Joint Research on 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

Mar.8, 2022

Content

- **Project Outline**
- **Work Progress**
- **APNIC ISIF Funding Program**

International Cooperation

14 countries, 23 research organizations

Excellent Mix of Key Experiences of 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

e-Hualu
NREN
BdREN
LEARN
CamREN
MYREN

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

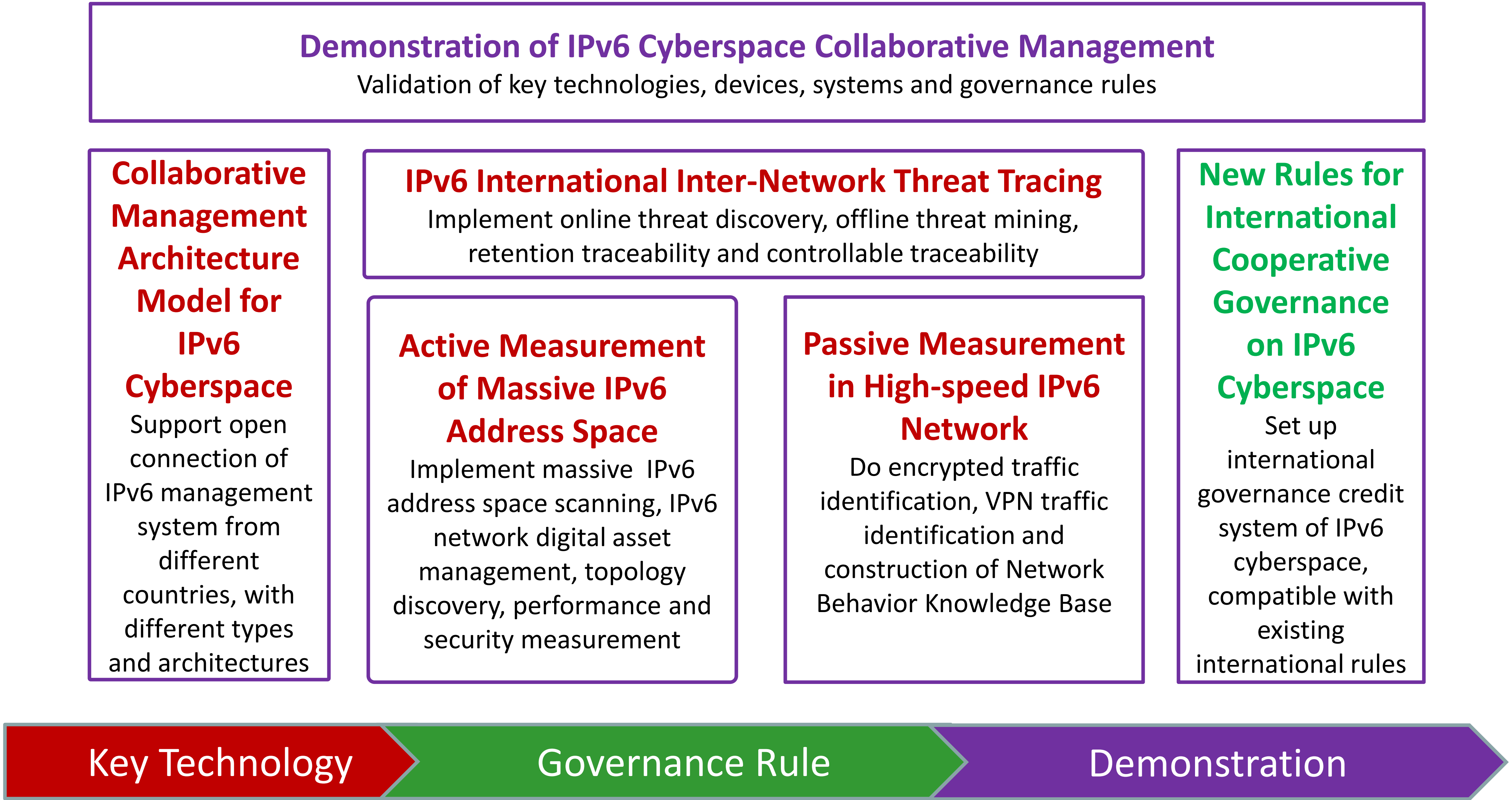
UESTC

Shandong University

eHualu

Promote Network Technology Innovation and Application Demonstration

Research Content



Demonstration of IPv6 Cyberspace Collaborative Management

Validation of key technologies, devices, systems and governance rules

Collaborative Management Architecture Model for IPv6 Cyberspace

Support open connection of IPv6 management system from different countries, with different types and architectures

IPv6 International Inter-Network Threat Tracing

Implement online threat discovery, offline threat mining, retention traceability and controllable traceability

Active Measurement of Massive IPv6 Address Space

Implement massive IPv6 address space scanning, IPv6 network digital asset management, topology discovery, performance and security measurement

Passive Measurement in High-speed IPv6 Network

Do encrypted traffic identification, VPN traffic identification and construction of Network Behavior Knowledge Base

New Rules for International Cooperative Governance on IPv6 Cyberspace

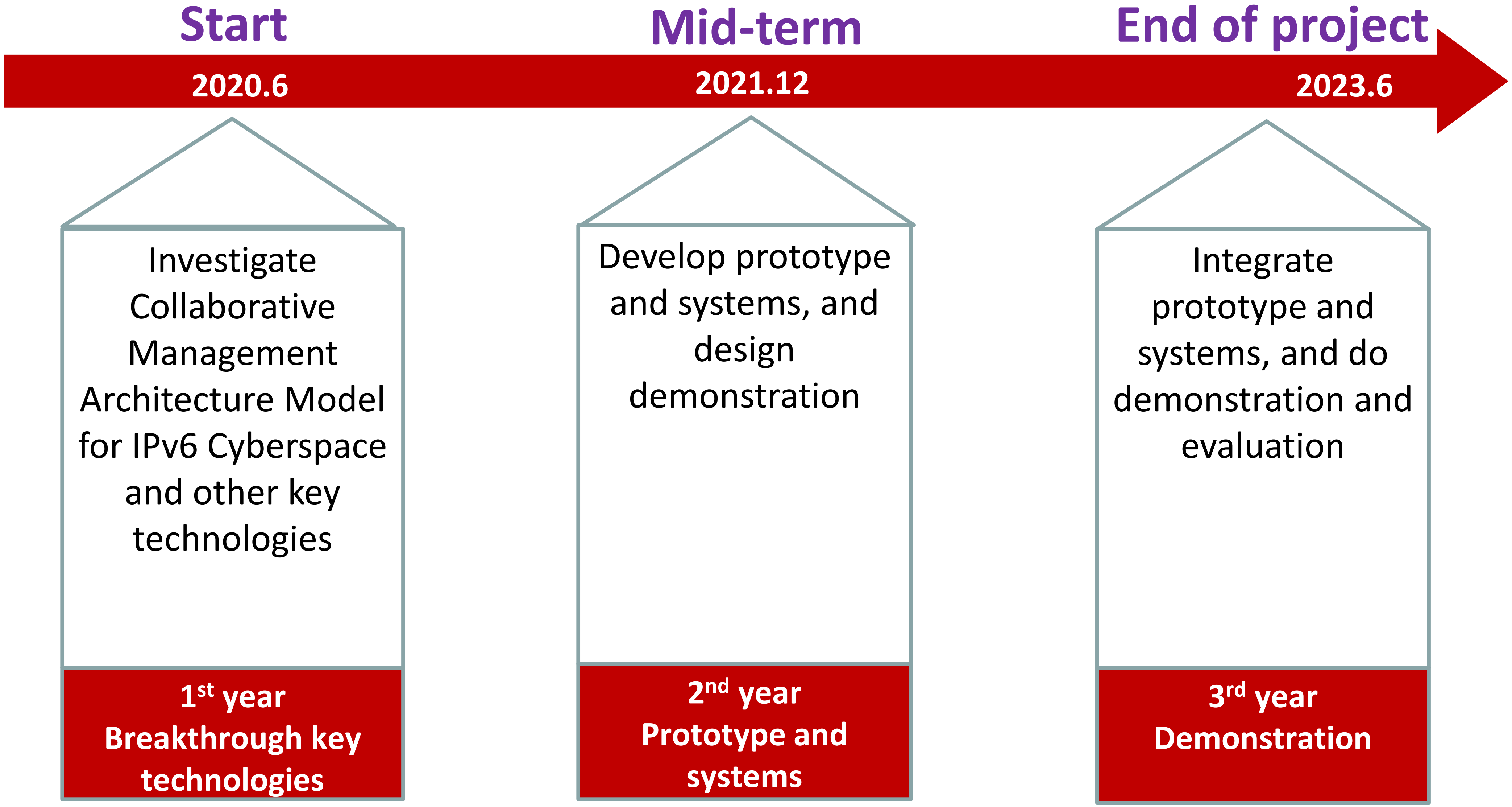
Set up international governance credit system of IPv6 cyberspace, compatible with existing international rules

Key Technology

Governance Rule

Demonstration

Project Plan & Schedule



Start

2020.6

Investigate Collaborative Management Architecture Model for IPv6 Cyberspace and other key technologies

1st year
Breakthrough key technologies

Mid-term

2021.12

Develop prototype and systems, and design demonstration

2nd year
Prototype and systems

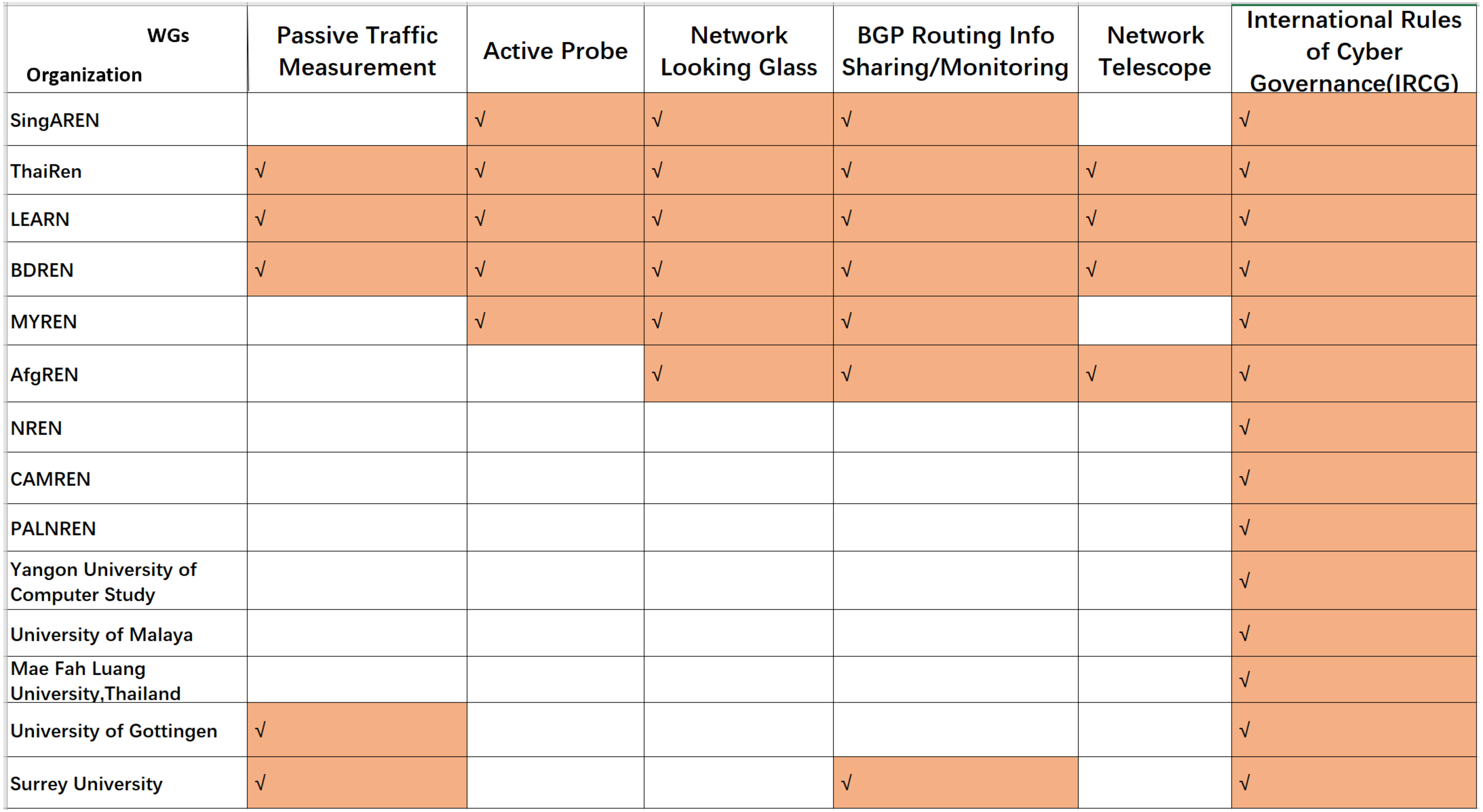
End of project

2023.6

Integrate prototype and systems, and do demonstration and evaluation

3rd year
Demonstration

Working Group



WGs 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						√
PALNREN						√
Yangon University of Computer Study						√
University of Malaya						√
Mae Fah Luang University,Thailand						√
University of Gottingen	√					√
Surrey University	√			√		√

Work Progress

- **Progress In the Following Aspect:**
  - Active Probe Platform—Gperf
  - Passive Traffic Measurement System—Flow Watch
  - BGP Routing Sharing Platform – CGTF RIS
  - BGP Routing Hijack Detecting--BGP Watch
  - Network Looking Glass- CGTF LG

Active Probe Platform—Gperf

What is Gperf ?

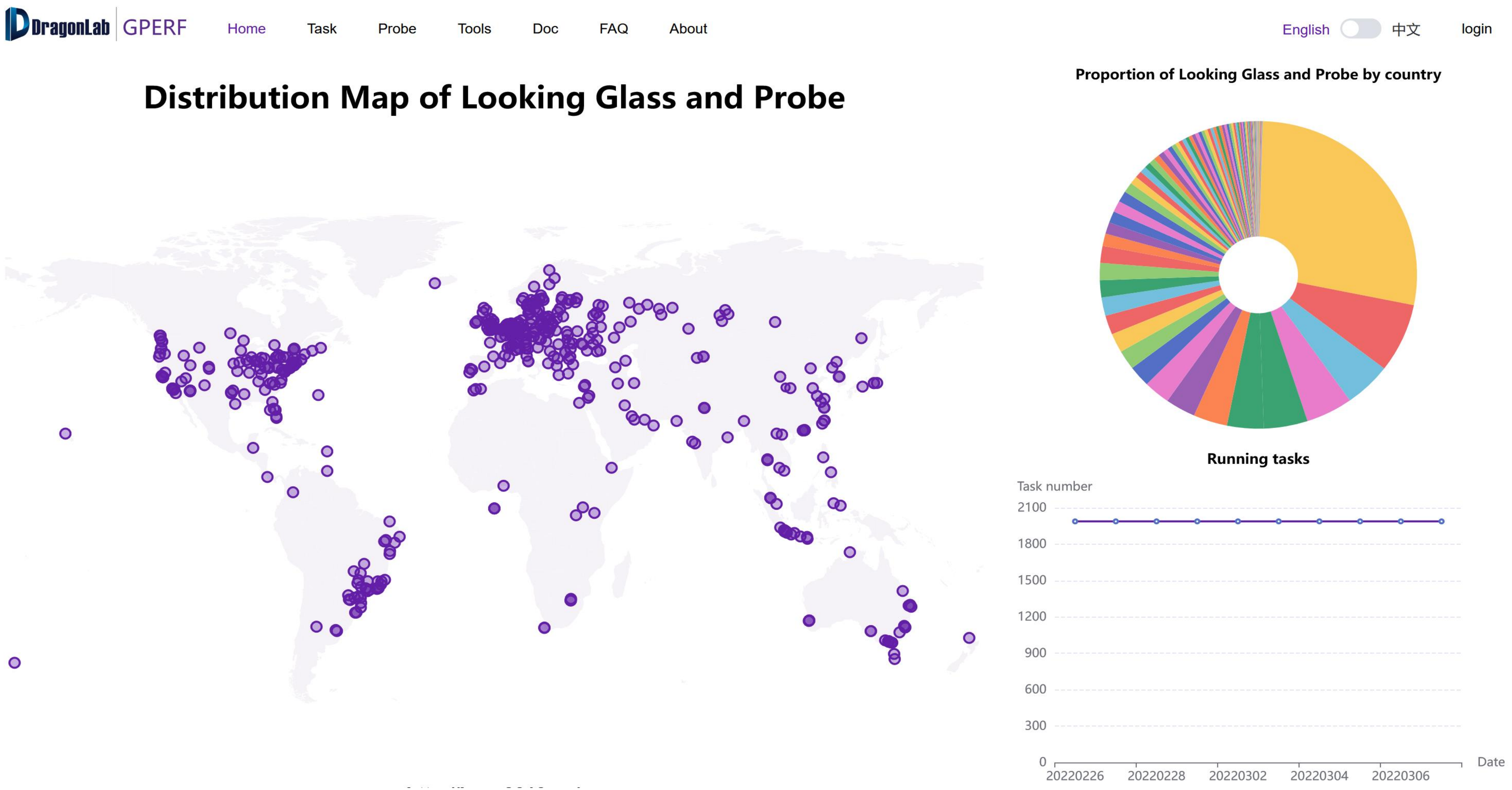
- An active Internet measurement platform
  - Mechanism: Initiate detections through several deployed probes
  - Target: Domain names on the Internet
  - Purpose: Obtain and visualize periodic results

