

# **WIT: A Watchdog System For Internet Routing**

## **Australian BGP Monitoring Service**

Dan Massey

# Broader BGP Monitoring Team



**SECURE 64**



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

# Why Track BGP Prefixes?

- Given a network outage report...
- Are key sectors such a financial, critical infrastructure, government impacted?
- What is the geographic range of the event?
- Is it an unintentional error or an attack?
- Who is responsible and who needs to act to repair it?

Technology

# Dodo takes blame for internet outage affecting millions

February 23, 2012

Ben Grubb and Asher Moses

Read later

Similar to ... Pin



Dodo MD Larry Kestelman. Photo: JESSICA SHAWNO

ISP **Dodo** played a role in causing the outage that affected millions of fixed-line and mobile Internet connections across the country this afternoon, Dodo's chief has confirmed.

"To be perfectly frank, the extent of what happened was more than anybody could've thought," Dodo managing director Larry Kestelman told this website in an interview, adding his team was still investigating exactly what caused the issue.

"What it looks like has happened ... is a very minor hardware failure on one of the routers that has caused some big issues between ourselves and Telstra and had a flow on effect to others which it absolutely shouldn't have," he said.

"Telstra is saying that there were some overseas routing issues as well - but to me it sounds like it was a combination of things that caused it."

Know more? [bggrubb@smh.com.au](mailto:bggrubb@smh.com.au)

Speculation the outage was caused by Dodo first appeared on the [Australian Network Operators Group](#) electronic mailing list - a list many Australian network administrators subscribe to - and [spread](#) to broadband forum [Whirlpool](#) shortly after.

# Sydney Morning Herald February 23, 2012

"Okay, who broke the internet?  
@iiNet and @Telstra both down

# Media Reports on the Outage



*The outage began about 1.40pm AEDT, lasted about 45 minutes, and affected customers nationwide*

*The CommBank website and NetBank were also affected by the outage but were now back online, a Commonwealth Bank spokesman said.*

Internet users said on Whirlpool that their connections were out in Sydney, Brisbane, Melbourne, Adelaide, Townsville, Tasmania, Canberra, the Gold Coast and Perth.

"Okay, who broke the internet? @iiNet and @Telstra both down.

