DragonLab | BGPWatch

USER MANUAL

DOCUMENT

www.bgpwatch.net

清華大學
Tsinghua University

APNIC
FOUNDATION

User Manual Documentation on BGP Watch

Background

Researchers and Engineers of Tsinghua University, under its initiated Joint IPv4/IPv6 project supported by Chinese Government, have developed a platform – called BGPWatch - which gives a full landscape of BGP routing and analyzing view by displaying the bi-directional routing path between Autonomous Systems, the incidents about route hijacking, the identity of the victims and the attackers, the hijacking statistics, the routing topology and many other features.

With the support of APNIC ISIF project called "Developing a Collaborative BGP Routing Analyzing and Diagnosing Platform", this platform has been further developed by Tsinghua team based on the technical advice and experiences provided by the 17 NREN partners, including AARNET, APAN-JP, BdREN, CERNET, DOST-ASTI, ERNET, HARNET, ITB, KREONET, LEARN, MYREN, NREN, PERN, REANNZ, SingAREN, ThaiREN, and TransPAC(APAN Routing Working Group).

What is BGP?

We are using computers or mobile phones and internet in our day-to-day life. But how are these devices connected to the internet? Computers are connected through wired or wireless media into an Ethernet Switch to form a Local Area Network or LAN in brief. A number of LANs get interconnected using a Router to form a Wide Area Network. Such a Network under a single administration is called an “Autonomous System”. So, an autonomous system is a large network or group of networks managed by a single organization. Internet is an integration of millions of such Autonomous System. Each computer is identified by an exclusive IP Address. This helps it in taking part in communicating with the other computers. A packet containing the IP Address of the destination computer gets routed as it passes through the networks to reach its desired destination. How does the packet find its route? It is the routing protocol which defines the route that the packet traverses through. There are two types of routing protocol. Within the Autonomous System, the packet is routed using Interior Routing Protocols like RIP, OSPF, IS-IS and similar others. But if the packet goes to another network under the purview of another organization or another AS, routing takes help of Exterior Routing Protocol. The most pervasive and widely used protocol in this case is Border Gateway Protocol, popularly known as BGP. Any of the routers in the Internet gets the routing information of all the network addresses using BGP. Hence, it can route the traffic in the best available path determined by BGP. Each BGP router stores a routing table with the best routes between autonomous systems. BGP always favors the shortest and the least-cost path as the packet traverses from AS to AS in order to reach the destination network. Truly speaking, BGP is the road map of the Internet.

The URL:

The URL to this platform is: **https://bgpwatch.cgtf.net/**

DragonLab | BGPWatch

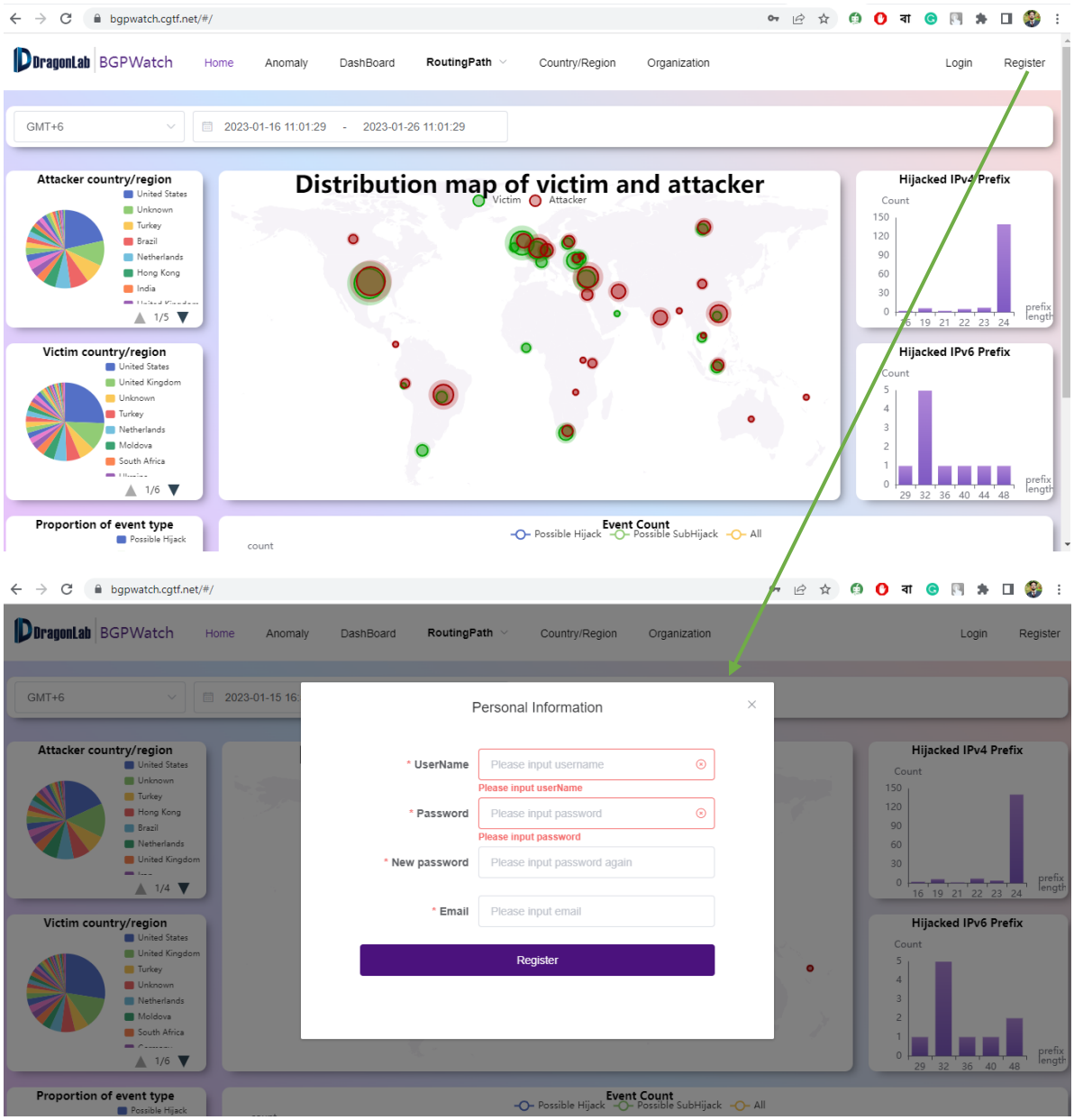
SECTION 1

REGISTRATION AND LOG IN

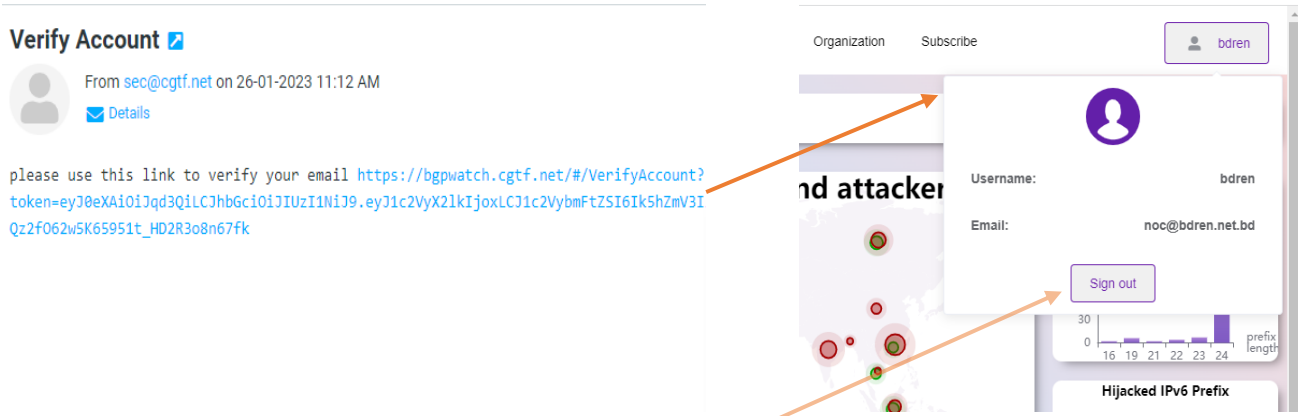
Section 1. Registration and Logging into BGP Watch

Introduction

First, you can register in the BGP Watch by clicking on the “Register” Button located at the top-right corner of the homepage. In the pop-up window, you need to put your username, password [twice for confirmation], and email address in the text boxes and then click on “Register” button to request for your registration. You are going to receive an email from sec@cgtf.net. If you put an username which is already in the system, it will give an error message “Duplicate Username”.

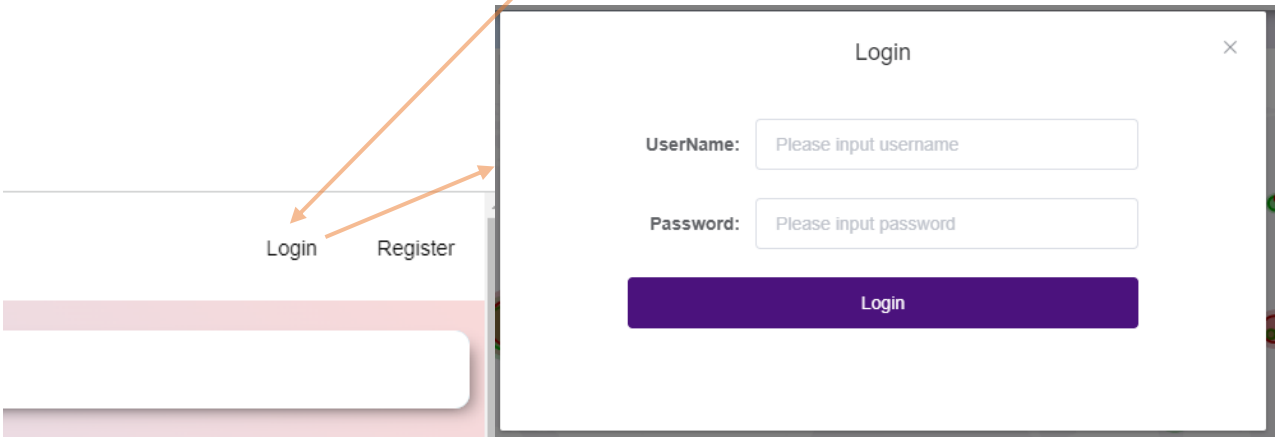


When you confirm your registration by clicking in the link received at your given email address, you will be automatically “logged in” to your account.



You can signout from the site by clicking the "**Sign out**" button.

Next time you log in, you simply click on the this **login** Button and login with your registered username and password. Logged in users will get additional options like Subscription and Email Notifications which is described at section 8.

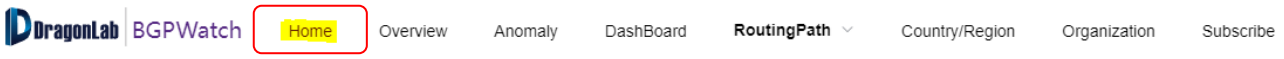


DragonLab | BGPWatch

SECTION 2

HOMEPAGE

Section 2. Homepage



Introduction

Now the question comes whether BGP is a safe protocol in routing the traffic to the desired destination. The answer is both yes and no. Many different ways have been devised out to make BGP routing safe and secured. However, there is route hijacking in BGP which makes it sometimes vulnerable.

So, how does it happen? Each administrator needs to advertise the network prefixes, a combination of IP Addresses, assigned by ICANN/IANA for BGP players to identify the devices configured under its administration. In doing so, if an administrator, intentionally or unintentionally, advertises a prefix which is not assigned by APNIC, then it is called “route hijacking” or BGP hijacking.

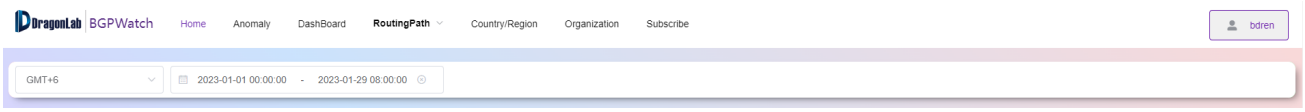
If we compare it with the road traffic system, it’s like placing an incorrect exit in a highway resulting in all traffic destined towards the wrong direction.

This is a very common phenomenon but can result in a severe disaster. We are aware that a few years back, when an ISP inadvertently advertised a YouTube prefix, all YouTube traffic started rushing towards the ISP servers, causing the latter to crash. The fallout was YouTube went offline for hours resulting in not only a huge loss for YouTube, but also a massive discontent among the netizens. In the BGP Watch platform, we can monitor all the past and ongoing BGP hijacking events.

Navigating the page

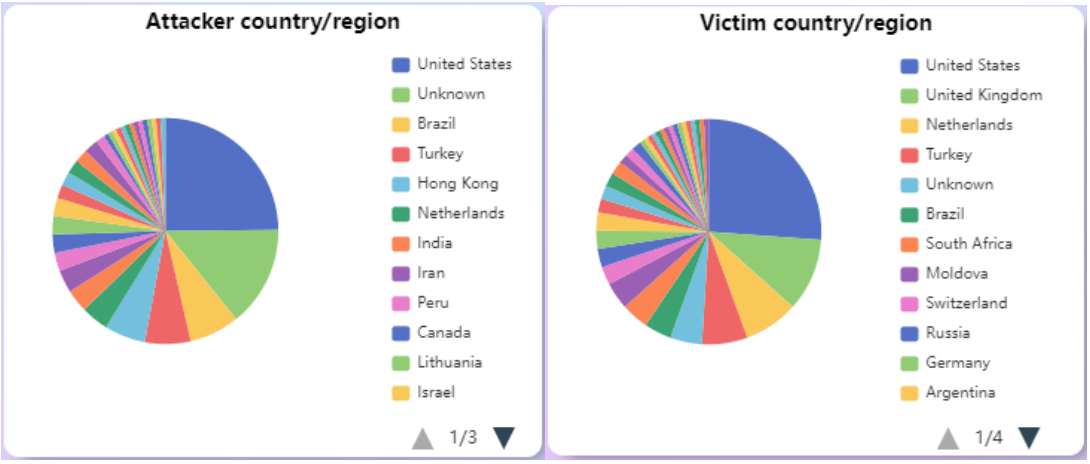
On top of the homepage, there is an <<Time Stamp>> input field for filtering the statistics displayed hereunder. All the following graphs will follow the filter that will be set here. The filter contains:

- Time zone
- Date range [to be picked from calendar]
  - Start Date
  - End Date

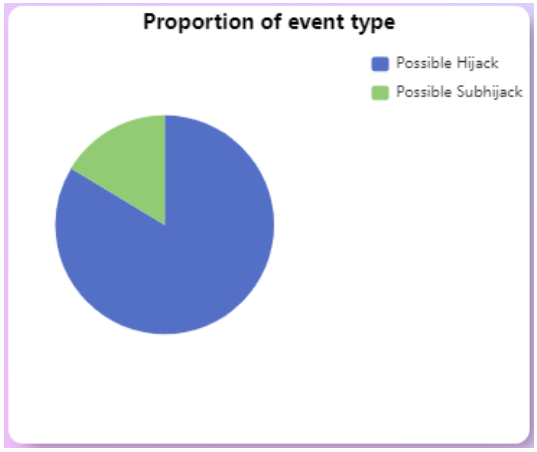


Following the input filter there are four (4) zones:

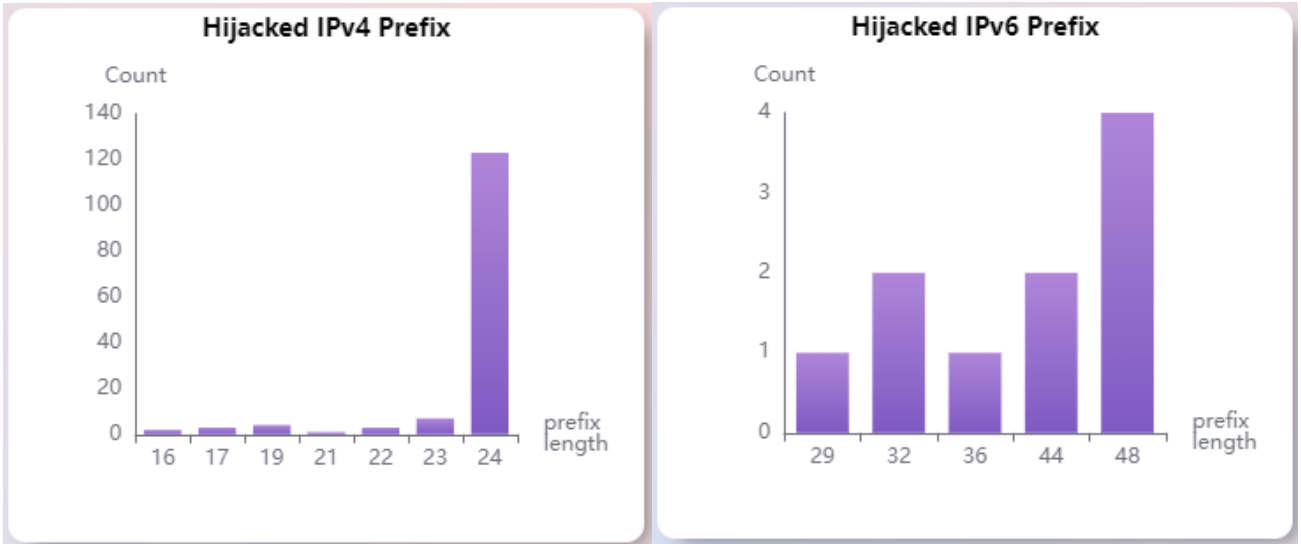
1. Left zone [contains three (3) pie-charts]
   a. The top two (2) charts portray country/region wise distribution of “attackers” and “victims”. Depending on your timestamp filter, you will be able to see: attackers’ and victims’ country/regions. This is an “interactive chart” and you can click on the legends to show or hide statistics of any of these countries.