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

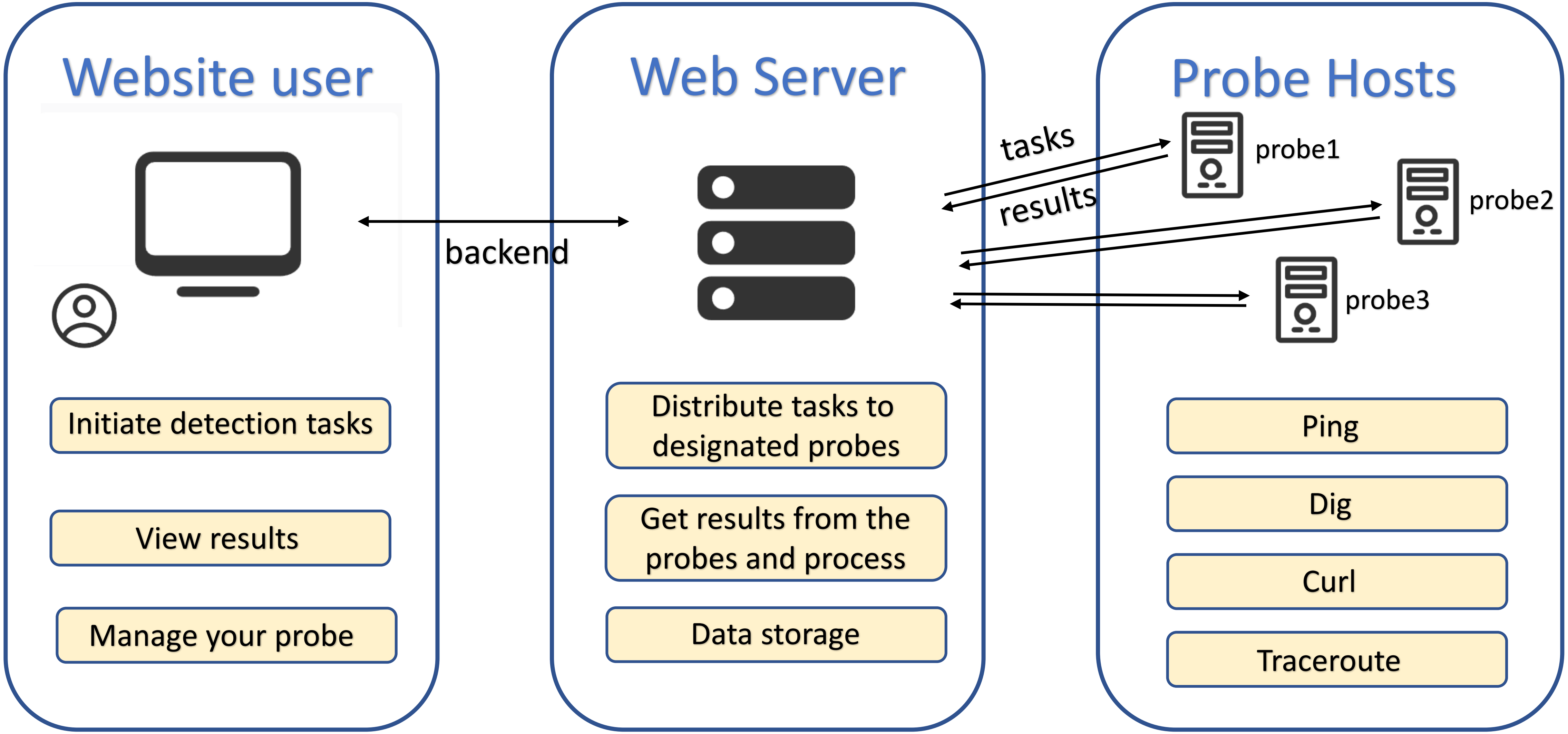
- Supports both **IPv4** and **IPv6**

Homepage

https://gperf.cgtf.net/



Gperf Architecture



Website user

- Initiate detection tasks
- View results
- Manage your probe

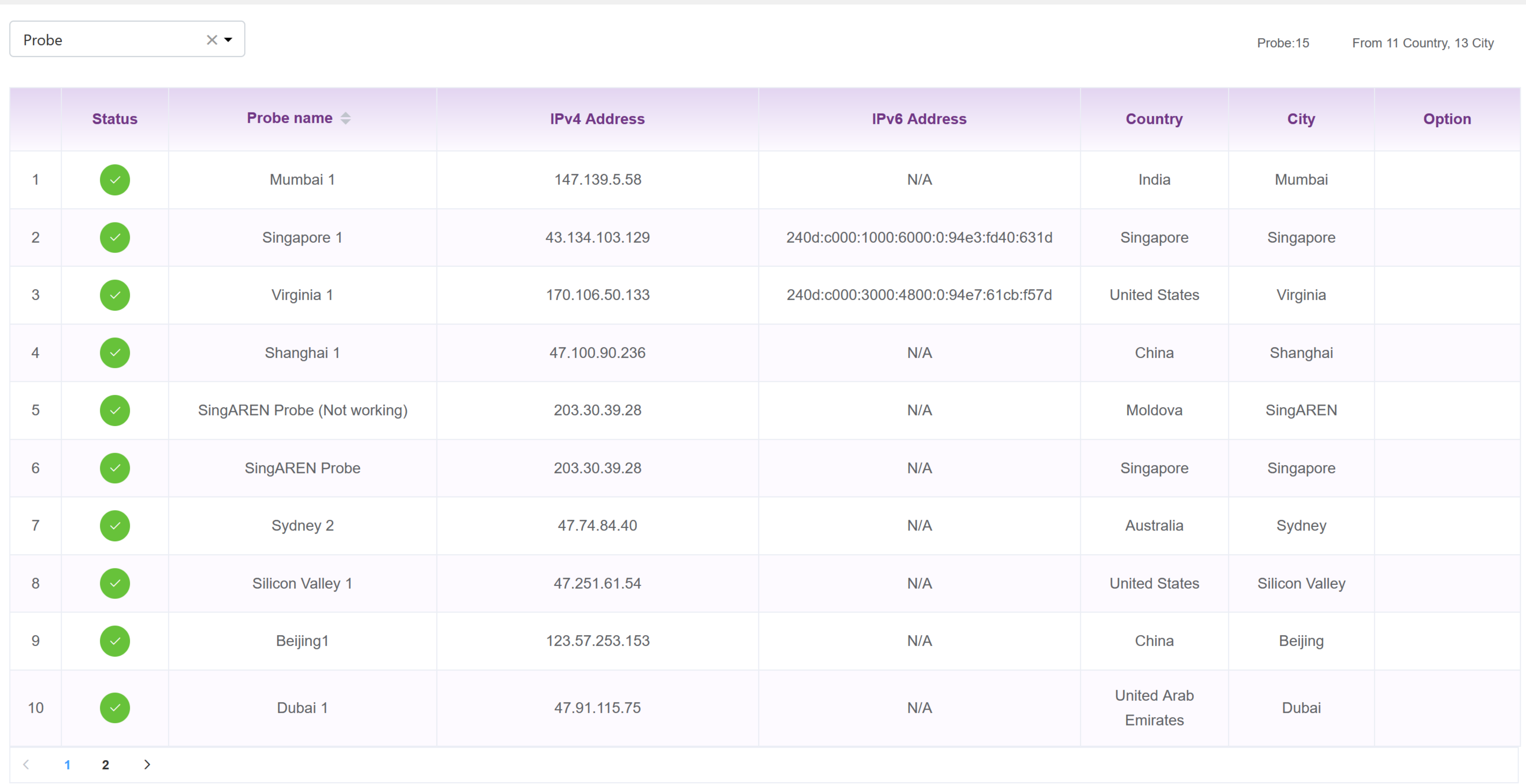
Web Server

- Distribute tasks to designated probes
- Get results from the probes and process
- Data storage

Probe Hosts

- Ping
- Dig
- Curl
- Traceroute

Available Probe list



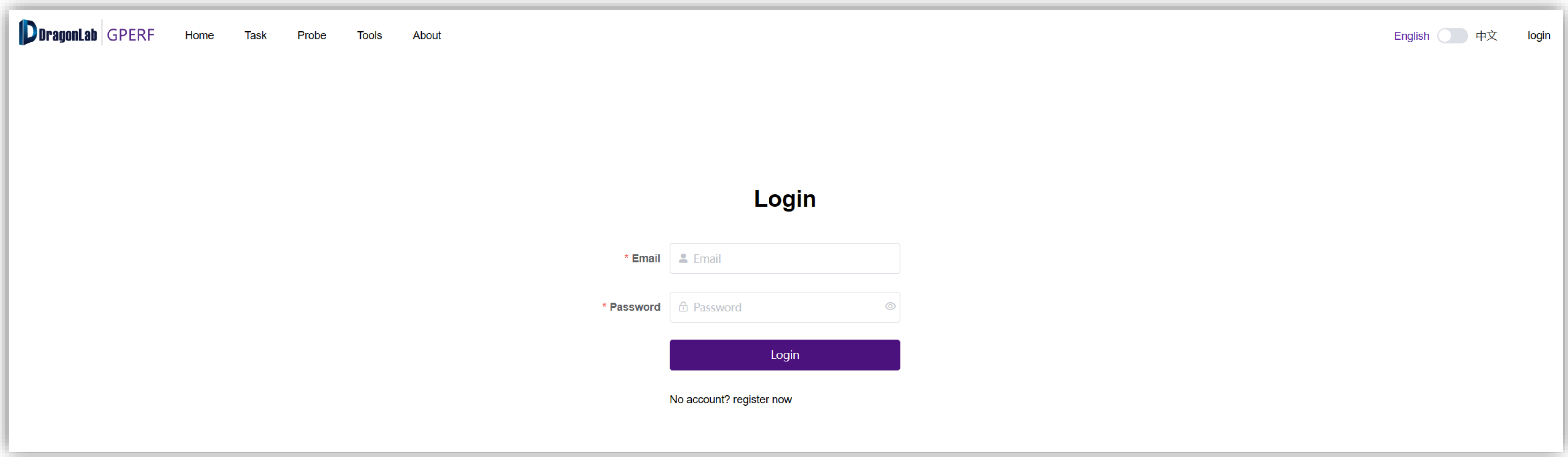
Probe × ▾

Probe:15 From 11 Country, 13 City

	Status	Probe name	IPv4 Address	IPv6 Address	Country	City	Option
1	✓	Mumbai 1	147.139.5.58	N/A	India	Mumbai	
2	✓	Singapore 1	43.134.103.129	240d:c000:1000:6000:0:94e3:fd40:631d	Singapore	Singapore	
3	✓	Virginia 1	170.106.50.133	240d:c000:3000:4800:0:94e7:61cb:f57d	United States	Virginia	
4	✓	Shanghai 1	47.100.90.236	N/A	China	Shanghai	
5	✓	SingAREN Probe (Not working)	203.30.39.28	N/A	Moldova	SingAREN	
6	✓	SingAREN Probe	203.30.39.28	N/A	Singapore	Singapore	
7	✓	Sydney 2	47.74.84.40	N/A	Australia	Sydney	
8	✓	Silicon Valley 1	47.251.61.54	N/A	United States	Silicon Valley	
9	✓	Beijing1	123.57.253.153	N/A	China	Beijing	
10	✓	Dubai 1	47.91.115.75	N/A	United Arab Emirates	Dubai	

< 1 2 >

Register An Account



DragonLab GPERF Home Task Probe Tools About English 中文 login

Login

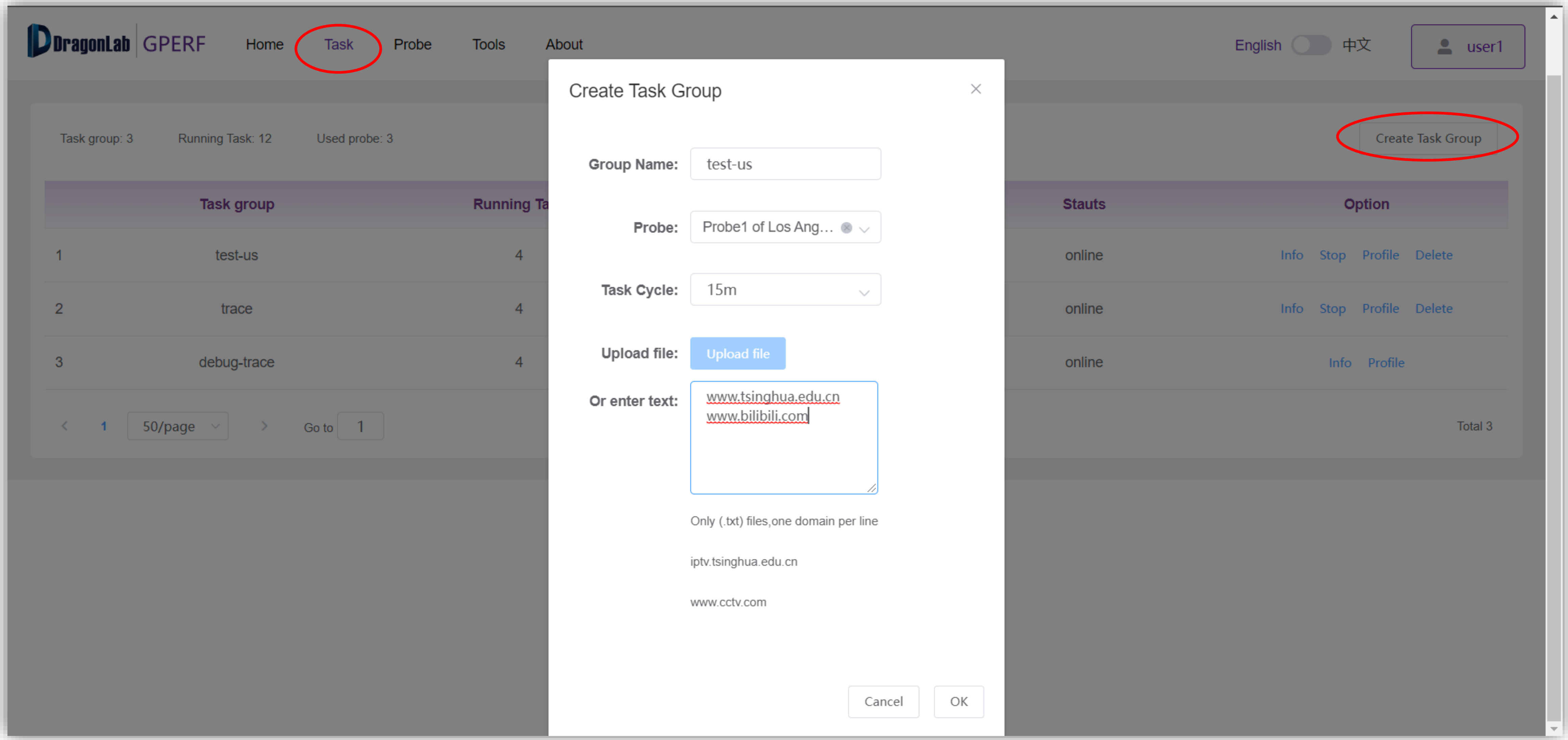
* Email: Email

* Password: Password

Login

No account? register now

Create your probe task goup



Task group: 3 Running Task: 12 Used probe: 3

	Task group	Running Ta	Stauts	Option
1	test-us	4	online	Info Stop Profile Delete
2	trace	4	online	Info Stop Profile Delete
3	debug-trace	4	online	Info Profile

< 1 50/page > Go to 1 Total 3

Create Task Group

Group Name: test-us

Probe: Probe1 of Los Ang...

