

**(APNIC Project)**

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

**--The 3rd Technical Committee Meeting**

**August 3, 2022**

# Outline

- **Project Progress**
  - The Updates of BGP Session Establishment with 9 Partners
  - The Improvement of Routing Path Search Function
  - User Registration, Subscription, and Email Alarm
- **Next month plan**
- **Review overall work plan**
- **Comments/Suggestions**

# BGP Route Information Sharing

We have established BGP session with **9 partners**.

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

And we are discussing detailed scheme with other partners

Maybe multi sessions are needed.

**AS 7660(APAN-JP)**

**AS 63961(BDREN)**

**AS 4538(CERNET)**

**AS 3662(HARNET)**

**AS 17579(KREONET)**

**AS 38229(LEARN)**

**AS 24514(MYREN)**

**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	

# Routing Path Search

APAN-JP | BDREN | CERNET | HARNET | LEARN | MYREN | SINGAREN | ThaiREN | KREONET

Basic | IPv4 Peers | IPv6 Peers | Routing Path | Routing Path2

IP: 166.0.128.0/21

You can input an IP address or prefix address. For example: 1.0.0.1, 1.0.0/16. The system will return all the subset and superset network of it.

166.0.128.0/24  
166.0.135.0/24  
166.0.129.0/24  
166.0.130.0/24  
166.0.131.0/24  
166.0.132.0/24  
**166.0.133.0/24**  
166.0.134.0/24

166.0.133.0/24 AS PATH 1072287 Prefix Total

AS Name: GTT-BACKBONE  
Org:STT Communications Inc  
Country: US

APAN-JP | BDREN | CERNET | HARNET | LEARN | MYREN | SINGAREN | ThaiREN | KREONET

Basic | IPv4 Peers | IPv6 Peers | Routing Path | Routing Path2

IP: 165.124.0.0/16

You can input an IP address or prefix address. For example: 1.0.0.1, 1.0.0/16. 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

165.124.0.0/16 AS path 24968 Prefix Total

AS Name: MREN  
Org:Metropolitan Research and Education Network  
Country: US

DragonLab BGPWatch Home Anomaly Overview DashBoard Resilience Login Register

APAN-JP | BDREN | CERNET | HARNET | LEARN | MYREN | SINGAREN | ThaiREN | KREONET

Basic | IPv4 Peers | IPv6 Peers | Routing Path | Routing Path2

IP: 165.124.0.0/16

You can input an IP address or prefix address. For example: 1.0.0.1, 1.0.0/16. 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 166162 Prefix Total

AS Name: TRANSAC  
Org:Indiana University  
Country: US

APAN-JP | BDREN | CERNET | HARNET | LEARN | MYREN | SINGAREN | ThaiREN | KREONET

Basic | IPv4 Peers | IPv6 Peers | Routing Path | Routing Path2

IP: 165.124.0.0/16

You can input an IP address or prefix address. For example: 1.0.0.1, 1.0.0/16. 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