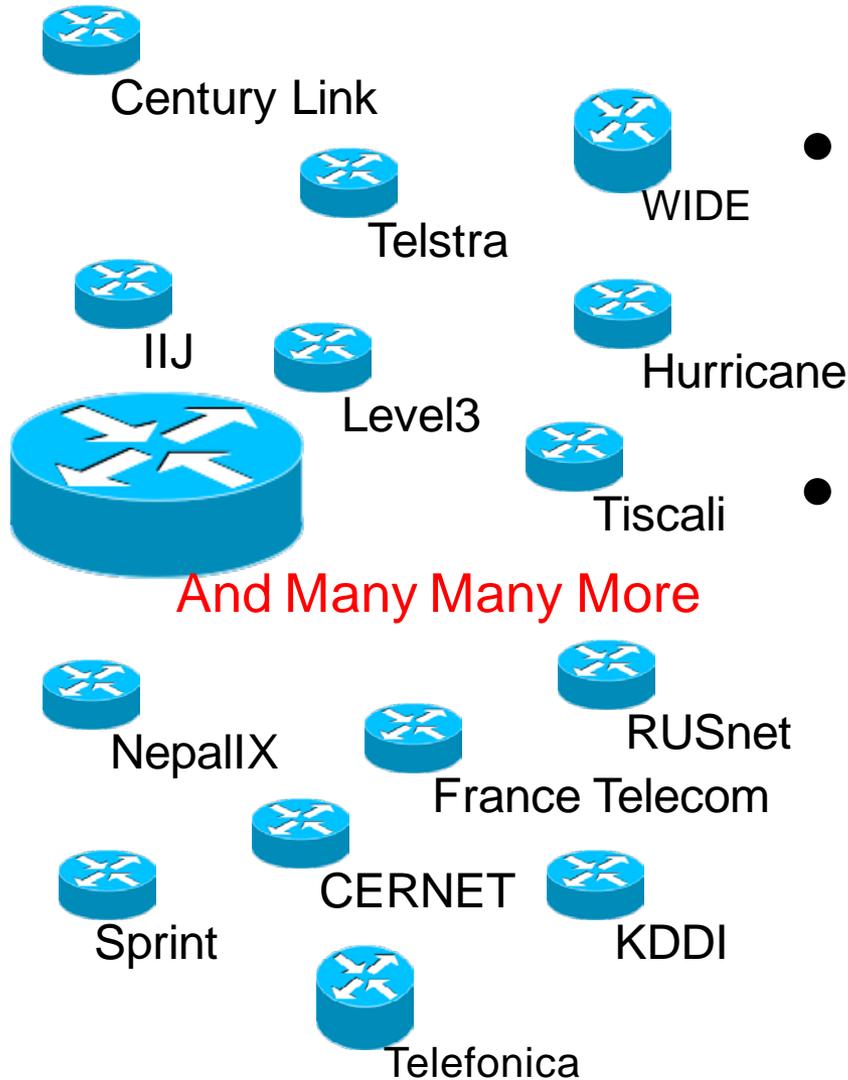


*You'd think the biggest news for today would be the death match between Kevin Rudd and Julia Gillard, but an apparent Telstra outage may well eclipse the two politicians as **a story of much greater significance to the everyday Australian.***

# Our Two Main Contributions

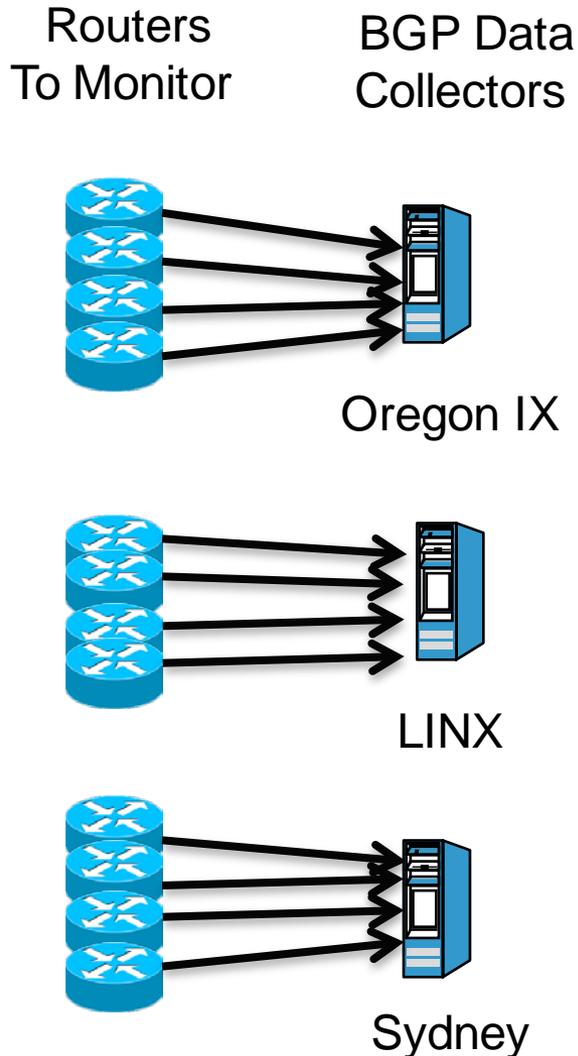
- **Routing Data Needed To Make Decisions**
  - Who is originating a route to your system?
  - Which routes changed during some major event?
  - Data from around the globe provided in real-time
- **A Prefix Monitoring System**
  - Digest the data and provide targeted alerts
  - Alarms indicating when you are being hijacked
  - Run internally or use our existing system

