Combining Active Route Measurements with Passive BGP Data

Dan Massey
Maka'ala Networks/Colorado State

Joe Gersch
Secure64 SW Corp

Cathie Olshanowsky
Colorado State University

John Kemp
RouteViews/University of Oregon

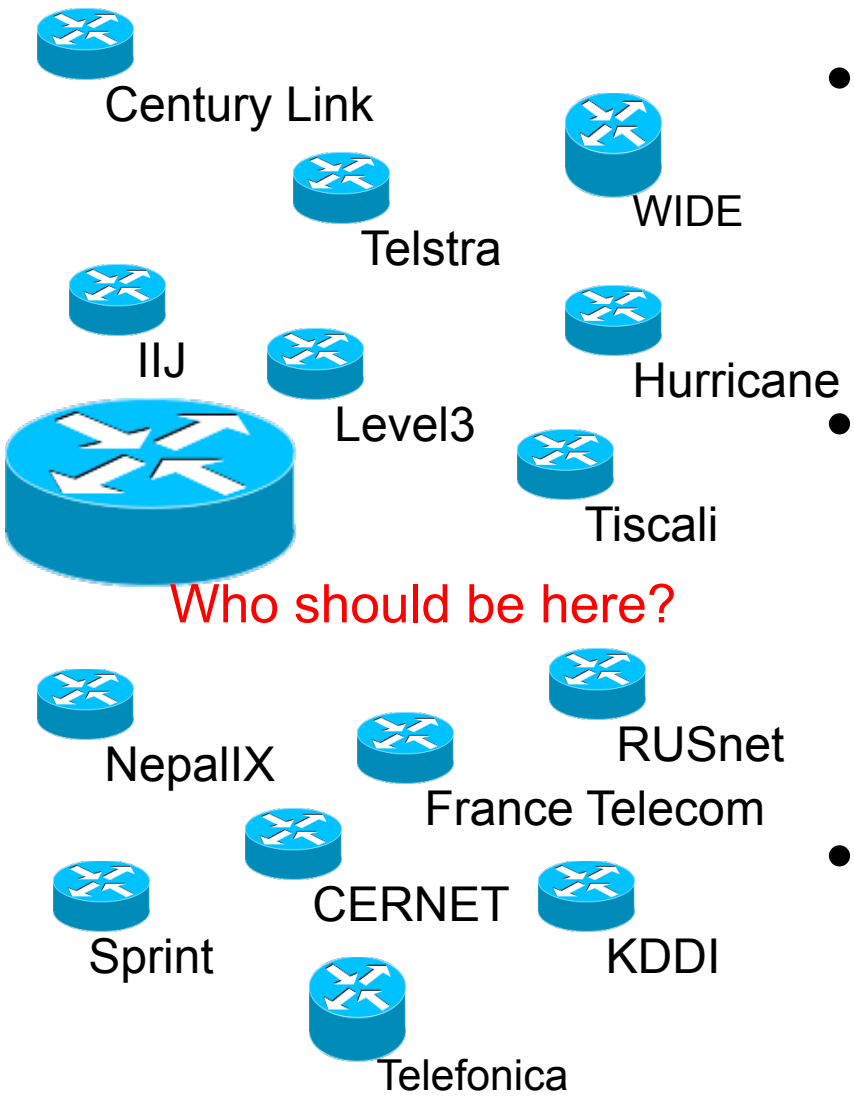
Broader BGP Monitoring Team

These organizations contribute the larger successful BGP monitoring effort, but positions in this tutorial are solely the opinion of Dr. Massey

BGP As Active Measurements?

