(APNIC Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

--The First Technical Committee Meeting

May 10, 2022

清華大學 Tsinghua University

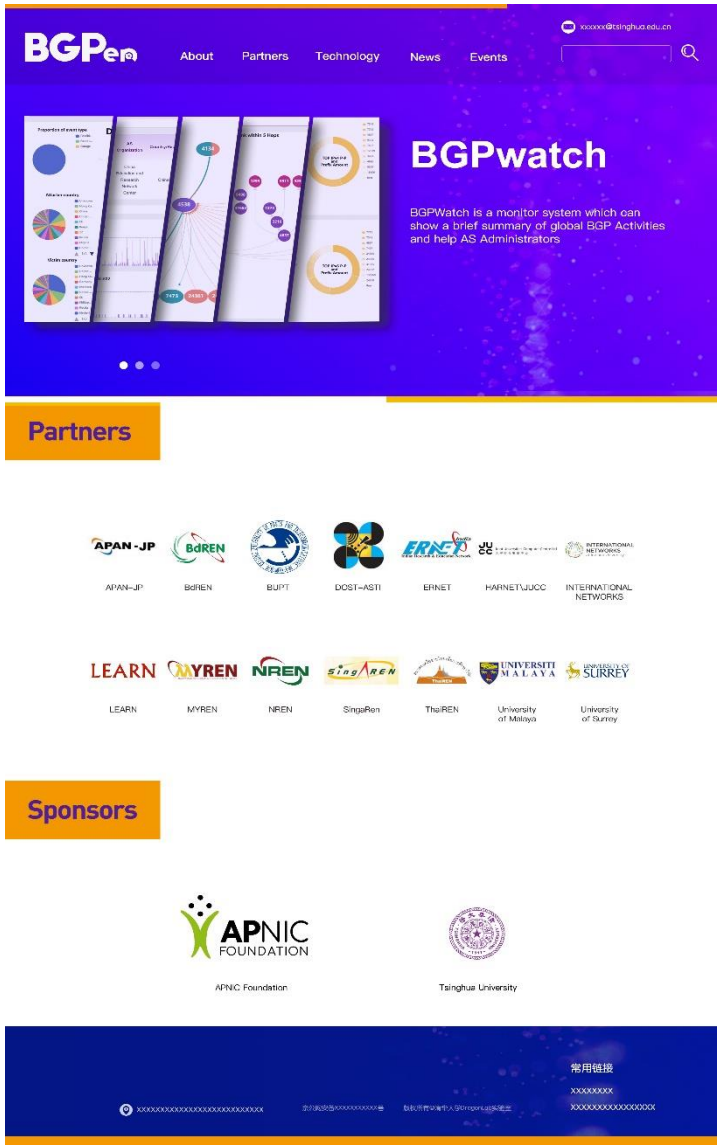
APNIC FOUNDATION

Outline

- Overall work plan
- Detailed work plan for each part
  - Web site
  - BGP sharing
  - Looking Glass
  - Analyzing and Diagnosing Platform
  - Research Topic
  - Knowledge Sharing
- The outcome from the bilateral meetings(Technical Part)
- Security Concerns
- Comments/Suggestions

	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-June
Looking Glass Platform	Requirements/Design(email, slack)	June
	Document info (How to implement, what partners need to do)	June
	Implement the connection with LG platform(meeting, email, slack)	June
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

