



RouteViews + BGPmon

Enabling BGP Monitoring and Analysis

Catherine Olschanowsky

Lawrence Weikum

John Kemp





RouteViews + BGPmon: A Community Infrastructure

- Started by the operations community
 - Unfunded grassroots effort
- Used by
 - University researchers
 - The operations community
 - Government contractors and security teams
- Maintained and Expanded by
 - University of Oregon
 - Colorado State University



Introduction

Deployment

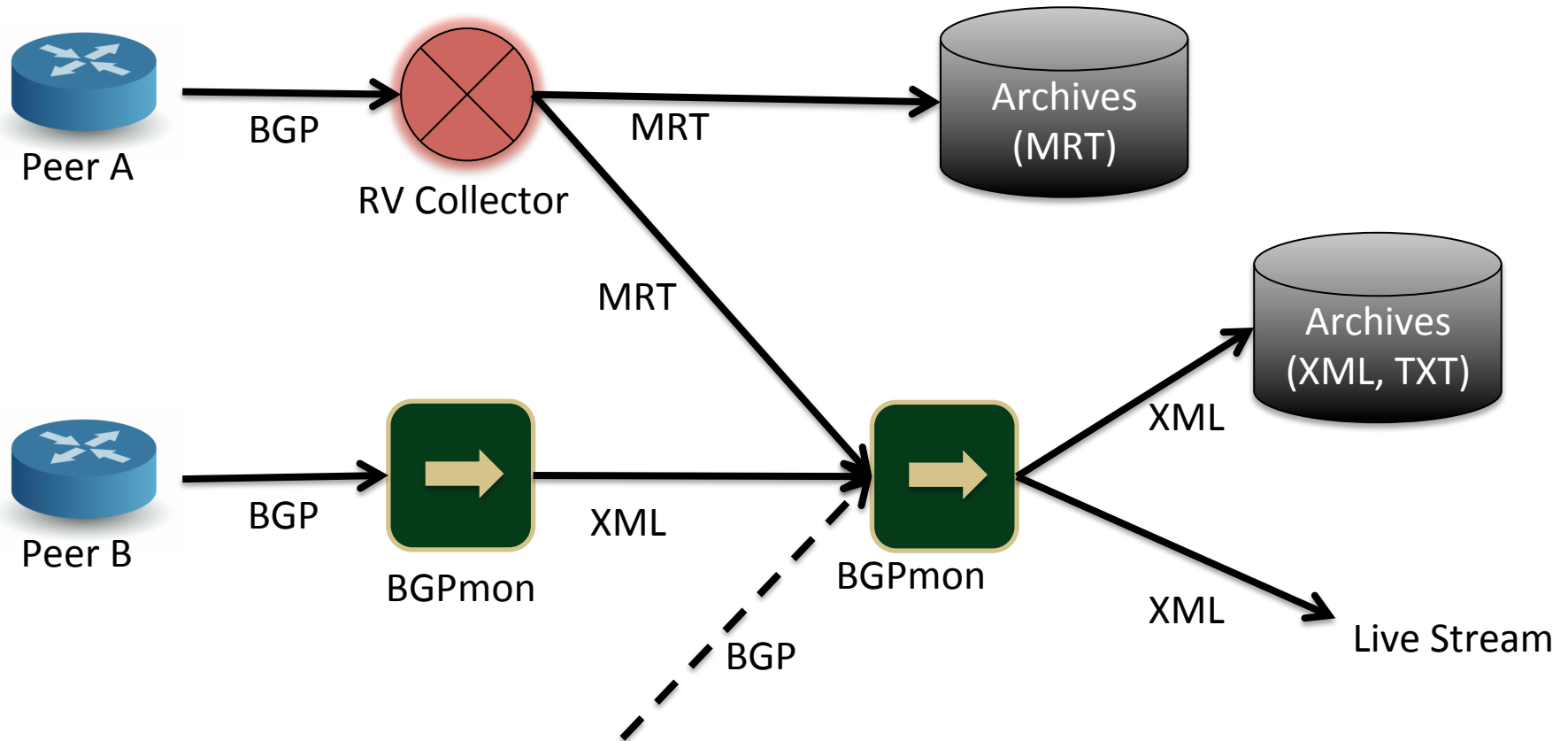
Demos

DIY

Updates



RouteViews + BGPmon: Public BGP Monitoring





RouteViews + BGPmon: Made possible by our peers



Núcleo de Informação
e Coordenação do
Ponto BR



Introduction

Deployment

Demos

DIY

Updates



RouteViews Deployment

BGP Collectors

- ☐ Multi-hop and at Major Exchanges
- ☐ 17 Collectors, 170 v4 peers, 75 v6 peers
- ☐ Telnet Cisco Command-Line with Open Access
- ☐ Full-Table View from Each Peer to AS6447

