ROUTEVIEWS: The BGP Collector for Today's Network Operator & Researcher

ROUTEVIEWS

A collaborative router looking glass to share BGP views among network operators and researchers.

ROUTEVIEWS

A collaborative router looking glass to share BGP views among network operators and researchers.

RouteViews was founded at the University of Oregon's Advanced Network Technology Center (ANTC) in 1995. Data archives began in 1997 and amount to 22TBs (compressed) today.

ROUTEVIEWS

A collaborative router looking glass to share BGP views among network operators and researchers.

RouteViews was founded at the University of Oregon's Advanced Network Technology Center (ANTC) in 1995. Data archives began in 1997 and amount to 22TBs (compressed) today.

The group is currently led by the network engineering team at the University of Oregon with assistance from the Network Startup Resource Center (NSRC) group.

ROUTEVIEWS

A collaborative router looking glass to share BGP views among network operators and researchers.

RouteViews was founded at the University of Oregon's Advanced Network Technology Center (ANTC) in 1995. Data archives began in 1997 and amount to 22TBs (compressed) today.

The group is currently led by the network engineering team at the University of Oregon with assistance from the Network Startup Resource Center (NSRC) group.

NSRC

NSRC supports the growth of global Internet infrastructure by providing engineering assistance, collaborative technical workshops, training, and other resources to university, research & education networks worldwide. NSRC is partially funded by the IRNC program of the NSF and Google with other contributions from public and private organizations.

ROUTEVIEWS

A collaborative router looking glass to share BGP views among network operators and researchers.

RouteViews was founded at the University of Oregon's Advanced Network Technology Center (ANTC) in 1995. Data archives began in 1997 and amount to 22TBs (compressed) today.

The group is currently led by the network engineering team at the University of Oregon with assistance from the Network Startup Resource Center (NSRC) group.

NSRC

NSRC supports the growth of global Internet infrastructure by providing engineering assistance, collaborative technical workshops, training, and other resources to university, research & education networks worldwide. NSRC is partially funded by the IRNC program of the NSF and Google with other contributions from public and private organizations.

UNIVERSITY OF OREGON

The University of Oregon is a public research institution in Eugene, Oregon, USA founded in 1876. UO is renowned for its research prowess and commitment to teaching. Both NSRC and RouteViews are based at the UO.

ROUTEVIEWS

The Team

DAVID TEACH

ERIC SMITH

FOOTPRINT


Iceland
Finland
Sweden
Norway
Russia
United Kingdom
Canada
Poland
Germany
Ukraine
Kazakhstan
Mongolia
France
Spain
Italy
Turkey
China
South Korea
Japan
United States
Afghanistan
Iraq
Iran
Pakistan
North Atlantic Ocean
Algeria
Libya
Egypt
Saudi Arabia
India
Thailand
Mexico
Mali
Niger
Sudan
Chad
Nigeria
Ethiopia
Venezuela
Colombia
DRC
Tanzania
Indonesia
Papua New Guinea
Brazil
Peru
Angola
Bolivia
Namibia
Madagascar
Indian Ocean
South Pacific Ocean
South Atlantic Ocean
Chile
Australia
Argentina
New Zealand

