ネットワーク管理システム： ベスト プラクティスのホワイト ペーパー

Document ID: 15114

Updated: 2007 年 7 月 11 日

PDF のダウンロード
印刷
フィードバック

目次

はじめに

International Organization for Standardization (ISO; 国際標準化機構) のネットワーク管理モデルでは、ネットワーク管理の機能領域として 5 つの領域が定義されています。 この文書ではすべて

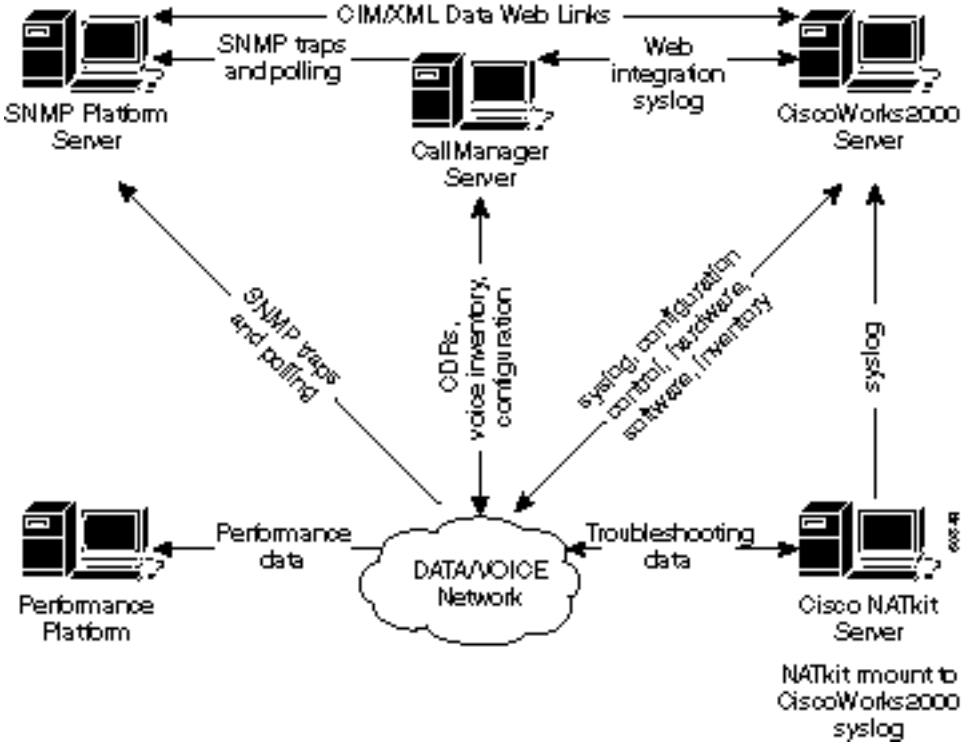
の機能領域について説明します。 この文書の全体的な目的は、現行の管理ツールや管理方法の効率全般を向上させるために、各機能領域の実用的な推奨事項を提供することです。 また、ネットワーク管理ツールとテクノロジーの将来的な実装についての設計ガイドラインも示します。

ネットワーク管理

ISO ネットワーク管理モデルの 5 つの機能領域は次のとおりです。

- 障害管理：ネットワークで発生した障害の検出、切り分け、通知、および修復を行います。
- 構成管理：コンフィギュレーション ファイル管理、在庫管理、ソフトウェア管理など、ネットワーク デバイスの設定に関する側面。
- パフォーマンス管理：全体的なパフォーマンスを許容レベルに維持するため、さまざまな角度からパフォーマンスを監視および測定します。
- セキュリティ管理：許可されたユーザに、ネットワーク デバイスや企業リソースへのアクセスを提供します。
- アカウンティング管理：ネットワーク リソースの使用状況に関する情報。

次の図は、データネットワークを管理するためにシスコシステムズが最低限必要なソリューションと考えている参照アーキテクチャを示します。 このアーキテクチャには、Voice over Internet Protocol（VoIP）の管理を計画している場合を考慮して、Cisco CallManager サーバが含まれています。 この図は、CallManager サーバを NMS トポロジにどのように統合すればよいかを示しています。



このネットワーク管理アーキテクチャには次のものが含まれます。

- 障害管理用の Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）プラットフォーム。
- 長期的な性能管理とトレンド分析を行うためのパフォーマンス監視プラットフォーム。
- 構成管理、syslog の収集、およびハードウェアとソフトウェアのインベントリ管理用の CiscoWorks2000 サーバ。

SNMP プラットフォームの中には、Common Information Model/eXtensible Markup

Language（CIM/XML）手法を使用して CiscoWorks2000 サーバと直接データを共有できるものがあります。 CIM は、ネットワーク環境や企業環境の管理情報全体を記述する、実装非依存方式の共通データ モデルです。 CIM は仕様とスキーマから構成されます。 仕様は SNMP MIB や Desktop Management Task Force Management Information Files（DMTF MIF）などの他の管理モデルとの統合について詳細に規定し、スキーマは実際のモデルを記述します。

XML は、構造化されたデータをテキスト形式で表現するためのマークアップ言語です。 XML は、SGML の記述能力をほとんど維持したまま、SGML の複雑さをできる限り軽減することを目標としていました。 XML は概念的には HTML に似ていますが、HTML が文書に関するグラフィカルな情報の伝達に使用されるのに対し、XML は文書内の構造化データを表現するために使用されます。

お客様がシスコの先進的なサービスを利用している場合は、予防的な監視とトラブルシューティングを行うシスコの NATkit サーバがネットワーク管理アーキテクチャに追加されます。 NATkit サーバには、リモート ディスク マウント機能（rmount）、または CiscoWorks2000 サーバ上のデータに対する File Transfer Protocol（FTP; ファイル転送プロトコル）アクセス機能があります。

『*インターネットワーキング テクノロジーの概要*』の「ネットワーク管理の基本」の章に、ネットワーク管理の基本に関する詳しい概要があります。

障害管理

障害管理の目標は、ネットワークの問題を検出、記録してユーザに通知し、（可能な範囲内で）自動的に解決することにより、ネットワークを実質的に稼働し続けることにあります。 障害はダウンタイムや許容できないネットワークの劣化を引き起こす可能性があるため、障害管理は ISO ネットワーク管理要素の中でおそらく最も幅広く実装されています。

ネットワーク管理プラットフォーム

企業に配置されたネットワーク管理プラットフォームは、マルチベンダーのネットワーク要素から成るインフラストラクチャを管理します。 ネットワーク管理プラットフォームは、ネットワーク内のネットワーク要素からイベントを受信し、処理します。 サーバやその他の重要なリソースからのイベントも、管理プラットフォームに転送できます。 標準の管理プラットフォームには、一般に次のような機能があります。

- ネットワーク ディスカバリ
- ネットワーク要素のトポロジ マッピング
- イベント処理
- パフォーマンス データの収集とグラフの作成
- 管理データのブラウズ

ネットワーク管理プラットフォームは、ネットワーク運用中にインフラストラクチャの障害を検出するためのメイン コンソールとして使用できます。 そのため、どのようなネットワークでも問題を迅速に検出できる能力が重要になります。 ネットワーク運用担当者は、グラフィカルなネットワーク マップを利用して、ルータやスイッチなどの重要なネットワーク要素の稼働状態を表示できます。

HP OpenView、Computer Associates Unicenter、SUN Solstice などのネットワーク管理プラットフォームには、ネットワーク デバイスのディスカバリ機能があります。 ネットワーク デバイスはそれぞれ、管理プラットフォームのコンソールにグラフィック要素で表されます。 ネットワーク デバイスの現在の稼働状態は、グラフィック要素の色で表されます。 ネットワーク デバイス

