

# **(APNIC ISIF Project Update)**

## **Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform**

**APAN 54  
25 August 2022**

# Agenda

- **Project Summary**
- **Project Progress**
  - Project web site implementation
  - BGP sharing platform
  - Looking Glass platform
  - Analyzing and Diagnosing Platform
  - Research Topic
- **Some Concerns**
- **Comments/Suggestions**

# Project Information

- **Name:** Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform
- **Date:** Feb.24, 2022 – Aug.23, 2023 (18 months)
- **Co-PI:** Jilong Wang (CERNET, CN)  
Chalermpol Charnsripinyo (ThaiREN, TH)  
Simon Green (SingAREN, SG)
- **Funding:**
  - USD150,000 (APNIC Foundation)
  - USD69,660 (in-kind contribution from Tsinghua Univ., China)
- **Objectives**
  - Build a collaborative community for enhancing the capacity of NRENs' network operation and measurement
  - Establish a distributed BGP routing monitoring platform and a looking glass platform in the Asia-Pacific region
  - Deploy a BGP hijacking detection and mitigation system and analyze the robustness of routing in the Asia-Pacific region
  - Share knowledge and experience globally

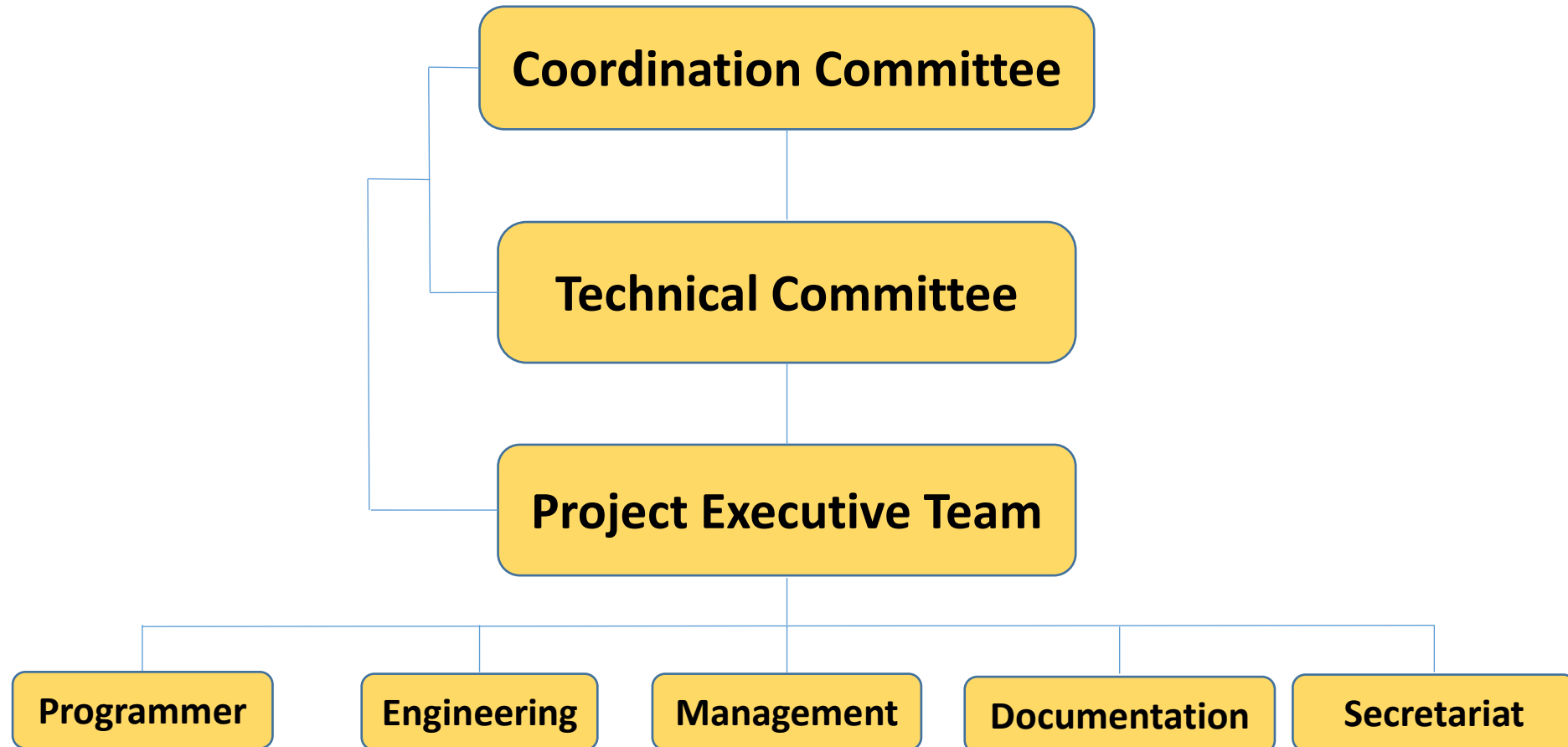
# Partnership

- **19 Partner Organizations (listed alphabetically)**

- AARNET(AU)
- APAN-JP(JP)
- BdREN(BD)
- CERNET(CN)
- DOST-ASTI(PREGINET)(PH)
- ERNET(IN)
- Gottingen University(DE)
- HARNET(JUCC, HK)
- ITB(ID)
- KREONET(KR)
- LEARN(LK)
- MYREN(MY)
- NREN(NP)
- PERN(PK)
- REANNZ(NZ)
- SingAREN(SG)
- Surrey University(UK)
- ThaiREN(TH)
- TransPAC(US, APAN/GNA-G Routing WG)

