

Joint Research on IPv4/IPv6 Network Management: Research Development and Demonstration



AfgREN



BdREN



CamREN



LEARN



Mae Fah Luang University



MYREN



NREN



PERN



SingAREN



TEIN'CC



ThaiREN



University of Computer Studies,
Yangon



University of Gottingen



University of Malaya



University of Surrey



Tsinghua University



Beijing University of Posts and
Telecommunications



The Institute of Information
Engineering, CAS



Bitway



The Department of Computing
(COMP), the Hong Kong
Polytechnic University



UESTC



E-Hualu



Shandong University

May 23, 2023

Content

- **Project Outline**
- **Work Progress Report**
- **Future Work**

Project Web Site:
<https://cgtf.net>

International Cooperation

14 countries, 23 research organizations

Excellent Mix of Key Experiences of IPv4/IPv6 Network Management

13 research organizations from

11 Asian countries

TEIN*CC

SingAREN, Singapore

ThaiRen, Thailand

MYREN, Malaysia

LEARN, Sri Lanka

NREN, Nepal

PERN, Pakistan

BdREN, Bengal

CamREN, Cambodia

AfgREN, Afghanistan

University of Computer Studies, Yangon,

Myanmar

University of Malaya , Malaysia

Mae Fah Luang University, Thailand



**2 research organizations from
European countries**

University of Gottingen, Germany

University of Surrey, UK

**8 Chinese research
organizations**

Tsinghua University

BUPT

CAS

Bit-Way

Shenzhen Research Institute, HKPU

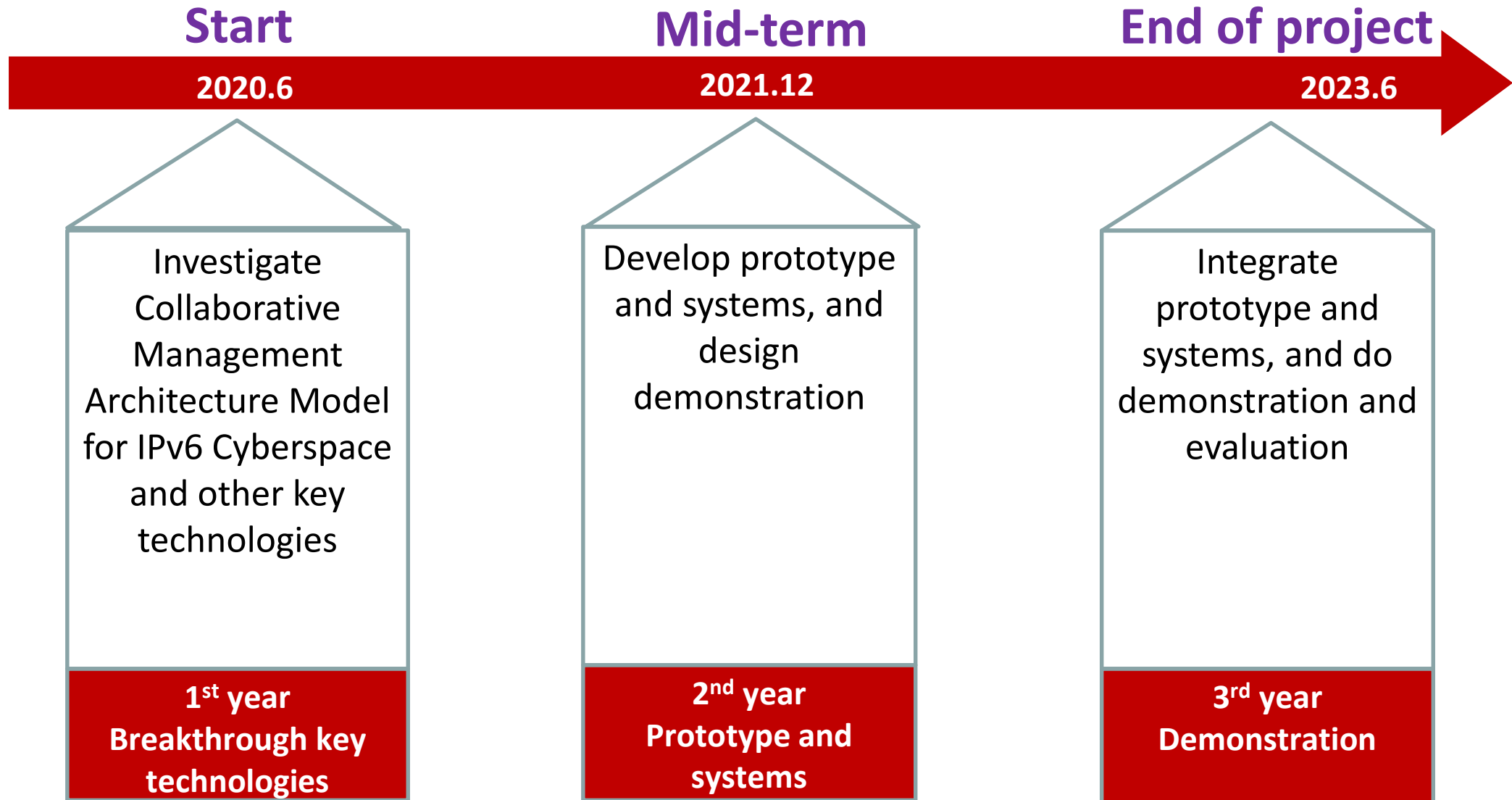
UESTC

Shandong University

eHualu

**Promote Network Technology Innovation and
Application Demonstration**

Project Plan & Schedule



Working Group

WG's Organization	Passive Traffic Measurement	Active Probe	Network Looking Glass	BGP Routing Info Sharing/Monitoring	Network Telescope	International Rules of Cyber Governance(IRCG)
SingAREN		√	√	√		√
ThaiRen	√	√	√	√	√	√
LEARN	√	√	√	√	√	√
BDREN	√	√	√	√	√	√
MYREN		√	√	√		√
AfgREN			√	√	√	√
NREN						√
CAMREN						√
PERN						√
Yangon University of Computer Study						√
University of Malaya						√
Mae Fah Luang University,Thailand						√
University of Gottingen	√					√
Surrey University	√			√		√

Work Progress

Project Web Site:
<https://cgtf.net>

- **Progress In the Following Aspect:**

- Active Probe Platform—GPerf
- Passive Traffic Measurement—FlowWatch
- Network Looking Glass—CGTF LG
- BGP Routing Sharing —CGTF RIS
- BGP Routing Monitoring and Analysis — BGPWatch

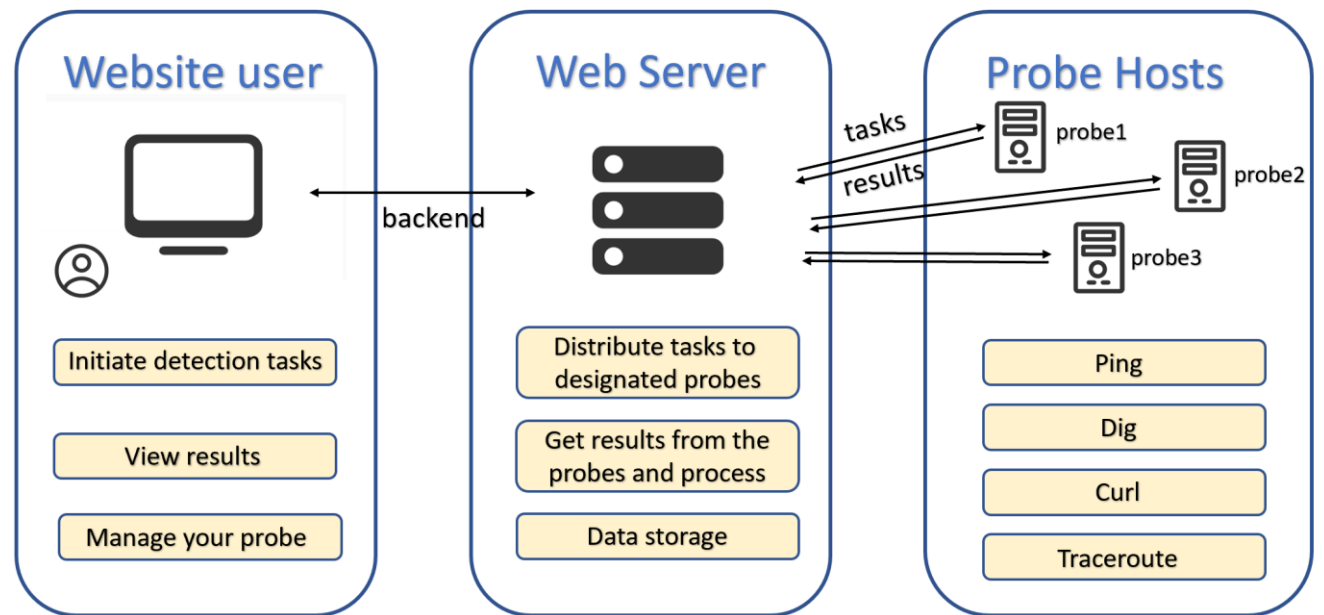
What is GPerf ?

- An active Internet measurement platform
 - Mechanism: Initiate detections through several deployed probes
 - Target: Domain names on the Internet
 - Purpose: Obtain and visualize periodic results

- Functions provided

- a) *ping*
- b) *dig*
- c) *curl*
- d) *traceroute*

- Supports both **IPv4** and **IPv6**



Available Probe list

Probe

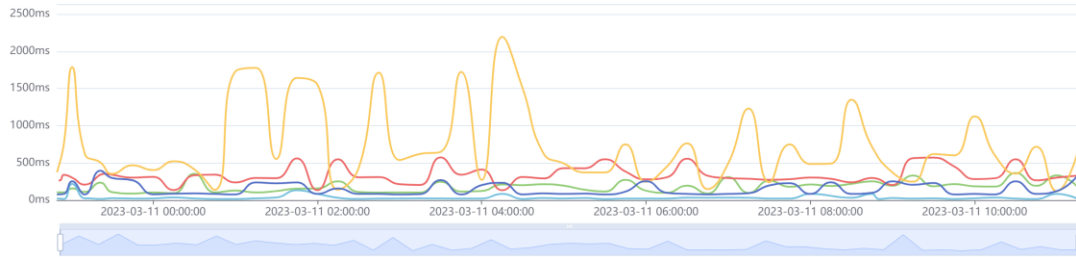
Probe:18 From 14 Country, 17 City

	Status	Probe name	IPv4 Address	IPv6 Address	Country	City	Total Task	Option
1		LEARN-Probe	192.248.3.218	2401:dd00:1:1:5054:ff:fe32:e3b2	Srilanka	Colombo	12	
2		ThaiREN	202.28.194.7	N/A	Thailand	Bangkok	4	
3		Tsinghua1	203.91.121.239	2001:da8:217:1213::239	China	Beijing	0	
4		SingAREN-SOE-1	203.30.39.26	2001:df0:21a:0:20c:29ff:fe56:5098	Singapore	Singapore	8	
5		TS-BJ-ali	101.200.124.121	2408:400a:69:cd00:3061:7f23:24a4:85f3	China	Bejing	404	
6		BdREN	103.157.134.4	N/A	Bangladesh	Dhaka	32	
7		TS-JP-ali	8.209.254.12	N/A	Japan	Japan	144	
8		TS-SG-ali	8.222.162.223	240b:4000:b:db00:8106:7413:738f:f1ee	Singapore	Singapore	708	
9		TS-GB-ali	8.208.87.165	N/A	United Kingdom	london	284	
10		TS-US-ali	47.251.15.44	N/A	United States	silicon valley	140	