165.124.0.0/16 AS PATH 28947 Prefix Total

AS Name: MREN  
Org:Metropolitan Research and Education Network  
Country: US

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

# Register and Subscribe AS

## Personal Information

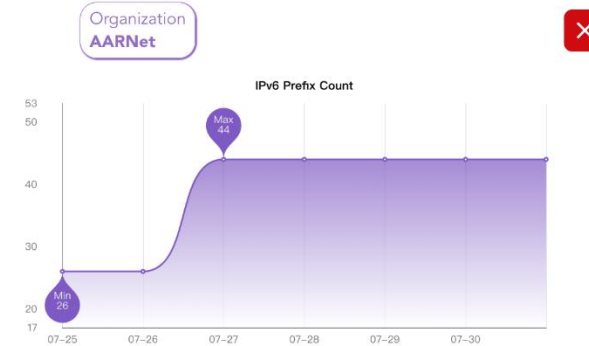
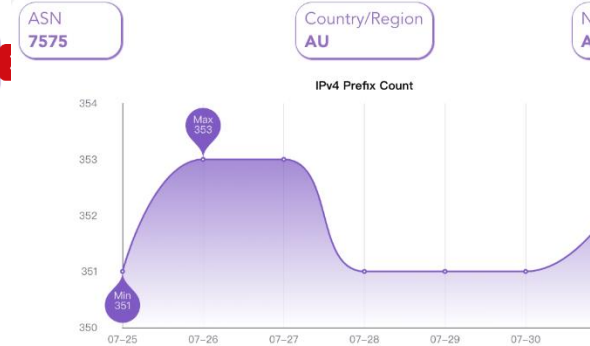
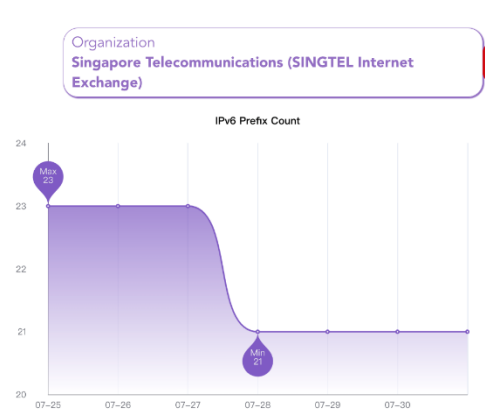
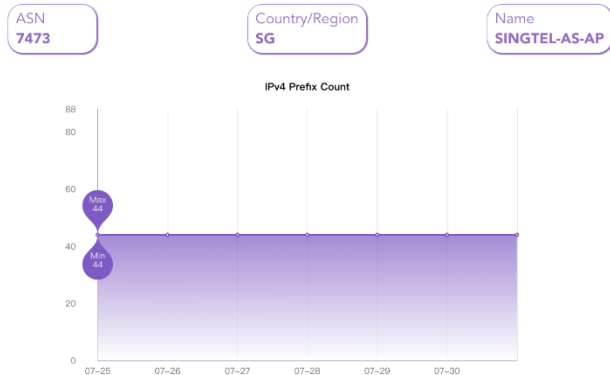
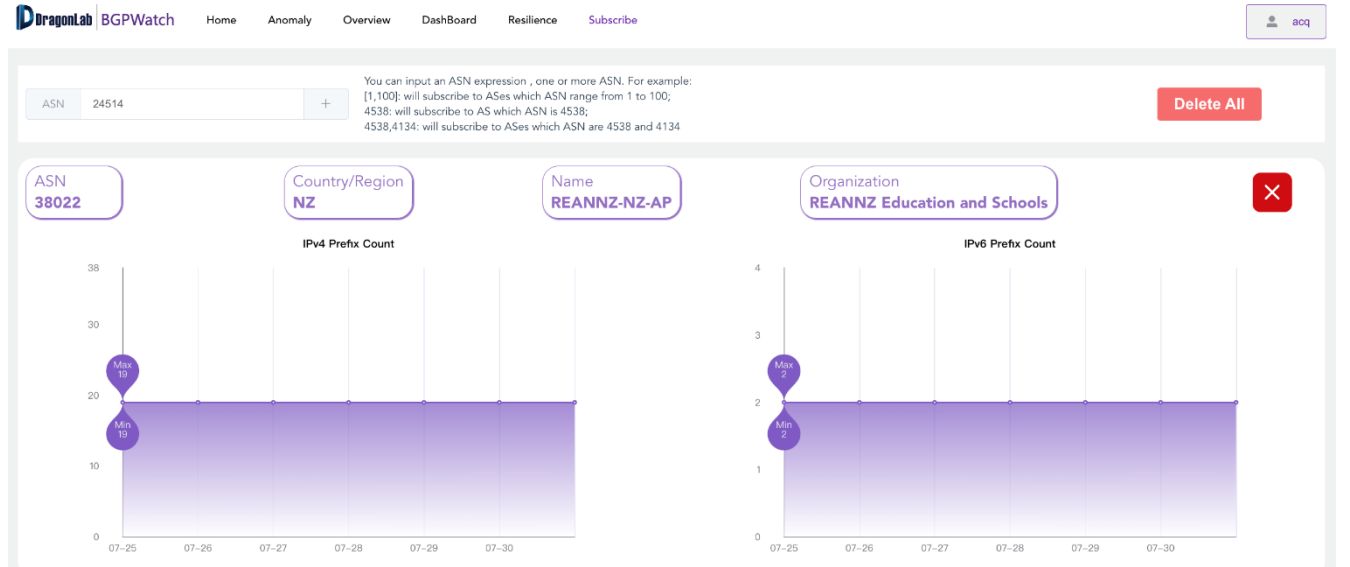
\* **UserName**

