Presentation

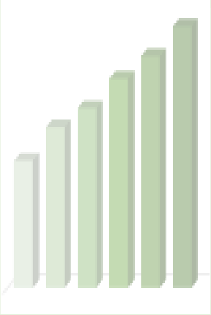
on

Features of BGP Watch Portal and suggested changes

Date: 14 March 2023

Time: 15:00hrs [GMT+6]

Prepared by
Mohammad Tawrit
CEO, BdREN



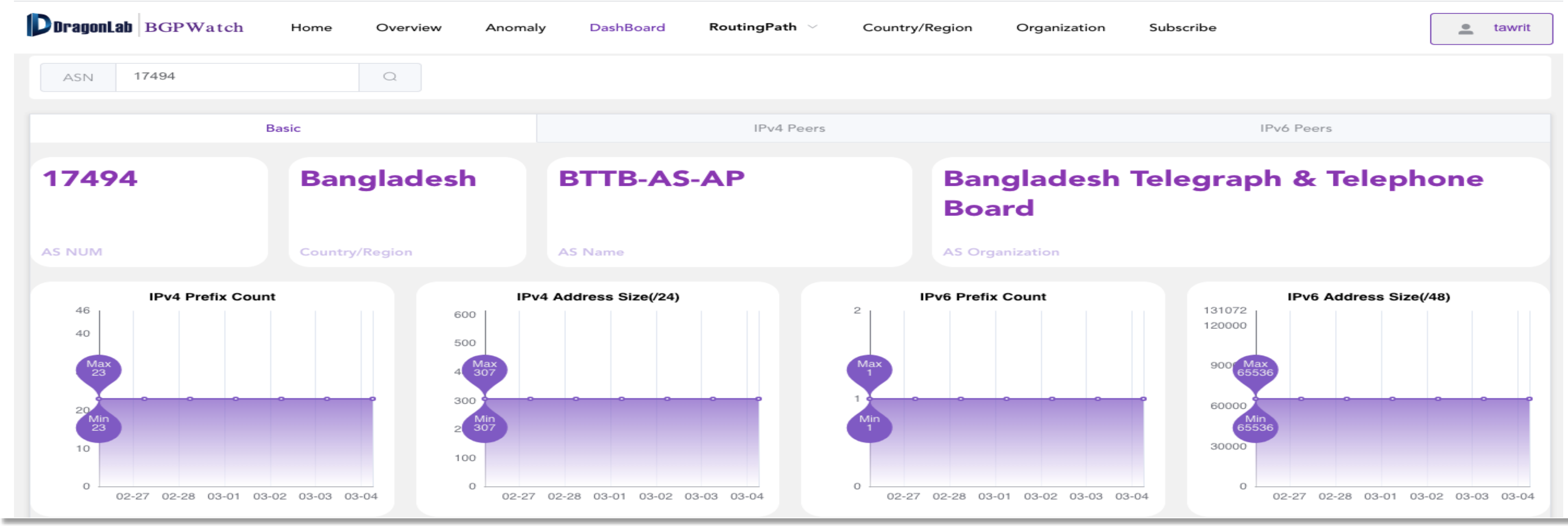
Connect
Collaborate
Innovate

Notable features of BGP Watch

1. Dashboard
2. Routing Path and Topology
3. Coverage of an Autonomous System => Cone size
4. Subscription and Reporting
5. Reporting Anomaly/hijacked Prefix Routing

1. Dashboard - Basic

- The “Dashboard”
  - Gives information about the number of IPv4 and IPv6 prefixes under a particular Autonomous System.



