.2-19）
- iSCSI ストレージの場所の作成（P.2-20）
- iSCSI ストレージの場所の編集（P.2-21）

NFS ストレージの場所の作成

NFS サーバは、NAM がそのサーバに書き込めるように適切に設定する必要があります。NAM は、UID=80（www）および UID=0（ルート）で NFS ディレクトリにアクセスします。NFS ディレクトリは、これらの UID を使用して完全にアクセス可能である必要があります。

これを実行する方法の 1 つが、NFS オプションの *all_squash* を使用して、これらの UID を `anonuid=<userID>` にマップする方法です。ここで、<userID> は、NFS ディレクトリへのフル アクセス権を持つローカル ユーザ ID です。

NFS サーバの設定

次の例は、Linux サーバ内に NAM（IP アドレス 1.1.1.2）がキャプチャ データを格納する NFS ディレクトリ（**/home/SomeUserName**）を設定する方法を示しています。キャプチャ データを格納するための NFS サーバを設定するには、次の手順を実行します。

ステップ 1　ターゲットの NFS ディレクトリに対する読み取りおよび書き込みアクセス権を持つ UID を検索します。

たとえば、ターゲット NFS ディレクトリが **/home/SomeUserName** の場合は、**/etc/password** ファイルを開き、次のように記述されたユーザ エントリを検索します。

```
SomeUserName:x:503:503::/home/SomeUserName:/bin/tcsh
```

この例では、UID は 503 です。

ステップ 2　**/etc/exports** ファイルを編集し、次の行を追加します。

```
/home/SomeUserName    1.1.1.2/255.255.255.255(rw,all_squash,anonuid=503)
```

ステップ 3　変更内容をアクティブにします。

/usr/bin/exportfs -a

（注） NFS ディレクトリに NAM が書き込みできないサブディレクトリが含まれる場合、これらのサブディレクトリは NAM キャプチャ画面には一覧されません。

NAM での NFS ストレージの場所の設定

リモート ファイル システム パーティションを指定して、NFS ストレージの場所を作成する手順は、次のとおりです。

ステップ 1　**Admin** > **Capture Data Storage** を選択します。

Capture Data Storage ウィンドウ（図 2-14）が表示され、設定済みのキャプチャ データ ストレージの場所が一覧されます。

ステップ 2　**Create NFS** をクリックします。

ステップ 3　New NFS Storage ウィンドウで、必要なパラメータを入力します。

表 2-10 に、NFS Storage Location パラメータを示します。

表 2-10　NFS Storage Location パラメータ

フィールド	説明
Name	リモート ファイル システム エントリの名前。
Server	リモート ファイル システム エントリの DNS 名。
Directory	リモート ファイル システム パーティションのパス名。
Basic NFS Options	各フィールドはデフォルト値を表示します。メニューから選択可能な値以外の値を使用する必要がある場合は、Advanced NFS Options を使用します。
Protocol	TCP または UDP を選択します。
Timeout	0.1 ～ 1.0 秒までの値のタイムアウトが設定できます。
NFS Version	NFS バージョンを 1 ～ 4 の中から選択します。
Retries	再試行回数を 1 ～ 5 の範囲で選択します。
Advanced NFS Options	このフィールドは、NFS ストレージの場所を作成するためのデフォルト値を表示します。テキストを編集して、Basic NFS Options のプルダウン メニューの範囲外の NFS オプションを使用できます。

ステップ 4　NFS ストレージの場所を作成するには、**Submit** をクリックします。それ以外の場合は、エントリを削除するには **Reset** をクリックし、変更を取り消すには **Cancel** をクリックします。

NFS ストレージの場所の編集

既存の NFS ストレージの場所を編集する手順は、次のとおりです。

（注）　編集（または変更）する NFS ファイル システム エントリを使用するキャプチャ セッションが設定されている場合は、NFS ファイル システム エントリを編集する前に、それらのキャプチャ セッションを削除する必要があります。アクティブなキャプチャ バッファを見つけるには、**Capture** > **Buffers** をクリックし、次に、*実行中*の各キャプチャを選択して、**Status** をクリックします。キャプチャが編集するファイルシステムを使用している場合は、**Clear** をクリックします。

ステップ 1　**Admin** > **Capture Data Storage** を選択します。

Capture Data Storage ウィンドウ（図 2-14）が表示され、設定済みのキャプチャ データ ストレージの場所が一覧されます。

ステップ 2　変更する NFS ストレージの場所をクリックして選択し、**Edit** をクリックします。

Edit Remote Storage Entry ウィンドウに選択した NFS ストレージの場所のパラメータが表示されます。

ステップ 3　必要に応じてパラメータを変更します。

表 2-10 に、NFS Storage Location パラメータを示します。

ステップ 4　NFS ストレージの場所のパラメータを変更するには、**Submit** をクリックします。それ以外の場合は、すべてのエントリを削除するには **Reset** をクリックし、変更を取り消すには **Cancel** をクリックします。

iSCSI ストレージの場所の作成

NAM キャプチャ データを格納するための iSCSI ストレージの場所を作成する手順は、次のとおりです。

ステップ 1　**Admin** > **Capture Data Storage** を選択します。

Capture Data Storage ウィンドウ（図 2-14）が表示され、設定済みのキャプチャ データ ストレージの場所が一覧されます。

ステップ 2　**Create iSCSI** をクリックします。

ステップ 3　New iSCSI Storage ウィンドウで、必要なパラメータを入力します。

表 2-11 に、iSCSI Storage Location パラメータを示します。

表 2-11　iSCSI Storage Location パラメータ

フィールド	説明
Name	リモート ストレージ エントリの名前。
Server	iSCSI サーバの DNS ホスト名または IP アドレス。
Target Name	リモート iSCSI サーバに設定されている iSCSI ターゲットの名前。
Format Disk:	**Format a new partition** をオンにすると、NAM は iSCSI ターゲットを単一の Linux パーティションとしてフォーマットします。 リモート iSCSI ターゲット ディスクがフォーマット済みで、パーティション テーブルが存在する場合は、**Use existing partition#** をオンにします。

ステップ 4　iSCSI ストレージの場所を作成するには、**Submit** をクリックします。それ以外の場合は、エントリを削除するには **Reset** をクリックし、変更を取り消すには **Cancel** をクリックします。

（注）　新しい iSCSI ストレージ エントリを有効にする前に、NAM システムをリブートする必要があります。

iSCSI ストレージの場所の編集

既存の iSCSI ストレージの場所を編集する手順は、次のとおりです。

(注) 編集（または変更）する iSCSI ファイル システム エントリを使用するキャプチャ セッションが設定されている場合は、iSCSI ファイル システム エントリを編集する前に、それらのキャプチャ セッションを削除する必要があります。アクティブなキャプチャ バッファを見つけるには、**Capture** > **Buffers** をクリックし、次に、*実行中*の各キャプチャを選択して、**Status** をクリックします。キャプチャが編集するファイルシステムを使用している場合は、**Clear** をクリックします。

ステップ 1　**Admin** > **Capture Data Storage** を選択します。

Capture Data Storage ウィンドウ（図 2-14）が表示され、設定済みのキャプチャ データ ストレージの場所が一覧されます。

ステップ 2　変更する iSCSI ストレージの場所をクリックして選択し、**Edit** をクリックします。

選択した iSCSI ストレージの場所のパラメータを示すウィンドウが表示されます。

ステップ 3　必要に応じてパラメータを変更します。

表 2-11 に、iSCSI Storage Location パラメータを示します。

ステップ 4　iSCSI ストレージの場所のパラメータを変更するには、**Submit** をクリックします。それ以外の場合は、エントリを削除するには **Reset** をクリックし、変更を取り消すには **Cancel** をクリックします。

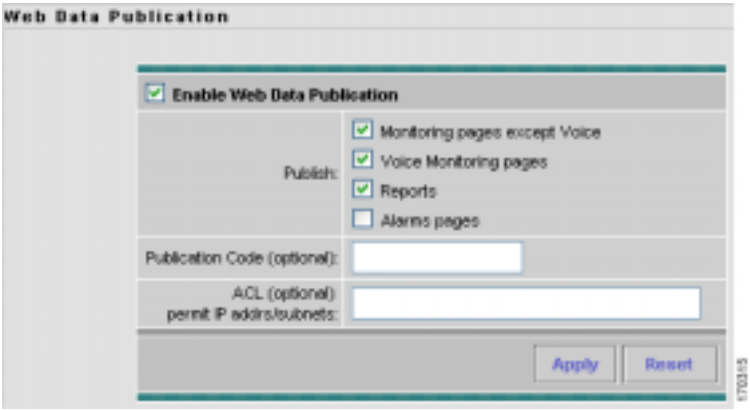
(注) iSCSI ストレージ エントリの変更内容を有効にする前に、NAM システムをリブートする必要があります。

Web パブリケーション

Web パブリケーションでは、一般の Web ユーザや Web サイトが、ログイン セッションを確立することなく、選択された NAM のモニタ画面やレポート画面にアクセス（または、リンク）できます。

Web パブリケーションは、オープンにすることもできれば、Access Control List（ACL; アクセス コントロール リスト）またはパブリケーション コード、もしくは両方を使用して制限することもできます。公開されたデータにアクセス可能にするために、必要な場合は、パブリケーション コードを URL アドレスまたはクッキーで提供する必要があります。図 2-15 に、Web Data Publication ウィンドウ を示します。

図 2-15　Web Data Publication ウィンドウ



Web パブリッシングをイネーブルにするには、次の手順を実行します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　System メニューで、**Web Publishing** をクリックします。

ステップ 3　Web パブリッシングで使用可能にする各項目をオンにします。

表 2-12、Web Data Publication プロパティに、Enable Web Publishing ウィンドウのフィールドを示します。

表 2-12　Web Data Publication プロパティ

フィールド	説明
Monitoring pages except Voice	オンにすると、Voice Monitoring 画面以外のすべての Monitor 画面を公開します。
Voice Monitoring pages	オンにすると、Voice Monitoring 画面を公開します。
Reports	オンにすると、すべてのレポートを公開します。
Alarms pages	オンにすると、NAM and Switch Alarms ページを公開します。
Publication Code	公開されたページにアクセスするために、URL のクッキーに必要なパスコード。たとえば、*abc123* に設定されたパブリケーション コードでは、次の URL にある公開された **Monitor** > **PortStat** ウィンドウにアクセスできます。 http://<nam-hostname>/monitor/sup/ether/supetherstats.php?sortCol=utilization&publicationcode=abc123
ACL permit IP addrs/subnets	何も入力しないと、対象を問わずオープンなアクセスを提供します。 IP アドレスまたはサブネットを入力すると、それらの IP アドレスまたはサブネットだけに、Web パブリケーションへのアクセスを許可します。

ステップ 4　Web パブリッシングをイネーブルにするには、**Apply** をクリックします。または、操作を取り消すには、**Reset** をクリックします。

診断

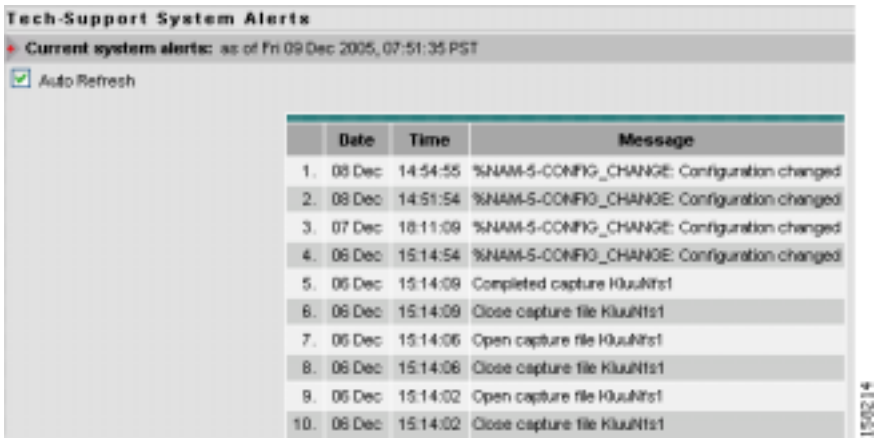
Admin タブの Diagnostics オプションには、トラブルシューティングを支援するツールがあります。Cisco Technical Assistance Center（TAC）からのサポートが必要な問題が発生したときに、これらのツールを使用できます。次のオプションがあります。

- システム アラートの表示
- 設定情報の監視とキャプチャ
- テクニカル サポートの表示

システム アラートの表示

通常の運用中に NAM Traffic Analyzer が検出した障害または問題を表示できます。System Alerts ページを表示するには、**Admin** > **Diagnostics** を選択します。System Alerts はデフォルト ページです。図 2-16 に、System Alerts ウィンドウを示します。

図 2-16　System Alerts ウィンドウ



各アラートに、日付、アラートが発生した時刻、アラートを説明するメッセージが示されます。

アラートの発生状況に気付き、アラートの原因となっている状況をトラブルシューティングし解決しようとする場合は、**Clear** をクリックしてアラートのリストを削除し、追加のアラートが発生するかどうかを確認します。

監査証跡の表示

Audit Trail オプションは、内部の **syslog** ログ ファイルに記録された最近の重要なアクティビティのリストを表示します。また、syslog メッセージを外部のログに送信することもできます。

監査証跡には、次のユーザ アクティビティが記録されます。

- すべての CLI コマンド
- ユーザ ログイン（失敗した試行を含む）
- 不正アクセスの試行
- SPAN の変更
- NDE データ ソースの変更

- データ収集のイネーブル化およびディセーブル化
- レポートの作成および削除
- キャプチャの開始および停止
- ユーザの追加および削除

各ログ エントリには、次の情報が含まれます。

- ユーザ ID
- タイムスタンプ
- IP アドレス（リモート Web アクセスの場合）
- アクティビティの説明

Audit Trail ウィンドウにアクセスするには、次の手順を実行します。

ステップ 1　**Admin** > **Diagnostics** を選択します。

ステップ 2　**Audit Trail** をクリックします。

Audit Trail ウィンドウ（図 2-17）が表示されます。

Audit Trail ウィンドウでは、ユーザ アクセス ログを表示し、時刻、ユーザ、実行元（IP アドレス）、またはアクティビティに基づいてエントリをフィルタできます。内部ログ ファイルは、一定のサイズ制限に達すると、順次、別の新たなログ ファイルが作成され記録されます。

図 2-17　Audit Trail ウィンドウ

設定情報の監視とキャプチャ

Monitor and Capture Configuration オプションには、NAM Traffic Analyzer およびその他の管理アプリケーションで設定された NAM データ収集に関する情報が含まれています。Owner カラムに名前 LocalMgr が表示された場合、その収集は NAM Traffic Analyzer で設定されたものです。

Cisco Technical Assistance Center（TAC）からのサポートが必要な問題が発生したときに、この情報を保存できます。

一般的な収集をいくつか示します。

表 2-13　収集タイプ

収集タイプ	作成元
host、hlhost	Host Monitor
matrix、hlmatrix	Conversation Monitor
art	Response Time Monitor
buffer、channel、filter	Capture
ds-	DiffServ Monitor
h323-voice-coll sccp-voice-coll mgcp-voice-coll	Voice Monitor
http-url-coll	HTTP URL Collection
http-url-filter	HTTP URL Filter
vlanstat、priostat	VLAN Monitor
prdist	Apps Monitor
nde-path	カスタム NetFlow データ ソース

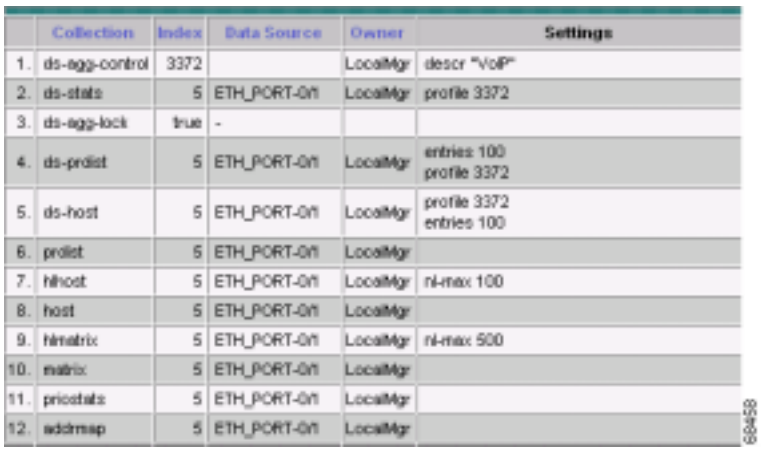
設定情報を監視およびキャプチャするには、次の手順を実行します。

ステップ 1　**Admin** > **Diagnostics** を選択します。

ステップ 2　コンテンツ メニューで **Monitor and Capture Configuration** をクリックします。

NAM が Monitor and Capture Configuration ウィンドウ（図 2-18）を表示します。

図 2-18　Monitor and Capture Configuration ウィンドウ



ステップ 3　情報を保存するには、ブラウザ メニューで **File>Save As...** を選択します。

ステップ 4　出力先、ファイル名、形式を選択して、**Save** をクリックします。

テクニカル サポートの表示

NAM の syslog は NAM システム アラートを記録します。アラートには、イベント内容の日付およびタイムスタンプが含まれ、予期しない、または潜在的に重大な状態が示されます。この機能によって、潜在的で広範囲にわたるさまざまな内蔵システムのトラブルシューティング コマンドおよびシステム ログの結果が表示される可能性があります。

この情報は、普通のユーザにはあまり重要ではありません。これは、Cisco TAC がデバッグを目的として使用するためのものです。この情報を理解する必要はありませんが、情報を保存し、Cisco TAC への電子メール メッセージに添付する必要があります。

Tech-Support ページを表示するには、**Admin** > **Users** ページで System Config ユーザ特権をイネーブルにする必要があります。ユーザ特権の編集については、P.2-4 の「ユーザの編集」を参照してください。

（注）　この情報は、NAM CLI で表示することもできます。NAM CLI の使用方法については、『*Cisco Network Analysis Module Command Reference*』、NM-NAM デバイスについては、『*Network Analysis Module (NM-NAM)* Feature Module』を参照してください。

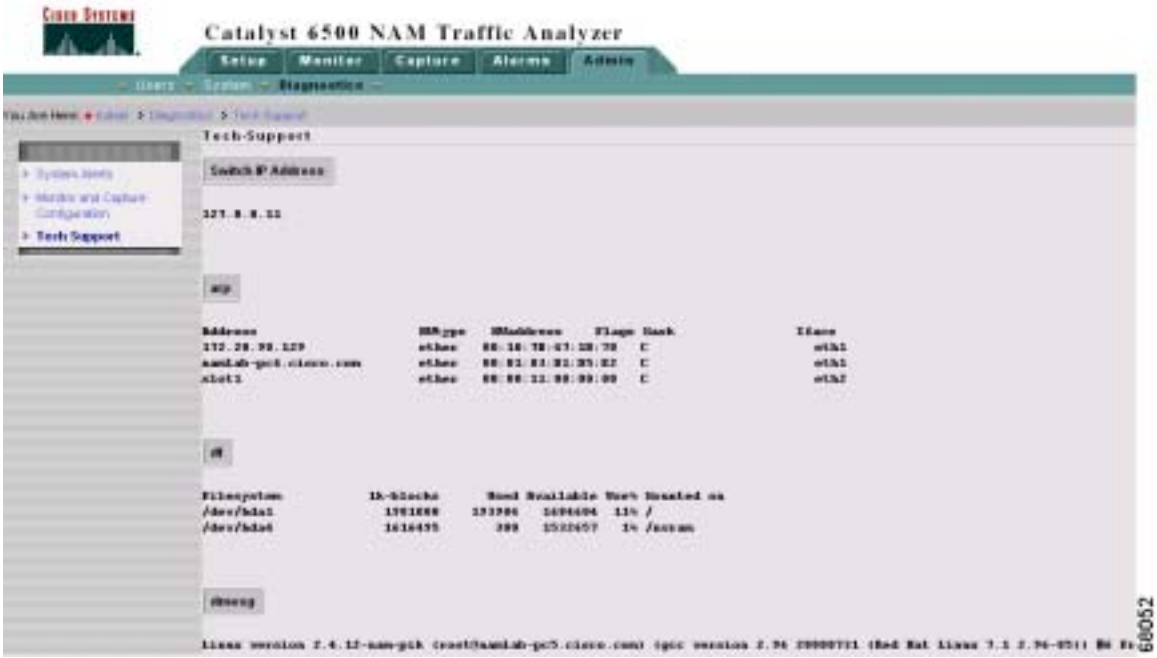
テクニカル サポートを表示するには、次の手順を実行します。

ステップ 1　**Admin** > **Diagnostics** を選択します。

ステップ 2　コンテンツで **Tech Support** をクリックします。

数分後、大量の診断情報が生成され、Diagnostics Tech Support ウィンドウ（図 2-19）に表示されます。

図 2-19　Diagnostics Tech Support ウィンドウ



ステップ 3　情報を保存するには、ブラウザ メニューで **File>Save As...** の順に選択します。

Internet Explorer を使用している場合は、ページ上部にある **Save This Page** ボタンをクリックすると、Tech-Support ページをテキスト ファイルとしてダウンロードできます。

ステップ 4　出力先、ファイル名、ファイル形式を選択して、**Save** をクリックします。

コア ファイルのダウンロード

Tech-Support ページからコア ファイルをダウンロードするには、Core Files セクションまで下にスクロールして、ファイル名をクリックします。

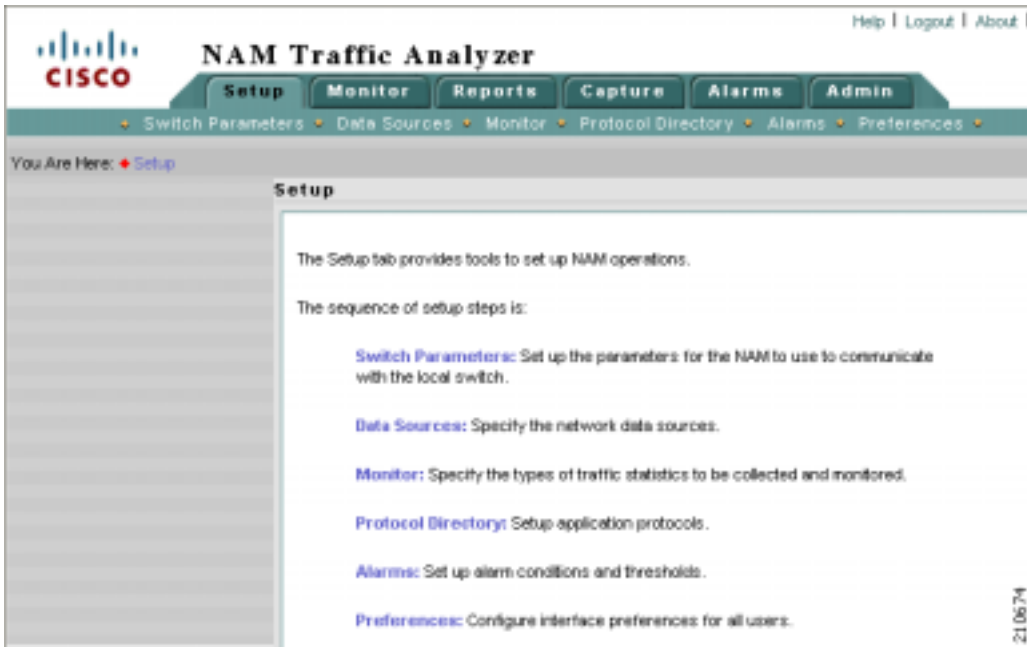
■ 診断

CHAPTER 3

アプリケーションのセットアップ

NAM Setup ウィンドウ（図 3-1）を使用して、NAM アプリケーションをセットアップおよび設定できます。NAM アプリケーションは、次に示す順序でセットアップします。

図 3-1　Setup ウィンドウ



この章には、次の項があります。

- スイッチ パラメータ（P.3-2）
- ルータ パラメータ（P.3-7）
- データ ソースのセットアップ（P.3-8）
- 監視のセットアップ（P.3-34）
- プロトコル ディレクトリのセットアップ（P.3-45）
- アラームしきい値の設定（P.3-56）
- グローバル プリファレンスの設定（P.3-68）

スイッチ パラメータ

Switch Parameter ウィンドウから、スイッチ システム情報の表示、NBAR のイネーブル化またはディセーブル化、ポート統計情報（Mini-RMON）のイネーブル化またはディセーブル化、およびスイッチ ログインの設定を実行できます。

- スイッチ情報の表示（P.3-2）
- NBAR プロトコル検出のセットアップ（P.3-3）
- ポート統計情報（Mini-RMON）のイネーブル化およびディセーブル化（P.3-4）
- スイッチ ログインの設定（P.3-6）

スイッチ情報の表示

（注）　この項は、WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスに適用されます。

Switch Information（表 3-1）を表示するには、**Setup** > **Switch Parameters** を選択します。

表 3-1　Switch Information

フィールド	説明
SNMP Test information	SNMP テストが発生した NAM およびスイッチの IP アドレスを表示します。
Name	スイッチの名前。
Hardware	スイッチのハードウェア記述。
Supervisor Software Version	Supervisor の現在のソフトウェア バージョン。
System Uptime	スイッチの合計稼動時間。
Location	スイッチの物理的な場所。
Contact	スイッチのネットワーク管理者の連絡先。
SNMP read from switch	SNMP 読み取りテストの結果。
SNMP write to switch	SNMP 書き込みテストの結果。
Mini-RMON on switch	Catalyst OS デバイスの場合は、Mini-RMON がイネーブル（Available）またはディセーブル（Unavailable）のどちらの状態であるかを表示します。 Cisco IOS デバイスの場合は、Mini-RMON が設定されているポートがある（Available）またはない（Unavailable）のどちらの状態であるかを表示します。
NBAR on switch	スイッチで NBAR が使用できるかどうかを表示します。
VLAN Traffic Statistics on Switch	VLAN データが Available であるか、または Unavailable であるかを表示します。 （注）　Catalyst 6500 シリーズのスイッチでは、Supervisor 2 カードまたは MSFC2 カードが必要です。

表 3-1　Switch Information（続き）

フィールド	説明
NetFlow Status	Catalyst OS デバイスの場合は、*リモート* NetFlow がスイッチに設定されていると、ポート < 番号 > の < アドレス > へのリモート エクスポートが表示されます。*ローカル* NetFlow がスイッチに設定されていると、モジュール < モジュール番号 > へのローカル エクスポートが表示されます。 Cisco IOS を実行している Catalyst 6500 シリーズのデバイスの場合は、NetFlow がスイッチに設定されていると、ポート < 番号 > の NAM < アドレス > へのリモート エクスポートが表示されます。設定されていない場合は、状態として Configuration unknown と表示されます。

NBAR プロトコル検出のセットアップ

Router Parameter ウィンドウまたは Switch Parameter ウィンドウから、NBAR Status 情報を表示したり、すべてのインターフェイス上で NBAR をイネーブルまたはディセーブルにしたりできます。NBAR プロトコル検出をセットアップするには、**Setup > Switch**（または）**Router Parameters > NBAR Protocol Discovery** を選択します。

次のオプションを含む NBAR Status ウィンドウが表示されます。

- **Details**：クリックすると、NBAR Interface Details（図 3-2 および表 3-2 を参照）が表示されます。
- **Save**：クリックすると、デバイスの実行コンフィギュレーションが保存されます。
- **Enable**：クリックすると、使用できるすべてのインターフェイス上で NBAR がイネーブルになります。
- **Disable**：クリックすると、すべてのインターフェイス上で NBAR がディセーブルになります。

（注） Save ボタンは、Cisco IOS を実行するスイッチだけで使用可能です。変更は Catalyst OS を実行するスイッチにすぐに反映されます。

図 3-2　NBAR Interface Details

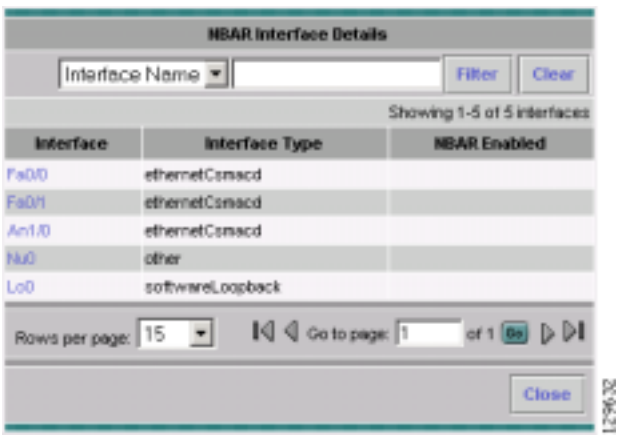


表 3-2　NBAR Interface Details

フィールド / 動作	説明
Interface	インターフェイスの名前。
Interface Type	インターフェイスの説明。
NBAR Enabled	チェック マークが付いている場合、NBAR はイネーブルになっています。

ヒント　Interface Details テーブル内の特定のインターフェイス名やインターフェイス タイプのデータを表示するには、テキスト ボックスにそのインターフェイス名またはインターフェイス タイプを入力してから、**Filter** をクリックします。Filter テキスト ボックスをクリアするには、**Clear** をクリックします。

ポート統計情報（Mini-RMON）のイネーブル化およびディセーブル化

Port Stats（Mini-RMON）テーブルを使用すると、使用可能な Port Stats 上の Mini-RMON をイネーブルまたはディセーブルにして、Mini-RMON がイネーブルになっている Port Stats に詳細を表示できます。また、このテーブルでは Port Stats と Mini-RMON の現在の状態を、次のように表示します。

- Enabled：Mini-RMON の使用可能なすべてのポートで Mini-RMON がイネーブルになっている。
- Partially Enabled：Mini-RMON の使用可能な一部のポートで Mini-RMON がイネーブルになっている。
- Disabled：Mini-RMON の使用可能なポートがすべてディセーブルになっている。

（注）　すべてのポートをディセーブルにすると、これらのポート用に存在しているレポートと警告に影響を与えます。Catalyst OS を実行するデバイスの場合、すべてのポートをディセーブルにすると、Mini-RMON を使用している他のアプリケーションもディセーブルになります。Cisco IOS を実行するデバイスの場合、モニタ オーナー ポートだけがディセーブルになります。

（注）　この項は、WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスに適用されます。

インターフェイスをイネーブルまたはディセーブルにしたり、ポート統計情報の詳細を表示したりするには、次の手順を実行します。

ステップ 1　**Setup**> **Switch Parameters** をクリックします。

Switch Information （表 3-1）が表示されます。

ステップ 2　コンテンツで **Port Stats (Mini-RMON)** をクリックします。

Port Stats (Mini-RMON) ダイアログボックスが表示されます。

ステップ 3　次のいずれかを実行します。

- インターフェイスをすべてイネーブルにするには、**Enable** をクリックします。
- インターフェイスをすべてディセーブルにするには、**Disable** をクリックします。
- Port Stats の詳細を表示するには、**Details** をクリックします。P.3-5 の「Port Stats (Mini-RMON) Details の表示」を参照してください。
- 起動設定（NVRAM）に設定を保存するには、**Save** をクリックします。

（注）　Save ボタンは、Cisco IOS を実行するスイッチだけで使用可能です。変更は Catalyst OS を実行するスイッチにすぐに反映されます。

Port Stats (Mini-RMON) Details の表示

ステップ 1　Port Stats の詳細を表示するには、Port Stats (Mini-RMON) ダイアログボックスで **Details** をクリックします。

Port Stats (Mini-RMON) Details（表 3-3）が表示されます。

表 3-3　Port Stats (Mini-RMON) Details

フィールド	説明
Port Name	ポートの名前。
Port Type	ポートのタイプ。
Mini-RMON Enabled	Mini-RMON がポート上でイネーブルになっているかどうかをチェックマークで示します。

ステップ 2　個々の Port Stat の詳細を表示するには、Port Name をクリックします。Port Stat Details ウィンドウに、次の情報が表示されます。

- Alias：ユーザ定義のポート名。
- Description：ポートの説明。
- Type：ポートのタイプ。
- Mtu：ポートが処理できる最大パケット サイズ（バイト単位）。
- Speed：ポートのスピード（ビット / 秒）。
- Physical Address：スイッチ内のポートの物理アドレス。
- Operational Status：ポートの現在の稼動状態。
- Admin Status：ポートの現在の管理状態。

ヒント　Port Stats (Mini-RMON) Details テーブル内の特定のポート名やポート タイプのデータを表示するには、テキスト ボックスにそのポート名またはポート タイプを入力してから、**Filter** をクリックします。

スイッチ ログインの設定

NAM は、スイッチ ログイン情報を使用してスイッチにログインし、MPLS を監視します。ユーザ名、パスワード（必要な場合）、およびログイン方法（telnet または SSH）を入力する必要があります。表 3-4 に、Switch Login Configuration ウィンドウのフィールドと機能を示します。

(注)　ネットワーク内で MPLS を使用していない場合、スイッチ ログイン設定は必要ありません。

表 3-4　Switch Login Configuration

フィールド	説明
User Name	スイッチ管理者のユーザ名。
PasswordVerify Password	スイッチ管理者のパスワード（必要な場合）。
Verify Password	スイッチ管理者の確認用パスワード（必要な場合）。
Login Method	telnet または SSH のどちらかを選択します。
Test Login	現在のスイッチ ログイン設定または新たに入力した設定（適用されていない場合でも）を使用してテスト ログインを実行します。
Apply	クリックすると、スイッチ ログイン設定を設定または変更します。
Reset	入力されたが適用されていないスイッチ ログイン設定を削除し、以前に保存された設定を復元します。
Clear	データベースからスイッチ ログイン設定を削除します。

ルータ パラメータ

Router Parameter ウィンドウから、ルータ情報を表示したり、NBAR プロトコル検出をセットアップしたりできます。

- ルータ システム情報の適用
- NBAR プロトコル検出のセットアップ

ルータ システム情報の適用

この項では、ルータ パラメータの設定方法を説明します。

(注)　この項の内容は、NM-NAM デバイスにしか適用できません。

ステップ 1　**Setup** > **Router Parameters** を選択します。

Router System Information ウィンドウは、表 3-5 のように表示されます。

表 3-5　Router System Information

フィールド	説明
Name	ルータの名前。
Hardware	ルータのハードウェア記述。
Router Software Version	ルータの現在のソフトウェア バージョン。
System Uptime	スイッチの合計稼動時間。
Location	ルータの物理的な場所。
Contact	ルータのネットワーク管理者名。
Router IP Address	ルータの IP アドレス。
SNMP Read-Write Community String	ルータに設定された SNMP リード / ライト（read/write）コミュニティ ストリング名。
Verify String	SNMP コミュニティ ストリングを確認します。
Netflow Active Timeout	ルータがアクティブなフローを削除する前に待機する分単位の長さ（1 ～ 60）。

ステップ 2　次の情報を入力します。

- Router IP Address
- SNMP Read Community String
- Verify String

データ ソースのセットアップ

NAM には、次の 4 つのバージョンがあります。

- WS-SVC-NAM-1
- WS-SVC-NAM-2
- NME-NAM
- NM-NAM

NME-NAM デバイスには、2 つのギガビット イーサネット ポート（内部インターフェイスと外部インターフェイス）があります。NM-NAM デバイスには、2 つの FastEthernet データ ソース（内部インターフェイスと外部インターフェイス）があります。2 つのインターフェイスのいずれかは、IP トラフィック（HTTP や SNMP など）用の NAM 管理ポートとして選択する必要があります。NAM は、内部インターフェイス、外部インターフェイス、またはその両方を同時に分析するためにトラフィックを監視します。通常、内部インターフェイスの LAN トラフィックと WAN トラフィックを監視するように設定します。ただし、外部インターフェイスは LAN トラフィックを監視するために使用できます。

次に、WS-SVC-NAM-1 および WS-SVC-NAM 2 デバイス用の NetFlow および SPAN セッションの設定方法について説明します。

WS-SVC-NAM-1 デバイスは、1 つのアクティブ SPAN セッションだけを持つことができます。スイッチ ポート、VLAN、または EtherChannel を SPAN ソースとして選択できますが、選択できる SPAN タイプは 1 つだけです。WS-SVC-NAM-2 デバイスおよびスイッチ ソフトウェアでは、2 つの SPAN 宛先ポートがサポートされています。

データを監視するには、まずスイッチを流れる特定のトラフィックを、監視用に NAM に向ける必要があります。トラフィックの方向指定の方法の表（表 3-6）に示されている方法に従ってください。

表 3-6　トラフィックの方向指定の方法

方法	使用法
スイッチ SPAN	物理ポート、VLAN、または EtherChannel のセットのいずれかを NAM に向けることができます。 SPAN ソースとして EtherChannel を選択すると、EtherChannel を構成するすべての物理ポートを SPAN ソースとして選択することになります。 **（注）** この方法は、NM-NAM デバイスには適用されません。
スイッチ Remote SPAN（RSPAN）	リモート スイッチからのすべてのトラフィックが、指定された RSPAN VLAN 上にあるローカル スイッチに届く場合、リモート スイッチからのパケット ストリームを監視できます。NAM の SPAN ソースとして、RSPAN VLAN を使用します。 **（注）** この方法は、NM-NAM デバイスには適用されません。
NetFlow データ エクスポート（NDE）	NDE レコードは、リモート スイッチまたはルータから直接監視できます。スイッチ CLI を使用して、ローカル スイッチまたはリモート ルータで NAM の NDE ソースを設定する必要があります。 SPAN ソースおよび NDE ソースは、同時に有効にできます。

SPAN セッション

(注)　この項は、WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスに適用されます。

SPAN ソース（表 3-7）に、SPAN ソースとして使用できるトラフィック ストリームを示します。

表 3-7　SPAN ソース

SPAN ソース	次のうちの 1 つを選択
物理ポートの任意のセット	• NAM Traffic Analyzer • スイッチ CLI • Supervisor portCopyTable（SNMP）
任意の EtherChannel	• NAM Traffic Analyzer • スイッチ CLI • Supervisor portCopyTable（SNMP）
ローカル スイッチ上に設定された任意の VLAN のセット	• NAM Traffic Analyzer • スイッチ CLI • Supervisor portCopyTable（SNMP）
リモート スイッチから RSPAN 経由で着信するパケット (注) SPAN ソースとして選択できる RSPAN VLAN は 1 つだけです。	• NAM Traffic Analyzer • スイッチ CLI • Supervisor portCopyTable（SNMP） *および* • リモート スイッチ上の設定

NAM 収集に取り込むパケット ストリームとして、ローカルに生成された NDE レコード（NDE ソース）も使用できます。NDE ソースでアクティブにできるのは、NDE 収集タイプの表（表 3-8）で定義された NAM 収集タイプのサブセットだけです。

(注)　これらは NDE ソースで監視がサポートされている唯一の収集タイプです。NDE レコードには、他の収集タイプを実装できるだけの十分な情報がありません。

表 3-8　NDE 収集タイプ表

収集タイプ	ソース
Protocol	RMON2 プロトコル分布テーブル
Host	RMON2 nlHost および alHost テーブル
Conversation	RMON2 nlMatrix および alMatrix テーブル
DiffServ stat	リモート スイッチおよびリモート ルータの DSMON 統計情報テーブル
DiffServ apps	リモート スイッチおよびリモート ルータの DSMON アプリケーション テーブル
DiffServ hosts	リモート スイッチおよびリモート ルータの DSMON ホスト テーブル

SPAN セッションの作成

（注）　この項は、WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスに適用されます。

SPAN セッションの作成方法は、Catalyst OS ソフトウェアが稼動するスイッチと Cisco IOS ソフトウェアが稼動するスイッチで異なります。特に明記しない限り、次の手順は、Catalyst OS および Cisco IOS ソフトウェアの両方を実行するスイッチに適用されます。

ステップ 1　**Setup** > **Data Sources** を選択します。

Active SPAN Sessions ダイアログボックス（表 3-9）が表示されます。デフォルトで NAM に向けた SPAN セッションが選択されています。または最初のオプション ボタンが選択されています。

表 3-9　Active SPAN Sessions ダイアログボックス

カラム	説明
Monitor Session	SPAN の監視セッション。 （注）　Cisco IOS ソフトウェアが稼動するスイッチのみ。
Type	SPAN ソースのタイプ。
Source - Direction	SPAN セッションのソースおよび SPAN トラフィックの方向。 ポート SPAN タイプの場合、ソースにはポート名と、SPAN 実行後のソースの状態（ダウン、テスト中、休止）が表示されます。 SPAN セッション作成時は、ポートの状態に関係なく、すべてのポートを選択できます。 （注）　Cisco IOS ソフトウェアが稼動するスイッチのみ。
Dest.Port	SPAN セッションの宛先ポート。
Dest.Module	SPAN セッションの宛先モジュール。
Status	SPAN セッションのステータス。

ステップ 2　**Create** をクリックします。

Create SPAN Session ダイアログボックス（表 3-10）が表示されます。SPAN Type のデフォルトは SwitchPort です。

ステップ 3　適切な情報を選択します。

表 3-10　Create SPAN Session ダイアログボックス

フィールド	説明
Monitor Session	SPAN の監視セッション。 **（注）** Cisco IOS または Catalyst OS 8.4（および、それ以降）ソフトウェアを実行しているスイッチの場合だけです。
SPAN Type	• SwitchPort • VLAN • EtherChannel • RSPAN VLAN **（注）** SPAN セッションごとに設定できる RSPAN VLAN ソースは 1 つだけです。
Switch Module List	NAM およびスイッチ ファブリック モジュール以外のスイッチ上のモジュールをすべて一覧表示。
SPAN Destination Interface	データの送信先の NAM インターフェイス。
SPAN Traffic Direction	• Rx（受信） • Tx（送信） • Both（両方向） **（注）** SPAN Type が RSPAN VLAN の場合は適用されません。
Available Sources	選択された SPAN タイプで使用できる SPAN ソース。
Add	選択された SPAN ソースを追加。
Remove	選択された SPAN ソースを削除。
Remove All	すべての SPAN ソースを削除。
Selected Sources	選択された SPAN ソース。
Refresh ボタン	NAM によって、現在の設定でスイッチ設定情報を更新。
Submit ボタン	SPAN 設定を作成。

ステップ 4　SPAN セッションを送信するには、**Submit** をクリックします。

Catalyst OS ソフトウェアだけが稼動するスイッチの場合、Active SPAN Sessions ウィンドウが表示され、SPAN セッションが保存されます。

ステップ 5　Cisco IOS ソフトウェアだけが稼動するスイッチで、実行コンフィギュレーションの現在のアクティブ SPAN セッションを起動設定に保存するには、Active SPAN Sessions ウィンドウで **Save** をクリックします。

（注） Cisco IOS ソフトウェアが稼動するスイッチの場合、保留中の実行コンフィギュレーションの変更がすべて起動設定に保存されます。

SPAN セッションの編集

編集できる SPAN セッションは、NAM に向けられたものだけです。

（注）　この項の内容は、NM-NAM デバイスには適用されません。

SPAN セッションを編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** をクリックします。

Active SPAN Sessions ダイアログボックスが表示されます。

ステップ 2　編集する SPAN セッションを選択し、**Edit** をクリックします。

Edit SPAN Session ダイアログボックス（表 3-11）が表示されます。

ステップ 3　必要な変更を行います。

表 3-11　Edit SPAN Session ダイアログボックス

フィールド	説明
Monitor Session	SPAN の監視セッション。
SPAN Type	SPAN セッションのタイプ。
Switch Module List	NAM およびスイッチ ファブリック モジュール以外のスイッチ上のモジュールをすべて一覧表示。
SPAN Traffic Direction	SPAN トラフィックの方向。 （注）　Catalyst OS ソフトウェアが稼動するスイッチでは SPAN 方向を編集できません。このようなスイッチの場合、SPAN セッションのすべての SPAN ソースを、すべて 1 つの方向だけにする必要があります。
Available Sources	選択された SPAN タイプで使用できる SPAN ソース。
Add	選択された SPAN ソースを追加。
Remove	選択された SPAN ソースを削除。
Remove All	すべての SPAN ソースを削除。
Selected Sources	選択された SPAN ソース。
Refresh ボタン	NAM によって、現在の設定でスイッチ設定情報を更新。
Submit ボタン	変更内容を保存。
Reset ボタン	すべての変更をクリア。

SPAN セッションの削除

(注)　この項の内容は、NM-NAM デバイスには適用されません。

SPAN セッションを削除するには、削除する SPAN セッションを Active SPAN Session ダイアログ ボックスで選択し、**Delete** をクリックします。

NetFlow インターフェイスについて

リモート デバイスを NAM の NDE データ ソースとして使用するには、NDE パケットが NAM の UDP ポート 3000 にエクスポートされるように、リモート デバイスそのものを設定する必要があります。デバイスは、インターフェイスごとに設定が必要な場合があります。NDE デバイスは、IP アドレスによって識別されます。デフォルトでは、スイッチのローカル スーパーバイザ エンジンを常に NDE デバイスとして使用できるようになっています。

追加の NDE デバイスを定義するには、IP アドレスおよび（オプションで）コミュニティ ストリングを指定します。コミュニティ ストリングは、NetFlow レコードで監視されるリモート デバイス上のインターフェイスに対する、便利なテキスト文字列をアップロードするために使用します。

今回のリリースには、リモート NDE デバイス上の異なるインターフェイスを識別する機能があります。そのため、すべてのフローを単純に同じ収集にまとめるのではなく、各リモート NDE デバイスのインターフェイスのグループを任意にまとめ、1 つの概念的なデータ ソースにすることができます。

すべてのリモート デバイス上のすべてのインターフェイスを識別しようとすると（特に両方向を別々に識別しようとすると）、データ ソースの数が多すぎて管理不可能になる可能性があります。概念的なデータ ソースを使用すると、すべてのインターフェイスをあらゆる方向に単一の概念的なデータ ソースにまとめるという柔軟性が得られます。

デバイスのインターフェイスごとに、別の概念的データ ソースを作成することもできます。一般的に、概念的データ ソースを作成するとき「単純なフロー パス」はいくつでも組み合せることができます。単純なフロー パスはそれぞれ、入力方向、出力方向、または両方向のいずれか 1 つのインターフェイスから構成されます。

概念的なデータ ソースの作成と、データ ソースへのフロー パスの割り当てには、次の制約があります。

- フロー パスの入力インターフェイスとして指定されているインターフェイスは、同じデバイスの別の概念的データ ソースの入力インターフェイスとしては指定できません。また、同じ概念的データ ソースの別のフロー パスの双方向インターフェイスとしても指定できません。
- フロー パスの出力インターフェイスとして指定されているインターフェイスは、同じデバイスの別の概念的データ ソースの出力インターフェイスとしては指定できません。また、同じ概念的データ ソースの別のフロー パスの双方向インターフェイスとしても指定できません。
- フロー パスの双方向インターフェイスとして指定されているインターフェイスは、同じデバイスの別の概念的データ ソースの双方向インターフェイスとしては指定できません。また、同じ概念的データ ソースの別のフロー パスの入力インターフェイスまたは出力インターフェイスとしても指定できません。

NetFlow フロー レコードについて

NDE パケットには、複数のフロー レコードが含まれます。各フロー レコードには次の 2 つのフィールドがあります。

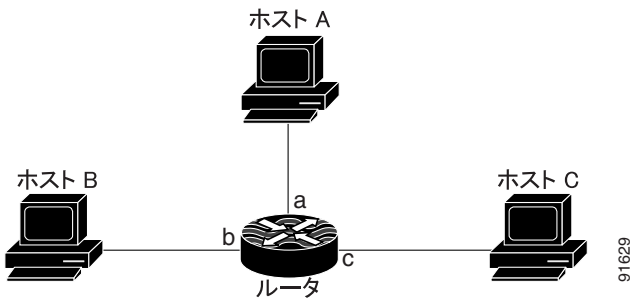
- 入力 SNMP ifIndex
- 出力 SNMP ifIndex

(注)

NDE 機能が Cisco IOS または Catalyst OS のバージョンと互換性がないか、または NDE のフローマスクの設定が原因で、この情報を利用できない場合があります。フローマスクの互換性の詳細については、P.4-5 の「NDE フロー マスクおよび V8 集約キャッシュ」を参照してください。

ほとんどの場合、インターフェイスで NetFlow をオンにすると、インターフェイスの入力方向にあるフローが、デバイスの NetFlow キャッシュに入ります。この結果、フロー レコード内の入力 SNMP ifIndex フィールドには、NetFlow をオンにしたインターフェイスの ifIndex が入ります。NetFlow ネットワークの例（図 3-3）は、NetFlow ルータを含むネットワーク構成の例を示しています。

図 3-3　NetFlow ネットワークの例



フロー レコードのレポートの表（表 3-12）に、NetFlow がインターフェイス a でイネーブルになっている場合にレポートされるフローを示します。

表 3-12　フロー レコードのレポート

入力インターフェイス	出力インターフェイス	フローのレポート
a	b	あり
a	c	あり
b	c	なし
b	a	なし
c	a	なし
c	b	なし

デバイスの NetFlow 設定

NDE パケットを NAM にエクスポートするための NetFlow デバイスの設定コマンドは、プラットフォームとデバイスによって異なります。ここに示す設定コマンドの例は、Cisco IOS または Catalyst OS が稼動するデバイスで最も一般的に見られるものです。詳細については、デバイスのマニュアルを参照してください。

Cisco IOS が稼動するデバイスの場合

ステップ 1　ルーティングされたフローのキャッシュをオンにするインターフェイスを選択します。

```
Prompt#configure terminal
Prompt(config)#interface <type slot/port>

Prompt(config-if)#ip route-cache flow
```

ステップ 2　ルーティングされたフローのキャッシュ エントリを NAM の UDP ポート 3000 にエクスポートします。

```
Prompt(config)#ip flow-export destination <NAM IP address> 3000
```

Cisco IOS が稼動するデバイスでマルチレイヤ スイッチングのキャッシュがサポートされている場合

ステップ 1　NDE のバージョンを選択します。

```
Prompt(config)#mls nde sender version <version-number>
```

（注）　NAM では、NDE バージョン 1、5、6、7、8、および v8 集約キャッシュがサポートされています。

ステップ 2　NDE のフロー マスクを選択します。

```
Prompt(config)#mls flow ip full
```

ステップ 3　NetFlow のエクスポートをイネーブルにします。

```
Prompt(config)#mls nde sender
```

ステップ 4　NetFlow を NAM の UDP ポート 3000 にエクスポートします。

```
Prompt(config)#ip flow-export destination <NAM IP address> 3000
```

Cisco IOS が稼動するデバイスで NDE v8 の集約がサポートされている場合

ステップ 1　v8 の集約を選択します。

```
Prompt(config)#ip flow-aggregation cache <aggregation-type>
```

aggregation-type は次の中から選択できます。

- destination-prefix
- source-prefix
- protocol-port
- prefix

ステップ 2　集約キャッシュをイネーブルにします。

```
Prompt(config-flow-cache)#enable
```

ステップ 3　集約キャッシュ内のフロー エントリを、NAM の UDP ポート 3000 にエクスポートします。

```
Prompt(config-flow-cache)#export destination <NAM address> 3000
```

Catalyst OS が稼動するデバイスの場合

ステップ 1　NDE のバージョンを選択します。

```
Prompt>(enable) set mls nde version <nde-version-number>
```

(注)　NAM では、NDE バージョン 1、5、6、7、8、および v8 集約キャッシュがサポートされています。

ステップ 2　NDE のフロー マスクとして full を選択します。

```
Prompt>(enable) set mls flow full
```

ステップ 3　NDE のエクスポートをイネーブルにします。

```
Prompt>(enable) set mls nde enable
```

ステップ 4　NDE パケットを NAM の UDP ポート 3000 にエクスポートします。

```
Prompt>(enable) set mls nde <NAM address> 3000
```

ブリッジ フロー統計情報からの NDE エクスポートをサポートするデバイスの場合

ステップ 1　VLAN でブリッジ フロー統計情報をイネーブルにします。

```
Prompt>(enable) set mls bridged-flow-statistics enable <vlan-list>
```

ステップ 2　NDE パケットを NAM の UDP ポート 3000 にエクスポートします。

```
Prompt>(enable) set mls nde <NAM address> 3000
```

デバイス スロットにある NAM の場合

NAM がデバイス スロットのいずれかにある場合、デバイスをセットアップして NDE パケットを NAM にエクスポートできます。

ステップ 1　NDE のバージョンを選択します。

```
Prompt>(enable) set mls nde version <nde-version-number>
```

ステップ 2　NDE のフロー マスクとして full を選択します。

```
Prompt>(enable) sel mls nde full
```

ステップ 3　NDE のエクスポートをイネーブルにします。

```
Prompt>(enable) set mls nde enable
```

ステップ 4　NDE パケットを NAM にエクスポートします。

```
Prompt>(enable) set snmp extendedrmon netflow enable <NAM-slot>
```

WAN インターフェイスの VACL 設定

WAN インターフェイスでは SPAN 機能がサポートされないため、NAM で WAN トラフィックを監視するには、スイッチ CLI を使用して VACL を手動で設定する必要があります。この機能は、WAN インターフェイスの IP トラフィックの場合のみ使用できます。

VACL は、NAM にトラフィックを向ける SPAN セッションがない場合にも使用できます。この場合、SPAN の代わりに VACL をセットアップして、VLAN のトラフィックを監視できます。

次の例で、ATM WAN インターフェイスに VACL を設定し、NAM に入トラフィックと出トラフィックの両方を転送する方法を示します。これらのコマンドは、Cisco IOS バージョン 12.1(13)E1 以降が稼動するスイッチ用です。Catalyst OS の LAN VACL の場合、セキュリティ Access Control List（ACL; アクセス コントロール リスト）機能で同様のことができます。これらの機能の使用方法については、スイッチのマニュアルを参照してください。

```
Cat6509#config terminal
Cat6509(config)#access-list 100 permit ip any any
Cat6509(config)#vlan access-map wan 100
Cat6509(config-access-map)#match ip address 100
Cat6509(config-access-map)#action forward capture
Cat6509(config-access-map)#exit
Cat6509(config)#vlan filter wan interface AM6/0/0.1
Cat6509(config)#analysis module 3 data-port 1 capture allowed-vlan 1-4094
Cat6509(config)#analysis module 3 data-port 1 capture
Cat6509(config)#exit
```

出トラフィックだけを監視するには、次のコマンドを使用して WAN インターフェイスに関連付けられた VLAN ID を入手します。

```
Cat6509#show cwan vlan
Hidden      VLAN    swidb->i_number    Interface
1017        94                         ATM6/0/0.1
```

VLAN ID を入手したら、次のコマンドを使用して NAM のデータ ポートを設定します。

```
Cat6509(config)#analysis module 3 data-port 1 capture allowed-vlan 1017
```

入トラフィックだけを監視するには、キャプチャ設定の VLAN 番号を、入トラフィックを伝達するネイティブ VLAN ID で置き換えます。たとえば、VLAN 1 が入トラフィックを伝達する場合、次のコマンドを使用できます。

```
Cat6509(config)#analysis module 3 data-port 1 capture allowed-vlan 1
```

LAN VLAN での VACL 設定

LAN で VLAN トラフィックの監視を行うには、スイッチの SPAN 機能を使用してトラフィックを NAM に送ります。ただし、SPAN 機能対象のトラフィックが NAM の監視能力を超える場合は、転送前に LAN のトラフィックをあらかじめフィルタリングすることができます。これには、VACL を使用します。

次の例で、LAN の VLAN インターフェイスについて VACL を設定する方法を示します。この例では、VLAN 1 のサーバ 172.20.122.226 に向けられたすべてのトラフィックがキャプチャされ、スロット 3 にある NAM に転送されます。

```
Cat6509#config terminal
Cat6509#(config)#access-list 100 permit ip any any
Cat6509#(config)#access-list 110 permit ip any host 172.20.122.226
Cat6509#(config)#vlan access-map lan 100
Cat6509#(config-access-map)match ip address 110
Cat6509#(config-access-map)#action forward capture
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan access-map lan 200
Cat6509#(config-access-map)#match ip address 100
Cat6509#(config-access-map)#action forward
Cat6509#(config-access-map)#exit
Cat6509#(config)#vlan filter lan vlan-list 1
Cat6509#(config)#analysis module 3 data-port 1 capture allowed-vlan 1
Cat6509#(config)#analysis module 3 data-port 1 capture
Cat6509#(config)#exit
```

NetFlow デバイスの管理

NetFlow データを監視するには、まず監視対象の NetFlow デバイスを追加する必要があります。また、NDE パケットを NAM にエクスポートできるように、リモート NDE デバイスも設定します。デバイスの NetFlow 設定の詳細については、P.3-15 の「デバイスの NetFlow 設定」またはデバイスのマニュアルを参照してください。次のトピックで、NetFlow の監視に使用するデバイスのセットアップと管理について説明します。

- デバイスの作成（P.3-19）
- デバイスの編集（P.3-20）
- デバイスの削除（P.3-20）
- デバイスのテスト（P.3-21）
- カスタム データ ソースの作成（P.3-21）
- リスニング モードの使用方法（P.3-24）

デバイスの作成

NetFlow デバイスを作成すると、そのデバイスに対して NetFlow データ ソースが自動的に作成されます。これらのデータ ソースで NDE パケットがアクティブになっているかどうかを確認するには、リスニング モードを使用します。リスニング モードの使用方法の詳細については、P.3-24 の「リスニング モードの使用方法」を参照してください。

デバイスを作成するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** をクリックします。

Active SPAN Sessions テーブルが表示されます。

（注）　NM-NAM デバイスの場合、Netflow Devices テーブルが表示されます。

ステップ 2　コンテンツで **Devices** をクリックします。

NetFlow Devices テーブルが表示されます。

ステップ 3　**Create** をクリックします。

New Device ダイアログボックスが表示されます。

ステップ 4　デバイス名とコミュニティ ストリングを入力し、次のいずれかを行います。

- 変更内容を保存するには、**OK** をクリックします。
- ダイアログボックスのエントリをクリアするには、**Reset** をクリックします。
- エントリを元のままにするには、**Cancel** をクリックします。

デバイスの編集

(注)　ローカル スイッチは編集できません。

デバイスを編集するには、次の手順を実行します。

ステップ 1　Setup タブをクリックします。

ステップ 2　**Data Sources** をクリックします。

Active SPAN Sessions テーブルが表示されます。

ステップ 3　コンテンツで **Devices** をクリックします。

NetFlow Devices テーブルが表示されます。

ステップ 4　テーブルで編集するデバイスを選択し、**Edit** をクリックします。

Edit Device ウィンドウが表示されます。

ステップ 5　必要な変更を加えてから、次のいずれかを行います。

- 変更内容を保存するには、**OK** をクリックします。
- 元のエントリに戻すには、**Reset** をクリックします。
- 設定を元のままにするには、**Cancel** をクリックします。

デバイスの削除

デバイスを削除するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** をクリックします。

Active SPAN Sessions テーブルが表示されます。

ステップ 2　コンテンツで **Devices** をクリックします。

NetFlow Devices テーブルが表示されます。

ステップ 3　削除するデバイスを Devices ダイアログボックスで選択し、**Delete** をクリックします。

(注)　デバイスに関連するカスタム NetFlow データ ソースがすべて削除されます。

デバイスのテスト

Devices テーブルのデバイスに対して、SNMP コミュニティ ストリングのテストができます。デバイスをテストするには、Devices テーブルでデバイスを選択し、**Test** をクリックします。Device System Information ダイアログボックス（表 3-13）が表示されます。

表 3-13　Device System Information ダイアログボックス

フィールド	説明
Name	デバイスの名前
Hardware	デバイスのハードウェア記述
Device Software Version	デバイスで実行している現在のソフトウェア バージョン
System Uptime	前回のリブート後の合計稼動時間。
Location	デバイスの場所。
Contact	デバイスの連絡先情報。
SNMP read from device	SNMP 読み取りテストの結果。ローカル デバイスのみ。

デバイスが NetFlow Version 9（V9）を送信している場合、NAM が NDE テンプレートを受信すると、Device System Information ウィンドウの下に V9 Templates ボタンが表示されます。

（注） すべての NDE パケットで NetFlow V9 テンプレートが表示されるわけではありません。テンプレートがない場合、**V9 Templates** ボタンは表示されません。

NetFlow V9 テンプレートを表示するには、**V9 Templates** ボタンをクリックします。詳細については、「リスニング モードの使用方法」の表 3-16 を参照してください。

カスタム データ ソースの作成

Devices セクションにデバイスを作成すると、自動的に NetFlow データ ソースが認識されます。NetFlow デバイスの作成の詳細については、P.3-19 の「デバイスの作成」を参照してください。このオプションを使用すると、NetFlow デバイスに、特定のインターフェイス情報を持ったカスタム データ ソースを作成できます。

カスタム データ ソースを作成するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** をクリックします。

ステップ 2　コンテンツ メニューで **Custom Data Sources** を選択します。

NetFlow Data Sources テーブルが表示されます。

ステップ 3　**Create** をクリックします。

次の表に、NetFlow データ ソースの作成または編集に使用されるウィザードを示します。

	ウィザードのページ	参照項目
ステップ 1	Device Selection	P.3-22 の「NetFlow デバイスの選択」
ステップ 2	Interface Selection	P.3-22 の「インターフェイスの選択」
ステップ 3	Summary	P.3-23 の「NetFlow データ ソース情報の確認」

NetFlow デバイスの選択

NetFlow デバイスを選択するには、次の手順を実行します。

ステップ 1　リストで、NetFlow デバイスを選択します。

ステップ 2　データ ソース名を入力します。何も入力しない場合、デフォルトの名前が作成されます。

ステップ 3　**Next** をクリックします。

インターフェイスの選択

インターフェイスを選択するには、次の手順を実行します。

ステップ 1　データ フローの方向を選択します。

ステップ 2　Available Interfaces セクションで、追加するインターフェイスを選択します。

ヒント　複数のインターフェイスを選択するには、Ctrl キーを押した状態でクリックします。

リストにインターフェイスが表示されない場合、インターフェイスを Interface Index テキスト ボックスに入力します。

ステップ 3　**Add** をクリックします。

選択したインターフェイスが Selected Interfaces セクションに表示されます。

- インターフェイスを削除するには、Selected Interfaces セクションで選択し、**Remove** をクリックします。
- Selected Interfaces セクションのインターフェイスをすべて削除するには、**Remove All** をクリックします。

ステップ 4　**Next** をクリックします。

特殊な（0）インターフェイス

NDE パケットには、入力 if-index と出力 if-index のどちらか（または両方）のフィールドを 0 としてレポートする NetFlow レコードが存在する場合があります。これは、次のような理由から起こります。

- フローがそのデバイスで終端。
- デバイスの設定。
- デバイスのプラットフォームで NetFlow 機能がサポートされていない。

詳細については、NetFlow デバイスのマニュアルを参照してください。

NetFlow データ ソース情報の確認

NetFlow データ ソース情報を確認するには、次の手順を実行します。

ステップ 1　情報が正しいことを確認します。

ステップ 2　次のいずれかを実行します。

- 設定を保存するには、**Finish** をクリックします。
- 変更をキャンセルして NetFlow Data Sources テーブルに戻るには、**Cancel** をクリックします。

カスタム データ ソースの編集

カスタム データ ソースを編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** を選択します。

ステップ 2　**Custom Data Sources** をクリックします。

NetFlow Data Sources テーブルが表示されます。

ステップ 3　編集するデータ ソースを選択し、**Edit** をクリックします。

NetFlow データ ソースの編集に使用するウィザードが表示されます。

ステップ 4　必要な変更を加えてから、次のいずれかを行います。

- 変更を確定するには、**Finish** をクリックします。
- 変更をキャンセルするには、**Cancel** をクリックします。

カスタム データ ソースの削除

データ ソースを削除するには、NetFlow Data Source テーブルで選択し、**Delete** をクリックします。

（注）　デフォルトのデータ ソースは削除できません。

リスニング モードの使用方法

NAM のリスニング モードでは、NAM に NDE パケットを送るデバイスの IP アドレス、NDE パケットの数、および最後に NDE パケットを受信したときの時間を表示できます。NetFlow Listening Mode テーブルには、NAM がその時点で NDE パケットを受け取っているデバイスのみが示されます。

リスニング モードを使用するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** を選択します。

ステップ 2　コンテンツで **Listening Mode** をクリックします。

NetFlow Listening Mode テーブル（表 3-14）が表示されます。

表 3-14　NetFlow Listening Mode テーブル

フィールド	説明
Start Time	Start ボタンがクリックされた時点のタイムスタンプ
Address	認識されたデバイスの IP アドレス
# Received NDE Packets	受信した NetFlow Data Export（NDE）パケットの数
Last Packet Received	最後に受信した NDE パケットのタイムスタンプ

ステップ 3　**Start** をクリックします。

ステップ 4　テーブルをクリアして監視を停止するには、**Stop** をクリックします。

（注）　認識は、1 時間後に自動的にディセーブルになります。

NetFlow Listening Mode テーブルの詳細表示

テーブルでデバイスを選択し、**Details** をクリックします。

Device Details ウィンドウ（表 3-15）が表示されます。

表 3-15　Device Details ウィンドウ

フィールド	説明
Device Added	デバイスが NAM デバイス テーブルに追加されているかどうかが示されます。
Interfaces Reported in NDE Packets	NDE パケットが検出されたインターフェイスが一覧表示されます。 次の例を参考にしてください。 Special (0) (Output) (1) (Input/Output) (2) (Input/Output) **（注）** Protocol-Prefix NDE パケットには、インターフェイス情報がありません。

デバイスが NetFlow Version 9（V9）を送信している場合、NAM が NDE テンプレートを受信すると、Device Details ウィンドウの下に V9 Templates ボタンが表示されます。詳細については、次の URL を参照してください。

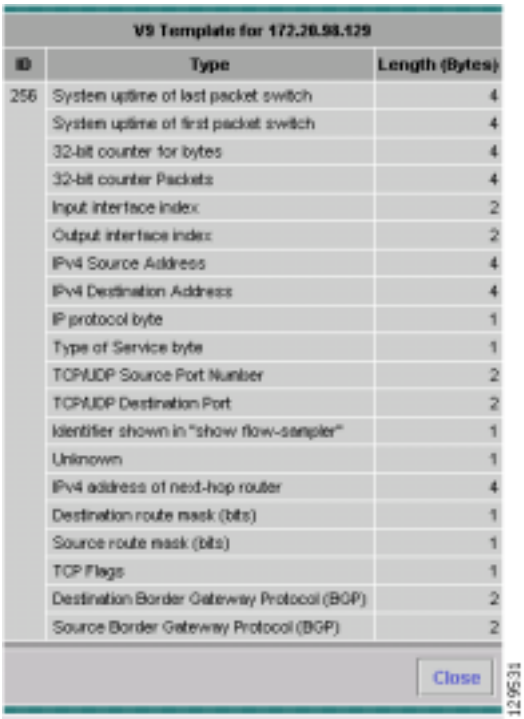
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_feature_guide09186a00801b0696.html

(注)　すべての NDE パケットで NetFlow V9 テンプレートが表示されるわけではありません。テンプレートがない場合、**V9 Templates** ボタンは表示されません。

NetFlow V9 テンプレートを表示するには、**V9 Templates** ボタンをクリックします。

V9 Templates ウィンドウ（図 3-4）が表示されます（次の例を参照してください）。

図 3-4　V9 Templates ウィンドウ



V9 Templates テーブル（表 3-16）に、テンプレート データを示します。

表 3-16　V9 Templates テーブル

フィールド	説明
Type	テンプレート データのタイプ
Length (Bytes)	テンプレート データの長さ（バイト単位）

監視するデバイスの追加

監視するデバイスを追加するには、次の手順を実行します。

ステップ 1　テーブルでデバイスを選択し、**Add** をクリックします。

New Device ウィンドウが表示されます。

ステップ 2　デバイスの情報を入力し、OK をクリックします。

デバイスが NetFlow Devices テーブルに追加されます。

ルータのコミュニティ ストリングのテスト

NM-NAM デバイスの場合のみ

ルータが SNMP を使用して NAM に情報を送るには、NAM Traffic Analyzer に設定されているルータのコミュニティ ストリングが、実際のルータに設定されたものと一致する必要があります。Router Parameters ダイアログボックスには、ルータ名、ハードウェア、Supervisor のソフトウェア バージョン、システムの稼動時間、場所、連絡先情報が表示されます。