BGP Data

- ☐ Collection, Distribution, Archiving, and Operations
- ☐ Archive Data in MRT Format, 1997 to present
- ☐ Live Data Streams in XML Format

[Introduction](#)

[Deployment](#)

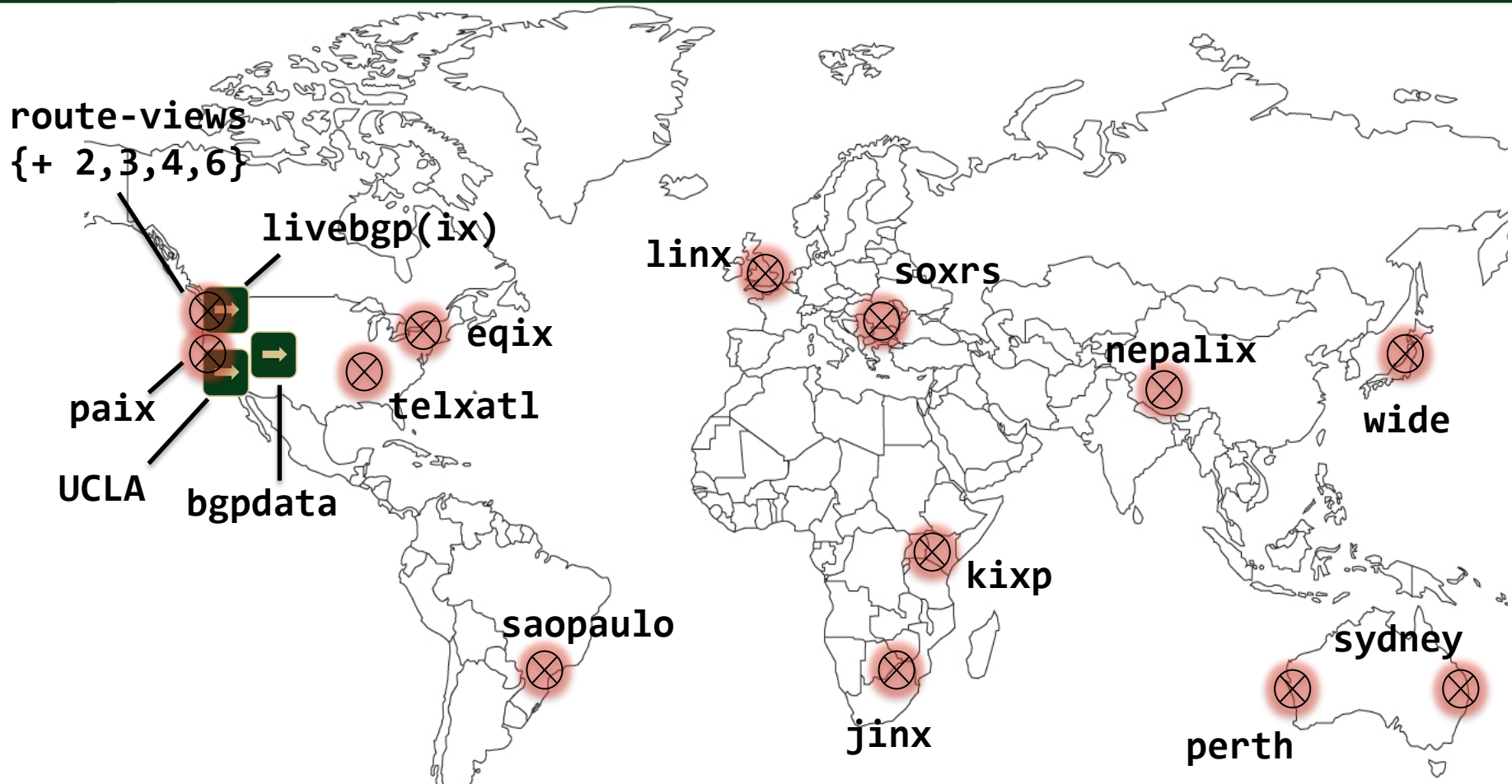
[Demos](#)

