ROUTEVIEWS

Global BGP Collector for Operators and Research

Presented by Greg Shepherd
shep@routeviews.org

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 50TBs (compressed) today.

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

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.

Why Routeviews?

IT'S YOUR INTERNET

- Originally conceived in 1995 as a tool for Internet operators to look at the BGP table from different backbones and locations around the world to troubleshoot and to asses:
  - reachability, hijacks, peer visibility, mass withdrawals, and RPKI status
- Operators who find it a valuable tool also peer to contribute to the value

- The 26-year data-set of BGP information archived by RouteViews since 1997 has become an invaluable research resource
  - RouteViews data has been used in over 1000 research papers.
  - http://www.routeviews.org/routeviews/index.php/papers/

RouteViews Impact

Geoff Huston wrote in his report, "BGP in 2022 – the routing table":

"I should take a moment to mention the Route Views Project. It was originally intended to offer a multi-perspective real-time view of the inter-domain routing system, allowing network operators to examine the current visibility of route objects from various points in the inter-domain topology.

What makes Route Views so unique is that it archives these routing tables every two hours and has done so for more than two decades. It also archives every BGP update message. ***This vast collection of data is a valuable research data source in its own right****, and here we are just taking a tiny slice of this data set to look at longer-term routing growth trends.*

The folk at the Route Views Project, with support from the University of Oregon and the US National Science Foundation, should be commended for their efforts here. This is a very unique data set if you are interested in the evolution of the Internet over the years."