# How BGP Data Collection Works (1/3)



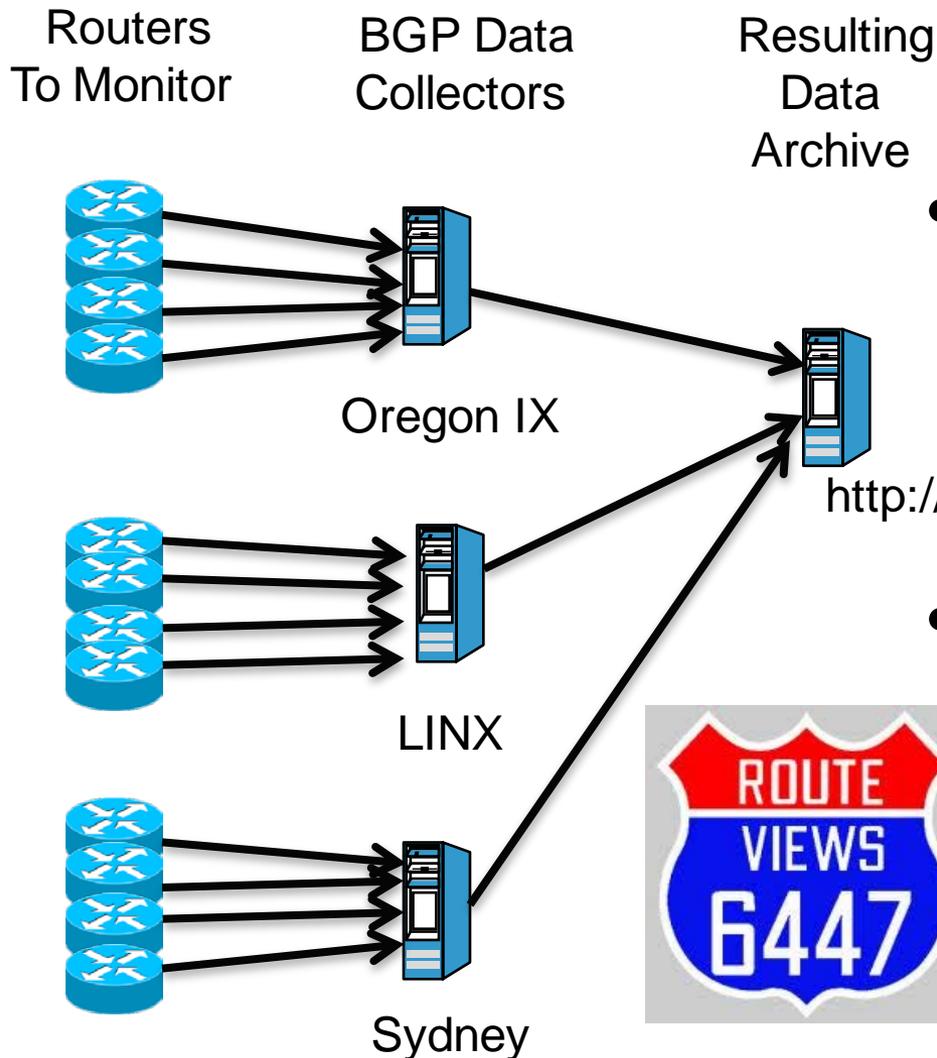
- ISPs around the world offer to provide BGP data
- Agree data can be made publically available to any operator or researcher

# How BGP Data Collection Works (2/3)



- Monitoring projects deploy collectors at exchange points
- ISP routers peer with collectors
- To the ISP router, the collector is just another BGP peer (e.g. router)
  - Only the collector never announces any routes!

