AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

The Role of CERT Australia in Infrastructure Monitoring

Simeon Simes
CERT Australia

Australian Government
Attorney-General's Department

CERT Australia

- CERT Australia, managed by the Attorney-General's Department, is Australia's national CERT

- Responsible for technical coordination & incident response with the private sector during a cyber incident

- Provides information on cyber threats and vulnerabilities to critical infrastructure and systems of national interest (SNI)

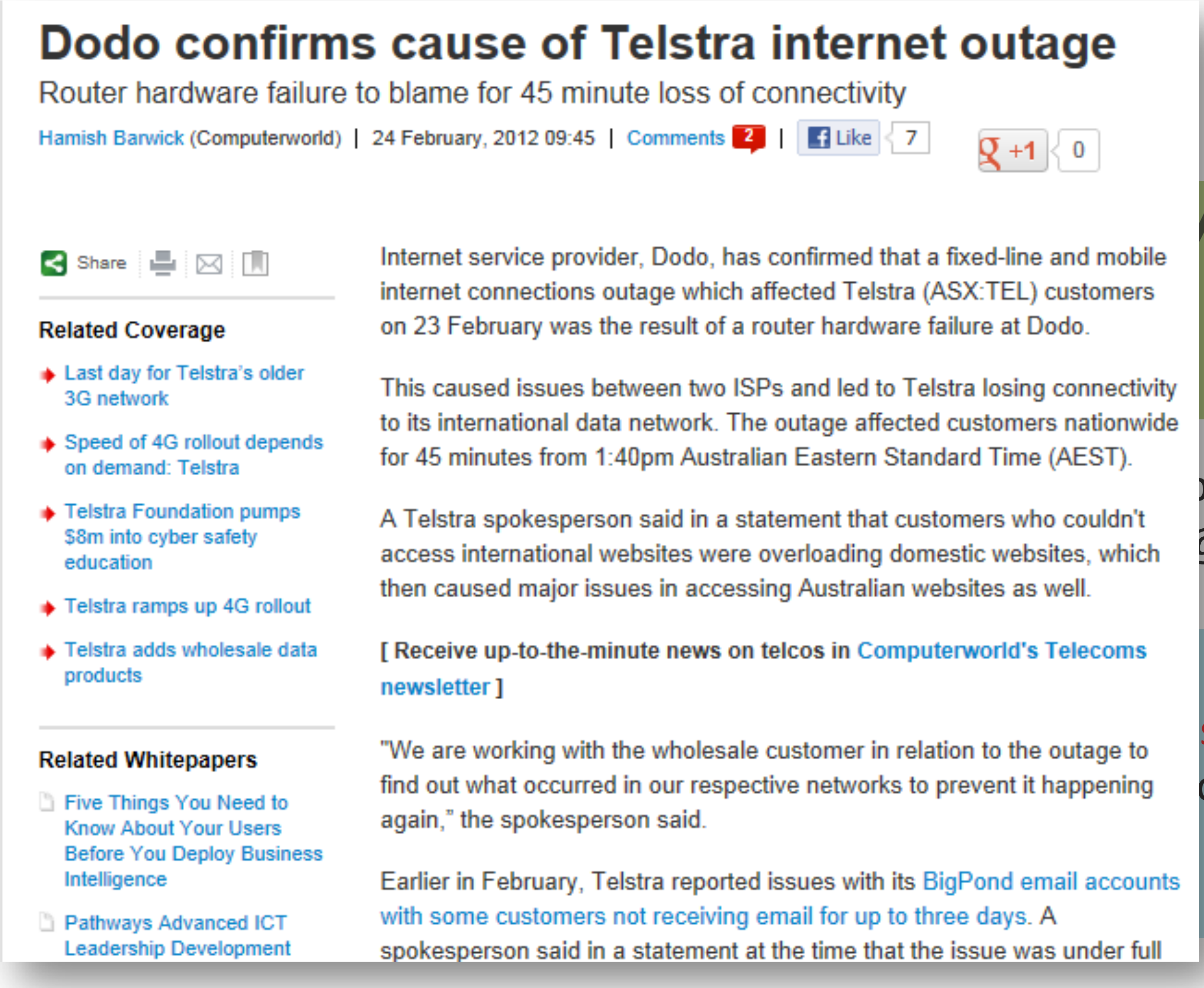
Outline – BGPmon Project

- Motivation and Objectives
- Improving Regional BGP Data Collection
- Accessing the BGP Data
- Participating in the Project

Motivation

- How does the Internet control plane affect Australian critical infrastructure and SNI.
- Part of the role of CERT Australia supporting critical infrastructure.
- To contribute as part a broader international effort looking to understand global routing infrastructure.

Major Events Do Occur



Dodo confirms cause of Telstra internet outage

Router hardware failure to blame for 45 minute loss of connectivity

Hamish Barwick (Computerworld) | 24 February, 2012 09:45 | Comments 2 | Like 7 +1 0

Related Coverage

- Last day for Telstra's older 3G network
- Speed of 4G rollout depends on demand: Telstra
- Telstra Foundation pumps $8m into cyber safety education
- Telstra ramps up 4G rollout
- Telstra adds wholesale data products

Related Whitepapers

- Five Things You Need to Know About Your Users Before You Deploy Business Intelligence
- Pathways Advanced ICT Leadership Development

Internet service provider, Dodo, has confirmed that a fixed-line and mobile internet connections outage which affected Telstra (ASX:TEL) customers on 23 February was the result of a router hardware failure at Dodo.

This caused issues between two ISPs and led to Telstra losing connectivity to its international data network. The outage affected customers nationwide for 45 minutes from 1:40pm Australian Eastern Standard Time (AEST).

A Telstra spokesperson said in a statement that customers who couldn't access international websites were overloading domestic websites, which then caused major issues in accessing Australian websites as well.

[Receive up-to-the-minute news on telcos in Computerworld's Telecoms newsletter]

"We are working with the wholesale customer in relation to the outage to find out what occurred in our respective networks to prevent it happening again," the spokesperson said.

Earlier in February, Telstra reported issues with its BigPond email accounts with some customers not receiving email for up to three days. A spokesperson said in a statement at the time that the issue was under full

ouTube

roke the internet?

