

BGP ルーティング情報の収集と分析 (wide-draft-mawi-v4bgpanaly-00.pdf)

小出 和秀 (koide@shiratori.riec.tohoku.ac.jp)

01/07/2005

1 BGP ルーティング情報の収集と分析

mawi ワーキンググループの活動の一貫として、従来より WIDE ネットワークの BGP ルータの経路情報の収集が行われている。BGP 情報は、mawi ワーキンググループと WNOC-Sendai(仙台 NOC) が協力して収集を行っており、2003 年 8 月 27 日に開始され、これまでに 1 年以上のデータを収集して来た。本稿は、これまでに収集された BGP 経路情報の分析結果を報告するものである。なお、本活動はもともと、ネットワーク情報の分析をより高度に行なうために BGP 経路情報を活用する目的で始められたものであるが、routeviews ワーキンググループが設立されたことにより、上記の研究は今後 routeviews ワーキンググループにおいて行い、成果の報告も行う予定である。本稿では上記の関連を考慮し、特に mawi ワーキンググループの研究領域である統計的情報に絞って報告を行う。

1.1 概要

WIDE(AS2500) の BGP ルータが持つ全ての経路 (full route) 情報を定期的に収集し、結果を保存している。データを蓄積している PC は仙台 NOC に設置しているが、仙台 NOC には full route を持つ BGP ルータが存在しないため、当該 PC において zebra を用いて BGP プロセスを起動し、LA-NOC に存在する CISCO ルータと ebgp multihop によって private peering を確立することで full route を取得している。

仙台 NOC において peering を行っている PC の諸元は以下の通りである。

- Name/IP : pc10.sendai.wide.ad.jp(203.178.138.26)
- OS : FreeBSD 4.10-Release-p5(2004/12/23 現在)
- Disk Space : 20GB + 120GB(RAID) + 700GB(RAID)
- BGP daemon : zebra-0.94.2(2004/12/23 現在) (zebra + bgpd)

peering 先は、

- cisco1.LosAngeles.wide.ad.jp(203.178.136.20)

である．full route を Mirroring する設定としている．以下に bgpd の設定ファイル (bgpd.conf) の内容を掲げる．

```
! -- bgp --
!
! BGPd configuratin file
!
hostname pc10.sendai.wide.ad.jp
password *****
enable password *****
!
router bgp 64514
  bgp router-id 203.178.138.26
  neighbor 203.178.136.20 remote-as 2500
  neighbor 203.178.136.20 ebgp-multihop 8
!
dump bgp all /db1/bgpdata/%Y.%m/BGPALL/all.%Y%m%d.%H%M 2h
dump bgp updates /db1/bgpdata/%Y.%m/UPDATES/updates.%Y%m%d.%H%M 15m
dump bgp routes-mrt /db1/bgpdata/%Y.%m/RIBS/rib.%Y%m%d.%H%M 2h
```

データの蓄積は，Routeviews Project(<http://www.routeviews.org/>) が蓄積している，BGP パケットの Full dump，UPDATE パケットの dump，および RIB データの 3 種類のデータを 2 時間毎に蓄積しているのに加えて，管理コンソールから (show ip bgp) を実行して得られる output も 1 時間毎に収集，蓄積している．

データ蓄積は，2003 年 8 月 27 日から現在まで継続して行なっている (PC のメンテナンス等のため，データの存在しない期間も若干ある)．現在，総データ量は 141.7GB 程度となっている．

1.2 統計情報

以下の統計情報について分析を行った．なお分析期間はほぼ 1 年間とし，開始当初から 2004 年 8 月末までのものである．データとして，上記で説明した，1 時間毎に取得している (show ip bgp) の結果を用いている．

- 学習したプレフィックスの総数
- 上記のプレフィックスに対応する，相異なる AS パスの総数
- AS パスの平均長
- プレフィックスおよび AS パスの安定性