Result Details

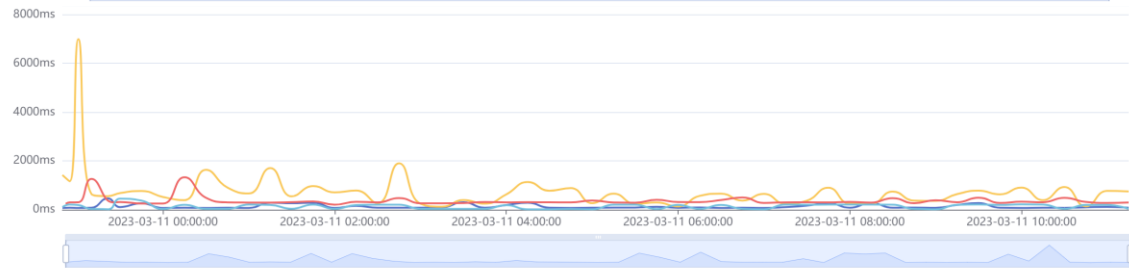
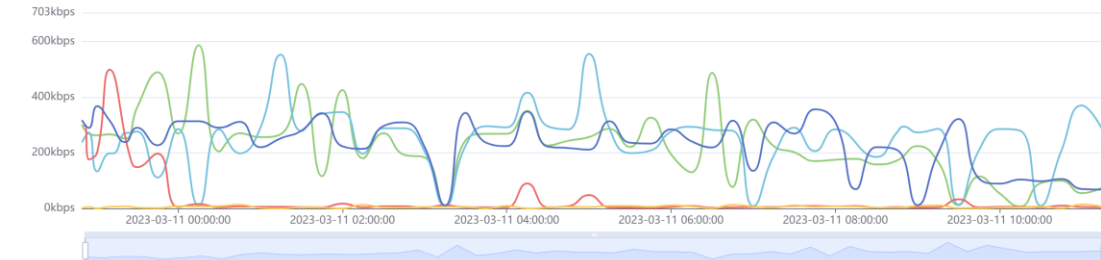
v4-curl-Connect

● BdREN ● MYREN ● TS-SG-ali ● TS-BJ-ali ● LEARN-Probe



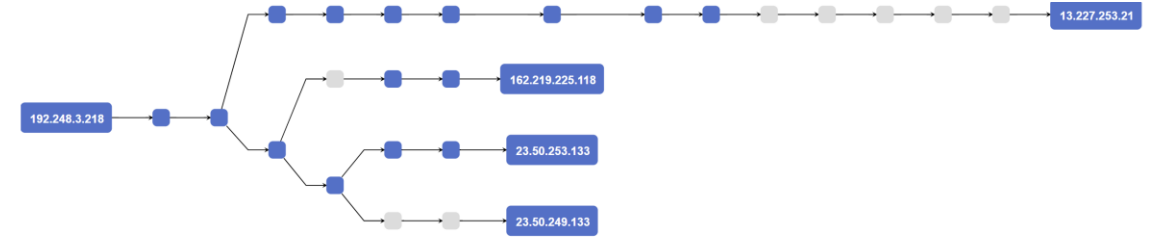
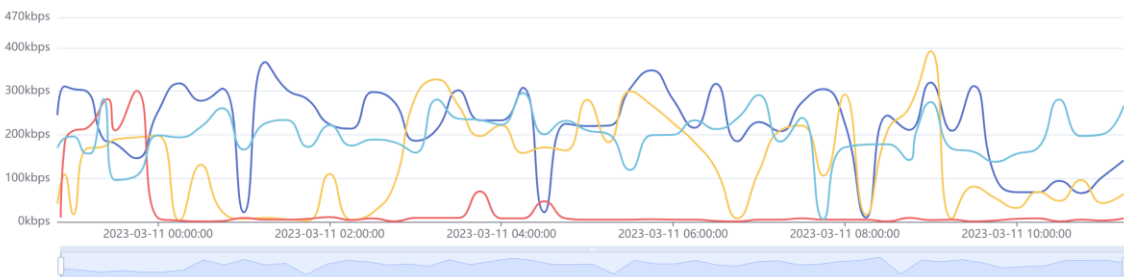
v4-curl-Download

● BdREN ● MYREN ● TS-SG-ali ● TS-BJ-ali ● LEARN-Probe

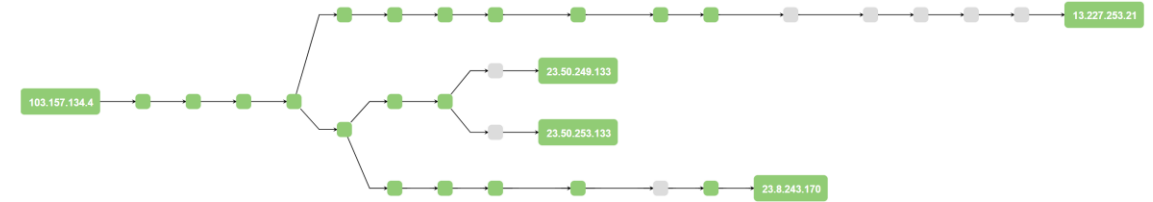


v6-curl-Download

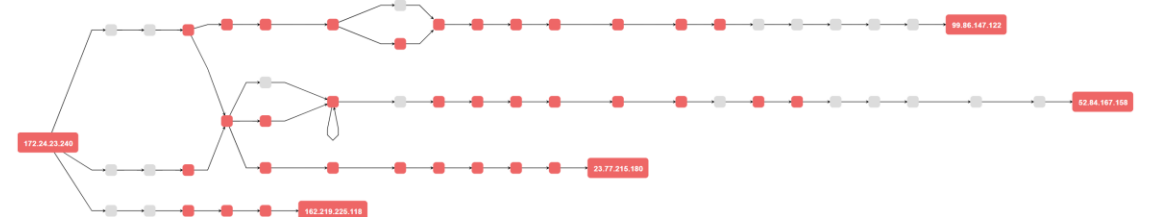
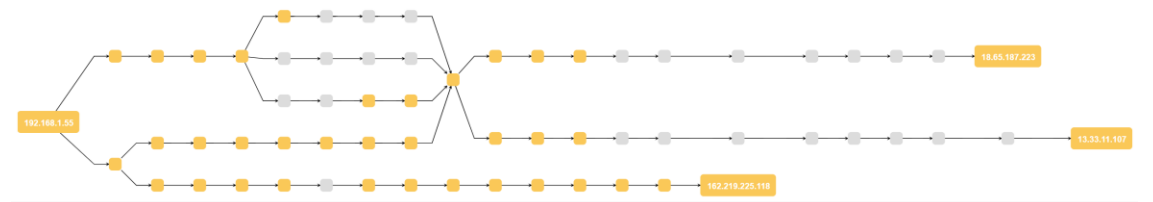
● LEARN-Probe ● TS-BJ-ali ● TS-SG-ali ● MYREN



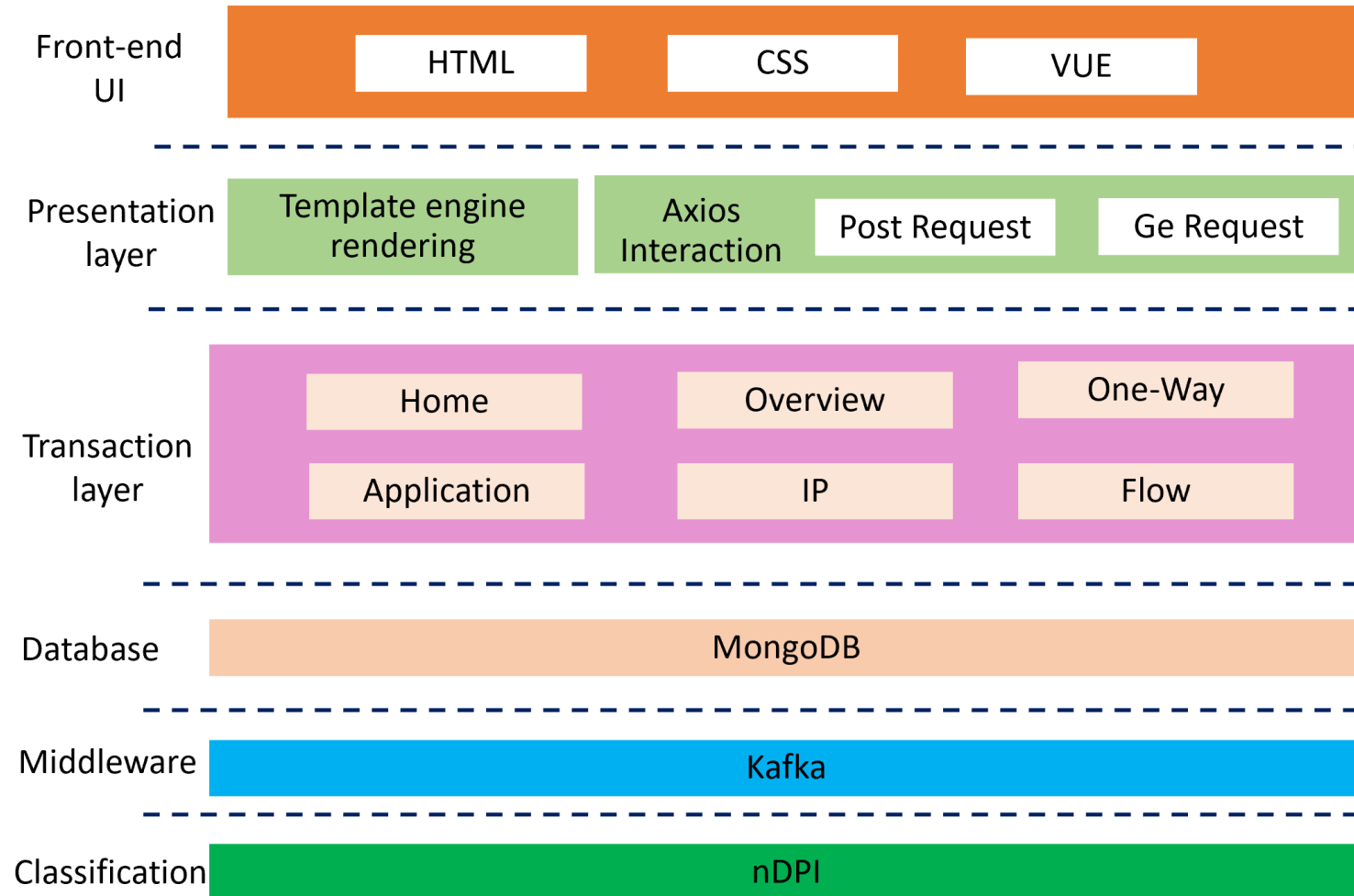
Route Path-BdREN



Route Path-TS-SG-ali



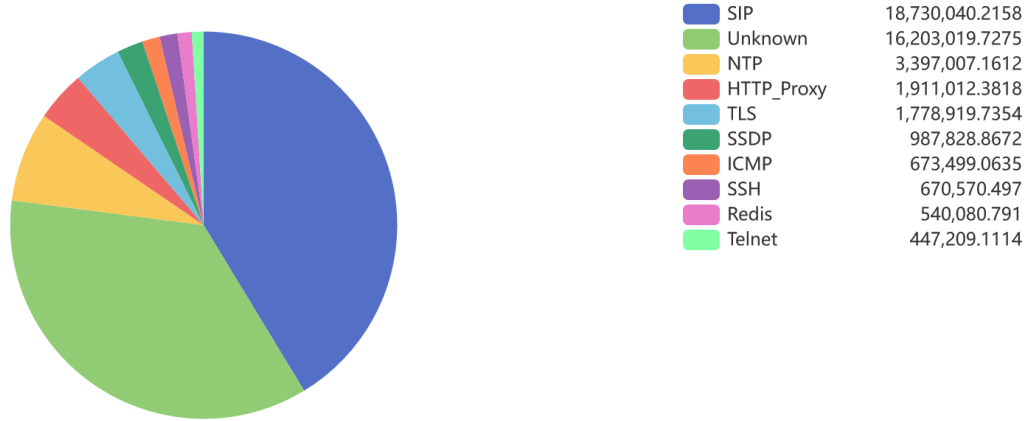
Traffic Measurement System



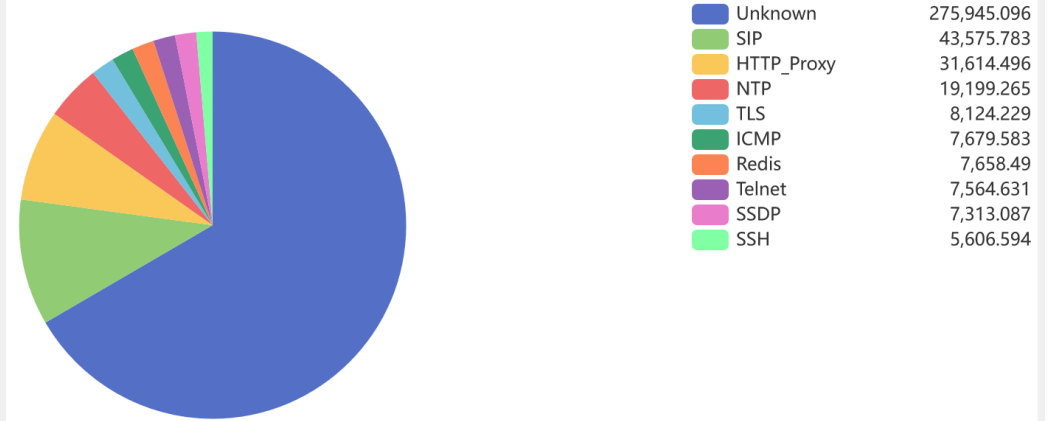
- Input: rawpacket or netflow traffic
- Classify traffic into application by nDPI
- Distribution data by Kafka to deal with high traffic
- Aggregate and do statistics on the data
- MongoDB can be clustered to deal with high traffic