- **Keep open till June, 2023**

# Project Governance

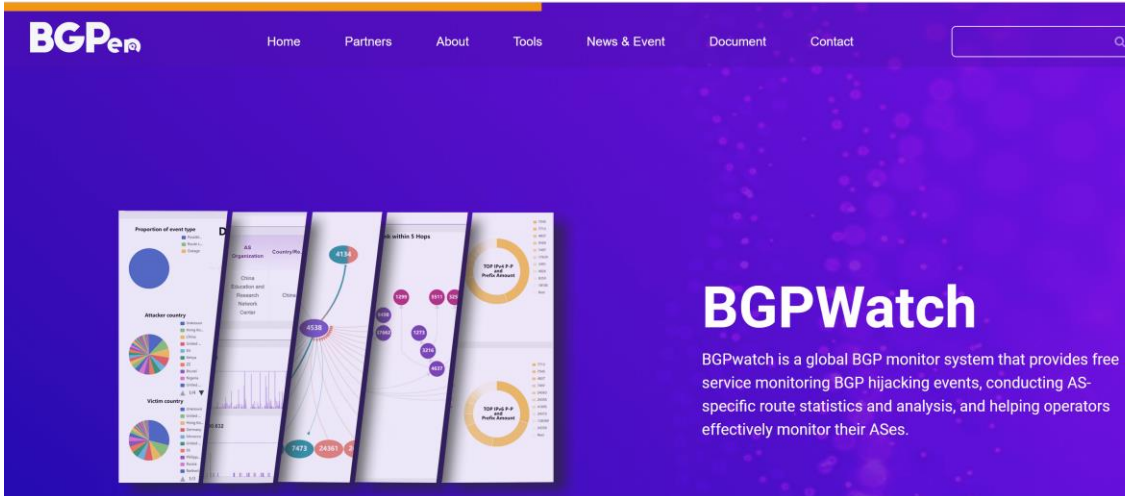


	Detailed Technical Committee Work Plan	Tentative Timeline
Timeline	Discussion on Timeline	May
Project Web Site	Requirements/Design	May
	Partner's information	May
	Setting up project website	May
BGP Routing Information Sharing	Requirements/Design(email, slack)	May-June
	Document info (How to implement, what partners need to do)	May-June
	Implement the peering (meeting, email, slack)	May- Continuously
Looking Glass Platform	Requirements/Design(email, slack)	August
	Document info (How to implement, what partners need to do)	
	Implement the connection with LG platform(meeting, email, slack)	
Hijack Detection and Mitigation	Problem and requirement sharing (meeting, email, slack)	June
	Confirm first stage functions	July
	Iterative feedback & development	July 2022 – July 2023
Research	Discussion on research topic, paper, technical document	July 2022 – July 2023
Knowledge Sharing	Any topic partners interested in , e.g. Problems, RPKI, BGPSEC, MANRS	regularly



# Project Web Site

<https://bgper.net>



The screenshot shows the BGPWatch homepage with a purple header and navigation bar. The main content area features a large graphic with various charts and maps, and a text block describing the BGPWatch system.

## BGPWatch

BGPWatch is a global BGP monitor system that provides free service monitoring BGP hijacking events, conducting AS-specific route statistics and analysis, and helping operators effectively monitor their ASes.



The screenshot shows the BGPWatch About page. The header is purple with a navigation bar. The main content area has a white background with a blue sidebar. The text describes the project's purpose and progress.

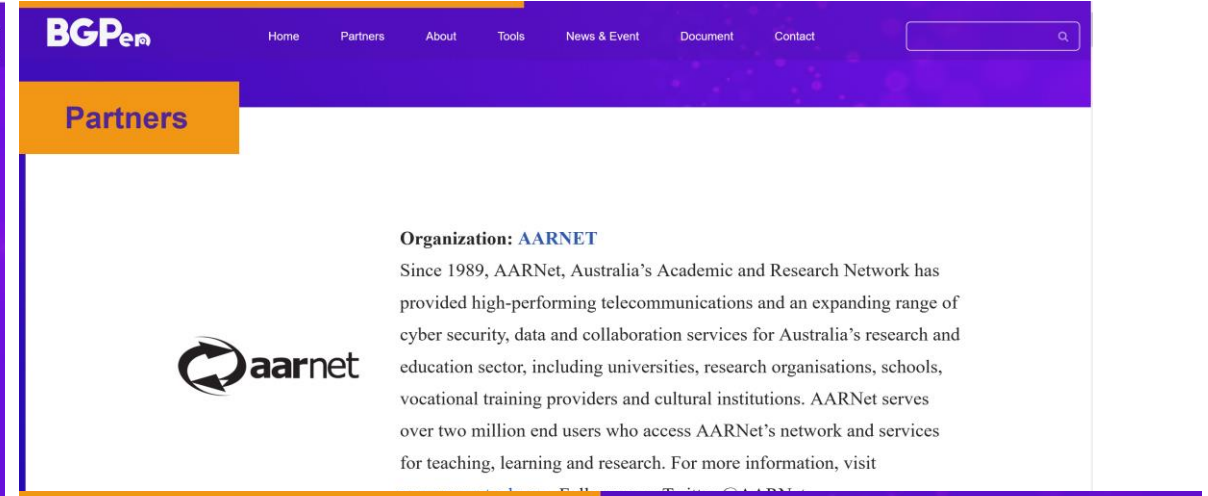
## About

### Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Project Duration: Feb. 2022 – Jul. 2023

In early 2022, based on the support of [APNIC ISIF Asia Grant](#), Tsinghua University joined with the NRENs and universities from 14 Asian and European countries started the project titled “Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform”.

By June 2022, 20 organizations from 19 countries/economies in Asia Pacific Region and Europe had joined the project. The coordination committee, technical committee and secretariat mainly responsible for the implementation of project management and research collaboration. The project remains open and welcomes the joining of new partners.




The screenshot shows the BGPWatch Partners page. The header is purple with a navigation bar. The main content area has a white background with a blue sidebar. The text describes the AARNET organization and its services.

## Partners

**Organization: AARNET**

Since 1989, AARNET, Australia’s Academic and Research Network has provided high-performing telecommunications and an expanding range of cyber security, data and collaboration services for Australia’s research and education sector, including universities, research organisations, schools, vocational training providers and cultural institutions. AARNET serves over two million end users who access AARNET’s network and services for teaching, learning and research. For more information, visit [aarnet.edu.au](#)



The screenshot shows the BGPWatch News & Event page. The header is purple with a navigation bar. The main content area has a white background with a blue sidebar. The text describes the project's first collaborative and technical meeting and its kick-off meeting.

## News & Event

### The First Collaborative and Technical Meeting of “Collaborative BGP Routing Analyzing and Diagnosing Platform” Project

News On May 10, 2022, the First Collaborative and Technical Meeting of the “Collaborative BGP Routing Analyzing and Diagnosing Platform”...

