(APNIC Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

--The 4th Technical Committee Meeting

Sep 29, 2022

清華大學 Tsinghua University

APNIC FOUNDATION

Outline

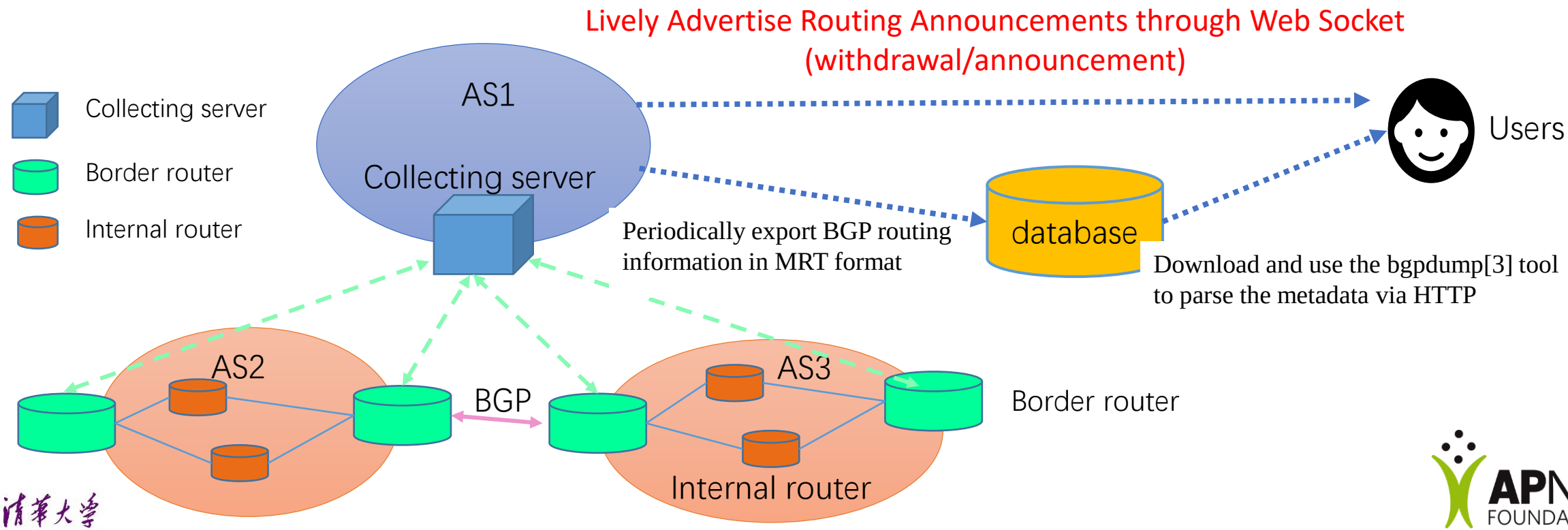
- Progress and Plan
- Detailed Project Progress in Last Three Month
  - BGP sharing platform
  - Looking Glass platform
  - Analyzing and Diagnosing Platform
  - Research Topic
- Future Plan
- Comments/Suggestions

Progress and Plan

Objectives	Detail work	Status
Build a collaborative community for enhancing the capacity of NRENs' network operation and measurement	Setting up project website	Finished in May
	Collaborative Work	See the next slides
	Platform development and deployment	See below
Establish a distributed BGP routing monitoring platform and a looking glass platform in the Asia-Pacific region	BGP Routing Information Sharing	13 partners
	Looking Glass Platform	6 partners
	Tools for operator(dashboard, routing path search, register and alarm email)	Partially done, still need improvement
Deploy a BGP hijacking detection and mitigation system and analyze the robustness of routing in the Asia-Pacific region	Development of prefix hijacking detection	Partially done, still need improvement
	Development of path hijacking detection	Oct – next June
	Research Paper: region resilience	The draft will be discussed in Oct
	Research Paper: routing hijacking detection	The draft will be discussed in Nov/Dec
Share knowledge and experience globally	RPKI, MANRS, BGPSEC, etc.(tbd)	Nov/Dec, next Apr/May
	paper, technical document	Keep updating

CGTF-RIS: Route Information Sharing

- Collecting server： Use routing FRR[2] to simulate a real BGP router
- Border routers: Connect with the collecting server by BGP peering
- Feature: Lively Advertise Routing Announcements



清華大學 Tsinghua University

APNIC FOUNDATION

BGP Route Information Sharing

We have established BGP session with 13 partners.
Data can be accessed at https://bgp.cgtf.net
Configuration manual can be accessed at
https://www.bgper.net/index.php/document/

No.	Partner	No.	Partner
1	APAN-JP	8	MYREN
2	BDREN	9	PERN
3	CERNET	10	REANNZ
4	HARNET	11	SINGAREN
5	ITB	12	ThaiSARN
6	KREONET	13	TransPAC
7	LEARN		