Task Cycle: 15m

Upload file:

Or enter text:
www.tsinghua.edu.cn
www.bilibili.com

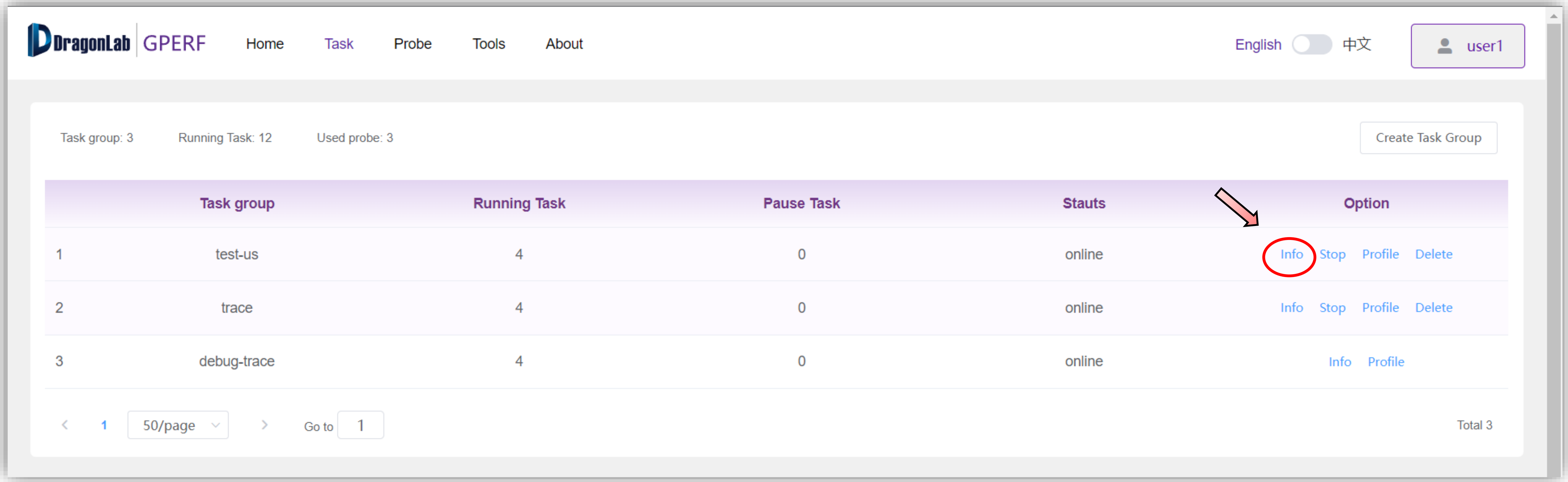
Only (.txt) files,one domain per line

iptv.tsinghua.edu.cn

www.cctv.com

Manage task group

- Only the task group creator can perform the ‘Stop’ and ‘Delete’ operations to the corresponding task
- Click the ‘Info’ operation of a task group to enter the task group details interface



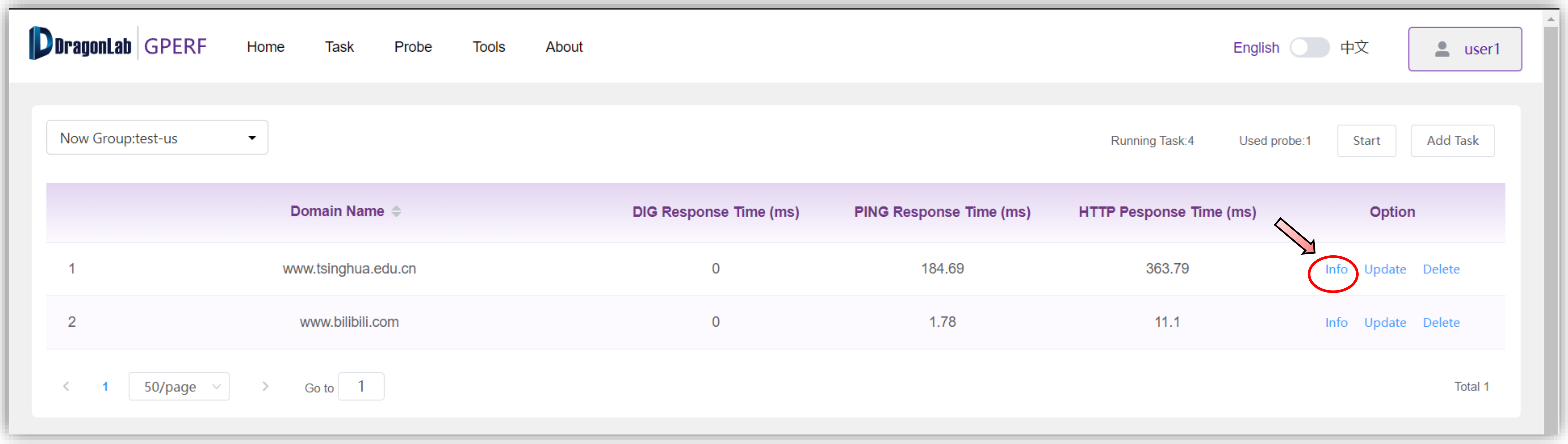
Task group: 3 Running Task: 12 Used probe: 3

	Task group	Running Task	Pause Task	Stauts	Option
1	test-us	4	0	online	Info Stop Profile Delete
2	trace	4	0	online	Info Stop Profile Delete
3	debug-trace	4	0	online	Info Profile

Total 3

View task results

- The task group interface shows the average value of the most recent detection results for each target domain name
- Click the ‘Info’ operation of a domain name row to view the details of detection results for the corresponding domain name



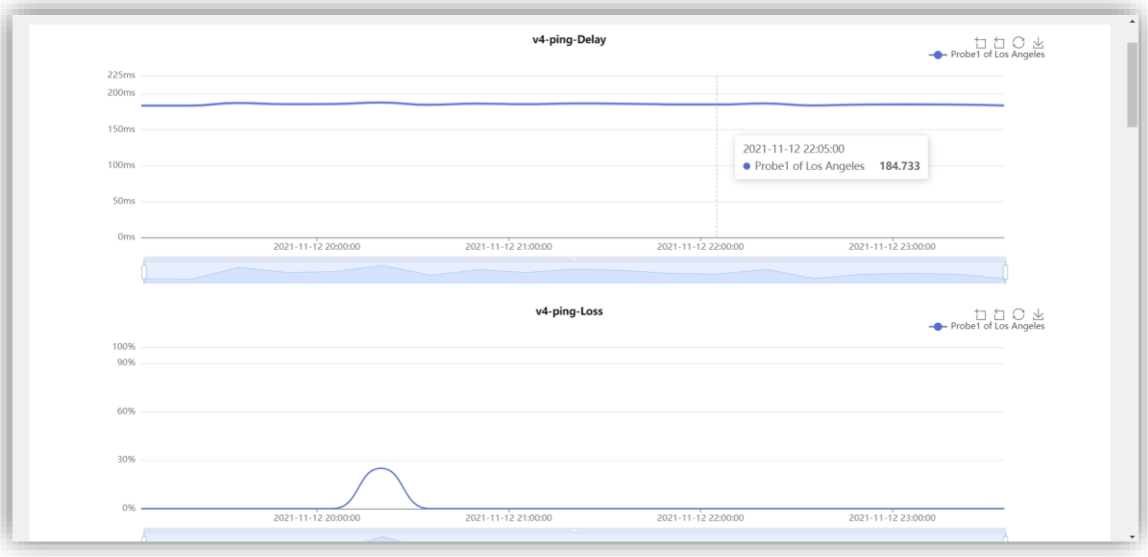
Now Group:test-us

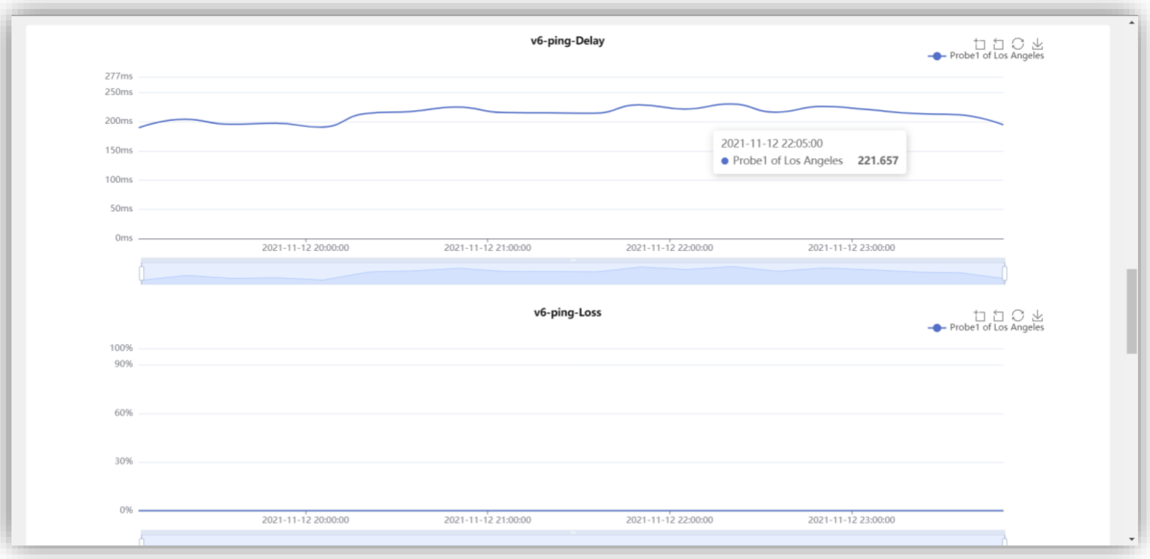
Running Task:4 Used probe:1

	Domain Name	DIG Response Time (ms)	PING Response Time (ms)	HTTP Pesponse Time (ms)	Option
1	www.tsinghua.edu.cn	0	184.69	363.79	Info Update Delete
2	www.bilibili.com	0	1.78	11.1	Info Update Delete

Result details

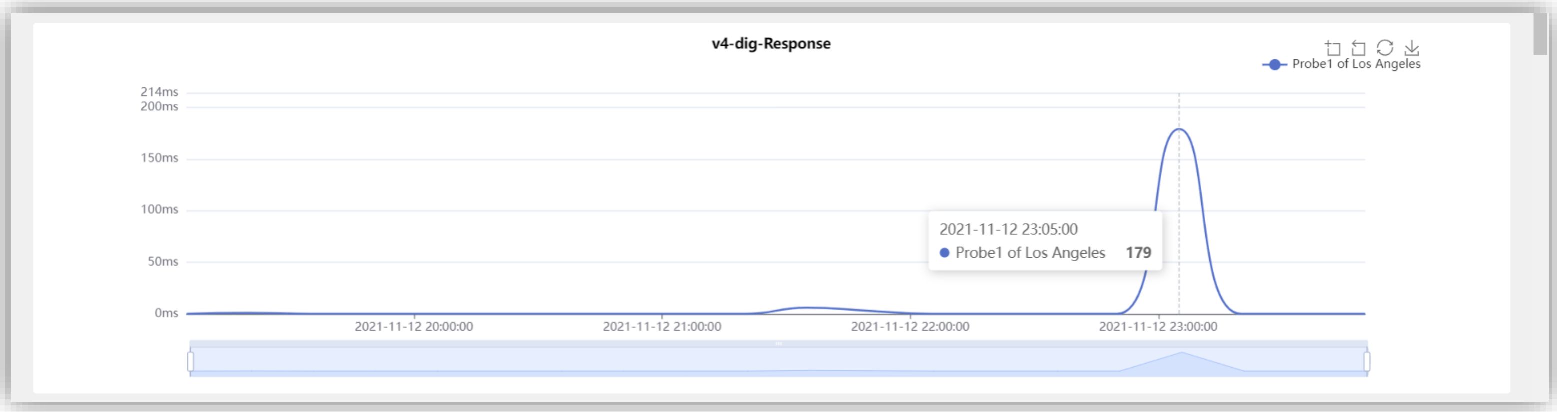
a) Time delay and packet loss rate of ‘***ping***’ command (IPv4 & IPv6)

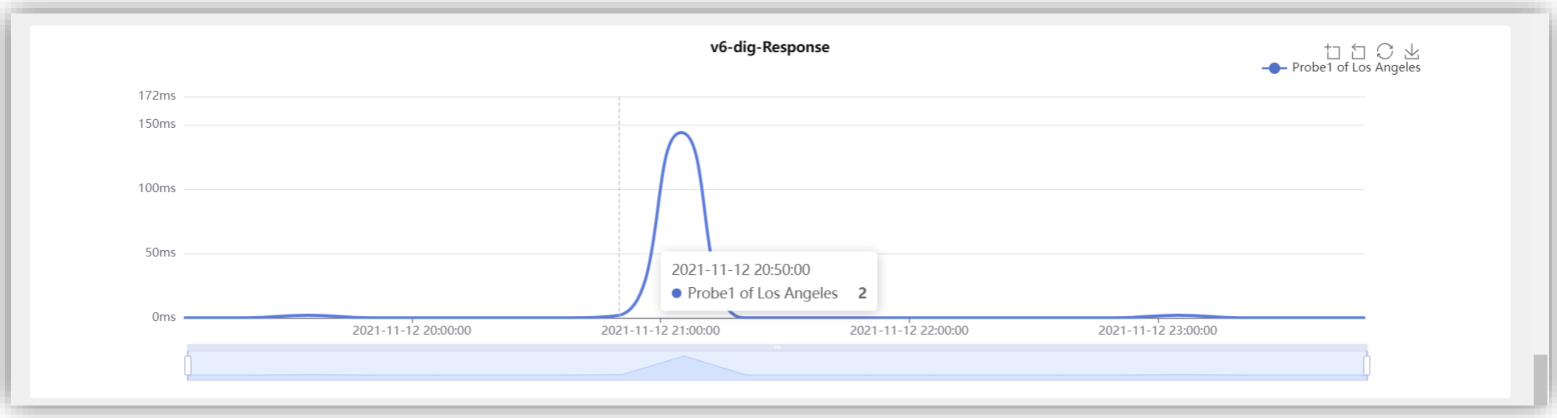




Result details

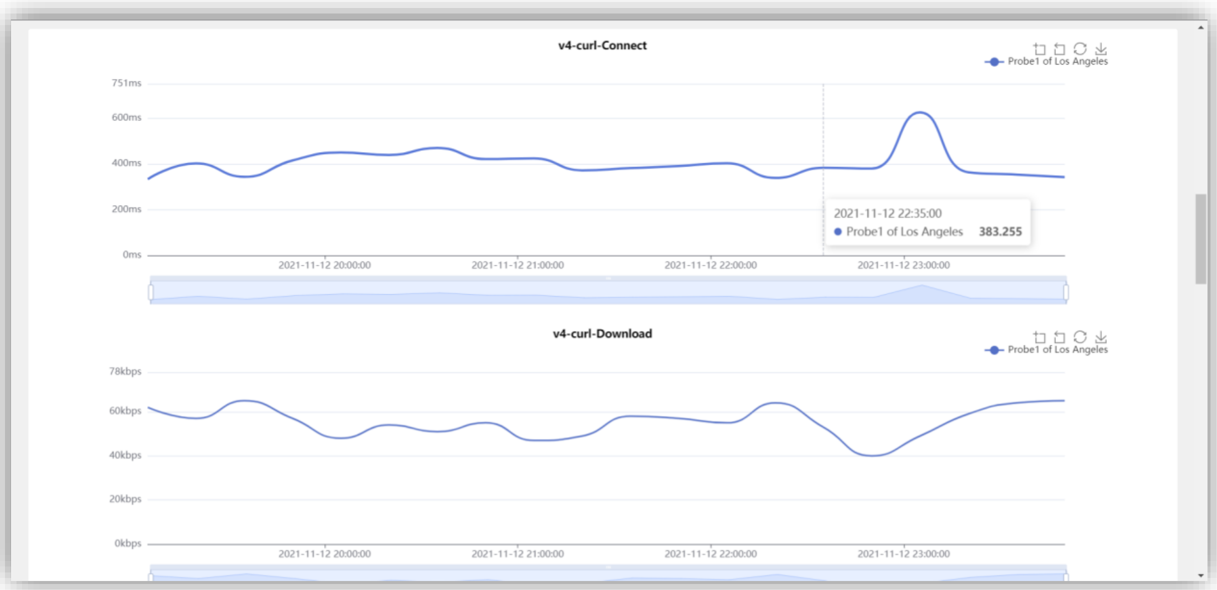
b) Response time of ‘*dig*’ command, indicates the time required for domain name resolution (IPv4 & IPv6)

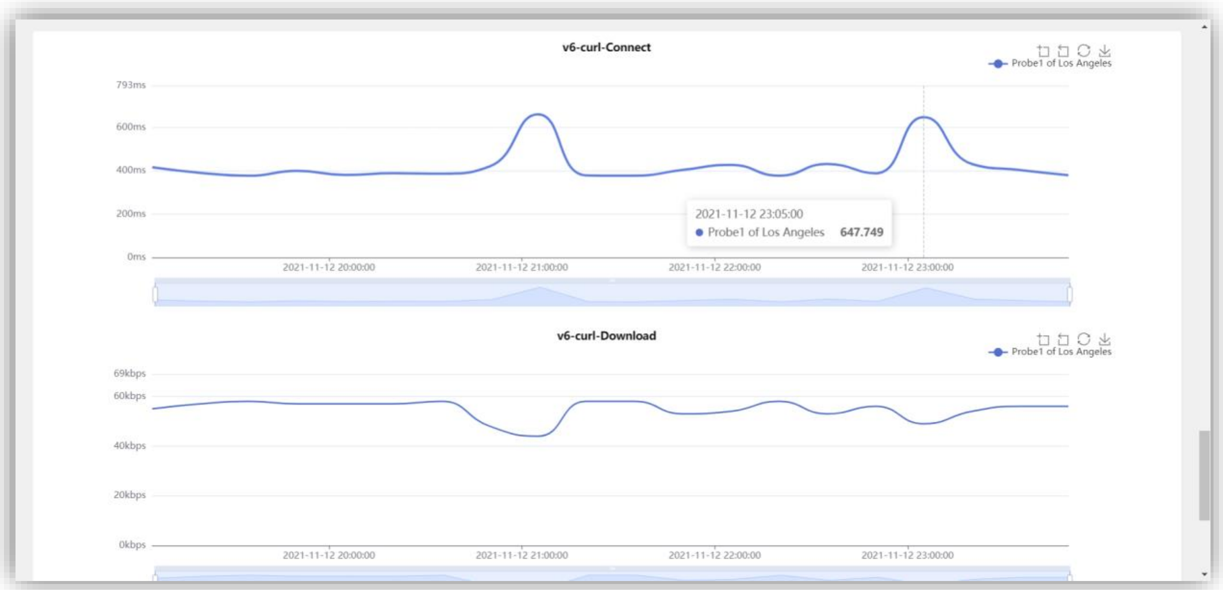




Result details

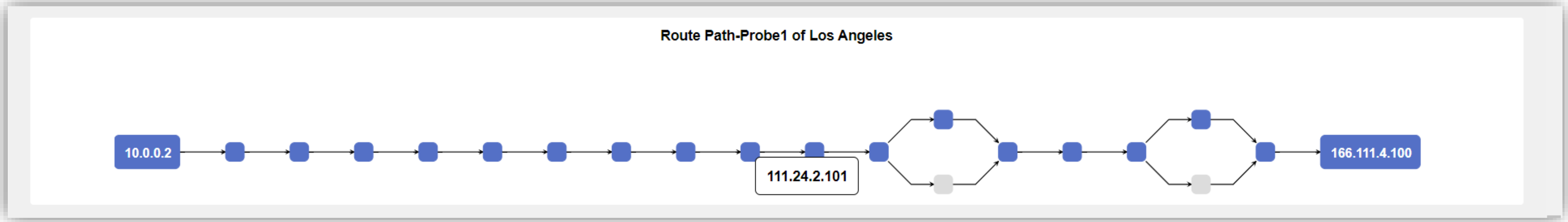
c) Http connection establishment time and download speed of ‘***curl***’ command (IPv4 & IPv6)