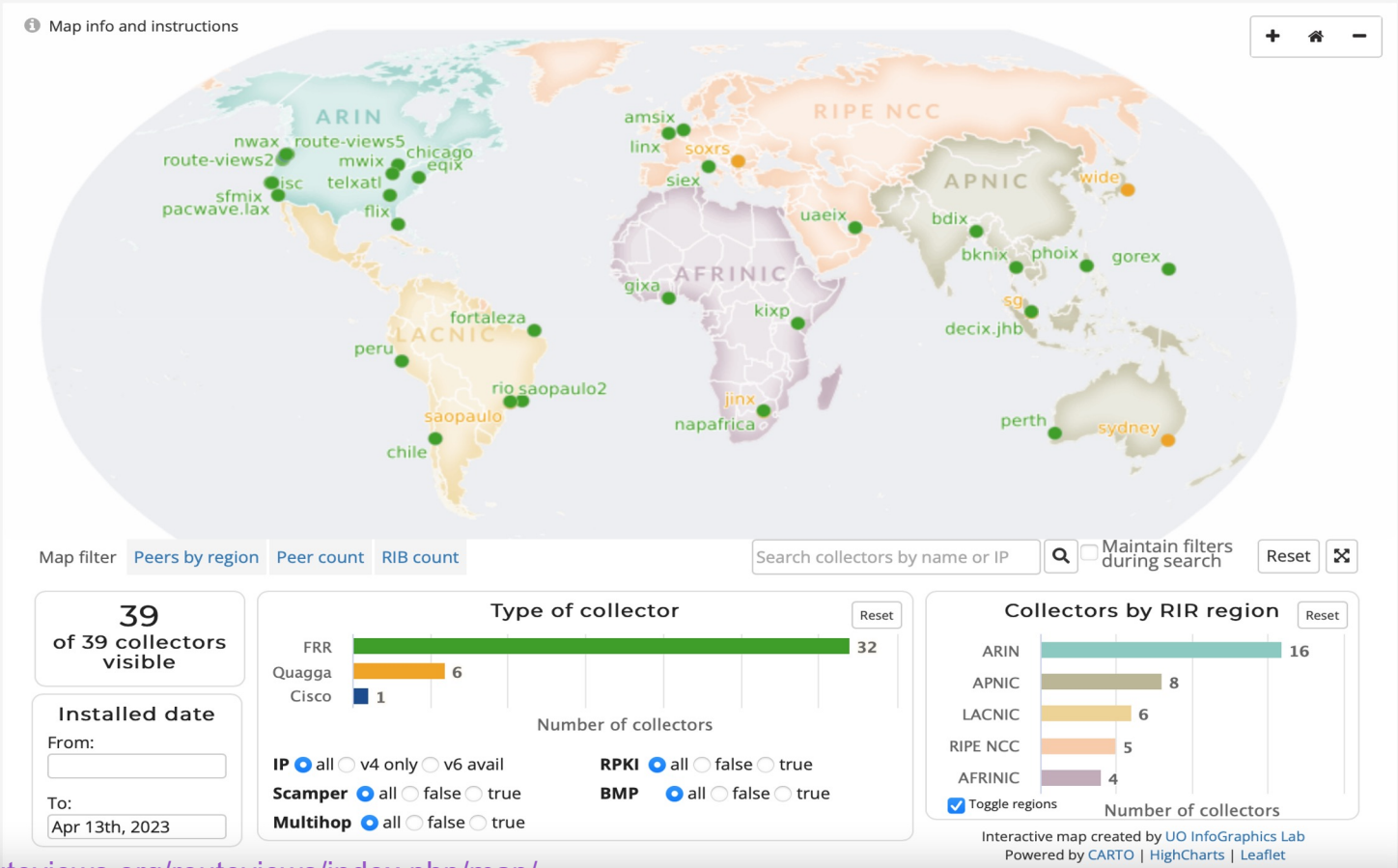
RouteViews Impact

Aftab Siddiqui:

"The MANRS Observatory relies heavily on BGPStream and GRIP for the detection of BGP related incidents such as BGP Leakss and BGP mis-origination. It is also very critical to verify that any incident highlighted by these services can be verified independently and to do that ***we require raw BGP data which is made available by 2 sources: RIPE RIS and Route Views.*** *Diversity of data sources is once again very important to verify any such incidents. NSRC, which manages the Route Views project, ensures that the routing data they provide is accurate and they have promptly addressed any issues or concerns raised by the MANRS team, whether it is related to changes in the MRT format causing problems in data parsing or helping with BMP data.* ***Actively maintaining Route Views provides community service by NSRC.***

MANRS has gained a lot of good reputation in the community due to the support and expertise provided by its partners such as NSRC. NSRC included MANRS Action explanation and implementation guidelines in their training courses for network operators and R&E networks, in their technical video content, and has been promoting various MANRS programs to respective communities specifically in Asia Pacific and Africa where the MANRS participation is low as compared to other regions."

Routeviews Collector Map



http://www.routeviews.org/routeviews/index.php/map/

COLLECTOR DEPLOYMENT

Physical

- Off the shelf hardware.
- Shipped to the IX.
- Least preferred.

Virtual

- Much quicker deployment time.
- Easier to upgrade.

Collectors

HARDWARE

Commodity

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

SOFTWARE

OpenSource

- Linux/Centos and…
- Quagga – bgpd
- FRR – bgpd
- Gobgpd
- OpenBMP
- GoBMP

Collector Deployment

MULTI-HOP

- Pros:
  - If you can reach the collector, you can peer.
- Cons:
  - Multi-hop peerings are subject to the routing anomalies RouteViews seeks to observe and archive.

IX-HOSTED/CO-LOCATED

- Pros:
  - Better positioned to address multi-hop issues.
  - Geographic diversity.
  - Peering diversity.
  - Scalable.
- Cons:
  - More infrastructure to manage.

Collector Data

Multi-Threaded Routing Toolkit (MRT)

- 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 archived every 2 hours
  - UPDATEs are archived every 15 minutes