TOP 10 APP

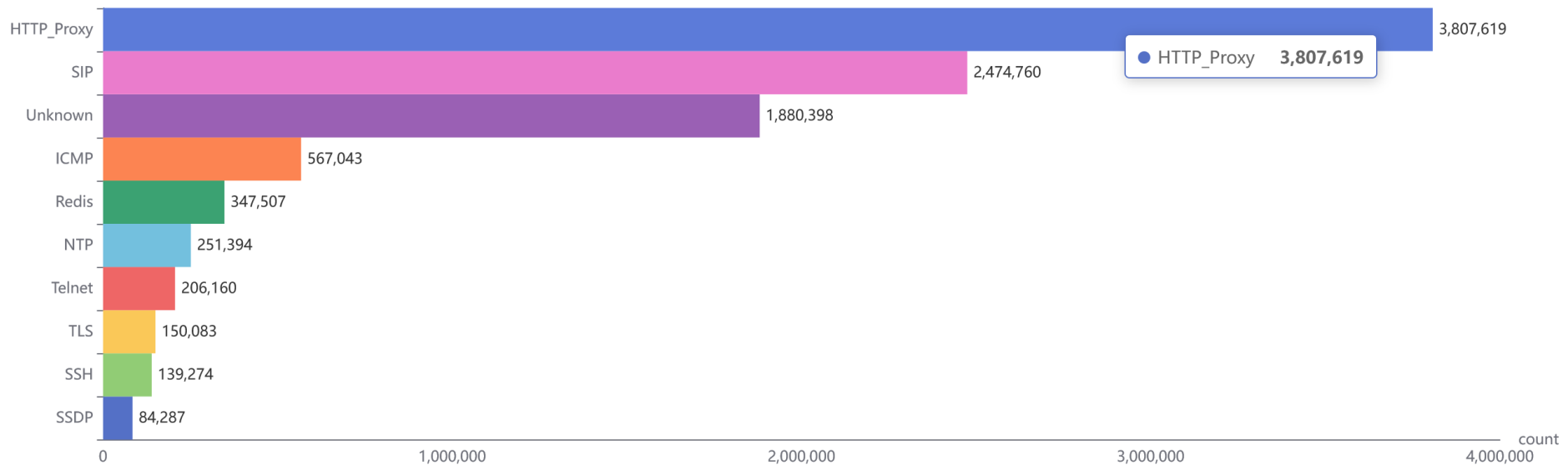
APP TOP 10 By Bytes



APP TOP 10 By Packets



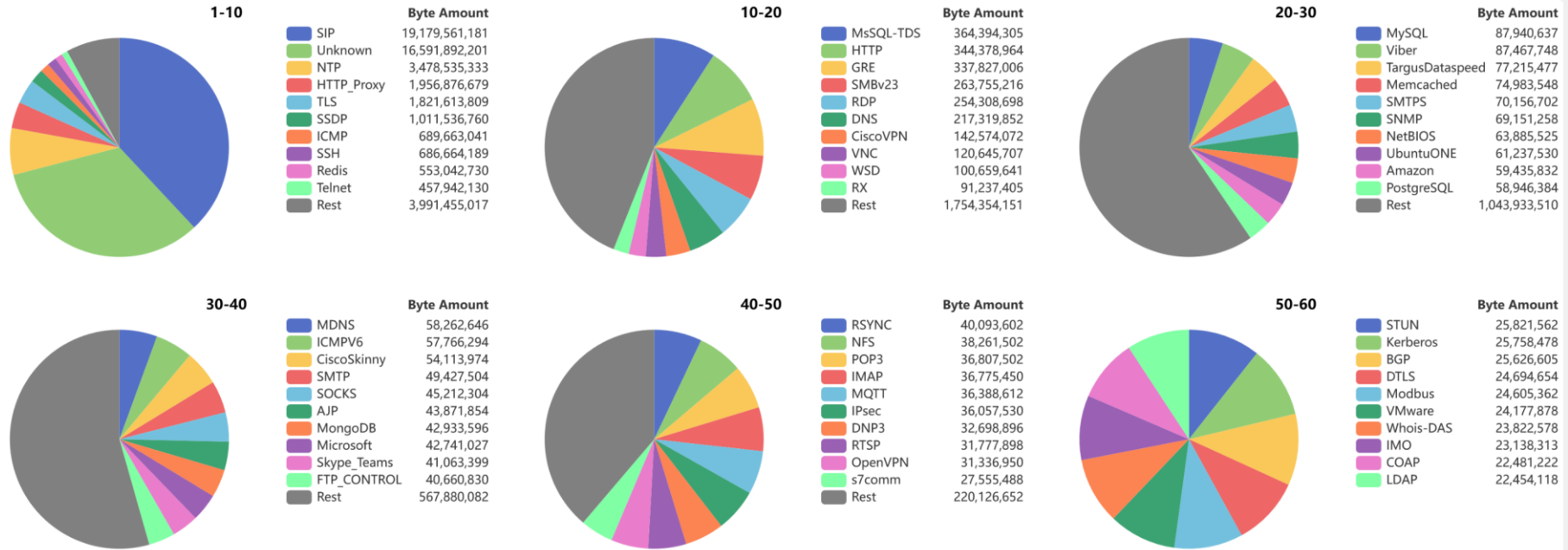
APP TOP 10 By Flow Amount



Statistics of Each APP

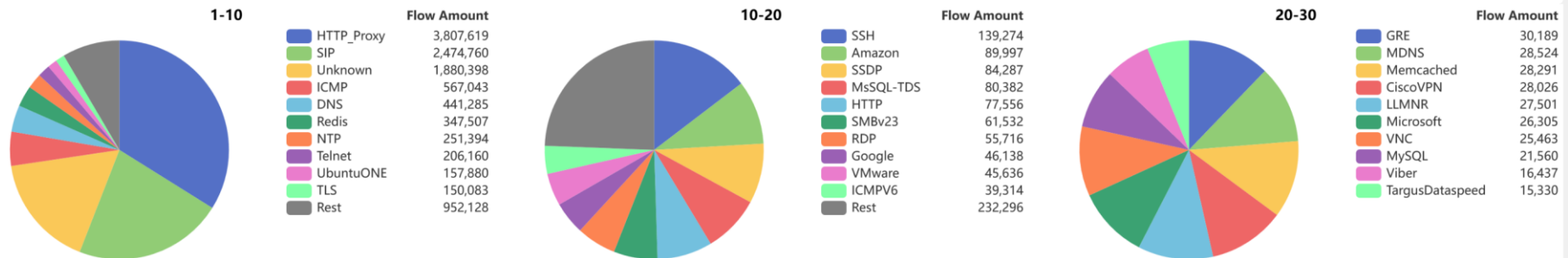
APP Statistics by Byte Amount

Top 60



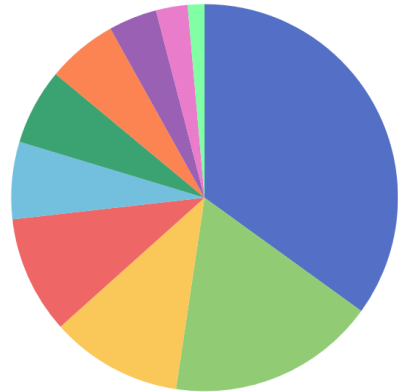
APP Statistics by Flow Amount

Top 30



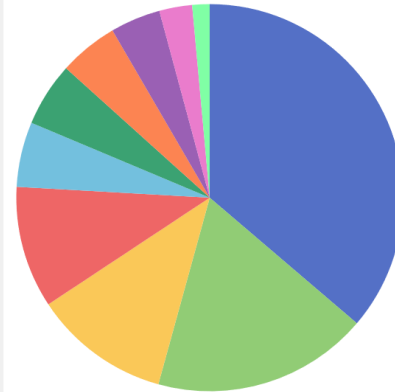
TOP 10 IP

IP TOP 10 By Bytes



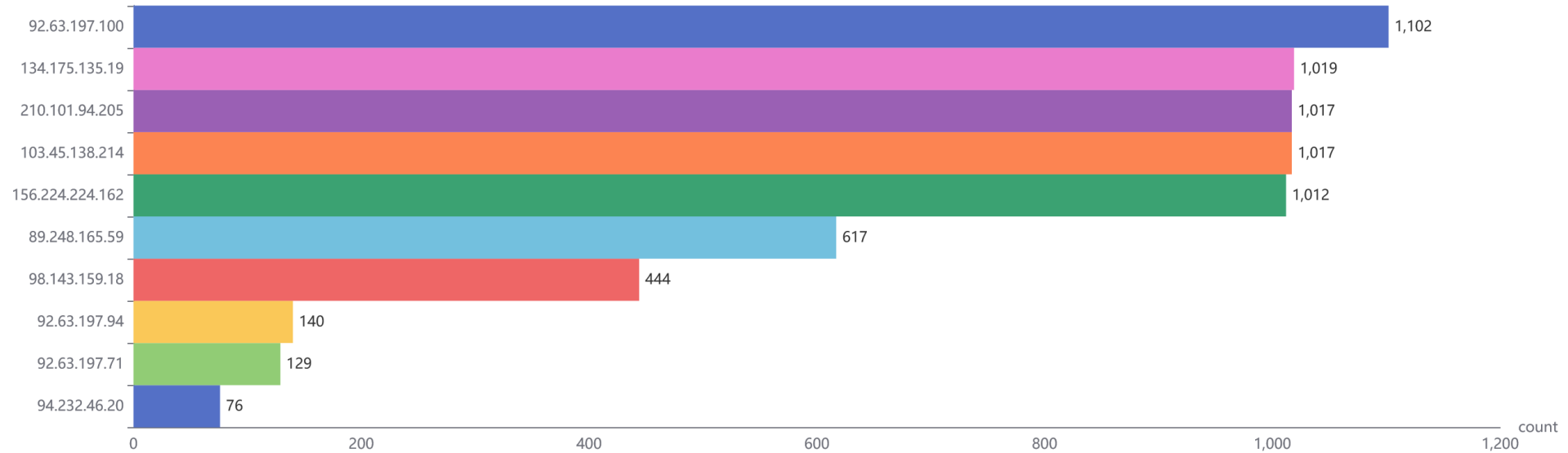
IP Address	K Bytes
92.63.197.100	8,276.4473
89.248.165.59	4,121.3613
103.45.138.214	2,610.1133
98.143.159.18	2,326.7012
156.224.224.162	1,528.6289
134.175.135.19	1,503.2617
210.101.94.205	1,394.6172
92.63.197.71	956.8828
94.232.46.20	627.4355
92.63.197.94	331.7676