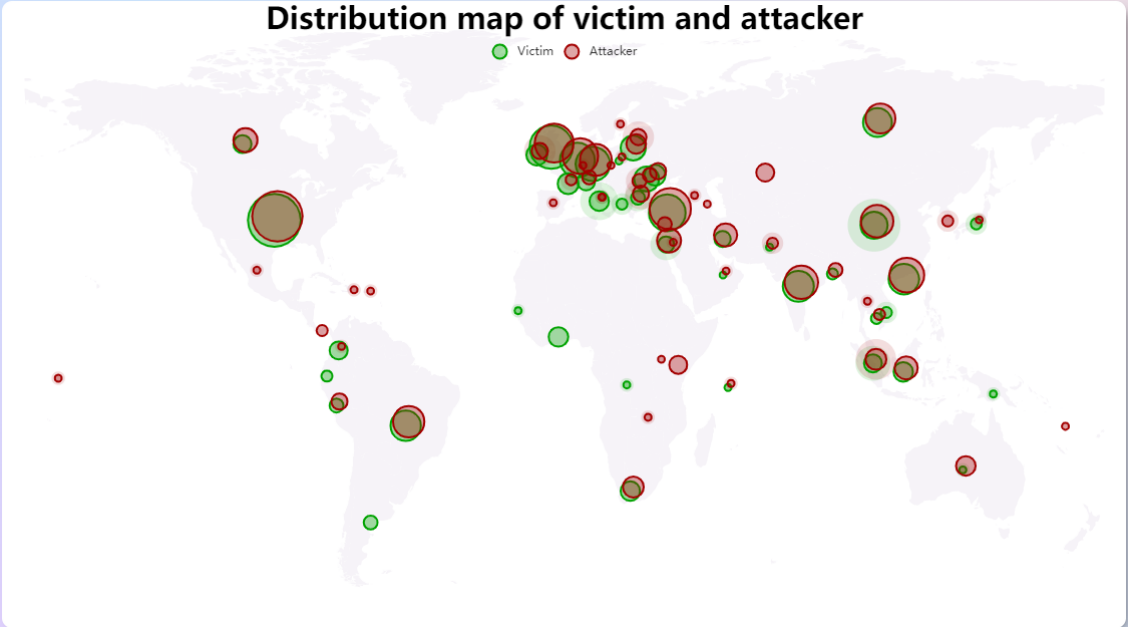
b. The pie-chart at the bottom shows the distribution of "Possible Hijack" and "Possible Subhijack" that took place during selected date range. Hover your mouse on the slices of the pie-graph to show the count of the event.



2. Top-right Zone contains Two bar charts on Hijacked IPv4 and IPv6 Prefix based on prefix length for your selected date range. The "Y-axis" defines the hijack count whereas the "X-axis" defines the prefix-length. Hover your mouse to show the exact count of each bar.

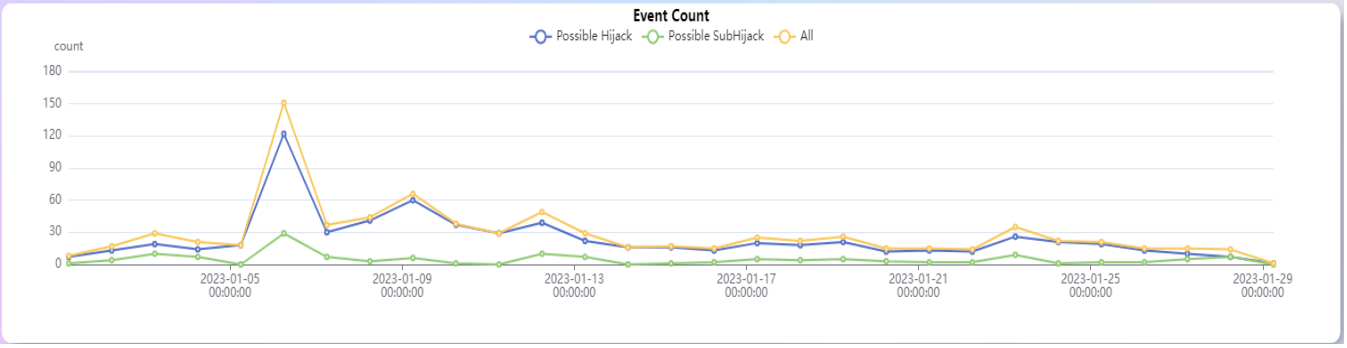


3. The Top-middle zone portrays a worldwide distribution map in the form of a “Bubble Chart” displaying the volume of country-wise Victims and Attackers. Hover your mouse to show the “Country” of the “Attacker” and the “Victim” as well as the “counts” of the event on the selected date range. As it is a bubble chart, “the bigger the bubble, the higher the number of attackers/victims”.



4. The bottom-middle zone displays a line-graph to show the day-wise count of “Possible Hijack”, “Possible Subhijack” and the “Total Hijack” events. Along the X-axis the graph shows the "Date” and Along the Y-axis it shows the “Count of the events”.

   This is an interactive graph as it displays the data if you hover your mouse on any of the lines. You can also click on the Legends to show/hide any of the displayed/hidden line-graph.

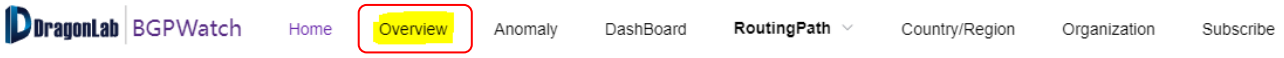


DragonLab | BGPWatch

SECTION 3

OVERVIEW

Section 3. Overview



Introduction

The Overview section shows the global hijacking event count in a bar chart at a varying time period [daily, weekly, monthly and yearly] for a specific country or for the whole world. The same periodic bar chart can also be displayed for different Autonomous System Numbers. The bar chart shows three events:

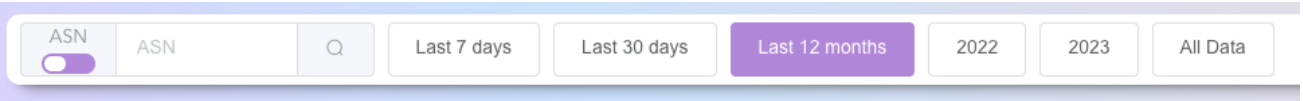
- Possible Hijack
- Possible SubHijack
- Total Hijack

Each of the above events has two players “Victims” and “Attackers” which are displayed only in the displayed chart for a specific country.

Navigating the page

Along the “Y-axis” the number of hijack-counts are displayed whereas along the “X-axis” the time-period is displayed.

On top of the section lies the “filter-bar” [as displayed below] using which you can tailor the graph.



You can filter it on two (2) criteria:

- Based on country
- Based on ASN

By default, it is based on country. But, if you click on the “Selector” button at the beginning of the “filter-bar”, the filter will automatically switch to “ASN”. Data against each of the categories [Country or ASN] can be displayed filtering them over time as follows:

1. Last 7 Days [can be displayed only on Daily basis]
2. Last 30 Days [can be displayed either on Daily or Weekly basis]
3. Last 12 Months [can be displayed on Daily, Weekly or Monthly basis]
4. Years (2022, 2023, years to come) [can be displayed on Daily, Weekly, Monthly or Yearly basis]

Example #1: Showing Global Hijacking Statistics for specific period

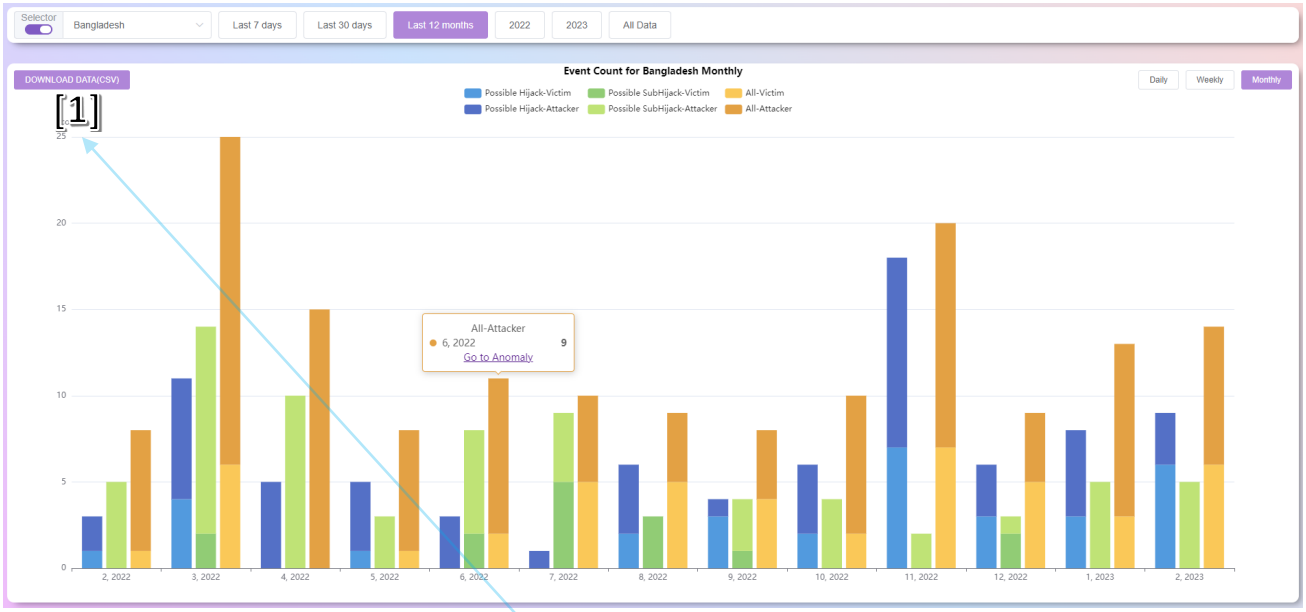
The following screen-shot shows the overall “Possible Hijack”, “Possible SubHijack”, and “Total Hijacks” for the last 12 months. The X-axis shows the “number of months” and Y-axis shows the “hijacked event-counts”.

If you want to filter the data based on other time period like “Last 7 days”, or “Last 30 days” or for any particular year, you can just click on the appropriate button in the “filter-bar” to display the statistics for the desired time period.

You can also select any country from the drop-down menu **[5]** or toggle to the AS number mode and search **[6]** with your desired AS number.

Example #2: Displaying Statistics for a specific country

If you select the text box for keying in the name of the country/region [indicated by "5" in the above example] and accordingly key-in the name as "Bangladesh" as indicated in the following figure, you are going to get the statistics for the hijacking with Bangladesh as "Victims" or "Attackers" in a "Stacked-Bar" graph.



This bar chart will show you the hijack-count of six (6) events:

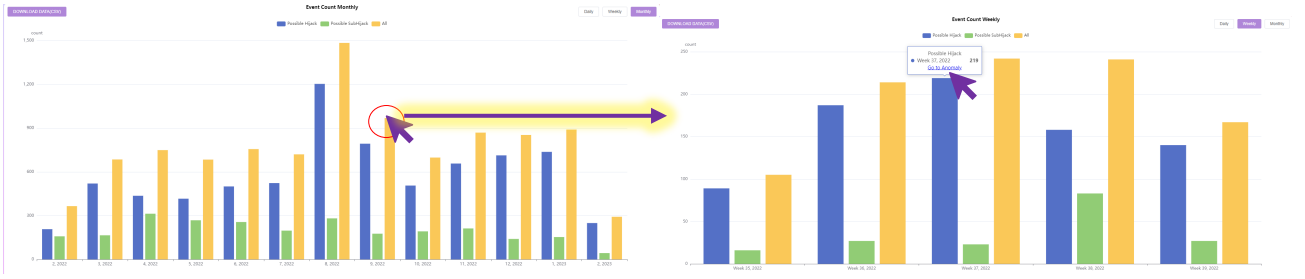
- Possible Hijack-Victim
- Possible Hijack-Attacker
- Possible SubHijack-Victim
- Possible SubHijack-Attacker
- All-Victim
- All-Attacker

on the Y-axis it is the hijack-count and on the "X-axis" it is the periodicity number of days, number of weeks or number of months based on your selection of "Daily", "Weekly" or "Monthly" button respectively at the top-right corner right above the Chart.

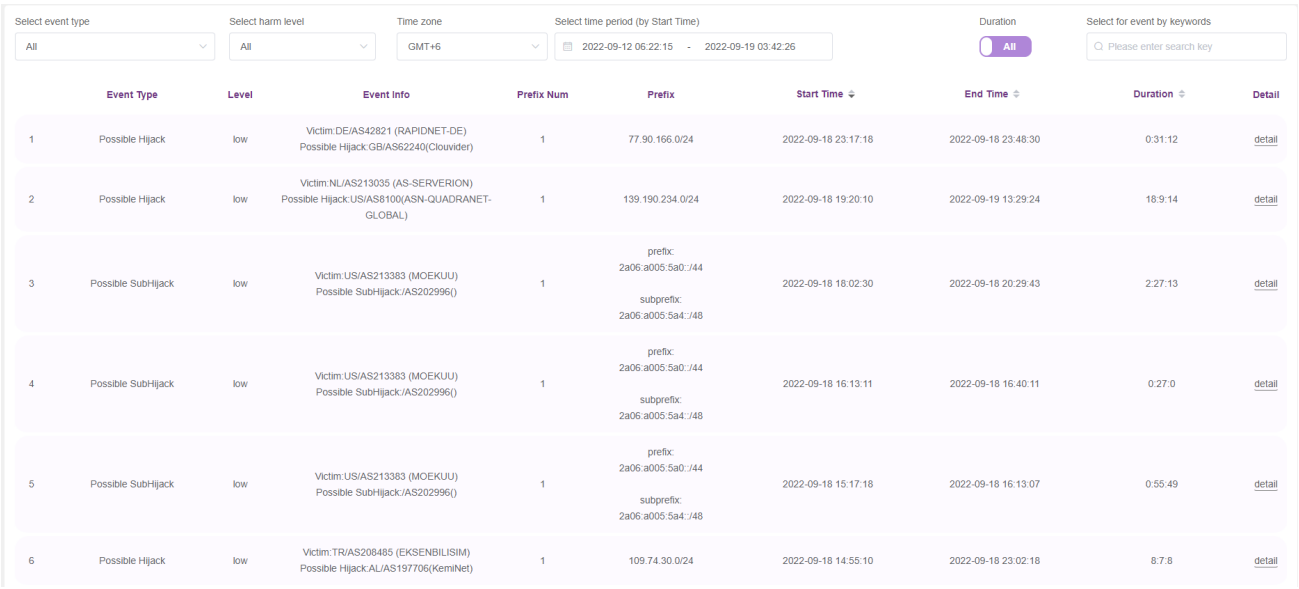
You can click on the graph legends in order to toggle the display of the graph. You can download and save the displayed graph-statistics by clicking the "Download Data (CSV)" button [1] at the top-left corner right above the displayed Chart.

Hover your mouse on top of each bar if you want to know the value of a particular bar. Click on any the bars if you want to switch the view from "Yearly to Monthly", or from "Monthly to Weekly", or from "Weekly to Daily" statistics. The same can be done using the "Daily", "Weekly" or "Monthly" button respectively at the top-right corner right above the Chart.

As displayed below clicking a bar displaying "Monthly" statistics switched it to "Weekly" statistics for that particular month.



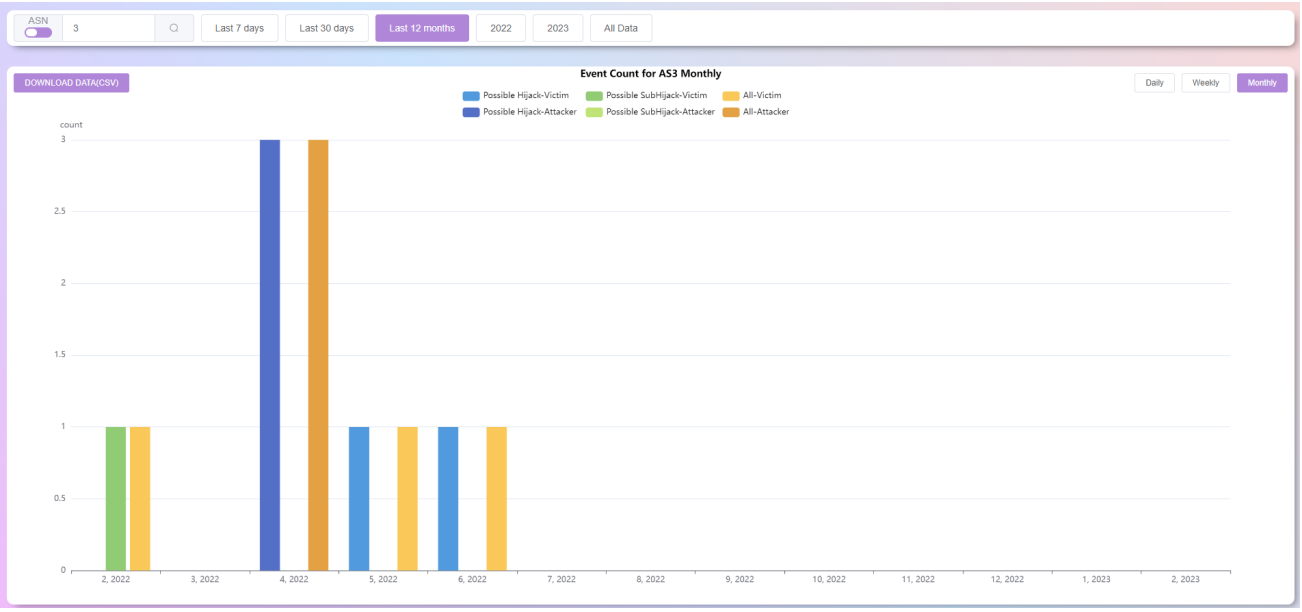
If you want to go to the Details of events for a desired time period of a bar, hover your mouse to the bar defining the statistics of the desired time period and click on ‘Go to Anomaly’. You will be redirected to ‘Anomaly’ section which is discussed in Section 4.