ASN 17494

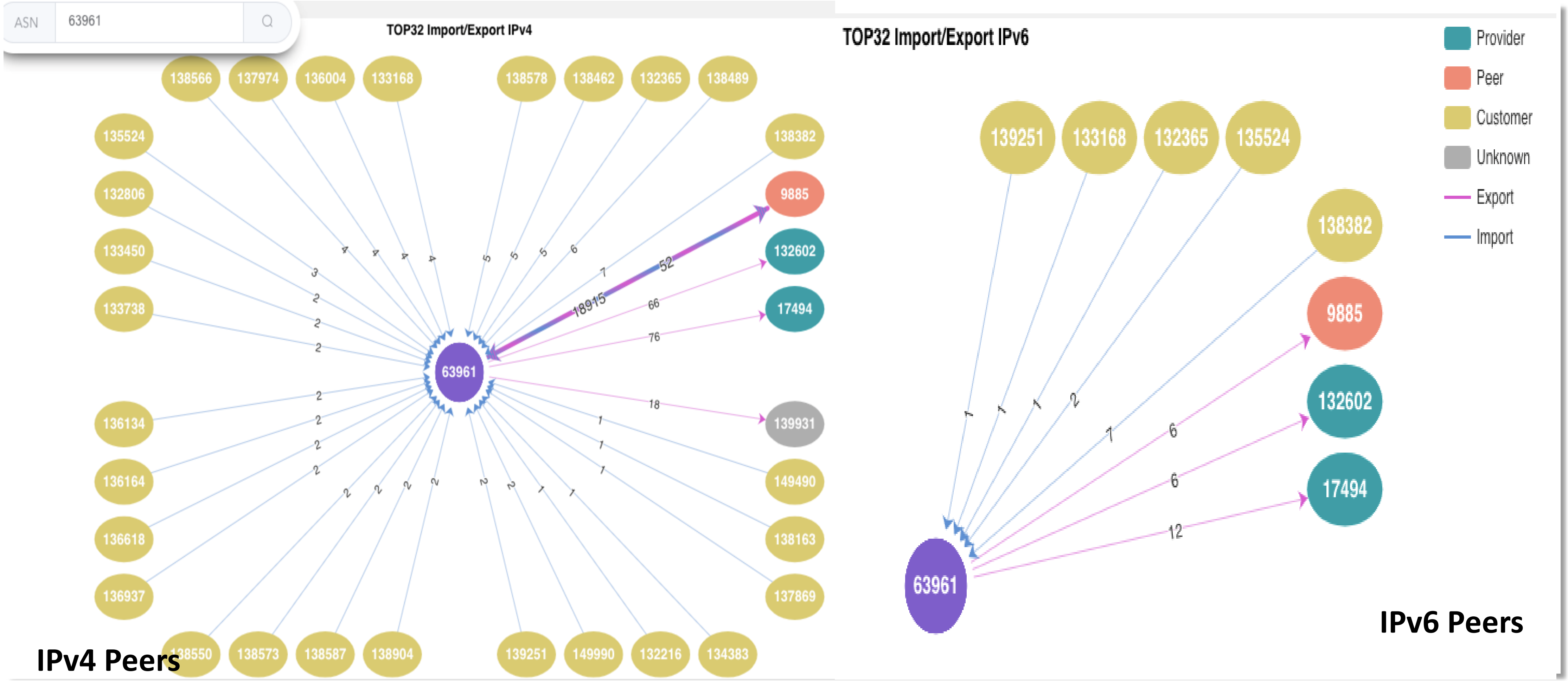
17494
AS NUM

Bangladesh
Country/Region

BTTB-AS-AP
AS Name

Bangladesh Telegraph & Telephone Board
AS Organization

1. Dashboard – IPv4 and IPv6 peers



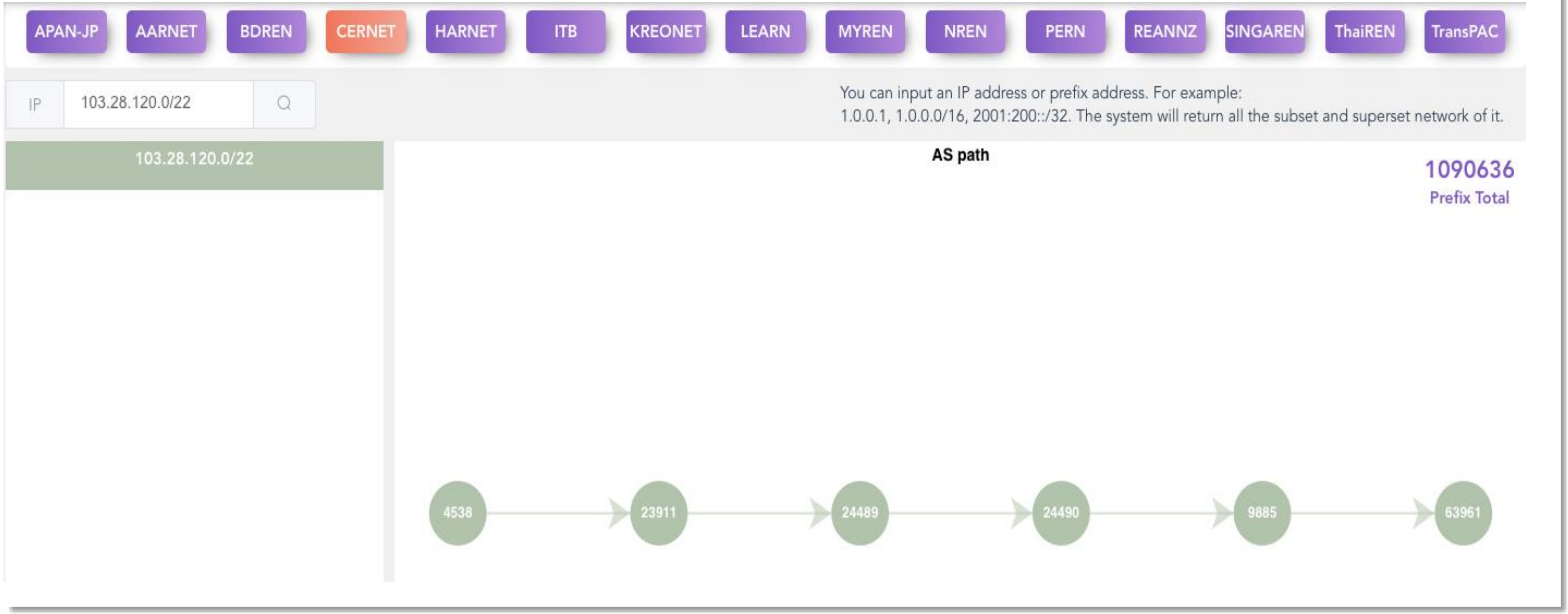
IPv4 Peers

IPv6 Peers

All Peer information is available at the bottom

2. Routing Path – IPv4

- Routing Path => Routing Path



103.28.120.0/22

You can input an IP address or prefix address. For example:
1.0.0.1, 1.0.0.0/16, 2001:200::/32. The system will return all the subset and superset network of it.

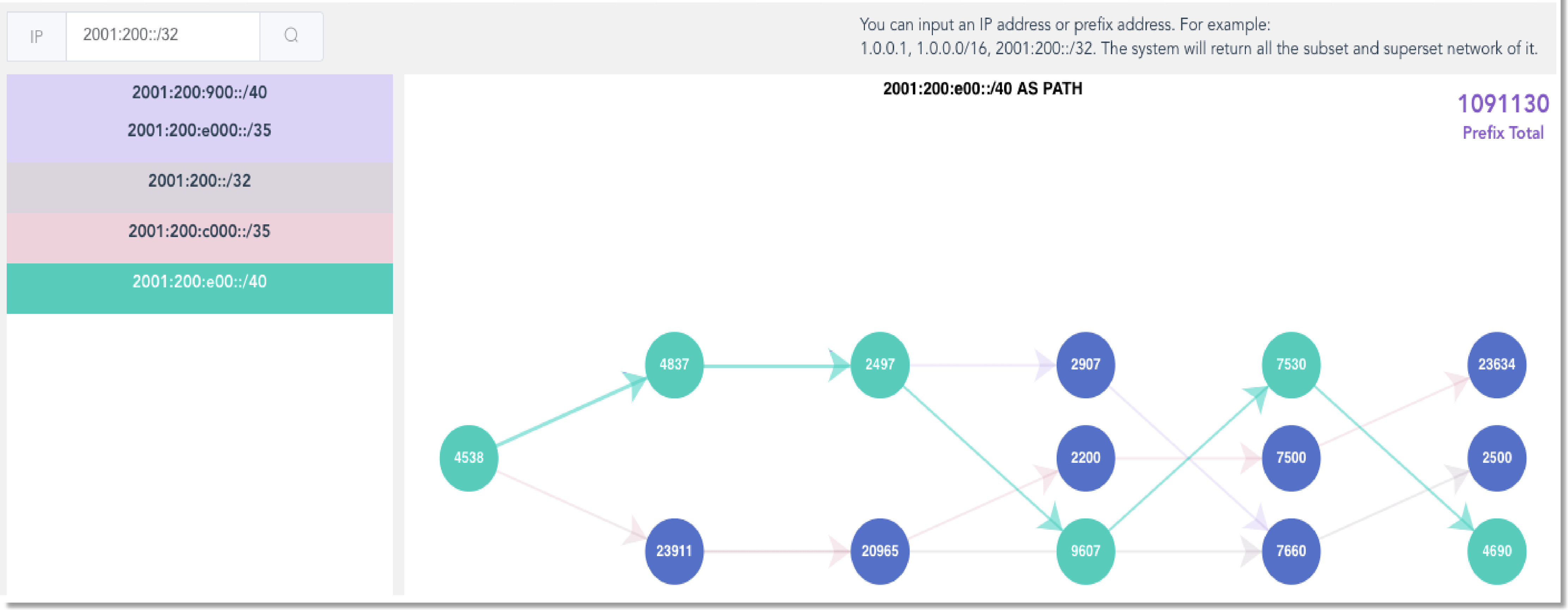
103.28.120.0/22

AS path

1090636
Prefix Total

2. Routing Path – IPv6

- Routing Path => Routing Path



You can input an IP address or prefix address. For example:
1.0.0.1, 1.0.0.0/16, 2001:200::/32. The system will return all the subset and superset network of it.

2001:200:900::/40

2001:200:e000::/35

2001:200::/32

2001:200:c000::/35

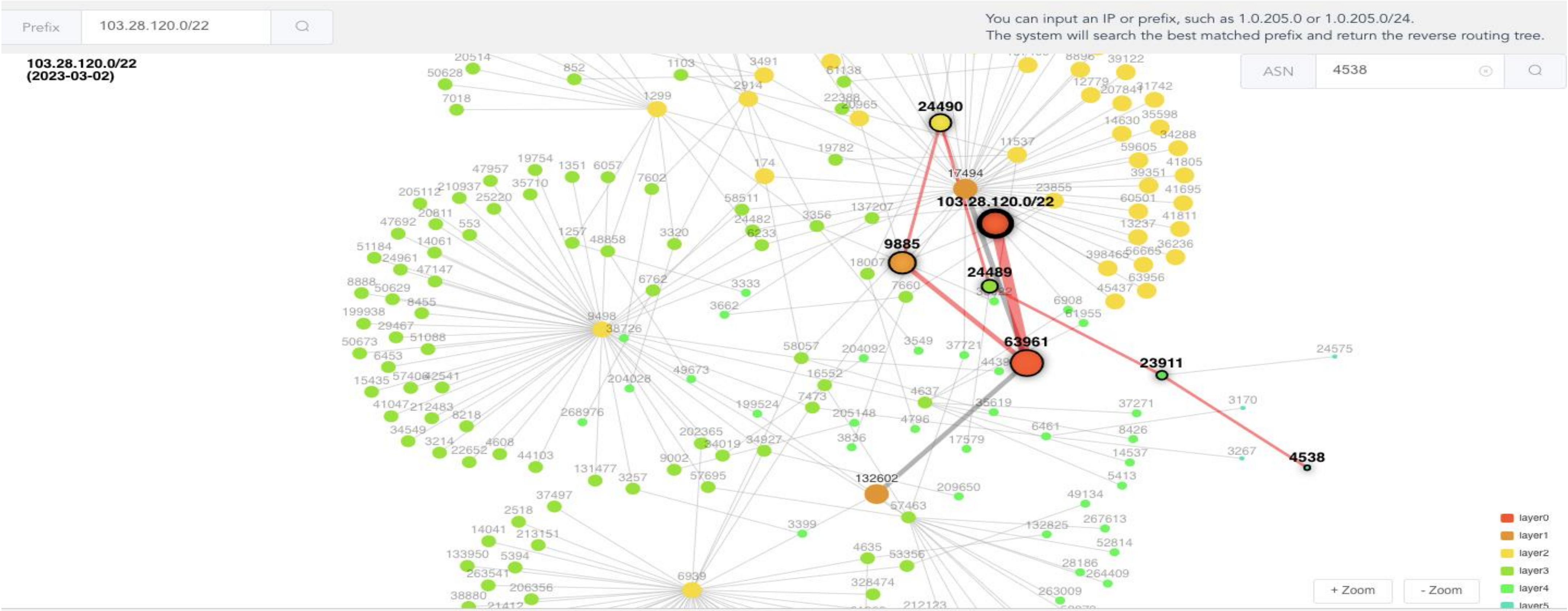
2001:200:e00::/40

2001:200:e00::/40 AS PATH

1091130
Prefix Total

Routing Topology

- Routing Path => Reverse Routing Path (TOPO)