は、ネットワーク管理プラットフォームに SNMP トラップと呼ばれる通知を送信するように設定できます。 通知が受信されると、その通知の重大度に応じて、ネットワーク デバイスを表すグラフィック要素の色が変わります。 さらに、その通知（通常はイベントと呼ばれます）がログファイルに記録されます。 Cisco デバイスからのさまざまなアラートが正しく解釈されるようにするため、SNMP プラットフォームに最新の Cisco Management Information Base（MIB; 管理情報ベース）ファイルをロードしておくことが特に重要です。

シスコでは、各種ネットワーク デバイスを管理するための MIB ファイルを公開しています。 cisco.com Web サイトに「Cisco MIB ファイル」のページがあり、次の情報が掲載されています。

- SNMPv1 形式で公開されている MIB ファイル
- SNMPv2 形式で公開されている MIB ファイル
- Cisco デバイスでサポートされている SNMP トラップ
- 現在の Cisco SNMP MIB オブジェクトの OID

ネットワーク管理プラットフォームの多くが、地理的に分散された複数のサイトを管理する機能を持っています。 この機能は、リモート サイトの管理コンソールとメイン サイトの管理ステーションとの間で管理データを交換することによって実現されています。 分散アーキテクチャの主な利点は、管理トラフィックが減少し、そのために帯域幅をより効果的に利用できるようになる点です。 分散アーキテクチャでは、システムを利用してリモート サイトからネットワークをローカルに管理することもできます。

管理プラットフォームには最近、Web インターフェイスを使用してリモートからネットワーク要素を管理する機能が装備されるようになりました。 この改良により、個々のユーザ ステーションに、管理プラットフォームにアクセスするための特別なクライアント ソフトウェアを導入する必要がなくなりました。

企業は通常、さまざまなネットワーク要素から構成されています。 ただし、ネットワーク要素を効果的に管理するために、各デバイスがベンダー固有の要素管理システムを必要とするのが普通です。 そのため、複数の管理ステーションが同じ情報を求めてネットワーク要素を二重にポーリングする事態が起こり得ます。 異なるシステムによって収集されたデータは別々のデータベースに格納されるため、管理上のオーバーヘッドが生じます。 このような制約から、ネットワーク ベンダーやソフトウェア ベンダーは Common Object Request Broker Architecture（CORBA）や Computer-Integrated Manufacturing（CIM）などの標準を積極的に採用するようになり、管理プラットフォームと要素管理システムとの間の管理データの交換が容易になりました。 管理システム開発に標準を採用しているベンダーを使用すれば、ユーザはインフラストラクチャの展開や管理において相互運用性とコストの節減を期待できます。

CORBA は、異種分散環境においてプログラマには意識されない方法でオブジェクト間の相互運用性を提供するシステムを規定します。 その設計は、オブジェクト管理グループ（OMG）のオブジェクト モデルに基づきます。

インフラストラクチャのトラブルシューティング

ネットワーク運用時にインフラストラクチャのトラブルシューティングを行うための重要なコンポーネントは、Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）サーバと system log（syslog）サーバです。 TFTP サーバは主に、ネットワーク デバイス用のコンフィギュレーション ファイルやソフトウェア イメージを保存するために使用します。 ルータとスイッチには、システムログ メッセージを syslog サーバに送信する機能があります。 これらのメッセージは、問題発生時のトラブルシューティングに役立ちます。 場合によっては、シスコ サポート担当者が根本原因を分析するために syslog メッセージを必要とすることがあります。

CiscoWorks2000 Resource Management Essentials（Essentials）の分散 syslog 収集機能を使用すると、リモート サイトに複数の UNIX または NT 収集ステーションを配置してメッセージの収集とフィルタリングを行うことが可能です。 フィルタを使用すれば、どの syslog メッセージをメインの Essentials サーバに転送するかを指定できます。 分散収集の主な利点は、メインの syslog サーバに転送されるメッセージの量を削減できる点にあります。

障害の検出と通知

障害管理の目的は、ネットワークで発生した障害の検出、切り分け、通知、および修復を行うことです。 ネットワーク デバイスには、自システムで障害が発生したことを管理ステーションに通知する機能があります。 効果的な障害管理システムはいくつかのサブシステムから構成されています。 障害検出は、デバイスが SNMP トラップ メッセージ、SNMP ポーリング、Remote Monitoring（RMON; リモート モニタリング）しきい値、および syslog メッセージを送信することによって行われます。 管理システムは、障害が報告されて修復処理が可能な場合にエンド ユーザに通知します。

トラップは、ネットワーク デバイス上で常に有効にする必要があります。 ルータおよびスイッチ用の新しい Cisco IOS ソフトウェア リリースでは、追加のトラップがサポートされています。 トラップが正しく解読されるようにするため、コンフィギュレーション ファイルをチェックし、アップデートすることが重要です。 シスコの Assured Network Services（ANS）チームにより設定されたトラップの定期的なレビューにより、ネットワークの効果的な障害検出が保証されます。

Cisco Catalyst LAN スイッチでサポートされていて、障害条件の監視に使用できる CISCO-STACK-MIB トラップを次の表に示します。

Trap	説明
moduleUp	モジュールのいずれかについて、この MIB の **moduleStatus** オブジェクトが **ok(2)** 状態に移行したことをエージェント エンティティが検出しました。
moduleDown	モジュールのいずれかについて、この MIB の *moduleStatus* オブジェクトが **ok(2)** 状態から別の状態に移行したことをエージェント エンティティが検出しました。
chassisAlarmOn	この MIB の *chassisTempAlarm*、*chassisMinorAlarm*、または *chassisMajorAlarm* オブジェクトが **on(2)** 状態に移行したことをエージェント エンティティが検出しました。 *chassisMajorAlarm* は、次の条件のいずれかが存在することを示します。 • なんらかの電圧障害 • 温度とファンの同時障害 • 電源装置の 100 % の障害（2 台中 2 台、または 1 台中 1 台の障害） • Electrically Erasable Programmable Read-Only Memory（EEPROM）障害 • Nonvolatile RAM（NVRAM; 不揮発性 RAM）障害 • MCP 通信障害

	• 不明な NMP ステータス chassisMinorAlarm は、次の条件のいずれかが存在することを示します。 • 温度アラーム • ファン障害 • 電源装置の部分的な障害（2 台中 1 台の障害） • 2 台の電源装置のタイプが適合していない
chassisAlarmOff	この MIB の *chassisTempAlarm*、*chassisMinorAlarm*、または *chassisMajorAlarm* オブジェクトが **off(1)** 状態に移行したことをエージェント エンティティが検出しました。

CISCO-ENVMON-MIB トラップでは、環境モニタリング（envmon）トラップが定義されています。 envmon トラップは、モニタ値が環境しきい値を超えたときに、Cisco Enterprise 固有の環境モニタ通知を送信します。 envmon を使用するときは、特定の環境トラップ タイプを有効にするか、または環境モニタリング システムのすべてのトラップ タイプを受け入れるかのどちらかを選択できます。 オプションを指定しない場合、すべての環境タイプが使用可能になります。 オプションには、次の値を 1 つ以上指定できます。

- voltage（電圧）：所定のテスト ポイントで測定された電圧が、そのテスト ポイントの正常な範囲から外れている場合（つまり、警告、重大、シャットダウンなどの段階にある場合）、ciscoEnvMonVoltageNotification が送信されます。
- shutdown（シャットダウン）：テスト ポイントが重大な状態に達し、シャットダウンを開始しようとしていることを環境モニタが検出した場合、ciscoEnvMonShutdownNotification が送信されます。
- supply（電源）：冗長電源（存在する場合）で障害が発生した場合、ciscoEnvMonRedundantSupplyNotification が送信されます。
- fan（ファン）：ファン アレイ（存在する場合）内のいずれか 1 つのファンで障害が発生した場合、ciscoEnvMonFanNotification が送信されます。
- temperature（温度）：所定のテスト ポイントで測定された温度が、そのテスト ポイントの正常な範囲から外れている場合（つまり、警告、重大、シャットダウンなどの段階にある場合）、ciscoEnvMonTemperatureNotification が送信されます。