\* **Password**

\* **New password**

\* **Email**

Register



# Send Alarm Email to Subscriber

Alarm! Announced prefixes changed ★

sec

发给 acq

发件人: sec <sec@cgtf.net>

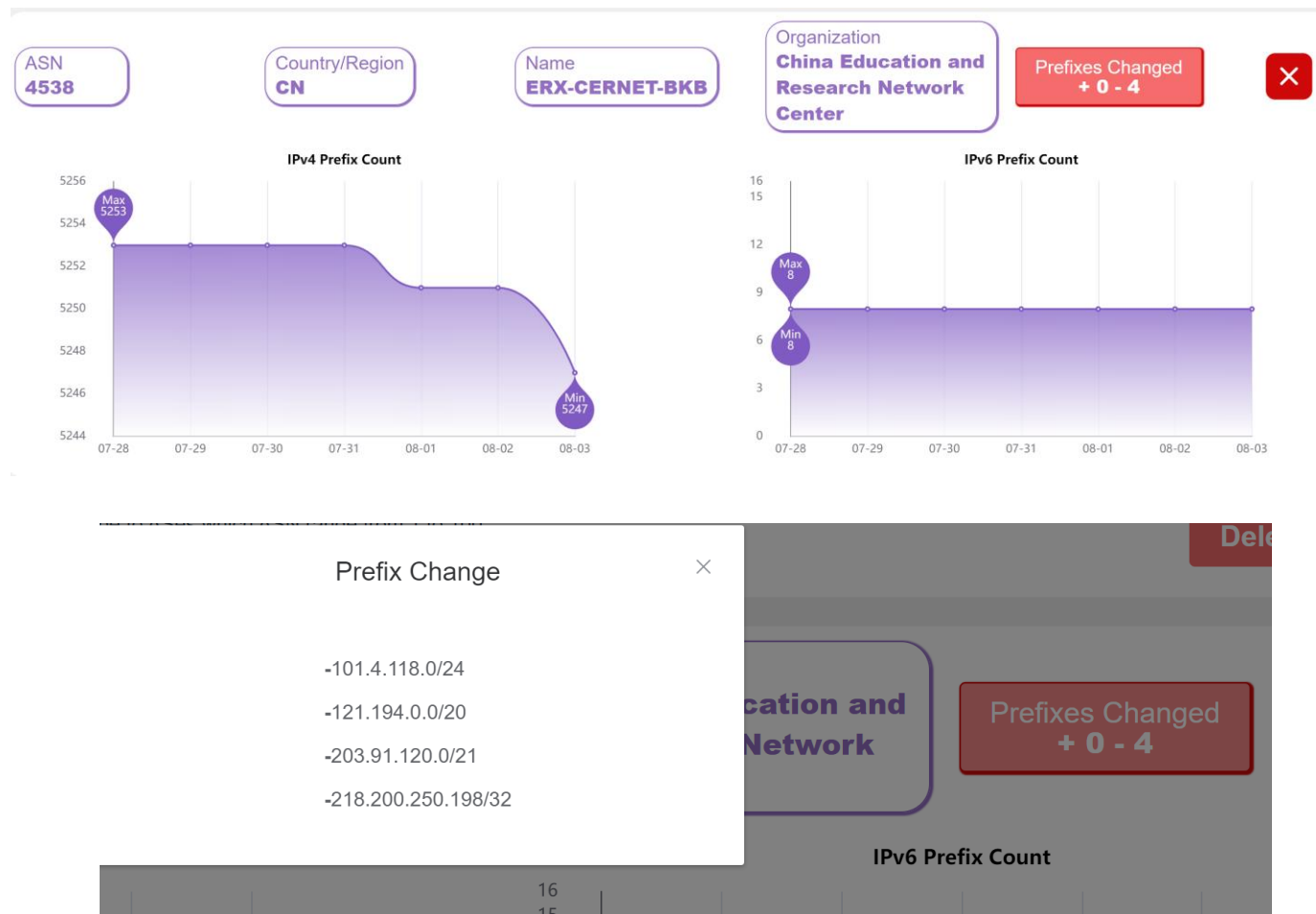
收件人: acq <acq@tsinghua.edu.cn>

时间: 2022年8月3日 (周三) 14:26

