ROVER
BGP Route Origin Verification via DNS

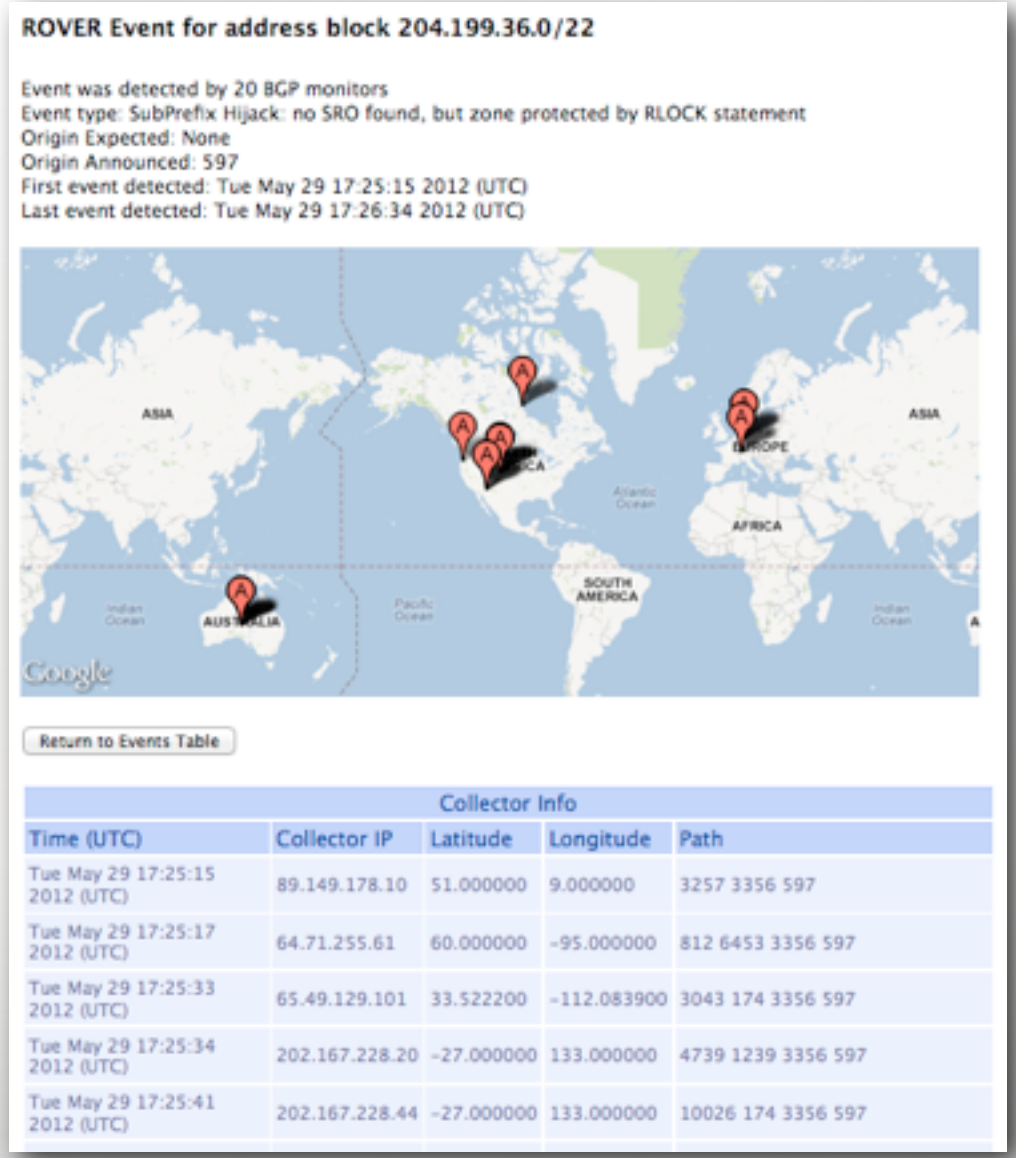
Joseph Gersch

Dan Massey, Michael Glenn, Christopher Garner

Introduction to Rover

SECURE64

- Basic Purpose:
  Protect against
  IP Hijacks
- Origin Hijacks
- Sub-prefix Hijacks
- Complementary to RPKI