	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Possible Hijack	low	Victim:DE/AS42821 (RAPIDNET-DE) Possible Hijack:GB/AS62240(Clouvider)	1	77.90.166.0/24	2022-09-18 23:17:18	2022-09-18 23:48:30	0:31:12	detail
2	Possible Hijack	low	Victim:NL/AS213035 (AS-SERVERION) Possible Hijack:US/AS8100(ASN-QUADRANET-GLOBAL)	1	139.190.234.0/24	2022-09-18 19:20:10	2022-09-19 13:29:24	18:9:14	detail
3	Possible SubHijack	low	Victim:US/AS213383 (MOEKUU) Possible SubHijack:/AS202996()	1	prefix: 2a06:a005:5a0::/44 subprefix: 2a06:a005:5a4::/48	2022-09-18 18:02:30	2022-09-18 20:29:43	2:27:13	detail
4	Possible SubHijack	low	Victim:US/AS213383 (MOEKUU) Possible SubHijack:/AS202996()	1	prefix: 2a06:a005:5a0::/44 subprefix: 2a06:a005:5a4::/48	2022-09-18 16:13:11	2022-09-18 16:40:11	0:27:0	detail
5	Possible SubHijack	low	Victim:US/AS213383 (MOEKUU) Possible SubHijack:/AS202996()	1	prefix: 2a06:a005:5a0::/44 subprefix: 2a06:a005:5a4::/48	2022-09-18 15:17:18	2022-09-18 16:13:07	0:55:49	detail
6	Possible Hijack	low	Victim:TR/AS208485 (EKSENBILISIM) Possible Hijack:AL/AS197706(KemiNet)	1	109.74.30.0/24	2022-09-18 14:55:10	2022-09-18 23:02:18	8:7:8	detail

Example-3: Displaying Statistics for an ASN

If you toggle the button [6] to ASN mode, the dropdown [5] will convert into the ASN search mode. you can put your desired AS in the search field. The system will return you the statistics for the hijacking events for the searched ASN as “Victims” or “Attackers” in a bar chart.



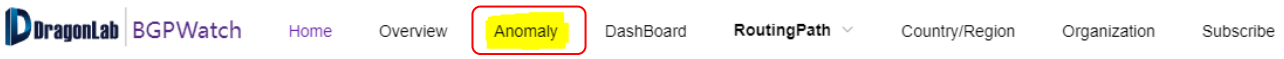
This in example above, you can see bar chart of the hijacking events for the last 12 months in the monthly periodicity for the searched ASN 3. The rest is same as shown in example 2.

DragonLab | BGPWatch

SECTION 4

ANOMALY

Section 4. Anomaly Events



Introduction

In the “Anomaly” section all of BGP hijacking is reported in different categories. There are two major categories of hijacking:

- **Possible Hijack:** A “Possible Hijack” refers to a BGP hijacking attack that targets the entire block that has been allocated. By advertising the entire prefix, an attacker can redirect traffic intended for a full network within the legitimate network to a malicious destination.
  For example, if the legitimate network is assigned the IP address block 192.168.0.0/16, an attacker can hijack the full prefix such as 192.168.0.0/16, which represents full-network containing multiple hosts or services. By advertising a route for this prefix, the attacker can redirect traffic intended for the full network to their own network, where it can be monitored or manipulated.

- **Possible SubHijack:** A “Possible SubHijack” refers to a BGP hijacking attack that targets a more specific sub-prefix of an IP address block rather than the entire block. By advertising a more specific route announcement for a sub-prefix, an attacker can redirect traffic intended for a specific host or service within the legitimate network to a malicious destination.
  For example, if the legitimate network is assigned the IP address block 192.168.0.0/16, an attacker can subhijack a more specific prefix such as 192.168.1.0/24, which represents a sub-network containing a particular host or service. By advertising a route for this sub-prefix, the attacker can redirect traffic intended for the specific host or service to their own network, where it can be monitored or manipulated.

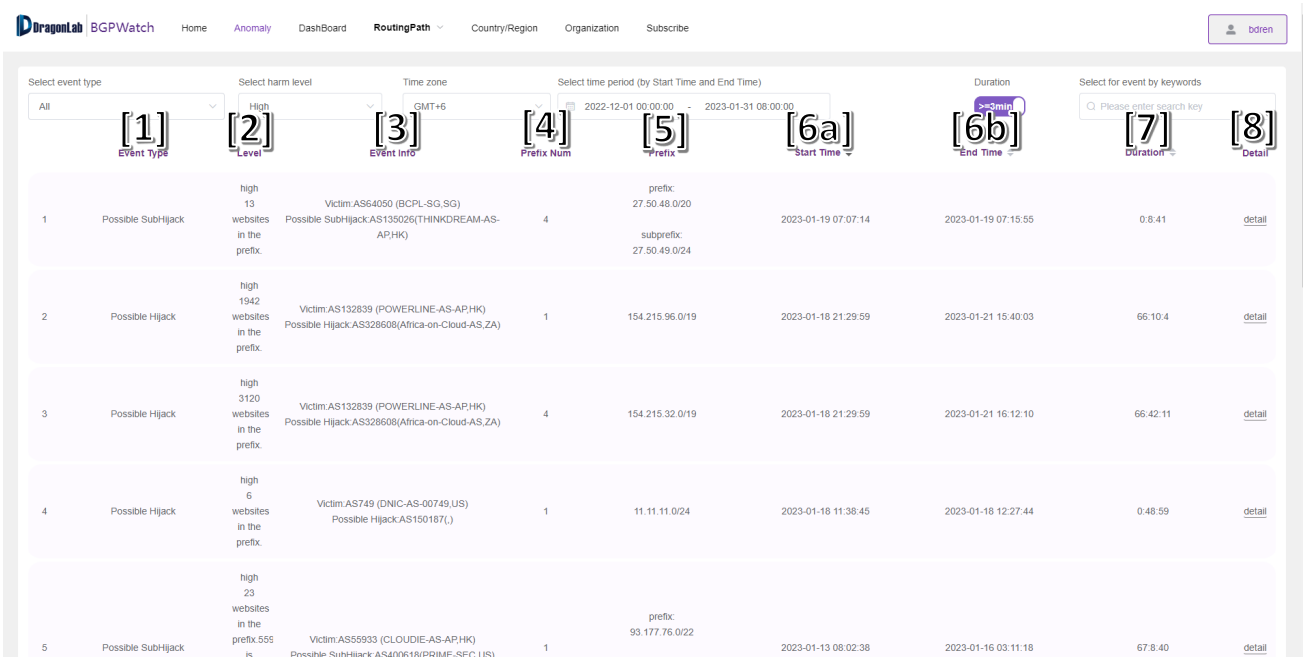
For each of the above categories there can be two (2) events. “Ongoing” if the event is continuing and “Terminated” if the event is already ended. For the “Terminated” one the event will be branded either as Possible Hijack or Possible SubHijack depending on the type of Hijack. For “Ongoing” one, the event will be termed as “Ongoing Possible Hijack” or “Ongoing Possible SubHijack”.

Each type of events is also tagged with the "level of damage” with “High”, “Medium” and “Low” level. When the number of websites contained in the hijacked prefix is greater than 5, the event is high level; when the number of websites contained in the hijacked prefix is greater than 1 but less than 5 or the victim AS is an IDC/CDN or a top ICP, the event is middle level, otherwise the event is low level.

Each event is also tagged with “Event Info” which further describes the event, number of prefixes and the particular prefix, start time, end time and duration of the event. As mentioned, if the event is “Ongoing”, there will be no associated “Endtime” and also the “Duration” field will remain blank.

Navigating the page

Click on "A**nomaly"** on the main menu. The following information will come up:



On this page, you will see a table populated with data in the following structure:

[1] Hijacking event type

Filled in Data

a. Possible Hijack
b. Possible SubHijack
c. Ongoing Possible Hijack
d. Ongoing Possible SubHijack

[2] Level of harm

Filled in Data

a. High
b. Medium
c. Low

[3] Event Information

a. Attacker and Victim AS Name and AS Number

[4] Number of Prefixes

[5] Prefix and subprefix

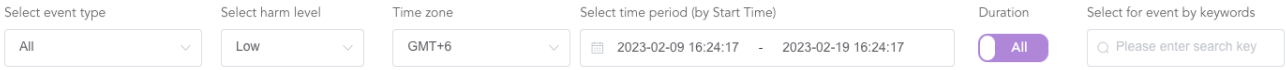
[6] Start and End Time of the hijack

[7] Duration

[8] Link to details of the hijacking event

There is a "Filter-bar" atop as follows:

[A] [B] [C] [D] [E]



You can filter the information placed in the table by putting data in the "Filter-bar". The fields that are available for such filtering are:

[A] event type {Possible Hijack, Possible SubHijack, Possible Hijack Ongoing, Possible SubHijack Ongoing} [needs selection from Pulldown menu]

[B] harm level {All, High, Middle, Low} [needs selection from pulldown menu]

[C] time period {Time zone, Start Time, End Time} [Time zone -> needs selection from pulldown menu, Start Time and End Time -> can be selected from Calendar]

[D] Duration {All, >= 3min} [a Toggle Button]

[E] Select for Events by Keyword {keywork placed in the Event Type, Level and Event Info field} [needs to key in the text to be searched. you can put any text/number like – AS number, Country, AS name etc for a wider array of filtering]

Sample Description of the Data placed in the Table

Example #1: Possible Hijack

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Possible Hijack	low	Victim:GB/AS212238 (CDNEXT) Possible Hijack:US/AS54103(MODMC)	1	154.16.199.0/24	2023-02-19 00:52:26	2023-02-19 01:22:11	0:29:45	detail

From the excerpts of the data displayed above, it is well understood that

- This is a "Possible Hijack" event with low level of damage.
- The victim is AS212238 which is located in Great Britain/United Kingdom.
- The Possible Hijacker is from USA with AS54103.
- One (1) Prefix 154.16.199.0/24 is possibly hijacked.
- Start Time of Hijacking: 19 Feb 2023 at 00:52:26 with the TZ selected in the "Filter-bar"
- End Time of Hijacking: 19 Feb 2023 at 01:22:11 with the TZ selected in the "Filter-bar"
- Duration of Hijacking is: 29 minutes 45 seconds

Example #2: Possible SubHijack

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Possible SubHijack	low	Victim:GB/AS52037 (y-internet) Possible SubHijack:US/AS834(IPXO)	2	prefix: 46.37.120.0/23 subprefix: 46.37.120.0/24	2023-02-17 14:04:07	2023-02-17 18:05:59	4:1:52	detail

From the excerpts of the data displayed above, it is well understood that

- This is a “Possible SubHijack” event with “low” level of damage.
- The victim is AS52037 which is located in Great Britain/United Kingdom.
- The Possible Hijacker is from USA with AS834.
- One sub-prefix 46.37.120.0/24 of the full prefix 46.37.120.0/23 is possibly hijacked.
- Start Time of Hijacking: 17 Feb 2023 at 14:04:07 with the TZ selected in the “Filter-bar”
- End Time of Hijacking: 17 Feb 2023 at 18:05:59 with the TZ selected in the “Filter-bar”
- Duration of Hijacking is: 4 hours 01 minutes 59 seconds

Example #3: Ongoing Possible Hijack

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible Hijack	low	Victim:GB/AS61317 (ASDETUK) Ongoing Possible Hijack:TR/AS210703(TR-MARKAHOST)	1	192.177.65.0/24	2023-02-19 06:52:02	-	-	detail

From the excerpts of the data displayed above, it is well understood that

- This is a “Ongoing Possible Hijack” [the hijacking is still on] event with “low” level of damage.
- The victim is AS61317 which is located in Great Britain/United Kingdom.
- The Possible Hijacker is from Turkey with AS210703.
- One Prefix 192.177.65.0/24 is possibly hijacked.
- Start Time of Hijacking: 19 Feb 2023 at 06:52:02 with the TZ selected in the “Filter-bar”
- End Time is missing as it is an “ongoing” hijack
- Duration is missing as it is an “ongoing” hijack

Example #4: Ongoing Possible SubHijack

	Event Type	Level	Event Info	Prefix Num	Prefix	Start Time	End Time	Duration	Detail
1	Ongoing Possible SubHijack	low	Victim:GB/AS49999 (BANDWIDTHTECH-AS) Ongoing Possible SubHijack:DE/AS58212(DATAFOREST)	1	prefix: 195.133.12.0/22 subprefix: 195.133.12.0/24	2023-02-18 20:26:58	-	-	detail

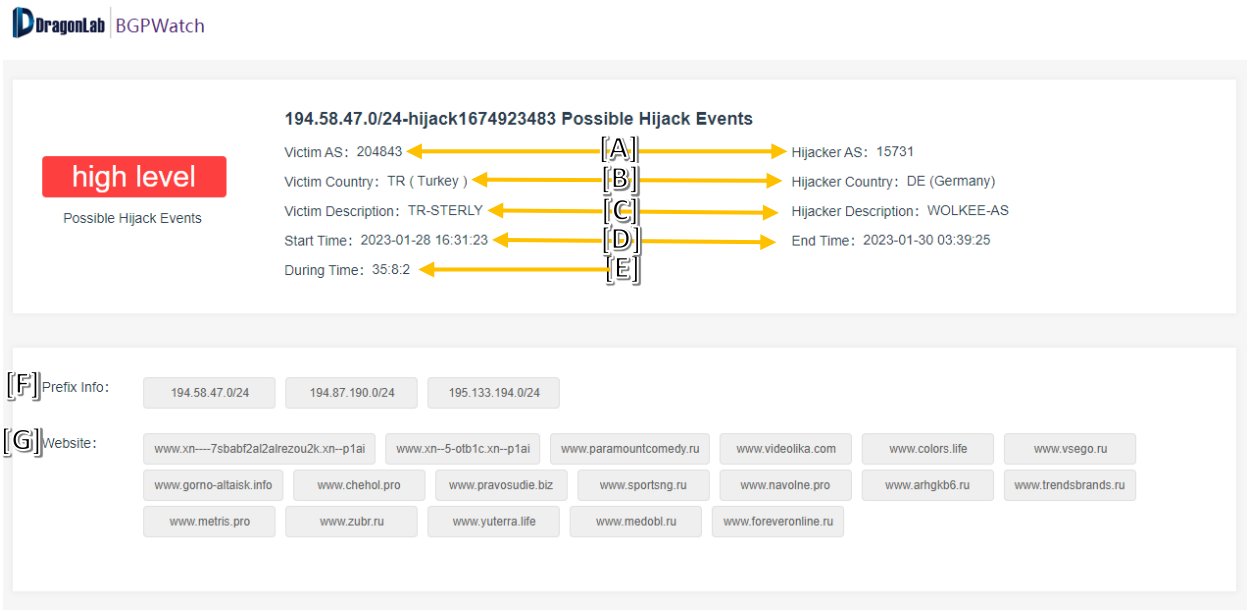
From the excerpts of the data displayed above, it is well understood that

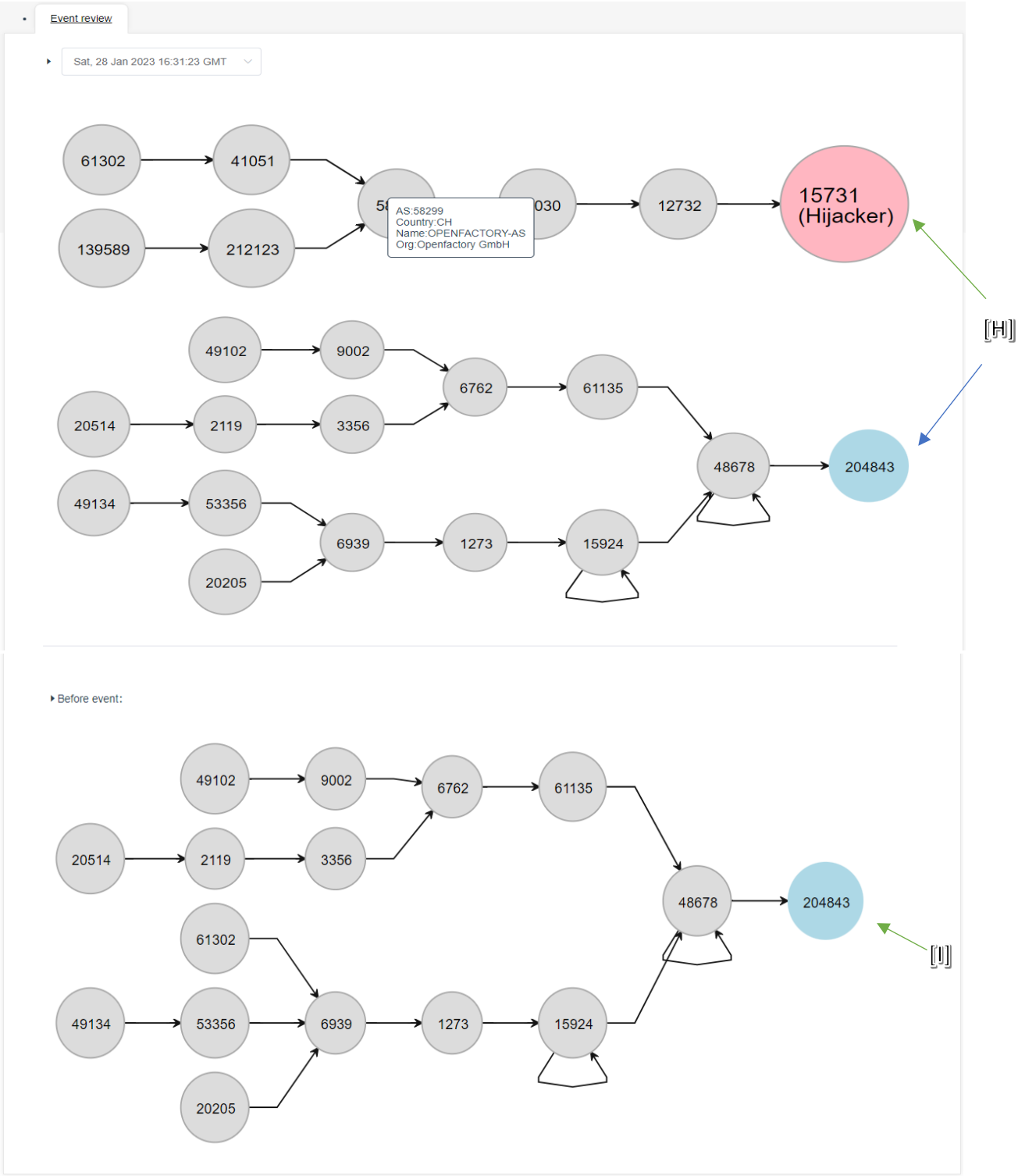
- This is a “Ongoing Possible SubHijack” [the hijacking is still on] event with “low” level of damage.
- The victim is AS49999 which is located in Great Britain/United Kingdom.
- The Possible Hijacker is from Denmark with AS58212.
- One subprefix 195.133.12.0/24 is possibly hijacked out of the full prefix of 195.133.12.0/22.
- Start Time of Hijacking: 18 Feb 2023 at 20:26:58 with the TZ selected in the “Filter-bar”
- End Time is missing as it is an “ongoing” hijack
- Duration is missing as it is an “ongoing” hijack

Anomaly Event Details:

If you want to see the hijacking event details, click on the details button which is placed at the end of each record. On this page, you will be able to see the details of the prefix that has been hijacked. They are-

(A) Victim and Hijacker AS
(B) Victim and Hijacker Country
(C) Victim and Hijacker Description
(D) Start and End Time
(E) Duration
(F) Prefix Information
(G) Websites that have been affected under this prefix
(H) Routing paths after hijacking for Hijacker AS and Victim AS
(I) Routing path before hijacking for Victim AS





In the example above, as you can see, after hijacking, AS61302 failed to find its destination to AS204843 for IP prefix 194.58.47.0/24 for which the owner is AS204843.