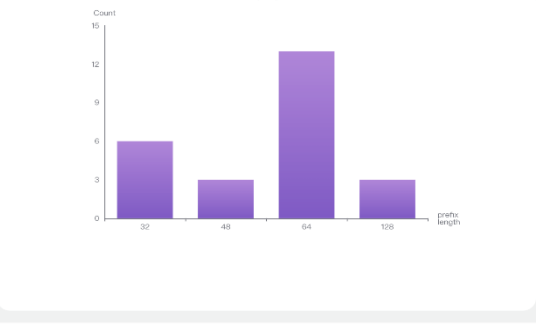
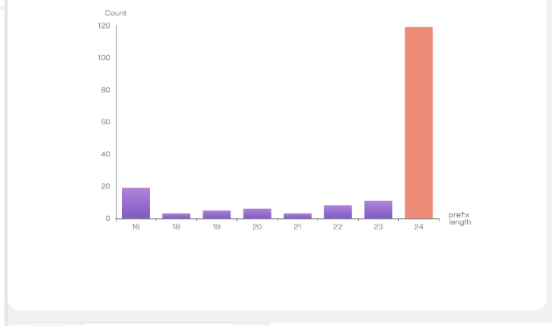
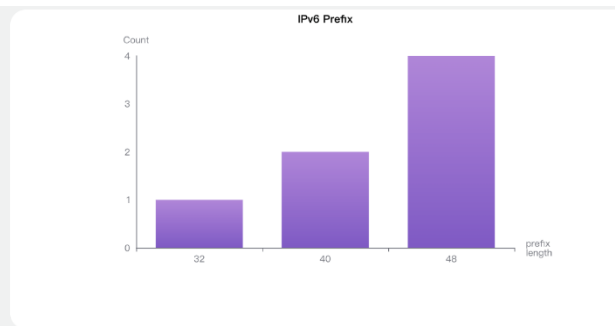
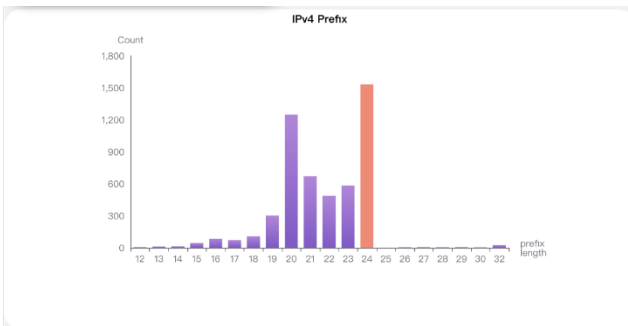
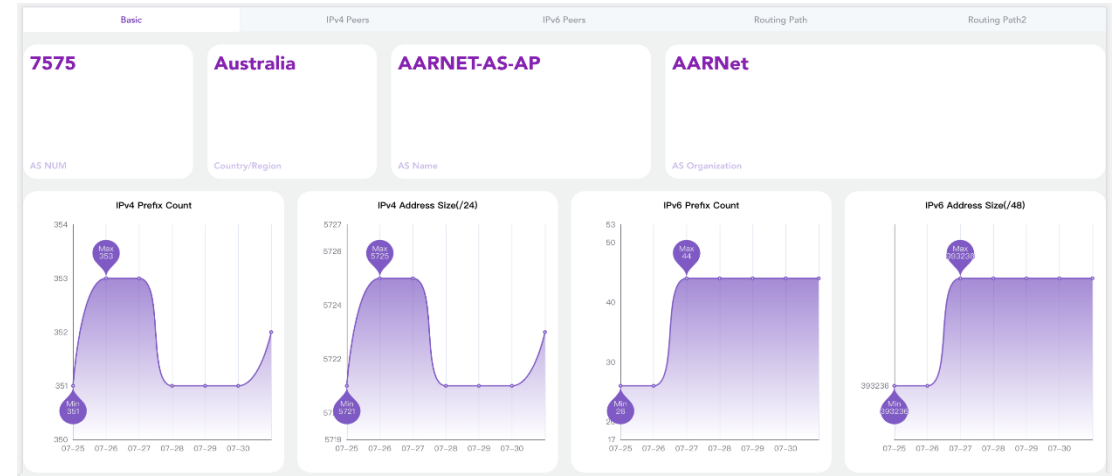
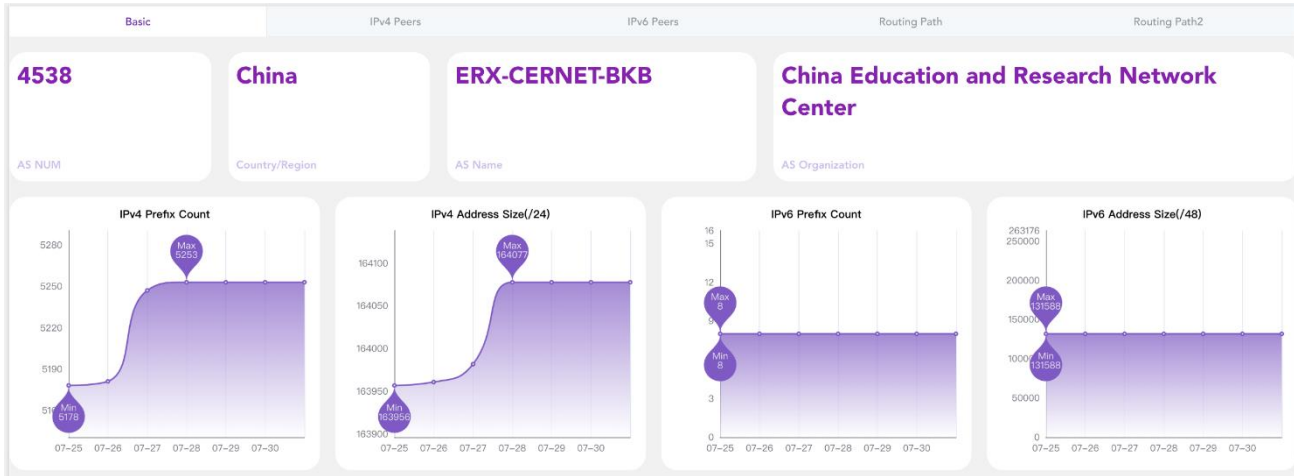
大小: 3 KB