ROVER Event for address block 204.199.36.0/22

Event was detected by 20 BGP monitors
Event type: SubPrefix Hijack: no SRO found, but zone protected by RLOCK statement
Origin Expected: None
Origin Announced: 597
First event detected: Tue May 29 17:25:15 2012 (UTC)
Last event detected: Tue May 29 17:26:34 2012 (UTC)

Return to Events Table

Collector Info				
Time (UTC)	Collector IP	Latitude	Longitude	Path
Tue May 29 17:25:15 2012 (UTC)	89.149.178.10	51.000000	9.000000	3257 3356 597
Tue May 29 17:25:17 2012 (UTC)	64.71.255.61	60.000000	-95.000000	812 6453 3356 597
Tue May 29 17:25:33 2012 (UTC)	65.49.129.101	33.522200	-112.083900	3043 174 3356 597
Tue May 29 17:25:34 2012 (UTC)	202.167.228.20	-27.000000	133.000000	4739 1239 3356 597
Tue May 29 17:25:41 2012 (UTC)	202.167.228.44	-27.000000	133.000000	10026 174 3356 597

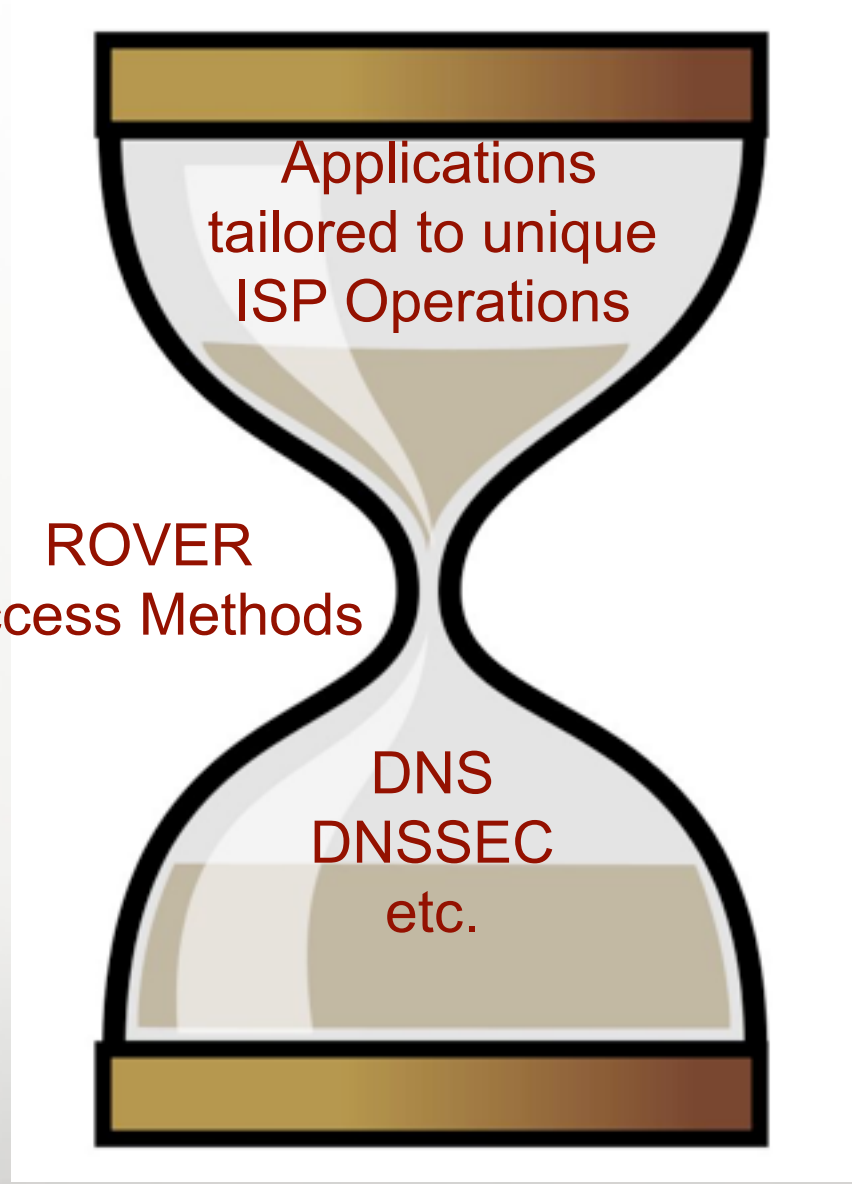
Two Basic ROVER Components

SECURE64

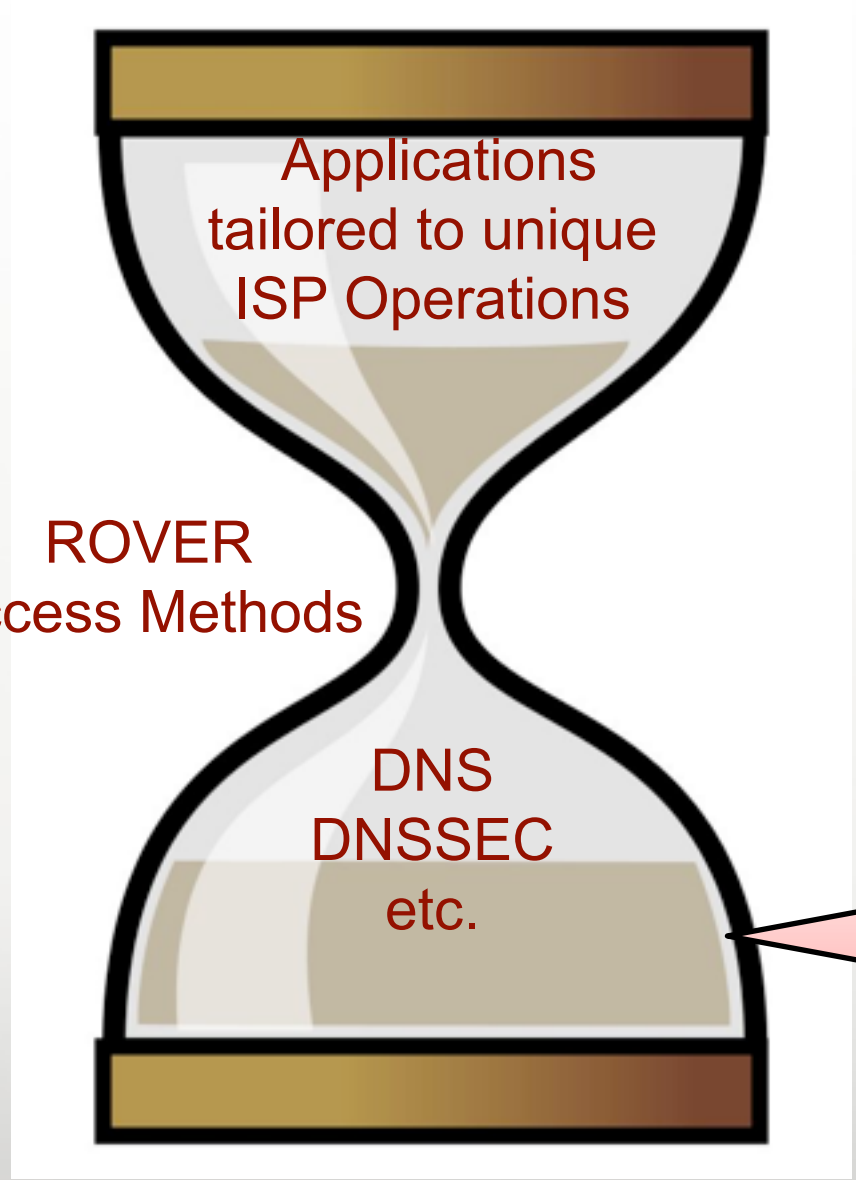
- **Publish**
  - route origin data placed in the reverse-DNS, authenticated via DNSSEC signatures
- **Access**
  - SW tools and appliances to match unique ISP operational procedures

