APNIC ISIF FUNDING PROJECT

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

Tsinghua University
China Education and Research Network (CERNET)

Mar.10, 2022

清華大學 Tsinghua University

APNIC FOUNDATION

Outline

- About CERNET & CERNET2
- Project Information & Partnership
- Objectives & Deliverables
- Activity Plans and Timeline
- Governance and Collaboration
- Works We Have Done

清華大學 Tsinghua University

APNIC FOUNDATION

About CERNET & CERNET2

We are running 2 networks and 1 exchange point in China: CERNET/CNGI-CERNET2 / CNGI-6IX

APNIC FOUNDATION

Tsinghua University

Project Information

- Name: Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform
- Co-PI: Jilong Wang, (Tsinghua University, CERNET, China)
- Co-PI: Chalermpol Charnsripinyo (ThaiREN, Thailand)
- Co-PI: Simon Peter Green (SingAREN, Singapore)

- Date: Feb. 24, 2022 - Aug. 23, 2023
- APNIC ISIF Grants : US$150,000.00
- Tsinghua University In-Kind Contribution: US$69,660.00
- Partnership: 13 Countries/Economies provided the letters of support
  - CERNET(China), ThaiREN(Thailand), SingAREN(Singapore), APAN-JP, HARNET/JUCC(Hong Kong, China), LEARN(Sri Lanka), BdREN(Bangladesh), MYREN(Malaysia), NREN(Nepal), ERNET(India), DOST-ASTI(PREGINET, Philippines), Gottingen University(Germany), Surrey University(UK), AfgREN

This is an open Project!
More participations are welcomed!

清華大學 Tsinghua University

APNIC FOUNDATION

Project Team

- CERNET, China
- SingAREN, Singapore
- ThaiREN, Thailand
- BdREN, Bangladesh
- LEARN, Sri Lanka
- AfgREN, Afghanistan
- MYREN, Malaysia
- NREN, Nepal
- Gottingen University, Germany
- Surrey University, UK

- APAN-JP, Japan
- ERNET, India
- DOST-ASTI(PREGINET), Philippines
- HARNET/JUCC, Hong Kong, China

More participations are welcomed!

Objectives & Deliverables

- Build a collaborative BGP routing analyzing and diagnosing platform
  - Looking Glass platform
  - BGP routing sharing platform
  - BGP monitoring and diagnosing platform, focusing on routing hijacking detection and mitigation system
  - BGP analysis platform, focusing on invulnerability analysis of regional routing
- Set up a website for sharing knowledge
- Enhance the NREN capacity of network operation and measurement in Asia Pacific area and promote international collaborations

清華大學 Tsinghua University

APNIC FOUNDATION

Proposed Activity Plans for Further Discussion

- Set up Coordination Committee and Technical Committee by meeting with all partner organizations
- Set up working mailing list and project website
- Arrange periodical online meetings of Coordination Committee and Technical Committee to discuss technical and collaborative issues, explore solutions and reach the consensuses
- Collaborate the platform development, implementation, test and demonstration
- Deliver meeting presentations, technical documentation and periodical project reports on website and via emails
- Organize online/offline project meetings and workshops at APAN meetings for exchanging information and welcome more participation

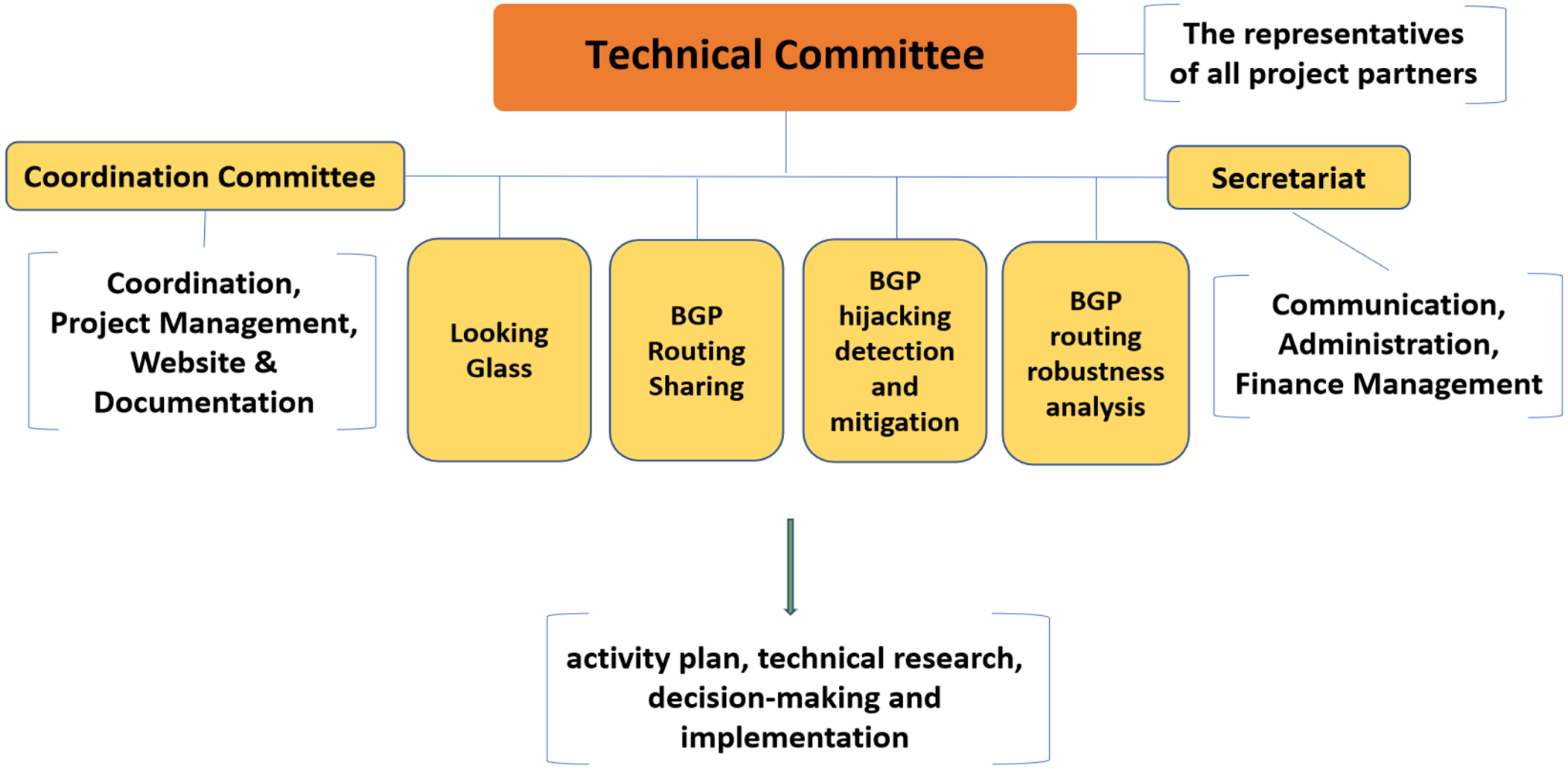
Activity and Timeline (Draft for Further Discussion)

	Activity	Tentative Timeline
1	Kick-off the project	Feb. 2022
2	Set up Coordination Committee and Technical Committee and working mailing list	Mar., 2022
3	Set up project website	Apr., 2022
4	Discuss technical and collaborative issues and collaborate on the platform development, implementation, test and demonstration	Apr. -
5	Arrange online meetings of Coordination Committee(bi-weekly) and Technical Committee(monthly)	Apr. 2022 – Jun. 2023
6	Organize online/offline project meetings(quarterly) and workshops at APAN meetings for information sharing and publicity to welcome more participation	Apr. 2022 – Jul. 2023
7	Deliver meeting presentations, technical documentation and periodical project reports on website and via emails	Jun.2022 – Jul. 2023

