Real-Time BGP Data Access

Dan Massey

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
BGP Message Example

• “Bits off the wire” between two BGP speakers:
  
  4001010040020C020536D900D10D1C10866E0F400304C
  02BD98D18BD5533
  
  • 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
Not difficult, right?
Next Hop data
Announced Prefix
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

BGPMon Peer Status (2001:1890:111d::1:179)

Date/Time

Number

Announcement
Dup Announcement
Same Path
Diff Path
Withdrawal
Dup Withdrawal

Real-Time BGP Data Access
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

More than 100 peers

Oregon RouteViews Collectors

Client A

Your BGPmon

Client B

BGPmon at Colorado State University

Your router

8 peers around the world

FRGP

Rogers

Tiscali

Real-Time BGP Data Access
BGPmon Architecture

- **Peer thread**
- **MRT thread**
- **Chain thread**
- **Peer Queue**
- **Label thread**
- **XML thread**
- **Server thread**
- **Periodic thread**
- **XML update queue**
- **XML RIB-IN queue**

**Components:**
- **Router 1**
- **Router 2**
- **Routing Collector**
- **BGPmon**
- **Client**

**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
Example BGP Peer Data

Statistics Report (Last generated on 08-22-2011 at 10:38)

1. BGP Peers

<table>
<thead>
<tr>
<th>IP</th>
<th>PORT</th>
<th>AS</th>
<th>Status</th>
<th>Uptime</th>
<th>#MsgRecvd</th>
<th>#Reset</th>
<th>#Prefix</th>
<th>#Attribute</th>
<th>Memory(k)</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>65.49.129.101</td>
<td>179</td>
<td>3043</td>
<td></td>
<td></td>
<td>1347763</td>
<td>0</td>
<td>365466</td>
<td>62041</td>
<td>39654.726</td>
<td>detail</td>
</tr>
<tr>
<td>205.167.76.241</td>
<td>179</td>
<td>10876</td>
<td></td>
<td></td>
<td>554129</td>
<td>0</td>
<td>362246</td>
<td>61062</td>
<td>30220.441</td>
<td>detail</td>
</tr>
<tr>
<td>89.149.178.10</td>
<td>179</td>
<td>3257</td>
<td></td>
<td></td>
<td>1177635</td>
<td>0</td>
<td>360993</td>
<td>61408</td>
<td>38722.232</td>
<td>detail</td>
</tr>
<tr>
<td>164.128.32.11</td>
<td>179</td>
<td>3303</td>
<td></td>
<td></td>
<td>1017777</td>
<td>0</td>
<td>142963</td>
<td>34371</td>
<td>21995.69</td>
<td>detail</td>
</tr>
<tr>
<td>64.71.255.61</td>
<td>179</td>
<td>812</td>
<td></td>
<td></td>
<td>2206875</td>
<td>0</td>
<td>352846</td>
<td>59641</td>
<td>35861.44</td>
<td>detail</td>
</tr>
<tr>
<td>192.43.217.141</td>
<td>179</td>
<td>1404</td>
<td></td>
<td></td>
<td>1045431</td>
<td>0</td>
<td>361378</td>
<td>60958</td>
<td>31936.445</td>
<td>detail</td>
</tr>
<tr>
<td>195.209.15.251</td>
<td>179</td>
<td>5568</td>
<td></td>
<td></td>
<td>7389</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3520.056</td>
<td>detail</td>
</tr>
</tbody>
</table>