Web Site Design

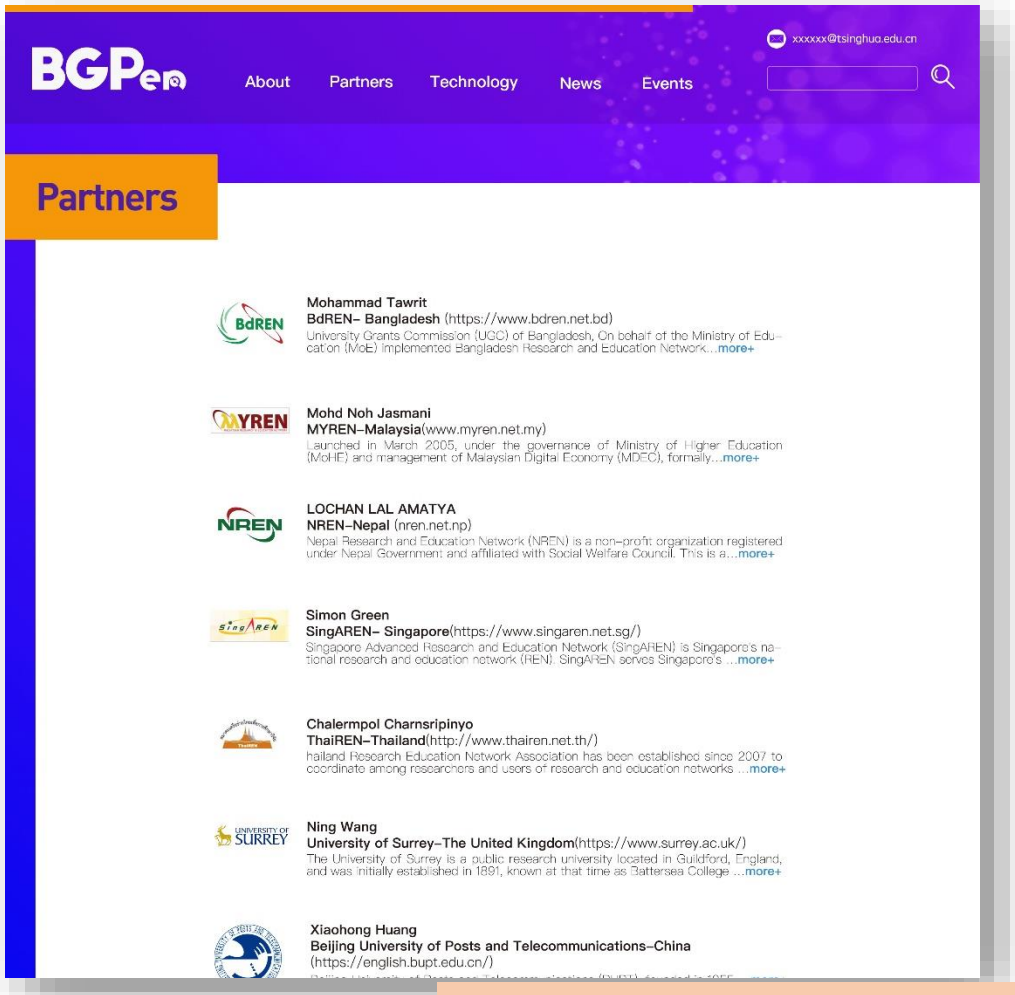


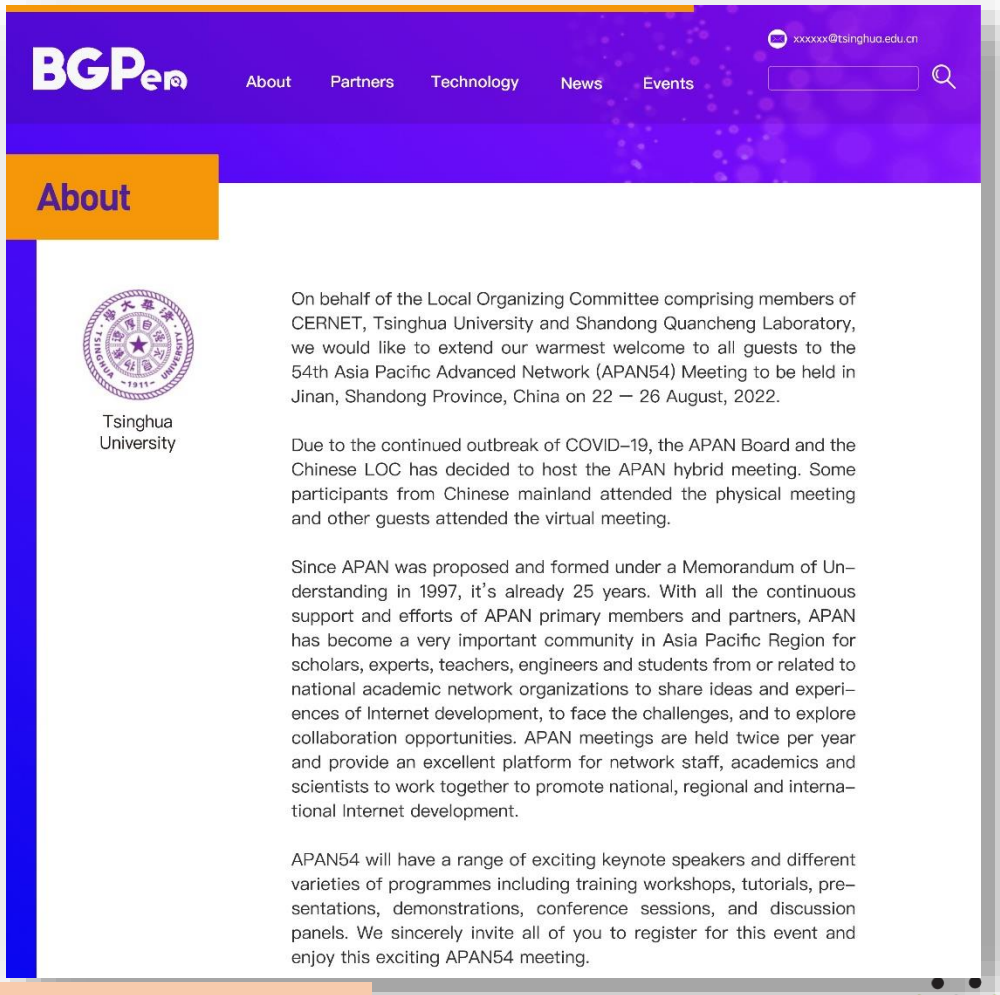
https://bgper.net

清華大學 Tsinghua University

APNIC FOUNDATION

Partner's Information in Web Site (Scheme 1)





Partners need to provide:
Logo, Introduction: 100-300 word

清華大學 Tsinghua University

APNIC FOUNDATION

Partner’s Information in Web Site (Scheme 2)

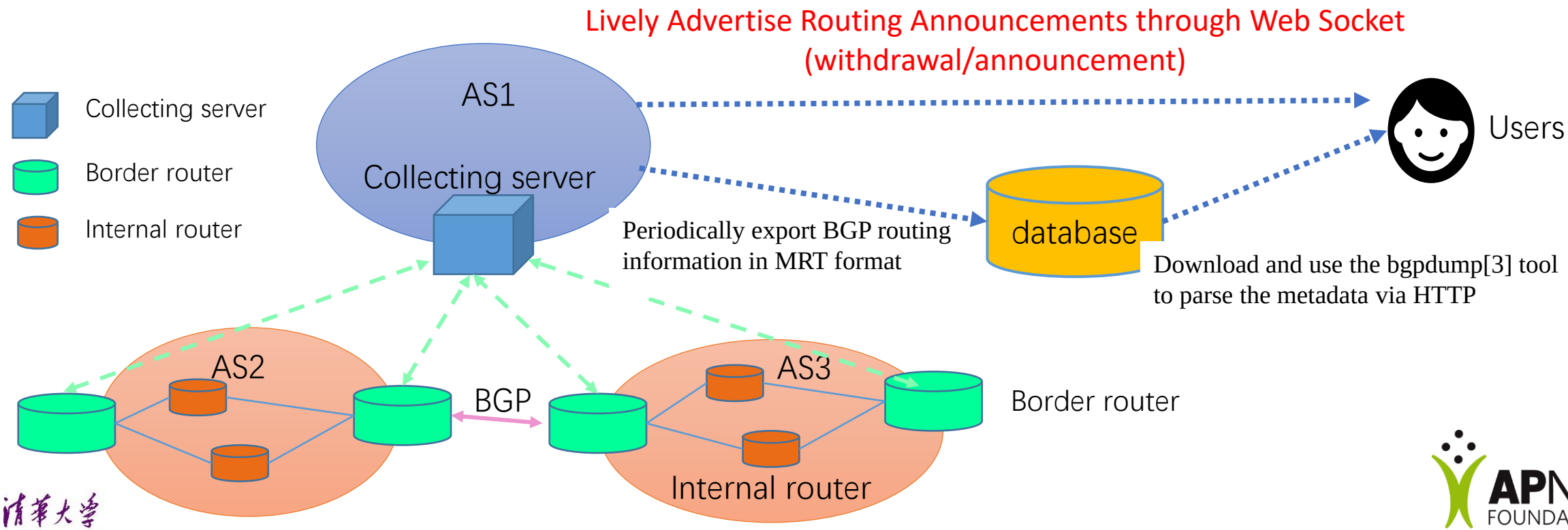
Alternative:
Logo, and a link to partner’s website