[DIY](#)

[Updates](#)



RouteViews + BGPmon Collectors



[Introduction](#)

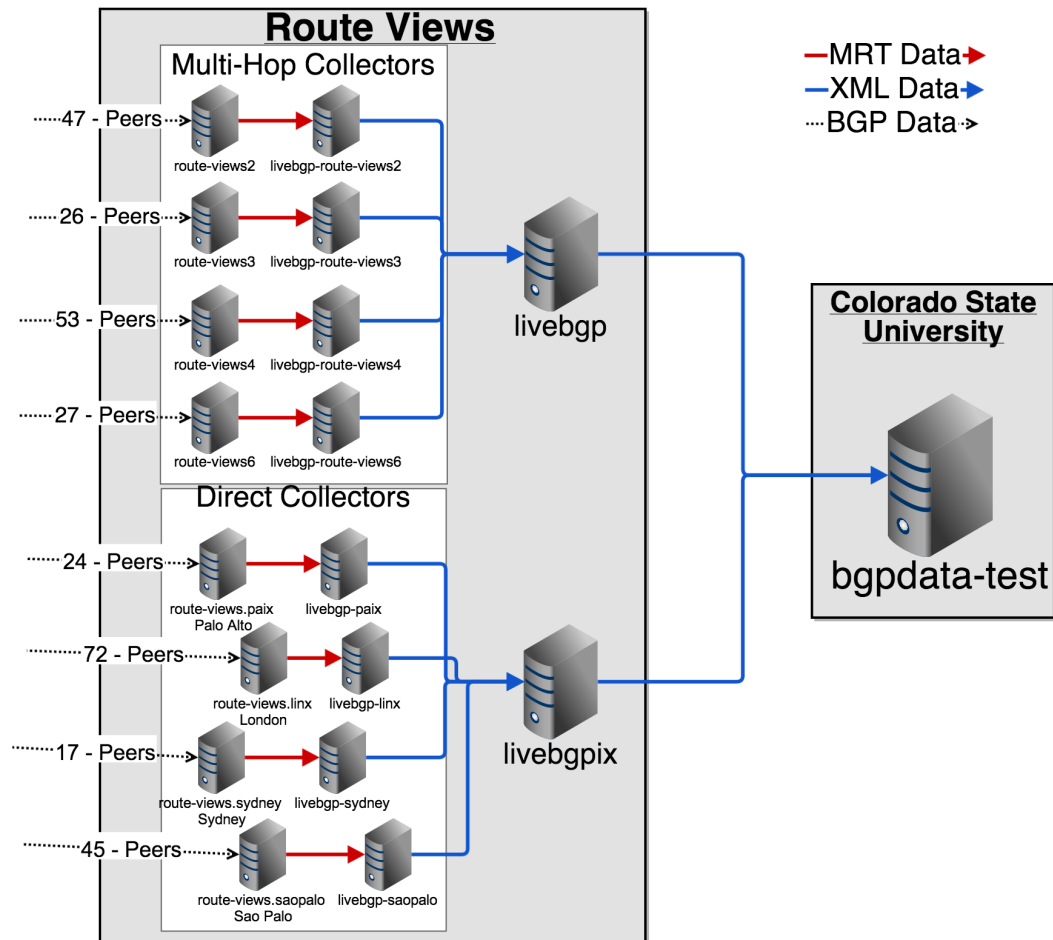
[Deployment](#)

[Demos](#)

[DIY](#)

[Updates](#)

