

WIDE のトランジットトラフィック概要

1 2015 年トラフィック概要

MAWI ワーキンググループでは、トラフィックを多次元集約する agurim ツール [1] を開発し、2013 年 2 月より WIDE のトランジット回線のトラフィックを継続的に記録している。2015 年 5 月には、ツールをオープンソースとして公開し、同時に、IP アドレスを匿名化した WIDE のトランジット回線のトラフィックデータを Web インターフェイスでブラウズ可能にした [2]。これによって、ネットワーク運用者や研究者が、バックボーンのトラフィック状況の詳細をブラウズできるようになり、トラフィック情報の共有や研究の促進に繋がることを期待している。

agurim ツールは、トラフィック量およびパケット数を使ってフローを集約する。パケットキャプチャしたデータを基に、30 秒間隔で一次集約フローデータを作成、保存している。また、このデータから 1 時間毎に再集約したデータを、さらにこの 1 時間毎のデータを基に 1 日毎の再集約データを生成している。データの閲覧する際には、Web ユーザインターフェイスから、時間粒度やフロー数を変化させて、グラフ生成を行なう。元データには、pcap、NetFlow、sFlow が利用可能である。

ここでは、2015 年 1 年間のトラフィック概要を、公開している匿名化データを使って示す。同じ元データから、アドレスを元に集約したトラフィック量 (図 1) とパケット量 (図 3)、プロトコルを元に集約したトラフィック量 (図 2) とパケット量 (図 4) の 4 つのグラフに表している。いずれのグラフも粒度は 1 日となっている。

なお、データを収集しているスイッチのポートミラーリング設定の不備により、2015 年 5 月 28 日から 6 月 1 日までの期間において大部分のパケットが重複して取得されていた。その結果、この期間のトラフィック量、パケット量ともに実際の倍近い値が記録されている。

グラフの各集約フローのラベルは、ソース、デスティネーション IP アドレス (レンジ) と全体に対する割合に続いて、そのうちの上位サブフローのリストが示される。サブフローは、プロトコル番号、ソース、デスティネーションポート番号と、その集約フローに対する割合で表される。“*” はワイルドカード (IPv6 アドレスの場合は “*::”) を示す。

全体を通して、1 日平均のトラフィック量は約 300-800Mbps、パケット量は 50-2000kpps 程度である。(前述のパケット重複を考慮した値である。) 個別の集約フローを見ると、/16 程度に集約されたネットワークに加えて、いくつかのホストが識別されている。ここには、ftp.jaist.ac.jp、pinger-j2.ant.isi.edu などが含まれる。ISI のマシンは SFC でホストしている pinger プローブである。