Result details

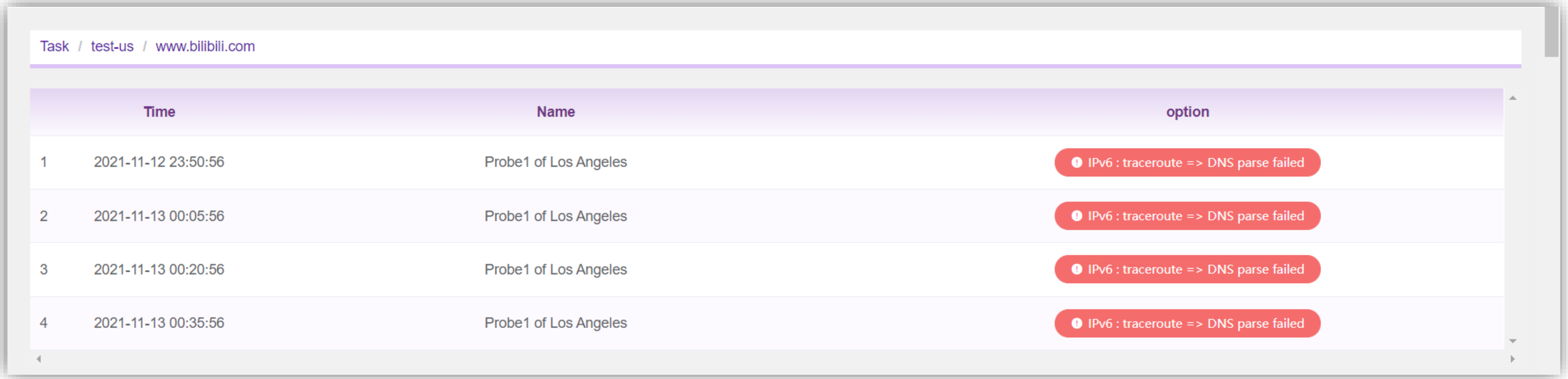
d) Traceroute topology result of ‘***traceroute***’ command (IPv4)



Route Path-Probe1 of Los Angeles

Result details

e) Alert information which is used to record errors occurred during the detection process



Task / test-us / www.bilibili.com

	Time	Name	option
1	2021-11-12 23:50:56	Probe1 of Los Angeles	IPv6 : traceroute => DNS parse failed
2	2021-11-13 00:05:56	Probe1 of Los Angeles	IPv6 : traceroute => DNS parse failed
3	2021-11-13 00:20:56	Probe1 of Los Angeles	IPv6 : traceroute => DNS parse failed
4	2021-11-13 00:35:56	Probe1 of Los Angeles	IPv6 : traceroute => DNS parse failed

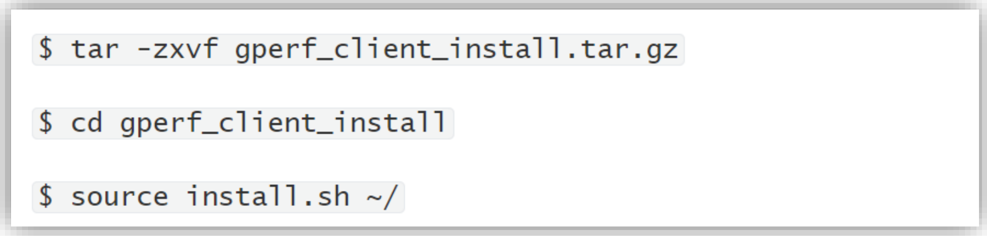
How to deploy your probe?

- The probe software can be installed in **Ubuntu & CentOS** hosts

- Following these simple steps:

① Download the install package from the website

② Install your probe

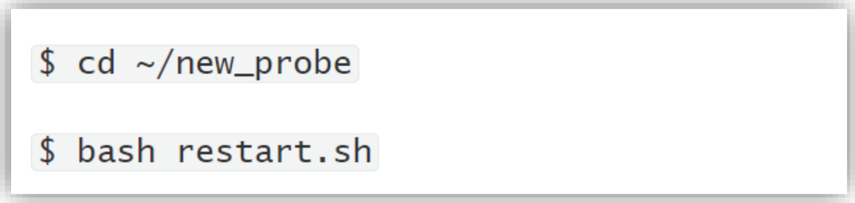


```
$ tar -zxvf gperf_client_install.tar.gz

$ cd gperf_client_install

$ source install.sh ~/
```

③ Run your probe

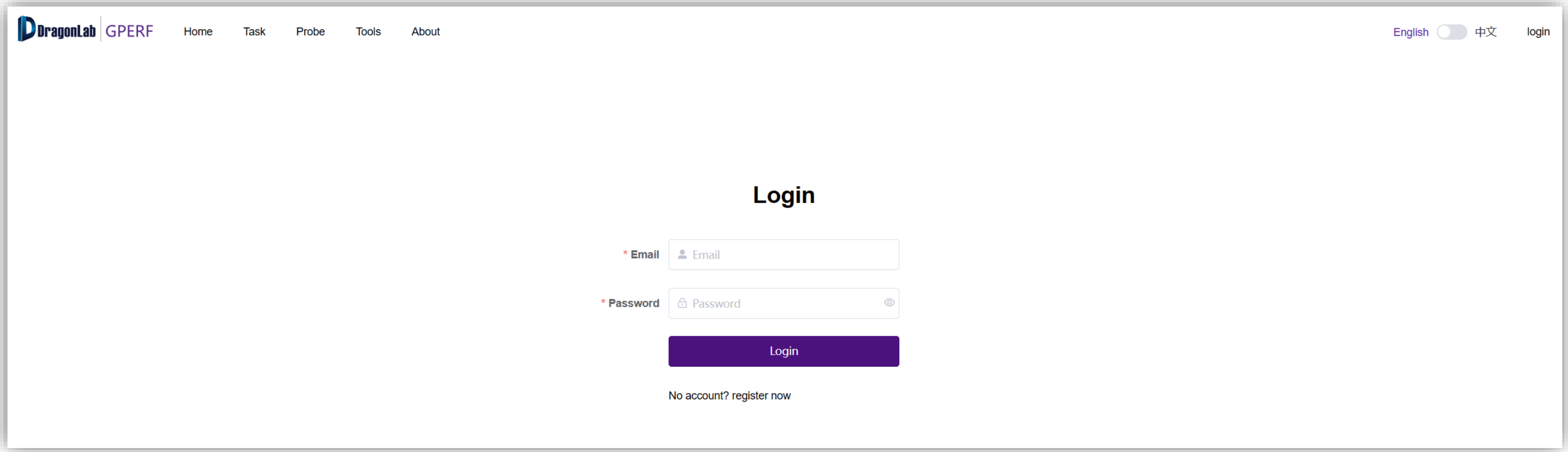


```
$ cd ~/new_probe

$ bash restart.sh
```

How to deploy your probe?

④ Login into your account



Login

* Email: Email

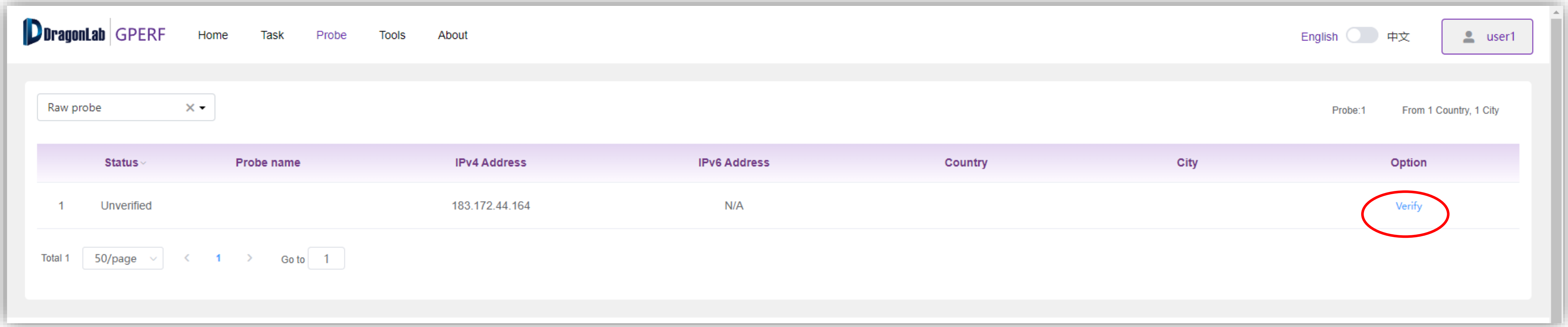
* Password: Password

Login

No account? register now

How to deploy your probe?

⑤ Verify your probe and enter its information



Raw probe

Probe:1 From 1 Country, 1 City

	Status	Probe name	IPv4 Address	IPv6 Address	Country	City	Option
1	Unverified		183.172.44.164	N/A			Verify

Total 1 50/page 1 Go to 1

⑥ Finally you can see this probe in available probe list

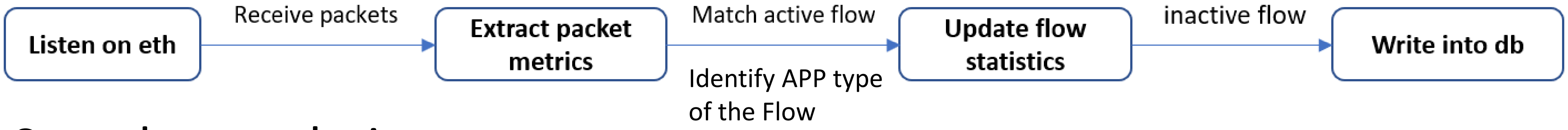
Future works

- Welcome more partners to join us
- Deploy more probes around the world
- Encourage participation through a reward mechanism

Passive Traffic Measurement—Flow Watch

Traffic Measurement System

- Workflow

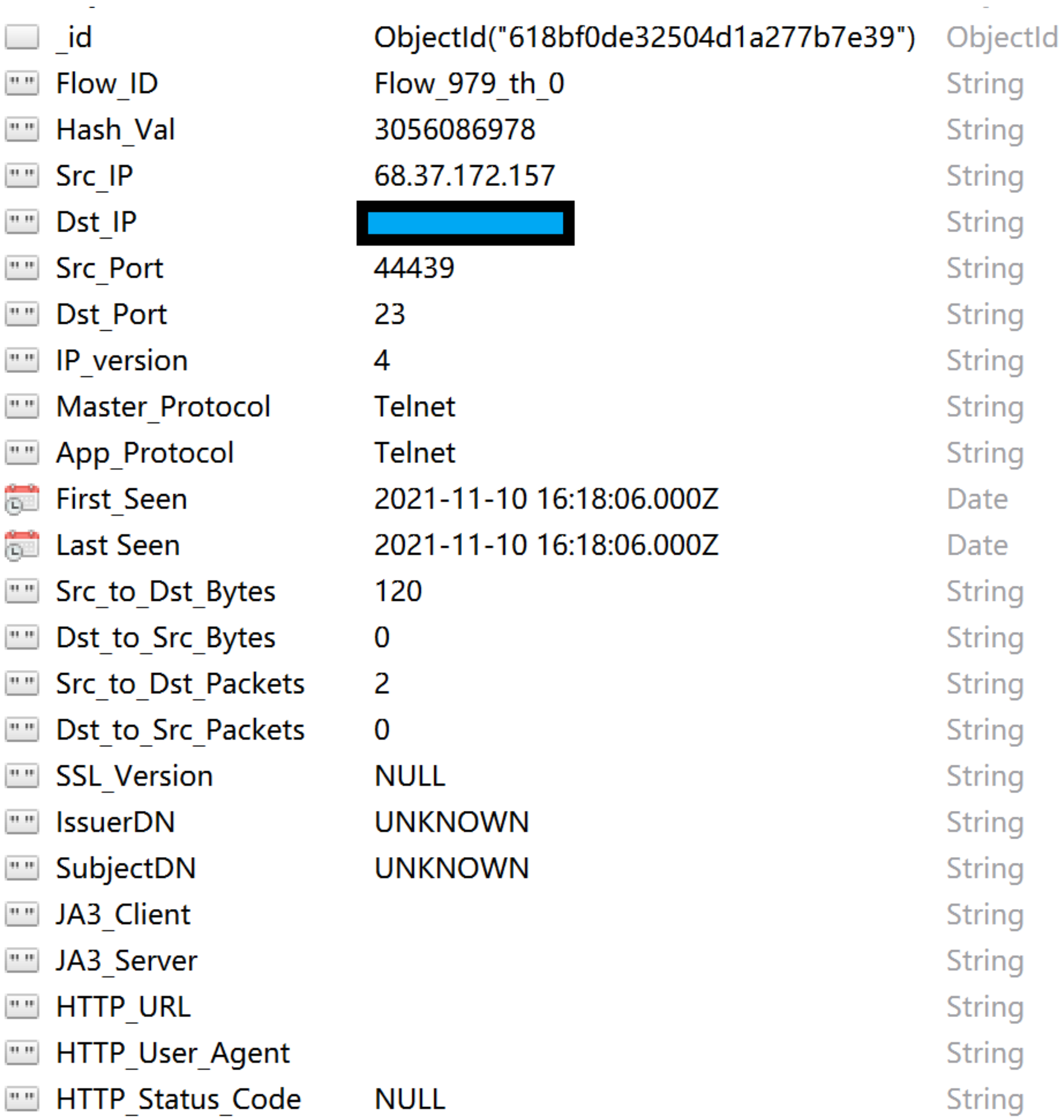


- Speed-up techniques
  - Each flow has a unique ID which is hashed with its five-tuple, so it’s fast to match the active flow that one packet belongs to
  - Use Aho-Corasick algorithm to match string pattern in the knowledge base
  - http://flowwatch.cgtf.net

Fields

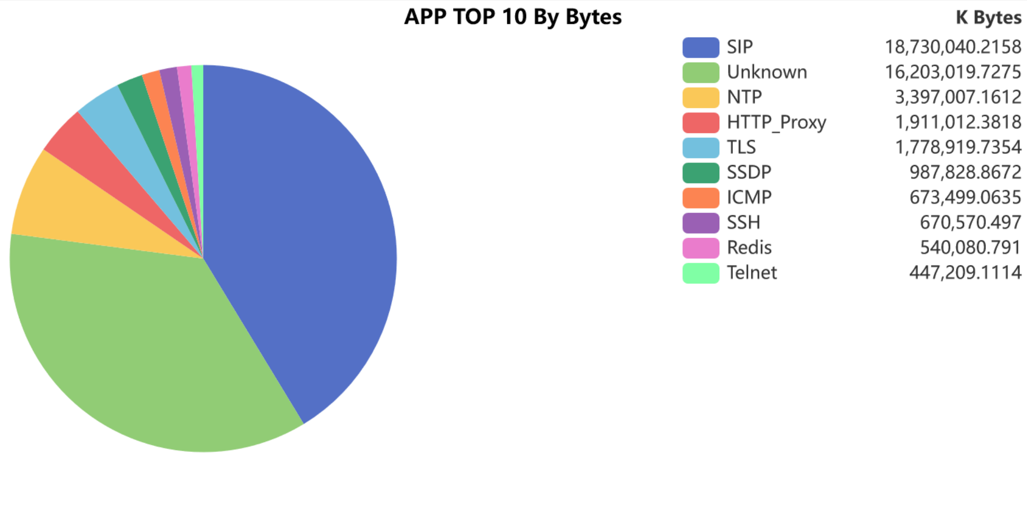
- Now we record 24 fields for each flow, including IP address, port, time, amount of transmitted data, protocol & application, and specific details about SSL and HTTP (if used).