# ASN 4538 #

- 101.4.118.0/24
- 121.194.0.0/20
- 203.91.120.0/21
- 218.200.250.198/32



# 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	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

# Next Month Plan

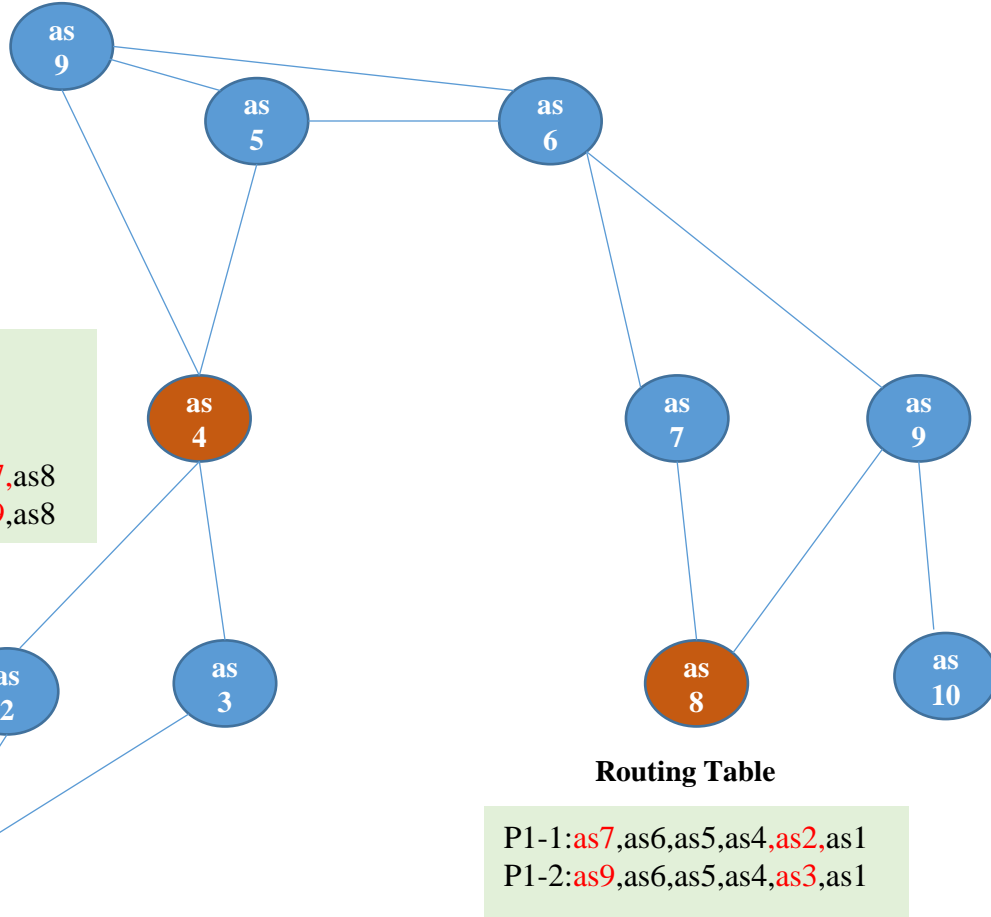
- Monitor prefix hijacking, and send alarm message to the victim
- Improve routing search function
- Research topic



