Routing Data in the Public Domain

PTT Fórum 6

John Kemp kemp@routeviews.org

Routing Data in the Public Domain

- What is it?
- What kinds of tools are available?
- What are some simple uses?
- What are some advanced uses?
- Opportunities for Research

RouteViews

- A **Collaborative** Router Looking Glass to share BGP Views among Network Operators
- Started in 1995 at the University of Oregon, Advanced Network Technology Center (ANTC)
- Data Archives begin in 1997, 7TB Today
- 16 Collectors, 170 IPv4 Peers, IP75 V6 Peers

- Primary Investigator: David Meyer, University of Oregon / Brocade
- Co-PI: Dan Massey, Colorado State University
- Co-PI: Lixia Zhang, University of California, Los Angeles
- Research Funded by the National Science Foundation, USA
- Areas of Research: Routing Dynamics, Internet Growth, Prefix Hi-jack Alert, and other BGP Issues

Routing Data: What is it?

- BGP Data, and Registry Data
- Data available to anyone
- Unrestricted Terms of Use
- No guarantees on service or quality
- Data formats: MRT, XML, Text, Database…
- Tools assume some Level of Expertise

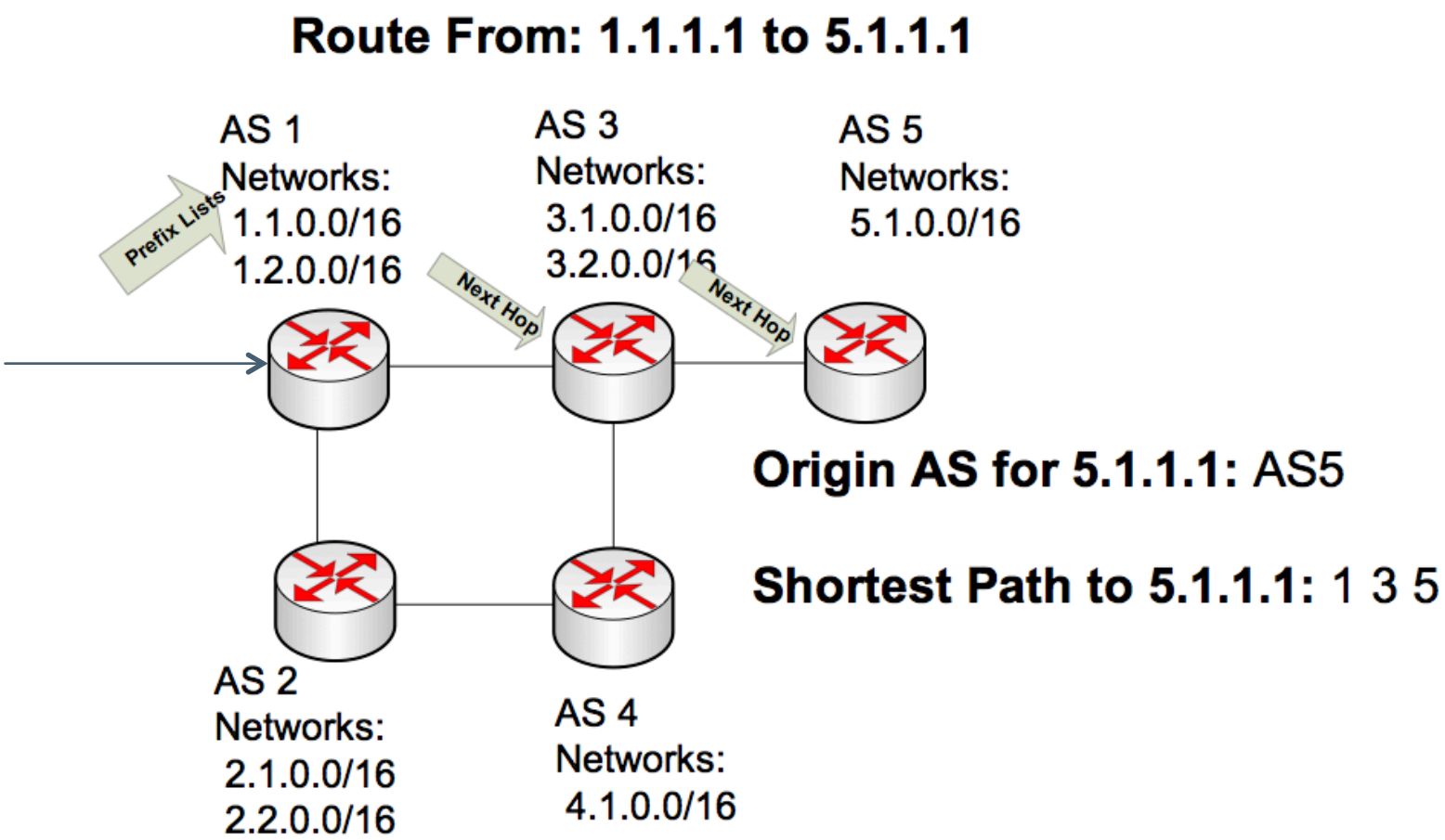
BGP Data

- Border Gateway Protocol
- BGP-4 RFC4271
- Path – Vector Protocol
- Prefix Lists, AS Paths, Next-Hop Router

- AS Numbers provide Path /Policy /and Summarization
- Updates and Withdrawals Announced to Neighbors
- Routes makes up the Router Information Base (RIB)
- Router selects the "Best Path" based on Attributes

  weight / local_pref / local / **SHORTEST AS_PATH** / igp egp incomplete / MED / multipath / age / router-id / neighbor address

BGP Terminology

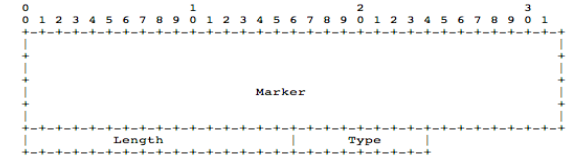


Data Formats: RFC, MRT, XFB

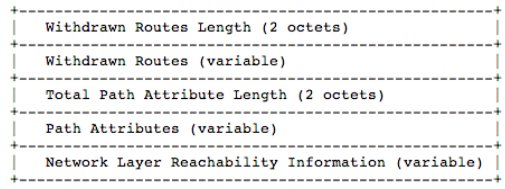
BGP-4 RFC4271
www.ietf.org/rfc/rfc4271.txt

4.1. Message Header Format

Each message has a fixed-size header. There may or may not be a data portion following the header, depending on the message type. The layout of these fields is shown below:



An UPDATE message is used to advertise feasible routes that share common path attributes to a peer, or to withdraw multiple unfeasibl routes from service (see 3.1). An UPDATE message MAY simultaneousl advertise a feasible route and withdraw multiple unfeasible routes from service. The UPDATE message always includes the fixed-size BG header, and also includes the other fields, as shown below (note, some of the shown fields may not be present in every UPDATE message



The mandatory category refers to an attribute that MUST be present both IBGP and EBGP exchanges if NLRI are contained in the UPDATE message. Attributes classified as optional for the purpose of the protocol extension mechanism may be purely discretionary, discretionary, required, or disallowed in certain contexts.

attribute	EBGP	IBGP
ORIGIN	mandatory	mandatory
AS_PATH	mandatory	mandatory
NEXT_HOP	mandatory	mandatory
MULTI_EXIT_DISC	discretionary	discretionary
LOCAL_PREF	see Section 5.1.5	required
ATOMIC_AGGREGATE	see Section 5.1.6 and 9.1.4	
AGGREGATOR	discretionary	discretionary

Multi-Threaded Router Toolkit:
tools.ietf.org//id/draft-ietf-grow-mrt-17.txt

2. MRT Common Header

All MRT format records have a Common Header which consists of a Timestamp, Type, Subtype, and Length field. The header is followed by a Message field. The MRT Common Header is illustrated below.

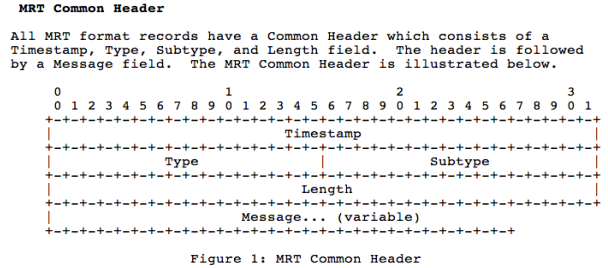


Figure 1: MRT Common Header

The format of the TABLE_DUMP Type is illustrated below.