MAWI ワーキンググループでは、今後も agurim ツールを使ったトラフィック状況の把握を行なっていく予定である。

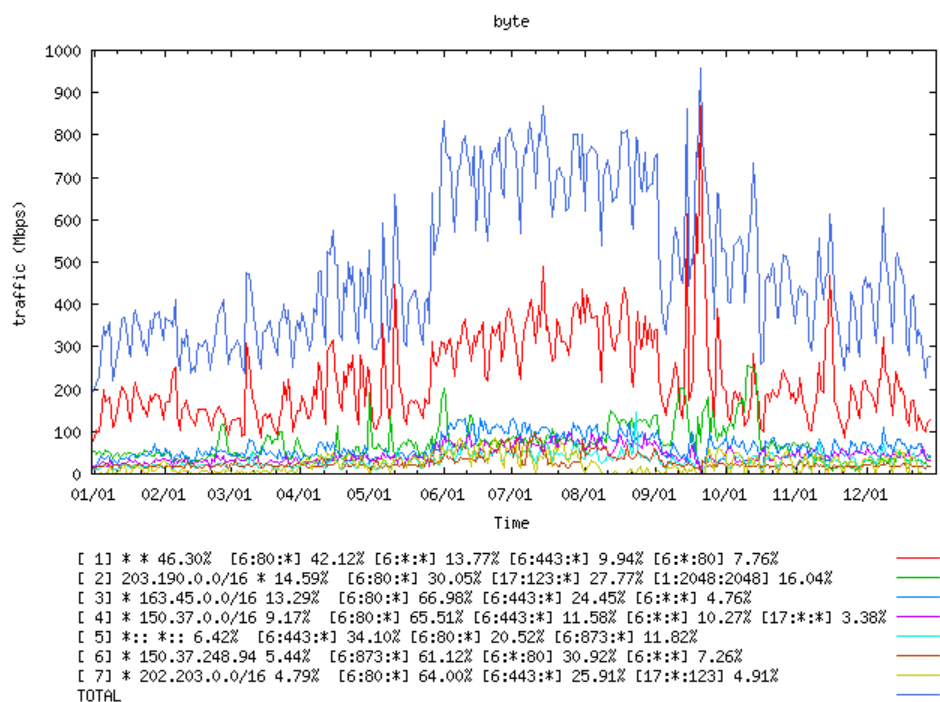


図 1: アドレス別トラフィック量 (2015 年 1 月-12 月)

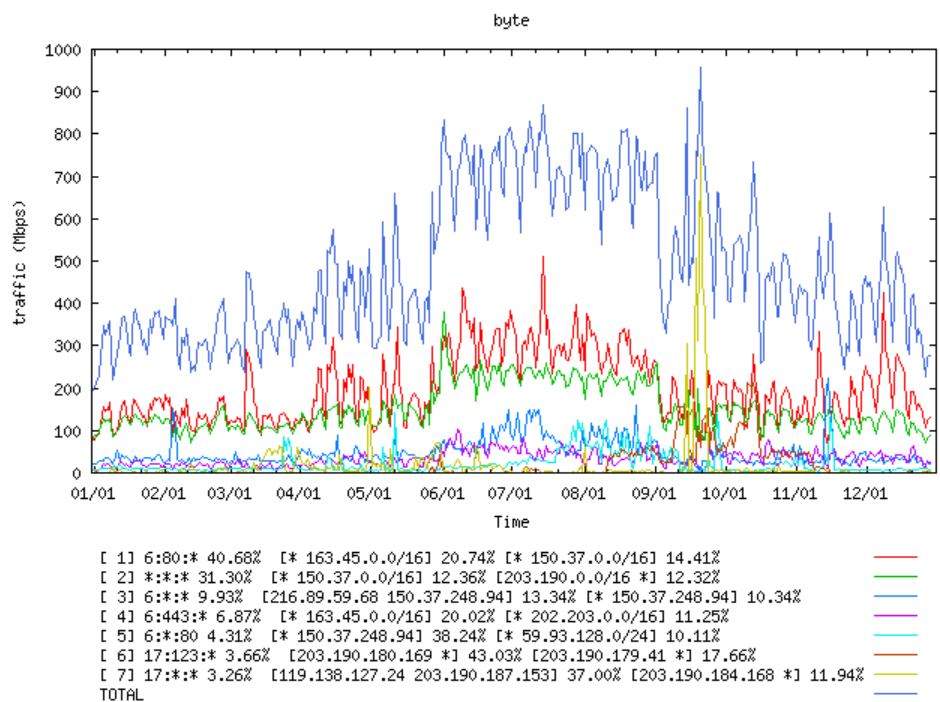


図 2: プロトコル別トラフィック量 (2015 年 1 月-12 月)

