(APNIC ISIF Project)

An Extension of the Ongoing Project “Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform” Project

Technical Committee Report

Tsinghua University
April 8, 2024

Outline

- Updates
- Demo of New Functions
- Future Work Plan
- Survey on Source Address Validation Deployment

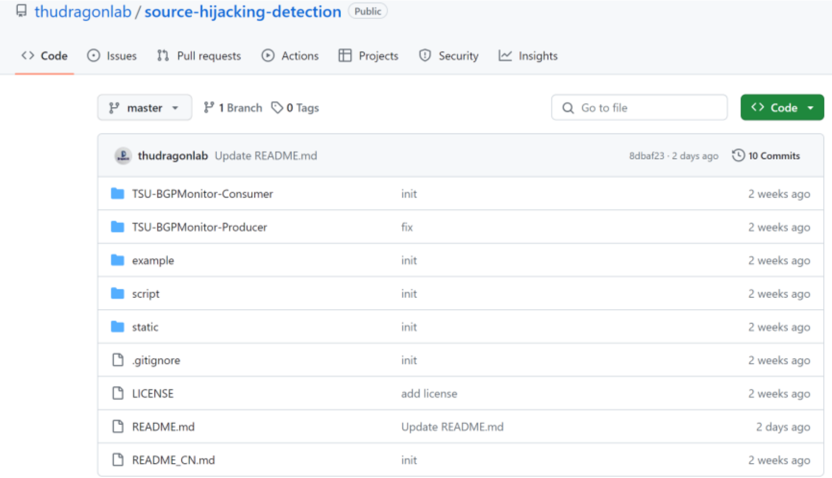
Open Source

https://github.com/thudragonlab/source-hijacking-detection

https://github.com/thudragonlab/bgpwatch-frontend

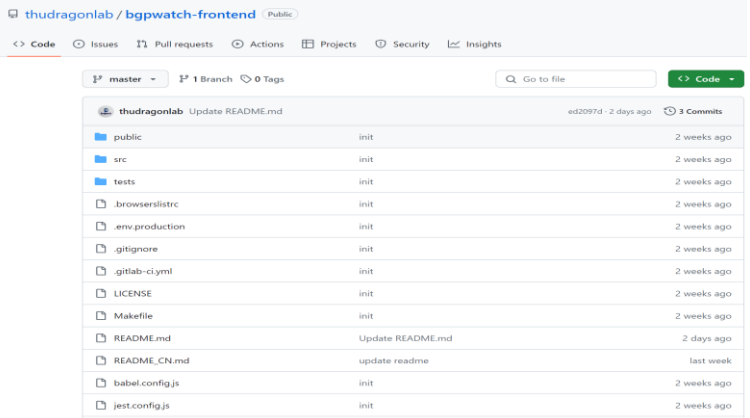
https://github.com/thudragonlab/bgpwatch-backend

https://github.com/thudragonlab/bgp-analysis



thudragonlab Update README.md 8dbaf23 · 2 days ago 10 Commits

TSU-BGPMonitor-Consumer	init	2 weeks ago
TSU-BGPMonitor-Producer	fix	2 weeks ago
example	init	2 weeks ago
script	init	2 weeks ago
static	init	2 weeks ago
.gitignore	init	2 weeks ago
LICENSE	add license	2 weeks ago
README.md	Update README.md	2 days ago
README_CN.md	init	2 weeks ago

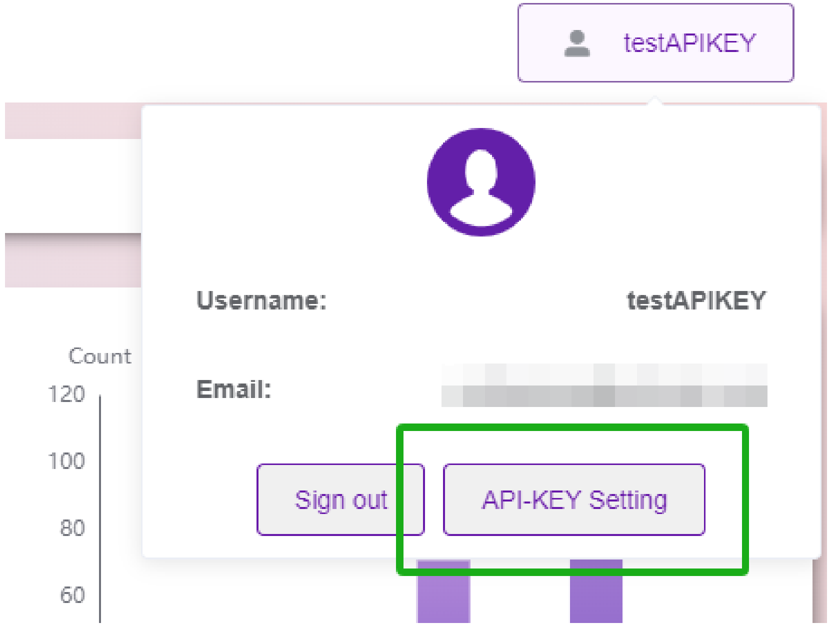


thudragonlab Update README.md ed2097d · 2 days ago 3 Commits

public	init	2 weeks ago
src	init	2 weeks ago
tests	init	2 weeks ago
.browserslistrc	init	2 weeks ago
.env.production	init	2 weeks ago
.gitignore	init	2 weeks ago
.gitlab-ci.yml	init	2 weeks ago
LICENSE	init	2 weeks ago
Makefile	init	2 weeks ago
README.md	Update README.md	2 days ago
README_CN.md	update readme	last week
babel.config.js	init	2 weeks ago
jest.config.js	init	2 weeks ago

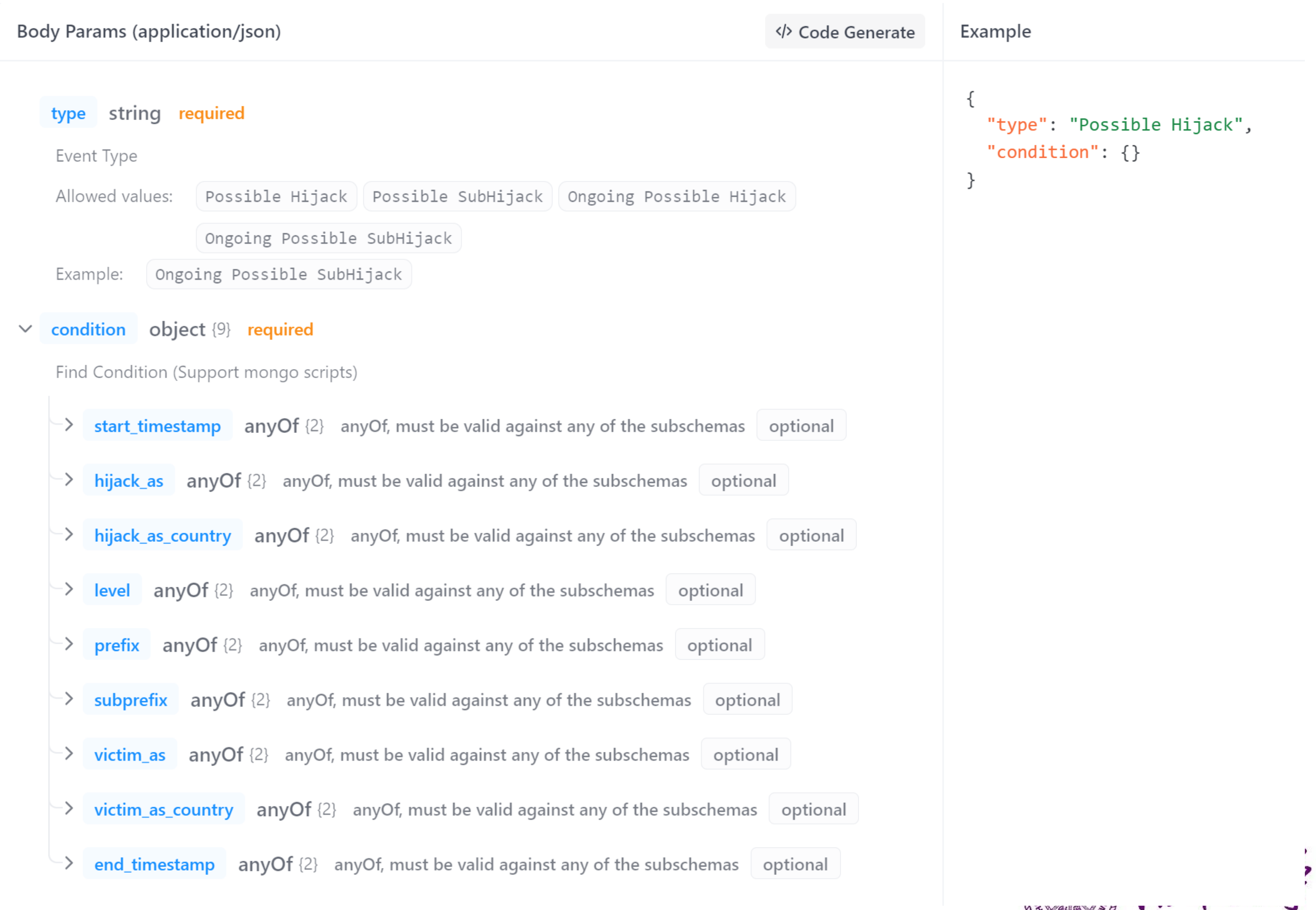
Open API

- /get_event_by_condition
- /get_event_detail



Username: testAPIKEY

Email: [redacted]