- Correct Route: AS61302 => AS6939 => AS1273 => AS15924 => AS48678 => AS204843 [Victim]
- Hijacked Route: AS61302 => AS41051 => AS58299 => AS13030 => AS12732 => AS15731 [Hijacker]

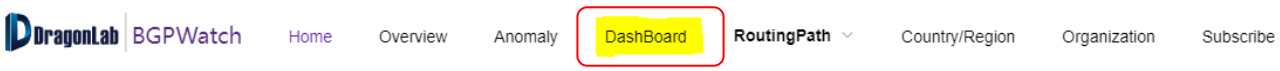
All of its traffic was redirected to the hijackers' AS15731. So now, the users of AS61302 will not be able to find any of the addresses or the websites inside AS204843, as shown in [G].

DragonLab | BGPWatch

SECTION 5

DASHBOARD

Section 5. Dashboard

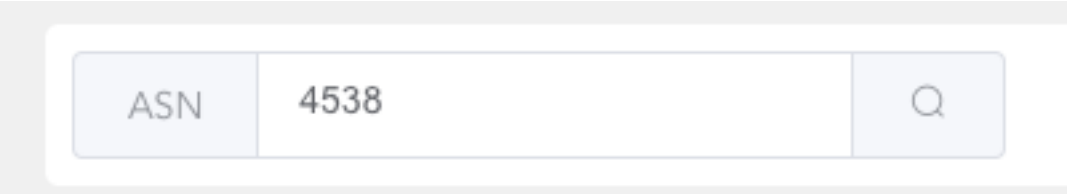


Introduction

The “Dashboard” contains ASN wise information on Name of the organization holding the ASN, Country in which the organization belongs and the Autonomous System Name. It will also contain details of advertised IPv4 and IPv6 prefixes. It displays the other Autonomous Systems the particular AS is peering to through both IPv4 and IPv6 addresses. At the same time the number of prefixes, both IPv4 and IPv6, that are being exchanged with the peered ASes are also displayed.

Navigating the page

If you click on the “Dashboard” button you will come up with a page having the following “Filter-bar” at the top:



You can key-in whatever ASN you want the information about.

Once you key in the ASN and click the “Search” glass at the right the information about the ASN will be displayed in three (3) exclusive sections as follows:

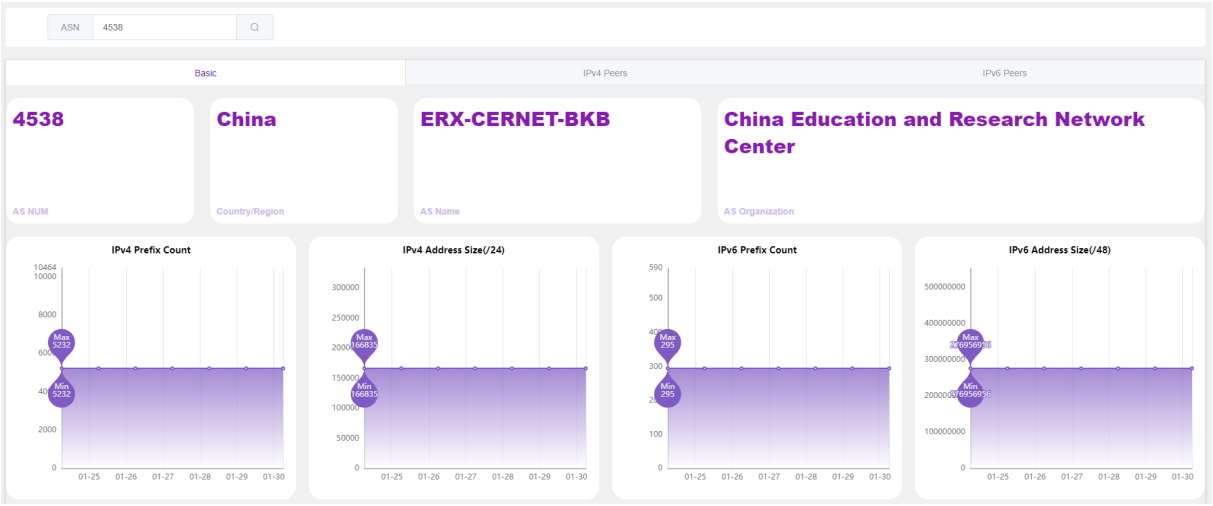
You can observe that the portal contains three (3) tabs.

- Basic
- IPv4 Peers
- IPv6 Peers

Basic:

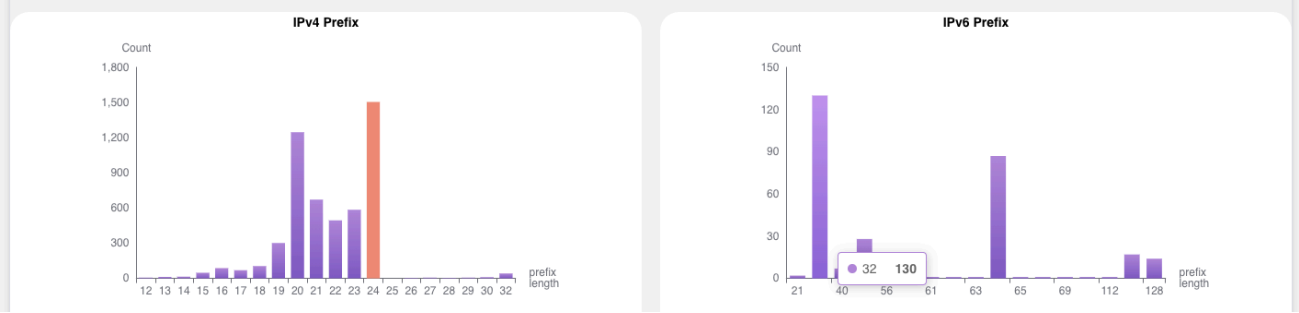
If you click on the “Basic” Tab, you will be able to find AS-wise IPv4 and IPv6 prefix information based on your searched “AS number”. The information is displayed under the following sections/fields:

(A) Country/Region
(B) AS Name
(C) AS Organization
(D) Max and Min Count of IPv4 Prefix of the last 7 days (Originated)
(E) Number of /24 IPv4 Addresses of the last 7 days (Originated)
(F) Max and Min Count of IPv6 Prefix of the last 7 days (Originated)
(G) Number of /48 IPv6 Addresses of the last 7 days (Originated)



At the bottom two (2) bar graphs are displayed having counts of advertised prefixes in the “Y-axis” and prefix-length in the “X-axis” both for IPv4 and IPv6 side-by-side as follows as follows:

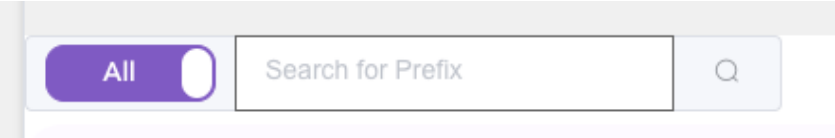
As you hover through the bards the actual count will be displayed. As implied from the above bar graph at the left the AS advertises 1505 IPv4 prefixes with /24 prefix-length.



Similarly, as shown in the above screenshot the concerned AS advertises 130 IPv6 prefixes with /32 prefixes.

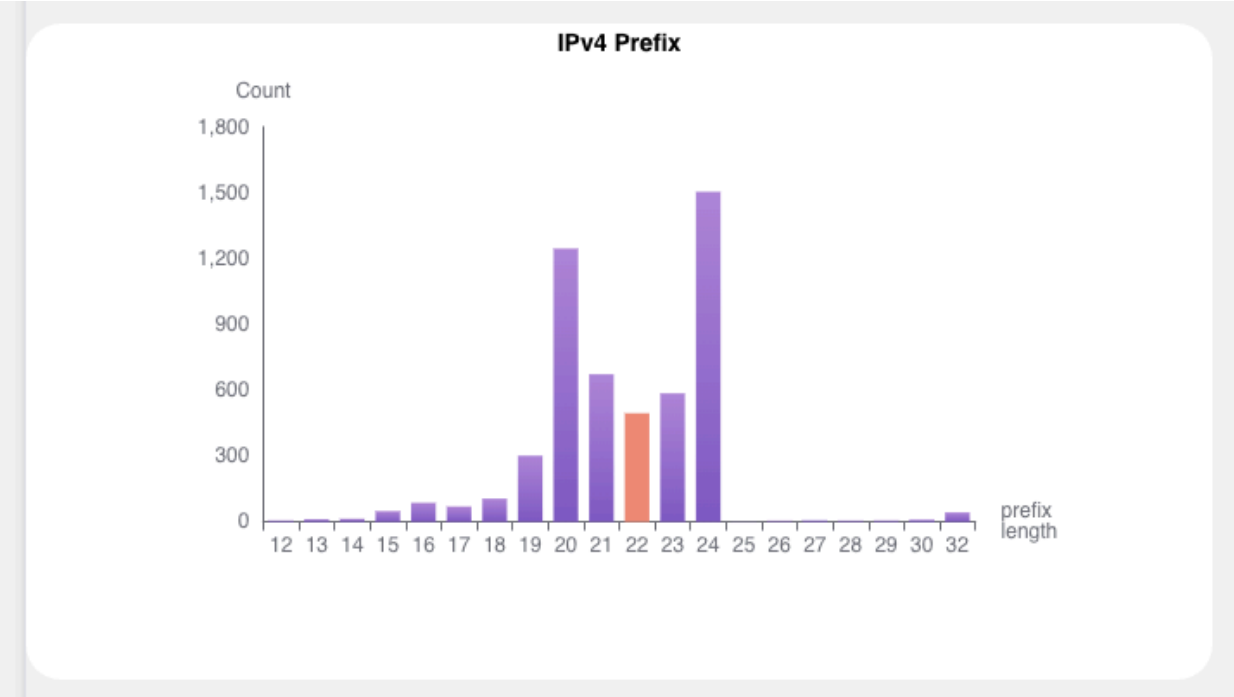
At the bottom of the page, you will find a table that shows IP Prefix lists that have originated from the selected AS. The toggle button on the top-left section can be used to display “All” or “Selected” advertised prefixes. If the toggle button is set to “All”, all prefixes will be listed. If the button is set to “Selected”, the advertised-prefix having prefix length in the selected “bar chart” displayed in “Orange” color will be listed.

The listed prefixes can be filtered on any string by placing the searched string in the search box displayed below:

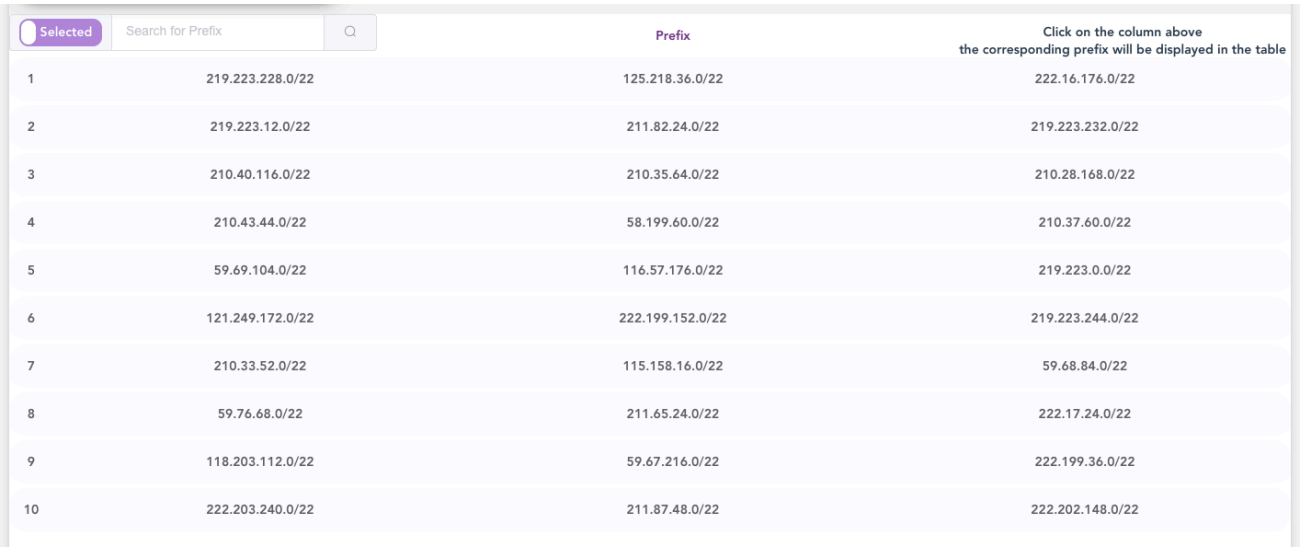


Example #1: Listing all prefixes with /22 length under IPv4 Prefix.

In the “Bar Graph” click on the bar having prefix-length of 22 bit along the “X-axis”



The “Toggle” button will automatically shift from “All” to “Selected” and the following information with /22 prefix-length will be displayed:

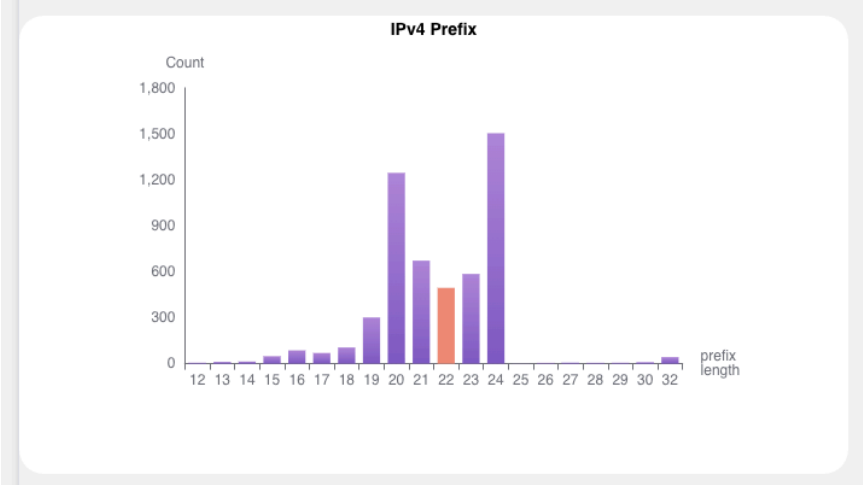


Selected | Search for Prefix

	Prefix		Click on the column above the corresponding prefix will be displayed in the table
1	219.223.228.0/22	125.218.36.0/22	222.16.176.0/22
2	219.223.12.0/22	211.82.24.0/22	219.223.232.0/22
3	210.40.116.0/22	210.35.64.0/22	210.28.168.0/22
4	210.43.44.0/22	58.199.60.0/22	210.37.60.0/22
5	59.69.104.0/22	116.57.176.0/22	219.223.0.0/22
6	121.249.172.0/22	222.199.152.0/22	219.223.244.0/22
7	210.33.52.0/22	115.158.16.0/22	59.68.84.0/22
8	59.76.68.0/22	211.65.24.0/22	222.17.24.0/22
9	118.203.112.0/22	59.67.216.0/22	222.199.36.0/22
10	222.203.240.0/22	211.87.48.0/22	222.202.148.0/22

Example #2: Listing all prefixes containing 210 and having /22 prefix length

In the “Bar Graph” click on the bar having prefix-length of 22 bit along the “X-axis”



The “Toggle” button will automatically shift from “All” to “Selected” and the following information with /22 prefix-length will be displayed:

Selected | Search for Prefix

	Prefix		Click on the column above the corresponding prefix will be displayed in the table
1	219.223.228.0/22	125.218.36.0/22	222.16.176.0/22
2	219.223.12.0/22	211.82.24.0/22	219.223.232.0/22
3	210.40.116.0/22	210.35.64.0/22	210.28.168.0/22
4	210.43.44.0/22	58.199.60.0/22	210.37.60.0/22
5	59.69.104.0/22	116.57.176.0/22	219.223.0.0/22
6	121.249.172.0/22	222.199.152.0/22	219.223.244.0/22
7	210.33.52.0/22	115.158.16.0/22	59.68.84.0/22
8	59.76.68.0/22	211.65.24.0/22	222.17.24.0/22
9	118.203.112.0/22	59.67.216.0/22	222.199.36.0/22
10	222.203.240.0/22	211.87.48.0/22	222.202.148.0/22

Then, place “210.” To list the prefixes containing only “210.”. The display will be as follows:

Selected | 210.

	Prefix		Click on the column above the corresponding prefix will be displayed in the table
1	210.40.116.0/22	210.35.64.0/22	210.28.168.0/22
2	210.43.44.0/22	210.37.60.0/22	210.33.52.0/22
3	210.30.16.0/22	210.40.112.0/22	210.33.132.0/22
4	210.28.120.0/22	210.39.104.0/22	210.32.24.0/22
5	210.29.144.0/22	210.33.116.0/22	210.35.0.0/22
6	210.43.40.0/22	210.47.12.0/22	210.32.48.0/22
7	210.33.8.0/22	210.31.96.0/22	210.37.24.0/22
8	210.38.60.0/22	210.33.40.0/22	210.35.168.0/22
9	210.41.220.0/22	210.44.244.0/22	210.38.56.0/22

IPv4 Peers:

If you select the “IPv4 Peers” tab, you will find a connectivity diagram of IPv4 BGP neighbors of selected AS. You can select and unselect the display of connectivity to the peers by clicking on the type of peering legend at the top-right of the diagram [1].

