BGP ルーティング情報の収集

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

07/30/2004

1 BGP ルーティング情報の収集

本稿は，仙台 NOC の wide-netman チームが行なっているネットワーク情報収集活動において，ネットワーク情報の分析をより高度に行なうために BGP プロトコルのルーティング情報を活用するため，仙台 NOC で 2003/8/27 より開始した BGP 情報の収集について報告するものである．

1.1 活動の背景

wide-netman チーム (仙台 NOC) では，パッシブ型モニタを用いたトラフィック情報の収集を継続して行なっている．パッシブモニタリングでは収集されるデータ量は膨大になるため，適切なサマライゼーションや可視化を行なう必要がある．我々はこれまで，ネットワーク地図を用いたネットワークの可視化の研究を行なっている．ネットワーク地図とトラフィック情報を組み合わせることで，より直観的にネットワークを把握することができ，ネットワークの障害検出なども容易になると考えられる．ネットワークマップのような情報はネットワーク情報の「コンテキスト情報」と考えられるが，このような情報源として BGP プロトコルのもつ情報が有用であると考え，データ収集を行なうこととした．

1.2 BGP 情報の有用性

BGP(Border Gateway Protocol) は，AS(Autonomous System) の概念に基づいたルーティングプロトコルである．各 BGP ルータは自身が広告するネットワークプレフィックスを，自身の AS 番号とともに BGP peer に対して広告する．BGP は AS パスの長さに基づいて，ネットワークプレフィックスの次ホップを決定する．BGP ルータは基本的には隣接する BGP ルータと peer を確立するため，ルーティング情報伝播の過程で生成される AS パス情報はネットワークマップとしての性格を持つ．また同時にルーティングのためのネットワークプレフィックスは現実に存在するネットワークアドレスである場合が多く，その情報はネットワーク構成情報としての性格も持つ．すなわち BGP の内部状態情報は，ネットワーク情報のコンテキスト情報や情報集約のためのネットワーク構成情報として有用である．

しかし，通常は BGP ルータのみがこれらの情報を持つことができるため，特にリアルタイムなネットワークモニタリングへの活用には問題もある．BGP 情報の収集を行なっているプロジェクトとしては

Routeviews Project(http://www.routeviews.org/) があるが，モニタリングポイントのネットワークに存在する BGP ルータから情報を取得しなければ正しいルーティング情報は得られない．

我々が開発を行っているパッシブモニタリング手法はネットワークに負荷を与えないため，詳細なトラフィックの分析が可能である．パッシブモニタが BGP の情報を取得する形態として以下の 3 つが考えられる (Fig 1).

1. BGP ルータと private peering を確立し，BGP ルータから情報を転送する
2. BGP ルータと private peering する peering server を設置し，peering server より SNMP や BGP-MIB 等を用いて情報を取得する
3. BGP ルータが peering しているリンクをパッシブモニタリングし，BGP パケットをリアセンブルして情報を取得する

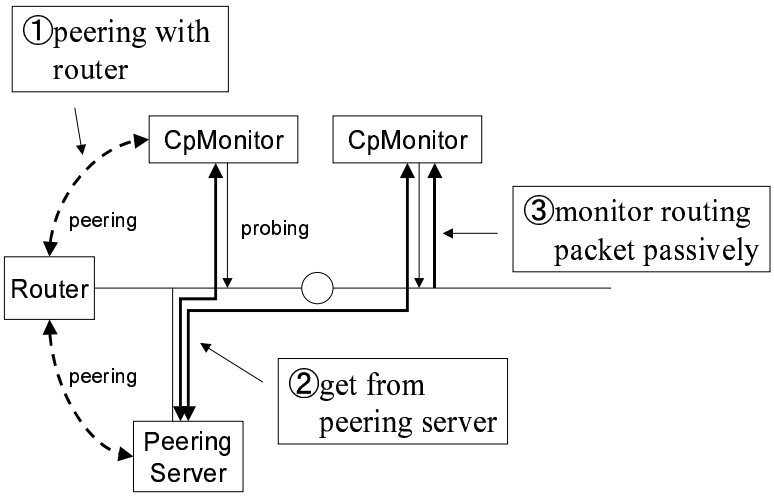

Figure 1: Injecting context information

1. の手法はもっとも理想的であるが，パッシブモニタの数が多数になる場合は有効ではない．また現実には BGP ルータとの peering はルータのポリシーの問題から難しい．

2. はパッシブモニタの数が多い場合に有効であるが，peering server へのポーリングのタイミングによって情報の更新にディレイが生じる．また，1. と同様のポリシーの問題がある．

3. はルータのポリシーに関係なく情報を取得でき，仕組みももっとも簡単である．しかし BGP ルータは情報を更新分だけ流すため，情報全体を取得するまでに時間がかかることと，情報が流れるリンクが限定されることが欠点である．

1.3 BGP 情報の収集

実験を行っている仙台 NOC には BGP ルータが存在しないため，1. および 3. のアプローチをとることはそのままでは出来ない．そのため，2. の方式を取る事と

し，WIDE の海外線に存在する CISCO ルータと ebgp multihop によって private peering を確立することとした．

これによって同時に 3. のアプローチを実験する環境も構築する事ができ，また同時に BGP の情報を収集，蓄積することで，オフラインでの解析や BGP データを用いたその他の解析にも役立てる事が出来る．

仙台 NOC において peering を行う 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 4.9-STABLE(2003/12/20 現在)
- Disk Space : 20GB + 120GB(RAID) + 700GB(RAID)
- BGP daemon : zebra-0.94(2003/12/20 現在) (zebra + bgpd)

peering 先は，

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

である．Full Route 情報を Mirroring する設定としている．

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 36.8GB 程度となっている．

1.4 今後の予定

現状では BGP ルータとの peering および情報の蓄積を始めた段階であり，peering server からパッシブモニタへの BGP 情報の注入機能の具体的な実装がこれからの課題である．