清華大學 Tsinghua University

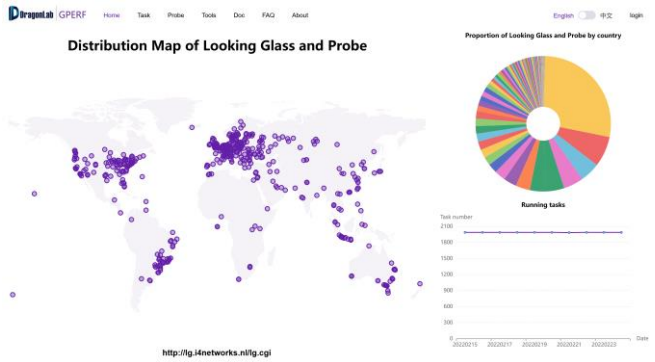
APNIC FOUNDATION

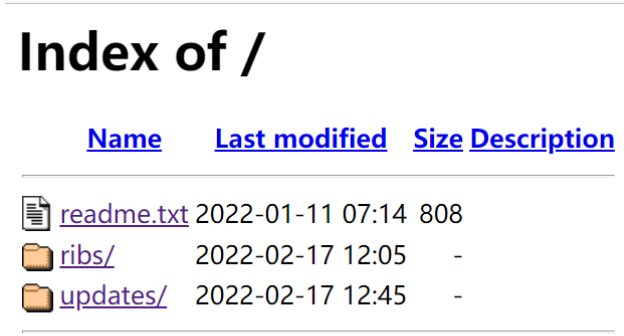
Governance and Collaboration



Works We Have Done

- We have got the funding support from the Research and Development Program of China for “Joint Research on IPv6 Network Management: Research Development and Demonstration”
- A looking glass platform is under development
- A BGP routing information sharing platform is under development
- A BGP Hijacking Monitoring Platform is under development



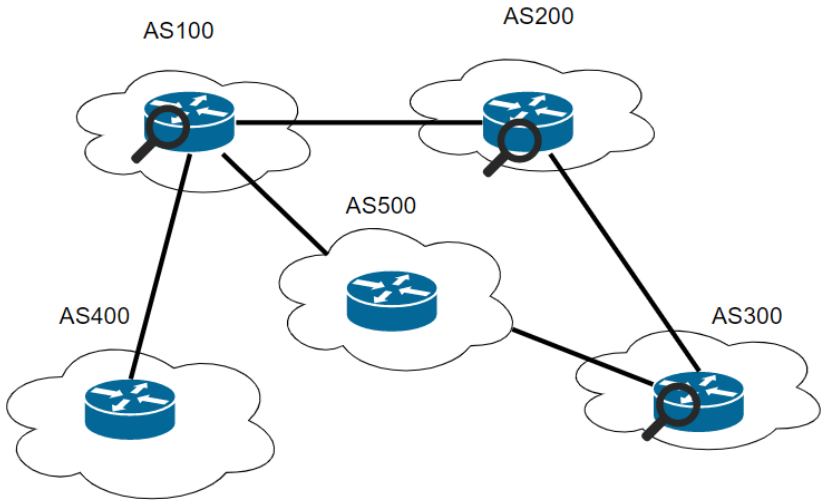


清華大學 Tsinghua University

APNIC FOUNDATION

Looking Glass

- The Internet is observed differently from different network locations.
- LG is a web interface that allows us to observe the Internet from different network locations
- What LG is used for?
  - Help network administrators diagnose network faults
  - Researchers use LG to acquire data. Do active /passive measurements with the help of LG.
  - ISPs use LG to let customers experience their networks before they buy services
- We can also enjoy the above benefits by deploying LG



HURRICANE ELECTRIC
INTERNET SERVICES

Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at route-server.he.net.

Routers

North America

H5 Data Centers ABQ 1, Albuquerque	Albuquerque, NM, US
Equinix Ashburn (DC2)	Ashburn, VA, US
Digital Realty / Telx Atlanta (ATL1), 56 Marietta	Atlanta, GA, US
Data Foundry Texas 1, Austin	Austin, TX, US
Zayo NP MSP1, Belle Plaine	Belle Plaine, MN, US
One Summer Boston	Boston, MA, US
Datahive Calgary	Calgary, AB, CA
Lumos / DC74 Data Center CLT-2 Charlotte	Charlotte, NC, US
ACT Cheyenne	Cheyenne, WY, US

Commands

- Ping
- Traceroute
- BGP Route
- BGP Summary (IPv4)
- BGP Summary (IPv6)

Arguments

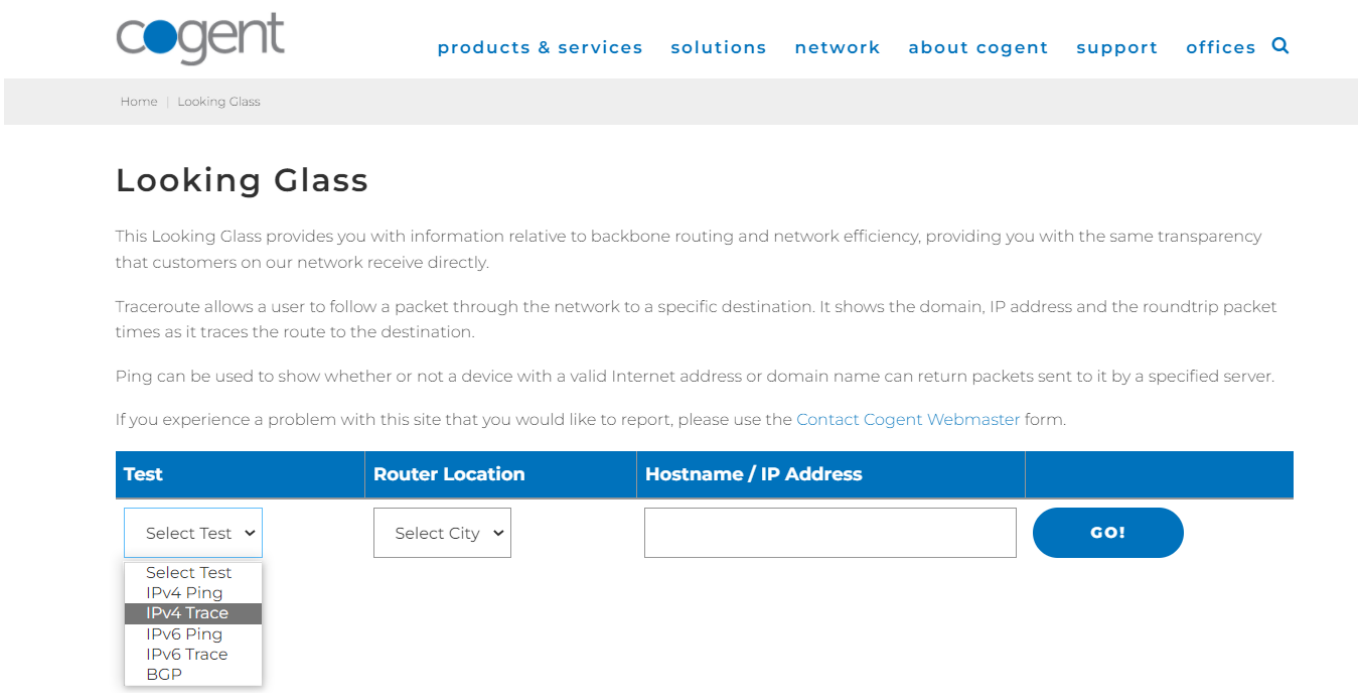
IP/Hostname: 103.145.73.99

Raw output (no tables)