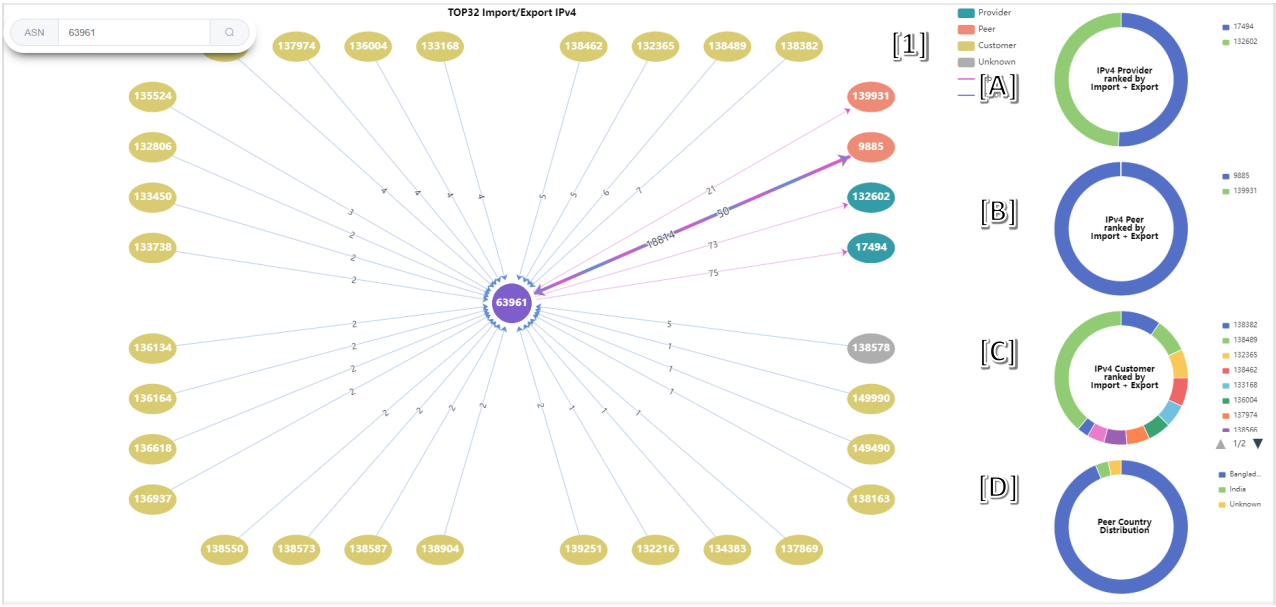
On the right side of this diagram, you will find the pie chart of the top ten peers ranked by sum of advertised and received prefixes [import plus export].

[A] Based on IPv4 Providers

[B] Based on IPv4 Peers

[C] Based on IPv4 Customers

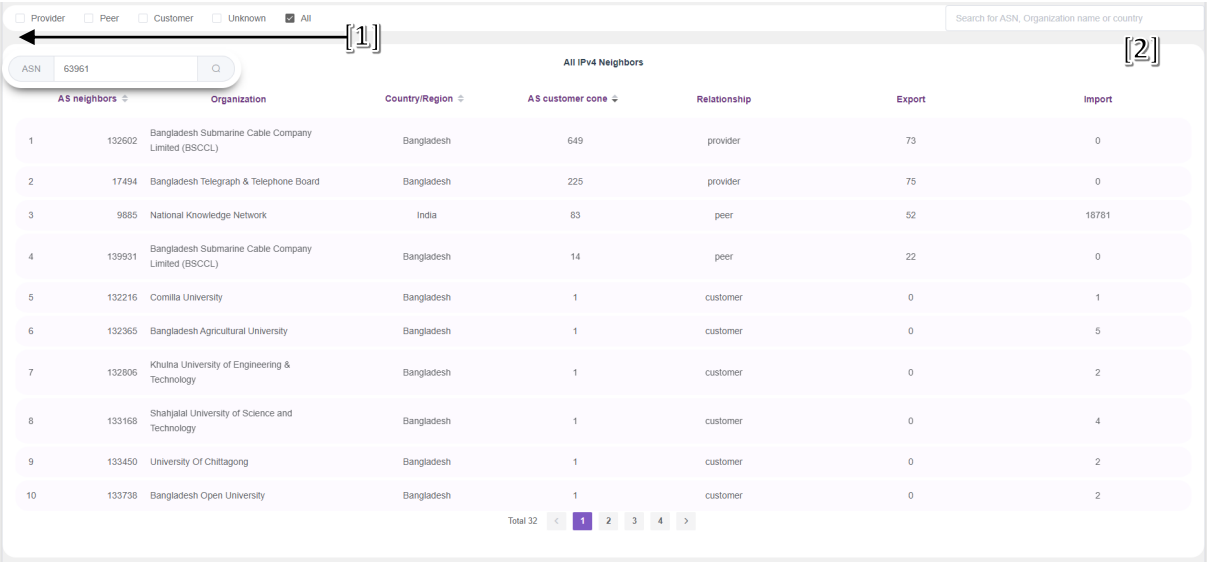
[D] Based on Peer Country



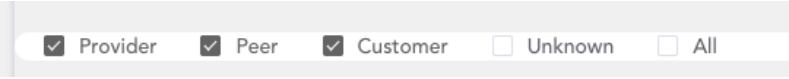
Along the line connecting the peers, the number of prefixes that are being received and advertised respectively from and to the providers, peers, and customers are displayed.

In this picture, you can see that the AS63961 has many neighbors including customers, peers and providers. If you hover your mouse on top of any link, you will be able to find the number of prefixes that the AS63961 is importing from or exporting to. For example, AS63961 is importing 18814 prefixes from its neighbor peer AS9885 and exporting 50 prefixes to it.

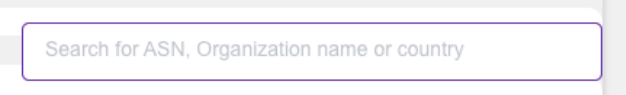
Below that, you will find a table that shows all the BGP neighbors’ AS numbers, organization name, Country/Region, AS customer cone, relationship with that neighbors, and number of prefixes that the selected AS is importing from or exporting to.



You can filter [1] this table based on the neighbor type (provider, peer, customer, unknown, all) using the check boxes in the “Filter-tab” right at the top-left side of the Table displayed as follows:

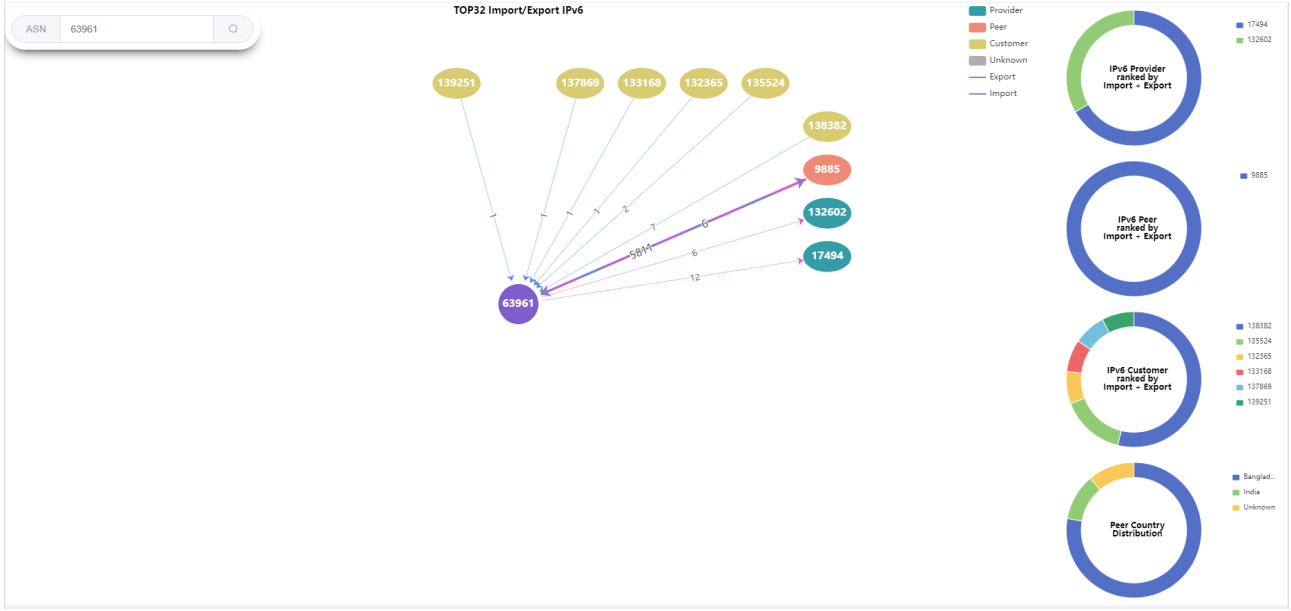


As shown above by default all the “Provider”, “Peer” and “Customer” neighbors are selected. You can also search [2] for ASN, Organization or Country in this table using the search field at the top-right side of the Table displayed as follows:



IPv6 Peers:

In the IPv6 Peers tab, you will find the same information as you are getting from the IPv4 tab, except that the information is based on IPv6 BGP neighbors.

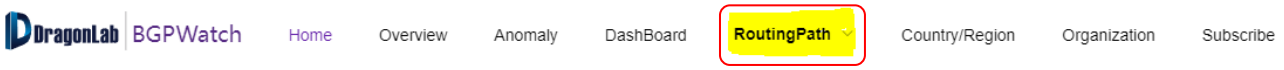


DragonLab | BGPWatch

SECTION 6

ROUTING PATH

Section 6. Routing Path



Introduction

BGP uses both forward and reverse routing paths to determine the best path for data packets to take to reach their destination.

In BGP, the forward routing path is used to determine the best route for a data packet to take from its source to its destination. The router evaluates various attributes of the different paths, such as the length of the path and the origin of the prefix, to determine the best route. The best route is then added to the BGP routing table and used to forward data packets.

The reverse path shows how a data packet is routed from an AS to a prefix of your AS.

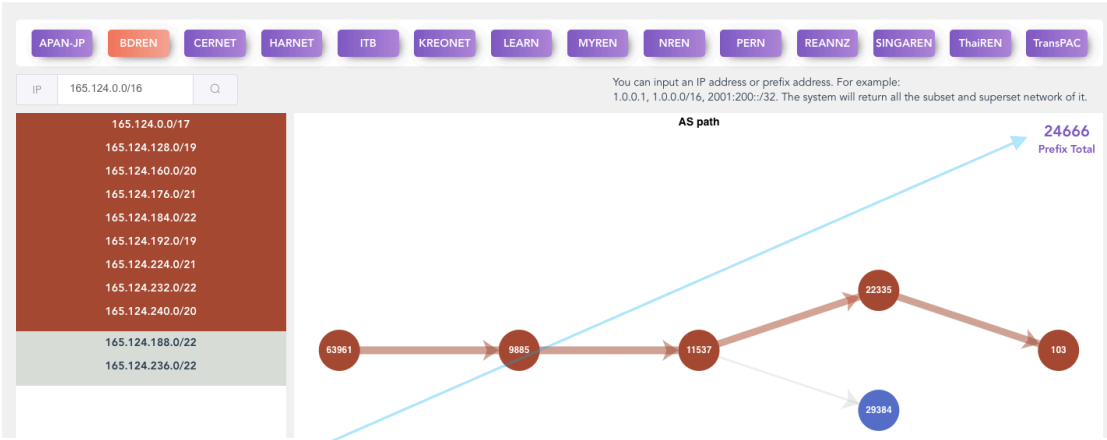
This specific menu option will give you information in four (4) different categories:

- Routing Path: provides you the forward routing path to a given prefix from the selected NREN.
- Reverse Routing Path: provides you the routing path from other ASes to a particular prefix. Usually operators are interested how traffic is routed to their network.
- Reverse Routing Path (Topology): provides you the full topology of reaching a particular prefix.
- Bi-Routing Path: provides you both the forward path and the reverse path between two selected prefixes.

Navigating the page

Routing path

In the routing path option (selecting “Routing Path” submenu under “Routing Path” menu), you will have to select the NRENs as a source from the “buttoned list” above and input an IP prefix or address as a destination, they can be either IPv4 or IPv6. The system will return paths of all sub networks and super networks of the input prefixes (destination) from the selected NREN (source) on the left. The sub / super networks have different length, with /17, /19, etc. This illustrates the fine-grained routing features.

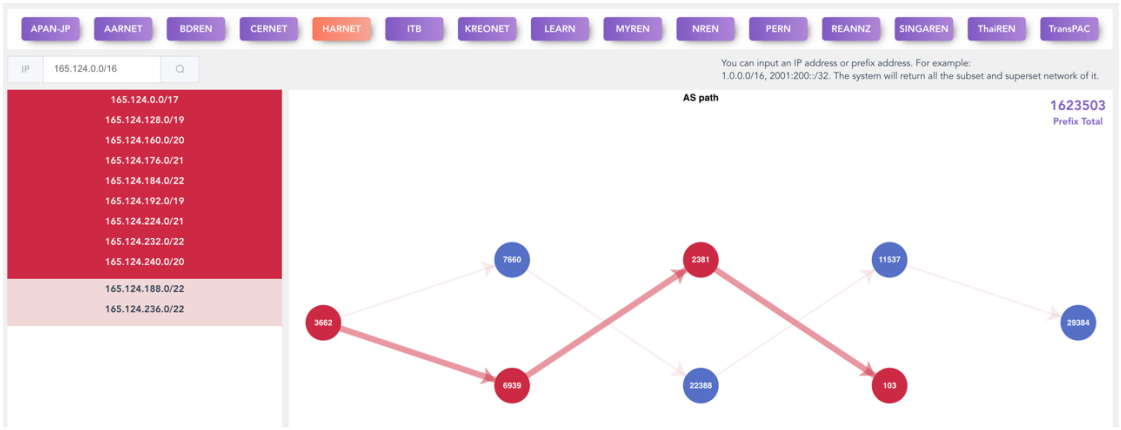


The left shows that some networks share the same path, and they are grouped with the same color. If you click on any of the same-colored block of prefixes, the forward path for that group will be highlighted.

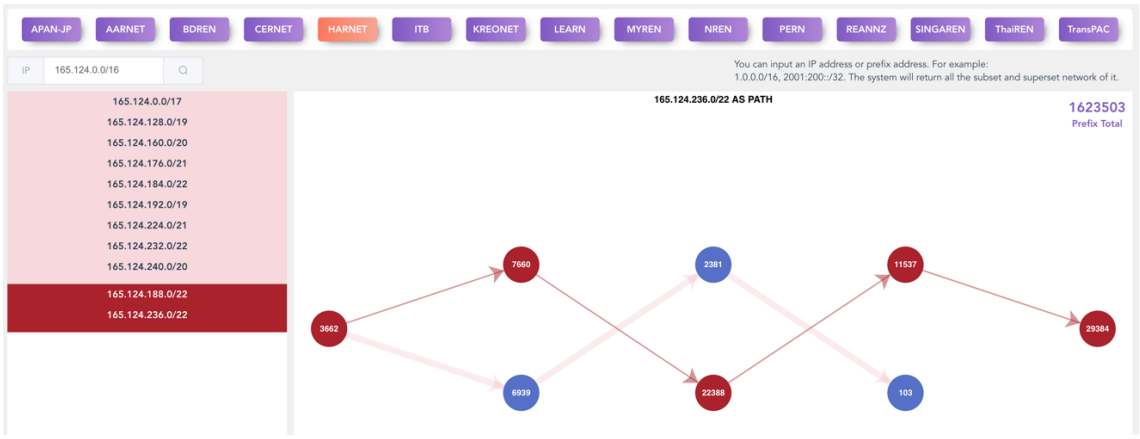
The “Prefix Total” at the top-right corner defines the total number of prefixes that your selected ASN shares with the platform.

Example #1: Checking a forward path from HARNET to an IPv4 prefix 165.124.0.0/16

Select HARNET as the source and 165.124.0.0/16 as the destination.



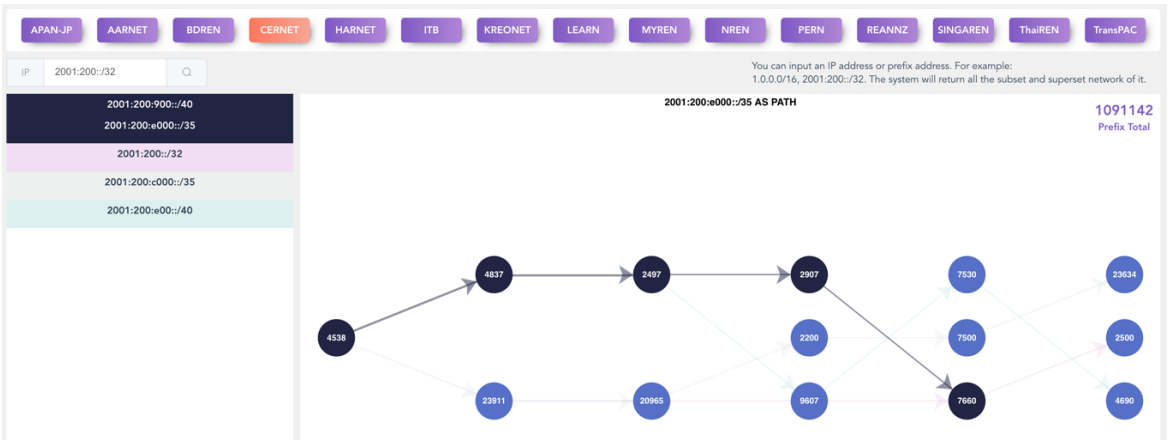
The system will show the path for the first colored block. Now, if you click on the next colored prefix block, the routing path to the next colored block will be shown.