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

2. MRT

<table>
<thead>
<tr>
<th>IP</th>
<th>PORT</th>
<th>AS</th>
<th>Status</th>
<th>Uptime</th>
<th>#MsgRecvd</th>
<th>#Reset</th>
<th>#Prefix</th>
<th>#Attribute</th>
<th>Memory(k)</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>202.167.228.20</td>
<td>179</td>
<td>4739</td>
<td></td>
<td></td>
<td>320591</td>
<td>0</td>
<td>369837</td>
<td>61390</td>
<td>28226.993</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::4826:1</td>
<td>179</td>
<td>4826</td>
<td></td>
<td></td>
<td>28221</td>
<td>0</td>
<td>751</td>
<td>512</td>
<td>3713.062</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::7575:1</td>
<td>179</td>
<td>7575</td>
<td></td>
<td></td>
<td>39677</td>
<td>0</td>
<td>1440</td>
<td>1091</td>
<td>3869.29</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::228.44</td>
<td>179</td>
<td>10026</td>
<td></td>
<td></td>
<td>623298</td>
<td>0</td>
<td>205860</td>
<td>35719</td>
<td>24079.732</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::228.37</td>
<td>179</td>
<td>38809</td>
<td></td>
<td></td>
<td>141477</td>
<td>0</td>
<td>31655</td>
<td>6954</td>
<td>7089.423</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::228.46</td>
<td>179</td>
<td>7575</td>
<td></td>
<td></td>
<td>103587</td>
<td>0</td>
<td>21318</td>
<td>4559</td>
<td>5645.269</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::228.74</td>
<td>179</td>
<td>4826</td>
<td></td>
<td></td>
<td>427622</td>
<td>0</td>
<td>313844</td>
<td>53951</td>
<td>26170.469</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::379:1</td>
<td>179</td>
<td>4739</td>
<td></td>
<td></td>
<td>51501</td>
<td>0</td>
<td>7021</td>
<td>4971</td>
<td>4690.063</td>
<td>detail</td>
</tr>
<tr>
<td>2001:de8:6::1:26:1</td>
<td>179</td>
<td>10026</td>
<td></td>
<td></td>
<td>23366</td>
<td>0</td>
<td>1216</td>
<td>877</td>
<td>3782.287</td>
<td>detail</td>
</tr>
<tr>
<td>2001:468:ff02::1</td>
<td>179</td>
<td>11537</td>
<td></td>
<td></td>
<td>144813</td>
<td>0</td>
<td>842</td>
<td>611</td>
<td>4141.752</td>
<td>detail</td>
</tr>
<tr>
<td>2001:218:0:1000:8006</td>
<td>179</td>
<td>2914</td>
<td></td>
<td></td>
<td>25173</td>
<td>0</td>
<td>1018</td>
<td>800</td>
<td>3781.243</td>
<td>detail</td>
</tr>
<tr>
<td>2001:2000:3018:4d::1</td>
<td>179</td>
<td>1299</td>
<td></td>
<td></td>
<td>14004</td>
<td>0</td>
<td>660</td>
<td>530</td>
<td>3667.723</td>
<td>detail</td>
</tr>
<tr>
<td>2001:388:1:16</td>
<td>179</td>
<td>7575</td>
<td></td>
<td></td>
<td>127945</td>
<td>0</td>
<td>6931</td>
<td>5047</td>
<td>5134.589</td>
<td>detail</td>
</tr>
<tr>
<td>2001:388:1:13</td>
<td>179</td>
<td>7575</td>
<td></td>
<td></td>
<td>109416</td>
<td>0</td>
<td>3092</td>
<td>2322</td>
<td>4495.666</td>
<td>detail</td>
</tr>
<tr>
<td>2001:da8:ff:301:1</td>
<td>179</td>
<td>23910</td>
<td></td>
<td></td>
<td>33860</td>
<td>0</td>
<td>1464</td>
<td>1115</td>
<td>3892.493</td>
<td>detail</td>
</tr>
<tr>
<td>2402:7400:0:3c::1</td>
<td>179</td>
<td>38883</td>
<td></td>
<td></td>
<td>8108</td>
<td>0</td>
<td>951</td>
<td>699</td>
<td>3687.844</td>
<td>detail</td>
</tr>
<tr>
<td>2001:468:2::1</td>
<td>179</td>
<td>11537</td>
<td></td>
<td></td>
<td>32823</td>
<td>0</td>
<td>149</td>
<td>115</td>
<td>3670.71</td>
<td>detail</td>
</tr>
<tr>
<td>2001:12b4::1</td>
<td>179</td>
<td>28289</td>
<td></td>
<td></td>
<td>46737</td>
<td>0</td>
<td>985</td>
<td>718</td>
<td>3817.608</td>
<td>detail</td>
</tr>
<tr>
<td>2001:15a:4:a:2</td>
<td>179</td>
<td>29449</td>
<td></td>
<td></td>
<td>17023</td>
<td>0</td>
<td>606</td>
<td>564</td>
<td>3674.557</td>
<td>detail</td>
</tr>
<tr>
<td>2001:420:fffe:4</td>
<td>179</td>
<td>34288</td>
<td></td>
<td></td>
<td>20268</td>
<td>0</td>
<td>835</td>
<td>648</td>
<td>3701.757</td>
<td>detail</td>
</tr>
<tr>
<td>2607:fc58:0:80:1:4</td>
<td>179</td>
<td>20225</td>
<td></td>
<td></td>
<td>28878</td>
<td>0</td>
<td>850</td>
<td>660</td>
<td>3734.274</td>
<td>detail</td>
</tr>
<tr>
<td>202.167.228.81</td>
<td>179</td>
<td>24436</td>
<td></td>
<td></td>
<td>2352</td>
<td>0</td>
<td>410</td>
<td>104</td>
<td>3563.141</td>
<td>detail</td>
</tr>
<tr>
<td>202.167.228.107</td>
<td>179</td>
<td>2622</td>
<td></td>
<td></td>
<td>8158</td>
<td>0</td>
<td>931</td>
<td>218</td>
<td>2831.142</td>
<td>detail</td>
</tr>
</tbody>
</table>
Current Progress and Next Steps

• Released version 7.2.2
• Collectors at RouteViews – Last week
• Collectors at RIPE – trials??

• Next Steps
  – Version 7.2.3 – minor fixes, no externally visible changes
  – Link to data plane work
  – Monitoring Systems/Hermes
  – Clients/demand base services
  – Formatting standards
  – BGP Security Analysis
Questions