NAM がローカル ルータと通信できるように、ローカル ルータの IP アドレスおよび SNMP コミュニティ ストリングを設定する必要があります。

ルータのコミュニティ ストリングを設定するには、ルータの CLI を使用します。CLI の使用方法の詳細については、デバイスに付属のマニュアルを参照してください。

注意　入力するルータのコミュニティ ストリングは、そのルータのリード / ライト コミュニティ ストリングに一致する必要があります。一致していない場合、ルータと通信できません。

ルータのコミュニティ ストリングをテストするには、次の手順を実行します。

ステップ 1　**Setup** > **Router Parameters** を選択します。

Router Parameters ダイアログボックスが表示されます。

ステップ 2　**Test** をクリックします。

Router Community String Test ダイアログボックスが表示されます。

インターフェイスのセットアップ

(注)　この項の内容は、NM-NAM デバイスにしか適用できません。

トラフィック統計情報と、アプリケーション、ホスト、および会話の TopN トラフィックを表示するには、事前にインターフェイスをセットアップしておく必要があります。

選択したインターフェイスとそのすべてのサブインターフェイスで Netflow NDE をイネーブルにするため、チェックボックスをオンにします。イネーブルなサブインターフェイスごとに、NAM NDE データ ソースが作成され、さらに、ホスト、会話、アプリケーションの NDE データ ソースも作成されます。このアクションは、**Monitor > Router** を選択すると表示される詳細ウィンドウに反映されます。このウィンドウに、ホスト、会話、およびアプリケーションの統計情報が示されます。

サブインターフェイスを持つ親インターフェイスの場合は、リーフで示された子インターフェイスだけがイネーブルになります。たとえば、ATM2/0.1-atm-subif は子 ATM2/0.1-aal5-layer を持っています。この場合、aal5-layer だけがイネーブルになります。NDE は、この子インターフェイスだけを認識します。

詳細情報画面とデータとの整合性を保持するために、Router Netflow Active Timeout を NAM と同じポーリング インターバルに設定することを推奨します。**Setup > Datasources > Interfaces** を選択して、Interfaces ウィンドウを表示するか、**Setup > Router Parameters** を選択して、Router Parameters ウィンドウを表示します。

トラフィック統計情報を表示できるようにインターフェイスをセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** を選択します。

NAM 3.6 は、最大 1,500 のデータソースをサポートします。

ステップ 2　コンテンツ メニューで **Interfaces** をクリックします。

Interfaces ウィンドウが表示されます。

ルータ インターフェイスと SNMP リード / ライト コミュニティ ストリングを設定する必要があります。詳細については、P.3-7 の「ルータ パラメータ」を参照してください。

ステップ 3　イネーブルにする各インターフェイスの **Enable** チェックボックスをオンにします。

MPLS データ ソース

MPLS ラベルを含むデータ パケットが NAM にスパンされた場合は、データ パケット内部のタグによってトラフィックを監視できます。この機能は、各 VPN からのトラフィックを MPLS ラベルの組み合せによって一意に識別できる、NPLS/VPN が配備されたネットワークで特に役立ちます。NAM は、スタックされた MPLS ラベルを認識すると、関連する最も奥のラベル（ラベル スタックの下部のタグ）だけを監視に使用します。

MPLS の RMON 監視をイネーブルにするには、最初に MPLS データ ソースを設定する必要があります。MPLS トラフィックの監視をイネーブルにするには、特定の MPLS タグに結合できる仮想インターフェイスの形式を作成する必要があります。カスタム MPLS データ ソースのセットアップ後に、次の監視をイネーブルにできます。

- MPLS タグごとのアプリケーション
- MPLS タグごとのホスト
- MPLS タグごとのホストの会話

この項では、次のトピックについて取り上げます。

- MPLS VPN ラベルの自動検出（P.3-28）
- レイヤ 3 VRF データ ソースのセットアップ（P.3-28）
- レイヤ 2 仮想回線データ ソースのセットアップ（P.3-29）
- MPLS ラベル データ ソースのセットアップ（P.3-31）
- VRF/VC 設定ファイルの作成（P.3-32）
- VRF/VC 設定ファイルのインポート（P.3-33）
- VRF/VC 設定ファイルのエクスポート（P.3-33）
- インポート ログ（P.3-33）

MPLS VPN ラベルの自動検出

MPLS VPN 環境では、NAM は VPN Routing/Forwarding（VRF; VPN ルーティング / 転送）テーブル名またはスイッチに設定された Virtual Circuit（VC; 仮想回線）ID のいずれかを使用してトラフィックを監視できます。この場合、抽象レベルが高くなるため、下位のラベル アソシエーションが隠れます。

スイッチ CLI からは、VRF および VC 情報だけを取得できます。この情報を取得するには、スイッチ ログイン クレデンシャル、ユーザ名とパスワード、スイッチ CLI に **telnet** または **ssh** のどちらを使用してアクセスするかを入力する必要があります。イネーブル モード パスワードは必要ありません。

VRF、VC、および関連付けられたラベルが検出されれば、下位のラベルについて知らなくても、NAM 監視機能を使用して、VRF 名または VC ID のどちらかを使用して VRF または VC を直接参照できます。

各 VRF または VC に関連付けられるラベルは、スイッチによって動的に割り当てられます。そのため、スイッチがリブートされるか、スーパーバイザのスイッチオーバーが発生した場合、ラベルは存続しません。これらの状況下では、NAM は VRF および VC 情報をスイッチから再検出する必要があります。オンデマンド リフレッシュのための手動のリフレッシュ機能も提供されています。

レイヤ 3 VRF データ ソースのセットアップ

レイヤ 3 VRF テーブル（L3 VRF）データ ソースをセットアップするには、次の手順を実行します。

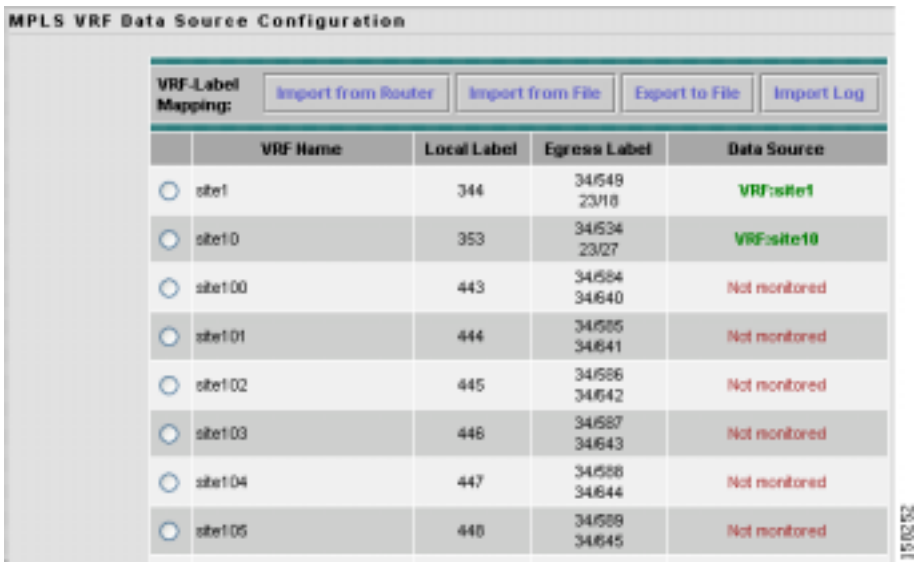
ステップ 1　**Setup** > **Data Sources** をクリックします。

Active SPAN Sessions テーブルが表示されます。

ステップ 2　コンテンツで **L3 VRF** をクリックします。

MPLS VRF Data Source Configuration ウィンドウ（図 3-5）が表示されます。

図 3-5　MPLS VRF Data Source Configuration ウィンドウ



ステップ 3　VRF 情報が表示されない場合、または一部の VRF 情報が欠落している場合は、**Import from Router** をクリックしてリストをリフレッシュします。

Import from Router をクリックしてもリストが空の場合は、NAM がルータからの VRF 設定の自動インポートに失敗しています。この場合は、手順 4 を実行します。VRF 情報が取得できた場合は、手順 5 に進みます。

NAM がルータからの VRF 設定の自動インポートに失敗した場合は、**Import Log** をクリックします。MPLS インポート ログには、接続問題の診断に役立つ可能性のある情報が含まれています。インポート ログの詳細については、P.3-33 の「インポート ログ」を参照してください。

ステップ 4　必要な場合は、VRF 情報を含むテキスト ファイルを作成し、**Import from File** をクリックします。

Import from File をクリックすると、Import VRF/VC Configuration ウィンドウが表示されます。このウィンドウで、VRF/VC 設定ファイルのインポート元を指定できます。VRF/VC 設定ファイルは、ローカル マシンまたはリモート URL に存在します。

VRF/VC 設定ファイルの作成方法の詳細については、P.3-32 の「VRF/VC 設定ファイルの作成」を参照してください。

ステップ 5　VRF データ ソースを選択し、**Create DataSrc** をクリックします。

NAM データ ソースの作成または削除は、スイッチ設定には影響しません。

レイヤ 2 仮想回線データ ソースのセットアップ

レイヤ 2（L2）仮想回線データ ソースをセットアップするには、次の手順を実行します。

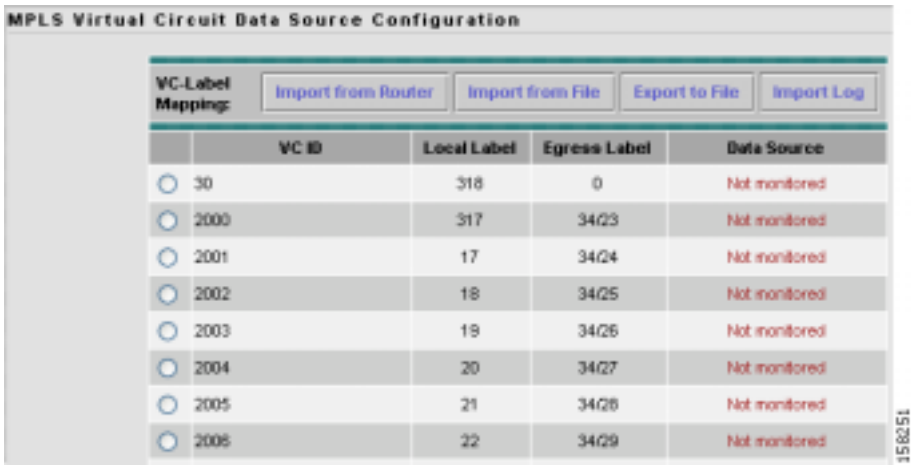
ステップ 1　**Setup** > **Data Sources** を選択します。

Active SPAN Sessions テーブルが表示されます。

ステップ 2　コンテンツで **L2 Virtual Circuit** をクリックします。

MPLS Virtual Circuit Data Source Configuration ウィンドウ（図 3-6）が表示されます。

図 3-6　MPLS Virtual Circuit Data Source Configuration ウィンドウ



ステップ 3　VC 情報が表示されない場合、または一部の VC 情報が欠落している場合は、**Import from Router** をクリックしてリストをリフレッシュします。

Import from Router をクリックしてもリストが空の場合は、NAM がルータからの VC 設定の自動インポートに失敗しています。この場合は、手順 4 を実行します。VC 情報が取得できた場合は、手順 5 に進みます。

NAM がルータからの VC 設定の自動インポートに失敗した場合は、**Import Log** をクリックします。MPLS インポート ログには、接続問題の診断に役立つ可能性のある情報が含まれています。インポート ログの詳細については、P.3-33 の「インポート ログ」を参照してください。

ステップ 4　必要な場合は、VC 情報を含むテキスト ファイルを作成し、**Import from File** をクリックします。

Import from File をクリックすると、Import VRF/VC Configuration ウィンドウが表示されます。このウィンドウで、VRF/VC 設定ファイルのインポート元を指定できます。VRF/VC 設定ファイルは、ローカル マシンまたはリモート URL に存在します。

VRF/VC 設定ファイルの作成方法の詳細については、P.3-32 の「VRF/VC 設定ファイルの作成」を参照してください。

ステップ 5　VC データ ソースを選択し、**Create DataSrc** をクリックします。

NAM データ ソースの作成または削除は、スイッチ設定には影響しません。

MPLS ラベル データ ソースのセットアップ

MPLS ラベル データ ソースをセットアップするには、次の手順を実行します。

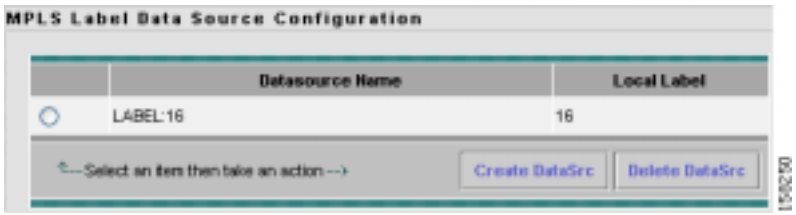
ステップ 1　**Setup** > **Data Sources** を選択します。

Active SPAN Sessions テーブルが表示されます。

ステップ 2　コンテンツで **Label** をクリックします。

MPLS Label Data Source Configuration ウィンドウ（図 3-7）が表示されます。

図 3-7　MPLS Label Data Source Configuration ウィンドウ



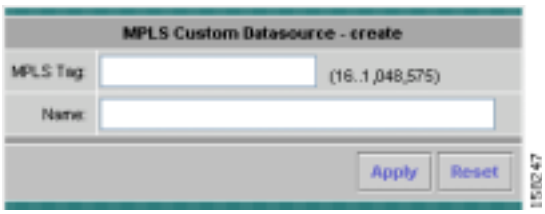
ステップ 3　**Create DataSrc** をクリックします。

最初に、VRF または VC の選択を求めるダイアログボックスが表示されます。

ステップ 4　**OK** をクリックします。

Create MPLS Custom Datasource ウィンドウ（図 3-8）が表示されます。

図 3-8　Create MPLS Custom Datasource ウィンドウ



ステップ 5　**MPLS Tag** フィールドに MPLS タグ番号を入力します。

タグ番号はパケット内の値に一致している必要があります。タグ番号はデータ ソース内だけに現れます。タグ番号は、ルータ設定から取得する必要があります。NAM は、入力された MPLS タグ番号に基づいて名前を割り当てます。

ステップ 6　NAM が MPLS タグ番号に基づいて割り当てた名前を受け入れるか、または Name フィールドに好みの名前を入力します。

Name フィールドを使用して、MPLS タグ値、VRF トンネル名、または他のそれに該当する名前（VPN-San_Jose-RTP など）を識別できます。

ステップ 7　**Apply** をクリックします。

VRF/VC 設定ファイルの作成

VRF/VC 設定ファイルには、ルータに設定されている VRF および VC に関するテキスト情報が含まれます。各設定行には、スペースで区切られた 4 つのフィールドがあります。表 3-17 に、設定行の形式を示します。

表 3-17　VRF/VC 設定行

フィールド	説明
Comment line	# 文字で始まります。
Type	VRF または VC。
Name	VRF の名前または VC ID。
Local label	VRF または VC のローカル ラベル。
Egress label	外部ラベル / 内部ラベル形式の出力ラベル スタック。1 つ以上のラベルがある場合は、各ラベル スタックがカンマで区切られ、スタック ラベル間にスペースは含まれません。

次に、VRF/VC 設定ファイルの例を示します。

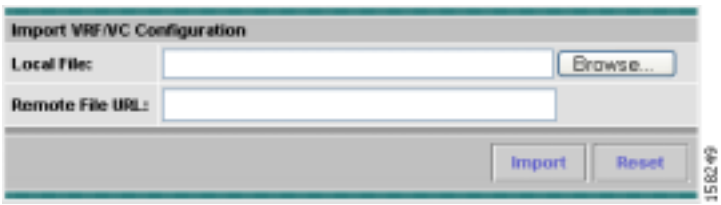
```
# MPLS configuration file
# Autogenerated at 2006-04-26 19:43
VRF customer_A 114 0
VRF customer_B 600 204/500,204/308
VC 201 111 204/309
VC 202 120 204/310
VC 203 121 204/311
VC 204 122 204/312
VC 205 123 204/313
VC 206 124 204/314
VC 207 125 204/315
VC 208 126 204/319
VC 209 127 204/317
VC 210 128 204/318
```

VRF/VC 設定ファイルのインポート

既知の VRF/VC 設定を含むテキスト ファイルがある場合は、**Import from File** をクリックして設定をインポートできます。このファイルは、**Export to File** ボタンを使用して作成されている場合もあります。図 3-9 に、Importing VRF/VC Configuration File ウィンドウを示します。

Browse をクリックしてインポートする設定ファイルを検索するか、リモート ファイルの URL を入力して、**Import** をクリックします。

図 3-9　Importing VRF/VC Configuration File ウィンドウ



VRF/VC 設定ファイルのエクスポート

NAM 上に望ましい MPLS 設定がある場合は、バックアップとして使用するために、その設定をファイルにエクスポートできます。バックアップ ファイルを作成しておくと、設定が失われた場合や以前の設定に戻す必要が生じた場合に、その設定をリロードできます。**Export to File** をクリックすると、MPLS VRF/VC データ ソース設定がエクスポートされます。

インポート ログ

ルータまたは VRF/VC データ ソース設定ファイルから VRF/VC データ ソース設定をインポートした後、**Import Log** をクリックすると、MPLS インポートのログを表示できます。MPLS インポート ログには、その接続でインポートが実行された履歴のリストが含まれるため、トラブルシューティングに役立つことがあります。ログには、無効なユーザ名やパスワード、スイッチへの接続の欠落、コマンドライン解析エラー、発生した可能性のあるその他の問題が示されていることがあります。MPLS インポート ログには、メッセージ *VRF/VC update successful* が含まれているはずです。

監視のセットアップ

データを監視するには、まず Setup タグの Monitor オプションで、データ収集をセットアップする必要があります。データ収集については、P.4-2 の「データ収集およびデータ ソースの概要」を参照してください。次のセットアップ オプションがあります。

- コア データの監視（P.3-34）
- 音声データの監視（P.3-36）
- 応答時間データの監視（P.3-37）
- DiffServ データの監視（P.3-39）
- DiffServ プロファイルのセットアップ（P.3-40）
- URL 収集データの監視（P.3-41）

コア データの監視

データ ソースごとに、コア データ収集を個別にイネーブルまたはディセーブルにできます。コア収集には次のものがあります。

- Application Statistics：データ ソースで観察されるアプリケーション プロトコルの監視が可能です。
- Host Statistics (Network and Application layers)：ネットワーク層のホスト アクティビティの監視が可能です。
- Host Statistics (MAC layer)：MAC 層のホスト アクティビティの監視が可能です。また、ホストの詳細ウィンドウ用の、ブロードキャスト回数およびマルチキャスト回数の監視も可能です。
- Conversation Statistics (Network and Application layers)：パケットを交換しているネットワーク層ホストのペアの監視が可能です。
- Conversation Statistics (MAC layer)：パケットを交換している MAC 層ホストのペアの監視が可能です。
- VLAN Traffic Statistics：データ ソースの各種 VLAN におけるトラフィック分布の監視が可能です。
- VLAN Priority (CoS) Statistics：802.1p プライオリティ フィールドのさまざまな値を使用したトラフィック分布の監視が可能です。
- Network-to-MAC Address Correlation：ホストの詳細ウィンドウに表示される、MAC レベルの統計情報の監視が可能です。この収集がないと、MAC ステーションを特定のネットワーク ホストに関連付けられません。
- NAM が受信したスイッチ エンジン モジュール（Supervisor）レコード：ポート統計情報、VLAN 統計情報、および NBAR 統計情報を任意に組み合せて選択できます。
- NAM が受信したルータ エンジン モジュール レコード（Router）：インターフェイス統計情報および NBAR 統計情報を任意に組み合せて選択できます。

（注）　MAC 収集と VLAN 収集は、NM-NAM デバイスでは使用できません。

（注）　システム パフォーマンスを全般的に向上させるには、監視する収集だけをイネーブルにします。

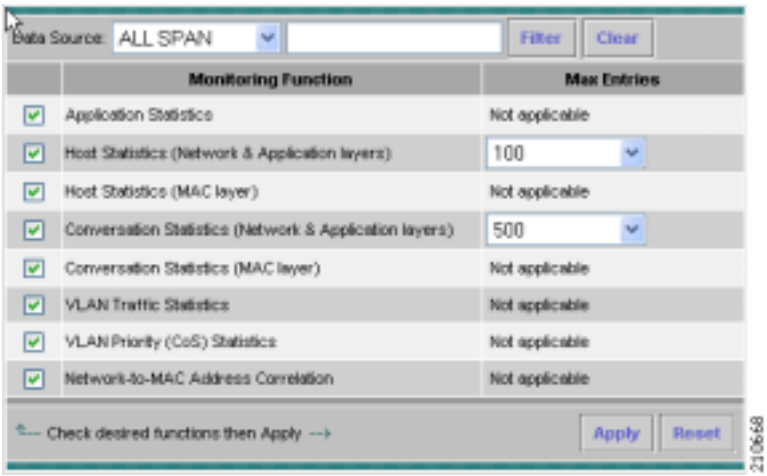
(注)　オフにする収集のレポートは、すべてディセーブルにする必要があります。オフにした収集でレポートが実行されていると、収集は自動的にオンになります。レポートのディセーブル化の詳細については、P.5-20 の「レポートのディセーブル化」を参照してください。

コア モニタリング機能をセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions ダイアログボックス（図 3-10）が表示されます。

図 3-10　Core Monitoring Functions ダイアログボックス



ステップ 2　Data Source ドロップダウン メニューで、収集のデータ ソースを選択します。

ルータのコア モニタリングをオンにするには、Data Source ドロップダウン メニューで Router を選択します。ルータの場合、次のデータ ソースを使用できます。

- Internal
- External
- NETFLOW
- Router

スイッチのコア モニタリング データをオンにするには、ドロップダウン メニューで Supervisor を選択します。スイッチの場合、次のデータ ソースを使用できます。

- ALL SPAN
- VLANs
- NETFLOW
- NDE
- Supervisor

データ ソースの名前の一部を入力して、**Filter** をクリックすることで、一致するデータ ソースを検索できます。**Clear** をクリックして、データ ソースの全体のリストに戻します。

ステップ 3　個々の監視機能をイネーブルにするには、そのチェックボックスをオンにします。

ステップ 4　Max Entries リストでエントリの最大数を選択します。

ステップ 5　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

Mini-RMON 収集のイネーブル化

(注)　この項の内容は、NM-NAM デバイスには適用されません。

スイッチの Supervisor で Mini-RMON をイネーブルにすると、各スイッチ ポートの統計情報を監視できます。Mini-RMON のイネーブル化は、CLI から特権モードで行います。Mini-RMON をイネーブルにするには、次のいずれかを行います。

Catalyst OS が稼動するスイッチの場合

set snmp rmon enable コマンドを入力します。

Cisco IOS が稼動するスイッチの場合

Mini-RMON を各インターフェイスでイネーブルにします。

次のコマンドを入力します。

```
Supervisor name(config) #interface interface-name
Supervisor name(config-if) #rmon collection stats collection-control-index owner
monitor
Supervisor name(config-if) #end
```

ここで、

- interface-name は、Mini-RMON をイネーブルにするインターフェイスの名前です。
- collection-control-index は、まだ使用されていない任意の番号です。

音声データの監視

音声データの監視をイネーブルにする場合、NAM Traffic Analyzer を通したときのみ結果を入手できます。収集された音声データを表示するには、Monitor タブを使用します。音声データの表示の詳細については、P.4-19 の「収集された URL の表示」を参照してください。

音声監視オプションはデフォルトでオンになっていますが、音声データを監視するには、NAM Traffic Analyzer で音声監視をイネーブルにする必要があります。

(注)　音声監視機能は、Cisco IP テレフォニー デバイスを使用している場合だけサポートされます。

音声監視をセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　コンテンツで **Voice Monitoring** をクリックします。

Voice Monitor Setup ダイアログボックス（表 3-18）が表示されます。

ステップ 3　適切な情報を選択します。

表 3-18　Voice Monitor Setup ダイアログボックス

フィールド	説明	使用法
Monitoring Enabled	SCCP、H.323、MGCP、および SIP といった音声プロトコルの音声監視をイネーブルにできます。	プロトコルを監視するには、チェックボックスをオンにします。
Number of phone table rows	監視できる通話記録の最大数。	10 ～ 1000 の数値を入力します。
Number of call table rows	監視できるアクティブ コールの最大数。	10 ～ 1000 の数値を入力します。
Number of top packet jitter rows	ジッタの多い TopN 通話数。	1 ～ 20 の数値を入力します。
Number of top packet loss rows	パケット損失の多い TopN 通話数。	1 ～ 20 の数値を入力します。
Debug	まだセットアップ状態にある通話をアプリケーションで表示可能にします。	クリックすると、デバッグ オプションがオンになります。

（注）　SCCP プロトコルのジッタとパケット損失を報告するには、Cisco Call Manager で CDR をイネーブルにする必要があります。Cisco CallManager の詳細については、Cisco CallManager のマニュアルを参照してください。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

応答時間データの監視

応答時間を監視すると、クライアントとサーバ間の応答時間を収集できます。応答時間の監視は、収集データ ソースごとにイネーブルまたはディセーブルにできます。応答時間の監視をイネーブルにすると、アプリケーションから、デフォルトの収集パラメータが設定されます。

応答時間の監視オプションはデフォルトでオンになっていますが、応答時間を監視するには、NAM Traffic Analyzer で応答時間の監視をイネーブルにする必要があります。

次のトピックで、応答時間の監視のセットアップと管理について説明します。

- 応答時間のデータ収集の作成（P.3-38）
- 応答時間のデータ収集の編集（P.3-38）
- 応答時間のデータ収集の削除（P.3-39）

応答時間のデータ収集の作成

Response Time データ収集をセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　コンテンツで **Response Time Monitoring** をクリックします。

Response Time Monitoring Setup テーブルが表示されます。

ステップ 3　**Create** をクリックします。

Response Time Monitoring Setup, Collection Configuration ダイアログボックス（表 3-19）が表示されます。

ステップ 4　適切な情報を選択します。

表 3-19　Response Time Monitoring Setup, Collection Configuration ダイアログボックス

フィールド	説明	使用法
Data Source List	利用可能なデータ ソースのリスト	リストからデータ ソースを選択します。
Report Interval (sec)	レポート間の秒数	秒数を入力します。デフォルトは 1800 です。
RspTime1 (msec)	最初のバケットの応答時間の上限	ミリ秒数を入力します。デフォルトは 5 です。
RspTime2 (msec)	2 番目のバケットの応答時間の上限	ミリ秒数を入力します。デフォルトは 15 です。
RspTime3 (msec)	3 番目のバケットの応答時間の上限	ミリ秒数を入力します。デフォルトは 50 です。
RspTime4 (msec)	4 番目のバケットの応答時間の上限	ミリ秒数を入力します。デフォルトは 100 です。
RspTime5 (msec)	5 番目のバケットの応答時間の上限	ミリ秒数を入力します。デフォルトは 200 です。
RspTime6 (msec)	6 番目のバケットの応答時間の上限	ミリ秒数を入力します。デフォルトは 500 です。
RspTimeMax (msec)	NAM が、クライアントのリクエストに対するサーバの応答を待つ最大時間	ミリ秒数を入力します。デフォルトは 3000 です。
Maximum Entries in Tables	レポートの最大行数	デフォルトは 500 です。

ステップ 5　変更を保存するには、**Submit** をクリックします。または、取り消すには、**Reset** をクリックします。

応答時間のデータ収集の編集

Response Time データ収集を編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　コンテンツで **Response Time Monitoring** をクリックします。

Response Time Monitoring Setup テーブルが表示されます。

データ ソースの名前の一部を入力して、**Filter** をクリックすることで、一致するデータ ソースを検索できます。**Clear** をクリックして、データ ソースの全体のリストに戻します。

ステップ 3　編集するデータ ソースを選択し、**Edit** をクリックします。

Response Time Monitoring Setup, Collection Configuration ダイアログボックス（表 3-19）が表示されます。

ステップ 4　必要な変更を加え、**Submit** をクリックして変更を保存するか、または **Reset** をクリックして変更を取り消します。

応答時間のデータ収集の削除

1 つ以上の応答時間のデータ収集を削除するには、Response Time Monitoring Setup テーブルでデータ収集を選択し、**Delete** をクリックします。

DiffServ データの監視

Differentiated Services Monitoring（DSMON または DiffServ）では、ネットワーク トラフィックによる Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値の使用を監視できます。

DiffServ データを監視するには、少なくとも 1 つの集約プロファイルと、各プロファイルに関連付けられた集約グループを 1 つ以上設定する必要があります。集約プロファイルの設定の詳細については、P.3-40 の「DiffServ プロファイルの作成」を参照してください。

Differentiated Service の監視をセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　DiffServ のコンテンツで、**Monitoring** をクリックします。

DiffServ Monitor Setup ダイアログボックス（表 3-20）が表示されます。

データ ソースの名前の一部を入力して、**Filter** をクリックすることで、一致するデータ ソースを検索できます。**Clear** をクリックして、データ ソースの全体のリストに戻します。

ステップ 3　適切な情報を選択します。

表 3-20　DiffServ Monitor Setup ダイアログボックス

要素	説明	使用法
Data Source List	利用可能なデータ ソースのリスト。	リストからデータ ソースを選択します。
DiffServ Profile List	利用可能なユーザ定義の DiffServ プロファイルのリスト。	リストから、ユーザ定義の DiffServ プロファイルを選択します。
Traffic Statistics	基本的な DSCP トラフィック分布を示します。	オンにしてイネーブルにするか、オフにしてディセーブルにします。
Application Statistics	アプリケーション プロトコルごとに DSCP トラフィック分布を示します。	オンにしてイネーブルにするか、オフにしてディセーブルにします。Max Entries リストで、エントリの最大数を選択します。
IP Host Statistics	ホストごとの DSCP トラフィック分布を示します。	オンにしてイネーブルにするか、オフにしてディセーブルにします。Max Entries リストで、エントリの最大数を選択します。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

DiffServ プロファイルのセットアップ

DiffServ プロファイルは、総括して監視できる集約グループのセットです。プロファイルを作成することで、DiffServ 収集をイネーブルにできます。DiffServ 収集のセットアップの詳細については、P.3-39 の「DiffServ データの監視」を参照してください。

次のトピックで、DiffServ プロファイルのセットアップと管理について説明します。

DiffServ プロファイルの作成

DiffServ プロファイルを作成するには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　DiffServ のコンテンツで、**Profile** をクリックします。

DiffServ Monitor Profile ダイアログボックスが表示されます。

ステップ 3　**Create** をクリックします。

DiffServ Profile Setup ダイアログボックス（表 3-21）が表示されます。

ステップ 4　適切な情報を選択します。

表 3-21　DiffServ Profile Setup ダイアログボックス

要素	説明	使用法
Template List	DiffServ プロファイルを作成するためのテンプレート	リストからテンプレートを選択します。テンプレートを使用しない場合は NONE を選択します。
Profile Name text box	プロファイルの名前	作成するプロファイルの名前を入力します。最大 64 文字です。
DSCP Value column	0 ～ 63 の、DSCP の数値	—
Group Description text boxes	各 DSCP 値の集約グループの名前	各 DSCP 値の集約グループの名前を入力します。最大 64 文字です。

ステップ 5　変更を保存するには、**Submit** をクリックします。または、取り消すには、**Reset** をクリックします。

DiffServ プロファイルの編集

DiffServ プロファイルを編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　DiffServ のコンテンツで、**Profile** をクリックします。

DiffServ Monitor Profile テーブルが表示されます。

ステップ 3　編集するプロファイルを選択し、**Edit** をクリックします。

DiffServ Profile Setup ダイアログボックス（表 3-21）が表示されます。

ステップ 4　必要な変更を加え、**Submit** をクリックして変更を保存するか、または **Reset** をクリックして変更を取り消します。

DiffServ プロファイルの削除

1 つまたは複数の DiffServ プロファイルを削除するには、DiffServ Monitor Profile テーブルでプロファイルを選択し、**Delete** をクリックします。

URL 収集データの監視

URL 収集では、選択されているデータ ソースの HTTP トラフィック（TCP ポート 80）が受信され、URL が収集されます。一度にイネーブルにできる収集は、1 つのデータ ソースで 1 つだけです。

URL（たとえば、**http://host.domain.com/intro?id=123**）は、ホスト部分（**host.domain.com**）、パス部分（**intro**）、および引数部分（**?id=123**）で構成されています。

収集では、すべての部分を収集するように設定することも、一部だけを収集して他の部分を無視するように設定することもできます。

この項では、次のトピックについて取り上げます。

- URL 収集のイネーブル化
- URL 収集の変更
- URL 収集のディセーブル化

URL 収集のイネーブル化

URL 収集をイネーブルにするには、次の手順を実行します。

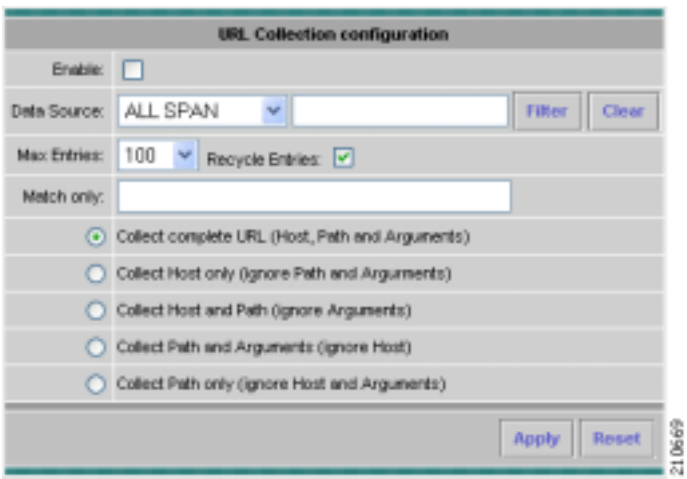
ステップ 1　**Setup** > **Monitor** を選択します。

Core Monitoring Functions テーブルが表示されます。

ステップ 2　**URL Collection** をクリックします。

URL Collection Configuration ダイアログボックス（図 3-11）が表示されます。

図 3-11　URL Collection Configuration ダイアログボックス



ステップ 3　URL 収集を開始するには、Enable チェックボックスをクリックします。

ステップ 4　URL Collection Configuration ダイアログボックス（表 3-22）に示されている情報を提供します。

データ ソースの名前の一部を入力して、**Filter** をクリックすることで、一致するデータ ソースを検索できます。**Clear** をクリックして、データ ソースの全体のリストに戻します。

(注) オプション ボタンのどのオプションが収集されるかによって、URL の形式が変わります。たとえば、「ホスト」部分が収集される場合は、先頭の *http:* 部分だけが存在します。*match only* 式を設定する場合は、この点に注意してください。

表 3-22　URL Collection Configuration ダイアログボックス

要素	説明	使用法
Datasource	アプリケーションから着信するトラフィックのタイプを示します。	ドロップダウン ボックスから、いずれかのオプションを選択します。
Max Entries	収集する URL の最大数。	ドロップダウン ボックスから、次のいずれかのオプションを選択します。 • 100 • 500 • 1000
Match only	照合対象のアプリケーション URL。	オプションのパラメータ。このフィールドの正規表現に一致する URL だけを収集するように制限します。

ステップ 5　エントリを再利用するには、Recycle Entries チェックボックスをクリックします。

ステップ 6　次のいずれかのチェックボックスをクリックします。

- Collect complete URL (Host, Path and Arguments)
- Collect Host only (ignore Path and Arguments)
- Collect Host and Path (ignore Arguments)
- Collect Path and Arguments (ignore Host)
- Collect Path only (ignore Host and Arguments)

ステップ 7　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

URL 収集の変更

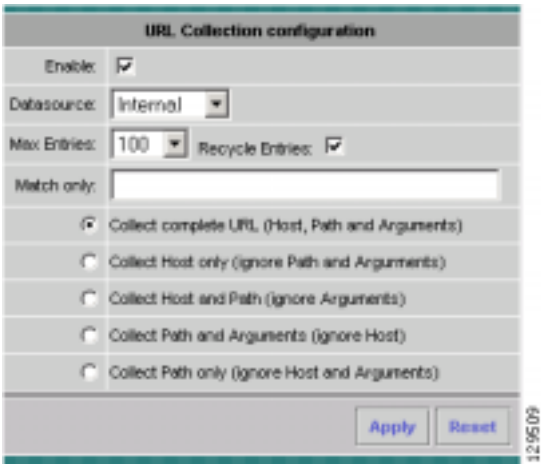
URL 収集を変更するには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

ステップ 2　**URL Collection** を選択します。

URL Collection Configuration ダイアログボックス（図 3-12）が表示されます。

図 3-12　URL Collection Configuration ダイアログボックス



ステップ 3　URL Collection Configuration ダイアログボックス（表 3-22）に示されている説明に従って情報を変更します。

（注）　パラメータを変更してその変更を適用すると、収集された URL がフラッシュされ、収集プロセスが再開されます。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

URL 収集のディセーブル化

URL 収集をディセーブルにするには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

ステップ 2　**URL Collection** をクリックします。

ステップ 3　Enabled ボックスをオフにします。

ステップ 4　**Apply** をクリックします。

プロトコル ディレクトリのセットアップ

NAM には、監視対象プロトコルのデフォルトのセットが含まれています。プロトコルは、NAM の RMON2 Protocol Directory テーブルで編集および削除できます。

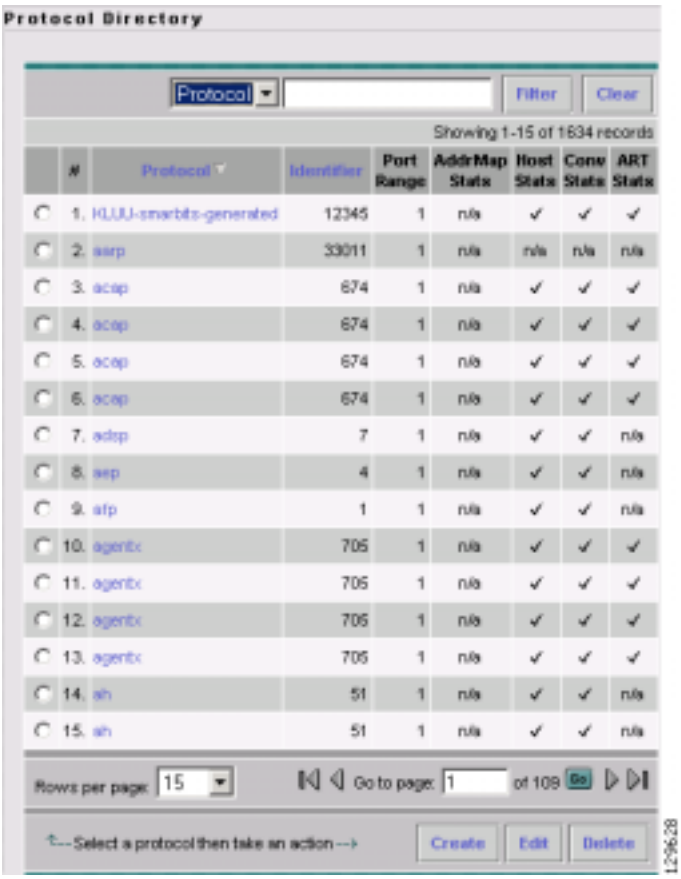
次のトピックで、プロトコル ディレクトリの管理について説明します。

- 個々のアプリケーション（P.3-45）
- アプリケーション グループのセットアップ（P.3-49）
- 自動認識プロトコルのセットアップ（P.3-50）
- URL ベースのアプリケーションのセットアップ（P.3-52）

個々のアプリケーション

Protocol Directory ウィンドウ（図 3-13）に、NAM にセットアップされているプロトコルが一覧されます。このウィンドウを使用して、表示、独自のプロトコルの追加、一般的なプロトコルの設定の編集を実行できます。

図 3-13　Protocol Directory テーブル



この項では、次のトピックについて取り上げます。

- 新しいプロトコルの作成（P.3-46）
- プロトコルの編集（P.3-47）
- プロトコルの削除（P.3-48）

新しいプロトコルの作成

ユーザはこの画面からプロトコル ディレクトリを変更しないでおくことを推奨します。NAM は、デフォルトのプロトコルで機能するように設計されています。また、SNMP 管理アプリケーションがプロトコル ディレクトリに加えた変更が、この画面でのカスタマイズの内容と競合することがあります。

新しいプロトコルを作成するには、次の手順を実行します。

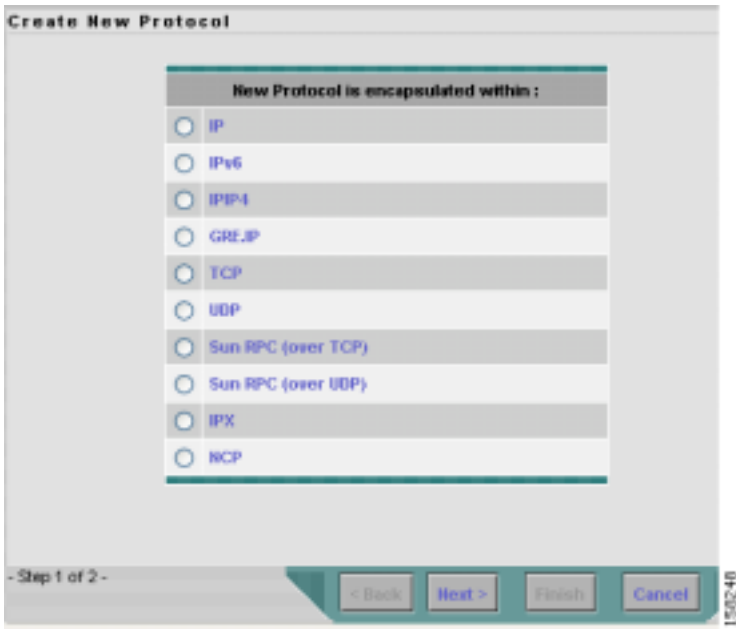
ステップ 1　**Setup** > **Protocol Directory** の順に選択します。

Protocol Directory テーブル（図 3-13）が表示されます。

ステップ 2　**Create** をクリックします。

Create New Protocol ウィンドウ（図 3-14）が表示されます。

図 3-14　New Protocol Parameters ウィンドウ



ステップ 3　新しいプロトコルのカプセル化方式を選択して、**Next** をクリックします。

New Protocol Parameters ウィンドウ（図 3-15）が表示されます。このウィンドウは、選択したプロトコル タイプに応じて異なります。

図 3-15　New Protocol Parameters ウィンドウ

ステップ 4　適切な情報を選択します。

表 3-23　New Protocol Parameters ダイアログボックス

フィールド	説明	使用法
Protocol Identification Value、たとえば次のような値 • IP Protocol • TCP Port • UDP Port	新しいプロトコルを識別する数値	1 ～ 255 の数値を選択します。
Name	プロトコルの完全な名前	—
Port Range	このプロトコルのポート範囲	1 ～ 255 の数値を選択します。
Affected Stats	• アドレス マップ • ホスト • 会話 • ART	プロトコルで収集すべき統計情報を選択します。 そのプロトコルで表示できない統計情報は、灰色で表示されます。

ステップ 5　変更を保存するには、**Finish** をクリックします。または、取り消すには、**Reset** をクリックします。

ヒント　完全なプロトコル名を表示するには、Protocol Directory テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

プロトコルの編集

NAM プロトコル ディレクトリの設定は何も変更しないことをお勧めします。デフォルトの設定を変更すると、NetScout nGenius Real-Time Monitor などの SNMP ベースの管理アプリケーションで予期しない動作が生じる場合があります。ただし、上級ユーザの場合、独自のプロトコルの監視や、一般的なプロトコルの通常の設定の変更を行うこともできます。

プロトコルを編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

Protocol Directory テーブルが表示されます。

ステップ 2　編集するプロトコルを選択し、**Edit** をクリックします。

Edit Protocol ダイアログボックス（表 3-24）が表示されます。

ステップ 3　必要な変更を加えます。

表 3-24　Edit Protocol ダイアログボックス

フィールド	説明	使用法
Name	プロトコルの名前	
Currently displayed as	Protocol Directory テーブルに表示されるプロトコル名	
Port Range	このプロトコルのポート範囲	
Encapsulation	プロトコルのカプセル化タイプ	
Affected Stats	プロトコルで収集できる統計情報 • アドレス マップ • ホスト • 会話 • ART	そのプロトコルで表示できない統計情報は、灰色で表示されます。

ステップ 4　次のいずれかを実行します。

- 変更を確定するには、**Submit** をクリックします。
- 設定を元のままにするには、**Cancel** をクリックします。
- プロトコルを削除するには、**Delete** をクリックします。

ヒント
- 特定のプロトコルの Edit Protocol ダイアログボックスを表示するには、Protocol Directory テーブルでプロトコル名をクリックします。
- 完全なプロトコル名を表示するには、Protocol Directory テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

プロトコルの削除

プロトコルを削除するには、Protocol Directory テーブルで選択し、**Delete** をクリックします。

ヒント　プロトコルは Edit Protocol Directory ダイアログボックスでも削除できます。プロトコルを選択し、**Delete** をクリックしてください。

アプリケーション グループのセットアップ

アプリケーション グループは、総括して監視できるアプリケーション プロトコルのセットです。次のトピックで、アプリケーション グループのセットアップと管理について説明します。

- アプリケーション グループの作成（P.3-49）
- アプリケーション グループの編集（P.3-50）
- アプリケーション グループの削除（P.3-50）

アプリケーション グループの作成

アプリケーション グループを作成するには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

Protocol Directory テーブルが表示されます。

ステップ 2　Content メニューから **Application Groups** を選択します。

ステップ 3　**Create** をクリックします。

New Application Group ダイアログボックス（表 3-25）が表示されます。

ステップ 4　アプリケーション グループ名を入力します。

ステップ 5　適切な情報を選択します。

表 3-25　New Application Group ダイアログボックス

要素	説明	使用法
Application Group Name	グループ名	グループ名を入力します。
Encapsulation	アプリケーションのカプセル化	ドロップダウン ボックスからカプセル化を選択します。
Application Filter	フィルタリングまたはクリアのためのオプション	フィルタリングするプロトコルの名前を入力します。最大 64 文字です。
Application	アプリケーションのリスト	アプリケーションを選択して、**Add** をクリックします。 Selected Applications ボックスにアプリケーションが表示されます。

ステップ 6　変更を保存するには、**Submit** をクリックします。または、取り消すには、**Reset** をクリックします。

アプリケーション グループの編集

アプリケーション グループを編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

Individual Applications ウィンドウが表示されます。

ステップ 2　Content メニューから Application Groups を選択します。

Application Groups ウィンドウが表示されます。

ステップ 3　編集するアプリケーション グループを選択して、**Edit** をクリックします。

Application Groups Edit ウィンドウが表示されます。

ステップ 4　必要な変更を加え、**Submit** をクリックして変更を保存するか、または **Reset** をクリックして変更を取り消します。

アプリケーション グループの削除

1 つまたは複数のアプリケーション グループを削除するには、Application Groups テーブルでプロファイルを選択し、**Delete** をクリックします。

自動認識プロトコルのセットアップ

Autolearned Protocols Preferences ウィンドウで、アプリケーション情報を自動的に認識するように NAM を設定できます。次のプリファレンスを設定できます。

- 認識対象のプロトコル数（100 ～ 500）
- 認識対象の TCP ポート数（0 ～ 65535）
- 認識対象の UDP ポート数（0 ～ 65535）
- 認識対象でない TCP ポート範囲（1 ～ 65535）
- 認識対象でない UDP ポート範囲（1 ～ 65535）

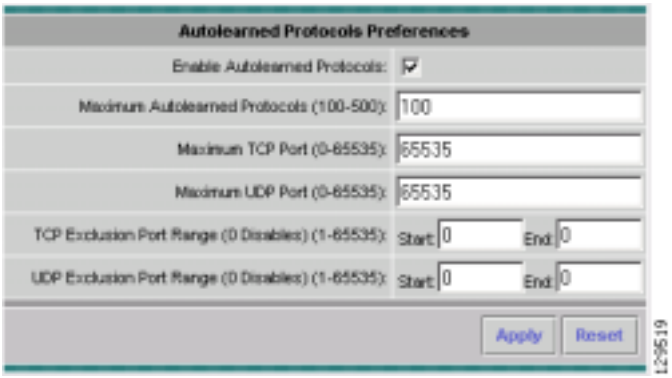
自動認識プロトコルのプリファレンスをセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

ステップ 2　**Autolearned Applications** をクリックします。

Autolearned Protocols Preferences ダイアログボックス（図 3-16）が表示されます。

図 3-16　Autolearned Protocols Preferences ダイアログボックス



ステップ 3　Autolearned Protocols Preferences ダイアログボックス（表 3-26）に示されている情報を入力または変更します。

表 3-26　Autolearned Protocols Preferences ダイアログボックス

フィールド	説明	使用法
Enable Autolearned Protocols	自動認識プロトコル機能をイネーブルにします。	チェックボックスをオンにするとイネーブルになります。
Maximum Autolearned Protocols	自動認識できるプロトコルの最大数。	100 ～ 500 の数値を入力します。デフォルトは 100 です。
Maximum TCP Port	自動認識できる TCP ポートの最大数。	0 ～ 65535 の数値を入力します。
Maximum UDP Port	自動認識できる UDP ポートの最大数。	0 ～ 65535 の数値を入力します。
TCP Exclusion Port Range	除外する TCP ポートの範囲を指定します。	0 ～ 65535 の数値を入力します（0 の場合はディセーブル）。
Start	除外範囲の最初の TCP ポートを指定します。	
End	除外範囲の最後の TCP ポートを指定します。	
UDP Exclusion Port Range:	除外する UDP ポートの範囲を指定します。	0 ～ 65535 の数値を入力します（0 の場合はディセーブル）。
Start	除外範囲の最初の UDP ポートを指定します。	
End	除外範囲の最後の UDP ポートを指定します。	

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

URL ベースのアプリケーションのセットアップ

URL ベースのアプリケーションは、プロトコル ディレクトリの拡張です。HTTP 要求内の URL（TCP ポート 80 上の URL）が URL ベースのアプリケーションの基準を満たすと、トラフィックはそのプロトコルとして分類されます。

URL ベースのアプリケーションは、プロトコル ディレクトリ内の他のプロトコルと同様に使用できます。たとえば、URL ベースのアプリケーションは、収集、キャプチャ、およびレポートで使用できます。

着信 URL は、一致が見つかるまで、インデックスの順序で、設定されている URL ベースのアプリケーションの基準と照合されます。一致が見つかった場合、残りの URL ベースのアプリケーションは照合対象になりません。

この項では、次のトピックについて取り上げます。

- URL ベースのアプリケーションの作成
- URL ベースのアプリケーションの編集
- URL ベースのアプリケーションの削除

URL ベースのアプリケーションの作成

URL は、次の部分で構成されています。

- ホスト
- パス
- 引数

たとえば、**URL http://host.domain.com/intro?id=123** の場合、次のようになります。

- 「*ホスト*」部分は **host.domain.com**
- 「*パス*」部分は **/intro**
- 「*引数*」部分は **?id=123**

URL ベースのアプリケーションの設定では、パス部分と引数パスが結合されて「*パス部分*」と呼ばれます。

（注） URL ベースのアプリケーションの一致文字列は、POSIX で規定されている正規表現です。

（注） URL ベースのアプリケーションは、最大 64 個定義できます。

URL ベースのアプリケーションをセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

ステップ 2　TOC で **URL-Based Applications** をクリックします。

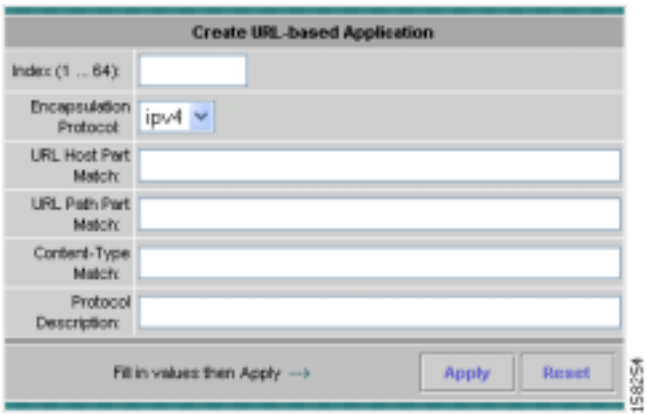
URL Matches ダイアログボックス（図 3-17）が表示されます。

図 3-17　URL Matches ダイアログボックス

ステップ 3　**Create** をクリックします。

Create URL Match Entry ダイアログボックス（図 3-18）が表示されます。

図 3-18　Create URL Match Entry ダイアログボックス



ステップ 4　URL Match Entry ダイアログボックス（表 3-27）に示されている情報を入力します。

プロトコル名の作成に関する規則は、RFC 2895 で規定されています。その規則に従って、次の文字だけを使用できます。

- A ～ Z
- a ～ z
- 0 ～ 9
- ダッシュ（-）
- 下線（_）
- アスタリスク（*）
- プラス記号（+）

（注）　その他すべての文字は、ダッシュ（-）に変更されます。

表 3-27　URL Match Entry ダイアログボックス

フィールド	説明	使用法
Index	このインデックスの順序で、URL 照合が実行されます。	1 ～ 64 の数値を入力します。 インデックスを変更するには、エントリを削除して、新しいインデックス値で作成し直す必要があります。
Encapsulation Protocol	URL をカプセル化するプロトコル。	ドロップダウン ボックスから IPv4 または IPv6 を選択します。
URL Host Part Match	ホスト部分の照合対象となる POSIX 正規表現。	たとえば、**domain.com**。
URL Path Part Match	URL のパス部分と引数部分の照合対象となる POSIX 正規表現。	たとえば、**/intro?id**。
Content Type Match	メッセージのデータ タイプを識別する HTTP ヘッダー内のコンテンツタイプ。MIME タイプとしても知られています。	次の例を参考にしてください。 application/octet-stream, text/html、または image/gif。
Protocol Description	URL ベースのアプリケーションの名前。	たとえば、**url-match-domain-com**。

ステップ 5　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

URL ベースのアプリケーションの編集

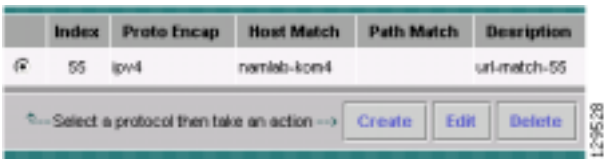
URL ベースのアプリケーションを編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

ステップ 2　TOC で **URL-Based Applications** をクリックします。

URL Matches ダイアログボックス（図 3-19）が表示されます。

図 3-19　URL Matches ダイアログボックス



ステップ 3　URL を選択し、**Edit** をクリックします。

Edit URL Match Entry ダイアログボックス（図 3-20）が表示されます。

(注)　URL　ベースのアプリケーションを編集する場合、インデックスは変更できません。インデックスを変更する（実行順序を変更する）には、URL ベースのアプリケーションを削除して作成し直してください。

図 3-20　Edit URL Match Entry ダイアログボックス

URL Match Entry ダイアログボックス（表 3-27）の説明に従って情報を変更します。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

URL ベースのアプリケーションの削除

URL ベースのアプリケーションを削除するには、次の手順を実行します。

ステップ 1　**Setup** > **Protocol Directory** を選択します。

ステップ 2　TOC で **URL-Based Applications** をクリックします。

URL Matches ダイアログボックス（図 3-21）が表示されます。

図 3-21　URL Matches ダイアログボックス

ステップ 3　URL を選択し、**Delete** をクリックします。

アラームしきい値の設定

NAM のアラームしきい値をセットアップするには、次の監視対象変数を NAM に設定します。

- 応答時間
- サーバとクライアント間の応答時間
- DiffServ ホストの統計情報
- DiffServ トラフィックの統計情報
- DiffServ アプリケーションの統計情報
- 音声プロトコル
- スイッチの Mini-RMON MIB
- ネットワーク層の統計情報
- MAC 層の統計情報
- アプリケーションの統計情報

(注)　MAC 層と Mini-RMON の統計情報は、NM-NAM デバイスには適用されません。

次のトピックで、アラームしきい値の設定のセットアップと管理について説明します。

- NAM の MIB しきい値の設定（P.3-56）
- 音声しきい値の設定（P.3-60）
- 上流 RTP ストリームのしきい値の設定（P.3-61）
- NAM Syslog のセットアップ（P.3-61）
- スイッチしきい値の設定（P.3-63）
- NAM のトラップ宛先の設定（P.3-66）
- NAM アラーム メールの設定（P.3-67）

NAM の MIB しきい値の設定

NAM の MIB しきい値は、アラームをトリガーする設定値です。しきい値はネットワーク ホスト、MAC 層ホスト、ネットワーク層の会話、および MAC 層の会話に対して設定できます。

(注)　MAC 層ホストと MAC 層の会話は、NM-NAM デバイスでは使用できません。

	ウィザードのページ	参照項目
ステップ 1	Select a Variable	P.3-57 の「NAM の MIB 変数の選択」
ステップ 2	Select Parameters	P.3-57 の「NAM の MIB パラメータの選択」

NAM の MIB 変数の選択

NAM の MIB 変数を選択するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

ステップ 2　Thresholds テーブルが表示されます。

ステップ 3　**Create** をクリックします。

ステップ 4　Alarms ウィザードが表示されます。次の表に、NAM の MIB しきい値を作成する手順を示します。

	ウィザードのページ	参照項目
ステップ 1	Select a Variable	P.3-57 の「NAM の MIB 変数の選択」
ステップ 2	Select Parameters	P.3-57 の「NAM の MIB パラメータの選択」

NAM の MIB パラメータの選択

NAM の MIB パラメータを選択するには、次の手順を実行します。

ステップ 1　Variable リストからアラーム変数を選択します。Variable リストには、しきい値を設定できる MIB 変数が表示されます。

ステップ 2　Network Protocol リストでネットワーク プロトコルを選択し、**Next** をクリックします。

New Alarm ダイアログボックス（表 3-28）が表示されます。

ステップ 3　適切な情報を選択します。

表 3-28　New Alarm ダイアログボックス

フィールド	説明	使用法
Data Source	NAM で使用できるデータ ソース	リストからデータ ソースを選択します。
Aggregate Group	選択した DiffServ プロファイルの集約グループ	DiffServ 変数のみ。
Network Protocol	監視対象として選択されたプロトコル	ウィザードのステップ 1 の変数。
Application Protocol	監視対象のアプリケーション プロトコル	リストからアプリケーション プロトコルを選択します。サーバおよびサーバクライアントの応答時間変数のみ。
Variable	監視対象として選択された変数	ウィザードのステップ 1 の変数。
Server Address	サーバのネットワーク アドレス	サーバおよびサーバクライアントの応答時間変数のみ。
Client Address	クライアントのネットワーク アドレス	サーバクライアントの応答時間変数のみ。
Network Address	ホストのネットワーク アドレス	ネットワーク層ホストの変数のみ。

表 3-28　New Alarm ダイアログボックス（続き）

フィールド	説明	使用法
MAC Address	ホストの MAC アドレス	MAC 層ホストの変数のみ。 **（注）** MAC 層の変数は、NM-NAM デバイスでは使用できません。
Dst Address	ホストの宛先 IP アドレスまたは MAC アドレス	MAC 層またはネットワーク層の会話の変数のみ。 **（注）** MAC 層の変数は、NM-NAM デバイスでは使用できません。
Src Address	ホストの送信元 IP アドレスまたは MAC アドレス	MAC 層またはネットワーク層の会話の変数のみ。 **（注）** MAC 層の変数は、NM-NAM デバイスでは使用できません。
Interval	サンプリング期間が継続するインターバルの秒数	10 進値を入力します。
Description	アラームの説明	128 文字以下にします。
Sample Type	実行するサンプリングのタイプ	• ある絶対値に達した場合にトリガーされるアラームを設定するには **Absolute** をクリックします。 • データ　レートの変更によってトリガーされるアラームを設定するには **Delta** をクリックします。
Rising Threshold	アラームをトリガーするパケットまたはオクテットの数。応答時間アラームの場合はミリ秒数	10 進数を入力します。
Falling Threshold	アラームをトリガーするパケットまたはオクテットの数。応答時間アラームの場合はミリ秒数	10 進数を入力します。
Alarm Action	アラームがトリガーされた場合に実行するアクション	• イベントをログに記録して Alarms タブに表示するには、**Log** をクリックします。 • イベントをトラップに送るには、**Trap** をクリックします。 • イベントをログに記録してトラップに送るには、**Log and Trap** をクリックします。
Community	トラップが送られる SNMP コミュニティ	このコミュニティ ストリングは、NAM トラップに設定されているコミュニティ ストリングと一致する必要があります。
Capture Trigger	アラームのしきい値がトリガーされたときにキャプチャを開始または停止	• Capture Trigger をディセーブルにするには **None** をクリックします。 • アラームしきい値がトリガーされた場合にキャプチャを開始するには **Start** をクリックします。 • アラームしきい値がトリガーされた場合にキャプチャを停止するには **Stop** をクリックします。

ステップ 4　変更を受け入れるには、**Finish** をクリックします。または、取り消すには、**Cancel** をクリックします。

NAM MIB Thresholds テーブルのアラーム詳細表示

NAM MIB Thresholds テーブルの特定のアラームの詳細を表示するには、オプション ボタンを選択し、**Details** をクリックします。Alarms Details テーブル（表 3-29）が表示されます。

表 3-29　Alarm Details テーブル

フィールド	説明
Variable	監視対象の変数。
Data Source	監視対象のデータ ソース。
Address	ホストの宛先アドレスおよび送信元アドレス。
Interval (seconds)	サンプリング期間のインターバル。
Description	アラームの説明。
Sample Type	アラームのサンプル タイプ：Absolute または Delta。
Rising Threshold	アラームをトリガーする増加パケットまたはオクテットの数。
Falling Threshold	アラームをトリガーする減少パケットまたはオクテットの数。
Alarm Action	アラームがトリガーされた場合に実行するアクション。
Community	トラップが送られる SNMP コミュニティ。
Trigger Set	None、Start、または Stop。Start は、このアラームがトリガーされるときにキャプチャ プロセスが開始することを示します。Stop は、このアラームがトリガーされるときにキャプチャ プロセスが停止することを意味します。None は、このアラームにキャプチャ トリガーが設定されていないことを意味します。 アラームによってトリガーされるキャプチャ機能の使用方法については、自動キャプチャ（アラームによってトリガーされるキャプチャ）の使用を参照してください。

NAM の MIB しきい値の編集

NAM の MIB しきい値を編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

Thresholds テーブルが表示されます。

ステップ 2　編集するアラームを選択し、**Edit** をクリックします。

Edit Alarm ダイアログボックスが表示されます。

ステップ 3　必要な変更を加えます。

ステップ 4　変更を保存するには、**Submit** をクリックします。または、取り消すには、**Reset** をクリックします。

NAM の MIB しきい値の削除

NAM の MIB しきい値を削除するには、Alarms テーブルで選択し、**Delete** をクリックします。

音声しきい値の設定

音声しきい値のイベントは、NAM にローカルにログ記録することも、リモートの Syslog ホストに送ることもできます。Syslog のセットアップについては、P.3-61 の「NAM Syslog のセットアップ」を参照してください。

音声しきい値を設定するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

NAM MIB Thresholds テーブルが表示されます。

ステップ 2　コンテンツ メニューで **NAM Voice Thresholds** をクリックします。

Voice Alarms ダイアログボックス（表 3-30）が表示されます。

ステップ 3　適切な情報を選択します。

表 3-30　Voice Alarms ダイアログボックス

プロトコル	条件	しきい値
SCCP	Jitter Threshold：ジッタを監視するときに選択します。	しきい値をミリ秒で入力します。
	Pkt Loss Threshold：パケット損失の数を監視するときに選択します。	しきい値として、1 通話あたりに損失されるパケットのパーセントを入力します。
H.323	Jitter Threshold：ジッタを監視するときに選択します。	しきい値をミリ秒で入力します。
	Pkt Loss Threshold：パケット損失の数を監視するときに選択します。	しきい値として、1 通話あたりに損失されるパケットのパーセントを入力します。
MGCP	Jitter Threshold：ジッタを監視するときに選択します。	しきい値をミリ秒で入力します。
	Pkt Loss Threshold：パケット損失の数を監視するときに選択します。	しきい値として、1 通話あたりに損失されるパケットのパーセントを入力します。
SIP	Jitter Threshold：ジッタを監視するときに選択します。	しきい値をミリ秒で入力します。
	Pkt Loss Threshold：パケット損失の数を監視するときに選択します。	しきい値として、1 通話あたりに損失されるパケットのパーセントを入力します。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、設定を変更せずそのままにしておくには、**Reset** をクリックします。

上流 RTP ストリームのしきい値の設定

RTP ストリームを監視し、RTP シーケンス番号に基づいてパケット損失統計情報を表示するように、NAM をセットアップできます。RTP ストリームのしきい値をセットアップし、アラームをイネーブルにすると、**Admin > System > EMail Configuration** で設定された宛先に E メール アラーム メッセージが送信されます。E メールを設定する方法については、P.2-15 の「E メールの設定」を参照してください。

ステップ 1　**Setup** > **Alarms** を選択します。

NAM MIB Thresholds テーブルが表示されます。

ステップ 2　コンテンツ メニューで **NAM RTP Stream Thresholds** をクリックします。

NAM RTP Steam Thresholds ウィンドウが表示されます。表 3-31 に、NAM RTP Steam Thresholds ウィンドウのフィールドを示します。

表 3-31　NAM RTP Steam Thresholds

フィールド	説明
Enable Alarm	オンにすると、NAM RTP ストリームしきい値アラームがイネーブルになります。
Number of Consecutive Packets Loss (1-10)	連続するパケットの損失数。ここで入力した数より多くの連続パケットを損失したストリームは、アラーム メッセージを生成します。
Packet Loss Threshold (10^{-6})	パケット損失率（1 ～ 100）。パケット損失率がここで入力した値を上回るストリームは、アラーム メッセージを生成します。

ステップ 3　Number of Consecutive Packets Loss フィールドに値（1 ～ 10）を入力します。

ステップ 4　Packet Loss Threshold フィールドに値（1 ～ 100）を入力します。

ステップ 5　**Enable Alarm** をオンにし、**Apply** をクリックして、NAM RTP ストリームしきい値をアクティブにします。

NAM Syslog のセットアップ

NAM Syslog は、MIB しきい値のイベント、音声しきい値のイベント、またはシステム アラートに関して作成されます。NAM では、Syslog ファイルが 2 つ保持されます。1 つは RMON のしきい値イベント（MIB しきい値および音声しきい値）のロギング用で、もう 1 つはローカル NAM のシステム アラートのロギング用です。

Syslog メッセージを NAM にローカルに記録するか、リモート ホストに記録するか、または両方に記録するかを指定できます。ローカル NAM の Syslog を表示するには、NAM Traffic Analyzer を使用します。

Syslog の表示については、第 7 章「アラームの表示」を参照してください。標準のテキスト エディタを使用して、リモート ホストに Syslog を表示できます。

NAM syslog をセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

NAM MIB Thresholds テーブルが表示されます。

ステップ 2　コンテンツ メニューで **NAM Syslog** をクリックします。

NAM Alarms Syslog ダイアログボックス（表 3-32）が表示されます。

ステップ 3　必要な変更を加えます。

表 3-32　NAM Alarms Syslog ダイアログボックス

フィールド	使用法
MIB Thresholds	• ローカル システムにメッセージを記録するには、**Local** を選択します。 • リモート システムにメッセージを記録するには、**Remote** を選択します。
Voice	• ローカル システムに音声しきい値の Syslog を記録するには、**Local** を選択します。 • リモート システムに音声しきい値の Syslog を記録するには、**Remote** を選択します。
RTP Stream	• ローカル システムに RTP ストリームしきい値の Syslog を記録するには、**Local** を選択します。 • リモート システムに RTP ストリームしきい値の Syslog を記録するには、**Remote** を選択します。
System	• ローカル システムにシステム アラートの Syslog を記録するには、**Local** を選択します。 • リモート システムにシステム アラートの Syslog を記録するには、**Remote** を選択します。 • アプリケーションから Syslog へのデバッグ メッセージを記録するには、**Debug** を選択します。
Remote Server Names	Syslog メッセージが記録されるリモート システムの IP アドレスまたは DNS 名を、最大 5 つまで入力します。入力した各アドレスでは、3 つのアラームすべて（MIB、音声、システム）の Syslog メッセージを受信します。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