IP TOP 10 By Packets

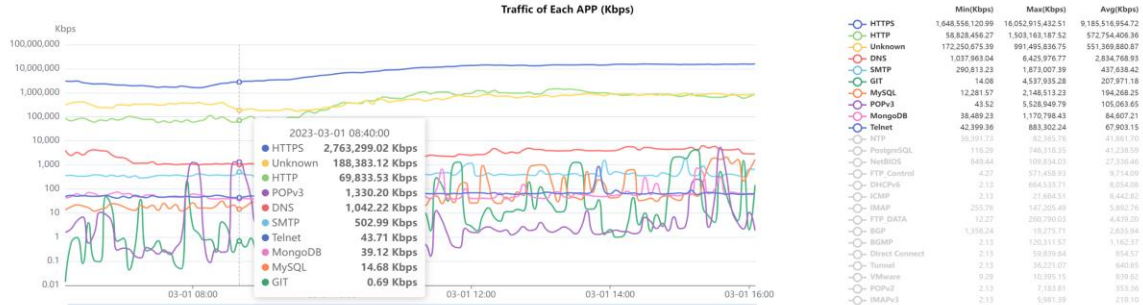


IP Address	K Packets
92.63.197.100	141.239
89.248.165.59	70.326
103.45.138.214	44.538
98.143.159.18	39.706
156.224.224.162	21.149
134.175.135.19	20.804
210.101.94.205	19.294
92.63.197.71	16.328
94.232.46.20	10.708
92.63.197.94	5.661

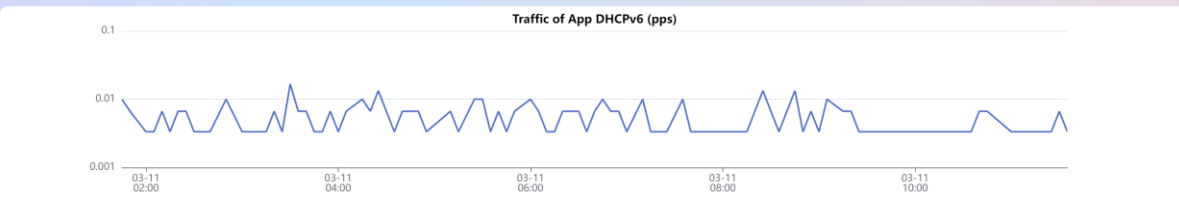
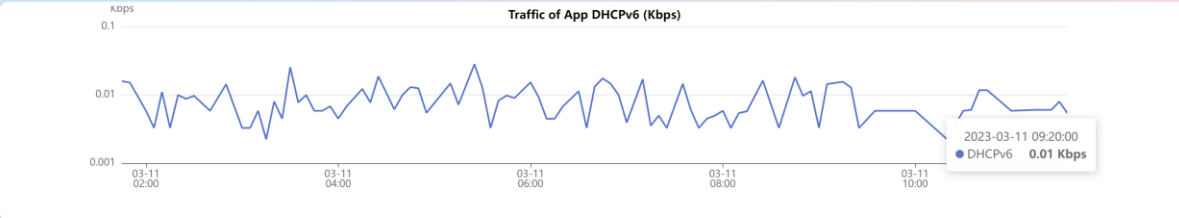
IP TOP 10 By Flow Amount



Detail of Application



GMT+8 | 2023-03-11 11:43:01 | Last 10 Hours | DHCPv6



Client IP	Flow Amount	Packet	Byte	Client to Server Packets	Client to Server Bytes	Server to Client Packets	Server to Client Bytes
2001:250:1e03:12::1	29	32	7,196	0	0	32	7,196
2001:da8:5000:440b::4321	34	36	5,052	1	136	35	4,916

App Name	Flow Amount	Packet	Byte	Client to Server Packets	Client to Server Bytes	Server to Client Packets	Server to Client Bytes
Unknown	79,671,262	404,375,915	325,154,832,723	150,388,395	146,071,958,770	253,987,520	179,082,873,953
HTTPS	46,734,483	341,152,151	323,457,986,096	131,683,047	138,337,456,479	209,469,104	185,120,529,617
HTTP	9,593,061	56,535,016	49,636,307,557	21,585,427	19,033,288,587	34,949,589	30,603,018,970
DNS	11,761,847	11,939,761	2,127,762,173	95,220	24,595,298	11,844,541	2,103,166,875
NTP	671,172	677,719	74,441,822	2,334	258,044	675,385	74,183,778
SMTP	10,108	37,327	29,738,475	13,928	14,573,013	23,399	15,165,462
IMAP	10,342	37,757	12,405,665	13,766	6,616,229	23,991	5,789,436
GIT	474	5,726	4,809,469	2,595	2,387,729	3,131	2,421,740
POPv3	1,378	5,306	3,858,950	2,208	2,827,843	3,098	1,031,107
MySQL	7,289	10,817	2,775,345	459	92,747	10,358	2,682,598
Telnet	5,952	11,654	1,970,722	1,129	219,182	10,525	1,751,540
BGP	2,897	5,498	1,258,347	961	409,303	4,537	849,044
PostgreSQL	2,532	4,346	654,021	119	46,935	4,227	607,086

Client IP	Flow Amount	Packet	Byte	Client to Server Packets	Client to Server Bytes	Server to Client Packets	Server to Client Bytes
2001:1900:2380:a07::1fe	6	10,791	11,449,329	3,574	334,278	7,217	11,115,051
2001:1900:2380:d03::1fe	12	4,732	4,734,608	1,691	161,345	3,041	4,573,263
2001:1900:2306:8f05::1fe	2	4,128	4,313,775	1,461	119,472	2,667	4,194,303
2001:1900:2380:e03::1fe	10	3,416	3,424,087	1,149	108,597	2,267	3,315,490
2001:1900:2380:e00::1fe	1	3,465	3,085,214	1,525	149,202	1,940	2,936,012
2001:1900:2306:4f0b::1fe	2	2,720	2,802,674	912	76,378	1,808	2,726,296
2001:1900:2306:8f09::1fe	1	1,481	1,619,116	478	46,252	1,003	1,572,864
2001:1900:2306:302d::1fe	3	1,380	1,354,882	478	44,978	902	1,309,904
2001:1900:230f:e00::1fe	1	1,234	1,296,958	403	38,667	831	1,258,291
2001:1900:2306:8f0b::1fe	2	370	339,645	144	11,881	226	327,764

Detail of IP

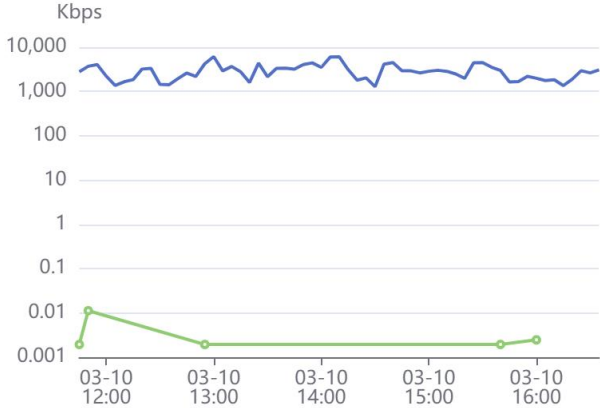
AS Server

Flow Per Second of IP 2620:1ec:8fa::8



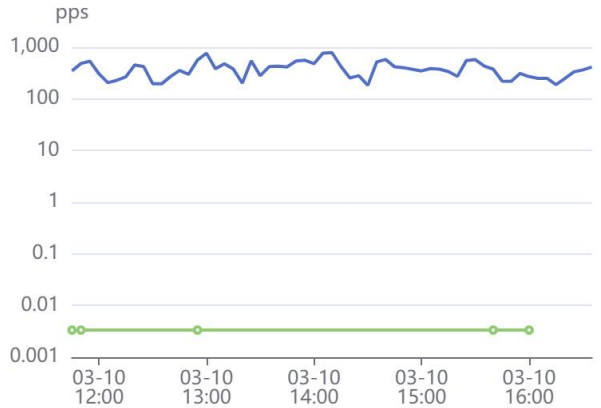
	Min	Max	Avg
— HTTPS	903	1,760	1,344
— HTTP	1	1	1

Traffic of IP 2620:1ec:8fa::8 (Kbps)



	Min(Kbps)	Max(Kbps)	Avg(Kbps)
— HTTPS	1,314.19	6,278.56	2,995.51
— HTTP	0.00	0.01	0.00

Traffic of IP 2620:1ec:8fa::8 (pps)



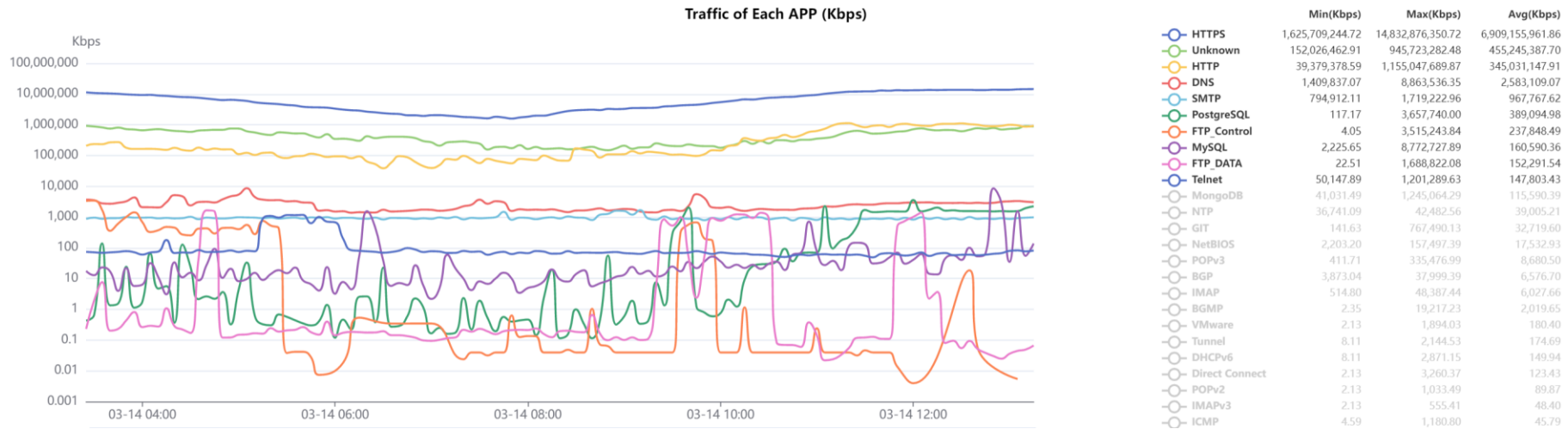
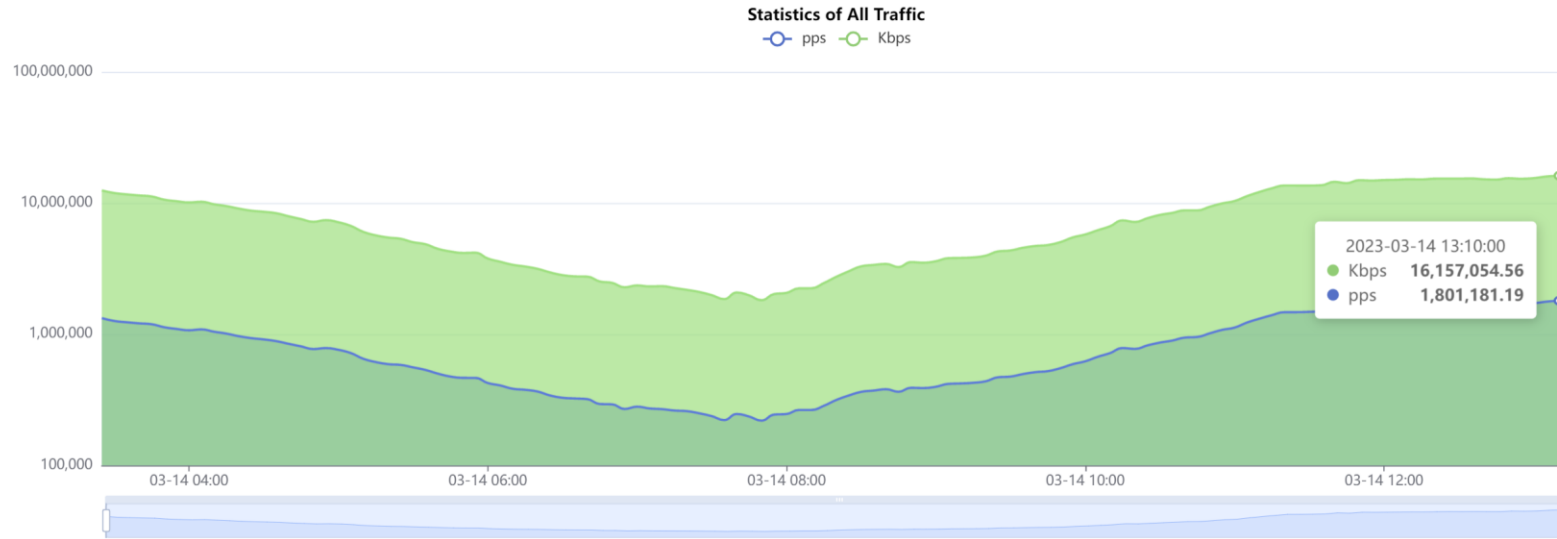
	Min(pps)	Max(pps)	Avg(pps)
— HTTPS	182.87	785.64	384.65
— HTTP	0.00	0.00	0.00