[Read More →](#)

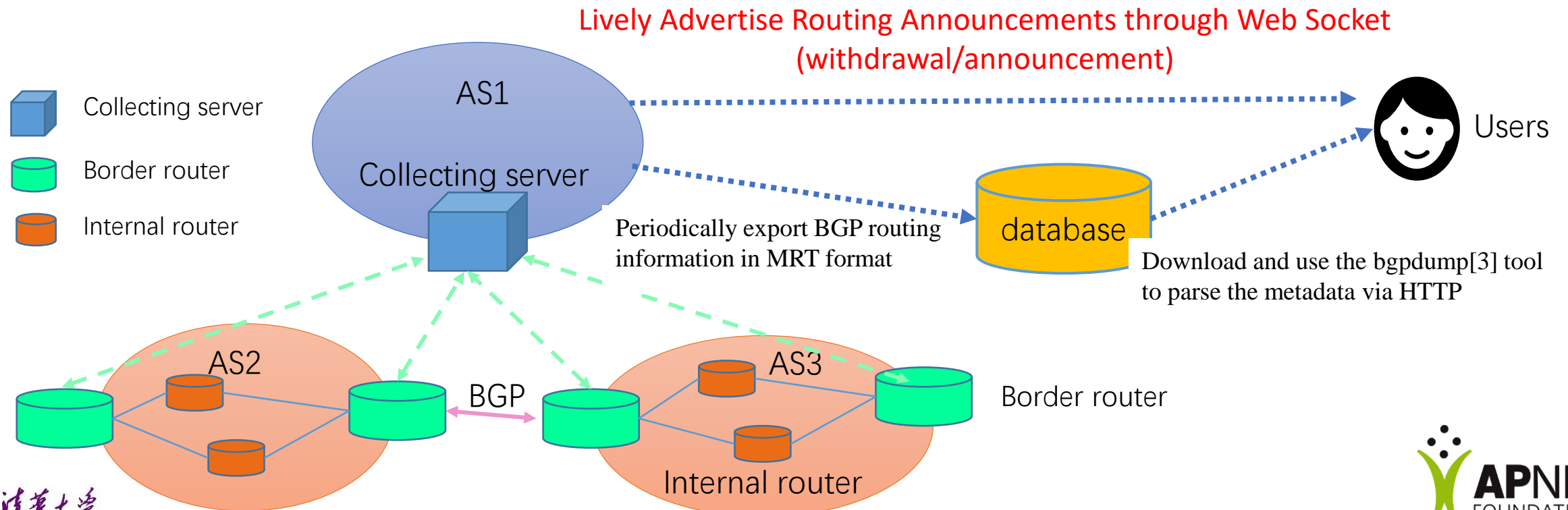
### “Collaborative BGP Routing Analyzing and Diagnosing Platform” Project Kick-off Meeting

News Collaborative BGP Routing Analyzing and Diagnosing Platform” Project Kick-off Meeting On February 24, 2022, Tsinghua University hosted the “Collaborative BGP Routing...

[Read More →](#)

# 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



# BGP Route Information Sharing

We have established BGP session with **11 partners**.

Data can be accessed at <https://bgp.cgtf.net>

Configuration manual can be accessed at <https://www.bgper.net/index.php/document/>

AS 7660(APAN-JP)

AS 63961(BDREN)

AS 4538(CERNET)

AS 3662(HARNET)

AS 4796(ITB)

AS 17579(KREONET)

AS 38229(LEARN)

AS 24514(MYREN)

AS 38022(REANNZ)

AS 23855(SINGAREN)

AS 3836(ThaiSARN)

## Index of /ribs/2022/07

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

# 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

## CGTF Looking Glass



Router to use

CERNET Juniper Router at CNGI-6IX  
ThaiREN Cisco Router  
BdREN Cisco Router  
SingAREN Juniper Router  
MYREN Cisco router

Command to issue

show route IP\_ADDRESS  
show route as-path-regex AS\_PATH\_REGEX  
show route ^AS  
ping IP\_ADDRESS|HOSTNAME  
traceroute IP\_ADDRESS|HOSTNAME

Parameter

|

Enter Reset

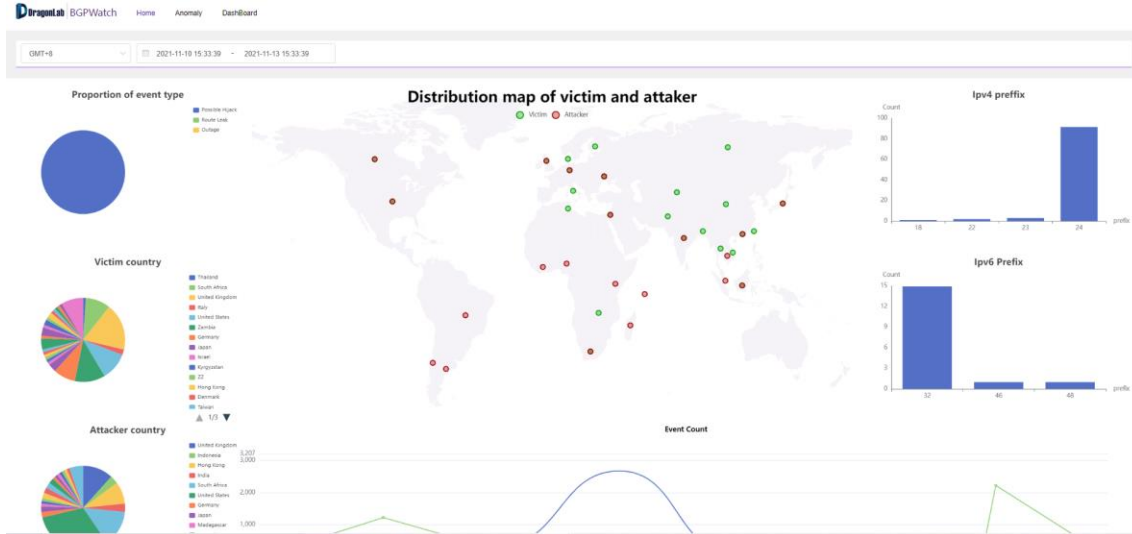
Help

NRENs' contribution:

CERNET, ThaiREN, BdREN, SingAREN, MYREN, LEARN

# BGP Routing Monitoring and Analysis --BGP Watch

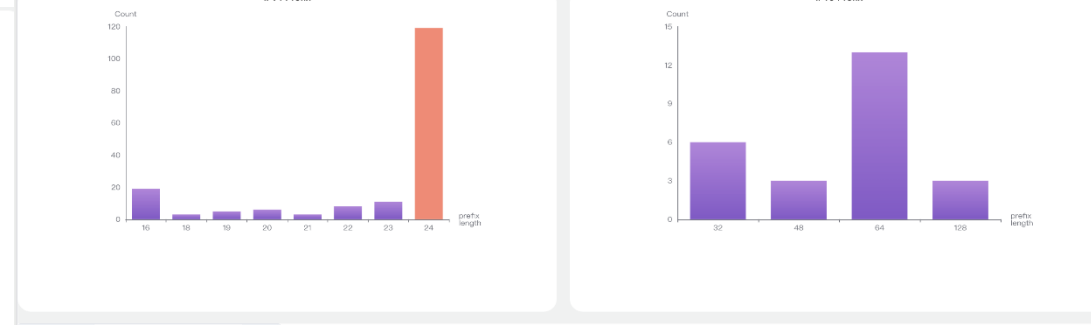
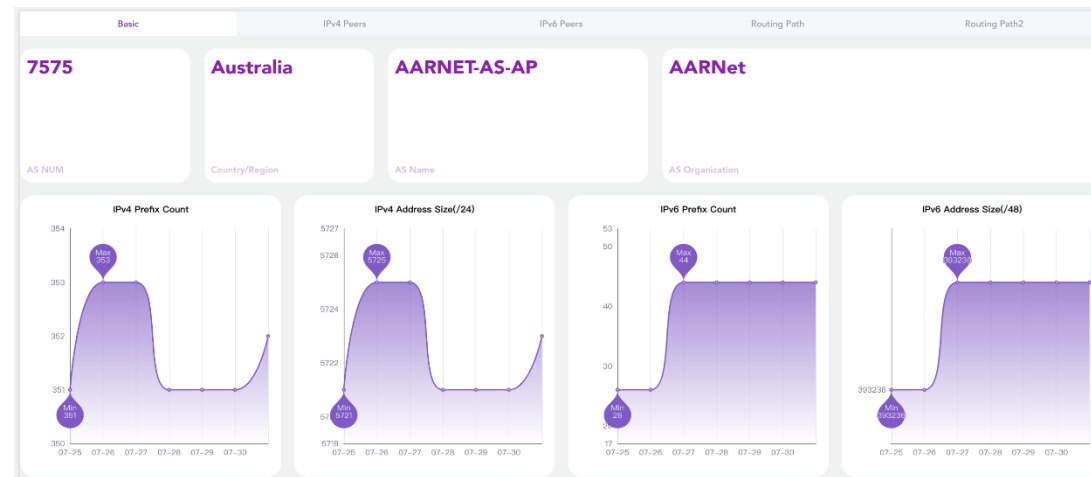
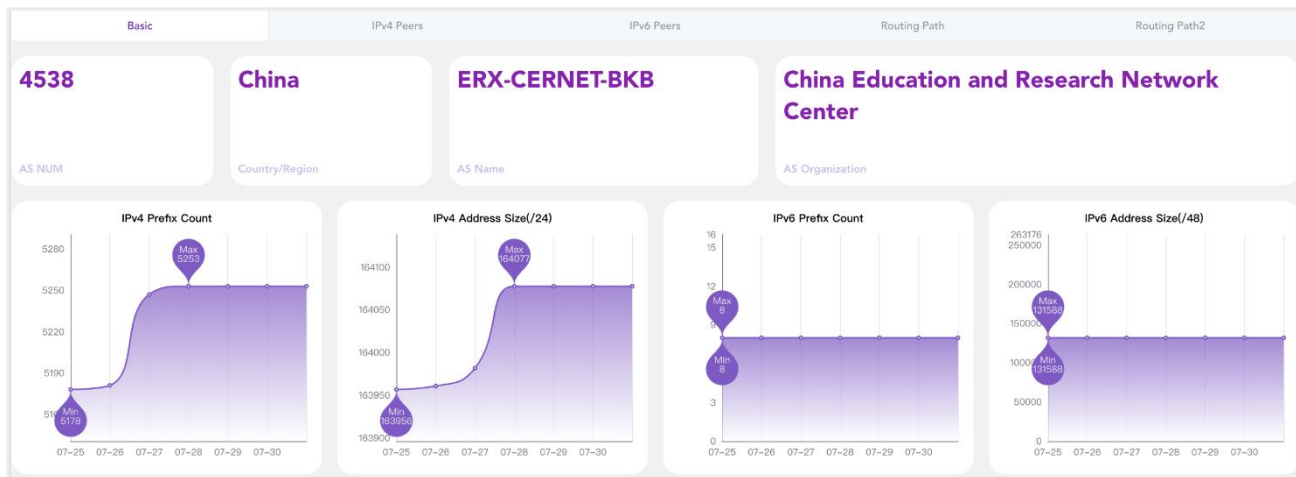
- <https://bgpwatch.cgtf.net>
- Knowledge-based real-time BGP hijacking Detection System
- Public BGP event reporting service
- Based on MOAS(subMOAS)
- Exclude legal MOAS by using domain knowledge and rules (ROA, IRR, AS relationship etc)



The screenshot displays the BGPWatch dashboard interface, showing a list of BGP hijacking events. The interface includes a navigation bar with 'Dragonlab BGPWatch', 'Home', 'Anomaly', and 'Dashboard'. Below the navigation bar, there are filters for 'Possible Hijack', 'All', 'GMT+8', and a date range from '2021-11-13 16:05:08' to '2021-11-16 16:05:08'. A search bar is also present. The main content area is a table with columns: 'id', 'Event Type', 'Event Info', 'Prefix Num', 'Prefix', 'Level', 'Start Time', 'End Time', 'Duration', and 'Detail'. The table lists 7 events, all categorized as 'Possible Hijack'.

id	Event Type	Event Info	Prefix Num	Prefix	Level	Start Time	End Time	Duration	Detail
1	Possible Hijack	Victim:AS4766 (KXS-AS-KR,KR) Possible Hijacker:AS45903(CMCTELEC-AS-VN,VN)	1	113.20.127.0/24	low	2021-11-16 14:33:52	2021-11-16 14:41:48	0:7:56	<a href="#">detail</a>
2	Possible Hijack	Victim:AS749 (DNIC-AS-00749,US) Possible Hijacker:AS22085(BR)	3	21.23.13.0/24	low	2021-11-16 14:33:48	2021-11-16 14:41:01	0:7:13	<a href="#">detail</a>
3	Possible Hijack	Victim:AS174 (COGENT-174,US) Possible Hijacker:AS12663(VODAFONE-GROUP,IT)	1	108.179.64.0/16	low	2021-11-16 13:37:25	2021-11-16 13:40:55	0:3:30	<a href="#">detail</a>
4	Possible Hijack	Victim:AS133748 (CORETELNET-AS-AP,SG) Possible Hijacker:AS135026(THINKDREAM-AS-AP,HK)	1	203.208.22.0/24	low	2021-11-16 13:04:02	2021-11-16 13:21:24	0:17:22	<a href="#">detail</a>
5	Possible Hijack	Victim:AS397464 (SAP-HYBRIS-WA1,US) Possible Hijacker:AS205356(SAP_DC_FRA,DE)	3	157.133.239.0/24	middle 2 websites in the prefix.	2021-11-16 13:03:58	2021-11-16 13:21:06	0:17:8	<a href="#">detail</a>
6	Possible Hijack	Victim:AS63981 (NTDKL-HK,HK) Possible Hijacker:AS59805(NovaNetwork,CN)	1	116.214.132.0/24	low	2021-11-16 10:37:28	2021-11-16 11:37:40	1:0:12	<a href="#">detail</a>
7	Possible Hijack	Victim:AS4766 (KXS-AS-KR,KR) Possible Hijacker:AS45903(CMCTELEC-AS-VN,VN)	1	113.20.127.0/24	low	2021-11-16 09:40:04	2021-11-16 10:25:04	0:45:0	<a href="#">detail</a>