# Discussion About Routing Path Search

1. Search routing path from an AS to a prefix
2. Search routing path from a prefix to a prefix (2 equals 1)
3. Search routing path from an AS to an AS (split to 1)
4. Search routing path to an AS (split to 3)
5. Report routing path changing between 2 dates

# How to Get Routing Path

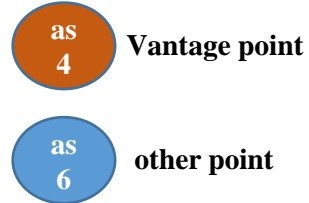


### Routing Table

P1-1:as2,as1  
 P1-2:as3,as1  
 .....  
 P8-1:as5,as6,as7,as8  
 P8-2:as5,as6,as9,as8

### Routing Table

P1-1:as7,as6,as5,as4,as2,as1  
 P1-2:as9,as6,as5,as4,as3,as1  
 .....  
 P4-1:as7,as6,as5,as4  
 P4-2:as9,as6,as5,as4



Assume each ASi has 2 prefix: pi-1, pi-2

From vantage point	Q:From as4,as8 to any as/prefix Q:From p1-*, p8-* to any as/prefix	Get exact info
To vantage point	Q:Routing to as4/as8 Q:Routing to p4-*,p8-*	Infer, get part info
From other point	Q:From as5/as7 to any as/prefix Q:From p5-*,p7-* to any as/prefix	
To other point	Q:Routing to as5/as7 (p5-*,p7-*) Q:Routing to p5-*,p7-*	

# 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.

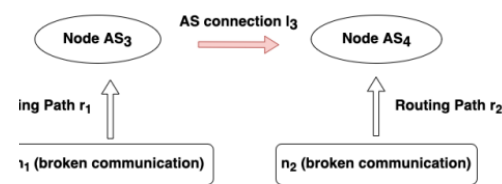
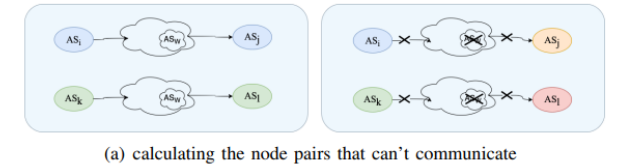
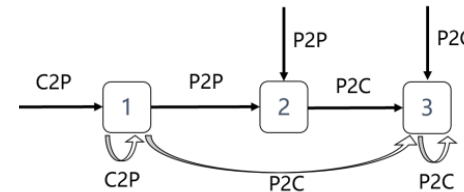


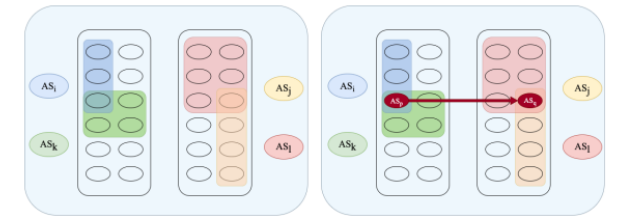
Fig. 2. The AS relationship and link optimization

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

Considering the valley-free principle, the following forming path relationship will not occur:  $p2c[1/n]$  &  $l/n]$  &  $c2p[1/n]$ , where  $n > 1$ . Fig. 3 shows the transition 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 higher number of ASes are recorded on the left.

Welcome partners to join in this work

	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



# Todo List

	Detailed Technical Committee Work Plan	Todo
BGP Routing Information Sharing	Document info (How to implement, what partners need to do)	<b>Executive Team</b> :send manual to partners, discuss with each partner, and implement the peering. <b>Partners</b> : setup peering.
	Implement the peering (meeting, email, slack)	
BGP Platform	Iterative feedback & development	<b>Partners</b> : Test new services <b>Executive Team</b> : Software Development
Looking Glass Platform	Document info (How to implement, what partners need to do)	<b>Executive Team</b> :send manual to partners, discuss with each partner, and implement the connection. <b>Partners</b> : setup connection.
	Implement the connection (meeting, email, slack)	

# Comments/Suggestions

- ??