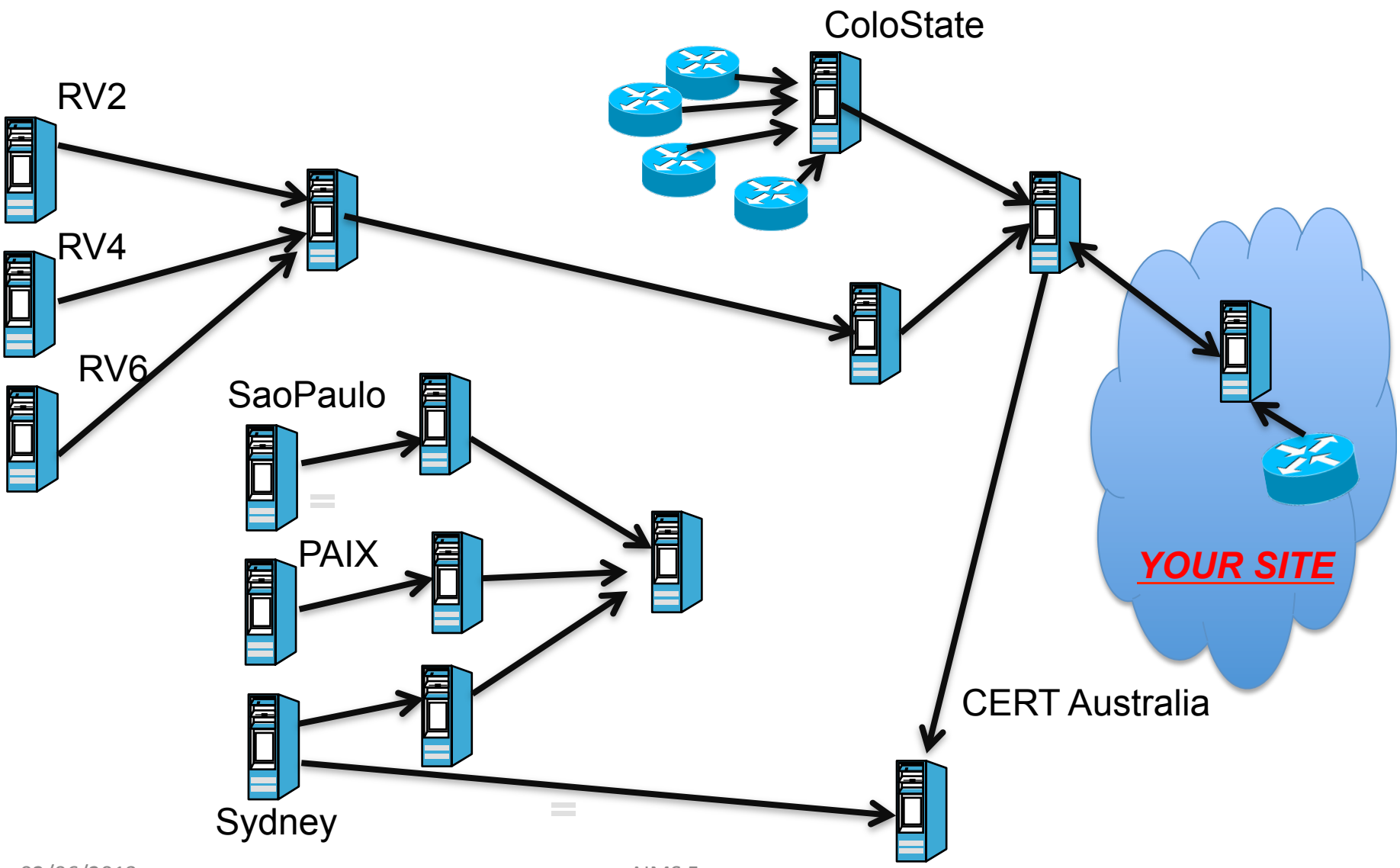
- Real-Time Data Can Enable Active Measurements
  - You can get BGP data in real-time!
  - More collectors in real-time feed
  - More collectors coming online
- Meta-Data, Formats, and Parsing
  - BGPdump, XML, and MRT formats
  - Perl Data Processing Tools

BGP Data Collection and Data Sharing



- ISPs around the world offer to provide BGP data
- Agree data can be made publically available to any operator or researcher
- Your organization should be here and/or how do you want here?