Body Params (application/json)

type string required

Event Type

Allowed values: `Possible Hijack` `Possible SubHijack` `Ongoing Possible Hijack` `Ongoing Possible SubHijack`

Example: `Ongoing Possible SubHijack`

condition object {9} required

Find Condition (Support mongo scripts)

- start_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- hijack_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- level anyOf {2} anyOf, must be valid against any of the subschemas optional
- prefix anyOf {2} anyOf, must be valid against any of the subschemas optional
- subprefix anyOf {2} anyOf, must be valid against any of the subschemas optional
- victim_as anyOf {2} anyOf, must be valid against any of the subschemas optional
- victim_as_country anyOf {2} anyOf, must be valid against any of the subschemas optional
- end_timestamp anyOf {2} anyOf, must be valid against any of the subschemas optional

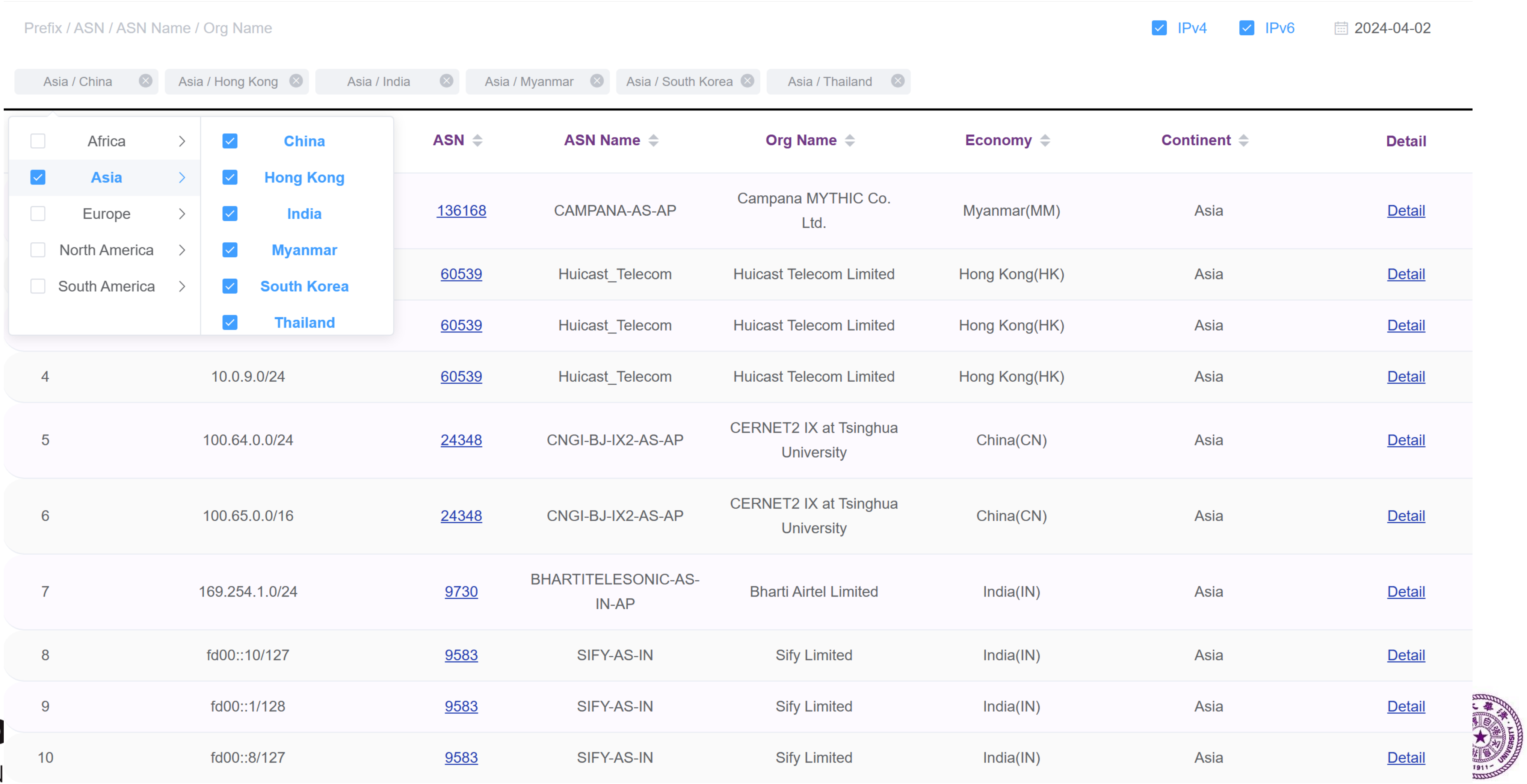
```
{
  "type": "Possible Hijack",
  "condition": {}
}
```

APNIC FOUNDATION

Tsinghua University

Bogon IP Address Detection

Support searching by continent, economy, AS



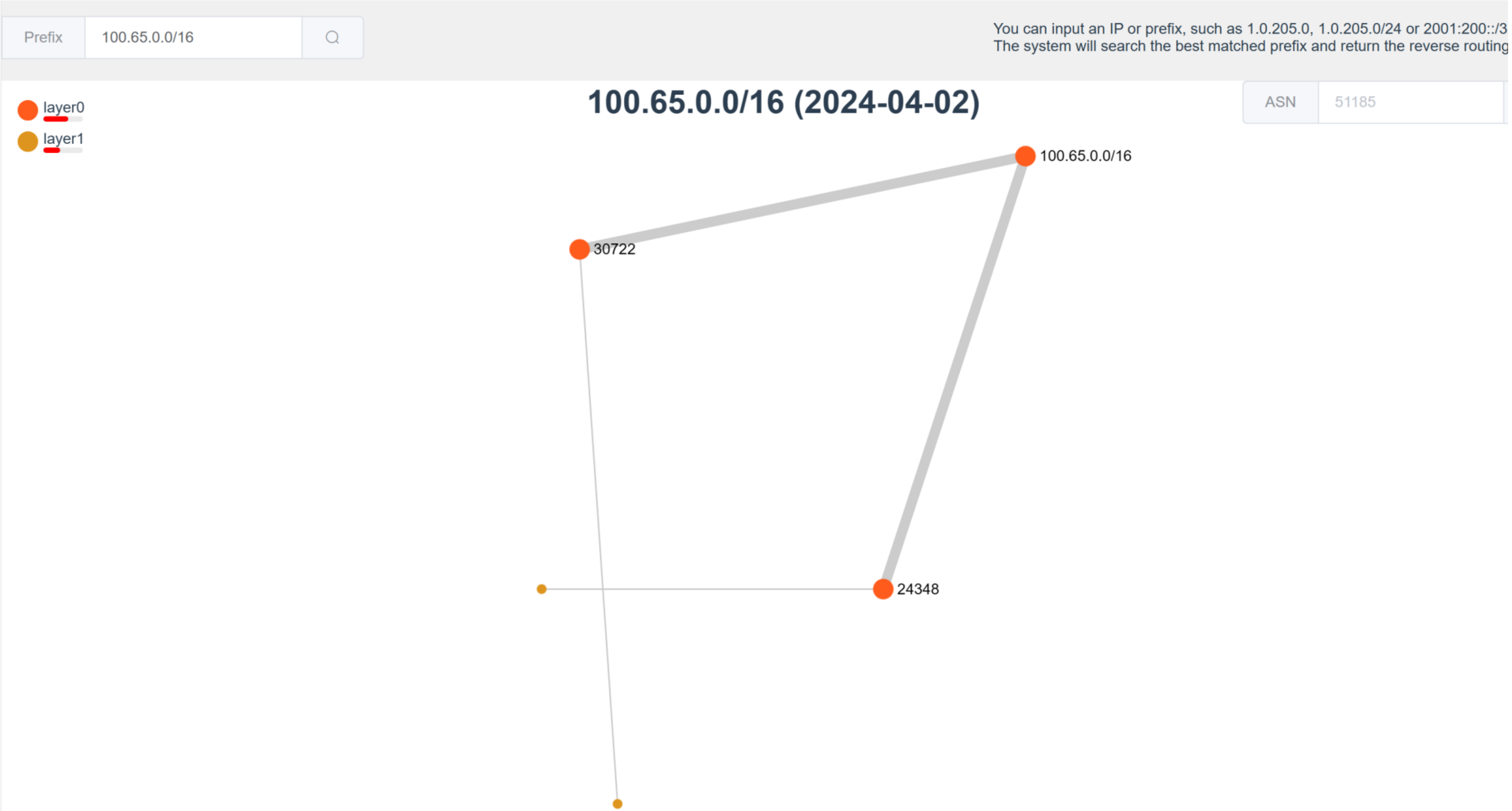
Prefix / ASN / ASN Name / Org Name

☑ IPv4 ☑ IPv6 2024-04-02

Asia / China ⊗ Asia / Hong Kong ⊗ Asia / India ⊗ Asia / Myanmar ⊗ Asia / South Korea ⊗ Asia / Thailand ⊗