@Telstra both down

s as,

om 1997,

Christmas

Infrastructure Monitoring Questions

- Given a network outage report...
- Is there an impact on key sectors such a financial, utilities, industry, or government?
- What is the geographic range of the event?
- Is it an unintentional error or something else?
- Who is responsible and who needs to act to repair it?

Media Reports on the Outage

smh.com.au
The Sydney Morning Herald

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.

itWire.
connecting technology professionals

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.

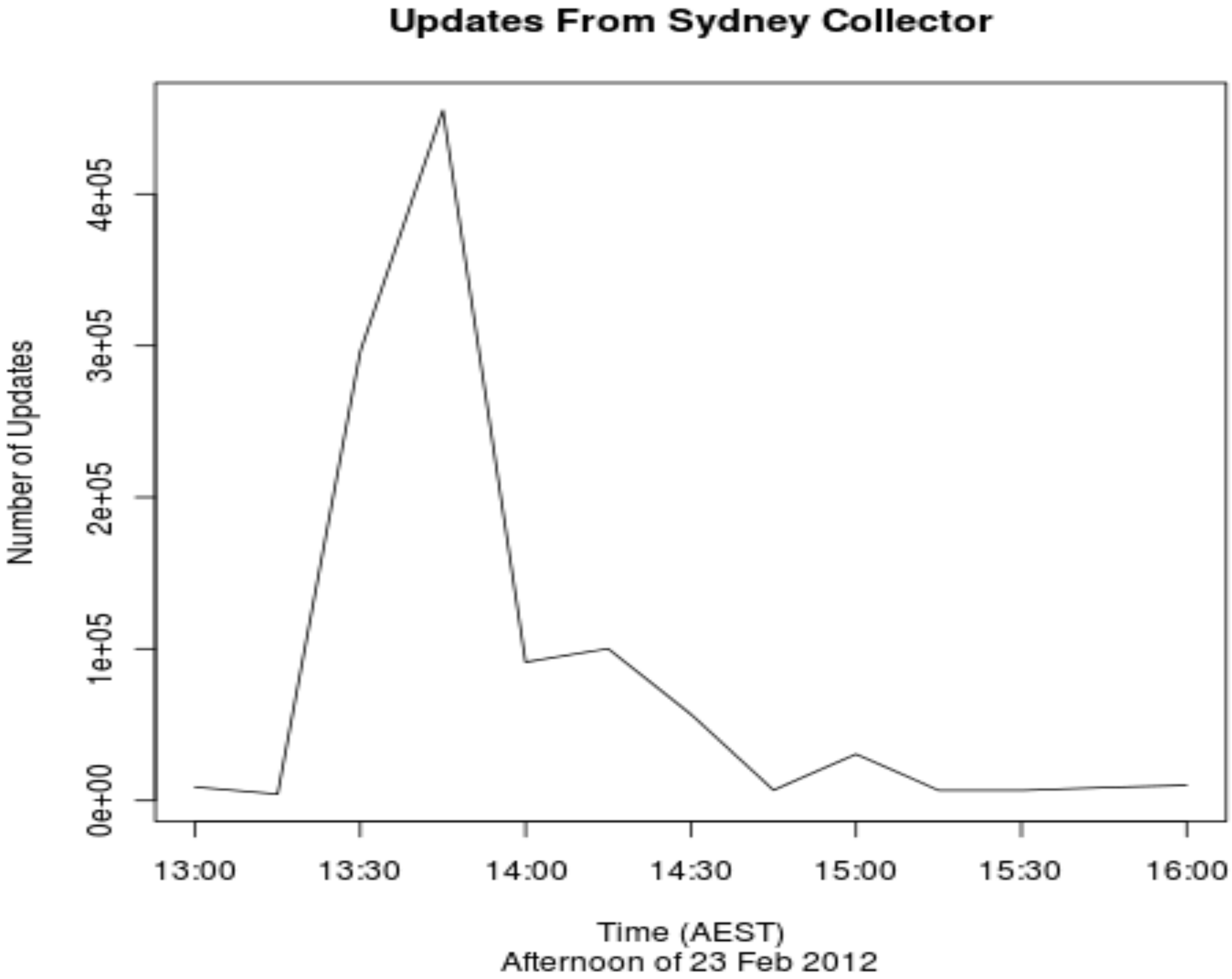
23 Feb Monitoring Data

- From the system planned for operation end of September 2012
  - Route collector in Sydney and remote peering with Telstra
  - Alpha software running at Colorado State

- Observed the behaviour immediately.
  - Press reports place the event start at 1:40 AEDT.
  - Colorado State's data also suggests the event began much earlier
  - This issue could have been detected 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
  - A 6,925% increase in activity.