ネットワーク要素の障害検出と監視は、デバイス レベルからプロトコルおよびインターフェイス レベルに拡張できます。 ネットワーク環境の場合、障害監視は Virtual Local Area Network（VLAN; バーチャル LAN）、Asynchronous Transfer Mode（ATM; 非同期転送モード）、物理インターフェイスの障害表示などを対象とすることができます。 プロトコルレベルの障害管理の実装は、CiscoWorks2000 Campus Manager などの要素管理システムを通じて使用できます。 Campus Manager の TrafficDirector アプリケーションは、Catalyst スイッチでのミニ RMON のサポートを利用したスイッチ管理に焦点を合わせています。

ネットワーク要素の数が増えてネットワークの問題が複雑になった場合は、各種ネットワーク イベント（syslog、トラップ、ログファイル）を関連付ける機能を持つイベント管理システムを導入するのも 1 つの案です。 このアーキテクチャは、イベント管理システムを背後から支える点で Manager of Managers（MOM）システムに似ています。 適切に設計されたイベント管理システムを使用すれば、ネットワーク オペレーション センター（NOC）の担当者は、予防的かつ効果的にネットワークの問題を検出し、診断できます。 イベントの優先順位付けと抑制により、ネットワーク運用スタッフは、重大なネットワーク イベントに注力でき、Cisco Info Center など複数のイベント管理システムを調査し、このようなシステムの機能を詳細に確認するフィージビリティ分析を行うことができます。 詳細情報を取得するには、Cisco Info Center を参照してください。

予防的な障害の監視と通知

RMON 仕様では、RMON アラームおよびイベントという 2 つのグループが規定されています。 管理ステーションは通常、ネットワーク デバイスをポーリングして特定の変数のステータスまたは値を取得します。 たとえば、管理ステーションはルータをポーリングして CPU 利用率を取得し、その値が設定されたしきい値に達していればイベントを生成します。 この方法はネットワークの帯域幅を浪費し、ポーリング間隔によっては実際のしきい値を取得できない場合もあります。

RMON アラームとイベントを使用する場合は、上昇しきい値と下降しきい値に対して自身を監視するようにネットワーク デバイスを設定します。 ネットワーク デバイスはあらかじめ指定された間隔で変数のサンプルを取得し、しきい値と比較します。 実際の値が、設定されたしきい値を超えた場合、またはそれを下回った場合は、管理ステーションに SNMP トラップを送信できます。 RMON アラームおよびイベント グループは、重要なネットワーク デバイスを予防的に管理するための方法を提供します。

シスコシステムズでは、重要なネットワーク デバイスに RMON アラームとイベントを実装することを推奨しています。 監視可能な変数には、CPU 利用率、バッファ エラー、入出力廃棄、その他整数型の変数などがあります。 Cisco IOS ソフトウェア リリース 11.1(1) 以降、すべてのルータ イメージが RMON アラームおよびイベント グループをサポートしています。

RMON アラームとイベントの実装の詳細については、「RMON アラームとイベントの実装」のセクションを参照してください。

RMON のメモリ制約

RMON のメモリ使用量は、すべてのスイッチ プラットフォームの間で、統計、履歴、アラーム、およびイベントに関して一定です。 RMON はいわゆるバケットを使用して RMON エージェント（この場合はスイッチ）に履歴と統計を保存します。 バケット サイズは RMON プローブ（SwitchProbe デバイス）または RMON アプリケーション（TrafficDirector ツール）で定義してから、設定するスイッチに送信します。

ミニ RMON をサポートするには、およそ 450 K のコード領域が必要です（たとえば、 統計、履歴、アラーム、イベントの 4 つの RMON グループをサポートする場合）。 RMON の動的なメモリ要件は実行時コンフィギュレーションによって決まるため、一定ではありません。

ミニ RMON グループ別の、RMON の実行時メモリ使用情報を次の表に示します。

RMON グループの定義	使用する DRAM の量	注意事項
統計情報	スイッチ イーサネット/ファースト イーサネット ポートごとに 140 バイト	ポート単位
履歴	50 バケットに対して 3.6 K *	追加バケットごとに 56 バイト使用
アラームとイベント	アラームと、それに対応するイベント エントリごとに 2.6 K	ポートごとのアラーム単位

* RMON はいわゆるバケットを使用して RMON エージェント（スイッチなど）に履歴と統計を保存します。

RMON アラームとイベントの実装

RMON を障害管理ソリューションの一部として組み込むことにより、潜在的な問題が発生する前に、ネットワークを予防的に監視できます。 たとえば、ブロードキャスト パケットの受信数が著しく増加している場合は、CPU 利用率が上昇するおそれがあります。 RMON アラームとイベントを実装することで、ブロードキャスト パケットの受信数を監視するしきい値を設定し、設定したしきい値に達した場合に SNMP トラップによって SNMP プラットフォームに通知できます。 RMON アラームとイベントを使用すれば、同じ目標を達成するために SNMP プラットフォームによって通常実行される過度のポーリングが解消されます。

RMON アラームとイベントは、次の 2 通りの方法で設定できます。

- CLI（コマンドライン インターフェイス）
- SNMP SET

次の手順例は、インターフェイスで受信されたブロードキャスト パケットの数を監視するためのしきい値を設定する方法を示します。 これらの手順では、このセクションの最後の show interface コマンドの例で示されているカウンタと同じカウンタが使用されます。

コマンドライン インターフェイスの例

CLI インターフェイスを使用して RMON アラームとイベントを実装するには、次の手順を実行します。

1. ifTable MIB をウォークして、Ethernet 0 に関連付けられているインターフェイス インデックスを特定します。
```
interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0"
interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet1"
interfaces.ifTable.ifEntry.ifDescr.3 = "FastEthernet0"
interfaces.ifTable.ifEntry.ifDescr.4 = "Fddi0"
```
2. 監視対象の CLI フィールドに関連付けられている OID を取得します。 この例では、「broadcasts」に対応する OID は 1.3.6.1.2.1.2.2.1.12 です。 cisco.com Web サイトの「特定の MIB 変数に対応する Cisco OID」ページを利用できます。
3. しきい値とイベントを設定するために次のパラメータを決定します。上昇しきい値と下降しきい値サンプリング タイプ（absolute または delta）サンプリング間隔しきい値に達したときのアクションこの例では、Ethernet 0 で受信されたブロードキャスト パケットの数を監視するしきい値を設定します。 ブロードキャスト パケットの受信数が 60 秒のサンプル間で 500 を超えた場合は、トラップを生成します。 取得したサンプル間で入力ブロードキャストの数が増えていない場合は、しきい値が再度アクティブ化されます。**注:** これらのコマンド パラメータの詳細については、Cisco Connection Online（CCO）で、特定の Cisco IOS バージョンの RMON アラームおよびイベント コマンドに関する文書を参照してください。
4. 次の CLI コマンドを使用して、しきい値に達したときに送信するトラップ（RMON イベント）を指定します（Cisco IOS コマンドは太字で表示されています）。**rmon event 1 trap gateway description "High Broadcast on Ethernet 0" owner ciscormon event 2 log description "normal broadcast received on ethernet 0" owner cisco**
5. 次の CLI コマンドを使用して、しきい値と、関連するパラメータ（RMON アラーム）を指定します。**rmon alarm 1 ifEntry.12.1 60 delta rising-threshold 500 1falling-threshold 0 2 owner cisco**