# How BGP Data Collection Works (3/3)

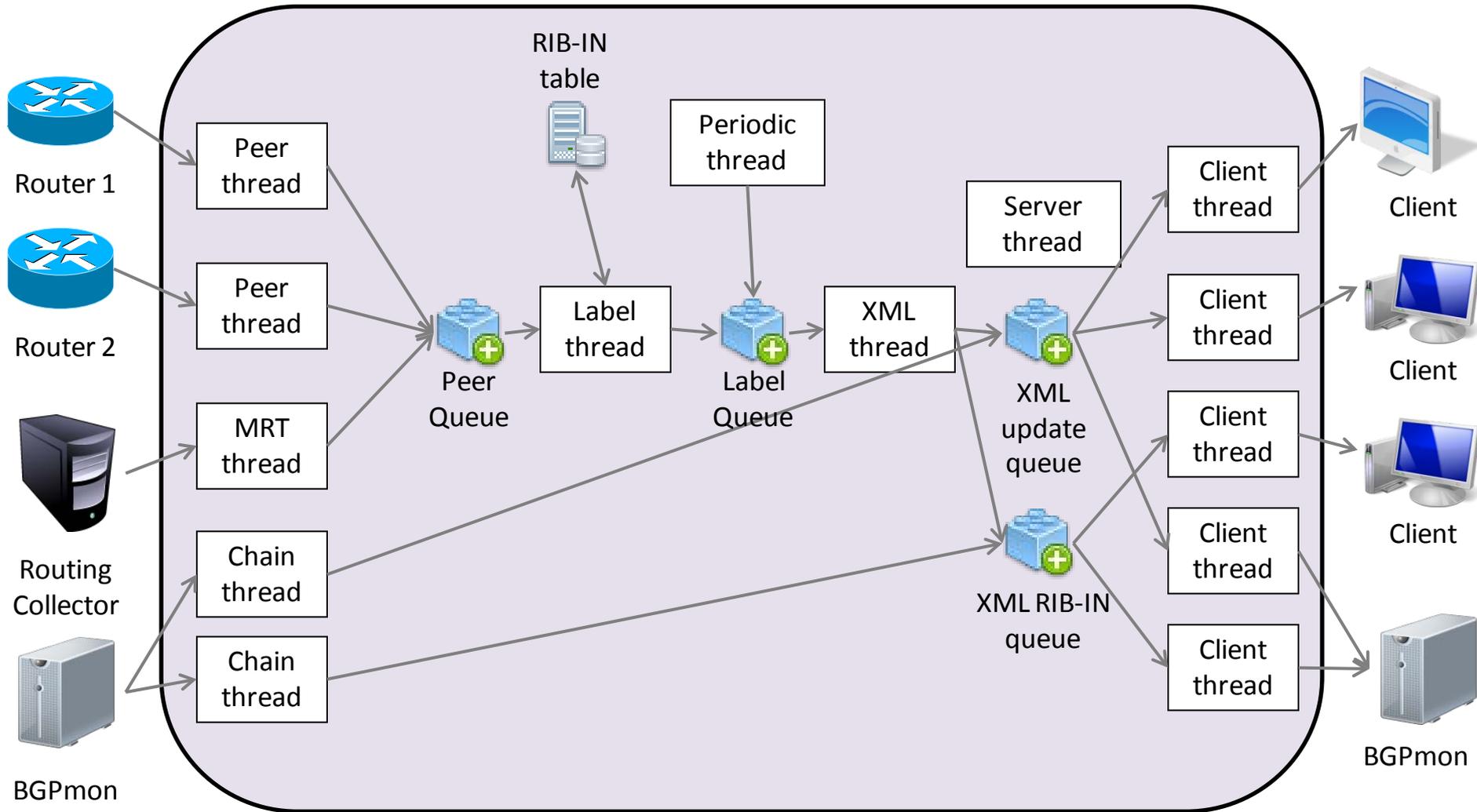


- All Route Updates Are Logged
  - 15 minute intervals
- Collector also archives routing table of each peer router
  - 2 hour intervals