# DashBoard --Basic Info



**Prefix** Search for Prefix Q

Click on the column above, the corresponding prefix will be displayed in the table

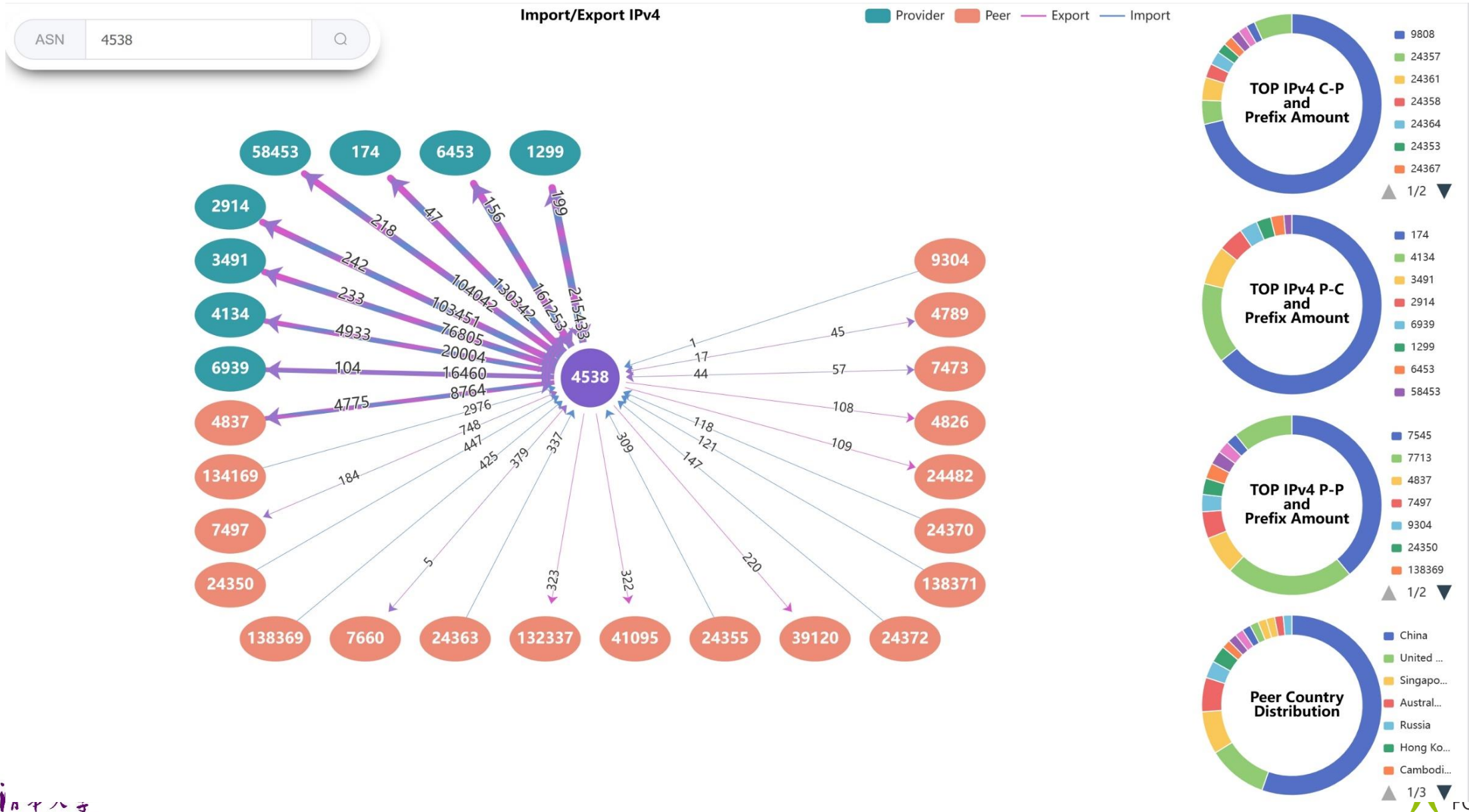
Prefix	Prefix	Prefix
1 1.51.112.0/24	42.244.13.0/24	42.247.1.0/24
2 42.247.5.0/24	42.247.8.0/24	42.247.9.0/24
3 42.247.13.0/24	42.247.18.0/24	42.247.19.0/24

**Prefix** Search for Prefix Q

Click on the column above, the corresponding prefix will be displayed in the table

Prefix	Prefix	Prefix
1 103.36.12.0/24	103.77.199.0/24	103.80.128.0/24
2 103.84.224.0/24	103.90.208.0/24	103.152.75.0/24
3 103.204.14.0/24	103.205.231.0/24	103.235.20.0/24
4 138.7.67.0/24	138.7.120.0/24	138.7.191.0/24
5 138.7.193.0/24	138.25.253.0/24	138.44.226.0/24