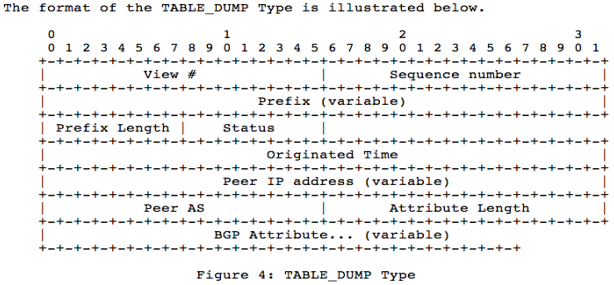


Figure 4: TABLE_DUMP Type

4.3.4. RIB Entries

The RIB Entries are repeated Entry Count times. These entries share a common format as shown below. They include a Peer Index from the PEER_INDEX_TABLE MRT record, an originated time for the RIB Entry, and the BGP path attribute length and attributes. All AS numbers in the AS_PATH attribute MUST be encoded as 4-Byte AS numbers.

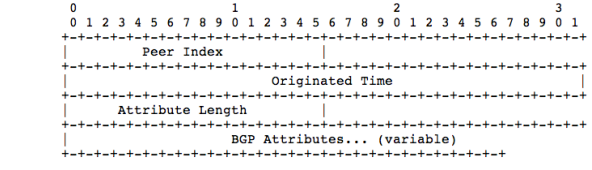


Figure 10: RIB Entries

XFB: XML Format for BGP
http://tools.ietf.org/id/draft-cheng-grow-bgp-xml-00.txt

```
<ASCII_MSG>
    <LENGTH>53</LENGTH>                          <-- BGP message total length
    <TYPE value="2">UPDATE</TYPE>                <-- BGP message type, according to RFC 4271
    <UPDATE>
        <ATTRIBUTE>
            <LENGTH>12</LENGTH>
            <TYPE value="2">AS_PATH</TYPE>
            <AS_PATH>
                <AS_SEG type="AS_SEQUENCE" length="5">
BGP AS Path data -->     <AS>14041</AS><AS>209</AS> <AS>3356</AS>
                         <AS>4230</AS><AS>28175</AS>
                </AS_SEG>
            </AS_PATH>
        </ATTRIBUTE>
        <ATTRIBUTE>
            <LENGTH>28</LENGTH>
            <TYPE value="14"> MP_REACH_NLRI</TYPE>
            <MP_REACH_NLRI>                      <-- Multi-protocol Support for v6
                .....
            <PREFIX label="DPATH" afi="IPV6" afi_value="2"
                safi="UNICAST" safi_value="1"> 2001:468:d01:33/96 </PREFIX>
        </ATTRIBUTE>                             <-- Announced Prefix
</UPDATE>
```

5.6.2. The UPDATE element

The following subelements are included in the UPDATE message: <withdrawn_routes_len>, <withdrawn_routes>, <path_len>, <path_attrib>, and <NLRI>.

Code	Type	Description
1	ORIGIN	This is a well-known mandatory attribute with value IGP, EGP, or INCOMPLETE.
2	AS_PATH	This is a well-known mandatory attribute with "type" attribute set to either as_set or as_sequence. It contains one or more AS subelements, each of which holds an Autonomous System number.
3	NEXT_HOP	This is a well-known mandatory attribute that holds the next hop address as its value.

Data Formats: Tools

- RIPE RIS libbgpdump (MRT -> ASCII)
  - https://bitbucket.org/ripencc/bgpdump/wiki/Home
  - http://www.ris.ripe.net/source/bgpdump/
- Zebra Dump Parser (MRT -> ASCII)
  - http://www.linux.it/~md/software/zebra-dump-parser.tgz
- UCLA Internet Research Lab BGP Parser (MRT -> XML)
  - http://irl.cs.ucla.edu/bgpparser/download.cgi?file=bgpparser-0.3b2.tgz
  - https://github.com/cawka/bgpparser

Simple Example

- Let's do a simple example to show some of the tools, and see how much we can find out about a particular site
- Let's take a look at www.uoregon.edu
- DNS Lookup returns: 128.223.142.125

Simple Example: IP2ASN, IP2Peer

6-hour Data from route-views2.routeviews.org

```
$ dig +short @asnums.routeviews.org -t TXT 223.128.aspath.routeviews.org.
"5413 1299 3356 3701 3582" "128.223.0.0" "16"

$ dig +short @asnums.routeviews.org -t TXT 223.128.asn.routeviews.org.
"3582" "128.223.0.0" "16"
```

Services of: http://www.team-cymru.org
Also: Darknets, Bogons, Malware

```
$ whois -h whois.cymru.com " -v 128.223.142.125"
AS      | IP               | BGP Prefix          | CC | Registry | Allocated  | AS Name
    3852| 128.223.142.125  | 128.223.0.0/16      | US | arin     | 1987-04-07 | UONET - University of
Oregon

$ dig +short  125.142.223.128.peer.asn.cymru.com TXT
"3701 4600 | 128.223.0.0/16 | US | arin | 1987-04-07"

$ dig +short AS3701.asn.cymru.com TXT
"3701 | US | arin | 1994-07-02 | NERONET - Oregon Joint Graduate Schools of Engineering"

$ dig +short AS4600.asn.cymru.com TXT
"4600 | US | arin | 1995-05-01 | UO-TRANSIT - Oregon GigaPOP"
```

Simple Example: route collector command-line route-views.saopaulo.routeviews.org

```
$ telnet route-views.saopaulo.routeviews.org
Connected to route-views.saopaulo.routeviews.org.
Escape character is '^]'.
Hello, this is Quagga (version 0.99.21).

route-views.saopaulo.routeviews.org> show ip bgp summary
BGP router identifier 187.16.216.223, local AS number 6447
RIB entries 819257, using 75 MiB of memory
Peers 29, using 129 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
187.16.216.20   4 28571 28274017  438471        0    0    0 01w2d18m   435579
187.16.216.24   4 16735 41656842  449811        0    0    0 2d10h19m   426530
187.16.216.56   4 14026  991581  224915         0    0    0 2d10h29m    17167

route-views.saopaulo.routeviews.org> show bgp summary
BGP router identifier 187.16.216.223, local AS number 6447
RIB entries 21352, using 2002 KiB of memory
Peers 29, using 129 KiB of memory

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:12f8::20   4 28571 16182259  438471        0    0    0 01w2d18h    11161
2001:12f8::24   4 16735 6304568  449806         0    0    0 22w2d04h    11077
```

Show all IPV4 peers

Show all IPV6 peers

route-views.saopaulo.routeviews.org

- Quagga BGP Route Collector located at PTTMetro
- Collaboration between NIC.br, PTT.br and RouteViews
- Started: March 17, 2011
- Open Peering Policy
- Full BGP Table from every Peer
- 25 IPV4 Peers, 7 IPV6 Peers

- Archived BGP Data Updates and RIB files in MRT Format : http://archive.routeviews.org/route-views.saopaulo
- Live BGP Data feeds into BGPMON and CYCLOPS: http://cyclops.cs.ucla.edu/ http://bgpmon.netsec.colostate.edu/

RouteViews Collectors

Simple Example: command-line

```
route-views.saopaulo.routeviews.org> show ip bgp 128.223.142.125

BGP routing table entry for 128.223.0.0/16
Paths: (9 available, best #9, table Default-IP-Routing-Table)
  Not advertised to any peer
  28303 18881 3549 3356 3701 3582
    187.16.217.30 from 187.16.217.30 (201.55.127.128)
      Origin IGP, localpref 100, valid, external
      Last update: Sun Nov 25 07:27:18 2012

  28289 53131 16735 1239 3356 3701 3582
    187.16.216.104 from 187.16.216.104 (189.36.224.1)
      Origin IGP, localpref 100, valid, external
      Community: 28289:65500
      Last update: Sun Nov 25 02:20:38 2012

  28571 1251 11537 4600 3582
    187.16.216.20 from 187.16.216.20 (143.107.255.15)
      Origin IGP, localpref 100, valid, external, best
      Last update: Wed Nov 21 04:52:28 2012
```

