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:
  - 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)

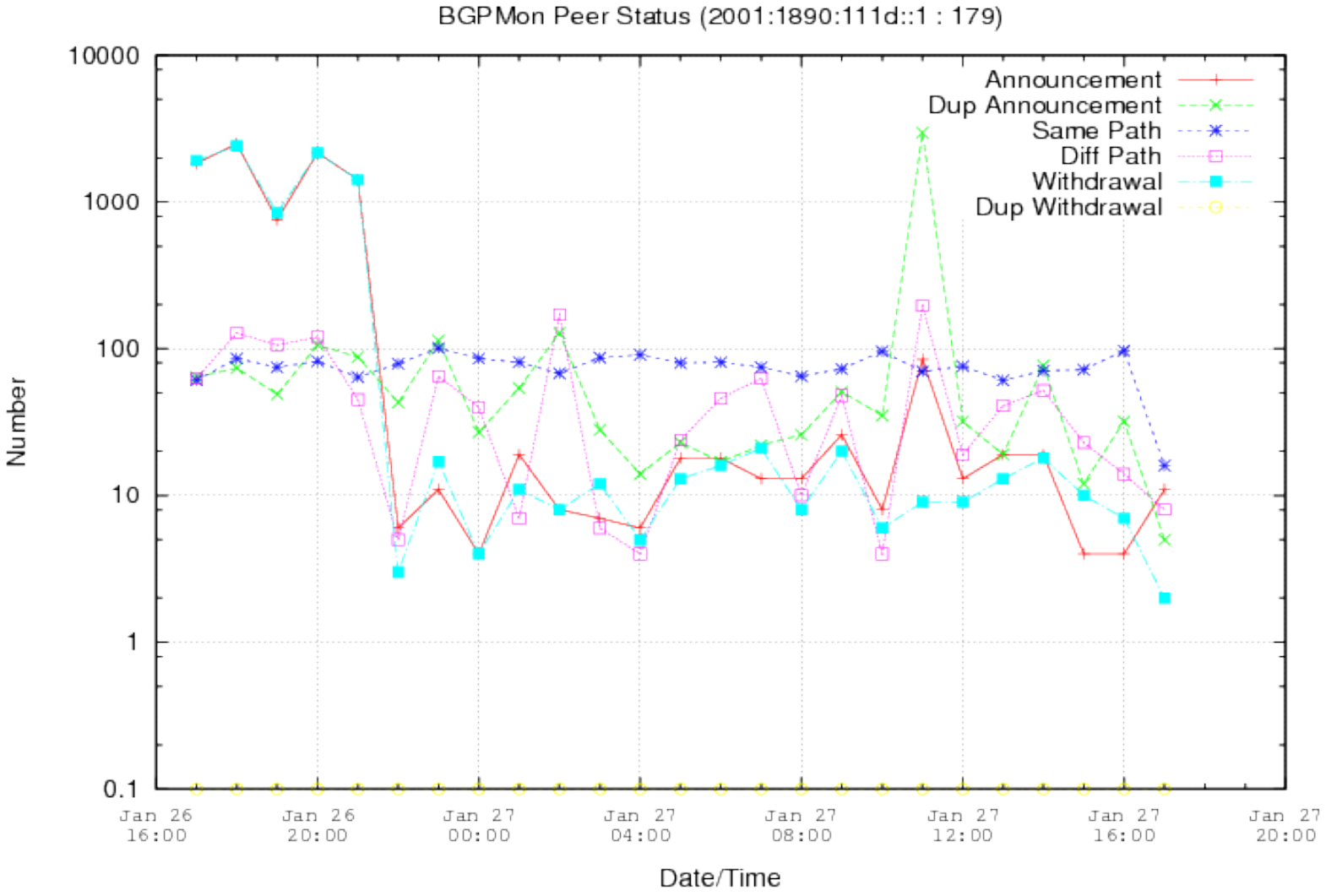
```
<ASCII_MSG>
    <LENGTH>53</LENGTH>                                  ← BGP message total length
    <TYPE value="2">UPDATE</TYPE>                        ← BGP message type, according to RFC 4271
    <UPDATE>
        <ATTRIBUTE>
            <LENGTH>12</LENGTH>
            <TYPE value="2">AS_PATH</TYPE>
            <AS_PATH>
                <AS_SEG type="AS_SEQUENCE" length="5">
                    <AS>14041</AS><AS>209</AS> <AS>3356</AS>
                    <AS>4230</AS><AS>28175</AS>          ← BGP AS Path data
                </AS_SEG>
            </AS_PATH>
        </ATTRIBUTE>
        <ATTRIBUTE>
            <LENGTH>4</LENGTH>
            <TYPE value="3">NEXT_HOP</TYPE>
            <NEXT_HOP>192.43.217.141</NEXT_HOP>          ← Next Hop data
        </ATTRIBUTE>
        <NLRI count="1">
            <PREFIX label="DPATH" afi="IPV4" afi_value="1" safi="UNICAST"
                                  safi_value="1">189.85.51/24</PREFIX>   ← Announced Prefix
        </NLRI>
</UPDATE>
```