スイッチしきい値の設定

(注)　この項の内容は、NM-NAM デバイスには適用されません。

スイッチの Mini-RMON MIB に、RMON のしきい値を設定できます。しきい値超過条件の監視で指定できるのは、Mini-RMON MIB の etherStatsTable の変数のみです。

次のトピックで、スイッチしきい値のセットアップと管理について説明します。

- スイッチしきい値の作成（P.3-63）
- スイッチしきい値の編集（P.3-65）
- スイッチしきい値の削除（P.3-65）

スイッチしきい値の作成

(注)　この項の内容は、NM-NAM デバイスには適用されません。

スイッチしきい値を作成するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

Thresholds テーブルが表示されます。

ステップ 2　コンテンツで **Switch Thresholds** をクリックします。

Switch Threshold Alarms ダイアログボックスが表示されます。

ステップ 3　**Create** をクリックします。

New Switch Alarm ダイアログボックス（表 3-33）が表示されます。

表 3-33　New Switch Alarm ダイアログボックス

フィールド	説明	使用法
Data Source List	スイッチからのデータ ソース。	—
Variable	次の変数が使用可能です。 • Broadcast Pkts • Collisions • CRC Align Errors • Drop Events • Fragments • Jabbers • Multicast Pkts • Bytes • Oversize Pkts • Packets • Pkts size 64 Bytes • Pkts 65 to 127 Bytes • Pkts 128 to 255 Bytes • Pkts 256 to 511 Bytes • Pkts 512 to 1023 Bytes • Pkts 1024 to 1518 Bytes • Undersize Pkts	—
Interval (seconds)	サンプリング期間が継続する時間の秒数。	10 進数を入力します。
Description	アラームの説明。	128 文字以下にします。
Sample Type	実行するサンプリングのタイプ。	• ある絶対値に達した場合にトリガーされるアラームを設定するには **Absolute** をクリックします。 • データ レートの変更によってトリガーされるアラームを設定するには **Delta** をクリックします。
Rising Threshold	アラームをトリガーするパケットまたはオクテットの数。	10 進数を入力します。
Falling Threshold	アラームをトリガーするパケットまたはオクテットの数。	10 進数を入力します。
Alarm Action	アラームがトリガーされた場合に実行するアクション。	• イベントをログに記録して Alarms タブに表示するには、**Log** をクリックします。 • イベントをトラップに送るには、**Trap** をクリックします。 • イベントをログに記録してトラップに送るには、**Log and Trap** をクリックします。
Community	トラップが送られる SNMP コミュニティ。	このコミュニティ ストリングは、スイッチに設定されているコミュニティ ストリングと一致する必要があります。

ステップ 4　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

（注）　Catalyst オペレーティング システム イメージが稼動しているスイッチの場合、スイッチのアラーム設定は自動的に保存されます。Cisco IOS イメージの場合は、アラームの設定を NVRAM に保存できます。

スイッチしきい値の編集

（注）　この項の内容は、NM-NAM デバイスには適用されません。

スイッチしきい値を編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

Thresholds テーブルが表示されます。

ステップ 2　コンテンツ メニューで **Switch Thresholds** をクリックします。

Switch Threshold Alarms ダイアログボックスが表示されます。

ステップ 3　編集するアラームを選択し、**Edit** をクリックします。

Edit Alarm ダイアログボックスが表示されます。

ステップ 4　必要な変更を加え、**Submit** をクリックして変更を保存するか、または **Reset** をクリックして変更を取り消し、設定を変更せずそのままにします。

スイッチしきい値の削除

（注）　この項の内容は、NM-NAM デバイスには適用されません。

既存のスイッチしきい値のアラームを削除するには、Switch Threshold Alarms テーブルで選択し、**Delete** をクリックします。

NAM のトラップ宛先の設定

トラップは、しきい値超過イベントによってトリガーされたアラームを格納するために使用されます。アラームがトリガーされると、イベントをトラップし、別のホストに送ることができます。

次のトピックで、NAM のトラップのセットアップと管理について説明します。

- NAM のトラップ宛先の作成（P.3-66）
- NAM のトラップ宛先の編集（P.3-66）
- NAM のトラップ宛先の削除（P.3-67）

NAM のトラップ宛先の作成

NAM トラップの宛先を作成するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

NAM MIB Thresholds テーブルが表示されます。

ステップ 2　コンテンツで **NAM Trap Destinations** をクリックします。

Traps ダイアログボックスが表示されます。

ステップ 3　**Create** をクリックします。

Create Trap ダイアログボックス（表 3-34）が表示されます。

ステップ 4　適切な情報を入力します。

表 3-34　Create Trap ダイアログボックス

フィールド	説明
Community	NAM の MIB しきい値に設定されているアラーム コミュニティ ストリングのコミュニティ ストリング
Address	アラームとトラップのコミュニティ ストリングが一致した場合にトラップが送信される IP アドレス
UDP Port	UDP ポート番号

ステップ 5　変更を保存するには、**Submit**　をクリックします。または、設定を変更せずそのままにしておくには、**Reset** をクリックします。

NAM のトラップ宛先の編集

NAM トラップの宛先を編集するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

Thresholds テーブルが表示されます。

ステップ 2　コンテンツで **NAM Traps** をクリックします。

Traps ダイアログボックスが表示されます。

ステップ 3　編集するトラップを選択し、**Edit** をクリックします。

Edit Trap ダイアログボックスが表示されます。

ステップ 4　必要な変更を加えます。

ステップ 5　変更を保存するには、**Submit** をクリックします。または、設定を変更せずそのままにしておくには、**Reset** をクリックします。

NAM のトラップ宛先の削除

既存のトラップを削除するには、Traps テーブルで選択し、**Delete** をクリックします。

NAM アラーム メールの設定

（注）　NAM アラームは、ルータ アラームまたはスイッチ アラームではなく、NAM アラームの結果として送信されます。

NAM アラームが発生した場合に、1 つ以上のアドレスに E メールを送信するように NAM を設定できます。E メール アラームを設定するには、次の手順を実行します。

ステップ 1　**Setup** > **Alarms** を選択します。

ステップ 2　コンテンツ メニューで **NAM Alarm Mail** をクリックします。

Alarm Mail Configuration ダイアログボックスが表示されます。

ステップ 3　**Mail Alarm to** フィールドで、NAM アラーム メールを受信する 1 つ以上の E メール アドレスを入力します。

jdoe@cisco.com などの E メール アドレスを使用します。複数の E メール アドレスを入力する場合は、スペースで区切ります。

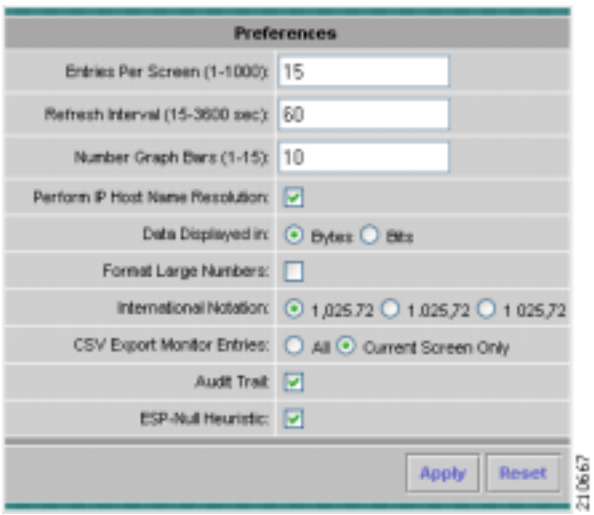
グローバル プリファレンスの設定

グローバル プリファレンスの設定は NAM のすべてのユーザに適用され、データの表示形式が決定されます。グローバル プリファレンスをセットアップするには、次の手順を実行します。

ステップ 1　**Setup** > **Preferences** を選択します。

Preferences ダイアログボックス（図 3-22）が表示されます。

図 3-22　Preferences ダイアログボックス



ステップ 2　Preferences ダイアログボックス（表 3-35）に示されている情報を入力または変更します。

表 3-35　Preferences ダイアログボックス

フィールド	説明	使用法
Entries Per Screen	表形式の画面で表示する行の数。	1 ～ 100 の数値を入力します。デフォルトは 15 です。
Refresh Interval	モニタ画面がリフレッシュされる間隔の秒数。	15 ～ 3600 の数値を入力します。デフォルトは 60 です。
Number Graph Bars	TopN 表示およびチャートで表示する棒グラフの数。	1 ～ 15 の数値を入力します。デフォルトは 10 です。
Perform IP Host Name Resolution	DNS 名がある場合、それを表示します。	オンにしてイネーブルにするか、オフにしてディセーブルにします。デフォルトではイネーブルです。 **（注）** ネーム サーバを設定しないで IP ホスト名の解決をイネーブルにすると、応答時間が低下する場合があります。

表 3-35　Preferences ダイアログボックス（続き）

フィールド	説明	使用法
Data Displayed in	データをビット単位またはバイト単位で表示するためのオプション。	Bytes または Bits を選択します。デフォルトは Bytes です。
Format Large Numbers	キロ（K）、メガ（M）、ギガ（G）、テラ（T）などのプレフィックスを付けて、適切な単位で大きな整数値を表示します。	大きな数値をフォーマットするためのチェックボックス。このボックスがオフである場合、大きな数値はフォーマットされません。デフォルトはオフです。
International Notation	次の形式で数値を出力するためのオプション。 1,025.72 1.025,72 1 025,72	デフォルトは 1,025.72 です。
CSV Export Monitor Entries	特定のモニタ テーブル内のすべてのエントリを CSV でエクスポートするか、または特定のウィンドウに表示されている現在のエントリだけを CSV でエクスポートするためのオプションを提供します。	デフォルトは、Current Window Only です。
Audit Trail	監査証跡をイネーブル化またはディセーブル化するためのチェックボックス。	重要なユーザ アクティビティの内部ログ ファイルへの記録をイネーブルにします。デフォルトでは、監査証跡はイネーブルです。 参照： • 監査証跡エントリについては、P.2-23 の「監査証跡の表示」を参照のこと。 • リモート ファイル ストレージのセットアップについては、P.3-61 の「NAM Syslog のセットアップ」を参照のこと。
ESP-Null Heuristic	NAM が、インターネット RFC 2410 の規定に従い、ESP ヌル暗号化を検出し、コンテンツを解析できるようにします。	ESP-Null Heuristic をイネーブルにすると、NAM は ESP ヘッダーを持つすべてのパケットをチェックし、ヌル暗号化を使用しているかどうかを確認します。ESP-Null Heuristic 機能は、処理オーバーヘッドを追加するため、デフォルトではディセーブルになっています。

ステップ 3　変更を保存するには、**Apply** をクリックします。または、取り消すには、**Reset** をクリックします。

CHAPTER 4

データの監視

Monitor タブには、さまざまなタイプの監視対象データを表示するオプションがあります。次のオプションがあります。

- データ収集およびデータ ソースの概要（P.4-2）
- Monitor Overview チャートの表示（P.4-6）
- アプリケーション グループの表示（P.4-9）
- 個別のアプリケーション データの表示（P.4-14）
- 収集された URL の表示（P.4-19）
- 音声データの表示（P.4-22）
- ホスト データの監視（P.4-32）
- 会話データの表示（P.4-41）
- VLAN データの表示（P.4-49）
- DiffServ データの表示（P.4-55）
- 応答時間データの監視（P.4-67）
- ポート / インターフェイス統計情報データの表示（P.4-81）
- システム状態の表示（P.4-90）
- NBAR の表示（P.4-98）
- MPLS トラフィック統計情報の表示（P.4-101）

データ収集およびデータ ソースの概要

NAM が作成するすべての統計情報および監視データは、さまざまなタイプの収集によって生成されます。収集はパケットのストリームに対して実行され、入力ストリームに基づいた出力が作成されます。ほとんどの場合、収集は RMON または SMON などの MIB テーブルと直接対応しています。

収集の定義の表（表 4-1）に、さまざまな収集タイプの定義を示します。

表 4-1　収集の定義

収集	定義	対応
ホスト	パケットのストリームを検査し、これらのパケットで確認されたすべてのネットワーク アドレスのテーブルを作成します（収集データとも言う）。エントリごとに、そのホストで送受信されたパケットとバイトの合計数、およびホストから送信された非ユニキャスト パケットの数が記録されます。	RMON2 nlHostTable（収集の実際の実装）
プロトコル	パケットのストリームを検査し、これらのパケットで確認されたすべてのプロトコルのテーブルを作成します。各エントリは、そのプロトコルで確認されたパケット数およびバイト数を示します。	RMON protocolDistStatsTable（収集の実際の実装）
キャプチャ	パケットのストリームを検査し、実際のパケット データのテーブルを作成します（captureBufferEntries）。各エントリには、パケットで確認されたデータの正確なコピーが含まれます。	RMON1 bufferTable、filterTable、および channelTable の各変数
音声（独自仕様）	パケットのストリームを検査し、IP テレフォニーに関するプロトコルのデータのテーブルを作成します。 • パケット ストリームで確認されたすべての IP 電話。 • パケット ストリームで確認された個別の通話。 • 各電話の統計情報（ジッタ、パケット損失など）および通話エントリを記録。 • 確認された最も品質が悪い通話（複数の特性によって判別）。	—

収集の実行対象となるパケットのストリームは、収集データ ソースと呼ばれます。これは、収集ごとに異なることがあります。収集で作成されるデータは、収集データと呼ばれます。

（注） 収集データは、通常、SNMP テーブル形式です（音声収集を除く）。

NAM は、異なる収集データ ソースで実行される、異なる収集の同時結合をサポートできます。

- 可能な同時収集の数は、CPU リソースおよびメモリ リソースによってのみ制限されます。
- 収集データ ソースは、SPAN ソースによって制限されます。SPAN ソースの詳細については、P.3-8 の「データ ソースのセットアップ」を参照してください。
- NAM 3.6 は、最大 1,500 のデータ ソースをサポートできます。

複数の収集の設定

複数の収集（ホスト、会話、プロトコル、ART、および音声）を NAM で同時に設定できます。収集は常に別のデータ ソースで設定されます。

各収集に関連付ける特定の収集データ ソースは、設定済みの SPAN/VACL トラフィック ストリームに直接対応しても、対応しなくてもかまいません。収集データ ソースの例として、次のものがあります。

- ポート /VLAN または送信元にかかわらず、すべての SPAN/VACL トラフィック ストリームのパケット（ALL SPAN）。
- 特定の VLAN（VLAN x）の SPAN/VACL トラフィック ストリームのすべてのパケット。
- 特定の NAM データ ポートに到達するように設定されたすべての SPAN/VACL トラフィック ストリームのパケット (DATA PORT 1 または DATA PORT 2)。
- ローカル Supervisor エンジン モジュールまたはその他のリモート NDE ソース（リモート ルータなど）から NAM が受信した NetFlow データ エクスポート（NDE）レコード（NAM-1 と NAM-2 だけで使用可能）。
- NAM が受信したスイッチ エンジン モジュール（Supervisor）レコード。ポート統計情報、VLAN 統計情報、および NBAR 統計情報を任意に組み合せて選択できます（NAM-1 と NAM-2 だけで使用可能）。
- NAM が受信したルータ エンジン モジュール レコード（Router）。インターフェイス統計情報および NBAR 統計情報を任意に組み合せて選択できます（NM-NAM だけで使用可能）。

（注） データ ソースは、すべての Monitor ウィンドウ間で持続します。たとえば、データ ソースとして VLAN2 を選択してから別の Monitor ウィンドウに移動しても、VLAN2 がその収集用に設定されていれば、そのウィンドウに表示されます。前に選択したデータ ソースが新しい Monitor ウィンドウで収集用に設定されていない場合は、NAM によってそのウィンドウのデフォルト データ ソースが表示されます。

それぞれの収集インスタンスは、設定されたデータ ソースに対応するトラフィック ストリームのパケットのみを処理します。たとえば、データ ソースに VLAN 12 が設定されたホスト収集には、受信 NDE フロー レコードは読み込まれません。VLAN 12 のタグが付いていない SPAN/VACL トラフィック ストリームのパケットも読み込まれません。

同様に、リモート ルータからの NDE レコードを指定するデータ ソースが設定された会話収集には、SPAN/VACL トラフィック ストリームで到達するパケットは読み込まれません。

シナリオ

VLAN 1、2、3 を含むように SPAN/VACL トラフィック ストリーム ソースを構成したとします。次に、この 3 つの VLAN 内のアプリケーション プロトコルごとに監視対象のパケット数およびバイト数をカウントするアプリケーション収集を開始します。

この収集の収集データ ソースを指定する必要があります。データ ソースは VLAN 1、VLAN 2、または VLAN 3 です。

データ ソースを VLAN 2 として設定すると、収集は VLAN 2 で受信したパケットの統計情報を生成します。ただし、VLAN 10 を収集データ ソースとして指定した場合、VLAN 10 が有効な VLAN ID であっても収集にデータは読み込まれません。これは、VLAN 10 が SPAN/VACL トラフィック ストリームの一部として設定されていないためです。

(注)

SPAN/VACL トラフィック ストリームは、ローカル Supervisor エンジン モジュールの SPAN または VACL 設定の結果として、監視のために NAM へ送信されたすべてのトラフィックの集約合計を表します。SPAN/VACL トラフィック ストリームの他に、ローカル Supervisor モジュール、リモート スイッチ、またはリモート ルータから 1 つ以上の NDE トラフィック ストリームを受信することがあります。特定の収集インスタンス用に設定されたデータ ソースは、これらのトラフィック ストリームのいずれかに出現するトラフィックと対応している必要があります。対応していない場合、収集統計情報は読み込まれません。

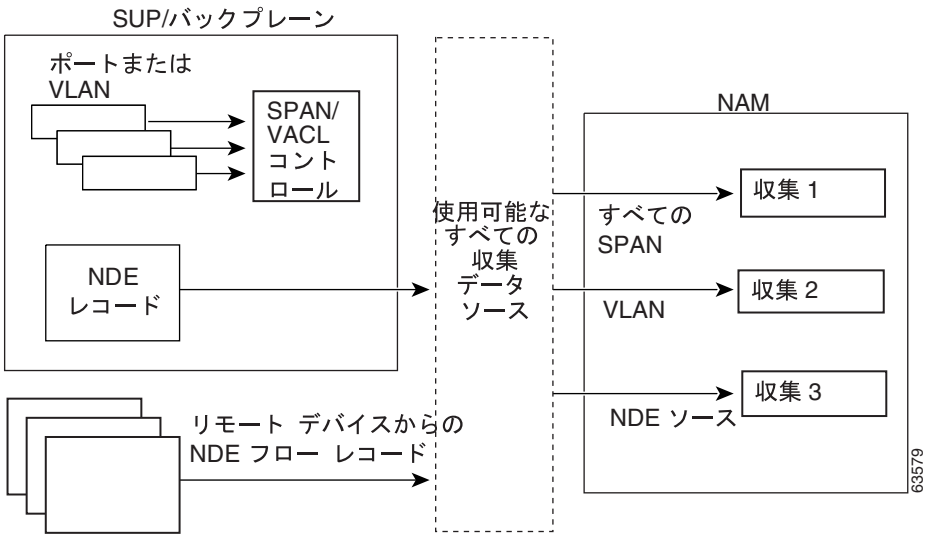
使用可能な収集データ ソースは、NAM ifTable（MIB-II）の ifEntry として表されます。収集データ ソースの表（表 4-2）に、有効な収集データ ソースを示します。

表 4-2　収集データ ソース

収集データ ソース	制限
すべての SPAN（SPAN/VACL トラフィック ストリームの集約）	SPAN または VACL トラフィック ソースが設定されていない場合、収集にデータは読み込まれません。
特定の VLAN ID	VLAN が SPAN/VACL トラフィック ストリームの一部として設定されていない場合、収集にデータは読み込まれません。
NDE データ ソース	NAM にレコードをエクスポートするデバイスでエクスポート パラメータを設定する必要があります。設定しないと、収集にデータは読み込まれません。監視は NAM 収集タイプのサブセットに制限されます。

SPAN、VACL、NDE トラフィック ストリームおよび収集データ ソースの図（図 4-1）に、SPAN および NDE データ ソースと収集データ ソース間の関係を示します。

図 4-1　SPAN、VACL、NDE トラフィック ストリームおよび収集データ ソース



NAM で設定した収集から、リアルタイム データを表示できます。NAM で収集を設定する方法については、P.6-3 の「キャプチャ設定の構成」を参照してください。

プロトコル自動検出

Traffic Analyzer は、最大 100 の不明なプロトコルを自動的に検出できます。プロトコルは親タイプおよび ID に従って表示されます。

自動検出されるプロトコルのタイプの表（表 4-3）に、自動的に検出できるプロトコルのタイプ、および表示方法の一覧を示します。

表 4-3　自動検出されるプロトコルのタイプ

プロトコル タイプ	表示方法
Ether2	ether2- *イーサタイプ番号*
SNAP	snap- *イーサタイプ番号*
IP	ip- *プロトコル タイプ番号*
TCP	tcp- *ポート番号*
UDP	udp- *ポート番号*
SUNRPC	sunrpc- *プログラム番号*

（注） 自動的に検出されたプロトコルは、NVRAM に保存されません。また、NAM をリブートしたときに失われます。自動検出されたプロトコルを保存するには、手動で Protocol Directory に入力します。詳細については、P.3-46 の「新しいプロトコルの作成」を参照してください。リブートせずに自動検出されたプロトコルをクリアするには、NAM CLI でコマンド no monitor protocol auto-learned と入力します。

NDE フロー マスクおよび V8 集約キャッシュ

デバイスで設定されたフロー マスクまたは集約によっては、NDE データ構造の一部のデータ フィールドが利用できないことがあります。その結果、一部のウィンドウには NetFlow データ ソースのデータが表示されなかったり、特定の条件が表示されたりします。フロー マスクおよび集約ウィンドウの条件の表（表 4-4）に、Monitor タブ下のウィンドウの表示条件と、その条件を引き起こすフローマスクまたは集約の一覧を示します。

表 4-4　フロー マスクおよび集約ウィンドウの条件

フロー マスクまたは集約キャッシュ	ウィンドウの条件
Full フロー マスク	すべてのウィンドウでサポートされます。
Destination only フロー マスク	• **Monitor** > **Apps** で「Others」だけが表示され、詳細ポップアップ ウィンドウにデータが表示されません。 • **Monitor** > **Hosts** で 0.0.0.0 が表示され、詳細ポップアップ ウィンドウにデータが表示されません。 • **Monitor** > **Conversations** で一部のホストの 0.0.0.0 が表示され、詳細ポップアップ ウィンドウにデータが表示されません。
Destination-Source フロー マスク	• **Monitor** > **Apps** で「Others」だけが表示され、詳細ポップアップ ウィンドウにデータが表示されません。 • **Monitor** > **Hosts** でデータが表示されますが、詳細ポップアップ ウィンドウには表示されません。 • **Monitor** > **Conversations** でデータが表示されますが、詳細ポップアップ ウィンドウには表示されません。

表 4-4　フロー マスクおよび集約ウィンドウの条件（続き）

フロー マスクまたは集約キャッシュ	ウィンドウの条件
V8-Protocol-Port-Aggregation	• **Monitor** > **Apps** でデータが表示されますが、詳細ポップアップ ウィンドウには 0.0.0.0 だけが表示されます。 • **Monitor** > **Host** で 0.0.0.0 だけが表示されます。 • **Monitor** > **Conversations** で 0.0.0.0 to 0.0.0.0 だけが表示されます。 • 特定のインターフェイス用に設定されたカスタム NetFlow データ ソースのデータがありません。 • TOS 0 および DSCP 0 以外の DiffServ がありません。 • **Setup** > **Data Sources** > **NetFlow Listening Mode** の詳細ポップアップ ウィンドウにインターフェイス情報が表示されません。
V8-Destination-Prefix-Aggregation	• **Monitor** > Apps で「Others」だけが表示されます。 • **Monitor** > Host でサブネットのデータおよび 0.0.0.0 が表示されます。詳細ポップアップ ウィンドウにデータが表示されません。 • **Monitor** > Conversations で 0.0.0.0 からサブネットのデータおよび 0.0.0.0 to 0.0.0.0 が表示されます。詳細ポップアップ ウィンドウにデータが表示されません。 • TOS 0 および DSCP 0 以外の DiffServ がありません。 • 特定のインターフェイス用に設定されたカスタム NetFlow データ ソースがサポートされます。
V8-Prefix-Aggregation	• **Monitor** > **Apps** で「Others」だけが表示されます。 • **Monitor** > **Host** でサブネットのデータおよび 0.0.0.0 が表示されます。詳細ポップアップ ウィンドウにデータが表示されません。 • **Monitor** > **Conversations** で、データおよび 0.0.0.0 to 0.0.0.0 が表示されます。詳細ポップアップ ウィンドウにデータが表示されません。 • TOS 0 および DSCP 0 以外の DiffServ がありません。 • 特定のインターフェイス用に設定されたカスタム NetFlow データ ソースがサポートされます。
V8-Source-Prefix-Aggregation	• **Monitor** > **Apps** で「Others」だけが表示されます。 • **Monitor** > **Host** でサブネットのデータおよび 0.0.0.0 が表示されます。詳細ポップアップ ウィンドウにデータが表示されません。 • **Monitor** > **Conversations** で、サブネットから 0.0.0.0 のデータおよび 0.0.0.0 to 0.0.0.0 が表示されます。詳細ポップアップ ウィンドウにデータが表示されません。 • TOS 0 および DSCP 0 以外の DiffServ がありません。 • 特定のインターフェイス用に設定されたカスタム NetFlow データ ソースがサポートされます。
V8-AS-Aggregation	サポートされません。

Monitor Overview チャートの表示

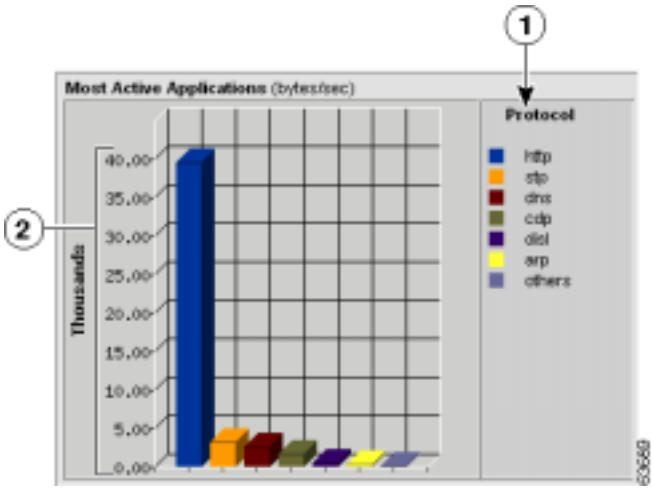
Monitor Overview チャートを使用すると、ネットワークで監視している TopN プロトコル スイート、アクティブ ホスト、アクティブ アプリケーション、およびアプリケーション応答時間をグラフ形式ですばやく表示できます。Monitor Overview チャートを表示するには、Monitor タブをクリックします。

次のチャートが表示されます。

- Most Active Applications チャート（図 4-2）

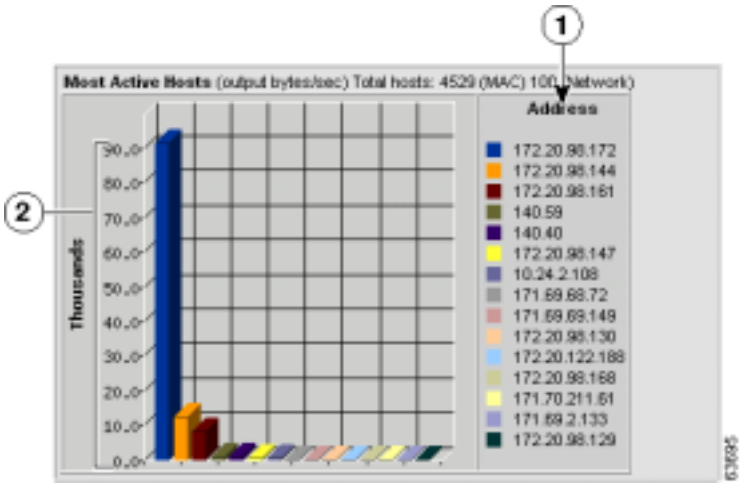
- Most Active Hosts チャート（図 4-3）
- Server Response Times チャート（図 4-4）
- Protocol Suites チャート（図 4-5）

図 4-2　Most Active Applications チャート



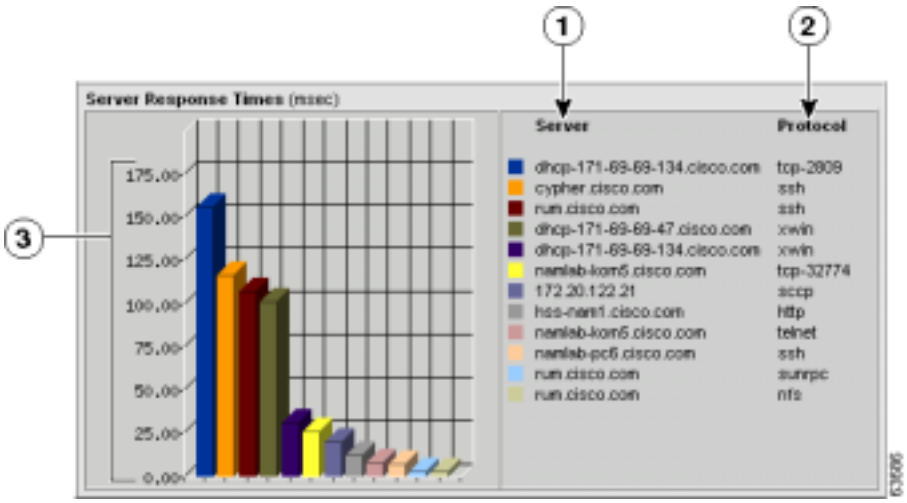
1	色別にソートされた TopN プロトコル	2	プロトコルごとの 1 秒あたりの収集バイト数

図 4-3　Most Active Hosts チャート



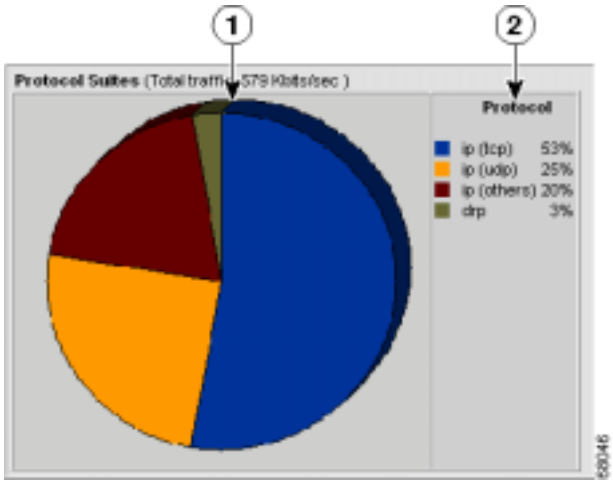
1	色別にソートされた TopN ネットワーク アドレス	2	アドレスごとの 1 秒あたりの収集バイト数

図 4-4　Server Response Times チャート



1	色別にソートされた TopN サーバ	3	サーバ応答時間
2	サーバが使用するプロトコル		

図 4-5　Protocol Suites チャート



1	ネットワーク プロトコルの使用状況を示す円グラフ	2	TopN ネットワーク プロトコル

データ ソースの持続性

ドロップダウン データ ソース リストを使用してモニタ ウィンドウを表示すると、NAM は選択されたデータ ソースを保存します。次にドロップダウン データ ソース リストを使用してモニタ ウィンドウを表示すると、NAM は前に保存したデータ ソースを表示します。前に表示および保存したデータ ソースがない場合、NAM はデフォルトのデータ ソースを表示します。別のモニタ ウィンドウに移動したときに、保存されたデータ ソースで収集が設定されていないと、デフォルトのデータ ソースが表示されます。

アプリケーション グループの表示

アプリケーション グループに基づいてパケットおよびバイトの分布を表示するには、Monitor タブをクリックしてから **Apps** をクリックし、Contents メニューから **Application Groups** を選択します。上部に 3 つのオプション ボタンがある Applications Group テーブルが表示されます。

次の用途に応じて、オプション ボタンを選択できます。

- Application Groups Current Rates テーブルの表示（P.4-9）
- Application Group TopN Chart の表示（P.4-11）
- Application Groups Cumulative Data テーブルの表示（P.4-12）

Application Groups Current Rates テーブルの表示

Application Groups Current Rates テーブルを使用して、アプリケーション グループごとに収集されたパケット数およびバイト数を表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数またはビット数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Application Groups Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　Current Rates table オプション ボタンをクリックします。

Application Groups Current Rates テーブル（表 4-5）が表示されます。

表 4-5　Application Groups Current Rates テーブル

フィールド	説明
Application Groups	アプリケーション グループの名前
Packets/s	収集された 1 秒あたりのパケット数
Bytes/s	収集された 1 秒あたりのバイト数
Bits/s	収集された 1 秒あたりのビット数

ステップ 2　Data Source リストから、監視するデータ ソースを選択します。

ステップ 3　特定のプロトコル グループのデータを表示するには、グループ名をテキスト ボックスに入力して、**Filter** をクリックします。

一致するすべてのグループが表示されます。

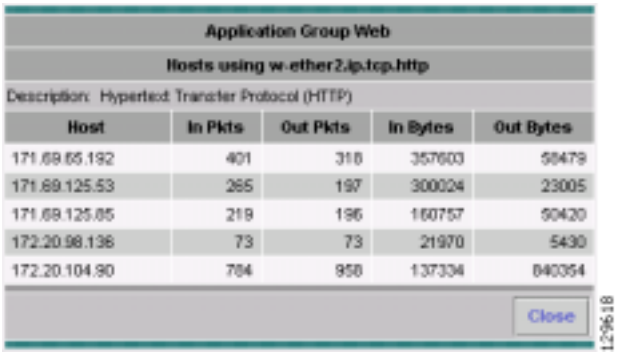
ヒント

- 特定のプロトコル グループのアプリケーション リストを表示するには、グループ名の前にあるプラス記号（+）をクリックします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

Application Group テーブルの詳細の表示

特定のアプリケーション グループの詳細を表示するには、アプリケーション グループを選択し、Details をクリックします。Application Group ウィンドウ（図 4-6）が表示され、そのグループのすべてのアプリケーション、およびそれらの特定のアプリケーションを使用するネットワーク ホストが表示されます。表示されるデータは、選択したデータ ソースに対して固有です。

図 4-6　Application Group ウィンドウ



Applications Group Detail ウィンドウには、表 4-6 に示されている情報が表示されます。

表 4-6　Application Group Detail ウィンドウのフィールド

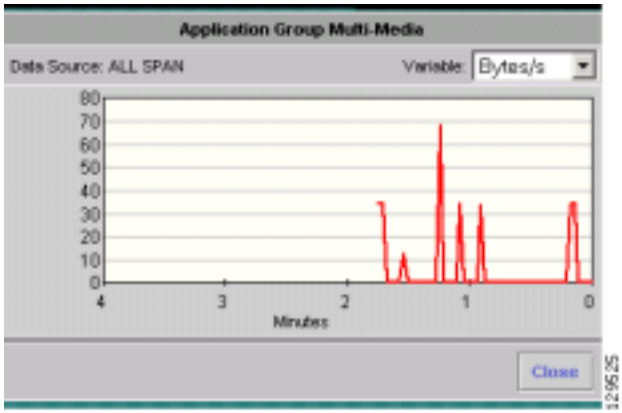
フィールド	説明
Description	そのグループの各アプリケーションの完全な名前と説明
Host	アプリケーション グループを使用しているコンピュータのホスト名
In Pkts	指定されたグループについてホストが受信したパケット数
Out Pkts	指定されたグループについてホストが送信したパケット数
In Bytes	指定されたグループについてホストが受信したバイト数
Out Bytes	指定されたグループについてホストが送信したバイト数

Application Group テーブルのリアルタイム データの表示

特定のアプリケーション プロトコルのリアルタイム データをグラフ形式で表示できます。

テーブルでプロトコルを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-7）が表示されます。

図 4-7　Real-Time グラフ



Application Group テーブルのレポートの表示

Applications テーブルから直接レポートを表示できます。レポートを表示するアプリケーション プロトコルを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートを設定していない場合は、選択したアプリケーションおよびデータ ソースに基づいて作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Application Group TopN Chart の表示

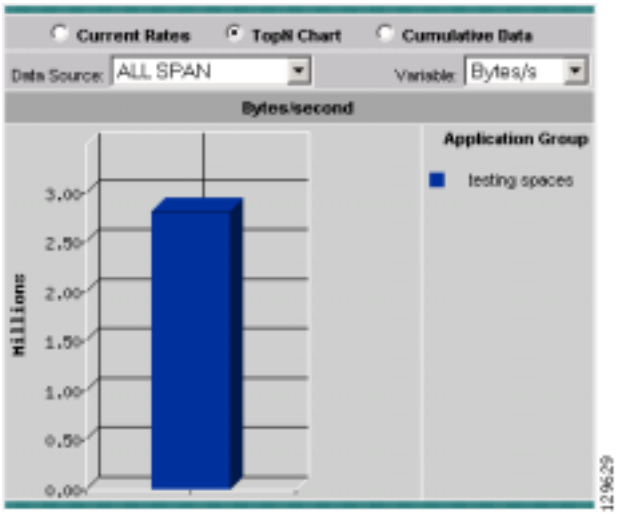
Applications TopN Chart を使用して、TopN アプリケーション プロトコルで収集されたパケット数およびバイト数をグラフ形式で表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Applications TopN Chart を表示するには、次の手順を実行します。

ステップ 1　TopN Chart オプション ボタンをクリックします。

Application Group TopN Chart（図 4-8）が表示されます。

図 4-8　Application Group TopN Chart



ステップ 2　Data Source リストから、監視するデータ ソースを選択します。

ステップ 3　Variable リストから、次のいずれかを選択します。

- Packets：監視される 1 秒あたりのパケット数が表示されます。
- Bytes：監視される 1 秒あたりのバイト数が表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、プロトコル名の上にカーソルを移動します。

Application Groups Cumulative Data テーブルの表示

Application Groups Cumulative Data テーブルを使用して、アプリケーション グループごとに収集されたパケット数およびバイト数を表示できます。表示されるデータは、収集が作成されてから、または NAM が再起動されてから収集されたパケットおよびバイトの合計数です。

Application Groups Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　Cumulative Data オプション ボタンをクリックします。

Application Group Cumulative Data テーブル（表 4-7）が表示されます。

表 4-7　Application Group Cumulative Data テーブル

フィールド	説明
Group Name	監視対象グループの名前
Packets	直前のインターバルで収集されたパケットの合計数
Bytes	直前のインターバルで収集されたバイトの合計数

ステップ 2　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 3　テーブルをリフレッシュするには、**Refresh** をクリックします。

ステップ 4　特定のグループのデータを表示するには、グループ名を Group テキスト ボックスに入力して、**Filter** をクリックします。

一致するすべてのグループが表示されます。

ヒント　合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

個別のアプリケーション データの表示

アプリケーション プロトコルに基づいてパケットおよびバイトの分布を表示するには、**Monitor** > **Apps** の順にクリックします。上部に 3 つのオプション ボタンがある Applications テーブルが表示されます。

次の用途に応じて、オプション ボタンを選択できます。

- Application Groups Current Rates テーブルの表示（P.4-9）
- Application Group TopN Chart の表示（P.4-11）
- Application Groups Cumulative Data テーブルの表示（P.4-12）

Applications Current Rates テーブルの表示

Applications Current Rates テーブルを使用して、アプリケーション プロトコルごとに収集されたパケット数およびバイト数を表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

（注） 自動認識されたプロトコルまたはユーザ定義のプロトコルはテーブルに表示されません。

Applications Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　Current Rates table オプション ボタンをクリックします。

Applications Current Rates テーブル（表 4-8）が表示されます。

表 4-8　Applications Current Rates テーブル

フィールド	説明
Protocol	アプリケーション プロトコルの名前
Packets/s	収集された 1 秒あたりのパケット数
Bytes/s	収集された 1 秒あたりのバイト数

ステップ 2　Data Source リストから、監視するデータ ソースを選択します。

ステップ 3　特定のプロトコルのデータを表示するには、プロトコル名を Protocol テキスト ボックスに入力して、**Filter** をクリックします。

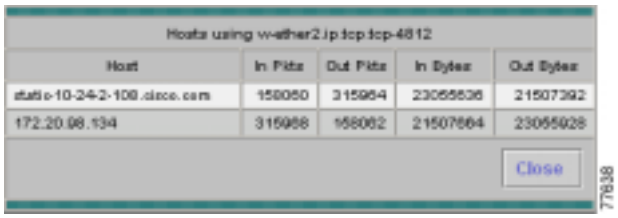
一致するすべてのプロトコルが表示されます。

ヒント
- 完全なプロトコル名を表示するには、Protocol Directory テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

Applications テーブルの詳細の表示

特定のアプリケーション プロトコルの詳細を表示するには、プロトコルを選択し、Details をクリックするか、Protocol カラムのプロトコル名をクリックします。Application Group ウィンドウ（図 4-6）が表示され、このプロトコルを使用するすべてのネットワーク ホストが表示されます。表示されるデータは、選択したデータ ソースに対して固有です。

図 4-9　Application Protocol Detail ウィンドウ



Applications Protocol Detail ウィンドウには、次の情報が表示されます。

表 4-9　Application Protocol Detail テーブル

フィールド	説明
Description	プロトコルの完全な名前と説明
Host	アプリケーション プロトコルを使用しているコンピュータのホスト名
In Pkts	指定されたプロトコルについてホストが受信したパケット数
Out Pkts	指定されたプロトコルについてホストが送信したパケット数
In Bytes	指定されたプロトコルについてホストが受信したバイト数
Out Bytes	指定されたプロトコルについてホストが送信したバイト数

Application テーブルのアプリケーション プロトコル データのキャプチャ

特定のアプリケーション プロトコルのデータを Application テーブルから直接キャプチャすることができます。

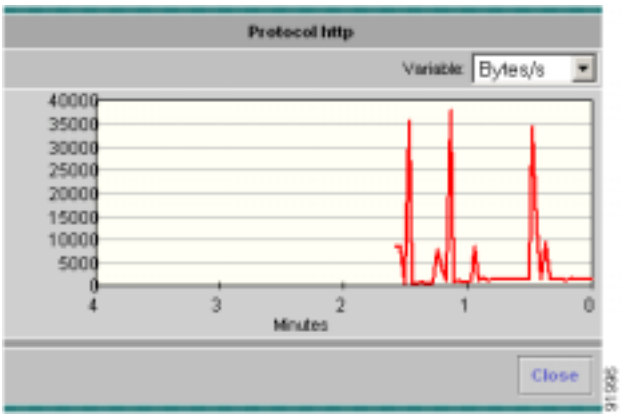
テーブルでプロトコルを選択して、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

キャプチャがすでに実行されている場合は、メッセージ ウィンドウが表示されます。**Yes** をクリックして現在のキャプチャを中止、または **No** をクリックして選択を取り消します。

Application テーブルのリアルタイム データの表示

特定のアプリケーション プロトコルのリアルタイム データをグラフ形式で表示できます。テーブルでプロトコルを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-10）が表示されます。

図 4-10　Real-Time グラフ



Applications テーブルのレポートの表示

Applications テーブルから直接レポートを表示できます。レポートを表示するアプリケーション プロトコルを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートを設定していない場合は、選択したアプリケーションおよびデータ ソースに基づいて作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Applications TopN Chart の表示

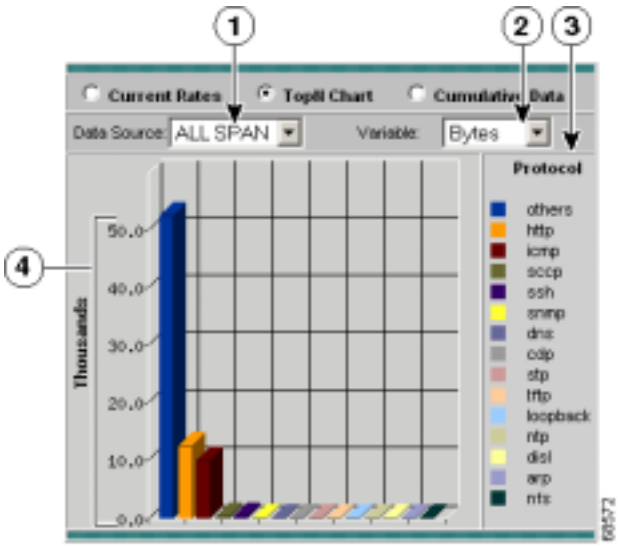
Applications TopN Chart を使用して、TopN アプリケーション プロトコルで収集されたパケット数およびバイト数をグラフ形式で表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Applications TopN Chart を表示するには、次の手順を実行します。

ステップ 1　TopN Chart オプション ボタンをクリックします。

Application Group TopN Chart（図 4-11）が表示されます。

図 4-11　Applications TopN Chart



1	データ ソース リスト	**3**	TopN アプリケーション プロトコル
2	変数リスト	**4**	TopN プロトコルごとの 1 秒あたりの収集されたバイト数またはパケット数

ステップ 2　Data Source リストから、監視するデータ ソースを選択します。

ステップ 3　Variable リストから、次のいずれかを選択します。

- Packets：監視される 1 秒あたりのパケット数が表示されます。
- Bytes：監視される 1 秒あたりのバイト数が表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、プロトコル名の上にカーソルを移動します。

Applications Cumulative Data テーブルの表示

Applications Cumulative Data テーブルを使用して、アプリケーション プロトコルごとに収集されたパケット数およびバイト数を表示できます。表示されるデータは、収集が作成されてから、または NAM が再起動されてから収集されたパケットおよびバイトの合計数です。

Applications Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　Cumulative Data オプション ボタンをクリックします。

Applications Cumulative Data テーブル（表 4-10）が表示されます。

表 4-10　Applications Cumulative Data テーブル

フィールド	説明
Protocol Name	監視対象プロトコルの名前
Packets	直前のインターバルで収集されたパケットの合計数
Bytes	直前のインターバルで収集されたバイトの合計数

ステップ 2　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 3　テーブルをリフレッシュするには、**Refresh** をクリックします。

ステップ 4　特定のプロトコルのデータを表示するには、プロトコル名を Protocol テキスト ボックスに入力して、**Filter** をクリックします。

一致するすべてのプロトコルが表示されます。

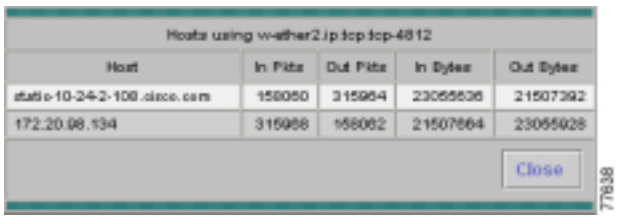
ヒント

- 完全なカプセル化されたプロトコル名を表示するには、Protocol Directory テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

Applications テーブルの詳細の表示

特定のアプリケーション プロトコルの詳細を表示するには、Protocol カラムのプロトコル名をクリックします。Protocol Detail ウィンドウ（図 4-12）が表示されます。

図 4-12　Protocol Detail ウィンドウ



Protocol Detail ウィンドウには、次の情報が表示されます。

表 4-11　Protocol Detail テーブル

フィールド	説明
Host	アプリケーション プロトコルを使用しているコンピュータのホスト名
In Pkts	指定されたプロトコルについてホストが受信したパケット数
Out Pkts	指定されたプロトコルについてホストが送信したパケット数
In Bytes	指定されたプロトコルについてホストが受信したバイト数
Out Bytes	指定されたプロトコルについてホストが送信したバイト数

収集された URL の表示

この項では、次のトピックについて取り上げます。

- 収集された URL の表示
- URL 収集リストのフィルタリング
- 収集された URL からの URL ベースのアプリケーションの作成

収集された URL の表示

収集された URL を表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **Apps** をクリックします。

ステップ 2　TOC で **URLs** をクリックします。

収集された URL を示す URLs ウィンドウ（図 4-13）が表示されます。

図 4-13　URLs ウィンドウ

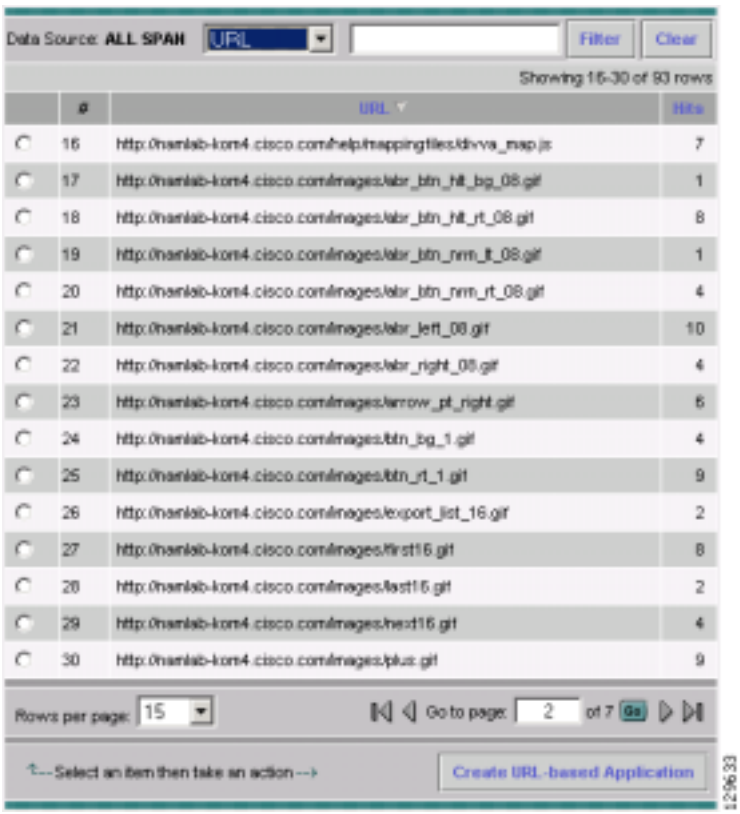


表 4-12　URLs テーブル

フィールド	説明
Index	URL インデックス
URL	URL の名前
Hits	ヒット数

(注)　一度にアクティブにできる URL 収集は 1 つだけです。データ ソースは、情報提供用です。

URL 収集リストのフィルタリング

URL 収集リストをフィルタリングするには、次の手順を実行します。

ステップ 1　URLs ウィンドウ（図 4-13）のドロップダウン リストから、フィルタリングする URL の部分を選択します。

- **URL**：URL の任意の部分をフィルタリングできます。
- **Host**：このフィルタは、収集された URL のホスト部分にだけ適用されます。
- **Path**：このフィルタは、収集された URL のパス部分にだけ適用されます。
- **Arguments**：このフィルタは、収集された URL の引数部分にだけ適用されます。

ステップ 2　フィルタ文字列を入力します。

ステップ 3　**Filter** をクリックし、フィルタを適用します。

(注)　表示フィルタを削除して、収集されたすべての URL を表示するには、**Clear** をクリックします。

収集された URL からの URL ベースのアプリケーションの作成

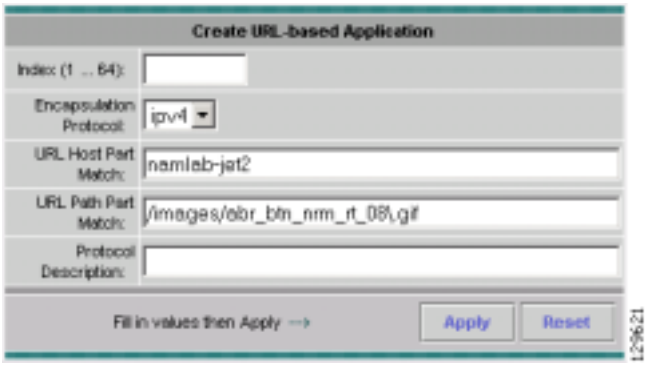
収集された URL から URL ベースのアプリケーションを作成するには、次の手順を実行します。

ステップ 1　Create URL-based Application ウィンドウの URL のリストで、オプション ボタンをクリックして URL リスト内の行を選択します。

ステップ 2　**Create URL-based Application** をクリックします。

Create URL-based Application ウィンドウ（図 4-14）が表示されます。

図 4-14　Create URL-based Application



ステップ 3　Index フィールドと Protocol Description フィールドに値を入力します。

Index フィールドと Protocol Description フィールドの適切な値については、P.3-52 の「URL ベースのアプリケーションの作成」を参照してください。

ステップ 4　**Apply** をクリックします。

音声データの表示

NAM Traffic Analyzer を使用して、NAM でイネーブルになっている音声プロトコルから収集したトラブルシューティング データを表示できます。データの表示により、音声ネットワークの潜在的な問題を識別できます。

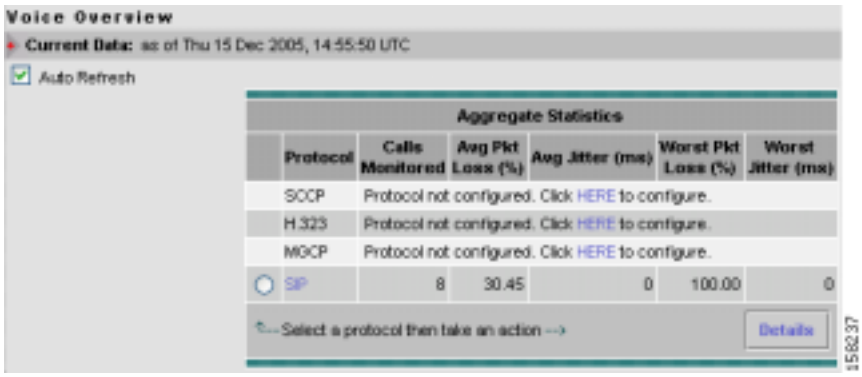
次のメニュー項目があります。

- 音声プロトコルの概要の表示（P.4-22）
- 既知の電話機の表示（P.4-24）
- アクティブ コールの表示（P.4-30）
- RTP ストリーム トラフィックの表示（P.4-31）

音声プロトコルの概要の表示

音声プロトコルの概要と Aggregate Statistics テーブルを表示するには、**Monitor** > **Voice/RTP Stream** を選択します。Aggregate Statistics テーブル（図 4-15）が表示されます。

図 4-15　Aggregate Statistics テーブル



Aggregate Statistics テーブル（表 4-13）には、ネットワークに実装された音声プロトコルの基本的なトラブルシューティング情報が含まれます。

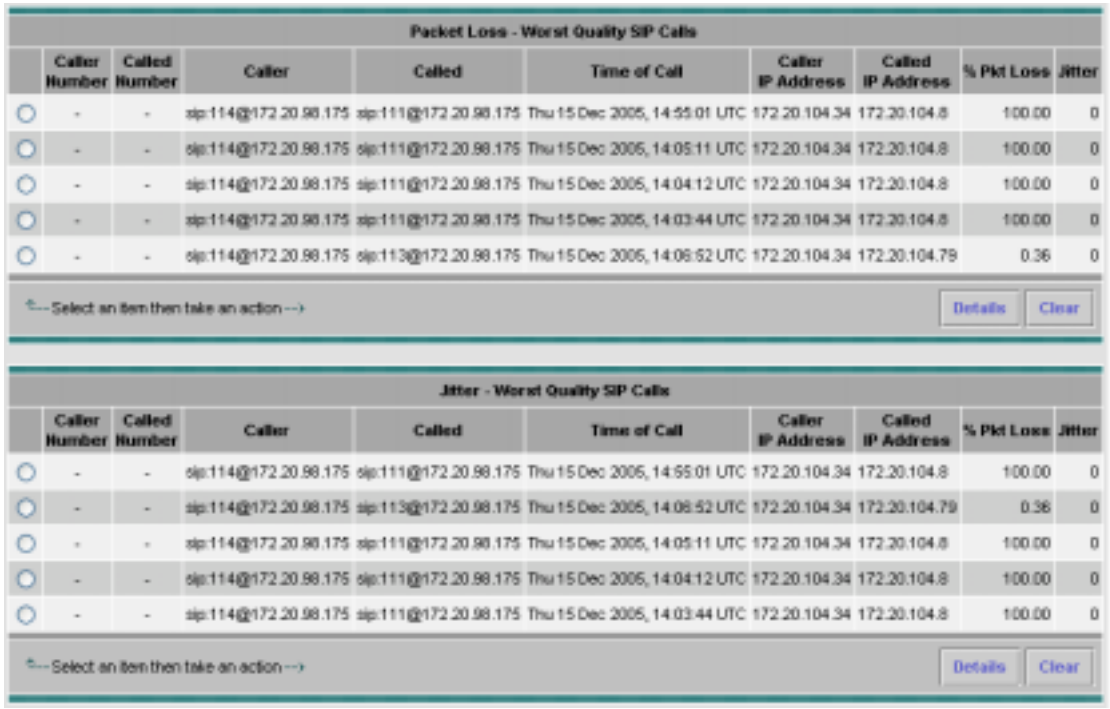
表 4-13　Aggregate Statistics テーブル

フィールド	説明
Protocol	音声プロトコルの名前（プロトコルには SCCP、H.323、MGCP、SIP が含まれる）
Calls Monitored	監視対象の通話の数
Avg Pkt Loss (%)	すべての通話に対する平均パケット損失
Avg Jitter (ms)	すべての通話に対する平均ジッタ
Worst Pkt Loss (%)	監視対象の最悪のパケット損失率
Worst Jitter (ms)	監視対象の最悪のジッタ

Aggregate Statistics テーブルのプロトコル詳細の表示

音声プロトコル詳細のウィンドウを表示するには、プロトコル名をオンにし、**Details** をクリックするか、プロトコル名をクリックします。Worst Quality Calls テーブル（図 4-16）が表示されます。

図 4-16　Worst Quality Calls テーブル



Worst Quality Calls テーブルには、次の 2 つのセクションがあります。

- **Packet Loss - Worst Quality Calls テーブル**：パケット損失に基づき、TopN 最悪通話が表示されます。
- **Jitter - Worst Quality Calls テーブル**：ジッタに基づき、TopN 最悪通話が表示されます。

テーブルの情報をクリアするには、**Clear** をクリックします。

表 4-14　Worst Quality Calls テーブル

フィールド	説明
Caller Number	発信者の電話番号
Called Number	着信者の電話番号
Caller	発信側電話機のエイリアス名、MGCP エンドポイント ID、または SIP URI
Called	着信側電話機のエイリアス名、MGCP エンドポイント ID、または SIP URI
Time of Call	通話が行われた時間
Caller IP Address	発信者の IP アドレス
Called IP Address	着信電話機の IP アドレス
% Packet Loss	通話でのパケット損失率
Jitter	通話でのジッタ量

既知の電話機の表示

ネットワークで監視しているすべての既知の電話機の基本情報および詳細情報を表示できます。

ネットワークで MGCP ゲートウェイを使用している場合、MGCP エンドポイントとエンドポイント ID は、指定された通話との接続を確立するために使用される MGCP ゲートウェイのポートを表しています。

既知の電話機を表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **Voice/RTP Stream** を選択します。

Aggregate Statistics テーブルが表示されます。

ステップ 2　コンテンツで **Known Phones** をクリックします。

Phones テーブル（表 4-15）が表示されます。

表 4-15　Phones テーブル

フィールド	説明
Phone	電話番号または MGCP エンドポイント
IP Address	電話機の IP アドレス
Name	電話機のエイリアス名または MGCP エンドポイント ID
Calls Monitored	監視対象の通話数および合計通話数に対する比率
Avg Pkt Loss %	電話機の平均パケット損失
Avg Jitter	電話機の平均ジッタ（ミリ秒単位）

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Known Phones テーブルの電話機詳細の表示

表 4-16　Phone Details テーブル

フィールド	説明
Phone	電話番号
Name	電話機のエイリアス名または MGCP エンドポイント ID
IP Address	電話機の IP アドレス
Switch Port	電話機が接続されている物理インターフェイス スイッチ ポート
Protocol	電話機が認識されるプロトコル

表 4-17　Aggregate Statistics テーブル

フィールド	説明
Calls Monitored	Call Monitoring を最後にイネーブルにしてから監視された通話数
Average Packet Loss (%)	すべての監視対象通話に対する平均パケット損失率
Average Jitter (msec)	すべての監視対象通話に対する平均ジッタ
Worst Packet Loss (%)	すべての監視対象通話に対する最悪パケット損失率
Worst Jitter (msec)	すべての監視対象通話に対する最悪ジッタ量

表 4-18　Last N Calls テーブル

フィールド	説明
Caller Number	発信者の電話番号
Called Number	着信電話機の電話番号
Caller	発信側電話機のエイリアス名、MGCP エンドポイント ID、または SIP URI
Called	着信側電話機のエイリアス名、MGCP エンドポイント ID、または SIP URI
Time of Call	通話が確立された時間
Caller IP Address	接続済み発信者の IP アドレス
Called IP Address	着信側の IP アドレス
% Pkt Loss	通話でのパケット損失率
Jitter (msec)	通話のジッタ SCCP、MGCP、および SIP の場合、電話機からジッタ値がレポートされます。H.323 の場合、検出されたすべての RTCP 受信者レポートの到着間隔ジッタの合計を、検出された RTCP 受信者レポートの数で割った、平均の到着間隔ジッタです。

Last N Calls テーブルの通話詳細の表示

Last N Calls テーブルから特定の通話の詳細を表示するには、オプション ボタンを選択して、**Details** をクリックします。

SCCP を使用している電話機の場合は、SCCP Call Detail テーブル（表 4-19）が表示されます。

H.323 を使用している電話機の場合は、H.323 Call Detail テーブル（表 4-20）が表示されます。

MGCP を使用している電話機の場合は、MGCP Call Detail テーブル（表 4-21）が表示されます。

SIP を使用している電話機の場合は、SIP Call Detail テーブル（表 4-22）が表示されます。

表 4-19　SCCP Call Detail テーブル

フィールド	説明
Phone Number	発信側および着信側の電話番号
Owner	発信側および着信側電話機のエイリアス名
IP Address	発信側および着信側の IP アドレス
Call Reference	通話確立メッセージのコール参照値フィールド
Call State	通話の現在の状態（Setup、Hold、Connected、Ended のいずれか）
Line Instance	通話の回線（line 1、line 2 など）

表 4-19　SCCP Call Detail テーブル（続き）

フィールド	説明
Receiving Audio Address	音声パケットの受信に使用する発信側および着信側電話機の IP アドレス
Receiving Audio Port	発信側と着信側で音声を受信するポート
Receiving Audio Codec	この通話で発信側および着信側電話機が使用する音声符号化方式
Receiving Audio Pass Through ID	この通話の有効な CCM 内部 ID
Receiving Video Address	ビデオ パケットの受信に使用する発信側および着信側電話機の IP アドレス
Receiving Video Port	発信側と着信側でビデオを受信するポート
Receiving Video Codec	この通話で発信側および着信側電話機が使用する符号化方式
Receiving Video Pass Through ID	この通話の有効な CCM 内部 ID
Receiving Data Address	データ パケットの受信に使用する発信側および着信側電話機の IP アドレス
Receiving Data Port	発信側と着信側でデータを受信するポート
Receiving Data Codec	この通話で発信側および着信側電話機が使用する符号化方式
Receiving Data Pass Through ID	この通話の有効な CCM 内部 ID
Start Time	通話が開始された曜日、日付および時刻
End Time	通話が終了した曜日、日付および時刻
Maximum Packet Loss	この通話の最大損失率
Maximum Jitter	この通話の最大ジッタ
Packets Sent	発信側および着信側電話機が報告した送信 RTP パケット数
Packets Received	発信側および着信側電話機が報告した受信 RTP パケット数
Octets Sent	発信側および着信側電話機が報告した送信 RTP オクテット数
Octets Received	発信側および着信側電話機が報告した受信 RTP オクテット数
Packet Loss (%)	報告された送信および受信パケットに基づく通話中のパケット損失率
Jitter (msec)	発信側および着信側電話機が報告した通話のジッタ
Switch Port	電話機が接続されているルータまたはスイッチ ポートの物理インターフェイス

表 4-20　H.323 Call Detail テーブル

フィールド	説明
Number	発信側および着信側の電話番号。
Q.931 IP Address	発信側の場合、Q.931 セットアップ メッセージのソース IP アドレス。着信側の場合、Q.931 接続メッセージのソース IP アドレス。
Q.931 Port	電話機が Q.931 メッセージの送信に使用しているポート。
Alias	発信側および着信側電話機のエイリアス名。
Call State	通話の状態：setup、connect、または ended。

表 4-20　H.323 Call Detail テーブル（続き）

フィールド	説明
Call Status	Good：ジッタとパケット損失がしきい値を超えていない。 Acceptable：ジッタまたはパケット損失あるいはその両方がしきい値を超えているが、超過分は値の 10% 以内。 Bad：ジッタまたはパケット損失あるいはその両方がしきい値の 10% を上回って超過。
Call Reference	通話確立メッセージのコール参照値フィールド。
Call Id	通話確立メッセージの通話 ID フィールド。
Conference Id	通話確立メッセージの会議 ID フィールド。
Conference Goal	発信者の会議アクション：Create、Invite、または Join。
Fast Start	true または false。通話がファーストスタート シーケンスを使用して通話を確立したかどうかを示す。
Tunneling	true または false。通話がメディア（RTP）チャネルを確立するときにトンネリングを使用したかどうかを示す。
Call Type	通話の種類：Point-to-Point、N-to-One、または One-to-N。
Product Id	通話確立メッセージに含まれる発信側および着信側の製品文字列。
Version Id	発信側および着信側の製品バージョン。
Session Id	発信側および着信側のメディア（RTP）チャネルのセッション番号。
Logical Channel Number	発信側および着信側のメディア（RTP）チャネルの論理チャネル番号値。
H.245 IP Address	発信側および着信側が通話のネゴシエーション時に H.245 メッセージを送信する IP アドレス。
H.245 Port	発信側および着信側が通話のネゴシエーション時に H.245 メッセージを送信するポート。
RTP IP Address	発信側および着信側が通話のネゴシエーション時に RTP パケットを送信する IP アドレス。
RTP Port	発信側および着信側が通話のネゴシエーション時に RTP パケットを送信するポート。
Codec	アナログ信号をデジタルに変換するために使用するエンコードまたはデコード方式。
RTCP IP Address	RTCP レポートの送信先 IP アドレス。
RTCP Port	RTCP レポートの送信先ポート。
Start Time	通話が開始された曜日、日付および時刻。
End Time	通話が終了した曜日、日付および時刻。
Synch Source	RTP パケットで発信側と着信側を表す同期ソース値。
Packets Sent	直前の RTCP 送信者レポートで報告された、通話で送信されたパケットの累積数。
Octets Sent	直前の RTCP 送信者レポートで報告された、通話で送信されたオクテットの累積数。
Packets Lost	直前の RTCP 送信者レポートで報告された、通話で損失したパケットの累積数。

表 4-20　H.323 Call Detail テーブル（続き）

フィールド	説明
Average Packet Loss (%)	検出された RTCP 受信者レポートで報告されたフラクション損失の合計を、検出された RTCP 受信者レポートの数で割った、平均フラクション損失。
Average Jitter (msec)	検出されたすべての RTCP 受信者レポート到着間隔ジッタの合計を、検出された RTCP 受信者レポートの数で割った、平均到着間隔ジッタ。