The Raw Data From Sydney



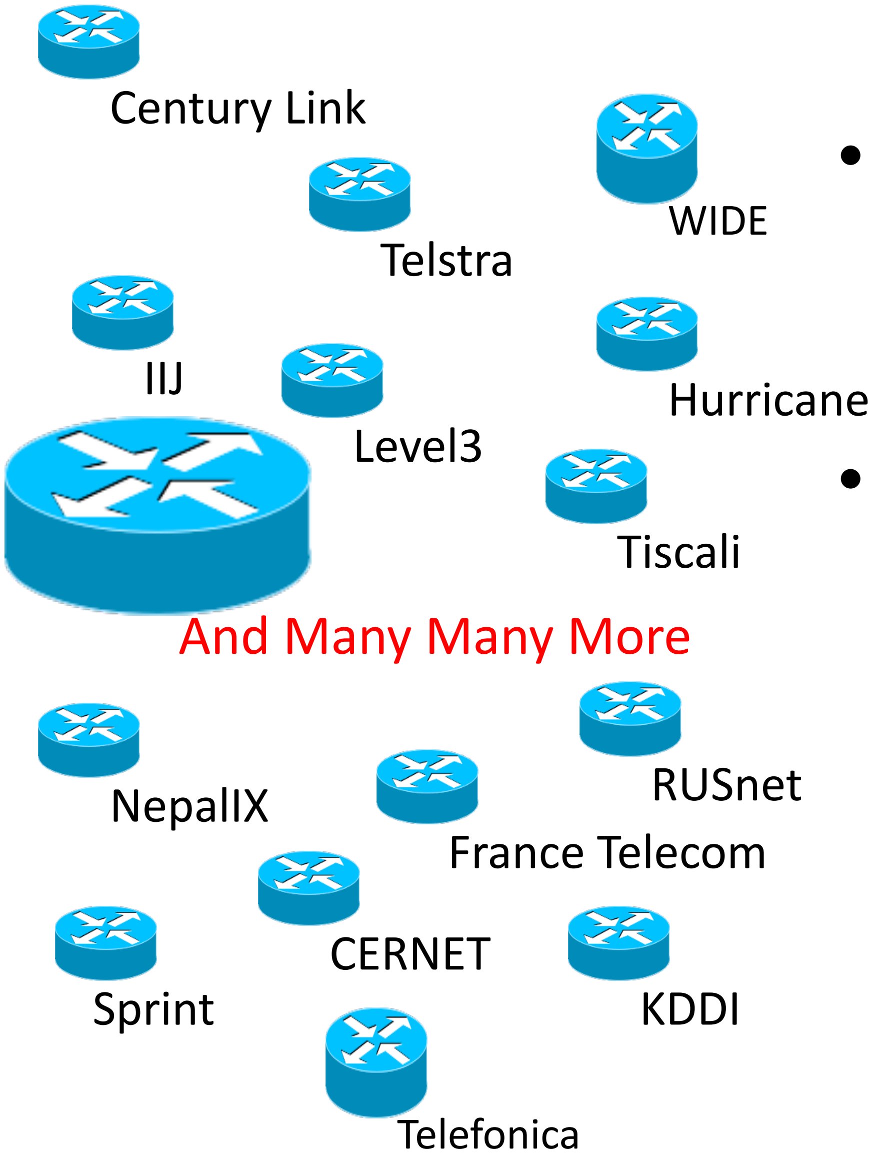
Broad Project Goals

- Better Regional Data Collection
  - Build on existing global data collection (RouteViews)
  - Add views into regionally relevant networks
  - Regional Analysis not dependent on remote links
- Better Data Access
  - Local archived data available to public
  - Considering real-time access to data

Outline

- Motivation and Objectives
- Improving Regional BGP Data Collection
- Accessing the BGP Data
- Participating in the Project

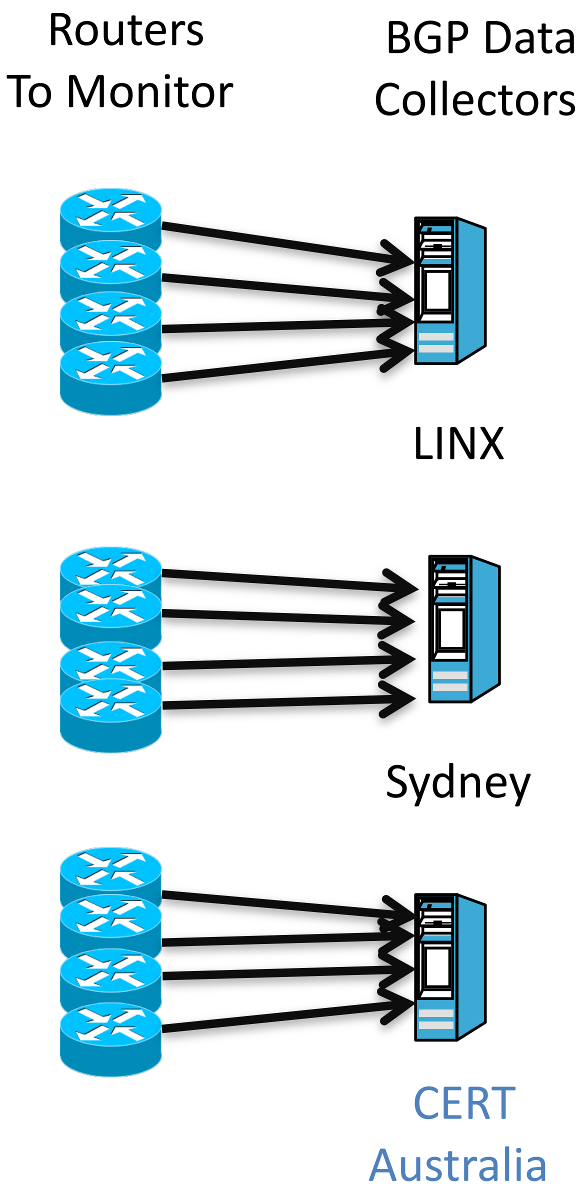
How BGP Data Collection Works (1/3)