Real-Time Rollout (Feb 2013)



Providing Data: Your Configuration

```
neighbor 129.82.138.6 remote-as 12145
neighbor 129.82.138.6 ebgp-multihop

neighbor 129.82.138.6 description BGPmon
neighbor 129.82.138.6 password YOURPASSWORD

neighbor 129.82.138.6 maximum-prefix  1
neighbor 129.82.138.6 distribute-list bgpmon-dist-in in
neighbor 129.82.138.6 distribute-list bgpmon-dist-out out
neighbor 129.82.138.6 filter-list bgpmon-filter-in in
neighbor 129.82.138.6 filter-list bgpmon-filter-out out

neighbor 129.82.138.6 no shutdown
```

Recommend:
Send all routes,
Accept no routes

Red Items Are Required

Password, description, and filters optional, *but recommended*

University of Oregon Route Views Archive Project
David Meyer

- Please see www.routeviews.org for a description of the route views project, bibliography, and additional information.
- For asn.routeviews.org zone files click here or ftp from: ftp.routeviews.org/dnszones/
- Data Archives
  - MRT format RIBs and UPDATEs (zebra bgpd, from route-views2.oregon-ix.net)
    MRT format RIBs and UPDATEs from Equinix Ashburn (zebra bgpd, from route-views.eqix.routeviews.org)
    MRT format RIBs and UPDATEs from ISC (PAIX) (zebra bgpd, from route-views.isc.routeviews.org)
    MRT format RIBs and UPDATEs from KIXP (zebra bgpd, from route-views.kixp.routeviews.org)
    MRT format RIBs and UPDATEs from JINX (zebra bgpd, from route-views.jinx.routeviews.org)
    MRT format RIBs and UPDATEs from LINX (zebra bgpd, from route-views.linx.routeviews.org)
    MRT format RIBs and UPDATEs from TELXATL (zebra bgpd, from route-views.telxatl.routeviews.org)
    MRT format RIBs and UPDATEs from DIXIE (WIDE) (zebra bgpd, from route-views.wide.routeviews.org)
    v6 MRT format RIBs and UPDATEs (zebra bgpd, from route-views6.oregon-ix.net)
    MRT format RIBs and UPDATEs (quagga bgpd, from route-views4.routeviews.org)
    MRT format RIBs and UPDATEs from SYDNEY (quagga bgpd, from route-views.sydney.routeviews.org)
    MRT format RIBs and UPDATEs from SAOPAULO (quagga bgpd, from route-views.saopaulo.routeviews.org)
    ipv6 data split out from the above files (multiple collectors)

Wednesday, January 09, 2013 TEXT_SIZE

BGPmon
Next generation BGP Monitor

Search...

Home | About | Download | Live data | Archives | Join the peering | Documentation | Community | Contact us

BGPmon Archiving

The BGPmon archiving project has two aims.

1. Archive the live BGPmon stream.
2. Archive historical RouteViews data.

The archiving project archives both the live stream and the RouteViews data in XML format as well as a format similar to that produced by the bgpdump program.

To archive the live BGPmon stream, the archiver connects to the live BGP updates stream at livebgp.netsec.colostate.edu and archives the raw XML stream. Messages for each collector feeding into the live BGP stream are archived separately.

Archiving the historical RouteViews data is done similarly. The MRT format files from RouteViews are fed to a BGPmon instance to convert them to a XML stream and then are archived similarly to the live BGP stream.

Data Organization

The archive data is available organized by date or by peer. BGPmon status messages, archiver logs and archiver status messages are also available.

