分散システム／インターネット運用技術　13－1
（１９９９．５．２１）

LANスイッチを導入したネットワークにおけるトラフィック分析手法

嶋田　雄二郎†　城所　銑一†　花井　克之†

(株) 東芝　情報・社会システム社　SI技術開発センター†

概要

ネットワーク管理のための有力な情報源の１つに，MIB-2やRMON／RMON2で収集するパフォーマンス／トラフィック情報があげられる．しかしながら，LANスイッチを導入した最近のネットワーク環境は，収集すべきMIB情報を飛躍的に増加させ，従来の手法では手におえない状況をもたらした．このようなネットワーク環境において有効なネットワーク管理を実現するには，膨大なMIB情報の効率よい分析手法の確立が必要である．本稿では，LANスイッチを導入したネットワークのトラフィック管理をRMONベースで行う上で，従来の手法の問題点を整理し，その問題点を解消する効率よいトラフィック分析手法の試みについて述べる．

An approach for traffic analysis in network environment with LAN-switching technology

Yujiro Shimada†　Senichi Kidokoro†　Katsuyuki Hanai†

†System Integration Technology Center,
Information and Industrial Systems & Services Company,
TOSHIBA Corporation

Abstract

One of the effective resources for network management is information about network performance and traffic which are provided by SNMP MIBs such as MIB-II and RMON/RMON2. Recently many network environments have introduced LAN-switching technology and enjoyed its benefits. However, in an aspect of network management, this LAN-switching technology requires a large increase in MIB information to be collected, which results in overloading traditional approach for network management. In this paper, we summarize features of this problem and discuss on an effective approach for traffic analysis in network environment with LAN-switching technology.

1. はじめに

今日のように複雑で増大しつつあるインターネット／イントラネット環境において，現在のネットワークを円滑に運用し，また将来的なネットワークの拡張や再構築を有効に行うために，ネットワーク管理は重要である．ネットワーク管理の対象項目となるものは以下のものがあげられる．

- 構成管理(ネットワーク上の機器が実際にネットワーク上で使用可能であるか?)
- 性能管理(ネットワーク設計上の期待される性能を実現しているか?)
- 障害管理(ネットワーク上の障害発生の防止や対処を柔軟に行うことができるか?)
- 機密管理(不正なネットワークの使用に対する防止や対処を有効に行えるか?)
- 課金管理(各エンドユーザのネットワーク利用状況に応じたコスト負担を適切に算出できるか?)

これらの管理項目に対応することが可能な標準化されたネットワーク管理プロトコルとアーキテクチャとして SNMP (Simple Network Management Protocol)があり，近年普及し，実績を上げている[1].

特にネットワーク・セグメントのトラフィックのリモート監視を実現することを目的とされた RMON (Remote MONitoring)技術は，セグメント上を流れるトラフィックの統計情報の収集機能と分析機能などを持つ．RMON のこれらの機能を活用することで，ネットワーク障害の原因や予兆の的確で迅速な把握と，ネットワーク設計における効果的なキャパシティ・プランニングなどを実現することができる．RMON は適切なトラフィック管理のために有用な技術といえる[2][3].

しかしながら，最近の LAN スイッチを導入したネットワーク環境下では，トラフィック管理のために収集すべき MIB 情報が飛躍的に増大する結果となった．このため，収集方法，収集データの保存，収集データの分析方法といった点において従来の手法ではネットワークの管理上不十分であることが認識されてきている[4].