- ISPs around the world offer to provide BGP data

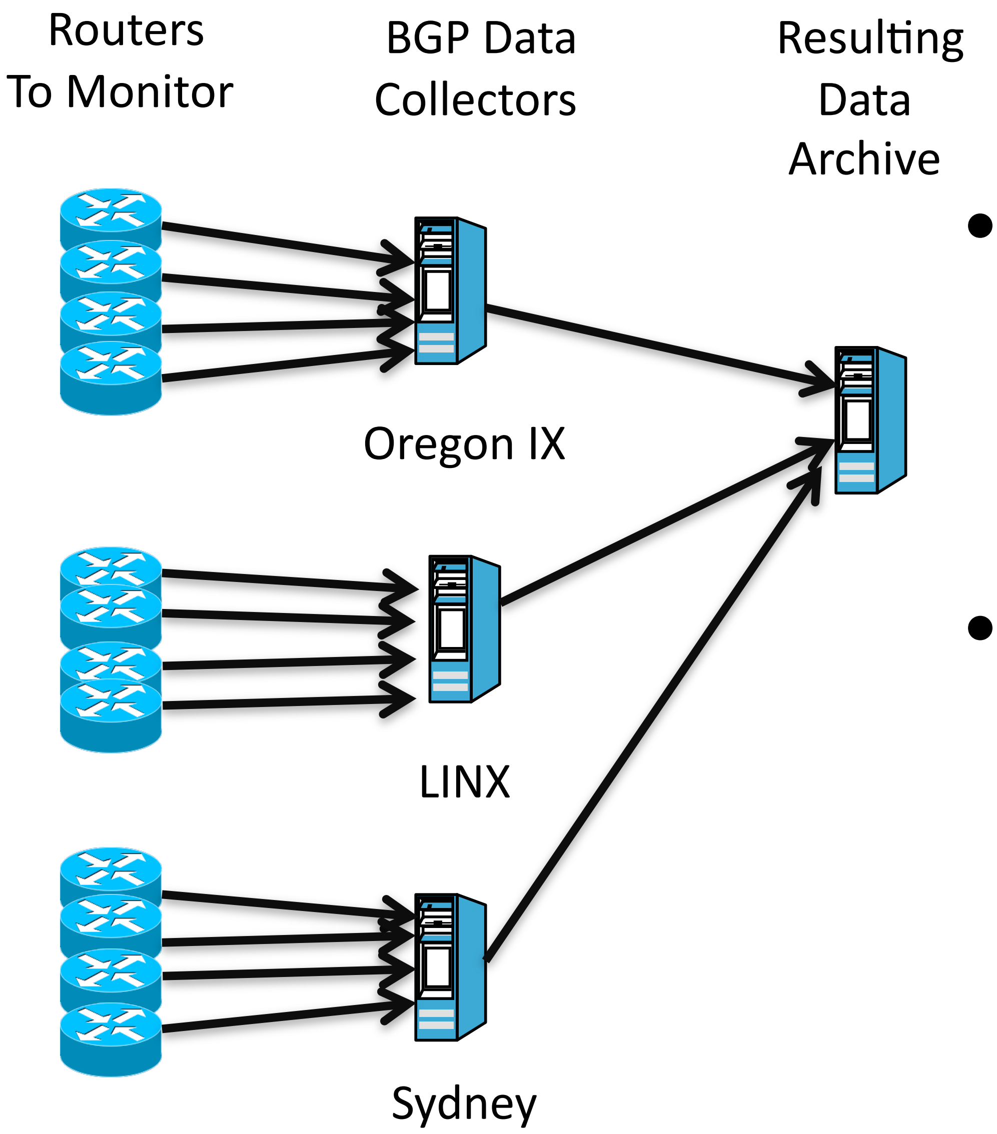
- Agree data can be made publically available to any operator or researcher

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

Australian Collector

- Peer With The CERT Australia BGP Data Collector
  - Dedicated IPv4 and IPv6 Peering
- Data Collector Appears As Just Another Peer
  - Imitates a BGP router, but never announces routes
    - No code to send BGP updates!
    - MD5 password
    - A route filter can also be used
  - Prefer full route tables (configure us as a customer)
  - Logs every update received
- Ensures your view is included in the data set – help with post incident analysis

Outline

- Motivation and Objectives
- Improving Regional BGP Data Collection
- Accessing the BGP Data
- Participating in the Project

Public Access to BGP Data

- Archived Data Available Online
  - One month of data uncompressed
  - Older compressed data also available

    http://bgp.cert.gov.au

- Links To Global BGP Research Efforts
  - Enhances the global view of Australian prefixes

XML-Based Format for Representing BGP Messages (XFB) & BGPDUMP Format

```
ARCHIVER|1346459566|OPENED|CREATE_NEW_FILE
BGP4MP|1346456743|A|89.149.178.10|3257|110.172.55.0/24|3257 6453 4755 45775
BGP4MP|1346456743|A|89.149.178.10|3257|223.223.128.0/20|3257 6453 4755 45775
BGP4MP|1346456743|A|89.149.178.10|3257|113.21.64.0/20|3257 6453 4755 45775
ARCHIVER|1346459566|CLOSED|RESET_START_TIME
ARCHIVER|1346459567|OPENED|RESUMING_OUTPUT_TO_FILE
BGP4MP|1346457125|W|89.149.178.10|3257|2.94.171.0/24
ARCHIVER|1346459567|CLOSED|RESET_START_TIME
ARCHIVER|1346459568|OPENED|RESUMING_OUTPUT_TO_FILE
BGP4MP|1346457180|W|89.149.178.10|3257|184.159.130.0/23
ARCHIVER|1346459568|CLOSED|RESET_START_TIME
ARCHIVER|1346459570|OPENED|RESUMING_OUTPUT_TO_FILE
BGP4MP|1346457401|W|89.149.178.10|3257|184.159.130.0/23
ARCHIVER|1346459570|CLOSED|RESET_START_TIME
ARCHIVER|1346459570|OPENED|RESUMING_OUTPUT_TO_FILE
BGP4MP|1346457406|A|89.149.178.10|3257|210.79.55.0/24|3257 3561 3561 3561 3561 4637 4637
4637 4637 9901 9901 9901 4768 38833
ARCHIVER|1346459570|CLOSED|RESET_START_TIME
…
ARCHIVER|1346459571|OPENED|RESUMING_OUTPUT_TO_FILE
ARCHIVER|1346459930|OPENED|RESUMING_OUTPUT_TO_FILE
BGP4MP|1346458476|A|89.149.178.10|3257|63.107.117.0/24|3257 3356 6517 11007
ARCHIVER|1346459930|CLOSED|ROLL_INTERVAL_REACHED
```

Outline

- Motivation and Objectives
- Improving Regional BGP Data Collection
- Accessing CERT Australia BGP Data
- Participating in the CERT Australia Project

Seeking Your Input On

- Adding additional peers and data sources
  - What data is critical?
  - Will you provide data?

- Making the data useful to operations
  - Importance of live data versus archived data?
  - Are there are data messages you want to see?