Example #2: Checking a forward path from CERNET to an IPv6 prefix 2001:200::/32

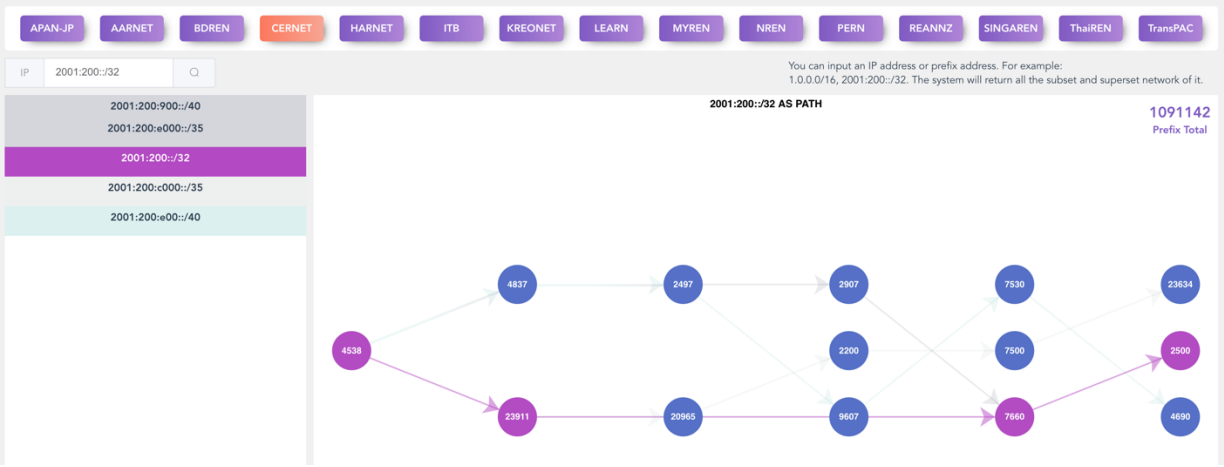
Select CERNET as the source and 2001:200::/32 as the destination. The system will return all the sub and super networks of that prefix with the different colored blocks.

Here, the system is showing four colored blocks. This is the routing path for the first colored block.

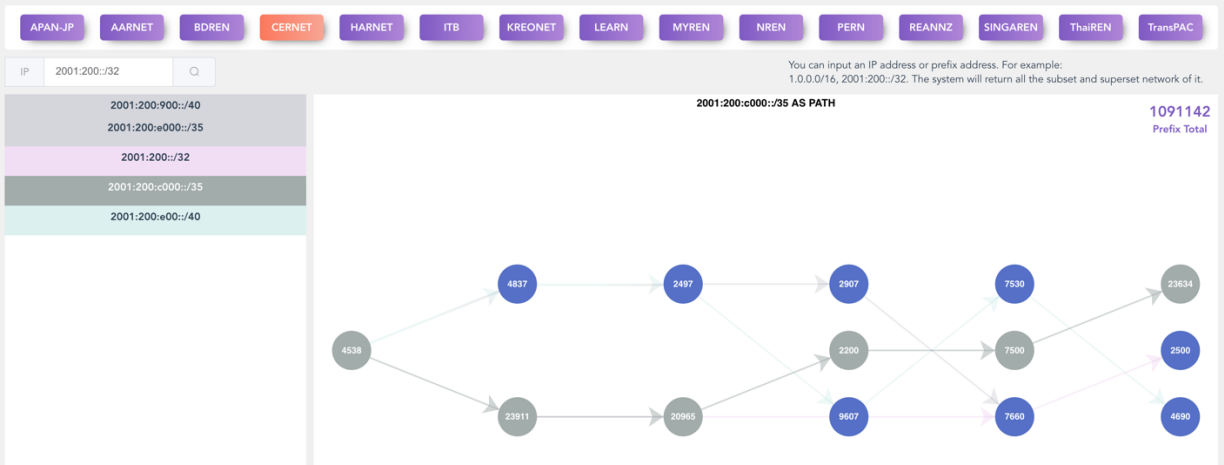


Click the second, third and fourth block to get the routing path for the second third and fourth colored block.

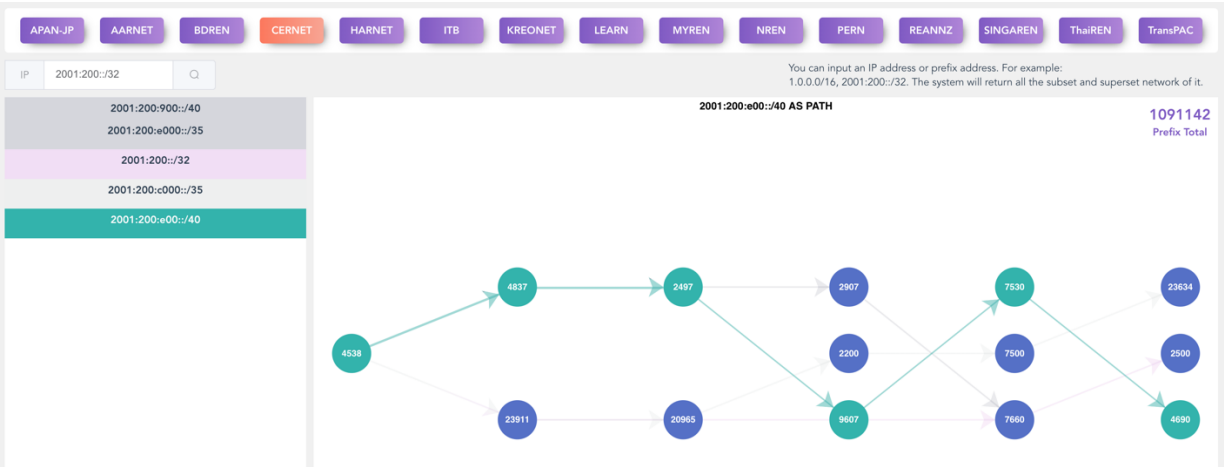
2nd colored block:



3rd colored block:



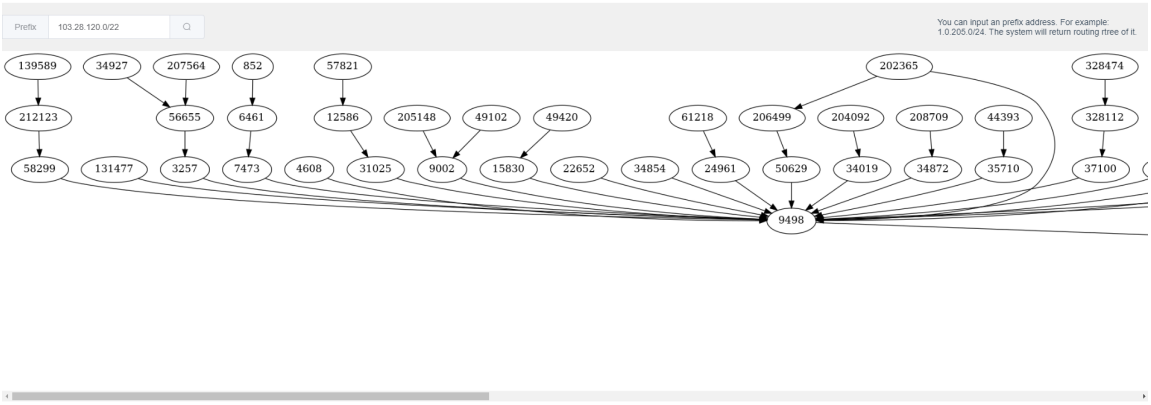
4th colored block:



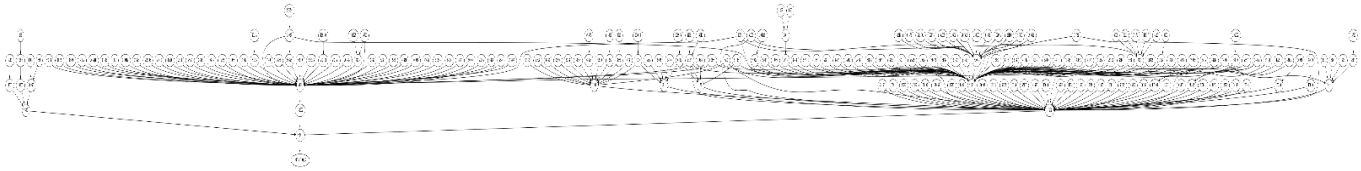
Reverse Routing Path

In the reverse routing path section, you will have to put a prefix or an IP and hit search, they can be either IPv4 or IPv6. The system will search the best matched prefix and return the reverse routing tree.

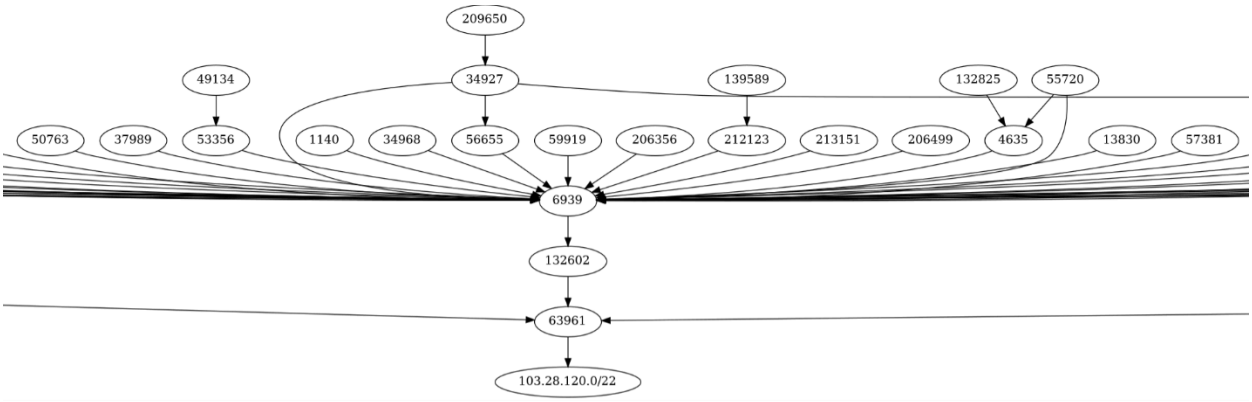
It will show you the reachability of the keyed-in prefix using BGP AS-path routing tree. Due to the huge amount of data, now the system only selects part data from all the routing information sharing platform. It usually defines the tree from 5-6 levels away.



In most cases, this is going to be a large tree. You can scroll left and right to view the full tree. You can also click on this tree to view, zoom and save it.



In this picture, the prefix 103.28.120.0/22 is under the AS63961 which is connected to AS9885, AS132602 and AS17494 at its upstream. Then these three (3) ASes are connected to other ASes at their upstream and so on. That is how the tree has been formed which expresses the reachability path of the prefix from the outside world.

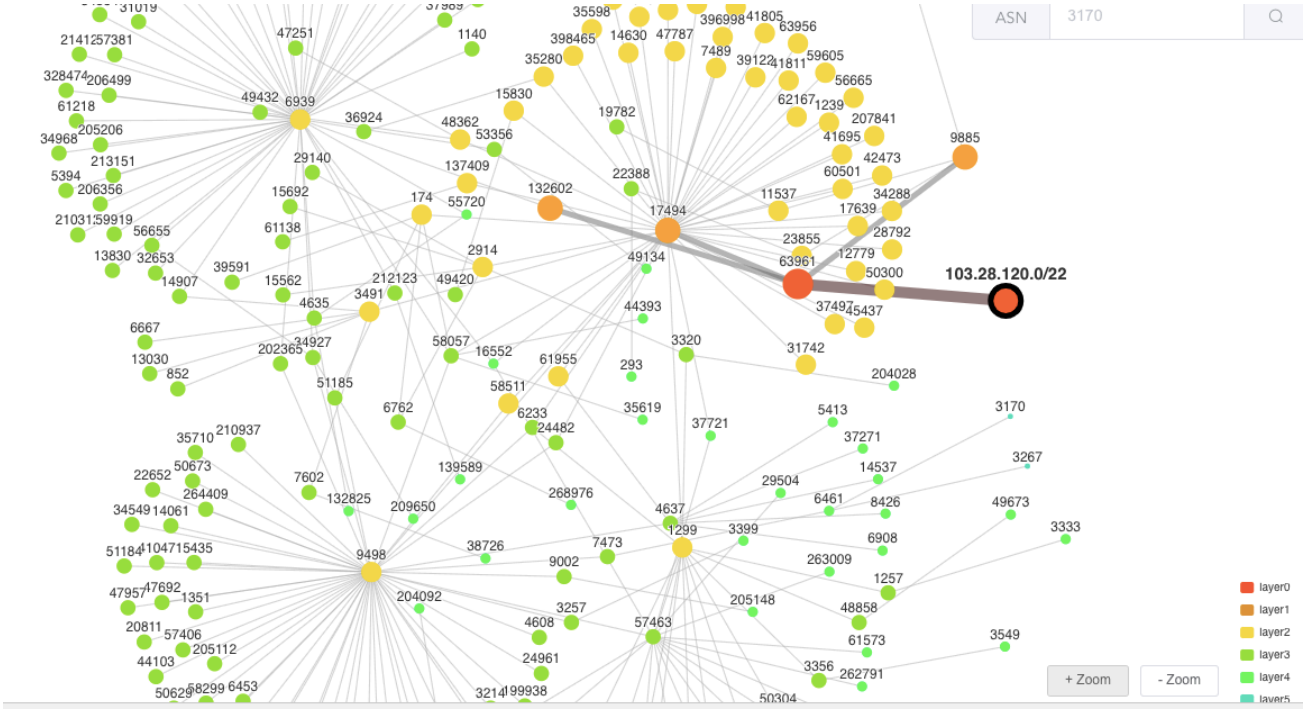


If we dig down and have a look at the above tree [which is the output of the reverse routing path of prefix 103.28.120.0/22], we can explain it in the way that prefix 103.28.120.0/22 can be reached from AS139589 following the route defining AS212123 => AS6939 => AS132602 => AS63961 which holds the prefix.

This is a completely dynamic picture of the routing path which keeps on changing depending on the routing configuration and route availability.

Reverse Routing Path (TOPO)

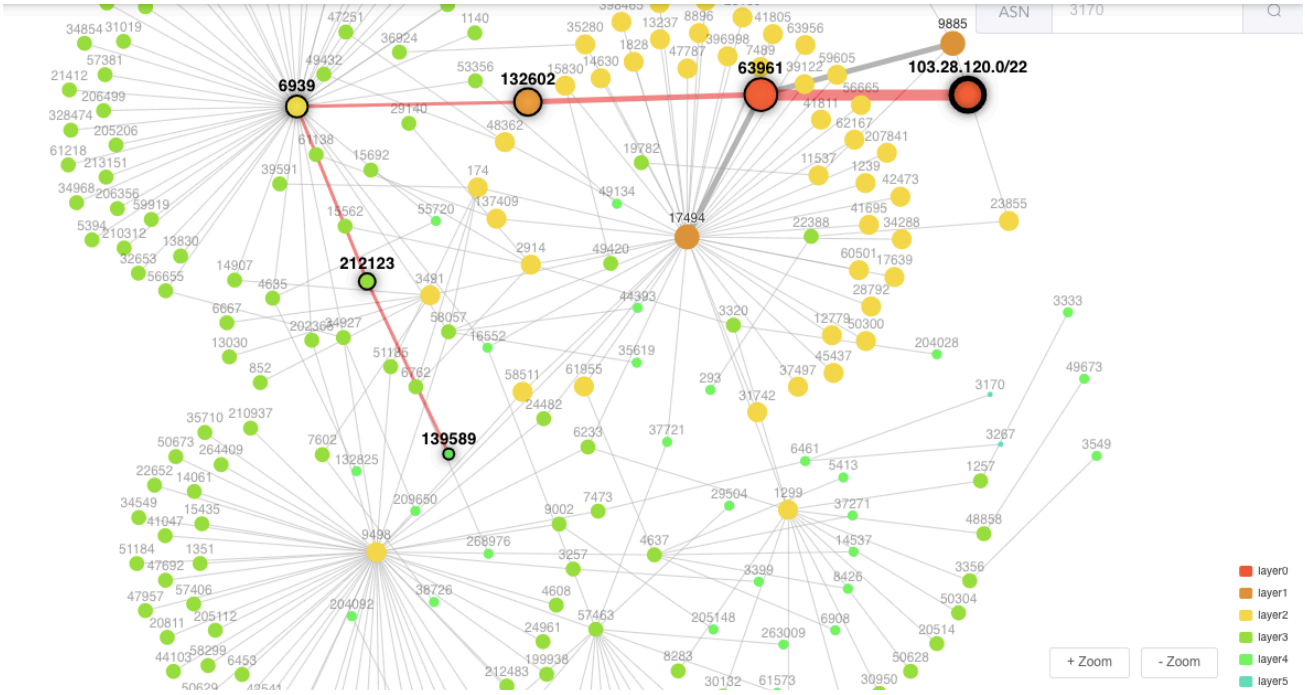
"Reverse Routing Path Topology" gives the same information as the "Reverse Routing Path" but in a more concise space in topology format. Same as "Reverse Routing Path" it takes an "IP prefix" as an input and the system will search the best matched topology to reach the prefix from the outside world.



In this figure, you can see that the system has returned a complete reverse routing tree for the input prefix 103.28.120.0/22.

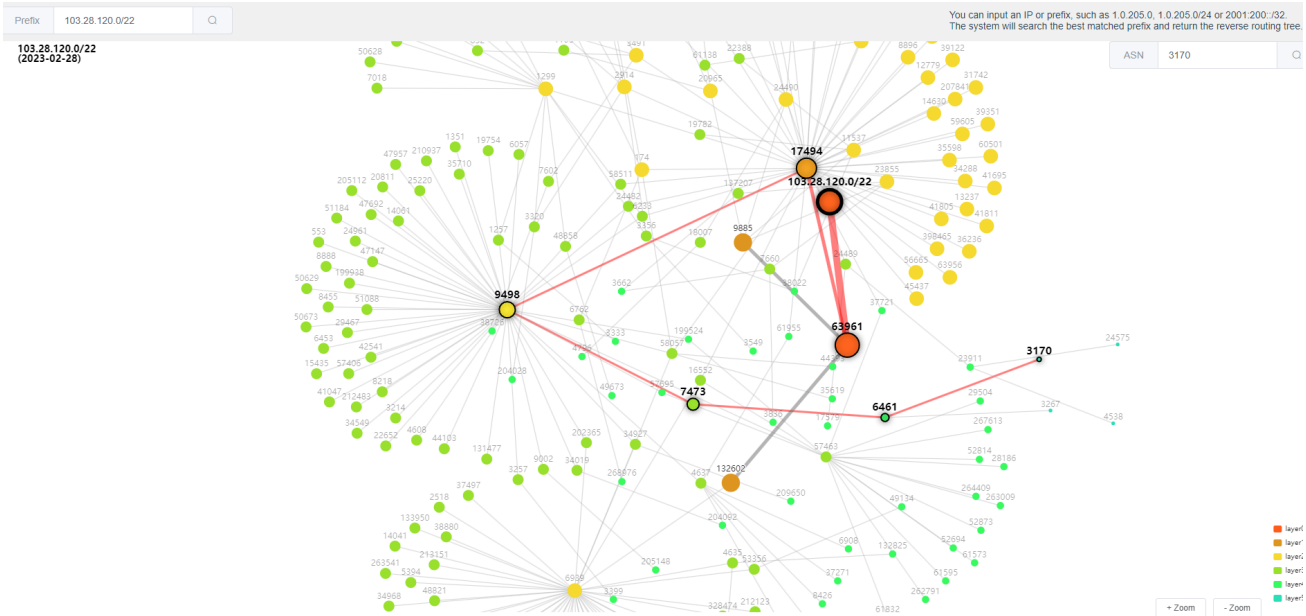
If we trace the same routing-path as expressed under the "Reverse Routing Path" we can see the same route path description of reachability of the 103.28.120.0/22 prefix from AS139589 through AS212123 => AS6939 => AS132602 => AS63961 which holds the said prefix.