FOOTPRINT

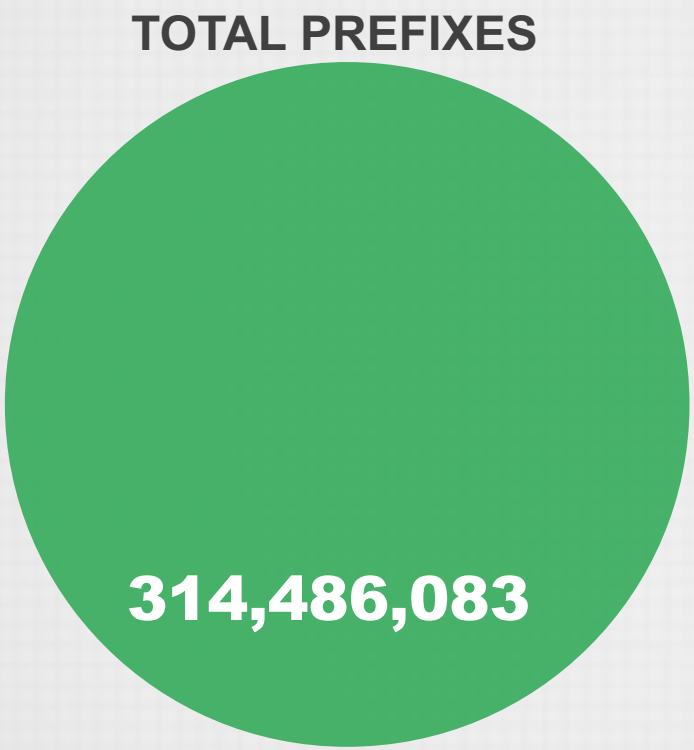
COLLECTOR LOCATIONS

- ✓ Atlanta (digital realty)
- ✓ Chicago (equinix)
- ✓ Chile
- ✓ DC (eqix)
- ✓ Eugene (Multi-hop)
- ✓ Indianapolis (MWIX)
- ✓ Johannesburg (JINX, NAPAfrica)
- ✓ London (LINX)
- ✓ Miami (flix)
- ✓ Nairobi (kixp)
- ✓ Palo Alto (PAIX)
- ✓ Perth (WAIX)
- ✓ Portland (NWAX)
- ✓ Sao Paulo (IX.br x4)
- ✓ San Francisco (sfmix)
- ✓ Singapore (Equinix SG)
- ✓ Serbia (sox)
- ✓ Stockholm (AMSIX)
- ✓ Sydney (equinix)
- ✓ Tokyo (DIX-IE)
- ✓ Cape Town

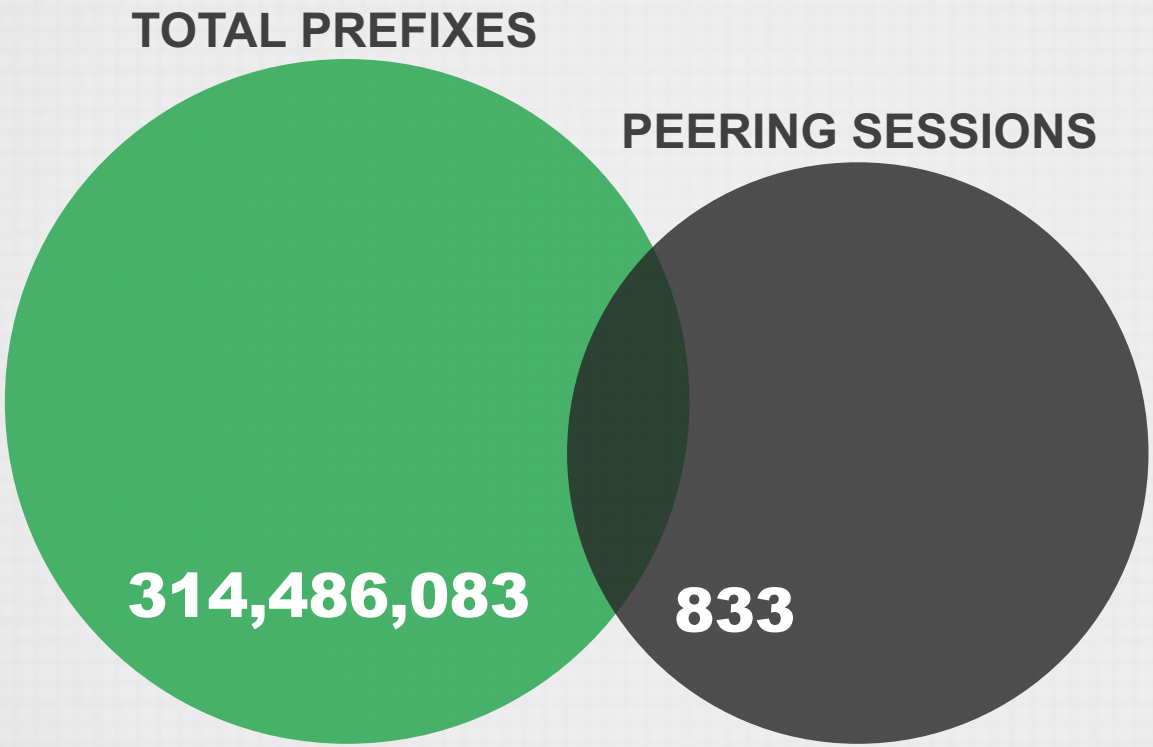
A complete list of current RouteViews locations is at https://as6447.peeringdb.com