LATEST NEWS

- BGPmon 7.2.3 Released
- BGPmon 7.2.2 Released
- BGPmon: Using Real-Time Data i Research and Operations
- Technical documentaion is updat
- BGPmon 7.2.1 Released

Index of /date/2013.01/09/UPDATES/

Name	Last Modified	Size	Type
Parent Directory/		-	Directory
status.20130109.0000.xml	2013-Jan-08 17:40:33	155.8K	application/xml
status.20130109.0015.xml	2013-Jan-08 18:00:33	100.1K	application/xml
status.20130109.0030.xml	2013-Jan-08 18:10:33	62.3K	application/xml
status.20130109.0045.xml	2013-Jan-08 18:20:33	129.2K	application/xml
status.20130109.0100.xml	2013-Jan-08 18:30:33	29.8K	application/xml

updates.20130109.0000.129.82.2.2.bgpdump-001	2013-Jan-08 17:40:33	337.2K	text/plain
updates.20130109.0000.129.82.2.2.xml	2013-Jan-08 17:40:33	3.0M	application/xml
updates.20130109.0000.164.128.32.11.bgpdump-001	2013-Jan-08 17:40:33	31.8K	text/plain
updates.20130109.0000.164.128.32.11.xml	2013-Jan-08 17:40:33	292.5K	application/xml
updates.20130109.0000.187.16.216.104.bgpdump-001	2013-Jan-08 17:25:09	0.2K	text/plain
updates.20130109.0000.187.16.216.104.xml	2013-Jan-08 17:25:09	2.3K	application/xml
updates.20130109.0000.187.16.216.20.bgpdump-001	2013-Jan-08 17:50:24	0.7K	text/plain

```
ARCHIVER|1357690229|OPENED|CREATE_NEW_FILE
BGP4MP|1357689610|A|164.128.32.11|3303|41.57.82.0/24|3303 6774 37410
BGP4MP|1357689610|W|164.128.32.11|3303|41.57.85.0/24
BGP4MP|1357689610|A|164.128.32.11|3303|163.162.0.0/16|3303 6762 5609
BGP4MP|1357689641|A|164.128.32.11|3303|205.68.192.0/20|3303 209 721 27066 1733 5237
BGP4MP|1357689641|A|164.128.32.11|3303|205.70.0.0/19|3303 209 721 27066 1733 5237
BGP4MP|1357689641|A|164.128.32.11|3303|205.90.0.0/20|3303 209 721 27066 1733 5237
BGP4MP|1357689641|A|164.128.32.11|3303|205.91.160.0/20|3303 209 721 27066 1733 5237
BGP4MP|1357689641|A|164.128.32.11|3303|194.42.148.0/24|3303 174 8544 16229
BGP4MP|1357689641|A|164.128.32.11|3303|41.37.192.0/18|3303 3320 3257 8452
BGP4MP|1357689641|A|164.128.32.11|3303|41.129.128.0/17|3303 3320 3257 8452 24863
BGP4MP|1357689641|W|164.128.32.11|3303|41.223.20.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|62.68.224.0/20
BGP4MP|1357689641|W|164.128.32.11|3303|62.68.240.0/20
BGP4MP|1357689641|W|164.128.32.11|3303|62.240.112.0/20
BGP4MP|1357689641|W|164.128.32.11|3303|196.221.0.0/20
BGP4MP|1357689641|W|164.128.32.11|3303|197.162.0.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|197.162.112.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|197.162.116.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|197.163.52.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|197.163.64.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|197.166.0.0/22