	IP	App	Flow Amount	Packet	Byte	Client to Server	Client to Server	Server to Client	Server to Client
						Packets	Bytes	Packets	Bytes
1	2620:1ec:8fa::8	HTTPS	79,300	6,808,309	6,627,571,694	3,167,658	1,539,588,423	3,640,651	5,087,983,271
2	2620:1ec:8fa::8	HTTP	5	5	746	0	0	5	746

Detail of Flow

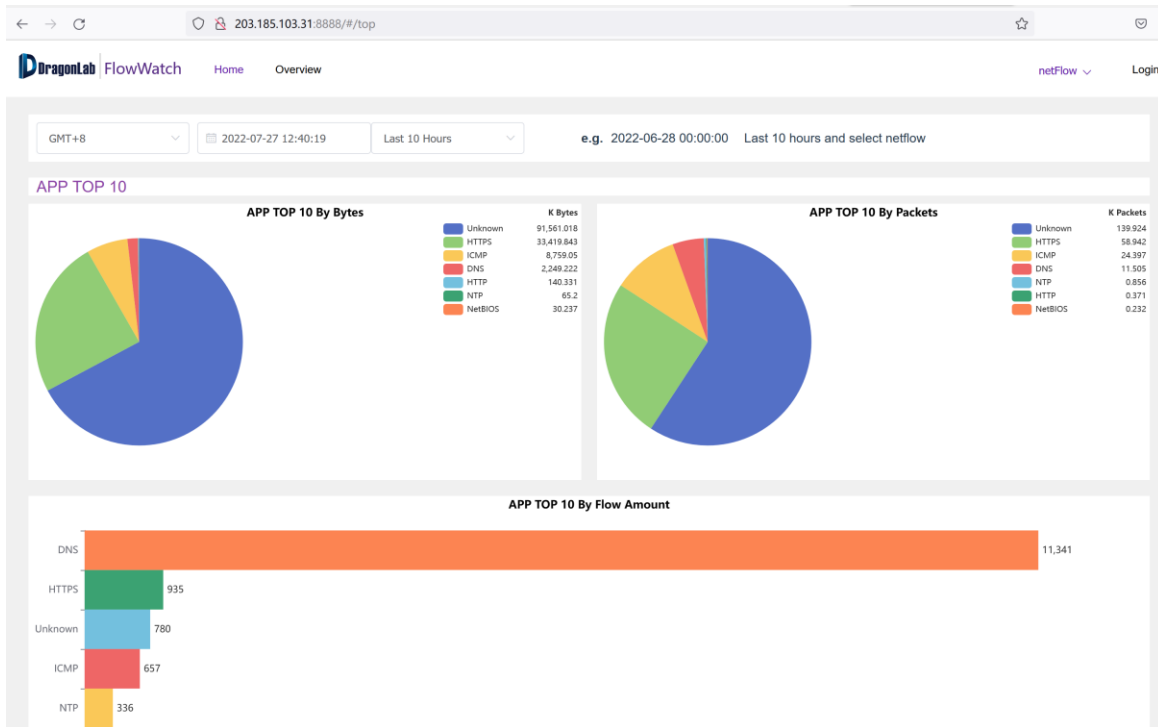
App	Client IP	Server IP	First Seen	Last Seen	Server Port	Client Port	Client to Server pps	Client to Server bps	Server to Client pps	Server to Client bps
HTTPS	2620:1ec:8fa::8	2001:da8:201:1085:11c:fa9e:872c:c356	2023-03-11 01:55:10	2023-03-11 01:59:54	49938	443	17.4533	215,307.6	16.93	10,256.6933
HTTPS	2620:1ec:8fa::8	2001:da8:e000:a015::2:11be	2023-03-11 10:54:31	2023-03-11 10:58:44	64552	443	9.1133	111,848.1067	6.0167	3,592.0533
HTTPS	2620:1ec:8fa::8	2001:da8:d800:172:5440:1b02:a414:6d8	2023-03-11 01:55:24	2023-03-11 01:56:12	9555	443	8.45	103,459.4933	5.0067	3,031.7867
HTTPS	2620:1ec:8fa::8	2001:da8:d800:172:5440:1b02:a414:6d8	2023-03-11 01:55:27	2023-03-11 01:56:11	9556	443	7.8367	97,867.0933	4.9467	3,038.4
HTTPS	2620:1ec:8fa::8	2001:250:1001:a008::3:8f7b	2023-03-11 09:54:35	2023-03-11 09:59:11	1144	443	7.4533	92,274.6667	4.6567	2,824.16
HTTPS	2620:1ec:8fa::8	240c:ca02:2169:35c:a43e:c83e:e233:e4f9	2023-03-10 22:56:35	2023-03-10 22:57:02	55092	443	4.6433	58,720.24	1.9033	1,135.7333
HTTPS	2620:1ec:8fa::8	240c:c001:1007:e3b7:ad2d:2083:92e9:46ca	2023-03-10 22:55:14	2023-03-10 22:57:19	11007	443	3.0833	39,146.8267	2.79	1,795.0933
HTTPS	2620:1ec:8fa::8	240c:ca04:2101:23b:a09e:9d85:49b5:d8a	2023-03-10 12:56:53	2023-03-10 13:00:01	24938	443	2.4	30,758.2133	2.3733	1,516.3733

Deployed at BDREN

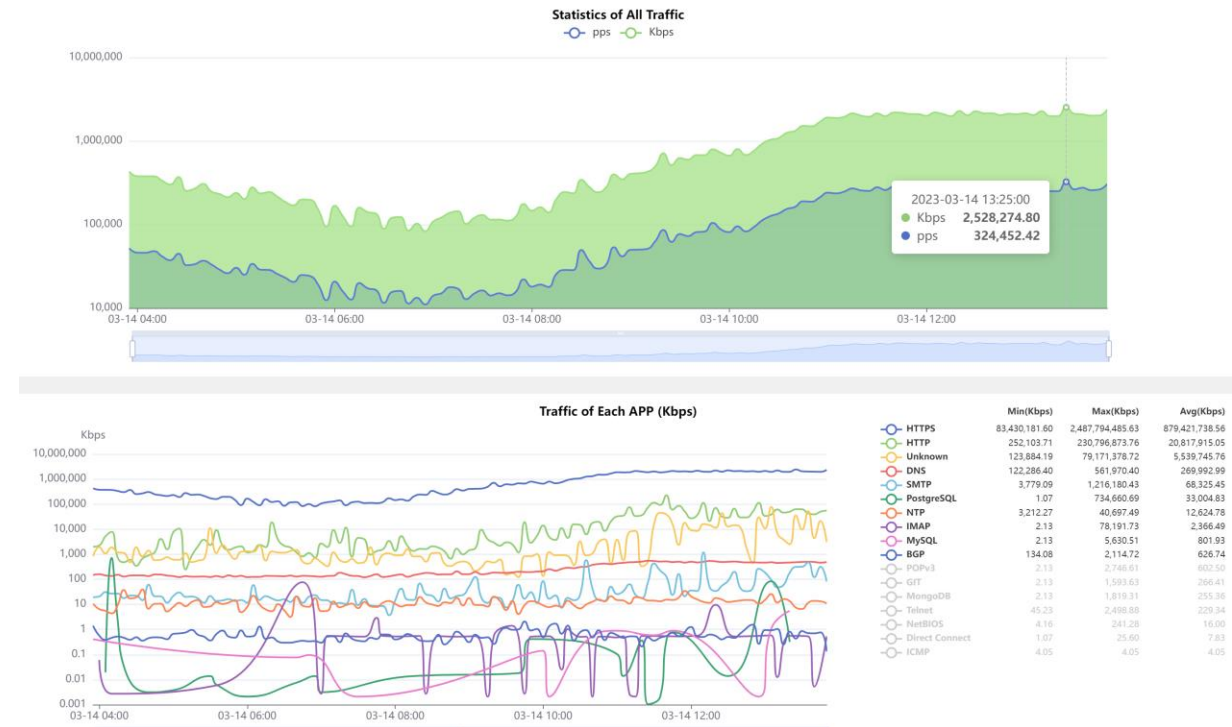


BDREN, throughput reaches 10Gbps

Deployed at ThaiREN and LEARN



ThaiREN



LEARN

CGT

- Open Source:
 - <https://github.com/gmazoyer/looking-g>
- 5 commands
- Query speed limit for security
- More partners is welcomed

```
show route IP_ADDRESS
show route as-path-regex AS_PATH_REGEX
show route ^AS
ping IP_ADDRESS|HOSTNAME
traceroute IP_ADDRESS|HOSTNAME
```

- Connect with partner's router: 7 partners
- Link to partner's Looking Glass: 3 partners

CGTF Looking Glass



Router to use

SingAREN Juniper Router
MYREN Cisco router
LEARN Guagga router
CERNET Guagga router
PERN Guagga 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

66.175.222.61 Help

Enter Reset

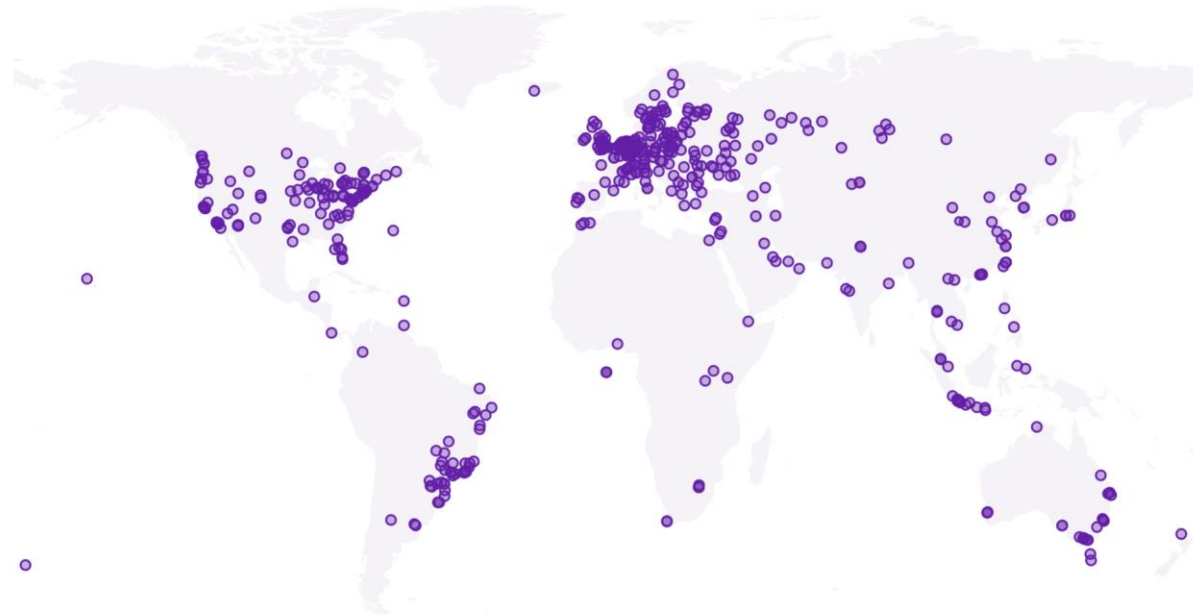
Your IP address: 66.175.222.61

Welcome to DragonLab's Network Looking Glass. The information provided by and the support of this service are on a best effort basis.