Prefix 103.28.120.0/22

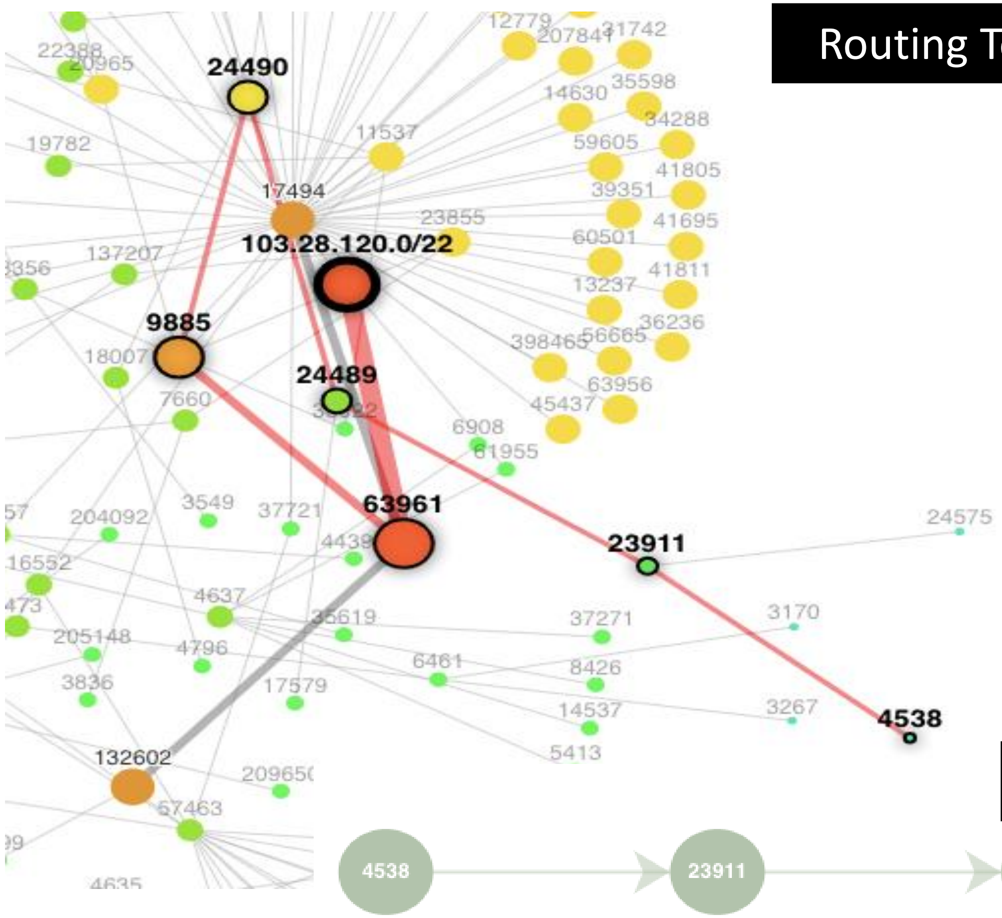
You can input an IP or prefix, such as 1.0.205.0 or 1.0.205.0/24.
The system will search the best matched prefix and return the reverse routing tree.

103.28.120.0/22
(2023-03-02)