本稿では LAN スイッチを導入したネットワーク環境下で RMON によるトラフィック管理を行う上で，従来の手法の問題点を整理する．さらにその問題点を解決する効率よいトラフィック分析手法の試みについて述べる．

なお，以下で想定するネットワーク規模としてはバックボーンに数台の基幹ルータを要するようなキャンパスレベルの中規模 LAN である．ISP レベルの大規模ネットワークや SOHO レベルの小規模ネットワーク管理は対象外である．

2. 標準的なトラフィック測定手法

2.1. SNMP

SNMP はクライアント・サーバ型のアーキテクチャで，ネットワーク上の SNMP エージェントと SNMP マネージャとの間で MIB (Management Information Base)と呼ばれる仮想的なデータベースの管理情報を SNMP プロトコルにより送受信することで成り立っている．SNMP エージェントは PC とサーバ，ルータと LAN スイッチ，または LAN プローブなどのネットワーク上の各ノードに実装される．この MIB の管理情報はノードの持つインターフェイスの送受信バイト数や送受信パケット数，エラー数などのインターフェイス統計情報と，各ベンダが独自に定義した拡張 MIB によるそのベンダ機器の情報と，LAN プローブが接続したセグメントのトラフィック統計情報などである．一方 SNMP マネージャは各 SNMP エージェントの取得するこれらの MIB 情報を一元的に管理することでネットワークの構成管理と性能管理を行う．また

SNMP エージェントがノードのアラートを検知したときに送信する TRAP 情報の宛先となることで，ネットワークの障害管理を行う．

2.2. RMON

SNMP 上でセグメントのトラフィック統計情報を取り扱うトラフィック管理技術が RMON である．特に RMON 情報を扱う SNMP エージェントを RMON エージェント，RMON 情報を扱う SNMP マネージャを RMON マネージャと呼ぶ．

RMON マネージャは通常ワークステーションやサーバ上のソフトウェアとして動作し，RMON エージェントから各セグメントのトラフィック情報を一括管理する．さらにこれらの情報をグラフ表示したりレポート表示する機能を持つことが多い．

3. スイッチド・ネットワークの特性と問題

3.1. スイッチド・ネットワーク

ここ数年で本格的に導入されてきたネットワーク技術に LAN スイッチによるネットワークのセグメント化がある．

キャンパス LAN で広く使用されている Ethernet や FastEthernet の伝送方式は CDMA/CD 方式であり，ひとつの伝送媒体を多数のノードが同時に使用する媒体共有を基本とする．

ブリッジハブは，このようなネットワークをセグメント化する従来から用いられていたネットワーク機器である．ブリッジハブはデータリンク層レベルでデータ・フレームを中継するマルチインターフェイスのネットワーク機器で，コリジョン・ドメインをブリッジバブの下のセグメント内へ閉じ込め，コリジョンの影響がネットワーク全体に広がらないようにする．

ブリッジバブの下位に接続する全ノードは一つの帯域を共有するので，ブリッジに１つのプローブなどの RMON エージェントを１つを配置することで，下位に接続する全ノードに関するトラフィック統計情報を収集することができる(図１)．

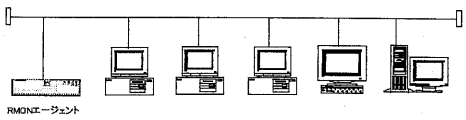

図１:ブリッジハブを用いたネットワーク

一方，ここ数年で本格的に導入されてきた LAN スイッチはブリッジハブにスイッチング機能を融合させたネットワーク機器である．スイッチング機能とは，多数のインターフェイスを備え，データリンク層アドレスに基づいて受信したデータ・フレームをあて先アドレスの接続インターフェイスのみに転送する機能である．また，最近ではスイッチング技術をデータリンク層以上に拡張したレイヤ３スイッチやレイヤ４スイッチも普及しはじめている．LAN スイッチの導入によってスイッチド・ネットワーク化を実現したネットワーク環境は，10BASE-T や 100BASE-TX，FDDI など複数のメディアの共存，インターフェイスごとの専有帯域，全２重の通信，論理的なデータリンクトポロジ(VLAN)の構成などブリッジハブベースでは提供できなかった柔軟性のあるキャンパス・ネットワークの構築を可能とした(図２)．