(注)　MGCP プロトコルの性質上、NAM が監視した通話には、発信側と着信側が逆になった情報が含まれる可能性があります。

表 4-21　MGCP Call Detail テーブル

フィールド	説明
Name	エイリアス名または MGCP エンドポイント ID。 (注)　この情報は、MGCP Call Detail テーブル上の別の Q.931 テーブルに表示されることがあります。
Phone Number	発信側および着信側の電話番号。 (注)　この情報は、MGCP Call Detail テーブル上の別の Q.931 テーブルに表示されることがあります。
Phone Number Confidence	プロトコルの性質上、エラーが検出される電話番号があります。 • High：電話番号の検出に誤りがある可能性があります。 • Low：MGCP プロトコルの性質上、電話番号の検出でエラーになることがあります。 (注)　この情報は、MGCP Call Detail テーブル上の別の Q.931 テーブルに表示されることがあります。
RTP Address	発信側および着信側の受信 RTP アドレス。
Endpoint ID	発信側および着信側の MGCP エンドポイント ID。
Agent Address	MGCP 通話エージェントの IP アドレス。
Gateway Address	MGCP ゲートウェイのネットワーク アドレス。
Call State	Setup：通話がセットアップされている。 Connected：通話が完全に確立されている。 Ended：通話が終了した。
Call Id	通話の MGCP 識別番号。
RTP Port	発信側および着信側の受信 RTP ポート。
Connection ID	通話の MGCP 接続識別番号。
RTP Sampling Period	転送のために RTP パケットをサンプリングする時間。

表 4-21　MGCP Call Detail テーブル（続き）

フィールド	説明
Silence Sup	On：通話がオンになっている場合の無音圧縮オプション。 Off：通話がオフになっている場合の無音圧縮オプション。
Codec	RTP ストリームのコーデック。
Start Time	通話が完全に確立された時間。
End Time	通話が終了した時間。
Packets Sent	MGCP 接続パラメータで報告され、発信側と着信側が送信した RTP パケットの数。
Packets Received	接続パラメータで報告され、発信側と着信側が受信した RTP パケットの数。
Octets Sent	MGCP 接続パラメータで報告され、発信側と着信側間で送信された RTP オクテットの数。
Octets Received	MGCP 接続パラメータで報告され、発信側と着信側間で受信された RTP オクテットの数。
Packet Loss (%)	MGCP 接続パラメータで報告され、パケット損失数に基づいて算出された損失率。
Jitter	MGCP 接続パラメータで報告された通話のジッタ。

表 4-22　SIP Call Detail テーブル

フィールド	説明
Name	SIP 電話機のエイリアス名。
Phone Number	SIP 電話機の電話番号。
IP Address	発信側および着信側の受信音声アドレス。
SIP URI	SIP 電話機の SIP URI を表す文字列。
Tag	通話シグナリング手順で使用される発信側および着信側のタグを表す文字列。
Call Id	通話シグナリング手順で使用される通話 ID を表す文字列。
Start Time	通話が確立された時間。
End Time	通話が終了した時間。
Session Owner	通話のグローバル SDP 所有者を表す文字列。
Session ID	通話のグローバル SDP ID を表す文字列。
Session Name	通話のグローバル SDP 名を表す文字列。
Receiving Audio Address	発信側および着信側が通話の音声パケットを受信するアドレス。
Receiving Audio Port	発信側および着信側が通話の音声パケットを受信するポート。
Audio Transport	通話の音声パケット形式。
Audio Payload	通話ネゴシエーション手順の SDP セッションで使用される音声コーデック。
Audio Packets Sent	電話機が報告した送信パケット数。
Audio Packets Received	電話機が報告した受信パケット数。
Audio Octets Sent	電話機が報告した送信オクテット数。
Audio Octets Received	電話機が報告した受信オクテット数。
Audio Packet Loss	電話機が報告した損失パケット数。

表 4-22　SIP Call Detail テーブル（続き）

フィールド	説明
Audio Jitter	電話機が報告したジッタ値。
Video Information	音声通話の場合は適用されない。
Application Information	音声通話の場合は適用されない。

(注)　通話がビデオまたはアプリケーション チャネルで行われた場合、SIP Call Detail テーブルには追加の行が表示されます。この行は、10 行ある *Audio* 行に似ていますが、Video または Application と名前が付けられます。

(注)　音声パケットまたはオクテットの送信、受信、損失、およびジッタは、SIP BYE と対応する BYE OK メッセージで取得されます。この情報は、シスコの SIP 電話機ファームウェア 6.3 以降で追加されますが、電話機の **Call Statistics** を Enabled に設定しておく必要があります。

アクティブ コールの表示

Active Calls テーブルには、現在監視されているすべての通話の情報が表示されます。

Active Calls テーブルを表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **Voice/RTP Stream** を選択します。

Aggregate Statistics テーブルが表示されます。

ステップ 2　コンテンツで **Active Calls** をクリックします。

Active Calls テーブル（表 4-23）が表示されます。

表 4-23　Active Calls テーブル

フィールド	説明
Caller Number	通話を発信した電話機の番号
Called Number	通話を受信した電話機の番号
Caller	発信側電話機のエイリアス名、MGCP エンドポイント ID、または SIP URI
Called	着信側電話機のエイリアス名、MGCP エンドポイント ID、または SIP URI
Time of Call	通話が行われた時間
Caller IP Address	通話を発信した電話機の IP アドレス
Called IP Address	通話を受信した電話機の IP アドレス

ステップ 3　Active Calls テーブルをクリアするには、**Clear** をクリックします。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Active Calls テーブルの通話詳細の表示

Active Calls テーブルから特定の通話の詳細を表示するには、Caller Number カラムで電話番号をクリックします。Active Call Detail ウィンドウが表示されます。

SCCP を使用している電話機の場合は、SCCP Call Detail テーブル（表 4-19）が表示されます。

H.323 を使用している電話機の場合は、H.323 Call Detail テーブル（表 4-20）が表示されます。

MGCP を使用している電話機の場合は、MGCP Call Detail テーブル（表 4-21）が表示されます。

SIP を使用している電話機の場合は、SIP Call Detail テーブル（表 4-22）が表示されます。

RTP ストリーム トラフィックの表示

RTP ストリーム トラフィックを表示するには、Content メニューで **Monitor** > **Voice/Video** を選択してから、**RTP Stream Traffic** を選択します。RTP Stream Traffic ウィンドウ（図 4-17）が表示されます。

図 4-17　RTP Stream Traffic ウィンドウ

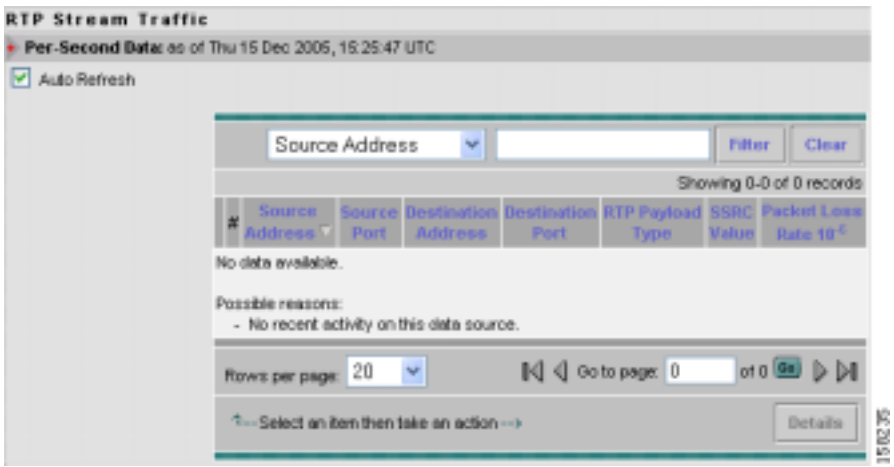


表 4-24 に、RTP Stream Traffic ウィンドウのフィールドを示します。

表 4-24　RTP Stream Traffic ウィンドウのフィールド

フィールド	説明
Source Address	RTP ストリーム トラフィックの送信元アドレス
Source Port	RTP ストリーム トラフィックの送信元ポート
Destination Address	RTP ストリーム トラフィックの宛先アドレス
Destination Port	RTP ストリーム トラフィックの宛先ポート
RTP Payload Type	RTP ストリーム内のペイロード タイプ
SSRC Value	RTP パケットの同期ソース
Packet Loss Rate 10^{-6}	実際のパケット損失率（見やすくするために 1,000,000 で除算）

ホスト データの監視

NAM の RMON1 および RMON2 ホスト テーブルにある、アクティブなホスト収集の結果を表示できます。

ホスト データを表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **Hosts** をクリックします。

上部に 3 つのオプション ボタンがある Network Hosts テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- Network Hosts Current Rates テーブルの表示（P.4-32）
- Network Hosts TopN Chart の表示（P.4-36）
- Network Hosts Cumulative Data テーブルの表示（P.4-37）

ステップ 2　ホストの MAC アドレスに基づいてデータを表示するには、コンテンツで **MAC Stations** をクリックします。

（注）　MAC 統計情報は、NM-NAM デバイスでは使用できません。

上部に 3 つのオプション ボタンがある Mac Stations テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- MAC Stations Current Rates テーブルの表示（P.4-37）
- MAC Stations TopN Chart の表示（P.4-38）
- MAC Stations Cumulative Data テーブルの表示（P.4-40）

Network Hosts Current Rates テーブルの表示

Network Hosts Current Rates テーブルを使用して、ホストごとに収集されたさまざまなデータを表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Network Hosts Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Network Hosts** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

Network Hosts Current Rates テーブル（表 4-25）が表示されます。

表 4-25　Network Hosts Current Rates テーブル

フィールド	説明
Address	ホストのネットワーク アドレス
Via	監視対象のプロトコル
In Packets/s	収集された 1 秒あたりの入力パケット数
Out Packets/s	収集された 1 秒あたりの出力パケット数
In Bytes/s	収集された 1 秒あたりの入力バイト数
Out Bytes/s	収集された 1 秒あたりの出力バイト数
Non Unicast/s	収集された 1 秒あたりの非ユニキャスト ブロードキャスト パケット数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　フィルタリングするアドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

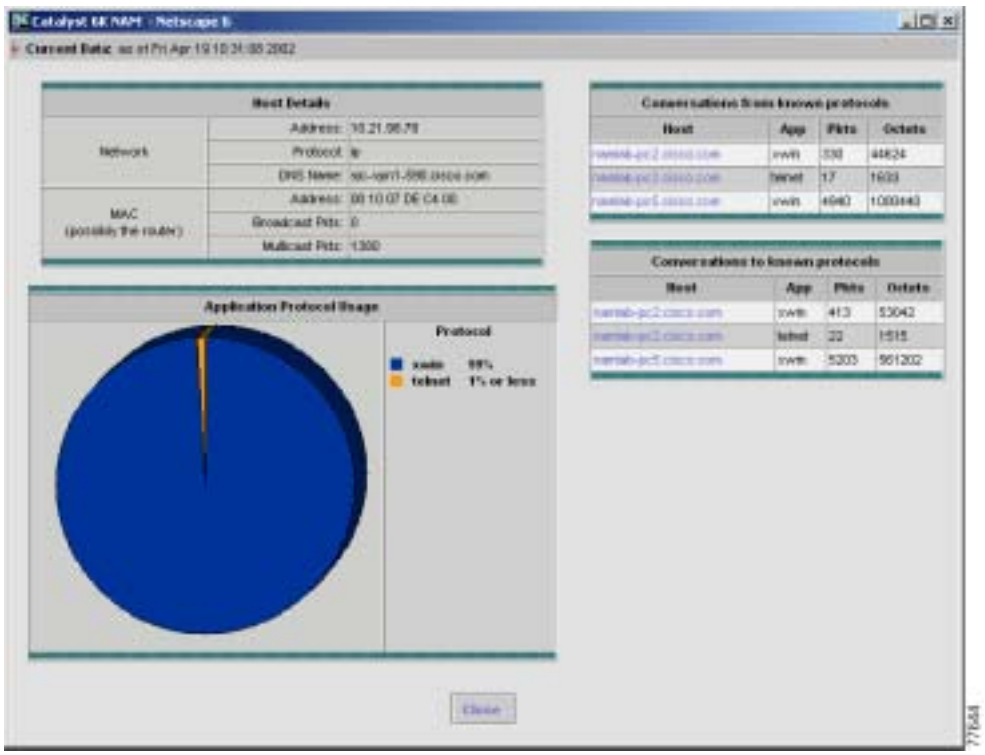
ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

ネットワーク ホストの詳細の表示

特定のホストの詳細を表示するには、Network Hosts テーブルの Address カラムでアドレスをクリックします。Network Hosts Detail ウィンドウ（図 4-18）が表示されます。

図 4-18　Network Hosts Detail ウィンドウ



- Host Details：ホストの詳細情報が表示されます。
- Application Protocol Usage チャート：ホストのアプリケーション プロトコル使用状況が、グラフ形式で表示されます。
- Conversations From Known Protocols：指定したホストから、既知のプロトコルを使用するネットワーク上の他のホストへの、既知の会話および統計情報が表示されます。
- Conversations To Known Protocols：既知のプロトコルを使用するネットワーク上の他のホストから、指定したホストへの、既知の会話および統計情報が表示されます。

(注)　完全なプロトコル名を表示するには、Application Protocol Usage チャートのプロトコル名の上にカーソルを移動します。

ヒント

完全なプロトコル名を表示するには、Application Protocol Usage チャートのプロトコル名の上にカーソルを移動します。

Network Host テーブルのネットワーク ホスト データのキャプチャ

特定のホストのデータを Network Host テーブルから直接キャプチャすることができます。

テーブルでホストを選択して、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

キャプチャがすでに実行されている場合は、メッセージ ウィンドウが表示されます。**Yes** をクリックして現在のキャプチャを中止、または **No** をクリックして選択を取り消します。

報告されたプロトコルのサブセットのみ、Capture ボタンが利用可能です。IP、IPv6 および GRE などのプロトコルの場合、カスタム フィルタを設定する必要があります。カスタム フィルタの設定の詳細については、P.6-21 の「カスタム キャプチャ フィルタの作成」を参照してください。

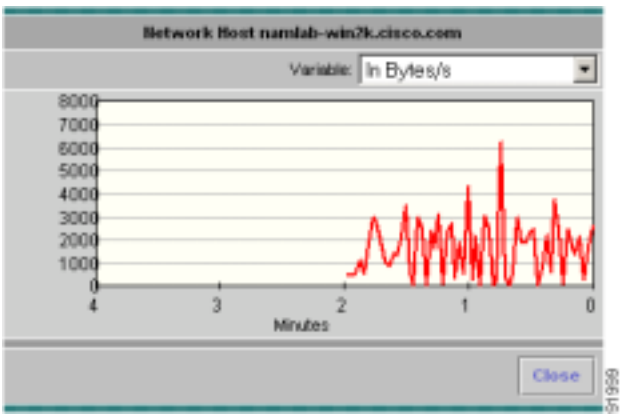
(注)　NetFlow ベースのデータ ソースには、Capture ボタンを使用できません。

Hosts テーブルのリアルタイム トラフィック統計情報の表示

特定のホストのリアルタイム トラフィック統計情報をグラフ形式で表示できます。テーブルでホストを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-19）が表示されます。

(注)　NetFlow ベースのデータ ソースには、Real-Time ボタンを使用できません。

図 4-19　Real-Time グラフ



Network Hosts テーブルのレポートの表示

Network Hosts テーブルから直接レポートを表示できます。レポートを表示するホストを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したホストおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Network Hosts TopN Chart の表示

Network Hosts TopN Chart を使用して、TopN ホストのさまざまなデータをグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

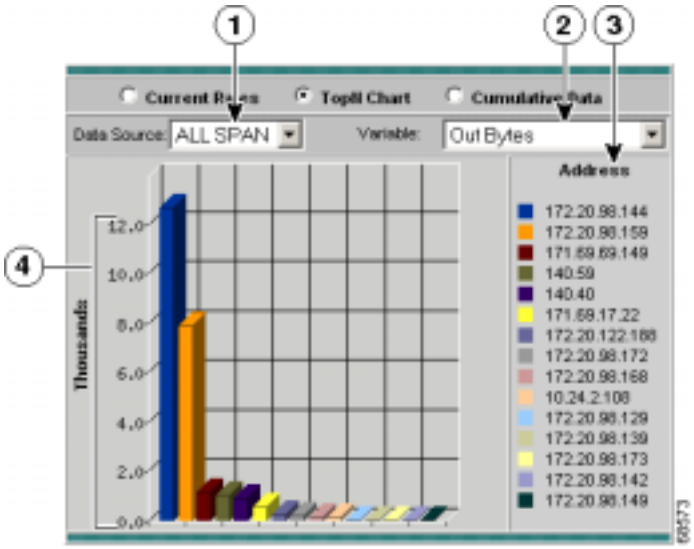
Network Hosts TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Network Hosts** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

Network Hosts TopN Chart（図 4-20）が表示されます。

図 4-20　Network Hosts TopN Chart



1	データ ソース リスト	3	TopN ネットワーク ホストのアドレス
2	変数リスト	4	TopN ホストごとの 1 秒あたりの入力 / 出力バイト数または入力 / 出力パケット数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　Sort Option リストから、次のいずれかを選択します。

- In Pkts：入力パケット数が表示されます。
- Out Pkts：出力パケット数が表示されます。
- In Bytes：入力バイト数が表示されます。
- Out Bytes：出力バイト数が表示されます。
- Non Unicast Pkts：非ユニキャスト パケット数が表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Network Hosts Cumulative Data テーブルの表示

Network Hosts Cumulative Data テーブルを使用して、ホストごとに収集されたさまざまなデータを表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。

Network Hosts Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Network Hosts** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

Network Hosts Cumulative Data テーブル（表 4-26）が表示されます。

表 4-26　Network Hosts Cumulative Data テーブル

フィールド	説明
Address	ホストのネットワーク アドレス
Via	監視対象のプロトコル
In Pkts	直前のインターバルでの入力パケット合計数
Out Pkts	直前のインターバルでの出力パケット合計数
In Bytes	直前のインターバルでの入力バイト合計数
Out Bytes	直前のインターバルでの出力バイト合計数
Non Unicast	直前のインターバルでの非ユニキャスト ブロードキャスト パケット合計数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　特定のアドレスのデータを表示するには、アドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

一致するすべてのアドレスが表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

MAC Stations Current Rates テーブルの表示

（注）　この項の内容は、NM-NAM デバイスには適用されません。

MAC Stations Current Rates テーブルを使用して、ホストごとに収集されたさまざまなデータを表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

MAC Stations Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **MAC Stations** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

MAC Stations Rates テーブル（表 4-27）が表示されます。

表 4-27　MAC Stations Rates テーブル

フィールド	説明
Address	ホストの MAC アドレス
In Packets/s	ホストが受信した 1 秒あたりのパケット数
Out Packets/s	ホストが送信した 1 秒あたりのパケット数
In Bytes/s	ホストが受信した 1 秒あたりのバイト数
Out Bytes/s	ホストが送信した 1 秒あたりのバイト数
Broadcasts/s	ホストが送信した 1 秒あたりのブロードキャスト数
Multicasts/s	ホストが送信した 1 秒あたりのマルチキャスト数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　フィルタリングするアドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

MAC Stations TopN Chart の表示

（注）　この項の内容は、NM-NAM デバイスには適用されません。

MAC Stations TopN Chart を使用して、ホストごとに収集されたさまざまなデータをグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

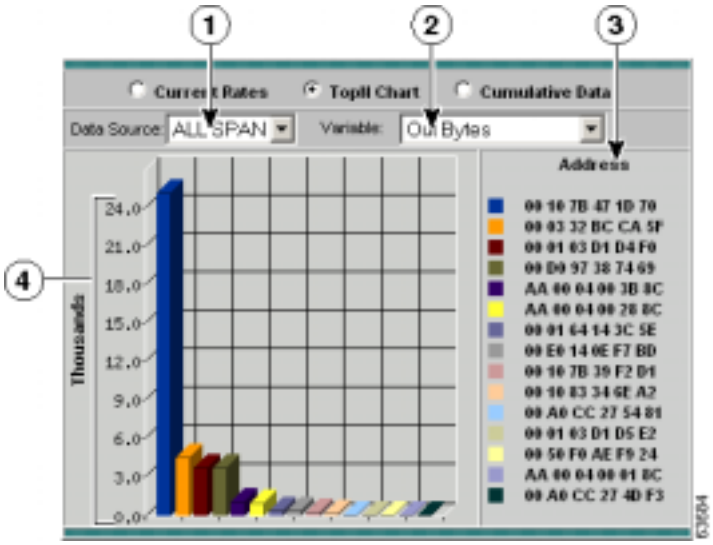
MAC Stations TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **MAC Stations** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

TopN MAC Stations Chart（図 4-21）が表示されます。

図 4-21　TopN MAC Stations Chart



1	データ ソース リスト	**3**	TopN MAC ホスト アドレス
2	変数リスト	**4**	TopN ホストごとの 1 秒あたりの入力 / 出力バイト数または入力 / 出力パケット数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　Sort Option リストから、次のいずれかを選択します。

- In Packets：1 秒あたりの入力パケット数が表示されます。
- Out Packets：1 秒あたりの出力パケット数が表示されます。
- In Bytes：1 秒あたりの入力バイト数が表示されます。
- Out Packets：1 秒あたりの出力バイト数が表示されます。
- Broadcast Packets：1 秒あたりのブロードキャスト パケット数に基づいてアドレスがソートされます。
- Multicast Packets：1 秒あたりのマルチキャスト パケット数に基づいてアドレスがソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

MAC Stations Cumulative Data テーブルの表示

(注)　この項の内容は、NM-NAM デバイスには適用されません。

MAC Stations Cumulative Data テーブルを使用して、ホストごとに収集されたさまざまなデータを表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。

MAC Stations Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **MAC Stations** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

MAC Stations Cumulative Data テーブル（表 4-28）が表示されます。

表 4-28　MAC Stations Cumulative Data テーブル

フィールド	説明
Address	ホストの MAC アドレス
In Packets	直前のインターバルでホストが受信したパケットの合計数
Out Packets	直前のインターバルでホストが送信したパケットの合計数
In Bytes	直前のインターバルでホストが受信したバイトの合計数
Out Bytes	直前のインターバルでホストが送信したバイトの合計数
Broadcasts	直前のインターバルでホストが送信したブロードキャストの合計数
Multicasts	ホストが送信したマルチキャストの合計数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　フィルタリングするアドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

ヒント
- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

会話データの表示

NAM で収集された会話データを表示できます。会話データは、2 つのホスト間で収集されたパケット数およびバイト数を表します。

会話データを表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **Conversations** をクリックします。

上部に 3 つのオプション ボタンがある Network Hosts Conversations テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- Network Host Conversations Current Rates テーブルの表示（P.4-41）
- Network Host Conversations TopN Chart の表示（P.4-44）
- Network Host Conversations Cumulative Data テーブルの表示（P.4-45）

ステップ 2　MAC アドレスに基づいて会話データを表示するには、コンテンツで **MAC Stations** をクリックします。

（注）　MAC 統計情報は、NM-NAM デバイスでは使用できません。

上部に 3 つのオプション ボタンがある MAC Station Conversations テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- MAC Station Conversations Current Rates テーブルの表示（P.4-46）
- MAC Station Conversations TopN Chart の表示（P.4-46）
- MAC Station Conversations Cumulative Data テーブルの表示（P.4-48）

Network Host Conversations Current Rates テーブルの表示

Network Host Conversations Current Rates テーブルを使用して、ホストの会話ごとに収集したパケット数およびバイト数を表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Network Host Conversations Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Network Hosts** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

Network Host Conversations Current Rates テーブル（表 4-29）が表示されます。

表 4-29　Network Host Conversations Current Rates テーブル

フィールド	説明
Source	会話の送信元アドレス
Via	ホストが会話をしているネットワーク層プロトコル
Destination	会話の宛先アドレス
Packets/s	直前のインターバルで収集された 1 秒あたりの会話のパケット数
Bytes/s	直前のインターバルで収集された 1 秒あたりの会話のバイト数

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　特定の送信元または宛先のデータを表示するには、リストから Source、Destination、または Source or Destination を選択します。

ステップ 5　アドレスをテキスト ボックスに入力して、**Filter** をクリックします。

一致するすべての送信元アドレスまたは宛先アドレスが表示されます。

ヒント
- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

ネットワーク ホスト会話の詳細の表示

特定のネットワーク会話の会話詳細を表示するには、Source カラムまたは Destination カラムでネットワーク アドレスをクリックします。次のテーブルが表示されます。

- Host Details：送信元ホストまたは宛先ホストの詳細情報が表示されます。
- Application Protocol Usage Chart：宛先ホストのソースのアプリケーション プロトコル使用状況が、グラフ形式で表示されます。
- Conversations From Known Protocols：指定したホストから、既知のプロトコルを使用するネットワーク上の他のホストへの、既知の会話および統計情報が表示されます。
- Conversations To Known Protocols：既知のプロトコルを使用するネットワーク上の他のホストから、指定したホストへの、既知の会話および統計情報が表示されます。

（注）　完全なプロトコル名を表示するには、Application Protocol Usage チャートのプロトコル名の上にカーソルを移動します。

Network Host Conversations テーブルからのネットワーク ホスト会話データのキャプチャ

特定のネットワーク ホストの会話データを Network Host Conversations テーブルから直接キャプチャすることができます。

テーブルで会話を選択して、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

キャプチャがすでに実行されている場合は、メッセージ ウィンドウが表示されます。**Yes** をクリックして現在のキャプチャを中止、または **No** をクリックして選択を取り消します。

報告されたプロトコルのサブセットのみ、Capture ボタンが利用可能です。IP、IPv6 および GRE などのプロトコルの場合、カスタム フィルタを設定する必要があります。カスタム フィルタの設定の詳細については、P.6-21 の「カスタム キャプチャ フィルタの作成」を参照してください。

(注)　NetFlow ベースのデータ ソースには、Capture ボタンを使用できません。

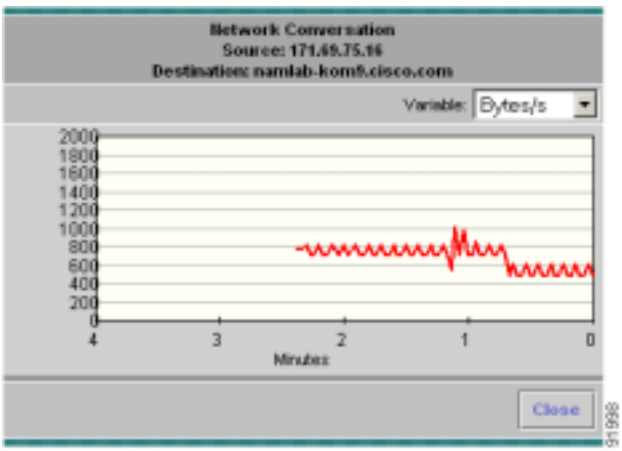
Network Host Conversations テーブルのリアルタイム トラフィック統計情報の表示

特定のホスト会話のリアルタイム トラフィック統計情報をグラフ形式で表示できます。

テーブルで会話を選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-22）が表示されます。

(注)　NetFlow ベースのデータ ソースには、Real-Time ボタンを使用できません。

図 4-22　Real-Time グラフ



Network Host Conversations テーブルのレポートの表示

Network Hosts Conversations テーブルから直接レポートを表示できます。レポートを表示する会話を選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したホストおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Network Host Conversations TopN Chart の表示

Network Host Conversations TopN Chart を使用して、TopN ネットワーク ホスト会話で収集されたパケット数とバイト数をグラフ形式で表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

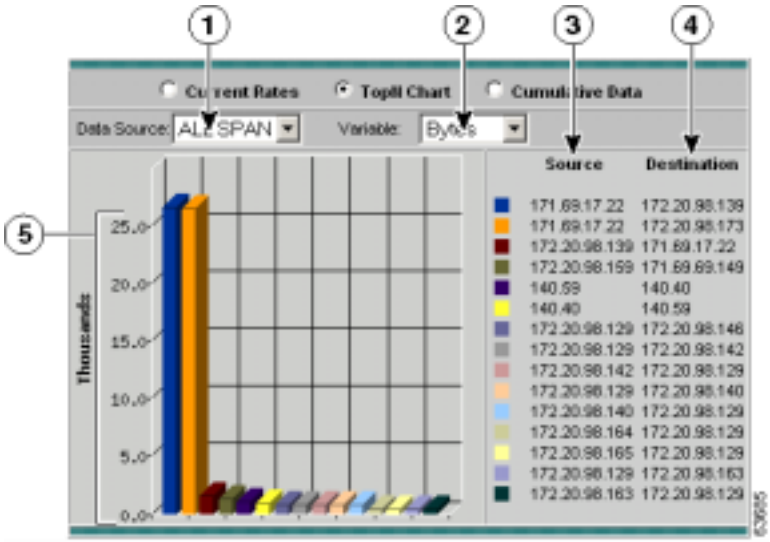
Network Host Conversations TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Network Hosts** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

Network Host Conversations TopN Chart（図 4-23）が表示されます。

図 4-23　Network Host Conversations TopN Chart



1	データ ソース リスト	4	TopN 宛先ネットワーク アドレス
2	変数リスト	5	収集された 1 秒あたりのパケット数またはバイト数
3	TopN 送信元ネットワーク アドレス		

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　Variable リストから、次のいずれかを選択します。

- Packets：パケット数に基づいてアドレスがソートされます。
- Bytes：バイト数に基づいてアドレスがソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Network Host Conversations Cumulative Data テーブルの表示

Network Host Conversations Cumulative Data テーブルを使用して、ホストの会話ごとに収集したパケット数およびバイト数を表示できます。表示されるデータは、収集が作成されてから、または NAM が再起動されてから収集されたパケットおよびバイトの合計数です。

Network Host Conversations Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Network Hosts** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

Network Host Conversations Cumulative Data テーブル（表 4-30）が表示されます。

表 4-30　Network Host Conversations Cumulative Data テーブル

フィールド	説明
Source	会話の送信元アドレス
Via	ホストが会話をしているネットワーク層プロトコル
Destination	会話の宛先アドレス
Packets	会話の直前のインターバルで収集されたパケットの合計数
Bytes	会話の直前のインターバルで収集されたバイトの合計数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　フィルタリングするアドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

ステップ 5　テーブルをリフレッシュするには、**Refresh** をクリックします。

ヒント　合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

ネットワーク ホスト会話の詳細の表示

特定のネットワーク会話の会話詳細を表示するには、Source カラムまたは Destination カラムでネットワーク アドレスをクリックします。次のテーブルが表示されます。

- Host Details：送信元ホストまたは宛先ホストの詳細情報が表示されます。
- Application Protocol Usage Chart：宛先ホストのソースのアプリケーション プロトコル使用状況が、グラフ形式で表示されます。
- Conversations From Known Protocols：指定したホストから、既知のプロトコルを使用するネットワーク上の他のホストへの、既知の会話および統計情報が表示されます。
- Conversations To Known Protocols：既知のプロトコルを使用するネットワーク上の他のホストから、指定したホストへの、既知の会話および統計情報が表示されます。

MAC Station Conversations Current Rates テーブルの表示

(注)　この項の内容は、NM-NAM デバイスには適用されません。

MAC Station Conversations Current Rates テーブルを使用して、ホストの会話ごとに収集したパケット数およびバイト数を表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

MAC Station Conversations Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **MAC Stations** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

MAC Station Conversations Current Rates テーブル（表 4-31）が表示されます。

表 4-31　MAC Station Conversations Current Rates テーブル

フィールド	説明
Source	会話の送信元 MAC アドレス
Destination	会話の宛先 MAC アドレス
Packets/s	直前のインターバルで収集された 1 秒あたりの会話のパケット数
Bytes/s	直前のインターバルで収集された 1 秒あたりの会話のバイト数
Errors/s	直前のインターバルで収集された 1 秒あたりの会話のエラー数

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　特定のアドレスのデータを表示するには、MAC アドレスの全体または一部を Address テキスト ボックスに入力して、**Filter** をクリックします。

一致するすべてのアドレスが表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

MAC Station Conversations TopN Chart の表示

(注)　この項の内容は、NM-NAM デバイスには適用されません。

MAC Station Conversations TopN Chart を使用して、TopN MAC ステーション会話で収集されたパケット数およびバイト数をグラフ形式で表示できます。表示されるデータは、直前のインターバルで収集された 1 秒あたりのパケット数およびバイト数です。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

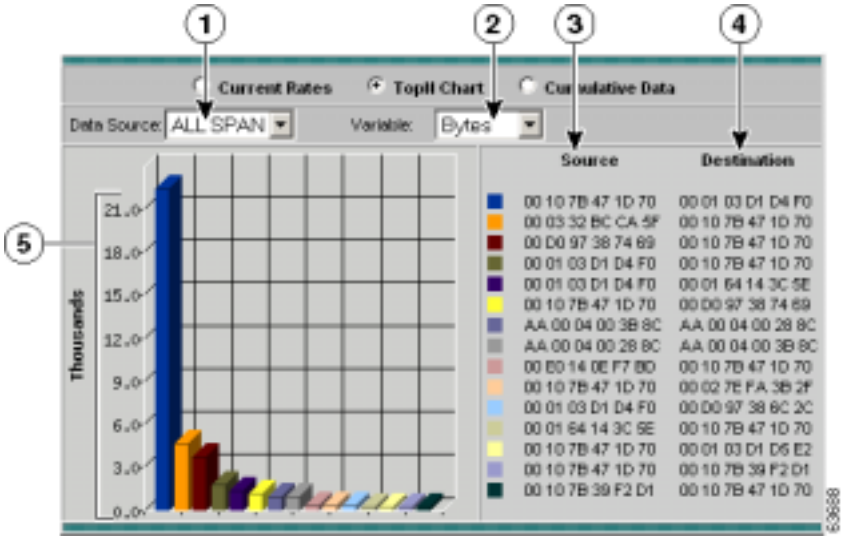
MAC Station Conversations TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **MAC Stations** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

MAC Station Conversations TopN Chart（図 4-24）が表示されます。

図 4-24　MAC Station Conversations TopN Chart



1	データ ソース リスト	**4**	TopN 宛先 MAC アドレス
2	変数リスト	**5**	収集された 1 秒あたりのパケット数、バイト数、またはエラー数
3	TopN 送信元 MAC アドレス		

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　Variable リストから、次のいずれかを選択します。

- Packets：パケット数が表示されます。
- Bytes：バイト数が表示されます。
- Errors：エラー数が表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

MAC Station Conversations Cumulative Data テーブルの表示

(注)　この項の内容は、NM-NAM デバイスには適用されません。

MAC Station Conversations Cumulative Data テーブルを使用して、MAC ステーションの会話ごとに収集したパケット数およびバイト数を表示できます。表示されるデータは、収集が作成されてから、または NAM が再起動されてから収集されたパケットおよびバイトの合計数です。

MAC Station Conversations Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **MAC Stations** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

MAC Station Conversations Cumulative Data テーブル（表 4-32）が表示されます。

表 4-32　MAC Station Conversations Cumulative Data テーブル

フィールド	説明
Source	会話の送信元 MAC アドレス
Destination	会話の宛先 MAC アドレス
Pkts	会話の直前のインターバルで収集されたパケットの合計数
Bytes	会話の直前のインターバルで収集されたバイトの合計数
Errors	会話の直前のインターバルで収集されたエラーの合計数

ステップ 3　Data Source リストから、データ ソースを選択します。

ステップ 4　フィルタリングするアドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

ステップ 5　テーブルをリフレッシュするには、**Refresh** をクリックします。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

VLAN データの表示

(注)　この項の内容は、NM-NAM デバイスには適用されません。

NAM で収集された VLAN トラフィック統計情報または VLAN プライオリティ（COS）統計情報を表示できます。Supervisor エンジン モジュール収集は、NAM の収集から独立して行われます。

(注)　Supervisor エンジン モジュールベースの収集には、スイッチに Supervisor II エンジン モジュール以降が必要です。

VLAN データを表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **VLAN** をクリックします。

上部に 3 つのオプション ボタンがある VLAN Traffic Statistics テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- VLAN Traffic Statistics Current Rates テーブルの表示（P.4-49）
- VLAN Traffic Statistics TopN Chart の表示（P.4-50）
- VLAN Traffic Statistics Cumulative Data テーブルの表示（P.4-51）

ステップ 2　VLAN プライオリティ（COS）統計情報に基づいて VLAN データを表示するには、コンテンツで **VLAN Priority (COS) Statistics** をクリックします。

上部に 3 つのオプション ボタンがある VLAN Priority (COS) Statistics テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- VLAN Priority (COS) Statistics Current Rates テーブルの表示（P.4-52）
- VLAN Priority (COS) Statistics TopN Chart の表示（P.4-53）
- VLAN Priority (COS) Statistics Cumulative Data テーブルの表示（P.4-54）

VLAN Traffic Statistics Current Rates テーブルの表示

(注)　この項の内容は、NM-NAM デバイスには適用されません。

VLAN Traffic Statistics Current Rates テーブルを使用して、VLAN ID ごとに収集されたさまざまなデータを表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

VLAN Traffic Statistics Current Rates テーブルを表示するには、Current Rates オプション ボタンをクリックします。

VLAN Traffic Statistics Current Rates テーブル（表 4-33）が表示されます。

表 4-33　VLAN Traffic Statistics Current Rates テーブル

フィールド	説明
VLAN ID	VLAN ID 番号
Packets/s	直前のインターバルで収集された 1 秒あたりのパケット数
Bytes/s	直前のインターバルで収集された 1 秒あたりのバイト数
Non-Unicast Packets/s	直前のインターバルで収集された 1 秒あたりの非ユニキャスト パケット数
Non-Unicast Bytes/s	直前のインターバルで収集された 1 秒あたりの非ユニキャスト バイト数

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

VLAN Traffic Statistics Current Rates テーブルのレポートの表示

VLAN Traffic Statistics Current Rates テーブルから直接レポートを表示できます。レポートを表示する VLAN ID を選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択した VLAN およびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

VLAN Traffic Statistics TopN Chart の表示

（注） この項の内容は、NM-NAM デバイスには適用されません。

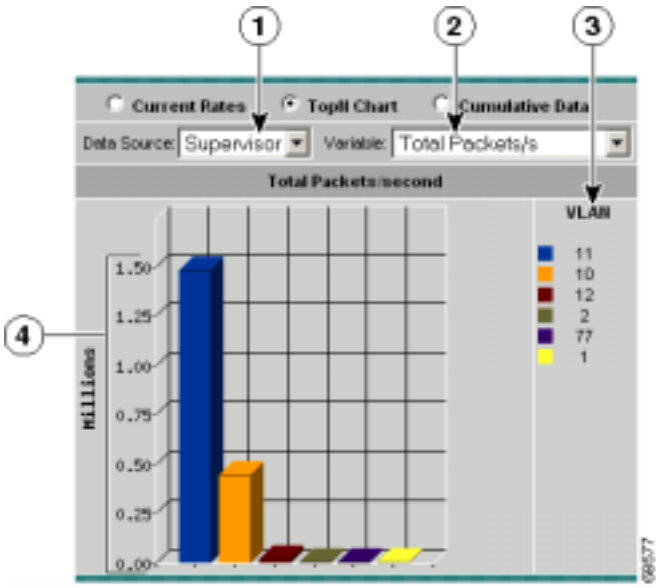
VLAN Traffic Statistics TopN Chart を使用して、TopN VLAN ID ごとに収集されたさまざまなデータをグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

VLAN Traffic Statistics TopN Chart を表示するには、次の手順を実行します。

ステップ 1　TopN Chart オプション ボタンをクリックします。

VLAN Traffic Statistics TopN Chart（図 4-25）が表示されます。

図 4-25　VLAN Traffic Statistics TopN Chart



1	データ ソース リスト	**3**	TopN VLAN ID
2	変数リスト	**4**	収集された 1 秒あたりのパケット数またはバイト数

ステップ 2　Data Source リストから、データ ソースを選択します。

ステップ 3　Variable リストから、次のいずれかを選択します。

- Total Packets：パケットの合計数が表示されます。
- Total Bytes：バイトの合計数が表示されます。
- Non-unicast Packets：非ユニキャスト パケット数が表示されます。
- Non-unicast Bytes：非ユニキャスト バイト数が表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

VLAN Traffic Statistics Cumulative Data テーブルの表示

（注）　この項の内容は、NM-NAM デバイスには適用されません。

VLAN Traffic Statistics Cumulative Data テーブルを使用して、VLAN ID ごとに収集されたさまざまなデータを表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。

VLAN Traffic Statistics Cumulative Data テーブルを表示するには、Cumulative Data オプション ボタンをクリックします。

VLAN Traffic Statistics Cumulative Data テーブル（表 4-34）が表示されます。

表 4-34　VLAN Traffic Statistics Cumulative Data テーブル

フィールド	説明
VLAN ID	VLAN ID 番号
Packets	直前のインターバルで収集されたパケットの合計数
Bytes	直前のインターバルで収集されたバイトの合計数
Non-Unicast Packets	直前のインターバルで収集された非ユニキャストのパケットの合計数
Non-Unicast Bytes	直前のインターバルで収集された非ユニキャストのバイトの合計数

ヒント　合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

VLAN Priority (COS) Statistics Current Rates テーブルの表示

（注）　この項の内容は、NM-NAM デバイスには適用されません。

VLAN Priority (COS) Statistics Current Rates テーブルを使用して、データ ソースごとのユーザ プライオリティ分布を表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

VLAN Priority (COS) Statistics Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Priority (COS) Statistics** をクリックします。

VLAN Priority (COS) Statistics Current Rates テーブル（表 4-35）が表示されます。

表 4-35　VLAN Priority (COS) Statistics Current Rates テーブル

フィールド	説明
Priority	Tag Control Information フィールドでエンコードされた 3 ビットのユーザ プライオリティ フィールドの値。
Packets/s	このプライオリティ レベルで収集されたパケット数。データは、直前のインターバルの 1 秒あたりのレートです。
Bytes/s	このプライオリティ レベルで収集されたバイト数。データは、直前のインターバルの 1 秒あたりのレートです。

ステップ 2　Data Source リストから、監視するデータ ソースを選択します。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

VLAN Priority (COS) Statistics TopN Chart の表示

（注） この項の内容は、NM-NAM デバイスには適用されません。

VLAN Priority (COS) Statistics TopN Chart を使用して、データ ソースごとのユーザ プライオリティ分布をグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

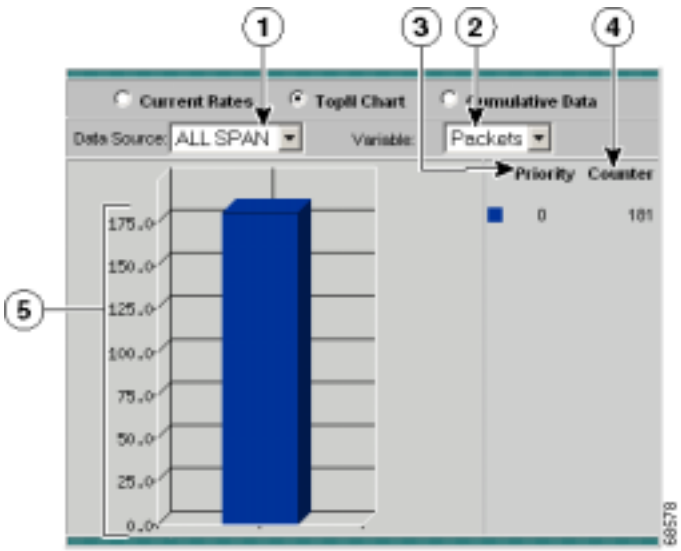
VLAN Priority (COS) Statistics TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Priority (COS) Statistics** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

VLAN Priorities (COS) Statistics TopN Chart（図 4-26）が表示されます。

図 4-26　VLAN Priorities (COS) Statistics TopN Chart



1	データ ソース リスト	4	VLAN カウンタ
2	変数リスト	5	収集された 1 秒あたりのパケット数またはバイト数
3	TopN VLAN のプライオリティ		

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　Variable リストから、次のいずれかを選択します。

- Packets：パケット数が表示されます。
- Bytes：バイト数が表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

VLAN Priority (COS) Statistics Cumulative Data テーブルの表示

（注）　この項の内容は、NM-NAM デバイスには適用されません。

VLAN Priority (COS) Statistics Cumulative Data テーブルを使用して、データ ソースごとのユーザ プライオリティ分布を表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

VLAN Priority (COS) Statistics Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Priority (COS) Statistics** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

VLAN Priority (COS) Statistics Cumulative Data テーブル（表 4-36）が表示されます。

表 4-36　VLAN Priority (COS) Statistics Cumulative Data テーブル

フィールド	説明
Priority	Tag Control Information フィールドでエンコードされた 3 ビットのユーザ プライオリティ フィールドの値
Packets	このプライオリティ レベルで収集されたパケットの合計数
Bytes	このプライオリティ レベルで収集されたバイトの合計数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ヒント　合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

DiffServ データの表示

NAM で収集された Differentiated Services（DiffServ）データに基づいて、パケットおよびバイトの分布を表示できます。

(注) DiffServ データは、ローカル NetFlow デバイスでは使用できません。これは、WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスに適用できます。

DiffServ データを表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **DiffServ** をクリックします。

上部に 3 つのオプション ボタンがある DiffServ Traffic Statistics テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- DiffServ Traffic Statistics Current Rates テーブルの表示（P.4-55）
- DiffServ Traffic TopN Chart の表示（P.4-57）
- DiffServ Traffic Statistics Cumulative Data テーブルの表示（P.4-58）

ステップ 2　アプリケーション統計情報に基づいて DiffServ データを表示するには、コンテンツで **Application Stats** をクリックします。

上部に 3 つのオプション ボタンがある DiffServ Applications Statistics テーブルが表示されます。次の用途に応じて、オプション ボタンを選択できます。

- DiffServ Application Statistics Current Rates テーブルの表示（P.4-58）
- DiffServ Application Statistics TopN Chart の表示
- DiffServ Application Statistics Cumulative Data テーブルの表示（P.4-61）

ステップ 3　ホスト統計情報に基づいて DiffServ データを表示するには、コンテンツで **Host Stats** をクリックします。

上部に 3 つのオプション ボタンがある DiffServ Host Statistics テーブルが表示されます。

次の用途に応じて、オプション ボタンを選択できます。

- DiffServ Host Statistics Current Rates テーブルの表示（P.4-62）
- DiffServ Host Statistics TopN Chart の表示（P.4-64）
- DiffServ Host Statistics Cumulative Data テーブルの表示（P.4-65）

DiffServ Traffic Statistics Current Rates テーブルの表示

DiffServ Traffic Statistics Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Traffic Stats** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

DiffServ Traffic Statistics Current Rates テーブル（表 4-37）が表示されます。

表 4-37　DiffServ Traffic Statistics Current Rates テーブル

フィールド	説明
Aggregation Group	集約グループの名前
Packets/s	直前のインターバルで収集された 1 秒あたりの合計パケット
Bytes/s	直前のインターバルで収集された 1 秒あたりの合計バイト

ステップ 3　Data Source-Profile リストから、監視するデータ ソースおよびプロファイルを選択します。

ステップ 4　フィルタリングする集約グループを Aggregation テキスト ボックスに入力して、**Filter** をクリックします。

指定した集約グループが表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

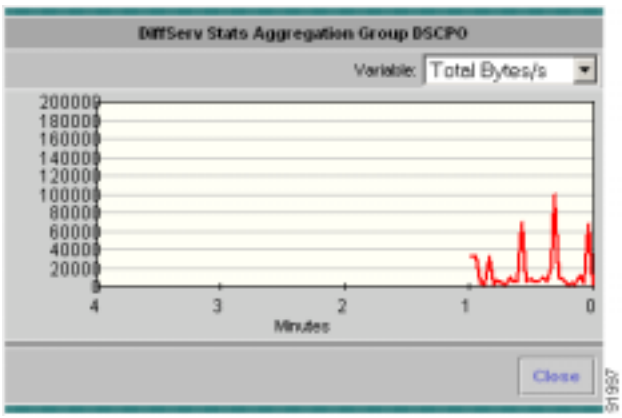
DiffServ Traffic Statistics テーブルのリアルタイム トラフィック統計情報の表示

DiffServ Traffic Statistics テーブルの特定の集約グループのリアルタイム トラフィック統計情報を、グラフ形式で表示できます。

テーブルで集約グループを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-27）が表示されます。

（注）　NetFlow ベースのデータ ソースには、Real-Time ボタンを使用できません。

図 4-27　Real-Time グラフ



DiffServ Traffic Statistics テーブルのレポートの表示

DiffServ Traffic Statistics テーブルから直接レポートを表示できます。レポートを表示する集約グループを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

DiffServ Traffic TopN Chart の表示

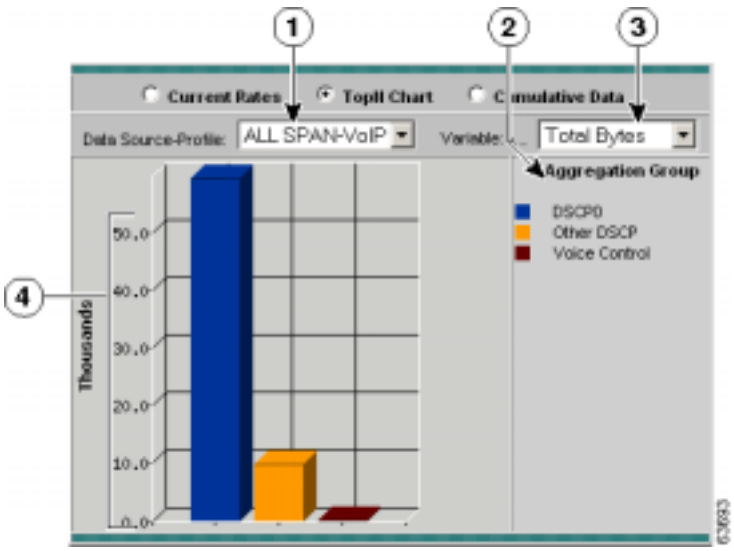
DiffServ Traffic TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Traffic Stats** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

DiffServ Aggregation Group TopN Chart（図 4-28）が表示されます。

図 4-28　DiffServ Aggregation Group TopN Chart



1	データ ソースとプロファイルのリスト	**3**	変数リスト
2	TopN 集約グループ	**4**	収集された 1 秒あたりのパケット数またはバイト数

ステップ 3　Data Source-profile リストから、監視するデータ ソースおよびプロファイルを選択します。

ステップ 4　Variable リストから、次のいずれかを選択します。

- Total Packets：パケットの合計数が表示されます。
- Total Bytes：バイトの合計数が表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

DiffServ Traffic Statistics Cumulative Data テーブルの表示

DiffServ Traffic Statistics Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Traffic Stats** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

DiffServ Traffic Statistics Cumulative Data テーブル（表 4-38）が表示されます。

表 4-38　DiffServ Traffic Statistics Cumulative Data テーブル

フィールド	説明
Aggregation Group	集約グループの名前
Packets	直前のインターバルで収集された合計パケット
Bytes	直前のインターバルで収集された合計バイト

ステップ 3　Data Source-profile リストから、監視するデータ ソースおよびプロファイルを選択します。

ステップ 4　フィルタリングする集約グループを Aggregation テキスト ボックスに入力して、**Filter** をクリックします。

指定した集約グループが表示されます。

ヒント
- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

DiffServ Application Statistics Current Rates テーブルの表示

DiffServ Application Statistics Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Application Stats** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

DiffServ Application Statistics Current Rates テーブル（表 4-39）テーブルが表示されます。

表 4-39　DiffServ Application Statistics Current Rates テーブル

フィールド	説明
Protocol Name	監視対象プロトコルの名前
Packets/s	直前のインターバルで収集された 1 秒あたりの合計パケット
Bytes/s	直前のインターバルで収集された 1 秒あたりの合計バイト

ステップ 3　Data Source-Profile リストから、監視するデータ ソースおよびプロファイルを選択します。

ステップ 4　Aggregation リストから集約グループを選択します。

ステップ 5　特定のプロトコルを表示するには、プロトコルを Protocol テキスト ボックスに入力して、**Filter** をクリックします。

指定したプロトコルが表示されます。

ヒント
- 完全なプロトコル名を表示するには、プロトコル名の上にカーソルを移動します。
- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

Application Statistics テーブルのアプリケーション会話の詳細の表示

Application Conversations 詳細テーブルを表示するには、Protocol Name カラムのプロトコル名をクリックします。Application Conversations テーブル（表 4-40）が表示されます。

表 4-40　Application Conversations テーブル

フィールド	説明
Source	会話の送信元ホスト アドレス
Destination	会話の宛先ホスト アドレス
Packets	会話中のパケット数
Bytes	会話中のバイト数

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

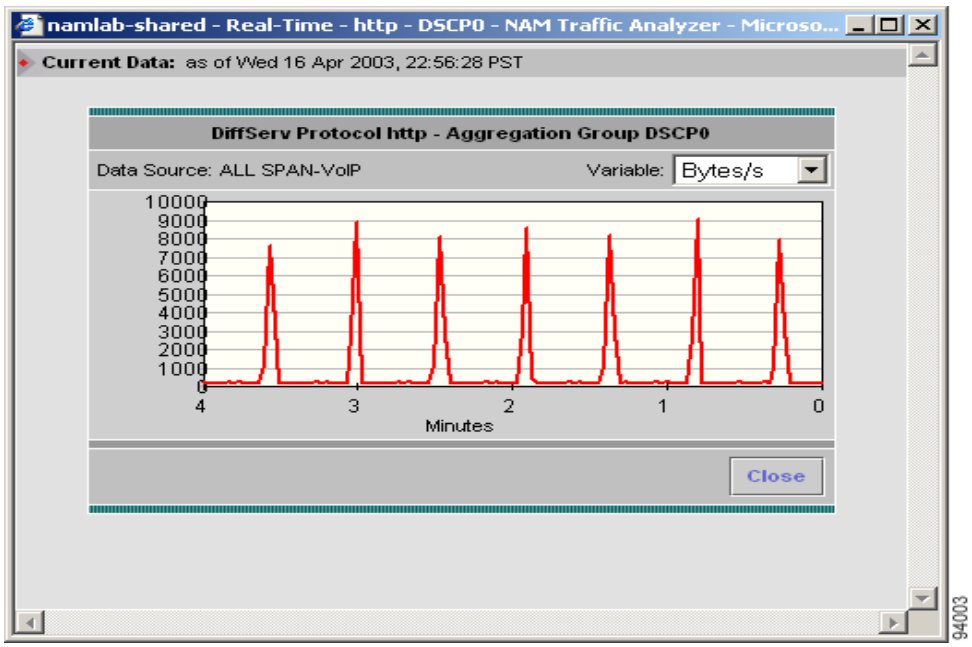
DiffServ Application Statistics テーブルのリアルタイム トラフィック統計情報の表示

DiffServ Application Statistics テーブルの特定のアプリケーション プロトコルのリアルタイム トラフィック統計情報を、グラフ形式で表示できます。

テーブルでアプリケーション プロトコルを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-29）が表示されます。

(注)　NetFlow ベースのデータ ソースには、Real-Time ボタンを使用できません。

図 4-29　Real-Time グラフ



DiffServ Application Statistics テーブルのレポートの表示

DiffServ Application Statistics テーブルから直接レポートを表示できます。レポートを表示するアプリケーション プロトコルを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したアプリケーションおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

DiffServ Application Statistics TopN Chart の表示

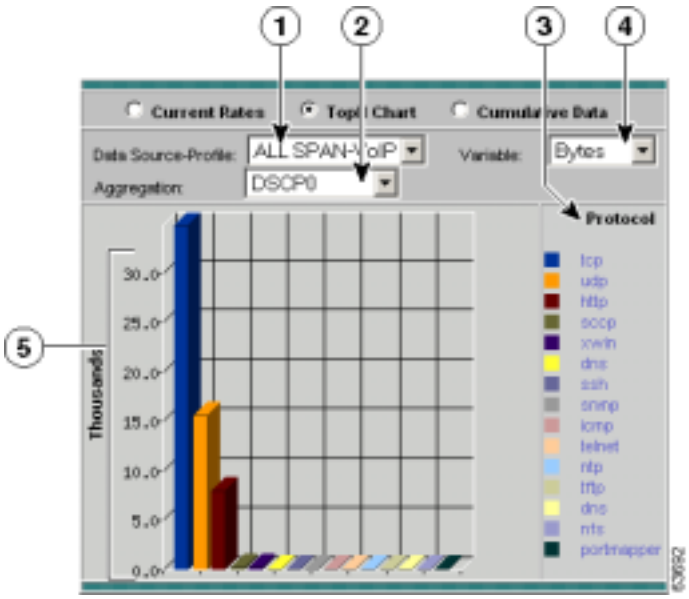
DiffServ Application Statistics TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Application Stats** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

DiffServ Application Statistics TopN Chart（図 4-30）が表示されます。

図 4-30　DiffServ Application Statistics TopN Chart



1	データ ソースとプロファイルのリスト	**4**	変数リスト
2	集約グループ リスト	**5**	プロトコルごとに収集された 1 秒あたりの合計パケット数またはバイト数
3	色別にソートされた TopN プロトコル		

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　Aggregation リストから集約グループを選択します。

ステップ 5　Variable リストから、次のいずれかを選択します。

- Total Packets：合計パケット数に基づいてアドレスがソートされます。
- Total Bytes：合計バイト数に基づいてアドレスがソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
完全なプロトコル名を表示するには、プロトコル名の上にカーソルを移動します。

DiffServ Application Statistics Cumulative Data テーブルの表示

DiffServ Application Statistics Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Application Stats** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

DiffServ Application Statistics Cumulative Data テーブル（表 4-41）が表示されます。

表 4-41　DiffServ Application Statistics Cumulative Data テーブル

フィールド	説明
Protocol Name	監視対象プロトコルの名前
Packets	直前のインターバルで収集された合計パケット
Bytes	直前のインターバルで収集された合計バイト

ステップ 3　Data Source-Profile リストから、監視するデータ ソースおよびプロファイルを選択します。

ステップ 4　Aggregation リストから集約グループを選択します。

ステップ 5　特定のプロトコルを表示するには、プロトコルを Protocol テキスト ボックスに入力して、**Filter** をクリックします。

指定したプロトコルが表示されます。

ヒント

- 完全なプロトコル名を表示するには、プロトコル名の上にカーソルを移動します。
- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

DiffServ Host Statistics Current Rates テーブルの表示

DiffServ Host Statistics Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Host Stats** をクリックします。

ステップ 2　Current Rates オプション ボタンをクリックします。

DiffServ Host Statistics Current Rates テーブル（表 4-42）が表示されます。

表 4-42　DiffServ Host Statistics Current Rates テーブル

フィールド	説明
Address	ホストのアドレス
Type	監視対象プロトコルの種類
In Packets/s	収集された 1 秒あたりの入力パケットの合計数
Out Packets/s	収集された 1 秒あたりの出力パケットの合計数
In Bytes/s	収集された 1 秒あたりの入力バイトの合計数
Total Bytes/s	収集された 1 秒あたりの出力バイトの合計数

ステップ 3　Data Source-Profile リストから、監視するデータ ソースおよびプロファイルを選択します。

ステップ 4　Aggregation リストから集約グループを選択します。

ステップ 5　特定のアドレスを表示するには、アドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

ヒント
- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

DiffServ Host Statistics テーブルのホスト会話の詳細の表示

Host Conversations 詳細テーブルを表示するには、Address カラムのアドレスをクリックします。Host Conversations テーブル（表 4-43）が表示されます。

表 4-43　Host Conversations テーブル

フィールド	説明
Source	会話の送信元ホスト アドレス
Application	会話で使用したアプリケーション プロトコル
Destination	会話の宛先ホスト アドレス
Packets	会話中のパケット数
Octets	会話中のオクテット数

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

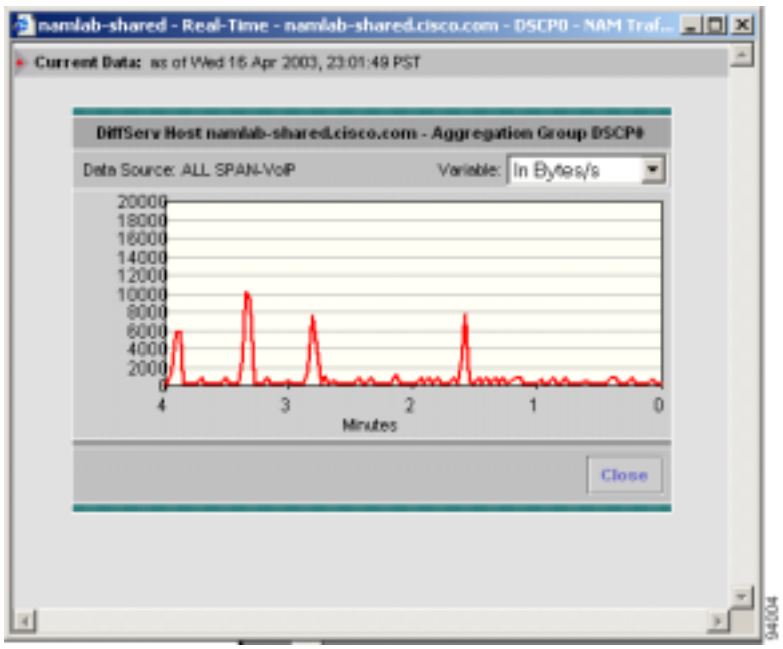
DiffServ Host Statistics テーブルのリアルタイム データの表示

DiffServ Host Statistics テーブルの特定のホストのリアルタイム データを、グラフ形式で表示できます。

テーブルでホストを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-31）が表示されます。

（注）　NetFlow ベースのデータ ソースには、Real-Time ボタンを使用できません。

図 4-31　Real-Time グラフ



DiffServ Host Statistics テーブルのレポートの表示

DiffServ Host Statistics テーブルから直接レポートを表示できます。レポートを表示するホストを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したホストおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

DiffServ Host Statistics TopN Chart の表示

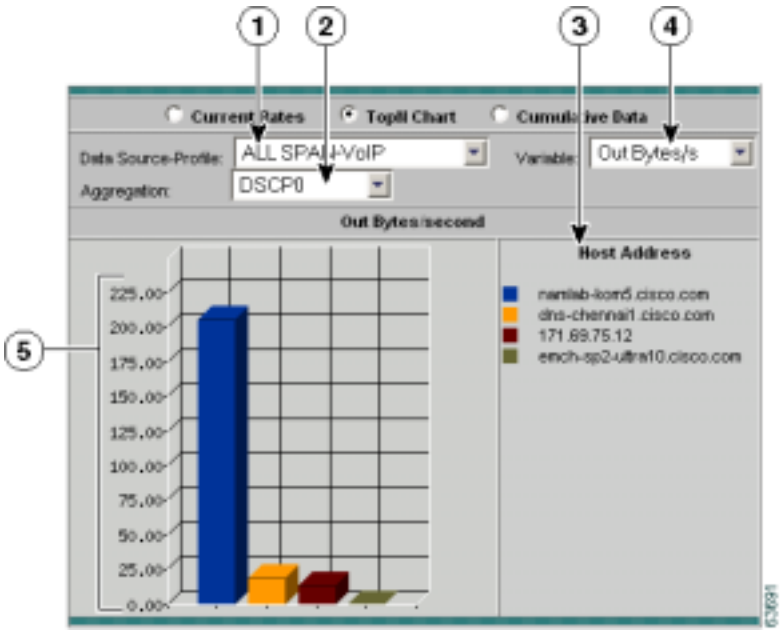
DiffServ Host Statistics TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Host Stats** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

DiffServ Host Statistics TopN Chart（図 4-32）が表示されます。

図 4-32　DiffServ Host Statistics TopN Chart



1	データ ソースとプロファイルのリスト	4	変数リスト
2	集約グループ リスト	5	アドレスごとに収集された 1 秒あたりの合計パケット数またはバイト数
3	色別にソートされた TopN ホスト アドレス		

ステップ 3　Data Source-Profile リストから、データ ソースおよびプロファイルを選択します。

ステップ 4　Aggregation リストから集約グループを選択します。

ステップ 5　Variable リストから、次のいずれかを選択します。

- Total Packets：合計パケット数に基づいてアドレスがソートされます。
- Total Bytes：合計バイト数に基づいてアドレスがソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

DiffServ Host Statistics Cumulative Data テーブルの表示

DiffServ Host Statistics Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Host Stats** をクリックします。

ステップ 2　Cumulative Data オプション ボタンをクリックします。

DiffServ Host Statistics Cumulative Data テーブル（表 4-44）が表示されます。

表 4-44　DiffServ Host Statistics Cumulative Data テーブル

フィールド	説明
Address	ホストのアドレス
Type	監視対象プロトコルの種類
In Packets	直前のインターバルで受信されたパケットの合計数
Out Packets	直前のインターバルで送信されたパケットの合計数
In Bytes	直前のインターバルで受信されたバイトの合計数
Out Bytes	直前のインターバルで送信されたバイトの合計数

ステップ 3　Data Source リストから、監視するデータ ソースを選択します。

ステップ 4　Aggregation リストから集約グループを選択します。

ステップ 5　特定のアドレスを表示するには、アドレスを Address テキスト ボックスに入力して、**Filter** をクリックします。

指定したアドレスが表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 合計に対する比率別にテーブル変数をソートするには、カラム ヘッダー上をクリックします。変数は、合計に対する比率に従って降順に表示されます。

応答時間データの監視

応答時間データは、TCP プロトコルに対する TCP 応答時間の情報を示します。NAM 3.6 では、次のようにネットワークおよび Application Response Time（ART; アプリケーション応答時間）を監視します。

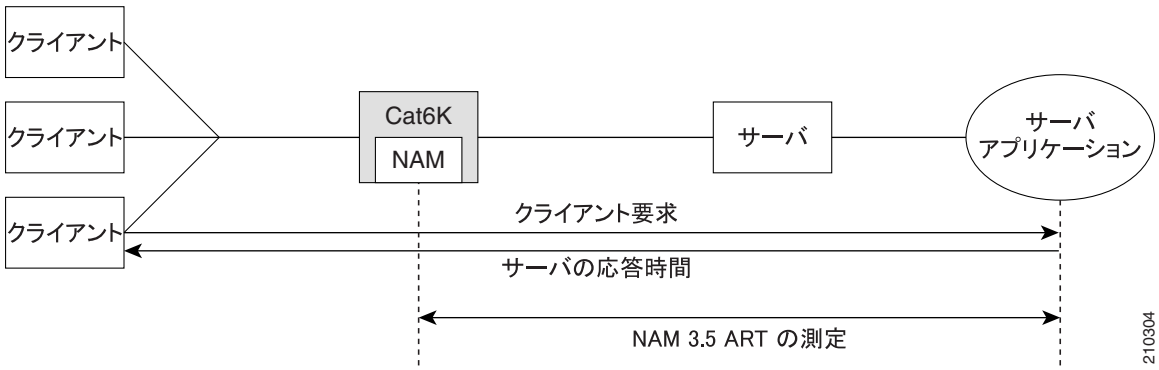
- サーバ アプリケーション応答時間（P.4-69）
- サーバ ネットワーク応答時間（P.4-71）
- サーバ / クライアント アプリケーション応答時間（P.4-74）
- サーバ / クライアント ネットワーク応答時間（P.4-78）

応答時間データを表示するには、**Monitor** > **Response Time** をクリックします。

レガシー アプリケーション応答時間の監視

図 4-33 に示すように、以前の NAM リリースでは、スイッチとサーバ アプリケーションの間で ART が測定されていました。この測定では、ルータにエンドツーエンドの応答時間が提供されませんでした。ネットワークとアプリケーションの遅延を確認するには、クライアントの近くとサーバの近くに 1 つずつ、2 つの NAM を配置する必要があります。その後で、2 つの NAM のデータを関連付ける必要があります。

図 4-33　NAM レガシー アプリケーション応答時間の測定



NAM 3.6 アプリケーション応答時間の測定

NAM 3.6 では ART およびネットワークの遅延がより見やすくなっています。表 4-45 に、NAM 3.6 による ART メトリック測定の定義を示します（図 4-34 を参照）。