6. SNMP を使用してこれらのテーブルをポーリングし、eventTable エントリがデバイスに作成されたことを確認します。

```
rmon.event.eventTable.eventEntry.eventIndex.1 = 1

rmon.event.eventTable.eventEntry.eventIndex.2 = 2

rmon.event.eventTable.eventEntry.eventDescription.1 =
"High Broadcast on Ethernet 0"

rmon.event.eventTable.eventEntry.eventDescription.2 =
"normal broadcast received on ethernet 0"

rmon.event.eventTable.eventEntry.eventType.1 = snmp-trap(3)

rmon.event.eventTable.eventEntry.eventType.2 = log(2)

rmon.event.eventTable.eventEntry.eventCommunity.1 = "gateway"

rmon.event.eventTable.eventEntry.eventCommunity.2 = ""

rmon.event.eventTable.eventEntry.eventLastTimeSent.1 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventLastTimeSent.2 =
Timeticks: (0) 0:00:00

rmon.event.eventTable.eventEntry.eventOwner.1 = "cisco"

rmon.event.eventTable.eventEntry.eventOwner.2 = "cisco"

rmon.event.eventTable.eventEntry.eventStatus.1 = valid(1)

rmon.event.eventTable.eventEntry.eventStatus.2 = valid(1)
```

7. SNMP を使用してこれらのテーブルをポーリングし、alarmTable エントリが設定されたことを確認します。

```
rmon.alarm.alarmTable.alarmEntry.alarmIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmInterval.1 = 60

rmon.alarm.alarmTable.alarmEntry.alarmVariable.1 = OID:
interfaces.ifTable.ifEntry.ifInNUcastPkts.2

rmon.alarm.alarmTable.alarmEntry.alarmSampleType.1 = absoluteValue(1)

rmon.alarm.alarmTable.alarmEntry.alarmValue.1 = 170183

rmon.alarm.alarmTable.alarmEntry.alarmStartupAlarm.1 =
risingOrFallingAlarm(3)

rmon.alarm.alarmTable.alarmEntry.alarmRisingThreshold.1 = 500

rmon.alarm.alarmTable.alarmEntry.alarmFallingThreshold.1 = 0

rmon.alarm.alarmTable.alarmEntry.alarmRisingEventIndex.1 = 1

rmon.alarm.alarmTable.alarmEntry.alarmFallingEventIndex.1 = 2

rmon.alarm.alarmTable.alarmEntry.alarmOwner.1 = "cisco"

rmon.alarm.alarmTable.alarmEntry.alarmStatus.1 = valid(1)
```

SNMP SET の例

SNMP SET コマンドを使用して RMON アラームとイベントを実装するには、次の手順を実行します。

1. 次の SNMP SET コマンドを使用して、しきい値に達したときに送信するトラップ（RMON イベント）を指定します。

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.1
  octetstring "High Broadcast on Ethernet 0"
  eventDescription.1 : DISPLAY STRING- (ascii): High Broadcast on Ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.1
  integer 3 eventType.1 : INTEGER: SNMP-trap

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.4.1 octetstring "gateway"
  eventCommunity.1 : OCTET STRING- (ASCII): gateway

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.1
  octetstring "cisco" eventOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.1 integer 1
  eventStatus.1 : INTEGER: valid
```

2. 次の SNMP SET コマンドを使用して、しきい値と、関連するパラメータ（RMON アラーム）を指定します。

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.2.2
  octetstring "normal broadcast received on ethernet 0"
  eventDescription.2 : DISPLAY STRING- (ASCII): normal broadcast
  received on ethernet 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.3.2 integer 2
  eventType.2 : INTEGER: log

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.6.2 octetstring "cisco"
  eventOwner.2 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.9.1.1.7.2 integer 1
  eventStatus.2 : INTEGER: valid
```

3. これらのテーブルをポーリングし、eventTable エントリがデバイスに作成されたことを確認します。

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.9.1

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.2.1 integer 60
  alarmInterval.1 : INTEGER: 60

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.3.1
 objectidentifier .1.3.6.1.2.1.2.2.1.12.2
  alarmVariable.1 : OBJECT IDENTIFIER:
.iso.org.dod.internet.mgmt.mib2.interfaces.ifTable
  ifEntry.ifInNUcastPkts.2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.4.1 integer 2

alarmSampleType.1 : INTEGER: deltaValue

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.7.1 integer 500
  alarmRisingThreshold.1 : INTEGER: 500

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.8.1 integer 0
  alarmFallingThreshold.1 : INTEGER: 0

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.9.1 integer 1
  alarmRisingEventIndex.1 : INTEGER: 1
```

```
# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.10.1 integer 2
  alarmFallingEventIndex.1 : INTEGER: 2

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.11.1 octetstring
"cisco"
  alarmOwner.1 : OCTET STRING- (ASCII): cisco

# snmpset -c private 172.16.97.132 1.3.6.1.2.1.16.3.1.1.12.1 integer 1
  alarmStatus.1 : INTEGER: valid
```

4. これらのテーブルをポーリングし、alarmTable エントリが設定されたことを確認します。

```
% snmpwalk -v 1 172.16.97.132 private .1.3.6.1.2.1.16.3.1
```

show interface

これは、**show interface** コマンドを入力したときの結果の例です。

gateway> **show interface ethernet 0**

```
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Description: NMS workstation LAN
Internet address is 172.16.97.132/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 27 drops; input queue 0/75, 0 drops
5 minute input rate 1000 bits/sec, 2 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
21337627 packets input, 3263376846 bytes, 0 no buffer

Received 7731303 broadcasts , 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
17328035 packets output, 2824522759 bytes, 0 underruns
174 output errors, 44368 collisions, 4 interface resets
0 babbles, 0 late collision, 104772 deferred
174 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

コンフィギュレーション管理

構成管理の目標は、ネットワークとシステムの構成情報を監視することで、異なるバージョンのハードウェアおよびソフトウェア要素がネットワーク運用に与える影響を追跡管理することにあります。

構成標準

配置されているネットワーク デバイスの数が増えるに伴い、ネットワーク デバイスの位置を正確に特定する能力が重要になります。 この位置情報は、ネットワークで問題が発生したときに、リソースを派遣する担当者が利用できる詳細な説明になります。 ネットワークで問題が発生したときに迅速に解決するため、各デバイスの管理担当者または管理部門の連絡先情報を確認しておく必要があります。 連絡先情報には、電話番号と担当者名または担当部門名が必要です。

構成標準の一環として、デバイス名から個々のインターフェイスに至るまで、ネットワーク デバイスの命名規則を作成し、実施します。 命名規則を適切に定義すれば、ネットワーク問題のトラブルシューティングを行うときに正確な情報が得られます。 デバイスの命名規則には、地理的な場所、ビル名、フロアなどを使用できます。 インターフェイスの命名規則では、ポートの接続先のセグメントや接続しているハブの名前などを含めるようにします。 シリアル インターフェイスでは、実際の帯域幅、ローカルの Data Link Connection Identifier (DLCI; データリンク接続識別子) 番号 (フレームリレーの場合)、宛先、キャリアから提供された 回線 ID や回線情報などを含めます。

コンフィギュレーション ファイルの管理

既存のネットワーク デバイスに新しい設定コマンドを追加するときは、実際に実装する前に、コマンドの整合性を確認する必要があります。 正しく設定されていないネットワーク デバイスは、ネットワークの接続性やパフォーマンスに甚大な影響を与えるおそれがあります。 ミスマッチや非互換性の問題を避けるために、設定コマンドのパラメータも必ずチェックしてください。 シスコ エンジニアによる設定の徹底的なレビューを定期的に開催することをお勧めします。

フル機能の CiscoWorks2000 Essentials には、ルータおよび Cisco Catalyst スイッチのコンフィギュレーション ファイルを自動的にバックアップする機能があります。 Essentials のセキュリティ機能を使用して、設定変更時に認証を行うことも可能です。 変更監査ログを使用すれば、変更内容と変更を行ったユーザの名前を追跡できます。 複数のデバイスで設定を変更するには、CiscoWorks2000 Essentials の最新バージョンに含まれている Web ベースの NetConfig と、**cwconfig** スクリプトの 2 通りの方法があります。 コンフィギュレーション ファイルは、CiscoWorks2000 Essentials で事前定義またはユーザ定義のテンプレートを利用してダウンロードまたはアップロードできます。