Probe Clear

Looking Glass

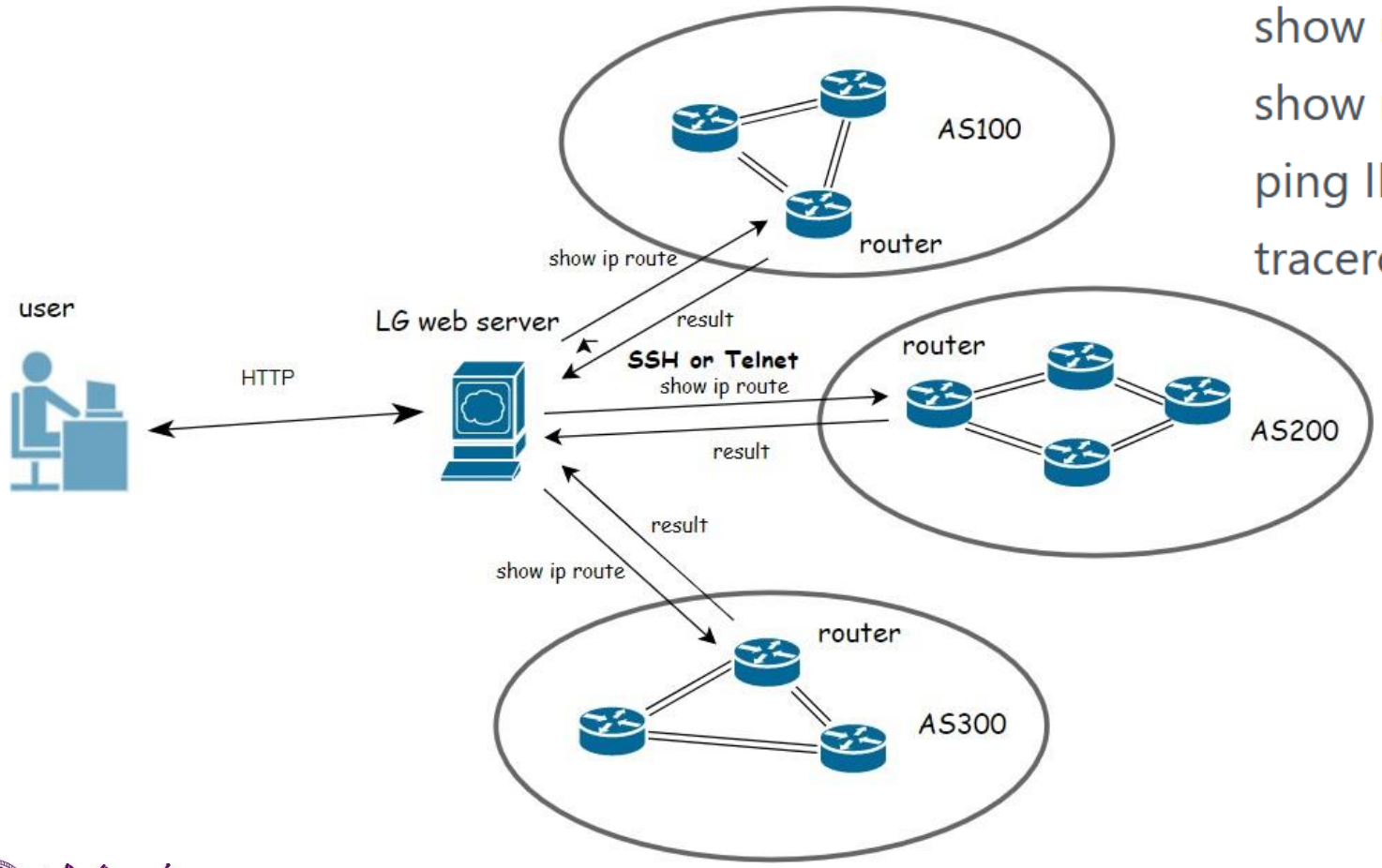
- Commonly used commands：
  - ping
  - traceroute
  - show bgp route
- LG is very common tool
  - many AS（Especially large ISPs）have deployed LG。
- LG is in line with nature of the Internet.（openness and sharing)



Tsinghua University

APNIC FOUNDATION

Looking Glass Architecture



show route IP_ADDRESS

show route as-path-regex AS_PATH_REGEX

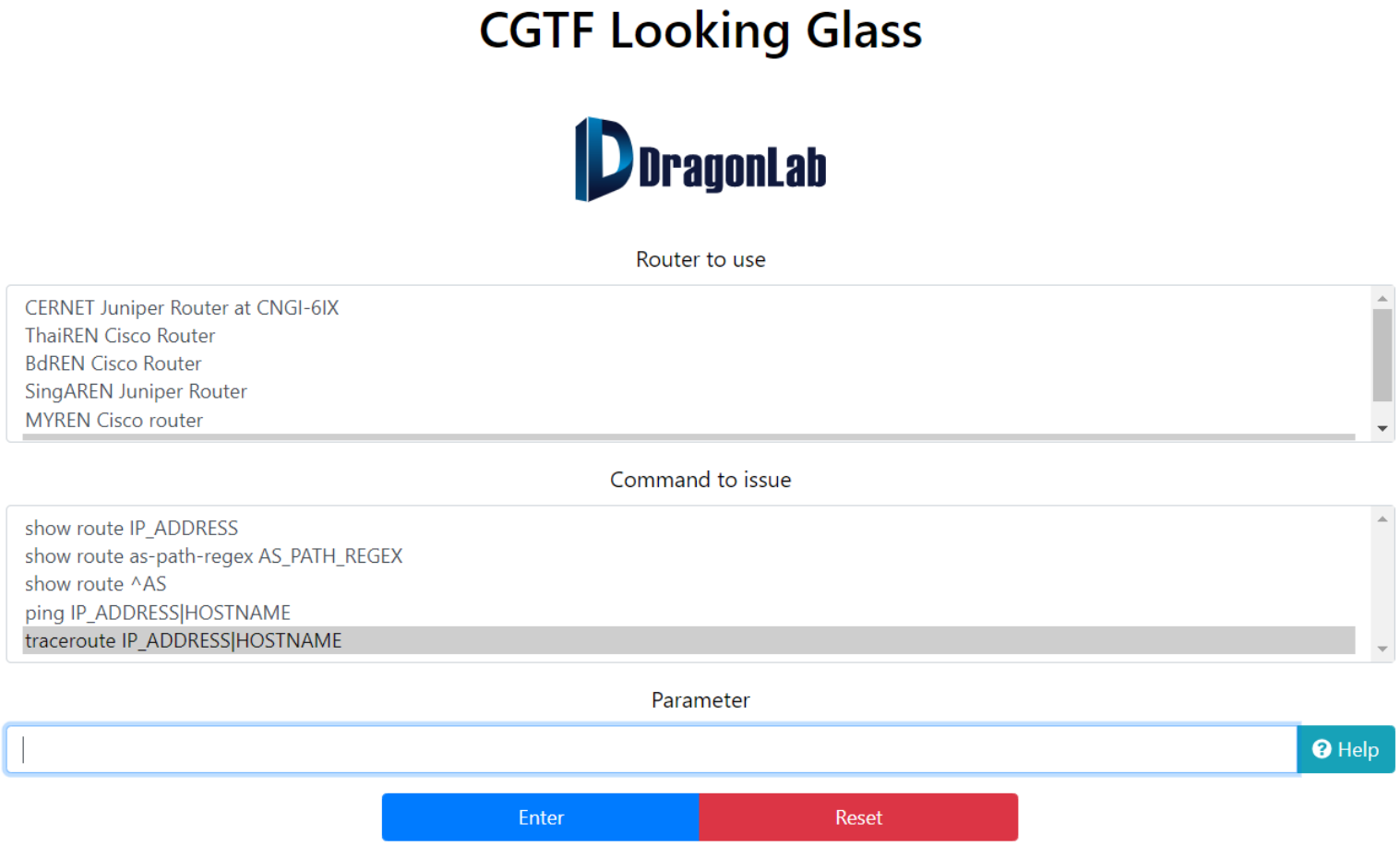
show route ^AS

ping IP_ADDRESS|HOSTNAME

traceroute IP_ADDRESS|HOSTNAME

OUR WORK ON LG - CGTF LG

- http://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



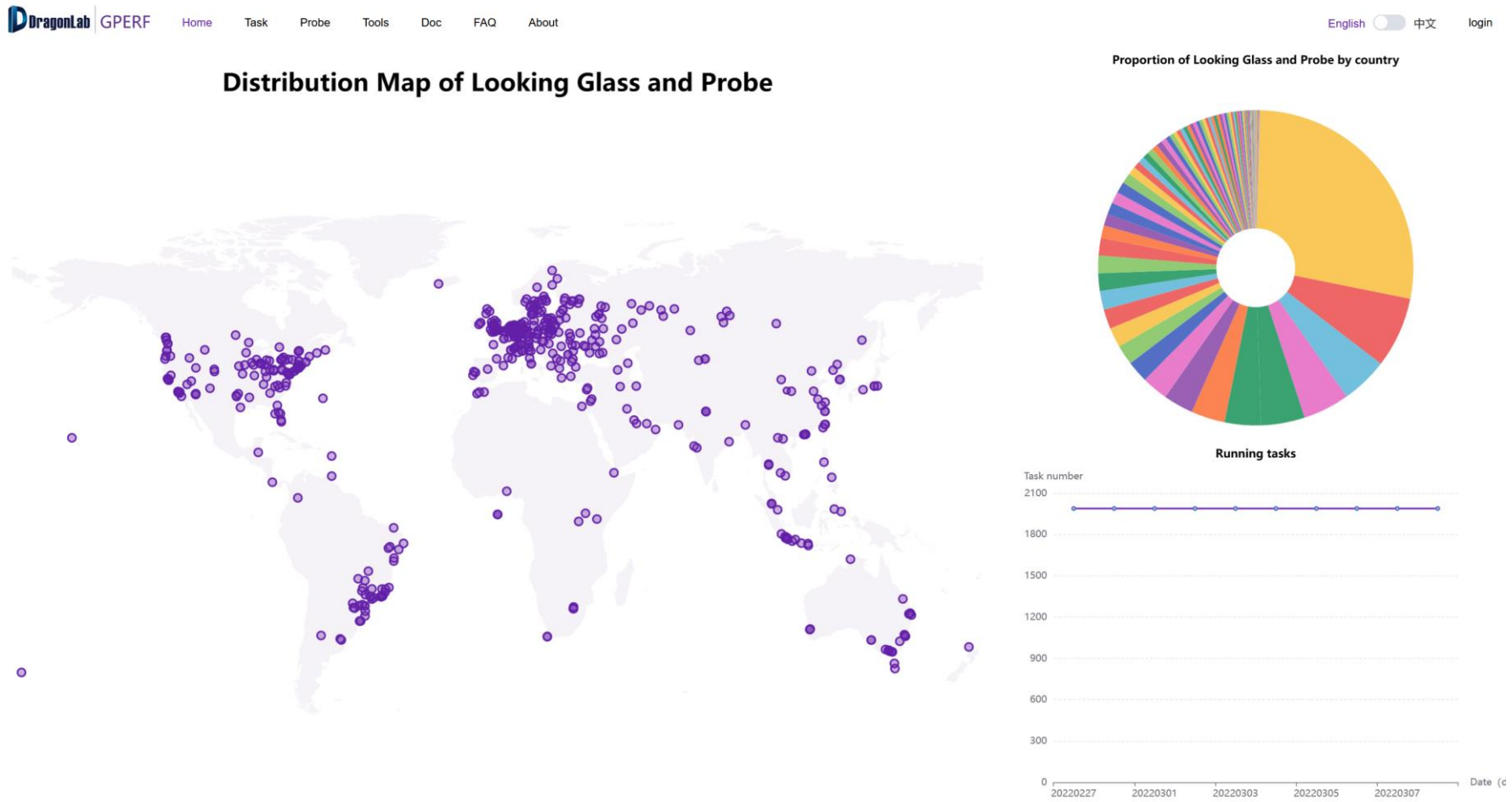
NRENs' contribution:

CERNET, ThaiREN, BdREN, SingAREN, MYREN,LEARN

Tsinghua University

APNIC FOUNDATION

OUR WORK ON LG



3814 LGs

- **Paper: "Discovering obscure looking glass sites on the web to facilitate internet measurement research"——CoNEXT'2021**

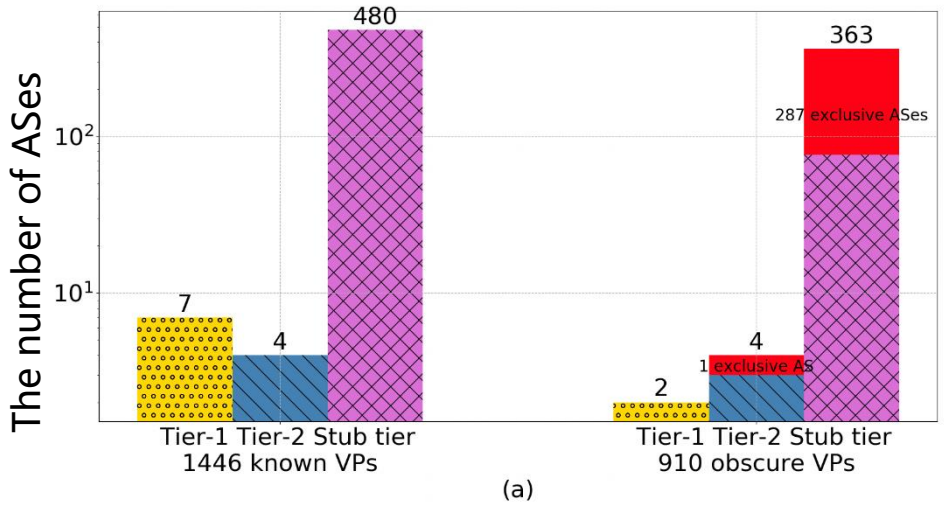
清華大學 Tsinghua University

APNIC FOUNDATION

OUR WORK ON LG

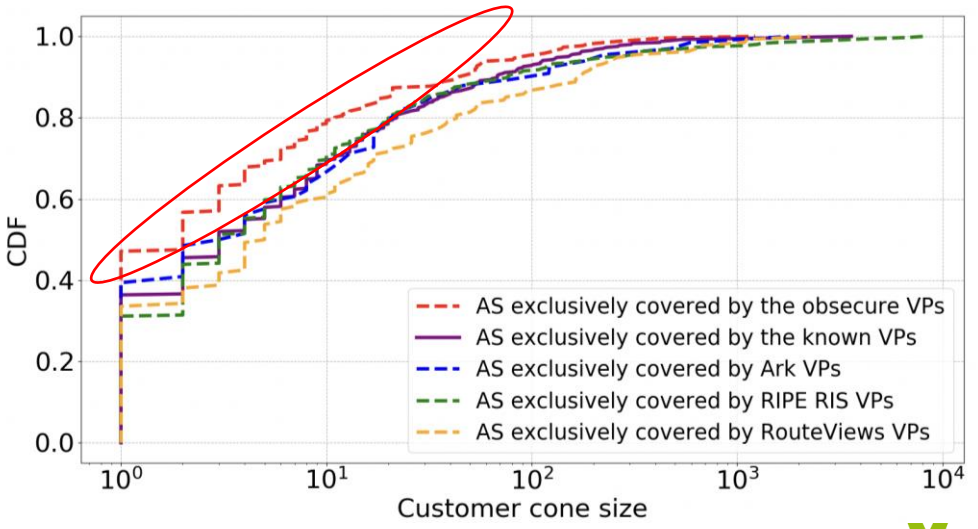
Network coverage improvements

- 910 obscure automatable LG VPs cover ***288 exclusive ASes***
- Compared with the VPs provided on other platforms (RIPE RIS/ Ark/ RouteViews)
  - ***Exclusively cover 262 ASes***



Most of the exclusive ASes are all ***in the stub tier***

	Ark VPs	RIPE RIS VPs	RouteViews VPs	Known LG VPs	Obscure LG VPs
ASes	115	520	270	491	369
Exclusive ASes	67	354	135	405	262



Tsinghua University

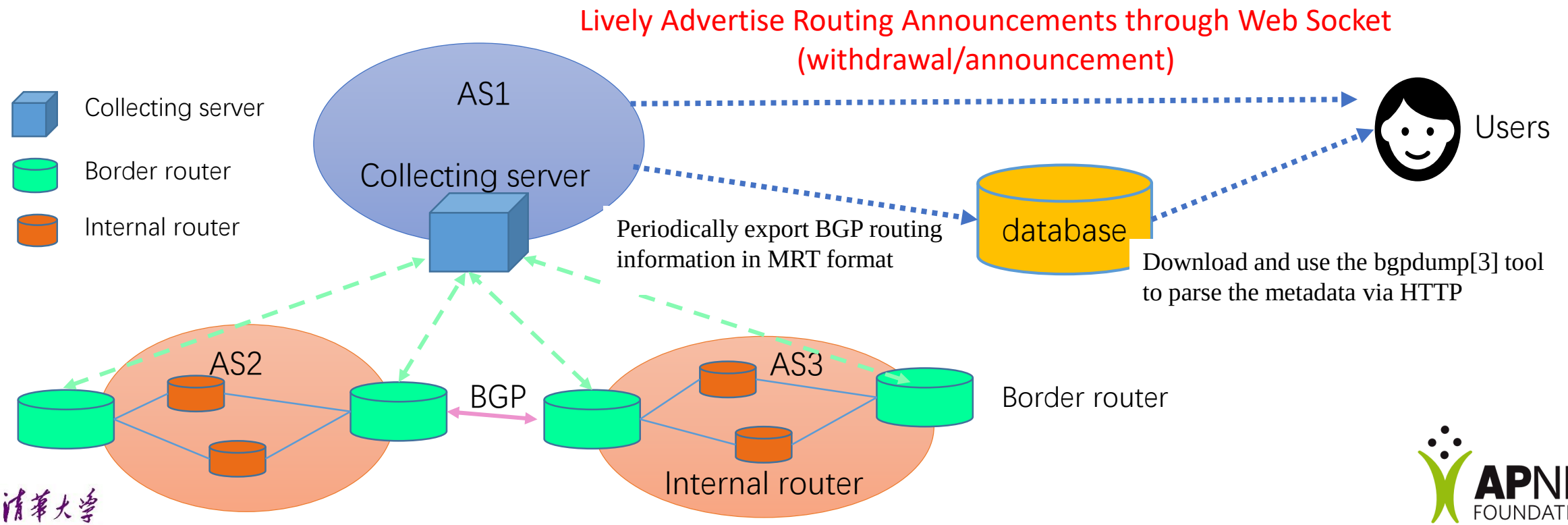
APNIC FOUNDATION

Route Information Sharing

- Looking Glass only for real time BGP route query
- RIS periodically dump BGP route for analysis and study
- Well-known RIS project
  - Route Views
  - RIPE RIS
  - PCH
  - BGPmon