RouteViews+BGPmon Deployment



Introduction

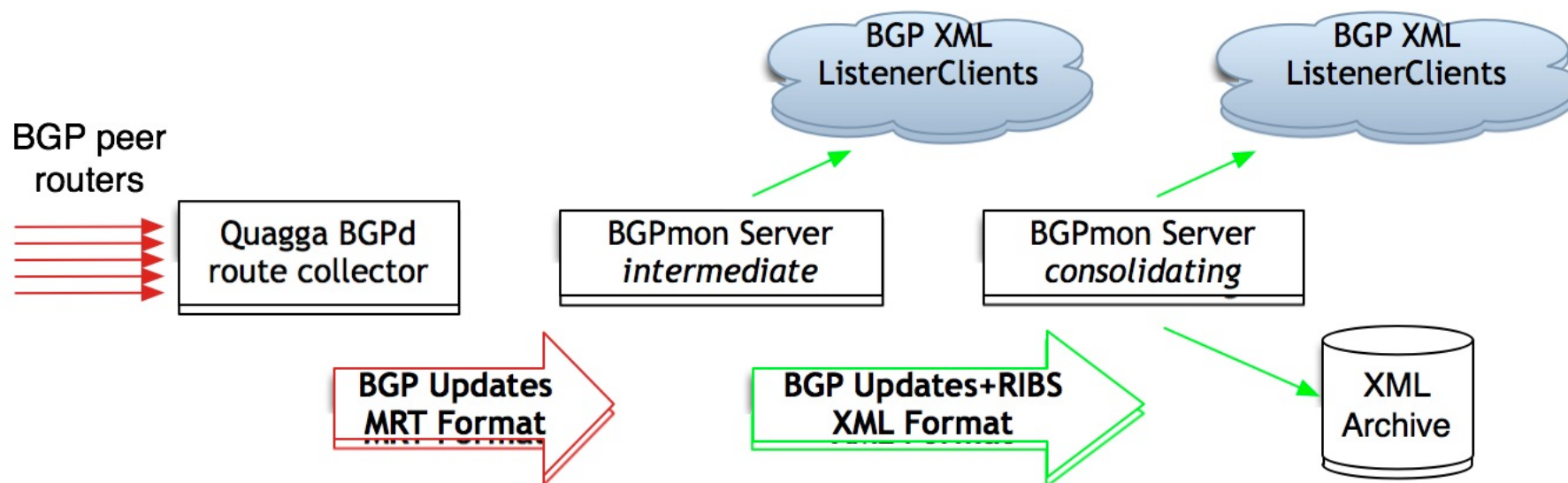
Deployment

Demos

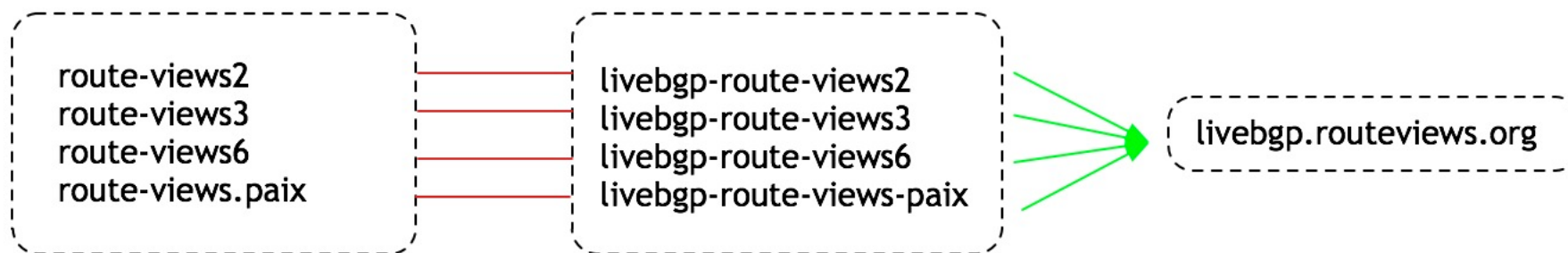
DIY

Updates

RouteViews-BGPmon Architecture (logical)



RouteViews-BGPmon Architecture (current)





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

Introduction

Deployment

Topic 3

Topic 4



Internet Wide Monitoring

- Hilbert Graph: Hierarchical view of prefix space (IPv4)
- Focuses on a single peer
- Shows what portion of the address space changes
- When the path for a prefix changes it turns white
- This is the Australian outage in Feb. 2012



Internet Wide Monitoring

A Retrospective on an Australian Routing Event

Kaustubh Gadkari² John Heidemann¹ Cathie Olschanowsky²
Christos Papadopoulos² Yuri Pradkin¹ Lawrence Weikum²