Simple Example: command line regexp

```
route-views.saopaulo.routeviews.org> show ip bgp regexp _3582$
BGP table version is 0, local router ID is 187.16.216.223
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  128.223.0.0      187.16.217.30                          0 28303 18881 3549 3356 3701 3582 i
*                   187.16.216.104                         0 28289 53131 16735 1239 3356 3701 3582 i
*                   187.16.217.154                         0 53175 8167 6453 3356 3701 3582 i
*                   187.16.216.24                          0 16735 1239 3356 3701 3582 i
*                   187.16.217.112                         0 53242 12956 3356 3701 3582 i
*                   187.16.217.129                         0 262354 262589 6762 3356 3701 3582 i
*                   187.16.216.219                         0 14840 18881 3549 3356 3701 3582 i
*                   189.40.251.107                         0 262757 26615 6762 3356 3701 3582 i
*>                  187.16.216.20                          0 28571 1251 11537 4600 3582 i
*  184.171.0.0/17   187.16.217.30                          0 28303 18881 3549 3356 3701 3582 i
*                   187.16.216.104                         0 28289 5313
*                   187.16.217.154                         0 5317
*                   187.16.216.24                          0 1
*                   187.16.217.112                         0
*                   187.16.217.129                         0 2
*                   187.16.216.219                         0 14
*                   189.40.251.107                         0 26275
*>                  187.16.216.20                          0 28571 1251 1153
*  207.98.72.0/21   187.16.217.30                          0 28303 18881 3549 3356 3701 3582 i
*                   187.16.216.104                         0 28289 53131 16735 1239 3356 3701 3582 i
*                   187.16.217.154                         0 53175 8167 6453 3356 3701 3582 i
*                   187.16.216.24                          0 16735 1239 3356 3701 3582 i
*                   187.16.217.112                         0 53242 12956 3356 3701 3582 i
*                   187.16.217.129                         0 262354 262589 6762 3356 3701 3582 i
*                   187.16.216.219                         0 14840 18881 3549 3356 3701 3582 i
*                   189.40.251.107                         0 262757 26615 6762 3356 3701 3582 i
*>                  187.16.216.20                          0 28571 1251 11537 4600 3582 i
```

Other examples:
show ip bgp regexp _4600_
show ip bgp regexp ^28571_
show bgp regexp _3582$

Simple Example: Visualization
Hurricane Electric BGP http://bgp.he.net/AS28571

HURRICANE ELECTRIC INTERNET SERVICES

Search

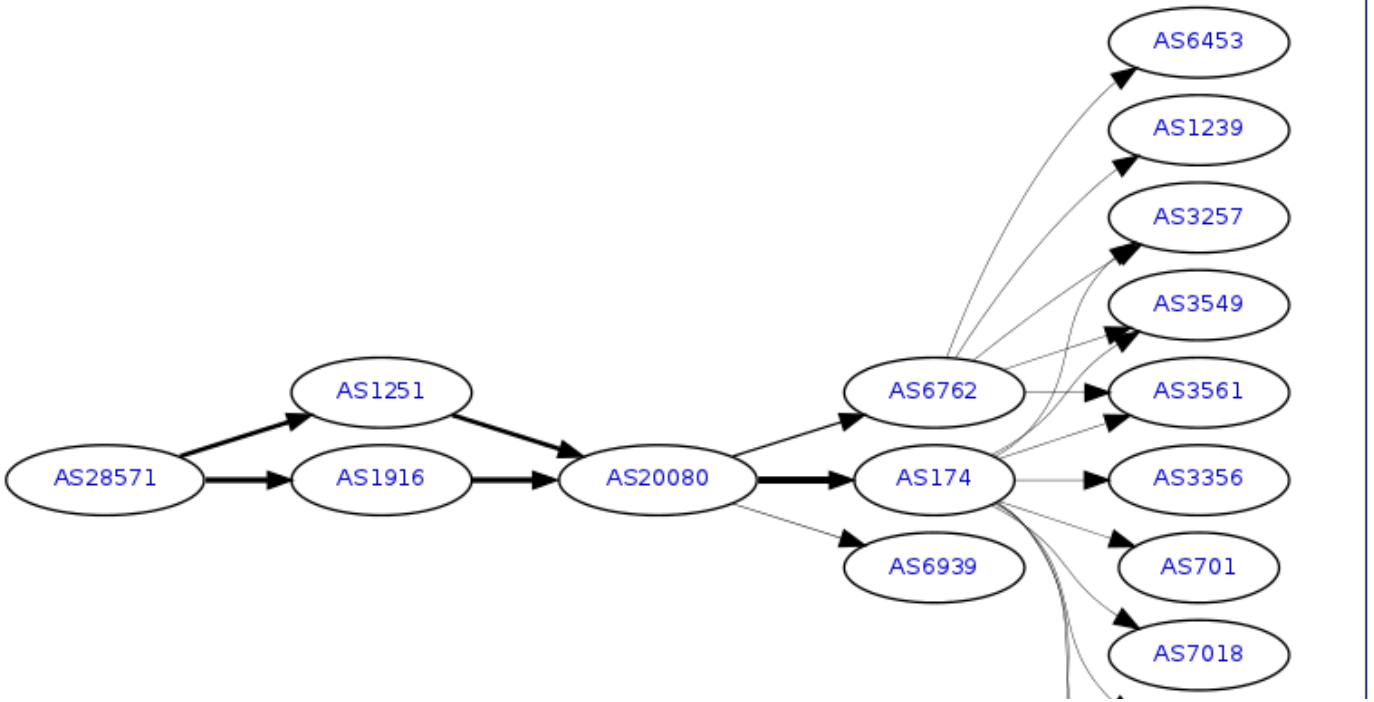
AS28571 UNIVERSIDADE DE SAO PAULO

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR

AS28571 IPv4 Route Propagation



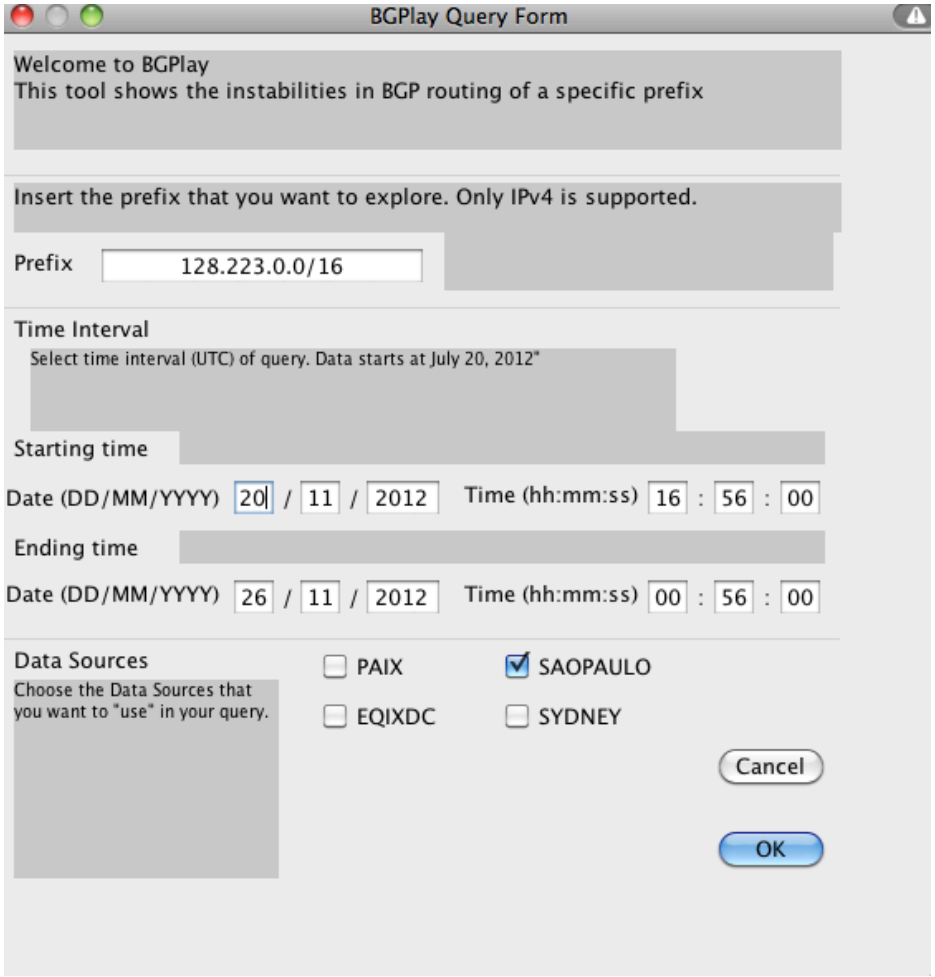
Simple Example: Visualization http://bgplay.routeviews.org