BGP4MP|1357689641|W|164.128.32.11|3303|206.39.148.0/22
BGP4MP|1357689641|A|164.128.32.11|3303|41.232.0.0/16|3303 3320 3257 8452
BGP4MP|1357689641|A|164.128.32.11|3303|82.129.128.0/18|3303 3320 3257 8452 24835 24835
BGP4MP|1357689641|A|164.128.32.11|3303|82.129.192.0/18|3303 3320 3257 8452 24835 24835
```

```
<xml>
<ARCHIVER><TIME timestamp="1357690229" datetime="2013-01-09T00:10:29Z"/><EVENT
cause="CREATE_NEW_FILE">OPENED</EVENT></ARCHIVER>

<BGP_MESSAGE length="00002095" version="0.4" xmlns="urn:ietf:params:xml:ns:xfb-0.4" type_value="2"
type="UPDATE"><BGPMON_SEQ id="2128112124" seq_num="1745871819"/><TIME timestamp="1357689610"
datetime="2013-01-09T00:00:10Z" precision_time="54"/><PEERING
as_num_len="2"><SRC_ADDR><ADDRESS>164.128.32.11</ADDRESS><AFI value="1">IPV4</AFI></
SRC_ADDR><SRC_PORT>179</SRC_PORT><SRC_AS>3303</SRC_AS><DST_ADDR><ADDRESS>129.82.138.6</
ADDRESS><AFI value="1">IPV4</AFI></DST_ADDR><DST_PORT>4321</DST_PORT><DST_AS>6447</
DST_AS><BGPID>0.0.0.0</BGPID></PEERING><ASCII_MSG length="77"><MARKER
length="16">FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF</MARKER><UPDATE withdrawn_len="0"
path_attr_len="50"><WITHDRAWN count="0"/><PATH_ATTRIBUTES count="5"><ATTRIBUTE length="1"><FLAGS
transitive="TRUE"/><TYPE value="1">ORIGIN</TYPE><ORIGIN value="0">IGP</ORIGIN></ATTRIBUTE><ATTRIBUTE
length="8"><FLAGS transitive="TRUE"/><TYPE value="2">AS_PATH</TYPE><AS_PATH><AS_SEG
type="AS_SEQUENCE" length="3"><AS>3303</AS><AS>6774</AS><AS>37410</AS></AS_SEG></AS_PATH></
ATTRIBUTE><ATTRIBUTE length="6"><FLAGS optional="TRUE" transitive="TRUE"/><TYPE
value="7">AGGREGATOR</TYPE><AGGREGATOR><AS>37410</AS><ADDR>4.164.128.32</ADDR></
AGGREGATOR></ATTRIBUTE><ATTRIBUTE length="4"><FLAGS transitive="TRUE"/><TYPE value="3">NEXT_HOP</
TYPE><NEXT_HOP>164.128.32.11</NEXT_HOP></ATTRIBUTE><ATTRIBUTE length="16"><FLAGS optional="TRUE"
transitive="TRUE"/><TYPE value="8">COMMUNITIES</TYPE><COMMUNITIES><COMMUNITY><AS>3303</
AS><VALUE>1004</VALUE></COMMUNITY><COMMUNITY><AS>3303</AS><VALUE>1006</VALUE></
COMMUNITY><COMMUNITY><AS>3303</AS><VALUE>3052</VALUE></COMMUNITY><COMMUNITY><AS>3303</
AS><VALUE>6774</VALUE></COMMUNITY></COMMUNITIES></ATTRIBUTE></PATH_ATTRIBUTES><NLRI
count="1"><PREFIX label="NANN"><ADDRESS>41.57.82.0/24</ADDRESS><AFI value="1">IPV4</AFI><SAFI