# IPv4 Key Peers Information



# IPv6 Peers Information

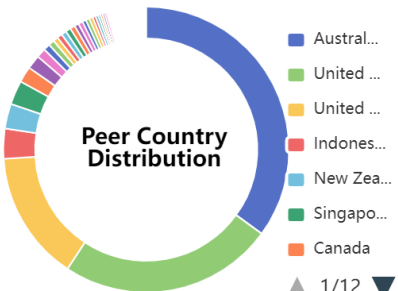
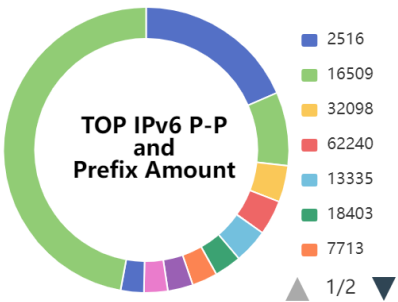
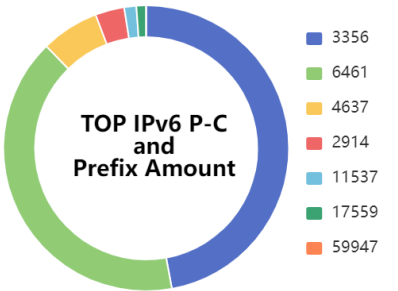
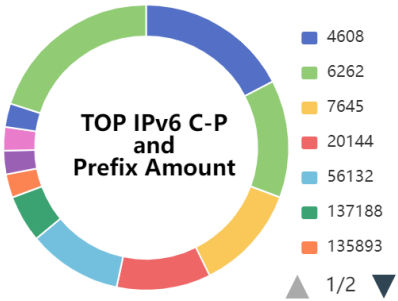
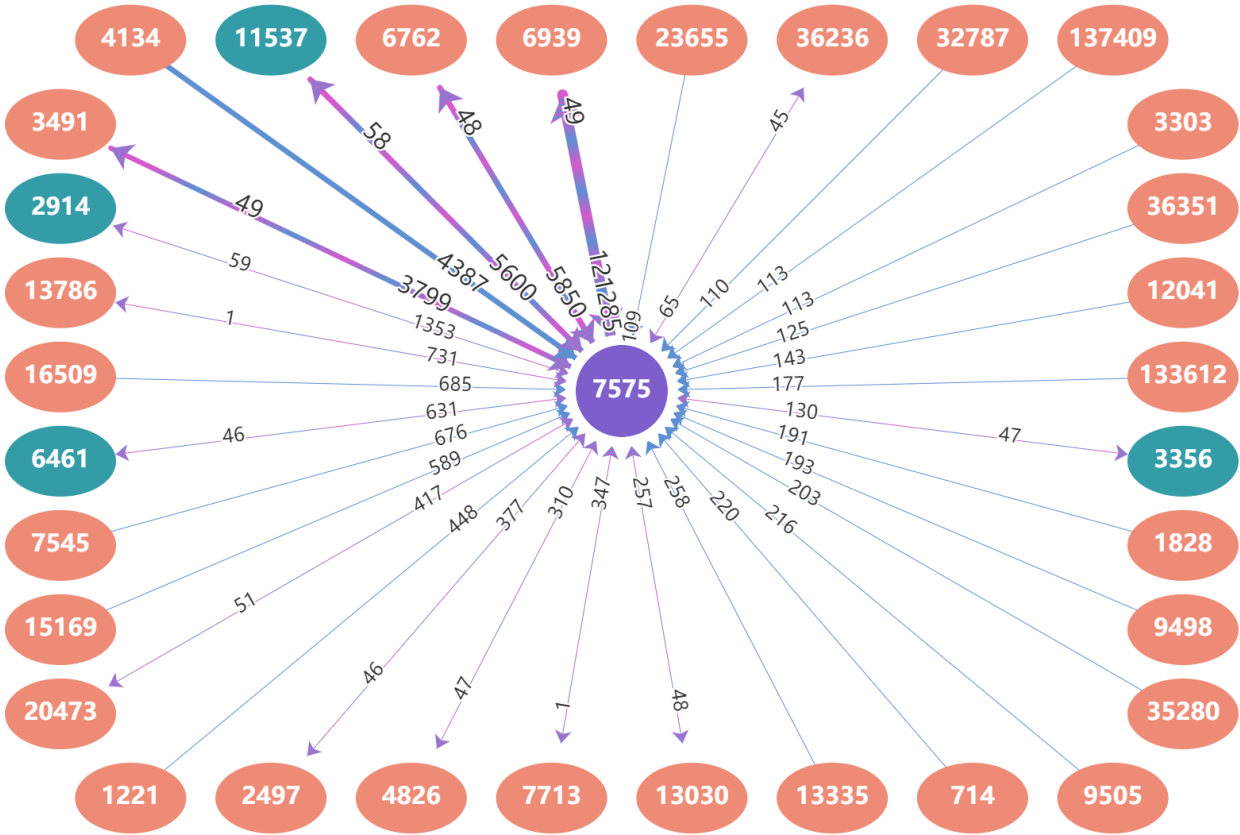
ASN

7575

Q

Import/Export IPv6

Provider Peer Export Import



# Routing Path Search

APAN-JP

BDREN

CERNET

HARNET

ITB

KREONET

LEARN

MYREN

REANNZ

SINGAREN

ThaiREN

Basic

IPv4 Peers

IPv6 Peers

Routing Path

IP

165.124.0.0/16

Q

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

165.124.0.0/17

165.124.128.0/19

165.124.160.0/20

165.124.176.0/21

165.124.184.0/22

165.124.192.0/19

165.124.224.0/21

165.124.232.0/22

165.124.240.0/20

165.124.188.0/22

165.124.236.0/22

AS path

1061514

Prefix Total

```
graph LR; 24575((24575)) --> 23911((23911)); 23911 --> 11537((11537)); 11537 --> 29384((29384)); 11537 --> 22335((22335)); 29384 --> 103((103)); 22335 --> 103
```

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

# Register and Subscribe AS

## Personal Information

\* Username

Please input username

\* Password

Please input password

\* New password

Please input password again

\* Email

Please input email

Register



BGPWatch

Home

Anomaly

Overview

DashBoard

Resilience

Subscribe

aqc

ASN

24514

+

You can input an ASN expression , one or more ASN. For example:  
[1,100]: will subscribe to ASes which ASN range from 1 to 100;  
4538: will subscribe to AS which ASN is 4538;  
4538,4134: will subscribe to ASes which ASN are 4538 and 4134

Delete All

ASN  
38022

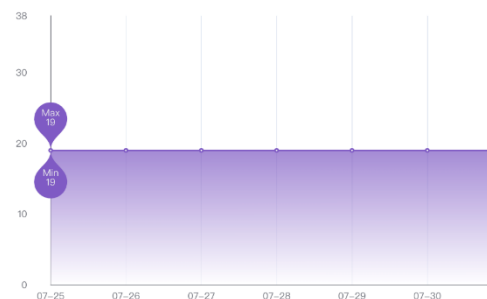
Country/Region  
NZ

Name  
REANNZ-NZ-AP

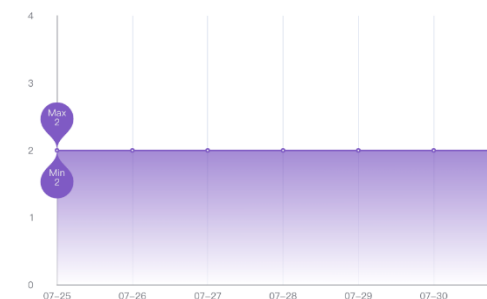
Organization  
REANNZ Education and Schools