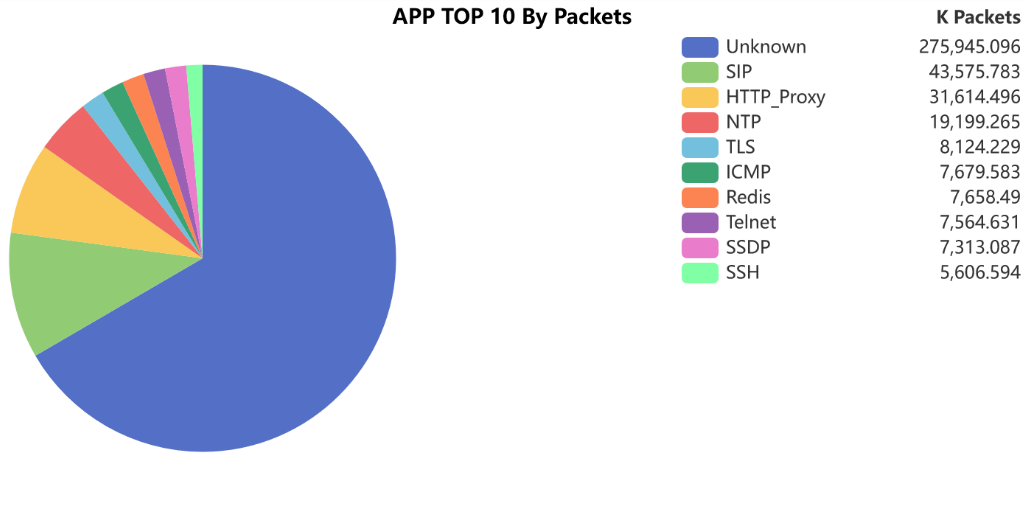
- SSL: version, certificate issuer and subject
- HTTP: user agent, URL and status code
- Can be expanded according to actual demand

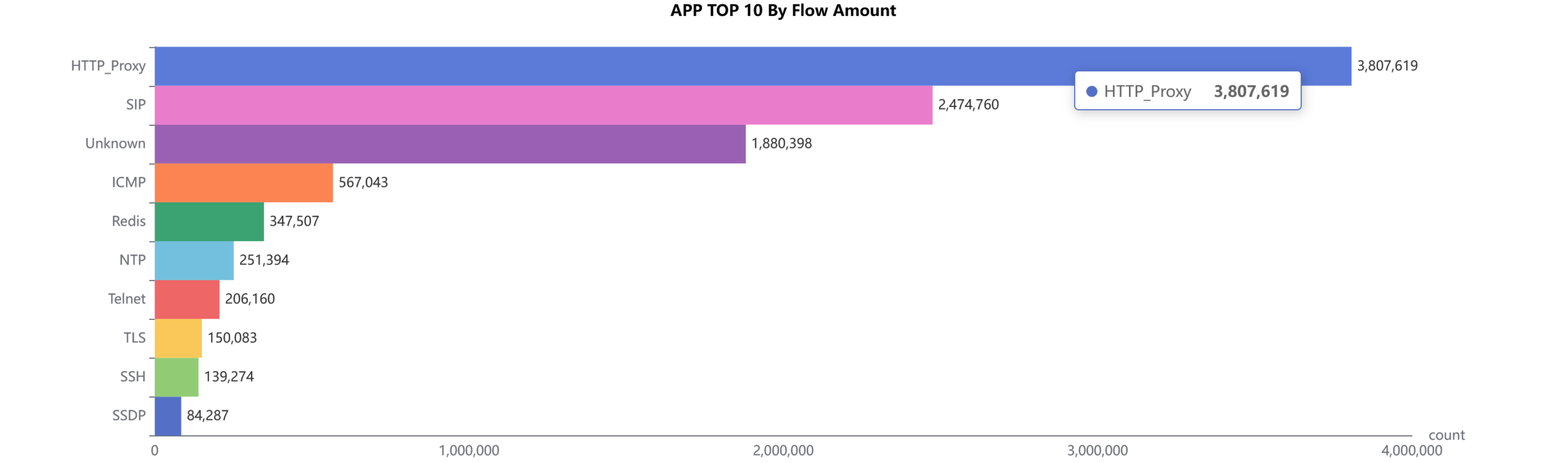


_id	ObjectId("618bf0de32504d1a277b7e39")	ObjectId
Flow_ID	Flow_979_th_0	String
Hash_Val	3056086978	String
Src_IP	68.37.172.157	String
Dst_IP	[redacted]	String
Src_Port	44439	String
Dst_Port	23	String
IP_version	4	String
Master_Protocol	Telnet	String
App_Protocol	Telnet	String
First_Seen	2021-11-10 16:18:06.000Z	Date
Last Seen	2021-11-10 16:18:06.000Z	Date
Src_to_Dst_Bytes	120	String
Dst_to_Src_Bytes	0	String
Src_to_Dst_Packets	2	String
Dst_to_Src_Packets	0	String
SSL_Version	NULL	String
IssuerDN	UNKNOWN	String
SubjectDN	UNKNOWN	String
JA3_Client		String
JA3_Server		String
HTTP_URL		String
HTTP_User_Agent		String
HTTP_Status_Code	NULL	String

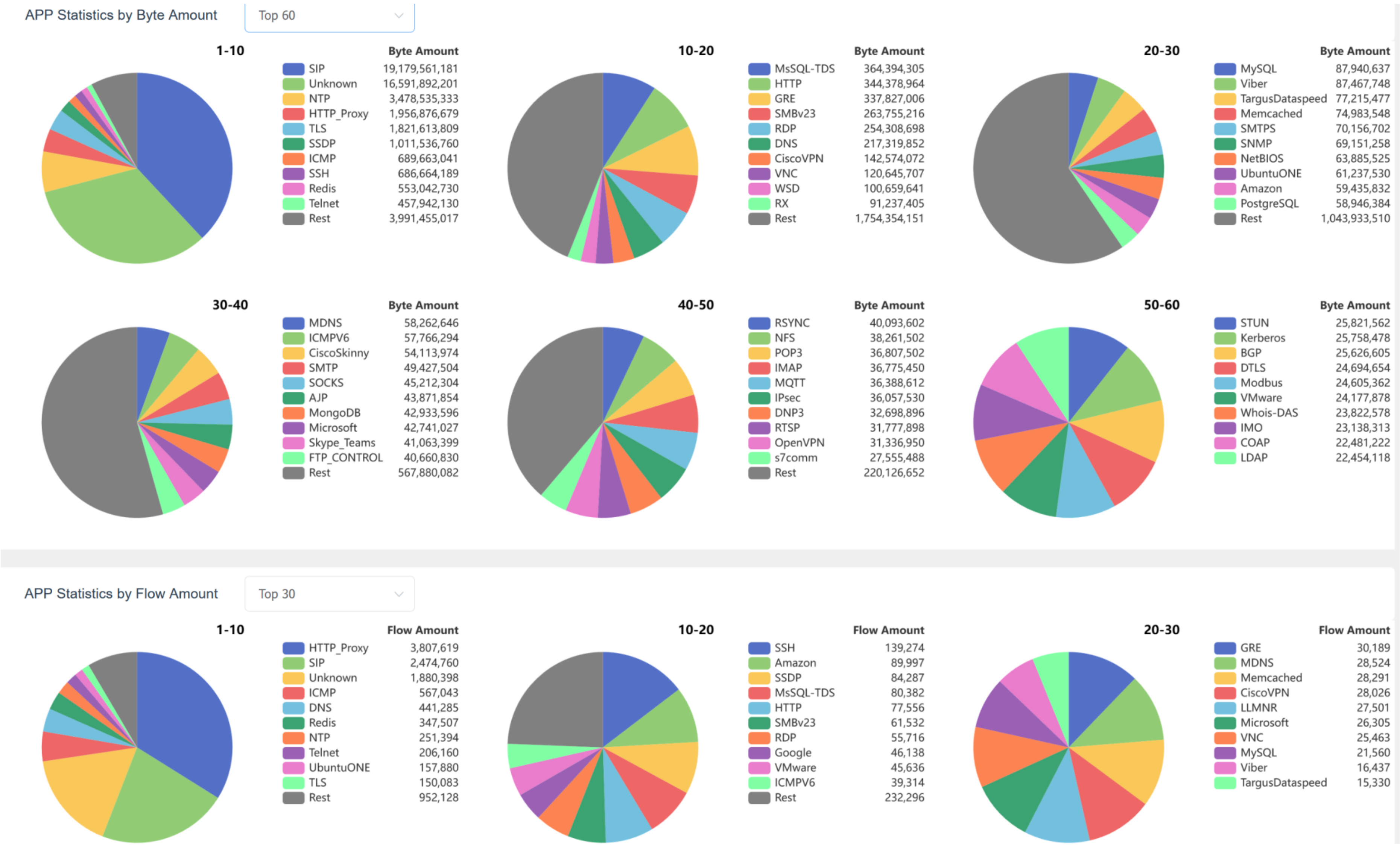
TOP 10 APP


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

1-10	Byte Amount
SIP	19,179,561,181
Unknown	16,591,892,201
NTP	3,478,535,333
HTTP_Proxy	1,956,876,679
TLS	1,821,613,809
SSDP	1,011,536,760
ICMP	689,663,041
SSH	686,664,189
Redis	553,042,730
Telnet	457,942,130
Rest	3,991,455,017

10-20	Byte Amount
MsSQL-TDS	364,394,305
HTTP	344,378,964
GRE	337,827,006
SMBv23	263,755,216
RDP	254,308,698
DNS	217,319,852
CiscoVPN	142,574,072
VNC	120,645,707
WSD	100,659,641
RX	91,237,405
Rest	1,754,354,151

20-30	Byte Amount
MySQL	87,940,637
Viber	87,467,748
TargusDataspeed	77,215,477
Memcached	74,983,548
SMTPS	70,156,702
SNMP	69,151,258
NetBIOS	63,885,525
UbuntuONE	61,237,530
Amazon	59,435,832
PostgreSQL	58,946,384
Rest	1,043,933,510

30-40	Byte Amount
MDNS	58,262,646
ICMPV6	57,766,294
CiscoSkinny	54,113,974
SMTP	49,427,504
SOCKS	45,212,304
AJP	43,871,854
MongoDB	42,933,596
Microsoft	42,741,027
Skype_Teams	41,063,399
FTP_CONTROL	40,660,830
Rest	567,880,082

40-50	Byte Amount
RSYNC	40,093,602
NFS	38,261,502
POP3	36,807,502
IMAP	36,775,450
MQTT	36,388,612
IPsec	36,057,530
DNP3	32,698,896
RTSP	31,777,898
OpenVPN	31,336,950
s7comm	27,555,488
Rest	220,126,652

50-60	Byte Amount
STUN	25,821,562
Kerberos	25,758,478
BGP	25,626,605
DTLS	24,694,654
Modbus	24,605,362
VMware	24,177,878
Whois-DAS	23,822,578
IMO	23,138,313
COAP	22,481,222
LDAP	22,454,118

APP Statistics by Flow Amount

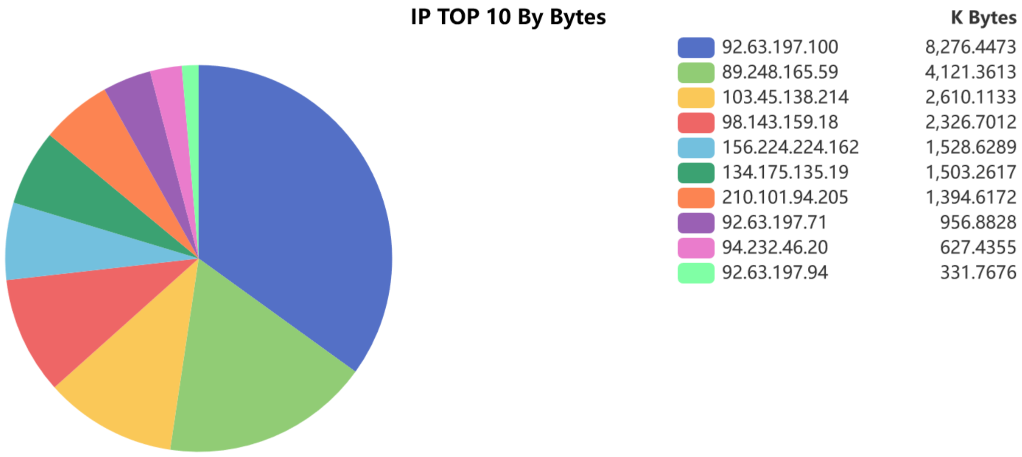
Top 30

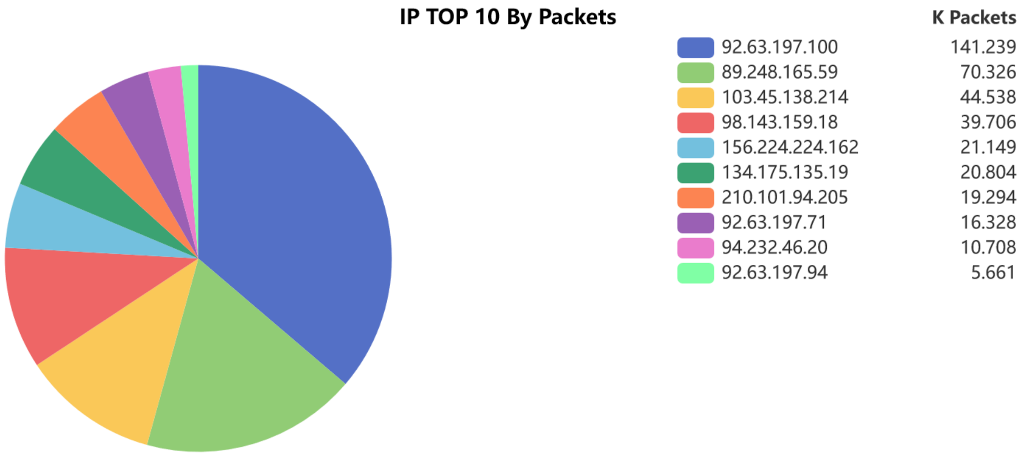
1-10	Flow Amount
HTTP_Proxy	3,807,619
SIP	2,474,760
Unknown	1,880,398
ICMP	567,043
DNS	441,285
Redis	347,507
NTP	251,394
Telnet	206,160
UbuntuONE	157,880
TLS	150,083
Rest	952,128

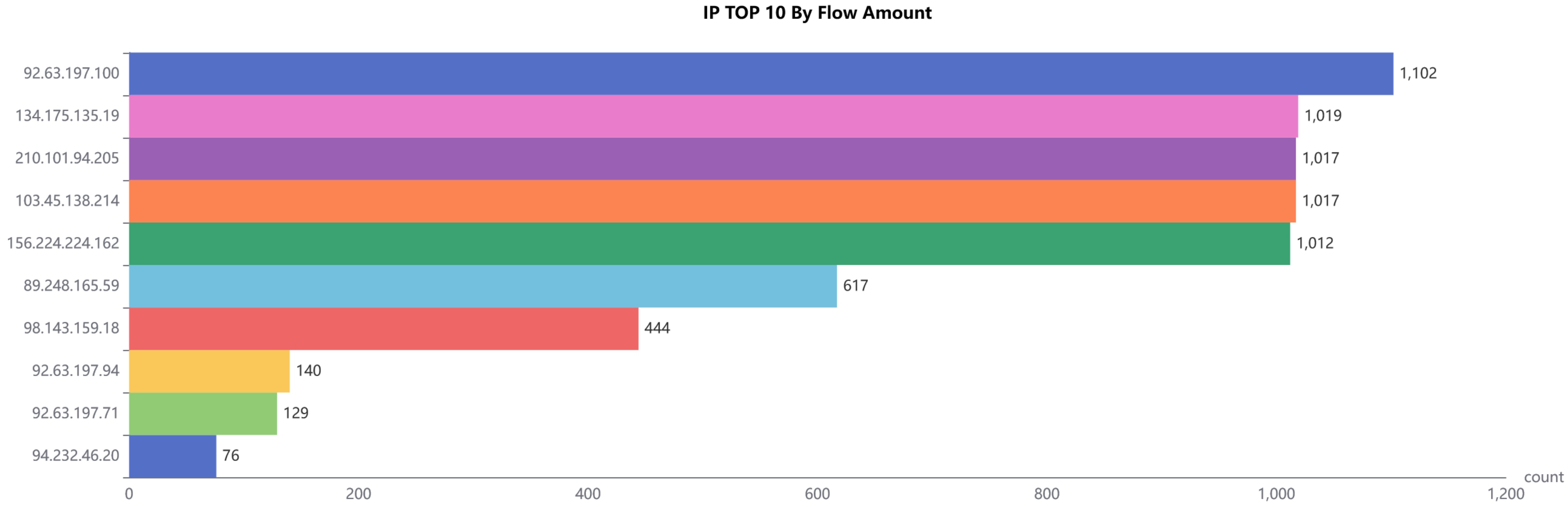
10-20	Flow Amount
SSH	139,274
Amazon	89,997
SSDP	84,287
MsSQL-TDS	80,382
HTTP	77,556
SMBv23	61,532
RDP	55,716
Google	46,138
VMware	45,636
ICMPV6	39,314
Rest	232,296

20-30	Flow Amount
GRE	30,189
MDNS	28,524
Memcached	28,291
CiscoVPN	28,026
LLMNR	27,501
Microsoft	26,305
VNC	25,463
MySQL	21,560
Viber	16,437
TargusDataspeed	15,330

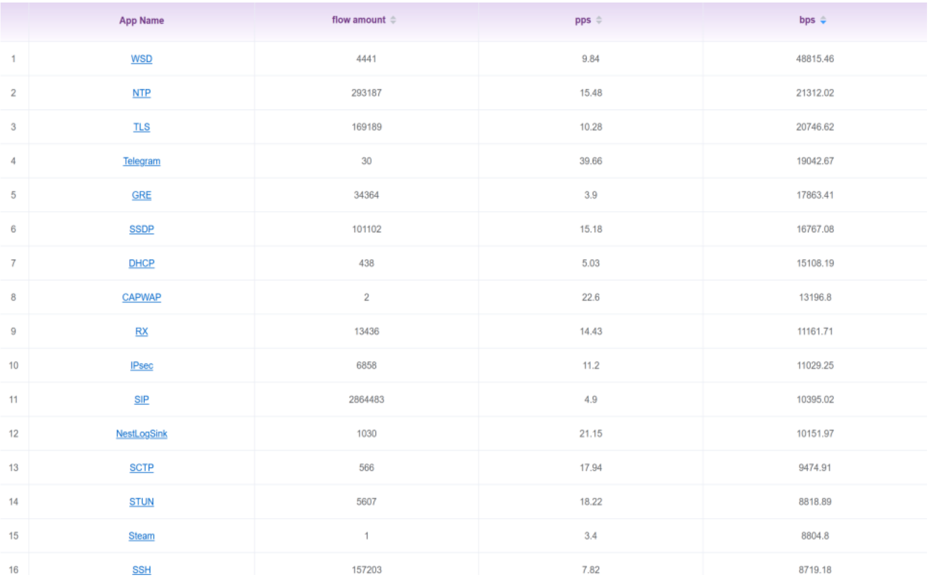
TOP 10 IP


IP TOP 10 By Bytes

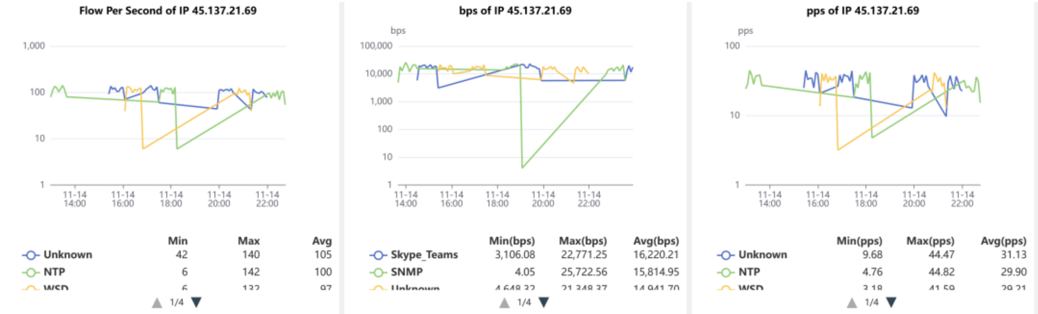

IP TOP 10 By Packets


IP TOP 10 By Flow Amount

Detail of APP, IP , FLOW



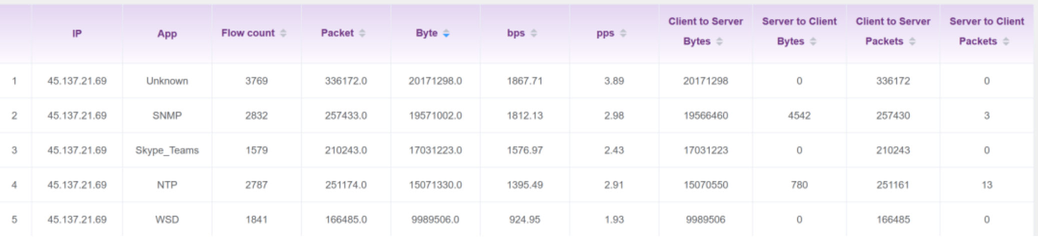
	App Name	flow amount	pps	bps
1	WSD	4441	9.84	48815.46
2	NTP	293187	15.48	21312.02
3	TLS	169189	10.28	20746.62
4	Telegram	30	39.66	19042.67
5	GRE	34364	3.9	17863.41
6	SSDP	101102	15.18	16767.08
7	DHCP	438	5.03	15108.19
8	CAPWAP	2	22.6	13196.8
9	RX	13436	14.43	11161.71
10	IPsec	6858	11.2	11029.25
11	SIP	2864483	4.9	10395.02
12	NestLogSink	1030	21.15	10151.97
13	SCTP	566	17.94	9474.91
14	STUN	5607	18.22	8818.89
15	Steam	1	3.4	8804.8
16	SSH	157203	7.82	8719.18