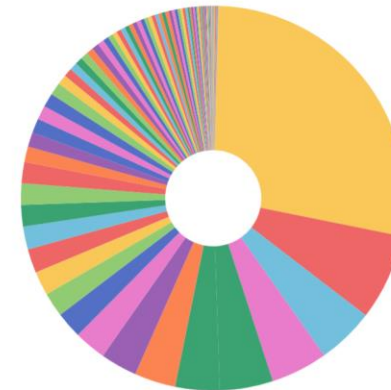
Looking Glass of Partners
<http://lg.kreonet2.net>
<http://lg.aarnet.edu.au>
<https://lg.myren.net.my/ig/ig.cgi>

Our Work on LG

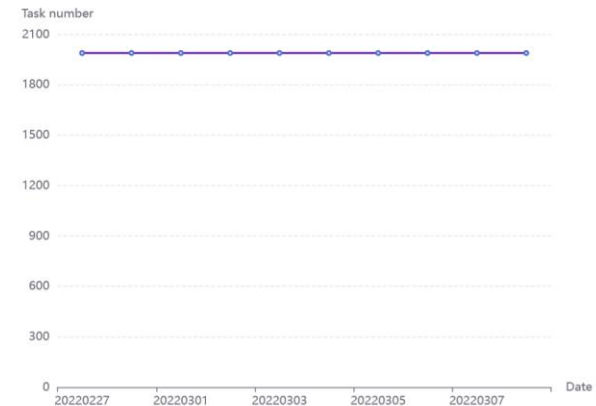
Distribution Map of Looking Glass and Probe



Proportion of Looking Glass and Probe by country



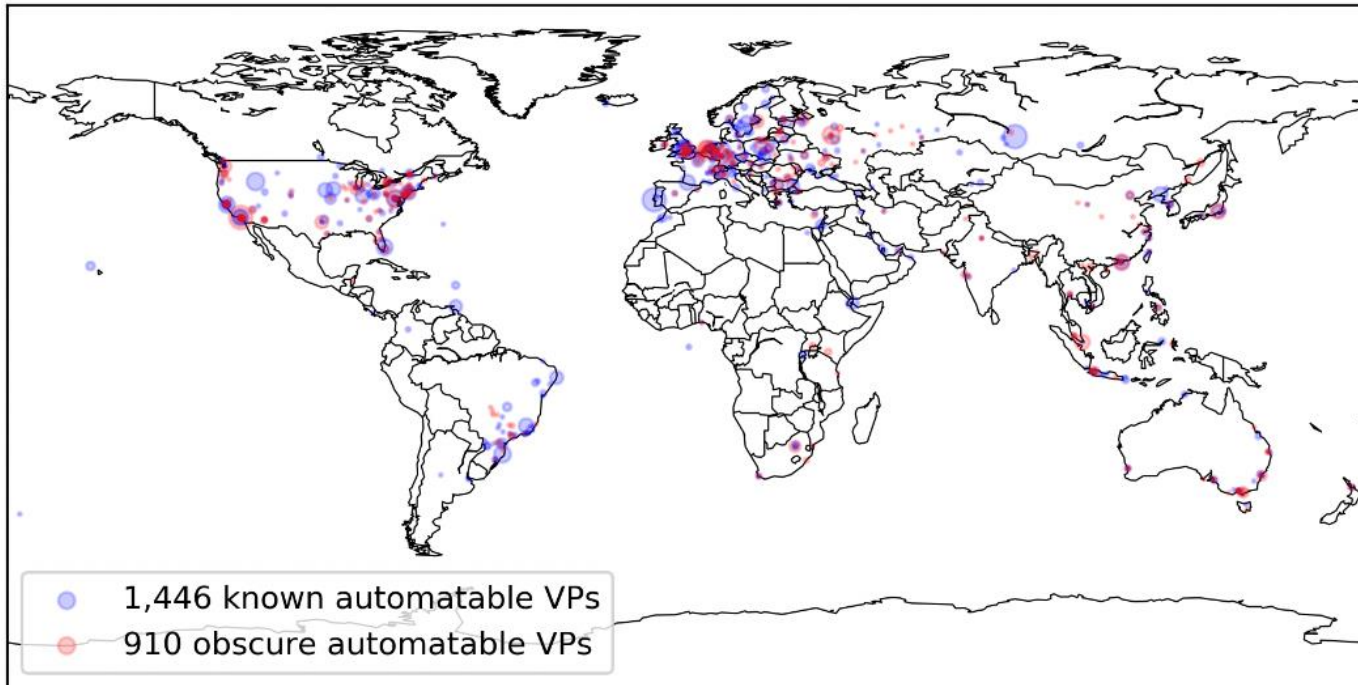
Running tasks



- Paper: “Discovering obscure looking glass sites on the web to facilitate internet measurement research” — — **CoNEXT’21**
- **2500 LGs**

Obscure Looking Glass Sites

- 1,446 known LG VPs in 386 cities of 75 countries
- 910 obscure LG VPs in 282 cities in 55 countries



- ✓ The 910 obscure VPs cover **8 exclusive countries** and **160 exclusive cities**, where no known LG VPs have been found before
- ✓ The 8 countries are mainly distributed in **East Africa** and **South Asia**

CGTF RIS













<https://bgp.cgtf.net>

We have established BGP session with **15 partners**.

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

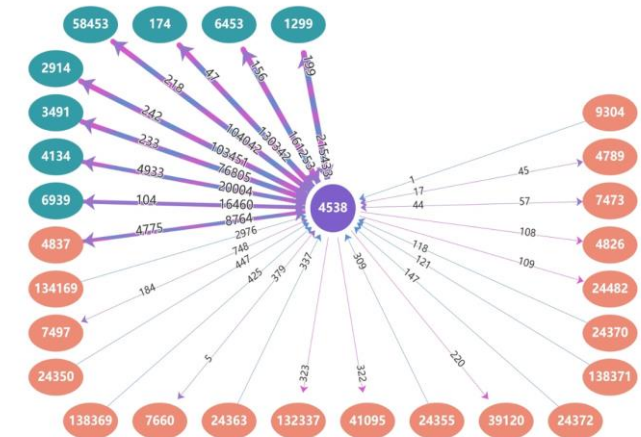
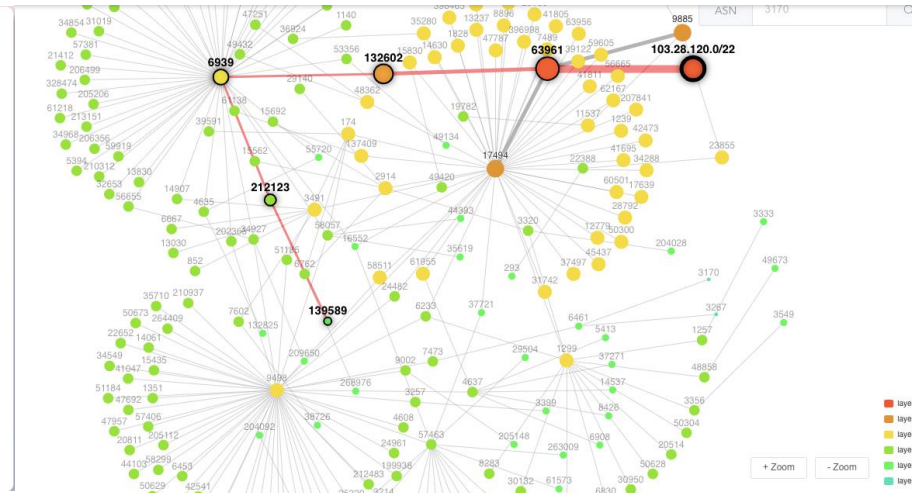
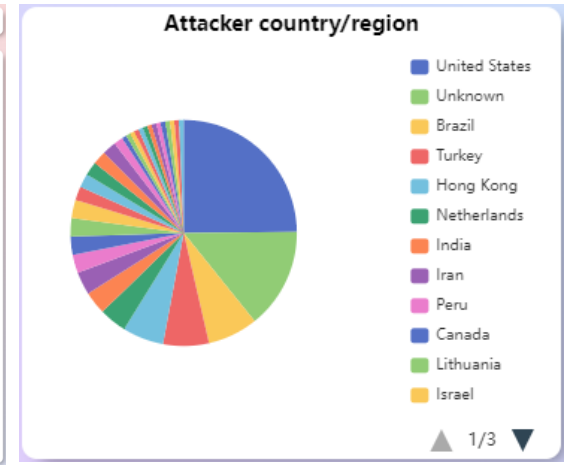
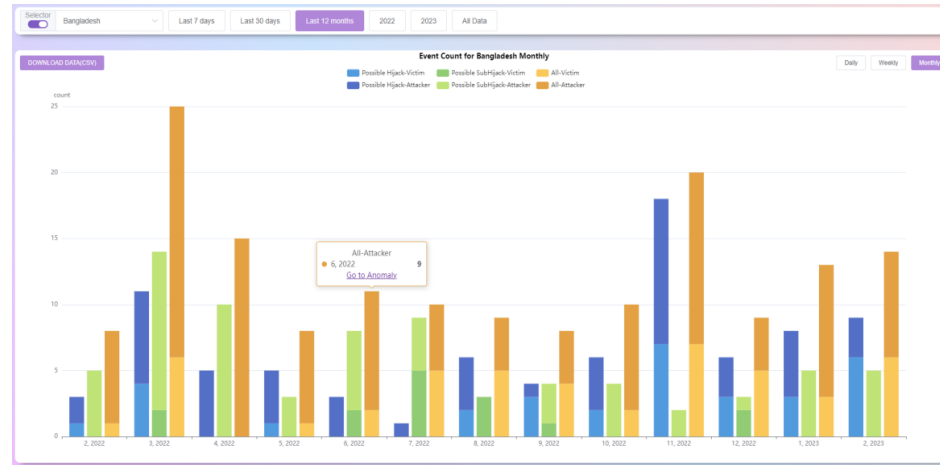
No.	Partner	No.	Partner
1	APAN-JP	9	MYREN
2	AARNET	10	PERN
3	BDREN	11	REANNZ
4	CERNET	12	SINGAREN
5	HARNET	13	ThaiSARN
6	ITB	14	TransPAC
7	KREONET	15	NREN
8	LEARN		

Index of /ribs/2022/07

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

BGP Routing Monitoring and Analysis: BGPWatch

- Hijacking Detection
- Hijacking Statistics
- Dashboard:AS info
- Routing Search:
 - forward, reverse, bi-direction
- Subscribe, Alarming



Hijacking Detection

- Knowledge-based real-time BGP hijacking Detection System
- Public BGP event reporting service
- Based on MOAS(subMOAS)
- Rely on Domain Knowledge (ROA, IRR, AS relationship etc)
- URL: <https://bgpwatch.cgtf.net>



The dashboard provides a detailed list of hijacking events, including filters for event type, harm level, time zone, and time period. The table below shows the first seven events:

Event ID	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible Hijack	low	Victim:TR/AS204843 (TR-STERLY) Attacker:US/AS397373(H4Y-TECHNOLOGIES)	1	206.206.119.0/24	2023-03-11 11:28:28	-	-	detail
2	Possible SubHijack	low	Victim:VN/AS45903 (CMCTELECOM-AS-VN) Attacker:HK/AS45474(NEXUSGUARD-AS-AP)	1	prefix: 144.48.27.0/24 subprefix: 144.48.27.132/32	2023-03-11 10:34:50	2023-03-11 11:34:55	1:0:5	detail
3	Possible Hijack	low	Victim:AS209260 () Attacker:IN/AS135752(EVOKEDS-AS)	3	84.32.26.0/24	2023-03-11 08:48:40	2023-03-11 08:48:41	0:0:1	detail
4	Ongoing Possible Hijack	low	Victim:PK/AS38616 (WORLDCALL-AS-KHI) Attacker:PK/AS141432(Tzees-AS-AP)	1	203.81.219.0/24	2023-03-11 07:53:48	-	-	detail
5	Possible Hijack	low	Victim:US/AS834 (IPXO) Attacker:AS200010()	3	206.206.109.0/24	2023-03-11 07:27:33	2023-03-11 07:50:05	0:22:32	detail
6	Ongoing Possible Hijack	low	Victim:HK/AS38136 (AKARI-NETWORKS-AS-AP) Attacker:AS393427()	1	46.3.243.0/24	2023-03-11 06:38:15	-	-	detail
7	Ongoing Possible Hijack	low	Victim:US/AS22773 (ASN-CXA-ALL-CCI-22773-RDC) Attacker:AS393427()	1	46.3.202.0/24	2023-03-11 06:38:13	-	-	detail

Features --- Event level evaluation

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

DragonLab | BGPWatch Home Overview Anomaly DashBoard RoutingPath Country/Region Organization Login Register

Select event type: All | Select harm level: All | Time zone: GMT+8 | Select time period (by Start Time): 2023-03-01 12:22:27 - 2023-03-11 12:22:27 | Duration: All | Select for event by keywords: Please enter search key

Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1 Ongoing Possible Hijack	low	Victim:TR/AS204843 (TR-STERLY) Attacker:US/AS397373(H4Y-TECHNOLOGIES)	1	206.206.119.0/24	2023-03-11 11:28:28	-	-	detail
2 Possible SubHijack	low	Victim:VN/AS45903 (CMCTELECOM-AS-VN) Attacker:HK/AS45474(NEXUSGUARD-AS-AP)	1	prefix: 144.48.27.0/24 subprefix: 144.48.27.132/32	2023-03-11 10:34:50	2023-03-11 11:34:55	1:0:5	detail

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)

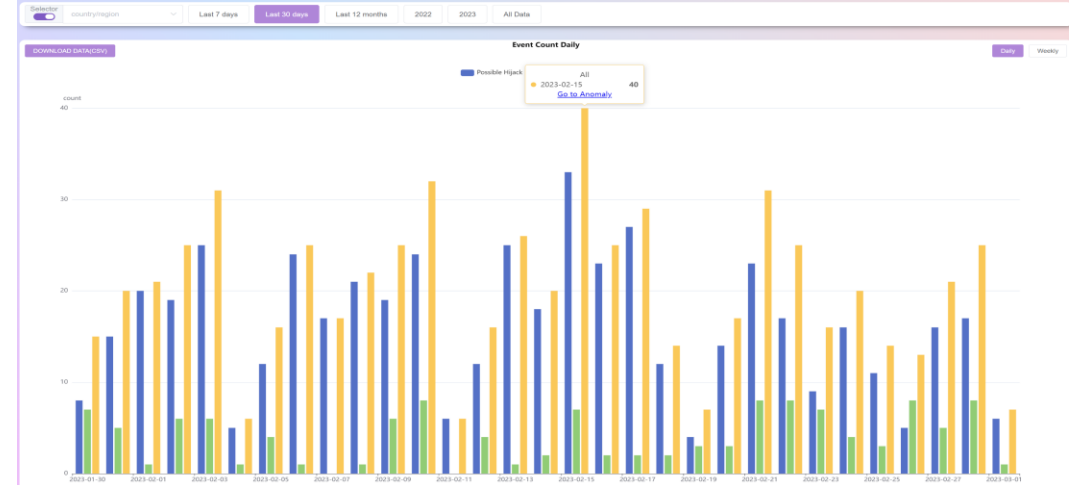
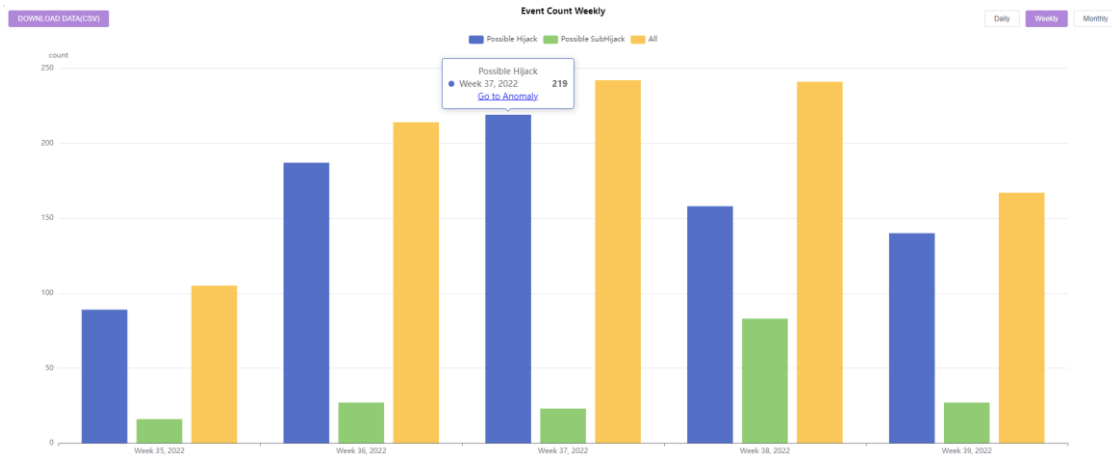
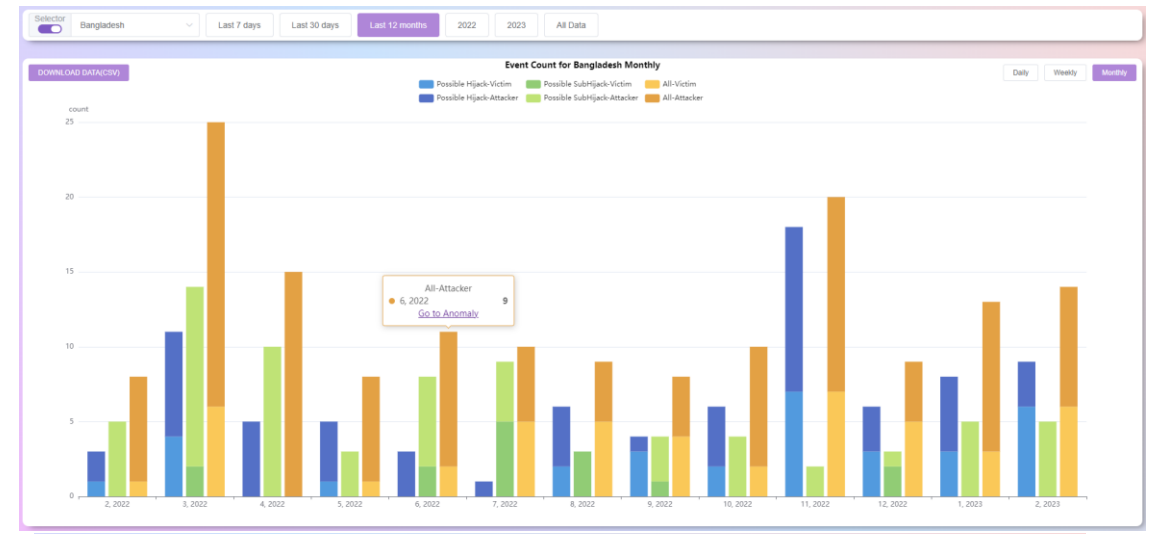
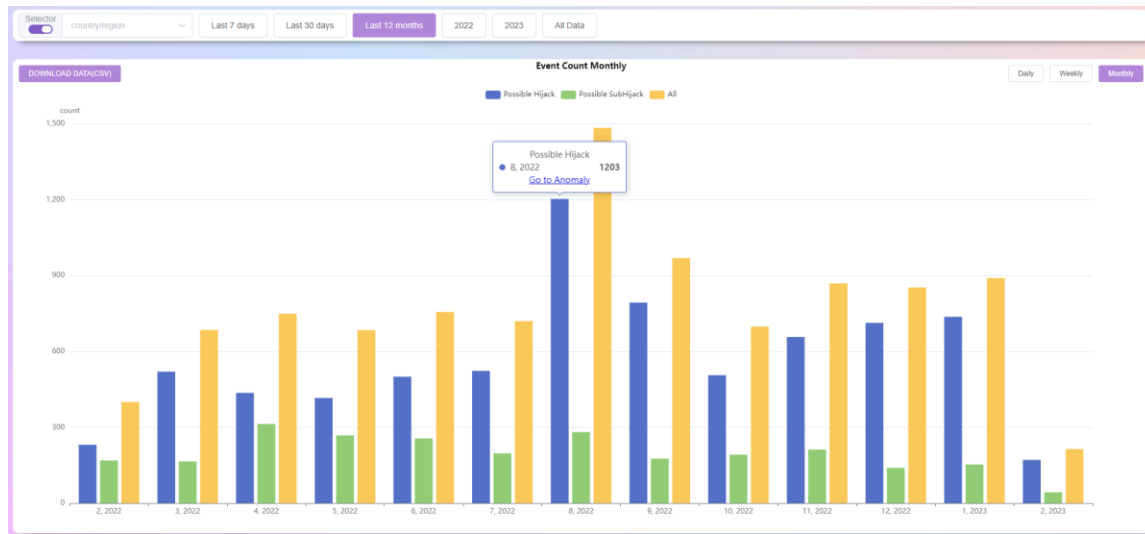
Hijacker Description: MITRE-AS-2