×

IPv4 Prefix Count



IPv6 Prefix Count



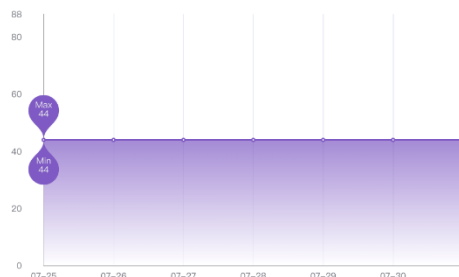
ASN  
7473

Country/Region  
SG

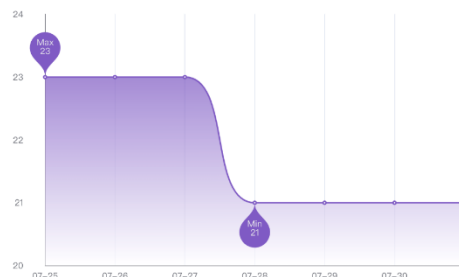
Name  
SINGTEL-AS-AP

Organization  
Singapore Telecommunications (SINGTEL Internet Exchange)

IPv4 Prefix Count



IPv6 Prefix Count



ASN  
7575

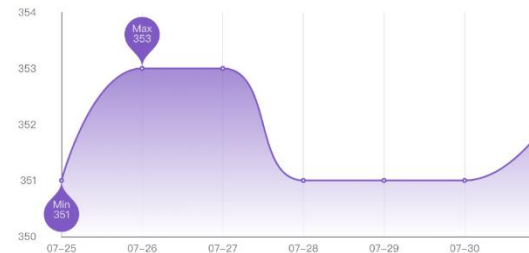
Country/Region  
AU

Name  
AARNET-AS-AP

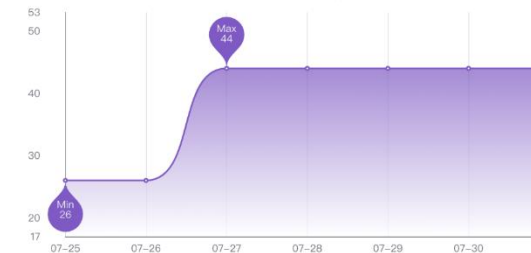
Organization  
AARNet

×

IPv4 Prefix Count



IPv6 Prefix Count



# Send Alarm Email to Subscriber

ASN  
**4538**

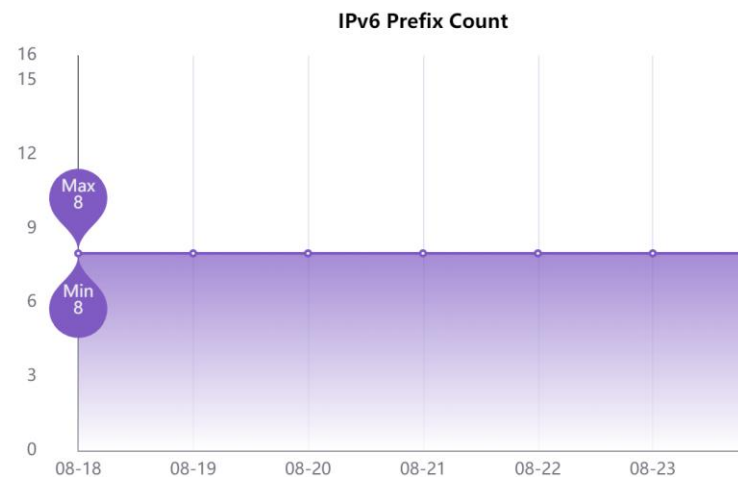
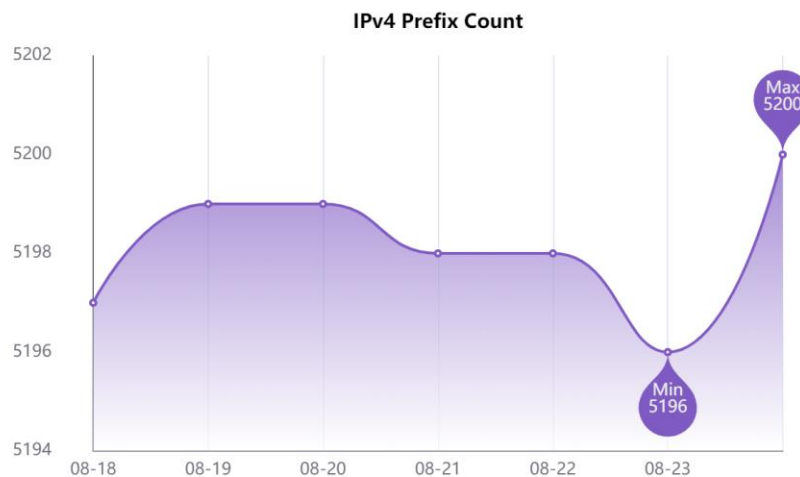
Country/Region  
**CN**

Name  
**ERX-CERNET-BKB**

Organization  
**China Education and  
Research Network  
Center**

Prefixes Changed  
**+ 4 - 0**

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

# Research Topic

- New routing information brought by our CGTF routing Information sharing platform
- Is peering relationships among NREN fully utilized?
- How about the resilience of the region network?

# Research Topic

## Evaluating and Improving Regional Network Robustness from AS TOPO Perspective

1 <sup>st</sup> Given Name Surname dept. name of organization (of Aff.) name of organization (of Aff.) City, Country email address or ORCID	2 <sup>nd</sup> Given Name Surname dept. name of organization (of Aff.) name of organization (of Aff.) City, Country email address or ORCID	3 <sup>rd</sup> Given Name Surname dept. name of organization (of Aff.) name of organization (of Aff.) City, Country email address or ORCID
4 <sup>th</sup> Given Name Surname dept. name of organization (of Aff.) name of organization (of Aff.) City, Country email address or ORCID	5 <sup>th</sup> Given Name Surname dept. name of organization (of Aff.) name of organization (of Aff.) City, Country email address or ORCID	6 <sup>th</sup> 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.

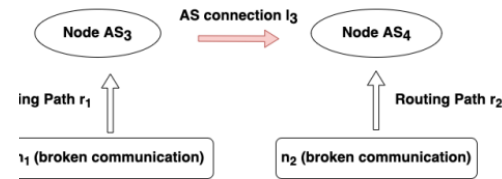


Fig. 2. The AS relationship and link optimization

$c2p[n]$ ,  
 $c2p[0/n]$  &  $p2p[0/1]$  &  $p2c[0/n]$ .  
 $n > 1$ .  $r[n]$  means there are  $n$  consecutive connections  
 $\geq r$  relationship in the routing path,  $r[0/n]$  means there  
or  $n$  consecutive connections with the  $r$  relationship in  
ing path,  $r[0/1]$  means there exists 0 or 1 connection  
 $\geq r$  relationship in the routing path, and the symbol &  
s that  $c2p[0/n]$ ,  $p2p[0/1]$ , and  $p2c[0/n]$  are adjacent  
outing path.