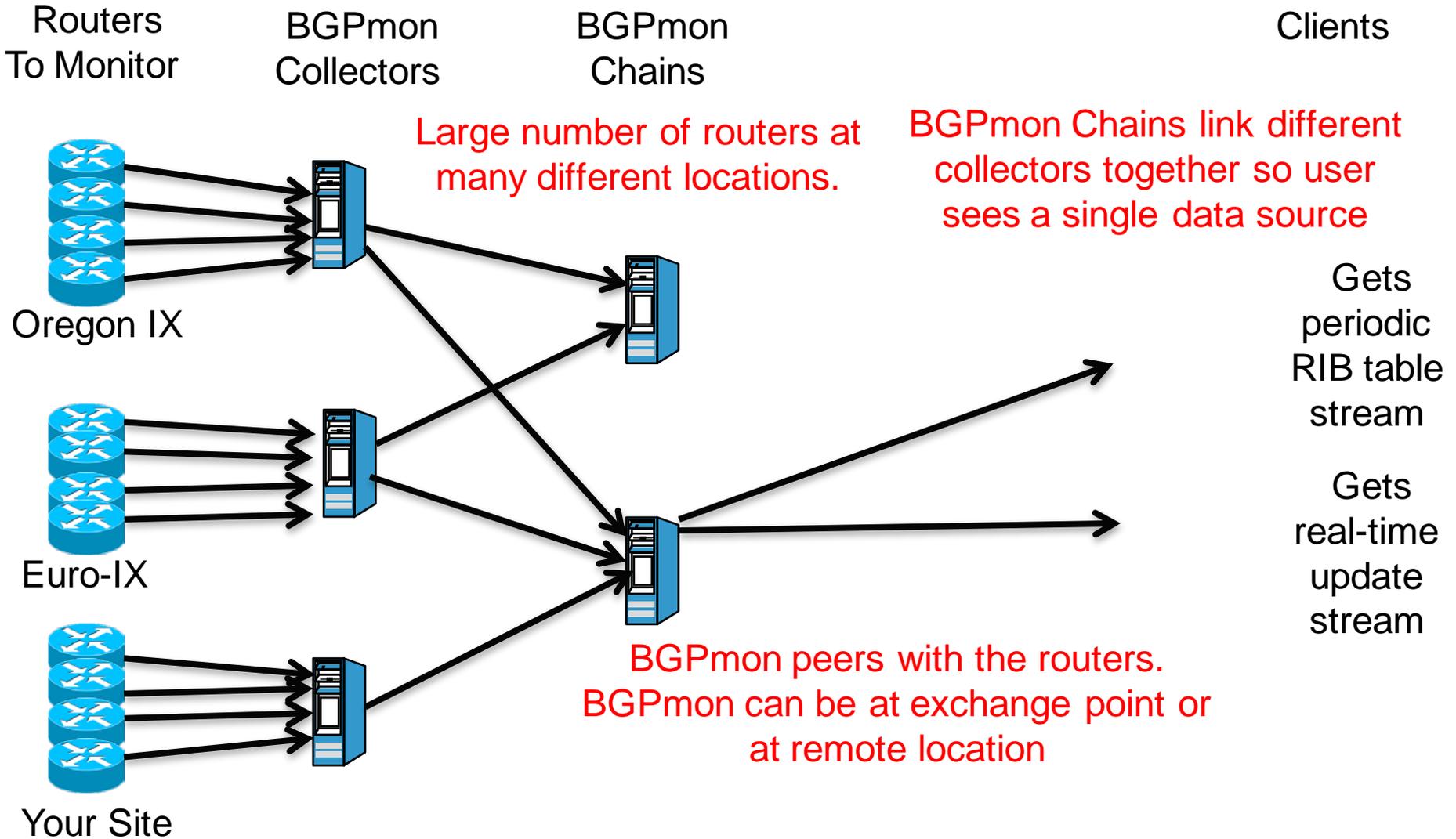
# Real-Time Data Access

- Fundamental Changes In Monitoring Infrastructure
  - Provide real-time access to route tables and incremental updates
  - Manage table transfers and update bursts from routers
  - Scale to large numbers of BGP peers
  - Scale to vast numbers of clients
  - Protect monitoring system from slow or misconfigured clients
- Requires Software Dedicated to Monitoring
  - BGPmon: dedicated software for monitoring and real-time delivery
  - XML format for resulting data with integrated updates and tables
- **BGPmon overcomes both design and deployment challenges**

