Vol.2015-IOT-31 No.14
Vol.2015-SPT-15 No.14
2015/9/26

OpenFlow ネットワークにおけるトラフィック測定方法の提案

薄田昌広[†1]

OpenFlow のフローエントリを冗長に記述することでネットワークのトラフィックを測定するための方法を提案した．この方法では測定のための追加機器が不要でありパケット転送に影響を与えない．提案した方法について，OpenFlow コントローラとハードウェアスイッチングハブで動作検証システムを構成して機能を検証した．

A Proposal for Traffic Measuring Method in OpenFlow Networks

MASAHIRO SUSUKITA[†1]

We proposed a method for measuring traffic in OpenFlow networks by describing the flow-entries. This method does not require any additional equipment for measurements and does not affect the packet transfer. We configured a verification system which consist of an OpenFlow controller and a hardware switching hub and verified the functionality of this method.

1. はじめに

企業などの組織内 LAN では，業務に利用する情報システムの性能維持, セキュリティ対策, 障害調査などのため，ネットワークに接続している端末の転送データ量や内容などトラフィック測定と分析を必要時に行っている．

近年，複雑なネットワーク設定をより柔軟に素早く行うために SDN という考え方が推進されており, 主要な標準規格として OpenFlow[a]のネットワーク機器への実装が進んでいる．OpenFlow では，ネットワーク全体を考慮した経路制御など，コントローラからネットワーク機器を細かく制御することが可能である．一方で，送信先や時刻などの条件で動的に経路を変更するような場合などは，トラフィック測定の場所設定や結果の分析などが困難となる．

本研究では, OpenFlow ネットワークで経路を指定するために使用するフローエントリを冗長に記述することでトラフィックの内訳を得る測定方法を提案し, OpenFlow 対応のスイッチングハブで動作を検証した．

2. 従来ネットワークでのトラフィック測定

簡略化した組織内 LAN でのトラフィック測定例を図 1 に示す．この例ではスイッチングハブ(図の Switch)，ユーザ PC（図の PC1, PC2），内部サーバ（図の SV）で LAN を構成しており，ファイア・ウォール（図の FW）を経由してインターネットへ接続している．この LAN でのトラフィック測定の例と問題について以下に述べる．

2.1 スイッチングハブポートの統計情報取得

一般的な業務用スイッチングハブではポートごとにパケット数やバイト数，エラー等を計測するためのポートカウンタ機能が実装されている．カウンタ値は SNMP などを用いて監視用のサーバから集約することも可能である．この測定は特に LAN の性能低下時にボトルネック部分の調査を行ったり，インターネット向け回線の増強を計画したり，という場合に行うが，トラフィックの内訳は分からないため，詳細な状況はまでは把握できない．

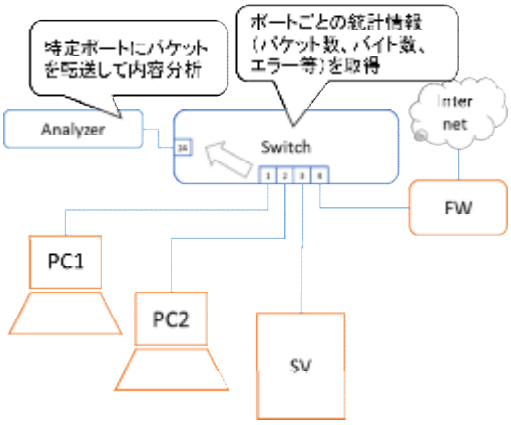

図 1　トラフィック測定例

2.2 パケットデータによる情報取得

スイッチングハブには，各ポートで転送しているパケットを測定用ポートに複製転送する機能をもつものもあり，この機能によってパケット自体を取得できる．ネットワーク障害の原因調査やセキュリティ事故の調査，ネットワークアプリケーションの利用状況の確認などでは測定用ポートに測定器（図の Analyzer）を接続して使用する．

この方法では詳細な情報を得ることができるが，測定対象が多い場合などは複数の測定器や高性能測定器が必要であり, OpenFlow ネットワークについてはコントローラが動

†1 関西電力株式会社
Kansai Electric Power Co., Inc.

a) Open Network Foundation (https://www.opennetworking.org/) による標準規格

Vol.2015-IOT-31 No.14
Vol.2015-SPT-15 No.14
2015/9/26

的に経路を設定する場合には対応づけが発生するなど，機器や手間についてのコストが高くなる．

3. 提案方法（フローエントリによるトラフィック測定）

本研究では，OpenFlow の仕様に基づき，経路設定のルールであるフローエントリを利用したトラフィック測定を行う方法を提案する．この方法では利用特定の経路を通過したトラフィックに対して送信元やネットワークアプリケーションの内訳を得る．この方法はネットワーク障害時のパケット到達判定や，ネットワークアプリケーション利用状況の確認などに適用可能である．また，専用の測定器は使用しないため，低コストで実現できる．

3.1 フローエントリについて

図 1 の従来スイッチを OpenFlow スイッチ(以下 OF スイッチ)に置換えた状態を図 2 に示す．OF スイッチには，制御のための OpenFlow コントローラ（図の OF Controller）を接続している．