1.2.1 プレフィックス数の変動

BGP ルータが学習した，相互に独立なプレフィックスの総数の変動を 1 時間毎にプロットした結果が Figure.1 である．

1 年間でほぼ 15000 個増加している．また 2004 年 3 月にプレフィックス数が一時的に減少している様子が分かる．

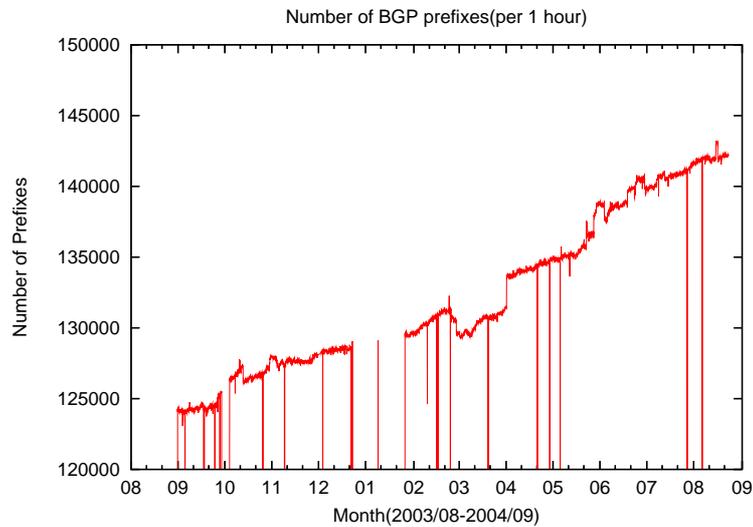


Figure 1: Number of prefixes

1.2.2 相異なる AS パス数の変動

Figure.1 で示したプレフィックスに対応する AS パスで、相互に独立なものの総数の変動を 1 時間毎にプロットした結果が Figure.2 である。すなわち異なるプレフィックスに対して同一の AS パスが学習されている場合には重複して数えることはしない。また、学習した全 AS パスの総数を示したものではない。つまり単一のプレフィックスに対応する複数の冗長な AS パスに関してはカウントしていない。

1 年間でほぼ 3000 個増加している。また Figure.1 同様、2004 年 3 月に AS パス数が一時的に減少している様子が分かる。

1.2.3 平均 AS パス長の変動

Figure.3 は、上記の Figure.2 で対象とした AS パスに対して、AS パス長の平均を取ったものである。傾向として安定していることが分かる。

なお、AS パスにおいては、いわゆるダミーが挿入されることにより、しばしば同一の AS 番号が連続することがある。これらを削除したものと削除しなかったものを同一にプロットした。結果、両者の差は 0.5 程度であった。