表 4-45　NAM 3.6 ART メトリック

ART メトリック	定義
Client Network Delay（CND; クライアント ネットワーク遅延）	CND は、クライアントと NAM スイッチまたはルータとの間のネットワーク ラウンドトリップ時間（経過時間）です。
Server Network Delay（SND; サーバ ネットワーク遅延）	SND は、サーバと NAM スイッチまたはルータとの間のネットワーク ラウンドトリップ時間（経過時間）です。

表 4-45　NAM 3.6 ART メトリック（続き）

ART メトリック	定義
Application Delay（AD; アプリケーション遅延）	AD は、サーバ アプリケーション（Web サーバ アプリケーションなど）が要求に応答するのにかかる時間です。これは、サーバ アプリケーションに到着したクライアント要求と、そのアプリケーションが戻す最初の応答との間の時間です。
Network Delay（ND; ネットワーク遅延）	ND は、NAM スイッチまたはルータを経由する、クライアントとサーバ間のネットワーク ラウンドトリップ時間（経過時間）です。ND は CND と SND の合計に等しくなります。
Total Delay（TD; 遅延合計）	TD は、クライアント要求の最初のパケットから、クライアントがアプリケーション サーバから最初の応答パケットを受信するまでの合計時間です。遅延合計（TD）は、ネットワーク遅延（ND）とアプリケーション遅延（AD）の合計です。
Transaction Time（TT; トランザクション時間）	TT は、クライアント要求の最初のパケットから、クライアントがサーバから最後の応答パケットを受信するまでの合計時間です。

図 4-34　NAM 3.6 アプリケーション応答時間の測定

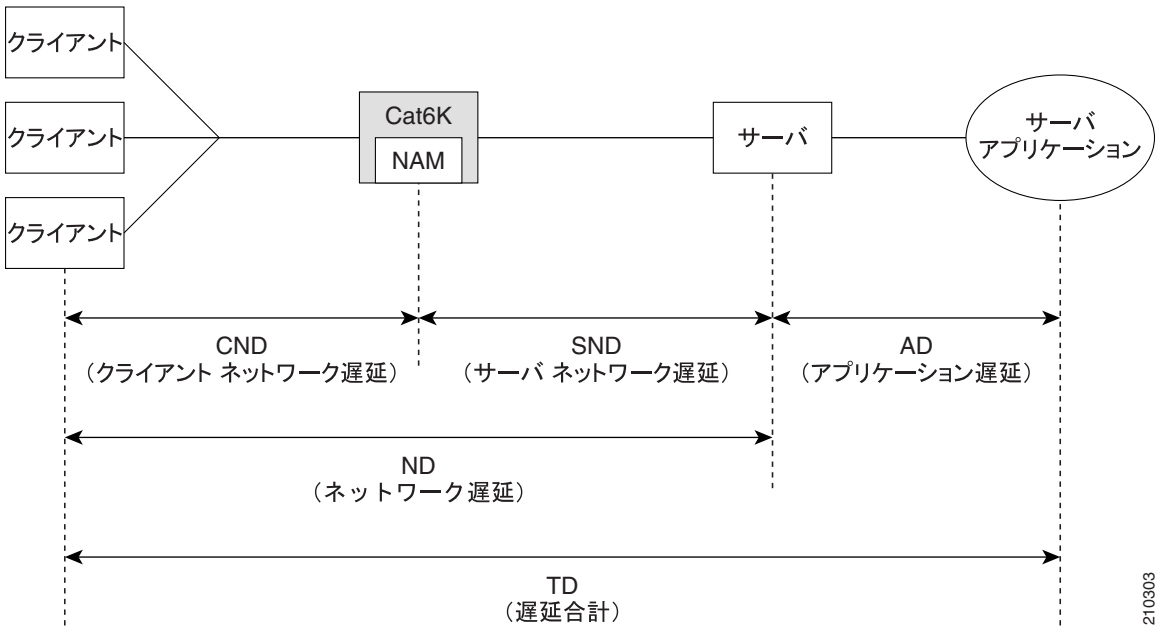
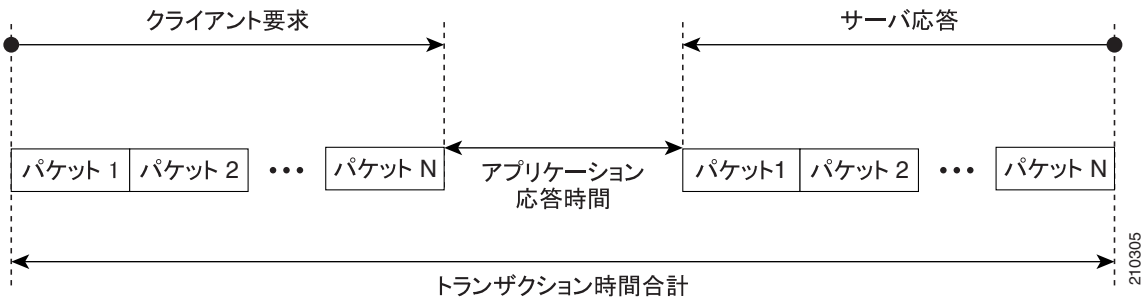


図 4-35　トランザクション時間と応答時間の測定



サーバ アプリケーション応答時間

Monitor > **Response Time** をクリックすると、デフォルトで Server Application Response Time ウィンドウが表示されます。All Data ウィンドウもデフォルトで表示されます。また、TopN Chart を表示して、最もアクティブなネットワークを表示することができます。

サーバ アプリケーション応答時間の表示

Server Application Response Time ウィンドウには、サーバ アプリケーションごとにアプリケーション応答時間（ART）の要約が示され、ここで、サーバの IP アドレス、使用アプリケーション、次についての最小、平均、最大応答時間を確認できます。

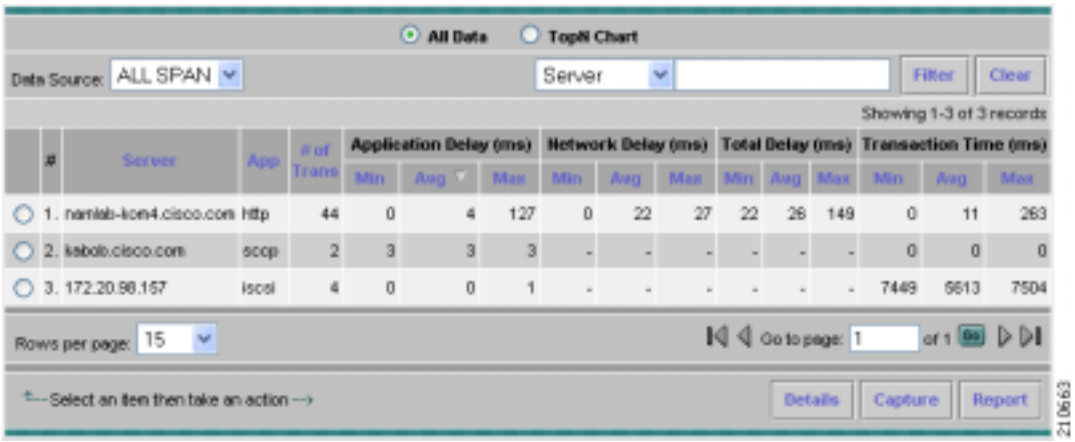
- アプリケーション遅延
- ネットワーク遅延
- 遅延合計
- トランザクション時間

(注)

NAM では TCP 3 ウェイ ハンドシェイクを使用してネットワーク遅延を計算します。ポーリング インターバルに新しい TCP 接続がない場合、NAM GUI は遅延値にダッシュ（-）を表示して、そのインターバルに遅延データがないことを示します。

図 4-36 に Server Application Response Time ウィンドウを示します。

図 4-36　Server Application Response Time ウィンドウ



サーバ ART の詳細の表示

特定のサーバの詳細を表示するには、Select カラムのオプション ボタンをクリックして、**Details** をクリックします。Server ART Detail ウィンドウが表示されます。応答時間の分布を示したチャートだけでなく、サーバの詳細情報（サーバ ネットワーク遅延の応答時間、ヒストグラム、オクテット カウント、最大値と最小値など）も表示できます。

表4-46 に、Server Application Response Time ウィンドウのフィールドについて詳細な説明を示します。

表 4-46　Server Application Response Time の詳細

フィールド	説明
Server	測定対象サーバの名前。
App	サーバが使用しているアプリケーション。
# of Trans	このサーバで現在アクティブなトランザクションの数。
Application Delay	AD の最小、平均、および最大値を表示します。AD は、サーバ アプリケーション（Web サーバ アプリケーションなど）が要求に応答するのにかかる時間です。これは、サーバ アプリケーションに到着したクライアント要求と、そのアプリケーションが戻す最初の応答との間の時間です。
Network Delay	ND の最小、平均、および最大値を表示します。ND は、NAM スイッチまたはルータを経由する、クライアントとサーバ間のネットワーク ラウンドトリップ時間（経過時間）です。ND は CND と SND の合計に等しくなります。
Transaction Time	TT の最小、平均、および最大値を表示します。TT は、クライアント要求の最初のパケットから、クライアントがサーバから最後の応答パケットを受信するまでの合計時間です。

サーバ ART データのキャプチャ

特定のサーバのデータを Server ART テーブルから直接キャプチャすることができます。

Select カラムのオプション ボタンをクリックしてテーブルからサーバを選択し、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

キャプチャがすでに実行されている場合は、メッセージ ウィンドウが表示されます。**Yes** をクリックして現在のキャプチャを中止、または **No** をクリックして選択を取り消します。

報告されたプロトコルのサブセットのみ、Capture ボタンが利用可能です。IP、IPv6 および GRE などのプロトコルの場合、カスタム フィルタを設定する必要があります。カスタム フィルタの設定の詳細については、P.6-21 の「カスタム キャプチャ フィルタの作成」を参照してください。

（注）　NetFlow ベースのデータ ソースには、Capture ボタンを使用できません。

Server Application Response Time ウィンドウのレポートの表示

Server Application Response Time ウィンドウから直接レポートを表示できます。レポートを表示するサーバを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したサーバおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Application Response Time TopN Chart の表示

最もアクティブなネットワークを表示するには、**TopN Chart** をクリックします。Server Application Response Time の TopN Chart を表示するには、次の手順を実行します。

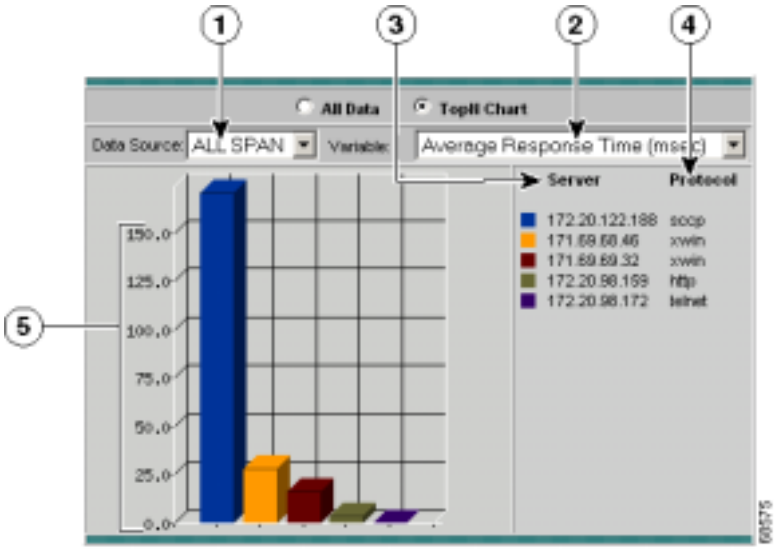
ステップ 1　**Monitor** > **Response Time** をクリックします。

Server Application Response Time ウィンドウが表示されます。

ステップ 2　**TopN Chart** オプション ボタンをクリックします。

Server Application Response Time TopN Chart（図 4-37）が表示されます。

図 4-37　Server Application Response Time TopN Chart



1	データ ソース リスト	**4**	サーバが使用するプロトコル
2	変数リスト	**5**	表示された変数の値（1 秒あたり）
3	色別にソートされた TopN サーバ アドレス		

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　Variable リストから、ソート オプションを選択します。

指定したオプションがチャートに表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

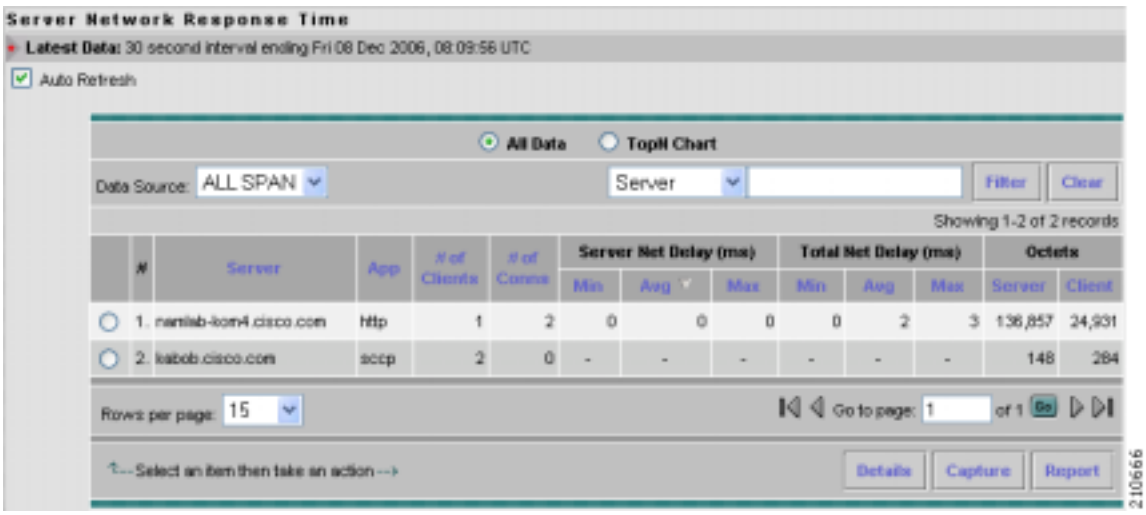
サーバ ネットワーク応答時間

Server Network Response Time ウィンドウには、サーバとスイッチとの間のネットワーク接続および応答に関する情報が表示されます。

図 4-38 に Server Network Response Time ウィンドウを示します。

(注)　NAM では TCP 3 ウェイ ハンドシェイクを使用してネットワーク遅延を計算します。ポーリング インターバルに新しい TCP 接続がない場合、NAM GUI は遅延値にダッシュ（-）を表示して、そのインターバルに遅延データがないことを示します。

図 4-38　Server Network Response Time ウィンドウ



サーバ ネットワーク応答時間の詳細の表示

表 4-47 に、Server Network Response Time ウィンドウのフィールドについて詳細な説明を示します。

表 4-47　Server Network Response Time ウィンドウの詳細

フィールド	説明
Server	測定対象サーバの名前。
App	サーバが使用しているアプリケーション。
# of Clients	サーバに接続されているクライアントの数。
# of Conns	サーバとのアクティブ接続の数。
Server Net Delay (SND)	SND の最小、平均、および最大値を表示します。SND は、サーバと NAM スイッチまたはルータとの間のネットワーク ラウンドトリップ時間（経過時間）です。
Total Net Delay	TD の最小、平均、および最大値を表示します。TD は、クライアント要求の最初のパケットから、クライアントがアプリケーション サーバから最初の応答パケットを受信するまでの合計時間です。遅延合計（TD）は、ネットワーク遅延（ND）とアプリケーション遅延（AD）の合計です。
Octets	サーバの場合、サーバからクライアントに送信されたオクテット（バイト）数。 クライアントの場合、クライアントからサーバに送信されたオクテット（バイト）数。

Server Network Response Time ウィンドウのデータのキャプチャ

特定のサーバのデータを Server Network Response Time ウィンドウから直接キャプチャすることができます。

Select カラムのオプション ボタンをクリックしてテーブルからサーバを選択し、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

キャプチャがすでに実行されている場合は、メッセージ ウィンドウが表示されます。**Yes** をクリックして現在のキャプチャを中止、または **No** をクリックして選択を取り消します。

報告されたプロトコルのサブセットのみ、Capture ボタンが利用可能です。IP、IPv6 および GRE などのプロトコルの場合、カスタム フィルタを設定する必要があります。カスタム フィルタの設定の詳細については、P.6-21 の「カスタム キャプチャ フィルタの作成」を参照してください。

(注)　NetFlow ベースのデータ ソースには、Capture ボタンを使用できません。

Server Network Response Time ウィンドウのレポートの表示

Server Network Response Time ウィンドウから直接レポートを表示できます。レポートを表示するサーバを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したサーバおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Server Network Response Time TopN Chart の表示

最もアクティブなネットワークを表示するには、**TopN Chart** をクリックします。Server Application Response Time の TopN Chart を表示するには、次の手順を実行します。

ステップ 1　**Monitor** > **Response Time** をクリックします。

Server Application Response Time ウィンドウが表示されます。

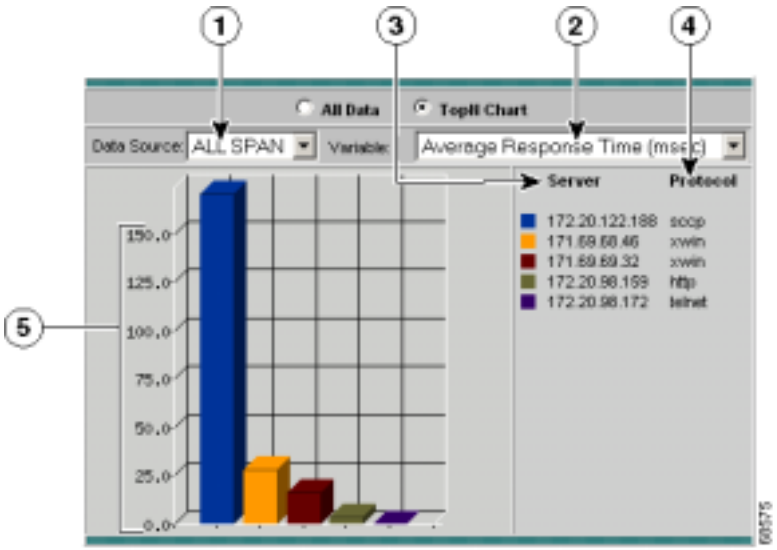
ステップ 2　メニュー領域の **Server Network** をクリックします。

Server Network Response Time ウィンドウが表示されます。

ステップ 3　**TopN Chart** オプション ボタンをクリックします。

Server Network Response Time TopN Chart（図 4-39）が表示されます。

図 4-39　Server Network Response Time TopN Chart



1	データ ソース リスト	**4**	サーバが使用するプロトコル
2	変数リスト	**5**	表示された変数の値（1 秒あたり）
3	色別にソートされた TopN サーバ アドレス		

ステップ 4　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 5　Variable リストから、ソート オプションを選択します。

指定したオプションがチャートに表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

サーバ / クライアント アプリケーション応答時間

Server/Client ART ウィンドウには、サーバおよびクライアントのアプリケーション応答時間データについて要約が示されます。ウィンドウのエントリを選択すると、詳細情報を表示できます。

サーバ / クライアント アプリケーション応答時間の表示

Server/Client Application Response Time ウィンドウを表示するには、次の手順を実行します。

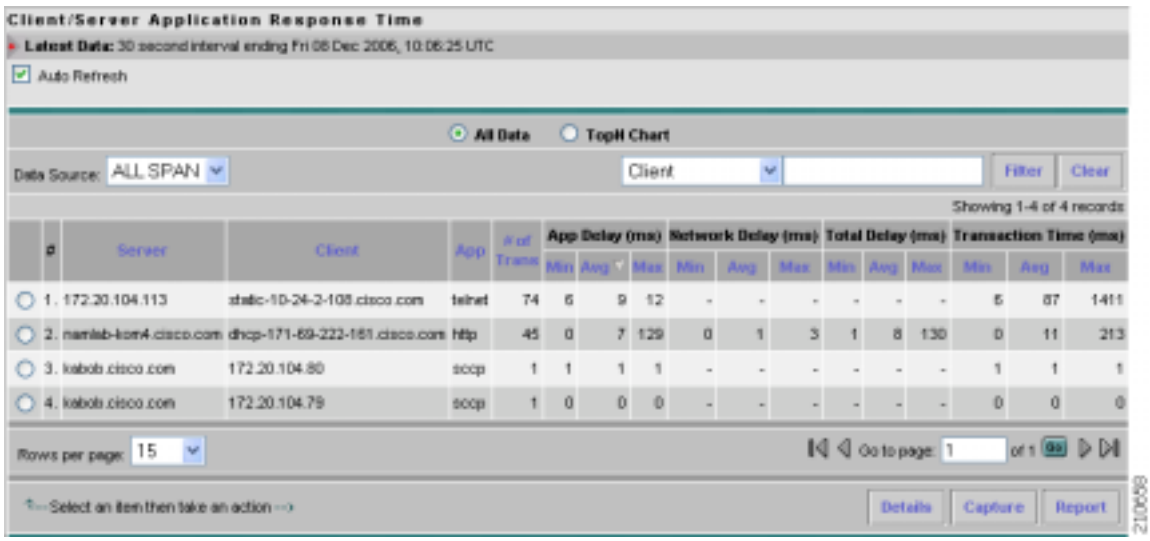
ステップ 1　コンテンツで **Server/Client Application** をクリックします。

図 4-40 に Server/Client Application Response Time ウィンドウを示します。

(注)

NAM では TCP 3 ウェイ ハンドシェイクを使用してネットワーク遅延を計算します。ポーリング インターバルに新しい TCP 接続がない場合、NAM GUI は遅延値にダッシュ（-）を表示して、そのインターバルに遅延データがないことを示します。

図 4-40　Server/Client Application Response Time ウィンドウ



Client/Server Application Response Time ウィンドウ（表 4-48）が表示されます。

表 4-48　Client/Server Application Response Time ウィンドウ

フィールド	説明
Server	サーバのホスト アドレス。
Client	クライアントのホスト アドレス。
App	サーバが使用しているアプリケーション。
# of Trans	現在のトランザクションの数。
Application Delay (AD)	AD の最小、平均、および最大値を表示します。AD は、サーバ アプリケーション（Web サーバ アプリケーションなど）が要求に応答するのにかかる時間です。これは、サーバ アプリケーションに到着したクライアント要求と、そのアプリケーションが戻す最初の応答との間の時間です。
Network Delay(ND)	ND の最小、平均、および最大値を表示します。ND は、NAM スイッチまたはルータを経由する、クライアントとサーバ間のネットワーク ラウンドトリップ時間（経過時間）です。ND は CND と SND の合計に等しくなります。
Total Delay (TD)	TD は、クライアント要求の最初のパケットから、クライアントがアプリケーション サーバから最初の応答パケットを受信するまでの合計時間です。遅延合計（TD）は、ネットワーク遅延（ND）とアプリケーション遅延（AD）の合計です。
Transaction Time	TT の最小、平均、および最大値を表示します。TT は、クライアント要求の最初のパケットから、クライアントがサーバから最後の応答パケットを受信するまでの合計時間です。

ステップ 2　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 3　フィルタ リストから、フィルタリングする変数を選択します。

ステップ 4　フィルタリングする変数名をフィルタ ボックスに入力して、**Filter** をクリックします。

指定した変数が表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

サーバ / クライアント アプリケーション応答時間の詳細の表示

特定のクライアント / サーバ会話の詳細を表示するには、Select カラムのオプション ボタンをクリックして、**Details** をクリックします。Server/Client Response Time Detail ウィンドウが表示されます。応答時間の分布を示したチャートだけでなく、クライアント / サーバ会話の詳細情報も表示できます。

Client/Server Application Response Time ウィンドウのプロトコル データのキャプチャ

特定のプロトコルのデータを Client/Server Response Time テーブルから直接キャプチャすることができます。

テーブルでサーバ プロトコルを選択して、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

報告されたプロトコルのサブセットのみ、Capture ボタンが利用可能です。IP、IPv6 および GRE などのプロトコルの場合、カスタム フィルタを設定する必要があります。カスタム フィルタの設定の詳細については、P.6-21 の「カスタム キャプチャ フィルタの作成」を参照してください。

（注）　NetFlow ベースのデータ ソースには、Capture ボタンを使用できません。

Client/Server Application Response Time ウィンドウのレポートの表示

Client/Server Response Time テーブルから直接レポートを表示できます。レポートを表示するプロトコルを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したクライアント / サーバおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Client/Server Application Response Time TopN Chart の表示

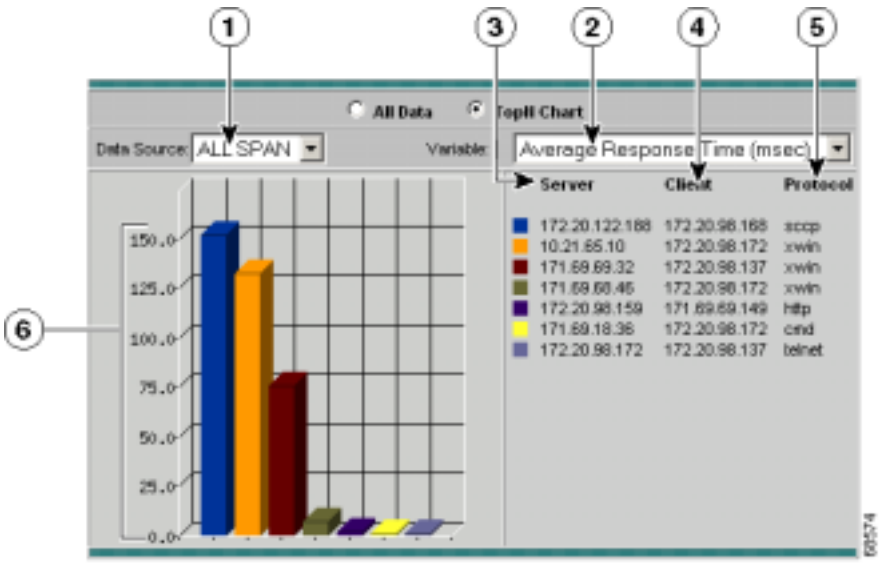
Client/Server Response Time TopN Chart を表示するには、次の手順を実行します。

ステップ 1　Contents メニューで **Client/Server Application** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

Client/Server Application Response Time TopN Chart（図 4-41）が表示されます。

図 4-41　Client/Server Application Response Time TopN Chart



1	データ ソース リスト	**4**	色別にソートされた TopN クライアント
2	変数リスト	**5**	会話に使用されたプロトコル
3	色別にソートされた TopN サーバ	**6**	クライアント / サーバ会話ごとの変数の値（1 秒あたり）

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　Variable リストから、ソート オプションを選択します。

指定したオプションがチャートに表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

サーバ / クライアント ネットワーク応答時間

Server/Client Network Response Time ウィンドウには、サーバとクライアントとの間のネットワーク接続（ネットワーク経過時間とも言う）に関する情報が表示されます。

サーバ / クライアント ネットワーク応答時間の表示

Server/Client Network Response Time ウィンドウを表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Server/Client Network** をクリックします。

図 4-42 に Server/Client Network Response Time ウィンドウを示します。

（注）　NAM では TCP 3 ウェイ ハンドシェイクを使用してネットワーク遅延を計算します。ポーリング インターバルに新しい TCP 接続がない場合、NAM GUI は遅延値にダッシュ（-）を表示して、そのインターバルに遅延データがないことを示します。

図 4-42　Server/Client Network Response Time ウィンドウ

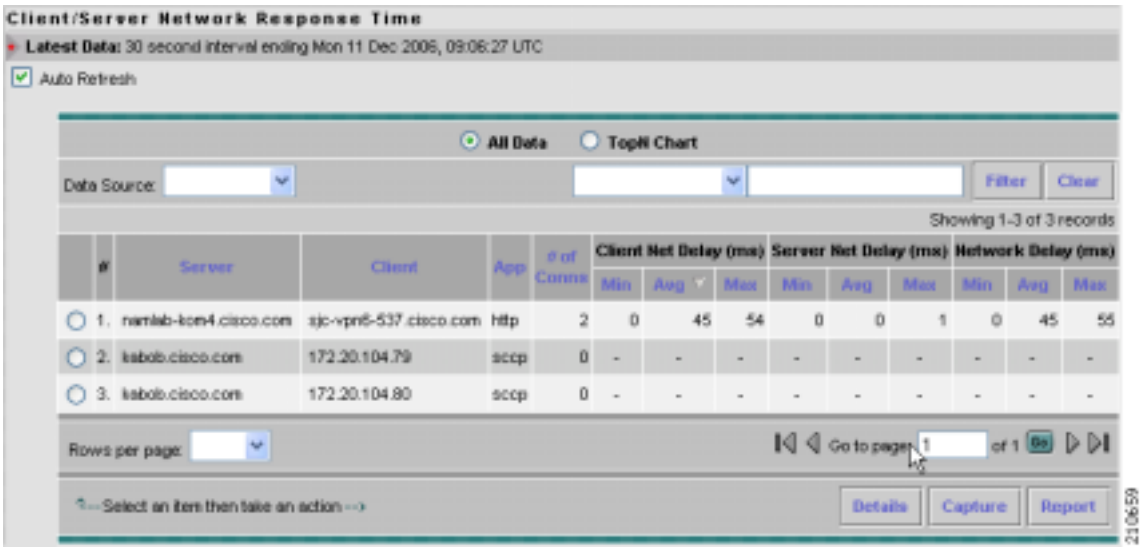


表 4-49 に、Server/Client Network Response Time ウィンドウのフィールドを示します。

表 4-49　Server/Client Network Response Time ウィンドウ

フィールド	説明
Server	サーバのホスト アドレス
Client	クライアントのホスト アドレス
App	サーバが使用しているアプリケーション
# of Conns	現在の接続の数
Client Network Delay	時間の最小、平均、および最大値
Server Network Delay	ネットワーク遅延合計の最小、平均、および最大値
Network Delay	ネットワーク遅延合計の最小、平均、および最大値

ステップ 2　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 3　フィルタ リストから、フィルタリングする変数を選択します。

ステップ 4　フィルタリングする変数名をフィルタ ボックスに入力して、**Filter** をクリックします。

指定した変数が表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

サーバ / クライアント応答時間の詳細の表示

特定のクライアント / サーバ会話の詳細を表示するには、Select カラムのオプション ボタンをクリックして、**Details** をクリックします。Server/Client Response Time Detail ウィンドウが表示されます。応答時間の分布を示したチャートだけでなく、クライアント / サーバ会話の詳細情報も表示できます。

Client/Server Application Response Time ウィンドウのプロトコル データのキャプチャ

特定のプロトコルのデータを Client/Server Response Time テーブルから直接キャプチャすることができます。

テーブルでサーバ プロトコルを選択して、**Capture** をクリックします。Packet Browser が表示されます。Packet Browser を使用したパケット表示の詳細については、P.6-14 の「詳細なプロトコル デコード情報の表示」を参照してください。

報告されたプロトコルのサブセットのみ、Capture ボタンが利用可能です。IP、IPv6 および GRE などのプロトコルの場合、カスタム フィルタを設定する必要があります。カスタム フィルタの設定の詳細については、P.6-21 の「カスタム キャプチャ フィルタの作成」を参照してください。

（注）　NetFlow ベースのデータ ソースには、Capture ボタンを使用できません。

Client/Server Response Time ウィンドウのレポートの表示

Client/Server Response Time テーブルから直接レポートを表示できます。レポートを表示するプロトコルを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したクライアント / サーバおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Client/Server Network Response Time TopN Chart の表示

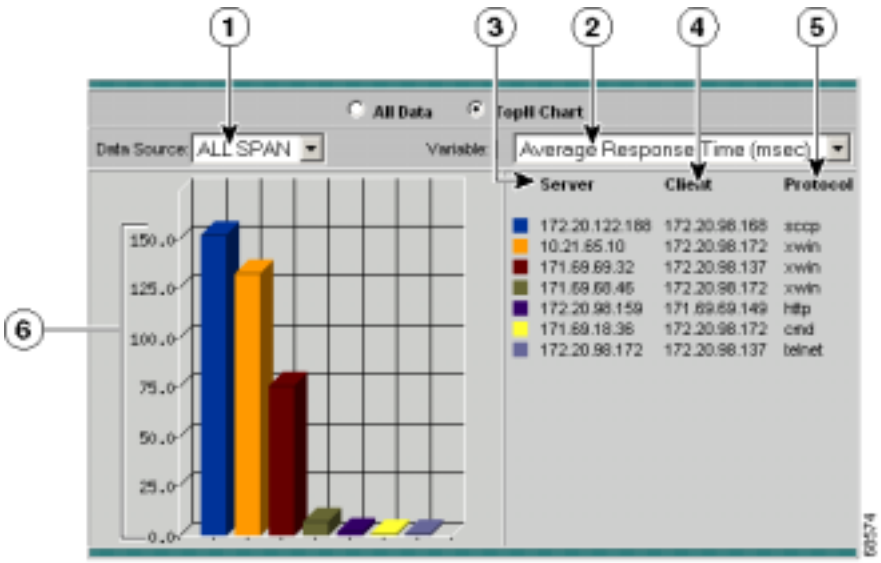
Server/Client Network Response Time TopN Chart を表示するには、次の手順を実行します。

ステップ 1　コンテンツで **Client/Server** をクリックします。

ステップ 2　TopN Chart オプション ボタンをクリックします。

Client/Server Network Response Time TopN Chart（図 4-43）が表示されます。

図 4-43　Client/Server Network Response Time TopN Chart



1	データ ソース リスト	**4**	色別にソートされた TopN クライアント
2	変数リスト	**5**	会話に使用されたプロトコル
3	色別にソートされた TopN サーバ	**6**	クライアント / サーバ会話ごとの変数の値（1 秒あたり）

ステップ 3　Data Source リストから、監視対象のデータ ソースを選択します。

ステップ 4　Variable リストから、ソート オプションを選択します。

指定したオプションがチャートに表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。
- 完全なプロトコル名を表示するには、テーブルの Protocol カラムのプロトコル名の上にカーソルを移動します。

ポート / インターフェイス統計情報データの表示

収集したスイッチまたはルータのさまざまなデータを表示するには、**Monitor** をクリックして、**Switch** または **Router** をクリックします。上部に 3 つのオプション ボタンがある Port Stats または Interface Stats テーブルが表示されます。

Port Stats の場合、次の用途に応じて、オプション ボタンを選択できます。

- Port Stats Current Rates テーブルの表示（P.4-81）
- Port Stats TopN Chart の表示（P.4-84）
- Port Stats Cumulative Data テーブルの表示（P.4-87）

Interface Stats の場合、次の用途に応じて、オプション ボタンを選択できます。

- Interface Stats Current Rates テーブルの表示（P.4-82）
- Interface Stats TopN Chart の表示（P.4-86）
- Interface Stats Cumulative Data テーブルの表示（P.4-88）

（注） NM-NAM デバイスの場合は、**Setup** > **Data Sources** で **Interfaces** をセットアップしていると、Details ウィンドウにホスト、会話、およびアプリケーションを表示することができます。

Port Stats Current Rates テーブルの表示

Port Stats Current Rates テーブルを使用して、スイッチで収集されたさまざまなデータを表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Count Types ドロップダウン メニューで、デフォルトの Traffic Rates を表示できます。

Port Stats Current Rates テーブル（Traffic Rates）を表示するには、次の手順を実行します。

ステップ 1　Current Rates オプション ボタンをクリックします。

Port Stats Current Rates テーブル（Traffic Rates）（表 4-50）に、Count Type が Traffic Rates に設定されている場合に表示されるフィールドの一覧を示します。

表 4-50　Port Stats Current Rates テーブル（Traffic Rates）

フィールド	説明
Port Name	ポート番号
Utilization %	ポートの使用率
Bytes/s	ポートで収集された 1 秒あたりのバイト数
Packets/s	ポートで収集された 1 秒あたりのパケット数
Broadcast Packets/s	収集された 1 秒あたりのブロードキャスト パケット数
Multicast Packets/s	収集された 1 秒あたりのマルチキャスト パケット数
Errors	検出されたすべてのタイプのエラー数（すべてのエラーのリストについては、表 4-51 を参照）

Port Stats Current Rates テーブル（Error Rates）（表 4-51）に、Count Type が Error Rates に設定されている場合に表示されるフィールドの一覧を示します。

表 4-51　Port Stats Current Rates テーブル（Error Rates）

フィールド	説明
Port Name	ポート番号
Utilization %	ポートの使用率
Dropped Events/s	1 秒あたりのドロップされたイベント数
CRC Align Errors/s	収集された 1 秒あたりの CRC Align エラー数
Undersize packets/s	収集された長さが 64 オクテット未満のパケット数
Oversize Packets/s	収集された長さが 1518 オクテット以上のパケット数
Fragments/s	長さが 64 オクテット未満で、不正な Frame Check Sequence（FCS）を持つ、収集された 1 秒あたりのパケット数
Jabbers/s	長さが 1518 オクテット以上で、不正な Frame Check Sequence（FCS）を持つ、収集された 1 秒あたりのパケット数
Collisions/s	Ethernet セグメントで収集された 1 秒あたりの衝突数

（注） 表 4-50 および表 4-51 は、Cumulative Data オプション ボタンをクリックした場合にも有効です。

ステップ 2　フィルタリングするポート名を Port Name テキスト ボックスに **Filter** をクリックします。

指定したポート名が表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Interface Stats Current Rates テーブルの表示

Interface Stats Current Rates テーブルを使用して、ルータで収集されたさまざまなデータを表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Interface Stats Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　Current Rates オプション ボタンをクリックします。

Interface Stats Current Rates テーブル（表 4-52）が表示されます。

表 4-52　Interface Stats Current Rates テーブル

フィールド	説明
Interface	インターフェイス番号
In % Utilization	ポートの使用率
Out % Utilization	ポートの使用率
In Packets/s	収集された 1 秒あたりのパケット数
Out Packets/s	送信された 1 秒あたりのパケット数
In Bytes/s	収集された 1 秒あたりのバイト数
Out Bytes/s	送信された 1 秒あたりのバイト数
In Non-Unicasts/s	収集された 1 秒あたりの非ユニキャスト数
Out Non-Unicasts/s	送信された 1 秒あたりの非ユニキャスト数
In Discards/s	収集された 1 秒あたりの破棄数
Out Discards/s	送信された 1 秒あたりの破棄数
In Errors/s	収集された 1 秒あたりのエラー数
Out Errors/s	送信された 1 秒あたりのエラー数

ステップ 2　フィルタリングするインターフェイス名を Filter テキスト ボックスに入力して、**Filter** をクリックします。

指定したインターフェイス名が表示されます。

ヒント

- 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

ポート / インターフェイスの詳細の表示

特定のポートまたはインターフェイスのパケット分布の詳細を表示するには、Port Name カラムでポート番号または Interface カラムでインターフェイス番号をクリックします。詳細ウィンドウが表示され、指定したポートまたはインターフェイスの 1 秒あたりのパケット分布を示すチャートが表示されます。

（注）　NM-NAM デバイスの場合は、**Setup > Data Source > Interface** ウィンドウでインターフェイスをセットアップしていると、詳細ウィンドウにアプリケーション、ホスト、および会話の TopN テーブルが表示されます。

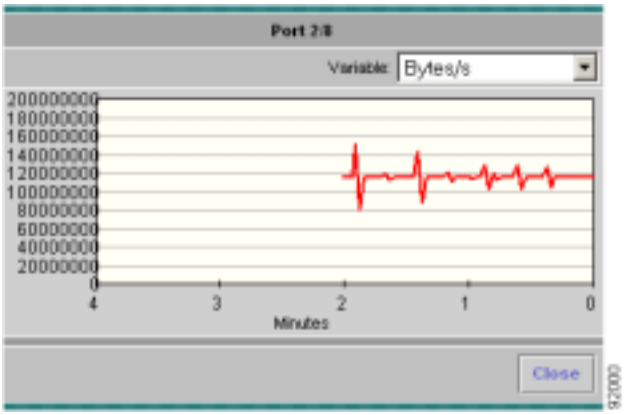
Port/Interface Stats テーブルのリアルタイム トラフィック データの表示

Port Stats テーブルまたは Inteface Status テーブルの特定のスイッチ ポートまたはインターフェイスのリアルタイム データを、グラフ形式で表示できます。

テーブルでスイッチ ポートまたはインターフェイスを選択して、**Real-Time** をクリックします。Real-Time グラフ（図 4-44）が表示されます。

(注)　NetFlow ベースのデータ ソースには、Real-Time ボタンを使用できません。

図 4-44　Real-Time グラフ



Port/Interface Stats テーブルのレポートの表示

Port Stats テーブルまたは Interface Stats テーブルから直接レポートを表示できます。レポートを表示するスイッチ ポートまたはインターフェイスを選択して、**Report** をクリックします。Basic Reports グラフが表示されます。レポートが設定されていない場合、Basic Reports 画面が表示され、選択したポートおよびデータ ソースの新しいレポートが作成されます。

レポートの表示および作成の詳細については、第 5 章「レポートの作成と表示」を参照してください。

Port Stats TopN Chart の表示

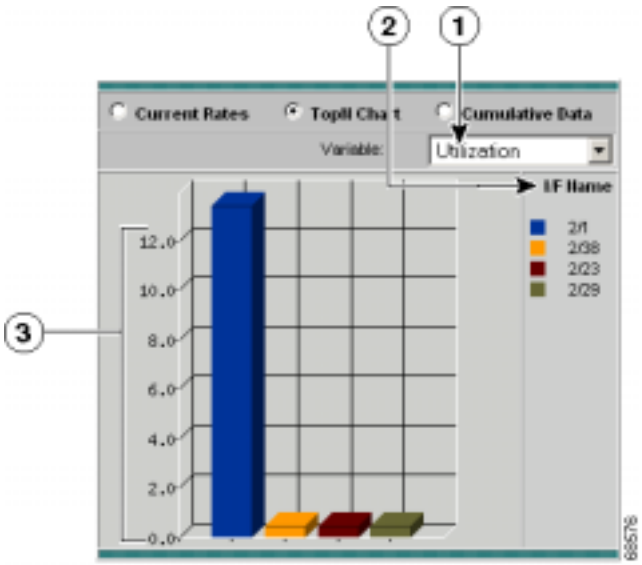
Port Stats TopN Chart を使用して、ポートごとに収集されたさまざまなデータをグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。

Port Stats TopN Chart を表示するには、次の手順を実行します。

ステップ 1　TopN Chart オプション ボタンをクリックします。

Port Stats TopN Chart（図 4-45）が表示されます。

図 4-45　Port Stats TopN Chart



1	変数リスト	**3**	スイッチ ポートごとの変数の値（1 秒あたり）
2	TopN スイッチ ポート		

ステップ 2　Variable リストから、次のいずれかを選択します。

- Utilization：使用率に基づいて、インターフェイス番号がソートされます。使用率が 0.1% 未満の場合は、0.0% としてチャートに表示されます。
- Dropped　Events：ドロップされたイベント数に基づいてインターフェイス番号がソートされます。
- Bytes：バイト数に基づいてインターフェイス番号がソートされます。
- Packets：パケット数に基づいてインターフェイス番号がソートされます。
- Broadcast Pkts：ブロードキャスト パケット数に基づいてインターフェイス番号がソートされます。
- Multicast Pkts：マルチキャスト パケット数に基づいてインターフェイス番号がソートされます。
- CRC Align Errors：CRC Align エラー数に基づいてインターフェイス番号がソートされます。
- Undersize Pkts：過小サイズ パケット数に基づいてインターフェイス番号がソートされます。
- Oversize Pkts：過大サイズ パケット数に基づいてインターフェイス番号がソートされます。
- Fragments：フラグメント数に基づいてインターフェイス番号がソートされます。
- Jabbers：ジャバー数に基づいてインターフェイス番号がソートされます。
- Collisions：衝突数に基づいてインターフェイス番号がソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Interface Stats TopN Chart の表示

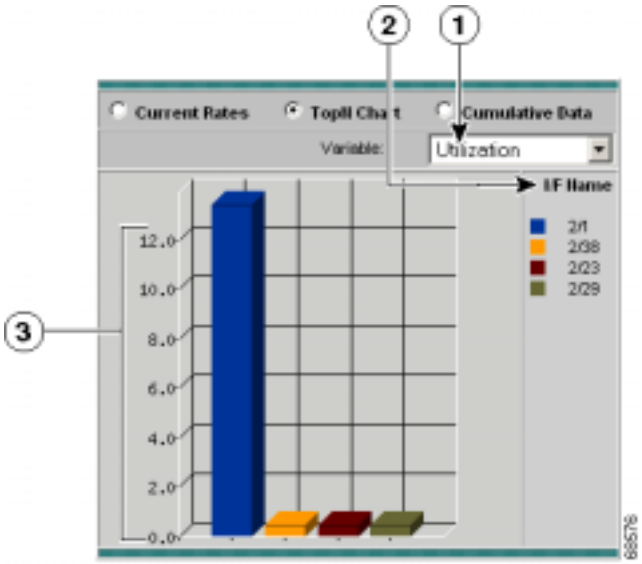
Interface Stats TopN Chart を使用して、インターフェイスごとに収集されたさまざまなデータをグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。

Interface Stats TopN Chart を表示するには、次の手順を実行します。

ステップ 1　TopN Chart オプション ボタンをクリックします。

Interface Stats TopN Chart（図 4-46）が表示されます。

図 4-46　Interface Stats TopN Chart



1	変数リスト	3	インターフェイスごとの変数の値（1 秒あたり）
2	Top N インターフェイス		

ステップ 2　Variable リストから、次のいずれかを選択します。

- In Packets/s：収集された 1 秒あたりのパケット数に基づいてインターフェイス番号がソートされます。
- Out Packets/s：送信された 1 秒あたりのパケット数に基づいてインターフェイス番号がソートされます。
- In Bytes/s：収集された 1 秒あたりのバイト数に基づいてインターフェイス番号がソートされます。
- Out Bytes/s：送信された 1 秒あたりのバイト数に基づいてインターフェイス番号がソートされます。
- In Non-Unicast Pkts/s：収集された 1 秒あたりの非ユニキャスト パケット数に基づいてインターフェイス番号がソートされます。
- Out Non-Unicast Pkts/s：送信された 1 秒あたりの非ユニキャスト パケット数に基づいてインターフェイス番号がソートされます。
- In Errors/s：収集された 1 秒あたりのエラー数に基づいてインターフェイス番号がソートされます。

- Out Errors/s：送信された 1 秒あたりのエラー数に基づいてインターフェイス番号がソートされます。
- In Discards/s：収集された 1 秒あたりの破棄数に基づいてインターフェイス番号がソートされます。
- Out Discards/s：送信された 1 秒あたりの破棄数に基づいてインターフェイス番号がソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

Port Stats Cumulative Data テーブルの表示

Port Stats Cumulative Data テーブルを使用して、スイッチで収集されたさまざまなデータを表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Port Stats Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　Cumulative Data オプション ボタンをクリックします。

Port Stats Cumulative Data テーブル（表 4-53）が表示されます。Traffic Rates を選択した場合は、エラーの合計数のフィールドと共にトラフィック データだけが表示されます。Error Rates を選択した場合は、Port Name フィールドと Utilization フィールド、および各エラー タイプのフィールドが表示されます。すべてのトラフィック レートとすべてのエラーを同時に表示するには、All を選択します。

表 4-53　Port Stats Cumulative Data テーブル

フィールド	説明
Port Name	ポート番号
Utilization	ポートの使用率
Bytes	ポートで収集されたバイト数
Packets	ポートで収集されたパケット数
Broadcast Packets	収集されたブロードキャスト パケット数
Multicast Packets	収集されたマルチキャスト パケット数
Errors	すべてのエラーの合計数 **（注）** このフィールドは、Traffic Rates を選択した場合にだけ表示されます。
Dropped Events	ドロップされたイベント数
CRC Align Errors	収集された CRC Align エラー数
Undersize packets	長さが 64 オクテット未満の収集されたパケット数
Oversize Packets	長さが 1518 オクテット以上の収集されたパケット数
Fragments	長さが 64 オクテット未満で、不正な Frame Check Sequence（FCS）を持つ、収集されたパケット数

表 4-53　Port Stats Cumulative Data テーブル（続き）

フィールド	説明
Jabbers	長さが 1518 オクテット以上で、不正な Frame Check Sequence（FCS）を持つ、収集されたパケット数
Collisions	Ethernet セグメントで収集された衝突数

ステップ 2　テーブルのデータをリフレッシュするには、**Refresh** をクリックします。

ステップ 3　フィルタリングするポート名を Port Name テキスト ボックスに入力して、**Filter** をクリックします。

指定したポート名が表示されます。

Interface Stats Cumulative Data テーブルの表示

Interface Stats Cumulative Data テーブルを使用して、ルータで収集されたさまざまなデータを表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

Interface Stats Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　Cumulative Data オプション ボタンをクリックします。

Interface Stats Cumulative Data テーブル（表 4-54）が表示されます。

表 4-54　Interface Stats Cumulative Data テーブル

フィールド	説明
Interface	インターフェイス番号
In Packets/s	収集された 1 秒あたりのパケット数
Out Packets/s	送信された 1 秒あたりのパケット数
In Bytes/s	収集された 1 秒あたりのバイト数
Out Bytes/s	送信された 1 秒あたりのバイト数
In Non-Unicasts/s	収集された 1 秒あたりの非ユニキャスト数
Out Non-Unicasts/s	送信された 1 秒あたりの非ユニキャスト数
In Discards/s	収集された 1 秒あたりの破棄数
Out Discards/s	送信された 1 秒あたりの破棄数
In Errors/s	収集された 1 秒あたりのエラー数
Out Errors/s	送信された 1 秒あたりのエラー数

ステップ 2　テーブルのデータをリフレッシュするには、**Refresh** をクリックします。

ステップ 3　フィルタリングするインターフェイス名を Filter テキスト ボックスに入力して、**Filter** をクリックします。

指定したインターフェイス名が表示されます。

インターフェイスの詳細の表示

特定のインターフェイスのパケット分布の詳細を表示するには、Interface カラムでインターフェイス番号をクリックします。詳細ウィンドウが表示され、指定したインターフェイスの合計パケット分布を示すチャートが表示されます。

システム状態の表示

NAM Traffic Analyzer を使用して、システム状態のデータを表示できます。スイッチまたはルータで収集されたシステム状態のデータを表示するには、**Monitor** > **Router** または **Monitor** > **Switch** の順に選択し、Content メニューから **Health** を選択します。

デバイスのタイプに応じて、次のいずれかのウィンドウが表示されます。

- Switch Health
- Router Health

Switch Health

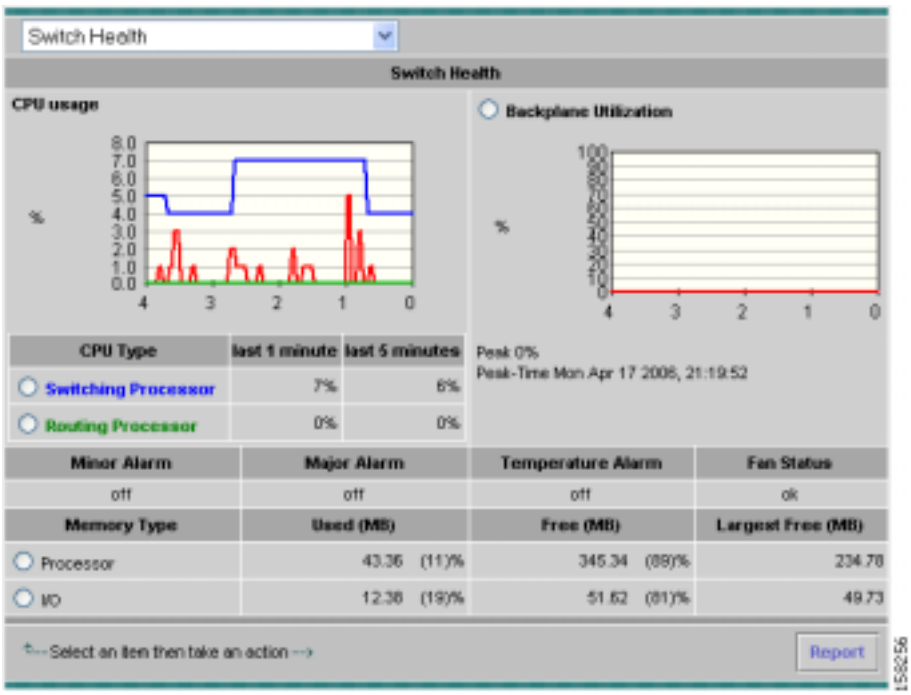
Switch Health ウィンドウは、次のオプションを提供するドロップダウン メニューと共に表示されます。

- Switch Health
- Switch Information
- Crossbar Switching Fabric
- Ternary Content Addressable Memory 情報

Switch Health

Switch Health ウィンドウ（図 4-47）には、2 つの Real-Time グラフが表示されます。

図 4-47　Switch Health ウィンドウ



直前の 5 分以内の CPU 使用率（CPU usage）

CPU Type

- last 1 minute（%）
- last 5 minutes（%）

トラフィック帯域幅（Traffic Bandwidth）

- Peak（%）
- Peak-Time（たとえば、Mon Nov 29 2004, 15:26:55）

Switch Health ウィンドウには、次の情報を含むマトリクスも表示されます。

- マイナー アラーム（Minor Alarm）（on、off）
- メジャー アラーム（Major Alarm）（on、off）
- 温度アラーム（Temperature Alarm）（on、off）
- ファンの状態（Fan Status）（other、ok、minorFault、majorFault、unknown）

表 4-55　スイッチのメモリ情報

カラム	説明
Memory Type	DRAM、FLASH、NVRAM、MBUF、CLUSTER、MALLOC など、メモリのタイプ
Used	特定のメモリ タイプで使用されている MB 数
Free	特定のメモリ タイプの空き MB 数
Largest Free	特定のメモリ タイプの連続した最大空き MB 数

Switch Information

Switch Information ウィンドウ（図 4-48）が表示されます。

図 4-48　Switch Information ウィンドウ

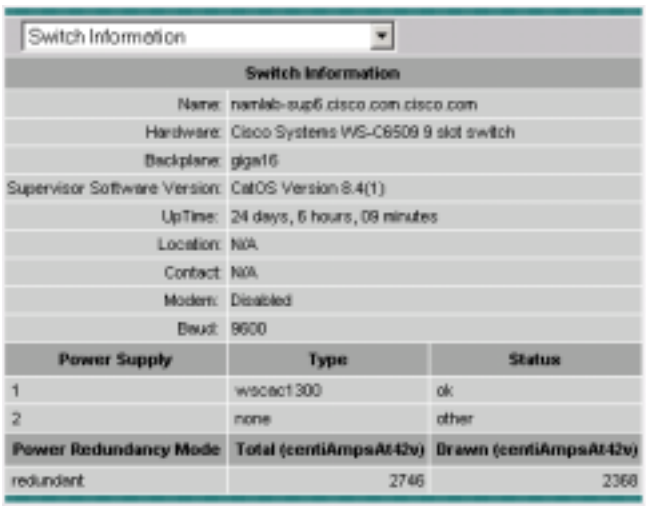


表 4-56　Switch Information

フィールド	説明
Name	管理者がこの管理対象ノードに割り当てた名前。これは、ノードの完全修飾ドメイン名です。
Hardware	物理エンティティの製造業者の名前を含み、物理エンティティのバージョンまたはモデルごとに固有の値に設定される必要のある説明。
Backplane	シャーシのバックプレーン タイプ。
Supervisor Software Version	システムのソフトウェア オペレーティングシステムおよびネットワーキング ソフトウェアの完全な名前とバージョン識別情報。
UpTime	システムのネットワーク管理部分が最後に再初期化されてからの時間（100 分の 1 秒単位）。
Location	このノードの物理的な場所。
Contact	この管理対象ノードの担当者の識別情報、およびその担当者への連絡方法に関する情報。
Modem	RS-232 ポートのモデム制御回線がイネーブルであるかどうかを示します。
Baud rate	RS-232 ポートのボー レート（ビット / 秒）。
Power Supply	取り付けられている電源の説明。
Power Supply Type	電源のタイプ： unknown ac dc externalPowerSupply internalRedundant
Power Supply Status	取り付けられている電源の現在の状態： 1：normal 2：warning 3：critical 4：shutdown 5：notPresent 6：notFunctioning
Power Redundancy Mode	電源の冗長モード： 電源の冗長モード 1：not supported 2：redundant 3：combined
Power Total	FRU に使用できる総電流。 冗長モードが redundant の場合、使用できる総電流は、2 つの電源のうち電力供給能力の小さい方の電源の能力となります。 冗長モードが combined の場合、使用できる総電流は、稼動しているすべての電源の容量の合計となります。
Power Drawn	電源の入っている FRU が得た電流の合計。

Crossbar Switching Fabric

このオプションは、クロスバー スイッチング ファブリック情報を表示します。

表 4-57　Crossbar Switching Fabric 情報

フィールド	説明
Crossbar Switching Fabric	モジュールに関する物理的な構成情報： **Active slot**：アクティブなスイッチング ファブリック モジュールのスロット番号を示します。値が 0 の場合、アクティブなスイッチング ファブリック モジュールの電源が入っていないか、シャーシに存在しないことを示します。 **Backup slot**：バックアップ スイッチング ファブリック モジュールのスロット番号を示します。値が 0 の場合、バックアップ スイッチング ファブリック モジュールの電源が入っていないか、シャーシに存在しないことを示します。 **Bus Only Mode Allowed**：各モジュールの値を決定します。True にセットした場合、どのモジュールもバス専用モードで実行できます。False にセットした場合、モジュールをバス専用モードで実行できません（ファブリックに対応していないモジュールの電源はすべて遮断されます）。ファブリック モジュールがないと、ファブリック対応モジュールの電源はすべて遮断されます。 **Truncated Mode Allowed**：デバイスで管理用に短縮モードがイネーブルになっているかどうかを示します。
Module Switching Mode	モジュールのスイッチング モード： **busmode**：モジュールはファブリックを使用しません。バックプレーンが使用して検索とデータ転送を行います。 **crossbarmode**：モジュールはバックプレーンを使用して転送を判別し、ファブリックを使用してデータ転送します。 **dcefmode**：モジュールはファブリックを使用して、データ転送とローカル転送をイネーブルにします。
Module-Channel	モジュールのスロット番号。
Module-Status	モジュールのファブリック チャネルの状態。
Fabric Status	スロットのファブリック チャネルの状態。
Speed (MB)	モジュールのスピード（MB/ 秒）。
Module-Channel	モジュールのチャネル。
In Errors	このエントリが最後に初期化されてから受信したエラー パケットの合計数。
Our Errors	このエントリが最後に初期化されてから送信されたエラー パケットの合計数。
Dropped	このエントリが最後に初期化されてから送信された、ドロップされたパケットの合計数。
In Utilization (%)	モジュールのチャネルの入力使用率。
Our Utilization (%)	モジュールのチャネルの出力使用率。

Ternary Content Addressable Memory 情報

Ternary Content Addressable Memory（TCAM）（図 4-49）の使用状況の情報を表示します。表 4-58 に、TCAM 情報の一覧を示して説明します。

図 4-49　Ternary Content Addressable Memory 情報

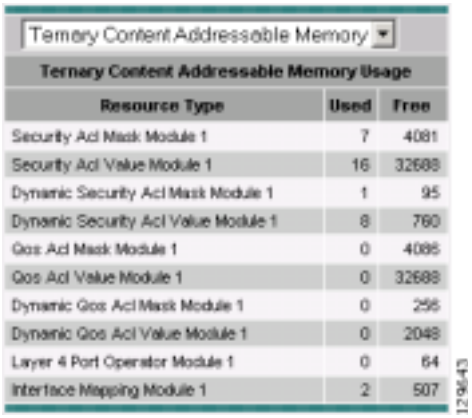


表 4-58　Ternary Content Addressable Memory 情報

フィールド	説明
Security Acl Mask	ACL マスクを格納するために TCAM 領域が割り当てられていることを示します。
Security Acl Value	ACL 値を格納するために TCAM 領域が割り当てられていることを示します。
Dynamic Security Acl Mask	ACL マスクを動的に格納するために TCAM 領域が割り当てられていることを示します。
Dynamic Security Acl Value	ACL 値を動的に格納するために TCAM 領域が割り当てられていることを示します。
Qos Acl Mask	QoS マスクを格納するために TCAM 領域が割り当てられていることを示します。
Qos Acl Value	QoS 値を格納するために TCAM 領域が割り当てられていることを示します。
Dynamic Qos Acl Mask	QoS マスクを動的に格納するために TCAM 領域が割り当てられていることを示します。
Dynamic Qos Acl Value	ACL 値を動的に格納するために TCAM 領域が割り当てられていることを示します。
Layer 4 Port Operator	レイヤ 4 ポート演算子のために TCAM 領域が割り当てられていることを示します。
Interface Mapping Module	インターフェイス マッピングのために TCAM 領域が割り当てられていることを示します。

Router Health

デバイスがルータである場合、次のオプションを提供するドロップダウン ボックスと共に Router Health ウィンドウが表示されます。

- Router Health
- Router Information

Router Health

Router Health ウィンドウには、Real-Time グラフおよびルータの状態に関する情報が表示されます（図 4-50 を参照してください）。表 4-59 に、Router Health ウィンドウの内容を示します。

図 4-50　Router Health ウィンドウ

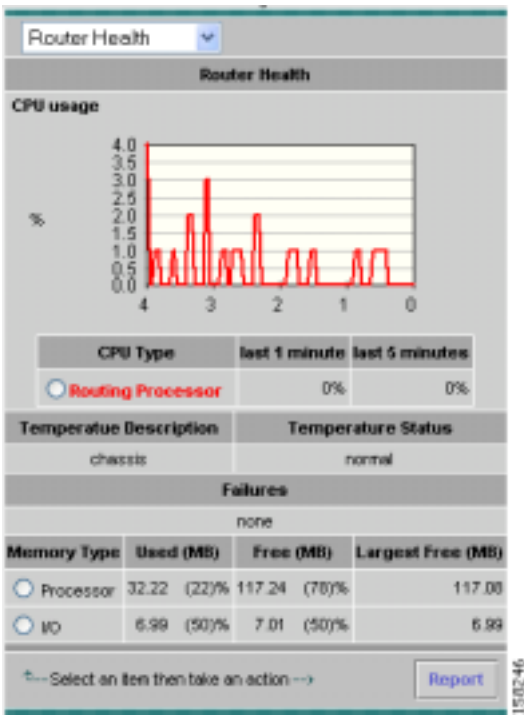


表 4-59　Router Health 情報

フィールド	説明
CPU Usage (graph)	直前 5 分間の全般的な CPU 使用率。
CPU Type	監視対象 CPU のタイプ。
Last 1 minute	直前 1 分間の全般的な CPU 使用率。
Last 5 minutes	直前 5 分間の全般的な CPU 使用率。
Temperature Description	測定対象テスト ポイントの説明。

表 4-59　Router Health 情報（続き）

フィールド	説明
Temperature Status	取り付けられているテスト ポイントの現在の状態。状態は、次のいずれかです。 • Normal • Warning • Critical • Shutdown • Not Present • Not Functioning • Unknown
Failures	取り付けられている電源で障害が発生しているコンポーネント。 • None：障害なし。 • inputVoltage：いずれかの電源の入力パワーが失われました。 • dcOutputVoltage：いずれかの電源の DC 出力電圧が失われました。 • Thermal：熱による電源の障害。 • Multiple：複数の障害。 • Fan：ファンの故障。 • Overvoltage：過電圧。
Memory Type	processor や I/O など、メモリのタイプ。
Used	特定のメモリ タイプで使用されている MB 数。
Free	特定のメモリ タイプの空き MB 数。
Largest Free	特定のメモリ タイプの連続した最大空き MB 数。

Router Information

Router Information ウィンドウ（図 4-51）にはルータの情報が表示されます。表 4-60 に、Router Information ウィンドウのフィールドの一覧を示して説明します。

図 4-51　Router Information ウィンドウ

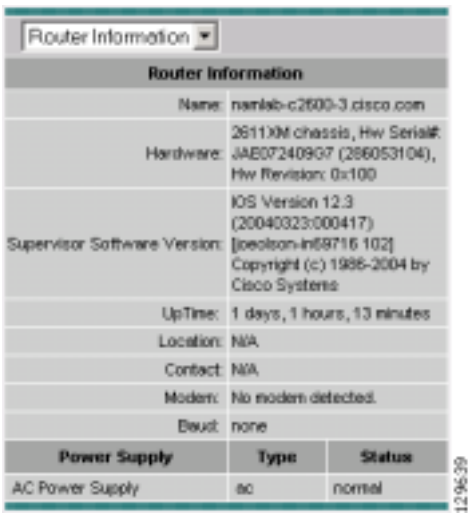


表 4-60　Router Information

フィールド	説明
Name	管理者がこの管理対象ノードに割り当てた名前。これは、ノードの完全修飾ドメイン名です。
Hardware	物理エンティティの製造業者の名前を含み、物理エンティティのバージョンまたはモデルごとに固有の値に設定される必要のある説明。
Supervisor Software Version	システムのソフトウェア オペレーティングシステムおよびネットワーキング ソフトウェアの完全な名前とバージョン識別情報。
Up Time	システムのネットワーク管理部分が最後に再初期化されてからの時間（100 分の 1 秒単位）。
Location	このノードの物理的な場所。
Contact	この管理対象ノードの担当者の識別情報、およびその担当者への連絡方法に関する情報。
Modem	RS-232 ポートのモデム制御回線がイネーブルであるかどうかを示します。
Baud	RS-232 ポートのボー レート（ビット / 秒）。
Power Supply	取り付けられている電源の説明。
Power Supply Type	電源のタイプ： unknown ac dc externalPowerSupply internalRedundant
Power Supply Status	取り付けられている電源の現在の状態。 1：normal 2：warning 3：critical 4：shutdown 5：notPresent 6：notFunctioning

NBAR の表示

NAM Traffic Analyzer を使用して、Network Based Application Recognition（NBAR）データを表示できます。スイッチまたはルータで収集された NBAR データを表示するには、**Monitor** > **Router** または **Switch** > **NBAR** の順に選択します。

上部に 3 つのオプション ボタンがある NBAR Current Rates テーブルが表示されます。

次の用途に応じて、オプション ボタンをクリックできます。

- NBAR Current Rates テーブルの表示（P.4-98）
- NBAR TopN Chart の表示（P.4-99）
- NBAR Cumulative Data テーブルの表示（P.4-100）

NBAR Current Rates テーブルの表示

NBAR Current Rates テーブルを使用して、デバイスで収集されたプロトコル データを表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

NBAR Current Rates テーブルを表示するには、次の手順を実行します。

ステップ 1　Current Rates オプション ボタンをクリックします。

NBAR Current Rates テーブル（表 4-61）が表示されます。

表 4-61　NBAR Current Rates テーブル

フィールド	説明
Protocol/s	プロトコル タイプ
In Packets/s	収集された 1 秒あたりのパケット数
Out Packets/s	送信された 1 秒あたりのパケット数
In Bytes/s	収集された 1 秒あたりのバイト数
Out Bytes/s	送信された 1 秒あたりのバイト数
In Bit rate/s	1 秒あたりの着信ビット レート
Out Bit rate/s	1 秒あたりの発信ビット レート

ステップ 2　（オプション）フィルタリングするプロトコル名を Filter テキスト ボックスに入力して、**Filter** をクリックします。

指定したプロトコルが表示されます。

ステップ 3　（オプション）ドロップダウン ボックスでインターフェイス名を選択します。

指定したインターフェイスが表示されます。

ステップ 4　（オプション）プロトコルを選択し、Real-Time をクリックします。

指定したプロトコルの Real-Time グラフが表示されます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