		ASN	ASN Name	Org Name	Economy	Continent	Detail
		136168	CAMPANA-AS-AP	Campana MYTHIC Co. Ltd.	Myanmar(MM)	Asia	Detail
		60539	Huicast_Telecom	Huicast Telecom Limited	Hong Kong(HK)	Asia	Detail
		60539	Huicast_Telecom	Huicast Telecom Limited	Hong Kong(HK)	Asia	Detail
4	10.0.9.0/24	60539	Huicast_Telecom	Huicast Telecom Limited	Hong Kong(HK)	Asia	Detail
5	100.64.0.0/24	24348	CNGI-BJ-IX2-AS-AP	CERNET2 IX at Tsinghua University	China(CN)	Asia	Detail
6	100.65.0.0/16	24348	CNGI-BJ-IX2-AS-AP	CERNET2 IX at Tsinghua University	China(CN)	Asia	Detail
7	169.254.1.0/24	9730	BHARTITELESONIC-AS-IN-AP	Bharti Airtel Limited	India(IN)	Asia	Detail
8	fd00::10/127	9583	SIFY-AS-IN	Sify Limited	India(IN)	Asia	Detail
9	fd00::1/128	9583	SIFY-AS-IN	Sify Limited	India(IN)	Asia	Detail
10	fd00::8/127	9583	SIFY-AS-IN	Sify Limited	India(IN)	Asia	Detail

Propagation of the Bogon IP Address



Prefix: 100.65.0.0/16

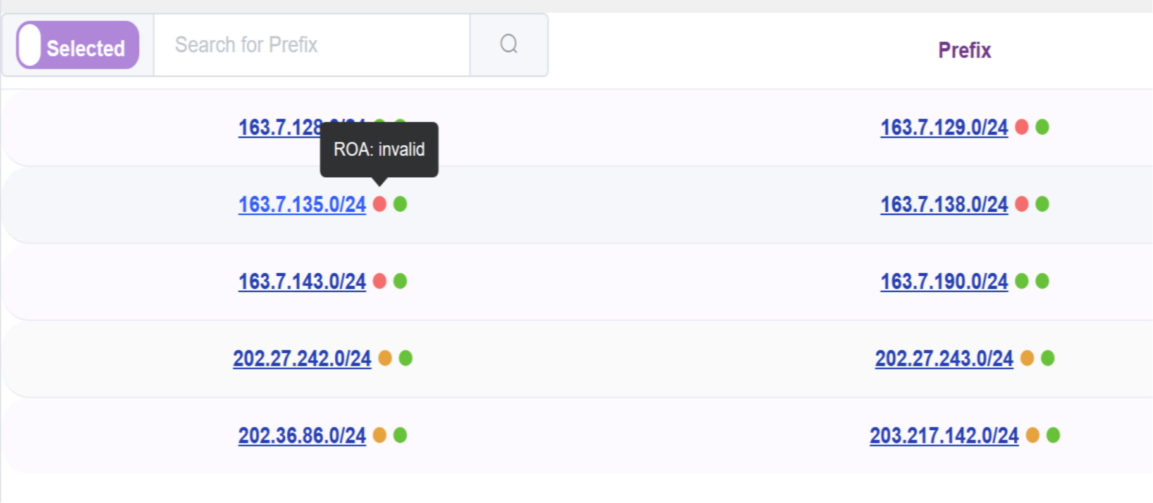
You can input an IP or prefix, such as 1.0.205.0, 1.0.205.0/24 or 2001:200::/3
The system will search the best matched prefix and return the reverse routing

100.65.0.0/16 (2024-04-02)

ASN: 51185

Consistency of Prefixes in RIR and ROA

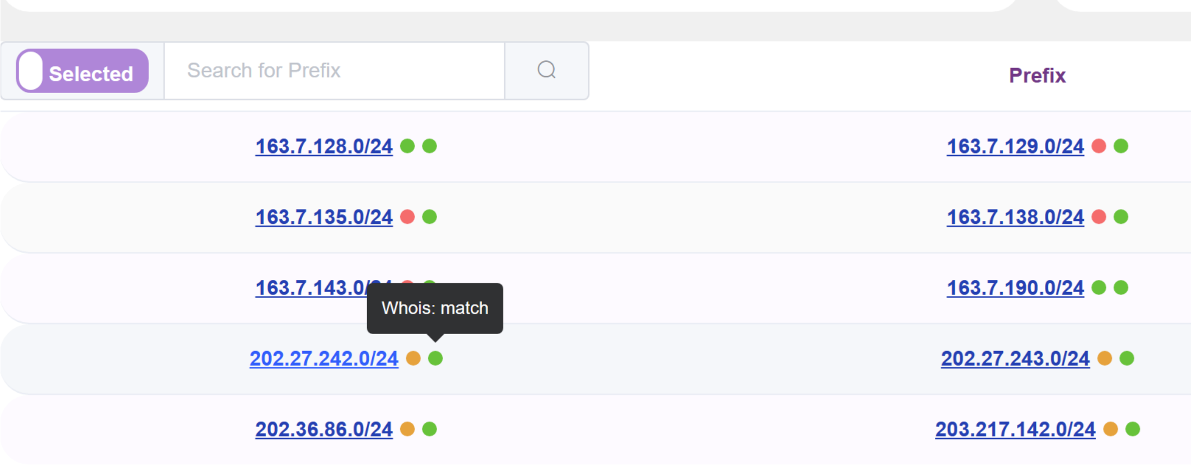
1. Consistency between Prefix Advertisement and RIR? Match/Not Match
2. Consistency between Prefix Advertisement and ROA? Match/ Invalid/ Not found



Selected | Search for Prefix | Prefix

163.7.128	163.7.129.0/24 🔴 🟢
163.7.135.0/24 🔴 🟢	163.7.138.0/24 🔴 🟢
163.7.143.0/24 🔴 🟢	163.7.190.0/24 🟢 🟢
202.27.242.0/24 🟠 🟢	202.27.243.0/24 🟠 🟢
202.36.86.0/24 🟠 🟢	203.217.142.0/24 🟠 🟢

ROA: invalid



Selected | Search for Prefix | Prefix

163.7.128.0/24 🟢 🟢	163.7.129.0/24 🔴 🟢
163.7.135.0/24 🔴 🟢	163.7.138.0/24 🔴 🟢
163.7.143.0/	163.7.190.0/24 🟢 🟢
202.27.242.0/24 🟠 🟢	202.27.243.0/24 🟠 🟢
202.36.86.0/24 🟠 🟢	203.217.142.0/24 🟠 🟢