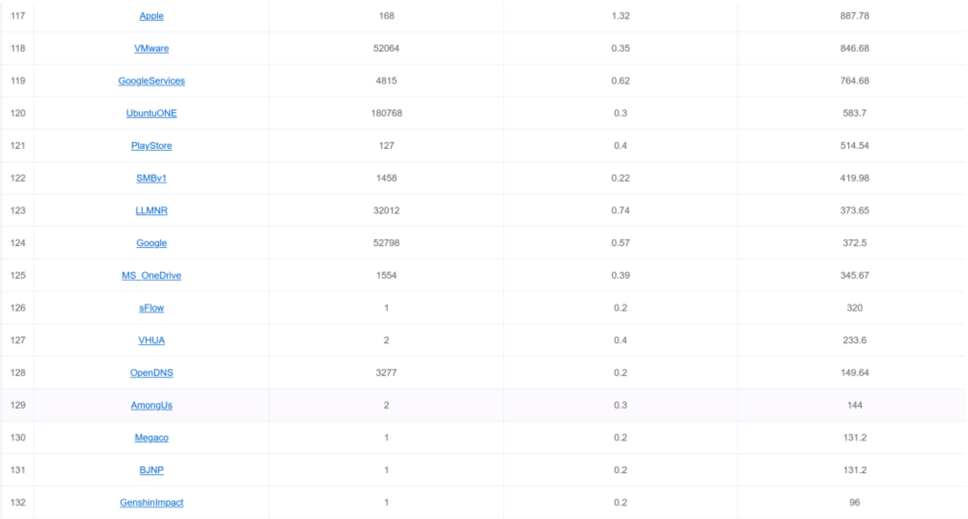
	Min	Max	Avg
Unknown	42	140	105
NTP	6	142	100
WSD	6	132	97

	Min(bps)	Max(bps)	Avg(bps)
Skype_Teams	3,106.08	22,771.25	16,220.21
SNMP	4.05	25,722.56	15,814.95
Unknown	4,648.32	21,348.37	14,941.70

	Min(pps)	Max(pps)	Avg(pps)
Unknown	9.68	44.47	31.13
NTP	4.76	44.82	29.90
WSD	3.18	41.59	29.21



	IP	App	Flow count	Packet	Byte	bps	pps	Client to Server Bytes	Server to Client Bytes	Client to Server Packets	Server to Client Packets
1	45.137.21.69	Unknown	3769	336172.0	20171298.0	1867.71	3.89	20171298	0	336172	0
2	45.137.21.69	SNMP	2832	257433.0	19571002.0	1812.13	2.98	19566460	4542	257430	3
3	45.137.21.69	Skype_Teams	1579	210243.0	17031223.0	1576.97	2.43	17031223	0	210243	0
4	45.137.21.69	NTP	2787	251174.0	15071330.0	1395.49	2.91	15070550	780	251161	13
5	45.137.21.69	WSD	1841	166485.0	9989506.0	924.95	1.93	9989506	0	166485	0

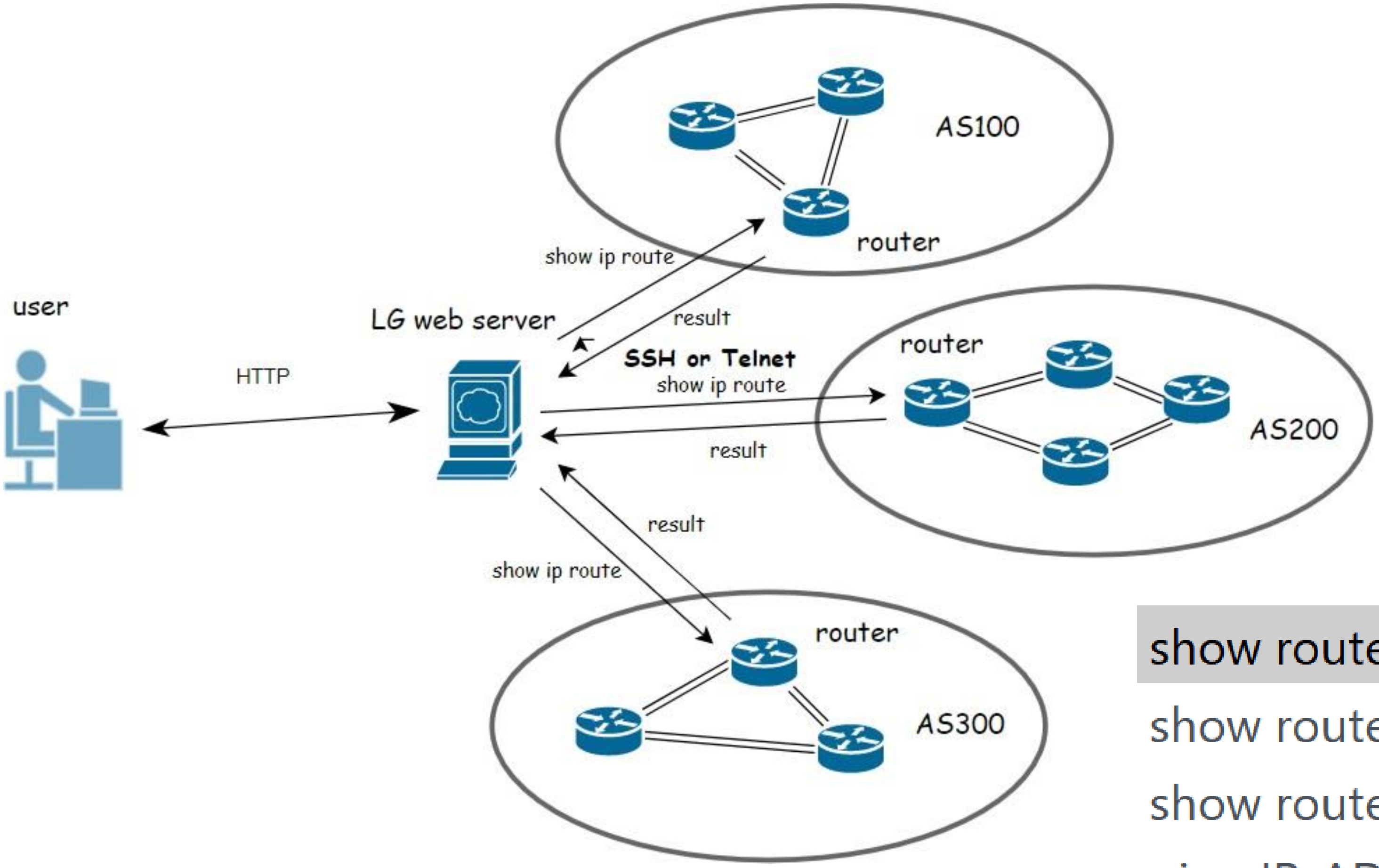


117	Apple	168	1.32	887.78
118	VMware	52064	0.35	846.68
119	GoogleServices	4815	0.62	764.68
120	UbuntuONE	180768	0.3	583.7
121	PlayStore	127	0.4	514.54
122	SMBv1	1458	0.22	419.98
123	LLMNR	32012	0.74	373.65
124	Google	52798	0.57	372.5
125	MS_OneDrive	1554	0.39	345.67
126	sFlow	1	0.2	320
127	VHUA	2	0.4	233.6
128	OpenDNS	3277	0.2	149.64
129	AmongUs	2	0.3	144
130	Megaco	1	0.2	131.2
131	BJNP	1	0.2	131.2
132	GenshinImpact	1	0.2	96

- Over 100 APP Identification
- Statistical analysis
- Detailed Flow Information

Network Looking Glass— CGTF LG

Looking Glass Architecture



show route IP_ADDRESS

show route as-path-regex AS_PATH_REGEX

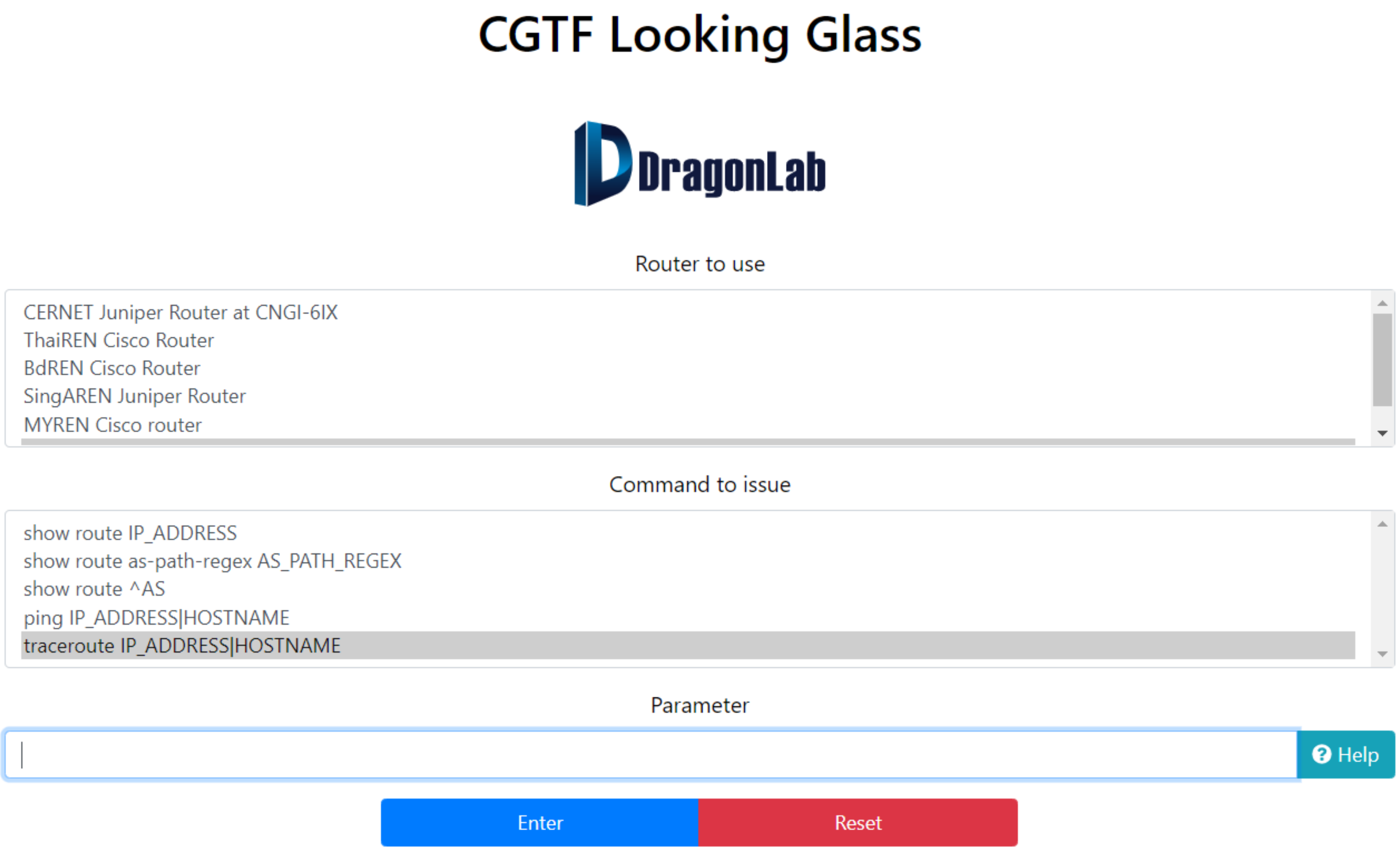
show route ^AS

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 routers
- 5 commands
- Query speed limit for security
- More partners is welcomed



CGTF Looking Glass

Router to use

CERNET Juniper Router at CNGI-6IX
ThaiREN Cisco Router
BdREN Cisco Router
SingAREN Juniper Router
MYREN Cisco router

Command to issue

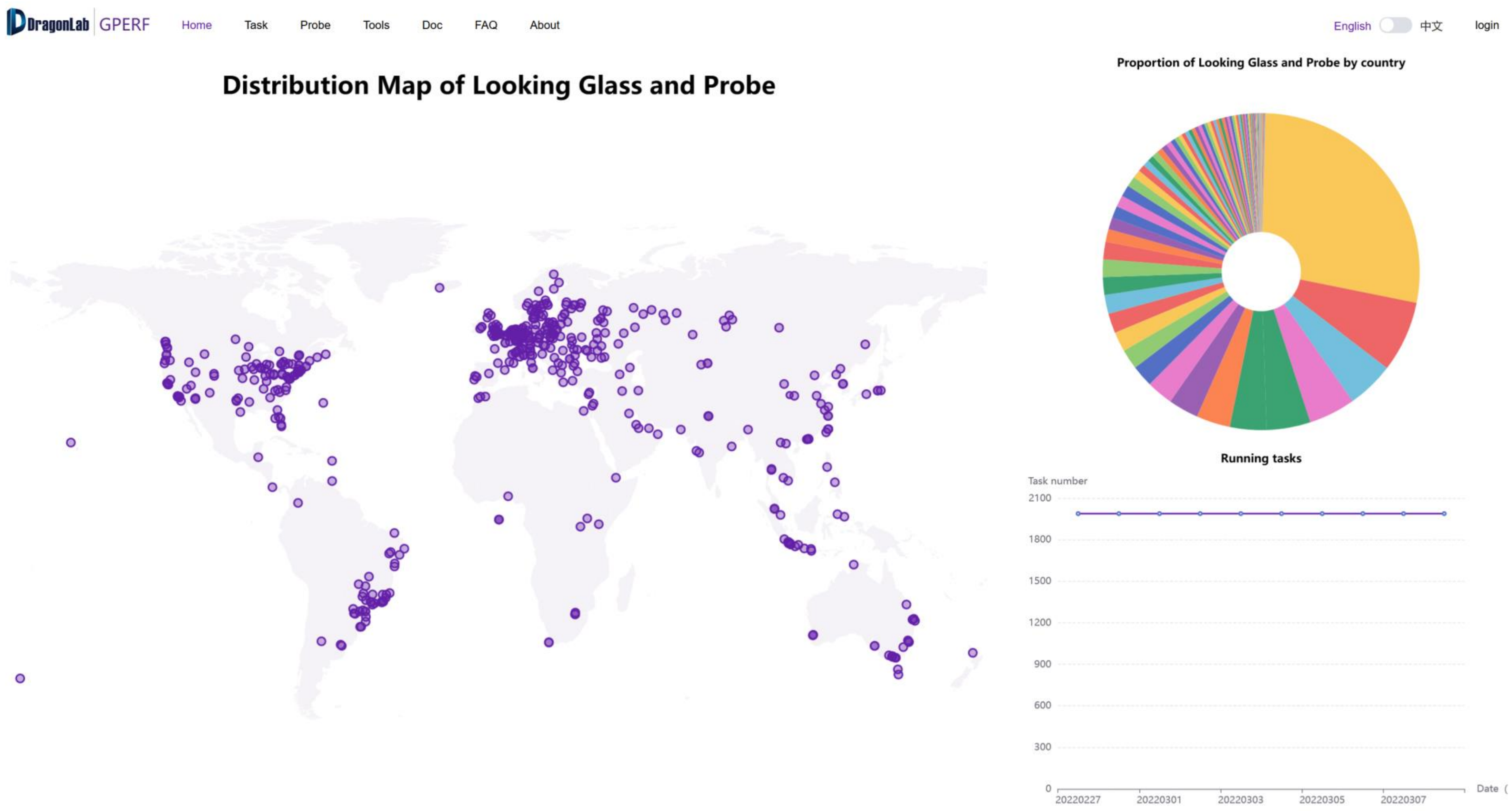
show route IP_ADDRESS
show route as-path-regex AS_PATH_REGEX
show route ^AS
ping IP_ADDRESS|HOSTNAME
traceroute IP_ADDRESS|HOSTNAME