NBAR TopN Chart の表示

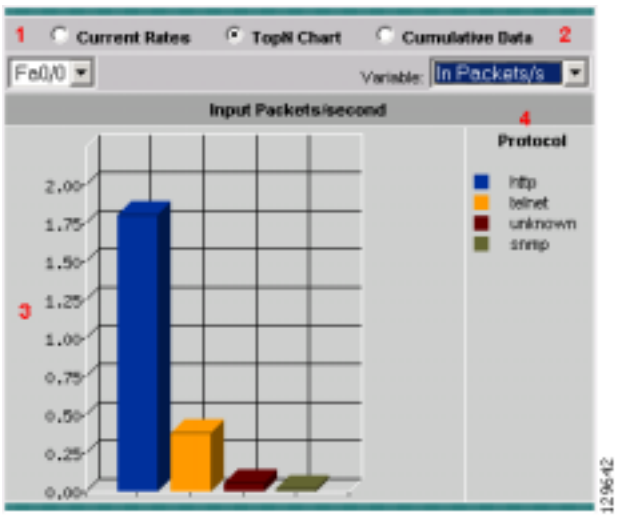
NBAR TopN Chart を使用して、プロトコルごとに収集されたさまざまなデータをグラフ形式で表示できます。表示される情報は、直前のインターバルで収集された 1 秒あたりのデータを表します。

NBAR TopN Chart を表示するには、次の手順を実行します。

ステップ 1　TopN Chart オプション ボタンをクリックします。

NBAR TopN Chart（図 4-52）が表示されます。

図 4-52　NBAR TopN Chart



1	インターフェイスのリスト（たとえば、Fa0/0）	3	プロトコルごとの変数の値（1 秒あたり）
2	変数のリスト（In Packets/s、Out Packets/s、In Bytes/s、Out Bytes/s、In Bit Rate、Out Bit Rate）	4	TopN プロトコル

ステップ 2　Interface リストからインターフェイスを選択します。

ステップ 3　Variable リストから、次のいずれかを選択します。

- In Packets/s：1 秒あたりの着信パケット数に基づいてインターフェイス番号がソートされます。
- Out Packets/s：1 秒あたりの発信パケット数に基づいてインターフェイス番号がソートされます。
- In Bytes/s：1 秒あたりの着信バイト数に基づいてインターフェイス番号がソートされます。
- Out Bytes/s：1 秒あたりの発信バイト数に基づいてインターフェイス番号がソートされます。
- In Bit Rate：着信ビット レートに基づいてインターフェイス番号がソートされます。
- Out Bit Rate：発信ビット レートに基づいてインターフェイス番号がソートされます。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

NBAR Cumulative Data テーブルの表示

NBAR Cumulative Data テーブルを使用して、スイッチまたはルータで収集されたさまざまなデータを表示できます。表示される情報は、収集が作成されてから、または NAM が再起動されてから収集された合計データを表します。インターバルの設定の詳細については、P.3-68 の「グローバル プリファレンスの設定」を参照してください。

NBAR Cumulative Data テーブルを表示するには、次の手順を実行します。

ステップ 1　Cumulative Data オプション ボタンをクリックします。

NBAR Cumulative Data テーブル（表 4-62）が表示されます。

表 4-62　NBAR Cumulative Data テーブル

フィールド	説明
Protocol	プロトコルの名前
In Packets/s	収集された 1 秒あたりのパケット数
Out Packets/s	送信された 1 秒あたりのパケット数
In Bytes/s	収集された 1 秒あたりのバイト数
Out Bytes/s	送信された 1 秒あたりのバイト数
In Bit rate/s	1 秒あたりの着信ビット レート
Out Bit rate/s	1 秒あたりの発信ビット レート

ステップ 2　（オプション）フィルタリングするプロトコル名を Filter テキスト ボックスに入力して、**Filter** をクリックします。

指定したプロトコルが表示されます。

ステップ 3　（オプション）ドロップダウン ボックスでインターフェイス名を選択します。

指定したインターフェイスが表示されます。

ステップ 4　（オプション）プロトコルを選択し、Real-Time をクリックします。

指定したプロトコルの Real-Time グラフが表示されます。

MPLS トラフィック統計情報の表示

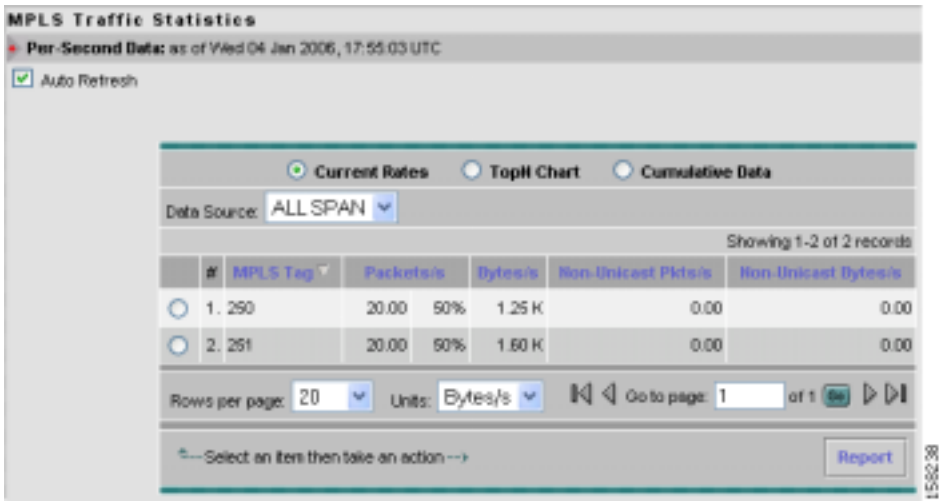
MPLS タグを含むデータ パケットが NAM にスパンされる場合、データ パケット内部のタグを使用してトラフィックを監視できます。この機能は、MPLS タグで各 VPN を固有に識別する MPLS/VPN を展開するネットワークの場合に、特に役立ちます。NAM はスタックされた MPLS タグを検出すると、最も内側の関連するタグだけを監視に使用します。

すべてのラベルの表示

MPLS トラフィック統計情報を表示するには、**Monitor** > **MPLS** をクリックします。GUI にデフォルト表示の Current Rates テーブルが表示されます。他の表示形式として TopN Chart または Cumulative Data を選択することもできます。

図 4-53 に、NAM データ ポートから受信した MPLS タグ付きトラフィックをすべて表示する MPLS Traffic Statistics を示します。

図 4-53　MPLS トラフィック統計情報の表示



MPLS タグによるトラフィック統計情報

VLAN の監視と同様に、トラフィック統計情報をタグで分類して表示できます。MPLS タグ付きトラフィック統計情報は、次の項目で監視できます。

- パケットの合計数
- バイトの合計数
- 非ユニキャスト パケットの合計数
- 非ユニキャスト バイトの合計数

カスタム RMON データ ソース

RMON による監視をイネーブルにするには、最初にデータ ソースを設定する必要があります。MPLS トラフィックの監視をイネーブルにするには、仮想インターフェイスの形式を作成して、特定の MPLS タグに関連付けます。特定の MPLS タグ選択して、そのタグ用にカスタム データ ソースを作成できます。

MPLS タグによるアプリケーションの監視

カスタム データ ソースを作成したら、そのデータ ソースでアプリケーションの監視をイネーブルにすることができます。この機能によって、特定の MPLS タグを使用すれば、伝達されるアプリケーションを見通せるようになります。

MPLS タグによるホストの監視

カスタム データ ソースを作成したら、このデータ ソースでホストの監視をイネーブルにすることができます。この機能によって、特定の MPLS タグを使用すれば、ホストの生成するトラフィックを見通せるようになります。

MPLS タグによるホスト会話の監視

カスタム データ ソースを作成したら、このデータ ソースでホスト会話の監視をイネーブルにすることができます。この機能によって、特定の MPLS タグを使用すれば、伝達されるホスト会話を見通せるようになります。

VRF および VC 統計情報の表示

VRF と VC 統計情報は、同じ形式で表示されます（図 4-54 を参照）。

図 4-54　VRF/VC Statistics

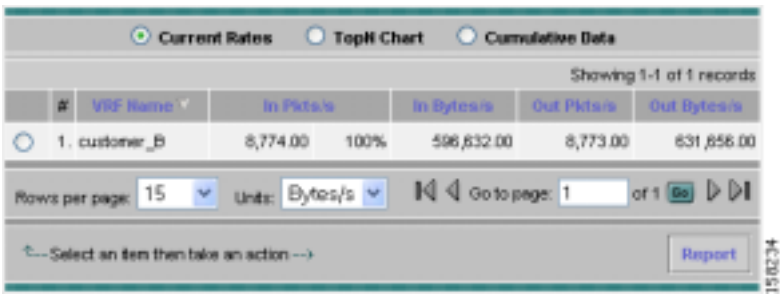


表 4-63 に、VRF/VC Statistics ウィンドウのフィールドの説明を示します。

表 4-63　VRF/VC Statistics ウィンドウ

フィールド	説明
VRF/VC Name	VRF または VC データ ソースの名前
InPackets	受信したパケット数
In Bytes	受信したバイトの合計数
Out Packets	送達したバイトの合計数
Out Bytes	送達したパケット数

CHAPTER 5

レポートの作成と表示

レポート機能を使用すると、NAM が監視するネットワーク トラフィックに関する 100 日間までの履歴データを保存および取得できます。Reports ウィンドウ（図 5-1）には、基本エクスポート、カスタム エクスポート、およびスケジュールされたエクスポートを作成および表示するためのオプションがあります。Reports ウィンドウのサブメニューには、次のオプションがあります。

- P.5-2 の「基本レポート」。基本履歴レポート用にデータ収集を設定し、これらのレポートをいくつかの形式で表示できます。
- P.5-21 の「カスタム レポート」。カスタム レポートを作成および表示できます。複数の基本レポートを 1 つのカスタム レポートに結合することもできます。
- P.5-24 の「スケジュールされたエクスポート」。レポートを自動的に生成して、電子メールまたは FTP 転送によってエクスポートするようにスケジュールできます。

図 5-1　Reports ウィンドウ

基本レポート

Basic Reports オプションを使用すると、ネットワーク ホストやプロトコル、最もアクティブなホストの TopN リストや最もアクティブなトップ プロトコルの TopN リストなど、特定のターゲットに関するレポートを表示できます。

基本レポートを作成する場合、バックグラウンド プロセスによって定期的にデータ ソースがポーリングされ、データがデータベースに保管されます。ポーリング インターバルは、基本レポートの作成時に設定できます。詳細については、P.5-4 の「基本レポートの作成」を参照してください。

図 5-2 に、Basic Reports ウィンドウの例を示します。

図 5-2　Basic Reports ウィンドウ

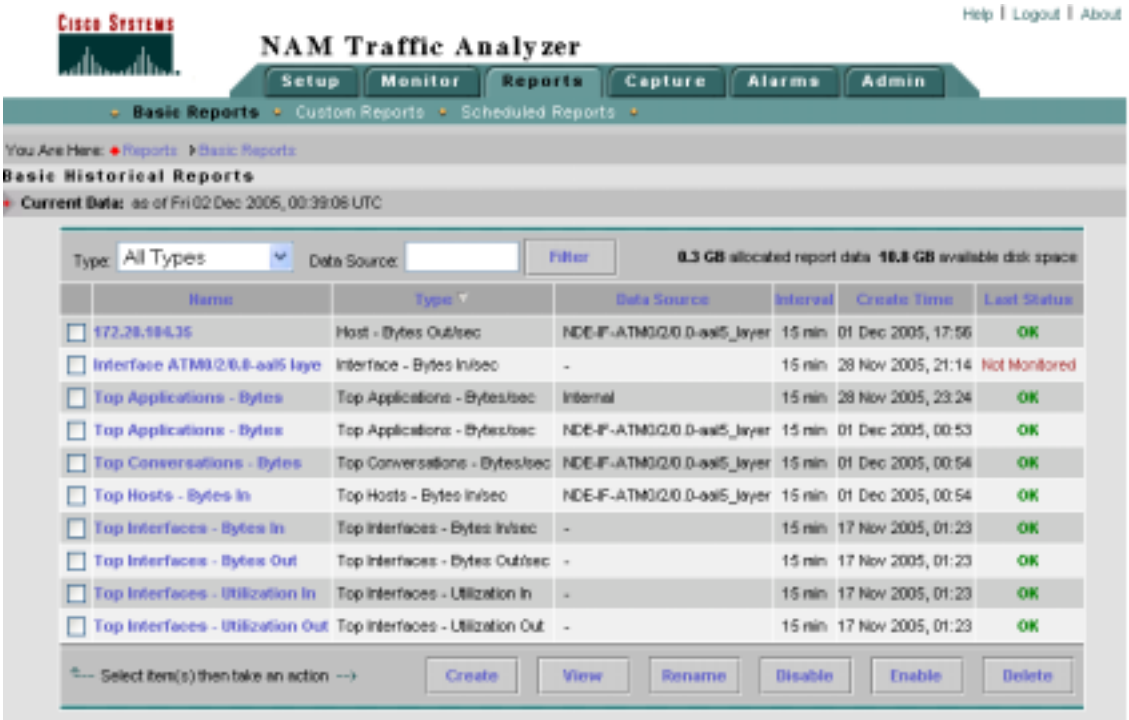


表 5-1 に、Basic Reports ウィンドウのフィールドの一覧を示して説明します。

表 5-1　Basic Reports テーブル

フィールド	説明
Basic Report Type	レポート タイプによってレポートのリストをフィルタリング。
Name	基本レポートの名前。
Type	レポート データのタイプ。
Data Source	レポート データの収集元のデータ ソース。
Interval	レポート データ収集のポーリング インターバル。デフォルトは 15 分です。ポーリングの頻度を高くすると、レポートは細かくなりますが、さらにデータ記憶域が必要になります。
Create Time	レポートの作成時刻。

表 5-1　Basic Reports テーブル（続き）

フィールド	説明
Last Status	• OK：レポートがイネーブルになっていて、データを収集中。 • Disabled：収集中のデータなし。 • Pending：レポートはイネーブルになっているが、収集中のデータなし。 • Inactive Data Source：データ ソースが削除されました。 • No Data：この期間のデータが収集されませんでした。原因として、レポートがディセーブルになっている、NAM が実行されていない、またはレポート データ収集タスクが実行されていないことが考えられます。 • No Activity：NAM はこのターゲットでトラフィック アクティビティを検出していません。これは、非アクティブなターゲットまたはデータ ソース設定の問題によって生じることがあります。 • Not Monitored：NAM またはスイッチ（あるいはその両方）で、このタイプのトラフィック統計情報の監視機能がイネーブルになっていないか、または利用できません。 （注）収集中のデータがない場合は、タイム スタンプに前回の収集が表示されます。

WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスには、デフォルトで作成済みの次のレポートがあります。

- Top ports—bytes per second
- Top ports—packets per second
- Top ports—utilization percentage
- Top ports—packet drops per second
- Top applications—Bytes
- Top Conversations—Bytes
- Top hosts—Bytes in
- Top Hosts—Bytes out

NM-NAM デバイスには、デフォルトで作成済みの次のレポートがあります。

- Top interfaces—bytes in
- Top interfaces—bytes out
- Top interfaces—utilization percentage in
- Top interfaces—utilization percentage out
- Top applications—Bytes
- Top Conversations—Bytes
- Top hosts—Bytes in
- Top Hosts—Bytes out

（注）レポートを実行しているデータ　ソースで収集をオフにした場合、レポート機能によって自動的に収集がオンに戻されます。

次の項では、基本レポートを管理する方法について説明します。

- 基本レポートの作成（P.5-4）
- 基本レポートの表示（P.5-17）
- レポート名の変更（P.5-20）
- レポートのイネーブル化（P.5-20）
- レポートのディセーブル化（P.5-20）
- レポートの削除（P.5-20）

基本レポートをカスタマイズおよび結合して、カスタム レポートを作成できます。カスタム レポートの詳細については、P.5-21 の「カスタム レポート」を参照してください。

基本レポートの作成

レポートを作成する前に、適切なネットワーク トラフィックが NAM に送信され、監視機能が統計情報およびデータ ソースのタイプに対してイネーブルになっていることを確認してください。監視機能をイネーブルにする方法の詳細については、P.3-34 の「監視のセットアップ」を参照してください。

基本レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスを使用して、次のレポートを作成できます。

- アプリケーション：P.5-5 の「アプリケーション レポートの作成」を参照
- アプリケーション グループ：P.5-7 の「アプリケーション グループ レポートの作成」を参照
- ホスト：P.5-7 の「ホスト レポートの作成」を参照
- 会話：P.5-9 の「会話レポートの作成」を参照
- VLAN：P.5-10 の「VLAN レポートの作成」を参照
- Differentiated Services：P.5-11 の「DiffServ レポートの作成」を参照
- 応答時間：P.5-12 の「応答時間レポートの作成」を参照
- スイッチ ポート：P.5-13 の「スイッチ ポート レポートの作成」を参照
- スイッチ状態：P.5-14 の「スイッチ状態レポートの作成」を参照
- MPLS：P.5-16 の「MPLS レポートの作成」を参照

NM-NAM デバイスを使用して、次のレポートを作成できます。

- アプリケーション：P.5-5 の「アプリケーション レポートの作成」を参照
- アプリケーション グループ：P.5-7 の「アプリケーション グループ レポートの作成」を参照
- ホスト：P.5-7 の「ホスト レポートの作成」を参照
- 会話：P.5-9 の「会話レポートの作成」を参照
- Differentiated Services：P.5-11 の「DiffServ レポートの作成」を参照
- 応答時間：P.5-12 の「応答時間レポートの作成」を参照
- ルータ インターフェイス：P.5-15 の「ルータ インターフェイス レポートの作成」を参照

- MPLS：P.5-16 の「MPLS レポートの作成」を参照

ステップ 3　レポート タイプを選択して **Next** をクリックします。

ステップ 4　選択したレポート タイプに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

図 5-3　基本履歴レポートの作成

アプリケーション レポートの作成

アプリケーション プロトコル レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**Applications** を選択して、**Next** をクリックします。

Create Applications Report ウィンドウが表示されます（図 5-4 を参照）。

図 5-4　Create Application Report ウィンドウ

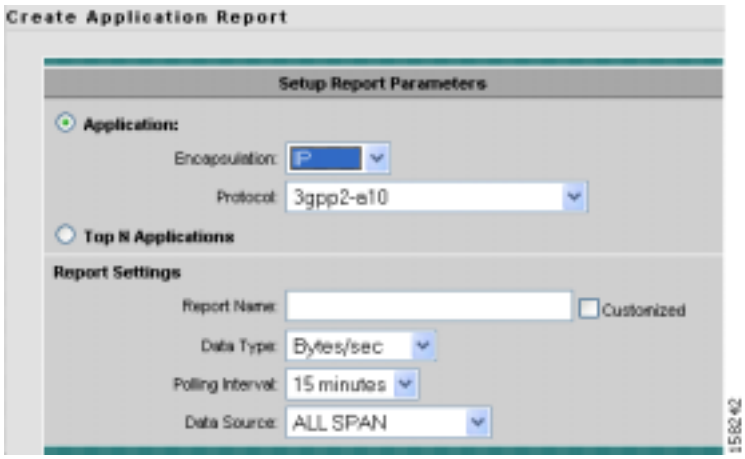


表 5-2 に、アプリケーション レポートのパラメータを示します。

表 5-2　アプリケーション レポートのパラメータ

フィールド	説明	使用法
Application	Application チェックボックス	特定のアプリケーションを選択する場合は、Application（デフォルト）をオンにします（Encapsulation と Protocol）。
Encapsulation	プロトコルのカプセル化タイプ	IP、IPIP4、GRE.IP、IPv6、Others のリストからカプセル化を選択します。
Protocol	アプリケーション プロトコルの名前	リストからプロトコルを選択します。
TopN Applications	1 秒あたりのバイト数または 1 秒あたりのパケット数に基づく、最もアクティブなアプリケーション プロトコルに関するレポート	最もアクティブなアプリケーションに関するレポートを作成する場合は、TopN Applications をオンにします。
Report Settings		
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** を選択してから名前を入力します。
Data Type	データのタイプ	リストからタイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。

ステップ 4　アプリケーション レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

アプリケーション グループ レポートの作成

アプリケーション グループ レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** を選択します。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　Application Group タイプを選択して **Next** をクリックします。

Create Application Group Report Parameters ダイアログボックスが表示されます。表 5-3 に、アプリケーション グループ レポートのパラメータを示します。

表 5-3　アプリケーション グループ レポートのパラメータ

フィールド	説明	使用法
Application Group	アプリケーション グループの名前	
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** を選択してから名前を入力します。
Data Type	データのタイプ	リストからタイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート　データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。

ステップ 4　アプリケーション グループ レポートに必要な必須パラメータを入力します。

ステップ 5　**Finish** をクリックします。

ホスト レポートの作成

ホスト レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　Hosts レポート タイプを選択して **Next** をクリックします。

Create Hosts Report ウィンドウが表示されます（図 5-5 を参照）。

図 5-5　Create Hosts Report ウィンドウ

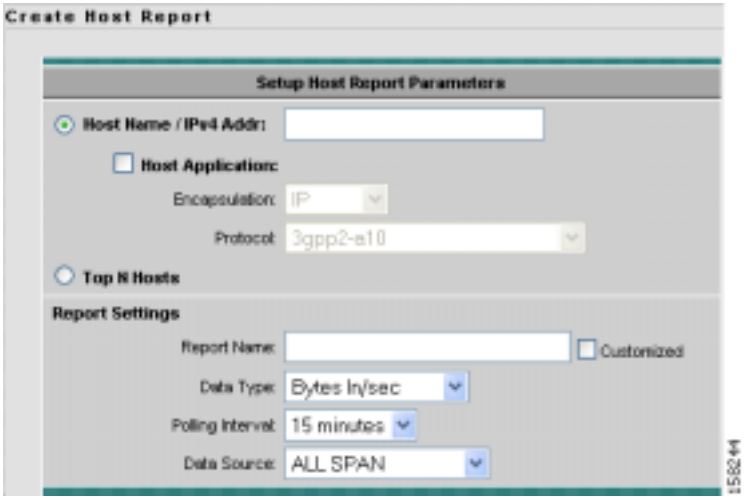


表 5-4 に、ホスト レポートのパラメータを示します。

表 5-4　Hosts Report Parameters ダイアログボックス

フィールド	説明	使用法
Host Name/ IPv4Addr:	データのポーリング元のホスト名	IPv4 ホスト名またはホストのアドレスを入力します。
Host Application	ホストの特定のアプリケーションについてレポートする場合、オン	オンの場合、プロトコルとカプセル化タイプを選択します。
Encapsulation	プロトコルのカプセル化タイプ	リストからカプセル化を選択します。
Protocol	アプリケーション プロトコルの名前	リストからプロトコルを選択します（オプション）。
TopN Hosts	1 秒あたりのバイト数（入力または出力）または 1 秒あたりのパケット数（入力または出力）に基づく、最もアクティブなホスト アドレスに関するレポート	最もアクティブなホストに関するレポートを作成する場合は、TopN Hosts をオンにします。
Report Settings		
Report Name	レポートの名前	レポート名は自動的に生成されます。名前を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	データのタイプ	リストからタイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。

ステップ 4　ホスト レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

会話レポートの作成

会話レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**Conversations** を選択して、**Next** をクリックします。

Create Host Conversation Report ウィンドウが表示されます（図 5-6 を参照）。

図 5-6　Create Host Conversation Report ウィンドウ

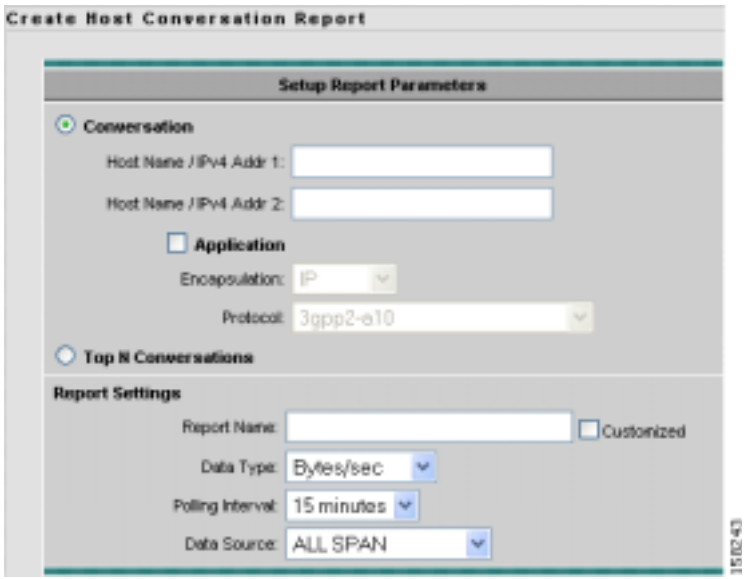


表 5-5 に、会話レポートのパラメータを示します。

表 5-5　会話レポートのパラメータ

フィールド	説明	使用法
Conversation	Conversation チェックボックス	特定のホスト名または IPv4 アドレスを入力する場合、Conversation（デフォルト）をオンにします。
Host 1 および Host 2	レポートする会話ホストの識別	• Host 1：IPv4 ホスト名または host 1 のアドレスを入力します。 • Host 2：IPv4 ホスト名または host 2 のアドレスを入力します。
Encapsulation	プロトコルのカプセル化タイプ	リストからカプセル化を選択します。
Protocol	アプリケーション プロトコルの名前	リストからプロトコルを選択します。

表 5-5　会話レポートのパラメータ（続き）

フィールド	説明	使用法
TopN Conversations	TopN Conversations チェックボックス	1 秒あたりのバイト数または 1 秒あたりのパケット数に基づいて、最もアクティブなホスト会話に関するレポートを作成する場合は、TopN Conversations をオンにします。
Report Settings		
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	データのタイプ	リストからタイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。

ステップ 4　会話レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

VLAN レポートの作成

（注） この項の内容は、NM-NAM デバイスには適用できません。

VLAN レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　VLAN レポート タイプを選択して **Next** をクリックします。

Create VLAN Report Parameters ダイアログボックスが表示されます。表 5-6 に、VLAN レポートのパラメータを示します。

（注） VLAN レポートは、NetFlow データ ソースに対して使用できません。

表 5-6　VLAN レポートのパラメータ

フィールド	説明	使用法
VLAN Number	レポートする VLAN の名前または番号	VLAN の名前または番号を入力します。
Top N VLANs	TopN VLAN をレポート	クリックして、TopN VLAN のレポートを選択します。
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	データのタイプ	リストからタイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。 **（注）** Supervisor エンジン モジュールベースのデータ ソースでは、Supervisor II エンジン モジュール以降が必要です。

ステップ 4　VLAN レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

DiffServ レポートの作成

Differentiated Services（DiffServ）レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**DiffServ** を選択して、**Next** をクリックします。

Create DiffServ Report Parameters ダイアログボックスが表示されます。表 5-7 に、DiffServ のパラメータを示します。

表 5-7　Differentiated Services レポートのパラメータ

フィールド	説明	使用法
DiffServ Information	レポートする Differentiated Services（DiffServ）統計情報の識別	• DiffServ Profile：DiffServ プロファイルの名前を選択します。 • Aggregation Group：集約グループを選択します。 • Encapsulation：Protocol チェックボックスがオンになっている場合、リストからカプセル化を選択します。 • Protocol：Protocol チェックボックスがオンになっている場合、リストからプロトコルを選択します。 • Host Name：Host チェックボックスがオンになっている場合、IPv4 ホスト名またはホストのアドレスを入力します（オプション）。
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	データのタイプ	リストからタイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。 **（注）** NetFlow をデータ ソースとして利用することはできません。

ステップ 4　DiffServ レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

応答時間レポートの作成

アプリケーション応答時間レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** を選択します。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**Response Time** を選択して、**Next** をクリックします。

Create Response Time Report Parameters ダイアログボックスが表示されます。表 5-8 に、応答時間レポートのパラメータを示します。

表 5-8　応答時間レポートのパラメータ

フィールド	説明	使用法
Target	レポートするアプリケーション応答時間（ART）統計情報の識別	• Encapsulation：リストからカプセル化を選択します。 • Protocol：リストからプロトコルを選択します。 • Server：サーバの名前を入力します。 • Client：クライアントの名前を入力します（オプション）。
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	データのタイプ	リストからデータ タイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	リストからソースを選択します。 **（注）** NetFlow をデータ ソースとして利用することはできません。

ステップ 4　アプリケーション応答時間レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

スイッチ ポート レポートの作成

（注） この項の内容は、NM-NAM デバイスには適用できません。

スイッチ ポート統計情報レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**Switch Port Statistics** を選択して、**Next** をクリックします。

Create Switch Port Statistics Report Parameters ダイアログボックスが表示されます。表 5-9 に、スイッチ ポート統計情報のパラメータを示します。

表 5-9　Switch Port Statistics Report Parameters ダイアログボックス

フィールド	説明	使用法
Switch Module/Port	スイッチ モジュールと、モジュールで利用可能な対応ポートのリスト	レポートを生成するスイッチ モジュールおよびポートを選択します。
Top N Ports	TopN スイッチ ポートをレポート	クリックして、TopN ポートのレポートを選択します。 Supervisor エンジン モジュールで Mini-RMON をイネーブルにする必要があります。
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	レポートするデータのタイプ • バイト / 秒 • パケット / 秒 • 使用率 • ブロードキャスト バイト / 秒 • マルチキャスト バイト / 秒 • ドロップ イベント / 秒	リストからデータ タイプを選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。

ステップ 4　スイッチ ポート統計情報レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

スイッチ状態レポートの作成

（注）　この項の内容は、NM-NAM デバイスには適用できません。

スイッチ状態レポートは、スイッチ状態の統計情報に関する履歴レポートです。スイッチ状態レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**Switch Health** を選択して、**Next** をクリックします。

Create Switch Statistics Report Parameters ダイアログボックスが表示されます。表 5-10 に、スイッチ状態レポートのパラメータを示します。

表 5-10　Switch Statistics Report Parameters ダイアログボックス

フィールド	説明	使用法
Component	レポート対象のコンポーネント	Switch DRAM Memory、Switch Backplane、Switching CPU、または Routing CPU から選択します。
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。
Data Type	レポートするデータのタイプ	選択されたコンポーネントの使用率。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。

ステップ 4　スイッチ統計情報レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

ルータ インターフェイス レポートの作成

（注）　この項の内容は、NM-NAM デバイスにしか適用できません。

ルータ インターフェイス レポートには、ルータのインターフェイス統計情報の履歴が含まれます。ルータ インターフェイス レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**Router Interfaces** を選択して、**Next** をクリックします。

Create Interface Stats Report Parameters ダイアログボックスが表示されます。表 5-11 に、ルータ インターフェイス レポートのパラメータを示します。

表 5-11　ルータ インターフェイス レポートのパラメータ

フィールド	説明	使用法
Interface	インターフェイスのリスト	レポートを生成するインターフェイスを選択します。
Top N Interfaces	TopN インターフェイスをレポート	クリックして、TopN インターフェイスのレポートを選択します。
Report Name	レポートの名前	レポート名は自動的に生成されます。レポート名を変更するには、**Customized** をクリックして、新しい名前を入力します。

表 5-11　ルータ インターフェイス レポートのパラメータ（続き）

フィールド	説明	使用法
Data Type	レポートするデータのタイプ	リストからデータ タイプ（Bytes/sec、Packets/sec、Non-unicasts Packets/sec、Discarded Packets/sec、Error Packets/sec、Utilization）を選択します。
Polling Interval	レポート データをポーリングするインターバル	リストからインターバルを選択します。

ステップ 4　ルータ インターフェイス レポートの作成に必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

MPLS レポートの作成

（注）　この項の内容は、NM-NAM デバイスには適用できません。

MPLS レポートには、MPLS データの集まりが含まれます。特定の MPLS タグに関するレポートをセットアップできます。MPLS レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Basic Reports** をクリックします。

Basic Historical Reports ウィンドウが表示されます。

ステップ 2　**Create** をクリックします。

Create Basic Historical Report ウィンドウが表示されます（図 5-3 を参照）。

ステップ 3　**MPLS** を選択して、**Next** をクリックします。

Create MPLS Report Parameters ダイアログボックスが表示されます。表 5-12 に、MPLS Report Parameters ダイアログボックスを示します。

表 5-12　MPLS レポートのパラメータ

フィールド	説明	使用法
MPLS Tag	特定の MPLS タグ	MPLS タグを入力します。
Report Name	レポートの名前	このレポートの名前を入力するか、または選択した MPLS タグから取得されたデフォルト名を使用します。
Data Type	データのタイプ	Bytes/sec（デフォルト）、Packets/sec、Non-unicast Bytes/sec、または Non-unicast Packets/sec のいずれかを選択します。
Polling Interval	レポート データをポーリングするインターバル	5 分（デフォルト）、15 分、30 分、1 時間、2 時間、4 時間、または 8 時間のいずれかを選択します。
Data Source	レポート データの収集元のネットワーク トラフィック ソース	ALL SPAN が使用可能な唯一のオプションです。

ステップ 4　MPLS レポートに必要なパラメータを入力します。

ステップ 5　**Finish** をクリックします。

基本レポートの表示

レポート データは NAM データベースに 100 日間保存されます。100 日よりも前のレポート データは、新しいレポート データによって順次上書きされます。基本レポートを表示するには、**Reports** > **Basic Reports** をクリックします。

Basic Reports ウィンドウが表示され、データ収集にセットアップされたすべての基本レポートのリストが示されます。図 5-7 を参照してください。

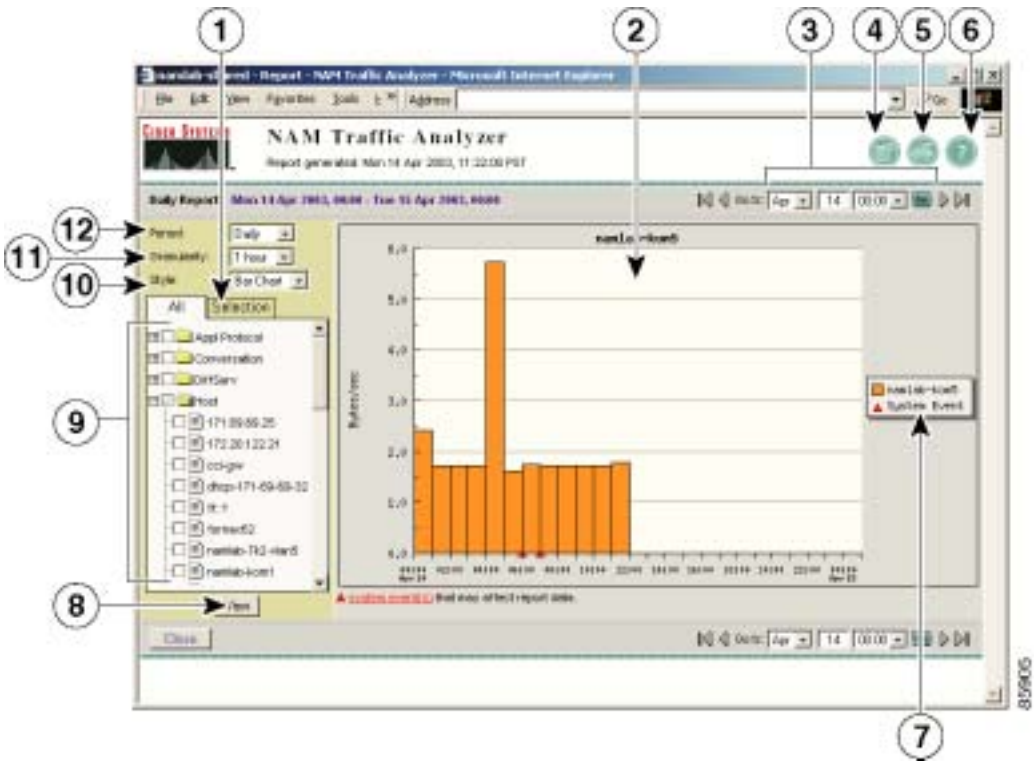
図 5-7　Basic Reports ウィンドウ

レポートの詳細の表示

レポートの詳細を表示するには、Basic Reports ウィンドウでレポート名をクリック、またはレポートを選択してから **View** をクリックします。

図 5-8 に、Application report ウィンドウの例を示します。

図 5-8　レポートの詳細の表示



1	選択したレポートが表示されます。	**7**	レポートの名前。
2	レポートのグラフ。	**8**	クリックすると、選択したレポートが表示されます。
3	表示する期間を指定します。	**9**	表示するターゲット レポートを選択します。
4	レポートをファイルにダウンロードします。	**10**	グラフのスタイル。
5	レポートを印刷します。	**11**	レポートの細かさです。
6	オンライン ヘルプを起動します。	**12**	レポート期間の長さです。

複数のターゲット レポートを選択し、同じグラフに表示できます。単位の異なる複数のレポートを選択した場合、レポート グラフ領域にサブレポートとして表示されます。

(注)　TopN レポートは 1 つだけ選択できます。

レポートの細かさは、レポートのポーリング頻度を超えて指定できません。たとえば、15 分のポーリング インターバルを持つレポートを 5 分の細かさで表示することはできません。ポーリング頻度よりも小さいレポートの細かさを選択した場合、レポート データはポーリング頻度に従って集約されます。

ディセーブルになっているレポート、およびエラー状態のレポートに対しては、レポート セレクタに赤い感嘆符が表示されます。エラー状態のレポートの詳細については、レポートのエラー状態（表 5-13）を参照してください。

表 5-13　レポートのエラー状態

エラー状態	説明
Not Started	この期間に対して、レポートが作成されず、データ収集は開始されていません。
Data Pending	現在の期間のデータは収集中です。
No Data	この期間のデータが収集されませんでした。次の原因が考えられます。 • レポートがディセーブルになっている。 • NAM が実行されていない。 • レポート データ収集タスクが実行されていない。
No Activity	NAM はこのターゲットでトラフィック アクティビティを検出していません。これは、非アクティブなターゲットまたはデータ ソース設定の問題によって生じることがあります。
Not Monitored	NAM またはスイッチ（あるいはその両方）で、このタイプのトラフィック統計情報の監視機能がイネーブルになっていないか、または利用できません。

システム イベント ログの表示

システム イベントは、レポート データ収集に影響を与えます。Reports ウィンドウには赤い三角形で表示されます。記録されるイベントとしては、システムの再起動、SPAN の変更、および、レポートのイネーブル化、ディセーブル化、作成、編集、および削除があります。

System Events Log を表示するには、**system events** をクリックします。System Config Log が表示されます。ログには、システム設定イベント、イベントの時刻、およびユーザが表示されます。表示されたイベントは、レポートの期間に対応しています。たとえば、1 週間分のレポートを表示する場合、System Config Log にはその週に発生したイベントが表示されます。

ヒント

- レポート セレクタでレポート名の上にマウス カーソルを移動すると、そのレポートについての詳細が表示されます。
- レポート　データ収集に関連するエラーまたは例外状態についての数値データおよび情報を表示するには、表形式レポート スタイルを使用します。

レポートのイネーブル化

レポートをイネーブルにして、レポート用のデータをポーリングするバックグラウンド プロセスをアクティブにします。Basic Reports ウィンドウから直接レポートをイネーブルにできます。レポートをイネーブルにするには、リストからレポートを選択し、**Enable** をクリックします。イネーブルにしたレポートは、ディセーブルになるまで実行が継続されます。

（注） Basic Reports テーブルのレポートは、デフォルトでイネーブルになっています。

レポートのディセーブル化

レポートをディセーブルにして、レポート用のデータをポーリングするバックグラウンド プロセスを一時停止します。前に収集したデータを表示することはできますが、データベースに新しいデータは追加されません。Basic Reports ウィンドウから直接レポートをディセーブルにできます。レポートをディセーブルにするには、リストからレポートを選択し、**Disable** をクリックします。

レポート名の変更

ステップ 1　Basic Reports ウィンドウでレポートを選択し、**Rename** をクリックします。

テキスト ウィンドウが表示されます。

ステップ 2　レポートの新しい名前を入力し、次のいずれかを行います。

- 変更を確定するには、**OK** をクリックします。
- 変更を削除し、Basic Reports テーブルに戻るには、**Cancel** をクリックします。

レポートの削除

レポートを削除するには、Basic Reports ウィンドウでレポートを選択し、**Delete** をクリックします。

カスタム レポート

Basic Reports テーブルでレポートを作成した後に、レポートを結合またはカスタマイズできます。次の項では、カスタム レポートを管理する方法について説明します。

- カスタム レポートの作成（P.5-21）
- カスタム レポートの編集（P.5-22）
- カスタム レポートの削除（P.5-22）
- カスタム レポートの表示（P.5-22）

カスタム レポートの作成

カスタム レポートを作成するには、次の手順を実行します。

ステップ 1　**Reports** > **Custom Reports** を選択します。

Custom Reports テーブルが表示されます。

ステップ 2　**Create** をクリックします。

Create Custom Report ダイアログボックス（表 5-14）が表示されます。

表 5-14　Create Custom Report ダイアログボックス

フィールド	使用法
Report Name	カスタム レポートの名前を入力します。
Folder	レポートを格納するフォルダを選択します。
Period	レポート期間の長さを選択します。
Granularity	レポートの日付の細かさを選択します。
Style	グラフのスタイルを選択します。
Report Data	カスタム レポートに含める基本レポートを選択します。ターゲット データのレポート タイプは複数選択できますが、1 つのカスタム レポートに含めることができる TopN レポート タイプは 1 つだけです。 選択したすべてのレポートを表示するには、Selection タブをクリックします。

ステップ 3　次のいずれかを実行します。

- 変更を確定するには、**Submit** をクリックします。
- 変更をクリアするには、**Reset** をクリックします。

新しいフォルダの作成

追加のカスタム レポートの保存用として、Custom Reports テーブルから直接新しいフォルダを作成できます。

ステップ 1　**New Folder** をクリックします。

テキスト ボックスが表示されます。

ステップ 2　フォルダの名前を入力し、**OK** をクリックします。

新しいフォルダが Custom Reports テーブルに表示されます。

カスタム レポートの編集

カスタム レポートを編集するには、次の手順を実行します。

ステップ 1　**Reports** > **Custom Reports** を選択します。

Custom Reports テーブルが表示されます。

ステップ 2　編集するカスタム レポートを選択し、**Edit** をクリックします。

Edit Custom Reports ダイアログボックスが表示されます。

ステップ 3　必要な変更を加えてから、次のいずれかを行います。

- 変更を確定するには、**Submit** をクリックします。
- 設定を元のままにするには、**Reset** をクリックします。

カスタム レポートの削除

カスタム レポートを削除するには、Custom Report ウィンドウでレポートを選択し、**Delete** をクリックします。

カスタム レポートの表示

カスタム レポートを表示するには、次の手順を実行します。

ステップ 1　**Reports** > **Custom Reports** を選択します。

Custom Reports ウィンドウが表示されます。

ステップ 2　表示するカスタム レポートを選択し、**View** をクリックします。

レポートの詳細の表示（図 5-8）が表示されます。

カスタム レポートの別のフォルダへの移動

カスタム レポートを別のフォルダへ移動するには、次の手順を実行します。

ステップ 1　**Reports** > **Custom Reports** をクリックします。

Custom Reports ウィンドウが表示されます。

ステップ 2　編集するカスタム レポートを選択し、**Edit** をクリックします。

Edit Custom Reports ダイアログボックスが表示されます。

ステップ 3　Folder ドロップダウン リストから新しいフォルダを選択し、**Submit** をクリックします。

スケジュールされたエクスポート

Scheduled Exports オプションを使用すると、レポートを自動的に生成して、特定の時間にエクスポートするようにスケジュールできます。レポートの形式は PDF、HTML、CSV、または XML になります。NAM は HTML レポートを電子メールで送信します。その他の形式は、電子メールまたは FTP で送信できます。

レポートのエクスポートのスケジューリング

レポートのエクスポートをスケジュールするには、次の手順を実行します。

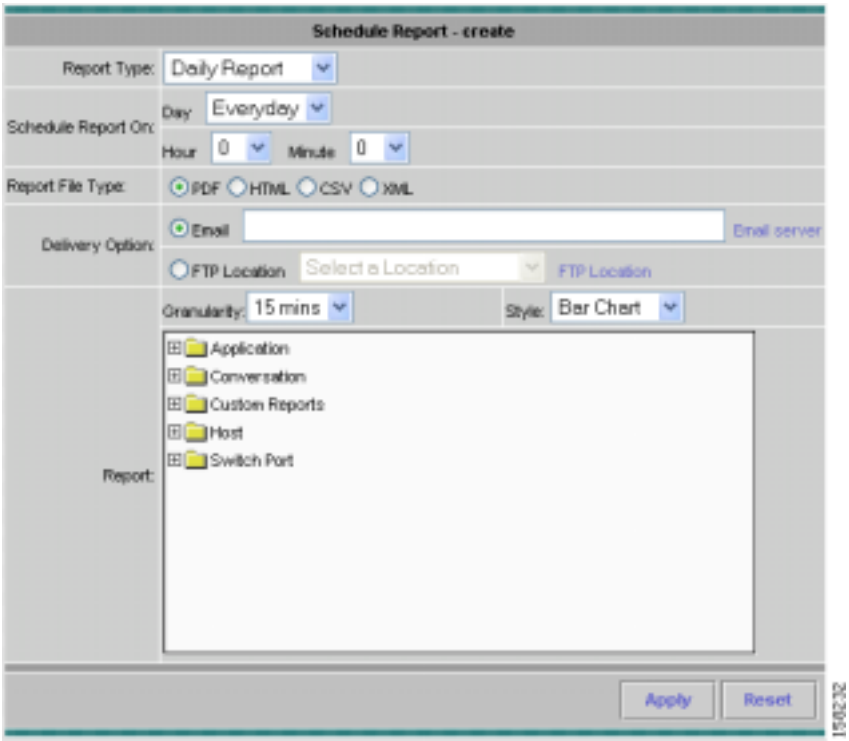
ステップ 1　レポートのエクスポートをスケジュールするためには、まず基本レポートまたはカスタム レポートを作成する必要があります。

レポートの作成の詳細については、P.5-2 の「基本レポート」または P.5-21 の「カスタム レポート」のいずれかを参照してください。

ステップ 2　**Reports** > **Scheduled Exports** をクリックします。

Scheduled Exports ウィンドウが表示されます。図 5-9 に、Scheduled Export ウィンドウの例を示します。

図 5-9　スケジュールされたエクスポートの作成



Scheduled Exports ウィンドウのオプション（表 5-15）に、使用可能な Scheduled Exports のオプションを示します。

表 5-15　Scheduled Exports ウィンドウのオプション

フィールド	説明	使用法
Report Type	レポートのタイプ	Daily、Weekly、Monthly からオプションを選択します。
Schedule Report On	レポートをエクスポートする日時	リストから次のオプションを選択して、レポートをエクスポートする時刻（時間と分）を入力します。 • Daily：レポートは毎日エクスポートされます。 • Weekly：レポートをエクスポートする曜日を選択します。 • Monthly：レポートをエクスポートする日を選択します。それには、特定の日を選択するか、月の初日または月末を選択します。
Report File Type	エクスポートするレポートのファイル形式	レポートは、PDF、HTML、CSV、または XML の 4 つの形式のいずれかでエクスポートできます。
Delivery Option	レポートの送達方法	EMail を選択して、1 つまたは複数の有効な電子メール アドレスをスペースで区切って入力します。 **（注）** さまざまな人物に異なるレポートを送信するようにスケジュールできます。 FTP Location を選択し、ドロップダウン リストから場所を選択します。FTP 送達オプションの設定の詳細については、P.2-16 の「FTP の設定」を参照してください。
Granularity	レポートの頻度	15 分、30 分、1 時間、4 時間、8 時間、12 時間、または 1 日 からオプションを選択します。 Granularity は、レポートに表示されるデータ ポイントの頻度を指定します。たとえば、Daily Report の場合、1 時間ごとのデータ ポイントを 24 回、または 15 分ごとのデータ ポイントを 96 回設定できます。15 分ごとの方が、より細かくなります。
Style	レポートの出力スタイル	Bar Chart、Stack Bar、Line Chart、Area Chart、または Tabular から選択します。
Report	設定されたレポートが含まれるフォルダ	各フォルダには、設定が完了してエクスポートできるレポートが含まれます。

ステップ 3　リストのオプションから Report Type を選択します。

ステップ 4　レポートをエクスポートする日を選択します。

このオプションは、選択した Report Type によって異なります。Daily Report を選択した場合、デフォルト（唯一のオプション）は Every Day です。Weekly Report の場合、レポートを作成する曜日を選択します。Monthly Report の場合、レポートを作成する日を選択します。

ステップ 5　レポートをエクスポートする時刻の時間と分を入力します。

ステップ 6　Report File Type を選択します。

ステップ 7　レポートのエクスポートの Delivery Option をクリックして選択し、電子メール アドレスを入力するか、または FTP Location を選択します。

ステップ 8　Granularity とレポートの Style を選択します。

ステップ 9　Scheduled Export のパラメータを指定した後、スケジュールされたエクスポートを確定するには **Apply** をクリックします。またはスケジュールされたエクスポートを放棄するには **Reset** をクリックします。

レポートのエクスポートの編集

レポートをエクスポートするようにスケジュールした後で、設定を修正することができます。レポートのエクスポートを編集するには、次の手順を実行します。

ステップ 1　**Reports > Scheduled Exports** を選択します。

Schedule Export ウィンドウが表示されます。

ステップ 2　レポートのチェックボックスをクリックしてリストからレポートを選択し、**Edit** をクリックします。

選択した Scheduled Export - edit ウィンドウが表示され、そのレポートの現在の設定が示されます。

ステップ 3　レポートのエクスポートに変更を加えて **Apply** をクリックします。または、変更を取り消すには **Reset** をクリックします。

設定オプションの詳細については、Scheduled Exports ウィンドウのオプション（表 5-15）を参照してください。

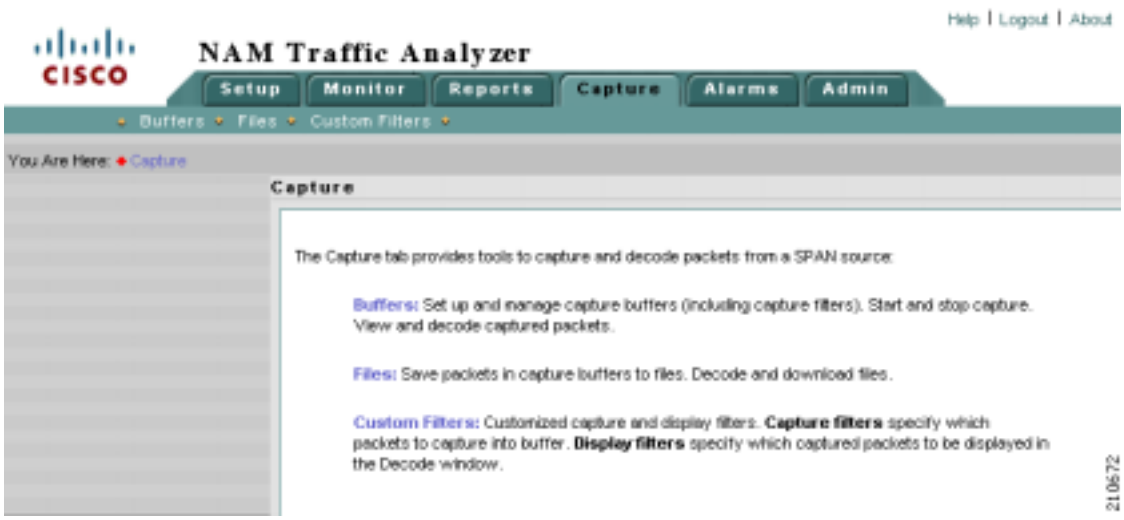
CHAPTER 6

パケット データのキャプチャとデコード

Capture タブでは、パケット データのキャプチャ、フィルタリング、およびデコード用の複数のバッファの設定、ファイル制御システム内のデータ管理、およびパケットの内容表示を行うことができます。

Capture タブ（図 6-1）には、パケット データのキャプチャおよびデコードに使用できるオプションが示されます。

図 6-1　Capture タブ



Capture タブでは、3 つのオプションを選択できます。

- バッファ（P.6-2）

  パケット データのキャプチャおよびデコード用の基本操作にアクセスするには、Buffers オプションを使用します。
- ファイル（P.6-15）

  ファイルを保存、デコード、またはダウンロードするには、Files オプションを使用します。
- カスタム キャプチャ フィルタ（P.6-21）

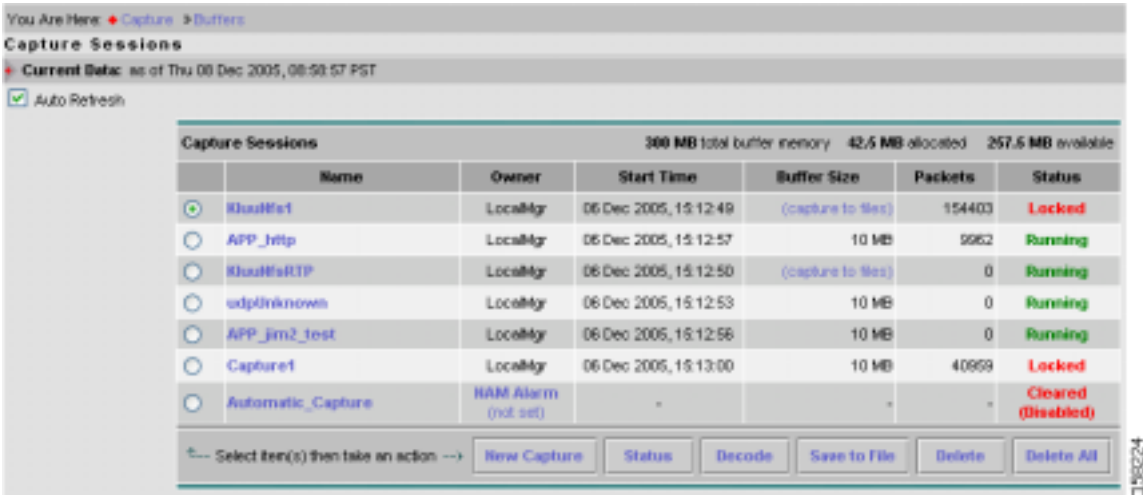
  カスタマイズしたキャプチャ フィルタおよび表示フィルタを作成するには、Custom Filters オプションを使用します。

バッファ

Capture Buffers （図 6-2）ウィンドウには、キャプチャ バッファのリストが表示されます。複数のキャプチャ バッファおよび 1 つの自動キャプチャ バッファを設定できます。

(注)　Auto Refresh チェックボックスをオンにすると、Capture Buffers ウィンドウが 60 秒ごとに自動的にリフレッシュされます。

図 6-2　Capture Buffers



Capture Buffers のフィールド（表 6-1）で、Capture Buffers のフィールドについて説明します。

表 6-1　Capture Buffers のフィールド

操作	説明
Name	キャプチャ バッファの名前
Owner	バッファの所有者
Start Time	キャプチャの開始時刻
Buffer Size	バッファのサイズ (注)　(Capture to files) は、キャプチャが 1 つ以上のファイルに格納されていることを示しています。
Packets	パケット数

表 6-1　Capture Buffers のフィールド（続き）

操作	説明
Status	現在のキャプチャの状態： • Running：パケット キャプチャが進行中です。 • Paused：パケット キャプチャが一時停止しています。キャプチャされたパケットはバッファに残っていますが、新しいパケットはキャプチャされていません。 • Cleared：キャプチャは（ユーザによって）中止され、バッファはクリアされます。 • Locked：バッファがいっぱいになったため、キャプチャがロック（中止）されました。

Capture Buffers での操作（表 6-2）で、Capture Buffers ウィンドウで行うことができる操作について説明します。

表 6-2　Capture Buffers での操作

操作	説明
New Capture	クリックすると、新しいキャプチャ バッファを作成できます。「キャプチャ設定の構成」を参照してください。
Status	クリックすると、選択したキャプチャの状態と設定値が表示されます。
Settings	クリックすると、キャプチャ設定の修正、キャプチャの一時停止、クリア、および再開を行うことができます。「キャプチャ設定の構成」を参照してください。
Decode	クリックすると、デコードされたパケットを表示できます。「パケット デコード情報の表示」を参照してください。
Save to File	クリックすると、バッファをファイルに保存できます。「ファイル」を参照してください。
Delete	クリックすると、バッファを削除できます。
Delete All	クリックすると、すべてのバッファを削除できます。

キャプチャ設定の構成

Capture Settings ウィンドウでは、新しいキャプチャ設定を構成したり、キャプチャ プロセスを制御したりすることができます。キャプチャ フィルタを設定して、キャプチャするパケットを絞り込むこともできます。

新しいキャプチャを設定するには、次の手順を実行します。

ステップ 1　**Capture** > **Buffers** を選択します。

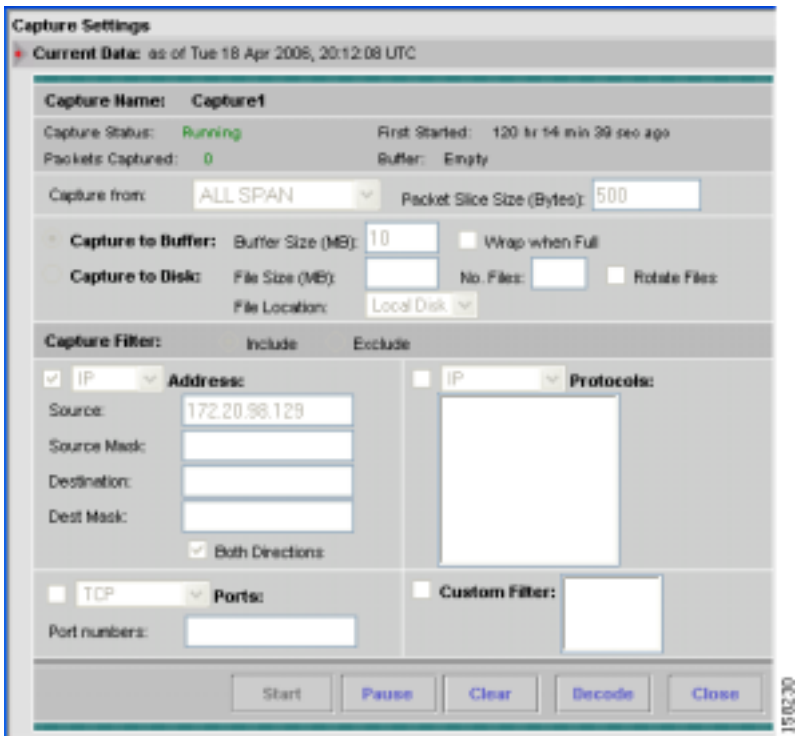
ステップ 2　新しいキャプチャをセットアップするには、**New Capture** を選択します。また、既存のバッファを選択して **Settings** をクリックすると、キャプチャ設定を変更、一時停止、クリア、または再開できます。

NAM Traffic Analyzer は Capture Settings ウィンドウ（図 6-3）を表示します。Capture Settings ウィンドウには、キャプチャ名を入力するためのフィールド、および表 6-3 で説明している 4 つのステータス インジケータがあります。

表 6-3　Capture Settings のステータス インジケータ

ステータス インジケータ	説明
Capture Status	現在のキャプチャの状態： • Running：パケット キャプチャが進行中です。 • Paused：パケット キャプチャが一時停止しています。キャプチャされたパケットはバッファに残っていますが、新しいパケットはキャプチャされていません。 • Cleared：キャプチャは（ユーザによって）中止され、バッファはクリアされます。 • Locked：バッファがいっぱいになったため、キャプチャがロックされました。
Packets Captured	キャプチャされ、キャプチャ バッファに保存されたパケットの数。 **（注）** キャプチャ バッファがいっぱいで、キャプチャが wrap-when-full モードの場合、新しいパケットが到着すると古いパケットがバッファから破棄されるため、キャプチャされたパケットの数は変動することがあります。
First Started	現在のキャプチャが開始された時刻を示します。必要に応じて何度でもキャプチャを一時停止および再開できます。キャプチャを中止して新しいキャプチャを開始する場合、このフィールドに新しいキャプチャの開始時刻が表示されます。
Buffer	現在のバッファの状態：Empty、Space Available、Full（Wrap）、または Full（Locked）。

図 6-3　Capture Settings



ステップ 3　必要に応じて、Capture Settings フィールド（表 6-4）に情報を入力します。

表 6-4　Capture Settings のフィールド

フィールド	説明	使用法
Capture Name	キャプチャの名前。	キャプチャ名を入力します。
Capture from	パケットのキャプチャ元であるデータ ソース。	リストからエントリを選択します。
Packet Slice Size	キャプチャされたパケットのサイズを制限するために使用する、バイト単位のスライス サイズ。	12 ～ 8192 の数値を入力します。 バッファが小さい場合、できるだけ多くのパケットをキャプチャするには、小さなスライス サイズを使用します。 指定したスライス サイズよりもパケット サイズが大きい場合、パケットはキャプチャ バッファに保存される前に「スライス」されます。たとえば、パケットが 1000 バイトでスライス サイズが 200 バイトの場合、パケットの最初の 200 バイトだけがキャプチャ バッファに保存されます。
Capture to Buffer	オンにすると、キャプチャはバッファに格納されます。	**Buffer Size** および **Wrap when Full** の値を入力します。
Buffer Size	キャプチャ バッファのサイズ（MB 単位）。	1 からプラットフォームの最大値までの数値を入力します。システム メモリが少ない場合は、割り当てられる実際のバッファ サイズが、ここで指定した数値よりも小さくなることがあります。キャプチャを開始すると、このフィールドには、割り当てられた実際のバッファ サイズが表示されます。 **（注）** WS-SVC-NAM-1 デバイスは 125 MB まで、WS-SVC-NAM-2 デバイスは 300 MB まで設定できます。NM-NAM デバイスは 70 MB まで設定できます。
Wrap when Full	オンにすると、バッファ内のデータがバッファ サイズを超えた場合にデータをラップします。	Check Wrap when Full をオンにすると、連続キャプチャがイネーブルになります。 **（注）** バッファがいっぱいの場合は、新しい入力パケット用の空きを作成するために、古いパケット データが削除されます。
Capture to File(s)	オンにすると、キャプチャをファイルに格納します。	**File Size** および **No. Files** の値を入力します。 **（注）** 作業ファイル用に約 400MB の空きディスク容量が予約されます。使用可能なディスク容量が 400MB を下回る場合は、ディスクへのキャプチャ セッションを新たに開始することはできません。
File Size (MB)	各キャプチャ ファイルの最大サイズ。	ファイル サイズは 1 ～ 1000 MB です。
File Location	プルダウン メニューからオプションを選択します。	デフォルトのローカル ディスクを使用するか、または以前に設定したリモート ストレージの場所を選択します。**Admin > System** をクリックし、コンテンツ メニューから Capture Data Storage を選択して、（NFS および iSCSI）リモート ストレージの場所を追加できます。
No. Files	連続キャプチャに使用するファイル数。	ファイル数は、1 ～ 50 です。

表 6-4　Capture Settings のフィールド（続き）

フィールド	説明	使用法
Rotate Files	オンにすると、連続キャプチャでファイルをローテーションします。	リモート ストレージでのみ使用可能です。 リモート ストレージの設定については、P.2-17 の「キャプチャ データ ストレージ」を参照してください。
Capture Filter: Include		Include（包含）フィルタは、フィルタ条件と一致するパケットだけをキャプチャします。
Capture Filter: Exclude		Exclude（排除）フィルタは、フィルタ条件を*除外*するパケットをキャプチャします。

ステップ 4　バッファにキャプチャする場合は、**Capture to Buffer** をオンにし、**Buffer Size** に MB 単位でサイズを入力します。最近のデータを連続してキャプチャする場合は、**Wrap when Full** をオンにします。

このタイプのキャプチャは、最大で Buffer Size に設定されたサイズまでパケット データを格納します。**Wrap when Full** がオフの場合は、データ量がバッファ サイズに達すると、キャプチャは終了します。

ステップ 5　ファイルにキャプチャする場合は、**Capture to File(s)** をオンにして、**File Size** および **No. Files** に値を入力します。

複数のファイルにキャプチャする場合は、ファイル名に拡張子が追加されます。たとえば、キャプチャ名が **CaptureA** の最初のファイルは **CaptureA_1**、2 番目のファイルは **CaptureA_2** といった具合にラベルが付けられます。

ステップ 6　ファイルにキャプチャする場合は、**Rotate Files** をオンにして、最近のパケット データを連続してキャプチャします。

Rotate Files オプションは、リモート ストレージでのみ使用できます。リモート ストレージの設定については、P.2-17 の「キャプチャ データ ストレージ」を参照してください。

（注）　**Rotate Files** オプションを選択している場合に、ファイル数が最大数に達すると、最も古いファイルが上書きされます。たとえば、**No. Files** を 10 に指定し、NAM がキャプチャ データをファイル **CaptureA_10** に書き込んだ場合、次の書き込み時にはファイル **CaptureA_1** が上書きされます。最近のキャプチャを判別するには、各ファイルのタイムスタンプをチェックします。

ステップ 7　Capture Filter ペインで、Include または Exclude をオンにします。

Include（包含）フィルタは、フィルタ条件と一致するパケットだけをキャプチャします。Exclude（排除）フィルタは、フィルタ条件を*除外*するパケットをキャプチャします。

ステップ 8　次のいずれかのチェックボックスをオンにして、該当するフィルタ タイプをイネーブルにします。

- **Address** では、IP、IPIP4、IPv6、GRE.IP、または MAC アドレスのタイプに基づいてトラフィックがフィルタリングされます（P.6-8 の「アドレス フィルタを使用したキャプチャ」を参照してください）。
- **Protocols**　では、特定のプロトコルに基づいてトラフィックがフィルタリングされます（P.6-9 の「プロトコル フィルタを使用したキャプチャ」を参照してください）。

- **Ports** では、ポート フィルタが使用されます（P.6-10 の「ポート フィルタを使用したキャプチャ」を参照してください）。
- **Custom Filter** では、カスタマイズしたフィルタが使用されます（P.6-10 の「カスタム フィルタを使用したキャプチャ」を参照してください）。

  カスタム キャプチャ フィルタの作成と編集の詳細については、P.6-21 の「カスタム キャプチャ フィルタ」を参照してください。

ステップ 9　Capture Settings での操作（表 6-5）に示されている操作のいずれかを選択します。

表 6-5　Capture Settings での操作

操作	説明
Start	クリックすると、キャプチャ操作が開始されます。
Pause	クリックすると、キャプチャ操作が一時停止されます。キャプチャ データはキャプチャ バッファに残りますが、新しいデータは格納されません。Start をクリックすると、キャプチャが再開します。
Clear	クリックすると、キャプチャが中止され、キャプチャ バッファがクリアされます。キャプチャ設定を変更する前に、キャプチャ バッファをクリアする必要があります。
Decode	クリックすると、キャプチャ バッファが表示されます。
Close	クリックすると、キャプチャ ウィンドウが閉じられます。

たとえば、111.122 クラス B ネットワークの HTTP および HTTPS パケットだけをキャプチャするには、次の手順を実行します。

ステップ 1　**Inclusive** チェックボックスをオンにします。

ステップ 2　**Address** チェックボックスをオンにします。

ステップ 3　IP ボタンをクリックします。

ステップ 4　**Both Directions** チェックボックスをオンにします。

ステップ 5　Source に **`111.122.0.0`** と入力します。

ステップ 6　Source Mask に **`255.255.0.0`** と入力します。

ステップ 7　**Protocol** チェックボックスをオンにします。

ステップ 8　**Shift** キーを押したまま、リストで HTTP と HTTPS をクリックして選択します。

アドレス フィルタを使用したキャプチャ

Address チェックボックスをオンにした場合は、必要に応じて Capture Settings Address Filter ダイアログボックス（表 6-6）に情報を入力します。