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



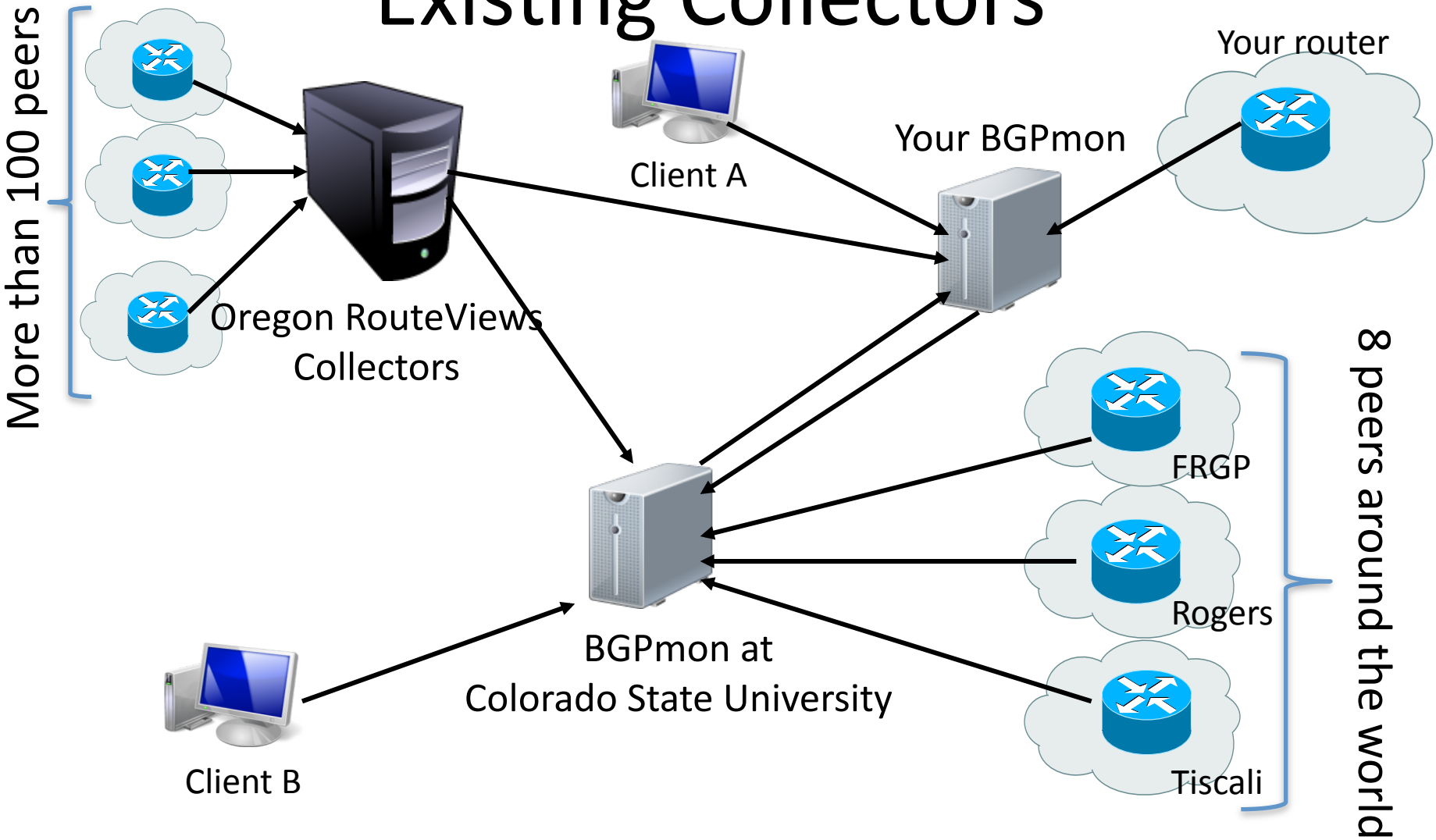
Running Your Own Collector

- 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.