value="1">UNICAST</SAFI></PREFIX></NLRI></UPDATE></ASCII_MSG><OCTET_MSG><OCTETS
length="77">FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF004D02000000324001010040020802030CE71A769222C00706
92220A620B01400304A480200BC008100CE703EC0CE703EE0CE70BEC0CE71A7618293952</OCTETS></
OCTET_MSG></BGP_MESSAGE>
```

```
Dans-MacBook-Air:~ massey$ telnet livebgp.netsec.colostate.edu 50001
Trying 129.82.138.26...
Connected to lisa.netsec.colostate.edu.
Escape character is '^]'.
<xml><BGP_MESSAGE length="00001964" version="0.4" xmlns="urn:ietf:params:xml:ns:xfb-0.4" type_value="2"
type="UPDATE"><BGPMON_SEQ id="127893688" seq_num="173356373"/><TIME timestamp="1357762305"
datetime="2013-01-09T20:11:45Z" precision_time="0"/><PEERING
as_num_len="4"><SRC_ADDR><ADDRESS>187.16.216.104</ADDRESS><AFI value="1">IPV4</AFI></
SRC_ADDR><SRC_PORT>179</SRC_PORT><SRC_AS>28289</SRC_AS><DST_ADDR><ADDRESS>200.160.6.217</
ADDRESS><AFI value="1">IPV4</AFI></DST_ADDR><DST_PORT>179</DST_PORT><DST_AS>6447</
DST_AS><BGPID>0.0.0.0</BGPID></PEERING><ASCII_MSG length="80"><MARKER
length="16">FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF</MARKER><UPDATE withdrawn_len="0"
path_attr_len="54"><WITHDRAWN count="0"/><PATH_ATTRIBUTES count="5"><ATTRIBUTE length="1"><FLAGS
transitive="TRUE"/><TYPE value="1">ORIGIN</TYPE><ORIGIN value="0">IGP</ORIGIN></ATTRIBUTE><ATTRIBUTE
length="22"><FLAGS transitive="TRUE"/><TYPE value="2">AS_PATH</TYPE><AS_PATH><AS_SEG
type="AS_SEQUENCE" length="5"><AS>28289</AS><AS>53131</AS><AS>16735</AS><AS>3549</AS><AS>27717</
AS></AS_SEG></AS_PATH></ATTRIBUTE><ATTRIBUTE length="4"><FLAGS transitive="TRUE"/><TYPE
value="3">NEXT_HOP</TYPE><NEXT_HOP>187.16.216.104</NEXT_HOP></ATTRIBUTE><ATTRIBUTE
length="8"><FLAGS optional="TRUE" transitive="TRUE"/><TYPE value="7">AGGREGATOR</
TYPE><AGGREGATOR><AS>0</AS><ADDR>192.8.4.110</ADDR></AGGREGATOR></ATTRIBUTE><ATTRIBUTE
length="4"><FLAGS optional="TRUE" transitive="TRUE"/><TYPE value="8">COMMUNITIES</
TYPE><COMMUNITIES><COMMUNITY><AS>28289</AS><VALUE>65500</VALUE></COMMUNITY></
COMMUNITIES></ATTRIBUTE></PATH_ATTRIBUTES><NLRI count="1"><PREFIX
label="DPATH"><ADDRESS>186.167.0.0/16</ADDRESS><AFI value="1">IPV4</AFI><SAFI value="1">UNICAST</
SAFI></PREFIX></NLRI></UPDATE></ASCII_MSG><OCTET_MSG><OCTETS
length="80">FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF005002000000364001010040021602050000 6E810000CF8B00004
15F00000DDD00006C45400304BB10D868C0070800006C45BE79ED04C008046E81FFDC10BAA7</OCTETS></
OCTET_MSG></BGP_MESSAGE>
```