清華大學 Tsinghua University

APNIC FOUNDATION

Architecture of Route Information Sharing Platform

- 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 Routing Information Sharing Platform

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 .
```

https://bgp.cgtf.net

NRENs' Contribution:

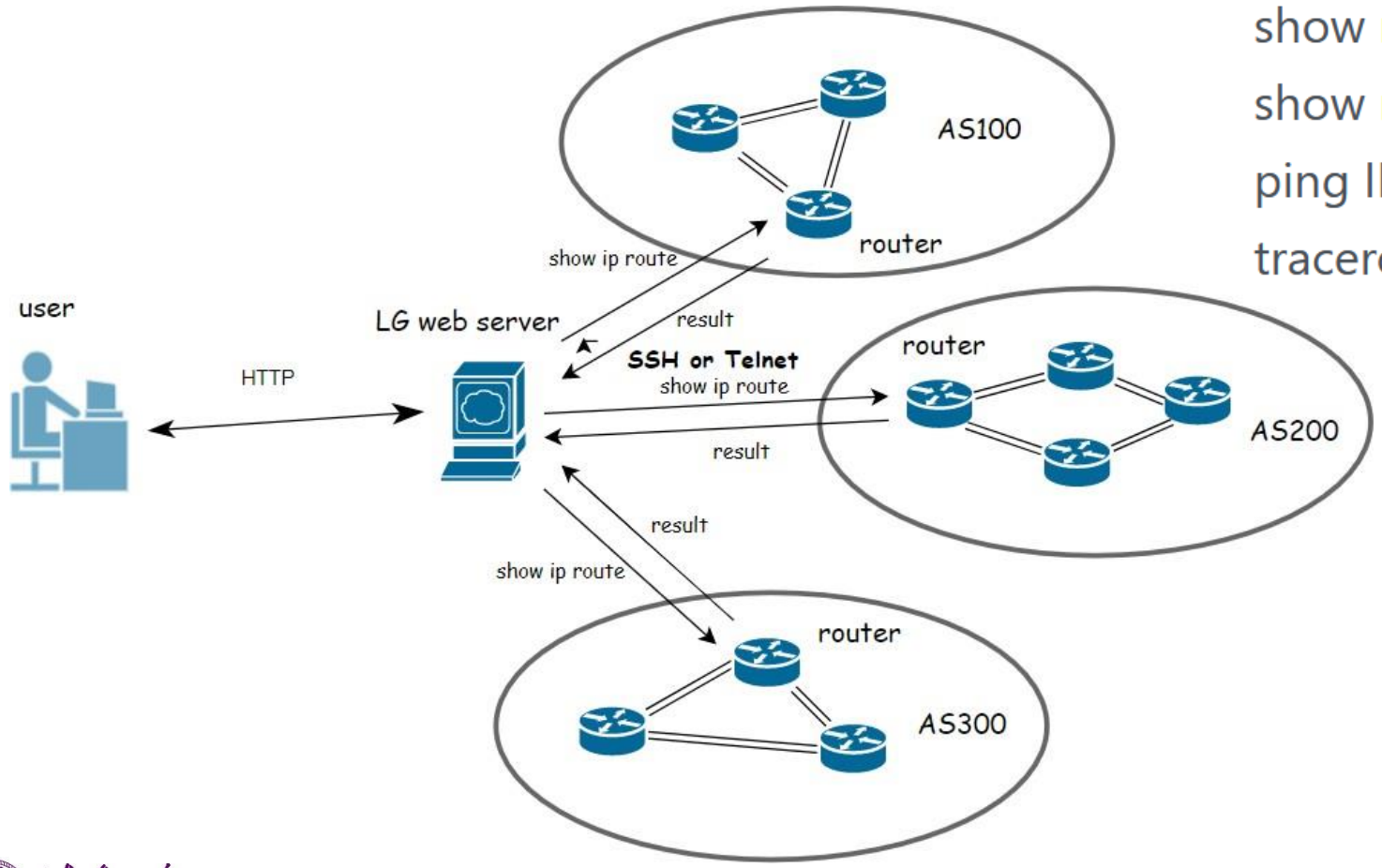
- CERNET
- SingAREN
- BdREN
- LEARN
- ThaiREN

- Executive Team will provide manual.
- Plan to be done in May-June.

清華大學 Tsinghua University

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

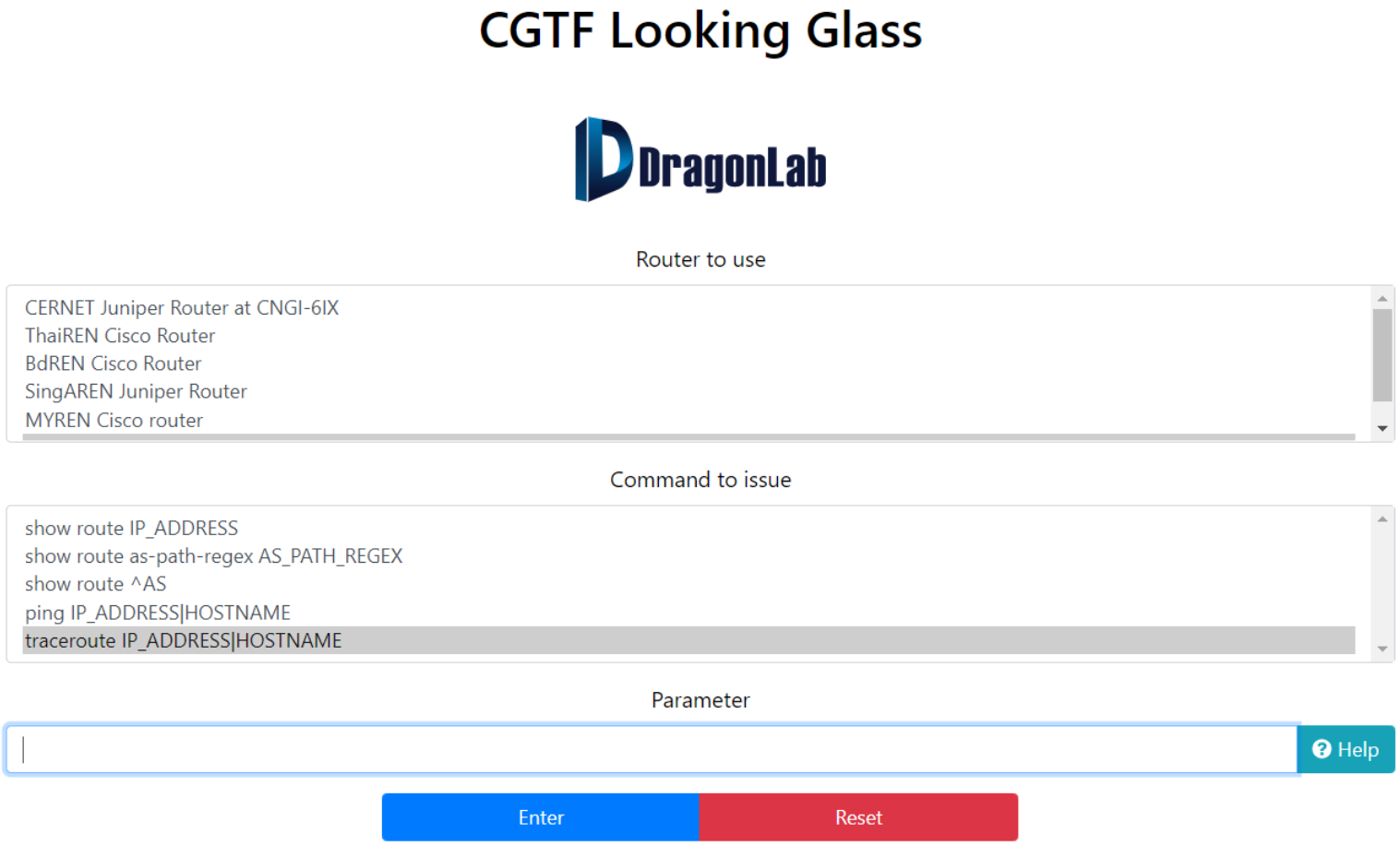
- Executive Team will provide manual.
- Plan to be done in June.

清華大學 Tsinghua University

APNIC FOUNDATION

Looking Glass Platform

- 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

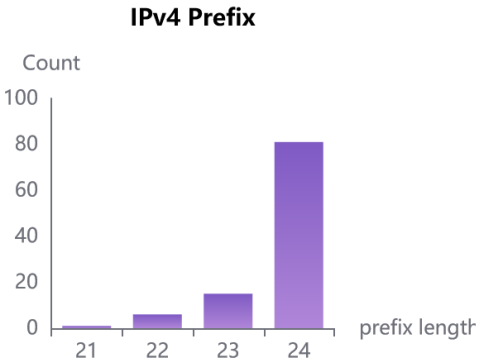
Tsinghua University

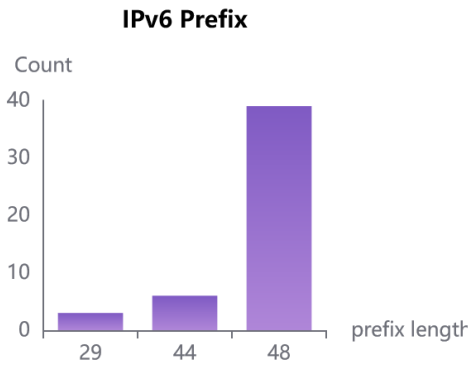
APNIC FOUNDATION

Analyzing and Diagnosing Platform

- Hijacking Detection
  - Prefix Hijacking Detection
  - Path Hijacking Detection
  - Send Alarm message to the victim