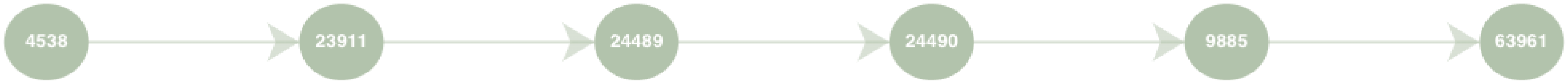
ASN 4538

Matching Routing Path with Topology

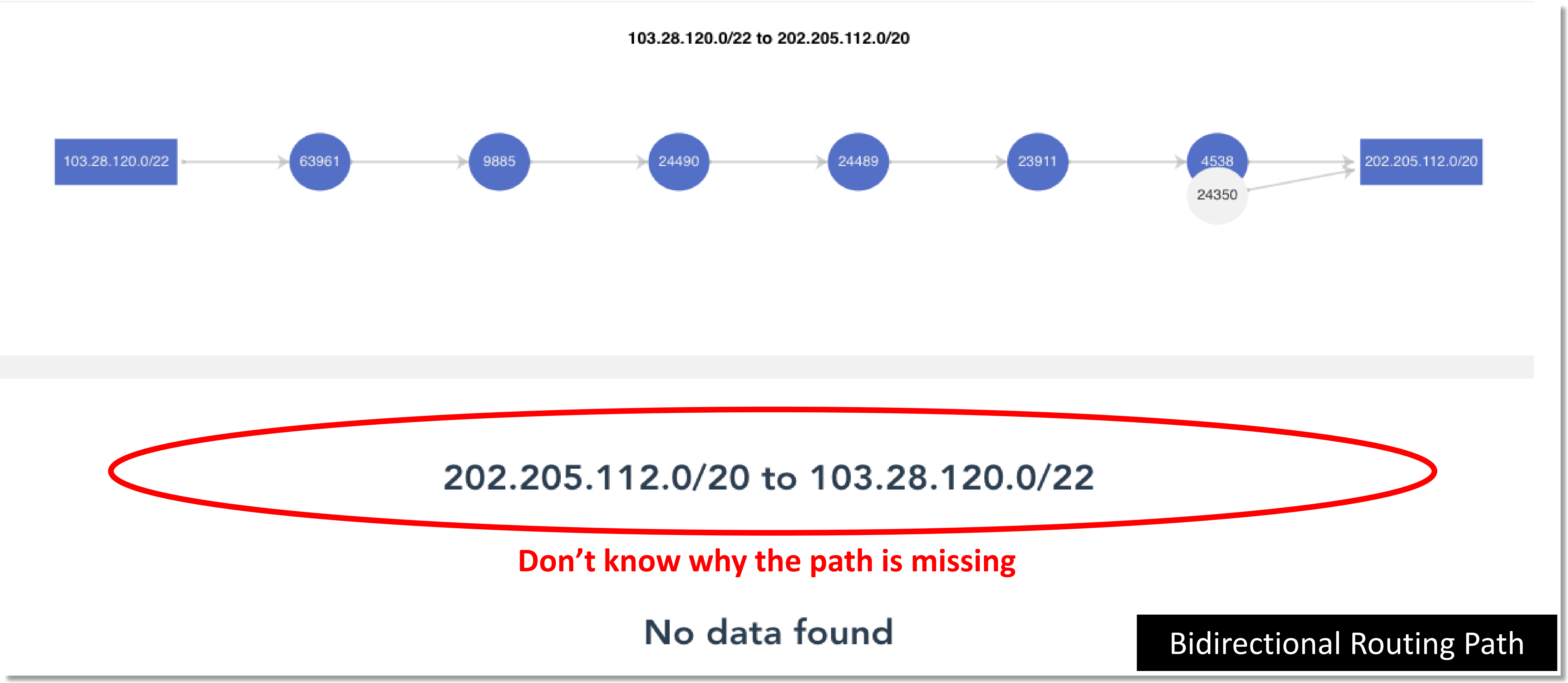
Routing Topology



Routing Path


4538 → 23911 → 24489 → 24490 → 9885 → 63961

Bidirectional Routing Path



103.28.120.0/22 to 202.205.112.0/20

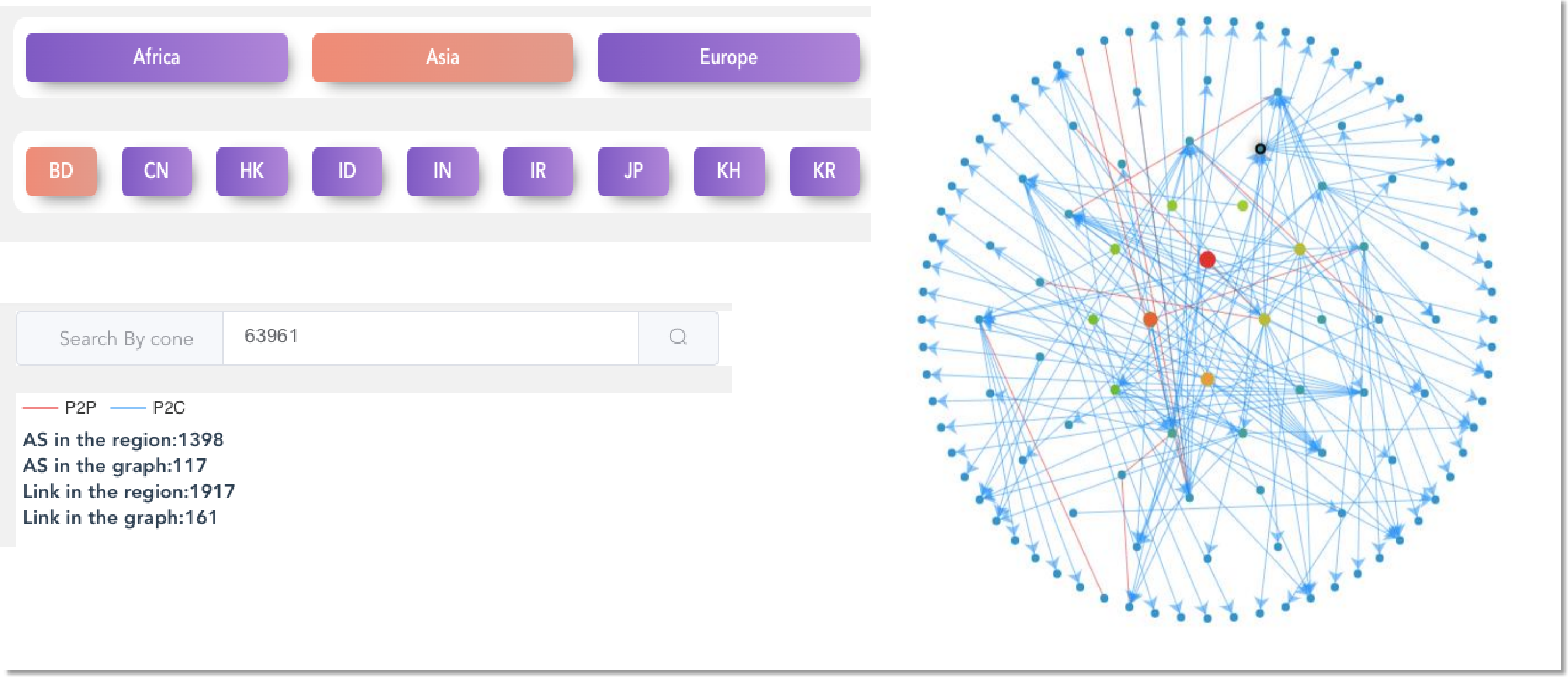
202.205.112.0/20 to 103.28.120.0/22

Don’t know why the path is missing

No data found

Bidirectional Routing Path

3. Rating ASN based on Cone size



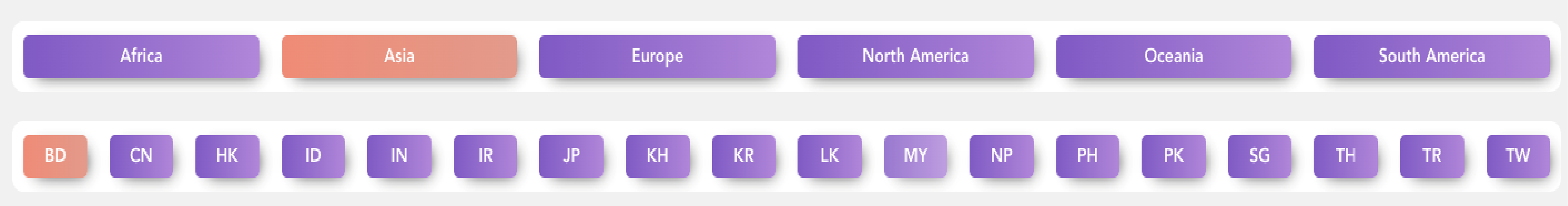
Search By cone: 63961

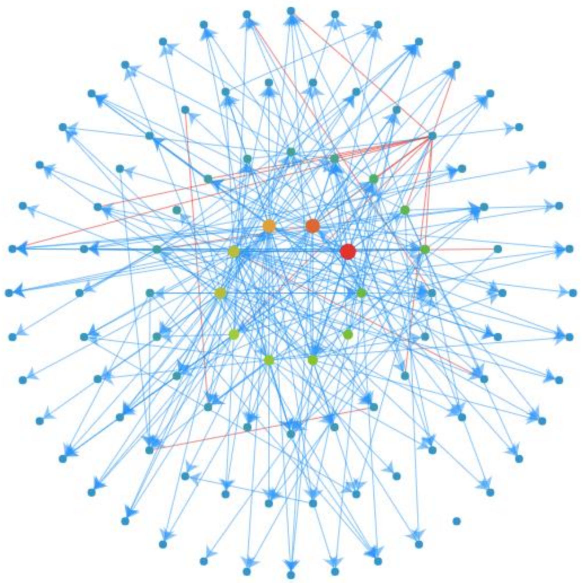
P2P P2C

AS in the region:1398
AS in the graph:117
Link in the region:1917
Link in the graph:161

Connect
Collaborate
Innovate

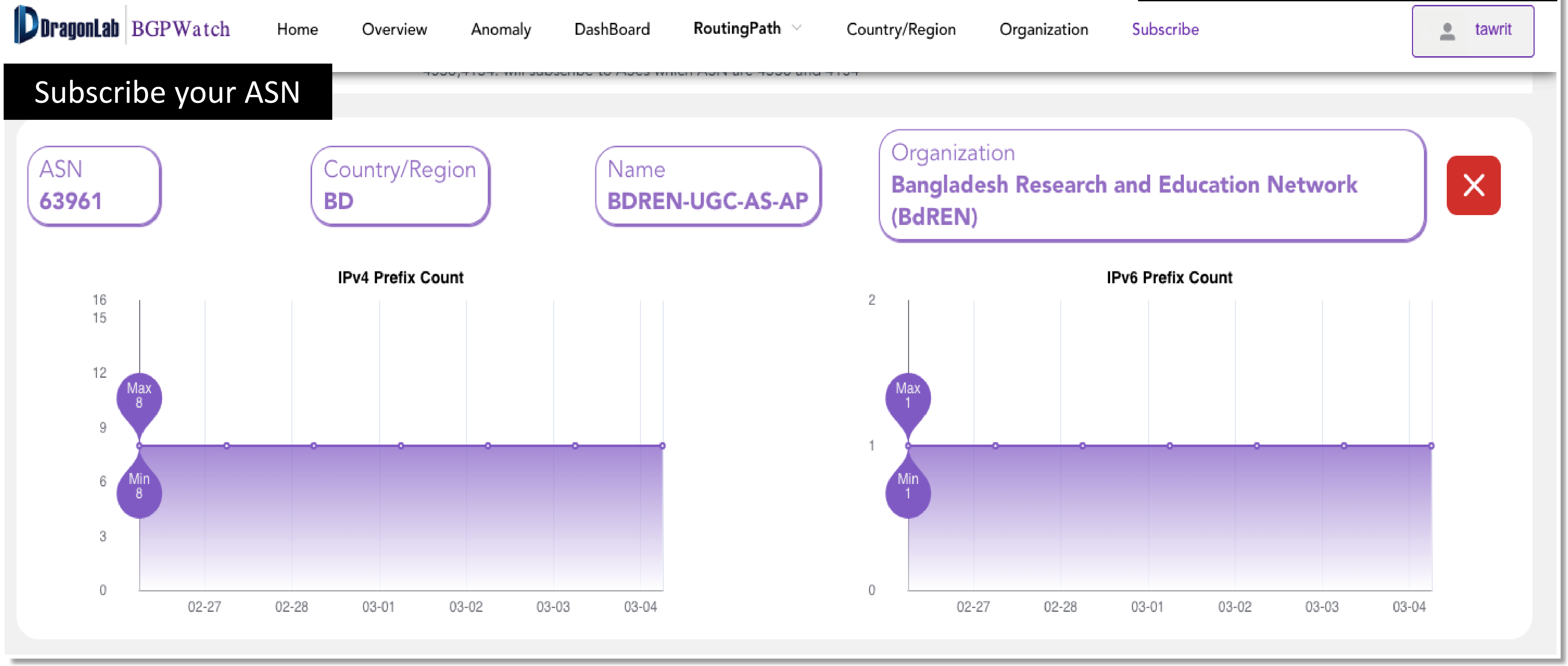
3. Ranking organizations on Cone Size





- Can we mention the name of the Top-10 organizations and their cone size next to the diagram? That will give an idea about the top service providers in each country.

4. Subscribing your Autonomous System



Register and Login

Subscribe your ASN

ASN
63961

Country/Region
BD

Name
BDREN-UGC-AS-AP

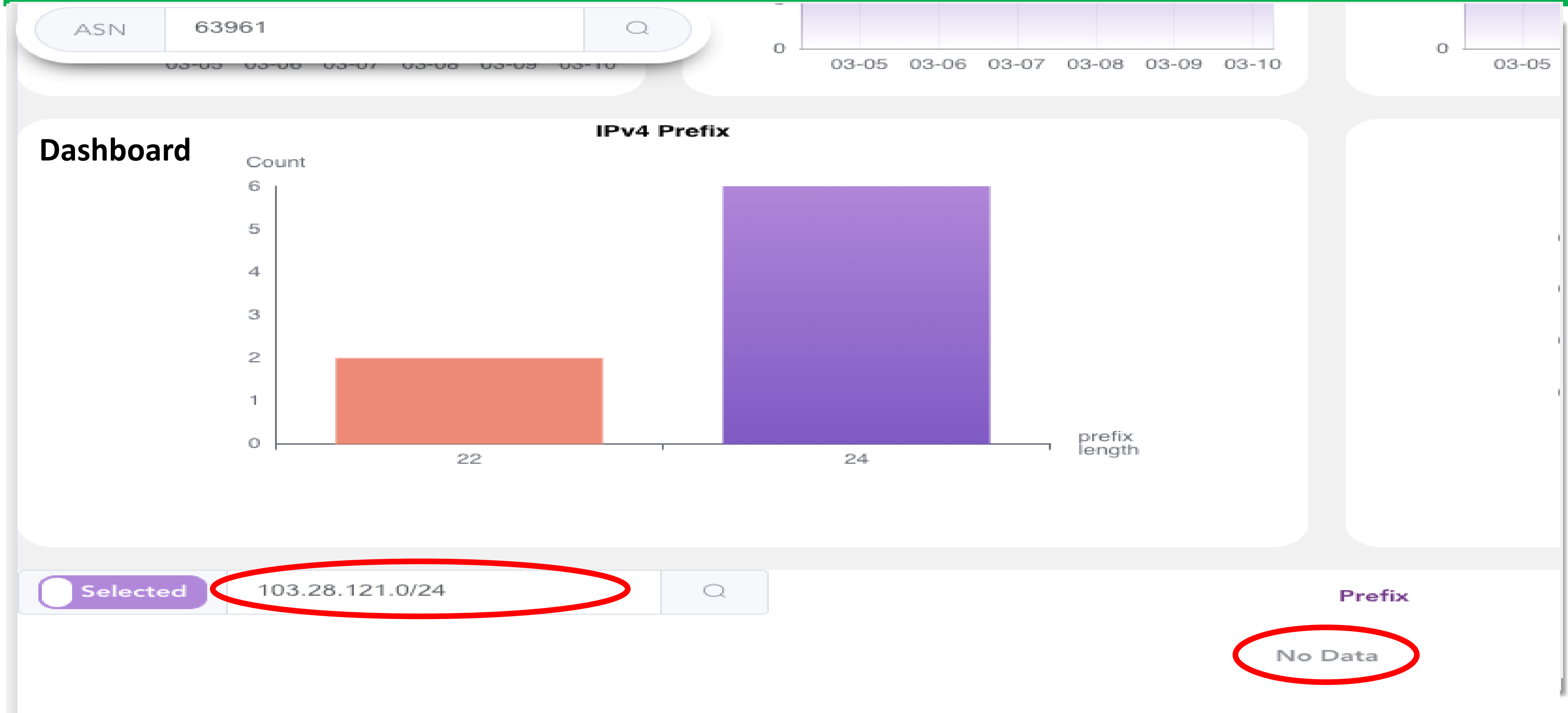
Organization
Bangladesh Research and Education Network (BdREN)

Suggested Changes => Prefix Search

Connect
Collaborate
Innovate

- In the “Dashboard”, it searches advertised prefixes but there is no subnet-wise search. Suppose, it will find out 103.28.120.0/22 under BdREN but cannot locate 103.28.121.0/24. The facility is available in “Reverse Routing Path” and “Reverse Routing Topology” part.

Suggested Changes => Prefix Search



ASN 63961

Dashboard

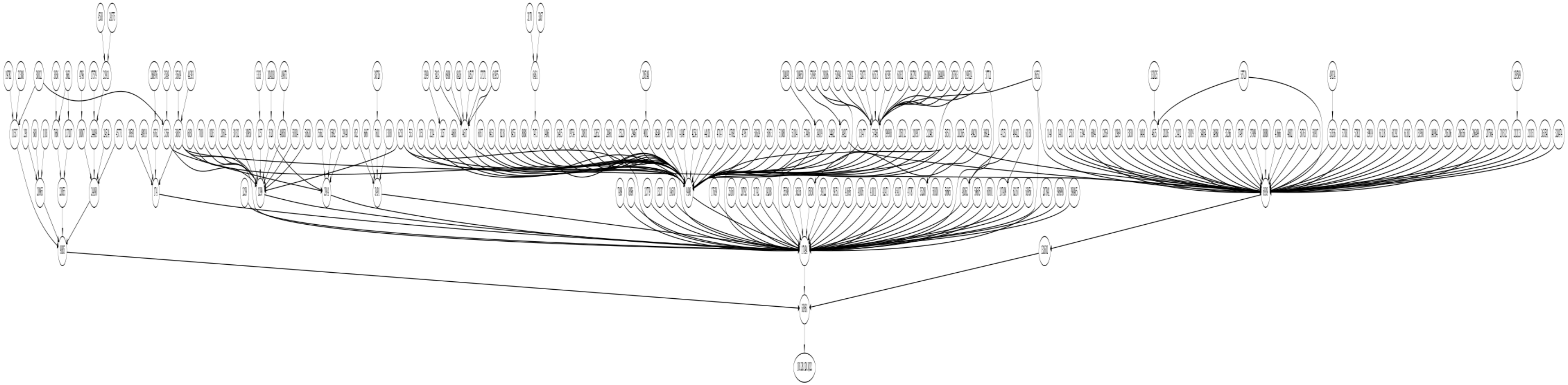
Selected 103.28.121.0/24

Prefix

No Data

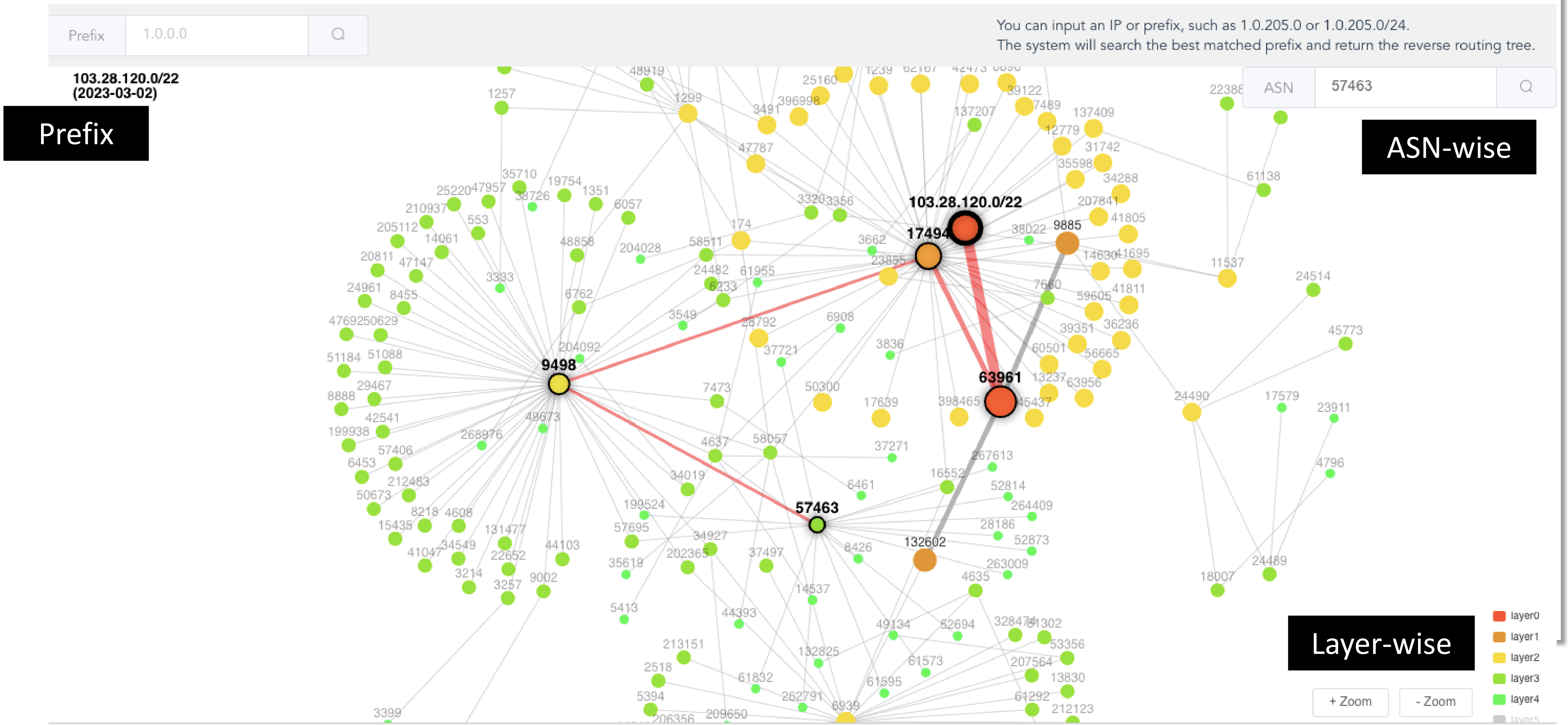
Routing Topology vs Reverse Routing Path

- “Reverse Route Topology” provides additional information than “Reverse Route Path”, hence there is not much usage of “Reverse Route Path”.



- It generates a file in “image” format which also doesn’t provide a legible view when enlarged. Better if it could be made available in pdf format.

Routing Topology vs Reverse Routing Path



Prefix 1.0.0.0

You can input an IP or prefix, such as 1.0.205.0 or 1.0.205.0/24.
The system will search the best matched prefix and return the reverse routing tree.

103.28.120.0/22
(2023-03-02)