Our Work on 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 Routing Information Sharing Platform -CGTF RIS

Index of /

Name	Last modified	Size	Description
readme.txt	2022-01-11 07:14	808	
ribs/	2022-02-17 12:05	-	
updates/	2022-02-17 12:45	-	

```
Our collector is currently peering with Following AS(Vantage Points) by private AS number 65534.
AS 23855(SINGAREN)
AS 4538(CERNET))
AS 38229(LEARN)
AS 63961(BDREN)
AS 24475(ThaiREN)

BGP RIB snapshot of colletor and BGP update messages it receives are periodically dumped,
2h for rib and 20 minutes for updates messages.

You can use 'bgpdump' to decompress  the compressed MRT format file for analysis.

This data is made available to anyone without restrictions.
If you copy the data and publish an analysis, please cite us in your publication.

Any question, please contact dev@dragonlab.org .
```

NRENs' Contribution:

- CERNET
- SingAREN
- BdREN
- LEARN
- ThaiREN

- https://bgp.cgtf.net
- Start from 2021-07-09
- Collector ASN：65534

清華大學 Tsinghua University

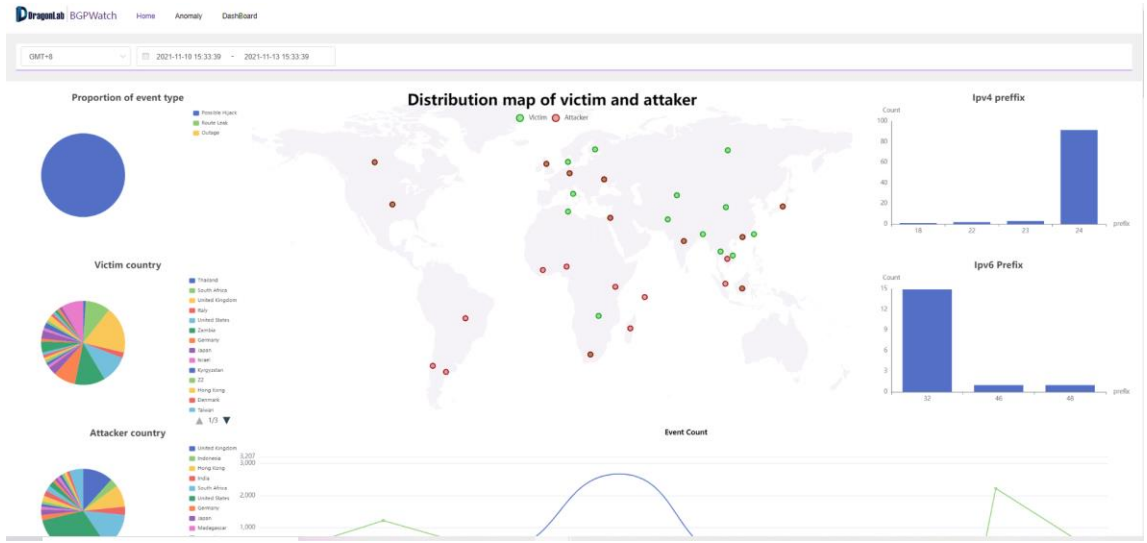
APNIC FOUNDATION

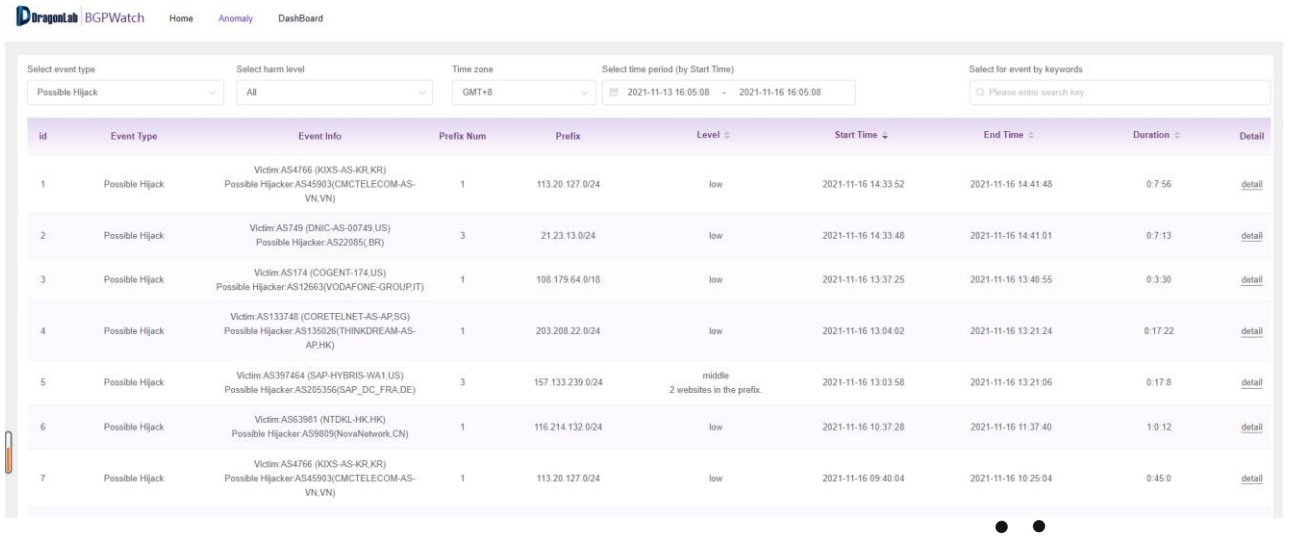
BGP Hijack

- Attackers maliciously reroute Internet traffic by announcing IP prefixes of other AS.
- BGP Hijack may cause great impact
- Countermeasures
  - Hijack Prevention
    - RPKI & BGPsec
  - Hijack detection
    - Hijack Detection System and mitigation

BGP Routing Monitoring and Analysis --BGP Watch

- http://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

Features --- Quick Response

- About 5 mins delay, much better than other systems
- Notify immediately when an event is detected, minimizing damage from hijackings

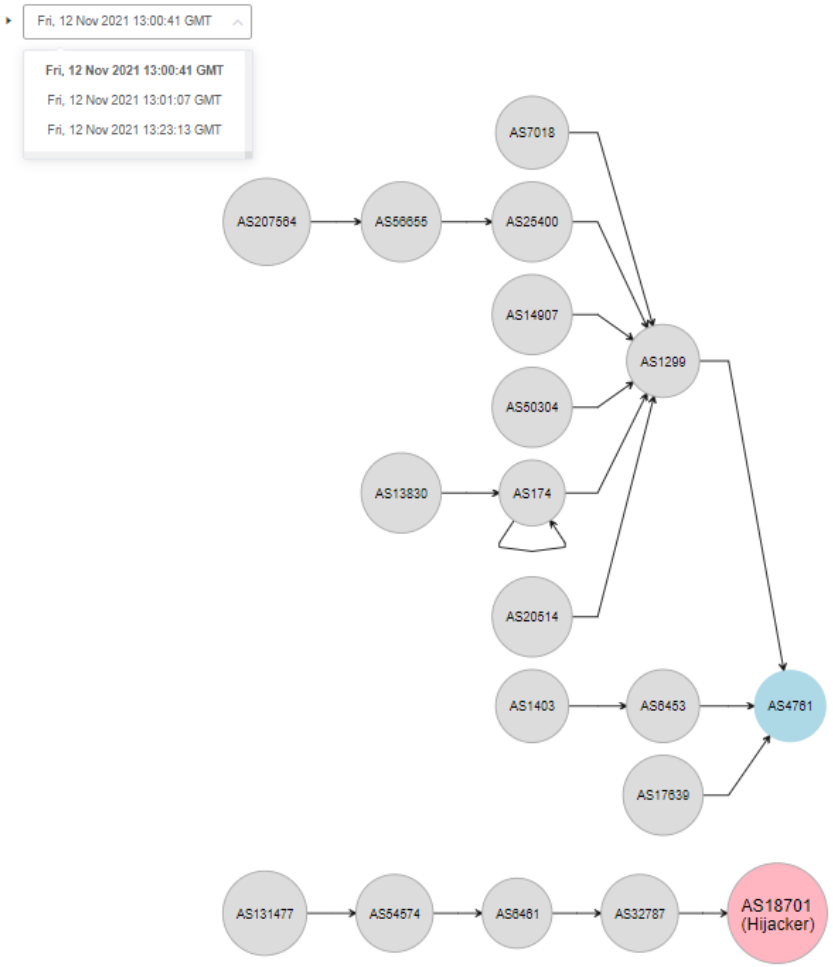
15	Ongoing Possible Hijack	Victim:AS58810 (IZUSCOLTD-BN,BN) Possible Hijacker:AS55547(WOODSNET-PH,PH)	1	146.88.165.0/24	low	2021-11-13 14:39:43	-	0:11:17	detail
16	Ongoing Possible Hijack	Victim:AS58810 (IZUSCOLTD-BN,BN) Possible Hijacker:AS55547(WOODSNET-PH,PH)	1	146.88.173.0/24	low	2021-11-13 14:39:43	-	0:11:17	detail
17	Ongoing Possible Hijack	Victim:AS58810 (IZUSCOLTD-BN,BN) Possible Hijacker:AS55547(WOODSNET-PH,PH)	1	43.251.69.0/24	low	2021-11-13 14:38:09	-	0:12:51	detail
18	Ongoing Possible Hijack	Victim:AS58810 (IZUSCOLTD-BN,BN) Possible Hijacker:AS55547(WOODSNET-PH,PH)	1	43.251.149.0/24	low	2021-11-13 14:38:09	-	0:12:51	detail
19	Ongoing Possible Hijack	Victim:AS58810 (IZUSCOLTD-BN,BN) Possible Hijacker:AS55547(WOODSNET-PH,PH)	1	135.84.249.0/24	low	2021-11-13 14:37:37	-	0:13:23	detail
20	Possible Hijack	Victim:AS137819 (BEEKS-AS-AP,JP) Possible Hijacker:AS206733(BFC-HK,GB)	1	103.100.74.0/24	low	2021-11-13 14:26:29	2021-11-13 14:29:46	0:3:17	detail