PEERING STATS

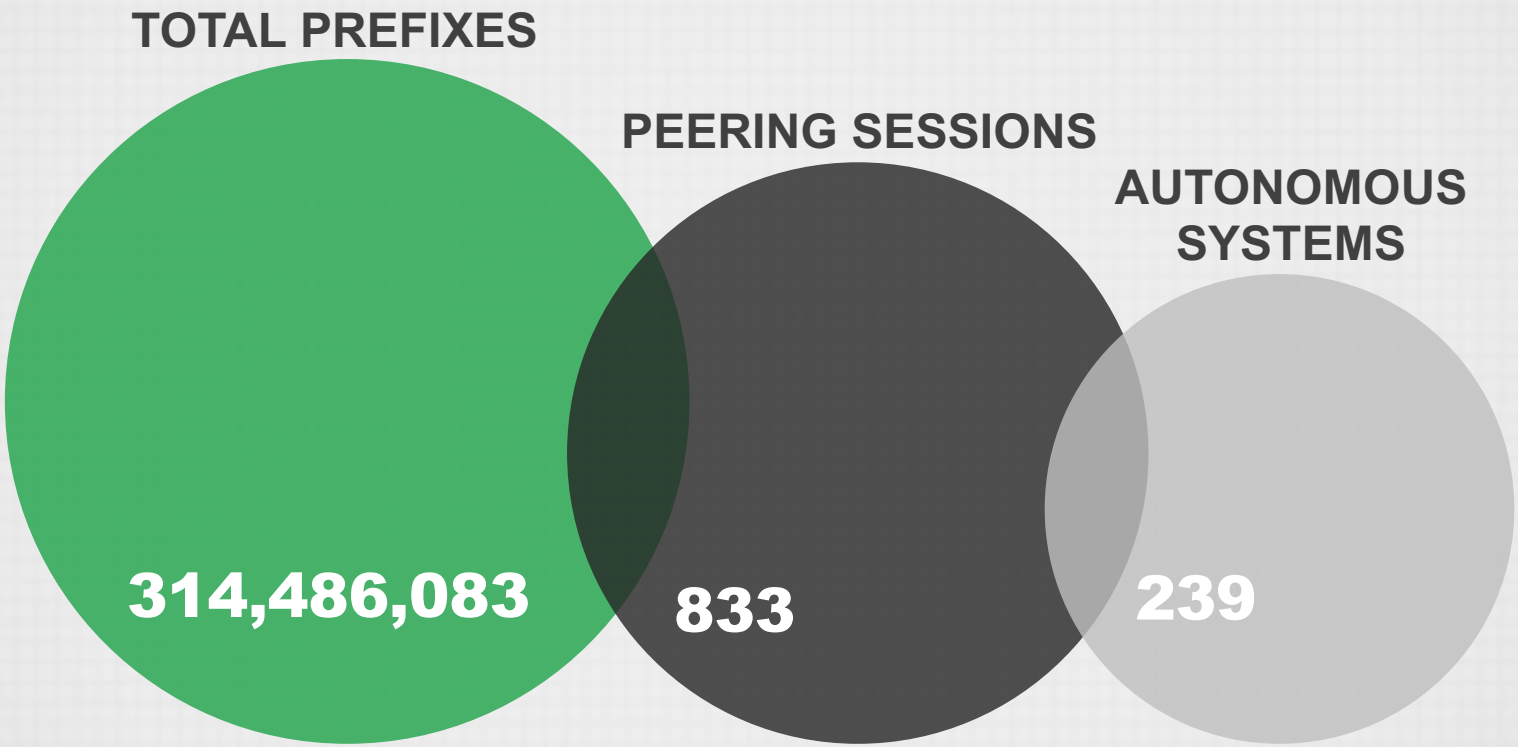
PEERING STATS



PEERING STATS



PEERING STATS



More peering information: www.routeviews.org/peers/peering-status.html

COLLECTORS

HARDWARE

Commodity

- 8-16 Cores
- 32G-64G Ram
- 400GB-1TB SSD
- 1/10 GB eth

Vendor

- ASR 1004

SOFTWARE

OpenSource

- Linux/Centos and…
- Quagga – bgpd
- FRR – bgpd

Vendor

- IOS XE

COLLECTORS OPERATIONS

MULTI-HOP

Pros

- If you can reach the collector, you can peer

Cons

- Peerings are subject to the routing anomalies that RouteViews seeks to observe and collect

INTERNET EXCHANGE

Pros

- Better positioned to address multi-hop issues
- Geographic diversity
- Peering diversity

COLLECTOR DATA

MRT

Multi-Threaded Routing Toolkit

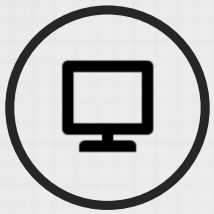
- https://tools.ietf.org/html/rfc6396
- MRT provides a standard for parsing or dumping routing information to a binary file.
- RouteViews Dumps consist of BGP RIBs and UPDATES.
  - RIBs are dumped every 2 hours
  - UPDATEs are dumped every 15 minutes

DATA ACCESS

- MRT files are bzipped and rsynced back to http://archive.routeviews.org/ regularly
- They can be accessed via, http, ftp and rsync.

MRT TOOLS

Isolario, RIPE libBGPdump, UCLA BGP Parser, NTT BGPdump2, etc:



- https://gitlab.com/Isolario
- https://bitbucket.org/ripencc/bgpdump/wiki/Home
- https://github.com/cawka/bgpparser
- https://github.com/yasuhiro-ohara-ntt/bgpdump2