（注） IPIP4 または GRE.IP などのトンネル アドレスでフィルタリングする場合、フィルタは内部または外部 IP ヘッダーのアドレスを照合します。

表 6-6　Capture Settings Address Filter ダイアログボックス

フィールド	説明	使用法
Address	どのアドレスをフィルタリングするかを指定します。	• パケットの送信元 / 宛先 MAC アドレスを使用するには、MAC を選択します。 • パケットの送信元 / 宛先 IP アドレスを使用するには、IP を選択します。 • IP プロトコル 4 経由でトンネルされるものを含む IP アドレスの場合は、IPIP4 を選択します。 • GRE 経由でトンネルされるものを含む IP アドレスの場合は、GRE.IP を選択します。 • IP バージョン 6 を使用するアドレスの場合は、IPv6 を選択します。
Both directions	フィルタが双方向のトラフィックに適用されるかどうかを指定します。	送信元がホスト A で宛先がホスト B の場合、双方向をイネーブルにすると、A から B および B から A のパケットがフィルタリングされます。 送信元がホスト A で宛先が指定されていない場合、双方向をイネーブルにすると、ホスト A へのパケットとホスト A からのパケットの両方がフィルタリングされます。
Source	パケットの送信元アドレス。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。次の例を参考にしてください。 — 1080::8:800:200C:417A — ::FFF:129.144.52.38 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 • MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。

表 6-6　Capture Settings Address Filter ダイアログボックス（続き）

フィールド	説明	使用法
Source Mask	送信元アドレスに適用されるマスク。 • Source Mask のビットが 1 に設定されている場合、アドレス内の対応ビットは関連があります。 • Source Mask のビットが 0 に設定されている場合、アドレス内の対応ビットは無視されます。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。デフォルト（ブランクの場合）は 255.255.255.255 です。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。IPv6 アドレスのデフォルト マスク（ブランクの場合）は、ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff です。 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 デフォルトは ff ff ff ff ff ff です。
Destination	パケットの宛先アドレス。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。デフォルト（ブランクの場合）は 255.255.255.255 です。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。次の例を参考にしてください。 — 1080::8:800:200C:417A — ::FFF:129.144.52.38 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 デフォルトは ff ff ff ff ff ff です。
Dest.Mask	宛先アドレスに適用されるマスク。 • Dest.Mask のビットが 1 に設定されている場合、アドレス内の対応ビットは関連があります。 • Dest.Mask のビットが 0 に設定されている場合、アドレス内の対応ビットは無視されます。	• IP、IPIP4、および GRE.IP アドレスの場合は、有効な IPv4 アドレスをドット付きの 4 つの数字列形式 *n.n.n.n*（*n* は 0 ～ 255）で入力します。デフォルト（ブランクの場合）は 255.255.255.255 です。 • IPv6 アドレスの場合は、有効な IPv6 アドレスを許可された任意の IPv6 アドレス形式で入力します。IPv6 アドレスのデフォルト マスク（ブランクの場合）は、ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff です。 **（注）** 有効なテキスト表現については、RFC 2373 を参照してください。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 デフォルトは ff ff ff ff ff ff です。

プロトコル フィルタを使用したキャプチャ

Protocol チェックボックスをオンにした場合は、キャプチャする 1 つ以上のプロトコルをドロップダウン リストから選択します。

複数のプロトコルを選択するには、Shift キーを押した状態でクリックします。

ポート フィルタを使用したキャプチャ

Capture Settings ウィンドウで、Ports チェックボックスをオンにして、1 つのポートを入力するか、または複数のポートをカンマで区切って入力します。

カスタム フィルタを使用したキャプチャ

ステップ 1　**Custom** チェックボックスをオンにします。

（注） Custom Filter チェックボックスをオンにすると Address Filter チェックボックスおよび Protocol Filter チェックボックスがディセーブルになり、Address Filter チェックボックスまたは Protocol Filter チェックボックスをオンにすると Custom Filter チェックボックスがディセーブルになります。

ステップ 2　リストから、1 つまたは複数のカスタム キャプチャ フィルタを選択します。複数のフィルタを選択するには、Shift キーを押した状態でクリックします。複数のカスタム フィルタを選択した場合、フィルタの条件は論理和がとられます（いずれかに一致）。

（注） リストが空の場合は、P.6-21 の「カスタム キャプチャ フィルタの作成」でカスタム キャプチャ フィルタの作成方法を参照してください。

ステップ 3　選択したカスタム キャプチャ フィルタを表示または編集するには、**Custom Filters > Capture Filters** の順に選択します。

（このステップはオプションです。）

自動キャプチャ（アラームによってトリガーされるキャプチャ）の使用

アラームによって自動的に開始または中止（一時停止）されるキャプチャを設定できます。**Capture > Buffer** の順に選択して Automatic Capture 設定を構成してから、**Setup > Alarms** の順に選択し、キャプチャをトリガーするアラームを設定します。

開始と停止という 2 つのタイプのキャプチャ トリガーがあります。一度に設定できるキャプチャ トリガーは 1 つだけです。アラームの設定の詳細については、P.3-56 の「アラームしきい値の設定」を参照してください。

開始キャプチャ トリガーの場合、最初にキャプチャ バッファを一時停止状態にする必要があります。バッファがクリアされているか実行中の場合、開始キャプチャ トリガーは動作しません。

停止キャプチャ トリガーの場合、最初にキャプチャ バッファが実行中になっている必要があります。バッファが一時停止またはクリアされている場合、停止トリガーは動作しません。最適な結果を得るためには、バッファ モードを Wrap when full に設定することをお勧めします。

パケット デコード情報の表示

バッファにパケットをいくつかキャプチャした後、Packet Decoder を使用してパケットの内容を表示できます。

Packet Decoder ウィンドウは、次の 4 つの部分で構成されます。

- Packet Decoder の操作
- Packet browser ペイン
- プロトコル デコード（P.6-14 の「詳細なプロトコル デコード情報の表示」を参照）
- パケットの 16 進数ダンプ

パケット デコード情報を表示するには、次の手順を実行します。

ステップ 1　**Capture > Buffers** または **Capture > Files** を選択します。

ステップ 2　キャプチャ バッファまたはファイルを選択し、**Decode** をクリックします。

Packet Decoder ウィンドウは、図 6-4 のように表示されます。

図 6-4　Packet Decoder ウィンドウ

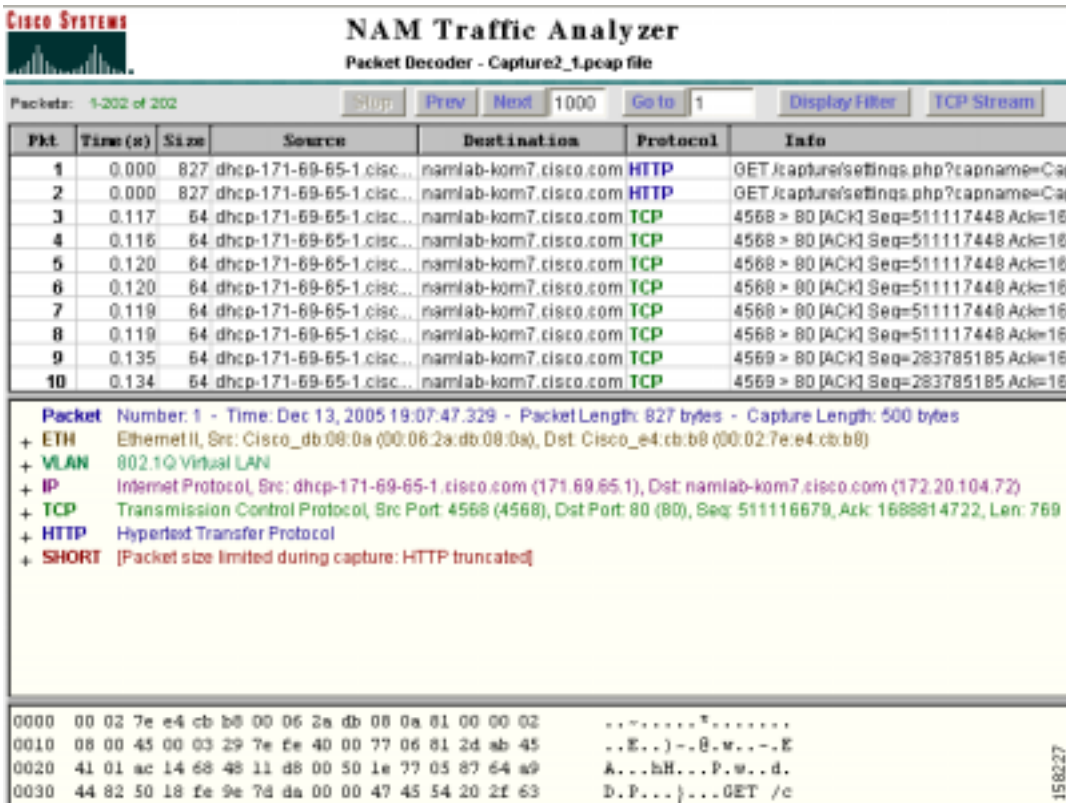


表 6-7 に、Packet Decoder の操作を示します。

表 6-7　Packet Decoder の操作

ボタン	説明
Stop	パケットのロードを中止します。
Prev	NAM からの直前のパケット ブロックをロードおよびデコードします。
Next	NAM からの次のパケット ブロックをロードおよびデコードします。
Go To	指定したパケット番号から始まるパケット ブロックをロードおよびデコードします。
Display Filter	Display Filter ダイアログを起動します。「Packet Decoder に表示されるパケットのフィルタリング」を参照してください。
TCP Stream	選択した TCP パケットの TCP ストリームに従います。

表 6-8 に、Packet Browser ペインに表示される情報を示します。

表 6-8　Packet Browser

フィールド	説明
Pkt	キャプチャ シーケンスの番号順に表示されたパケット番号。デコード（表示）フィルタがアクティブな場合、パケット番号は連続しないことがあります。
Time	表示された最初のパケット（バッファ内の最初のパケットではありません）に関して、パケットがキャプチャされた時間。 **（注）** 絶対時間を調べるには、Detail ウィンドウを参照します。
Size	パケットのサイズ（バイト単位）。
Source	パケットの送信元。ホスト名、IP、IPX、または MAC アドレスとして表示されることがあります。 **（注）** IP アドレスのホスト名解決をオンまたはオフにするには、Setup タブをクリックして、Preferences でこの設定を変更します。
Destination	パケットの宛先。ホスト名、IP、IPX、または MAC アドレスとして表示されることがあります。
Protocol	パケットのトップ レベルのプロトコル。
Info	パケットの内容に関する短いテキスト情報。

Packet Decoder でのパケットの表示

パケット ブラウザを使用して、キャプチャしたパケットのリストを表示したり、次のことを実行したりできます。

- プロトコル、IP アドレス、MAC アドレス、カスタム表示フィルタによるフィルタリング
- **Next**、**Previous**、および **Go To** ボタンを使用したキャプチャ バッファからのパケットのロード

（注） これらの機能を使用するには、キャプチャを一時停止または停止する必要があります。

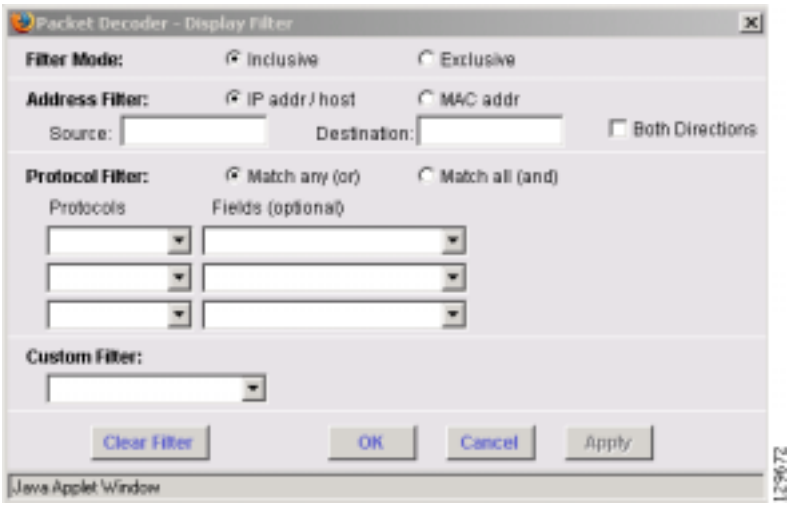
Packet Decoder に表示されるパケットのフィルタリング

Packet Decoder に表示されたパケットをフィルタするには、次の手順を実行します。

ステップ 1　Packet Decoder ウィンドウで、Display Filter ボタンをクリックします。

Packet Decoder - Display Filter ウィンドウ（図 6-5）が表示されます。

図 6-5　Packet Decoder - Display Filter ウィンドウ



ステップ 2　次の操作を行います。

- **Filter Mode** について次のいずれかを選択します。
  - **Inclusive** を選択すると、条件に一致するパケットが表示されます。
  - **Exclusive** を選択すると、条件に一致しないパケットが表示されます。
- **Address Filter** について次のように選択します。
  - IP アドレスの場合は **IP address** フィルタ。
  - MAC アドレスの場合は **MAC Address** フィルタ。
  - **Source** では、送信元アドレスを指定できます。指定する必要のない場合はブランクのままにすることができます。
  - **Destination** では、宛先アドレスを指定できます。指定する必要のない場合はブランクのままにすることができます。
  - **Both Directions** をオンにすると、どちらの方向に移動するパケットも照合できます。
- **Protocol Filter** について次のように定義します。
  - いずれかのプロトコルまたはフィールドに一致するパケットを表示するには、**Match any** を選択します。

  または
  - すべてのプロトコルまたはフィールドに一致するパケットを表示するには、**Match all** を選択します。
  - **Protocols** リストからプロトコルを選択します。

（注） プロトコル名の先頭の数文字を入力して、目的のプロトコルに直接移動できます。タイプミスをした場合にリセットするには、**Esc** キーまたは **Space** キーを押します。

　　— 必要に応じて、Fields リストからプロトコルのフィールドを選択し、フィールド値を指定します。

- **Custom Filter** について選択します。カスタム表示フィルタの設定方法については、「カスタム表示フィルタ」を参照してください。

ステップ 3　プロトコル名、IP アドレス、MAC アドレス、照合テキスト、またはカスタム デコード フィルタを指定します。

ステップ 4　**Filter** をクリックします。

ステップ 5　フィルタ条件を*除外*するパケットを表示するには、Filter ボタンの横の **exclusive** チェックボックスをオンにします。

詳細なプロトコル デコード情報の表示

詳細なプロトコル情報を表示するには、次の手順を実行します。

ステップ 1　詳細情報を必要とするパケット番号を強調表示します。

パケットに関する詳細情報が、Protocol Decode ペインおよびウィンドウ下部の 16 進数ダンプ ペインに表示されます。

（注） Protocol Decode ペインで詳細を強調表示すると、対応するバイトが下の 16 進数ダンプ ペインで強調表示されます。

ステップ 2　情報を調べるには、下部ペインのスクロール バーを使用します。

ヒント

- プロトコルは、Packet Browser および Protocol Decode ペインの両方で色分けされます。
- プロトコル情報を縮小および展開するには、Protocol Decode ペインでプロトコル名をクリックします。
- ペインのサイズを調整するには、ペイン フレームをクリックし、上または下にドラッグします。

ファイル

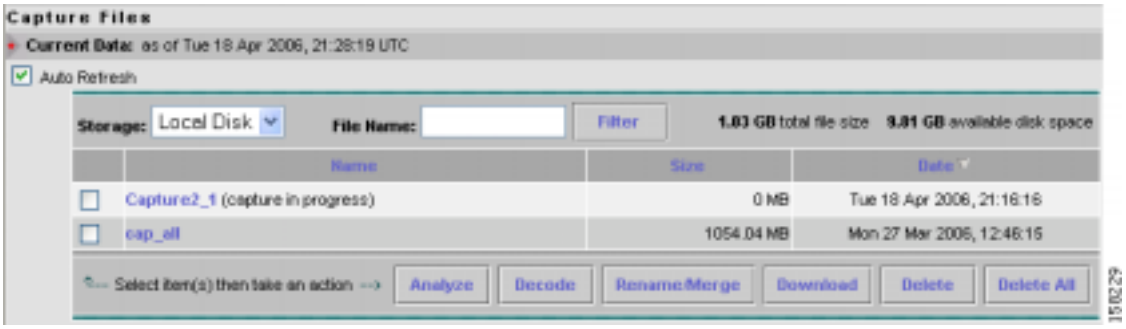
保存済みのキャプチャ ファイルを分析、デコード、マージ、ダウンロード、または削除するには、Files オプションを使用します。キャプチャ バッファをファイルに保存する方法については、P.6-2 の「バッファ」および表 6-2 を参照してください。ファイルは、Sniffer **.enc** ファイル形式でダウンロードできます。

Capture > **Files** を選択すると、Capture Files ウィンドウ（図 6-6）が表示されます。

(注)

Auto Refresh チェックボックスをオンにすると、Capture Files ウィンドウが 60 秒ごとに自動的にリフレッシュされます。

図 6-6　Capture Files ウィンドウ



Capture Files ウィンドウには、次のオプションがあります。

- プルダウン リストからストレージの場所を選択すると、その場所にあるキャプチャ ファイルが表示されます。リモート ストレージのサブディレクトリは、NAM がそれらのリモート ディレクトリに対してフル アクセス権を持つ場合にだけ一覧されます。
- キャプチャを選択して **Analyze** をクリックすると、ファイルのパケットが表示されます。
- キャプチャを選択して **Decode** をクリックすると、ファイルのパケットが表示されます。
- **Rename/Merge** をクリックすると、ファイルのパケットがマージされます。ファイルのパケットは、古い順にマージされます。
- **Download** をクリックすると、ファイルが Sniffer **.enc** ファイル形式でコンピュータにダウンロードされます。
- **Delete** または **Delete All** をクリックすると、ファイルが削除されます。

キャプチャ ファイルの分析

Capture Files ウィンドウの Analyze ボタンをクリックすると、キャプチャ期間のトラフィック レート（バイト / 秒）、ネットワーク トラフィックに関連付けられたホスト、会話、およびアプリケーションのリストを含むさまざまな統計情報を取得できます。図 6-7 に、Capture Analysis ウィンドウの例を示します。

このウィンドウでは、特定のネットワーク トラフィック セットのより詳細な表示にドリル ダウンすることもできます。**Traffic over Time** グラフの上のペインでは、**From:** および **To:** フィールドにグラフに示されている時間が表示されます。また、Protocol フィールド、Host/subnet フィールド、および **Drill-Down** ボタンもあります。

Traffic over Time グラフの各スライスには、キャプチャ ファイルの Granularity に設定された一定時間のトラフィック量が表示されます。

From: および **To:** フィールドに時間を入力し、**Drill-Down** をクリックすると、特定の時間に関するより詳細な情報を表示できます。また、特定の **プロトコル**または**ホスト / サブネット** アドレスについてドリル ダウンすることもできます。

図 6-7　Capture Statistical Analysis ウィンドウ

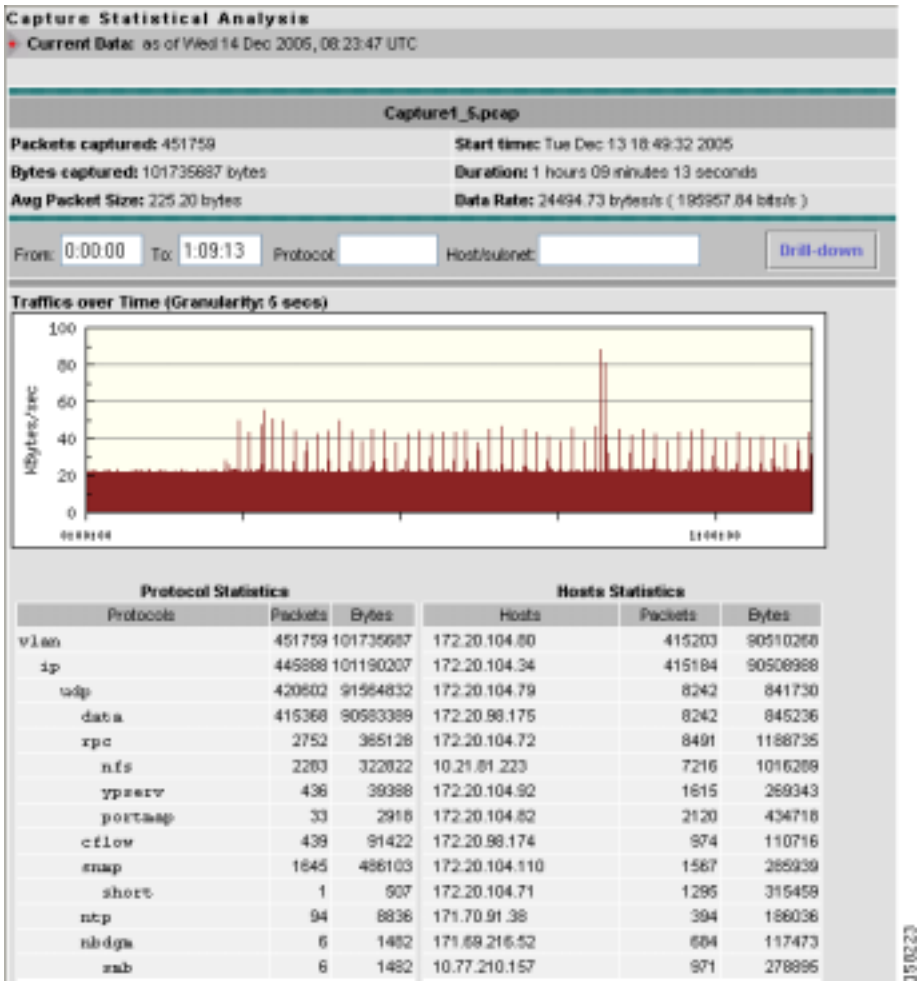


表 6-9 に、Capture Analysis ウィンドウのさまざまな領域を示します。

表 6-9　Capture Analysis ウィンドウのフィールド

フィールド	説明
Capture Overview	キャプチャされたパケット数、キャプチャされたバイト数、平均パケット サイズ、キャプチャの開始時間、キャプチャ期間、データ転送レート（バイト / 秒とビット / 秒の両方）を含む、表示されたキャプチャの要約を示します。
Traffic over Time	ネットワーク トラフィックのグラフィック イメージ（KB/ 秒）を表示します。
Protocol Statistics	プロトコルごとに、転送されパケット数とバイト数を表示します。
Hosts Statistics	ホスト アドレスごとに、転送されパケット数とバイト数を表示します。

キャプチャ ファイルのデコード

キャプチャ ファイルのデコードについては、P.6-11 の「パケット デコード情報の表示」で説明しています。

キャプチャ ファイルの名前の変更とマージ

Rename/Merge ボタンを使用して、単一のキャプチャ ファイルの名前を変更したり、複数のキャプチャ ファイルを 1 つのファイルにマージしたりできます。

キャプチャ ファイルの名前の変更

キャプチャ ファイルの名前を変更するには、次の手順を実行します。

ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Rename/Merge** をクリックします。

ダイアログボックスが表示され、選択したキャプチャ ファイルの新しい名前を入力するように要求されます。

図 6-8　Rename Capture File ダイアログボックス

ステップ 4　キャプチャ ファイルの新しい名前を入力し、**OK** をクリックします。

キャプチャ ファイルのマージ

複数のキャプチャ ファイルを 1 つのキャプチャ ファイルにマージするには、次の手順を実行します。

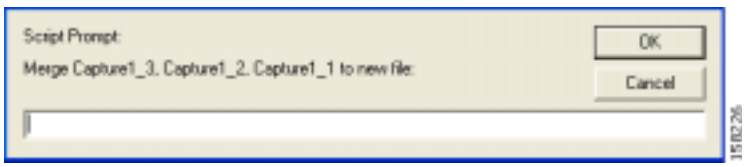
ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストから、2 つ以上のキャプチャ ファイルを選択します。

ステップ 3　**Rename/Merge** をクリックします。

ダイアログボックスが表示され、マージしたキャプチャ ファイルの新しい名前を入力するように要求されます。

図 6-9　Merging Capture Files ダイアログボックス



ステップ 4　マージしたキャプチャ ファイルの名前を入力し、**OK** をクリックします。

キャプチャ ファイルは、最も古いものから最新のものへ、タイムスタンプの順番でマージされます。

キャプチャ ファイルのダウンロード

次に、キャプチャ ファイルをコンピュータにダウンロードする手順を示します。1 度に 1 つのキャプチャ ファイルしかダウンロードできません。

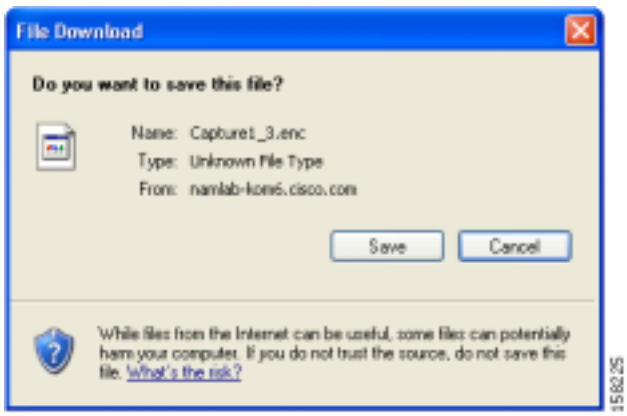
ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Download** をクリックします。

File Download ダイアログボックスが表示され、「**Do you want to save this file?**」というファイルの保存を確認するメッセージが表示されます。

図 6-10　Download Capture File ダイアログボックス



ステップ 4　**Save** をクリックします。

Save As ダイアログボックスが開きます。ここで、ファイルの名前を変更し、選択した場所にそのファイルを保存できます。

キャプチャ ファイルの削除

キャプチャ ファイルを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Delete** をクリックします。

ダイアログボックスが表示され、「**Delete the following file(s)?**」というファイルの削除を確認するメッセージとファイル名が表示されます。

ステップ 4　ファイルを削除するには **OK** をクリックします。または、ファイルをそのまま残すには **Cancel** をクリックします。

すべてのキャプチャ ファイルの削除

1 度にすべてのキャプチャ ファイルを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Files** を選択します。

ステップ 2　キャプチャのリストからキャプチャ ファイルを選択します。

ステップ 3　**Delete All** をクリックします。

ダイアログボックスが表示され、「**Delete all capture file(s)?**」という全キャプチャ ファイルの削除を確認するメッセージが表示されます。

ステップ 4　すべてのファイルを削除するには **OK** をクリックします。または、ファイルをそのまま残すには **Cancel** をクリックします。

カスタム キャプチャ フィルタ

カスタム キャプチャ フィルタを使用すると、データのキャプチャ時に不必要な情報をすべて無視する特別なフィルタを作成および保存できます。

データのキャプチャ時にカスタム フィルタを使用する方法については、P.6-10 の「カスタム フィルタを使用したキャプチャ」を参照してください。

カスタム キャプチャ フィルタの設定および管理のヘルプについては、次のトピックを参照してください。

- カスタム キャプチャ フィルタの作成（P.6-21）
- カスタム キャプチャ フィルタの編集（P.6-24）
- カスタム キャプチャ フィルタの削除（P.6-24）

カスタム キャプチャ フィルタの作成

カスタム キャプチャ フィルタを作成するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

Custom Capture Filters ダイアログボックスが表示されます。

ステップ 2　**Create** をクリックします。

Custom Capture Filter ダイアログボックス（表 6-10）が表示されます。

ステップ 3　必要に応じて、各フィールドに情報を入力します。

表 6-10　Custom Capture Filter ダイアログボックス

フィールド	説明および使用法
Filter Name	新しいフィルタの名前を入力します。
Description	フィルタの短い説明。 1 ～ 35 文字の説明を入力します。
Protocol	パケットと照合するプロトコル。 ドロップダウン リストからカプセル化を選択して、プロトコルを選択します。
Data	パケットと照合するデータ パターン。Offset フィールドを使用して、データをチェックする開始位置を指定します。 *hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 たとえば、10 進数の *15* を指定する場合は、16 進数の *0f* を使用します。10 進数 *255* の場合は、16 進数 *ff* を使用します。10 進数 *16* の場合は、16 進数 *10* を使用します。その他の例については、P.6-23 の「カスタム キャプチャ フィルタ式作成のヒント」を参照してください。 使用しない場合は、ブランクにします。 パケットが短すぎて照合するデータが足りない場合、パケットは照合に失敗します。

表 6-10　Custom Capture Filter ダイアログボックス（続き）

フィールド	説明および使用法
Data Mask	データ照合に適用されるマスク。 *hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 すべてのデータ ビットが関連する場合は、ブランクにします。 Data Mask のビットが 1 に設定されている場合、パケット内の対応ビットは照合アルゴリズムに関連があります。 Data Mask のビットが 0 に設定されている場合、パケット内の対応ビットは無視されます。 Data Mask を指定しない場合、または Data フィールドよりも短い場合は、Data フィールドの長さになるまで Data Mask に「1」ビットが埋め込まれます。たとえば、Data フィールドに 4 バイト値を入力し、Data Mask フィールドをブランクにした場合は、Data Mask に *ff ff ff ff* を指定したのと同じになります。
Data Not Mask	反転データ照合に適用されるマスク。 *hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 反転データ照合を行わない場合は、ブランクにします。 0 に設定された（または指定されていない）Data Not Mask 内のビットの場合、パケット内の関連ビットは、Data フィールド内の対応ビットと一致している必要があります。 1 に設定された Data Not Mask のビットの場合、パケット内の少なくとも 1 つの関連ビットは Data フィールド内の対応ビットと異なっている必要があります。 Data Not Mask を指定しない場合、または Data フィールドよりも短い場合は、Data フィールドの長さになるまで Data Not Mask に「0」ビットが埋め込まれます。
Offset	パケット データ照合を開始するオフセット（Base からのバイト数）を 10 進数で入力します。 このオフセットは、Data、Data Mask、および Data Not Mask の各フィールドに適用されます。
Base	オフセットを計算するためのベースとして、absolute またはプロトコルを選択します。 absolute を選択した場合、オフセットはパケットの絶対開始位置（イーサネット フレームの先頭）から計算されます。WS-SVC-NAM-1 および NAM-2 デバイスのオフセットを計算するときは、802.1q ヘッダーを考慮する必要があります。 プロトコルを選択した場合、オフセットはパケットのプロトコル部分の先頭から計算されます。パケットにプロトコルが含まれていない場合、パケットはこの照合に失敗します。
Status	パケットと照合するステータス。 0 ～ 65535 の数値を入力します。不要な場合はブランクにします。 イーサネット パケット キャプチャの場合、ステータス ビットは次のとおりです。 ビット 0：1518 オクテットよりも長いパケット ビット 1：64 オクテットよりも短いパケット ビット 2：CRC またはアラインメント エラー たとえば、イーサネット フラグメントは 6 のステータス値（ビット 1 と 2 のセット）。

表 6-10　Custom Capture Filter ダイアログボックス（続き）

フィールド	説明および使用法
Status Mask	ステータス照合に適用されるマスク。0 ～ 65535 の数値を入力します。すべてのステータス ビットが関連する場合は、ブランクにします。 Status Mask のビットが 1 に設定されている場合、パケット ステータス内の対応ビットは照合アルゴリズムに関連があります。 Status Mask ビットが 0 に設定されている場合、パケット ステータス内の対応ビットは無視されます。 Status Mask を指定しない場合、または Status フィールドよりも短い場合は、Status フィールドの長さになるまで Status Mask に「1」ビットが埋め込まれます。
Status Not Mask	反転ステータス照合に適用されるマスクとして、0 ～ 65535 の数値を入力します。 反転ステータス照合を行わない場合は、ブランクにします。 0 に設定された（または指定されていない）Status Not Mask 内のビットの場合、パケットの関連ステータス ビットは、Status フィールド内の対応ビットと一致している必要があります。 1 に設定された Status Not Mask のビットの場合、ステータス パケットの少なくとも 1 つの関連ビットは Status フィールド内の対応ビットと異なっている必要があります。 Status Not Mask を指定しない場合、「0」ビットが埋め込まれます。

ステップ 4　ファイルを作成するには、**Apply** をクリックします。または、変更を取り消すには、**Reset** をクリックします。

カスタム キャプチャ フィルタ式作成のヒント

TOS 値は、IP ヘッダーのバイト 1（2 番目のバイト）に保存されます。16 の TOS 値（0x10）を持つ IP パケットを照合するには、次のように入力します。

Data：10
Offset：1
Base：IP

Data Mask に何も指定されていない場合、有効な値は *ff* です。

IP パケットの送信元アドレスは、IP ヘッダーのバイト 12 ～ 15 に保存されます。15.16.17.18 の送信元アドレスを持つ IP パケットを照合するには、次のように入力します。

Data：0f 10 11 12
Offset：12
Base：IP

15.*.*.18 の送信元アドレスを持つ IP パケット（* は 0 ～ 255 の任意の数値）を照合するには、次のように入力します。

Data：0f 00 00 12
Data Mask：ff 00 00 ff
Offset：12
Base：IP

送信元アドレスが 15.16.17.18、宛先アドレスが 15.16.17.19 と異なる IP アドレスで照合するには、次のように入力します。

Data：f0 10 12 12 0f 10 11 13
Data Mask：ff ff ff ff ff ff ff ff
Data Not Mask：00 00 00 00 00 00 00 00
Offset：12
Base：IP

カスタム キャプチャ フィルタの編集

カスタム キャプチャ フィルタを編集するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

Custom Capture Filters ダイアログボックスが表示されます。

ステップ 2　編集するフィルタを選択して、**Edit** をクリックします。

Custom Capture Filter ダイアログボックス（表 6-10 を参照）が表示されます。

ステップ 3　必要に応じて、各フィールドに情報を入力します。

ステップ 4　次のいずれかを実行します。

- 変更を適用するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

カスタム キャプチャ フィルタの削除

カスタム キャプチャ フィルタを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

Custom Capture Filters ダイアログボックスが表示されます。

ステップ 2　削除するフィルタを選択して、**Delete** をクリックします。

ステップ 3　確認のダイアログボックスで、次のいずれかを選択します。

- フィルタを削除するには、**OK** をクリックします。
- 取り消すには、**Cancel** をクリックします。

カスタム表示フィルタ

カスタム表示フィルタを使用して、カスタマイズしたフィルタを作成および保存すると、Decode ウィンドウで使用して表示するパケットを制限できます。

カスタム表示フィルタの設定および管理のヘルプについては、次のトピックを参照してください。

- カスタム表示フィルタの作成（P.6-25）
- カスタム表示フィルタの編集（P.6-28）
- カスタム表示フィルタの削除（P.6-28）

カスタム表示フィルタの作成

カスタム表示フィルタを作成するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

ステップ 2　コンテンツで **Display Filters** をクリックします。

Custom Display Filters ダイアログボックスが表示されます。

ステップ 3　**Create** をクリックします。

Custom Decode Filter ダイアログボックス（表 6-11）が表示されます。

ステップ 4　必要に応じて、各フィールドに情報を入力します。

表 6-11　Custom Decode Filter ダイアログボックス

フィールド	説明	使用法
Filter Name	キャプチャ フィルタの名前。	作成するフィルタの名前を入力します。
Description	キャプチャ フィルタの説明。	フィルタの説明を入力します。
Protocol	パケットと照合するプロトコル。	リストからプロトコルを選択します（プロトコルに関係なくすべてのパケットを照合する場合は **All** を選択します）。
Address（MAC または IP）	MAC アドレスまたは IP アドレスのどちらでフィルタリングするかを指定します。	パケットの送信元または宛先 MAC アドレスを使用してフィルタリングするには、MAC を選択します。 パケットの送信元または宛先アドレスを使用してフィルタリングするには、IP を選択します。
Both Directions	フィルタが双方向のトラフィックに適用されるかどうかを指定します。	送信元がホスト A で宛先がホスト B の場合、双方向をイネーブルにすると、A から B および B から A のパケットがフィルタリングされます。 送信元がホスト A で宛先が指定されていない場合、双方向をイネーブルにすると、ホスト A へのパケットとホスト A からのパケットの両方がフィルタリングされます。

表 6-11　Custom Decode Filter ダイアログボックス（続き）

フィールド	説明	使用法
Source	パケットの送信元アドレス。	IP アドレスの場合は、*n.n.n.n*（*n* は 0 ～ 255）または *n.n.n.n/s*（*s* はサブネット マスク 0 ～ 32）を入力します。 MAC アドレスの場合は、*hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。
Destination	パケットの宛先アドレス。	IP アドレスの場合は、*n.n.n.n*（*n* は 0 ～ 255）または *n.n.n.n/s*（*s* はサブネット マスク 0 ～ 32）を入力します。 MAC アドレスの場合は、*hh hh hh hh hh hh*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。
Offset	パケット データ照合を開始する Base からのオフセット（バイト数）。	10 進数を入力します。
Base	オフセットが計算されるベース。 absolute を選択した場合、オフセットはパケットの絶対開始位置（たとえば、イーサネット フレームの先頭）から計算されます。 プロトコルを選択した場合、オフセットはパケットのプロトコル部分の先頭から計算されます。パケットにプロトコルが含まれていない場合、パケットはこの照合に失敗します。	**absolute** またはプロトコルを選択します。
Data Pattern	パケットと照合するデータ。	*hh hh hh ...*（*hh* は 0 ～ 9 または a ～ f の 16 進数）を入力します。 使用しない場合は、ブランクにします。
Filter Expression	複雑なフィルタ条件を設定する高度な機能。 最も単純なフィルタにより、プロトコルまたはフィールドの存在をチェックできます。たとえば、単純なフィルタ式 **ipx** を使用して、IPX プロトコルを含むすべてのパケットを表示できます。	P.6-27 の「カスタム デコード フィルタ式作成のヒント」を参照してください。

ステップ 5　次のいずれかを実行します。

- フィルタを作成するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

カスタム デコード フィルタ式作成のヒント

表 6-12 に示されている論理演算子および比較演算子を使用して、カスタム デコード フィルタ式を構築できます。

表 6-12　論理演算子と比較演算子

演算子	意味
and	論理積
or	論理和
xor	排他的論理和
not	論理否定
==	等しい
!=	等しくない
>	不等号（大なり）

カッコ内で部分式をグループ化することもできます。フィルタ式では次のフィールドを使用できます。

フィールド	フィルタ基準	フォーマット
eth.addr eth.src eth.dst	MAC アドレス	*hh hh hh hh hh hh*（h は 0 ～ 9 または a ～ f の 16 進数）。
ip.addr ip.src ip.dst	IP アドレス	*n.n.n.n* または *n.n.n.n/s*（n は 0 ～ 255 の数値、s は 0 ～ 32 のハイフンを含まないホスト名）。
tcp.port tcp.srcport tcp.dstport	TCP ポート番号	0 ～ 65535 の 10 進数。
udp.port udp.srcport udp.dstport	UDP ポート番号	0 ～ 65535 の 10 進数。
protocol	プロトコル	Custom Decode Filter ダイアログボックスの Protocol リストをクリックして、フィルタリングできるプロトコルのリストを確認します。
protocol [*offset*:*length*]	プロトコルのデータ パターン	*hh:hh:hh:hh...*（hh は 0 ～ 9 または a ～ f の 16 進数）。 *offset* および *length* は 10 進数。 *offset* は 0 から開始し、パケットの *protocol* 部分の先頭と関連しています。
frame.pkt_len	パケット長	パケット長を表す 10 進数。切り捨てられたキャプチャ パケット長ではありません。

カスタム デコード フィルタ式の例

- 111.122.133.144 からの SNMP パケットを照合するには、次のように入力します。

```
snmp and (ip.src == 111.122.133.144)
```

- 111.122 クラス B ネットワークからの IP パケットを照合するには、次のように入力します。

```
ip.addr == 111.122.0.0/16
```

- ポート 80 への TCP パケットおよびポート 80 からの TCP パケットを照合するには、次のように入力します。

  ```
  tcp.port == 80
  ```

- TOS 値は、IP ヘッダーのバイト 1（2 番目のバイト）に保存されます。16 の TOS 値（0x10）を持つ IP パケットを照合するには、次のように入力します。

  ```
  ip[1:1] == 10
  ```

- TCP 確認応答番号は、TCP ヘッダーのバイト 8 ～ 11 に保存されます。確認応答番号 12345678（0xBC614E）を持つ TCP パケットを照合するには、次のように入力します。

  ```
  tcp[8:4] == 00:BC:61:4E
  ```

（注） Custom Decode Filter ダイアログボックスでは、フィルタ式を他のフィールドと組み合せて使用できます。この場合、フィルタ式は他の条件との論理積がとられます。
無効または矛盾するフィルタ式では、パケットは照合されません。

カスタム表示フィルタの編集

カスタム表示フィルタを編集するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

ステップ 2　コンテンツで **Display Filters** をクリックします。

Custom Display Filters ダイアログボックスが表示されます。

ステップ 3　編集するフィルタを選択して、**Edit** をクリックします。

ステップ 4　必要に応じて、各フィールドの情報を変更します。

ステップ 5　次のいずれかを実行します。

- 変更を適用するには、**Apply** をクリックします。
- 変更を取り消すには、**Reset** をクリックします。

カスタム表示フィルタの削除

カスタム表示フィルタを削除するには、次の手順を実行します。

ステップ 1　**Capture** > **Custom Filters** を選択します。

ステップ 2　コンテンツで **Display Filters** をクリックします。

Custom Display Filters ダイアログボックスが表示されます。

ステップ 3　削除するフィルタを選択して、**Delete** をクリックします。

ステップ 4　確認のダイアログボックスで、次のいずれかを選択します。

- フィルタを削除するには、**OK** をクリックします。
- 取り消すには、**Cancel** をクリックします。

CHAPTER 7

アラームの表示

アラームとは、上昇データのしきい値、下降データのしきい値、またはその両方に基づいてあらかじめ定義された条件です。Setup タブで、NAM MIB、NAM 音声監視、またはスイッチに対してしきい値を設定できます。NAM MIB しきい値、NAM 音声監視しきい値、およびスイッチしきい値の設定については、P.3-56 の「アラームしきい値の設定」を参照してください。

(注) 外部 SNMP マネージャを使用して、NAM でアラームおよびイベント テーブルを設定することにより、NAM MIB 変数のしきい値を設定できます。ただし、音声監視変数のしきい値は、Catalyst 6500 NAM Traffic Analyzer だけが設定できます。

Syslog メッセージは、MIB しきい値イベント、音声しきい値イベント、またはシステム アラートに対して作成されます。次の 2 つのアラーム ログを表示できます。

- NAM ログの表示（P.7-2）
- スイッチ ログの表示（P.7-3）

(注) スイッチ ログは、NM-NAM デバイスには適用されません。

NAM ログの表示

NAM ログには、NAM MIB しきい値と NAM 音声監視しきい値のすべてのしきい値イベントが表示されます。

ステップ 1　**Alarms** > **NAM** を選択します。

ステップ 2　NAM Threshold Alarms ウィンドウ（表 7-1）が表示されます。

表 7-1　NAM Threshold Alarms

フィールド	説明
Date	アラームが発生した日付
Time	アラームが発生した時刻
Description	アラームの説明
Variable	トリガーされたアラーム変数
Alarm Value	アラームの値
Message	アラーム メッセージ

ステップ 3　画面をクリアするには、**Clear** をクリックします。

ヒント　自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

スイッチ ログの表示

（注） この項の内容は、NM-NAM デバイスには適用されません。

スイッチ ログには、スイッチの Mini-RMON MIB からの RMON ログ テーブルが表示されます。

スイッチの CLI、またはスイッチの Mini-RMON MIB を設定する外部 SNMP マネージャを使用して、アプリケーションからスイッチしきい値を設定できます。

アプリケーションを使用してスイッチしきい値を設定する方法については、P.3-63 の「スイッチしきい値の作成」を参照してください。

スイッチの CLI の使用方法については、『*Catalyst 6000 Content Switching Module Installation and Configuration Note*』を参照してください。

ステップ 1　**Alarms** > **Switch** を選択します。

Switch Threshold Alarms ウィンドウ（表 7-2）が表示されます。

表 7-2　Switch Threshold Alarms

フィールド	説明
Date	アラームが発生した日付
Time	アラームが発生した時刻
Description	アラームの説明

ヒント 自動リフレッシュをオフにするには、Auto Refresh チェックボックスをオフにします。

APPENDIX A

トラブルシューティング

この付録では、NAM Traffic Analyzer の使用時に発生する一般的な問題について説明します。

- ユーザ名およびパスワードの問題（P.A-3）
- ログインの問題（P.A-5）
- パケットのキャプチャの問題（P.A-8）
- アラームとインターフェイス統計情報またはポート統計情報の問題（P.A-10）
- SPAN に関連する問題（P.A-7）
- NetFlow および NBAR の監視の問題（P.A-11）
- レポートの問題（P.A-15）
- イメージのアップグレードおよびパッチの問題（P.A-16）
- Web ブラウザの応答時間および表示の問題（P.A-17）
- NAM とスイッチの日付と時刻の同期の問題（P.A-18）
- 診断エラー メッセージの問題（P.A-18）
- ホスト名解決の問題（P.A-19）
- データ不一致の問題（P.A-20）
- HTTPS および セキュリティ証明書の問題（P.A-21）
- SNMP の問題（P.A-22）
- プロトコル サポートの問題（P.A-23）
- 音声監視の問題（P.A-24）

NAM の一般的な問題

Q. NAM が応答しない場合、どのような情報を収集する必要がありますか、また、他にどのような作業を行う必要がありますか。

A. 次の事項について確認し、情報を収集します。また、次の操作を実行します。

- スイッチまたはルータの CLI からの **session** は機能するか。
- EOBC（127 サブネット）を介した **ping** は成功するか。
- 管理 IP アドレスへの **ping** は成功するか。
- NAM およびスイッチまたはルータから **show tech-support** コマンドの出力を収集する。
- コア ファイルを収集する。
- NAM がシャーシに正しく取り付けられているかどうかを確認する。
- NAM をリセットする。
- メンテナンス イメージまたはメンテナンス ヘルパーにリセットする。
- 設定をクリアする。
- （できる限り、再パーティション オプション *--install* を指定して）アプリケーション イメージを再インストールする。

ユーザ名およびパスワードの問題

Q. CLI のユーザ名（root または guest）およびパスワードを使用して、NAM Traffic Analyzer にログインできますか。または、NAM Traffic Analyzer のユーザ名およびパスワードを使用して、NAM CLI にログインできますか。

A. いいえ。Web と CLI のユーザは別々に管理されています。Web ユーザは、ローカル データベースで作成、または TACACS+ を使用して作成できます。CLI で使用しているものと同じユーザ名とパスワードで、Web ユーザを作成できます。ただし、両方でパスワードの変更を行う必要があります。

Q. TACACS+ を使用する場合、ローカル データベースで Web ユーザを定義する必要がありますか。

A. いいえ。ローカル データベースに加えて、またはローカル データベースの代わりに TACACS+ を使用できます（常に、ローカル データベースが先に確認されます）。TACACS+ だけを使用するには、次のいずれかの方法でローカル データベース ユーザを削除できます。

- NAM CLI の **rmwebusers** コマンドを使用して、TACACS+ ユーザではなく、ローカル ユーザだけを削除します。各ユーザは TACACS+ サーバで別に管理されます。
- Admin タブで **Users** をクリックしてから、すべてのローカル データベース ユーザを個別に削除します。

注意　TACACS+ ユーザとして NAM Traffic Analyzer にログインできることを確認するまでは、ローカル データベース Web ユーザをすべて削除しないでください。

Q. どうすればローカル Web admin ユーザのパスワードを回復できますか。

A. ローカル Web admin ユーザ パスワードを忘れた場合や、Account 権限を持つ別のユーザがログインして、ローカル Web admin ユーザ パスワードを変更した場合は、パスワードを回復できます。

ローカル Web admin ユーザ パスワードを回復するには、次の手順を実行します。

ステップ 1　NAM CLI にアクセスします。

ステップ 2　次のコマンドを入力します。

```
web-user
user name <name>
exit
```

ステップ 3　プロンプトに対して、新しいパスワードを入力します。

ステップ 4　**Y** を入力して、新しいパスワードを確認します。

Q. NAM および TACACS+ サーバ間で TACACS+ 設定を混合してしまいましたが、NAM で TACACS+ 設定を修復するローカル データベース ユーザ アカウントがない場合、どうすれば回復できますか。

A. TACACS+ サーバからこの問題を修復できない場合は、NAM CLI で **ip http tacacs+ enable** と入力して、TACACS+ 設定を再設定します。

Q. アップグレードを実行、またはパッチを適用する場合、パスワードの使用に制限はありますか。

A. はい。アップグレードおよびパッチ　コマンドの引数としてパスワードを使用しないでください。次の形式のコマンド構文を使用します。

patch ftp://*user@host***/***full-patch***/***filename*

プロンプトが表示されたら、パスワードを入力します。

ログインの問題

Q. なぜログイン セッションがタイムアウトするのですか。

A. ログイン セッションは、約 1 時間操作が行われないと自動的にタイムアウトし、ユーザは NAM Traffic Analyzer からログアウトされます。

（注） 自動リフレッシュ機能がイネーブルである画面が表示されている場合、ログイン セッションはタイムアウトしません。

Q. ユーザ アカウントが削除されても、そのユーザがログインしたままなのはなぜですか。

A. ユーザのログイン中にユーザ アカウントを削除した場合、そのユーザはログインしたままで、その特権も保持されます。セッションは、そのユーザがログアウトするまで有効です。セッション中にアカウントを削除、または権限を変更した場合、影響があるのはその後のセッションのみです。ログインしているユーザを強制的にログアウトするには、NAM を再起動します。

Q. TACACS+ が設定された NAM Traffic Analyzer にログインできないのはなぜですか。

A. 正しい TACACS+ サーバ名および秘密鍵が入力されて、TACACS+ サーバで設定した鍵と同じ秘密鍵を使用していることを確認します。汎用 TACACS+ サーバを使用している場合は、Password Authentication Protocol（PAP; パスワード認証プロトコル）がサポートされ、PAP が選択されていることを確認します。

システム アラートで TACACS+ 関連メッセージを調べることもできます。

ステップ 1　NAM Traffic Analyzer にローカル ユーザとしてログインします。

ステップ 2　**Admin** > **Diagnostics** を選択します。

ステップ 3　コンテンツで **Tech Support** をクリックします。

ステップ 4　**/var/log/messages** セクションまで下にスクロールします。

ステップ 5　次のようなメッセージを探し、内容に応じて対応します。

メッセージ	考えられる原因と対応
...PAM-tacplus[612]:auth failed:Login incorrect	ユーザ名およびパスワードが、TACACS+ サーバ内のどのユーザ名およびパスワードとも一致しません。 1. TACACS+ サーバにログインします。 2. NAM ユーザを認証および認可するようにサーバを設定します。 P.2-5 の「TACACS+ 認証および認可の設定」を参照してください。
... httpd: tac_authen_pap_read: error reading PAP authen header, read -1 of 12: Connection reset by peer ... PAM-tacplus[10455]: auth failed: Authentication error, please contact administrator.	NAM が ACS/TACACS+ サーバの NAS（AAA クライアント）リストに追加されていません。 1. TACACS+ サーバにログインします。 2. NAM が NAS（AAA クライアント）リストにあり、TACACS+ が認証方法として選択されていることを確認します。 P.2-5 の「TACACS+ 認証および認可の設定」を参照してください。
...httpd:tac_authen_pap_read:invalid reply content, incorrect key? ...PAM-tacplus[616]:auth failed:Authentication error, please contactadministrator.	NAM で設定した TACACS+ 秘密鍵が TACACS+ サーバの秘密鍵と一致しません。 1. **Admin** > **Users** を選択します。 2. コンテンツで **TACACS+** をクリックします。 3. Secret Key フィールドおよび Repeat Secret Key フィールドに正しい秘密鍵を入力します。 4. **Apply** をクリックします。
..httpd:tac_connect:connection to 172.20.122.183 failed:Connection timed out ...httpd:tac_connect:all possible TACACS+ servers failed ...PAM-tacplus[613]:connection failed srv 0: Connection timed out ...PAM-tacplus[613]:no more servers to connect	NAM で誤った TACACS+ サーバ IP アドレスが設定されています。 1. **Admin** をクリックします。 2. **Users** をクリックします。 3. コンテンツで **TACACS+** をクリックします。 4. 正しい TACACS+ サーバ アドレスを入力します。 5. **Apply** をクリックします。
Not authorized... （NAM Traffic Analyzer へのアクセス時）	ユーザに必要なアクセス権がありません。 1. TACACS+ サーバにログインします。 2. ユーザに適切な権利を与えます。 P.2-7 の「NAM ユーザまたはユーザ グループの追加」を参照してください。

SPAN に関連する問題

(注)　この項は、Catalyst NAM だけに適用されます。

Q. SPAN セッションが Active SPAN ウィンドウに表示されない場合はどうなりますか。

A. スイッチが Catalyst OS を実行している場合、宛先ポートを格納しているモジュールをスイッチのシャーシから取り外すと、SPAN セッションは非アクティブになります。この場合、Supervisor エンジン モジュールによって SPAN 設定が SNMP エージェントから削除されているため、NAM に SPAN セッションは表示されません。

Q. Cisco IOS を実行しているスイッチで SPAN セッションの作成に失敗するのはなぜですか。

A. Cisco IOS を実行しているスイッチの場合、SPAN セッションは送信元タイプまたは宛先ポートだけで部分的に定義できます。NAM は、この部分的な SPAN セッションを表示しません。ただし、部分的に設定された SPAN セッションでは、送信元タイプまたは宛先ポートとの競合がある場合、SPAN 作成要求が失敗することがあります。

Q. 一方向だけにスパンするように SPAN セッションを変更したり、SPAN セッション タイプをスイッチ ポートから VLAN、または VLAN からスイッチ ポートに変更するにはどうしたらよいですか。

A. SPAN セッションの作成後は、NAM Traffic Analyzer を使用してこれらの特性を編集することはできません。その代わり、SPAN セッションを削除して、必要な特性を持つ新しいセッションを作成する必要があります。

（SPAN セッションを削除せずに）**Create** をクリックするだけで、現在の SPAN を上書きすることもできます。

(注)　Setup SPAN Sources ダイアログボックスで、SPAN セッションの VLAN（現在の SPAN セッションがすでに VLAN の場合）を追加または削除できます。（VLAN からポートへの変更、またはトラフィックの方向の変更など）SPAN トラフィック タイプを変更することはできません。

Q. Setup SPAN Sources ダイアログボックスで SPAN セッションの作成または編集時に「`Failed to create SPAN session for...`」というメッセージが表示されることがあるのはなぜですか。

A. これは、通常スイッチ上で SPAN の限度に達したために発生します。該当する限度を調べるには、Catalyst OS または Cisco IOS のマニュアルを参照してください。最も簡単な解決策は、SPAN（該当する場合は RSPAN）セッションを削除して、新しいセッションを編集または作成することです。

パケットのキャプチャの問題

Q. Capture Settings ダイアログボックスでキャプチャ バッファがロックされ、パケットがキャプチャされないのはなぜですか。

A. **Lock when full** を選択すると、バッファがいっぱいのときにキャプチャ処理でその内容を上書きできなくなります。

ロックされているキャプチャを再開するには、まずキャプチャ バッファをクリアする必要があります。クリアする前に、キャプチャ バッファをファイルに保存します。

(注) **Wrap when full** を選択して、キャプチャ バッファがいっぱいのときに、新しく着信したパケットで以前のパケットを上書きする方法もあります。

Q. Capture Settings ダイアログボックスでキャプチャ設定を行い、**Start** をクリックしても、パケットのキャプチャに問題が生じるのはなぜですか。

A. これにはいくつかの原因が考えられます。

Capture packets from リストで選択したデータ ソースが NAM にスパンされていることを確認します。

ヒント NAM はスイッチから自動的に VLAN を認識しますが、自動的には VLAN をスパンしません。そのため、Active SPAN Sources ウィンドウを使用して VLAN をスパンする必要があります。

SPAN セッションが動作していることを確認するには、次の手順を実行します。

ステップ 1　**Setup** > **Data Sources** を選択します。

ステップ 2　パケット トラフィックが適切なソースからスパンされていることを確認します。

ステップ 3　スパンされていない場合は、**Create** または **Edit** をクリックして、必要な SPAN ソースを追加します。

ステップ 4　**Submit** をクリックします。

ステップ 5　**Capture** > **Settings** を選択します。

ステップ 6　**Start** をクリックします。

Capture Settings ダイアログボックスで、フィルタが選択されていることも慎重に確認する必要があります。作成したフィルタの制限が大きすぎる可能性があります（詳細については、第 6 章「パケット データのキャプチャとデコード」を参照してください）。

それでもパケットをキャプチャできない場合は、すべてのキャプチャ ファイルを削除してみます。

ステップ 1　**Capture** > **Buffers** を選択します。

ステップ 2　キャプチャ バッファを選択し、**Settings** をクリックします。

ステップ 3　Address、Protocol、Port、Custom の各チェックボックスをオフにします。

ステップ 4　キャプチャを再開するには、**Start** をクリックします。

SNMP マネージャまたは別の Web サーバによって NAM プロトコル ディレクトリから削除されたプロトコルに基づいて、フィルタを選択した可能性もあります。

フィルタリングに使用可能なプロトコルを表示するには、次の手順を実行します。

ステップ 1　**Setup** > **Monitor** を選択します。

ステップ 2　コンテンツで **Protocol Directory** をクリックします。

キャプチャ バッファに使用できるメモリがないため、キャプチャを開始できない場合があります。NAM キャプチャ メモリの使用状況を調べるには、**Capture** > **Buffers** の順に移動します。キャプチャ メモリを解放するには、古いバッファをクリアまたは削除します。

Q.　キャプチャされたパケットが重複して表示されるのはなぜですか。

A.　Capture Decode ダイアログボックスでパケットが 2 つ表示される場合は、双方向（送信と受信）でスパニングを行っている可能性があります。

Q.　自動キャプチャ トリガーが停止または開始しないのはなぜですか。

A.　自動キャプチャに関連付けられているアラームがまだ発生していない可能性があります。**Alarms** > **NAM** の順に移動して、過去に発生したアラームのリストを確認します。さらに、開始キャプチャ トリガーの場合、最初にキャプチャ バッファを一時停止状態にする必要があります。

バッファがクリアされているか実行中の場合、開始キャプチャ トリガーは動作しません。停止キャプチャ トリガーの場合、最初にキャプチャ バッファが実行中になっている必要があります。バッファが一時停止またはクリアされている場合、停止トリガーは動作しません。詳細については、P.6-3 の「キャプチャ設定の構成」を参照してください。

Q.　Monitor ウィンドウでキャプチャを開始できないのはなぜですか。

A.　バッファが完全に他のキャプチャ　プロセスに割り当てられており、使用できるバッファが　0 MB の場合、キャプチャ プロセスは開始しません。この問題を解決するには、既存のキャプチャ プロセスをクリアしてバッファを解放し、新しいプロセスが開始できるようにします。

Q.　NM-NAM の内部ポートでキャプチャされたパケットのレイヤ 2 情報が間違っているように見えるのはなぜですか。

A.　ルータは、CEF パスで NM-NAM にパケットをコピーします。その時点で、レイヤ 2 は取り除かれています。特別なレイヤ 2 ヘッダーを使用して、パケットが NM-NAM に送信されます。

Q. NM-NAM 内部ポート上に、監視対象として設定したトラフィック以外のトラフィックが存在するのはなぜですか。

A. 分析モジュール監視機能によって NM-NAM にコピーされるトラフィック以外に、管理トラフィックもキャプチャされて NM-NAM に向けられることがあります。

アラームとインターフェイス統計情報またはポート統計情報の問題

Q. Setup/Alarm/NAM MIB Thresholds ウィンドウのアラームのいずれかで、Data Source に Collection Deleted と表示されるのはなぜですか。

A. Data Source はテーブル収集インデックスにマップされています。Setup/Monitor/Core ウィンドウで収集を削除すると、テーブル インデックスが削除されます。アラーム データ ソースをテーブル インデックスにマップできなくなったため、アラームを削除して作成し直す必要があります。

Q. しきい値アラームを作成したり、インターフェイスまたはポート統計情報を表示できないのはなぜですか。

A. 2 つの典型的な原因として、スイッチと NAM と間の接続がない、またはスイッチで Mini-RMON がイネーブルになっていないことが考えられます。

WS-SVC-NAM-1 および WS-SVC-NAM-2 デバイスの場合

接続があることを確認するには、**Setup>Switch Parameters>Switch Information** の順に移動して、スイッチからの SNMP 読み取り、およびスイッチへの SNMP 書き込みの結果を表示します。Switch Information テーブルの詳細については、P.3-2 の「スイッチ情報の表示」を参照してください。

スイッチで Mini-RMON がイネーブルになっていることを確認するには、**Setup > Switch Parameters > Port Stats (Mini-RMON)** の順に移動して、テーブルに Current Status を表示します。Mini-RMON をイネーブルにする方法の詳細については、P.3-36 の「Mini-RMON 収集のイネーブル化」を参照してください。

NM-NAM デバイスの場合

接続があることを確認するには、コミュニティ ストリングが設定されていることを確認します。また、**Setup>Router Parameters** の順に移動し、**Test** ボタンをクリックすると、コミュニティ ストリングが正しいかどうかを確認できます。ルータのコミュニティ ストリングのテストの詳細については、P.3-26 の「ルータのコミュニティ ストリングのテスト」を参照してください。

Q. Alarms ウィンドウに負の数が表示されるのはなぜですか。

A. アラーム カウンタが直前のポーリングと現在のポーリング間で 0 に設定されています。

Q. ポートまたはインターフェイス統計情報の Cumulative Data テーブルをロードするのに時間がかかるのはなぜですか。

A. 接続に問題があるか、または接続が存在していない可能性があります。接続を確認するには、**Setup >Switch Parameters** の順に移動し、**Test** をクリックします。

（注） NM-NAM デバイスの場合、**Setup>Router Parameters** の順に移動します。

NetFlow および NBAR の監視の問題

Q. デバイスのデフォルトの NetFlow データ ソースにデータがないのはなぜですか。

A. **Setup** > **Data Sources** > **NetFlow** > **Listening Mode** の順に選択し、**Start** をクリックします。デバイスがテーブルに表示される場合は、P.A-11 の「Listening Mode テーブルは NAM がデバイスから NDE パケットを受信していることを示しているのに、収集にデータがないのはなぜですか。」を参照してください。3 回のリフレッシュ サイクルの後でもデバイスがテーブルに表示されない場合、NAM はそのデバイスからの NetFlow パケットを検出していません。ネットワークに問題があるか、デバイスの設定が正しくありません。

NetFlow デバイスが NetFlow パケットを NAM の UDP ポート 3000 に送信するように設定されていることを確認するには、次のコマンドを使用します。

```
prompt#show ip flow export
```

または

```
prompt#show mls nde
```

表示される情報は、NetFlow のエクスポートがイネーブルまたはディセーブルのどちらになっているか、NetFlow パケットのエクスポート先の IP アドレスとポート、および NAM に送信された NDE パケットの数を示しています。NetFlow デバイスの設定の詳細については、P.3-15 の「デバイスの NetFlow 設定」または付属のデバイス マニュアルを参照してください。

Q. Listening Mode テーブルは NAM がデバイスから NDE パケットを受信していることを示しているのに、収集にデータがないのはなぜですか。

A. **Monitor** > **Hosts**、**Monitor** > **Apps** および **Monitor** > **Conversations** の各ページで、収集にデータがあることを確認します。Monitor ページに NetFlow データがある場合は、自動リフレッシュ インターバルが短すぎる可能性があります。自動リフレッシュ インターバルのトラブルシューティングの詳細については、P.A-11 の「Monitor> Hosts、Monitor > Apps、および Monitor > Conversations の各ページに、2 回（またはそれ以上）の自動リフレッシュ サイクルごとしかデータが表示されないのはなぜですか。」および P.A-14 の「Monitor>Conversations ページの Network Conversations テーブルで、ソース カラムのすべてのエントリが 0.0.0.0 になっているのはなぜですか。」を参照してください。

Monitor ページに NetFlow データがない場合は、互換性のない NDE のバージョンを使用している可能性があります。NDE のバージョンが 1、5、6、7、または 8 であることを確認します。詳細については、P.A-12 の「Monitor>Hosts ページおよび Monitor>Conversations ページにアクティブなフロー データがないのはなぜですか。」を参照してください。

（注） NDE バージョン v8-AS-Aggregation はサポートされていません。

Q. **Monitor> Hosts**、**Monitor** > **Apps**、および **Monitor** > **Conversations** の各ページに、2 回（またはそれ以上）の自動リフレッシュ サイクルごとしかデータが表示されないのはなぜですか。

A. NDE ソース デバイスの実装に原因があります。NetFlow キャッシュのエントリは、接続の終了が検出された場合、または期限の時間に達した場合など、非アクティブの特定のレベルになると期限切れになります。期限切れになったフローも、宛先にエクスポートされます。エージング タイムが NAM のリフレッシュ インターバルよりも長い場合、NAM の 1 回のリフレッシュ インターバルでは NetFlow パケットが表示されません。

この問題を解決するには、**Setup** > **Preferences** の順に選択し、NAM の自動リフレッシュ インターバルを長くするか、NetFlow エントリのエージング タイムを変更します。NDE ソース デバイスでエージング タイムを変更する前に、NDE の使用に関するガイドラインを参照してください。

Cisco IOS を実行しているデバイスの場合、次のコマンドを使用してエージング タイムを指定します。

```
Prompt(config)#ip flow-cache timeout <active | inactive> <seconds>
```

または

```
Prompt(config)#mls aging <fast time | long | normal> <seconds>
```

Catalyst OS を実行しているデバイスの場合、次のコマンドを使用してエージング タイムを指定します。

```
Prompt>(enable) set mls agingtime <long-duration | fast | ip>
```

コマンドの意味は次のとおりです。

- long-duration：長い時間アクティブなフローのエージング タイムを設定します。
- fast：パケットしきい値を超えないフローのエージング タイムを設定します。
- ip：IP フローのエージング タイムを設定します。

Q. カスタム NetFlow データ ソースに収集がないのはなぜですか。

A. データ ソースが入力方向のインターフェイスで設定されていることを確認します。出力および双方向は、特別な場合にのみ推奨されます。これらの設定では、すべてのインターフェイスで NetFlow をイネーブルにして、包括的な出力方向のフロー データを取得することが必要な場合があります。NetFlow フロー レコードの詳細については、P.3-14 の「NetFlow フロー レコードについて」を参照してください。

NetFlow Listening Mode テーブルの Detail ボタンをクリックして、インターフェイスの方向を確認できます。NetFlow Listening Mode の使用方法の詳細については、P.3-24 の「リスニング モードの使用方法」を参照してください。

カスタム NetFlow データ ソースが、正しくないインターフェイス ifIndex でデータを収集している可能性もあります。これは、デバイスのリブート後に持続していないリモート NetFlow デバイスの ifIndex に原因があります。サポートされるすべてのデバイスで、ifIndex 持続機能を使用することをお勧めします。Cisco IOS を実行しているデバイスの場合、ifIndex はインターフェイスごとに持続したり、すべての ifIndex でグローバルに持続することができます。
例：

- snmp ifindex persist
- snmp-server ifindex persist

Catalyst OS を実行しているデバイスの場合、ifIndex は常に持続されます。

Q. Monitor>Hosts ページおよび Monitor>Conversations ページにアクティブなフロー データがないのはなぜですか。

A. アクティブ フローが期限切れになっていないか、デバイスに NDE フィルタがあるか、またはキャッシュがいっぱいで新しいエントリをキャッシュに挿入できないことが原因です。いずれの場合も、NAM にエクスポートされている NetFlow パケットにアクティブ フローがありません。

この問題を解決するには、デバイスに NDE フィルタがないことを確認し、長いエージング タイムおよびドロップされたフロー パケットがあるかどうかをチェックします。

長いエージング タイムをチェックしてアクティブ フローが期限切れになっているかどうかを確認するには、次のいずれかのコマンドを入力します。

```
Prompt>(enable)show ip cache flow

Prompt>(enable)show mls netflow aging

Prompt>(enable)show mls
```

アクティブ時間が長期エージング タイムよりも短いアクティブ フローは、まだ期限切れにならず、NAM にエクスポートされていません。エージング タイムはさらに小さい値に設定できます。設定方法については、NDE デバイスのユーザ マニュアルを参照してください。