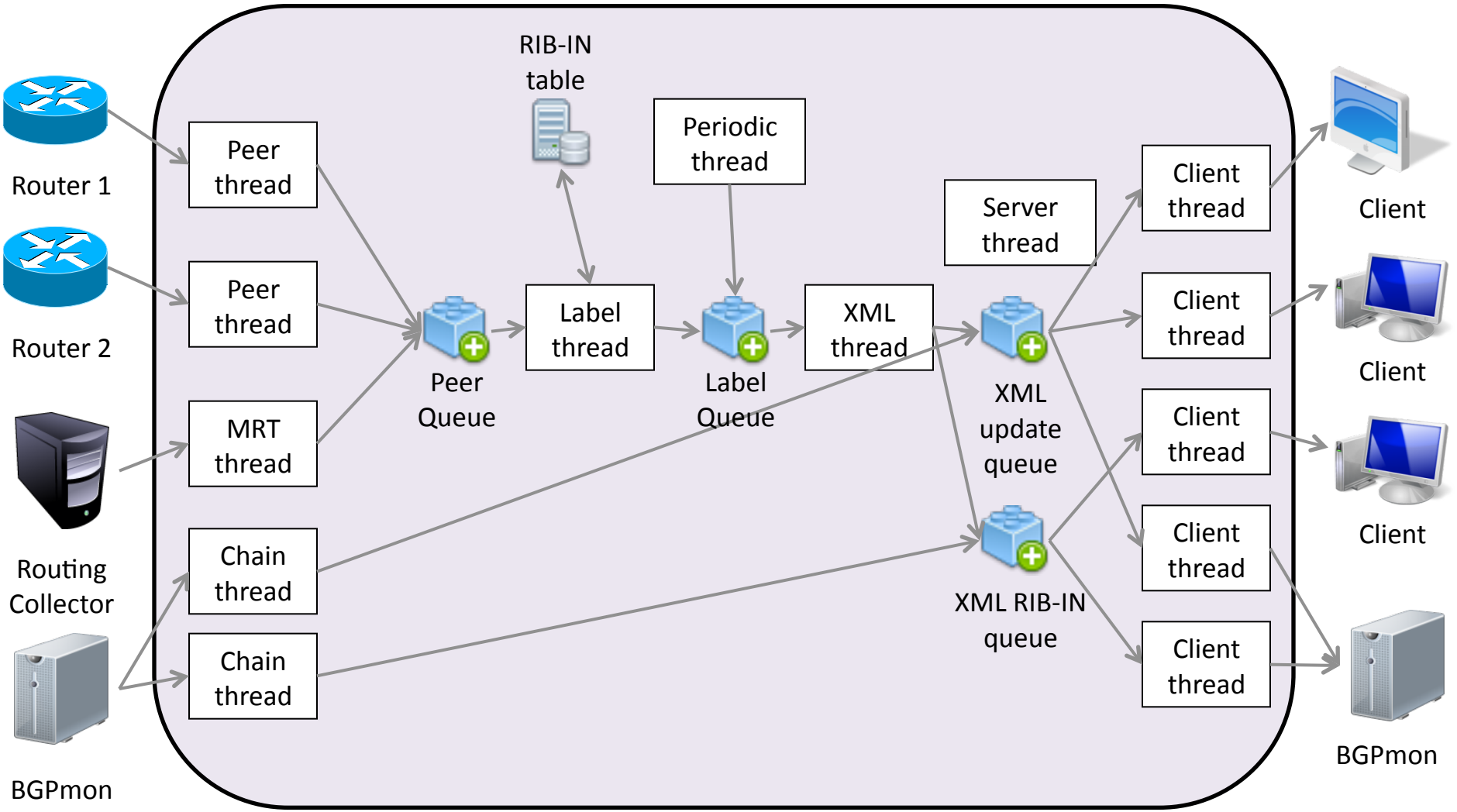
- Project Website

  http://bgpmon.netsec.colostate.edu

Merging Your Collector with Existing Collectors



BGPmon Architecture



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

BGP Monitoring System 8/22/11 12:41 PM

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

1. BGP Peers

IP	PORT	AS	Status	Uptime	#MsgRcvd	#Reset	#Prefix	#Attribue	Memory(k)	Detail
65.49.129.101	179	3043	✓		1347763	0	365466	62041	39654.726	detail
205.167.76.241	179	10876	✓		554129	0	362246	61062	30220.441	detail
89.149.178.10	179	3257	✓		1177635	0	360993	61408	38722.232	detail
164.128.32.11	179	3303	✓		1017777	0	142963	34371	21995.69	detail
64.71.255.61	179	812	✓		2206875	0	352846	59641	35861.44	detail
192.43.217.141	179	14041	✓		1045431	0	361378	60958	31936.445	detail
195.209.15.251	179	5568	✓		7389	3	0	0	3520.056	detail

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

2. MRT

IP	PORT	AS	Status	Uptime	#MsgRcvd	#Reset	#Prefix	#Attribue	Memory(k)	Detail
202.167.228.20	179	4739		N/A	320591	0	369837	61390	28226.993	detail
2001:de8:6::4826:1	179	4826		N/A	28221	0	751	512	3713.062	detail
2001:de8:6::7575:1	179	7575		N/A	39677	0	1440	1091	3869.29	detail
202.167.228.44	179	10026		N/A	623298	0	205606	35719	24079.732	detail