What Next

- Increasing Peers / data sources
- Provide data to researches / organisations
- Research Questions

CERT Australia

AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

Thank you

http://www.cert.gov.au

info@cert.gov.au

1300 172 499

Australian Government
Attorney-General's Department

Backup Slides

XML-Based Format for Representing BGP Messages (XFB)

```
<ASCII_MSG>
        <LENGTH>53</LENGTH>
        <TYPE value="2">UPDATE</TYPE>
        <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>
                                </AS_SEG>
                        </AS_PATH>
                </ATTRIBUTE>
                <ATTRIBUTE>
                        <LENGTH>28</LENGTH>
                        <TYPE value=“14”> MP_REACH_NLRI</TYPE>
                        <MP_REACH_NLRI>
                    …….
                        <PREFIX label="DPATH" afi="IPV6" afi_value=“2"
                    safi="UNICAST” safi_value="1”> 2001:468:d01:33/96  </PREFIX>
                </ATTRIBUTE>
</UPDATE>
```

BGP message total length

BGP message type, according to RFC 4271

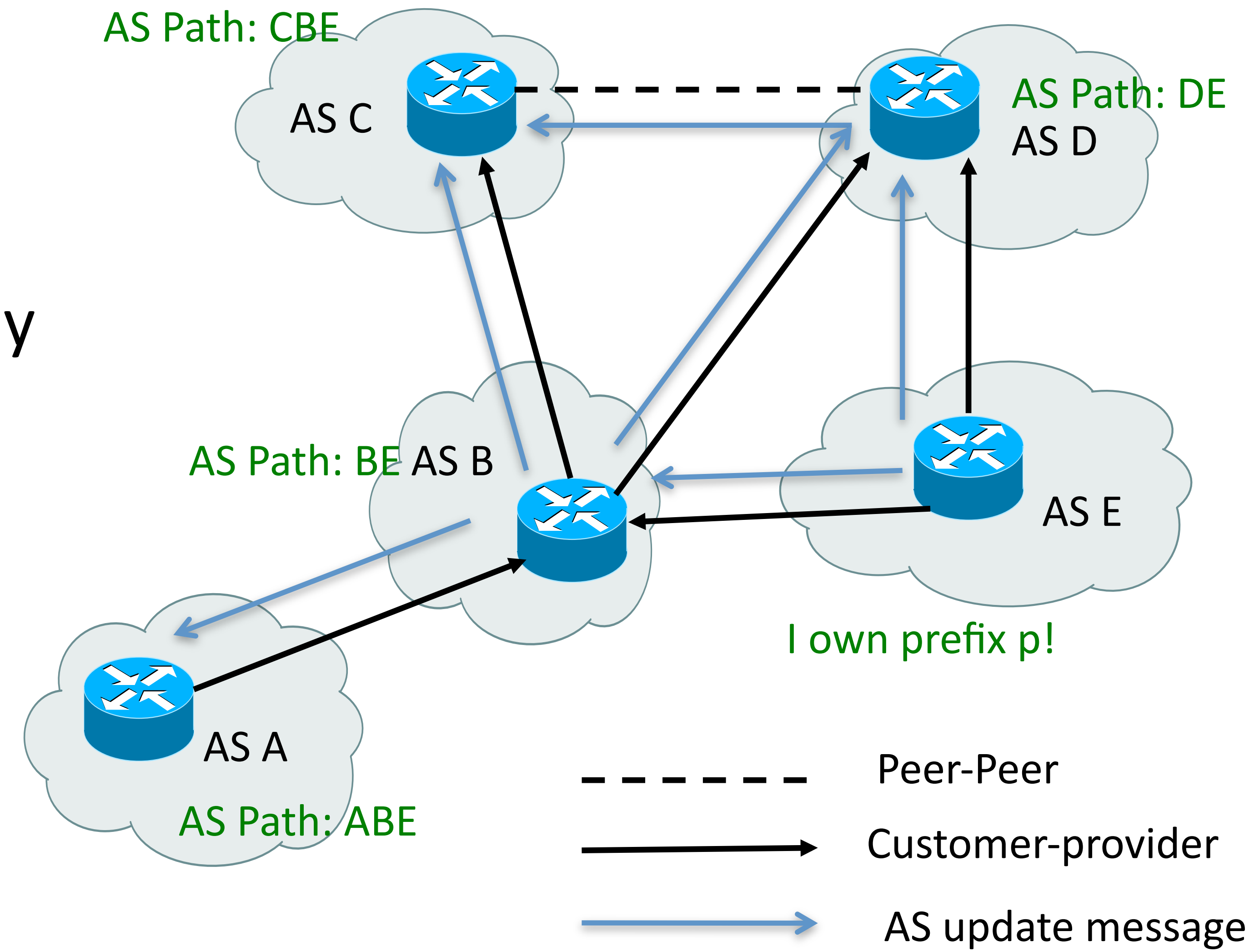
BGP AS Path data

Multi-protocol Support for v6

Announced Prefix

Brief Overview of BGP Routing

- Autonomous System (AS)
- Border Gateway Protocol (BGP)
- Profit-driven policy



AS Path: CBE

AS C

AS Path: DE

AS D

AS Path: BE

AS B

AS E

I own prefix p!