BGPlay developed by:
Lorenzo Collitti, Maurizio Pizzonia, et.al.
Roma Tre' Universita

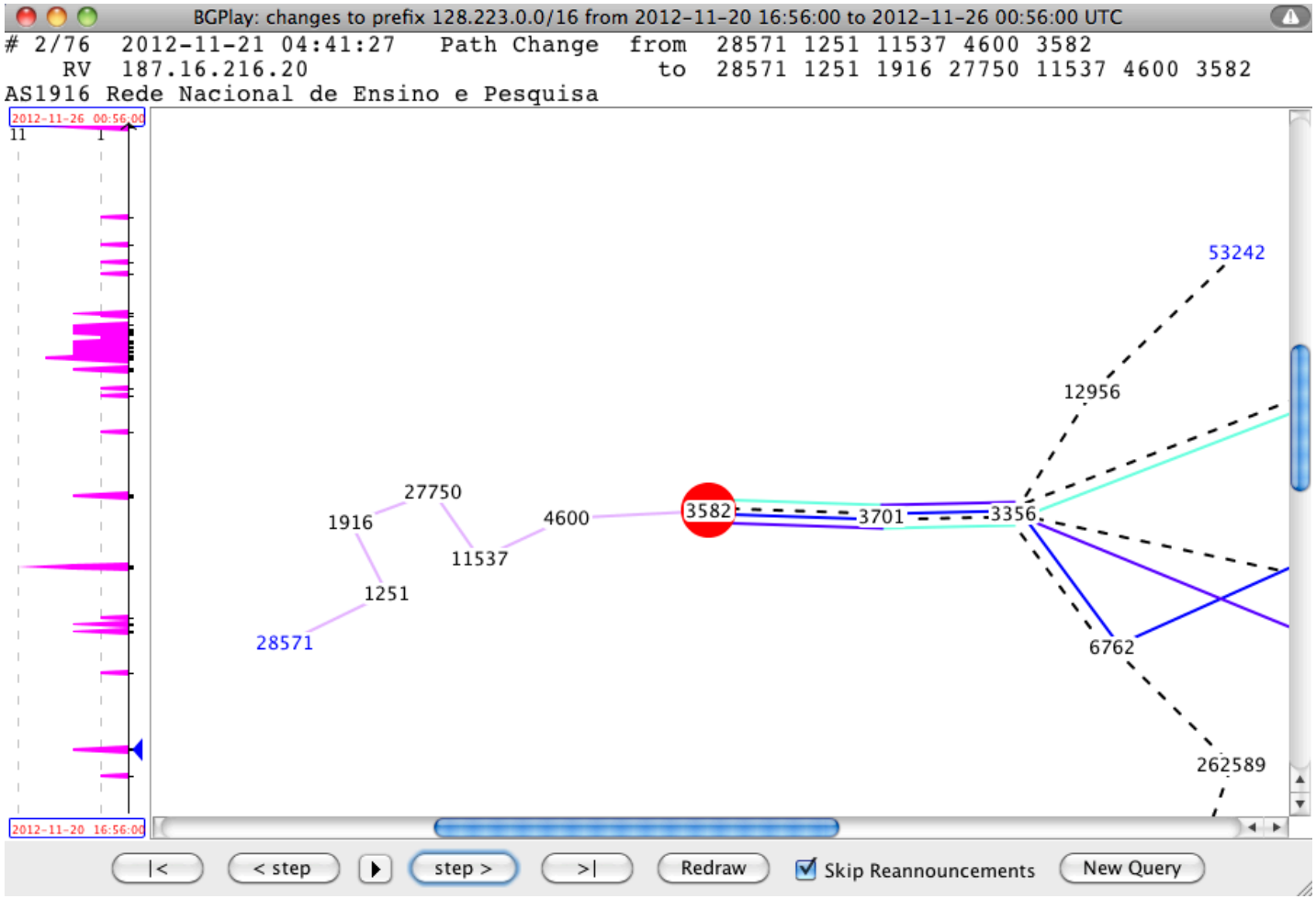
This instance hosted by RouteViews

http://www.dia.uniroma3.it/~compunet/www/view/tool.php?id=bgplay

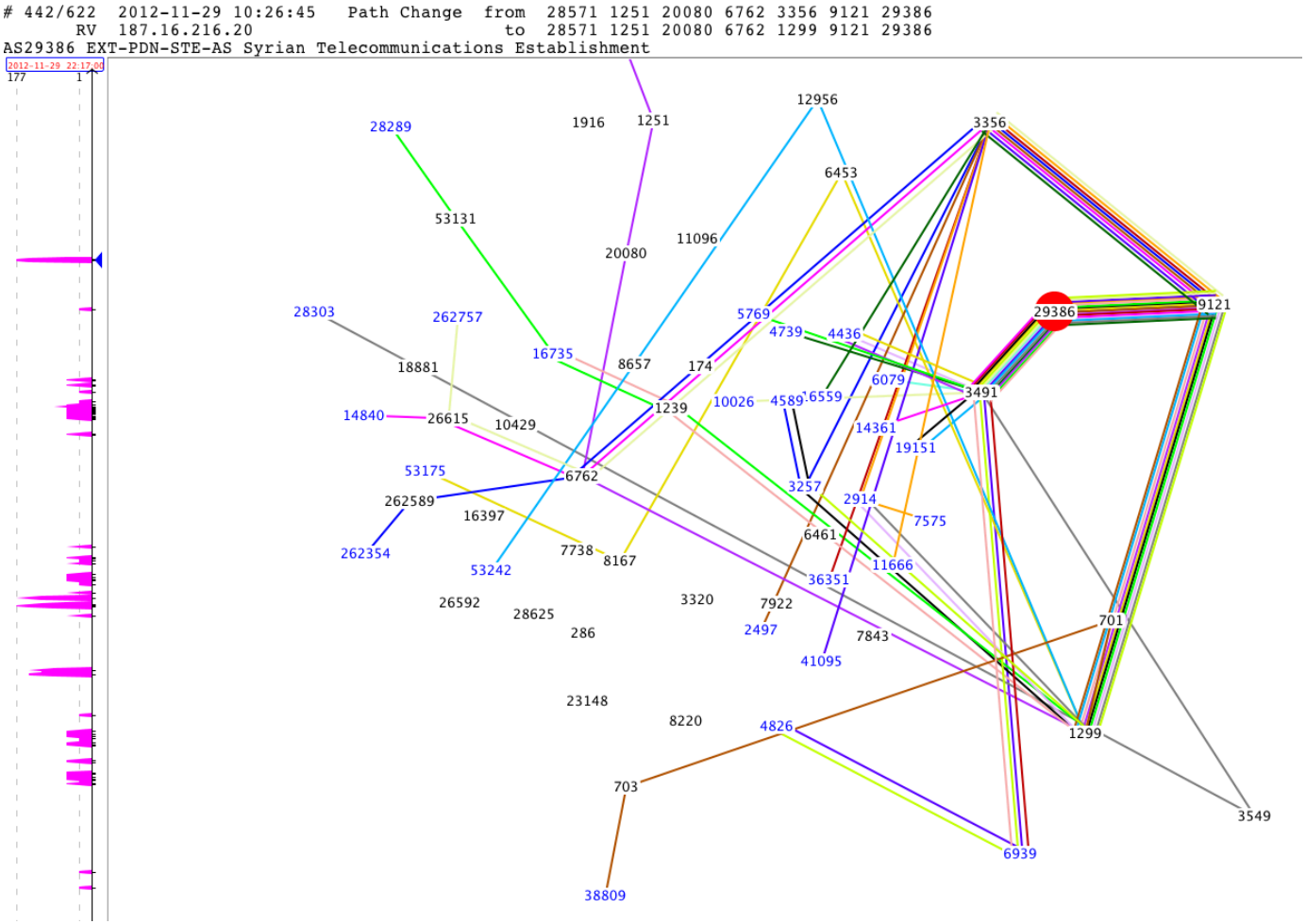
See also RIPE Historical BGPlay
http://sga.ripe.net/hbgplay