1.2.4 プレフィックス数および AS パス数の安定性

長期に渡って同一のプレフィックスや AS パスが観測されるとき、それらを「安定」と呼ぶ。安定的なプレフィックスやパスがどの程度の割合で存在するのかを確かめた。

なお、「安定」を示す指標には 2 種類ある。一つは「流行性 (prevalence)」と呼べるものであり、当該期間に何回観測されたかという指標である。もう一つは

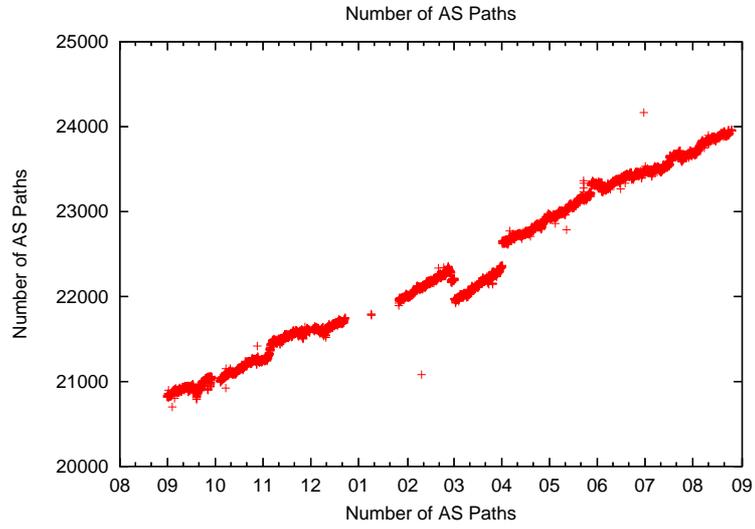


Figure 2: Number of different AS paths

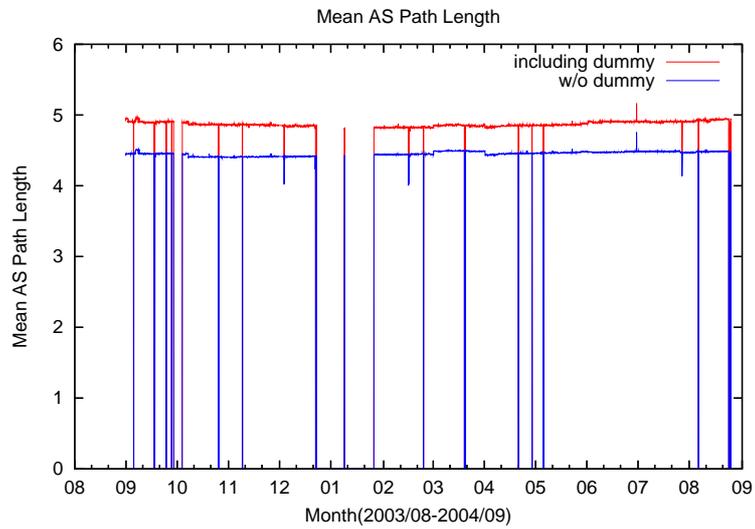


Figure 3: Mean AS path length

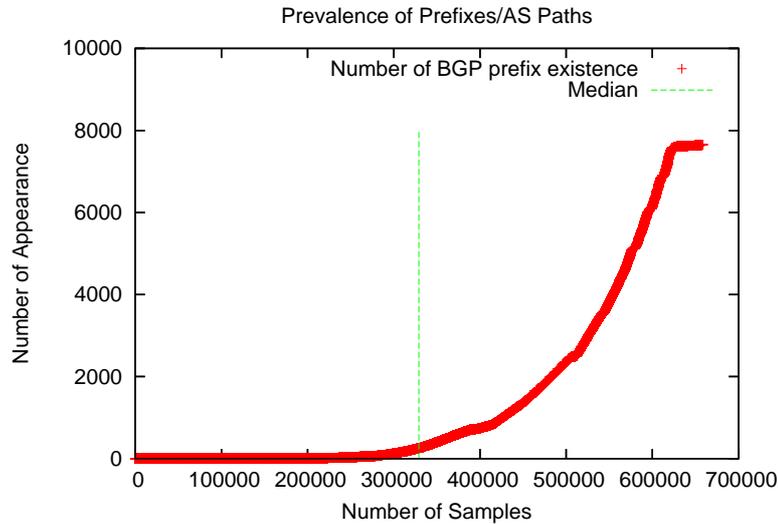


Figure 4: Prevalence of prefixes

「持続性 (persistency)」と呼ばれるもので、連続して観測される期間が長いかどうかを示す指標である。

Figure.4 は個別のプレフィックスについて、1年間を通しての累積観測回数を示したものである。これは上記の「流行性」を評価するものといえる。観測機会は、取得失敗が無かったとすると1年間で8760回となるので、これが累積観測回数の最大値である。また1年間を通して、プレフィックスおよびプレフィックス長が異なるケースが1回でも観測された場合はすべて個別のものとして計数している。トータルのケース数は658334であった。

このうち、カウント数が8760に近い、すなわち1年間でほぼ通して観測されたものも少なからずあることがグラフから分かる。一方で、カウント数の少ない、すなわち「流行性」の低いものも多い。計測数のメジアン値をとると257回であることがわかる。これはほぼ1週間分の計測機会に相当する。つまり、半分以上のプレフィックスは1週間分はBGP経路情報上に存在していたこととなる。

Figure.5 は「持続性」を評価したグラフである。観測のある時点から、個別のプレフィックスがどの程度連続して観測されたかをプロットしている。持続期間は1日、および1週間と設定した。グラフでは、ある観測点において、その時点で上記の期間以上の長さで連続して観測されているプレフィックスに関してカウントしたグラフを、全体のプレフィックス数と比較している。連続して観測されていたプレフィックスがある観測点から観測されなくなり、しばらくして再び観測されるようになった場合については一切考慮せず、再び観測されるようになった点を始点として持続期間を再カウントする。ただし、前述の通り、データ収集PCのメンテナンス等の理由からデータには部分的に抜けがあることがある。この点にそれらのプレフィックスが存在していたかどうかは判断できないため、便宜上、観測1回分の不連続性については無視することとした。