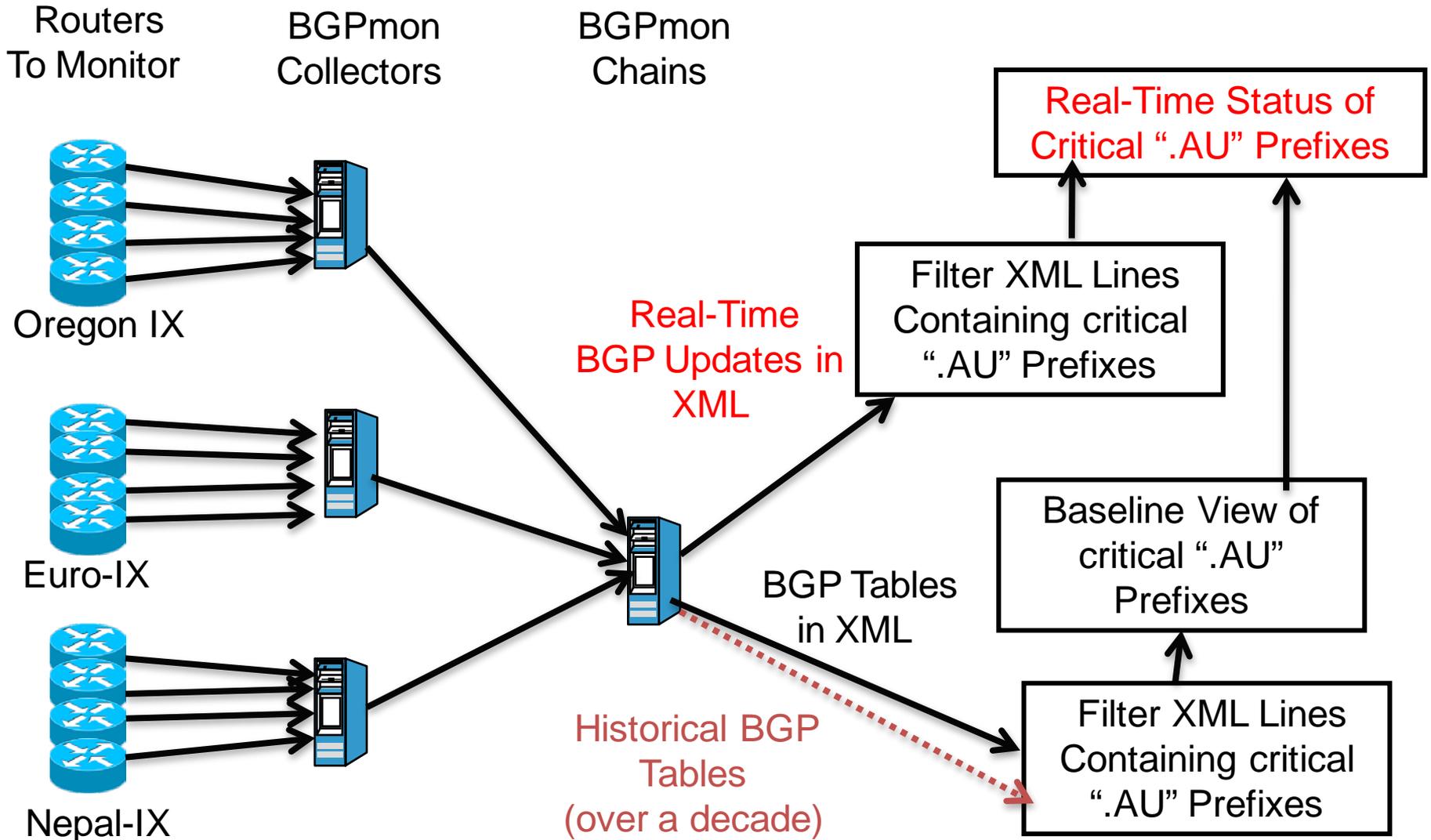
# BGPmon Architecture



# BGPmon Base Infrastructure



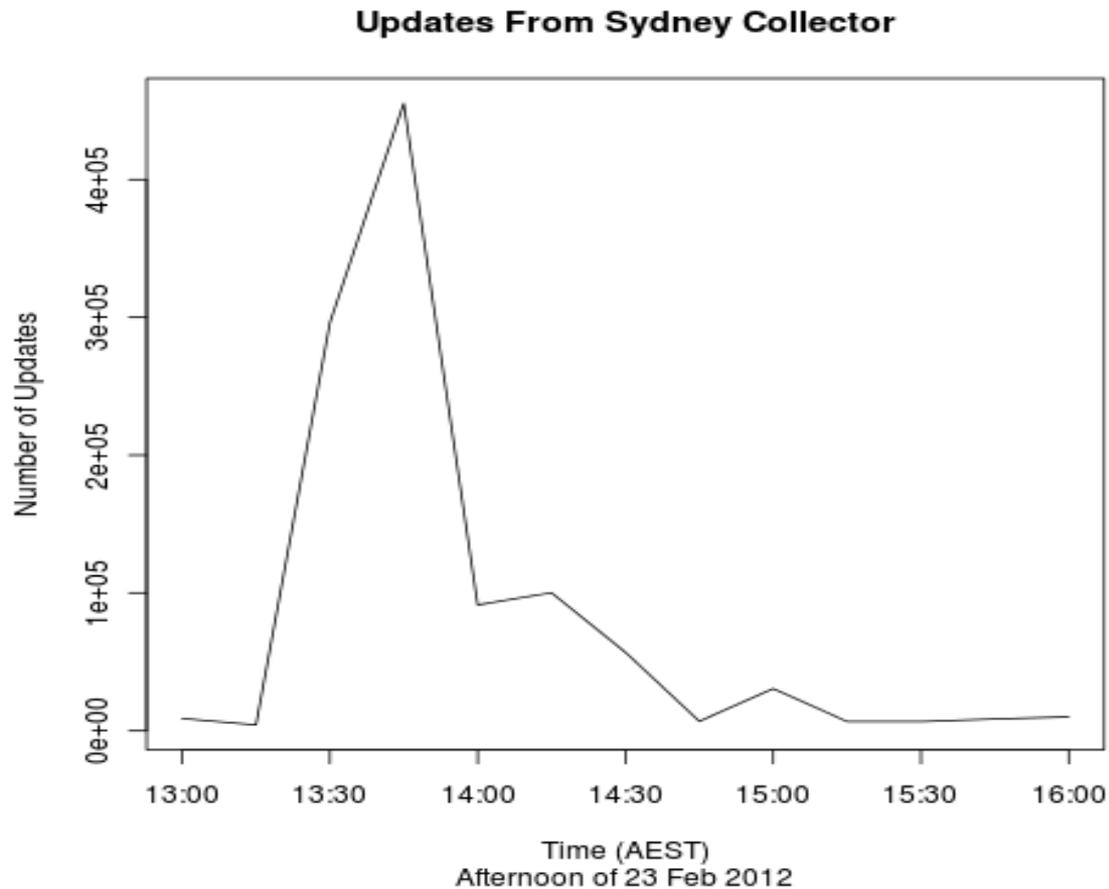
# Australia Vantages: Monitoring Australian Critical Infrastructure



# Feb 23<sup>rd</sup> Monitoring Data

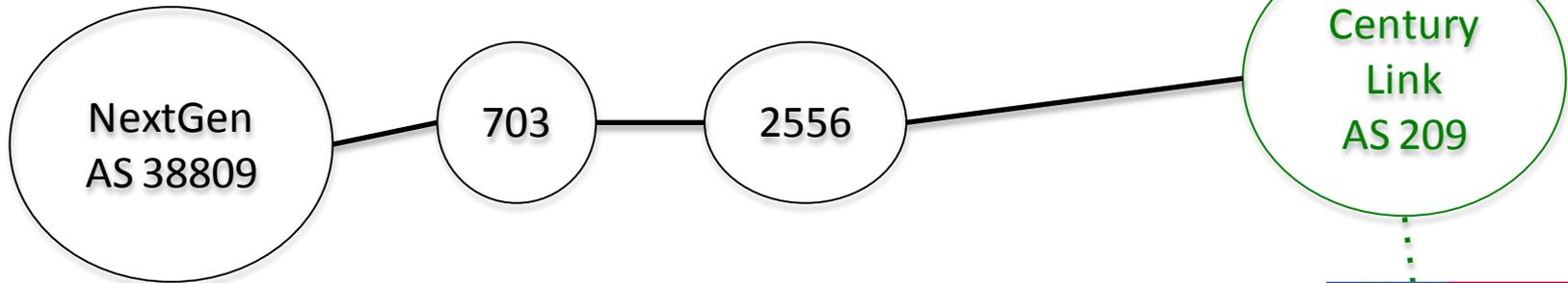
- System planned for completion in September 2012
  - Route collector in Sydney and remote peering with Telstra
  - Alpha software running at Colorado State
- Observed the behavior immediately.
  - Press reports place the event start at 1:40 AEDT.
  - Our data also suggests the event began much earlier
  - We could have issued a warning at least several minutes before.
- Observed a dramatic spike in routing activity.
  - Between 1:15 and 1:30 Sydney observed 4,215 updates
  - Between 1:30 and 1:45 Sydney observed 296,089 updates
  - Not difficult anomaly to detect!.