Module Version: 1.062 Source

NAME
SYNOPSIS
EXPORT
SUBROUTINES/METHODS
init_bgpdata
connect_bgpdata
read_xml_message
close_connection

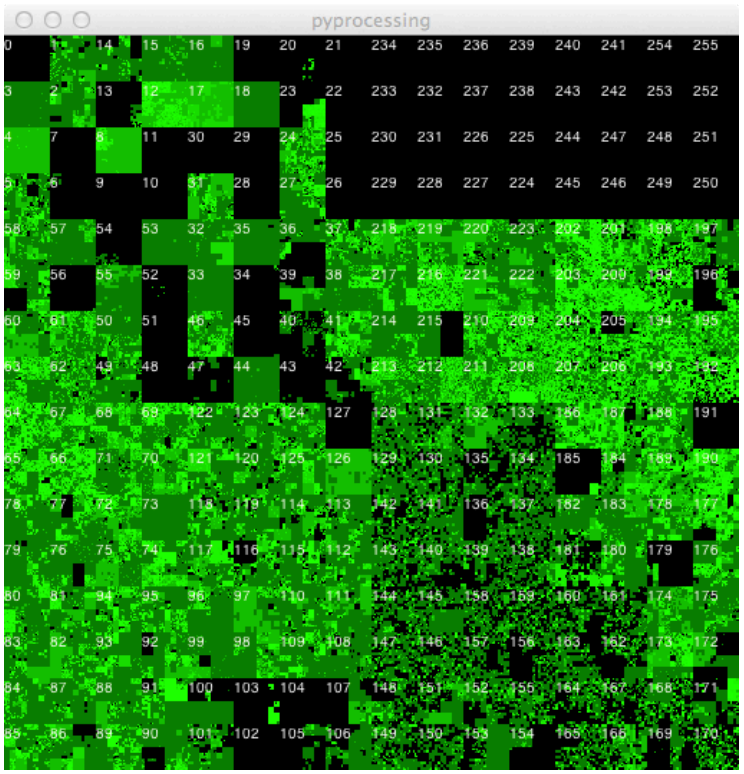
Download:
BGPmon-core-1-062.tar.gz

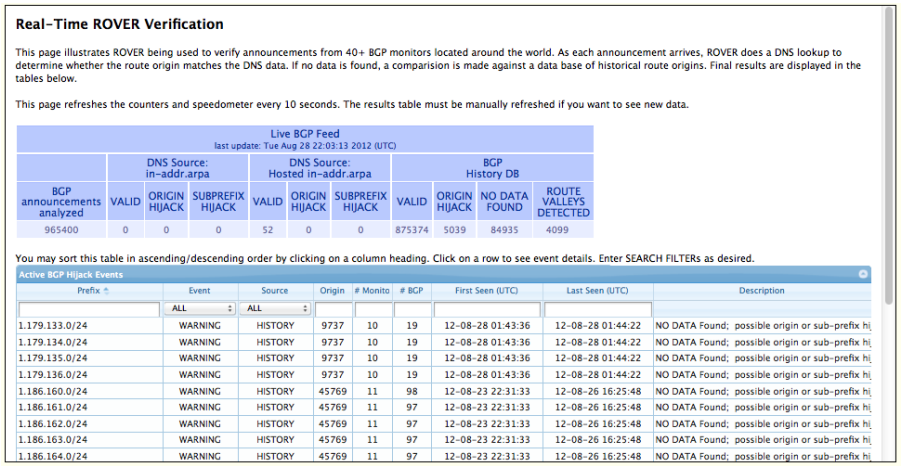
Dependencies

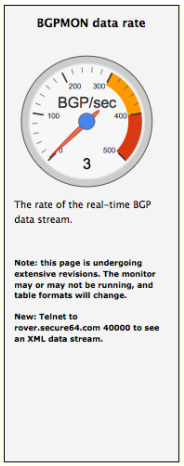
```
use BGPmon::Fetch;
my $ret = init_bgpdata();
my $ret = connect_bgpdata();
my $xml_msg = read_xml_message();
if ( !defined($xml_msg) ){
    print get_error_code() . ": " . get_error_msg();
}
my $ret = is_connected();
my $num_read = messages_read();
my $uptime = uptime();
my $ret = close_connection();
my $downtime = connection_endtime();
```