AS A

AS Path: ABE

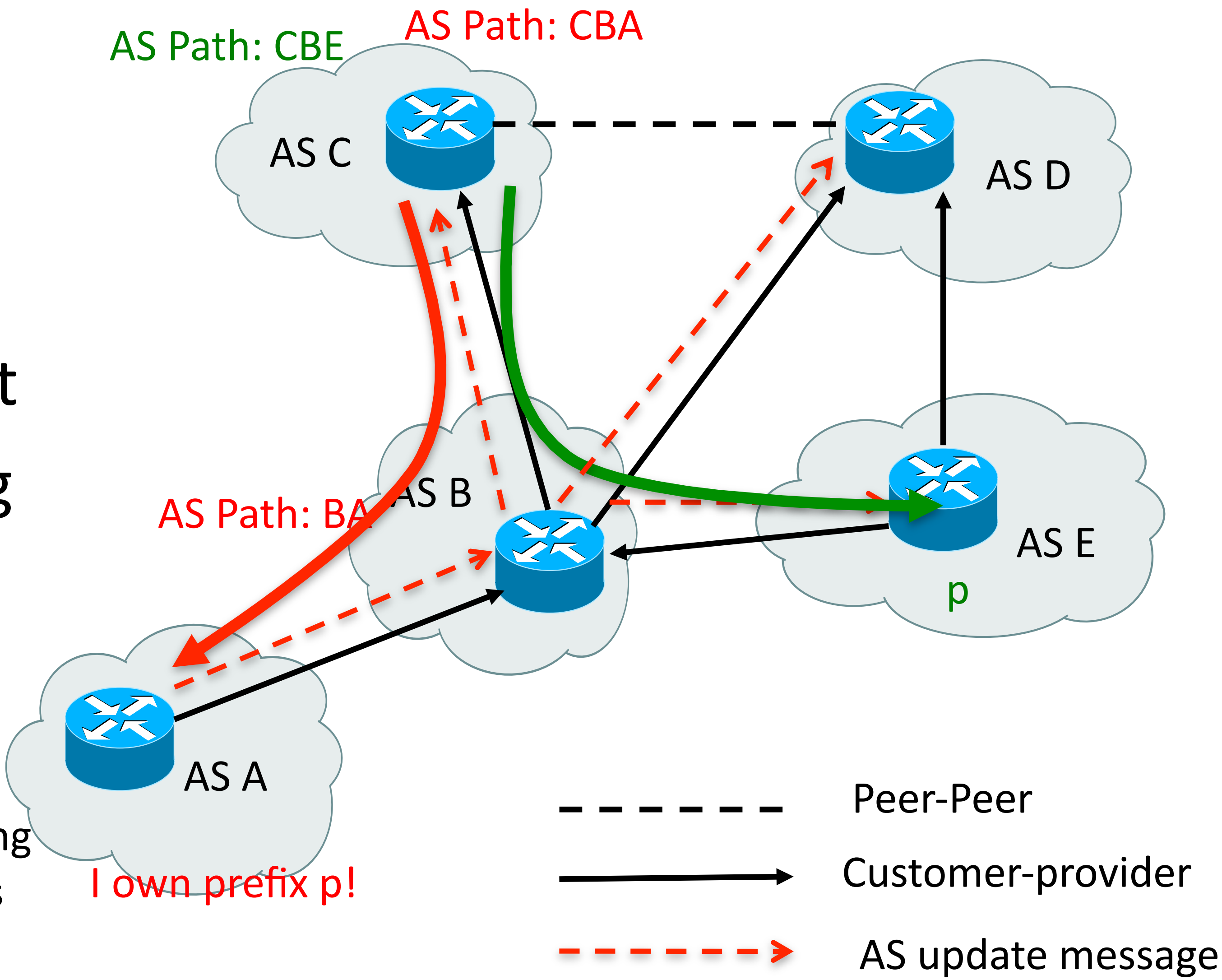
Peer-Peer

Customer-provider

AS update message

BGP Security Challenges

- BGP lacks authentication
- Fabricated AS announcement
- Prefix hijacking



April 8, 2010: Chinese ISP hijacks the Internet: China Telecom originated 37,000 prefixes not belonging to them in 15 minutes, causing massive outage of services globally.