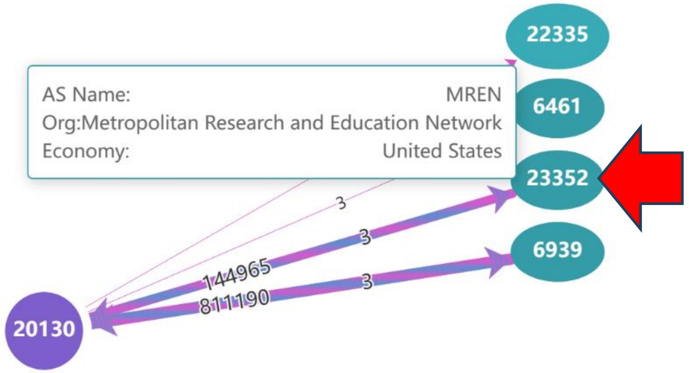
Whois: match

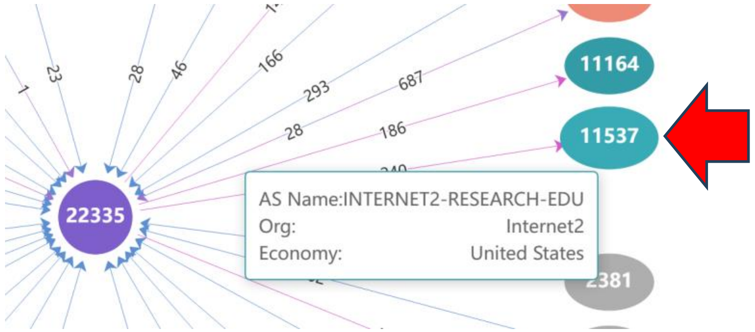
APNIC FOUNDATION

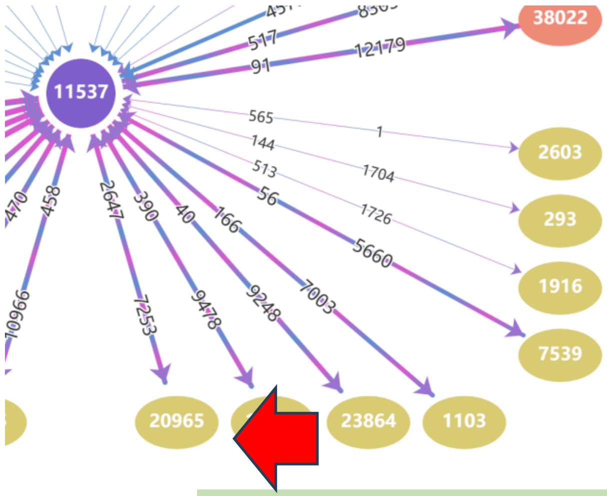
清華大學 Tsinghua University

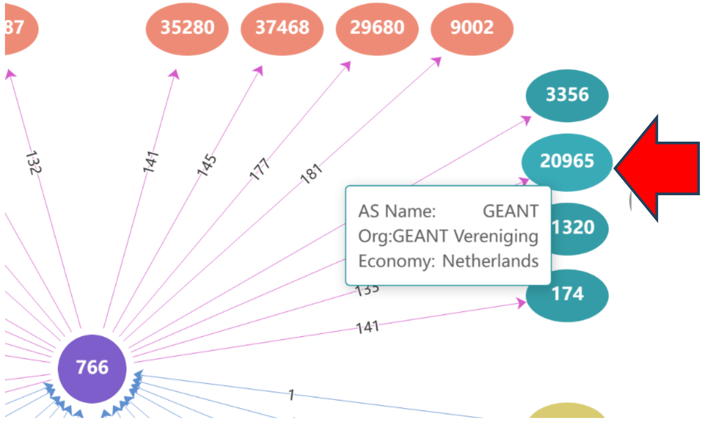
R&E ASes Transit Through Commercial ASes

R&E AS and Prefix :
https://bgp.nsrc.org/REN/GEANT/bgp.ipv4
https://bgp.nsrc.org/REN/GEANT/bgp.ipv6


AS Name: MREN
Org:Metropolitan Research and Education Network
Economy: United States


AS Name:INTERNET2-RESEARCH-EDU
Org: Internet2
Economy: United States




AS Name: GEANT
Org:GEANT Vereniging
Economy: Netherlands

```
"prefixes" : [
        "80.73.144.0/21",
        "80.73.156.0/22",
        "185.190.240.0/22",
        "80.73.152.0/23"
],
Real Routing Path: "20130 6939 766 34511",
```

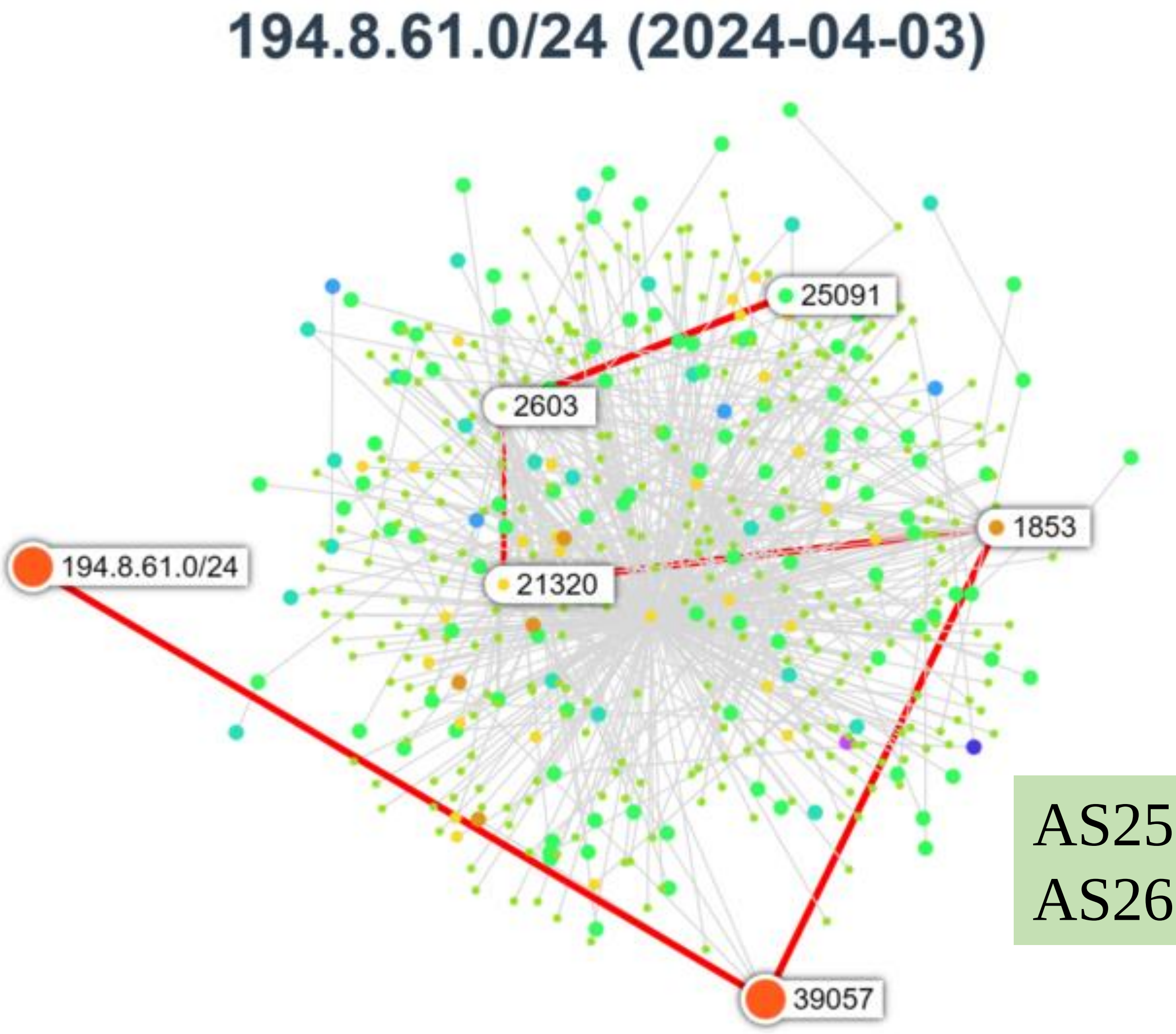
There exist R&D path:20130 22335 11537 20965 766, but the path with commercial AS 6939 is used.

6939

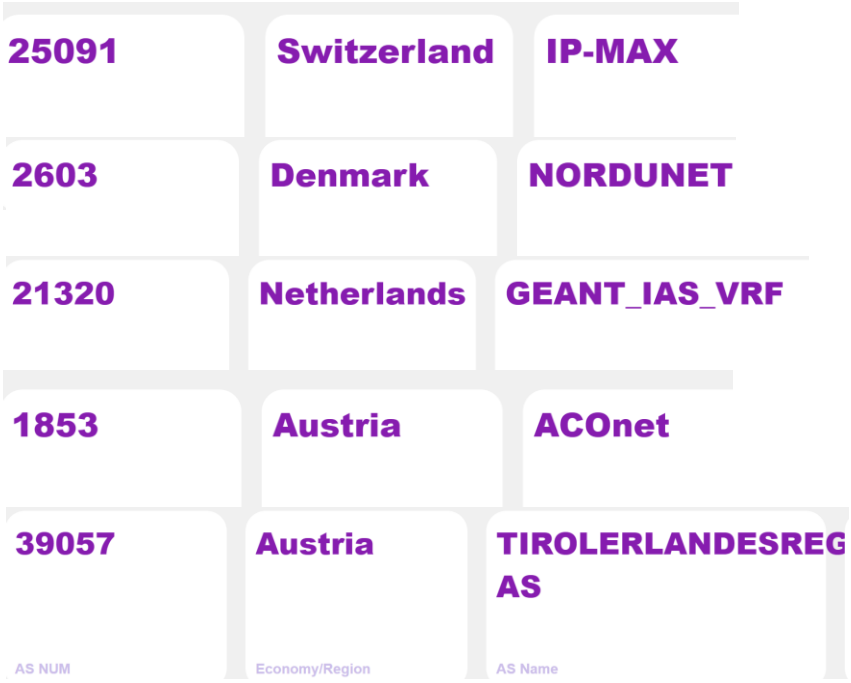
APNIC FOUNDATION

清華大學 Tsinghua University

Commercial ASes Transit Through R&E ASes



194.8.61.0/24 (2024-04-03)



