(APNIC ISIF Project)

Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform

--The 6th Technical Committee Meeting

April 27, 2023

清華大學 Tsinghua University

APNIC FOUNDATION

Outline

- Project Update
  - Knowledge Sharing Events at APAN55
  - Feedback from Partners before and at APAN55
  - Development Progress
- Work Plan for the Next Four Months(till August)
- Proposal of Next APNIC ISIF Funding (Draft)
- Project Meeting in May in Beijing (Draft)
- Comments/Suggestions

清華大學 Tsinghua University

APNIC FOUNDATION

Project Update – Knowledge Sharing at APAN55

- Knowledge Sharing Events at APAN55 were very successful
  - 4 sessions for RPKI Theory and Hands-on
  - 1 session for RPKI User Cases and Experience Sharing
  - 2 sessions for MANRS: What, Why and How, and User Cases and Experience Sharing
  - About 170 training opportunities were provided with very good feedback
  - A small complain is that the meeting room seemed too small because of more participants
- Acknowledgement
  - Tsinghua team, APNIC, APAN, NREN (NP), and the support from other NREN partners
  - Warrick Mitchell (AARNET)
    - Gave a lots of advice on these events organization
    - Chair of one MANRS session
    - Trainer of MANRS
    - Speaker of two sessions: RPKI and MANRS Experience Sharing
  - Other trainers/speakers from APNIC and NREN partners
    - Jamie Gillespie (APNIC), Dibya Khatiwada (APNIC Community Trainer)
    - Aaron Murrihy (REANNZ), Christopher Bruton (CENIC), Jiang Zhu (China Telecom), Yanbiao Li (CSTNET), Zhonghui Li (CERNET)
    - Two NREN assistant trainers from Nepal NREN: Binita Kusum Dhamala, Milan Adhikari

清華大學 Tsinghua University

APNIC FOUNDATION

RPKI Training Session at APAN55

清華大學 Tsinghua University

APNIC FOUNDATION

Project Update – Project Meeting at APAN55

- BGPWatch Manual and Demonstration Video
  - Joint efforts of BdREN and Tsinghua University
  - Link: https://www.bgper.net/index.php/document/
- APNIC ISIF Project Meeting at APAN55
  - Project update – Changqing An (Tsinghua University)
  - BGPWatch demonstration – Md Ariful Islam (BdREN)

清華大學 Tsinghua University

APNIC FOUNDATION

Project Update - Feedback from Partners I

- Screen Resolution Auto Adaption (done)
- Error when search IPv6 address routing(done)
- Statistics error on Home page(done)
- Configure interested prefix/AS, and send alert when anomaly/hijacking
- More BGP related alert, such as peer change/path change
- Send message by slack channel
- Bi direction routing path(done)
- Reverse routing path(done)
- Monthly /weekly summary(done)
- Show alternative routing path/track multi path
- Path performance

Been Fixed

清華大學 Tsinghua University

APNIC FOUNDATION

Project Update - Feedback from Partners II

- If you want to search an “Organization” using name, AS-name or AS-number you have to go to the “Organization” menu
  - Organization Name is “Case sensitive”, better if it is made “Case insensitive”
- The prefixes in “Dashboard=>IPv4 Peers” and that of “Routing Path” should match.
- Needs to put the “last date of update” for the records which will be periodically updated.
- Remedial Measures： Once the “Hijacker” is suspected, can we warn the suspected entity AS20853 along with its upstream provider AS 1299 with emails. The process may be automatized if we can collect the administrative contacts of each AS from APNIC.

Been Fixed

Project Update - Feedback from Partners III

- Reporting Anomaly： Incomplete information, Timezone undefined
- Fault alarm (Must sync ROA & RIR data timely)
- Bidirectional Routing Path: some paths are missing
- Can we mention the name of the Top-10 organizations and their cone size next to the diagram? That will give an idea about the top service providers in each country.

- In the “Dashboard”, it searches advertised prefixes but there is no subnet-wise search. Suppose, it will find out 103.28.120.0/22 under BdREN but cannot locate 103.28.121.0/24.

- There is not much usage of “Reverse Route Path”. It generates a file in “image” format which also doesn’t provide a legible view when enlarged. Better if it could be made available in pdf format.

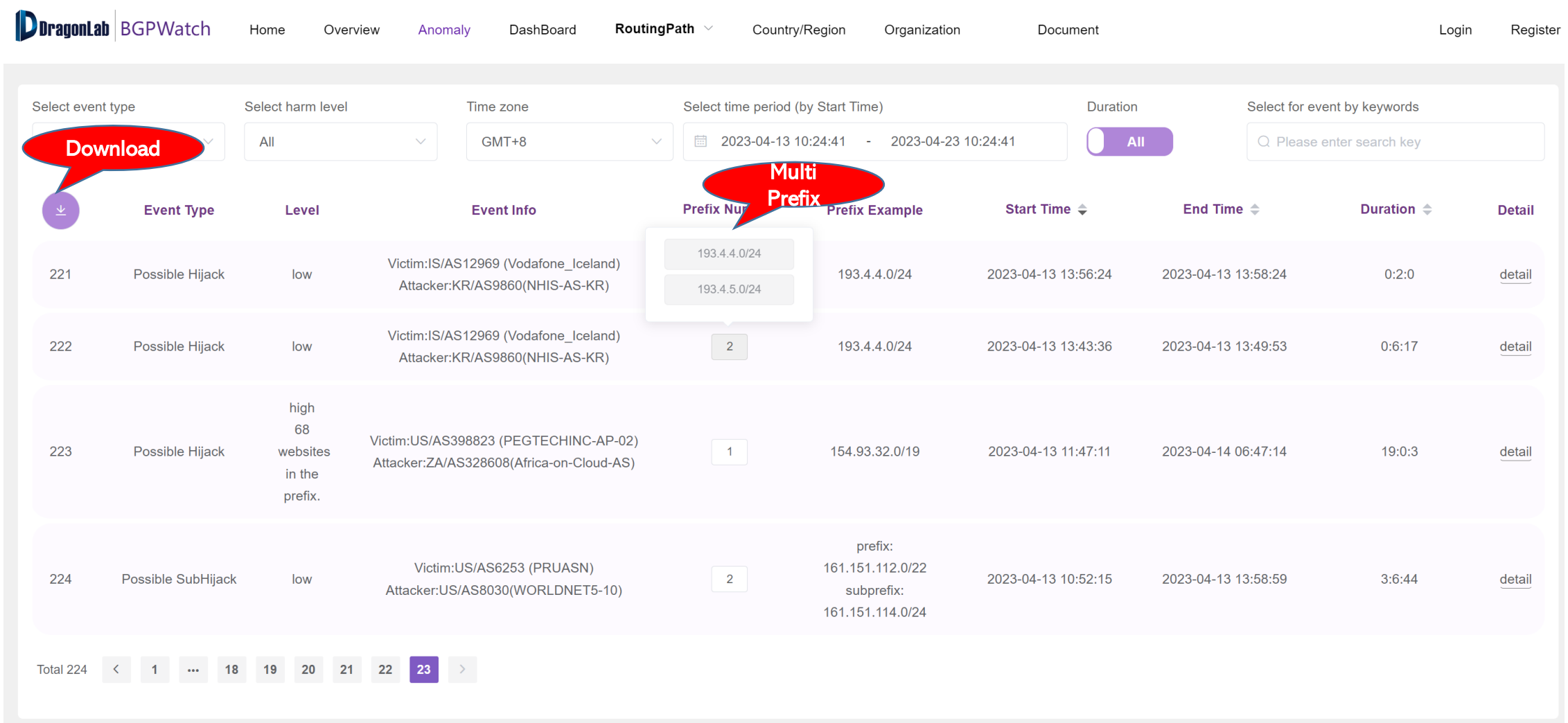
Been Fixed

Project Update - Feedback from Partners IV

- Suggestion on Visual improvements
  - Visual directional relationship from attacker to victim
  - Zooming of Map
  - Larger view/pop-out view of other surrounding windows
- Prefix information should be updated regularly
- Wrong direction in Bi-Routing Path
- Mitigation feature support is highly required
- Monitoring or alerting system for AS path change to a selected destination
- API for receiving data to display on partner customized applications and monitoring systems
- Some topologies does not show ASN details when hovering over the ASN nodes

Been Fixed

Development Progress - Anomaly Report



- Support download and show multi prefix
- Sync ROA & RIR data daily

清華大學 Tsinghua University

APNIC FOUNDATION

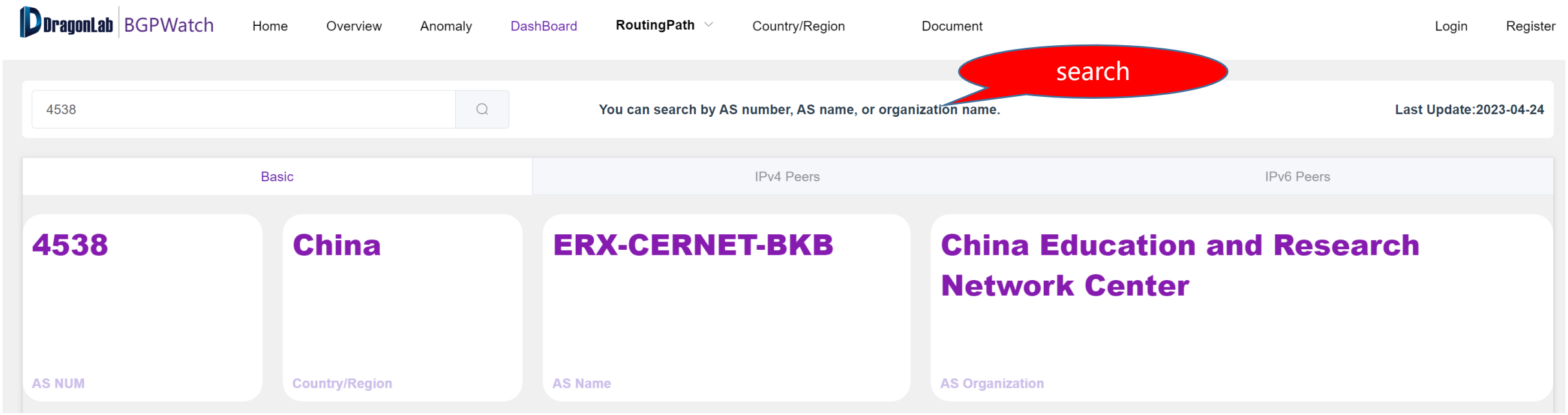
Development Progress - Anomaly Detail

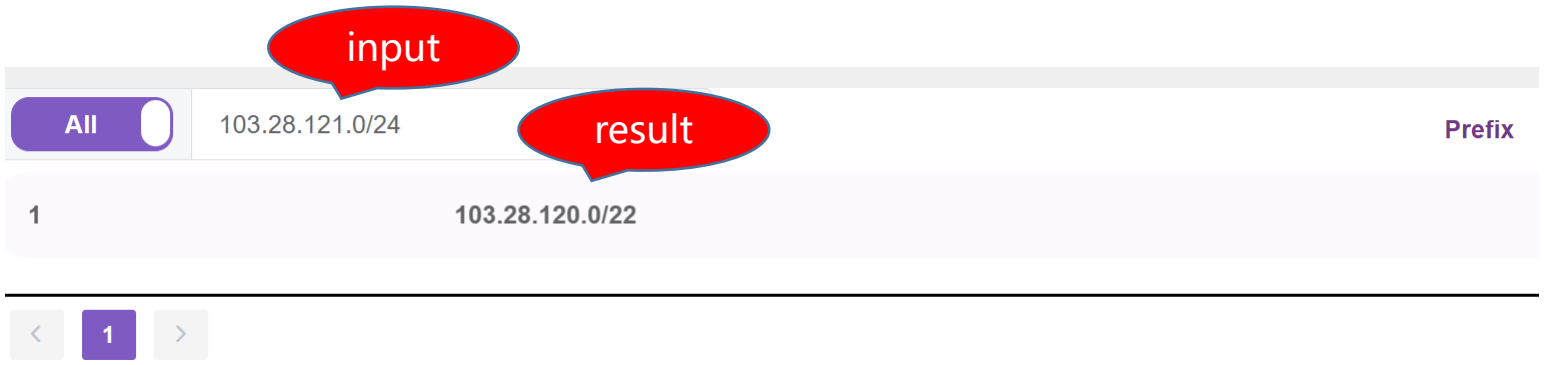
Add Nav Bar and Time Zone

清華大學 Tsinghua University

APNIC FOUNDATION

Development Progress - DashBoard



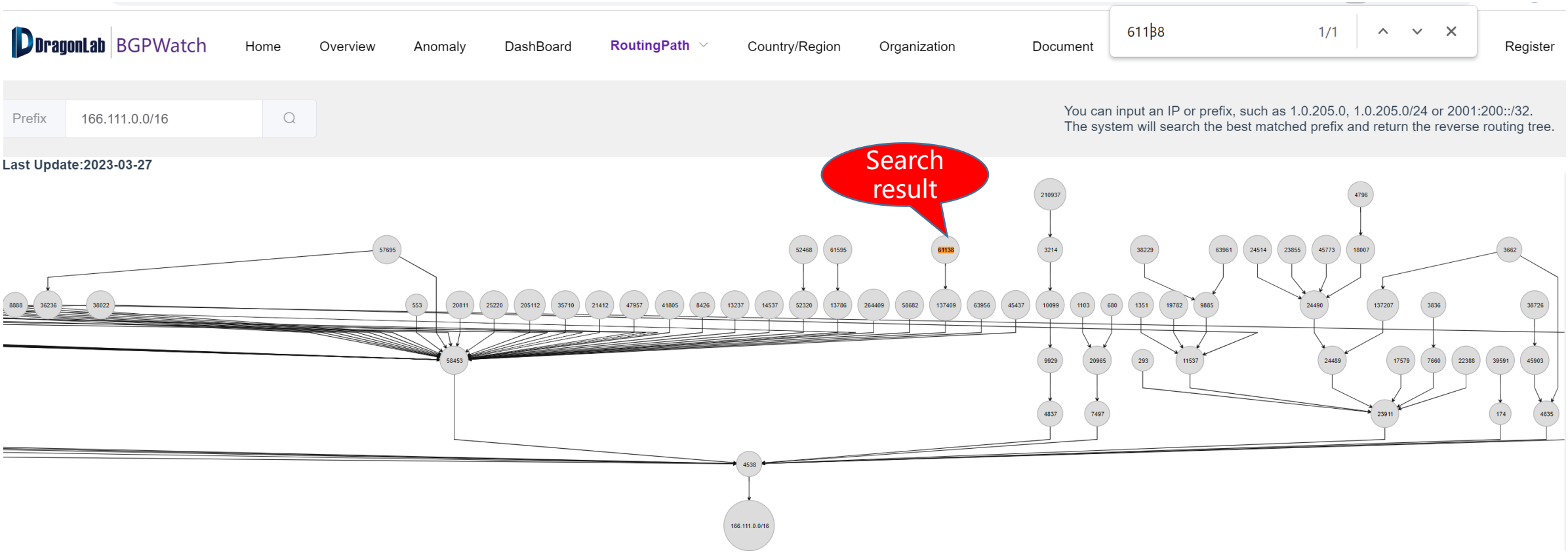


- Subnet and Super-Net of Prefix are searched
- Merge Organization to Dashborad

清華大學 Tsinghua University

APNIC FOUNDATION

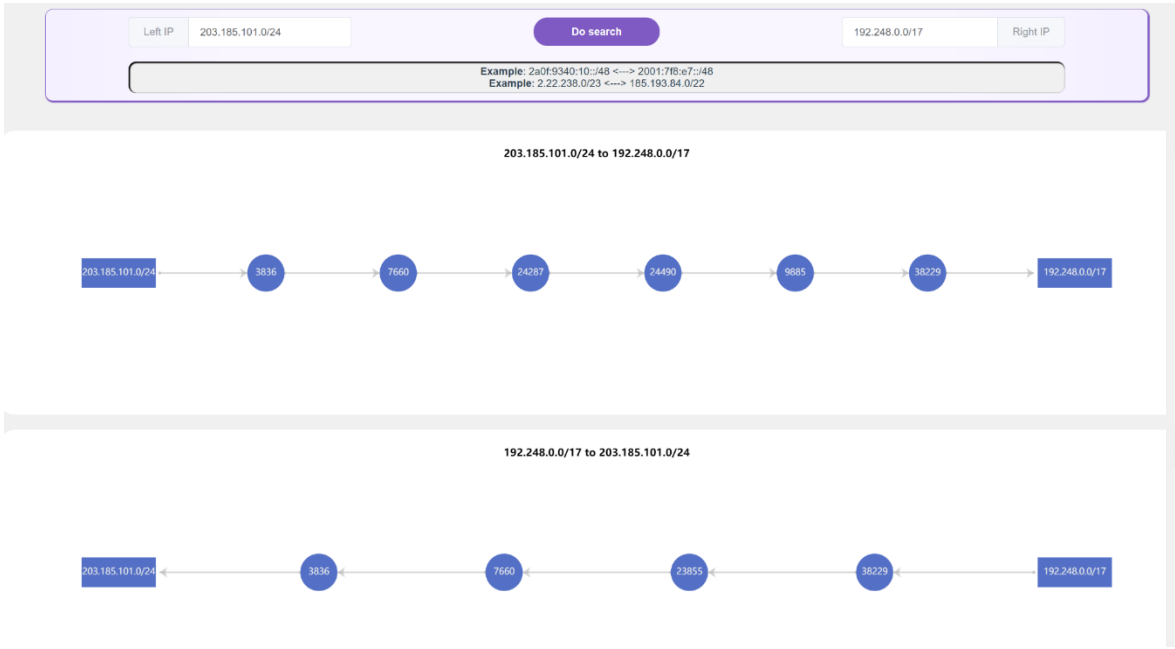
Development Progress - Reverse Routing Path



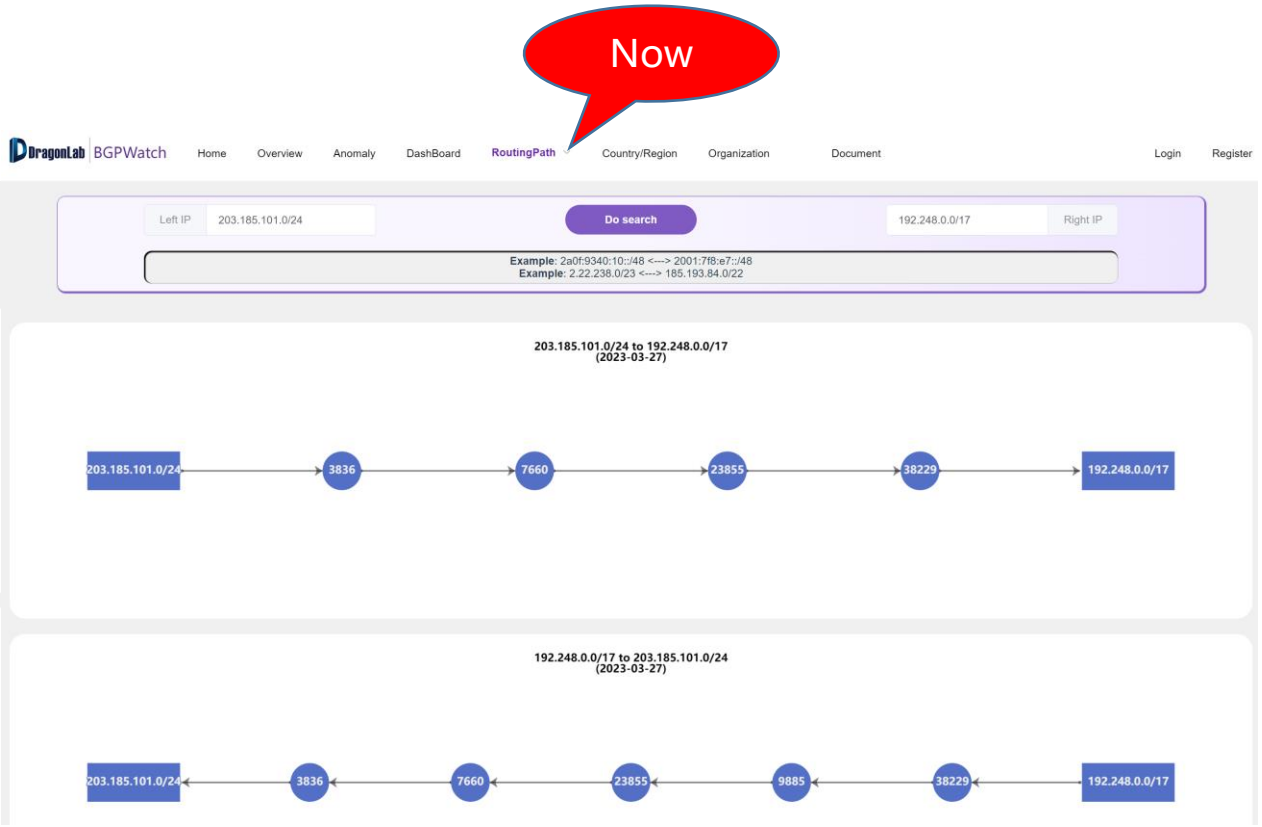
Support browser search

Development Progress - Wrong Direction in Bi-Routing Path

Before



Now

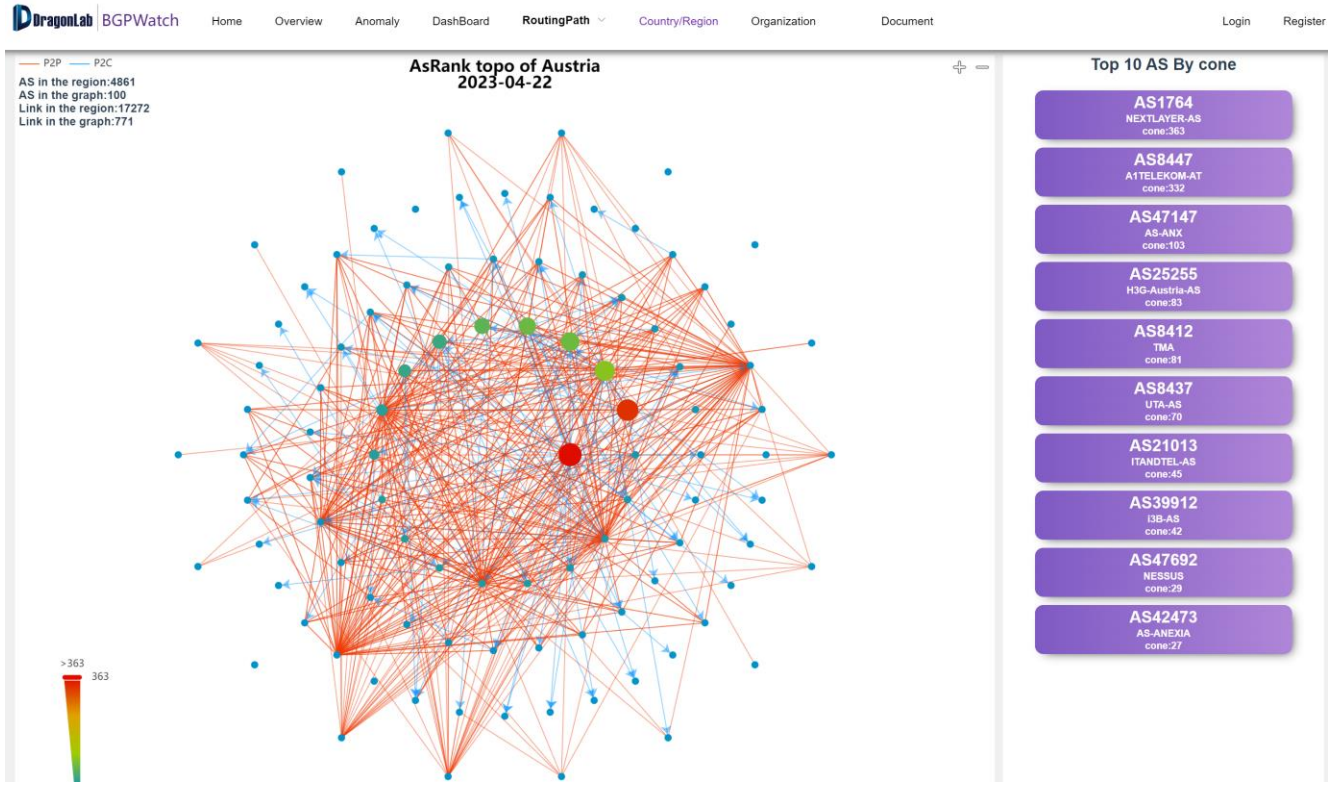


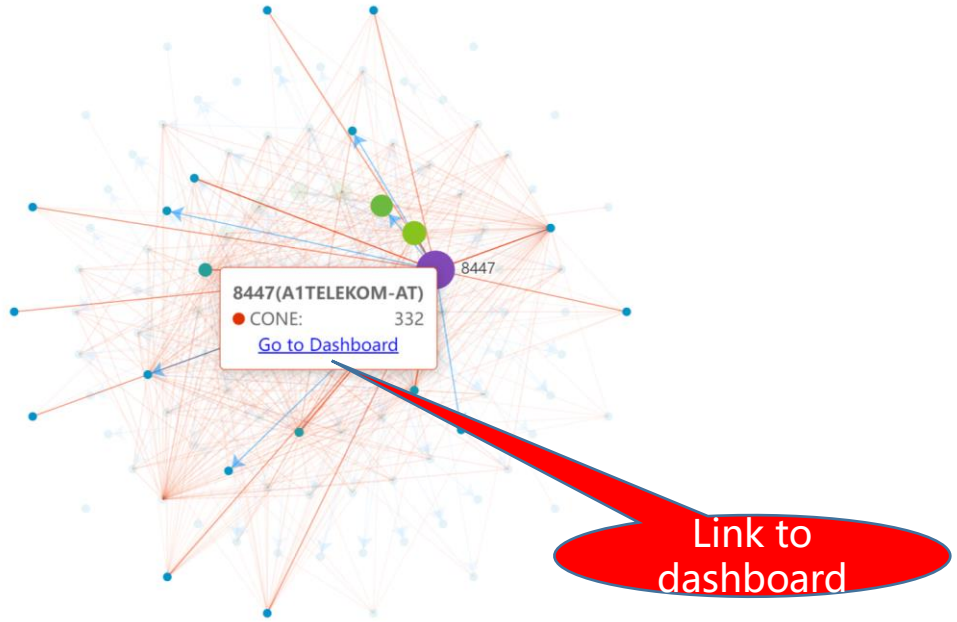
- Left : 203.185.101.0/24 , from ThaiREN
- Right: 192.248.0.0/17 , from LEARN

Tsinghua University

APNIC FOUNDATION

Development Progress - Country/Region of BGPWatch





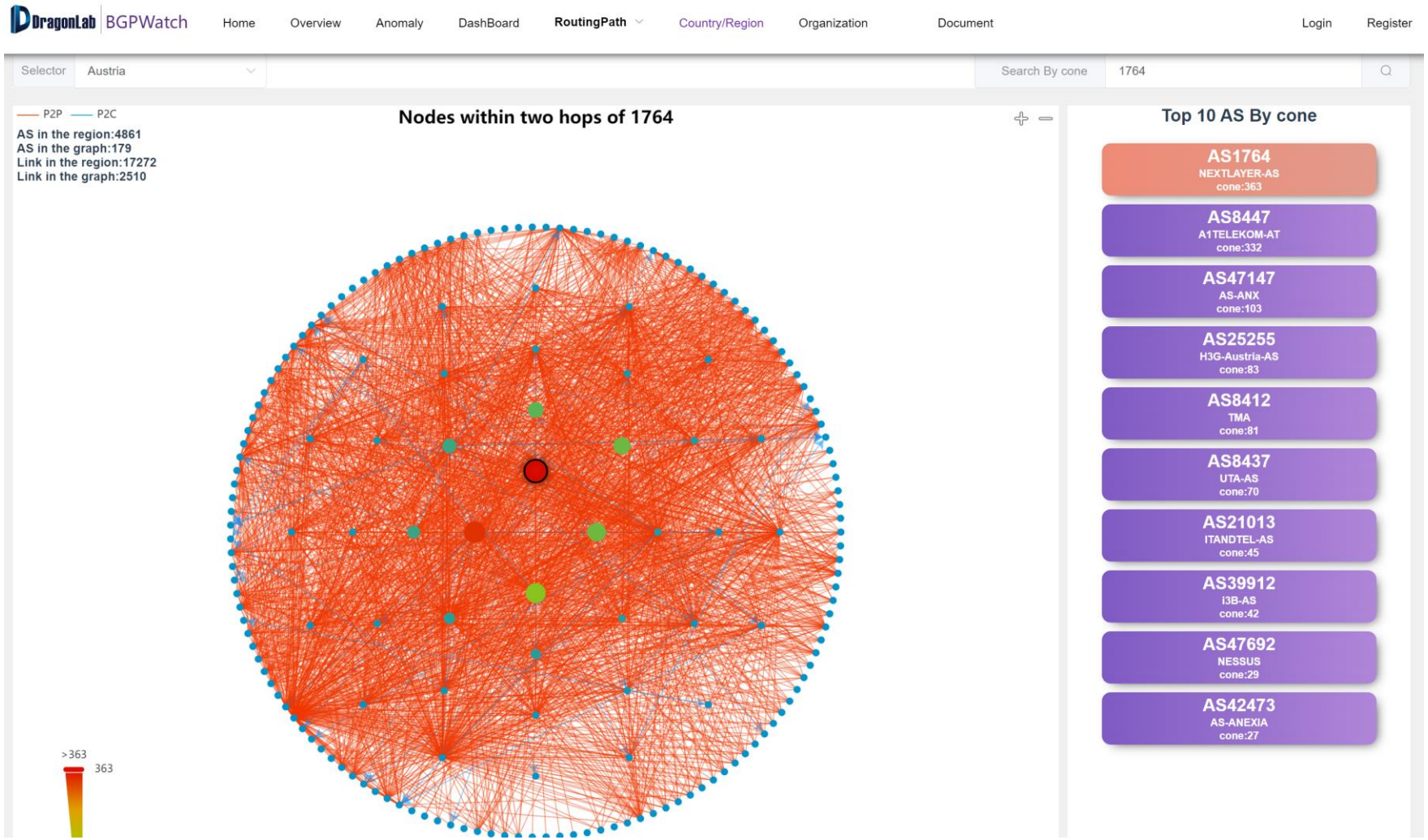
Show TOP 10 AS

Link to Dashboard

Tsinghua University

APNIC FOUNDATION

Development Progress - Country/Region of BGPWatch



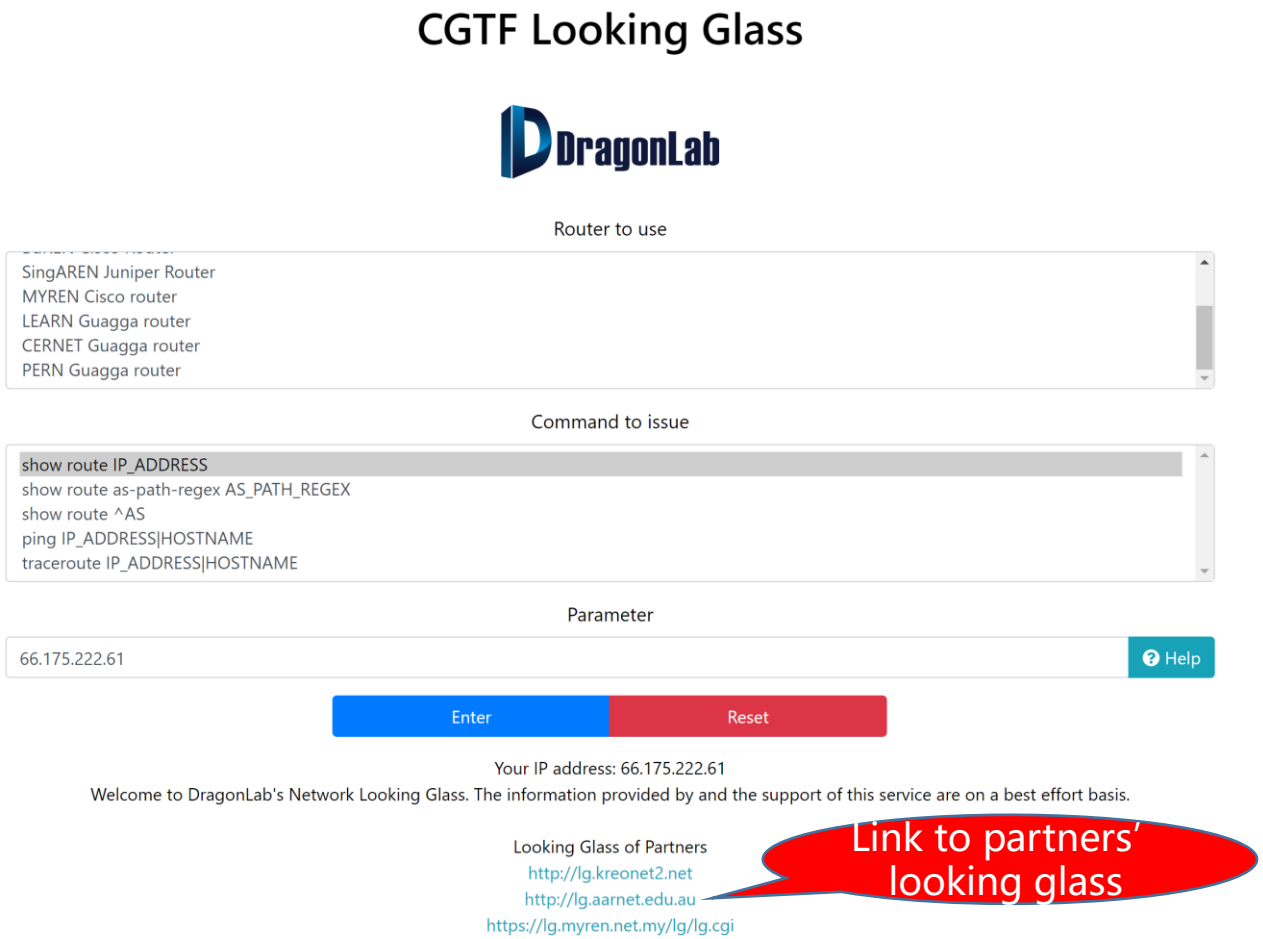
Click the AS button, show nodes within two hops of it

Tsinghua University

APNIC FOUNDATION

Development Progress - CGTF Looking Glass

- https://lg.cgtf.net
- Open Source:
  - https://github.com/gmazoyer/looking-glass
- 5 commands
- Query speed limit for security
- More partners is welcomed



Add links to partners' looking glass

清華大學 Tsinghua University

APNIC FOUNDATION

Work Plan for the Next Four Months

- Continue working on feedback from partners
- Parallel Computing and Clusters to handle big routing data
  - There are huge amount routing data from RouteViews, RIS, PCH, CGTF. Now we only use part of there data. We'll try to process all the data by Parallel Computing and Clusters. Even though, no one can get all the path information, so it's a best effort system.
  - Consider to analyze data by user request, not all path change, but the specific prefix user subscribed.
- Knowledge Sharing(DNSSEC Training in May in Beijing)
- Project Meeting and Documents

Proposal of the Next APNIC ISIF Funding (Draft)

- Deadline: 30 April
- Project name: An Extension of the Ongoing Project ‘Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform’ Project
- Funds: USD85,000
- Duration: 18 months
- Objectives:
  - Develop an integrated looking glass platform, which can leverage many looking glasses and return data to users
  - Use looking glass to further check routing hijacking at the data plan, and to improve detection accuracy
  - Develop path hijacking detection and routing leak detection
  - Continue to maintain and fix bugs of BGPWatch platform
  - Continue the community development and international collaboration

清華大學 Tsinghua University

APNIC FOUNDATION

The Program of the Project Meeting in May in Beijing (Draft)

- 22 May (Monday) Arrive in the Beijing Friendship Hotel
- 23 May (Tuesday)
  - 0930-1000 Registration
  - 1000-1100 Project Overview and Discussion
  - 1100-1130 Coffee Break
  - 1130-1230 The Research Outcomes of Working Groups I
    - Survey and Research on Internet Governance
    - Survey and Research on Internet Governance Rules
  - 1230-1430 Lunch
  - 1430-1530 The Research Outcomes of Working Groups II
    - Research on Classification of Encrypted Traffic
    - Research on Internet Attack and Spam
  - 1530-1600 Coffee Break
  - 1600-1700 The Research Outcomes of Working Groups III
    - Research on Internet Topo Discovery
    - Research on Data Sharing

The Program of the Project Meeting in May in Beijing (Draft)