Naïve BGP Security

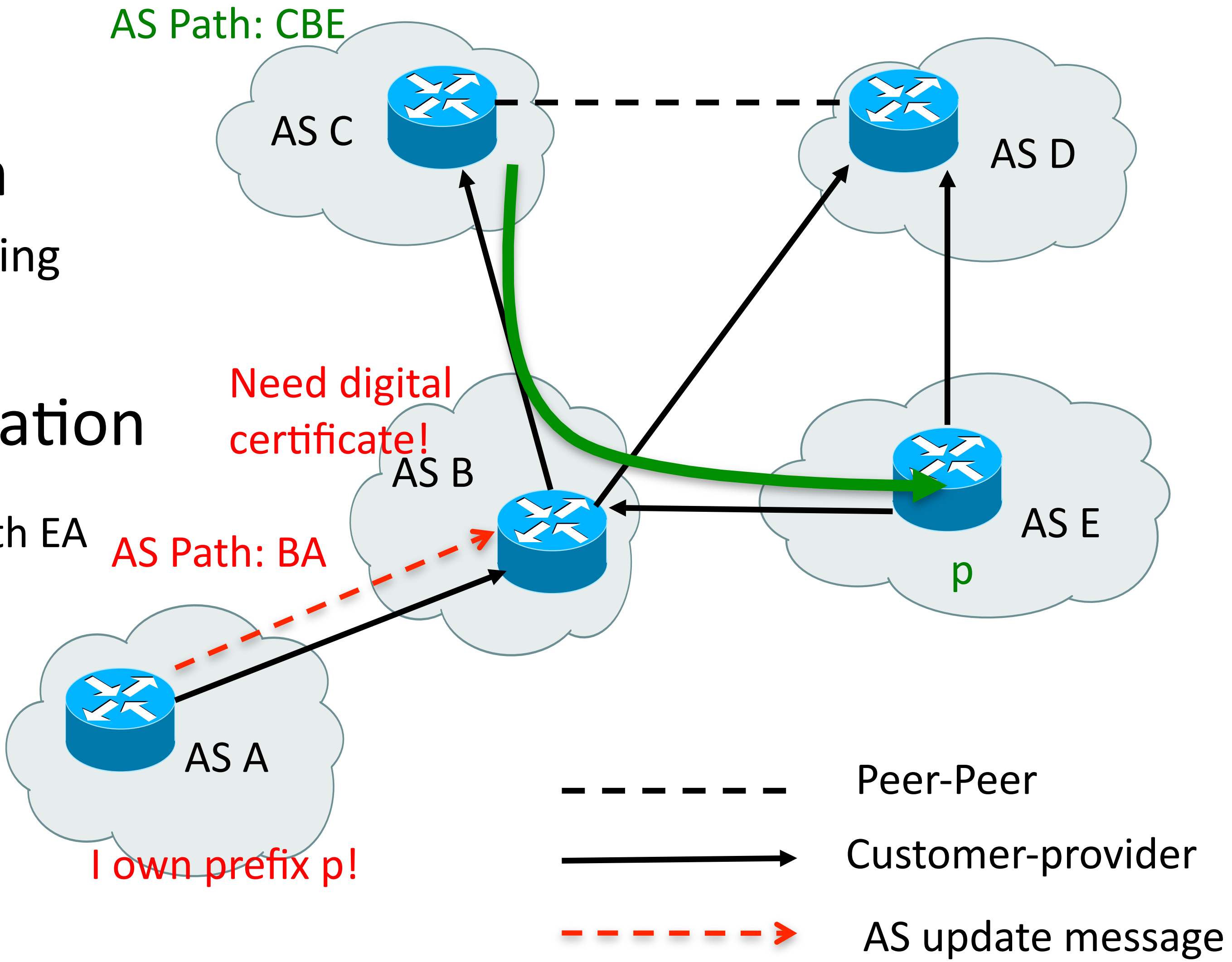
- Add Origin Authentication

  Digital certificate proving prefix ownership

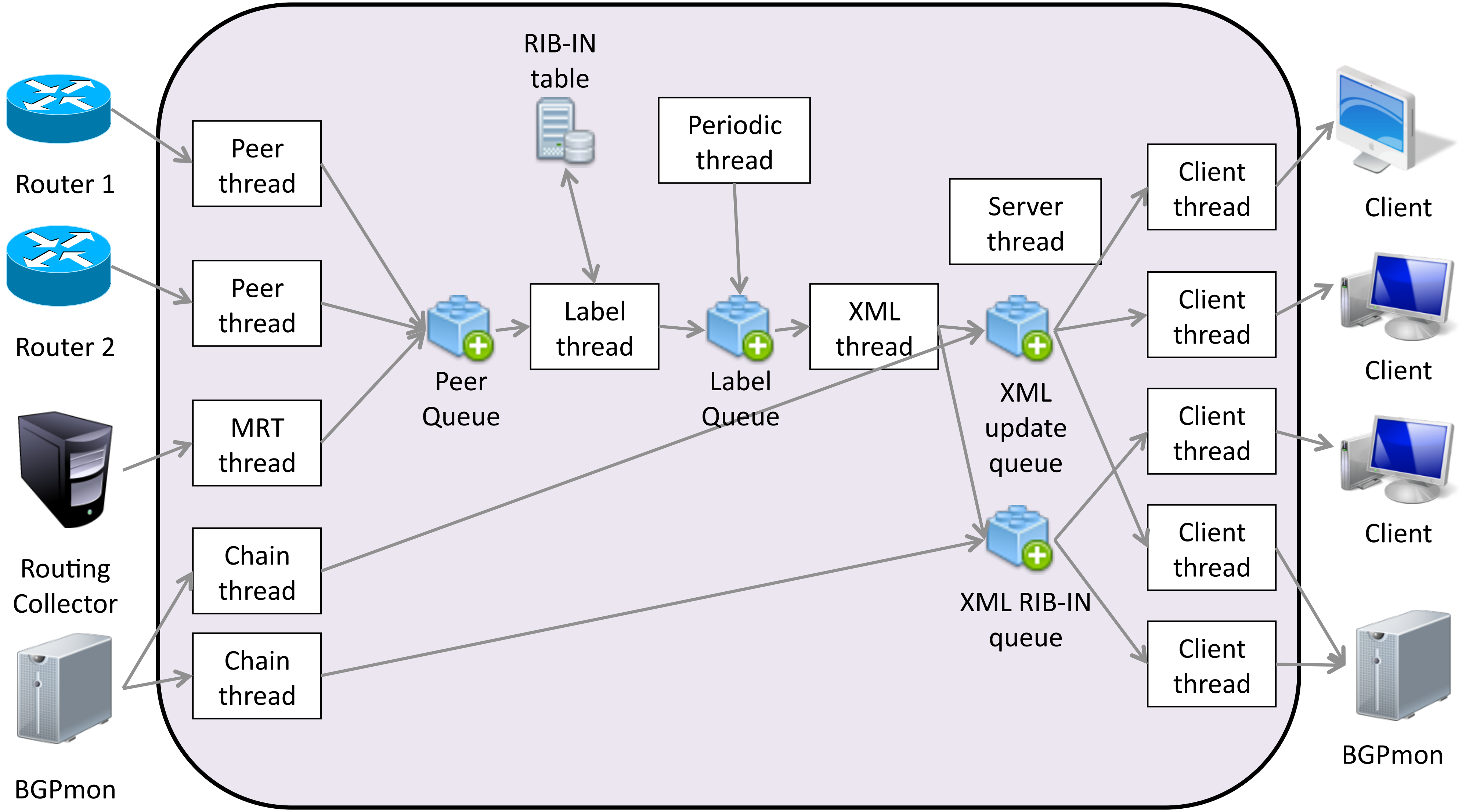
- Add Path Validation

Suppose A announces path EA

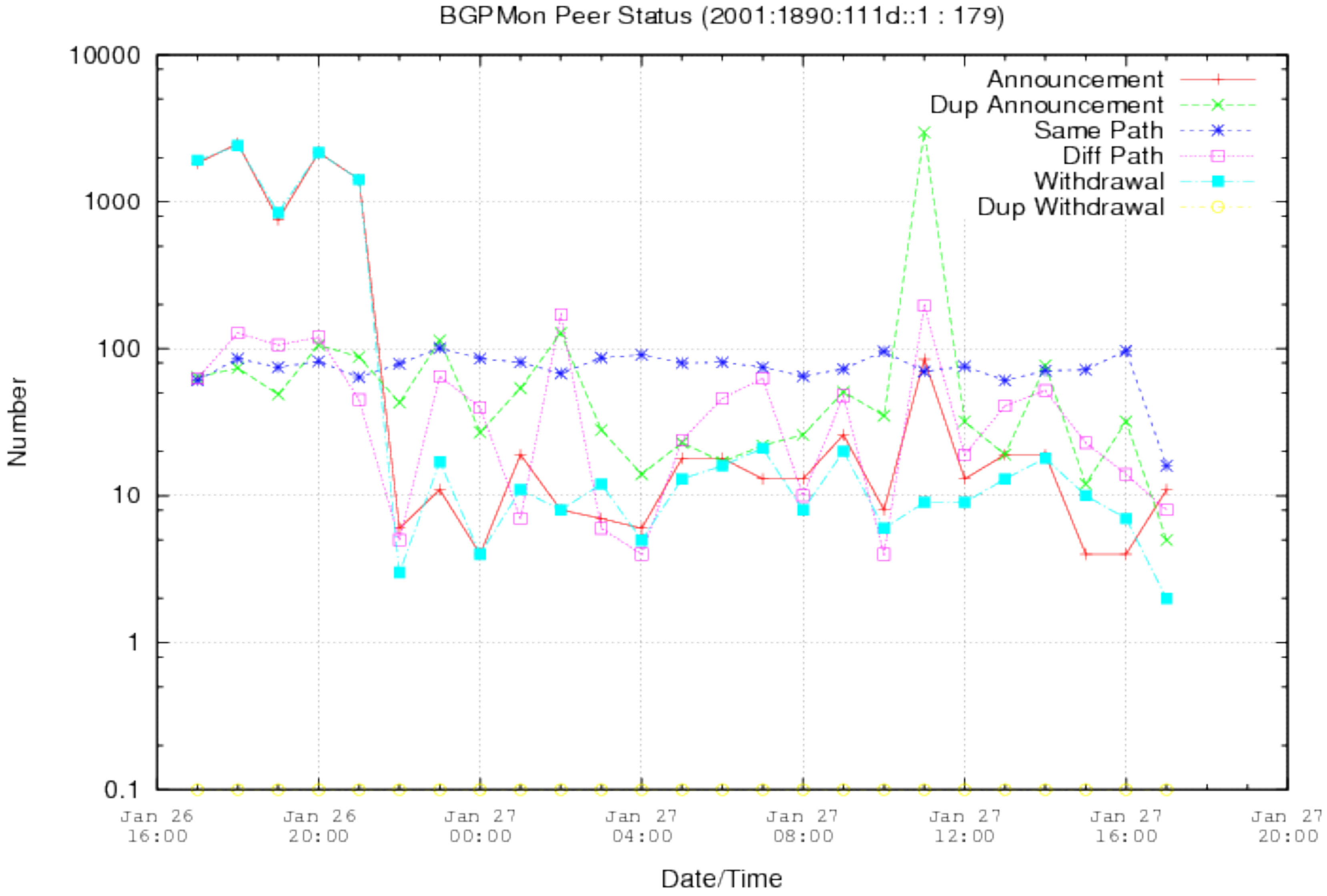
Need signature proving E announced the route to A.