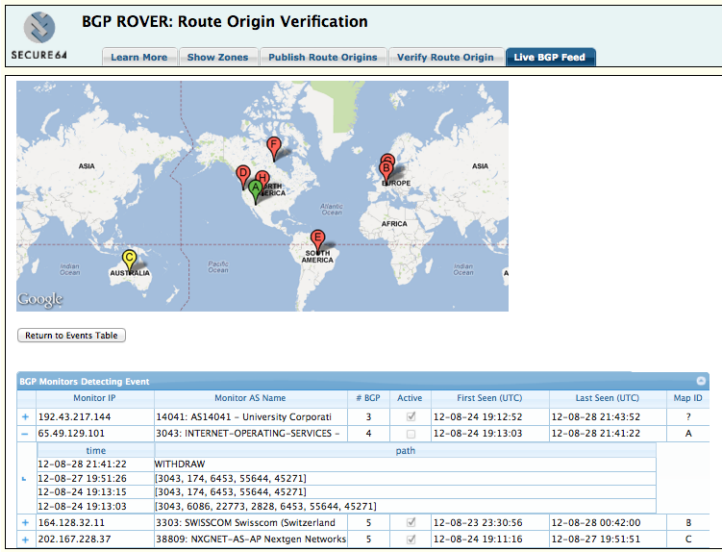
EXPORT

Data Visualization and ROVER
http://rover.secure64.com

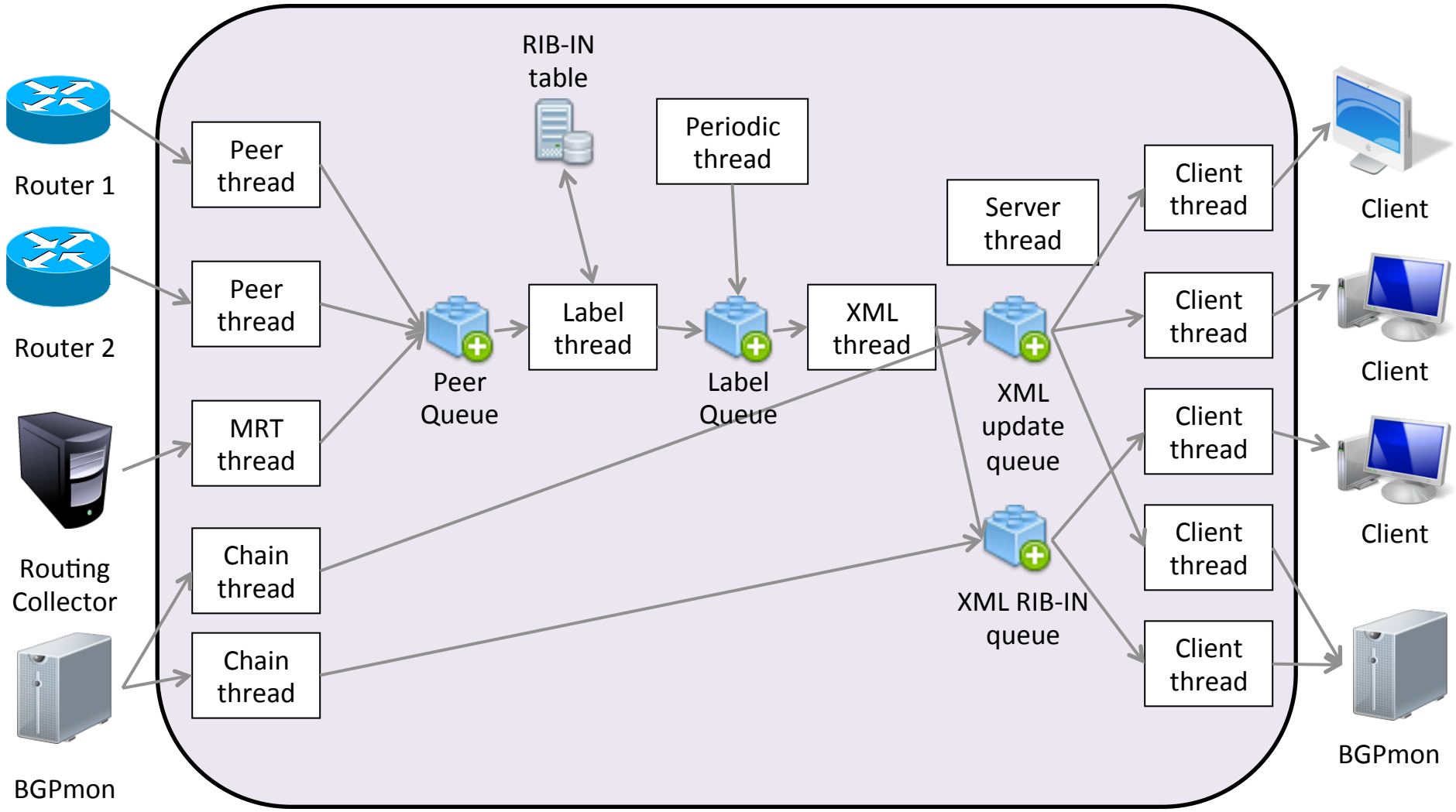








Questions

Additional Information

BGPmon Architecture