The legends on the bottom right corner shows the layer of the reverse path with a color code. For example, the Red color nodes are layer 0, which is your searched prefix or IP. You can click on the legends to remove or add the layers to your routing tree.



Moreover, if you want to see the reverse routing path of the prefix from a specific AS, you can simply click on that AS or input an ASN in the search field. You will be able to see how traffic is coming to your searched prefix as a reverse path. Following the same example of reaching 103.28.120.0/22 from AS139589, clicking right on the source AS, the above-portrayed topology is obtained which clearly defines the reachability path.

As mentioned before, the same can be obtained by putting the ASN in the “Search box” at the top-right corner and clicking on the “searching glass” [please see below].



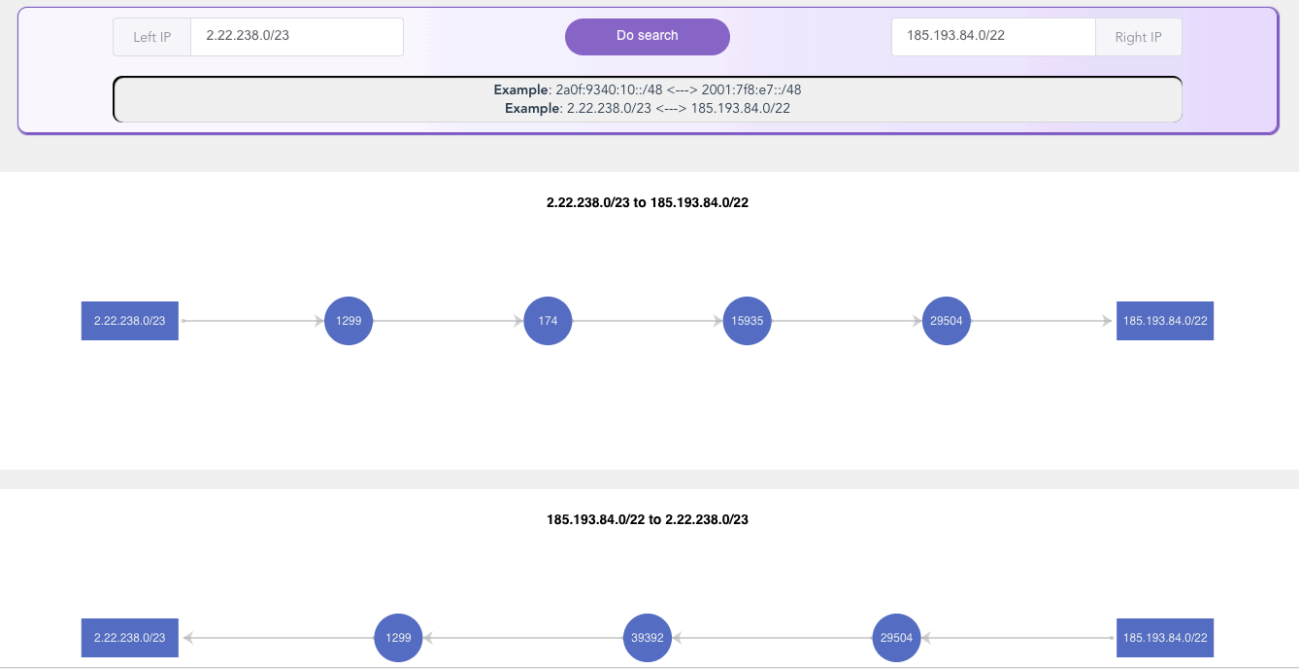
Bi-directional Path

In the “BiRoutingPath” submenu of the “RoutingPath” menu, you can find forward and reverse routing path between a source and destination IP address or prefix. The left and right IP addresses or prefix for the input field, they can be either IPv4 or IPv6.

This is very much similar to the SUBSECTION ‘routing path’ except that the routing path is bi-directional here.

There is a search-box at the top where you can put under “Left IP” the source prefix and under the “Right IP” the destination prefix. It will give you both the forwarding and the reverse path as displayed below.

Due to the huge amount of data, now the system only selects part data from all the routing information sharing platform. If the system return “no data found”, it doesn’t mean there isn’t a routing path, it maybe just because the system hasn’t processed the corresponding data.

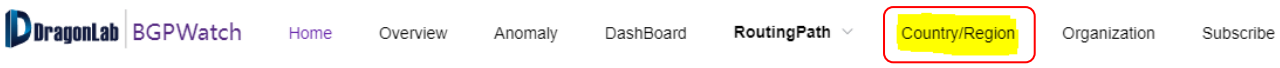


DragonLab | BGPWatch

SECTION 7

COUNTRY-WISE AS RANKS WITH CONE

Section 7. Country-wise AS ranks with Cone



Introduction

The Country/Region section tries to give a global picture of BGP based on the "Cone" size of each operator. First of all, the world is divided into six (6) continents: Africa, Asia, Europe, North America, Oceania and South America. Under each of the continents, the names of the countries are listed and under each country the top 100 operators are ranked based on their "AS-cone" size. Each operator is represented by a circle with the circle size being proportional to the corresponding "AS-cone" size. Connectivity of each operator with their customers are also mapped.

The page also shows the number of ASes that is there in the selected country, the number of BGP links, the number of operators in the graph and the number of links defined in the graph.

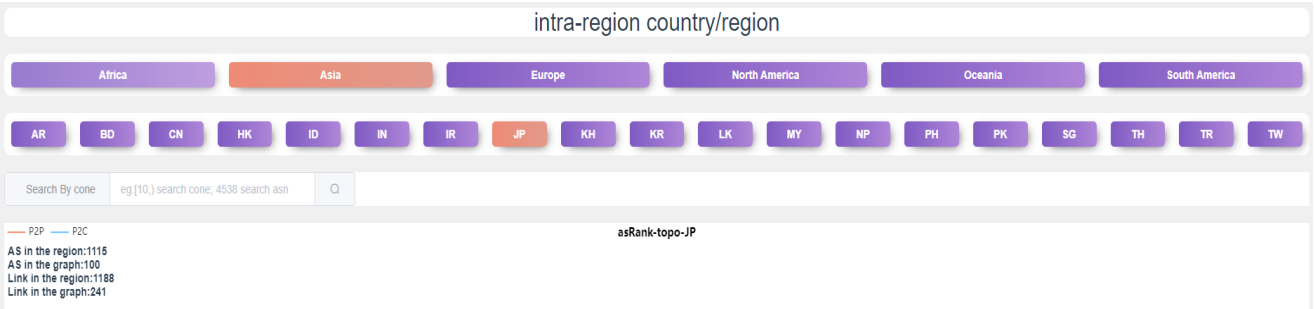
So, what is an "AS-Cone"?

"AS-cone" or "Customer Cone" is the number of ASes that can be reached from a given AS following only customer links.

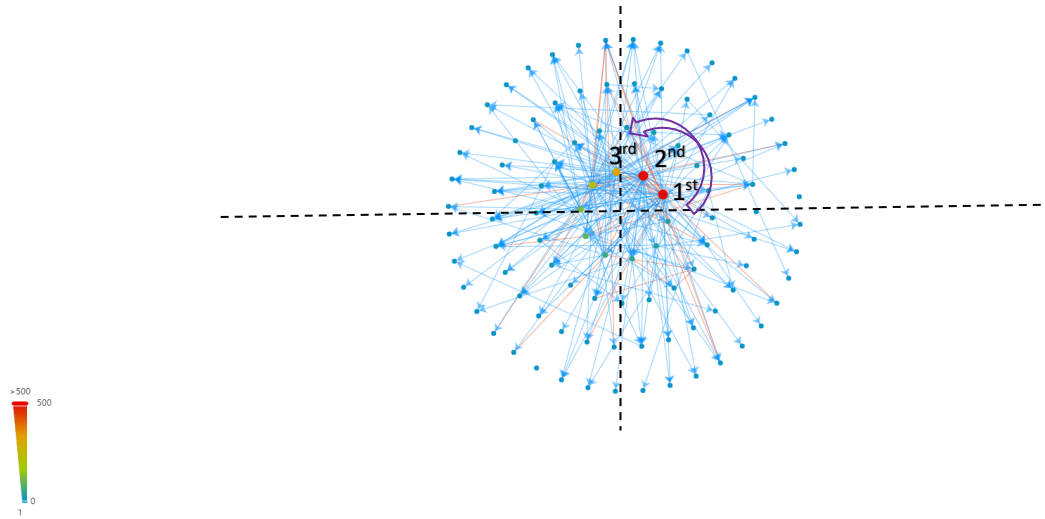
Let's consider an AS number 63961. AS63961's AS customer cone is defined as the AS63961 itself plus all the ASes that can be reached from 63961 following only p2c links in BGP paths. In other words, 63961's customer cone contains 63961, plus 63961's customers, plus its customers' customers, and so on. The size of the customer cone of an AS reflects the number of ASes, IPv4 prefixes, or IPv4 addresses found in its set. An AS in the customer cone is assumed to pay, directly or indirectly, for transit. "AS-cone" provides a coarse metric of the size or influence of an AS in the routing system.

Navigating the page

Once you click the menu "Country/Region" you will be displayed with the following page:



To select a country, you have to select the continent first. Then the name of the countries under the continent will be displayed. Once you select the country, you will see a graph showing the ASes under it as the nodes. The top 100 ASes will be displayed in the graph ranked by their "AS-Cone" size.

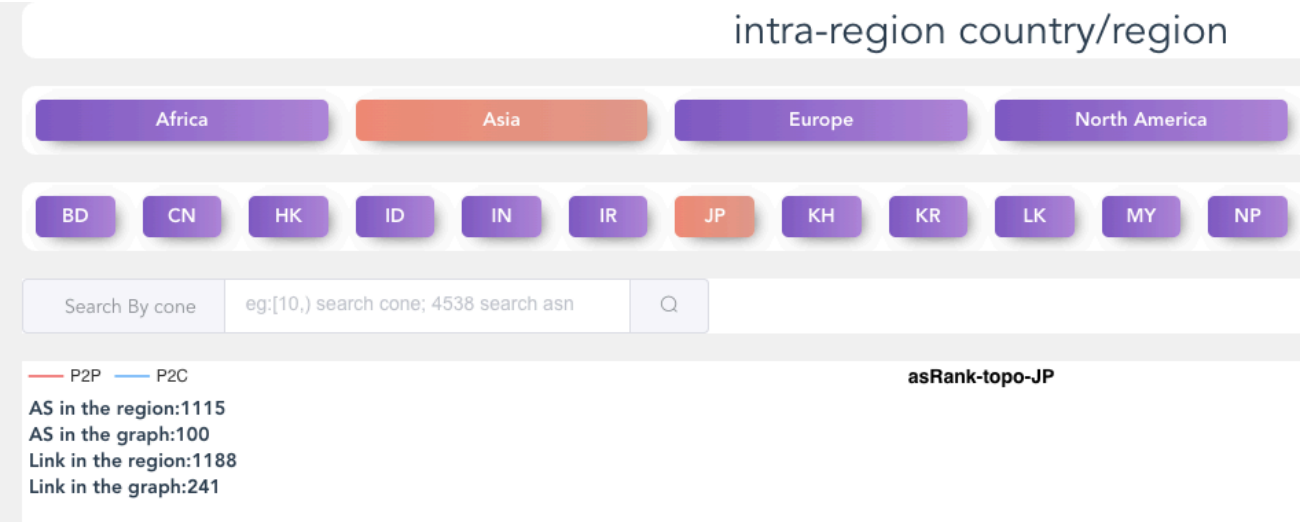


These nodes are colored [in line with the color scheme defined in the bottom-left corner] and enlarged according to their cone size and placed counterclockwise in accordance with their rank. The links are shown as straight lines. The blue lines indicate peer-to-customer (P2C) and the orange lines indicate peer-to-peer (P2P) connection.

In the top-left of the graph, it shows information about the total number of -

i. AS in the region
ii. AS in the graph
iii. Link in the region
iv. Link in the graph

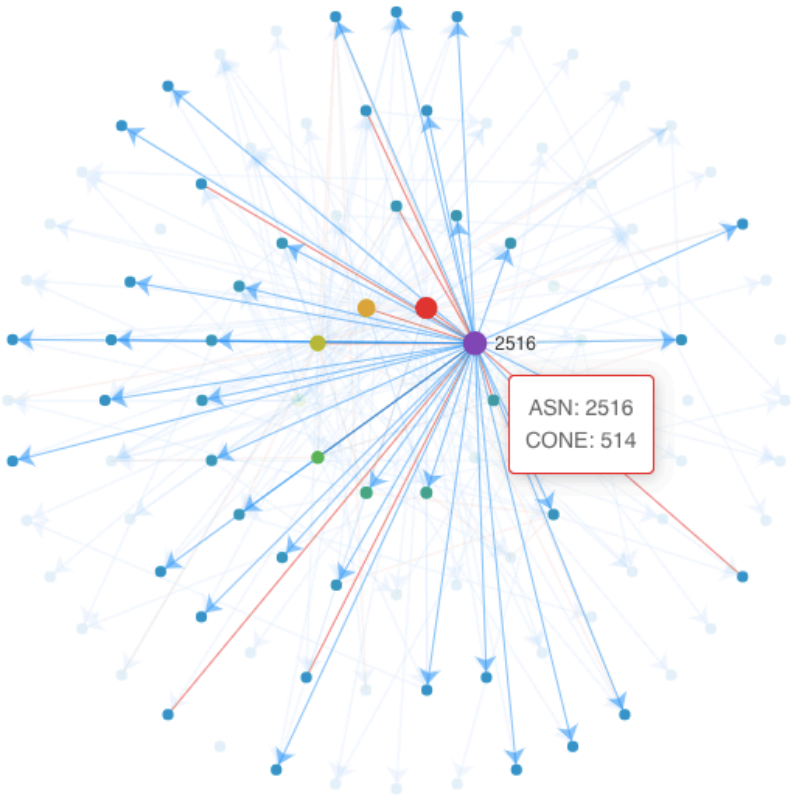
You can select the Continents and Countries on top of the graph.



In this figure, the selected country was JAPAN which has the 1115 number of ASes and 1188 links.

This graph is showing the top 100 ranked AS of Japan based on their cone size. The highest number cone is the red one at 0 degree horizontally. Then the 2nd, 3rd and more is being shown in the counter clockwise direction.

If you hover your mouse over any node, it will show you the AS number and cone size of that node as follows.

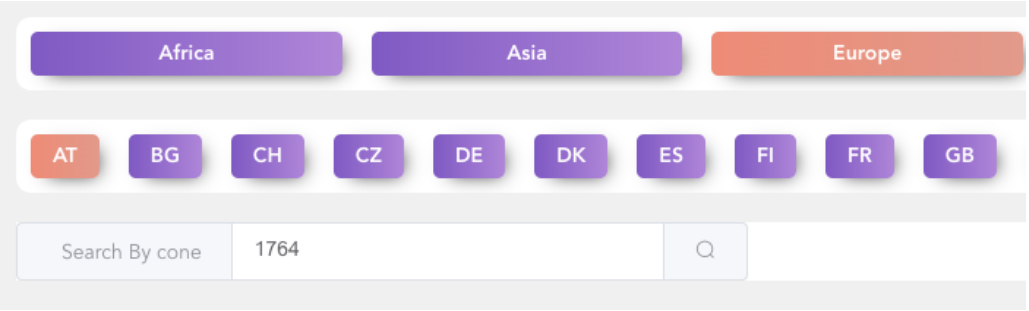


The size of the nodes depends on the cone size and color of the nodes depends on the color scale located at the bottom left of the page.

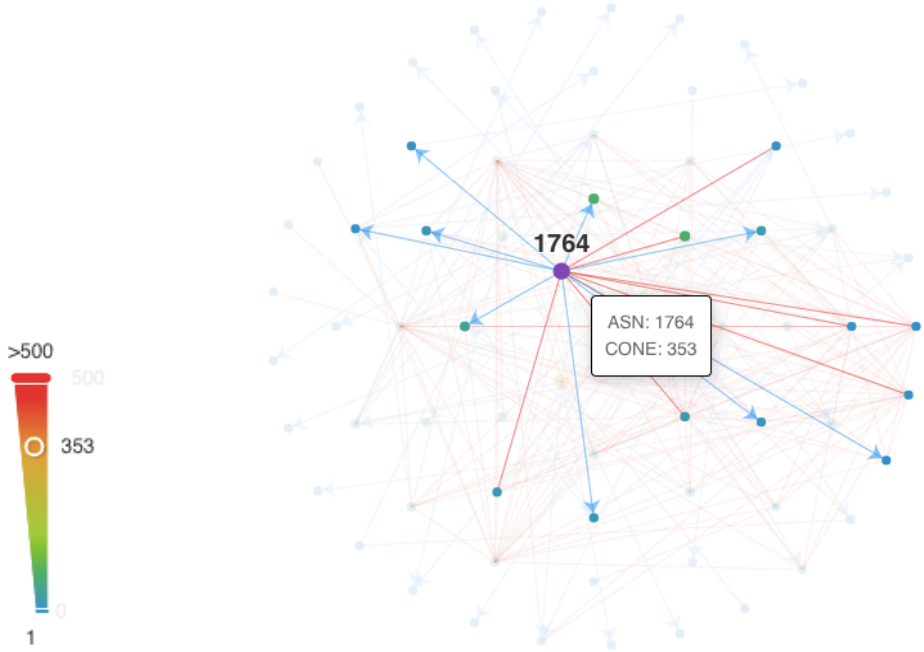
You can search with the cone and AS number in the graph. You can also filter this graph by the number of cones located at the left top region.