Considering 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.

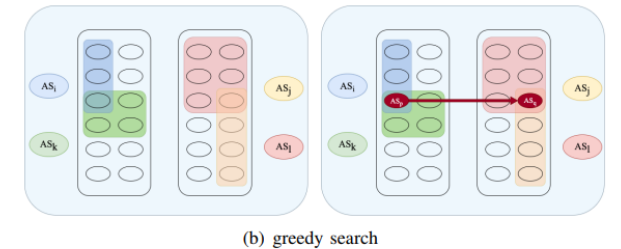
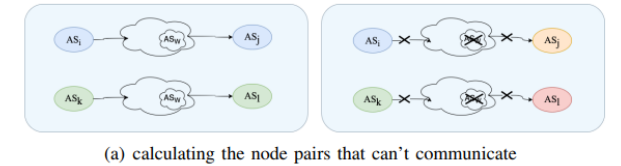
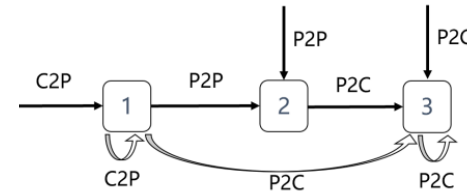


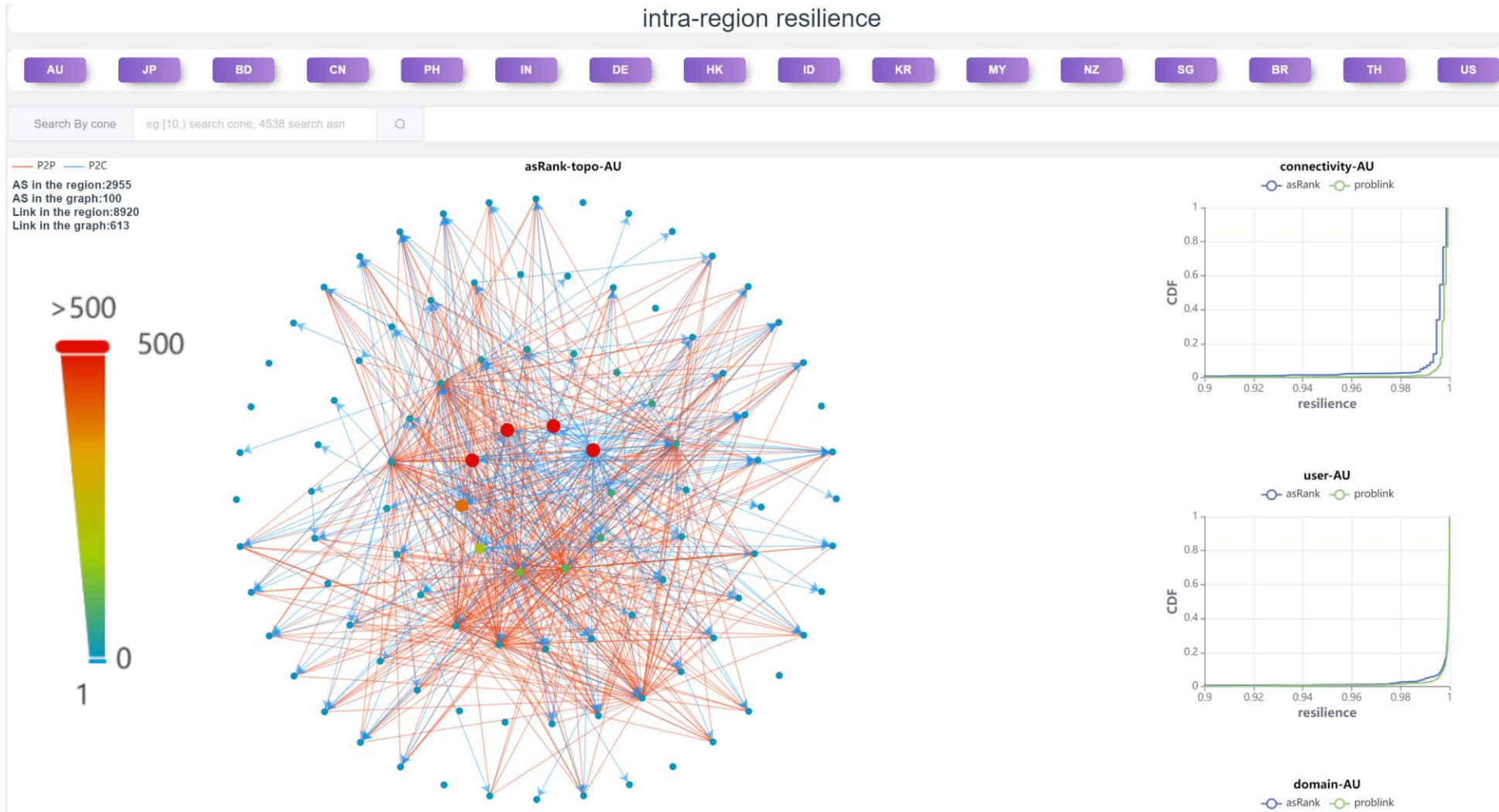
Fig. 4. Searching the optimal link

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 higher number of ASes are recorded on the left.

Welcome partners to join in this work

# Intra-region resilience



Color and size represent cone size of the AS

# Some Concerns

- Where the data is stored?
  - BGP sharing platform: Cloud server in Singapore
  - BGPWatch: Cloud server in Hongkong
  - Looking Glass: Cloud server in Hongkong
- Will peering harm my network?
  - We use open software routing FRR[2] to simulate a real BGP router and it won't send routing announcement.
- Will sharing routing information harm my network?
  - Routeviews and RIPE RIS are two most famous RIS sharing platform.
- Our policy doesn't permit ssh/telnet access from other network
  - Such as SingAREN, they use a VM to simulate a router, and peer with their real router. Then our looking glass access to the VM.

# Future Work

- Improve prefix hijacking detection algorithm
- Develop path hijacking detection function
- Support user registration and send alarm message to the victim
- Continue on the research topic

# Project Secretariat and Contact

**Welcome to join us!**  
**Please contact us at:**

- Web Site
  - <https://bgper.net>
- International Coordination
  - Ms.Weiqi Zhao      zhao-wq@tsinghua.edu.cn
- Technical Contact:
  - Ms.Linmei Zu      zulinmei@tsinghua.edu.cn