- https://github.com/t2mune/mrtparse (Python)
- https://github.com/rfc1036/zebra-dump-parser (Perl)
- https://github.com/CAIDA/libparsebgp

COLLECTOR ACCESSIBILITY

telnet://route-views*.routeviews.org

- No username necessary.
- Users are able to run show commands, e.g. show ip bgp x.x.x.x/x.

GOTCHAS

- Why not SSH?!
  - RouteViews data is publicly available. We've got nothing to hide.
  - We use ssh for host management.
- show ip route x.x.x.x next-hop is incorrect!
  - Remember, this is a collector. There's no data-plane, thus no true FIB.

USE CASES

OPERATIONS

- BGP is the backbone of the Global Routing Infrastructure.
- To ensure its stability, it needs to be constantly monitored.
- RouteViews provides:
  - Command-Line/ Looking Glass
  - Prefix Visibility, Verify Convergence, Path Stability
  - Comparing Local/Regional/Global Views
  - Troubleshooting Reachability

USE CASES

OPERATIONS

- Worldwide CLI access – how to access a collector
- telnet://route-views.routeviews.org
  - *route-views, route-views{2,3,4,6}* are all housed at University of Oregon in the United States, and each collector has eBGP Multihop sessions with peers from around the world
- telnet://route-views.linx.routeviews.org
  - Other collector locations accessible via these 3rd level domains (replace "linx"): *saopaulo, saupaulo2, telxatl, jinx, napafrica, perth, soxrs, eqix, nwax, sg, sfmix, flix, amsix, chicago, chile, isc, sydney, mwix, kixp, & wide*