  - Partners can register for their AS , Prefix

https://bgpwatch.cgtf.net





DragonLab | BGPWatch Home Anomaly DashBoard

Select event type: Possible Hijack | Select harm level: All | Time zone: GMT+8 | Select time period (by Start Time): 2022-04-04 15:49:49 - 2022-04-14 15:49:49 | Select for event by keywords: Please enter search key

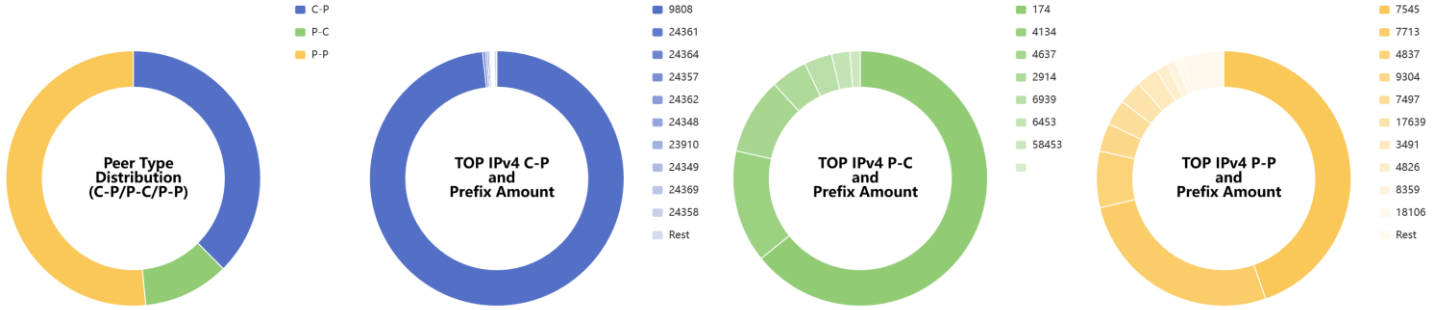
	Event Type	Event Info	Prefix Num	Prefix	Level	Start Time	End Time	Duration	Detail
1	Possible Hijack	Victim:AS401307 (,) Possible Hijacker:AS237(MERIT-AS-14,US)	2	136.228.50.0/24	low	2022-04-07 06:00:51	2022-04-07 06:06:34	0:5:43	detail
2	Possible Hijack	Victim:AS272021 (,) Possible Hijacker:AS28103(,PY)	1	2801:1a1::/44	low	2022-04-07 04:52:23	2022-04-07 04:57:24	0:5:1	detail
3	Possible Hijack	Victim:AS206943 (EANCENTER,US) Possible Hijacker:AS327790(Wirels-Connect,ZA)	1	161.123.144.0/22	low	2022-04-07 03:51:17	2022-04-07 03:54:28	0:3:11	detail
4	Possible Hijack	Victim:AS209014 (ITgration,DE) Possible Hijacker:AS49321(KULIKOV-AS,ZZ)	2	45.149.2.0/24	low	2022-04-07 02:58:59	2022-04-07 13:00:59	10:2:0	detail