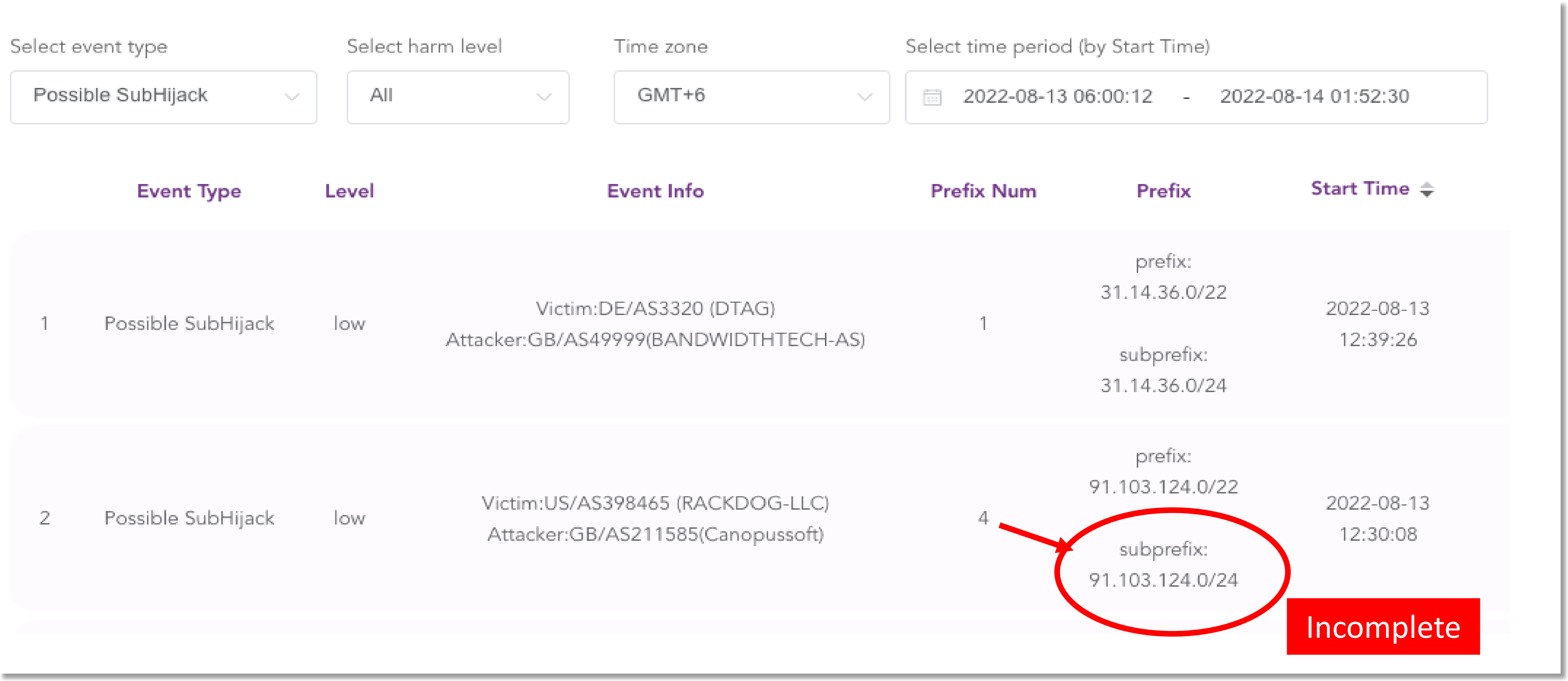
ASN 57463

Prefix

ASN-wise

Layer-wise

4. Reporting Anomaly



Select event type: Possible SubHijack

Select harm level: All

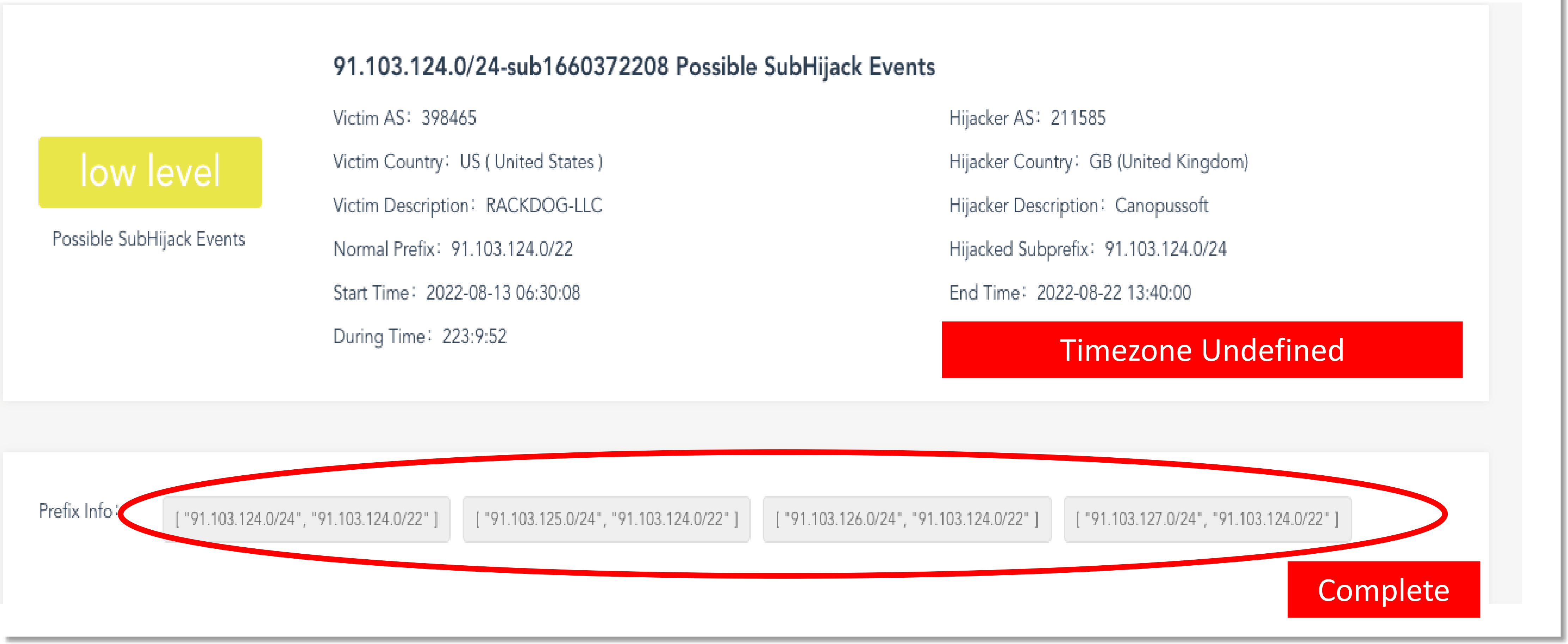
Time zone: GMT+6

Select time period (by Start Time): 2022-08-13 06:00:12 - 2022-08-14 01:52:30

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time
1	Possible SubHijack	low	Victim:DE/AS3320 (DTAG) Attacker:GB/AS49999(BANDWIDTHTECH-AS)	1	prefix: 31.14.36.0/22 subprefix: 31.14.36.0/24	2022-08-13 12:39:26
2	Possible SubHijack	low	Victim:US/AS398465 (RACKDOG-LLC) Attacker:GB/AS211585(Canopussoft)	4	prefix: 91.103.124.0/22 subprefix: 91.103.124.0/24	2022-08-13 12:30:08

Incomplete

Suggested Changes=>Anomaly and Prefixes



low level

Possible SubHijack Events

91.103.124.0/24-sub1660372208 Possible SubHijack Events

Victim AS：398465

Victim Country：US (United States)

Victim Description：RACKDOG-LLC

Normal Prefix：91.103.124.0/22

Start Time：2022-08-13 06:30:08

During Time：223:9:52

Hijacker AS：211585

Hijacker Country：GB (United Kingdom)

Hijacker Description：Canopussoft

Hijacked Subprefix：91.103.124.0/24

End Time：2022-08-22 13:40:00

Timezone Undefined

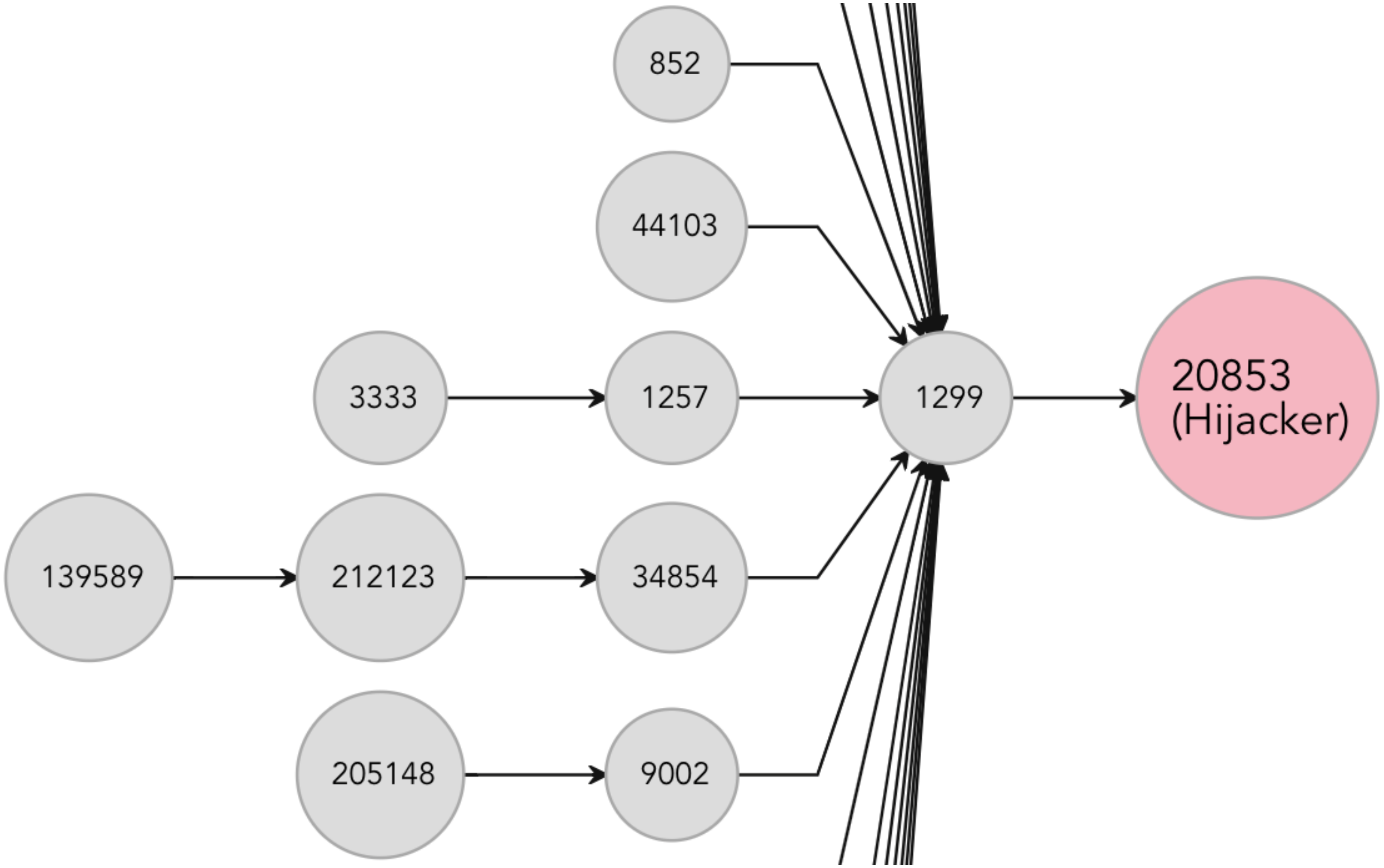
Prefix Info：["91.103.124.0/24", "91.103.124.0/22"] ["91.103.125.0/24", "91.103.124.0/22"] ["91.103.126.0/24", "91.103.124.0/22"] ["91.103.127.0/24", "91.103.124.0/22"]