- 24 May (Wednesday)
  - 0900-0915 Registration
  - 0915-1045 Internet Governance Workshop I
    - Talk from Tsinghua University from China
    - Talk from Malaya University from Malaysia
    - Talk from Mae Fah Luang University from Thailand
  - 1045-1100 Coffee Break
  - 1100-1230 Internet Governance Workshop II
    - Other partners will share the ideas of Internet governance from their perspectives
  - 1400-1500 APNIC Project Meeting – Some Research Outcomes
    - Research on Route Path Hijacking
    - Research on Route Hijacking Mitigation
  - 1500-1730 Bilateral Meetings of APNIC ISIF project

清華大學 Tsinghua University

APNIC FOUNDATION

The Program of the Project Meeting in May in Beijing (Draft)

- 25 May (Thursday)
  - 0900-0930 Registration
  - 0930-1730 DNSSEC Training
  - Link: https://wiki.apnictraining.net/dnssec-20230525

- 26 May (Friday)
  - 0930-1030 The closing
  - 1030-1230 visit

清華大學 Tsinghua University

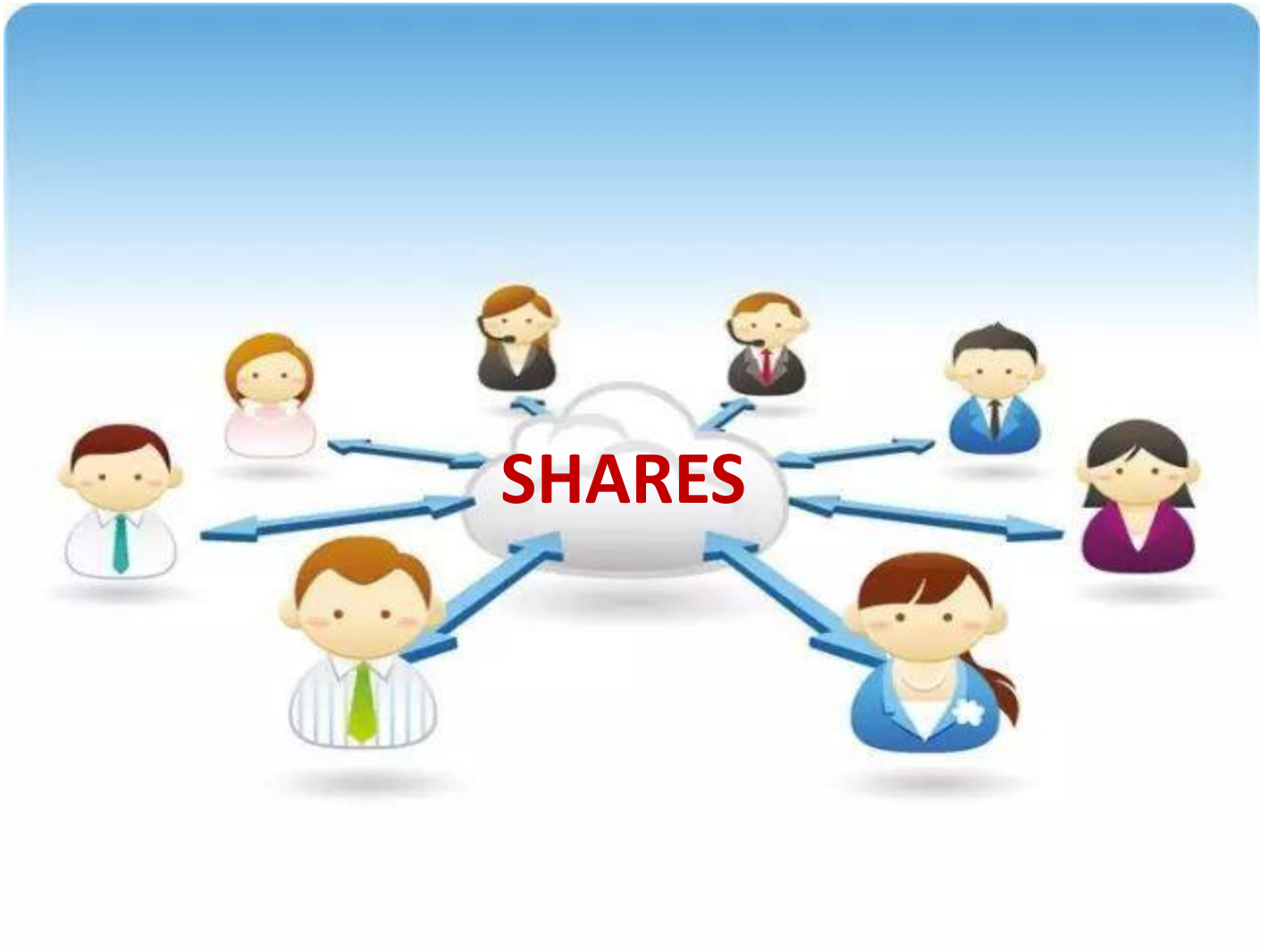
APNIC FOUNDATION

The Logistics of the Project Meeting in May in Beijing

- Hotel: Beijing Friendship Hotel
- Venue: Room B-102 in Lee Shau Kee Science and Technology Building, Tsinghua University
- Other Logistics
  - Transportation from the Hotel to the venue will be provided.
  - Visas: **F visa** is required.
  - Airplane tickets should be booked by participants themselves.
  - Hotel booking has been made by Tsinghua University, but the participants should pay their stay when they check out.
  - The project will cover the travel cost of one representative from one partner organization, and the reimbursement will be made within one month after the meeting.
  - More further information of this meeting will be shared via emails and slack.

清華大學 Tsinghua University

APNIC FOUNDATION



Comments and Suggestions?