5	Possible Hijack	Victim:AS209014 (ITgration,DE) Possible Hijacker:AS49321(KULIKOV-AS,ZZ)	1	146.19.146.0/24	low	2022-04-07 02:58:59	2022-04-07 13:02:08	10:3:9	detail
6	Possible Hijack	Victim:AS209014 (ITgration,DE) Possible Hijacker:AS49321(KULIKOV-AS,ZZ)	4	185.245.58.0/23	low	2022-04-07 02:58:54	2022-04-07 13:02:36	10:3:42	detail
7	Possible Hijack	Victim:AS40065 (CNSERVERS,US) Possible Hijacker:AS138628(GDI-AS-AP,HK)	1	23.225.155.0/24	high 155 websites in the prefix.	2022-04-07 01:20:15	2022-04-07 01:43:37	0:23:22	detail

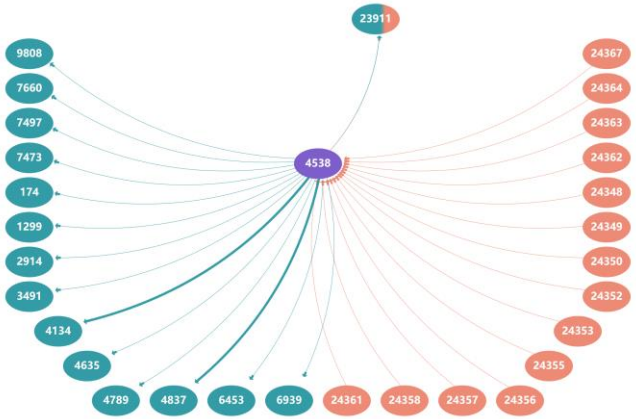
清華大學 Tsinghua University

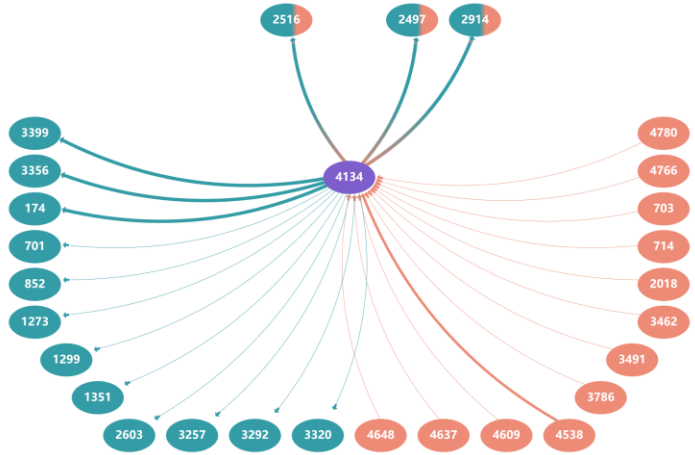
APNIC FOUNDATION

Analyzing and Diagnosing Platform

- Dashboard
  - Detailed information for AS
  - Peer relationship
  - Prefix import/export
  - Real time announcement received from peers
  - Path to a specific prefix
  - Path visualization
  - ……







清華大學 Tsinghua University

APNIC FOUNDATION

Research Topic