Parameter

NRENs’ contribution:

CERNET, ThaiREN, BdREN, SingAREN, MYREN,LEARN

Our Work on LG

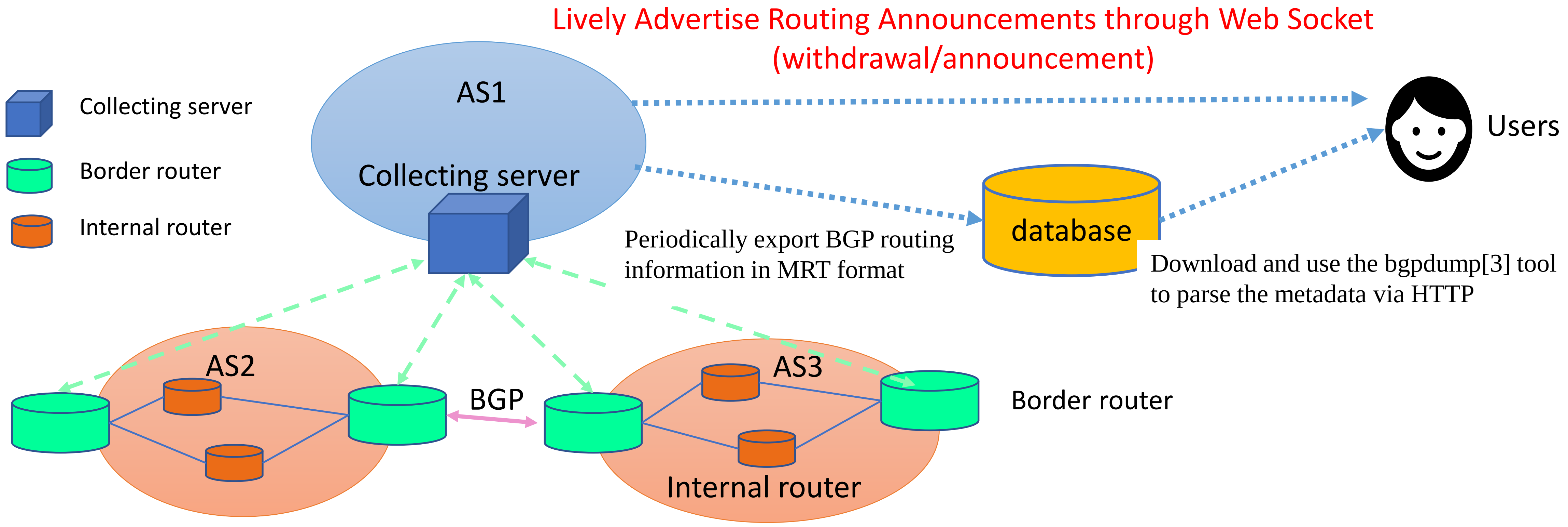


- Paper: “Discovering obscure looking glass sites on the web to facilitate internet measurement research”——CoNEXT’21
- 3814 LGs

BGP Routing Sharing — CGTF RIS

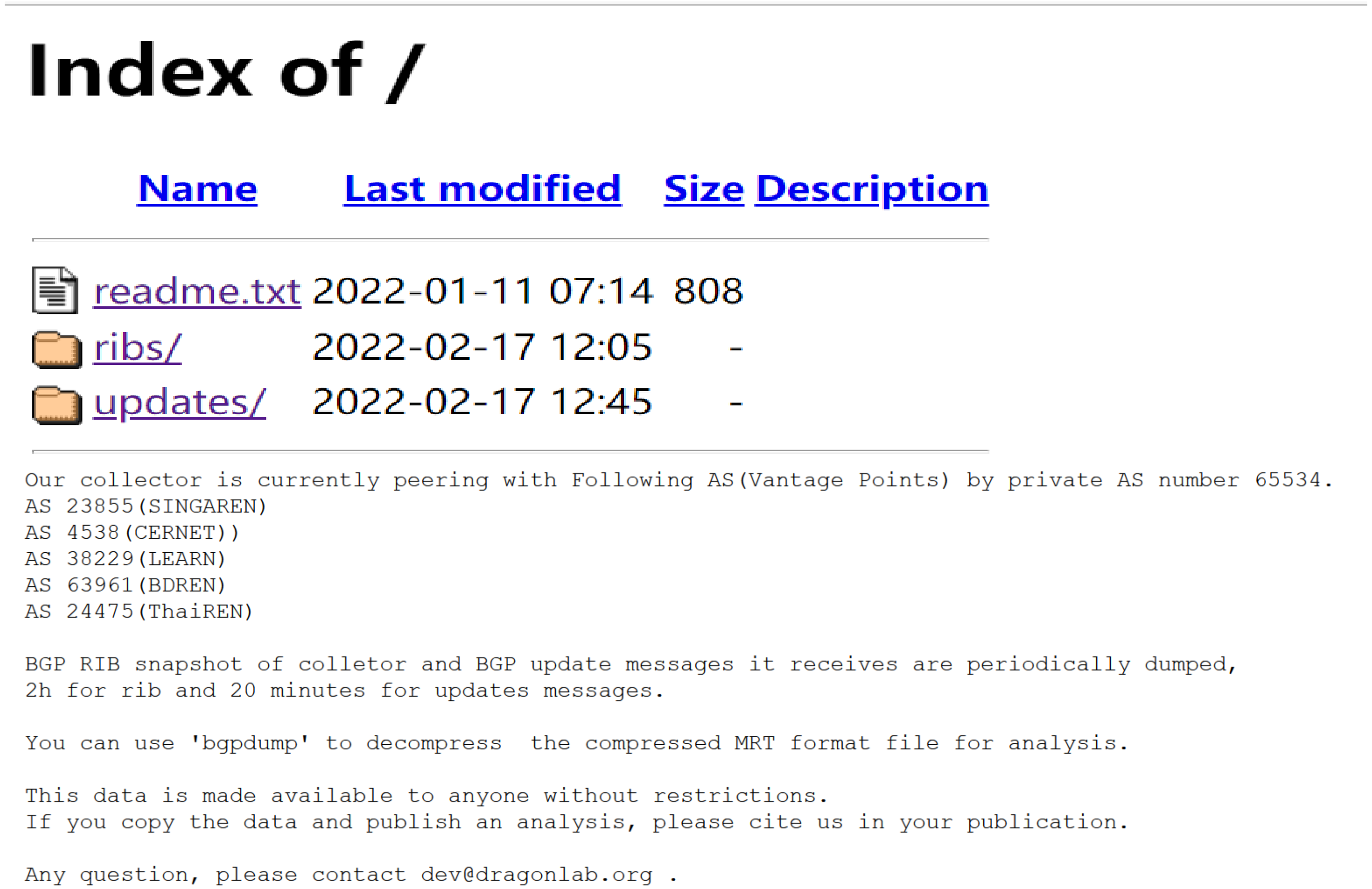
BGP Routing Sharing

- 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



Lively Advertise Routing Announcements through Web Socket (withdrawal/announcement)
Collecting server
Border router
Internal router
AS1
Collecting server
Users
database
Periodically export BGP routing information in MRT format
Download and use the bgpdump[3] tool to parse the metadata via HTTP
AS2
AS3
BGP
Border router
Internal router