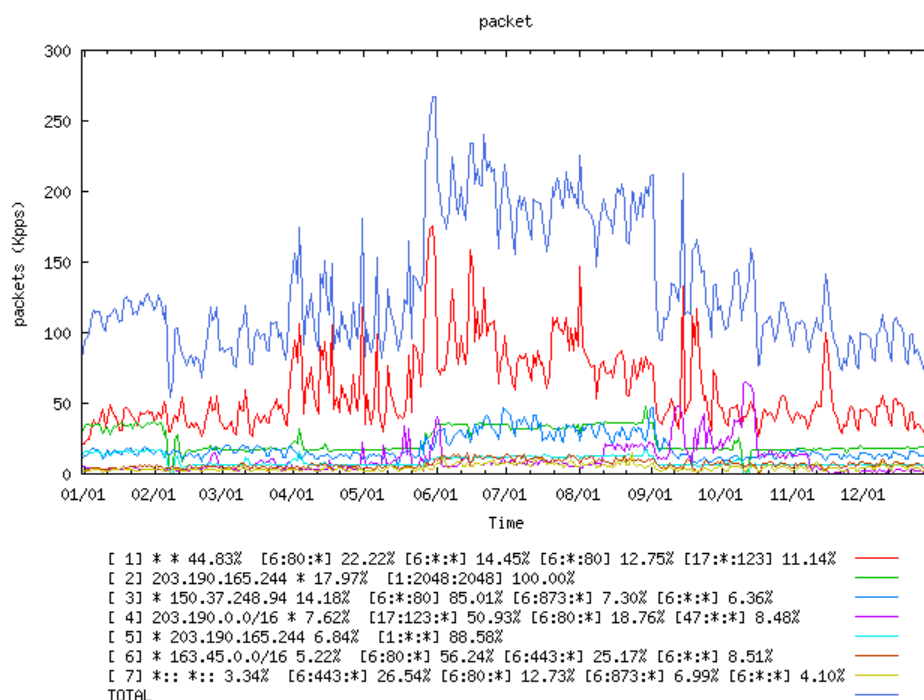


図 3: アドレス別パケット量 (2015 年 1 月-12 月)

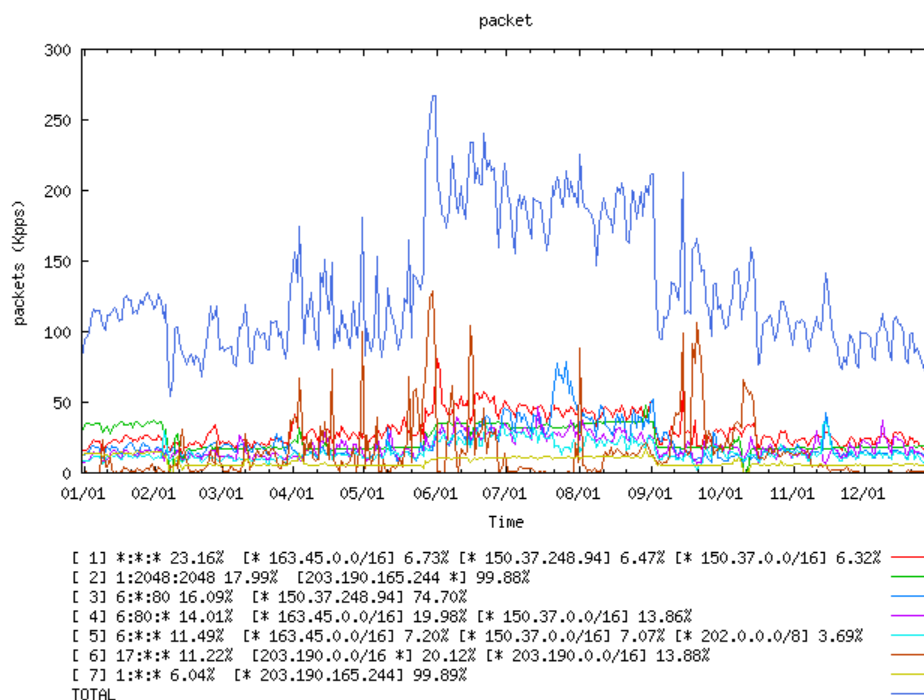


図 4: プロトコル別パケット量 (2015 年 1 月-12 月)

参考文献

- [1] Midori Kato, Kenjiro Cho, Michio Honda, Hideyuki Tokuda. Monitoring the Dynamics of Network Traffic by Recursive Multi-dimensional Aggregation. OSDI2012 MAD Workshop. Hollywood, CA. October 2012.
- [2] Agurim Web site. <http://mawi.wide.ad.jp/~agurim/about.html>