End Time: 2021-11-08 17:13:46

middle level

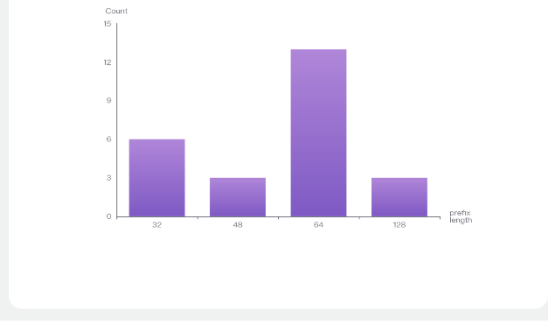
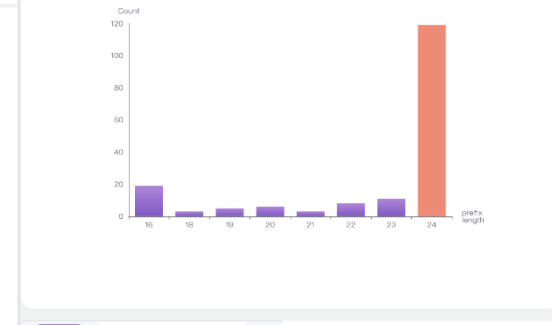
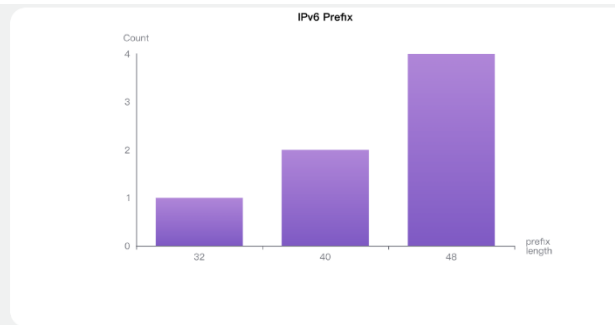
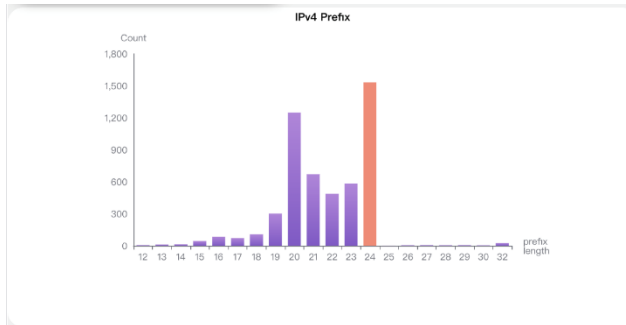
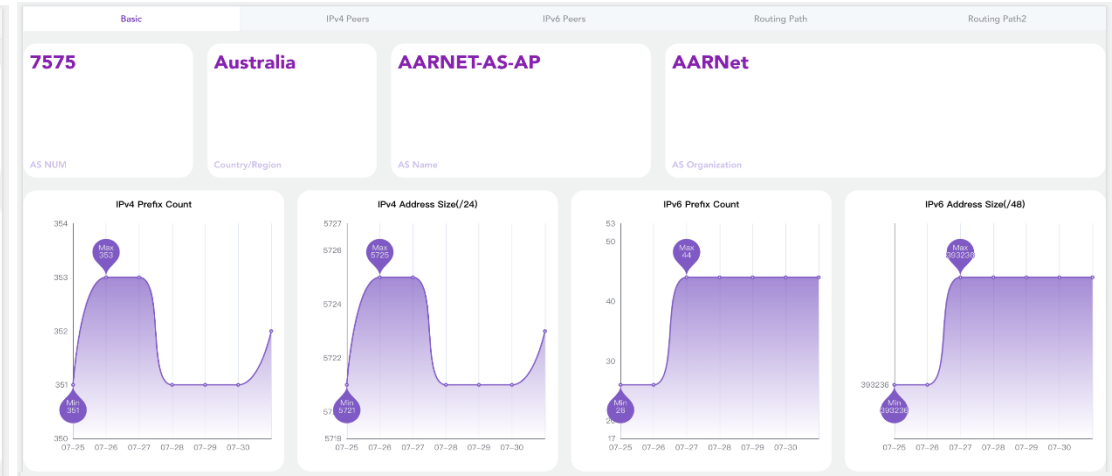
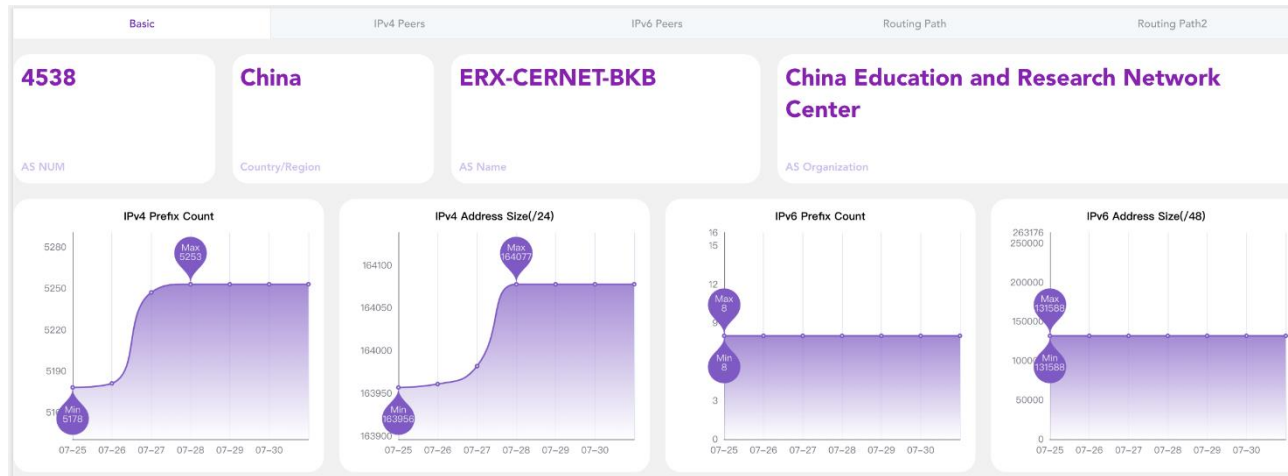
Possible Hijack Events

Overview---Statistics for Anomaly Events



Do statistics by country/region, AS, and by yearly, monthly, weekly, and daily

DashBoard --Basic Info



Prefix Search for Prefix

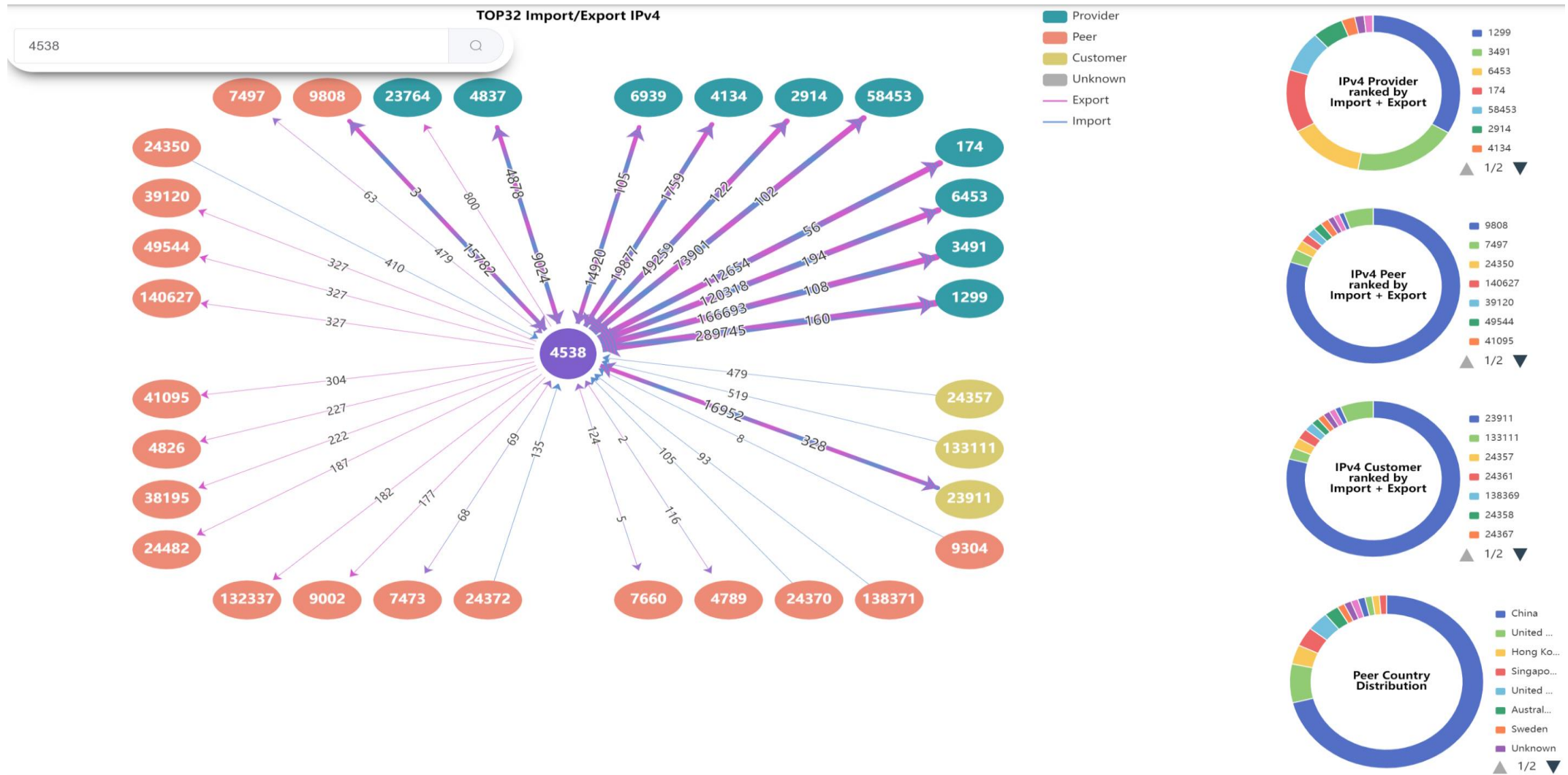
Prefix	Click on the column above, the corresponding prefix will be displayed in the table
1	1.51.112.0/24 42.244.13.0/24 42.247.1.0/24
2	42.247.5.0/24 42.247.8.0/24 42.247.9.0/24
3	42.247.13.0/24 42.247.18.0/24 42.247.19.0/24

Prefix Search for Prefix

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

Support Prefix Searching

Key Peers Information



Prefix Exchange of Key Partners

Routing Path Search

APAN-JP AARNET BDREN CERNET HARNET ITB KREONET LEARN MYREN NREN PERN **REANNZ** SINGAREN ThaiREN TransPAC

IP 2001:200::/32

You can input an IP address or prefix address. For example:
1.0.0.0/16, 2001:200::/32. The system will return all the subset and superset network of it.

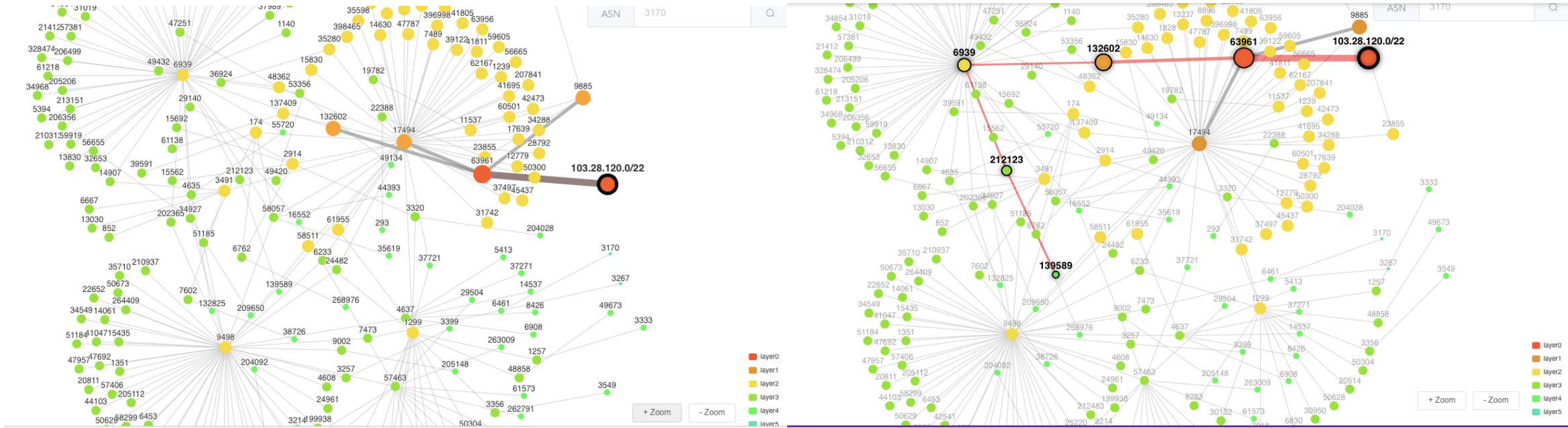
2001:200:900::/40
2001:200:e000::/35
2001:200::/32
2001:200:c000::/35
2001:200:e00::/40

2001:200:e00::/40 AS PATH **1090415**
Prefix Total

```
graph LR; 38022((38022)) --> 3356((3356)); 38022 --> 6939((6939)); 38022 --> 2907((2907)); 3356 --> 9607((9607)); 3356 --> 7500((7500)); 6939 --> 7500; 2907 --> 7660((7660)); 2907 --> 2914((2914)); 9607 --> 23634((23634)); 9607 --> 7530((7530)); 7500 --> 23634; 7500 --> 2500((2500)); 7660 --> 7530; 2914 --> 7530; 23634 --> 4690((4690)); 2500 --> 4690; 7530 --> 4690;
```

Put a prefix or an IP, they can be either IPv4 or IPv6. Return paths of all sub networks and super networks of the input prefix. Group Prefixes with the same routing path.

Reverse Routing Path



- With better interactivity
- Can display the path to a prefix
- Support search
- The number of layers to display can be selected

+

o

•

Comments and Suggestion?