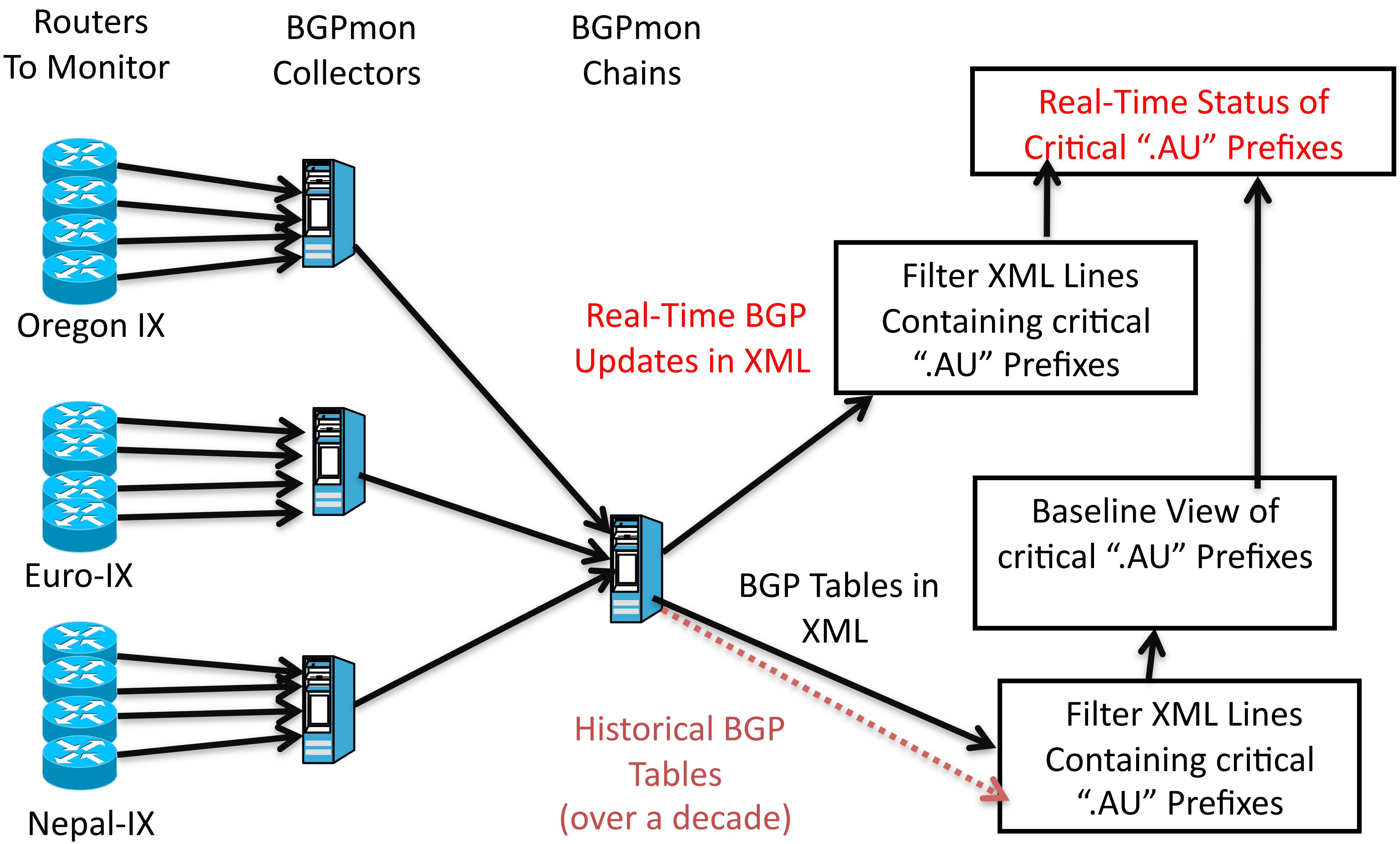
BGPmon Architecture



XML Data From One Peer



Australia Vantages: Monitoring Australian Critical Infrastructure


Routers
To Monitor
BGPmon
Collectors
BGPmon
Chains
Real-Time Status of
Critical ".AU" Prefixes
Oregon IX
Real-Time BGP
Updates in XML
Filter XML Lines
Containing critical
".AU" Prefixes
Baseline View of
critical ".AU" Prefixes
Euro-IX
BGP Tables in
XML
Filter XML Lines
Containing critical
".AU" Prefixes
Historical BGP
Tables
(over a decade)
Nepal-IX