Real-Time BGP Data Access

Mikhail Strizhov

Colorado State University
Introduction

• Real-Time BGP data
  – What is it and Do you really need it?
  – What can you do with it?
  – Where and how can you get it?

• Running your own BGP collector
  – BGPMon: real-time, scalable, extensible monitoring system
    • Software architecture and design
    • BGPMon at Colorado State University

Real-Time BGP Data Access
Background

- Autonomous System (AS)
- Border Gateway Protocol (BGP)
- Profit-driven policy

Real-Time BGP Data Access
• BGP lacks authentication
• Fabricated AS announcement
• Prefix hijacking

April 8, 2010: Chinese ISP hijacks the Internet: China Telecom originated 37,000 prefixes not belonging to them in 15 minutes, causing massive outage of services globally.
BGP Message Example

• “Bits off the wire” between two BGP speakers:
  – 4001010040020C020536D900D10D1C10866E0F400304C02BD98D18BD5533
    • Not easy to analyze. RFC 4271 has all details.

• How we can represent BGP message in human readable format?
  – Extensible Markup Language (XML)
    • Extensible and easy to use data format.
    • It is widely used for the representation of arbitrary data structures.
    • It is common for XML to be used in interchanging data over the Internet (RFC 3023).
XML-Based Format for Representing BGP Messages (XFB)

```
<ASCII_MSG>
  <LENGTH>53</LENGTH>
  <TYPE value="2">UPDATE</TYPE>
  <UPDATE>
    <ATTRIBUTE>
      <LENGTH>12</LENGTH>
      <TYPE value="2">AS_PATH</TYPE>
      <AS_PATH>
        <AS_SEG type="AS_SEQUENCE" length="5">
          <AS>14041</AS><AS>209</AS> <AS>3356</AS>
          <AS>4230</AS><AS>28175</AS>
        </AS_SEG>
      </AS_PATH>
    </ATTRIBUTE>
    <ATTRIBUTE>
      <LENGTH>4</LENGTH>
      <TYPE value="3">NEXT_HOP</TYPE>
      <NEXT_HOP>192.43.217.141</NEXT_HOP>
    </ATTRIBUTE>
    <NLRI count="1">
      <PREFIX label="DPATH" afi="IPV4" afi_value="1" safi="UNICAST"
      safi_value="1">189.85.51/24</PREFIX>
    </NLRI>
  </UPDATE>
</ASCII_MSG>
```

BGP message total length
BGP message type, according to RFC 4271
BGP AS Path data
Next Hop data
Announced Prefix

*Not difficult, right?*
Receiving Data in Real-time

• Service is available now!
  – BGP update messages are accessible within a few seconds
    • Open telnet session or establish TCP connection to
      livebgp.netsec.colostate.edu port 50001
  – Full BGP table snapshots are available every 2 hours
    • Open telnet session or establish TCP connection to
      livebgp.netsec.colostate.edu port 50002
Example of XML Data

BGP Mon Peer Status (2001:1890:111d::1 : 179)

- Announcement
- Dup Announcement
- Same Path
- Diff Path
- Withdrawal
- Dup Withdrawal

Number

Date/Time

Real-Time BGP Data Access 8
Running Your Own Collector

• In order to monitor your own BGP router and network prefixes, you should:
  – Download and install BGP Monitoring System (BGPmon)
  – Run usual ./configure && make && make install
  – Create BGP peering session between router and BGPmon instance.
  – That’s all! Real-time data is available at port 50001 and 50002 of your BGPmon.

• Project Website

  http://bgpmon.netsec.colostate.edu
Merging Your Collector with Existing Collectors

Your router

More than 100 peers

Oregon RouteViews Collectors

BGPmon at Colorado State University

Client A

Your BGPmon

Client B

8 peers around the world

Real-Time BGP Data Access
BGPMon Architecture

Real-Time BGP Data Access
BGPmon features

• Open Source multi-threaded software
• Support IPv4 and IPv6
• Support 2-byte and 4-byte AS numbers
• Load balancing (Fast writers/Slow readers)
  – Queuing and Pacing Algorithms
• Backward-compatible with existing Routing Collectors via MRT format (draft-ietf-grow-mrt-13)
  • Quagga to BGPmon patch available from RouteViews
Conclusions

• BGPmon Provides Real-Time BGP data in a scalable way.
  – Essential Data Necessary for BGP Analysis
  – Enables Wide Range of New Services
• BGPmon represents an important change in how BGP monitoring is accomplished in the Internet
• BGPmon makes it much simpler for researchers and operators to obtain BGP data.

Service is available now – http://bgpmon.netsec.colostate.edu
Questions