USE CASES

OPERATIONS

```
route-views>sh ip bgp 194.126.81.35
BGP routing table entry for 194.126.64.0/19, version 143916617
Paths: (32 available, best #29, table default)
  Not advertised to any peer
  Refresh Epoch 1
  57866 2914 5413, (aggregated by 5413 62.72.136.6)
    37.139.139.0 from 37.139.139.0 (37.139.139.0)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Community: 2914:420 2914:1206 2914:2203 2914:3200 57866:11 57866:100 57866:103
  Refresh Epoch 1
  8283 5413, (aggregated by 5413 62.72.136.6)
    94.142.247.3 from 94.142.247.3 (94.142.247.3)
      Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate
      Community: 6777:65011 6777:65023 8283:1 8283:101
      unknown transitive attribute: flag 0xE0 type 0x20 length 0x18
        value 0000 205B 0000 0000 0000 0001 0000 205B
              0000 0005 0000 0001
```

Setting aggregator attribute

Communities set by peers

Unsupported BGP attribute

USE CASES

OPERATIONS

```
route-views>sh ip bgp 194.126.81.35
BGP routing table entry for 194.126.64.0/19, version 143916617
Paths: (32 available, best #29, table default)
  Not advertised to any peer
...
 Refresh Epoch 1
  4901 6079 1299 5413 5413, (aggregated by 5413 62.72.136.161)
    162.250.137.254 from 162.250.137.254 (162.250.137.254)
      Origin incomplete, localpref 100, valid, external, atomic-aggregate
      Community: 65000:10100 65000:10300 65000:10400
  Refresh Epoch 1
  101 101 3356 5413 5413 5413, (aggregated by 5413 62.72.136.7)
    209.124.176.223 from 209.124.176.223 (209.124.176.223)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Community: 101:20100 101:20110 101:22100 3356:2 3356:22 3356:100 3356:123
3356:500 3356:2064 65001:0
      Extended Community: RT:101:22100
```

AS4901 communities?

Extended BGP community

USE CASES

OPERATIONS

```
route-views>sh ip bgp 194.126.81.35 | i aggregated
  701 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  57866 2914 5413, (aggregated by 5413 62.72.136.6)
  8283 5413, (aggregated by 5413 62.72.136.6)
  3333 5413, (aggregated by 5413 62.72.136.6)
  53767 3257 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  58901 51167 8220 5413, (aggregated by 5413 62.72.136.161)
  7660 2516 3356 5413 5413 5413, (aggregated by 5413 62.72.136.7)
  4901 6079 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  101 101 3356 5413 5413 5413, (aggregated by 5413 62.72.136.7)
  7018 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  3277 3267 5413, (aggregated by 5413 62.72.136.6)
  3267 5413, (aggregated by 5413 62.72.136.6)
  49788 12552 5413, (aggregated by 5413 62.72.136.6)
  53364 3257 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  54728 20130 6939 5413, (aggregated by 5413 62.72.136.6)
  286 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  852 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  3549 3356 3356 5413 5413 5413, (aggregated by 5413 62.72.136.7)
  20912 1267 5413, (aggregated by 5413 62.72.136.6)
  1403 6461 5413, (aggregated by 5413 62.72.136.161)
  1403 6461 5413, (aggregated by 5413 62.72.136.161)
  2497 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  1221 4637 5413, (aggregated by 5413 62.72.136.6)
  1351 6939 5413, (aggregated by 5413 62.72.136.6)
  3561 209 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  6079 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  6079 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  1239 1299 5413 5413, (aggregated by 5413 62.72.136.161)
  3303 5413, (aggregated by 5413 62.72.136.6)
  4826 6939 5413, (aggregated by 5413 62.72.136.6)
  6939 5413, (aggregated by 5413 62.72.136.6)
  19214 174 1299 5413 5413, (aggregated by 5413 62.72.136.161)
```