Index of /ribs/2022/07

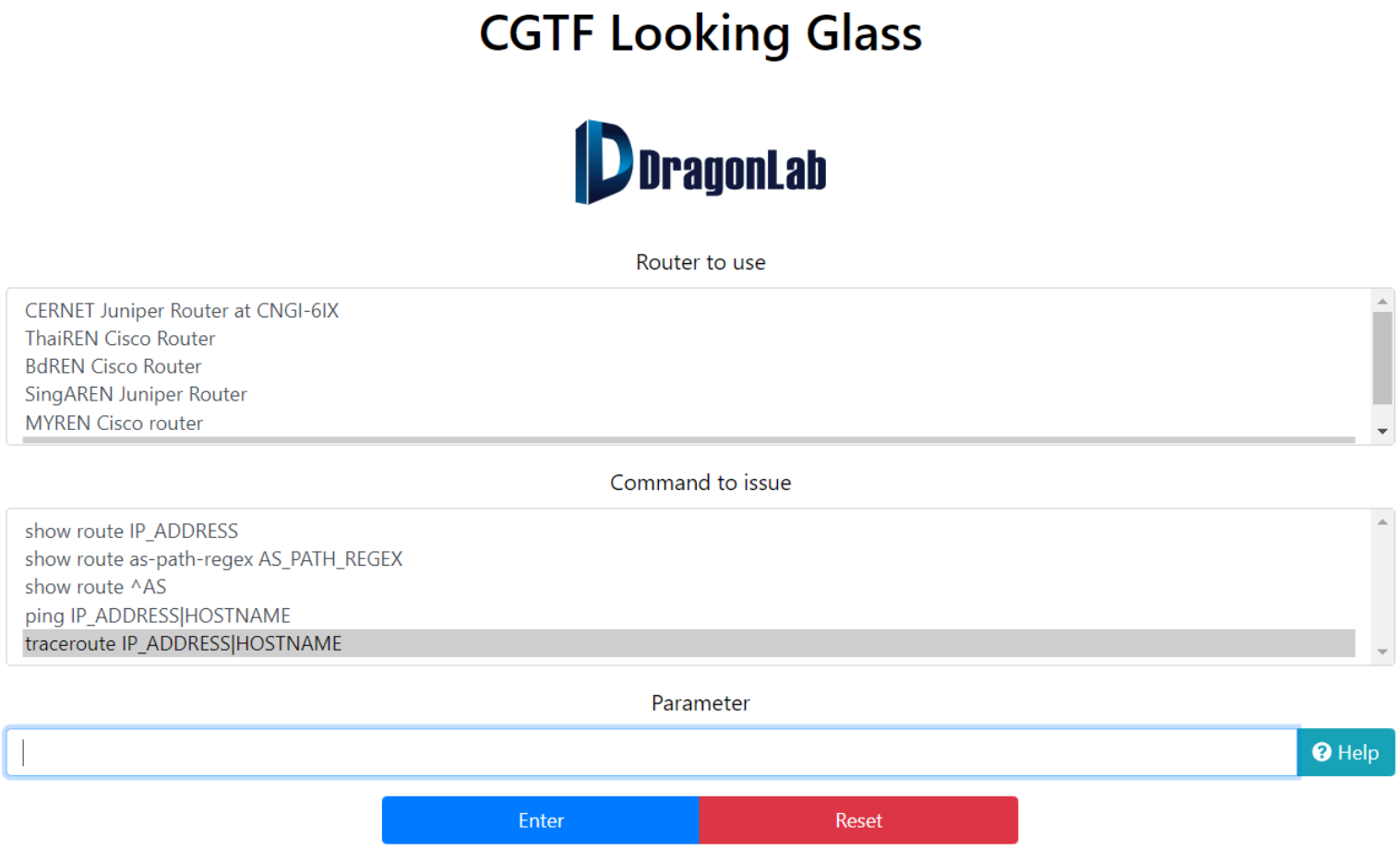
Name	Last modified	Size	Description
rib.20220730.0600.mrt.bz2	2022-07-30 06:00	13M	
rib.20220730.0800.mrt.bz2	2022-07-30 08:00	13M	
rib.20220730.1000.mrt.bz2	2022-07-30 10:00	13M	
rib.20220730.1200.mrt.bz2	2022-07-30 12:00	13M	
rib.20220730.1400.mrt.bz2	2022-07-30 14:00	13M	
rib.20220730.1600.mrt.bz2	2022-07-30 16:00	13M	
rib.20220730.1800.mrt.bz2	2022-07-30 18:00	13M	
rib.20220730.2000.mrt.bz2	2022-07-30 20:00	13M	
rib.20220730.2200.mrt.bz2	2022-07-30 22:00	13M	
rib.20220731.0000.mrt.bz2	2022-07-31 00:00	13M	
rib.20220731.0200.mrt.bz2	2022-07-31 02:00	13M	
rib.20220731.0400.mrt.bz2	2022-07-31 04:00	13M	
rib.20220731.0600.mrt.bz2	2022-07-31 06:00	13M	
rib.20220731.0800.mrt.bz2	2022-07-31 08:00	13M	
rib.20220731.1000.mrt.bz2	2022-07-31 10:00	13M	

清華大學 Tsinghua University

APNIC FOUNDATION

CGTF Looking Glass

- https://lg.cgtf.net
- Open Source:
  - https://github.com/gmazoyer/looking-glass
- 6 Education & Research network joined
- 5 commands
- Query speed limit for security
- More partners is welcomed