清華大學 Tsinghua University

APNIC FOUNDATION

Features --- Event replay

- Understanding how the BGP routing changes
- Analyze the extent of the impact of the event



清華大學 Tsinghua University

APNIC FOUNDATION

Features --- Event level evaluation

- **Evaluate event impact based on importance of AS and prefix.**

	Event Type	Event Info	Prefix Num	Prefix	Level	Start Time	End Time	Duration
1	Possible Hijack	Victim:AS18241 (SPINET,CN) Possible Hijacker:AS18214(TELUS-INTERNATIONAL,PH)	1	210.77.176.0/24	high 11 websites in the prefix.	2022-03-08 14:39:56	2022-03-08 15:11:43	0:31:47
2	Possible Hijack	Victim:AS50133 (WIMIFI,FR) Possible Hijacker:AS60304(STARNET,AL)	1	91.239.6.0/24	middle 2 websites in the prefix.	2022-03-07 18:55:58	2022-03-07 21:51:33	2:55:35
3	Possible Hijack	Victim:AS136907 (HWCLOUDS-AS-AP,HK) Possible Hijacker:AS55990(HWCSNET,CN)	2	139.9.98.0/24	middle 55990 is Cloud|IDC|CDN or top content provider.	2022-03-08 00:47:00	2022-03-08 06:54:05	6:7:5
4	Possible Hijack	Victim:AS18241 (SPINET,CN) Possible Hijacker:AS18214(TELUS-INTERNATIONAL,PH)	1	210.77.178.0/24	middle 3 websites in the prefix.	2022-03-08 14:39:56	2022-03-08 15:06:23	0:26:27
5	Possible Hijack	Victim:AS29538 (LINKOTEL-AS,LT) Possible Hijacker:AS209242(CLOUDFLARESPECTRUM,US)	1	45.158.56.0/24	middle 209242 is Cloud|IDC|CDN or top content provider.	2022-03-08 17:36:08	2022-03-08 21:17:13	3:41:5
6	Possible Hijack	Victim:AS29538 (LINKOTEL-AS,LT) Possible Hijacker:AS209242(CLOUDFLARESPECTRUM,US)	1	212.24.127.0/24	middle 209242 is Cloud|IDC|CDN or top content provider.	2022-03-08 17:36:08	2022-03-08 21:17:44	3:41:36

清華大學 Tsinghua University

APNIC FOUNDATION

Features --- Event Statistics Analysis

- Statistical analysis of event time, affected prefix, AS, country, etc.
- Global routing system security situational awareness

清華大學 Tsinghua University

APNIC FOUNDATION

Features - Low False Negtive , Low False Positive

- We use monitors all over the world （RIPE RIS & RouteViews & CGTF RIS）
- We check every BGP update message and use a lot of domain knowledge and rules for detecting

middle level

Possible Hijack Events

124.156.136.0|22-0 Possible Hijack Events

Victim AS：132203

Victim Country：CN (China)

Victim Description：TENCENT-NET-AP-CN

Start Time：2021-11-08 17:03:38

During Time：0:10:8

Hijacker AS：64

Hijacker Country：US (United States)

Hijacker Description：MITRE-AS-2

End Time：2021-11-08 17:13:46

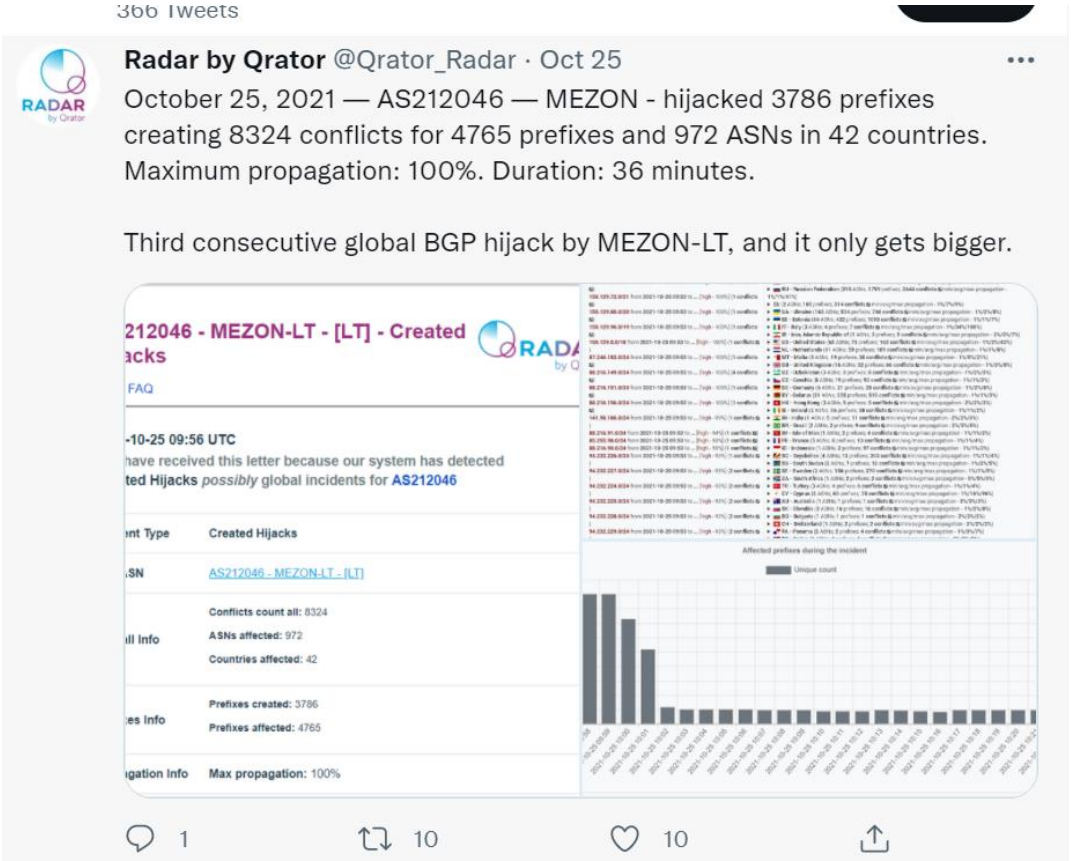
Comparison

	BGPWatch	CAIDA HI3	bgpstream
Real-time delay	5mins delay	More than 2 hours	More than 2 hours
Event replay	√	×	√
Event statistical analysis	√	×	×
Event level evaluation	√	×	×
Benign MOAS report	√	√	×
Reported hijack events per day	About 15-25	About 30-40	Less than 10
medium-scale Hijack events	√	√	√

Case-study – 1 UAB mezon Hijacking

- 2021-10-25 09:55 UTC AS212046（UAB Mezon, Lithuania ,AS rank:11754/73296） hijacked more than 2807 prefixes and 445 ASNs in 30 countries.