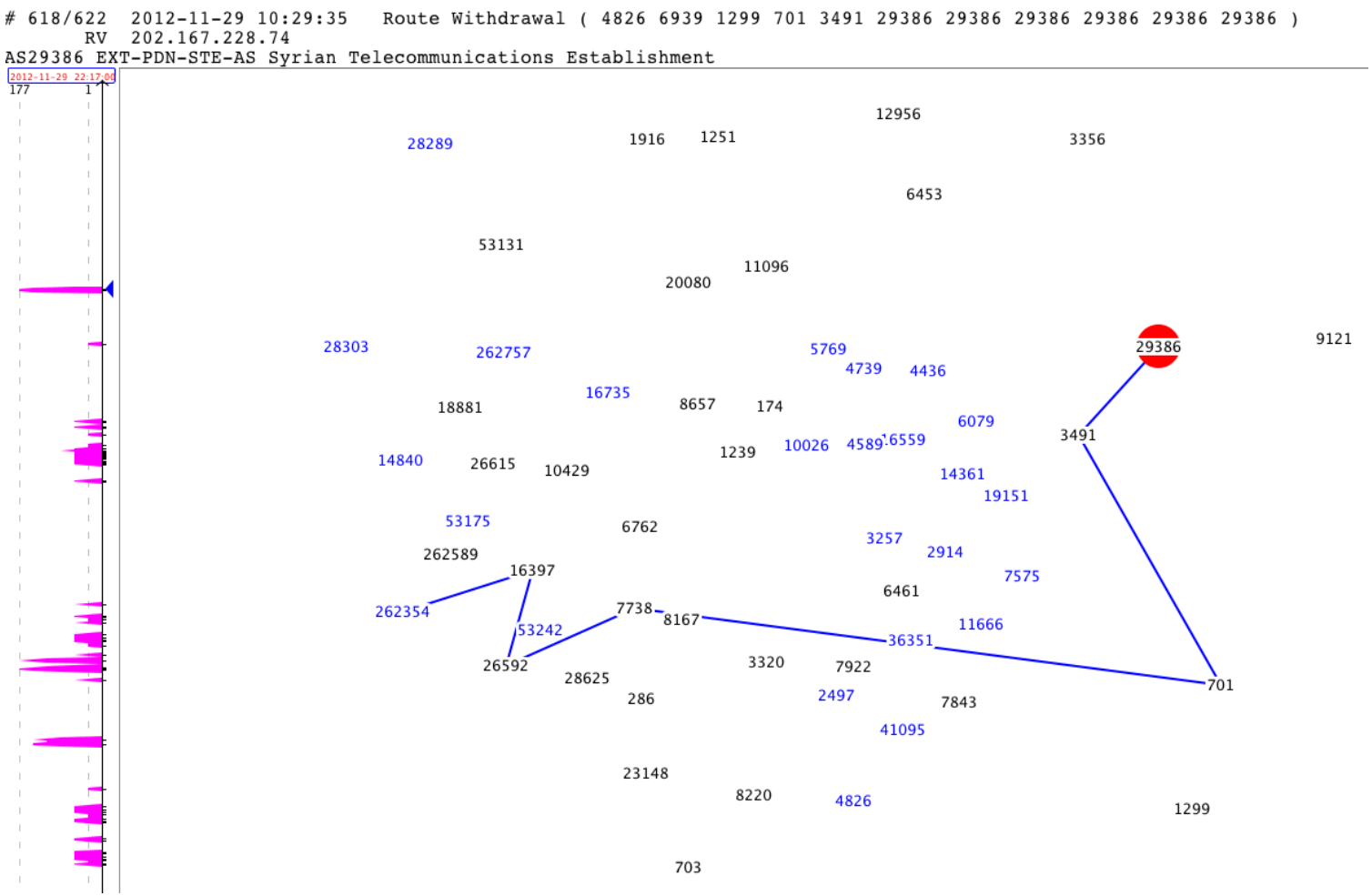
bgplay.routeviews.org



AS29386: 2012-11-29 10:26:45



AS29386: 2012-11-29 10:29:35



Simple Example: Summary

Given an IP Address, We can Easily Determine*:

- AS Number, and Registry Info
- Prefix Lists (Network Address Space)
- Best Path To the AS
- Routes Advertised by The AS
- Primary Peers of the AS
- We Can Visualize AS Paths
- We Can Visualize Path Changes

Routing Data: Advanced Uses

It would be nice if we could do more…

- Verify the Source (Origin Validation, RPKI)
- Verify the Complete Path (BGPsec)
- Notify on Prefix List - AS Origin Changes
- Notify on my AS Path Changes
- Notify on my AS Unusual Path Changes
- Apply Arbitrary Filters to Real-time Data
- Search Historical Routing Data Quickly/Easily

Cyclops

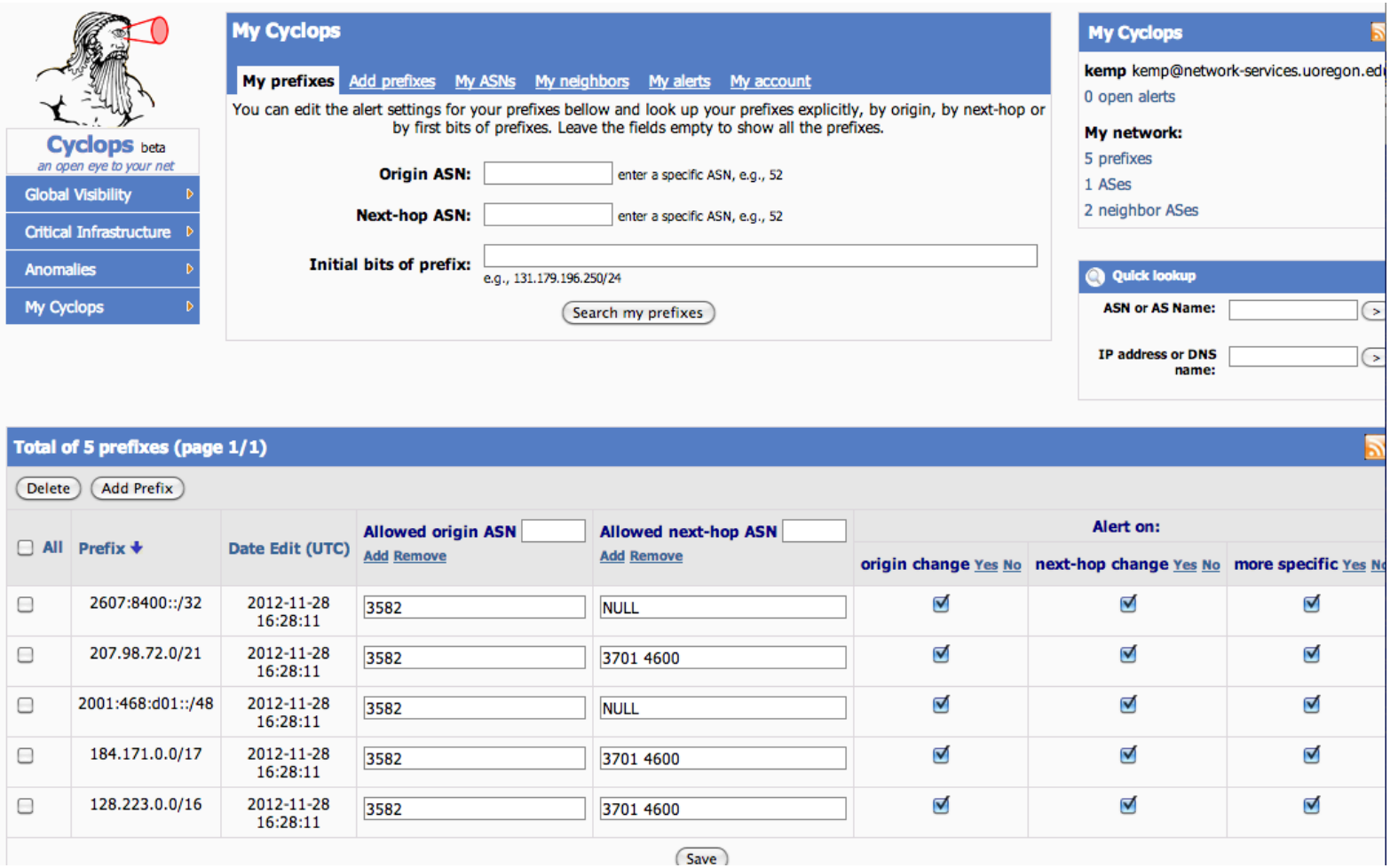
- Lixia Zhang, Ricardo Oliviera, et.al., UCLA
- Internet Topology Database and BGP Notification System
- BGP Data -> Internet Topology -> DB, Event Correlation
- "Event" means
  - sustained AS Path Change in comparison to previously stored AS Paths
  - based on "Link Weight" between ASNs -- #Peers, Peer+, Peer –
- IPV6 Development at cyclops6.6watch.net
  - Pei-chun Cheng, Alexander Afanasyev