これらの機能は、CiscoWorks2000 Essentials の構成管理ツールで実行できます。

- Essentials 設定アーカイブから 1 台または複数のデバイスへのコンフィギュレーション ファイルの送信
- デバイスから設定を取得し、Essentials アーカイブへ追加
- アーカイブから最新の設定を抽出し、ファイルに書き込み
- 設定をファイルからインポートし、その設定をデバイスに送信
- Essentials アーカイブに最後に格納された 2 つの設定を比較
- 指定した日付またはバージョンより古い設定をアーカイブから削除
- スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピー

在庫管理

ほとんどのネットワーク管理プラットフォームのディスカバリ機能は、ネットワーク内で見つかったデバイスのリストを動的に作成することを目的としています。 インベントリ管理には、ネットワーク管理プラットフォームに実装されているディスカバリ エンジンを利用します。

インベントリ データベースには、ネットワーク デバイスの詳細な構成情報が格納されています。 通常は、ハードウェアのモデル、取り付けられているモジュール、ソフトウェア イメージ、マイクロコードのレベルなどの情報が含まれます。 これらの情報はすべて、ソフトウェアやハードウェアのメンテナンスなどの作業を行う際に重要になります。 ディスカバリ プロセスによって収集されたネットワーク デバイスの最新リストは、SNMP またはスクリプトを使用してインベントリ情報を収集する際のマスター リストとして使用できます。 また、Cisco Catalyst スイッチの最新のインベントリを取得するために、CiscoWorks2000 Campus Manager から CiscoWorks2000 Essentials のインベントリ データベースにデバイス リストをインポートできます。

ソフトウェア管理

ネットワーク デバイスの Cisco IOS イメージを正常にアップグレードするには、メモリ、ブート ROM、マイクロコードのレベルなどの要件を詳細に分析する必要があります。 要件は通常文書化されており、リリース ノートやインストール ガイドの形式でシスコの Web サイトに掲載されています。 Cisco IOS を実行するネットワーク デバイスのアップグレード プロセスは、CCO からの正しいイメージのダウンロード、現在のイメージのバックアップ、すべてのハードウェア要件が満たされていることの確認、新規イメージのデバイスへのロードというステップで構成されます。

一部の組織では、限られたアップグレード期間内にデバイスのメンテナンスを完了する必要があります。 リソースが限られた大規模なネットワーク環境では、業務時間後にソフトウェアのアップグレードをスケジュールし、自動的に実行しなければならない場合があります。 アップグレード手順には、Expect などのスクリプト言語や、アップグレードのために特別に記述したアプリケーションを使用できます。

Cisco IOS イメージやマイクロコードのバージョンなど、ネットワーク デバイスのソフトウェアへの変更は、別のソフトウェア メンテナンスの分析フェーズで利用するために追跡管理する必要があります。 変更履歴レポートをすぐに入手できれば、アップグレードを実行するユーザが互換性のないイメージやマイクロコードをネットワーク デバイスにロードしてしまう危険を最小限に抑えることができます。

パフォーマンス管理

サービス レベル契約

Service Level Agreement（SLA; サービス レベル契約）は、サービス プロバイダーとお客様の間で取り交わされた、ネットワーク サービスの期待されるパフォーマンス レベルについての契約書です。 SLA は、プロバイダーとお客様の間で合意されたメトリックで構成されています。 メトリックに対して設定された価値は、両者にとって現実的で、意味があり、測定可能であることが必要です。

パフォーマンス レベルを測定するために、ネットワーク デバイスからさまざまなインターフェイス統計情報を収集できます。 これらの統計情報を、SLA のメトリックとして組み込むことができます。 入力キュー廃棄、出力キュー廃棄、ignored パケットなどの統計情報は、パフォーマンス関連の問題を診断する際に役立ちます。

デバイス レベルのパフォーマンス メトリックには、CPU 利用率、バッファ割り当て（大サイズ バッファ、中サイズ バッファ、割り当てエラー、ヒット率）、メモリ割り当てなどを含めることができます。 ある種のネットワーク プロトコルのパフォーマンスは、ネットワーク デバイスのバッファをどれだけ利用できるかに直接関係しています。 デバイスレベルのパフォーマンス統計情報の測定は、高レベル プロトコルのパフォーマンスを最適化する際に重要になります。

ルータなどのネットワーク デバイスは、Data Link Switching Workgroup（DLSW）、Remote Source Route Bridging（RSRB）、AppleTalk などのさまざまな上位層プロトコルをサポートします。 フレームリレー、ATM、Integrated Services Digital Network（ISDN; サービス総合デジタル ネットワーク）などの WAN テクノロジーのパフォーマンス統計情報も監視および収集できます。

パフォーマンスの監視、測定、および報告

インターフェイス レベル、デバイス レベル、およびプロトコル レベルの各種パフォーマンス メトリックを、SNMP を使用して定期的に収集します。 データ収集にはネットワーク管理システムのポーリング エンジンを利用できます。 ほとんどのネットワーク管理システムには、ポーリングしたデータを収集し、保存、表示する機能があります。

市場では、企業環境の性能管理ニーズに対応するさまざまなソリューションが提案されています。 これらのシステムには、ネットワーク デバイスやサーバからデータを収集し、保存、表示する機能があります。 ほとんどの製品が Web ベースのインターフェイスを備えており、企業内のどこからでもパフォーマンス データにアクセスできるようになっています。 導入事例の多い性能管理ソリューションには次のようなものがあります。

- InfoVista VistaView
- SAS IT Service Vision
- Trinagy TREND

上記の製品の評価は、それらが各種ユーザの要件を満たすかどうかによって決まります。 一部のベンダーは、ネットワーク管理プラットフォームとシステム管理プラットフォームの統合をサポートしています。 たとえば InfoVista は、アプリケーション サーバからの重要なパフォーマンス統計情報を提供するために、BMC Patrol Agent をサポートしています。 各製品の価格モデルは互いに異なっており、基本製品で提供される機能も同じではありません。 NetFlow、RMON、Cisco IOS Service Assurance Agent/Response Time Reporter (RTR/SAA CSAA/RTR) などの Cisco デバイスの性能管理機能は、一部のソリューションでサポートされています。 Concord には最近、パフォーマンス データの収集と表示に使用できる、シスコの WAN スイッチのサポートが追加されました。

Cisco IOS の CSAA/RTR Service Assurance Agent (SAA; サービス保証エージェント) /Response Time Reporter (RTR) 機能は、IP デバイス間の応答時間の測定に利用できます。 CSAA が設定された送信元ルータは、宛先 IP デバイス (ルータまたは IP デバイス) への応答時間を測定できます。 応答時間の測定は、送信元と宛先の間、またはパス上のホップごとに行うことが可能です。 また、SNMP トラップを設定し、応答時間があらかじめ定義されたしきい値を超えた場合に管理コンソールに通知することもできます。

最近の改良により、Cisco IOS の CSAA 機能は次のものを測定できるように拡張されました。

- HyperText Transfer Protocol (HTTP; ハイパーテキスト転送プロトコル) サービスのパフォーマンスDomain Name System (DNS; ドメイン ネーム システム) lookupTransmission Control Protocol (TCP; 伝送制御プロトコル) 接続HTTP トランザクション時間
- Voice over IP (VoIP) トラフィックのパケット間遅延変動 (ジッタ)
- 特定の Quality Of Service (QOS) に関連するエンド ポイント間の応答時間IP Type Of Service (TOS; サービス タイプ) ビット
- CSAA 生成パケットを使用したパケット損失