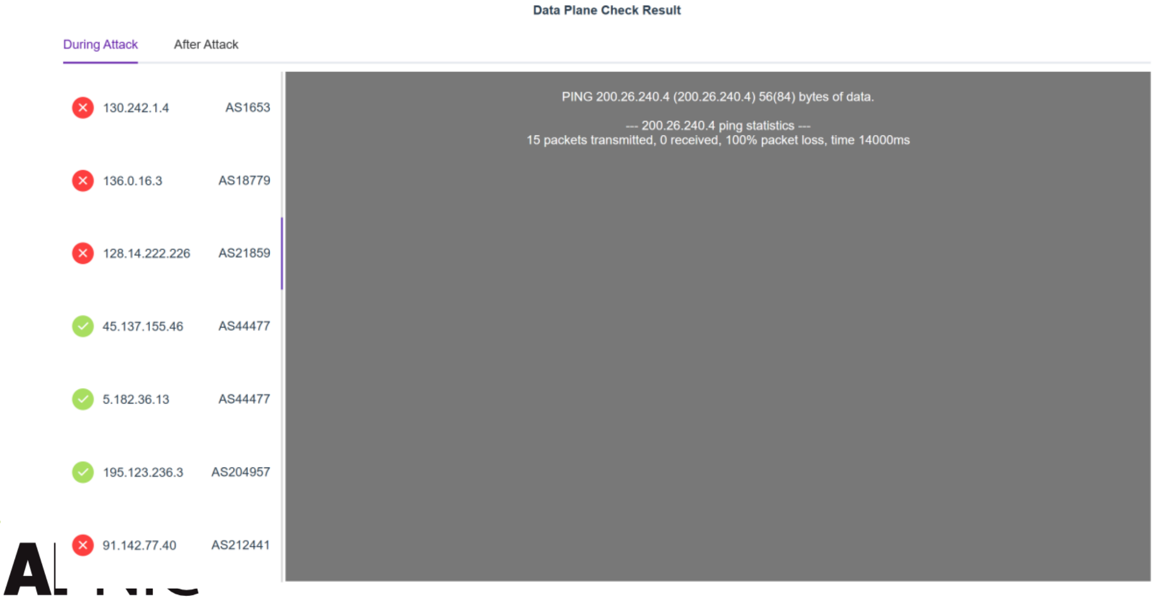
AS NUM	Economy/Region	AS Name
25091	Switzerland	IP-MAX
2603	Denmark	NORDUNET
21320	Netherlands	GEANT_IAS_VRF
1853	Austria	ACOnet
39057	Austria	TIROLERLANDESREG AS

AS25091, AS39057 are commercial ASes.
AS2603, AS21320, AS1853 are R&D Ases.

Hijack Detection through Data Plane Probing

Still Under Developing

1. Select anchor server for the prefix/subprefix
2. Select looking glass vantage point from affected ASes and unaffected ASes.
3. Check reachability during attack and after attack. Ping? Tracert?
4. Hijack? Traffic Engineering? Multihoming? IP address Renting?
5. Is it the same Server? TTL feature?



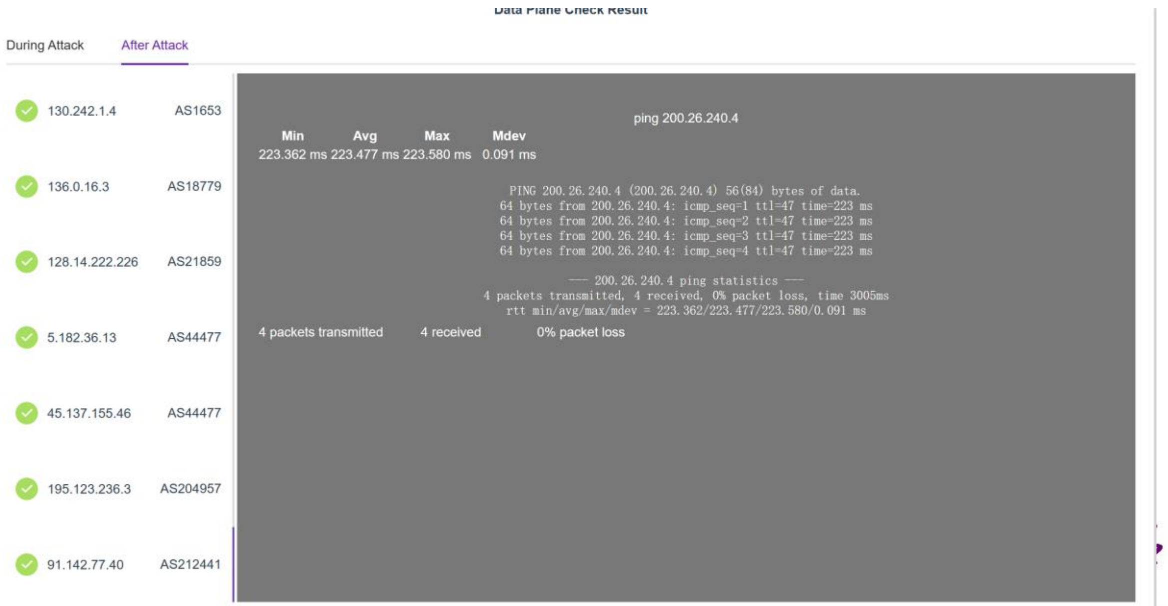
Data Plane Check Result

During Attack   After Attack

✗	130.242.1.4	AS1653
✗	136.0.16.3	AS18779
✗	128.14.222.226	AS21859
✓	45.137.155.46	AS44477
✓	5.182.36.13	AS44477
✓	195.123.236.3	AS204957
✗	91.142.77.40	AS212441

```
PING 200.26.240.4 (200.26.240.4) 56(84) bytes of data.

--- 200.26.240.4 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14000ms
```



Data Plane Check Result

During Attack   After Attack

✓	130.242.1.4	AS1653
✓	136.0.16.3	AS18779
✓	128.14.222.226	AS21859
✓	5.182.36.13	AS44477
✓	45.137.155.46	AS44477
✓	195.123.236.3	AS204957
✓	91.142.77.40	AS212441

ping 200.26.240.4

Min	Avg	Max	Mdev
223.362 ms	223.477 ms	223.580 ms	0.091 ms

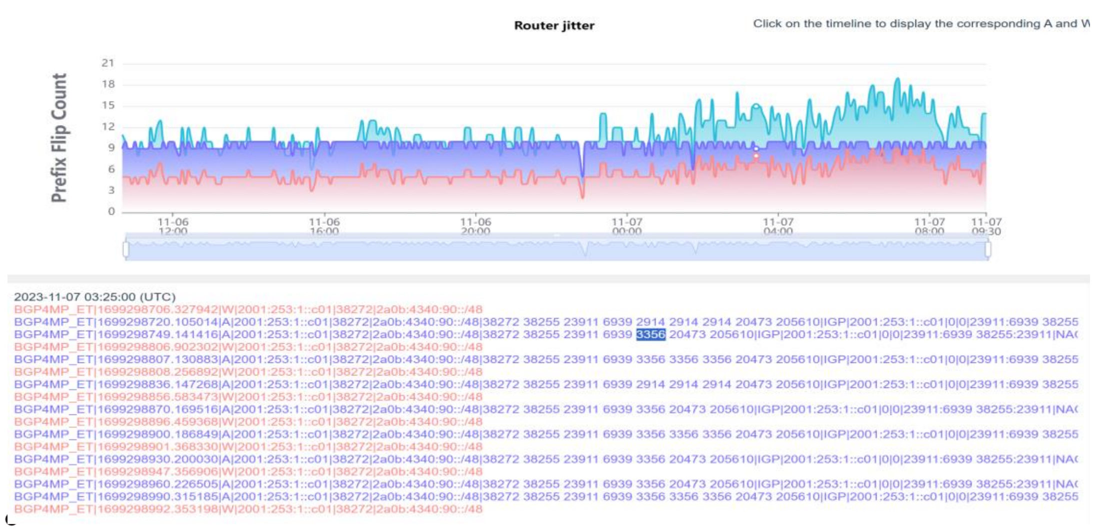
```
PING 200.26.240.4 (200.26.240.4) 56(84) bytes of data.
64 bytes from 200.26.240.4: icmp_seq=1 ttl=47 time=223 ms
64 bytes from 200.26.240.4: icmp_seq=2 ttl=47 time=223 ms
64 bytes from 200.26.240.4: icmp_seq=3 ttl=47 time=223 ms
64 bytes from 200.26.240.4: icmp_seq=4 ttl=47 time=223 ms

--- 200.26.240.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 223.362/223.477/223.580/0.091 ms
```