結果として、全体の88%程度に相当する110000以上のプレフィックスについ

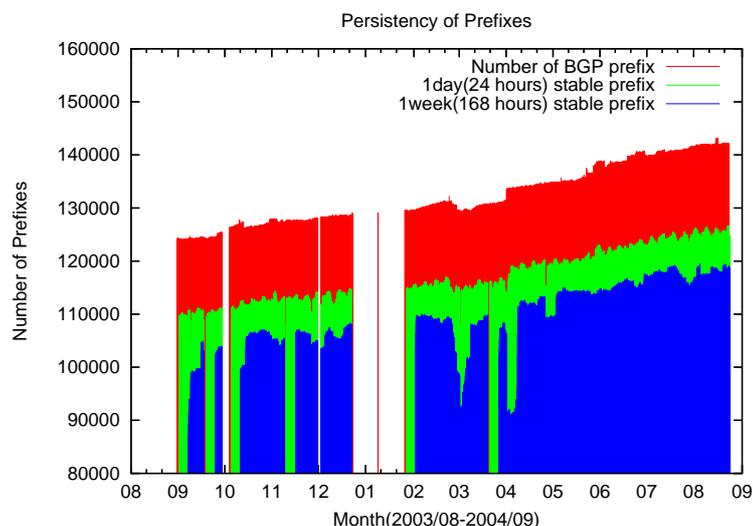


Figure 5: Persistency of prefixes

てはほぼ1日以上連続して観測され、さらに全体の83%程度に相当する100000以上のプレフィックスに関しては1週間以上連続して観測されていることが分かる。

1.2.5 2004年3-4月に見られたギャップについて

前述した、2004年3月から4月にかけてのプレフィックス数およびAS数のギャップについて考察する。経路数が元の傾向に回復したのは2004年4月1日から2日にかけてであった。この区間においてプレフィックスの変動の差分を分析すると、おおむねAS701(UUNET),AS11537(ABILENE),AS7660の関与する変動であることが分かった。これを元に、それらのAS番号をASパスに含むものについて、観測個数の変動を当該ギャップ区間においてプロットしたものがFigure.6である。

当該期間にはAS701をoriginとする経路が15000程度上昇しているのに対し、AS11537, AS7660の両方で12000程度の経路が減少している。これはネットワークの切替えに際して、AS701が経路の広告を代行したためと推測される。なお、当該時期にはJGNネットワークに関連するネットワークの切替えが実際に行われており、この観測結果はこれに伴う変動を表しているものと考えられる。

1.3 今後の方針

データの収集は今後も継続して行う方針である。

データの分析に関しては、同様の分析は様々な組織で行われていることから、より様々な切口の分析を行う必要があると考える。特徴的なパラメータの一つに、割り当てられているIPアドレスのうちどの程度の割合のアドレスの経路が広告されているか、というものが考えられる。これは実際に使用されているアドレスの割合を表すことになる。

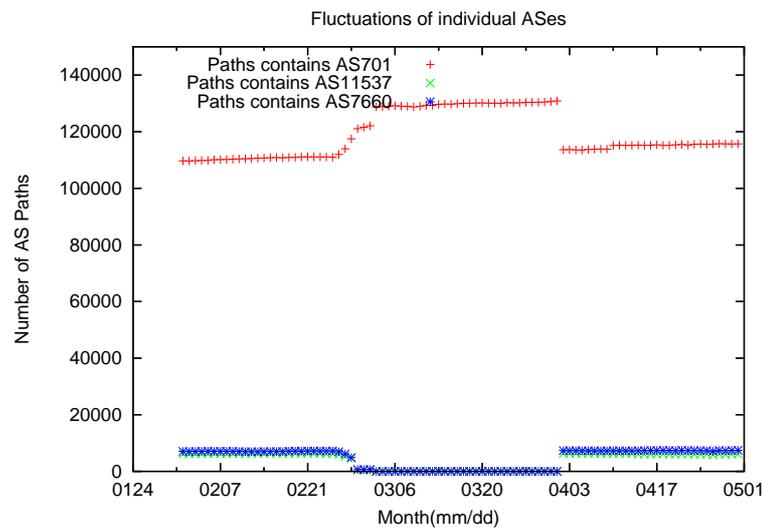


Figure 6: Fluctuations of some ASes

MAWI ワーキンググループでは IPv6 の BGP 情報の収集も行われているので、IPv4 および IPv6 の BGP 情報の統計を比較することも加味しながら今後の分析を進めることとなる。

Copyright Notice

Copyright (C) WIDE Project (2005). All Rights Reserved.