- Free To Join Cyclops
  - visit http://cyclops.cs.ucla.edu
  - create an account
  - add AS / Prefix (automatic) / Neighbors (automatic)
  - select alerts (origin, neighbor, more specifics)

Cyclops: What It Detects

- Origin Change (Hijack*)
- Next-hop Change
- New Prefix, and More Specific Prefix (Hijack*)
- New Neighbors
- Transit, My AS in a New Path
- Bogons (both ASNs and Prefixes)

Cyclops: My AS



Cyclops: Alerts

Cyclops beta
open eye to your net

- Global Visibility >
- Critical Infrastructure >
- Anomalies >
- My Cyclops >

No. of BGP feeds: **960**

My Cyclops

My Prefixes | Add Prefixes | My ASNs | My Neighbors | **My Alerts** | My Account

Bellow are the alerts that were created for your account. You can search alerts, close or delete them. Click on alert id for alert details.

Start date: * 2011-04-29

End date: * 2011-05-20

ASNs:

e.g. 52,7018

Prefixes:

e.g. 192.154.2.0/24, 2607:f010::/32

Alert type: Origin change

Activity: All

Alert status: All

Show my alerts

My Cyclops

Mr. Guest
rveloso@cs.ucla.edu

150172 open alerts

My network:

79 prefixes

8 ASes

3429 neighbor ASes

Quick lookup

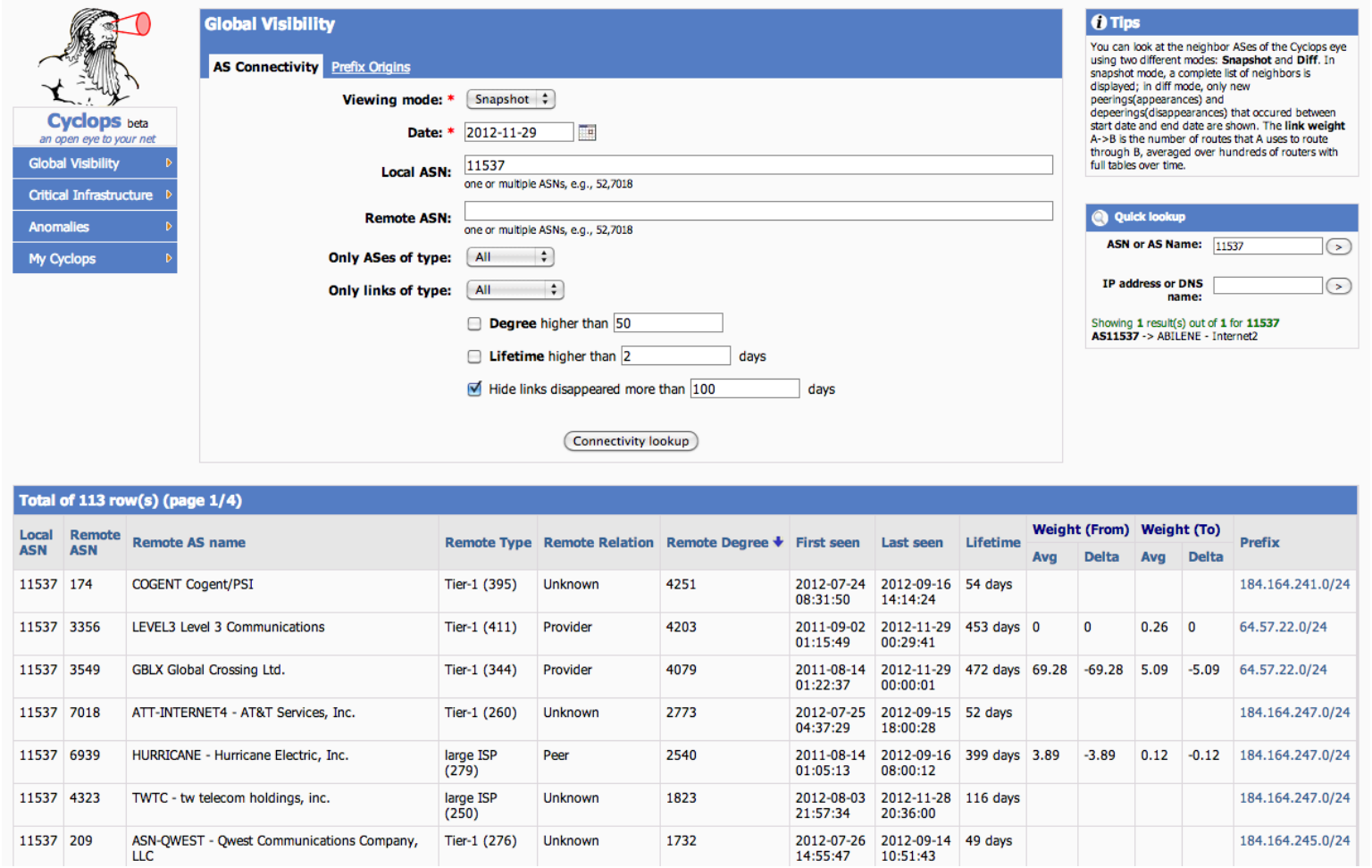
ASN or AS Name: >

IP address or Host name: >

Total of 139 alerts (page 1/7)

Select: All None Delete Open Close Mark as false alert	Alert id	Monitored ASN / prefix	Date (UTC)	Type	Announced prefix	Announced AS path	Duration / Activity	No. monitors	Status
☐	75385483	195.27.162.0/23	2011-05-18 00:56:13	**origin change**	195.27.162.0/23	53070 16735 6762 3320 12888	00:23:54 / **Off**	2	Open
☐	75475728	195.27.162.0/23	2011-05-17 22:45:09	**origin change**	195.27.162.0/23	14537 3356 1273 12888	04:14:32 / **Off**	2	Open
☐	75346385	195.27.162.0/23	2011-05-17 22:20:31	**origin change**	195.27.162.0/23	31500 174 3320 12888	00:36:10 / **Off**	2	Open

Cyclops: Topology



Cyclops beta
an open eye to your net

- Global Visibility
- Critical Infrastructure
- Anomalies
- My Cyclops

Global Visibility

AS Connectivity | Prefix Origins

Viewing mode: * Snapshot

Date: * 2012-11-29

Local ASN: 11537
one or multiple ASNs, e.g., 52,7018

Remote ASN:
one or multiple ASNs, e.g., 52,7018

Only ASes of type: All

Only links of type: All

Degree higher than 50

Lifetime higher than 2 days

Hide links disappeared more than 100 days

Connectivity lookup

Tips

You can look at the neighbor ASes of the Cyclops eye using two different modes: **Snapshot** and **Diff**. In snapshot mode, a complete list of neighbors is displayed; in diff mode, only new peerings(appearances) and depeerings(disappearances) that occured between start date and end date are shown. The **link weight** A->B is the number of routes that A uses to route through B, averaged over hundreds of routers with full tables over time.