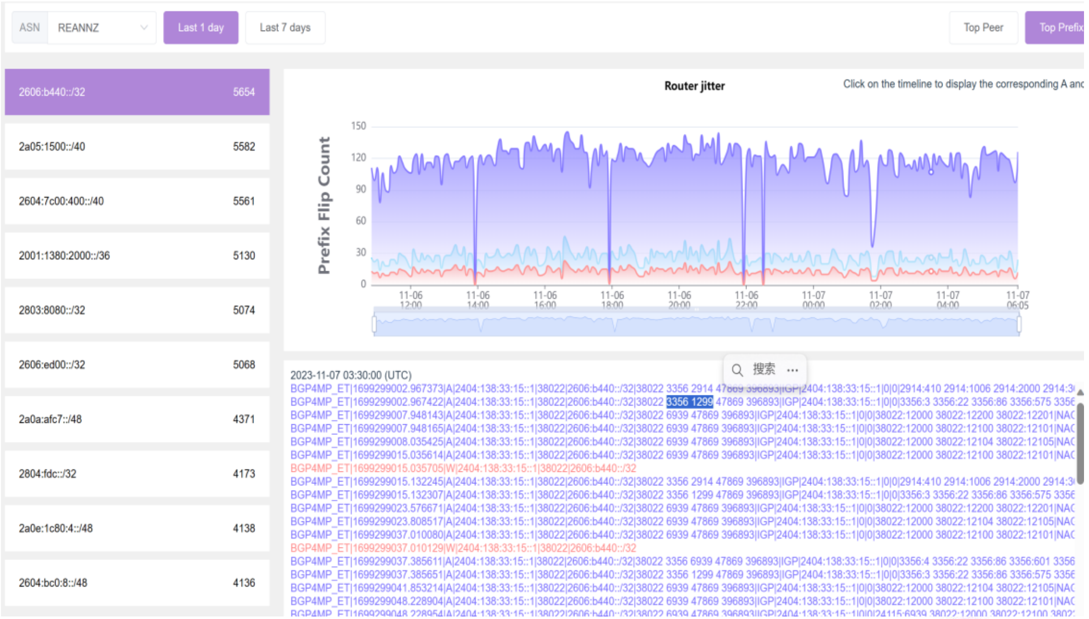
4 packets transmitted   4 received   0% packet loss

Router Jitter

- The advertisement and withdraw messages are received frequently.
- If this will harm internet performance?
- We may conduct some data plane testing in the future.



```
2023-11-07 03:25:00 (UTC)
BGP4MP_ET|1699298706.327942|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298720.105014|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 2914 2914 2914 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255
BGP4MP_ET|1699298749.141416|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255:23911|NA(
BGP4MP_ET|1699298806.902302|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298807.130883|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 3356 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255
BGP4MP_ET|1699298808.256892|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298836.147268|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 2914 2914 2914 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255
BGP4MP_ET|1699298856.583473|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298870.169516|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255:23911|NA(
BGP4MP_ET|1699298896.459368|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298900.186849|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 3356 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255
BGP4MP_ET|1699298901.368330|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298930.200030|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255:23911|NA(
BGP4MP_ET|1699298947.356906|W|2001:253:1::c01|38272|2a0b:4340:90::/48
BGP4MP_ET|1699298960.226505|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255:23911|NA(
BGP4MP_ET|1699298990.315185|A|2001:253:1::c01|38272|2a0b:4340:90::/48|38272 38255 23911 6939 3356 3356 3356 20473 205610|IGP|2001:253:1::c01|0|0|23911:6939 38255
BGP4MP_ET|1699298992.353198|W|2001:253:1::c01|38272|2a0b:4340:90::/48
```



2606:b440::/32	5654
2a05:1500::/40	5582
2604:7c00:400::/40	5561
2001:1380:2000::/36	5130
2803:8080::/32	5074
2606:ed00::/32	5068
2a0a:afc7::/48	4371
2804:fdc::/32	4173
2a0e:1c80:4::/48	4138
2604:bc0:8::/48	4136

```
2023-11-07 03:30:00 (UTC)
BGP4MP_ET|1699299002.967373|A|2404:138:33:15::1|38022|2606:b440::/32|38022 3356 2914 47869 396893|IGP|2404:138:33:15::1|0|0|2914:410 2914:1006 2914:2000 2914:3
BGP4MP_ET|1699299002.967422|A|2404:138:33:15::1|38022|2606:b440::/32|38022 3356 1299 47869 396893|IGP|2404:138:33:15::1|0|0|3356:3 3356:22 3356:86 3356:575 3356
BGP4MP_ET|1699299007.948143|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12200 38022:12201|NA(
BGP4MP_ET|1699299007.948165|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12100 38022:12101|NA(
BGP4MP_ET|1699299008.035425|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12104 38022:12105|NA(
BGP4MP_ET|1699299015.035614|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12100 38022:12101|NA(
BGP4MP_ET|1699299015.035705|W|2404:138:33:15::1|38022|2606:b440::/32
BGP4MP_ET|1699299015.132245|A|2404:138:33:15::1|38022|2606:b440::/32|38022 3356 2914 47869 396893|IGP|2404:138:33:15::1|0|0|2914:410 2914:1006 2914:2000 2914:3
BGP4MP_ET|1699299015.132307|A|2404:138:33:15::1|38022|2606:b440::/32|38022 3356 1299 47869 396893|IGP|2404:138:33:15::1|0|0|3356:3 3356:22 3356:86 3356:575 3356
BGP4MP_ET|1699299023.576671|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12200 38022:12201|NA(
BGP4MP_ET|1699299023.808517|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12104 38022:12105|NA(
BGP4MP_ET|1699299037.010080|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12100 38022:12101|NA(
BGP4MP_ET|1699299037.010129|W|2404:138:33:15::1|38022|2606:b440::/32
BGP4MP_ET|1699299037.385611|A|2404:138:33:15::1|38022|2606:b440::/32|38022 3356 6939 47869 396893|IGP|2404:138:33:15::1|0|0|3356:4 3356:22 3356:86 3356:601 3356
BGP4MP_ET|1699299037.385651|A|2404:138:33:15::1|38022|2606:b440::/32|38022 3356 1299 47869 396893|IGP|2404:138:33:15::1|0|0|3356:3 3356:22 3356:86 3356:575 3356
BGP4MP_ET|1699299041.853214|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12104 38022:12105|NA(
BGP4MP_ET|1699299048.228904|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|38022:12000 38022:12100 38022:12101|NA(
BGP4MP_ET|1699299048.228954|A|2404:138:33:15::1|38022|2606:b440::/32|38022 6939 47869 396893|IGP|2404:138:33:15::1|0|0|24115:6939 38022:12000 38022:12100 3802
```

APNIC FOUNDATION

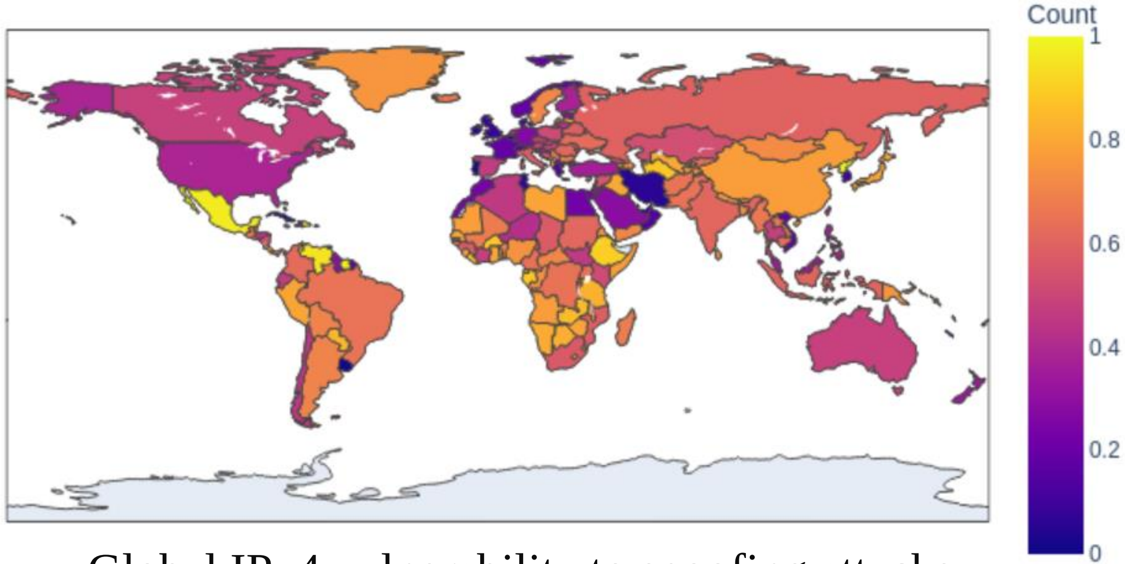
Tsinghua University

Future Work Plan

Objectives	Work Plan	Tentative Timeline
Develop an integrated Looking Glass platform	Find obscure Looking Glass VP regularly	Dec. 2023 Done
	Develop integrated Looking Glass platform	Feb. 2024 Done
	Develop Looking Glass API	Mar. 2024 Done
Use Looking Glass to further check routing hijacking at the data plan	Develop data plan detection method and decision algorithm	June 2024 Ongoing
	Integrate the algorithm to the system	Aug. 2024
Implement path hijacking detection and routing leak detection methods	Develop path hijacking detection method	Nov. 2024
	Develop routing leak detection method	Jan. 2025
Continue to maintain and fix bugs in the BGPWatch platform	Continually test and get suggestions from user	Throughout the entire project duration
Continue community development and engagement, and international collaboration	The second phase of the project (**Dec.06, 2023 – June 06, 2025 (18 months)**) **Welcome new partners to join!**	Throughout the entire project duration