Complete

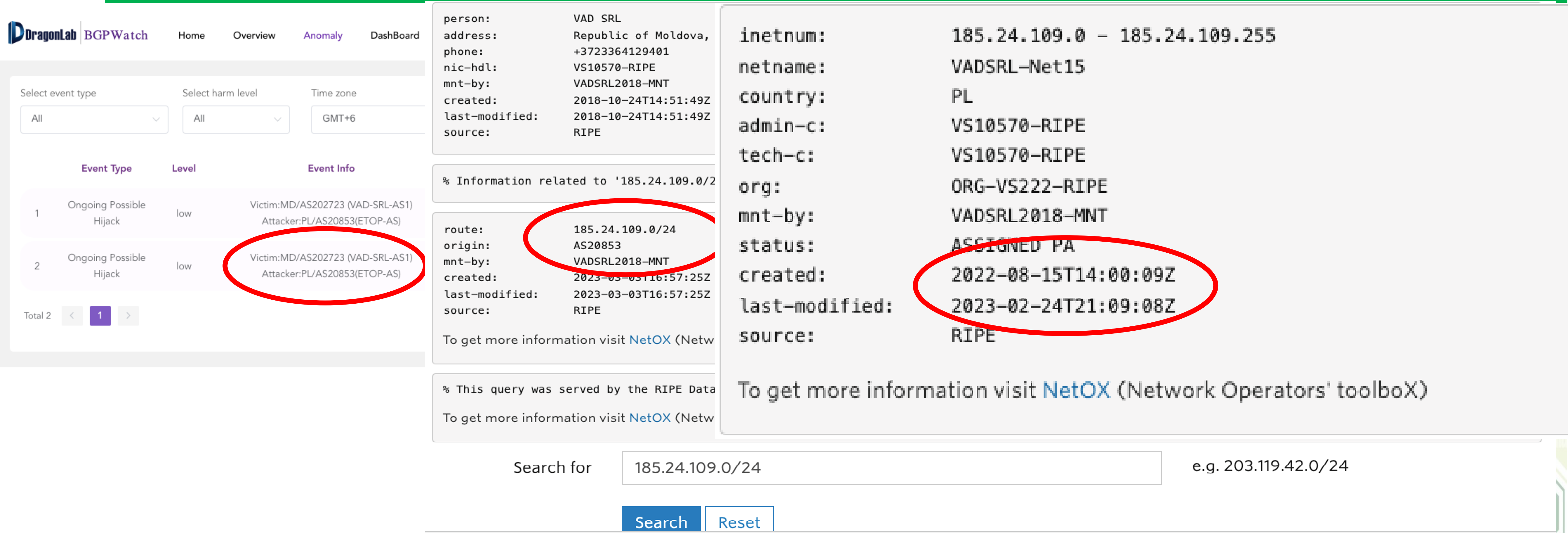
Recommendations => Remedial Measures

- Once the “Hijacker” is suspected, can we warn the suspected entity AS20853 along with its upstream provider AS 1299 with emails.

- The process may be automatized if we can collect the administrative contacts of each AS from APNIC.



False Alarm



Select event type: All

Select harm level: All

Time zone: GMT+6

	Event Type	Level	Event Info
1	Ongoing Possible Hijack	low	Victim:MD/AS202723 (VAD-SRL-AS1) Attacker:PL/AS20853(ETOP-AS)
2	Ongoing Possible Hijack	low	Victim:MD/AS202723 (VAD-SRL-AS1) Attacker:PL/AS20853(ETOP-AS)

Total 2

```
person:         VAD SRL
address:        Republic of Moldova,
phone:          +3723364129401
nic-hdl:        VS10570-RIPE
mnt-by:         VADSRL2018-MNT
created:        2018-10-24T14:51:49Z
last-modified:  2018-10-24T14:51:49Z
source:         RIPE
```

```
% Information related to '185.24.109.0/2
```

```
route:          185.24.109.0/24
origin:         AS20853
mnt-by:         VADSRL2018-MNT
created:        2023-03-03T16:57:25Z
last-modified:  2023-03-03T16:57:25Z
source:         RIPE
```

To get more information visit NetOX (Netw

```
% This query was served by the RIPE Data
```

To get more information visit NetOX (Netw

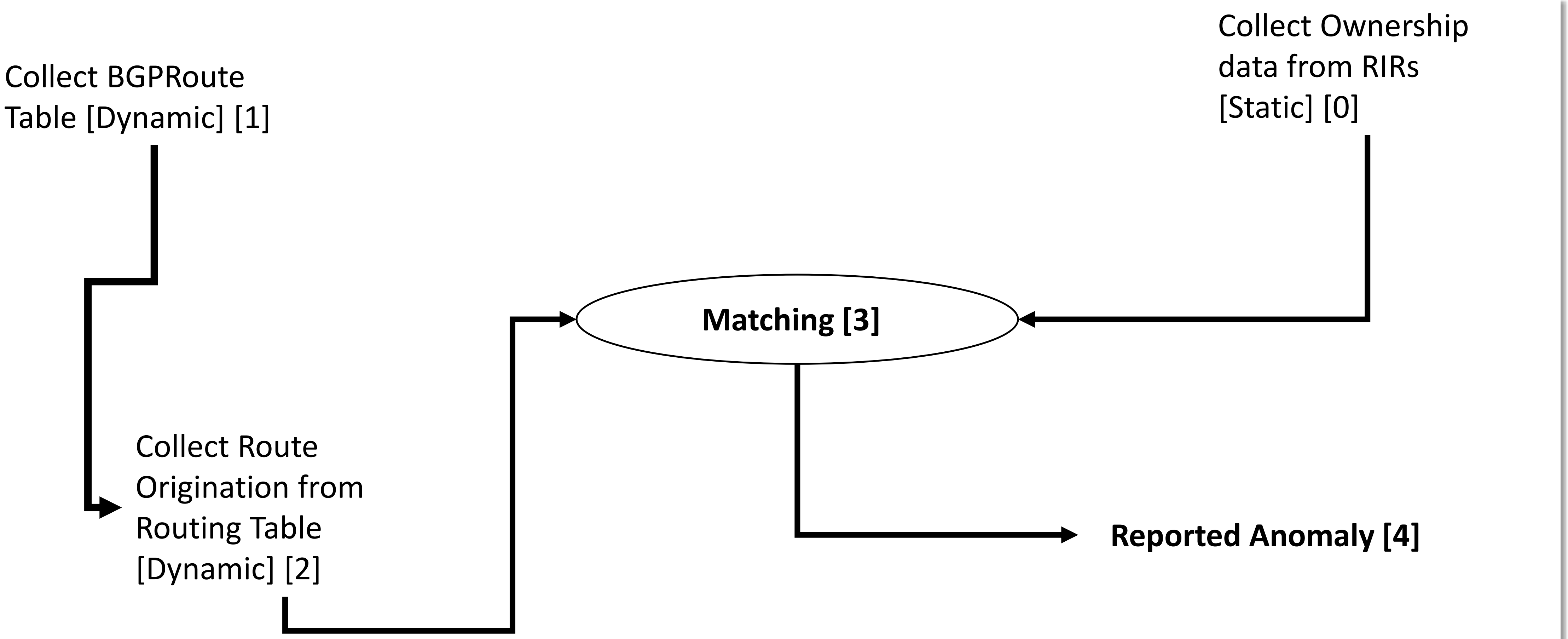
```
inetnum:        185.24.109.0 - 185.24.109.255
netname:        VADSRL-Net15
country:        PL
admin-c:        VS10570-RIPE
tech-c:         VS10570-RIPE
org:            ORG-VS222-RIPE
mnt-by:         VADSRL2018-MNT
status:         ASSIGNED PA
created:        2022-08-15T14:00:09Z
last-modified:  2023-02-24T21:09:08Z
source:         RIPE
```

To get more information visit NetOX (Network Operators' toolboX)

Search for: 185.24.109.0/24 e.g. 203.119.42.0/24

Needs to verify the problems in the algorithm, if any.

False Alarm



Collect BGPRoute Table [Dynamic] [1]

Collect Ownership data from RIRs [Static] [0]

Matching [3]

Collect Route Origination from Routing Table [Dynamic] [2]

Reported Anomaly [4]

Suggested Changes

- If you want to search an “Organization” using name, AS-name or AS-number you have to go to the “Organization” menu
  - Organization Name is “Case sensitive”, better if it is made “Case insensitive”
- The prefixes in “Dashboard=>IPv4 Peers” and that of “Routing Path” should match.
- Needs to put the “last date of update” for the records which will be periodically updated.

Recommendations

- The ”Working Groups” should be more active and should work with the goal of “transferring the technology”.
- Number of Adjacencies should be increased to make the BGP Portal more effective by reporting the reverse routing path.

THANK YOU

BdREN

Connect
Collaborate
Innovate