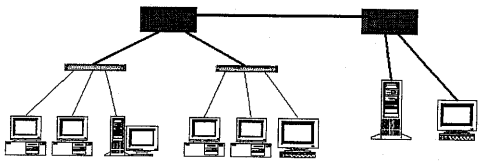

図２:スイッチド・ネットワーク

3.2. スイッチド・ネットワークにおけるトラフィック統計情報の収集

しかしながら，LAN スイッチを導入したネットワーク環境下で RMON によるトラフィック管理を適用するにはブリッジハブベースでは不要であった課題が生じた．プローブを LAN スイッチに接続して取得できるトラフィック統計情報は，そのインターフェイスにスイッチングされるトラフィック情報のみである．ブリッジハブでは下の全インターフェイスのトラフィック統計情報は 1 つのプローブで収集できたのに対して，LAN スイッチでは同等の手法ではインターフェイスの数だけプローブを用意しないと全インターフェイスのトラフィック統計情報の収集は実現できない．これが LAN スイッチにおけるトラフィック統計情報収集上の問題点である．

ただし，LAN スイッチにおけるトラフィック統計情報収集上の問題点は内蔵 RMON エージェントとミラーリング機能などで対応が可能である．

内蔵 RMON エージェントとは，LAN スイッチ自体に全インターフェイスのトラフィック統計情報の収集を行う RMON エージェントの機能を実装したものである．しかしながら内蔵 RMON エージェントは LAN スイッチの本来のスイッチング機能の負担とならないように，収集できる RMON 情報を RMON の Statistics グループや History グループ程度に制限していることがある．この制限を補完するのが，インターフェイス・トラフィックのミラーリング機能である．ミラーリング機能とは，特定のインターフェイスについてフルに RMON の機能が可能となるように，そのインターフェイスのトラフィックをプローブを接続した監視用インターフェイスへコピーする機能である．

この内蔵 RMON エージェントとミラーリング機能を用いることで，LAN スイッチの場合でも下位に接続する全ノードに関するトラフィック統計情報を収集することができる．

3.3. スイッチド・ネットワークにおけるトラフィック統計情報データ量の問題

最近認識されているのが，こうして収集した LAN スイッチからのトラフィック統計情報が，MIB 情報として膨大になるという問題点である．

ブリッジハブの場合は，トラフィック統計情報の収集の基本単位がハブ単位であった．これに対して，LAN スイッチの場合，各インターフェイスがトラフィック統計情報の収集の基本単位となる．ブリッジハブ・ベースのネットワークを数十個のインターフェイスからなる LAN スイッチに代替することでスイッチド・ネットワーク化する場合，トラフィック統計情報は実質的にネットワークの規模が以前の数十倍になったのと同等になる．

対処すべきデータ量が数倍程度なら従来の手法を改良することで対処が可能であるが，数十倍となると根本的に対処法が変化する．

例えばブリッジハブベースの場合の保持するデータが 100MB 程度だったとすると，これが LAN スイッチを導入することで数 GB 程度へ増加することになる．100MB 程度なら単純なデータファイルとしてアプリケーションで処理できる分量であるが，数 GB となるとデータ構造を意識した手法を確立しないと，収集データ保存の段階で破綻してせっかくの収集データを活用できなくなってしまう．

3.4. スイッチド・ネットワークにおけるトラフィック統計情報の集計上の問題

膨大な収集データの保存方法とは別に，集計上の問題がある．収集データそれ自体の中身は MIB 項目の情報であるが，実際にトラフィック分析に

活用するには収集データの集計加工作業が必要となる.

たとえば, ネットワークの平均的な利用状況を収集データから知るためには, 週平均や月平均の集計作業が必要となる. この作業自体の手間は, ブリッジハブでは装置1台ごとに1回の作業に対して, LAN スイッチでは各ポートごとに必要となり, データ数の増大に応じた手間が必要となる. この作業の負担も大きなものとなる.

3.5. レポート作成上の問題

トラフィック分析の結果は, 最終的には何らかのレポートとして作成することになる. 週平均や月平均の集計結果を得た場合は, 週次報告書や月次報告書といった形で要約されることになろう. この場合, 集計結果の表現形式としては帳票やグラフなどが一般的である. たとえば集計結果をスプレッドシートによって加工して月次報告書に添付する表やグラフを作成することになるが, この労力も決して小さくはない.