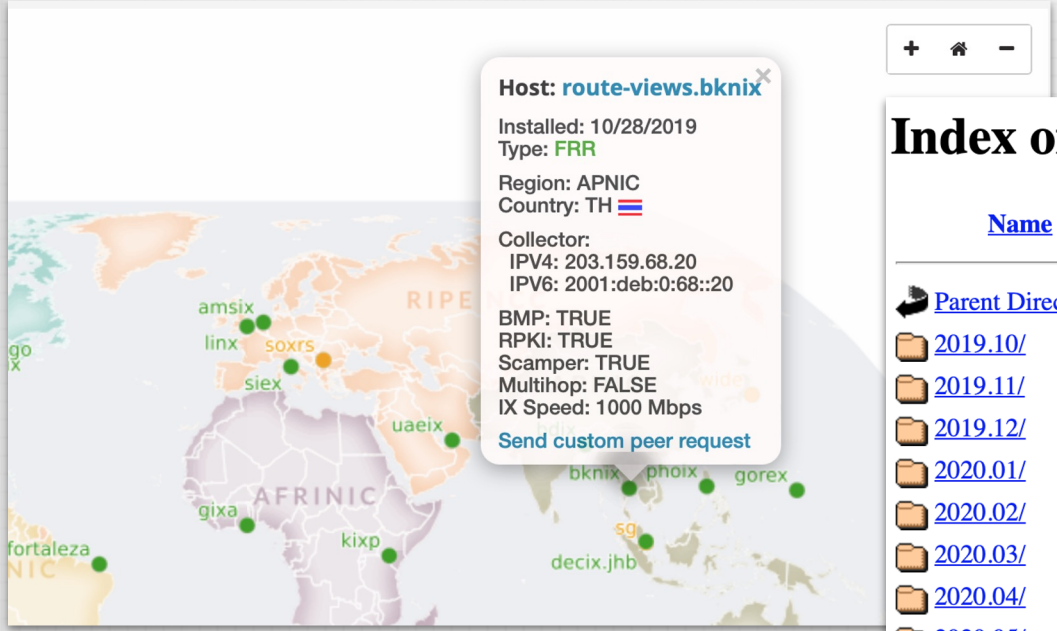
Data Access

- MRT files are bzipped and rsynced back to http://archive.routeviews.org/ on above schedule
- They can be accessed via, http, ftp and rsync
- Map view tool is interactive

Direct BMP Feed

- New Model
- BMP upstream from collectors, not FROM peers

Collector Data



Index of /route-views.bknix/bgpdata

Name	Last modified	Size	Description
Parent Directory		-	
2019.10/	2019-10-28 23:01	-	
2019.11/	2019-10-28 23:01	-	
2019.12/	2019-11-28 23:01	-	
2020.01/	2019-12-28 23:01	-	
2020.02/	2020-01-28 23:01	-	
2020.03/	2020-02-28 23:01	-	
2020.04/	2020-03-28 23:01	-	
2020.05/	2020-04-28 23:01	-	
2020.06/	2020-05-28 23:01	-	
2020.07/	2020-06-28 23:01	-	

http://archive.routeviews.org/route-views.bknix/bgpdata/

MRT Tools

RIPE libbgpdump, UCLA BGP Parser, NTT bgpdump2, etc.

- 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)

NEW COLLECTOR FEATURES

BMP

- BMP data will feed tools like BGPStream and ARTEMIS.
- Or write your own Kafka consumer for raw BMP data.
- Limited access at first.
- Wider availability to follow.

RPKI

- RPKI data will be accessible directly from the collectors.
- We also are establishing an archive of RPKI ROA data.
- Working on back-filling that data set from the RIR/CAs.

PEERING HowTo

BGP CONFIGURATION

- Send full-table if you can
- Remove default route
- Remove NULL routes
- Remove RFC-1918 addresses
- We don’t accept ADD-PATH TX/RX
- We don’t send any routes back
- When peering with multi-hop collectors, set ebgp-multihop

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
  - Access to historical BGP data, ie “When did this happen??”

Use Cases

Accessing a Collector

- telnet://route-views*.routeviews.org
- No username necessary.
- Users are able to run show commands, e.g. show ip bgp x.x.x.x/
- Telnet access is rate-limited to prevent automation overuse
- PLEASE don't script. There is an API for that.

Gotchas

- Why not SSH?!
  - RouteViews data is publicly available. We've got nothing to hide.
- 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
  - Kernel default-route points to transit provider next-hop

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

- Legacy Naming Scheme
  - telnet://route-views.bknix.routeviews.org
  - Other collector locations accessible via these 3rd level domains (replace “bknix”): saopaulo, saupaulo2, telxatl, jinx, napafrica, perth, soxrs, eqix, nwax, sg, sfmix, flix, amsix, chicago, chile, isc, sydney, mwix, kixp, & wide

- New Naming Scheme
  - (exchange).(closest airport).routeviews.org
  - ie: decix.jhb.routeviews.org - Malaysia IX, JHB airport

USE CASES

OPERATIONS

route-views.bknix.routeviews.org> sh ip bg sum

IPv4 Unicast Summary (VRF default):
BGP router identifier 203.159.68.20, local AS number 6447 vrf-id 0
BGP table version 58060
RIB entries 2141, using 401 KiB of memory
Peers 6, using 4345 KiB of memory

Only 6 peers currently

Not full routes.. :(

Neighbor	V	AS		MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd	PfxSnt	Desc
203.159.68.1	4	63528	2	16880			197077			0	0	
	0	04w3d03h	3	0	BKNIX							
203.159.68.2	4	63528	216945		197077		0			0	0	19w3d20h
	3	0	BKNIX									
203.159.68.5	4	63528	394163		394153		0			0	0	19w3d20h
	6	0	BKNIX									
203.159.68.122	4	132280	414908	394155	0	0	0		14w5d19h	518	0	
Symphony												
203.159.68.130	4	16509	441589		394152	0	0			0	19w3d20h	652
	0	Amazon.com										
203.159.68.131	4	16509	441609		394152	0	0			0	19w3d20h	652
	0	Amazon.com										

Total number of neighbors 6
route-views.bknix.routeviews.org>

USE CASES

OPERATIONS

ThaiNOG event prefix

Covered by /22

```
route-views>sh ip bgp 103.120.115.0/28 short
BGP table version is 15689777, local router ID is 128.223.51.103
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
V*   103.120.112.0/22 206.24.210.80                            0 3561 209 3356 9002 9304 135419 i
V*                    194.85.40.15             0               0 3267 1299 15412 9304 135419 i
V*                    208.74.64.40                             0 19214 174 9304 135419 i
V*                    217.192.89.50                            0 3303 9304 135419 i
V*                    212.66.96.126                            0 20912 3257 2914 9304 135419 i
V*                    202.232.0.2                              0 2497 9304 135419 i
V*                    162.250.137.254                          0 4901 6079 15412 9304 135419 i
V*                    144.228.241.130        156               0 1239 9304 135419 i
…
```

USE CASES

OPERATIONS

ThaiNOG IPv6 global reach

```
route-views>sh bgp ipv6 uni 2403:56c0:0522::/30 long
BGP table version is 8597067, local router ID is 128.223.51.103
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
V*   2403:56C0::/32   2001:1860::223                           0 101 6939 10089 135419 i
V*                    2600:803::15                              0 701 5511 45629 135419 i
V*                    2001:1890:111D:1::63                      0 7018 1299 10089 135419 i
V*                    2A00:A7C0:E20A::17                        0 57866 9002 45629 135419 i
V*                    2A02:898:0:300::3                                 0 8283 1299 10089 135419 i
V*                    2A02:D140:1::60                           0 49788 12552 6939 10089 135419 i
```

USE CASES

OPERATIONS

route-views2.routeviews.org> sh ip bg sum

77 peers, multi-hop

IPv4 Unicast Summary (VRF default):
BGP router identifier 128.223.51.102, local AS number 6447 vrf-id 0
BGP table version 14375055
RIB entries 1786807, using 327 MiB of memory
Peers 77, using 54 MiB of memory

Not all peers are up..

Neighbor	V	AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd PfxSnt Desc						
4.68.4.46	4	3356	0	7241	0	0	0	never
	Active	0 Level3						
5.101.110.2	4	14061	0	0	0	0	0	never
	Connect	0 DIGITALOCEAN						
12.0.1.63	4	7018 3986207	14643	0	0	0 01w3d04h	907452	0 ATT
37.139.139.17 4	57866 3740071	29283	0	0	0 01w3d04h	910247	0 Fusix	
43.226.4.1	4	63927	0	0	0	0	0	never
	Connect	0 Rise						
45.61.0.85	4	22652 3583124	29285	0	0	0 2d07h01m	911510	0 FIBRENOIRE
62.115.128.137 4	1299 9158678	14643	0	0	0 01w3d04h	883318	0 Telia	
64.71.137.241 4	6939 3389354	14642	0	0	0 01w3d04h	933920	0 Hurricane Electric	
64.71.255.61	4	812	0	0	0	0	0	never
	Connect	0 Sprint						
66.185.128.1	4	1668	0	0	0	0	0	never
	Connect	0 AOL						
67.219.192.18 4	19653	0	0	0	0	0	never	Active
	0 CTSTelecom							
68.67.63.245	4	22652	0	0	0	0	0	never
	Active	0 FIBRENOIRE						
80.241.176.31 4	20771	0	0	0	0	0	never	Connect
	0 CAUCASUS							
85.114.0.217	4	8492 5173073	29285	0	0	0 4d09h09m	940862	0 OBITRU
87.121.64.4	4	57463 1247665	14641	0	0	0 01w3d03h	417683	0 NETIXLTD
89.149.178.10 4	3257 3545660	14643	0	0	0 01w3d04h	907675	0 Tiscali	
91.209.102.1	4	39756	0	0	0	0	0	never
	Connect	0 HOSTWAY-RO						
91.218.184.60 4	49788 5731466	14642	0	0	0 01w3d04h	913404	0 NEXTHOPNO	

…

Total number of neighbors 77

Lots of full tables

USE CASES

OPERATIONS

```
route-views2.routeviews.org> sh ip bgp 130.105.44.0/22
BGP routing table entry for 130.105.44.0/22, version 13607198
Paths: (29 available, best #25, table default)
  Not advertised to any peer
  22652 6453 23944
                    45.61.0.85 from 45.61.0.85 (184.95.245.30)
                    Origin IGP, valid, external, rpki validation-state: valid
                    Community: 6453:50 6453:3000 6453:3400 6453:3409
                    Last update: Mon May  8 01:08:57 2023
  3130 1239 6453 23944
                    147.28.7.1 from 147.28.7.1 (147.28.7.1)
                    Origin IGP, valid, external, rpki validation-state: valid
                    Community: 1239:321 1239:1000 1239:1010
                    Last update: Mon May  8 01:56:35 2023
  8492 31133 23944
…
                    37.139.139.17 from 37.139.139.17 (37.139.139.17)
                    Origin IGP, metric 0, valid, external, rpki validation-state: valid
                    Community: 6453:50 6453:3000 6453:3400 6453:3409 57866:100 65100:6453 65103:1 65104:31
                    Large Community: 57866:100:6453 57866:101:100 57866:103:1 57866:104:31
                    Last update: Mon May  8 01:57:01 2023
  37100 23944
```

Communities set by peers

RPKI Validation State

Large Communities

USE CASES

OPERATIONS

```
route-views2.routeviews.org> sh ip bgp  45.235.208.0/22
BGP routing table entry for 45.235.208.0/22, version 1474520
Paths: (30 available, best #25, table default)
  Not advertised to any peer
  11686 52320 22381 22381 22381 22381 11432 11432 11432 11432 11432 11432 11432 11432 11432 11432 11432 11432 11432 11432
11432 11432 11432 11432 11432 11432 11432 11432 11432 268214
                    96.4.0.55 from 96.4.0.55 (96.4.0.55)
                    Origin IGP, valid, external, rpki validation-state: not found
                    Community: 11686:294
                    Last update: Tue May  9 04:34:01 2023
  22652 4230 11432 268214
                    45.61.0.85 from 45.61.0.85 (184.95.245.30)
                    Origin IGP, valid, external, rpki validation-state: not found
                    Community: 4230:11 4230:30 4230:511 4230:5101
                    Last update: Sat May  6 08:05:45 2023
  8492 31133 3356 268214 268214
                    85.114.0.217 from 85.114.0.217 (85.114.0.104)
                    Origin IGP, valid, external, rpki validation-state: not found
                    Community: 8492:1104 8492:1601
                    Last update: Thu May  4 05:57:42 2023
…
```

WHAT IS ASN:11432 TRYING TO ACHIEVE BY PREPENDING 23 TIMES??