Example #1: To search a Cone by ASN

To search for a specific ASN, please key in the ASN in the search bar. As an example, if you want to list the cone-wise mapping of ASN1764 which is in Austria (AT) under continent “Europe”, put 1764 in the search box and click the magnifying glass.

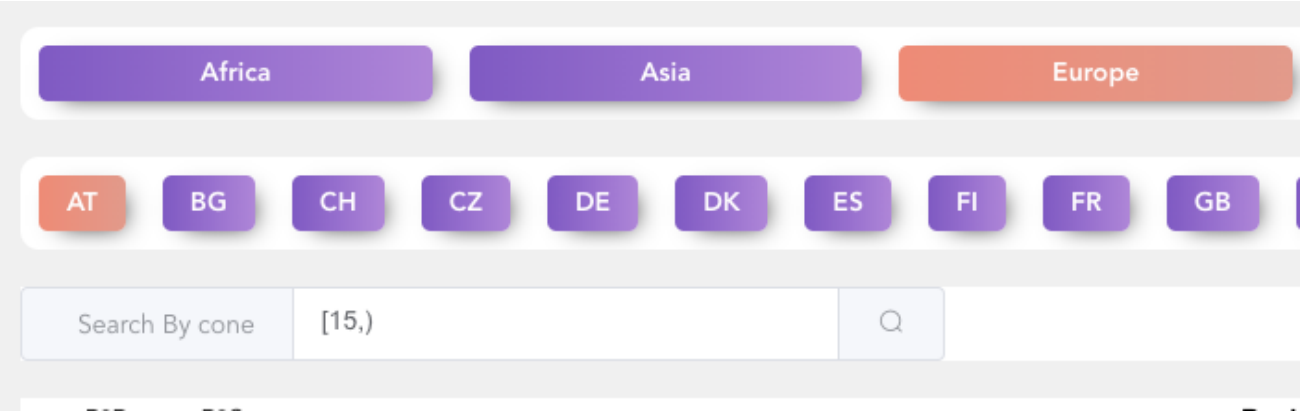


You are going to get the following mapping:

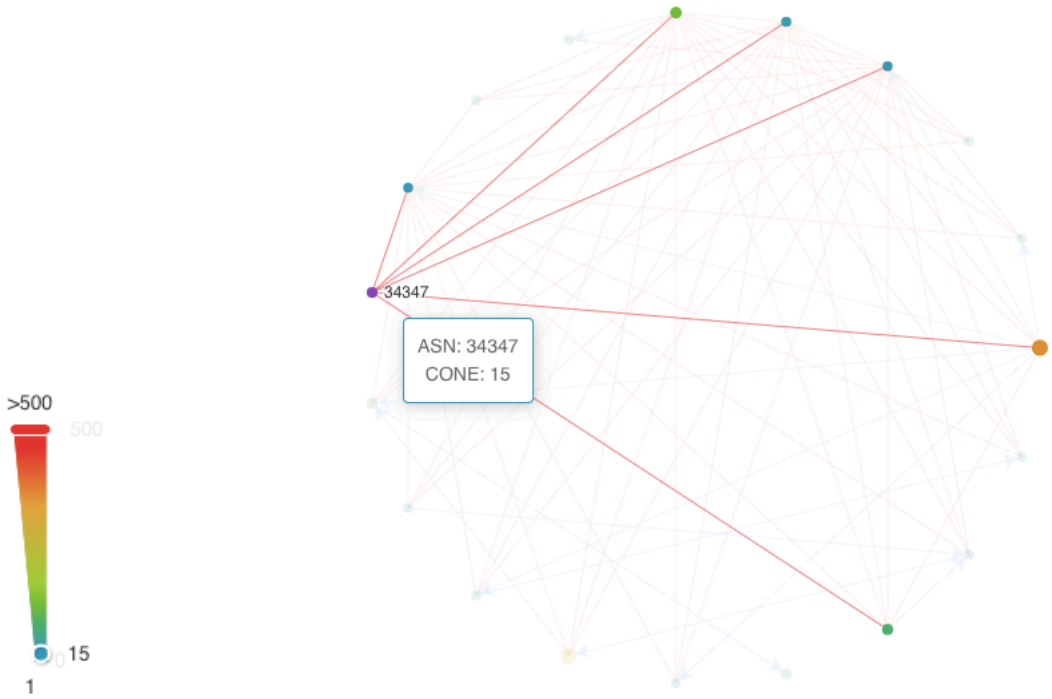


Example #2: To search by Cone size

To search for a specific cone size, please key in the cone number in the search bar. As an example, if you want to list the AS mapping for a cone size >=15 for country Austria (AT) under continent “Europe”, put “[15,)” in the search box as follows and click the magnifying glass.



Following screen will come up:



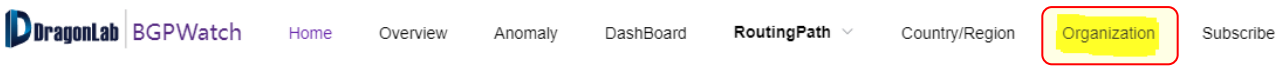
You can see that ASN 34357 with a cone-size of 15 and all other nodes having larger than a cone-size of 15 have been displayed.

DragonLab | BGPWatch

SECTION 8

ORGANIZATION

Section 8. Organization



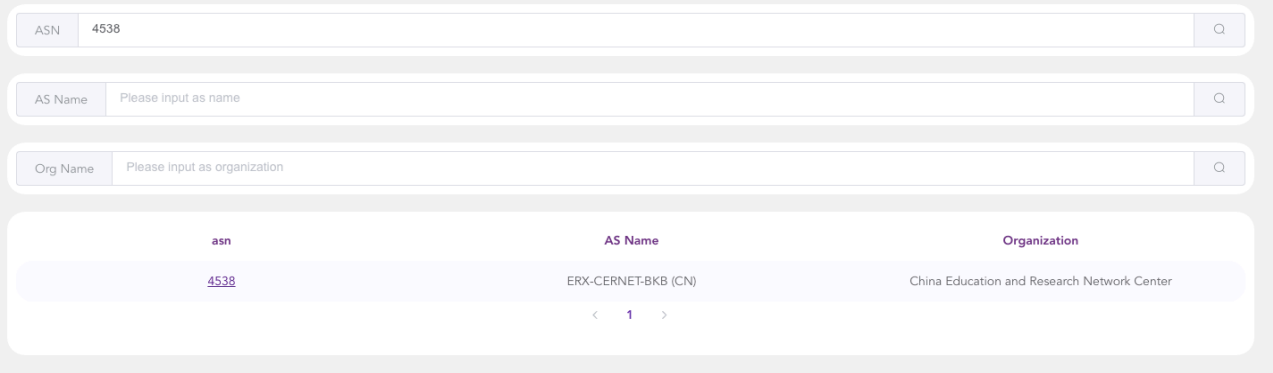
Introduction

In the organization section, you can find the AS Number, AS Name, and Organization Name according to your searched AS.

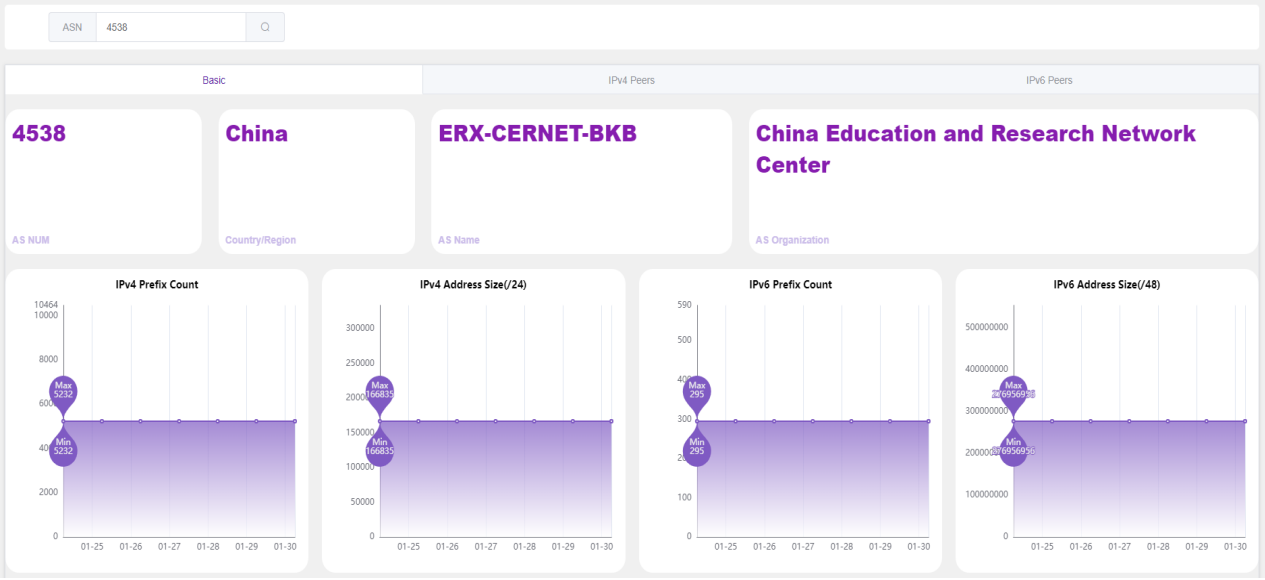
Navigating the page

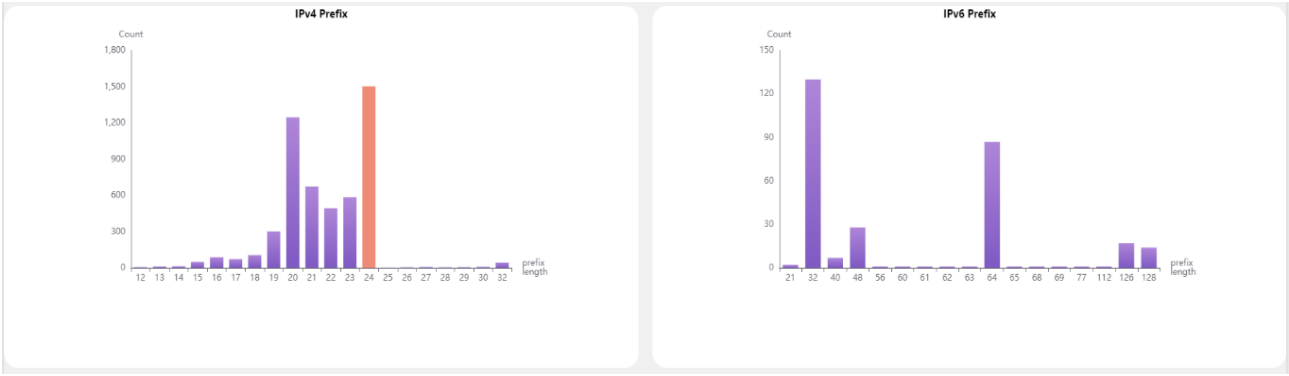
If you click on the AS number that is related to your search, you will be redirected to the “dashboard” of that particular ASN where you will get the same information as described in section 4.

If you put 4538 right after in the ASN field and click the glass to list the information pertaining to ASN458 as follows:

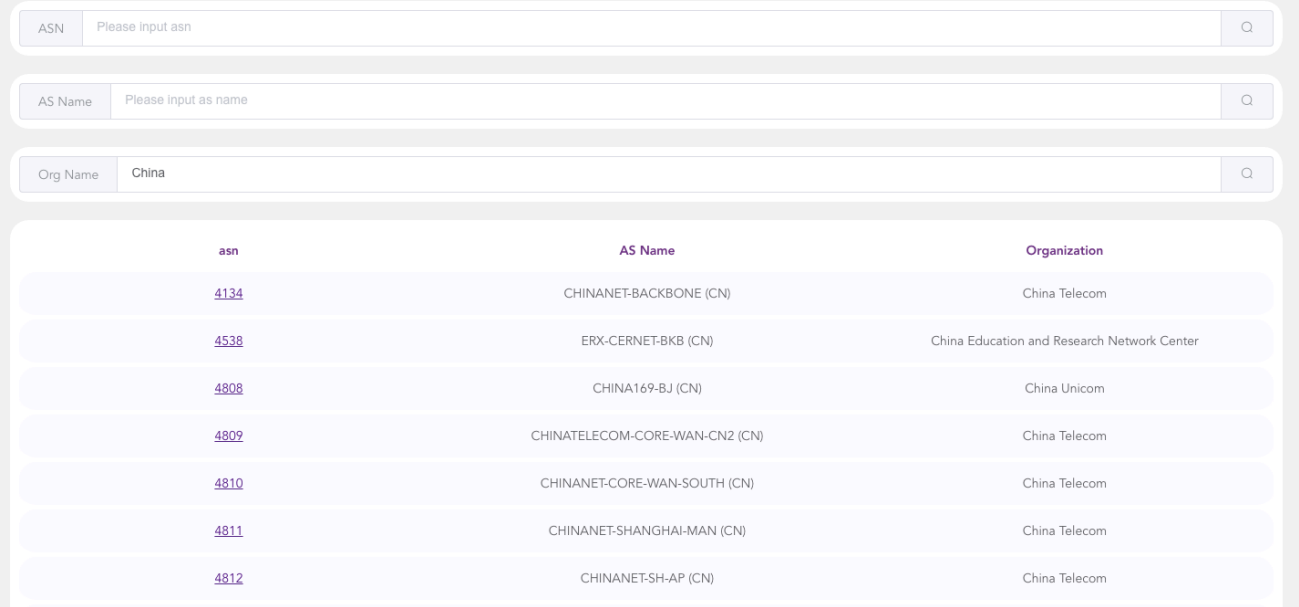


The following page will be displayed:





Similarly, you can search by putting “AS Name” and “Organization Name” in the respective field and do the searching. AS Name and Org Name search by matching strings. If you put “China” as Org Name then all the organizations containing “China” in their name, will be listed as follows:



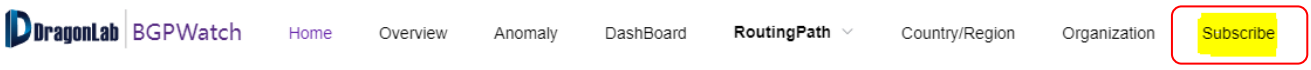
asn	AS Name	Organization
4134	CHINANET-BACKBONE (CN)	China Telecom
4538	ERX-CERNET-BKB (CN)	China Education and Research Network Center
4808	CHINA169-BJ (CN)	China Unicom
4809	CHINATELECOM-CORE-WAN-CN2 (CN)	China Telecom
4810	CHINANET-CORE-WAN-SOUTH (CN)	China Telecom
4811	CHINANET-SHANGHAI-MAN (CN)	China Telecom
4812	CHINANET-SH-AP (CN)	China Telecom

DragonLab | BGPWatch

SECTION 9

AS INFORMATION BASED ON SUBSCRIPTION

Section 9. AS Information based on Subscription



Introduction

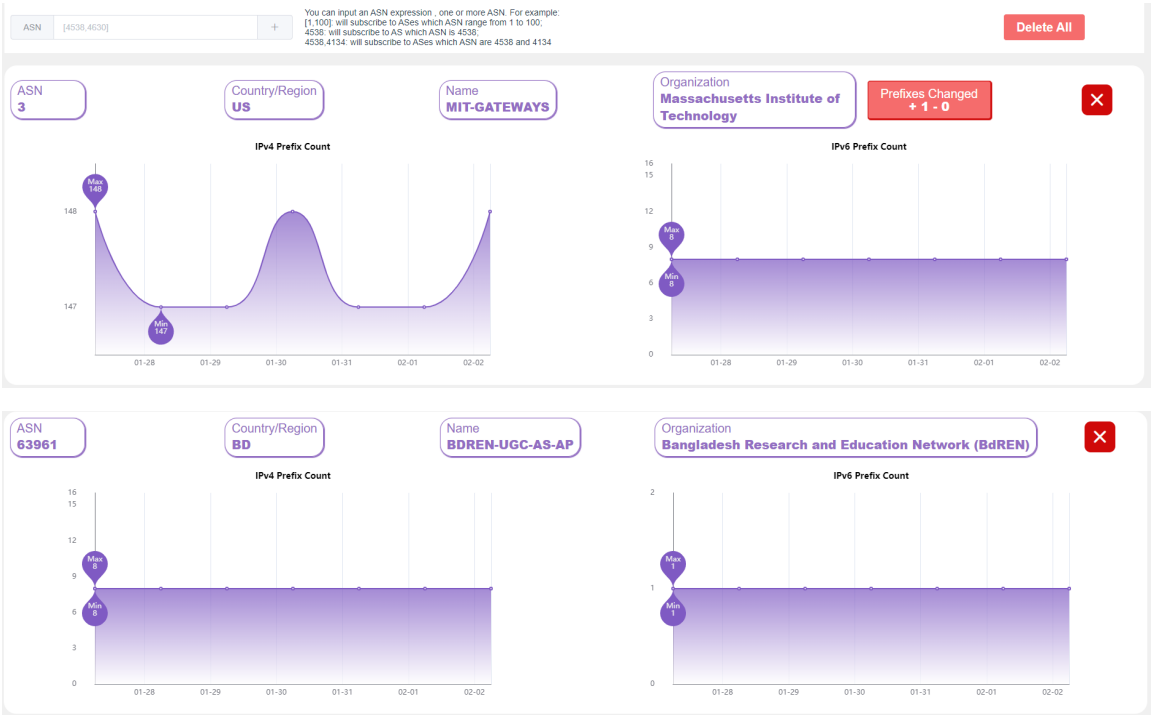
This section is used for subscription of ASes. Operators can subscribe ASes they are interested in, the system will monitor the ASes, and send alert message via email to the operators.

Navigating the Page

In the subscribe section, you can find the AS details based on the subscription that you have added. On the search bar, you can input an ASN expression to add one or more ASNsFor example:

- [1,100]: will subscribe all ASes ranging from AS1 to AS100;
- 4538: will subscribe AS4538;
- 4538,4134: will subscribe AS4538 and AS4134.

If there is any change in the prefix for any particular ASN, it will show an alarm button about the change. You will also be notified through email that you are registered with.



In this figure, the ASN 3 does have a prefix change. The prefix has changed from 147 to 148. That's why, a button has appeared for the ASN 3 subscription. The plus (+) sign in the "Prefix Changed" box indicates the number of prefixes that have increased and the minus (-) sign will indicate the number of prefixes that have decreased. If you click on this "Prefix Changed" box, you will be able to see prefixes that have been added or removed as follows: