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

Content

- **Project Outline:Task & Expected Outcome**
- **Project Plan & Schedule**
- **Work Progress**
- **ISIF Asia Funding Application**

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

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

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

IPv6 International Inter-Network Threat Tracing

Online threat discovery, offline threat mining, retention traceability and controllable traceability

Active Measurement of Massive IPv6 Address Space

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

Passive Measurement in High-speed IPv6 Network

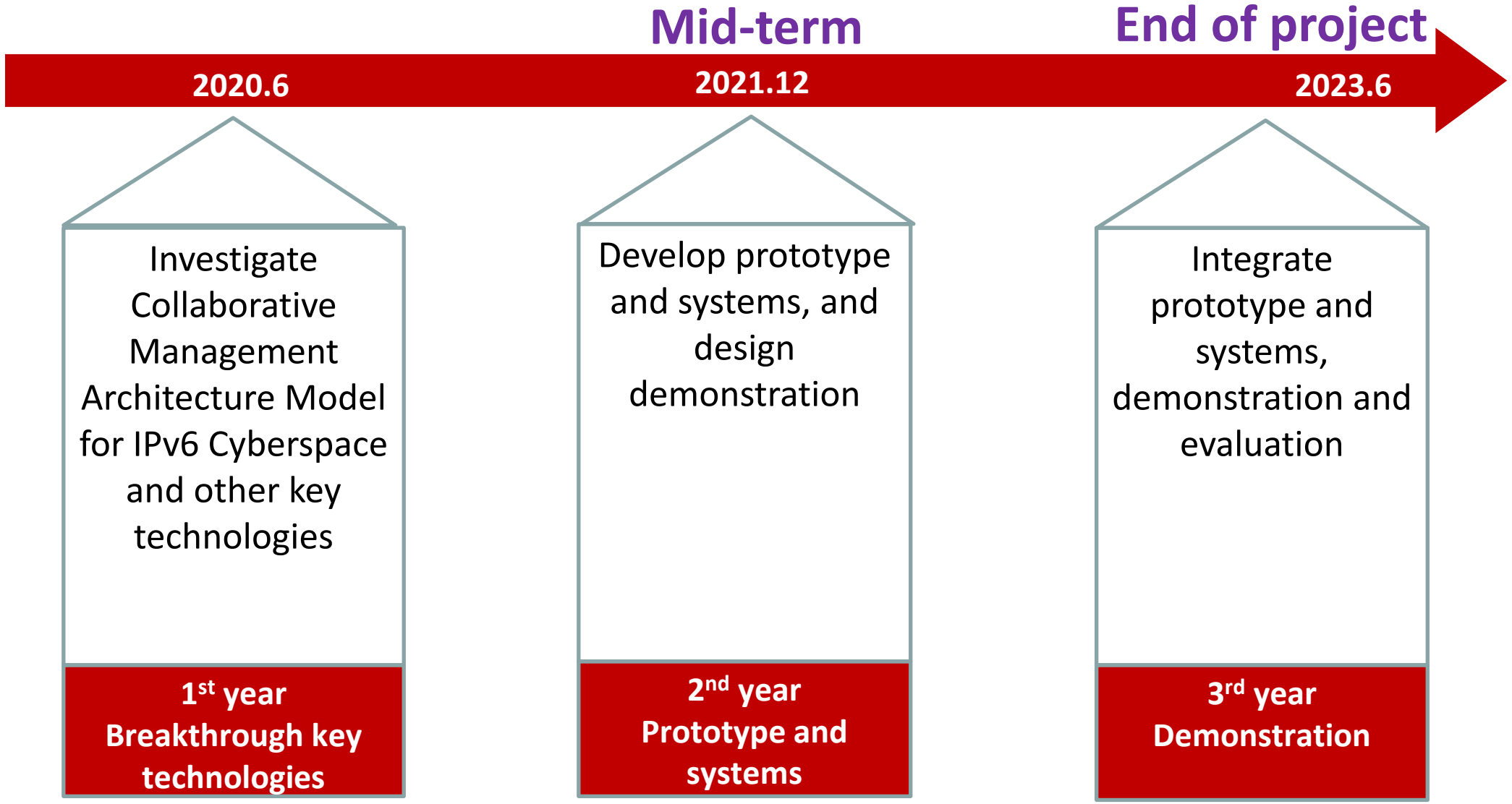
Encrypted traffic identification, VPN traffic identification and construction of Network Behavior Knowledge Base

New Rules for International Cooperative Governance on IPv6 Cyberspace

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

Key Technology → Governance Rule → Demonstration

Project Plan & Schedule



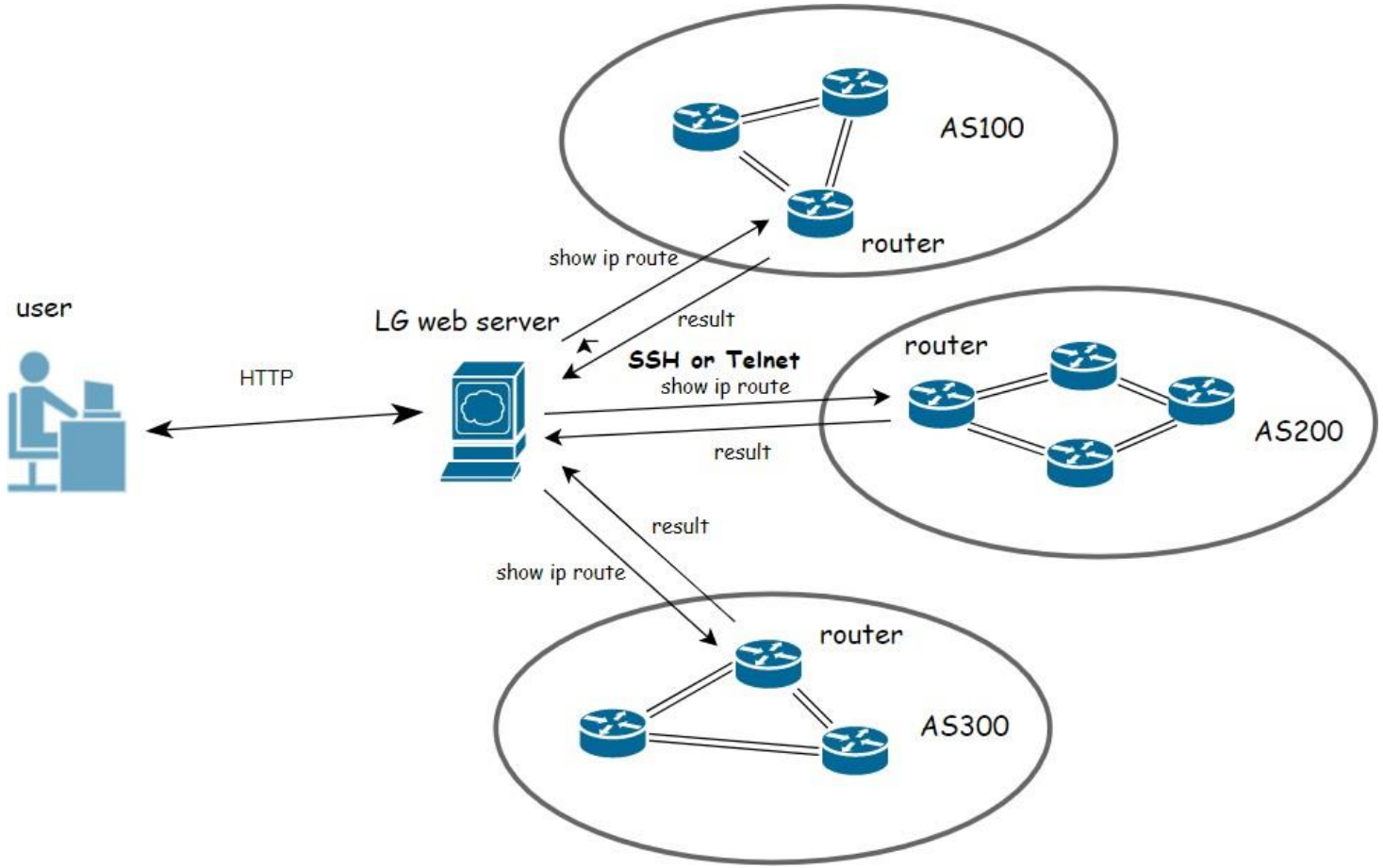
Work Progress

- Progress in the following aspect:
  - Looking Glass
  - BGP Routing Sharing
  - Active Probe
  - Network Telescope
  - Passive Measurement
  - Research on SRv6

Working Group

WGs / 参与单位	Passive measurement	IPv4/IPv6 network telescope	BGP routing sharing	Active Probe	Looking glass	IRCG
University of Gottingen德国						
Surrey University英国	√		√			
SingAREN新加坡GMT+8			√		√	
ThaiRen泰国GMT+7	√	√	√	√	√	√
MYREN马来西亚GMT+8			√		√	√
LEARN斯里兰卡GMT+5.5	√	√	√	√	√	√
NREN尼泊尔						
PALNREN巴基斯坦						
BDREN孟加拉国GMT+6	√	√	√	√	√	√
CAMREN柬埔寨						
AfgREN阿富汗GMT+4.5		√	√		√	√
Yangon University of computer study缅甸						
University of Malaya 马来西亚						√
Mae Fah Luang University,Thailand泰国						√

Looking Glass




```
ping <ip>
traceroute <ip>
show ip route <prefix>
show ip bgp summary
show ip bgp neighbors
show ip bgp <prefix>
```

Looking Glass

- You can access it at http://lg.cgtf.net
- Four partners has set up connection with it.

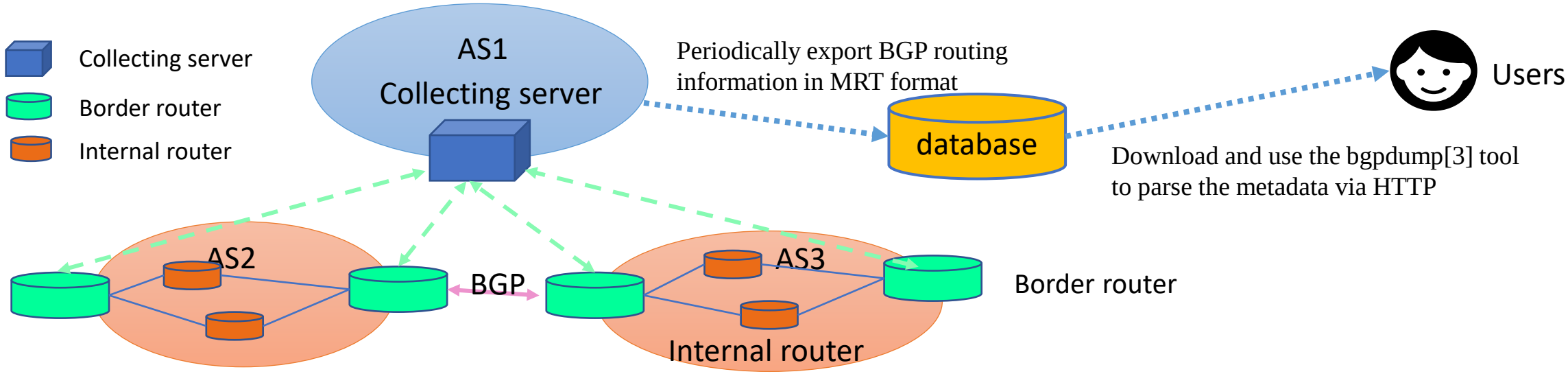
CGTF Looking Glass

Router to use

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

BGP Routing Sharing Architecture

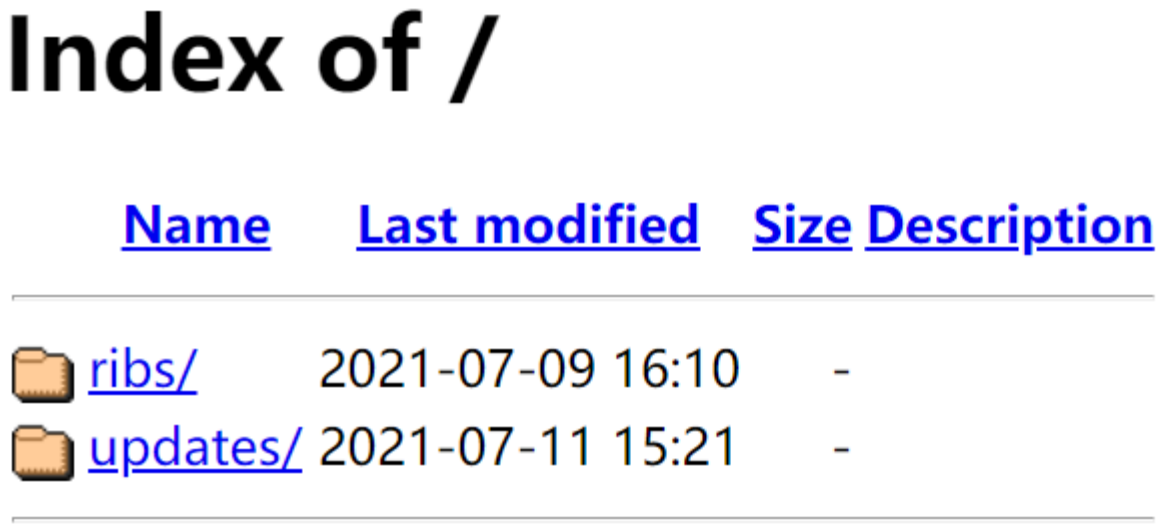
- Collecting server
  - Use routing software like Quagga[1] and FRR[2] to simulate a real BGP router
  - It is only used for routing information collection and avoids announcing or forwarding routing messages
- Deployment requirements for each network: border routers shall be connected to the server
- Two ways to set up the connection
  - BGP peers: exchange routing info over TCP connections
  - BMP protocol: send the routing info to the server



[1] Quagga, https://frrouting.org/, [2] FRR, https://frrouting.org/, [3] bgpdump. https://github.com/RIPE-NCC/bgpdump。

Our Deployment so far

- 1 Collector:47.241.43.108 （Running **FRR** ）
- 1 Vantage Point :203.91.121.206（**CERNET2** Juniper Router)
- Collected data on **http://bgp.cgtf.net**

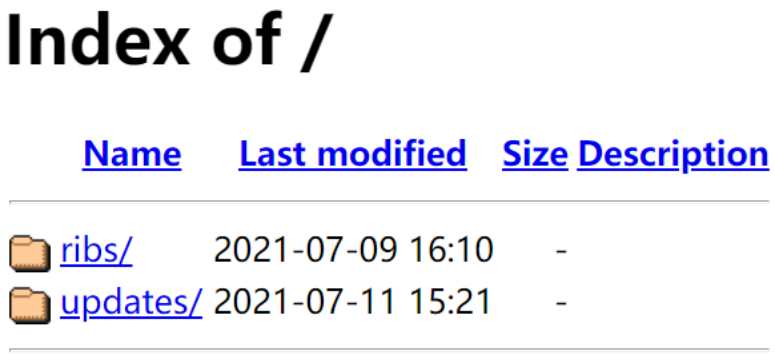


What partners need to do?

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

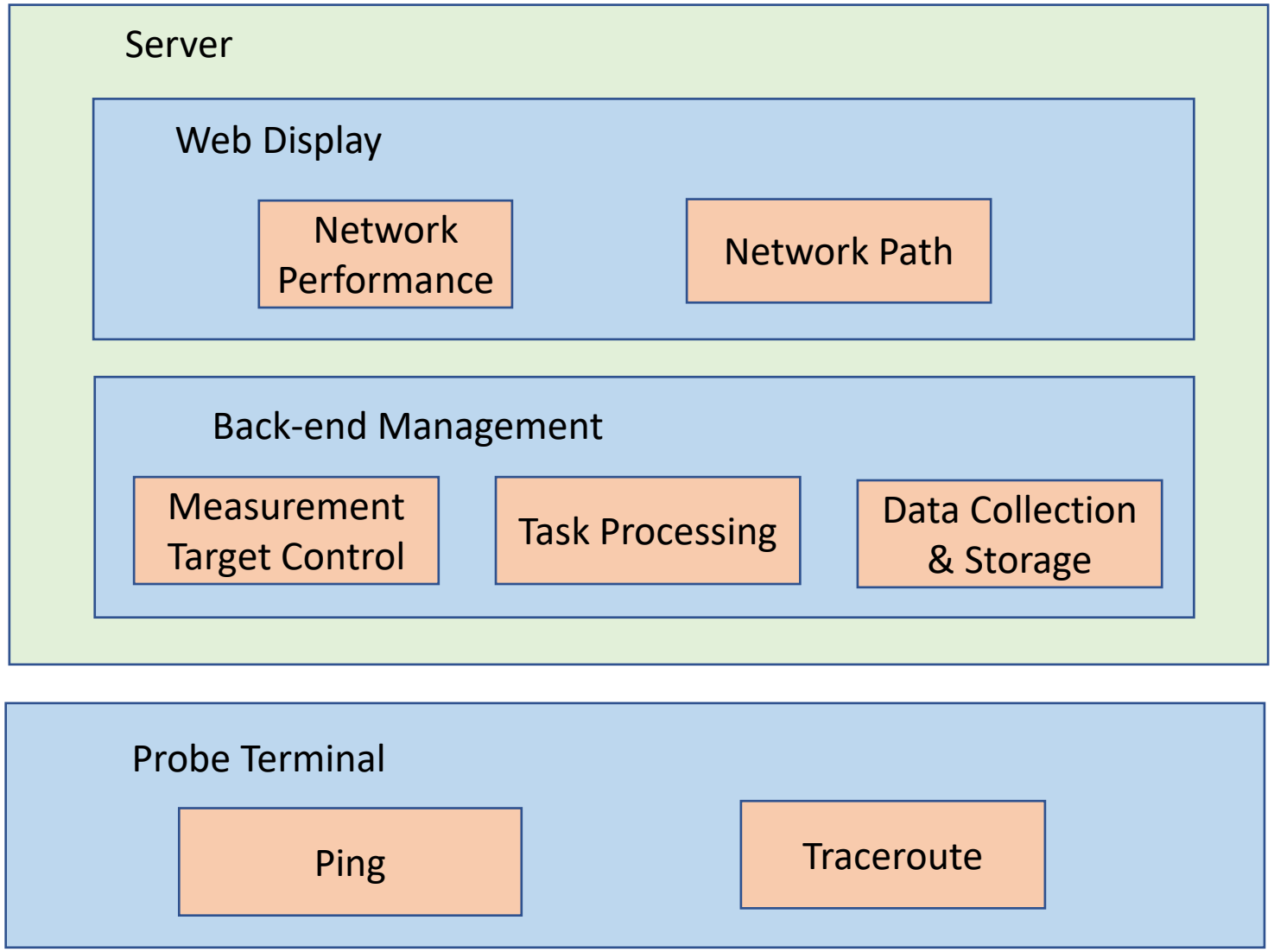
Benefit for partners

- Get collected data on **http://bgp.cgtf.net**



- **Gain a better understanding of partners' network.**
- **Help to identify problems in partners' network.**
- **Prompt research in Asia-Pacific Area.**

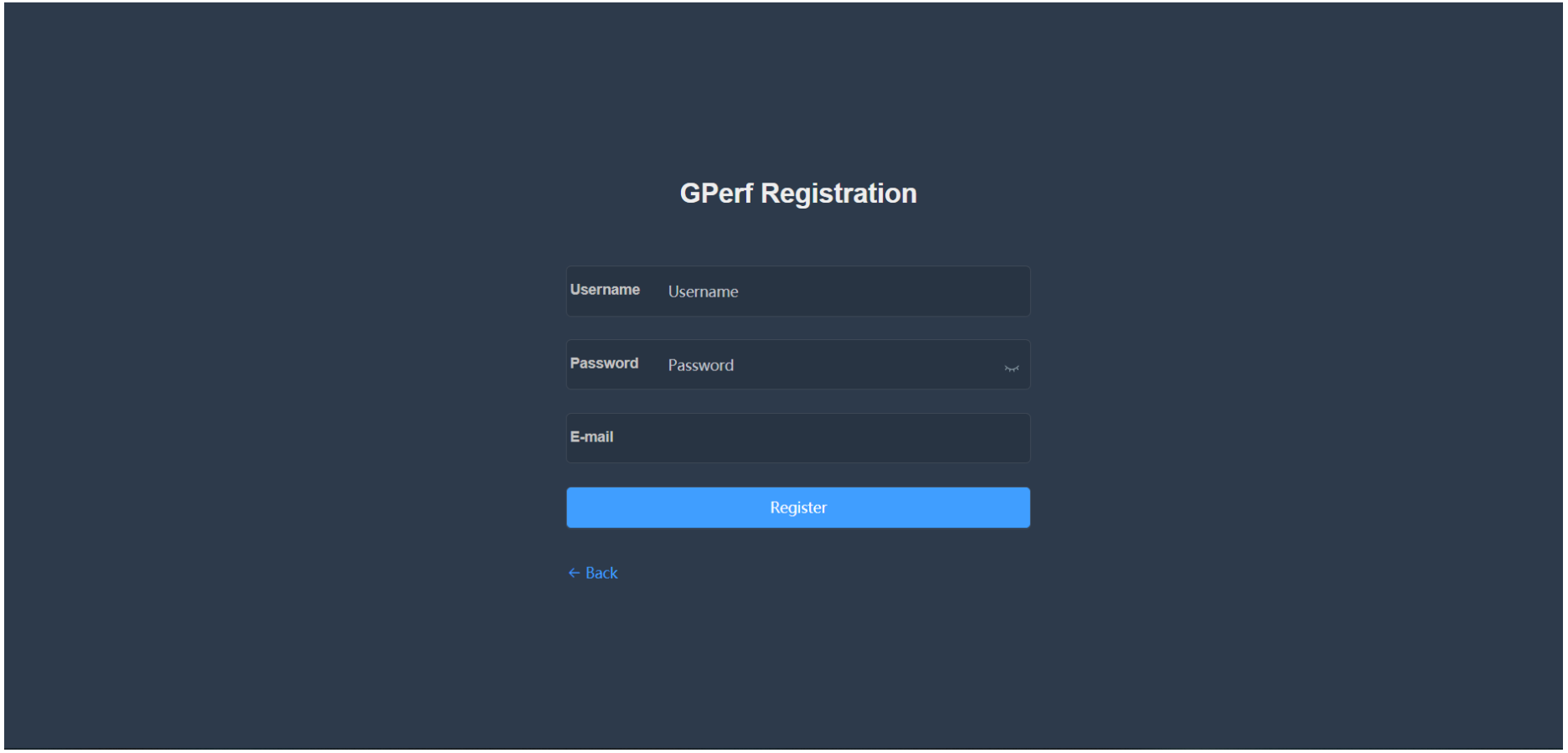
Active Probe Architecture



The system includes:

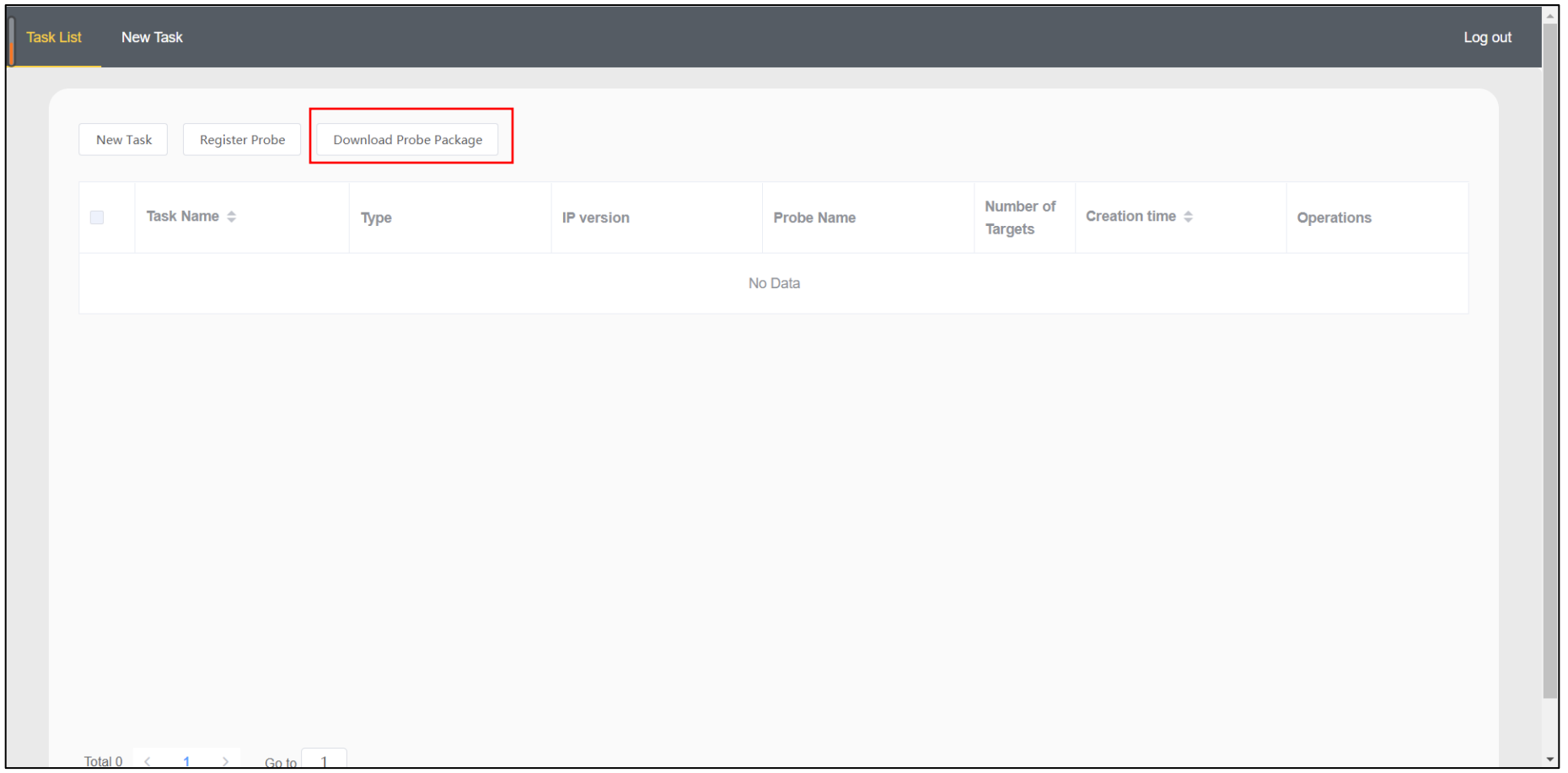
- Probe Terminal
- Back-end Management
- Web Display

The System of Active Measurement——Registration



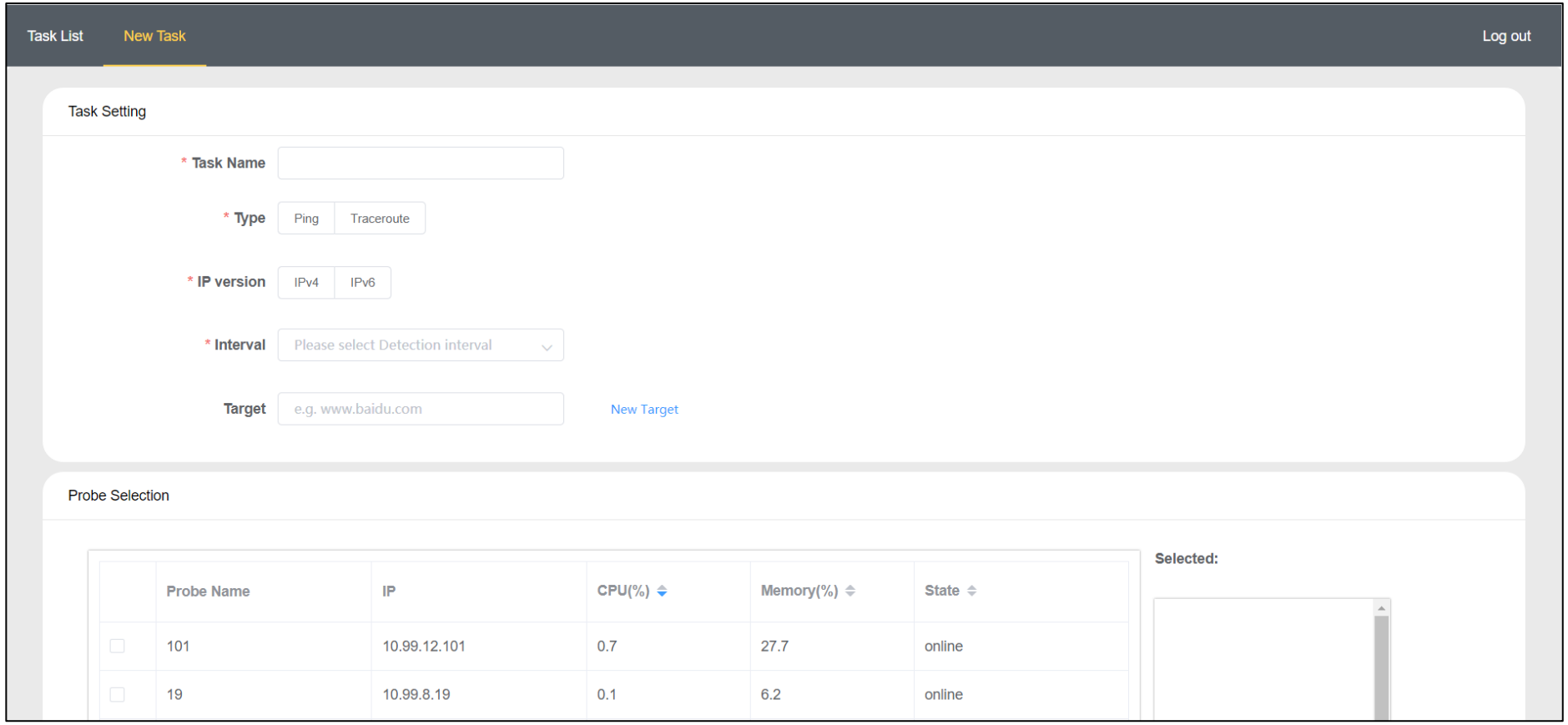
- Enter username, password and email, they will receive one activation email
- Once users complete activation, they can log in to their account

The System of Active Measurement——Probe Deployment



- Download the probe package from homepage and install it on their own CentOS or Ubuntu devices
- Register their probes, which input the IP address and MAC address of the probe.

The System of Active Measurement——Create Task



- You can config the tasks, such as IP version, detection interval and so on
- Select available probes according to CPU and Memory

The System of Active Measurement——Result Show

Ping results of Probe (ID:19) detecting www.baidu.com

Telescope

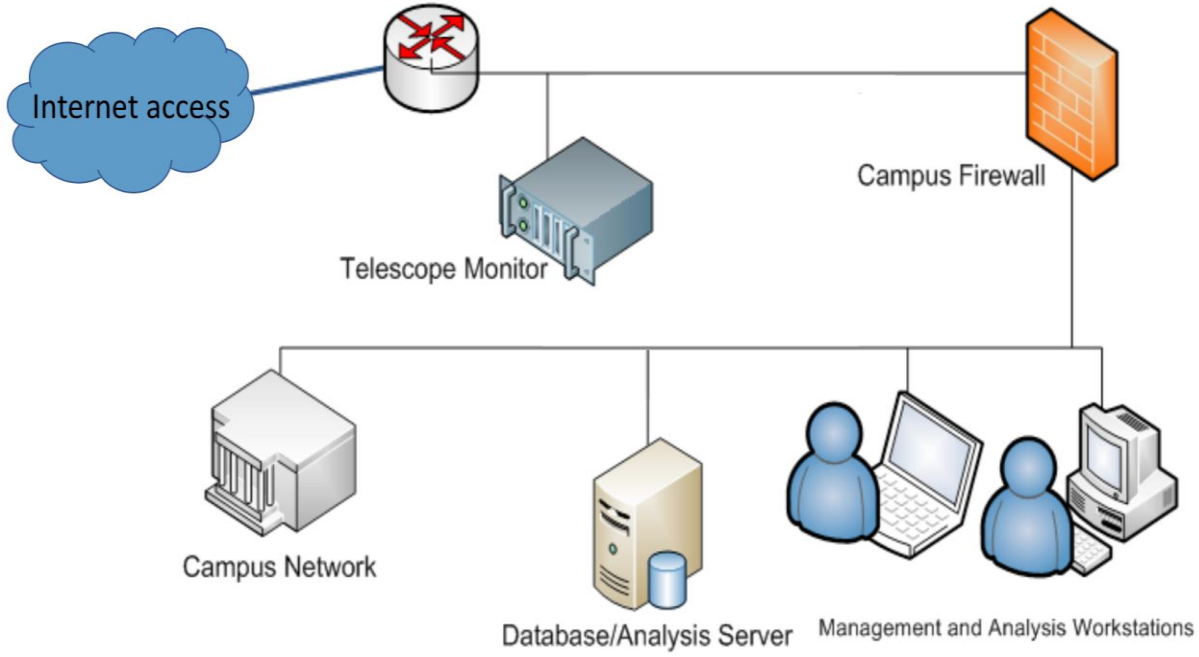
☐ Concept & Principle

- The network telescope observes the **unused part of the IP address** space in which there is little or no legal traffic
- View **network security event**, include **DOS**, **Internet worm infection** and **network scanning**
- Having a **larger IP address** space can provide more data, so improve the resolution of network events

Telescope

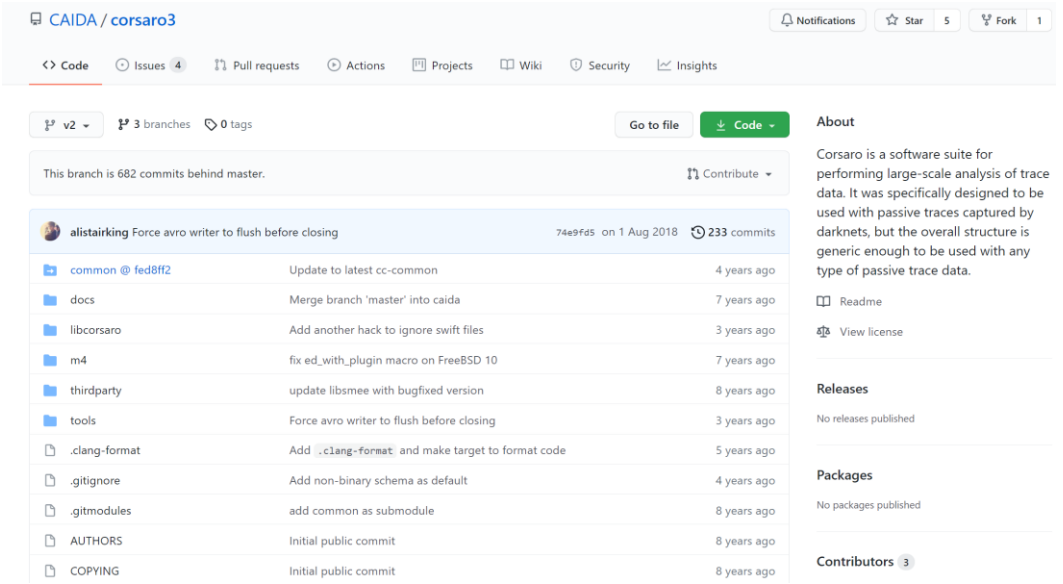
☐ Deploy Network Topology

- The telescope server obtain copies of all incoming traffic before network traffic passes through the firewall
- The server processes the data through analysis tools



Deployment

1. **Download corsaro and install**
    1. Corsaro is an open source software package for preliminary data processing.
    2. Download the corsaro(version 2 or version 3).
2. **Data Analysis**
    - ➢ According to the data processed by corsaro, we can further analyze it.
    - Sight of large-scale Internet (security) events
    - Identifying DoS attacks
    - Internet statistic reports
    - Network anomaly detection.

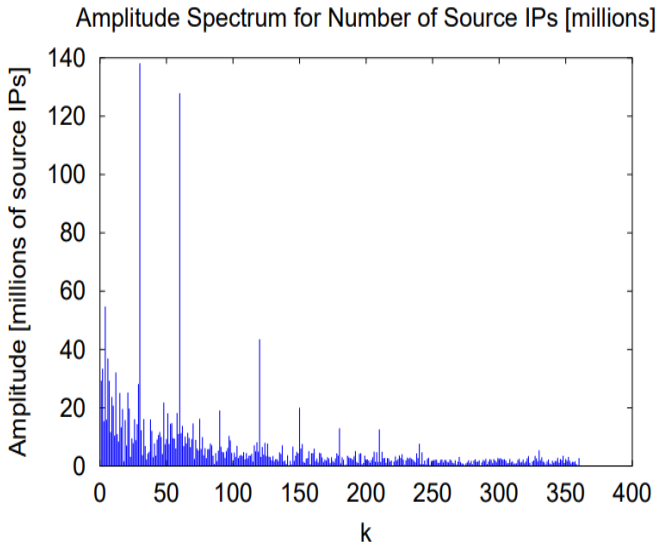



```
root@DL-telescope:~# corsaro
ERROR: At least one trace file must be specified
usage: corsaro [-alP] -o outfile [-i interval] [-m mode] [-n name]
               [-p plugin] [-f filter] [-r intervals] trace_uri [trace_uri...]
       -a             align the end time of the first interval
       -o <outfile>   use <outfile> as a template for file names.
                       - %P => plugin name
                       - %N => monitor name
                       - see man strftime(3) for more options
       -f <filter>    BPF filter to apply to packets
       -G             disable the global metadata output file
       -i <interval>  distribution interval in seconds (default: 60)
       -l             the input file has legacy intervals (FlowTuple only)
       -L             disable logging to a file
       -m <mode>      output in 'ascii' or 'binary'. (default: binary)
       -n <name>      monitor name (default: DL-telescope)
       -p <plugin>    enable the given plugin, -p can be used multiple times (default: all)
                      available plugins:
                       - flowtuple
                      use -p "<plugin_name> -?" to see plugin options
       -P             enable promiscuous mode on the input (if supported)
       -r             rotate output files after n intervals
       -R             rotate corsaro meta files after n intervals
```

Function

☐ Preliminary data process

- ➢ Users can use corsaro and other tools to preliminarily analyze traffic data:
  - Count packets per hour.
  - Count different types of packets.
  - Observe the periodicity characteristic of packets.
- ➢ Figure shows the flowtuple format, packets per hour, and source IP spectrum per hour.




```
root@DL-telescope:~/telescope# cors-ft-aggr
processing ./example.flowtuple.cors
# CORSARO_INTERVAL_START 0 1625649386
0.0.0.0|0.0.0.0|0|0|0|0|0x00|0,211015
# CORSARO_INTERVAL_END 0 1625652984
# CORSARO_INTERVAL_START 1 1625652985
0.0.0.0|0.0.0.0|0|0|0|0|0x00|0,201443
# CORSARO_INTERVAL_END 1 1625656584
# CORSARO_INTERVAL_START 2 1625656585
0.0.0.0|0.0.0.0|0|0|0|0|0x00|0,138589
# CORSARO_INTERVAL_END 2 1625659217
```

```
# CORSARO_INTERVAL_START 0 1625649386
START flowtuple_backscatter 178
203.91.121.202|104.238.220.196|3|3|1|64|0x00|248,1
217.150.49.161|203.91.123.33|11|0|1|241|0x00|56,1
212.133.164.0|203.91.123.20|80|51649|6|46|0x12|44,1
212.133.164.0|203.91.123.102|80|4753|6|46|0x12|44,1
212.133.164.1|203.91.123.161|80|3031|6|46|0x12|44,1
212.133.164.1|203.91.123.169|80|59007|6|46|0x12|44,1
212.133.164.2|203.91.123.21|80|62903|6|46|0x12|44,1
212.133.164.2|203.91.123.151|80|1876|6|46|0x12|44,1
212.133.164.3|203.91.123.95|80|51334|6|46|0x12|44,1
212.133.164.5|203.91.123.194|80|51064|6|46|0x12|44,1
212.133.164.10|203.91.123.127|80|2401|6|46|0x12|44,1
212.133.164.11|203.91.123.255|80|59563|6|46|0x12|44,1
```

Passive Traffic Classification

TMT-RF: Tunnel Mixed Traffic Classification Based on Random Forest Securecomm 2021 CCF-C

The tunnel traffic is encrypted and encapsulated, and the traffic is **mixed** and **overlapped**, making it difficult to extract a single application traffic.

Existing tunnel traffic identification is for **single application traffic** and cannot identify mixed traffic in the tunnel. Therefore, relevant research is difficult to apply in practice.

The tunnel traffic has **complex and diverse** mixed traffic, which brings challenges to the identification of the traffic in the tunnel.

- ✓ A two-level segmentation framework is proposed for the segmentation of three types of mixed flows in the tunnel.
- ✓ The first segmentation module uses a method based on a combination of data packets and classifiers to realize network behavior transition detection in the tunnel.
- ✓ The secondary segmentation module uses burst segmentation and combined methods to achieve the secondary segmentation of the tunnel overlapped traffic.
- ✓ The tunnel playback method is proposed, and three types of mixed traffic in the tunnel are generated and marked.
- ✓ Compared with the state-of-the-art methods in existing research on three types of mixed data sets (positive time separation application, zero time separation application and negative time separation application), the results show that TMT-RF is the best performance on all data sets .

Passive Traffic Classification

SIAMHAN: IPv6 Address Correlation Attacks on TLS Encrypted Traffic via Siamese Heterogeneous Graph Attention Network

USENIX Security 2021 CCF-A

User Activity Correlation

- Leveraging traffic meta-information to identify and track users
- Could work even on traffic encrypted by Transport Layer Security (TLS)

Work on IPv6

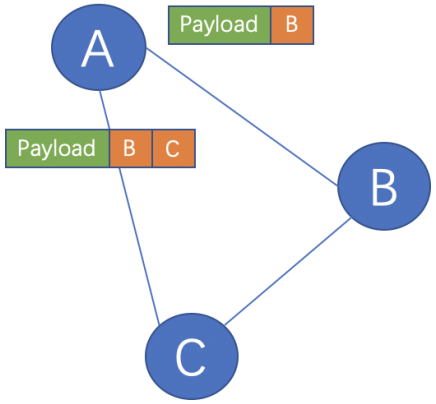
- Unlike IPv4 - rare deployment of Network Address Translation (NAT)
- An IPv6 address usually corresponds to one single user
- **Serious individual-level privacy threat!**

Contributions

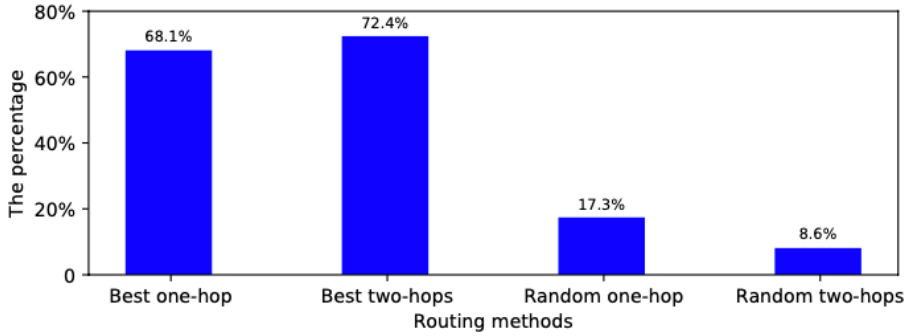
- We introduce a new **IPv6 address correlation attack** that effectively correlates a user's TLS encrypted traffic with its dynamic address.
- We present a knowledge graph-based approach to model user behavior behind addresses. It exploits multi-type semantic meta-information to facilitate user correlation.
- We propose a correlation attack model – SIAMHAN which demonstrates superior performance on IPv6 user activity correlation.
- We conduct extensive experiments on a 5-month IPv6 user TLS traffic dataset. Results show that SIAMHAN is robust and could reach drastically high accuracy on multiple long-term user correlation tasks.

SRv6 Research Ideas

- Leverage triangle inequality violation (TIV) to provide low-latency indirect path.



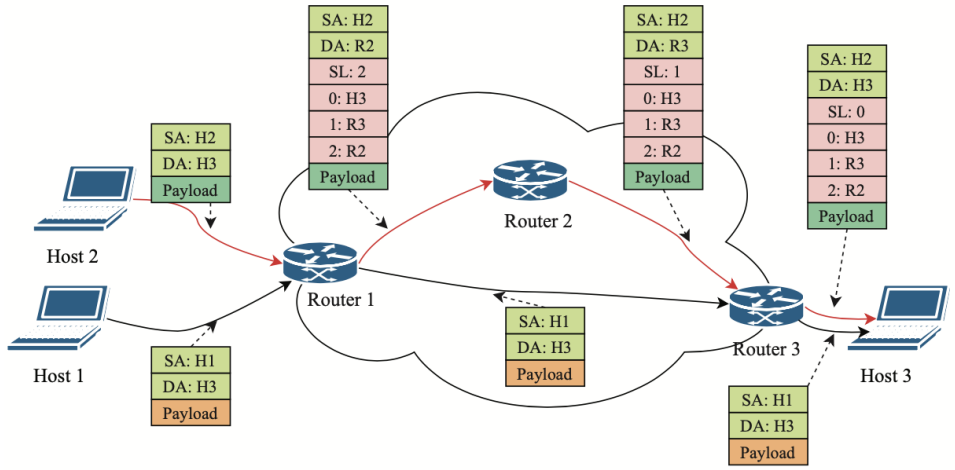
$t_{AB} > t_{AC} + t_{CB}$



In the trace, about 70% pair of nodes can have lower latency routing through one-hop or two-hops indirect paths

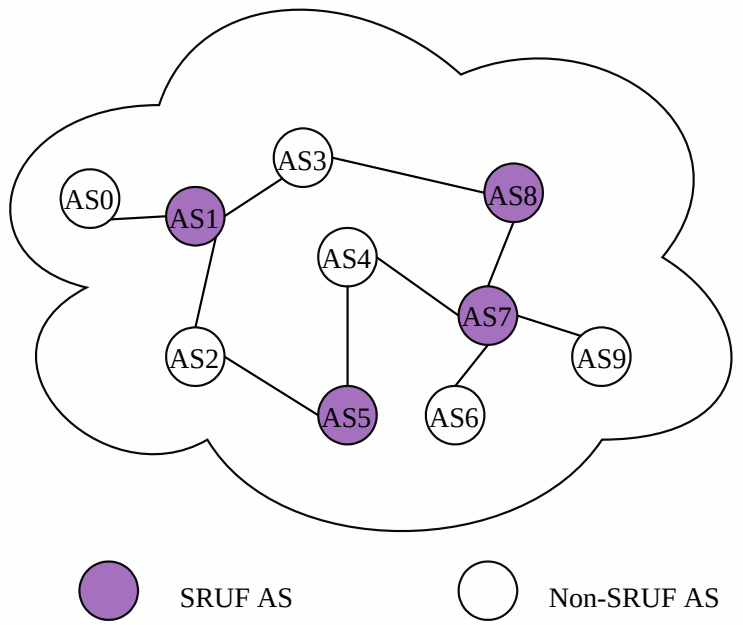
Research Ideas

- Leverage SRv6 to steer the flow along the low-latency indirect path



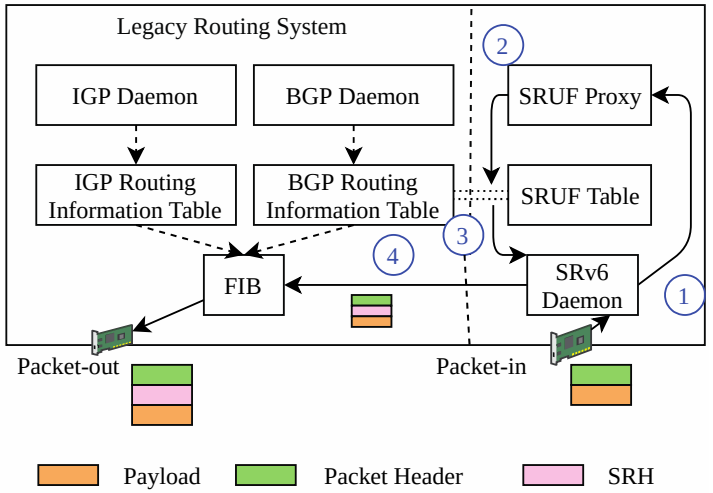
SRv6 is a source routing that has the addresses of intermediate nodes in packet header.

SRUF: SRv6 Underlay Federation



- In this example, there are four ASes in SRUF
- These four ASes can find the low-latency indirect paths among them.
- The indirect paths are recorded in a table, SRUF table.
- Assume that $t_{AS1 \rightarrow AS5} + t_{AS5 \rightarrow AS7} < t_{AS1 \rightarrow AS7}$

SRUF: SRv6 Underlay Federation



① SRv6 daemon intercept the packet, activate the corresponding segment and then pass it to SRUF proxy.

② SRUF proxy find that the AS path is $\{AS3 \rightarrow AS8 \rightarrow AS7 \rightarrow AS9\}$

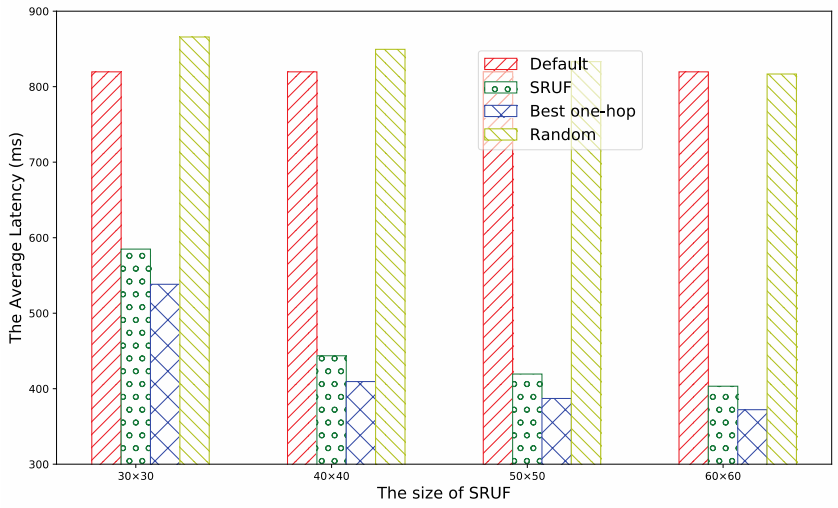
③ The proxy knows that $\{AS1 \rightarrow AS5 \rightarrow AS7\}$ has the lower latency, so it will insert AS5 into the packets segment routing header.

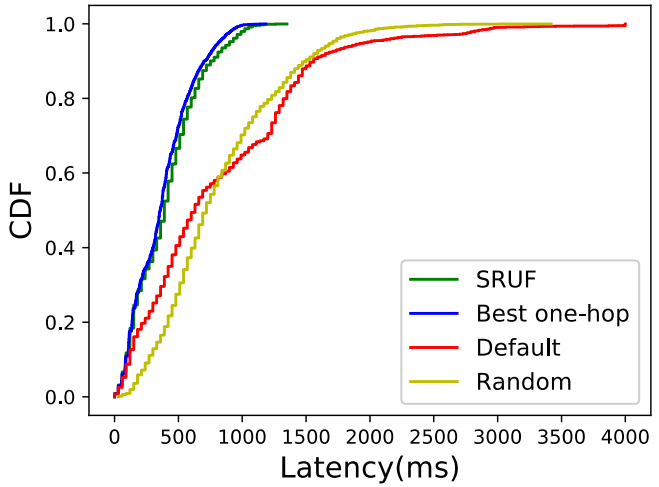
④ The new encapsulated packet will be forwarded to AS5 according to FIB

The key challenge is how to find the low-latency routing paths efficiently ?
How to construct SRUF Table in each member efficiently?