ROVER Design Model

SECURE64



ROVER Design Model

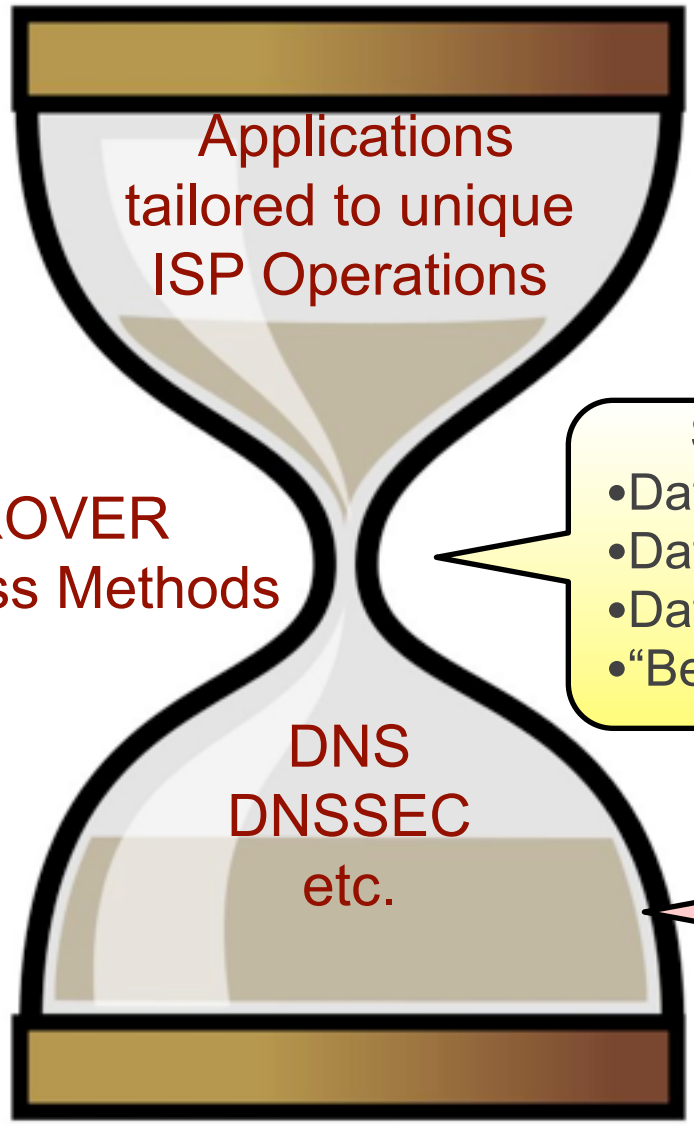


Foundations / Protocols

- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates

ROVER Design Model

SECURE64



Small set of methods:

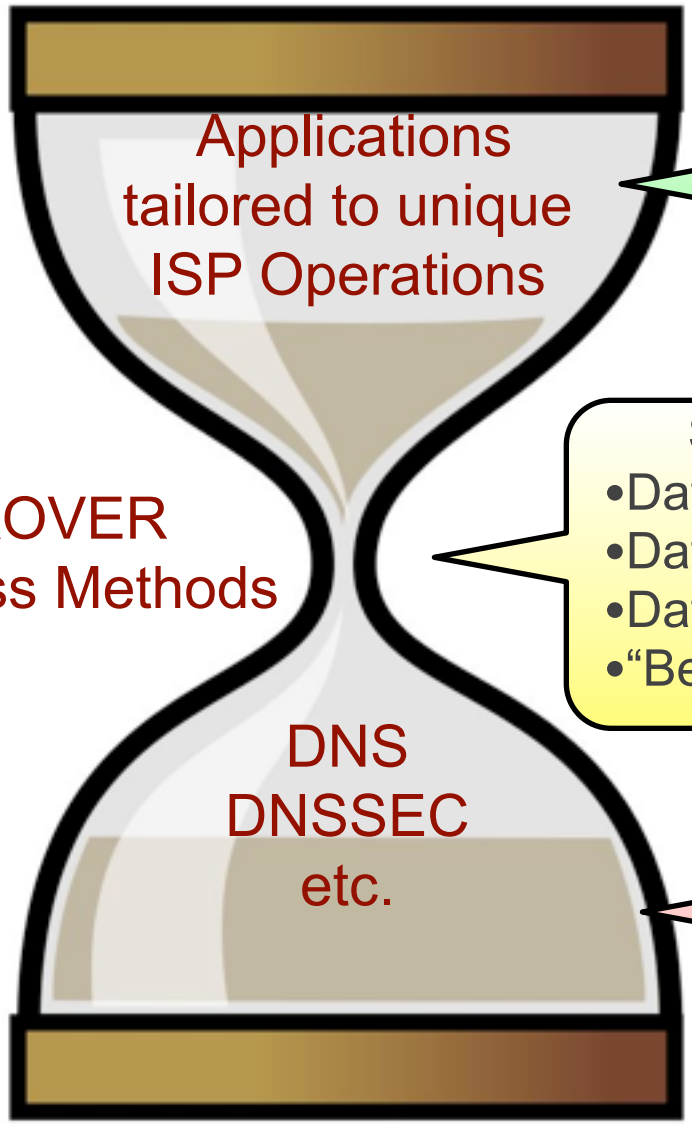
- Data Naming Convention
- Data Publishing Format
- Data Authentication
- "Best Effort" retrieval