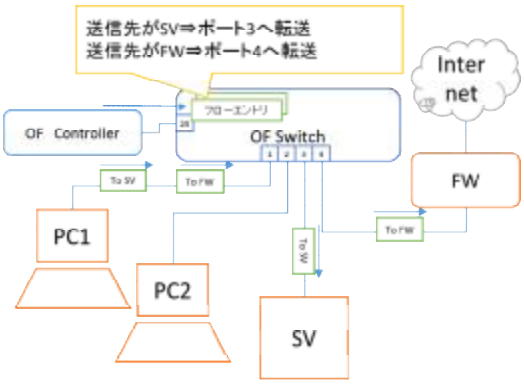

図 2 OpenFlow の例

OpenFlow においては，OpenFlow スイッチのポートに入ってきたパケットに対して，フローエントリというルールを順に適用して処理を決める．個々のフローエントリは，条件を判定するためのマッチ部分と出力先などを決定するアクション部分で構成される．マッチ部分では，イーサネット（レイヤ 2）ヘッダだけではなく IP（レイヤ 3）ヘッダ，TCP や UDP（レイヤ 4）ヘッダなど複数の通信階層の合致条件を指定することができ，エントリにマッチした場合は回数などの統計情報を記録するカウンタに結果が反映される．

3.2 フローエントリの分割

ここで，同じ送信先に対するフローエントリのマッチ条件を送信元別に分け，複数のエントリに分割しても転送結果には変化がない．同様に同じ転送先に対してのフローエントリをレイヤ 4 の異なるポート番号へのマッチに分割することができる．

図 2 のネットワークでサーバ向けのフローエントリを分割した例を図 3 に示す．この例では一つのフローエントリを送信元アドレスとレイヤ 4 送信先ポート（図の L4 送信先列）別に四分割している．

送信元	送信先	プロトコル	L4送信元	L4送信先	出力先
*	SV	*	*	*	ポート3

送信元	送信先	プロトコル	L4送信元	L4送信先	出力先
PC1	SV	TCP	*	HTTP	ポート3
PC1	SV	TCP	*	SMB	ポート3
PC2	SV	TCP	*	HTTP	ポート3
PC2	SV	TCP	*	SMB	ポート3

図 3

同様に，ファイア・ウォール向けのエントリやサーバやファイア・ウォールから PC への下りトラフィックのフローエントリも分割できる．ここで，PC 向けの下りトラフィックについては，PC からの上りトラフィックに対応づけるために L4 送信元ポートで分割することで上りトラフィックと対応づけ．についてのネットワークアプリケーションごとの統計情報が記録される．

3.3 統計情報の取得

記録した統計情報は OF コントローラを利用して定期的に取得する．送信元や送信先で集計すると，取得時点でのトラフィックの内訳を知ることができる．この方法により，測定用機器を追加することなくネットワークアプリケーションの利用状況などのトラフィック測定が実現できる．

4. 提案方法の検証

4.1 検証システム

図 4 のとおり試験システムを構成し，提案方法の動作を検証した．OF スイッチはオープンフロー対応のギガビット 24 ポートハードウェアスイッチングハブを，コントローラは OpenDaylight Hydrogen を使用した．コントローラとスイッチは OF バージョン 1.0 で接続した．

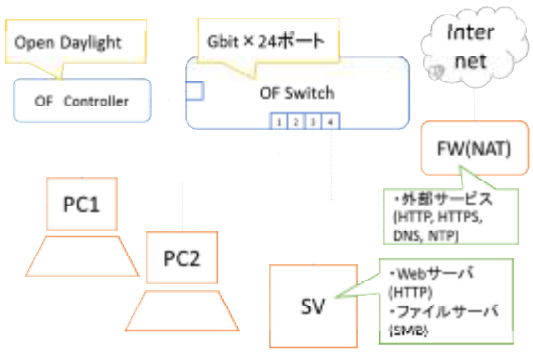

図 4　動作検証システム

4.2 機能検証

コントローラから OF スイッチに対して測定用フローエントリを設定した後，通信試験を行った．検証システムに設定したフローエントリ数は 38 であった. 通信試験の結果, PC～サーバ間，PC～ファイア･ウォール間のすべての通信が正常に実施できており，測定用フローエントリによる機器の通信の支障は無いことが確認できた．

通信試験実施後，コントローラからスイッチに各フローエントリのカウンタ値の要求を行い，それぞれのカウンタ値を得ることができた．これらのカウンタ値を集計することで，サーバ向けとファイア・ウォール向けトラフィックの内訳を確認することができ，提案した測定方法が機能することを検証できた．

4.3 機器に与える影響

今回の方法ではスイッチに接続する PC などの台数に比べてフローエントリが多くなる．また，物理ポート番号，レイヤ 3 アドレス，レイヤ 4 ポート番号など複数のマッチ条件を利用する．これらの設定による OF スイッチの転送性能への影響を調査するため転送速度を測定した．

ネットワーク性能測定器を OF スイッチの各ポートに接続して，PC～サーバ間，PC～ファイア・ウォール間のトラフィックを生成して転送速度とパケットロスを測定した．結果，ポート性能の 1Gbit/秒での転送が行われており，パケットロスも発生しないことを確認した．

5. まとめと今後の予定

OpenFlow ネットワークでの障害対応やネットワークアプリケーションの利用状況確認などを目的とした低コストのトラフィック測定方法を提案し，実際のハードウェアスイッチングハブで正しく機能することを確認した．また，この方式による性能低下も発生しなかった．

今後は，複数スイッチへの適用などシステムの拡大，フローエントリ登録から統計情報の表示までの連携のシステム化などを検討して実ネットワークでの試用を進める予定である．