USE CASES

OPERATIONS

```
route-views2.routeviews.org> sh ip bgp rpki invalid
….
I*  212.193.8.0/24   168.209.255.56                    0 3741 5511 6453 8551 203905 i
I*                   194.153.0.253                      0 5413 8551 203905 i
I*                   45.61.0.85                         0 22652 6453 8551 203905 i
I*                   91.218.184.60                      0 49788 12552 8551 203905 i
I*                   198.129.33.85            710       0 293 6453 8551 203905 i
I*                   212.66.96.126                      0 20912 49367 6762 61135 61135 60446 204843 204843 204843 i
I*                   202.232.0.3                        0 2497 6453 8551 203905 i
I*>                  85.114.0.217                       0 8492 8551 203905 i
I*                   203.189.128.233                    0 23673 23764 8551 203905 i
I*                   94.156.252.18            0         0 34224 6453 8551 203905 i
```

ASN: 203905 ??

ASN: 204843 ??

TWO ASN: OF ORIGIN ??

USE CASES

OPERATIONS

WHOIS Lookup (212.193.8.0)

inetnum:	212.193.8.0 - 212.193.8.255
netname:	AjyalFiCompanyLLC
country:	PS
admin-c:	KB5060-RIPE
tech-c:	KB5060-RIPE
status:	ASSIGNED PA
abuse-c:	AR68281-RIPE
mnt-by:	lir-ae-rcstechnologies-1-MNT
mnt-by:	interlir-mnt
created:	2023-01-12T18:31:35Z
last-modified:	2023-01-12T18:31:35Z
source:	RIPE

PALESTINE

USE CASES

OPERATIONS

WHOIS Lookup (AS204843)

…

organisation: ORG-SVMY1-RIPE
org-name: STERLY VERI MERKEZI YAZILIM VE SIBER GUVENLIK HIZMETLERI A.S.
country: TR
org-type: OTHER
address: KONAK MAH. BARIS(120) SK. OFIS ARTI BLOK NO:3 IC KAPI NO:10 NILUFER/BURSA
abuse-c: ACRO48320-RIPE
mnt-ref: ulasatakan
mnt-ref: bggroupittelecom-mnt
mnt-by: lir-tr-teknosos-1-MNT
mnt-by: Teknosos-TR
created: 2022-05-27T09:14:49Z
last-modified: 2022-12-01T17:27:16Z
source: RIPE # Filtered

FROM TURKEY ??

USE CASES

OPERATIONS

WHOIS Lookup (AS203905)

…
as-block: AS196608 - AS207419
…
admin-c: KB5060-RIPE
tech-c: KB5060-RIPE
status: ASSIGNED
mnt-by: RIPE-NCC-END-MNT
mnt-by: DigiComm-MNT
created: 2015-10-06T13:35:54Z
last-modified: 2023-02-04T17:55:17Z
source: RIPE # Filtered

organisation: ORG-DCL18-RIPE
org-name: Digital Communication Company for Telecommunications and Information Technology LTD
country: PS
org-type: LIR
address: Omar Al-Mokhtar st., Khaduir Building Floor #2
address: 9990300
address: Gaza Al-Remal
address: PALESTINE, STATE OF

FROM PALESTINE

USE CASES

OPERATIONS

ASN: 203905

```
route-views2.routeviews.org> sh ip bgp rpki invalid
....
I*  212.193.8.0/24   168.209.255.56                    0 3741 5511 6453 8551 203905 i
I*                   194.153.0.253                      0 5413 8551 203905 i
I*                   45.61.0.85                         0 22652 6453 8551 203905 i
I*                   91.218.184.60                      0 49788 12552 8551 203905 i
I*                   198.129.33.85            710       0 293 6453 8551 203905 i
I*                   212.66.96.126                      0 20912 49367 6762 61135 61135 60446 204843 204843 204843 i
I*                   202.232.0.3                        0 2497 6453 8551 203905 i
I*>                  85.114.0.217                       0 8492 8551 203905 i
I*                   203.189.128.233                    0 23673 23764 8551 203905 i
I*                   94.156.252.18            0         0 34224 6453 8551 203905 i
```

ASN: 204843 NOT VALID ORIGIN ?

MISS-CONFIGURATION? PREFIX HIJACK??

OTHER BITS..

RouteViews email list

- https://lists.nsrc.org/listinfo/routeviews-users
- Also available on the Contact page at routeviews.org
- A place to ask question and receive updates on RouteViews activities.
- Hosted by the wonderful folks at NSRC.

Route Views

The Internet works because a lot of people cooperate to do things together.

Jon Postel

THANK YOU

Questions?