Quick lookup

ASN or AS Name: 11537 >

IP address or DNS name: >

Showing 1 result(s) out of 1 for **11537**
AS11537 -> ABILENE - Internet2

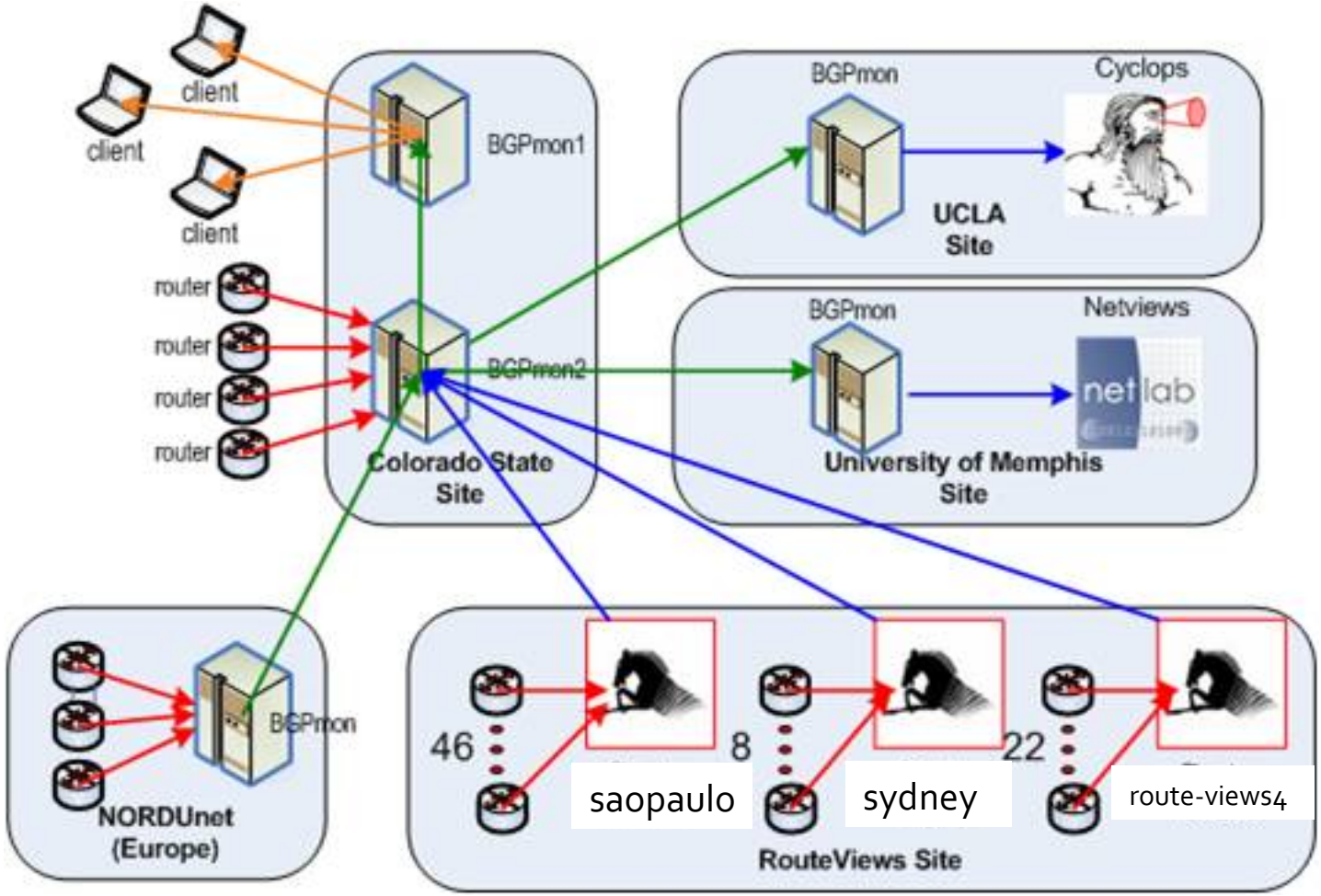
Total of 113 row(s) (page 1/4)

Local ASN	Remote ASN	Remote AS name	Remote Type	Remote Relation	Remote Degree	First seen	Last seen	Lifetime	Weight (From)		Weight (To)		Prefix
									Avg	Delta	Avg	Delta	
11537	174	COGENT Cogent/PSI	Tier-1 (395)	Unknown	4251	2012-07-24 08:31:50	2012-09-16 14:14:24	54 days					184.164.241.0/24
11537	3356	LEVEL3 Level 3 Communications	Tier-1 (411)	Provider	4203	2011-09-02 01:15:49	2012-11-29 00:29:41	453 days	0	0	0.26	0	64.57.22.0/24
11537	3549	GBLX Global Crossing Ltd.	Tier-1 (344)	Provider	4079	2011-08-14 01:22:37	2012-11-29 00:00:01	472 days	69.28	-69.28	5.09	-5.09	64.57.22.0/24
11537	7018	ATT-INTERNET4 - AT&T Services, Inc.	Tier-1 (260)	Unknown	2773	2012-07-25 04:37:29	2012-09-15 18:00:28	52 days					184.164.247.0/24
11537	6939	HURRICANE - Hurricane Electric, Inc.	large ISP (279)	Peer	2540	2011-08-14 01:05:13	2012-09-16 08:00:12	399 days	3.89	-3.89	0.12	-0.12	184.164.247.0/24
11537	4323	TWTC - tw telecom holdings, inc.	large ISP (250)	Unknown	1823	2012-08-03 21:57:34	2012-11-28 20:36:00	116 days					184.164.247.0/24
11537	209	ASN-QWEST - Qwest Communications Company, LLC	Tier-1 (276)	Unknown	1732	2012-07-26 14:55:47	2012-09-14 10:51:43	49 days					184.164.245.0/24