202.167.228.37	179	38809		N/A	141477	0	31655	6954	7089.423	detail
202.167.228.46	179	7575		N/A	103587	0	21318	4559	5645.269	detail
202.167.228.74	179	4826		N/A	427622	0	313844	53951	26170.469	detail
2001:de8:6::4739:1	179	4739		N/A	51501	0	7021	4971	4690.063	detail
2001:de8:6::1:26:1	179	10026		N/A	23366	0	1216	877	3782.287	detail
2001:468:ff02::1	179	11537		N/A	144813	0	842	611	4141.752	detail
2001:218:0:1000::f006	179	2914		N/A	25173	0	1018	800	3781.243	detail
2001:2000:3018:4d::1	179	1299		N/A	14004	0	660	530	3667.723	detail
2001:388:1::16	179	7575		N/A	127945	0	6931	5047	5134.589	detail
2001:388:1::13	179	7575		N/A	109416	0	3092	2322	4495.666	detail
2001:da8:ff:301::1	179	23910		N/A	33860	0	1464	1115	3892.493	detail
2402:7400:0:3c::1	179	38883		N/A	8108	0	951	699	3687.844	detail
2001:468:2::1	179	11537		N/A	32823	0	149	115	3670.71	detail
2001:12b4::1	179	28289		N/A	46737	0	985	718	3817.608	detail
2001:15a8:a:a::2	179	29449		N/A	17023	0	606	564	3674.557	detail
2001:4b20::fffe:4	179	34288		N/A	20268	0	835	648	3701.757	detail
2607:fc58:0:80::1:4	179	20225		N/A	28878	0	850	660	3734.274	detail
202.167.228.81	179	24436		N/A	2352	0	410	104	3563.141	detail

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