All the paths to this destination

USE CASES

OPERATIONS

```
route-views>sh bgp ipv6 uni 2001:44B8::/32 lo | i 2001:44B8
 *   2001:44B8::/32   2606:6D00:EB0::254
 *   2001:44B8:24::/48
 *   2001:44B8:25::/48
 *   2001:44B8:26::/48
 *   2001:44B8:27::/48
 *   2001:44B8:28::/48
 *   2001:44B8:29::/48
 *   2001:44B8:2A::/48
 *   2001:44B8:2B::/48
 *   2001:44B8:2C::/48
 *   2001:44B8:2D::/48
 *   2001:44B8:2E::/48
 *   2001:44B8:2F::/48
 *   2001:44B8:30::/48
 *   2001:44B8:31::/48
 *   2001:44B8:32::/48
 *   2001:44B8:33::/48
 *   2001:44B8:34::/48
 *   2001:44B8:35::/48
 *   2001:44B8:36::/48
 *   2001:44B8:37::/48
 *   2001:44B8:38::/48
 *   2001:44B8:39::/48
 *   2001:44B8:60:2300::/56
 *   2001:44B8:60:2500::/56
 *   2001:44B8:1058::/48
 *   2001:44B8:1059::/48
 *   2001:44B8:105A::/48
```


Lots of /48s out of /32 covering aggregate, why??

USE CASES

OPERATIONS

```
route-views>sh ip bgp 202.144.128.0/19
BGP routing table entry for 202.144.128.0/19, version 143910183
Paths: (32 available, best #30, table default)
  Not advertised to any peer
  Refresh Epoch 1
  701 6461 17660
    137.39.3.55 from 137.39.3.55 (137.39.3.55)
      Origin IGP, localpref 100, valid, external
  Refresh Epoch 1
  3277 3267 6461 17660
    195.208.112.161 from 195.208.112.161 (194.85.4.13)
      Origin IGP, localpref 100, valid, external
      Community: 3277:3267 3277:65100 3277:65320 3277:65326 3277:65331
  Refresh Epoch 1
  3267 6461 17660
    194.85.40.15 from 194.85.40.15 (185.141.126.1)
      Origin IGP, metric 0, localpref 100, valid, external
```

32 paths to this aggregate, but look at next slide…

USE CASES

OPERATIONS

```
route-views>sh ip bgp 202.144.128.0/20
BGP routing table entry for 202.144.128.0/20, version 129174671
Paths: (5 available, best #4, table default)
  Not advertised to any peer
  Refresh Epoch 1
  1351 6939 17660 18024
    132.198.255.253 from 132.198.255.253 (132.198.255.253)
      Origin IGP, localpref 100, valid, external
  Refresh Epoch 1
  58901 51167 8220 17660 18024
    178.238.225.14 from 178.238.225.14 (178.238.233.155)
      Origin IGP, localpref 100, valid, external
  Refresh Epoch 1
  54728 20130 6939 17660 18024
    140.192.8.16 from 140.192.8.16 (140.192.8.16)
      Origin IGP, localpref 100, valid, external
  Refresh Epoch 1
  6939 17660 18024
    64.71.137.241 from 64.71.137.241 (216.218.252.164)
      Origin IGP, localpref 100, valid, external, best
  Refresh Epoch 1
  4826 17660 18024
    114.31.199.1 from 114.31.199.1 (114.31.199.1)
      Origin IGP, localpref 100, valid, external
      Community: 4826:5101 4826:6570 4826:51011 24115:17660
```

This /20 is only announced at one IXP - so who is **leaking**?