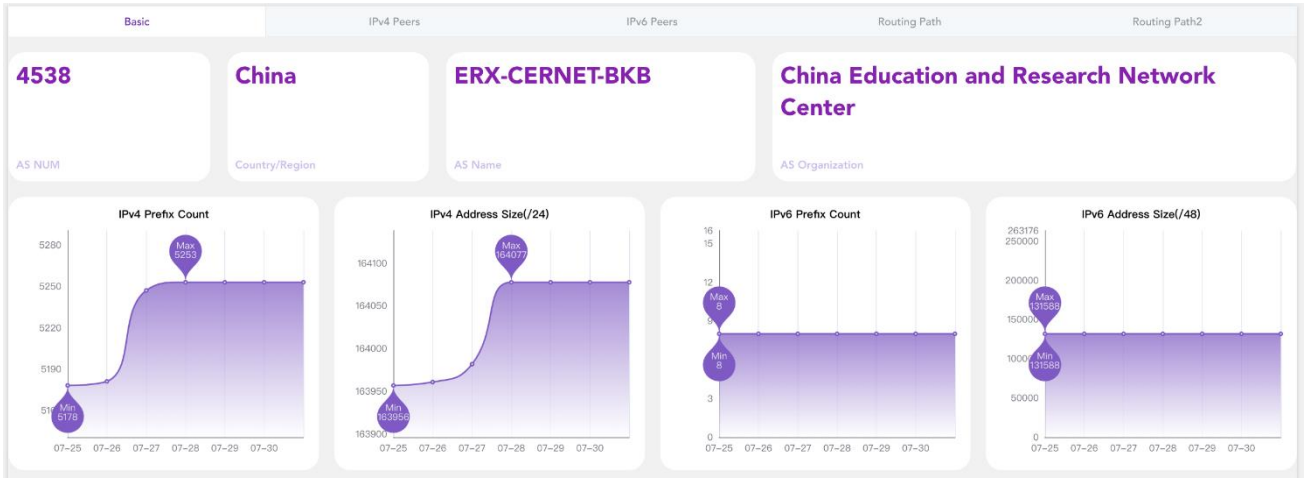


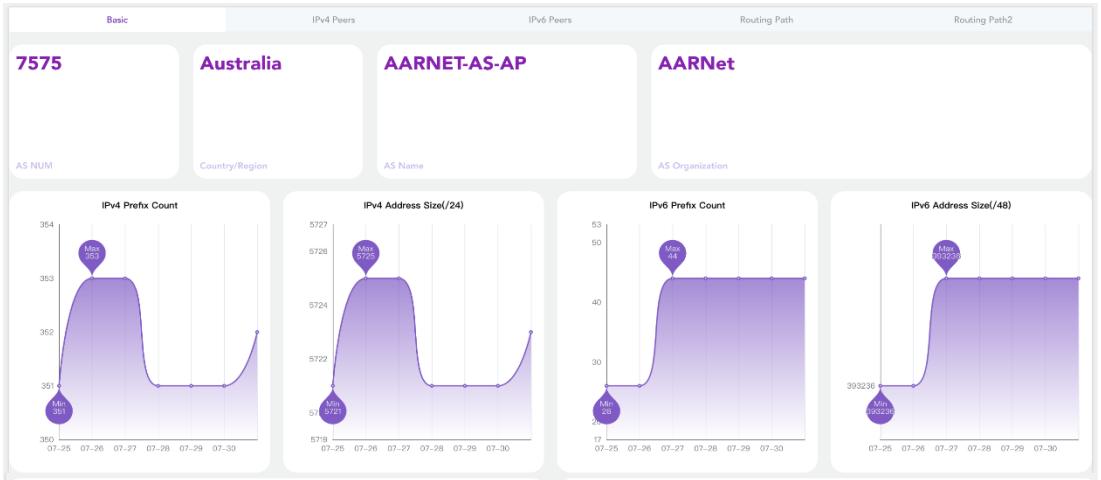
We'll focus on this work in Oct to Dec

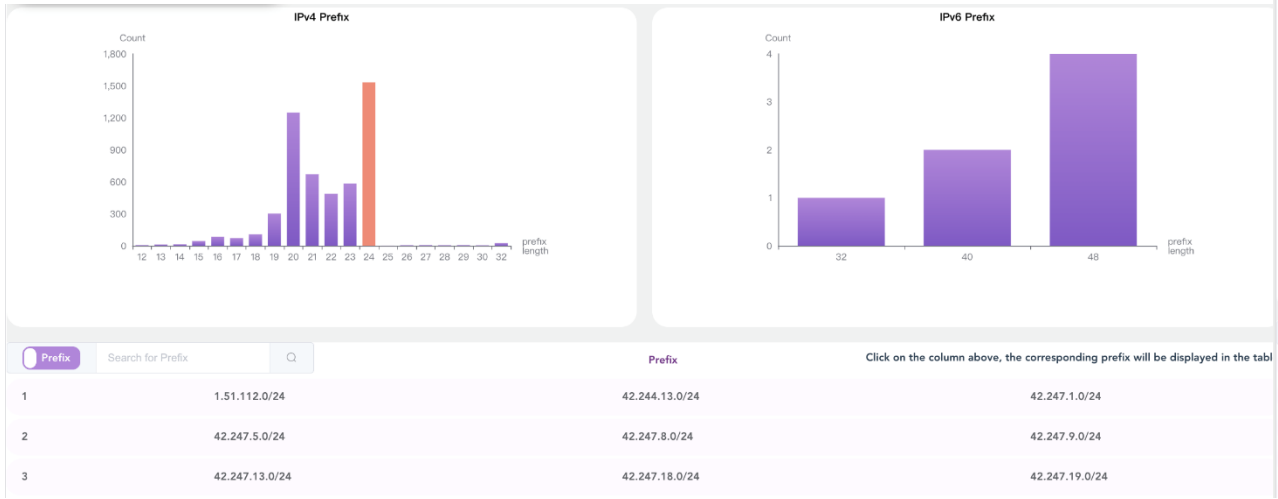
清華大學 Tsinghua University

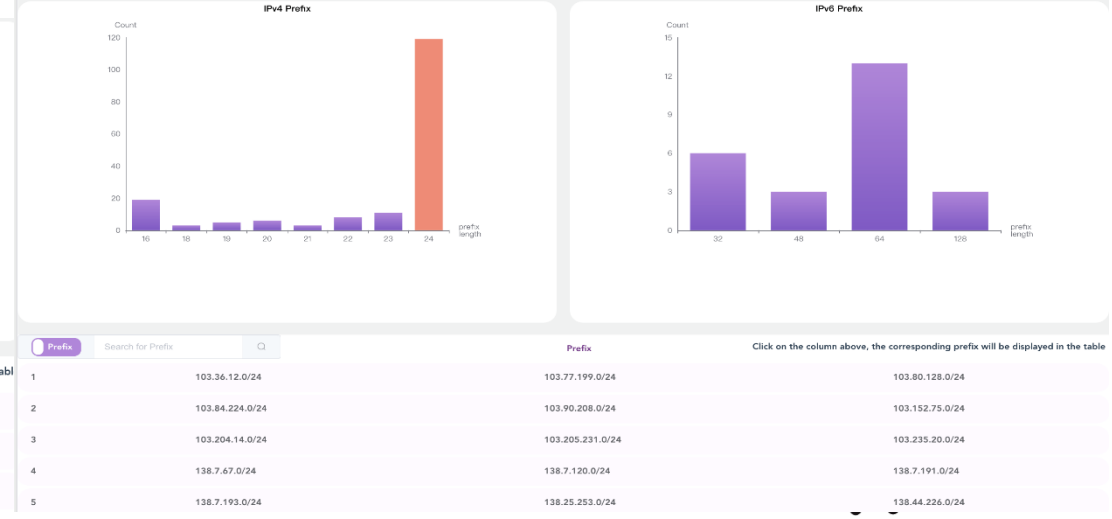
APNIC FOUNDATION