4. 問題点解決へのポイント

以上述べたように, LAN スイッチを導入したネットワークでトラフィック管理を行うためには, 収集データが膨大となるという根本的な問題から, データ保存の問題, データ集計の問題, レポート作成の問題と解決すべき課題が生じる. ISP のような大規模ネットワークなら, 専門のネットワーク管理者による特別な対応が可能である. また SOHO のような小規模なネットワークなら手作業の範囲での解決の可能性がある. しかしながら, 中規模なネットワークの場合は手作業で補完するにはデータ量が膨大となりすぎ, そうかといって大規模ネットワークのような特別な対応も人員や予算の都合上不可能である.

中規模ネットワークで問題点を解決する指針は, 問題点への負荷を大幅に削減できるような標準化した自動化と, 体系的な分析手法の確立である.

以下に述べるのは, データ集計の問題を改善するためのポイントである.

4.1. MIB-II/RMON の使い分け

RMON の場合インスタンスが動的に生成され, インターフェイスと対応付けて集計するのが煩雑である. MIB-II ではインターフェイス ID で容易に index できる.

- LAN スイッチのポート単価の低下に伴う 1 ポート-1 ノード接続の増加.
- スイッチング能力の向上によるエラーフリーフォワーディング(store-and-forward)の実現.

により collision や runts 等, RMON-MIB のエラーオブジェクトはあまり重要で無くなりつつある. パケット数やオクテット数のカウントであれば MIB-II の interfaces グループを使うことで, 集計・レポート作成が容易になる.

4.2. 適切な aggregation

収集したトラフィックデータは日次・月次単位で集計が必要である. これらの集計をインターフェイス毎, VLAN 毎, あるいはスイッチ毎といった単位で行う必要がある. 現在 IETF で標準化過程にある switch RMON (SMON)ではスイッチでの aggregation が実装される予定だが, 当面は外部のマネージャ側で aggregation を行う必要がある[5]. この場合集計期間が長くなるほど処理するデータ量が多くなり, 集計時の作業量が大きくなるので, あらかじめデータを予集計しておくことが効率化につながる. 例えば月次集計には既に日次集計で纏められたデータを用いることで扱うデータ量を減らすことができる.

但しその際集計によって生じる丸め誤差の累積に留意する必要がある.

4.3. SNMP プロセスと集計プロセスの分離

収集データの集計には CPU やディスク等のリソースを消費する．測定対象オブジェクトが多い場合にはSNMP の読みこぼしが発生しないよう，SNMP マネージャプロセスと集計プロセスで使用する CPU やディスクを分離する等の配慮が必要になる．

5. まとめ

本稿では，LAN スイッチを導入したネットワークのトラフィック管理を RMON ベースで行う場合，収集すべき MIB 項目が膨大になることに起因する問題点を整理した．また，問題点を解消する効率よいトラフィック分析手法のポイントについて述べた．

現在，著者は統計情報データ量の問題とレポート作成上の問題に対して試作ツールを開発中である．また，これらのツールを用いることでの実際のトラフィック管理手法確立へ向けて検討を行っている．

参考文献

[1] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)", RFC1157, May 1990.

[2] S.Waldbusser, "Remote Network Monitoring Management Information Base", RFC1757, February 1995.

[3] S.Waldbusser, "Remote Network Monitoring Management Information Base Version 2 using SMIv2", RFC2021, January 1997.

[4] 林 英輔，中山雅也，箱崎勝也："総論：安定したネットワークの構築，運用をめざして"，情報処理学会誌 Vol.39 No.10，1998 年 10 月．

[5] R. Waterman, B. Lahaye, D.Romascanu, S. Waldbusser, "Remote Network Monitoring MIB Extensions for Switched Networks Version 1.0", INTERNET DRAFT, February 1999.