# The Raw Data From Sydney



# Australia to US DoD

## 13:00 AEDT



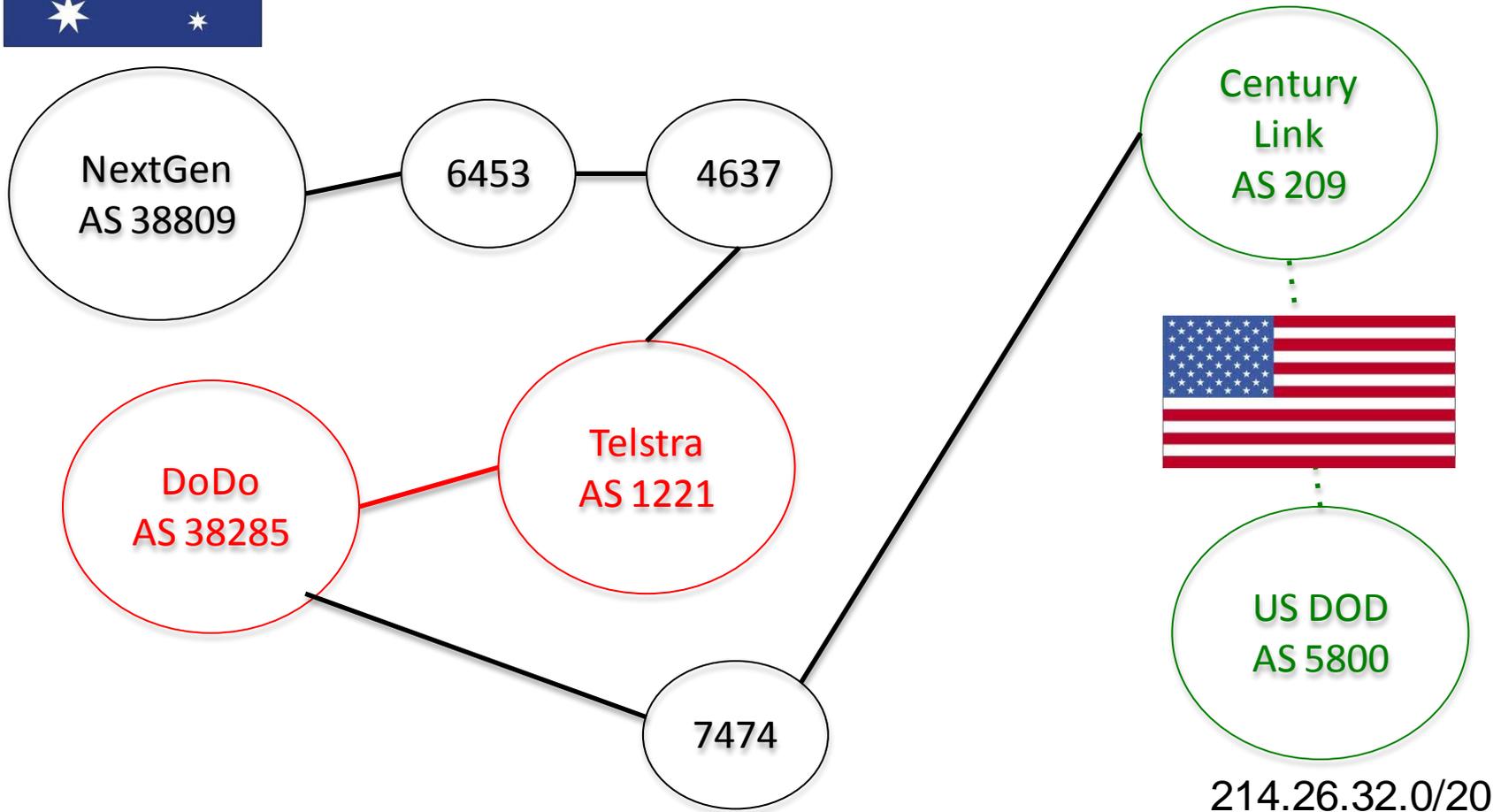
Route from the 13:00 route table  
Collected in Sydney by RouteViews



214.26.32.0/20

# Australia to US DoD

## 13:59:52 AEDT



# Recent/Wrap-Up Results

- New BGP Data Archive
  - ASCII BGPdump format available directly
  - Archived XML Data
  - Data organized by peer or by date

<http://bgpmon.netsec.colostate.edu/>
- New Open Source XML Tools
  - Perl modules to read and parse XML
  - Easily available on CPAN

<http://search.cpan.org/~bgpmon/>
- Critical Prefix Finder
  - Tool for easily identifying critical prefix
  - Jointly developed with CERT Australia

# Questions