ルータで CSAA 機能を設定するには、Cisco Internetwork Performance Monitor (IPM) アプリケーションを使用します。 CSAA/RTR は Cisco IOS ソフトウェアの多くのフィーチャ セットに組み込まれていますが、すべてのフィーチャ セットに組み込まれているわけではありません。 IPM でパフォーマンス統計情報の収集に使用するデバイスには、CSAA/RTR をサポートする Cisco IOS リリースをインストールする必要があります。 CSAA/RTR/IPM をサポートする Cisco IOS バージョンの要約については、「IPM に関するよく寄せられる質問 (FAQ)」の Web サイトを参照してください。

IPM の詳細については、次のリンクを参照してください。

- IPM の概要

- サービス保証エージェント

パフォーマンスの分析と調整

ユーザ トラフィックは近年著しく増加し、ネットワーク リソースに対する要求も増大しています。 ネットワーク管理者は通常、ネットワークを流れているトラフィックのタイプについて限られた情報しか得ることができません。 ユーザ トラフィックとアプリケーション トラフィックをプロファイリングすれば、ネットワーク上のトラフィックについて詳細な情報が得られます。 トラフィック プロファイルの収集は、RMON プローブと NetFlow という 2 つのテクノロジーによって実現されています。

RMON

RMON 規格は、エージェント（組み込みエージェントまたはスタンドアロン プローブのエージェント）が SNMP を通じて中央ステーション（管理コンソール）と通信する分散アーキテクチャで展開されることを想定して設計されています。 RFC 1757 RMON 規格は監視機能を 9 グループに分類し、イーサネット トポロジをサポートしています。トークンリング固有のパラメータは、RFC 1513 で 10 番目のグループとして追加されています。 ファースト イーサネット リンクの監視は RFC 1757 規格のフレームワークで、Fiber-Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）リングの監視は RFC 1757 と RFC 1513 の両方のフレームワークで、それぞれ提供されています。

新たに制定された RFC 2021 RMON 仕様は、Media Access Control（MAC; メディア アクセス制御）層を越えてネットワーク層およびアプリケーション層までリモート モニタリング規格を拡張します。 この設定を実装すれば、管理者は Web トラフィック、NetWare、Notes、電子メール、データベース アクセス、Network File System（NFS）などのネットワーク対応アプリケーションの分析とトラブルシューティングを行うことができます。 RMON のアラーム、統計、履歴、ホスト/カンバセーション グループは現在、アプリケーション層トラフィック（ネットワークで最も重要なトラフィック）に基づくネットワーク アベイラビリティの予防的な監視とメンテナンスに使用できます。 RMON2 を導入すると、ネットワーク管理者は、ミッションクリティカルなサーバベースのアプリケーションをサポートする標準ベースの監視ソリューションを継続的に展開できます。

RMON グループの機能を次の表に示します。

RMON グループ（RFC 1757）	機能
統計情報	セグメントまたはポートに関するパケット、オクテット、ブロードキャスト、エラー、およびオファーのカウンタ。
履歴	統計グループ カウンタのサンプルを定期的に取得し、後で利用するために保存します。
ホスト	セグメントまたはポート上に存在するホスト デバイスごとの統計情報を維持します。
ホス	統計カウンタ別に分類された、ホスト グループ

トップ N	のユーザ定義サブセット レポート。 結果のみを返すことで、管理トラフィックが最小限に抑えられます。
トラフィック マトリックス	ネットワーク上に存在するホスト間のカンバセーション統計を維持します。
アラーム	予防管理のために重要な RMON 変数に対して設定できるしきい値。
イベント	実際の値がアラーム グループのしきい値を超えたときに、SNMP トラップとログ エントリを生成します。
パケット キャプチャ	管理コンソールに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用のバッファを管理します。
トークン リング	リング ステーション：個々のステーションの詳細な統計 リング ステーション オーダ：現在呼び出しているステーションのオーダ リスト リング ステーション設定：ステーションごとの設定および挿入/取り外し 送信元ルーティング： ホップ カウントなどの送信元ルーティングの統計

RMON2	機能
プロトコル ディレクトリ	エージェントが統計情報を監視および維持する対象のプロトコル。
プロトコル分布	プロトコルごとの統計情報。
ネットワーク層ホスト	セグメント、リング、またはポート上に存在するネットワーク層アドレスごとの統計情報。
ネットワーク層マトリックス	ネットワーク層アドレスのペアに関するトラフィック統計情報。
アプリケーション層ホスト	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別統計情報。
アプリケーション層マトリックス	ネットワーク層アドレスのペアに関するアプリケーション層プロトコル別のトラフィック統計情報。
ユーザ定義可能履歴	RMON1 リンク層統計情報を越えて、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。
アドレス マッピング	MAC アドレスとネットワーク層アドレスのバインディング。
設定グループ	エージェントの機能と設定。

NetFlow

Cisco NetFlow 機能を使用すると、キャパシティ計画、課金、およびトラブルシューティング機能のためにトラフィック フローの詳細な統計情報を収集できます。 NetFlow は個々のインターフェイスに対して設定可能で、そのインターフェイスを通過するトラフィックの情報を提供します。 提供される詳細なトラフィック統計には、次のような情報が含まれます。

- 発信元および宛先 IP アドレス
- 入力および出力インターフェイス番号
- TCP/UDP 送信元ポートと宛先ポート
- フロー内のバイト数とパケット数
- 送信元および宛先自律システム番号
- IP Type Of Service（TOS; サービス タイプ）

ネットワーク デバイスについて収集された NetFlow データは収集マシンにエクスポートされます。 収集マシンはデータ量の軽減（フィルタリングと集約）、階層的なデータの保存、ファイル システム管理などの機能を実行します。 シスコでは、ルータおよび Cisco Catalyst スイッチからデータを収集して分析するために、NetFlow Collector および NetFlow Analyzer アプリケーションを用意しています。 Cisco NetFlow User Datagram Protocol（UDP; ユーザ データグラム プロトコル）レコードを収集できる cflowd などのシェアウェア ツールもあります。

NetFlow データは UDP パケットを使用し、次の 3 種類のフォーマットで転送されます。

- バージョン 1：初期の NetFlow リリースでサポートされる元のフォーマット。
- バージョン 5：Border Gateway Protocol（BGP）の自律システム情報とフロー シーケンス番号が追加された、後の改良バージョン。
- バージョン 7：NetFlow フィーチャ カード（NFFC）を搭載した Cisco Catalyst 5000 シリーズ スイッチのための NetFlow スイッチングのサポートが追加された、さらに後の改良バージョン。

バージョン 2 ~ 4 とバージョン 6 はリリースされておらず、FlowCollector でサポートされていません。 3 つのバージョンすべてにおいて、データグラムはヘッダーと 1 つ以上のフロー レコードから成ります。

詳細については、『NetFlow サービス ソリューション ガイド』ホワイト ペーパーを参照してください。

次の表は、ルータおよび Catalyst スイッチからの NetFlow データの収集をサポートする Cisco IOS のバージョンをまとめたものです。

Cisco IOS ソフトウェア リリース	サポートされている Cisco ハードウェア プラットフォーム	サポートされている NetFlow エクスポート バージョン

11.1 CA と 11.1 CC	Cisco 7200、7500、RSP7000	V1 と V5
11.2 と 11.2 P	Cisco 7200、7500、RSP7000	V1
11.2 P	Cisco Route Switch Module（RSM）	V1
11.3 と 11.3 T	Cisco 7200、7500、RSP7000	V1
12.0	Cisco 1720、2600、3600、4500、4700、AS5800、7200、uBR7200、7500、RSP7000、RSM	V1 と V5
12.0 T	Cisco 1720、2600、3600、4500、4700、AS5800、7200、uBR7200、7500、RSP7000、RSM、MGX 8800 RPM、BPX 8600	V1 と V5
12.0（3）T 以降	Cisco 1600、1720、2500**、2600、3600、4500、4700、AS5300*、AS5800、7200、uBR7200、7500、RSP7000、RSM、MGX8800 RPM、BPX 8650	V1、V5、V8
12.0（6）S	Cisco 12000	V1、V5、V8
	NetFlow Feature Card（NFFC）が搭載された Cisco Catalyst 5000 ***	V7

* Cisco 1600 および 2500 プラットフォームでの NetFlow エクスポート V1、V5、および V8 のサポートは Cisco IOS ソフトウェア リリース 12.0(T) を対象としている。 これらのプラットフォームの NetFlow サポートは、Cisco IOS 12.0 メインライン リリースでは使用できない。

** AS5300 プラットフォームでの NetFlow V1、V5、および V8 のサポートは Cisco IOS ソフトウェア リリース 12.06(T) を対象としている。

*** MLS および NetFlow データ エクスポートは、Catalyst 5000 シリーズ スーパーバイザ エンジン ソフトウェア リリース 4.1（1）以降でサポートされている。

セキュリティ管理

セキュリティ管理の目標は、ローカルのガイドラインに従ってネットワーク リソースへのアクセスを制御し、ネットワークを（故意か過失かにかかわらず）妨害できないようにすることにあります。 セキュリティ管理サブシステムには、たとえば、ネットワーク リソースへのユーザのログインを監視したり、不適切なアクセス コードを入力したユーザのアクセスを拒否したりする機能があります。 セキュリティ管理は非常に範囲の広いテーマです。 そのため、ここでは SNMP に関連したセキュリティと基本的なデバイス アクセスのセキュリティのみを取り上げます。

高度なセキュリティの詳細については、次のリンクを参照してください。

- IP ネットワークでのセキュリティの強化
- OpenSystems

適切なセキュリティ管理を実装するには、最初に強固なセキュリティ ポリシーとセキュリティ手順を確立します。 セキュリティとパフォーマンスに関する業界の最良実施例に基づき、すべてのルータとスイッチについてプラットフォーム固有の最小限の設定標準を作成することが重要です。

Cisco ルータおよび Catalyst スイッチでは、さまざまな方法でアクセスを制御できます。 たとえば、次のような方法があります。

- Access Control List（ACL; アクセス コントロール リスト）
- デバイスに対してローカルなユーザ ID とパスワード
- Terminal Access Controller Access Control System（TACACS）

TACACS は、ネットワーク上のクライアント デバイスと TACACS サーバの間で動作する IETF（RFC 1492）標準のセキュリティ プロトコルです。 TACACS はデバイスの識別情報を認証する認証メカニズムで、特権データベースへのリモート アクセスを求めるデバイスの認証に使用します。 TACACS のバリエーションとして TACACS+ があります。TACACS+ は認証、許可、およびアカウンティング機能を区別する AAA アーキテクチャです。

シスコでは、非特権モードおよび特権モードで Cisco デバイスにアクセスできるユーザを細かく制御するために TACACS+ を使用しています。 耐障害性を考慮して複数の TACACS+ サーバを設定できます。 TACACS+ を有効にすると、ルータおよびスイッチはユーザ名とパスワードを入力するプロンプトをユーザに表示します。 認証はログイン制御のためだけでなく、個々のコマンドを認証するためにも設定できます。

認証

認証とはユーザを識別するプロセスを指し、ログインおよびパスワード ダイアログ、確認要求と応答、メッセージングのサポートなどで構成されます。 認証では、ルータまたはスイッチへのアクセスを許可する前にユーザが識別されます。 認証と許可との間には根本的な関係があります。ユーザに与えられる許可特権が大きいほど、より強力な認証が必要となります。

許可

許可はリモート アクセスを制御するための仕組みで、1 回限りの許可や、ユーザが要求するサービスごとの許可などがあります。 Cisco ルータでは、ユーザに対して 0 ~ 15 の許可レベルを設定できます。0 が最低レベルで、15 が最高レベルです。

アカウンティング

アカウンティングは、ユーザ ID、開始時刻と終了時刻、実行されたコマンドなど、課金、監査、およびレポートに使用するセキュリティ情報の収集と送信を可能にします。 アカウンティングを

有効にすることで、ネットワーク管理者は、ユーザがアクセスしているサービスやネットワークリソースの使用量を追跡できます。

次の表は、Cisco ルータおよび Catalyst スイッチで TACACS+、認証、許可、およびアカウンティングを使用する場合の基本的なコマンド例を示しています。 より詳細なコマンドについては、『認証、許可、アカウンティング コマンド』文書を参照してください。

Cisco IOS コマンド	目的
ルータ	
aaa new-model	アクセス制御の主要方式として Authentication, Authorization, Accounting (AAA; 認証、許可、アカウンティング) を有効にします。
AAA accounting {system / *network* / *connection* / *exec* / *command level*} {start-stop / *wait-start* / *stop-only*} {tacacs+ / radius}	グローバル設定コマンドでアカウンティングを有効にします。
AAA authentication login default tacacs+	login default が設定された任意の端末回線への接続を TACACS+ によって認証し、なんらかの理由で認証が失敗した場合は接続が失敗するように、ルータを設定します。
AAA autho rizatio	ユーザが EXEC シェルの実行を許可されているかどうかを TACACS+ サーバに問い合せてチェックするように、ルータを設定します。

n exec default tacacs+ none	
tacacs-server host tacacs+ server ip address	認証に使用する TACACS+ サーバをグローバル設定コマンドで指定します。
tacacs-server key shared-secret	TACACS+ サーバと Cisco ルータが知っている共有シークレットをグローバル設定コマンドで指定します。
Catalyst スイッチ	
set authentication login tacacs enable [all / *console* / *http* / *telnet*] [primary]	通常のログイン モードに対して TACACS+ 認証を有効にします。 コンソール ポートまたは Telnet による接続に対してのみ TACACS+ を有効にする場合は、console または telnet キーワードを使用します。
set authorization exec enable {option} fallba	通常のログイン モードに対して許可を有効にします。 コンソール ポートまたは Telnet による接続に対してのみ許可を有効にする場合は、console または telnet キーワードを使用します。

ck option} [console / *telnet* / *both*]	
Set tacacs-server key shared-secret	TACACS+ サーバとスイッチが知っている共有シークレットを指定します。
Set tacacs-server host tacacs+ server ip address	認証に使用する TACACS+ サーバをグローバル設定コマンドで指定します。
Set accounting commands enable {config / all} {stop-only} tacacs+	設定コマンドのアカウンティングを有効にします。

Catalyst エンタープライズ LAN スイッチで AAA を設定してコマンドライン インターフェイスへのアクセスを監視および制御する方法の詳細については、『認証、許可、およびアカウンティングを使用したスイッチ アクセスの制御』ドキュメントを参照してください。

SNMP セキュリティ

SNMP プロトコルは、CLI からコマンドを発行する場合と同様に、ルータおよび Catalyst スイッチの設定変更に使用できます。 SNMP による不正なアクセスと変更を防ぐために、ネットワーク

デバイスに適切なセキュリティ対策を設定する必要があります。 コミュニティ ストリングは、長さ、文字、および推測の難しさに関する標準パスワード ガイドラインに従って設定します。 コミュニティ ストリングをパブリックおよびプライベートのデフォルトから変更することが重要です。

SNMP 管理ホストにはすべてスタティック IP アドレスを設定し、IP アドレスと Access Control List (ACL; アクセス コントロール リスト) によってあらかじめ定義されたネットワーク デバイスとの SNMP 通信の権限を明示的に付与します。 Cisco IOS および Cisco Catalyst ソフトウェアには、許可された管理ステーションのみがネットワーク デバイスの変更を実行できるようにするセキュリティ機能が用意されています。

ルータのセキュリティ機能

SNMP 特権レベル

この機能は、管理ステーションがルータに対して実行できる操作の種類を制限します。 ルータの特権レベルには、 読み取り専用 (RO) および読み取りと書き込み (RW) の 2 つのタイプがあります。 RO レベルは、管理ステーションに対してルータ データの問い合せのみを許可します。 ルータのリブートやインターフェイスのシャットダウンなどの設定コマンドを実行することは許可されません。 このような操作を実行するには RW 特権レベルが必要です。