Experiments

- AS-topology: 6313 nodes
- Link latency: synthetic data (sampled from a trace)





Current Progress

- Two paper has been finished.
  - SRUF: Low-Latency Path Routing with SRv6 Underlay Federation in Wide Area Network. In Proc. of ICDCS, 2021.
  - Optimal Deployment of SRv6 to Enable Network Interconnection Service. ACM/IEEE Transactions on Networking. (Second-round revision)

ISIF Asia Funding

— Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

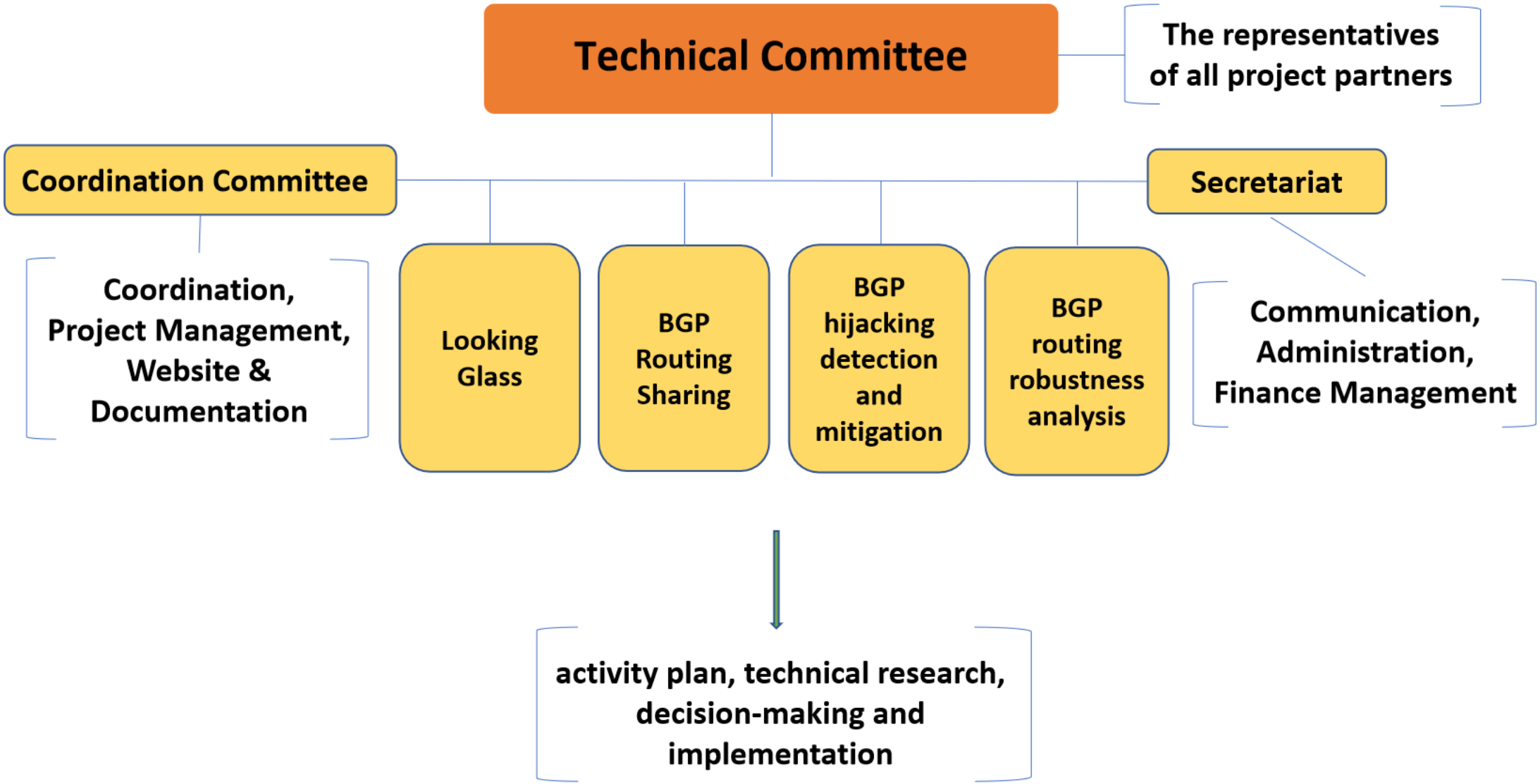
Project Team

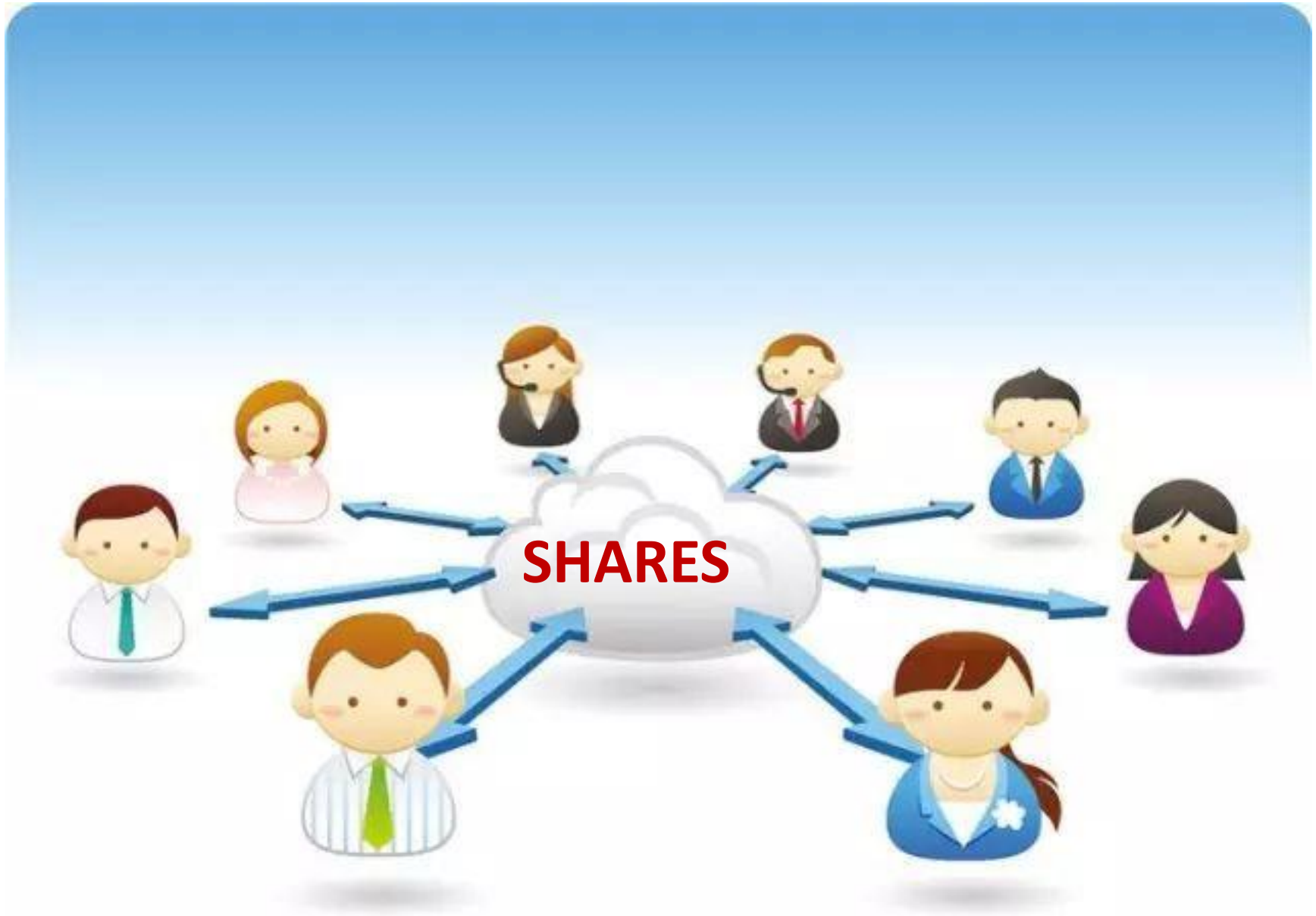
- CERNET, China
- SingAREN, Singapore
- ThaiREN, Thailand
- BdREN, Bangladesh
- LEARN, Sri Lanka
- AfgREN, Afghanistan
- MYREN, Malaysia
- NREN, Nepal
- Gottingen University, Germany
- Surrey University, UK

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

More NRENs' participations are welcomed!

Project Summary




SHARES

Comments and suggestions are welcome