Foundations / Protocols

- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates

ROVER Design Model

SECURE64



ISP Applications:
- verify routing DB
- build prefix filters
- interface to RTR
- real-time notification/block
- (exponential retry)

Small set of methods:
- Data Naming Convention
- Data Publishing Format
- Data Authentication
- "Best Effort" retrieval

Foundations / Protocols
- pre-existing DNS infrastructure
- IN-ADDR.ARPA signed with DNSSEC
- redundancy/resiliency
- real-time updates

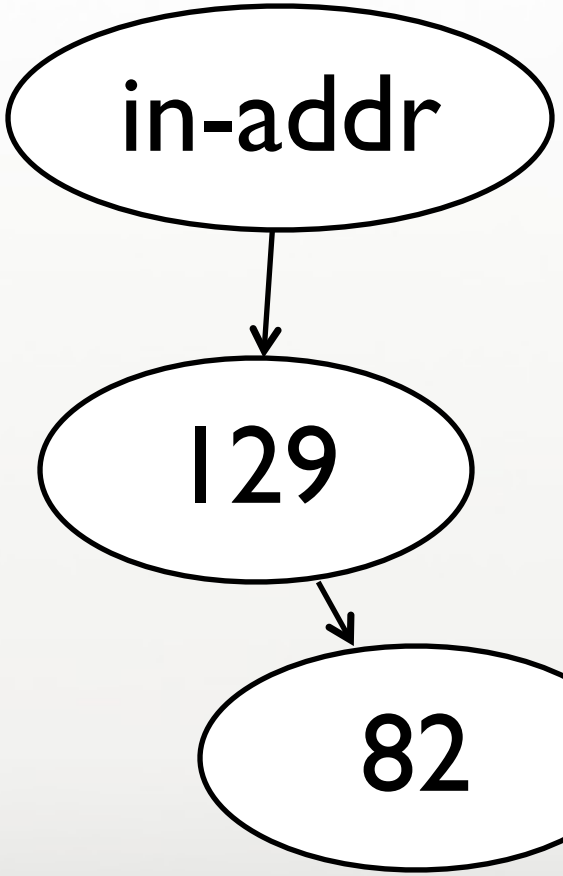
Publishing ROVER Data

Reverse DNS publishing method

SECURE64

- General-Purpose Naming convention designed to specify CIDR address blocks. Example:
  - 129.82.128.0/18 --> 0.1.m.82.129.in-addr.arpa
- 2 New DNS records
  - RLOCK: Route lock (opt in)
  - SRO: "Secure Route Origin"
- 2 Internet Drafts
  - `draft-gersch-dnsop-revdns-cidr`
  - `draft-gersch-grow-revdns-bgp`

Example:
publish origins for one /16 and four /18's



Zone file: (uses CIDR reverse-DNS naming convention)

```
$ORIGIN 82.129.in-addr.arpa
$TTL 3600

@      IN  RLOCK  ; secure entire zone
m      IN  SRO 12145  ;129.82.0.0/16
0.0.m IN  SRO 12145  ;129.82.0.0/18
1.0.m IN  SRO 12145  ;129.82.64.0/18
0.1.m IN  SRO 12145  ;129.82.128.0/18
1.1.m IN  SRO 12145  ;129.82.192.0/18

; can now directly add /24 SROs
; or can let the lower octet do it

; existing delegations

0     IN   NS    rush.colostate.edu
1     IN   NS    rush.colostate.edu
;....
255   IN   NS    rush.colostate.edu
```

RLOCK = Route LOCK (currently using TYPE65400)
SRO = Secure Route Origin (currently using TYPE65401)
Automated provisioning tools have been written

CIDR Prefix Naming

SECURE64

- Naming Convention Being Considered in IETF DNSOP
  - draft-gersch-dnsop-revdns-cidr-02.txt
- Many Uses for Naming Prefixes in Reverse DNS
  - Route Security Discussed Here
  - Attaching GeoLocation (GEO DNS RR)
  - ... And So Forth
- Seeking Your Input In The Discussion
  - dnsop@ietf.org

Publishing Call To Action

SECURE64

- Two Mechanisms to Participate
  - Publish your data in the rover.secure64.com testbed
  - Publish your data in the actual reverse DNS
- Publishing in ROVER Testbed
  - Auto-detects your prefixes
  - Allows you to confirm/customize entries
  - Builds zone file and stores in shadow reverse tree
- Publishing Your Data in Reverse DNS
  - Need to enable DNSSEC in your reverse tree
  - Add RLOCK and SRO records to your existing zone(s)
    - Optionally create new zones for ease of management
  - Does not break existing zones

Using ROVER Data

ROVER Applications

SECURE64

- Applications can access the reverse DNS records to:
  - Generate real-time alarms for a NOC
  - Verify route filters on a periodic basis
  - Perform real-time control plane adjustments
    - check a BGP announcement against the published authorized data in the reverse-DNS:
      - valid, invalid, unknown
    - interface to router and make adjustments
  - Other tools and building blocks
- Clearly the first step is simply verification of BGP announcements from the published data

Is There Data Available Now?

SECURE64

- CenturyLink and Level3 have data in the reverse DNS
- You can query for this data now:

```
dig +dnssec -t TYPE65400 199.204.in-addr.arpa

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53238
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;m.199.204.in-addr.arpa.            IN      TYPE65400

;; ANSWER SECTION:
m.199.204.in-addr.arpa.     45149 IN      TYPE65400 \# 0
m.199.204.in-addr.arpa.     45149 IN      RRSIG         TYPE65400 5 5 86400
20120628153051 20120529145853 44445 m.199.204.in-addr.arpa. M/JtnJNX6jhE/
kN0kn7WZwCmLHVvCtp/u36L60k6Q2MysBqZZ6S0QihW
NX198IeXz5MFJ0I5ippfnjMUa8ydDrusQl1mjESiAJ7iI8sAsqW0THXN
6hcMarszZaGDePtxlUKS/XrlgA6sQls3S/fumAmay8kq82UD3bsyZdek HcA=
```

Call To Action

SECURE64

- Two Mechanisms to Participate
  - Use Rover to generate real-time alarms
  - Verify your own BGP updates
- BGP Verification Application in ROVER Testbed
  - Receives RouteViews BGP data in real-time via Colorado State BGP Monitor
  - Accesses published data and performs comparison
    - In the reverse DNS
    - In the ROVER testbed
- Or access the data yourself with reverse DNS digs

Example BGP Verification Application

SECURE64

SECURE64

BGP ROVER: Route Origin Verification

jgersch
logout

Learn More | Show Zones | Publish Route Origins | Verify Route Origin | Live BGP Feed

Real-Time ROVER Verification

This page illustrates ROVER being used to verify announcements from 40+ BGP monitors located around the world. As each announcement arrives, ROVER does a DNS lookup to determine whether the route origin matches the DNS data. Results are displayed in the tables below.

This page refreshes itself every 10 seconds.

Live BGP Feed
last update: Thu May 31 21:14:11 2012 (UTC)

	announcements analyzed	VALID (origin matches DNS)	VIABLE (no DNS data found)	INVALID origin hijack detected	INVALID (subprefix hijack detected)
in-addr.arpa	537674	0	537674	0	0
testbed	537674	75	537599	0	0

Most Recent Events Detecting VALID or INVALID Announcements
click on a row to view a map of collectors involved in the event

Event Time (UTC)	Prefix	# Collectors Detecting Event	Type of Event (origin or subprefix hijack)	Origin Expected	Origin Announced
Tue May 29 17:26:34 2012	204.199.36.0/22	20	subPrefix		597
Mon May 28 18:34:33 2012	67.148.132.0/23	1	subPrefix		21864
Thu May 24 08:21:54 2012	67.148.132.0/23	1	subPrefix		21864
Thu May 24 06:29:02 2012	67.148.132.0/23	1	subPrefix		21864
Tue May 22 14:04:49 2012	152.91.0.0/16	8	subPrefix		9555
Tue May 22 13:27:12 2012	152.91.0.0/16	3	subPrefix		9555
Mon May 21 23:28:55 2012	205.159.182.0/24	3	subPrefix		6582
Mon May 21 22:08:56 2012	67.148.130.0/24	1	subPrefix		11710
Mon May 21 21:37:40 2012	67.148.130.0/24	1	subPrefix		11710
Thu May 17 17:00:46 2012	204.199.36.0/24	1	subPrefix		597

BGPMON data rate

The rate of the real-time data stream from CSU's BGPMON & Oregon Routeviews monitors.

Search Event Database

Register for Email Alerts

Questions