1: USC/Information Sciences Institute, 2: Colorado State University
January 2014

Copyright © 2014 by the authors
Release terms: CC-BY-NC 4.0 international





Internet Wide Monitoring Multi-Peer View

- Traffic Analytics Feeding Alerts
 - Send Rate
 - Origin Changes
 - Path Changes
 - New Entries
 - Withdrawals
- Alerts triggered by
 - > 1500 path updates (yellow alert)
 - > 3000 path updates (red alert)
 - > 1000 origin changes (yellow alert)



Internet Wide Monitoring

Thu Feb 23 02:30:05 2012 GMT

Peer	RIB Entries	Send Rate	Path Changes	Origin Changes	New Entries	Num Withs
2 [redacted] 1	7949	0	0	0	0	0
2 [redacted] 1	7265	0	0	0	0	0
2 [redacted] 9:1	7971	0	0	0	0	0
2 [redacted] :1	7970	0	0	0	0	0
2 [redacted] :1	7950	0	0	0	0	0
2 [redacted] :1	6157	0	0	0	0	0
2 [redacted]	18823	0	0	0	0	0
2 [redacted]	399679	0	0	0	0	0
2 [redacted]	397282	36	8	0	3	0
2 [redacted]	10300	0	0	0	0	0
2 [redacted]	395645	0	0	0	0	0
2 [redacted]	185564	0	0	0	0	0
2 [redacted]	396498	0	0	0	0	0
2 [redacted]	25143	0	0	0	0	0

[Introduction](#)

[Deployment](#)

[Demos](#)

[DIY](#)

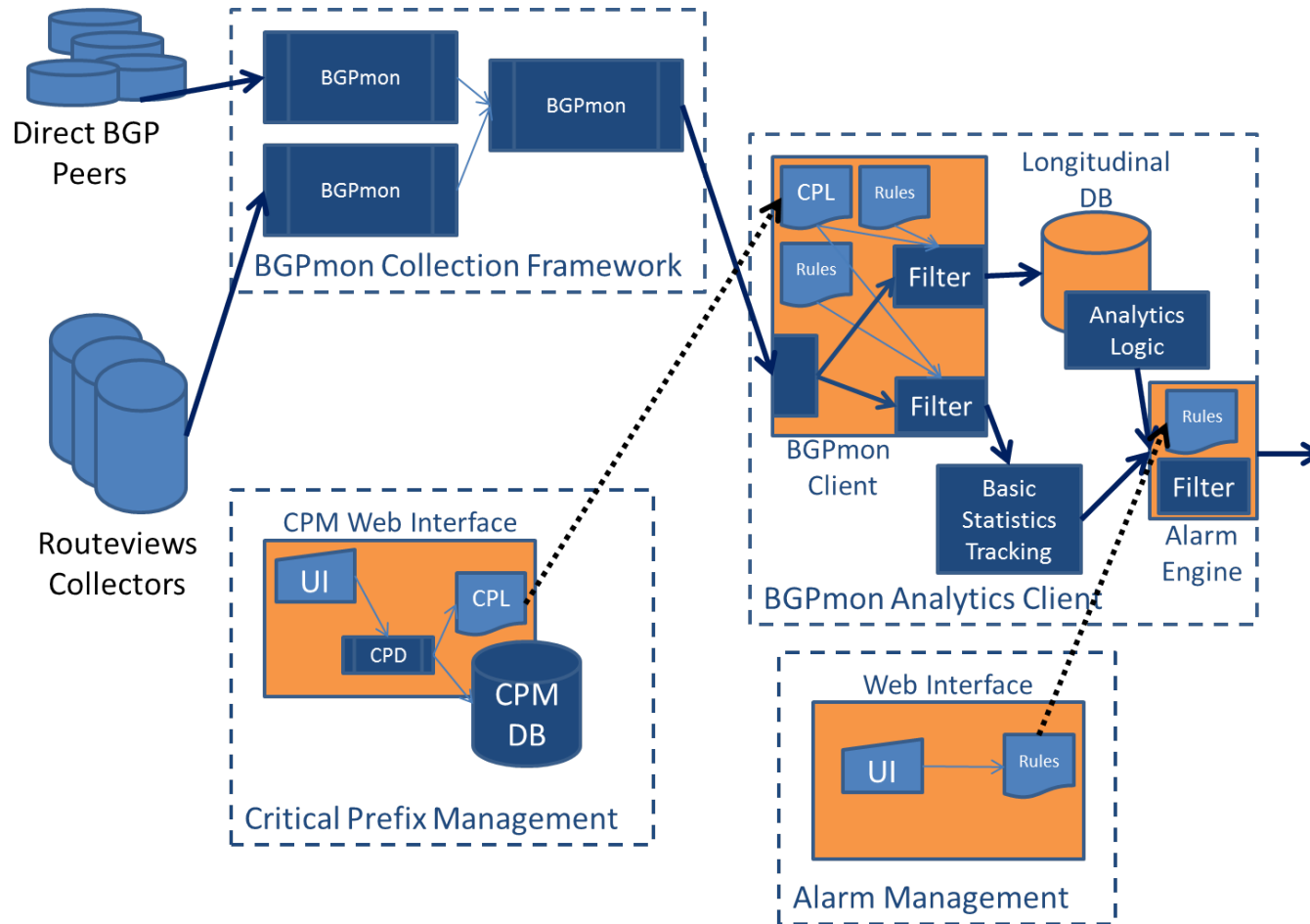
[Updates](#)