Q. 特定のインターフェイスに対して設定した NetFlow データ ソースにはデータがなく、デフォルトの NetFlow データ ソースにデータが*ある*のはなぜですか。

A. 特定のインターフェイス情報を持つ NetFlow レコードがないことが考えられます。リスニング モードを使用して、NetFlow レコードを持つインターフェイスを検索します。

ステップ 1　**Setup** > **Data Sources** > **NetFlow**> **Listening Mode** を選択します。

ステップ 2　**Start** をクリックします。

ステップ 3　デバイス テーブルの MDE パケット カウントが 3 を超えるまで待ちます。

ステップ 4　対象デバイスを選択します。

ステップ 5　**Details** をクリックします。

インターフェイスが Details ウィンドウにない場合は、NetFlow ソース デバイスを手動で設定する必要があります。

Cisco IOS を実行しているデバイスの場合

```
Prompt(config)#interface <type> <slot/port>
Prompt(config-if)#ip route cache flow
Prompt(config)#mls nde interface
```

Catalyst OS を実行しているデバイスの場合

```
Prompt>(enable) set mls nde destination-ifindex enable
Prompt>(enable) set mls nde source-ifindex enable
```

フロー マスクが full または interface-full に設定されていることを確認してください。

Q. **Setup** > **Data Sources** > **NetFlow** > **Custom Data Sources** ページで NetFlow データ ソースを作成した場合、ドロップダウン リストにローカル デバイス アドレスしか表示されないのはなぜですか。

A. はじめに **Setup** > **Data Sources** > **NetFlow** > **Devices** ページでデバイスを追加する必要があります。デバイスのデフォルトの NetFlow データ ソースが **Setup** > **Data Sources** > **NetFlow** > **Custom Data Sources** ページに表示されます。これでドロップダウン リストにそのデバイスが表示されます。

Q. NetFlow データ ソースの作成時に、利用できるインターフェイス リストがないのはなぜですか。

A. コミュニティ ストリングが正しいことを確認します。**Setup** > **Data Sources** > **NetFlow** > **Devices** ページで NetFlow Devices テーブルの Test ボタンを使用します。詳細については、P.3-21 の「デバイスのテスト」を参照してください。

エラーが発生する場合は、コミュニティ ストリングが正しくない可能性があります。NetFlow Devices テーブルからデバイスを選択し、**Edit** をクリックして、正しいコミュニティ ストリングを入力します。リモート デバイスが SNMP 接続を受け入れることも確認します。

Q. Monitor>Conversations ページの Network Conversations テーブルで、ソース カラムのすべてのエントリが 0.0.0.0 になっているのはなぜですか。

A. NDE デバイスでフロー マスクが destination に設定されているためです。フロー マスクを full、interface-destination-source、または interface-full に設定するには、次のコマンドを使用します。

Cisco IOS を実行しているデバイスの場合

```
Prompt(config)#mls flow ip <full | interface-full>
```

Catalyst OS を実行しているデバイスの場合

```
Prompt>(enable) set mls flow full
```

(注) NAM では NDE バージョン 1、5、6、7、8、送信元プレフィックス、送信先プレフィックス、プレフィックス、およびプロトコル ポート集約がサポートされています。

フロー マスクおよび Monitor ページの詳細については、P.4-5 の「NDE フロー マスクおよび V8 集約キャッシュ」を参照してください。

Q. スイッチで NBAR を使用できないのはなぜですか。

A. Catalyst 6500 スイッチでコマンドラインを使用して NBAR を設定できますが、現在、このスイッチは NBAR を設定および監視するための MIB を提供していません。

レポートの問題

Q. 一部またはすべての期間で、レポートにデータが表示されないのはなぜですか。

A. これにはいくつかの原因が考えられます。

- レポートが最近作成され、データがまだ収集されていない可能性があります。最初のデータ ポイントを表示するには、最低 2 ポーリング インターバルが必要です。
- 適切なトラフィック データ ソースが NAM に送信されていません。たとえば、SPAN セッションの設定が不適切で、レポート用の適切なトラフィックが含まれていない可能性があります。**Setup** > **Data Source** に移動して、レポートのデータ ソースが適切に設定されていることを確認します。
- レポートがディセーブルになっています。
- NAM はその期間にシャットダウンされていたか、または実行されていません。
- レポート ターゲットが非アクティブです。

Q. レポート ステータスが OK を示しているのに、一部またはすべての期間でレポートにデータがないのはなぜですか。

A. エラー条件または例外が発生している可能性があります。レポート ウィンドウで表レポート スタイルを選択し、**system events** をクリックして、レポート エラー条件および例外を表示します。レポート エラー条件および例外の詳細については、表 5-13 を参照してください。

Q. すべての PortStat レポートにデータがないのはなぜですか。

A. PortStat レポートでは、スイッチが Mini-RMON 機能を持っている必要があります。スイッチが Mini-RMON をサポートし、その機能がイネーブルになっていることを確認します。

Q. すべての VLAN レポートにデータがないのはなぜですか。

A. Supervisor エンジン モジュールをデータ ソースとする Top N VLAN レポートおよびターゲット VLAN レポートでは、スイッチの Supervisor が SMON 機能を持っている必要があります。Supervisor エンジン モジュールが SMON 機能をサポートし、その機能がイネーブルになっていることを確認します。

Q. Response Time レポートのデータが複数の間隔で一定なのはなぜですか。

A. 選択したレポート インターバルが長すぎる可能性があります。**Setup** > **Monitor**> **Response Time Monitoring** の順に選択し、短いレポート インターバルを選択します。Response Time レポートと同じポーリング インターバルを選択することをお勧めします。たとえば、レポートで 60 分のレポート インターバルおよび 15 分のポーリング インターバルを選択した場合、レポート データが頻繁にポーリングされ、連続する 15 分のインターバル 4 回で同じデータが繰り返し表示されます。

Q. DNS 解決の設定を変更すると、レポートにどのような影響がありますか。

A. Monitor ウィンドウでレポートを表示できなくなります。DNS をオンにしてレポートを作成した場合、DNS 名をホストとしてレポートが設定されます。次に DNS をオフにすると、Monitor ウィンドウは DNS 名の代わりに IP アドレスを参照します。

イメージのアップグレードおよびパッチの問題

Q. NAM のアプリケーション イメージのアップグレードをどのように行いますか。

A. NAM-1 および NAM-2 の場合は、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Network Analysis Module Installation and Configuration*』を参照してください。

(注) NM-NAM の場合は、『*Network Analysis Module (NM-NAM) Feature Guide*』を参照してください。

Q. NAM イメージのアップグレード中に問題が起きるのはなぜですか。

A. 次の点を確認してください。

1. NAM を正しいパーティションに入れて起動している。
   - NAM アプリケーション イメージをアップグレードするには、NAM をメンテナンス パーティションに入れて起動する必要があります。
   - NAM メンテナンス イメージをアップグレードするには、NAM をアプリケーション パーティションに入れて起動する必要があります。
2. URL が正しいイメージの場所を指定している。正しくない場合は、正しい URL を入力します。
3. アップグレードが中断されていない。中断された場合は、NAM をリブートして、アップグレードを再開します。

(注) 詳細については、『*Network Analysis Module (NM-NAM) Feature Module*』を参照してください。

Q. パッチの適用時に問題が発生するのはなぜですか。

A. 次の点を確認してください。

- URL が正しいイメージの場所を指定しているか。正しくない場合は、正しい URL を入力します。
- パッチ プロセスが中断されたか。中断された場合は、プロセスを再開します。

Q. NAM にインストールされているパッチを確認するにはどうしたらよいですか。

A. コマンドラインの **show patches** コマンドを使用するか、または NAM Traffic Analyzer のユーザ インターフェイスのツールバーで **About** をクリックします。

Web ブラウザの応答時間および表示の問題

Q. ブラウザ ウィンドウ（Packet Decode ウィンドウまたは Monitor タブの下のウィンドウなど）のリフレッシュが非常に遅いことがあるのはなぜですか。

Q. Packet Decoder ウィンドウで、パケットの表示が非常に遅いのはなぜですか。

A. DNS ネーム サーバが有効な DNS サーバを指定していることを確認する必要があります。

ヒント

- ネーム サーバが、存在しないまたは設定に誤りのある DNS サーバを指定している場合、検索が 20 ～ 30 秒後にタイムアウトします。
- DNS のない環境では、ネーム サーバを設定しないでください。
  自動ホスト名解決もオフにすることが必要な場合もあります。

ステップ 1　**Setup** > **Preferences** を選択します。

ステップ 2　Perform IP Host Name Resolution チェックボックスをオフにします。

ステップ 3　**Apply** をクリックします。

（注）　詳細については、P.A-19 の「ホスト名解決の問題」を参照してください。

ソートおよび表示されるデータ量が原因で、ブラウザ ウィンドウのリフレッシュが遅くなることもあります。収集（会話の数など）を制限し、該当する（Setup タブの）Monitoring ウィンドウの最大エントリ数を減らすことで、応答時間を改善してください。

Q. ブラウザ ウィンドウまたはポップアップ ウィンドウのフォーマットが正しくないように見えることがあるのはなぜですか。

A. ブラウザ ウィンドウのフォーマットが正しくない場合は、ブラウザの **Refresh** ボタンをクリックします。ポップアップのフォーマットが正しくない場合は、ポップアップを閉じてから、再び開きます。

NAM とスイッチの日付と時刻の同期の問題

Q. NAM の日付および時刻がスイッチの日付および時刻と異なるのはなぜですか。

A. NAM の起動時、NAM の日付および時刻はスイッチの日付および時刻と同期されます。ただし、日付と時刻が一致しない場合は、**Admin**> **System**>**NAM System Time** へ移動して、NAM のシステム時刻をスイッチまたは NTP サーバと同期させます。NAM システム時刻の使用の詳細については、P.2-14 の「NAM のシステム時刻」を参照してください。

Q. NTP からスイッチに時刻の同期方式を変更すると、NAM が正しくない時刻を表示するのはなぜですか。

A. 7.5(1) 以前の Catalyst OS イメージを実行する Supervisor の場合、NAM のシステム時刻は起動時にだけスイッチと同期します。NTP 時刻からスイッチ時刻へ変更すると、NAM はスイッチと時刻を再同期しません。この問題を回避するには、NAM をリセットしてください。

診断エラー メッセージの問題

Q. Diagnostics Tech Support ウィンドウの次のエラーは何を示していますか。

```
Fri Nov 16 11:33:33 2001] [error] [client 172.20.9.52] File does not exist:
/usr/local/ apache/htdocs/scripts/..%2f../winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/scripts/root.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/MSADC/root.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/c/winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/d/winnt/system32/cmd.exe
[Fri Nov 16 11:35:31 2001] [error] [client 172.20.102.27] File does not exist:
/usr/local/ apache/htdocs/scripts/..%5c../winnt/system32/cmd.exe
```

A. これらのエラーは、ウイルスに感染したクライアントが、次の感染先システムを探していることを示している可能性があります。

一部のウイルスはポート 80 で実行している Web サーバの脆弱性を探します。次のようないくつかの対策があります。

- クライアントのウイルスを駆除する（IP アドレスを記録しておく）
- Access Control List（ACL; アクセス コントロール リスト）を実装して、NAM へのアクセスを防止する
- 別のポートで NAM の Web サーバを実行する（多くのウイルスはポート 80 だけを攻撃するため）

ホスト名解決の問題

Q. `ip hosts add ...` コマンドを使用すると、リモート ホスト ファイルのインポートに失敗するのはなぜですか。

A. これには次の原因が考えられます。

- hosts ファイルのフォーマットが正しくありません。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note Release 3.1*』を参照してください。
- ローカル ホスト ファイルは 1000 エントリまでに制限されています。1000 を超えるエントリを追加しようとしていないか確認します。NAM CLI コマンド **show tech-support** を使用して、次のような行を探します。

  `Total number of entries in hosts files: nn`

ヒント
- ファイルで設定されているエントリを調べるには、**show hosts** コマンドを使用します。
- 1000 を超えるホストを追加する必要がある場合は、DNS を使用するか、またはローカル名解決に最も重要な 1000 のホストを選択します。

Q. NAM へのリモート Telnet セッション中に大幅な遅れが生じるのはなぜですか。

A. DNS サーバ アドレスに問題がある可能性があります。DNS サーバ アドレスは、運用 DNS サーバの IP アドレスに設定する必要があります。正しくないアドレス、サーバへの接続不能、または非運用サーバが原因で NAM がサーバに接続できない場合、大幅な遅れが生じることがあります。

この問題を解決するには、DNS サーバを動作しているサーバの IP アドレスに変更するか、またはそのサーバを削除します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **Network Parameters** をクリックします。

ステップ 3　必要に応じてパラメータを変更します。

ステップ 4　**Apply** をクリックします。

NAM CLI コマンド **ip nameserver** *nameserver_addr* を使用して、特定のネーム サーバを選択するか、または **ip nameserver disable** コマンドでネーム サーバを完全に削除することもできます。

Q. 診断テクニカル サポートの出力に大幅な遅延が生じるのはなぜですか。

A. DNS サーバ アドレスに問題がある可能性があります。この問題を解決するには、DNS サーバを動作しているサーバの IP アドレスに変更するか、またはそのサーバを削除します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **Network Parameters** をクリックします。

ステップ 3　必要に応じてパラメータを変更します。

ステップ 4　**Apply** をクリックします。

NAM CLI コマンド **ip nameserver** *nameserver_addr* を使用して、特定のネーム サーバを選択するか、または **ip nameserver disable** コマンドでネーム サーバを完全に削除することもできます。

Q. **ip hosts add ...** コマンドおよび **ip hosts delete ...** コマンドを使用して、ローカル ホスト ファイルに対して特定の IP アドレスを追加または削除する場合の制限はありますか。

A. はい。127.*x.x.x* で始まる NAM IP アドレスまたは IP アドレスを使用してホスト エントリを追加または削除しないでください。

データ不一致の問題

Q. Monitor タブをクリックしてから、**Hosts** または **Conversations** をクリックしました。Network Host テーブルが表示されました。ホスト名をクリックしたとき、ポップアップ チャートおよびテーブルのデータが一致しないことがあります。このようになるのはなぜですか。

A. 詳細ポップアップのチャートおよびテーブルに使用されるデータのソースは独立しており、異なるインターバルでエージング アウトすることがあります。

HTTPS および セキュリティ証明書の問題

Q. https を使用して NAM に Web ブラウザを指定した場合、証明書の期限が満了しているという警告メッセージが表示されるのはなぜですか。

A. これは証明書の期限が満了していることが原因です。この問題を解決するには、次のいずれかを実行します。

- 自己署名証明書を生成します。
- 証明書署名要求を生成します。認証局に要求を送信し、受信した証明書をインストールします。

いずれの場合も、NAM CLI コマンドを使用します。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note Release 3.4*』を参照してください。

Q. セキュリティ証明書の名前がサイトの名前と一致しないという警告メッセージが Web ブラウザに表示された場合はどうしたらよいですか。

A. この問題を解決するには、次のいずれかを実行します。

- 自己署名証明書を生成します。この場合は、証明書署名要求を再利用するかどうかを確認する画面が表示されるので、**no** と入力します。これで新しい証明書署名要求と自己署名証明書が生成されます。通常名を要求された場合は、ホスト名を入力します。
- 証明書署名要求を生成します。通常名を要求された場合は、ホスト名を入力します。認証局に要求を送信し、受信した証明書をインストールします。

  いずれの場合も、NAM CLI コマンドを使用します。詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Network Analysis Module Installation and Configuration Note Release 3.4*』を参照してください。

  上記の操作を実行しても警告メッセージが表示される場合は、ブラウザのアドレス ウィンドウに NAM の完全ホスト名を入力してください。たとえば、NAM の完全ホスト名が nam1.cisco.com の場合は、https:/nam1 ではなく、https://nam1.cisco.com と入力します。

Q. 信頼していない会社によってセキュリティ証明書が発行されたという警告メッセージがブラウザに表示された場合はどうしたらよいですか。

A. 証明書を表示して、その認証局を信頼するかどうかを判断します。NAM の HTTPS 証明書が工場（テスト）証明書、または自己署名証明書である場合、このメッセージが表示されることがあります。**Proceed** をクリックします。

SNMP の問題

Q. NAM は SNMPv3 をサポートしていますか。

A. NAM は、Mini-RMON ポート統計情報およびスイッチベースのアラームについて NAM と対話する外部 SNMP マネージャおよびスイッチと対話する NAM の両方を含む、SNMPv1 および SNMPv2c だけをサポートします。

Q. Router Parameters ダイアログボックスで **Test** をクリックすると、ルータからの SNMP 読み取りに失敗したというウィンドウが表示されます。

A. 入力された SNMP リード / ライト コミュニティ ストリングが、ルータ用に定義された SNMP リード / ライト コミュニティ ストリングと同じであることを確認する必要があります。コミュニティ ストリングが正しくてもテストに失敗する場合は、ルータで IP 許可リストがイネーブルになっていることを確認します。

Catalyst OS を実行しているスイッチの場合のみ

ステップ 1　イネーブル モードでスイッチにログインします。

ステップ 2　**show IP permit** と入力します。

IP 許可リストがイネーブルになっている場合、NAM の内部アドレスがそのリストに追加されていることを確認します。

（注） Traffic Analyzer で NAM の内部 IP アドレスを表示するには、**Setup>Switch Parameters** を選択し、Switch Community String ダイアログボックスの **Test** をクリックします。Switch Community String Test ダイアログボックスが表示されます。

set IP permit *NAM ip address* **SNMP** と入力します。

Q. NAM Traffc Analyzer を使用するとき、NAM SNMP エージェントをイネーブルにする必要がありますか。

A. いいえ。外部 SNMP マネージャからの SNMP 通信をサポートするために必要なのは SNMP エージェントだけです。NAM で SNMP をディセーブルにするには、次の手順を実行します。

ステップ 1　**Admin** > **System** を選択します。

ステップ 2　コンテンツで **NAM SNMP** をクリックします。

ステップ 3　NAM Community Strings ペインで、すべての NAM コミュニティ ストリングを選択し、削除します。

プロトコル サポートの問題

Q. 一部のプロトコル（sunrpc など）が、アプリケーション統計情報ウィンドウで 2 回表示されることがあるのはなぜですか。

A. 最上位のプロトコルだけが表示されます。場合によっては、上位のプロトコルが複数の下位レイヤ プロトコル上で実行されることがあります。たとえば、sunrpc は TCP と UDP で実行されます。NAM Traffic Analyzer では、この 2 つを区別するため、2 行の項目が表示されます。そのプロトコルの上にマウスのポインタを置くと、関連するすべてのプロトコル スタックが小さなポップアップに表示されます。

Q. Monitor タブ、**DiffServ**、**Application Stats** の順にクリックすると、下位レイヤ プロトコルの TCP に比べて 1 秒あたりのパケット数（またはバイト数）が多い http などのプロトコルが表示されることがあります。このようになるのはなぜですか。

A. Differentiated Services 監視（DiffServ）統計情報では、使用可能な最上位のプロトコルのパケットだけがカウントされます。したがって、...tcp.http パケットは http パケットとしてのみカウントされます。TCP として分類されたパケットは、NAM が処理できる最上位のパケットだったことを意味しています。これは、認識されていない TCP ポート、または分類する先行パケットを NAM が検出しなかった状態ベースのプロトコルが原因で発生した可能性があります。

Q. NAM がサポートするすべてのプロトコルのリストはどこにありますか。

A. NAM が監視するすべてのプロトコルのリストは、**Setup>Monitor** の Protocol Directory テーブルに表示されます。SNMP ツールを使用して、プロトコルを取得したり更新したりすることもできます。

Q. **Setup>Capture>Settings** ページにプロトコルのリストが表示されないのは、NAM でそのプロトコルが認識されないことが原因で、Monitor ディスプレイに表示されないのでしょうか。

A. Protocols チェックボックスがオンになっていて Protocols ドロップダウン リストで All が選択されている場合、NAM が監視できるプロトコルすべてが選択ボックスに一覧表示されます。Protocols ドロップダウン リストを使用して、特定の環境のプロトコルの適切なサブセットを選択できます。

Q. NAM が Monitor ディスプレイ（Monitor Apps、Monitor Overview など）で追跡するすべてのプロトコルは、Capture Decode ダイアログボックスでデコードできますか。

A. いいえ。デコードは、NAM でサポートされている一部のプロトコルでしか利用できません。デコードを追加するには、サードパーティ製アプリケーションの使用を検討してください。Capture Download 機能を使用して、トレース ファイルをサードパーティ製アプリケーションにエクスポートできます。

Q. 一部の NAM Web ウィンドウ上の「*others*」というプロトコル エントリは何を表していますか。

A. 「*others*」というプロトコル エントリは、パケット データで NAM が最上位のアプリケーション層を識別できないトラフィックの合計を表します。たとえば、認識されない TCP/UDP ポートや、NAM がセットアップ トランザクションを解析できない動的に割り当てられたポートです。詳細を入手する唯一の方法は、NAM のキャプチャ機能を使用してパケット データをキャプチャし、**Capture>Decode** ウィンドウで完全にデコードできていないパケットを検索することです。

音声監視の問題

Q. VoIP 電話および通話を表示する詳細ウィンドウで、一部のカラムがブランクになっているのはなぜですか。

A. NAM が VoIP トラフィックに提供できる詳細情報の量は、IP Phone、CallManager、および H.323 ゲートキーパー、および MGCP ゲートウェイに関連する NAM の物理的配置によって変わります。また、スイッチまたはルータのどのトラフィックのサブセットが NAM にスパンまたはコピーされているかによっても異なります。NAM はリモート ネットワーク上の電話に対するコール セットアップ トランザクションを直接監視できないことがあります。通常は、NAM が監視できる電話および通話のすべての詳細情報は、Web ディスプレイのフィールドに表示されます。

Q. 一部のディスプレイでは、電話プロトコルが実際とは異なる SCCP（H.323 または MGCP）として表示されるのはなぜですか。

A. 電話に関連付けられたプロトコルは、必ずしも電話機で使用されるプロトコルではなく、NAM が最初に電話機を認識したプロトコルを示しています。

たとえば、SCCP 電話機が H.323 電話機を呼び出し、NAM がコール セットアップの SCCP 側だけを直接監視している場合、SCCP プロトコルは通話の両側に関連付けられます。NAM はこのようにして両方の電話機を認識します。

Q. SCCP 通話の品質統計情報（ジッタ、パケット損失）が表示されないのはなぜですか。

A. NAM が SCCP 通話のジッタおよびパケット損失統計情報をレポートするには、Cisco CallManager で Call Maintenance Record および Call Detail Record をイネーブルにする必要があります。

Cisco Call Manager 3.1 で CMR および CDR をオンにするには、次の手順を実行します。

ステップ 1　Cisco CallManager Administration ウィンドウに移動します。

ステップ 2　**Service > Service Parameters** の順に選択します。

ステップ 3　Cisco CallManager サーバの IP アドレスを選択します。

ステップ 4　**Next** ボタンをクリックします。

ステップ 5　Cisco CallManager サービスを選択します。

ステップ 6　Parameter Value フィールドで、Call Diagnostics Enabled に対して **True** を選択します。

ステップ 7　CdrEnabled サービス パラメータまで下にスクロールし、その値に **True** を選択します。

ステップ 8　**Update** ボタンをクリックします。

ステップ 9　呼詳細レコードのロギングがすぐに開始されます。

（注）　この手順は CallManager version 3.1 だけで有効です。ただし、他のバージョンでも、よく似たプロセスを使用します。

Q. **Monitor**>**Voice**>**Known Phones** ウィンドウの MGCP エンドポイントは何ですか。

A. MGCP エンドポイント エントリは、複数の IP Phone が PSTN の電話機と通信するために使用する、MGCP ゲートウェイ トランク ポートを表します。

Q. 一部の MGCP Call Detail テーブルに Q.931 詳細情報が含まれているのはなぜですか。

A. Cisco CallManager と Cisco MGCP ゲートウェイ トラフィックが NAM にコピーされると、MGCP コールの電話番号および電話エイリアス情報が Q.931 トラフィックから取得されることがあります。このようなことがあれば、MGCP Call Detail テーブルは、詳細情報を含む Q.931 テーブルを分離します。

APPENDIX **B**

サポートされている MIB オブジェクト

NAM は、次の MIB グループをすべてサポートしています。

- RMON
- RMON2
- DSMON
- 大容量 RMON：medialIndependentGroup を除く
- SMON
- Application Response Time（ART; アプリケーション応答時間）MIB

サポートされている MIB

表 B-1 に、スーパーバイザ エンジンと NAM でサポートされる RMON オブジェクトと RMON2 MIB オブジェクトを示します。スーパーバイザ エンジンは、表 B-1 で指定されている RMON MIB からいくつかのオブジェクトを実装します。スーパーバイザ エンジンの RMON 実装は、NAM 実装から完全に独立しています。また、MIB オブジェクトはまったく共有されません。

スイッチの物理インターフェイスから etherStats を収集するには、NAM ではなくスーパーバイザ エンジンで etherStatTable を設定します。etherStats は、複数の物理インターフェイスで同時に、正確に収集されます。

特定の VLAN 用に etherStats を収集する場合は、NAM で etherStatsTable を設定します。データ ソースの場合は、その VLAN に対応している ifIndex を使用します。

スーパーバイザ エンジンで設定されている alarmVariable はすべて、スーパーバイザ エンジンで MIB オブジェクトを参照する必要があります。NAM で設定されている alarmVariable は、NAM で MIB オブジェクトを参照する必要があります。

(注) スーパーバイザ エンジンで MIB オブジェクトを参照する NAM の alarmVariable は設定できません。また、NAM で MIB オブジェクトを参照するスーパーバイザ エンジンの alarmVariable は設定できません。

表 B-1　Supervisor エンジン モジュールと NAM RMON サポート

モジュール	オブジェクト識別子（OID）と説明	ソース
Supervisor Engine	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1) ...mib-2(1).rmon(16).statistics(1).tokenRingMLStats Table(2)...mib-2(1).rmon(16).statistics(1).tokenRingPStatsTable(3)	RFC 2819（RMON-MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB）
	パケット、オクテット、ブロードキャスト、エラーなどのカウンタ。	
Supervisor Engine	...mib-2(1).rmon(16).history(2).historyControlTable(1) ...mib-2(1).rmon(16).history(2).etherHistoryTable(2) ...mib-2(1).rmon(16).history(2).tokenRingMLHistory Table(3)...mib-2(1).rmon(16).history(2).tokenRingPHistoryTable(4)	RFC 2819（RMON-MIB） RFC 2819（RMON-MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB）
	後で検索するために、統計グループのカウンタを定期的にサンプリングおよび保存します。	
Supervisor Engine	...mib-2(1).rmon(16).alarm(3)	RFC 2819（RMON-MIB）
	ネットワーク マネジメントのために重要な RMON 変数で設定できるしきい値。	
Network Analysis	...mib-2(1).rmon(16).alarm(3)	RFC 2819（RMON-MIB）
	ネットワーク マネジメントのために重要な RMON 変数で設定できるしきい値。	
Network Analysis	...mib-2(1).rmon(16).hosts(4)	RFC 2819（RMON-MIB）
	セグメント上またはポート上の各ホスト デバイスで統計情報を保持します。	
Network Analysis	...mib-2(1).rmon(16).hostTopN(5)	RFC 2819（RMON-MIB）
	統計カウンタ別にソートされたホスト グループのユーザ定義サブセット レポート。	
Network Analysis	...mib-2(1).rmon(16).statistics(1).etherStatsTable(1)	RFC 2819（RMON-MIB）
Network Analysis	...mib-2(1).rmon(16).matrix(6)	RFC 2819（RMON-MIB）
	ネットワーク上のホスト間の会話の統計情報を保持します。	
Network Analysis	...mib-2(1).rmon(16).filter(7)	RFC 2819（RMON-MIB）
	指定したパターンに一致するフレームからパケット ストリームを生成するフィルタ エンジン。	
Network Analysis	...mib-2(1).rmon(16).capture(8)	RFC 2819（RMON-MIB）
	マネジメント コンソールへアップロードするために、フィルタ グループによってキャプチャされたパケットのバッファを管理します。	
Supervisor Engine	...mib-2(1).rmon(16).event(9)	RFC 2819（RMON-MIB）
	アラーム グループのしきい値を超えてイベントを記録すると、SNMP トラップを生成します。	
Network Analysis	...mib-2(1).rmon(16).event(9)	RFC 2819（RMON-MIB）
	アラーム グループのしきい値を超えてイベントを記録すると、SNMP トラップを生成します。	

表 B-1　Supervisor エンジン モジュールと NAM RMON サポート（続き）

モジュール	オブジェクト識別子（OID）と説明	ソース
SupervisorEngine	...mib-2(1).rmon(16).tokenRing(10).ringStationControlTable(1) ...mib-2(1).rmon(16).tokenRing(10).ringStationTable(2) ...mib-2(1).rmon(16).tokenRing(10).ringStationOrderTable(3) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigControlTable(4) ...mib-2(1).rmon(16).tokenRing(10).ringStationConfigTable(5) ...mib-2(1).rmon(16).tokenRing(10).sourceRoutingStatsTable(6)	RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB） RFC 1513（TOKEN-RING-RMON MIB）
	詳細なトークン リング統計情報を集約します。	
Network Analysis	...mib-2(1).rmon(16).protocolDir(11)	RFC 2021（RMON2-MIB）
	Network Analysis Module が統計情報をモニタおよび維持するプロトコルのテーブル。	
Network Analysis	...mib-2(1).rmon(16).protocolDist(12)	RFC 2021（RMON2-MIB）
	protocolDir(11) 内のプロトコルごとの統計情報のテーブル。	
Network Analysis	...mib-2(1).rmon(16).addressMap(13)	RFC 2021（RMON2-MIB）
	MAC 層アドレスとネットワーク層アドレスのバインディングのリスト。	
Network Analysis	...mib-2(1).rmon(16).nlHost(14)	RFC 2021（RMON2-MIB）
	ネットワーク層アドレスごとの統計情報。	
Network Analysis	...mib-2(1).rmon(16).nlMatrix(15)	RFC 2021（RMON2-MIB）
	ネットワーク層アドレスのペアのトラフィック統計情報。	
Network Analysis	...mib-2(1).rmon(16).alHost(16)	RFC 2021（RMON2-MIB）
	ネットワーク アドレスごとのアプリケーション層プロトコルによる統計情報。	
Network Analysis	...mib-2(1).rmon(16).alMatrix(17)	RFC 2021（RMON2-MIB）
	ネットワーク層アドレスのペアの、アプリケーション層プロトコルによるトラフィック統計情報。	
Network Analysis	...mib-2(1).rmon(16).usrHistory(18)	RFC 2021（RMON2-MIB）
	RMON1 リンク層の統計情報を、RMON、RMON2、MIB-I、または MIB-II 統計情報をすべて含むように履歴を拡張します。	
Supervisor Engine	...mib-2(1).rmon(16).probeConfig(19)	RFC 2021（RMON2-MIB）
	エージェントの機能と設定のリストを表示します。	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1) dataSourceCaps(1).dataSourceCapsTable(1)	RFC 2613（SMON-MIB）
	物理エンティティおよび VLAN を ifEntries にマップします。	
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIBObjects(1) smonStats(2).smonVlanStatsControlTable(1)	RFC 2613（SMON-MIB）
	VLAN ID 番号によるトラフィック統計情報。	

表 B-1　Supervisor エンジン モジュールと NAM RMON サポート（続き）

モジュール	オブジェクト識別子（OID）と説明	ソース
Network Analysis	...mib-2(1).rmon(16).switchRMON(22).smonMIB Objects(1).smonStats(2).smonPrioStatsControlTable(3)	RFC 2613（SMON-MIB）
	802.1p ユーザ優先順位値によるトラフィック統計情報。	
Network Analysis	...frontier(141).mibdoc2(2).netscout2(1).art(5).art ControlTable(2)	draft-warth-rmon2-artmib-01.txt（ART-MIB）
	ART 統計情報。	
Network Analysis	...mib-2(1).rmon(16).mediaIndependentStats(21)	RFC 3273（HC-RMON-MIB）
	パケット、オクテット、ブロードキャスト、エラーなどのカウンタ。	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonAggObjects(1). dsmonMaxAggGroups(1)rmon.dsmonMib(26).dsmonObjects(1). dsmonAggObjects(1).dsmonAggControlLocked(2)rmon.dsmon Mib(26).dsmonObjects(1).dsmonAggObjects(1).dsmonAggControl Changes(3)rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1)..dsmonAggControlLastChangeTime(4)rmon.dsmon Mib(26).dsmonObjects(1).dsmonAggObjects(1).dsmonAggControl Table(5)rmon.dsmonMib(26).dsmonObjects(1).dsmonAgg Objects(1).dsmonAggProfileTable(6)rmon.dsmonMib(26).dsmon Objects(1).dsmonAggObjects(1).dsmonAggGroupTable(7)	RFC 3287（DSMON-MIB）
	集約またはプロファイルを制御する変数およびテーブル。	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonStatsObjects(2). dsmonStatsControlTable(1)rmon.dsmonMib(26).dsmonObjects(1). dsmonStatsObjects(2).dsmonStatsTable(2)	RFC 3287（DSMON-MIB）
	データ ソースあたりの統計情報の収集テーブル。	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonPdistObjects(3). dsmonPdistCtlTable(1)rmon.dsmonMib(26).dsmonObjects(1). dsmonPdistObjects(3).dsmonPdistStatsTable(2)rmon.dsmon Mib(26).dsmonObjects(1).dsmonPdistObjects(3).dsmonPdistTop NCtlTable(3)rmon.dsmonMib(26).dsmonObjects(1).dsmonPdist Objects(3).dsmonPdistTopNTable(4)	RFC 3287（DSMON-MIB）
	プロトコルあたりの統計情報の収集テーブル。	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonHostObjects(4). dsmonHostCtlTable(1)rmon.dsmonMib(26).dsmonObjects(1). dsmonHostObjects(4).dsmonHostTable(2)rmon.dsmonMib(26). dsmonObjects(1).dsmonHostObjects(4).dsmonHostTopNCtl Table(3)rmon.dsmonMib(26).dsmonObjects(1).dsmonHost Objects(4).dsmonHostTopNTable(4)	RFC 3287（DSMON-MIB）
	ホストあたりの統計情報の収集テーブル。	
	rmon.dsmonMib(26).dsmonObjects(1).dsmonCapsObjects(5). dsmonCapabilities(1)	RFC 3287（DSMON-MIB）
	DSMON 機能の変数。	

表 B-1　Supervisor エンジン モジュールと NAM RMON サポート（続き）

モジュール	オブジェクト識別子（OID）と説明	ソース
	rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixCtlTable(1)rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixSDTable(2)rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixDSTable(3)rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixTopNCtlTable(4)rmon.dsmonMib(26).dsmonObjects(1).dsmonMatrixObjects(6).dsmonMatrixTopNTable(5)	RFC 3287（DSMON-MIB）
	マトリクス統計情報の収集テーブル。	
Supervisor Engine	...ciscoMgmt(9).ciscoNbarProtocolDiscoveryMIB(244).cnpdMIBObjects(1).cnpdStatus(1)	CISCO-NBAR-PROTOCOL-DISCOVER-MIB
	NBAR プロトコル検出が有効であるかどうかをインターフェイスごとに示します。	
Supervisor Engine	...ciscoMgmt(9).ciscoNbarProtocolDiscoveryMIB(244).cnpdMIBObjects(1).cnpdAllStats(2)	CISCO-NBAR-PROTOCOL-DISCOVER-MIB
	NBAR プロトコル検出に関するインターフェイスごとの統計情報。	
Network Analysis	...mib-2(1).entityMIB(47).entityMIBObjects(1).entityPhysical(1).entPhysicalTable(1)	RFC 2737（ENTITY-MIB）
	エンティティの物理的な説明。	
Network Analysis	...mib-2(1).entityMIB(47).entityMIBObjects(1).entityGeneral(4)	RFC 2737（ENTITY-MIB）
Network Analysis	...ciscoMgmt(9).ciscoCdpMIB(23).ciscoCdpMIBObjects(1).cdpInterface(1)	CISCO-CDP-MIB
Network Analysis	...ciscoMgmt(9).ciscoCdpMIB(23).ciscoCdpMIBObjects(1).cdpCache(1)	CISCO-CDP-MIB
Network Analysis	...ciscoMgmt(9).ciscoCdpMIB(23).ciscoCdpMIBObjects(1).cdpGlobal(3)	CISCO-CDP-MIB
Supervisor Engine	...ciscoMgmt(9).ciscoProcessMIB(109).ciscoProcessMIBObjects(1).cpmCPU(1).cpmCPUTotalTable(10).cpmCPUTotalEntry(1)	CISCO-PROCESS-MIB
	CPU 統計情報。	
Supervisor Engine	...cisco(9).workgroup(5).ciscoStackMib(1).systemGrp(1).sysTrafficPeak(19)	CISCO-STACK-MIB
	ピーク トラフィック メーター値。	
Supervisor Engine	..cisco(9).workgroup(5).ciscoStackMib(1).systemGrp(1).sysTrafficPeakTime(20)	CISCO-STACK-MIB
	最後のピーク トラフィック メーター値が発生してからの時間。	
Supervisor Engine	...ciscoMgmt(9).ciscoMemoryPoolMIB(48).ciscoMemoryPoolEntry(1)	CISCO-MEMORY-POOL-MIB
	連続メモリの最大空きブロック。	

表 B-1　Supervisor エンジン モジュールと NAM RMON サポート（続き）

モジュール	オブジェクト識別子（OID）と説明	ソース
Supervisor Engine	...mgmt(20).mib-2(1).entityMIB(47).entityMIBObjects(1).entity Physical(1)	ENTITY-MIB
	物理エンティティの説明。	
Supervisor Engine	...ciscoMgmt(9).ciscoEnvMonMib(13).ciscoEnvMonObjects(10)	CISCO-ENVMON-MIB
	電力、温度、およびファンの状態。	
Supervisor Engine	...cisco(9).workgroup(5).ciscoStackMIB(1).ciscoStatckMIB Conformance(31).ciscoStaticMIBGroups(20)chassisGroup(3)	CISCO-STACK-MIB
	デバイスのシャーシに関する情報を提供するオブジェクトの集まり。	
Supervisor Engine	...ciscoMgmt(9).ciscoCat6kCrossbarMIB(217).ciscoCat6kXbar MIBObjects(1)	CISCO-CAT6K-CROSSBAR-MIB
	シャーシの統計情報。	
Supervisor Engine	...ciscoMgmt(9).ciscoMIBObjects(1).cseMIBObjects(1).cseTcam Usage(9).cseTcamUsageTable(1).cseTcamUsageEntry(1)	CISCO-SWITCH-ENGINE
	リソース タイプの説明、そのタイプに割り当てられている TCAM の総量、およびすでに使用されている割り当てリソースの量。	

INDEX

A

Applications Cumulative Data テーブル、使用　4-12, 4-17
　収集したパケット数とバイト数　4-12, 4-17
　詳細　4-18
Applications Current Rates テーブル、使用　4-9, 4-14
　アプリケーション プロトコル データのキャプチャ　4-11, 4-15
　特定のプロトコルの詳細、表示　4-10, 4-15
　リアルタイム データ、表示　4-11, 4-16
　レポート　4-11, 4-16
Applications TopN Chart、使用　4-11, 4-16
ART　4-69

C

Capture Analysis
　ドリル ダウン　6-16
Catalyst 6500 の NAM のバージョン　3-8
Client/Server Response Time Top N Chart、使用　4-77
Client/Server Response Time テーブル、使用　4-74
　詳細　4-76, 4-79
　データ、キャプチャ　4-76, 4-79
　レポート　4-76, 4-79

D

Diagnostics Tech Support ウィンドウ（図）　2-27
Differentiated Services レポート
　作成　5-4
DiffServ Application Statistics Cumulative Data テーブル、使用　4-61
DiffServ Application Statistics Current Rates テーブル、使用　4-58
　アプリケーション会話の詳細　4-59
　グラフ形式のリアルタイムの統計情報　4-59
　レポート　4-60
DiffServ Application Statistics Top N Chart、使用　4-60
DiffServ Host Statistics Cumulative Data テーブル、使用　4-65
DiffServ Host Statistics Current Rates テーブル、使用　4-62
　ホスト会話の詳細　4-63
　リアルタイム データをグラフ形式で　4-63
　レポート　4-64
DiffServ Host Statistics Top N Chart、使用　4-64
DiffServ Traffic Statistics Cumulative Data テーブル、使用　4-58
DiffServ Traffic Statistics Current Rates テーブル、使用　4-55
DiffServ Traffic Statistics Top N Chart、使用　4-57
DiffServ Traffic Statistics テーブル、使用
　リアルタイム トラフィック統計情報をグラフ形式で　4-56
　レポート　4-57
DiffServ データ、表示　4-55
　アプリケーション会話の詳細　4-59
　特定のアプリケーション プロトコルのリアルタイム トラフィック　4-59
　特定の集約グループのリアルタイム トラフィック　4-56
　特定のホストのリアルタイム データ　4-63
　ホスト会話の詳細　4-63
　役立つテーブルとチャート
　　DiffServ Application Statistics Cumulative Data テーブル　4-61
　　DiffServ Application Statistics Current Rates テーブル　4-58
　　DiffServ Application Statistics Top N Chart　4-60
　　DiffServ Host Statistics Cumulative Data テーブル　4-65
　　DiffServ Host Statistics Current Rates テーブル　4-62
　　DiffServ Host Statistics Top N Chart　4-64
　　DiffServ Traffic Statistics Cumulative Data テーブル　4-58
　　DiffServ Traffic Statistics Current Rates テーブル　4-55
　　DiffServ Traffic Top N Chart　4-57

レポート
Application Statistics 4-60
Host Statistics 4-64
Traffic Statistics 4-57
DiffServe プロファイル、管理
削除 3-41, 3-50
作成 3-40, 3-49
セットアップ 3-40
編集 3-41, 3-50
Drill-Down ボタン 6-16
DSMON のデータ収集、セットアップ 3-39

E

E メール アラーム 3-67

H

H.323
音声アラーム 3-60
音声監視 3-37
HTTPS/ セキュリティ証明書、トラブルシューティング A-21

I

Interface Stats Current Rates テーブル、使用 4-82, 4-98
Interface Top N Chart、使用 4-86
IP ホスト名の解決、応答時間の低下、トラブルシューティング 3-68

L

LastN Calls テーブル、通話の詳細の表示 4-25

M

MAC ステーション、データの監視
TopN 4-38
現在のレート 4-37
累積 4-40
MAC ステーションの会話、監視
TopN 4-46
現在のレート 4-46
累積 4-48
MGCP
音声アラーム 3-60
音声監視 3-37
MGCP ゲートウェイ、表現方法 4-24
Monitor Overview チャート、表示 4-6
MPLS インポート ログ 3-33
MPLS トラフィック統計情報 4-101

N

NAM
MIB アラームしきい値
削除 3-60
作成 3-57
設定 3-56
編集 3-59
MIB アラーム変数、選択 3-57
SNMP システム グループ、設定と表示 2-12
コミュニティ ストリング、使用 2-13
削除 2-14
作成 2-13
システム時刻、設定 2-14
NTP サーバによる設定 2-15
スイッチまたはルータとの同期 2-15
スイッチの日付/時刻の同期、～と、トラブルシューティング A-18
トラップ
削除 3-67
作成 3-66
設定 3-66
編集 3-66
バージョン 3-8
リスニング モード、使用 3-24
NAM Traffic Analyzer の GUI、ナビゲート 1-2
NAM Traffic Analyzer の概要 1-1
GUI 1-2
アラーム ログ 7-1
データ ソース 4-2
データ収集 4-2
ナビゲーションおよび制御要素 1-4
ユーザ インターフェイス コンポーネント 1-3
NAM Traffic Analyzer の設定 3-1
コミュニティ スイッチ ストリング、設定と表示 3-26
データ ソース、セットアップ 3-8

データ収集、セットアップ　3-34
DiffServe プロファイル、セットアップ　3-40
DSMON データ、監視　3-39
応答時間データ、監視　3-37
音声データ、収集　3-36
コア データ、収集　3-34
トラフィック、スパニング用の方向指定　3-8
NDE の収集タイプ（表）　3-9
NetFlow インターフェイス、～について　3-13
NetFlow デバイス、管理　3-19
NetFlow、デバイスでの設定　3-15
NetFlow レコード、～について　3-14
SPAN セッションの削除　3-13
SPAN セッションの作成　3-10
SPAN セッションの編集　3-12
SPAN ソース（表）　3-9
VACL、LAN の VLAN での設定　3-18
VACL、WAN インターフェイスでの設定　3-17
カスタム NetFlow データ ソース、作成　3-21
トラフィックの方向指定の方法（表）　3-8
リスニング モード、使用　3-24
ルータのパラメータ、表示　3-7
NAM Traffic Manager のアカウント、管理　1-6
NDE フロー マスク、と V8 集約キャッシュ　4-5
NetFlow
インターフェイス、～について　3-13
監視の問題、トラブルシューティング　A-11
データ ソース、管理
NetFlow デバイス、選択　3-22
インターフェイス、選択　3-22
削除　3-23
作成　3-21
ソース情報、確認　3-23
編集　3-23
デバイス、管理　3-19
削除　3-20
作成　3-19
テスト　3-21
編集　3-20
デバイスでの設定　3-15
Catalyst OS　3-16
Cisco IOS　3-15
NDE v8 集約　3-16
NDE のエクスポート　3-17
デバイス スロットにある NAM　3-17
マルチレイヤ スイッチングのキャッシュ　3-15
レコード、～について　3-14
NetFlow データ ソース情報の確認　3-23
NetFlow デバイスのテスト　3-21
NFS サーバ
キャプチャ データ ストレージの設定　2-18
NM-NAM デバイス
Router Parameters オプション、および　1-6
VLAN データ、および　1-7
サポートされている NAM のバージョン　3-8

P

Port Stats Current Rates テーブル、使用　4-81
詳細　4-83, 4-99
リアルタイム データをグラフ形式で　4-83
レポート　4-84
Port Stats Top N Chart、使用　4-84, 4-99
詳細　4-89
累積データ　4-87, 4-100

R

Refresh ボタン
SPAN セッションの作成　3-11
RMON
ログ テーブル、表示　7-3

S

SCCP
音声アラーム　3-60
音声監視　3-37
Server Response Time Top N Chart、使用　4-73
Server Response Time テーブル、使用
詳細　4-72
データ、キャプチャ　4-73
レポート　4-70, 4-73
SIP
音声アラーム　3-60
音声監視　3-37
SNMP
トラブルシューティング　A-22
SPAN
関連する問題、トラブルシューティング　A-7

セッション
削除 3-13
作成 3-10
編集 3-12
syslog アラームしきい値、セットアップ 3-61
System Config Log 5-19

T

TAC（Technical Assistance Center)
（「トラブルシューティング」も参照） A-1
TACACS+
サーバ、NAM サポートの設定 2-7
秘密鍵、必要なこと 2-7
認証と認可、規定 2-5
TopN レポート 5-18

V

V8 集約キャッシュ、と NDE フロー マスク 4-5
VACL、設定
LAN の VLAN 3-18
WAN インターフェイス 3-17
VC 統計情報 4-102
VLAN Priority (COS) Statistics
Cumulative Data テーブル、使用 4-54
Current Rates テーブル、使用 4-52
TopN Chart、使用 4-53
VLAN Traffic Statistics
Cumulative Data テーブル、使用 4-51
Current Rates テーブル、使用 4-49
TopN Chart、使用 4-50
VLAN データ、表示 4-49
VLAN ID ごとの累積データ 4-51
データ ソースごとのユーザ プライオリティ分布
現在のレート 4-52
累積 4-54
役立つテーブルとチャート
VLAN Priority (COS) Statistics Cumulative Data テーブル 4-54
VLAN Priority (COS) Statistics Current Rates テーブル 4-52
VLAN Priority (COS) Statistics Top N Chart 4-53
VLAN Traffic Statistics Cumulative Data テーブル 4-51
VLAN Traffic Statistics Current Rates テーブル 4-49
VLAN Traffic Statistics Top N Chart 4-50
ユーザ プライオリティ分布をグラフ形式で 4-53
レポート 4-50
VLAN レポート
作成 5-4
VPN ルーティング / 転送テーブル 3-28
VRF 統計情報 4-102

W

WAN インターフェイス 3-27
WS-SVC-NAM-1 3-8
WS-SVC-NAM-2 3-8

あ

アドレス フィルタ、使用したキャプチャ設定 6-8
アプリケーション データ、表示 4-9
アプリケーション プロトコル、データのキャプチャ 4-11, 4-15
収集したパケット数とバイト数
プロトコルごと 4-9, 4-14
累積 4-12, 4-17
詳細
プロトコルごと 4-10, 4-15
累積 4-18
役立つテーブルとチャート
Applications Cumulative Data テーブル 4-12, 4-17
Applications Current Rates テーブル 4-9, 4-14
ApplicationsTopN Chart 4-11, 4-16
リアルタイム データをグラフ形式で 4-11, 4-16
レポート
Application テーブルのレポート 4-11, 4-16
Application レポート、作成 5-4
アプリケーション応答時間レポート
作成 5-4
アラーム
E メール アドレス 3-67
アラーム、表示 7-1
NAM ログ、表示 7-2
アラーム ログ、概要 7-1
スイッチ ログ、表示 7-3

アラームしきい値、設定　3-56
NAM MIB 変数、選択　3-57
NAM の MIB しきい値　3-56
削除　3-60
作成　3-57
編集　3-59
syslog、セットアップ　3-61
音声しきい値　3-60
スイッチしきい値　3-63
削除　3-65
作成　3-63
編集　3-65

い

イネーブル化
監査証跡　3-69
イメージのアップグレード、トラブルシューティング　A-16
インターフェイス データ、表示
詳細　4-89

え

エラー メッセージ（「トラブルシューティング」を参照）　A-18

お

応答時間データ、表示　4-67
詳細
クライアント / サーバ　4-76, 4-79
サーバ　4-72
役立つテーブルとチャート
Client/Server Response Time Top N Chart　4-77
Client/Server Response Time テーブル　4-74
Server Response Time Top N Chart　4-73
レポート
クライアント / サーバ　4-76, 4-79
サーバ　4-70, 4-73
応答時間データの収集、管理
削除　3-39
作成　3-38
セットアップ　3-37
編集　3-38
音声アラーム　3-60
音声アラームしきい値、設定　3-60
音声監視　3-37
音声監視、トラブルシューティング　A-24
音声データ
収集　3-36
表示　4-19
アクティブな通話　4-30
音声プロトコルの概要　4-22
既知の電話機　4-24

か

回復、パスワードの　2-2
会話データ、表示　4-41
MAC ステーション会話で収集されたパケット数とバイト数　4-46
TopN ホスト会話のパケット数とバイト数　4-44
ホスト会話ごとのパケット数とバイト数　4-41
詳細　4-42
データのキャプチャ　4-43
リアルタイム トラフィック統計情報をグラフ形式で　4-43
レポート　4-43
ホスト会話ごとの累積データ　4-45
役立つテーブルとチャート
MAC Conversations Top N Chart　4-46
MAC Station Conversations Cumulative Data テーブル　4-48
Network Host Conversations Cumulative Data テーブル　4-45
Network Host Conversations Current Rates テーブルの表示　4-41
Network Host Conversations Top N Chart　4-44
カスタム キャプチャ　6-21
カスタム キャプチャ フィルタ
管理
削除　6-24
作成　6-21
セットアップ　6-21
編集　6-24
作成　6-21
使用方法　6-10
カスタム デコード フィルタ、管理
削除　6-28
作成　6-25

セットアップ　6-25
編集　6-28
カスタム フィルタ　6-21
カスタム レポート　5-21
新しいフォルダの作成　5-22
削除　5-22
表示　5-22
別のフォルダへの移動　5-23
編集　5-22
仮想回線　3-28
監査証跡　2-23
監査証跡の表示　2-23
監視
アプリケーション応答時間　4-69
管理（「システム管理」を参照）　2-1

き

キャプチャ データ
ストレージ　2-17
キャプチャ ファイル
Analyze ボタン　6-16
共通のナビゲーションおよび制御要素（表）　1-4

く

グローバル プリファレンス、設定　3-68

こ

コア データ、収集　3-34
コア モニタリング
スイッチ　3-35
ルータ　3-35
コミュニティ スイッチ ストリング、設定と表示　3-26

さ

削除
DiffServe プロファイル　3-41, 3-50
NAM Traffic Analyzer アカウント　1-6
NAM トラップ　3-67
NAM の MIB しきい値　3-60
NetFlow デバイス　3-20
SPAN セッション　3-13
カスタム NetFlow データ ソース　3-23
カスタム キャプチャ フィルタ　6-24
カスタム デコード フィルタ　6-28
カスタム レポート　5-22
基本レポート　5-20
スイッチしきい値　3-65
プロトコル　3-48
作成
NAM Traffic Analyzer アカウント　1-6
NAM トラップ　3-66
NetFlow デバイス　3-19
SPAN セッション　3-10
カスタム NetFlow データ ソース　3-21
NetFlow デバイス、選択　3-22
インターフェイス、選択　3-22
データ ソース、削除　3-23
データ ソース、編集　3-23
データ ソース情報、確認　3-23
カスタム キャプチャ フィルタ　6-21
カスタム デコード フィルタ　6-25
カスタム レポート　5-21
基本レポート　5-4
スイッチしきい値　3-63
プロトコル　3-46

し

システム アラート　2-23
キャプチャ　2-26
表示　2-23
システム イベント　5-19
システム イベント ログ
表示　5-19
システム管理　2-1
システム リソース、表示　2-10
システム管理作業の概要　2-10
NAM SNMP システム グループ、設定と表示　2-12
NAM コミュニティ ストリング、使用　2-13
NAM システム時刻、設定　2-14
システム リソース、表示　2-10
ネットワーク パラメータ、設定と表示　2-11
診断、テクニカル サポートのための生成　2-23
ユーザ管理作業の概要　2-2

TACACS+ サーバ、NAM サポートの設定 2-7
TACACS+ 認証と認可、規定 2-5
User Sessions テーブル、表示 2-9
定義済みの NAM ユーザ アカウント、変更 2-3
パスワード、回復 2-2
ユーザ、削除 2-5
ユーザ、新規作成 2-3
ユーザ、編集 2-4
ユーザの特権（表） 2-2
収集（「データ収集」の「セットアップ」を参照） 1-6
診断、生成 2-23
システム アラート、キャプチャ 2-26
システム アラート、表示 2-23
設定情報、監視とキャプチャ 2-25
診断エラー メッセージ（「トラブルシューティング」を参照） A-18

す

スイッチ
NAM の日付 / 時刻の同期の問題、～と、トラブルシューティング A-18
アラームしきい値
削除 3-65
作成 3-63
設定 3-63
編集 3-65
アラームとポート統計情報の問題、トラブルシューティング A-10
スイッチ ポート レポート
作成 5-4
スケジュールされたレポート 5-24
スパニング、トラフィックの方向指定 3-8
NDE の収集タイプ（表） 3-9
NetFlow デバイス、管理 3-19
削除 3-20
作成 3-19
テスト 3-21
編集 3-20
NetFlow、デバイスでの設定 3-15
Catalyst OS 3-16
Cisco IOS 3-15
NDE v8 集約 3-16
NDE のエクスポート 3-17
デバイス スロットにある NAM 3-17
マルチレイヤ スイッチングのキャッシュ 3-15
SPAN セッション
削除 3-13
作成 3-10
編集 3-12
SPAN ソース（表） 3-9
VACL、設定
LAN の VLAN 3-18
WAN インターフェイス 3-17
カスタム NetFlow データ ソース、作成 3-21
NetFlow デバイス、選択 3-22
インターフェイス、選択 3-22
データ ソース、削除 3-23
データ ソース、編集 3-23
データ ソース情報、確認 3-23
方法（表） 3-8
リスニング モード、使用 3-24
スパニング、トラブルシューティング A-8
スパニング用のトラフィックの方向指定 3-8
NDE の収集タイプ（表） 3-9
NetFlow デバイス、管理 3-19
削除 3-20
作成 3-19
テスト 3-21
編集 3-20
NetFlow、デバイスでの設定 3-15
Catalyst OS が稼動するデバイス 3-16
Cisco IOS が稼動するデバイス 3-15
NDE v8 の集約をサポートするデバイス 3-16
NDE のエクスポートをサポートするデバイス 3-17
vi 集約をサポートするデバイス 3-16
デバイス スロットにある NAM 3-17
マルチレイヤ スイッチングのキャッシュをサポートするデバイス 3-15
SPAN セッション
削除 3-13
作成 3-10
編集 3-12
SPAN ソース（表） 3-9
VACL、LAN の VLAN での設定 3-18
VACL、WAN インターフェイスでの設定 3-17
カスタム NetFlow データ ソース、作成 3-21
NetFlow デバイス、選択 3-22
インターフェイス、選択 3-22

データ ソース、削除　3-23
データ ソース、選択　3-23
データ ソース、編集　3-23
データ ソース情報、確認　3-23
方法（表）　3-8
リスニング モード、使用　3-24

せ

設定
NAM SNMP システム グループ　2-12
アラームしきい値　3-56
NAM の MIB しきい値　3-56
syslog　3-61
音声しきい値　3-60
スイッチしきい値　3-63
コミュニティ スイッチ ストリング　3-26
ネットワーク パラメータ　2-11

た

対象読者、このマニュアルの　xiv

ち

注意
意味　xiv
～について
NAM コミュニティ ストリング、削除　2-14
スイッチのストリングとリード/ライト コミュニティ ストリングが一致　3-26
ローカル データベース Web ユーザ、すべてを削除　A-3

て

データ ソース
コア モニタリング　3-35
持続性　4-8
データ ソース、概要　4-2
NDE フロー マスク、と V8 集約キャッシュ　4-5
複数の収集、設定　4-3
プロトコル自動検出　4-5
データ ソース、セットアップ　3-8
データ収集
概要　4-2
セットアップ　3-34
DiffServe プロファイル データ　3-40
DSMON データ　3-39
応答時間データ　3-37
音声データ　3-36
コア データ収集　3-34
データソース
サポートされる最大数　3-27
データの監視　4-1
DSMON　3-39
Monitor Overview チャート、表示　4-6
アプリケーション　4-9
アプリケーション プロトコルごとのパケット数とバイト数　4-9, 4-14
リアルタイム データをグラフ形式で　4-11, 4-16
レポート　4-11, 4-16
応答時間　3-37
データ収集、削除　3-39
データ収集、作成　3-38
データ収集、編集　3-38
音声　4-19
アクティブな通話　4-30
音声プロトコルの概要　4-22
既知の電話機　4-24
データ ソース、概要　4-2
NDE フロー マスク、と V8 集約キャッシュ　4-5
複数の収集、設定　4-3
プロトコル自動検出　4-5
データ収集、概要　4-2
ホスト　4-32
MAC ステーション　4-38
累積データ　4-37
データのキャプチャ　6-1
アプリケーション プロトコル　4-11, 4-15
応答時間　4-76, 4-79
カスタム キャプチャ フィルタ、セットアップ　6-21
削除　6-24
作成　6-21
編集　6-24
カスタム デコード フィルタ、セットアップ　6-25
削除　6-28

作成　6-25
編集　6-28
キャプチャ バッファ
データの表示　1-8
ファイルへのダウンロード　6-15
キャプチャ設定、構成　6-3
アドレス フィルタの使用　6-8
カスタム フィルタの使用　6-10
プロトコル フィルタの使用　6-9
クライアント / サーバ応答時間　4-76, 4-79
サーバの応答時間　4-73
サーバの詳細　4-73
ネットワーク ホストの現在のレート　4-35
パケット デコード情報、表示　6-11
プロトコル デコード情報、表示　6-14
ホスト会話　4-43
データ不一致、トラブルシューティング　A-20
テクニカル サポート、取得
診断、生成　2-23
システム アラート、キャプチャ　2-26
システム アラート、表示　2-23
設定情報、監視とキャプチャ　2-25
（「トラブルシューティング」も参照）　A-1

と

統計情報
VRF/VC の表示　4-102
トラブルシューティング　A-1
HTTPS/ セキュリティ証明書の問題　A-21
NAM とスイッチの日付 / 時刻の同期の問題　A-18
NetFlow 監視の問題　A-11
SNMP の問題　A-22
SPAN に関連する問題　A-7
Web ブラウザの応答時間と表示の問題　A-17
イメージの アップグレードおよびパッチの問題　A-16
応答時間の低下　3-68
音声監視の問題　A-24
診断エラー メッセージの問題　A-18
スイッチ アラームとポート統計情報の問題　A-10
スイッチ、通信できない　3-26
データ不一致の問題　A-20
パケットのキャプチャとスパニングの問題　A-8
プロトコル サポートの問題　A-23
ホスト名解決の問題　A-19
ユーザ名とパスワードの問題　A-3
すべてのローカル データベース Web ユーザの削除に関する注意　A-3
レポートの問題　A-15
ログインの問題　A-5

な

ナビゲーションおよび制御要素　1-4

ね

ネームサーバ、応答時間の低下、トラブルシューティング、　3-68
ネットワーク トラフィック データ、保存および取得　1-8
ネットワーク トラフィック データ履歴、保存および取得　1-8
ネットワーク パラメータ、設定と表示　2-11
ネットワーク ホスト データのチャートとテーブル、使用
Network Host Current Rates
グラフ形式のリアルタイムの統計情報　4-35
Network Host Conversations Cumulative Data テーブル、使用　4-45
Network Host Current Rates　4-35
詳細　4-33
特定のホストのデータ、キャプチャ　4-35
Network Host TopN Chart　4-36

は

ハードウェア、NAM 組み込み、および Catalyst 6000 および 6500 シリーズ スイッチ　1-1
Cisco 2600、3660、および 3700 シリーズ ルータ　1-1
パケットのキャプチャ、トラブルシューティング　A-8
パスワード、回復　2-2
パッチ、トラブルシューティング　A-16

ひ

表記法、このマニュアルで使用されている　xiv

表示
DiffServ データ 4-55
ホスト会話の詳細 4-63
ホスト統計情報 4-64
リアルタイム データをグラフ形式で 4-63
リアルタイム トラフィック統計情報をグラフ形式で 4-56
レポート 4-57
MAC ステーション会話ごとのパケット数とバイト数 4-48
Monitor Overview チャート 4-6
MPLS トラフィック統計情報 4-101
NAM SNMP システム グループ 2-12
NAM の MIB アラームの詳細 3-59
NAM ログ 7-2
RMON ログ テーブル 7-3
TopN MAC ステーション会話で収集されたパケット数とバイト数 4-46
User Sessions テーブル 2-9
VLAN データ 4-49
TopN VLAN ID ごとに収集、グラフ形式で 4-50
VLAN ID ごとの累積データ 4-51
データ ソースごとのユーザ プライオリティ分布 4-52, 4-54
ユーザ プライオリティ分布をグラフ形式で 4-53
レポート 4-50
アクティブな通話データ 4-30
アプリケーション データ 4-9
キャプチャ、特定のプロトコル 4-11, 4-15
収集したパケット数とバイト数 4-12, 4-17
特定のプロトコルの詳細 4-18
リアルタイム データをグラフ形式で 4-11, 4-16
レポート 4-11, 4-16
アラーム 1-9
応答時間データ 4-67
クライアント / サーバ 4-76, 4-79
クライアント / サーバの詳細 4-76, 4-79
サーバ 4-70, 4-73
サーバの詳細 4-72
音声データ 4-19
アクティブな通話 4-30
音声プロトコルの概要 4-22
既知の電話機 4-24
会話データ 4-41
ホスト会話ごとのパケット数とバイト数 4-41
カスタム レポート 5-22
キャプチャ バッファ データ 1-8
コミュニティ スイッチ ストリング 3-26
システム アラート 2-23
システム リソース 2-10
スイッチ
ログ 7-3
ネットワーク トラフィック データ 1-8
ネットワーク パラメータ 2-11
ポート統計情報データ 4-81, 4-90
詳細 4-83, 4-99
リアルタイム データをグラフ形式で 4-83
累積 4-87, 4-100
レポート 4-84
ホスト データ 4-32
MAC ステーションの現在のレート 4-37
グラフ形式のリアルタイムの統計情報 4-35
直前のインターバルで収集 4-32
特定のホスト、キャプチャ 4-35
累積 MAC ステーション データ 4-40
レポート 4-35
ルータ パラメータ 3-7
レポート 1-8

ふ

フィルタリング
監査証跡 2-24
フォルダ、カスタム レポートの移動 5-23
ブラウザの応答時間と表示、トラブルシューティング A-17
プロトコル サポート、トラブルシューティング A-23
プロトコル ディレクトリ
管理
プロトコルの削除 3-48
プロトコルの作成 3-46
プロトコルの編集 3-47
セットアップ 3-45
プロトコル データ、キャプチャ
クライアント / サーバ データ 4-76, 4-79
サーバ データ 4-73
プロトコル フィルタ、キャプチャ設定 6-9

へ

ヘルプ
診断、テクニカル サポートのための生成 2-23
システム アラート、キャプチャ 2-26
システム アラート、表示 2-23
設定情報、監視とキャプチャ 2-25
（「トラブルシューティング」も参照） A-1
編集
DiffServe プロファイル 3-41, 3-50
NAM Traffic Analyzer アカウント 1-6
NAM トラップ 3-66
NAM の MIB しきい値 3-59
NetFlow デバイス 3-20
SPAN セッション 3-12
カスタム キャプチャ フィルタ 6-24
カスタム デコード フィルタ 6-28
カスタム レポート 5-22
スイッチしきい値 3-65
プロトコル 3-47

ほ

ポート統計情報データ、表示 4-81, 4-90
詳細 4-83, 4-99
役立つテーブルとチャート
Interface Stats Current Rates テーブル 4-82, 4-98
Interface Stats Top N Chart 4-86
Port Stats Current Rates テーブル 4-81
Port Stats Top N Chart 4-84, 4-99
リアルタイム データをグラフ形式で 4-83
累積データ 4-87, 4-100
レポート 4-84
ポート統計情報の問題、トラブルシューティング A-10
ホスト データ、表示 4-32
MAC ステーションの累積データ 4-40
Network Hosts テーブルのレポート 4-35
TopN MAC ステーションのデータ 4-38
グラフ形式のリアルタイムの統計情報 4-35
詳細 4-33
特定のホストのデータ、キャプチャ 4-35
ホスト会話レポート
作成 5-4
ホストごとの累積データ 4-37
役立つテーブルとチャート
MAC Stations Current Rates テーブル 4-37
MAC Stations Top N Chart 4-38
Network Hosts Cumulative Data テーブル 4-37
Network Hosts Current Rates テーブル 4-32
Network Hosts Top N Chart 4-36
ホスト名解決、トラブルシューティング A-19

ま

マニュアル
使用されている表記法 xiv
対象読者 xiv
表記法 xiv

ゆ

ユーザ
Sessions テーブル、表示 2-9
Users テーブル（図） 2-3
管理（「システム管理」を参照） 2-1
特権（表） 2-2
ユーザ名とパスワードの問題、トラブルシューティング A-3

り

リアルタイム データ表示、設定 1-7
リスニング モード（NAM）、使用 3-24

る

ルータ パラメータの表示 3-7

れ

レポート
TopN 5-18
アクセス 1-8
エラー状態 5-19
カスタム
削除 5-22
作成 5-21
表示 5-22

フォルダ間の移動　5-23
編集　5-22
基本レポートのタイプの管理　5-2
イネーブル化　5-20
削除　5-20
作成　5-4
ディセーブル化　5-20
テーブル、表示　5-17
名前の変更　5-20
削除　5-20
カスタム　5-22
基本　5-20
作成　5-1
カスタム　5-21
基本　5-4
ディセーブル化　5-20
トラブルシューティング　A-15
表示　5-1
カスタム レポート　5-22
レポートのエクスポート
スケジューリング　5-24
編集　5-26
レポートの詳細
表示　5-18
レポート名の変更　5-20
連続キャプチャ　6-5

ろ

ログ
MPLS インポート　3-33
ログイン
トラブルシューティング　A-5