BGP Routing Collection 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 .
```

NRENs' Contribution:

- CERNET
- SingAREN
- BdREN
- LEARN
- ThaiREN

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

Benefit for partners

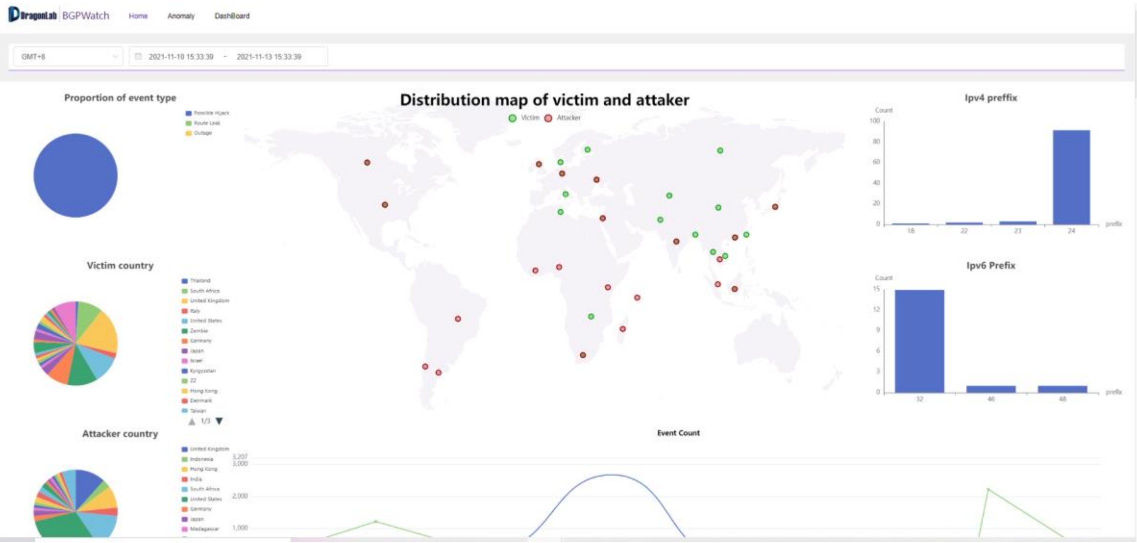
- **Partners can gain a better understanding of their network.**
- **Help to identify problems in partners’ network.**
- **Prompt research in Asia-Pacific Area.**

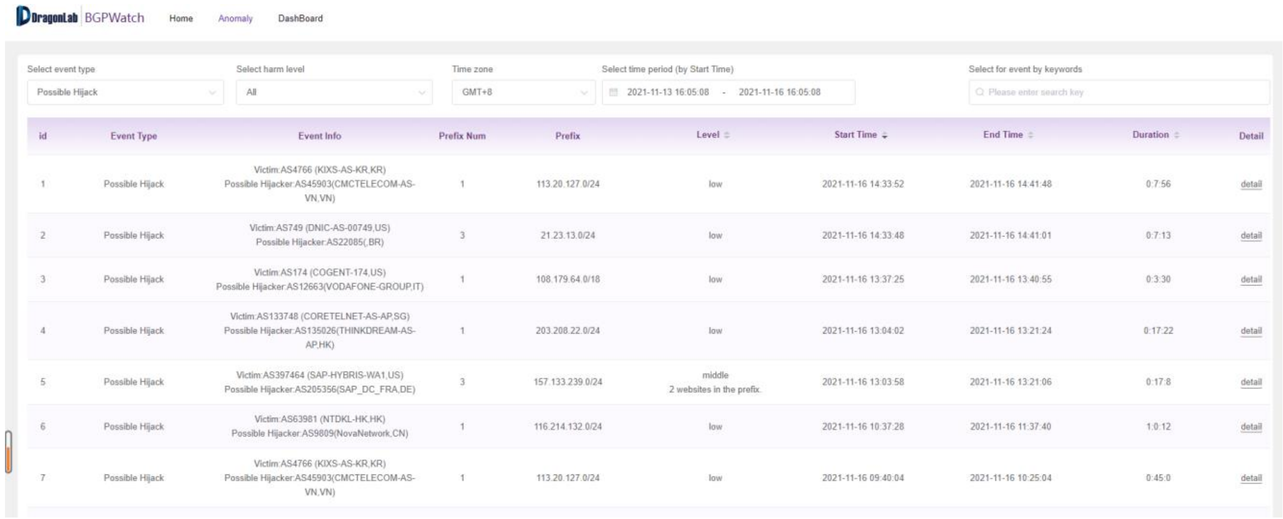
- Just have your border router **establish an eBGP session** with our collector（47.241.43.108）
- We have prepared a documentation which contains the configuration details

BGP Routing Monitoring and Analysis — BGP Watch

BGP Routing Monitoring and Analysis
--BGP Watch

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





Select event type: Possible Hijack

Select harm level: All

Time zone: GMT+8

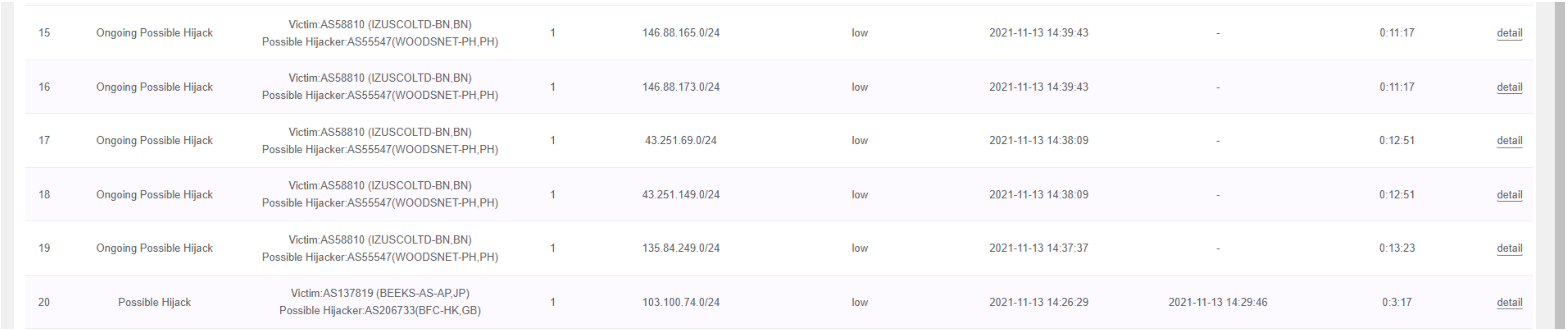
Select time period (by Start Time): 2021-11-13 16:05:08 - 2021-11-16 16:05:08

Select for event by keywords: Please enter search key

id	Event Type	Event Info	Prefix Num	Prefix	Level	Start Time	End Time	Duration	Detail
1	Possible Hijack	Victim:AS4766 (KIXS-AS-KR,KR) Possible Hijacker:AS45903(CMCTELECOM-AS-VN,VN)	1	113.20.127.0/24	low	2021-11-16 14:33:52	2021-11-16 14:41:48	0:7:56	detail
2	Possible Hijack	Victim:AS749 (DNIC-AS-00749,US) Possible Hijacker:AS22085(,BR)	3	21.23.13.0/24	low	2021-11-16 14:33:48	2021-11-16 14:41:01	0:7:13	detail
3	Possible Hijack	Victim:AS174 (COGENT-174,US) Possible Hijacker:AS12663(VODAFONE-GROUP,IT)	1	108.179.64.0/18	low	2021-11-16 13:37:25	2021-11-16 13:40:55	0:3:30	detail
4	Possible Hijack	Victim:AS133748 (CORETELNET-AS-AP,SG) Possible Hijacker:AS135026(THINKDREAM-AS-AP,HK)	1	203.208.22.0/24	low	2021-11-16 13:04:02	2021-11-16 13:21:24	0:17:22	detail
5	Possible Hijack	Victim:AS397464 (SAP-HYBRIS-WA1,US) Possible Hijacker:AS205356(SAP_DC_FRA,DE)	3	157.133.239.0/24	middle 2 websites in the prefix.	2021-11-16 13:03:58	2021-11-16 13:21:06	0:17:8	detail
6	Possible Hijack	Victim:AS63981 (NTDKL-HK,HK) Possible Hijacker:AS9809(NovaNetwork,CN)	1	116.214.132.0/24	low	2021-11-16 10:37:28	2021-11-16 11:37:40	1:0:12	detail
7	Possible Hijack	Victim:AS4766 (KIXS-AS-KR,KR) Possible Hijacker:AS45903(CMCTELECOM-AS-VN,VN)	1	113.20.127.0/24	low	2021-11-16 09:40:04	2021-11-16 10:25:04	0:45:0	detail

Features --- Real time

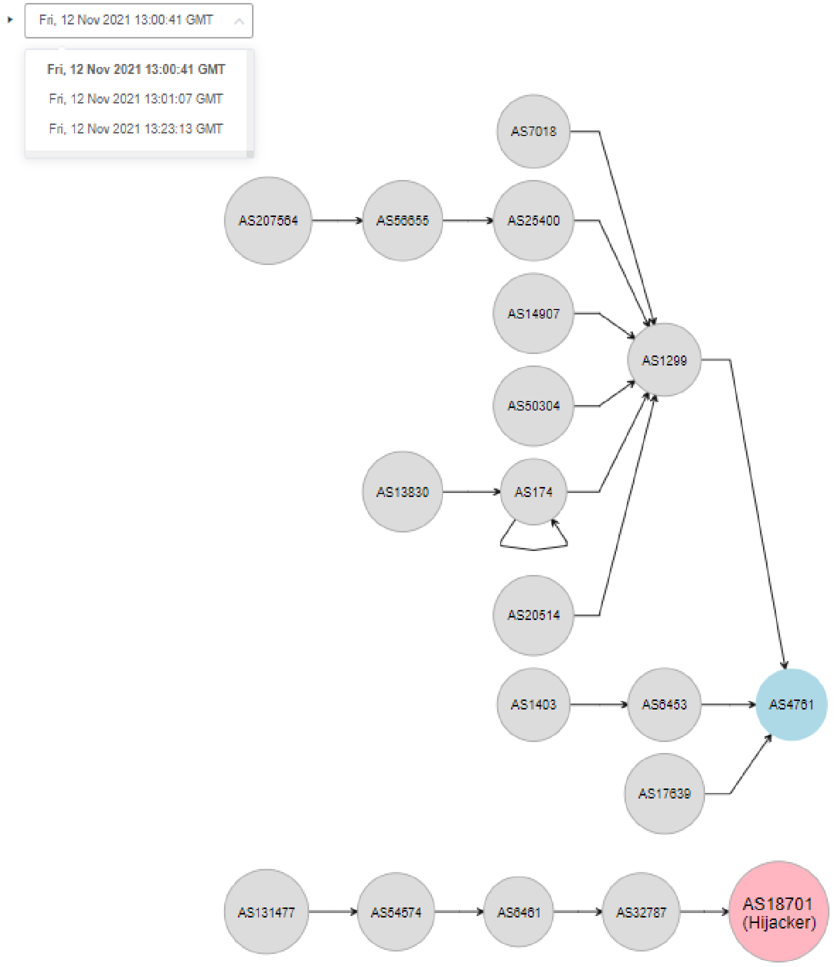
- About 5 mins delay, much better than other systems
- Notify immediately when an event is detected, minimizing damage from hijackings



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

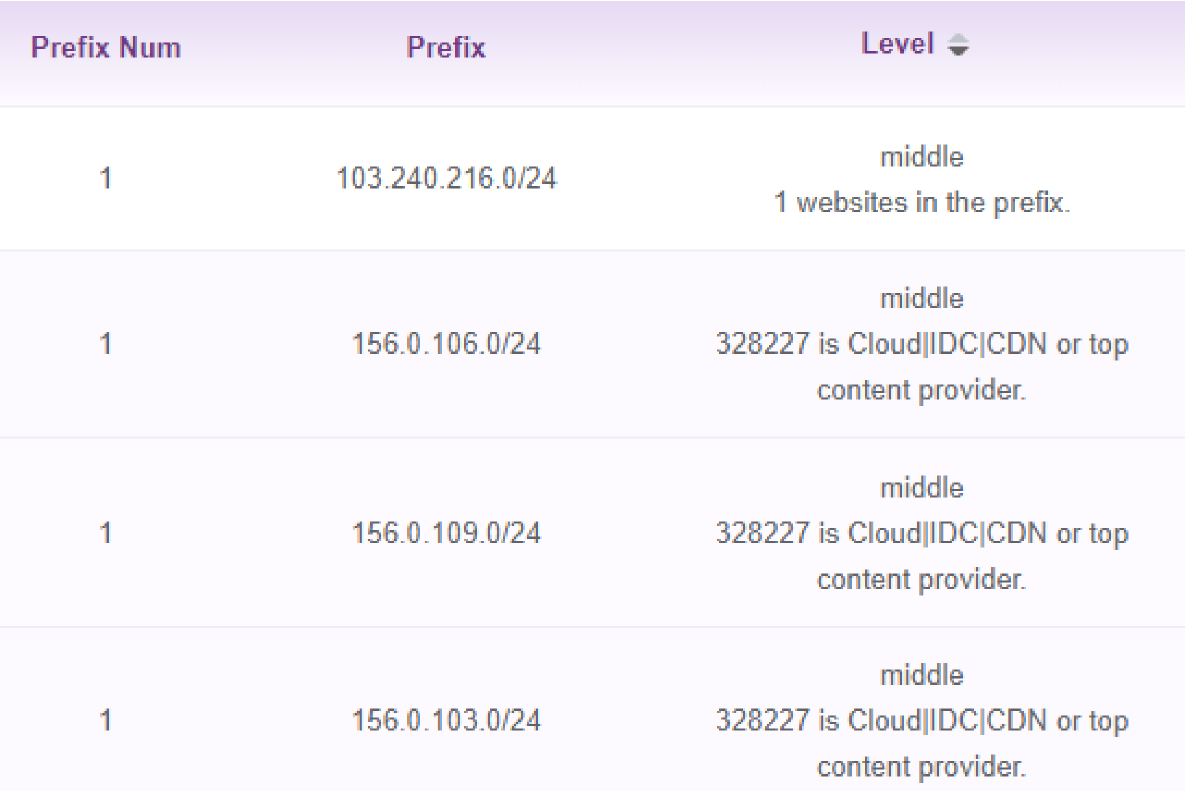
Features --- Event replay

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



Features --- Event level evaluation

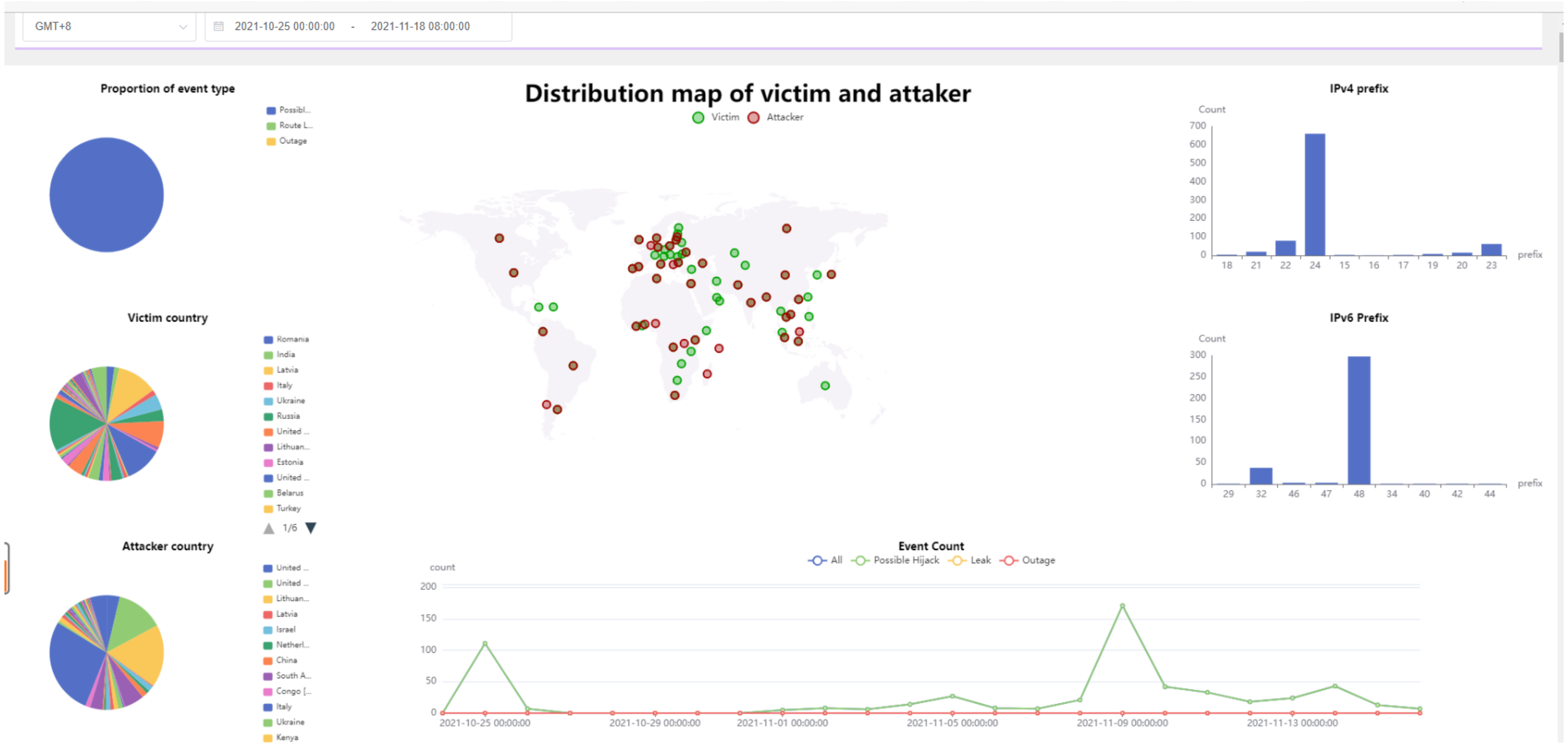
- **Evaluate event impact based on importance of AS and prefix.**



Prefix Num	Prefix	Level
1	103.240.216.0/24	middle 1 websites in the prefix.
1	156.0.106.0/24	middle 328227 is Cloud|IDC|CDN or top content provider.
1	156.0.109.0/24	middle 328227 is Cloud|IDC|CDN or top content provider.
1	156.0.103.0/24	middle 328227 is Cloud|IDC|CDN or top content provider.

Features --- Event Statistics Analysis

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

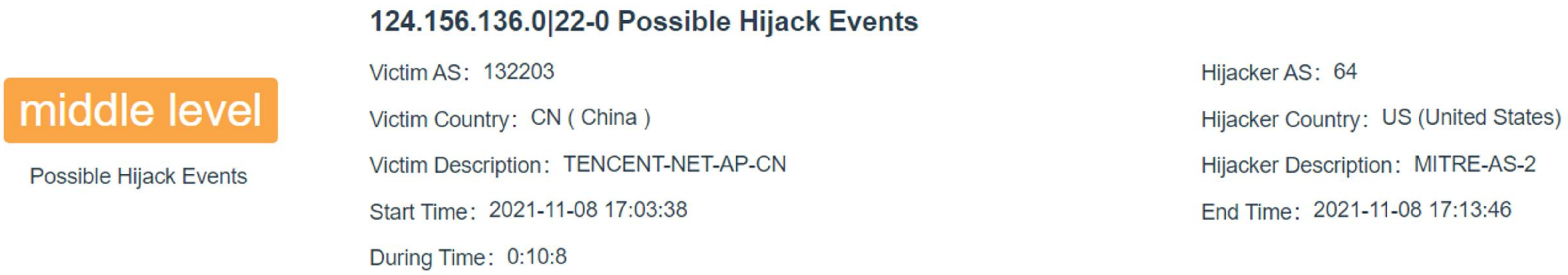


GMT+8

2021-10-25 00:00:00 - 2021-11-18 08:00:00

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	√	√	√

APNIC ISIF FUNDING PROGRAM

-- Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

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: 2022.2.1 - 2023.7.30 (tbc with APNIC Foundation)
- 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

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

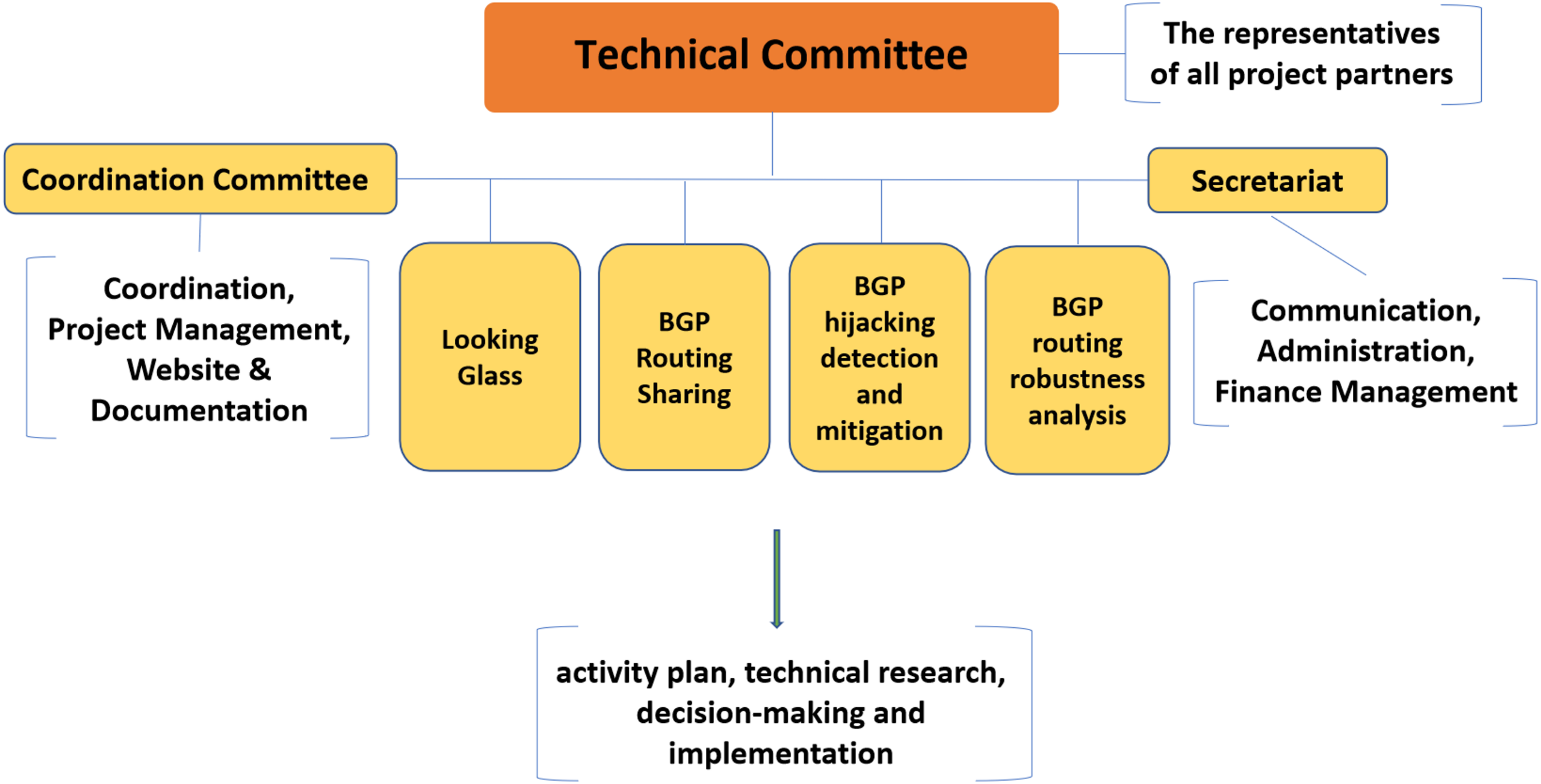
Project Team

- 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!

Governance and Collaboration



Technical Committee

The representatives of all project partners

Coordination Committee

Coordination, Project Management, Website & Documentation

Looking Glass

BGP Routing Sharing

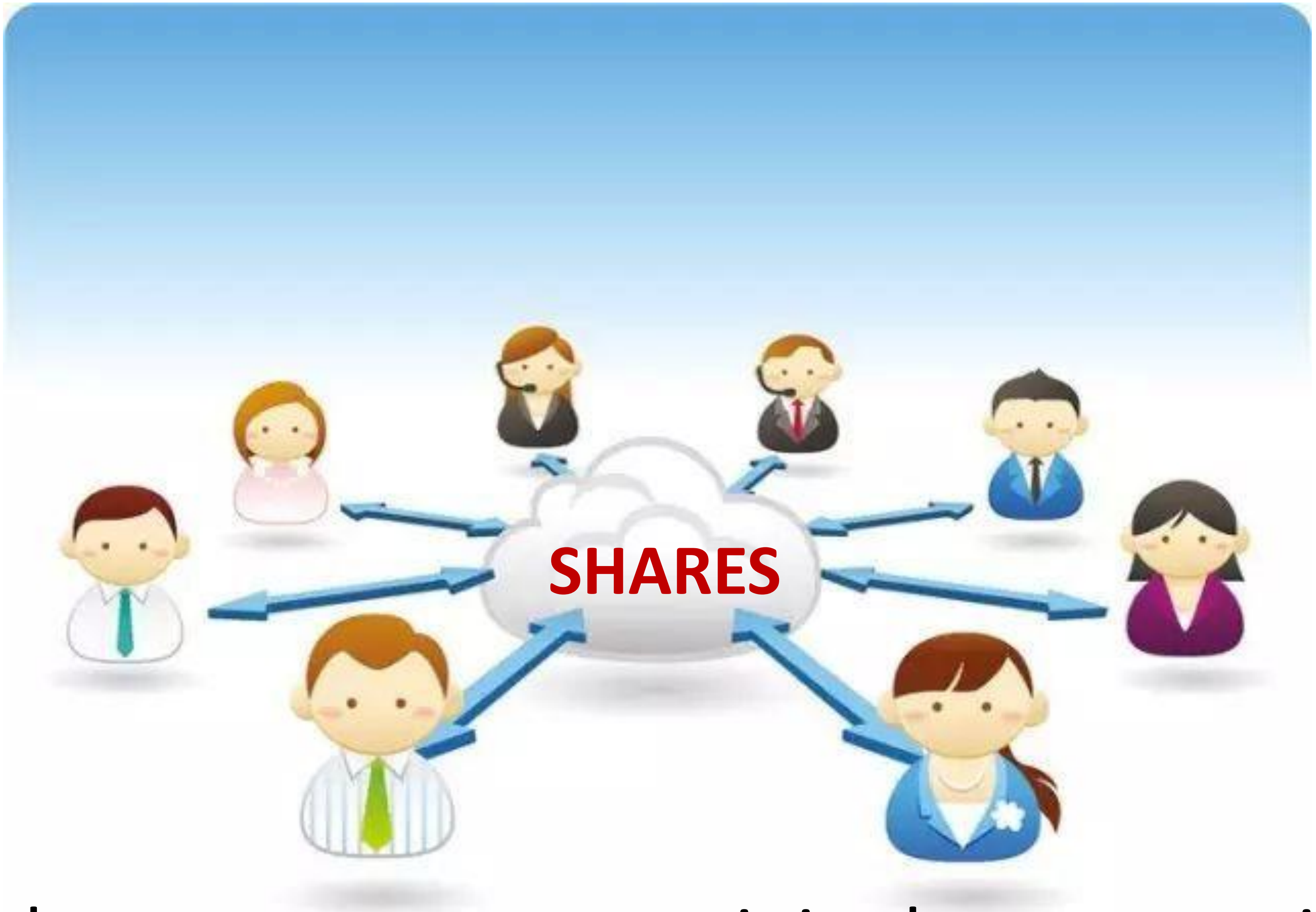
BGP hijacking detection and mitigation

BGP routing robustness analysis

Secretariat

Communication, Administration, Finance Management

activity plan, technical research, decision-making and implementation



Welcome more partners join the community

Contact us: acq@tsinghua.edu.cn