SNMP アクセス コントロール リスト (ACL)

SNMP ACL 機能は、SNMP 特権機能と組み合せて、特定の管理ステーションがルータから管理情報を要求できないようにするために使用できます。

SNMP ビュー

この機能は、管理ステーションがルータから取得できる情報を制限します。 SNMP 特権レベルおよび SNMP ACL 機能と組み合せて、管理コンソールからのデータ アクセスを制限するために使用できます。 SNMP ビューの設定例については、snmp-server view を参照してください。

SNMP バージョン 3

SNMP バージョン 3 (SNMPv3) は、ネットワーク デバイスと管理ステーションの間で管理データを安全に交換する仕組みを提供します。 SNMPv3 の暗号化機能と認証機能は、管理コンソールにパケットを転送する際の高度なセキュリティを確保します。 SNMPv3 は、Cisco IOS ソフトウェア リリース 12.0(3)T 以降でサポートされます。 SNMPv3 の技術概要については、SNMPv3 ドキュメントを参照してください。

インターフェイス上のアクセス コントロール リスト (ACL)

ACL 機能は、IP スプーフィングなどの攻撃を防ぐためのセキュリティ対策になります。 ACL はルータの着信インターフェイスまたは発信インターフェイスに適用できます。

Catalyst LAN スイッチのセキュリティ機能

IP 許可リスト

IP 許可リスト機能は、権限のない送信元 IP アドレスからスイッチへの着信 Telnet アクセスおよび SNMP アクセスを制限します。 違反または不正アクセスが発生したときに管理システムに通知するため、syslog メッセージと SNMP トラップがサポートされています。

Cisco IOS のセキュリティ機能と組み合せて使用すれば、ルータと Catalyst スイッチを管理できます。 スイッチとルータにアクセスできる管理ステーションの数を制限するセキュリティ ポリシーを確立する必要があります。

IP ネットワークのセキュリティを強化する方法の詳細については、『IP ネットワークでのセキュリティ強化』を参照してください。

アカウンティング管理

課金管理とは、課金またはチャージバックの目的でネットワーク上の個々のユーザまたはグループ ユーザを適切に管理するために、ネットワーク利用パラメータを測定するプロセスを指します。 適切な課金管理を行うための最初のステップは、性能管理と同様に、すべての重要なネットワーク リソースの使用状況を測定することです。 ネットワーク リソースの使用状況は、Cisco NetFlow および Cisco IP Accounting 機能を使用して測定できます。 これらの方法によって収集したデータを分析することで、現在の使用状況パターンを把握できます。

使用状況に基づく課金および請求システムは、Service Level Agreement (SLA; サービス レベル契約) の不可欠な要素です。 このシステムは、SLA で規定された責任範囲の定義と、SLA の条件から外れた動作がもたらす明確な結果のどちらをも提供します。

データはプローブまたは Cisco NetFlow によって収集できます。 シスコでは、ルータおよび Catalyst スイッチからデータを収集して分析するために、NetFlow Collector および NetFlow Analyzer アプリケーションを用意しています。 cflowd などのシェアウェア アプリケーションも、NetFlow データの収集に使用できます。 リソースの使用状況を継続的に測定すれば、請求情報だけでなく、十分かつ最適なリソースが維持されているかどうかを評価するための情報も得られます。 導入事例の多い課金管理ソリューションには次のようなものがあります。

- 明確なソフトウェア

NetFlow のアクティブ化とデータ収集方針

NetFlow (ネットワーク フロー) は、ネットワーク計画、監視、および課金アプリケーションに必要なデータを収集する、入力側の測定技術です。 NetFlow は、サービス プロバイダーのエッジ/集約ルータ インターフェイス、または企業ユーザの WAN アクセス ルータ インターフェイスに装備する必要があります。

シスコシステムズでは、これらの戦略的に配置されたルータに NetFlow をどのように装備するかを綿密に計画することを推奨しています。 NetFlow はネットワーク上のすべてのルータに装備する必要はありません。装備する範囲をインターフェイス単位で徐々に広げたり、適切なルータのみに戦略的に装備したりすることが可能です。 シスコの担当者がお客様と協力し、お客様のトラフィック フロー パターン、ネットワーク トポロジ、およびアーキテクチャに基づいて、どのキー ルータおよびキー インターフェイスで NetFlow をアクティブ化すればよいかを判断します。

NetFlow を展開する際の主な注意事項を次に示します。

- NetFlow サービスはエッジ測定とアクセス リストの高速化ツールとして利用してください。*処理量の多いコア/バックボーン ルータ*や CPU 使用率が高いルータではアクティブにしないでください。
- アプリケーションのデータ収集要件を理解します。 課金アプリケーションでは発信元ルータと終端ルータのフロー情報しか必要ありませんが、監視アプリケーションではより包括的 (データ集約的) なエンドツーエンドの情報が必要となる場合があります。

- ネットワーク トポロジの影響とフロー収集方針のルーティング ポリシーについて理解します。 たとえば、フロー情報を重複して収集しないようにするため、トラフィックが発信または終端する主要な集約ルータで NetFlow をアクティブにし、同じフロー情報を提供するバックボーン ルータまたは中継ルータでは NetFlow をアクティブにしないようにします。
- *中継通信*事業 (トラフィックを伝送するだけで、自社のネットワークでは発信も終端もしない) を営むサービス プロバイダーでは、NetFlow エクスポート データを利用して通過トラフィックによるネットワーク リソースの使用状況を測定し、アカウンティングおよび請求に使用できます。

IP アカウンティングの設定

Cisco IP アカウンティングのサポートは基本的な IP アカウンティング機能を提供します。 IP アカウンティングを有効にすると、発信元と宛先の IP アドレスに基づいて Cisco IOS ソフトウェアでスイッチされたバイトとパケットの数が分かります。 測定されるのは発信方向の通過 IP トラフィックのみです。 ソフトウェアが生成したトラフィックや、ソフトウェアで終了したトラフィックは、アカウンティング統計情報に含まれません。 このソフトウェアでは、アカウンティングの集計精度を維持するために、 アクティブ データベースとチェックポイント データベース

Cisco IP アカウンティングのサポートは、IP アクセス リストによって拒否された IP トラフィックを識別する情報も提供します。 IP アクセス リストに違反した IP 送信元アドレスが見つかったということは、セキュリティ侵犯の可能性があることを意味します。 また、そのデータも、IP アクセス リストの設定を確認する必要があることを示します。 この機能をユーザに対して使用可能にするには、**ip accounting access-violations** コマンドを使用して、アクセス リスト違反の IP アカウンティングを有効にします。 これにより、ユーザは送信元と宛先のペアのアクセス リストに反してセキュリティ侵犯を試みた単一ソースからのバイト数とパケット数を表示できます。 デフォルトでは、IP アカウンティングはアクセス リストによって許可され、ルーティングされたパケットの数を表示します。

IP アカウンティングを有効にするには、インターフェイス設定モードで、インターフェイスごとに次のコマンドのいずれかを使用します。

コマンド	目的
ip accounting	基本的な IP アカウンティングを有効にします。
ip accounting access violations	IP アカウンティングを有効にし、IP アクセス リストによって拒否された IP トラフィックの識別機能をオンにします。

その他の IP アカウンティング機能を設定するには、グローバル設定モードで、次のコマンドを 1 つ以上使用します。

コマンド	目的
ip accounting-threshold threshold	作成するアカウンティング エントリの最大数を設定します。
ip accounting-list ip-address wildcard	ホストのアカウンティング情報をフィルタに掛けます。
ip accounting-	IP アカウンティング データベースに格

transits count	納する通過レコードの数を制御します。

このドキュメントで使用されている表記法の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Updated: 2007 年 7 月 11 日
Document ID: 15114