Source Address Validation

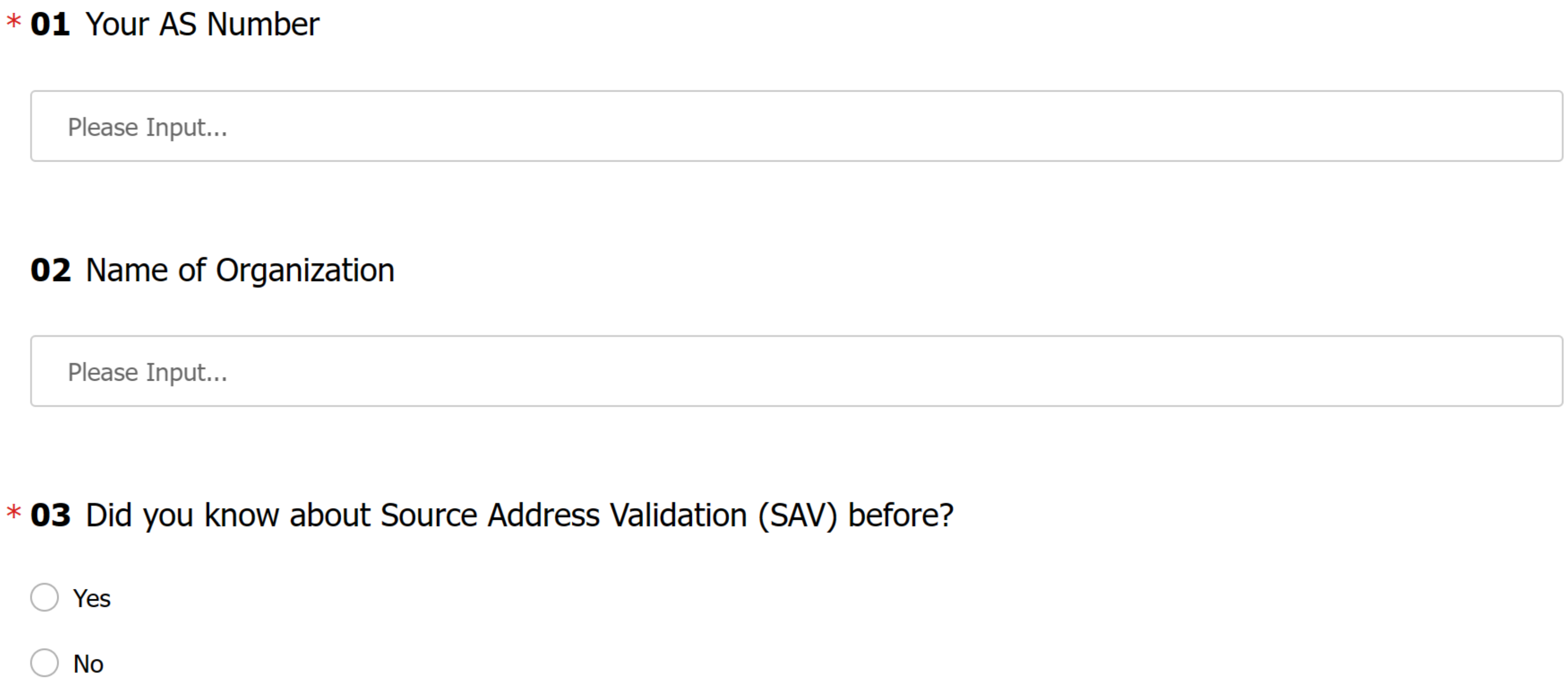
- Source address validation (SAV) is one important way to mitigate source address spoofing attacks in the data plane.
  - As defined in MANRS Action 2: Prevent traffic with spoofed source IP addresses – Filtering:
  - A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.
  - We are conducting large-scale SAV deployment probing.



Global IPv4 vulnerability to spoofing attacks
(darker colors are more secure)

SAV Deployment Survey

- Survey Link: https://www.survio.com/survey/d/E4V1T2S9X9W6N0X5I



* **01** Your AS Number

Please Input...

02 Name of Organization

Please Input...

* **03** Did you know about Source Address Validation (SAV) before?

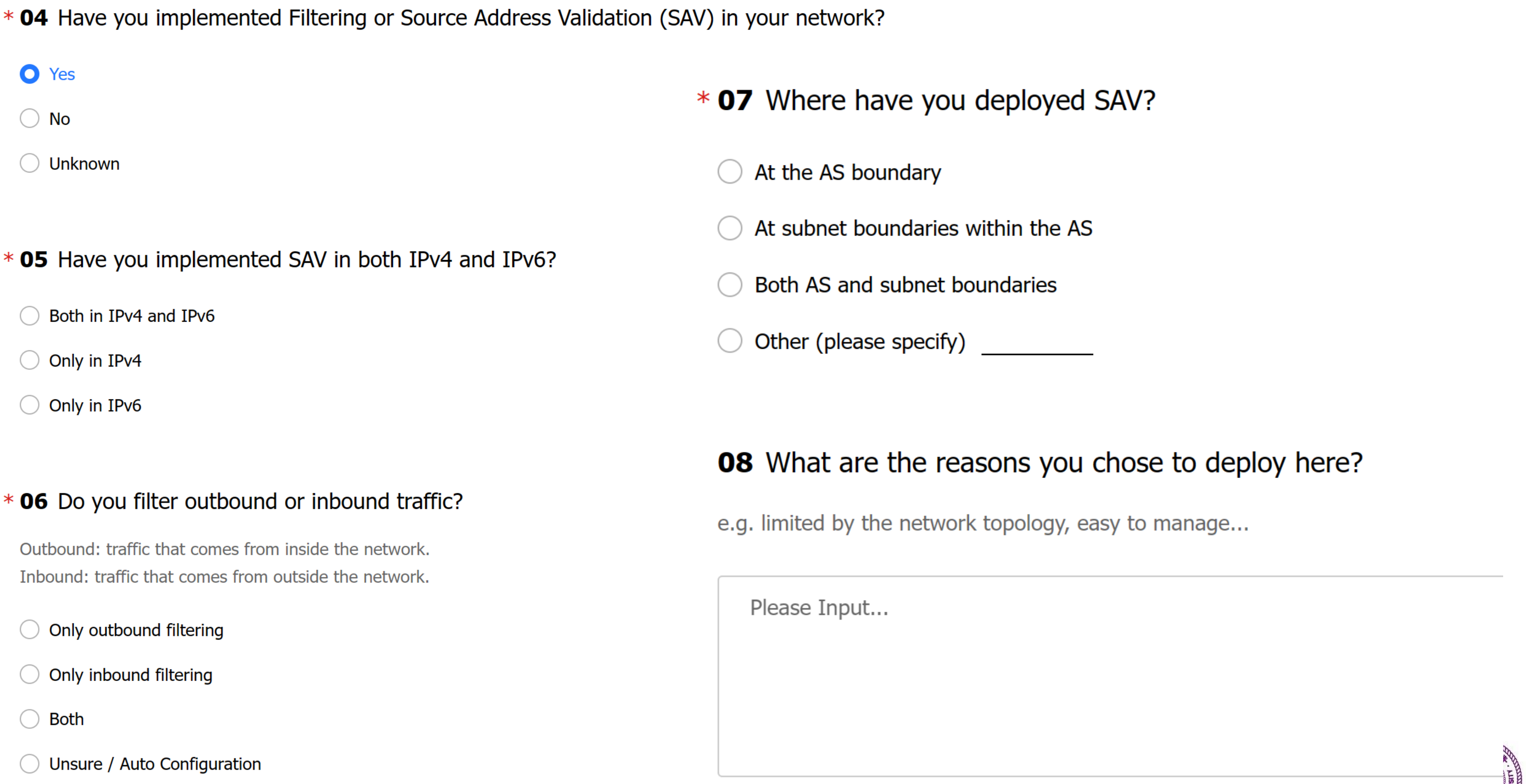
○ Yes

○ No

APNIC FOUNDATION

清華大學 Tsinghua University

SAV Deployment Survey



* **04** Have you implemented Filtering or Source Address Validation (SAV) in your network?

● Yes

○ No

○ Unknown

* **05** Have you implemented SAV in both IPv4 and IPv6?

○ Both in IPv4 and IPv6

○ Only in IPv4

○ Only in IPv6

* **06** Do you filter outbound or inbound traffic?

Outbound: traffic that comes from inside the network.
Inbound: traffic that comes from outside the network.

○ Only outbound filtering

○ Only inbound filtering

○ Both

○ Unsure / Auto Configuration

* **07** Where have you deployed SAV?