USE CASES

OPERATIONS

What is AS8697 trying to achieve with 26x prepend?

```
route-views>sh ip bgp 37.202.76.0/24
BGP routing table entry for 37.202.76.0/24, version 149008178
Paths: (31 available, best #7, table default)
  Not advertised to any peer
  Refresh Epoch 1
  701 3356 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697
8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8376, (aggregated by 8376 10.50.253.13)
    137.39.3.55 from 137.39.3.55 (137.39.3.55)
      Origin IGP, localpref 100, valid, external
  Refresh Epoch 1
  24441 3491 3491 3356 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697
8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8376, (aggregated by 8376
10.50.253.13)
    202.93.8.242 from 202.93.8.242 (202.93.8.242)
      Origin IGP, localpref 100, valid, external
  Refresh Epoch 1
  7018 3356 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697
8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8697 8376, (aggregated by 8376 10.50.253.13)
    12.0.1.63 from 12.0.1.63 (12.0.1.63)
      Origin IGP, localpref 100, valid, external, best
      Community: 7018:5000 7018:37232
```

USE CASES

OPERATIONS – HIJACK or MISCONFIGURATION ?

```
route-views>sh ip bgp 202.134.24.0/21 | i 9241
  3267 174 9241 38201
  49788 174 9241 38201
  57866 1299 174 9241 38201
  3333 1257 174 9241 38201
  3277 3267 174 9241 38201
  54728 20130 6939 1299 174 9241 38201
  852 174 9241 38201
  8283 38930 174 9241 38201
  4826 174 9241 38201
  6079 3257 174 9241 38201
  101 101 174 9241 38201
  24441 3491 3491 174 9241 38201
  1403 174 9241 38201
  1403 174 9241 38201
  6079 3257 174 9241 38201

etc
```

The aggregate

Correctly originated by AS38201

202.134.24.0/21 and its two subnets, 202.134.24.0/22 and 202.134.28.0/22

USE CASES

OPERATIONS – HIJACK or MISCONFIGURATION ?

```
route-views>sh ip bgp 202.134.24.0/22 | i 9241
  3267 1299 4648 9241 38201
  49788 1299 4648 9241 38201
  57866 2914 4648 9241 38201
  3333 1257 1299 4648 9241 38201
  3277 3267 1299 4648 9241 38201
  54728 20130 6939 4648 9241 38201
  852 1299 4648 9241 38201
  6079 1299 4648 9241 38201
  1403 1299 4648 9241 38201
  1403 1299 4648 9241 38201
  101 101 11164 4648 9241 38201
  4826 38456 4648 9241 38201
  24441 3491 3491 1299 4648 9241 38201
  286 1299 4648 9241 38201
  6079 1299 4648 9241 38201

etc
```

The first subnet

Correctly originated by AS38201

202.134.24.0/21 and its two subnets, 202.134.24.0/22 and 202.134.28.0/22

USE CASES

OPERATIONS – HIJACK or MISCONFIGURATION ?

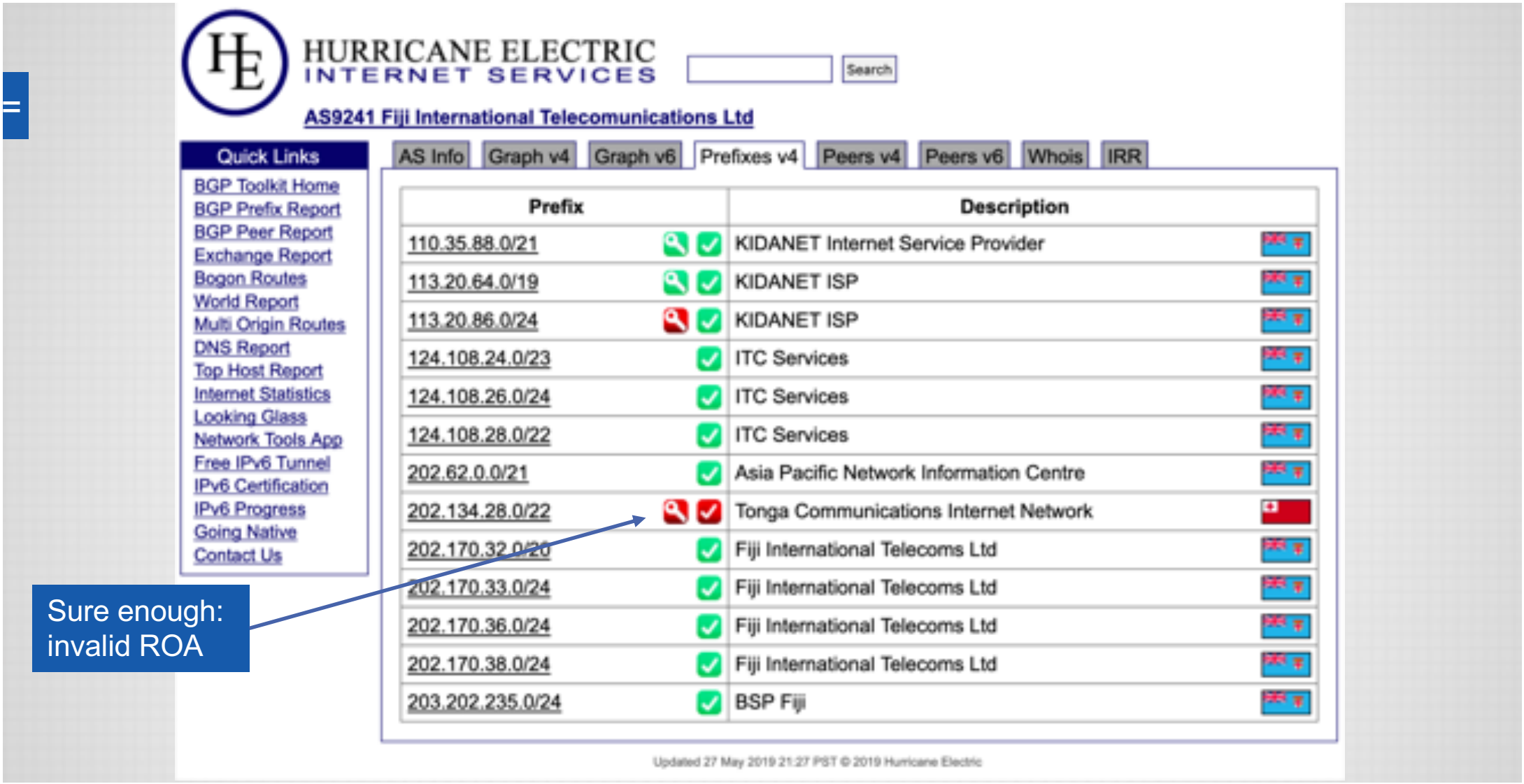
```
route-views>sh ip bgp 202.134.28.0/22 | i 9241
  3267 1299 4648 9241
  49788 1299 4648 9241
  57866 2914 4648 9241
  3333 1257 1299 4648 9241
  3277 3267 1299 4648 9241
  54728 20130 6939 4648 9241
  852 1299 4648 9241
  1403 1299 4648 9241
  1403 1299 4648 9241
  101 101 11164 4648 9241
  24441 3491 3491 1299 4648 9241
  6079 1299 4648 9241
  4826 38456 4648 9241
  6079 1299 4648 9241
  286 1299 4648 9241

etc
```

The second subnet

Originated by the Transit AS ?!

202.134.24.0/21 and its two subnets, 202.134.24.0/22 and 202.134.28.0/22



Sure enough: invalid ROA

USE CASES

RESEARCH

- BGP anomalies and dynamics are critical as well.
- RouteViews Provides:
  - Network Topology Monitoring
  - Route Leaks/Hijacks (ex. Artemis, Cyclops)
  - Network Optimization
  - Growth, Aggregation, etc. in AS/v4/v6
  - Address Provenance
- ~500 research publications have used RouteViews data
- More info: http://www.routeviews.org/routeviews/index.php/papers/

THANK YOU

COMMUNITY SUPPORT

- RouteViews would not be possible without:
  - Hosts like IX.br, Netflix, 31173.ab, Equinix, and many many more, who host the collectors and provide free power, cooling, transit connectivity, IX connectivity, and so on

- RouteViews is a beacon of the collaboration successes of the global network engineering community

THANK YOU

Questions?