- Alarmed on multiple platforms
  - **CGTF BGPwatch （Alarm first)**
  - CAIDA HI3
  - Cisco BGPstream
  - Qrator Labs （through twitter)



Case-study – 1 UAB mezon Hijacking

BGPWatch oberserved that

- Duration varies with the hijacked prefixes, range from several seconds to tens of hours
- More 40 prefixes have websites
- The most affected country is Latvia(LV), more than 111 prefixes in LV were hijacked
- This event is very likely to be a malicious hijacking

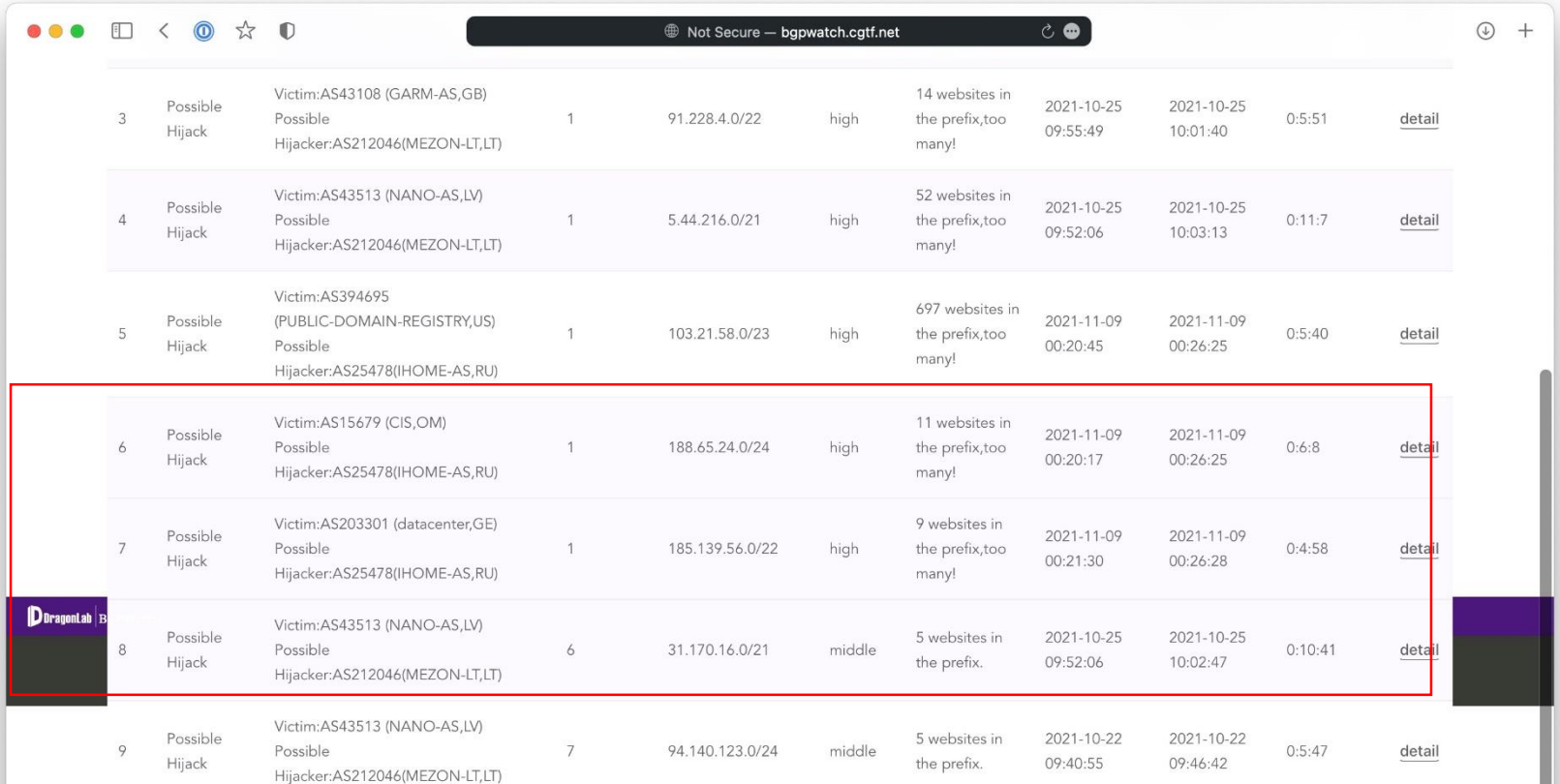
1	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	6	31.170.16.0/21	high	11 websites in the prefix,too manyl	2021-10-25 09:52:06	2021-10-25 10:02:47	0:10:41	detail
2	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	18	94.140.112.0/23	high	18 websites in the prefix,too manyl	2021-10-25 09:55:49	2021-10-25 10:02:04	0:6:15	detail
3	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	7	94.140.123.0/24	high	52 websites in the prefix,too manyl	2021-10-22 09:40:55	2021-10-22 09:46:42	0:5:47	detail
4	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	1	185.61.150.0/24	high	8 websites in the prefix,too manyl	2021-10-25 09:55:51	2021-10-25 10:03:45	0:7:54	detail
5	Possible Hijack	Victim:AS43108 (GARM-AS,GB) Possible Hijacker:AS212046(MEZON-LT,LT)	1	91.194.76.0/23	high	37 websites in the prefix,too manyl	2021-10-25 09:52:14	2021-10-25 10:01:40	0:9:26	detail
6	Possible Hijack	Victim:AS43108 (GARM-AS,GB) Possible Hijacker:AS212046(MEZON-LT,LT)	1	91.228.4.0/22	high	14 websites in the prefix,too manyl	2021-10-25 09:55:49	2021-10-25 10:01:40	0:5:51	detail
7	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	1	5.44.216.0/21	high	52 websites in the prefix,too manyl	2021-10-25 09:52:06	2021-10-25 10:03:13	0:11:7	detail

清華大學 Tsinghua University

APNIC FOUNDATION

Case-study – 2 IHOME-AS Hijacking

- 2021-11-9 00:21:00 UTC or so， AS 25478 (IHOME，Russia，ownes 5~7 prefixes） hijacked more than 181 prefixes and 135 ASes from 32 countries about 5 minutes
- Our system alarmed this event first again, about 5 minutes after the events happened
- At 10:23 Beijing Time (2:23 UTC，2 hours after the event)，bgpstram and CAIDA HI3 still no report （later , both platforms reported it)



3	Possible Hijack	Victim:AS43108 (GARM-AS,GB) Possible Hijacker:AS212046(MEZON-LT,LT)	1	91.228.4.0/22	high	14 websites in the prefix,too many!	2021-10-25 09:55:49	2021-10-25 10:01:40	0:5:51	detail
4	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	1	5.44.216.0/21	high	52 websites in the prefix,too many!	2021-10-25 09:52:06	2021-10-25 10:03:13	0:11:7	detail
5	Possible Hijack	Victim:AS394695 (PUBLIC-DOMAIN-REGISTRY,US) Possible Hijacker:AS25478(IHOME-AS,RU)	1	103.21.58.0/23	high	697 websites in the prefix,too many!	2021-11-09 00:20:45	2021-11-09 00:26:25	0:5:40	detail
6	Possible Hijack	Victim:AS15679 (CIS,OM) Possible Hijacker:AS25478(IHOME-AS,RU)	1	188.65.24.0/24	high	11 websites in the prefix,too many!	2021-11-09 00:20:17	2021-11-09 00:26:25	0:6:8	detail
7	Possible Hijack	Victim:AS203301 (datacenter,GE) Possible Hijacker:AS25478(IHOME-AS,RU)	1	185.139.56.0/22	high	9 websites in the prefix,too many!	2021-11-09 00:21:30	2021-11-09 00:26:28	0:4:58	detail
8	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	6	31.170.16.0/21	middle	5 websites in the prefix.	2021-10-25 09:52:06	2021-10-25 10:02:47	0:10:41	detail
9	Possible Hijack	Victim:AS43513 (NANO-AS,LV) Possible Hijacker:AS212046(MEZON-LT,LT)	7	94.140.123.0/24	middle	5 websites in the prefix.	2021-10-22 09:40:55	2021-10-22 09:46:42	0:5:47	detail

BGP hujack by AS25478?