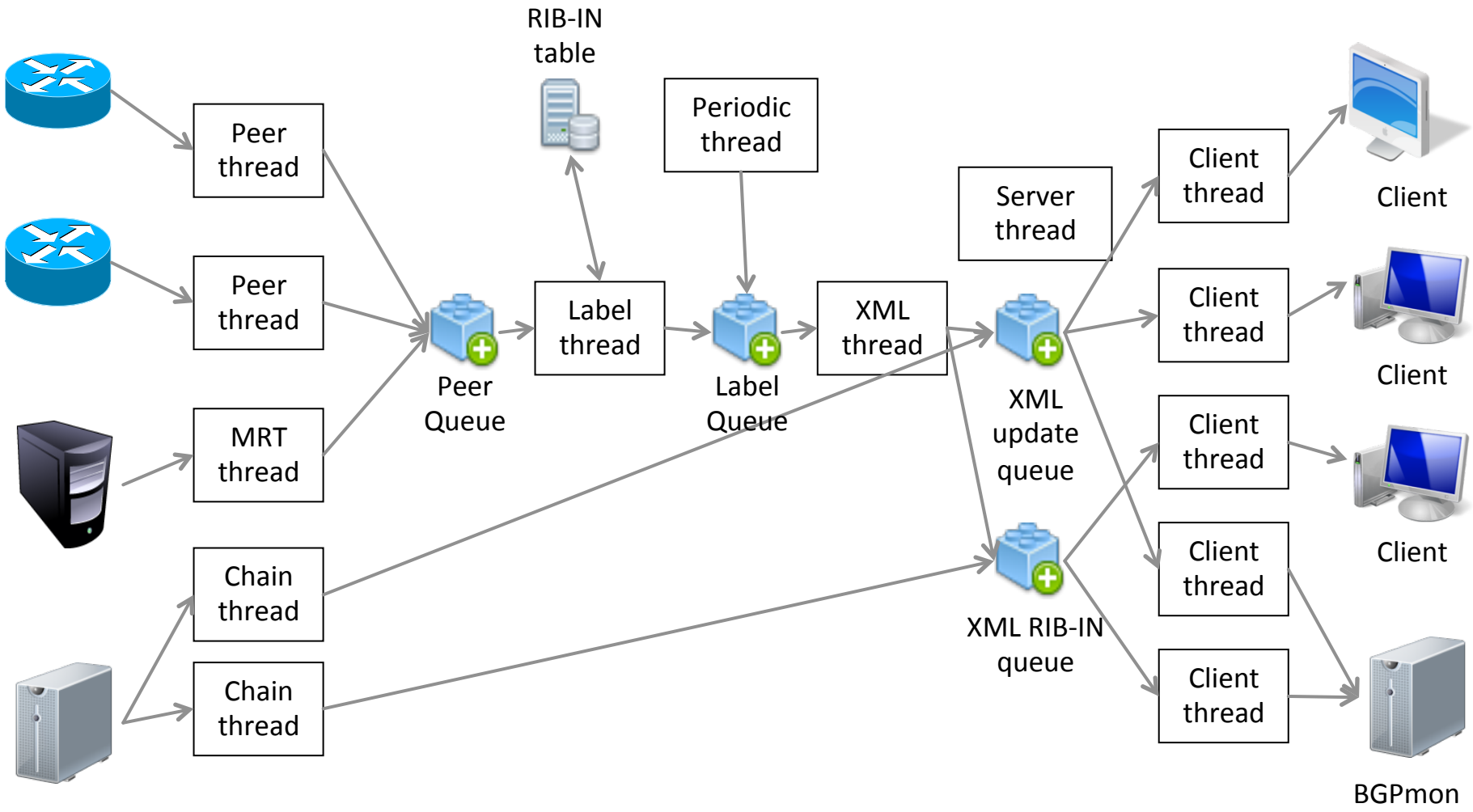
BGPmon

- Dan Massey, Catherine Olschanowsky
  Colorado State University
  http://bgpmon.netsec.colostate.edu
- BGP Monitor Scalability
  - Supports Directly Connected Peers
  - Supports Quagga/MRT Forwarding Peers
  - Supports BGPmon Servers, "Chaining"
- Produces a Consolidated Live Data Stream!!!
- Output Data Stream Format Is XML
- BGPmon feeds into Cyclops
- MRT Peers: route-views.saopaulo, route-views.sydney

BGPmon Today



BGPmon: Architecture



livebgp.netsec.colostate.edu 50001

```
[kemp@archive ~]$ telnet livebgp.netsec.colostate.edu 50001
Trying 129.82.138.26...
Connected to livebgp.netsec.colostate.edu.
Escape character is '^]'.
<xml><BGP_MESSAGE length="00002763" version="0.2" xmlns="urn:ietf:params:xml:ns:
xfb-0.2" type_value="3" type="MESSAGE"><TIME><TIMESTAMP>1305662362</TIMESTAMP><D
ATETIME>2011-05-17T19:59:22Z</DATETIME><PRECISION_TIME>902</PRECISION_TIME></TIM
E><PEERING><SRC_ADDR afi="IPV4" afi_value="1" if_index="0">128.223.51.102</SRC_A
DDR><SRC_PORT>179</SRC_PORT><SRC_AS>6447</SRC_AS><DST_ADDR afi="IPV4" afi_value=
"1" if_index="0">208.51.134.246</DST_ADDR><DST_PORT>179</DST_PORT><DST_AS>3549</
DST_AS><BGPID>0.0.0.0</BGPID><AS_NUM_LEN>2</AS_NUM_LEN></PEERING><ASCII_MSG><MAR
KER length="16">FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF</MARKER><LENGTH>105</LENGTH><TY
PE value="2">UPDATE</TYPE><UPDATE><WITHDRAWN_LEN>0</WITHDRAWN_LEN><WITHDRAWN cou
nt="0"/><PATH_ATTRIBUTES_LEN>74</PATH_ATTRIBUTES_LEN><PATH_ATTRIBUTES count="5">
<ATTRIBUTE><FLAGS><TRANSITIVE/></FLAGS><LENGTH>1</LENGTH><TYPE value="1">ORIGIN<
/TYPE><ORIGIN value="0">IGP</ORIGIN></ATTRIBUTE><ATTRIBUTE><FLAGS><TRANSITIVE/><
/FLAGS><LENGTH>10</LENGTH><TYPE value="2">AS_PATH</TYPE><AS_PATH><AS_SEG type="A
S_SEQUENCE" length="4"><AS>3549</AS><AS>22822</AS><AS>13720</AS><AS>13720</AS></
AS_SEG></AS_PATH></ATTRIBUTE><ATTRIBUTE><FLAGS><TRANSITIVE/></FLAGS><LENGTH>4</L
ENGTH><TYPE value="3">NEXT_HOP</TYPE><NEXT_HOP>208.51.134.246</NEXT_HOP></ATTRIB
UTE><ATTRIBUTE><FLAGS><OPTIONAL/></FLAGS><LENGTH>4</LENGTH><TYPE value="4">MULTI
_EXIT_DISC</TYPE><MULTI_EXIT_DISC>2504</MULTI_EXIT_DISC></ATTRIBUTE><ATTRIBUTE><
FLAGS><OPTIONAL/><TRANSITIVE/></FLAGS><LENGTH>40</LENGTH><TYPE value="8">COMMUNI
TIES</TYPE><COMMUNITIES><COMMUNITY><AS>3549</AS><VALUE>4524</VALUE></COMMUNITY><
COMMUNITY><AS>3549</AS><VALUE>8280</VALUE></COMMUNITY><COMMUNITY><AS>3549</AS><V
ALUE>31826</VALUE></COMMUNITY><COMMUNITY><AS>13720</AS><VALUE>103</VALUE></COMMU
NITY><COMMUNITY><AS>13720</AS><VALUE>201</VALUE></COMMUNITY><COMMUNITY><AS>13720
</AS><VALUE>886</VALUE></COMMUNITY><COMMUNITY><AS>13720</AS><VALUE>887</VALUE></
```

BGPmon Tools

- PERL CPAN BGPMON
  - http://www.cpan.org/authors/id/B/BG/BGPMON/
- BGPmon-core
  - Connect to livebgp, "BGPmon::Fetch"
  - Filter based on AS / Prefix, "BGPmon::Filter"
  - Translate XML to ASCII or MRT, "BGPmon::Translator"
  - Requires: Net::IP, Regexp::IPv6, WWW::Curl, XML::LibXML
  - Sample Code: bgpmon-filter.pl
- BGPmon-Archiver, Store XML Data in Filesystem
- BGPmon-Analytics, Store XML Data in Database

BGPmon Tools

```
use BGPmon::Fetch;
use BGPmon::Filter;
use BGPmon::Translator;

connect_bgpdata();

my $xml_msg = read_xml_message();
while($xml_msg){
        # throw out everything except routes from our desired ASN
        if (ComesFrom($desiredASN)){
                # extract a print the prefix and path
                my $time = get_time($xml_msg);
                my $prefix = get_prefix($xml_msg);
                my $path= get_aspath($xml_msg);
                print "At time $time, there is route $prefix path $path\n";
        }
        $xml_msg = read_xml_message();
}
close_connection();
```

BGPmon Resources

- Archive Data (example)
  - http://archive.netsec.colostate.edu/peers/187.16.216.20/2012.11/UPDATES/
- Server Source Code
  - http://bgpmon.netsec.colostate.edu/download/src/bgpmon-7.2.3.tar.gz
- Perl Scripting Modules
  - http://www.cpan.org/authors/id/B/BG/BGPMON/
- Recent Publications
  - http://www.cs.colostate.edu/~mstrout/RMCWiC2012/csuconf-final19.pdf
- Mailing List
  - http://www.netsec.colostate.edu/cgi-bin/mailman/listinfo/bgpmon
- Contact: bgpmon@netsec.colostate.edu

RouteViews Resources

- RouteViews
  - http://www.routeviews.org/
- PeeringDB, Complete List of Collectors / Exchanges
  - http://www.peeringdb.com/view.php?asn=6447
- A Typical RIB, Route-views2 Every 2 Hours
  - http://archive.routeviews.org/oix-route-views/oix-full-snapshot-latest.dat.bz2
- RouteViews Data
  - {http,ftp}://archive.routeviews.org/
  - rsync –list-only archive.routeviews.org::routeviews
  - rsync –av archive.routeviews.org::routeviews/bgpdata .
- BGPlay
  - http://bgplay.routeviews.org/
- ASpath DNS Files
  - http://archive.routeviews.org/dnszones/
- Contact: help@routeviews.org