Tools for operator –Dashboard







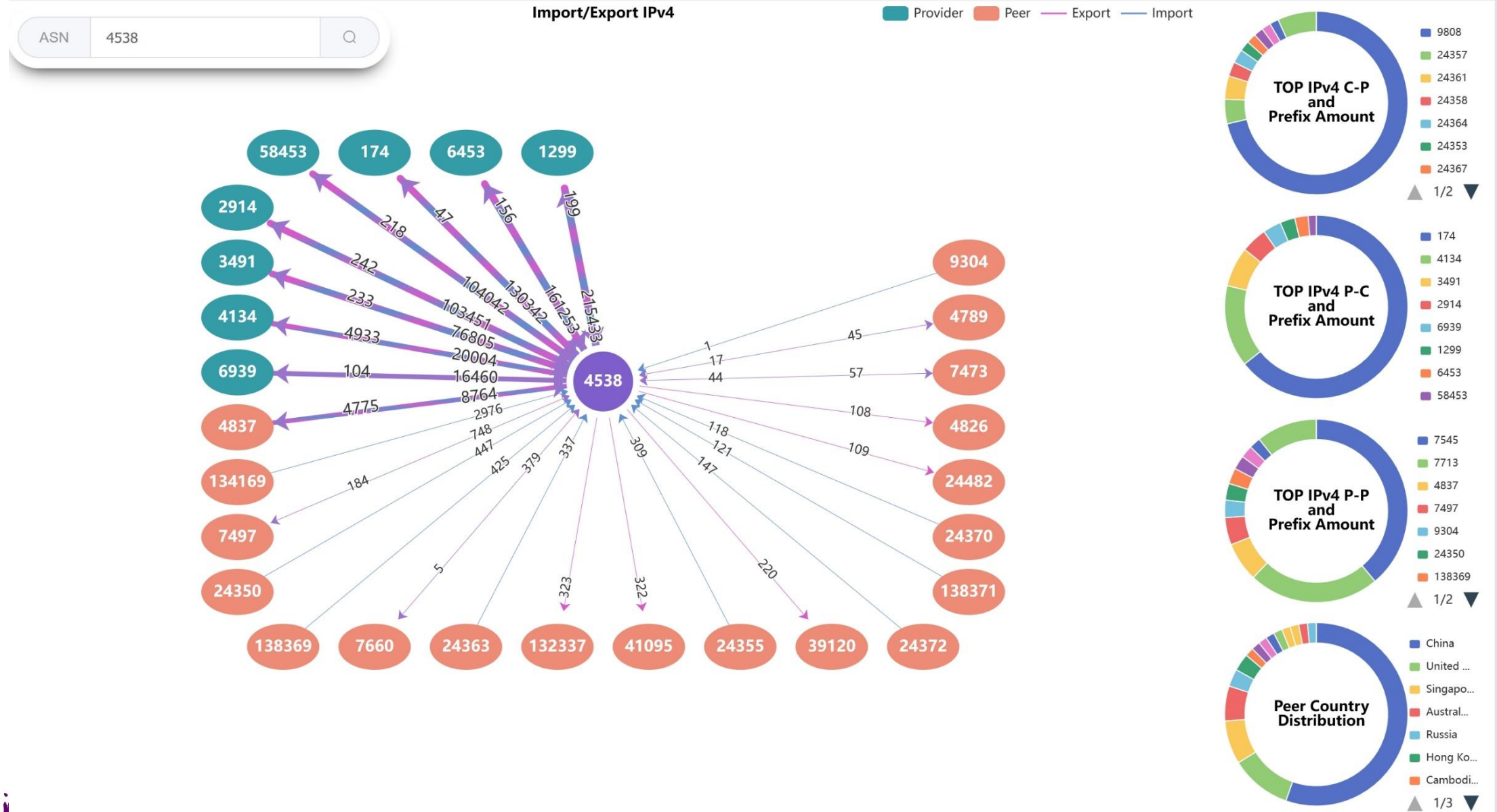


https://bgpwatch.cgtf.net

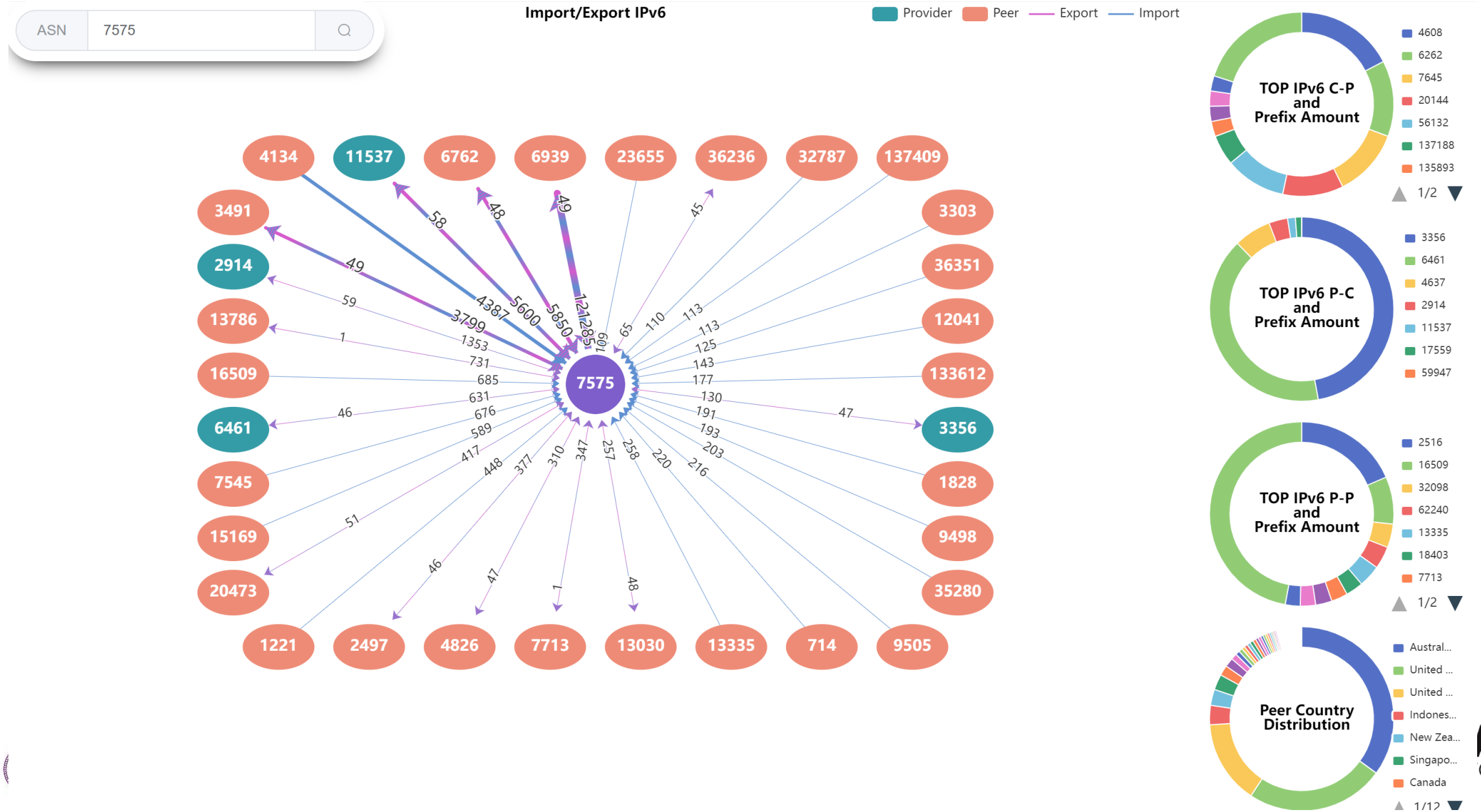
清華大學 Tsinghua University

APNIC FOUNDATION

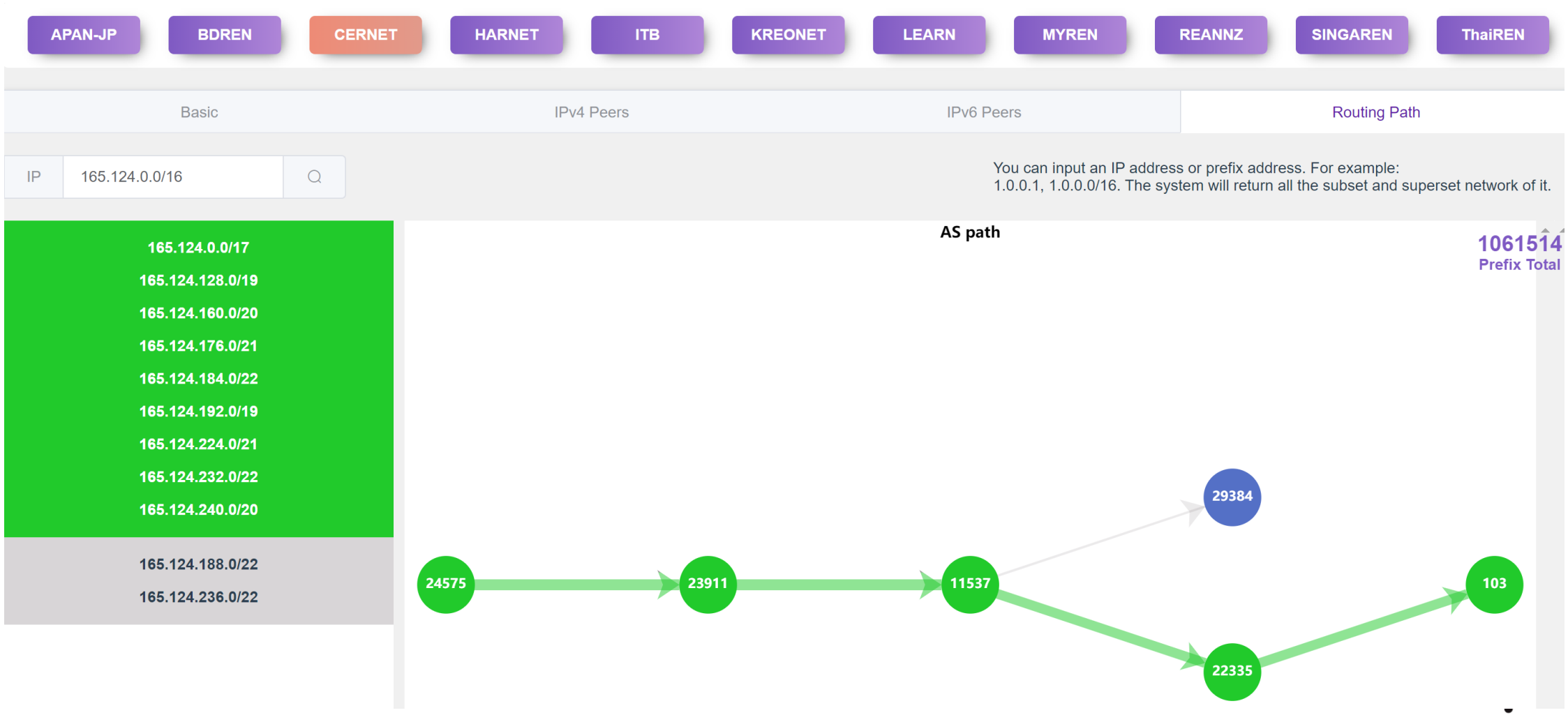
Tools for operator – IPv4 Key Peers



Tools for operator – IPv6 Peers



Tools for operator – Routing Path Search

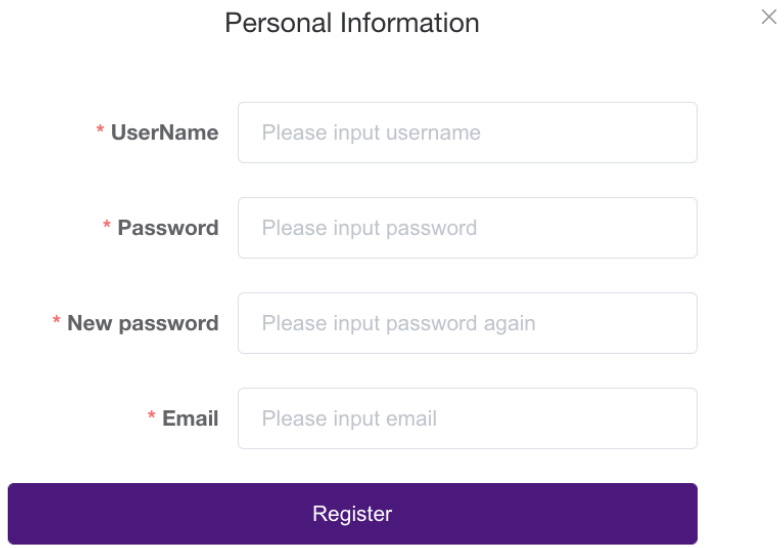


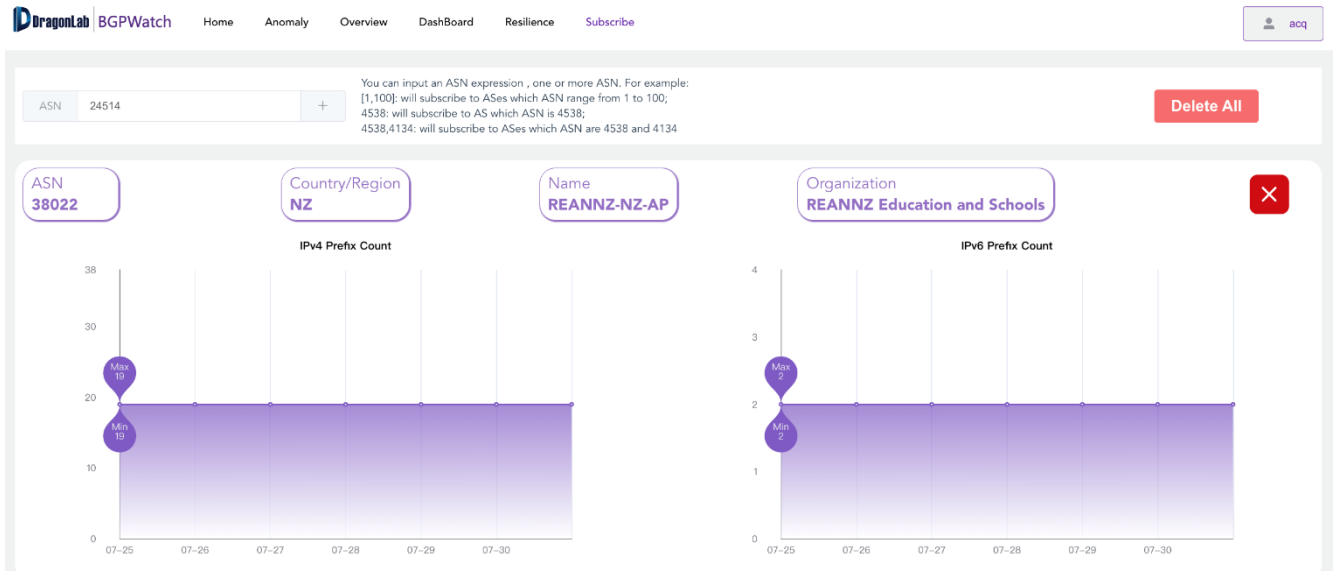
Return paths of all sub networks and super networks of the input prefix.
Group Prefixes with the same routing path .

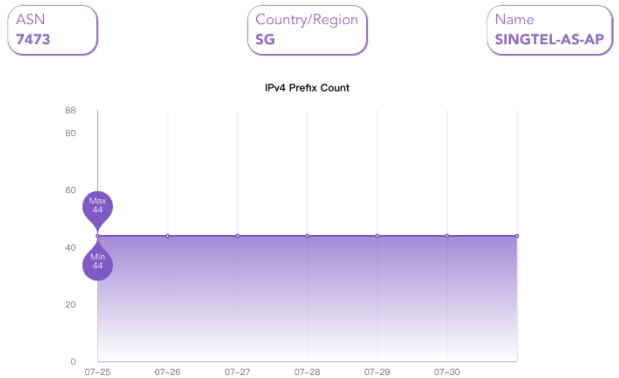
清華大學 Tsinghua University

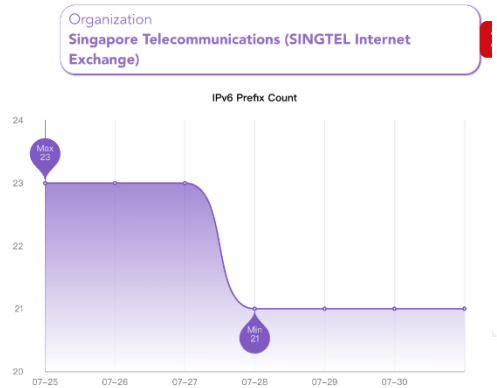
APNIC FOUNDATION

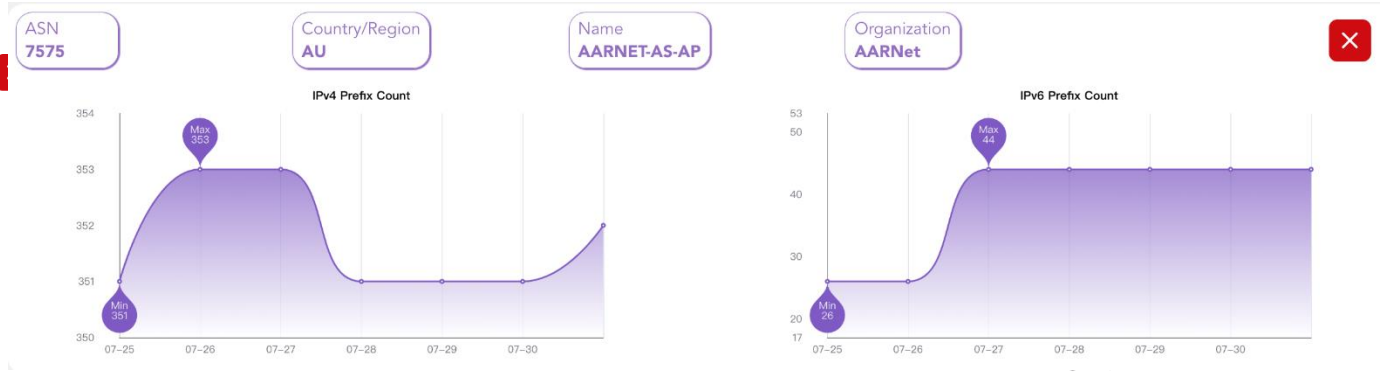
Tools for operator – Register and Subscribe AS











清華大學 Tsinghua University

APNIC FOUNDATION

Tools for operator – Send Alarm Email to Subscriber

ASN
4538

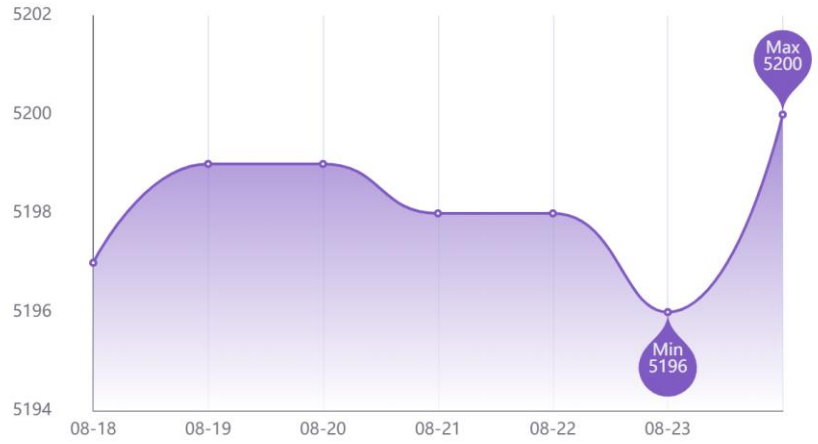
Country/Region
CN

Name
ERX-CERNET-BKB

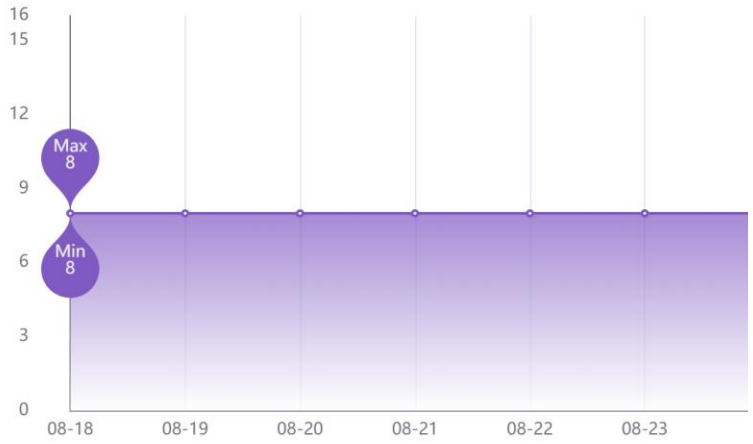
Organization
China Education and Research Network Center

Prefixes Changed
+ 4 - 0

IPv4 Prefix Count



IPv6 Prefix Count



Prefix Change

+59.64.64.0/20

+121.194.32.0/20

+211.68.32.0/20

+211.82.96.0/20

Announced prefixes changes between 2022-08-24 00:00:00 (GMT) and 2022-08-23 00:00:00 (GMT)

ASN 7575
+ 203.6.255.0/24

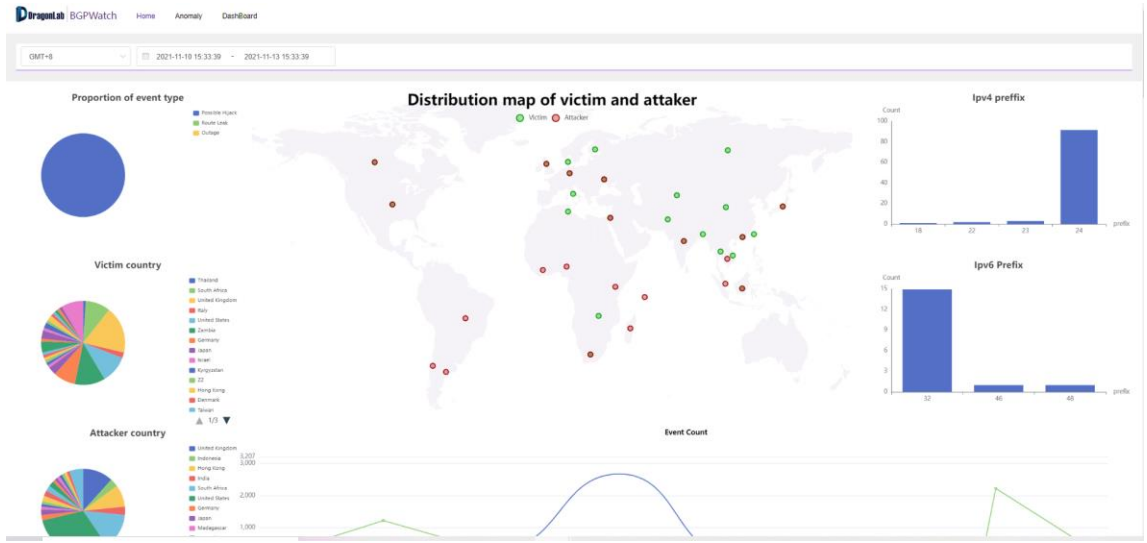
ASN 4538
+ 59.64.64.0/20
+ 121.194.32.0/20
+ 211.68.32.0/20
+ 211.82.96.0/20

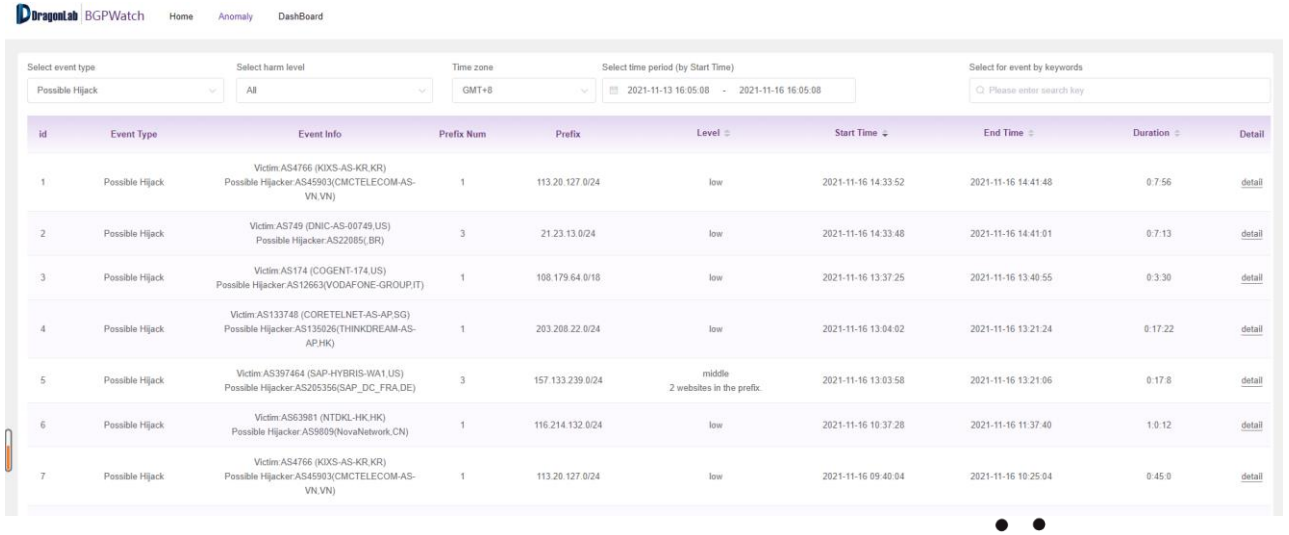
清華大學 Tsinghua University

APNIC FOUNDATION

BGP Routing Hijacking Detection

- https://bgpwatch.cgtf.net
- Knowledge-based real-tIme BGP hIjacking Detection System
- Public BGP event reporting servcie
- Based on MOAS(subMOAS)
- Exclude legal MOAS by using domain knowledge and rules（ROA，IRR，AS relationship etc）





清華大學 Tsinghua University

APNIC FOUNDATION

Research Paper

Evaluating and Improving Regional Network Robustness from AS TOPO Perspective

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

5th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

6th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—Currently, national and regional networks are subject to various security attacks and threats, including various types of malicious behaviors and specific natural disasters. This paper borrows the quantitative ranking idea from the fields of economy and society and proposes a ranking method for evaluating regional resilience. A large-scale simulation was made and the sampling data were acquired from each AS and region. A significance tester that measures the impact of events from the overall level and variance aspect was also implemented. To improve a region's robustness, this paper proposes a greedy algorithm to optimize the resilience of regions by increasing key links among AS. This paper selects the AS topology of 50 countries/regions for research and ranking, evaluating the topology robustness from connectivity, user, and domain perspective, clustering the results, and searching for optimal links to improve the network resilience. Experimental results have shown that the resilience of regional networks can be greatly improved by slightly increasing the number of connections, which demonstrates the effectiveness of the optimization method.**

***Index Terms*—Autonomous System (AS), network resilience, network security**

Is there any difference in the resilience of each region, and if so, how big is the difference; what is the key weak topology that causes such a gap; how should the region optimize the topology to improve its own resilience? We conducted comprehensive assessment of the resilience of regional network to solve the above problems and made three major contributions.

Assess resilience in each region: To address these problems, we proposed a statistical method to evaluate the resilience of a region under attack. We simulated a damage event according to the probability of the event to approximate the damage caused by the simulated event in the real situation. For a comparative analysis of regional resilience, we implemented a significance tester using the Kruskal-Wallis test [21] method to make a comparison among regions and measure the impact of regional attack events from the overall level and variance aspect, respectively. To get the ranking and clustering results of fifty regions, we clustered the regional resilience at the overall level and variance aspect.

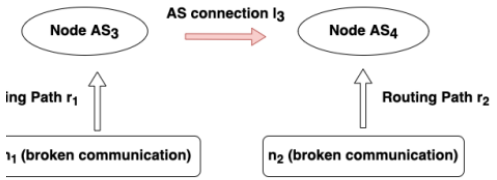
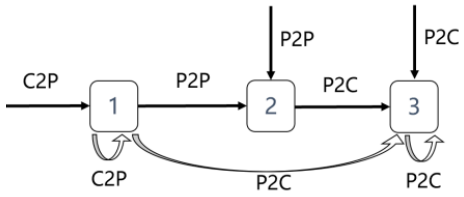
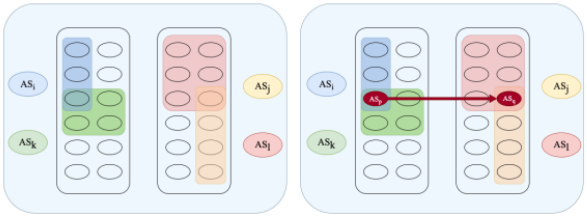


Fig. 2. The AS relationship and link optimization

: $c2p[n]$,
: $c2p[0/n]$ & $p2p[0/1]$ & $p2c[0/n]$.
$n > 1$. $r[n]$ means there are n consecutive connections
r relationship in the routing path, $r[0/n]$ means there
or n consecutive connections with the r relationship in
ting path, $r[0/1]$ means there exists 0 or 1 connection
r relationship in the routing path, and the symbol &
s that $c2p[0/n]$, $p2p[0/1]$, and $p2c[0/n]$ are adjacent
outing path.
idering the valley-free principle, the following form
ing path relationship will not occur: $p2c[1/n]$ &
$l/n]$ & $c2p[1/n]$, where $n > 1$. Fig. 3 shows the
nsition diagram.



(a) calculating the node pairs that can't communicate



(b) greedy search

Fig. 4. Searching the optimal link

Based on the routing tree of each node, we compare the nodes on the routing tree before and after the weak group is destroyed, and obtain the node pairs that cannot communicate after the weak group is destroyed, as shown in Fig. 4(a). The weak group AS_W may consist of multiple AS nodes and links. When nodes and links in AS_W are destroyed, AS_i and AS_j can't communicate, neither can AS_k and AS_l.

We store pairs of nodes that cannot communicate according to certain rules. When the nodes are AS, the records are sorted according to the number of their customers, and the AS nodes with a higher number of customers are recorded on the left; when the nodes are region, the records are sorted according to the number of ASes in the region, and the regions with a

Welcome partners to join in this work

Tsinghua University

APNIC FOUNDATION

Future Work

- Improve prefix hijacking detection algorithm
- Improve dashboard function
- Develop path hijacking detection function
- Continue on the research topic
- Knowledge sharing
- Documents

Next Month Plan

- Help partners connect with our looking glass platform
- Improve operator tools
- Discuss research paper

Todo List

Task	Detail	Todo
BGP Routing Information Sharing	Just 4 few partners have not peered with the BGP platform	Continue
Looking Glass Platform	Document info (How to implement, what partners need to do)	Executive Team :send manual to partners, discuss with each partner, and implement the connection. Partners: setup connection.
	Implement the connection (meeting, email, slack)	
Paper Discussion		Executive Team : Prepare and invite partners

Comments/Suggestions

- ??

Thanks!