Organizational Level

- Create a Critical Prefix List (CPL)
- Monitor your address space
- Monitor space of other's whom you depend on for reachability and services.
- Store and compare updates with PostgreSQL database



Organizational Level Monitoring (CERT Australia)



DIY Perl Tools

- Open source Perl Modules Available on CPAN
 - BGPmon-core
 - Fetch, Translate, Configure, Log
 - BGPmon-Archiver
 - Standalone application + modules
 - BGPmon-AnalyticsDB
 - Experimental relational database
 - BGPmon-CPM
 - Critical prefix discover and management

[Introduction](#)[Deployment](#)[Demos](#)[DIY](#)[Updates](#)

Example Client:

Counts Path Changes for a Specific Peer

```
use BGPmon::Fetch qw/connect_bgpdata read_xml_message is_connected/;
use BGPmon::Translator::XFB2PerlHash::Simpler qw/parse_xml_msg extract_nlri
extract_aspath/;

connect_bgpdata($source, $port);
while(is_connected()){
    my $msg = read_xml_message();
    parse_xml_msg($msg);
    my @as_path = extract_aspath();
    my @announcements = extract_nlri();
    foreach(@announcements){
        num_orig_change += 1 if not(@{ rib->{$_} } ~~ @as_path);
    }
}
```



7.3.3 Release of BGPmon

- Improved Stability
- XSD
- Message changes
- Side-by-side deployments
 - Live feed from `bgpdata-test.netsec.colostate.edu`
 - Updates on 50001
 - RIBs on 50002
- Receives direct peering data as well as chains from BGPmons at RouteViews.

Conclusions

- RouteViews+BGPmon is a public infrastructure and a valuable community resource
- Our deployment spans 6 continents and comprises over 200 peers
- Internet-wide and organization specific BGP monitoring are well supported
- Try out our DIY Perl tools!

[Introduction](#)[Deployment](#)[Demos](#)[DIY](#)[Updates](#)

Acknowledgements

- RouteViews Team
 - John Kemp
 - David Meyer
- BGPmon Team
 - Catherine Olschanowsky
 - Lawrence Weikum
 - Kaustubh Gadhari
 - Lixia Zhang
 - Christos Papadopoulos
- Previous Team Members
 - Daniel Massey

- IPv4 Demo (ISI)
 - Yuri Pradkin
 - John Heidemann

This material is based upon work supported by Department of Homeland Security Science and Technology Directorate, Cyber Security Division, via SPAWAR Systems Center Pacific under Contract No. N66001-13-C-3001.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of SSC-Pacific.

This work has been supported by the DHS Science and Technology Directorate contract number N66001-08-C-2028 and the National Science Foundation's CISE Research Infrastructure (CRI) Program contract number CNS-1305404.

[Introduction](#)[Deployment](#)[Demos](#)[DIY](#)[Updates](#)