- New routing information brought by the BGPer routing Information sharing platform
- Analyzing the robustness of the Asia Pacific Area routing
- Is peering relationships among NREN fully utilized?

Knowledge Sharing

- Any topic partners interested
  - Problems
  - RPKI
  - BGPSEC
  - MANRS

The outcome from the bilateral meetings

- APAN-JP: RPKI is becoming popular and the JP NIC is pushing like that way. Notification service will be very helpful. RADAR
- TransPAC: Asymmetrical routing. Traffic taking inefficient route
- ITB： Check and make sure routing going specific path, monitoring, debugging
- PREGINET: Find inefficient routing , BGP visualization. Open source: Zabbix, MRTG.
- KREONET: Real system in production level, time schedule, long term running, security concern with looking glass.
- REANNZ:MANRS compliance
- AARNET: GRIP (CAIDA’S BGP OBSERVATORY)

Security Concerns

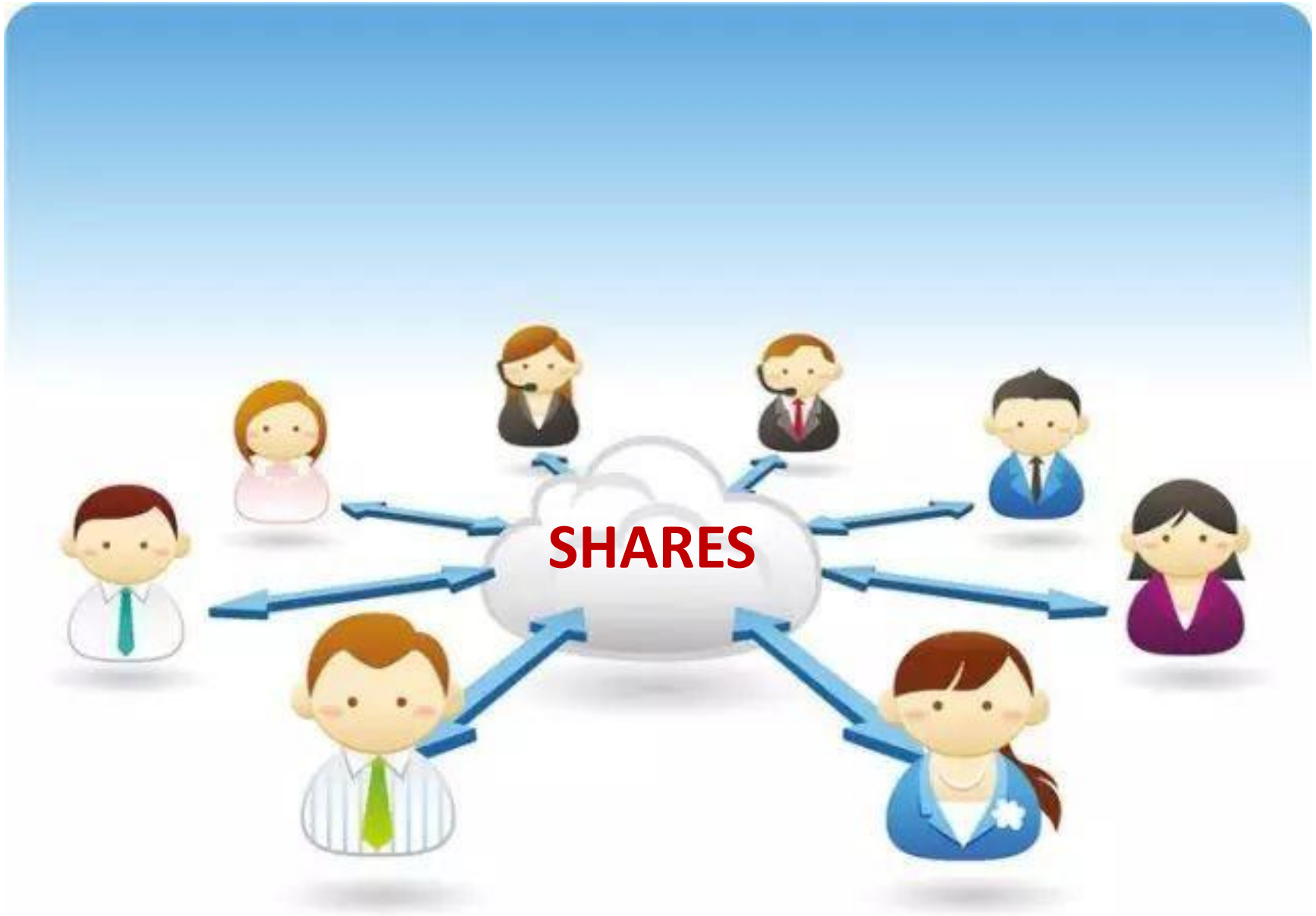
- Where the data is stored?
  - BGP peering server: Cloud server in Singapore
  - BGPWatch: Cloud server in Hongkong
  - Looking Glass: Cloud server in Hongkong
- Will peering harm my network?
  - We use routing FRR[2] to simulate a real BGP router and it won't send routing anouncement.
- Will sharing routing information harm my network?
  - Routeviews and RIPE RIS are two most famous RIS sharing platform.
- Our security 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.

Todo List

	Detailed Technical Committee Work Plan	Tentative Timeline	Todo
Timeline	Discussion on Timeline	May	
Project Web Site	Requirements/Design	May	
	Partner's information	May	Partners:send logo, introduction (100-300 words) to executive team:
	Setting up project website	May	Executive Team: set up the website.
BGP Routing Information Sharing	Requirements/Design(email, slack)	May-June	Executive Team :send manual to partners, discuss with each partner, and implement the peering. Partners: setup peering.
	Document info (How to implement, what partners need to do)	May-June	
	Implement the peering (meeting, email, slack)	May-June	

Comments/Suggestions

- ??


SHARES