○ At the AS boundary

○ At subnet boundaries within the AS

○ Both AS and subnet boundaries

○ Other (please specify) __________

08 What are the reasons you chose to deploy here?

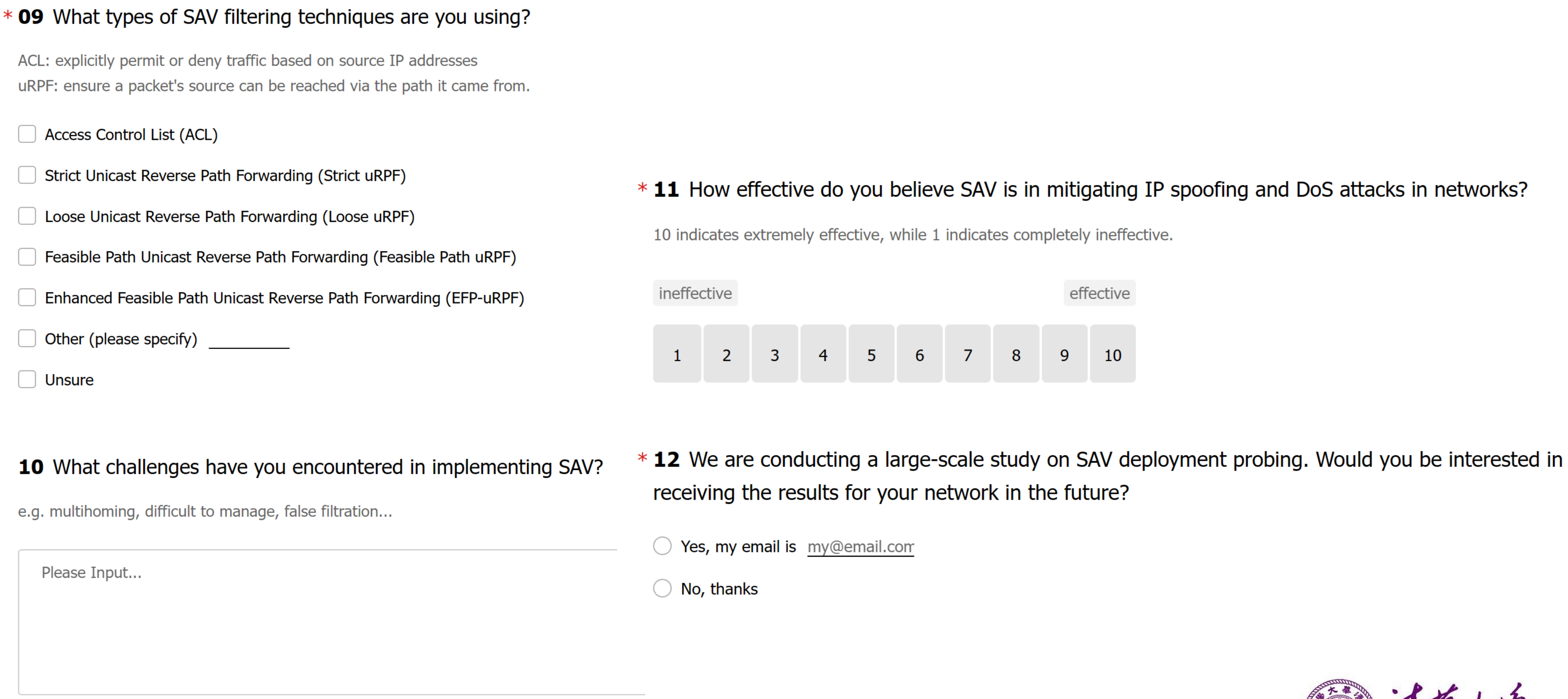
e.g. limited by the network topology, easy to manage...

Please Input...

APNIC FOUNDATION

清華大學 Tsinghua University

SAV Deployment Survey



* **09** What types of SAV filtering techniques are you using?

ACL: explicitly permit or deny traffic based on source IP addresses
uRPF: ensure a packet's source can be reached via the path it came from.

- □ Access Control List (ACL)
- □ Strict Unicast Reverse Path Forwarding (Strict uRPF)
- □ Loose Unicast Reverse Path Forwarding (Loose uRPF)
- □ Feasible Path Unicast Reverse Path Forwarding (Feasible Path uRPF)
- □ Enhanced Feasible Path Unicast Reverse Path Forwarding (EFP-uRPF)
- □ Other (please specify) __________
- □ Unsure

10 What challenges have you encountered in implementing SAV?

e.g. multihoming, difficult to manage, false filtration...

Please Input...

* **11** How effective do you believe SAV is in mitigating IP spoofing and DoS attacks in networks?

10 indicates extremely effective, while 1 indicates completely ineffective.

ineffective effective

1 2 3 4 5 6 7 8 9 10

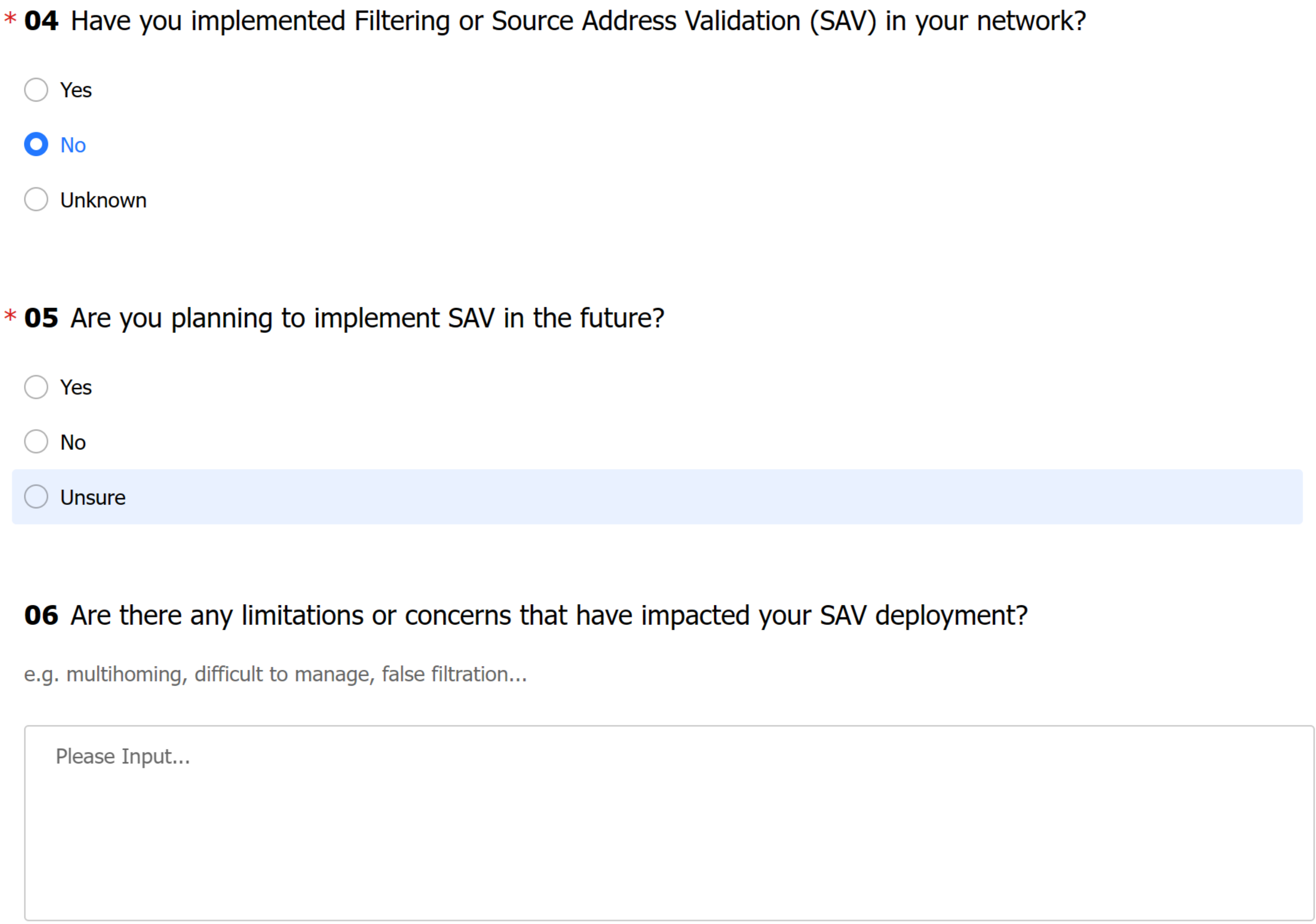
* **12** We are conducting a large-scale study on SAV deployment probing. Would you be interested in receiving the results for your network in the future?

- ○ Yes, my email is my@email.com
- ○ No, thanks

APNIC FOUNDATION

清華大學 Tsinghua University

SAV Deployment Survey



* **04** Have you implemented Filtering or Source Address Validation (SAV) in your network?

○ Yes

● No

○ Unknown

* **05** Are you planning to implement SAV in the future?

○ Yes

○ No

○ Unsure

06 Are there any limitations or concerns that have impacted your SAV deployment?

e.g. multihoming, difficult to manage, false filtration...

Please Input...

Comments and Suggestions?

Contact us at:

sec@cgtf.net

APNIC FOUNDATION

清華大學 Tsinghua University