Aftab Siddiqui aftab.siddiqui at gmail.com
Tue Nov 9 07:50:53 UTC 2021

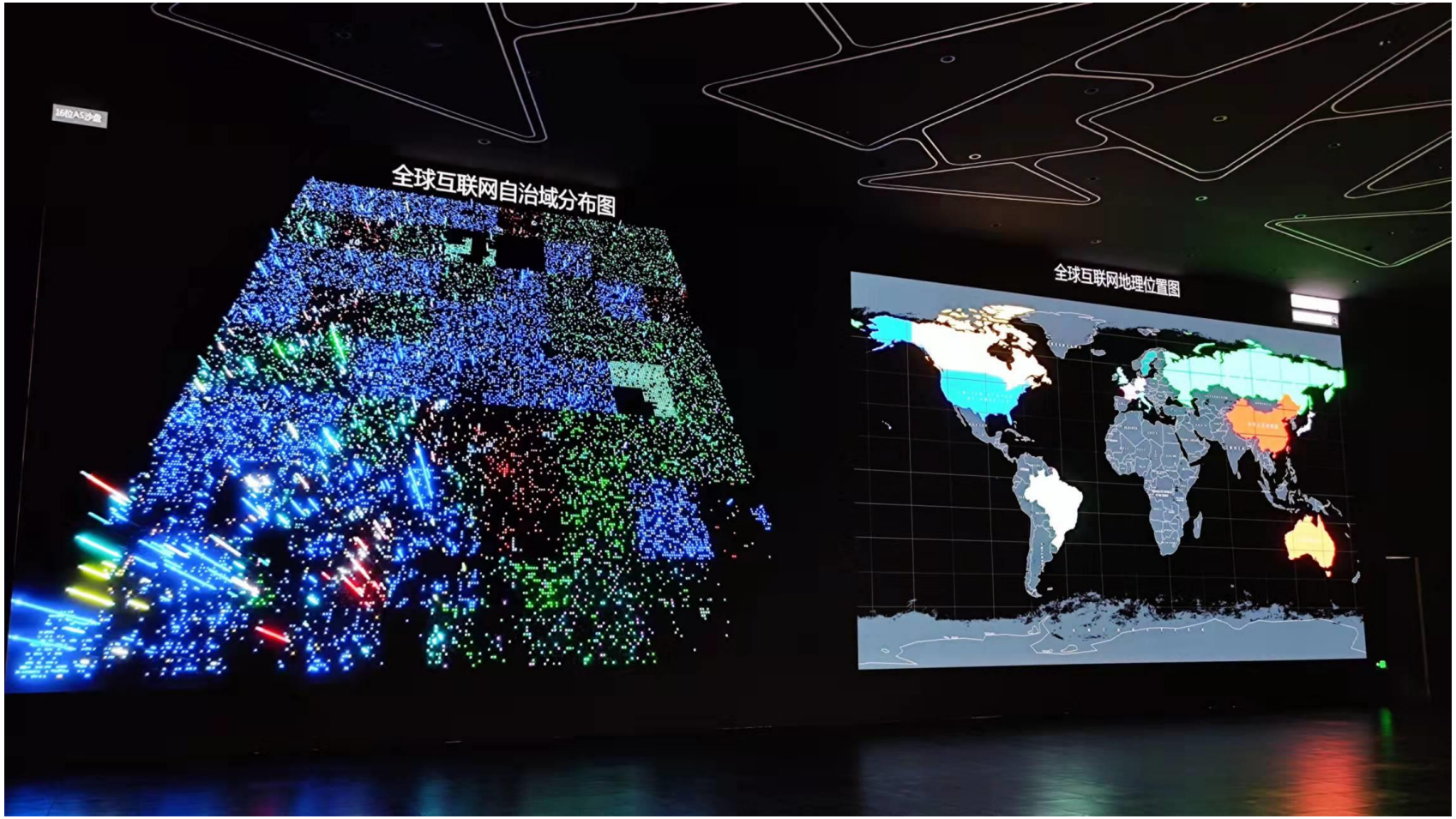
- Previous message (by thread): BGP hujack by AS25478?
- Next message (by thread): BGP hujack by AS25478?
- **Messages sorted by:** [date] [thread] [subject] [author]

Noction - could be but there were not many specifics in around 3200 routes they originated, there were few /12, /13, /14

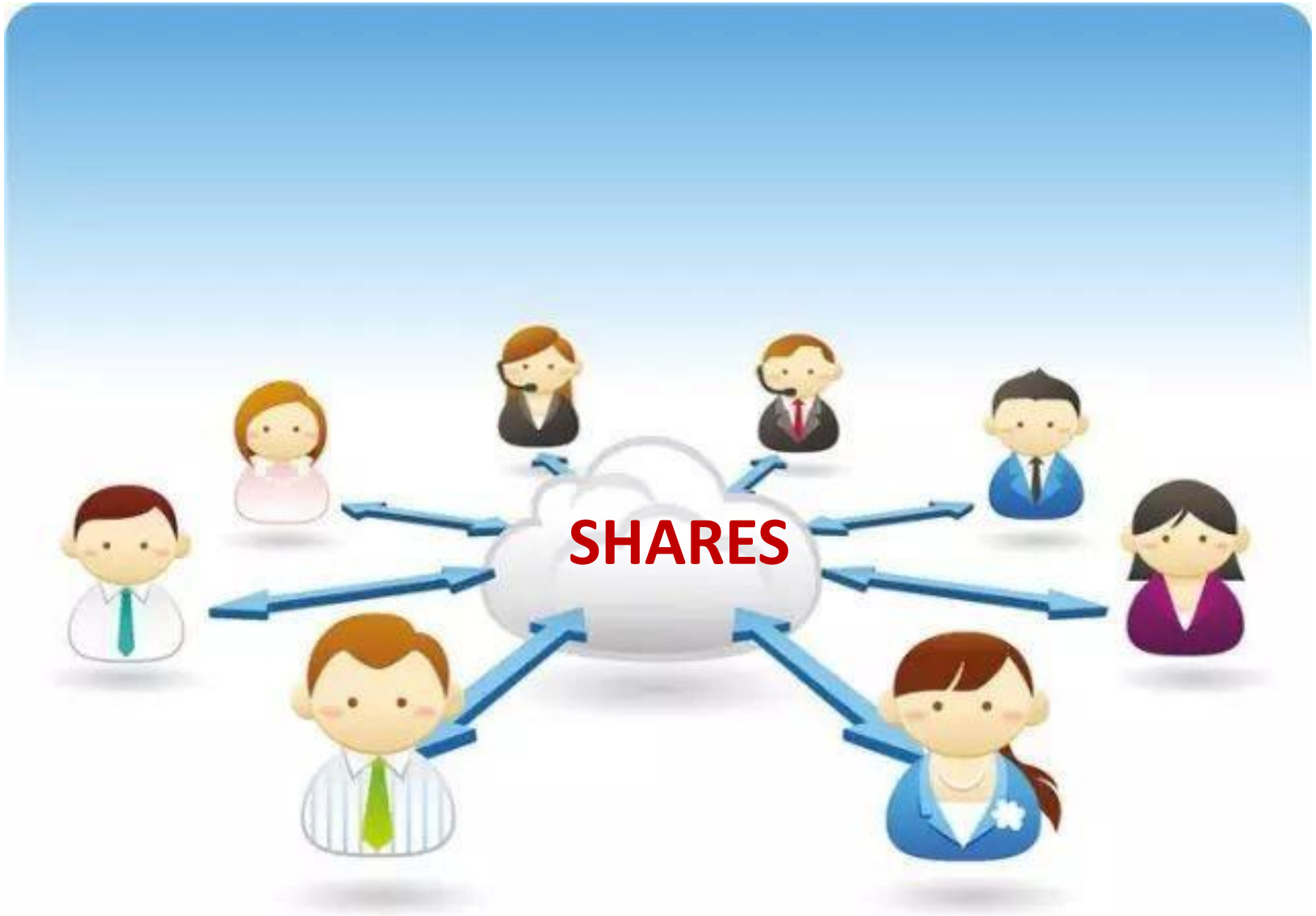
mistake probably.

```
121.128.0.0/12 39120 65478 25478
121.128.0.0/12 61568 65478 25478
121.144.0.0/13 61568 65478 25478
141.48.0.0/13 61568 65478 25478
203.40.0.0/13 39120 65478 25478
203.40.0.0/13 61568 65478 25478
```

Cyberspace Map



The cyberspace map is based on the original attributes of cyberspace: IP address, Protocol Port, and AS Number.
The right is the geographic map.
Cyberspace measurement information is displayed simultaneously on the two map system.



Looking forward to collaborating with all of you!

Contact us: acq@tsinghua.edu.cn

清華大學 Tsinghua University

APNIC FOUNDATION