BGP Security

Hijack and Route Leak Detection

Lefteris Manassakis | COO, Code BGP

✉ lefteris@codebgp.com

Peering Days

March 29, 2023
Sofia, Bulgaria

About me

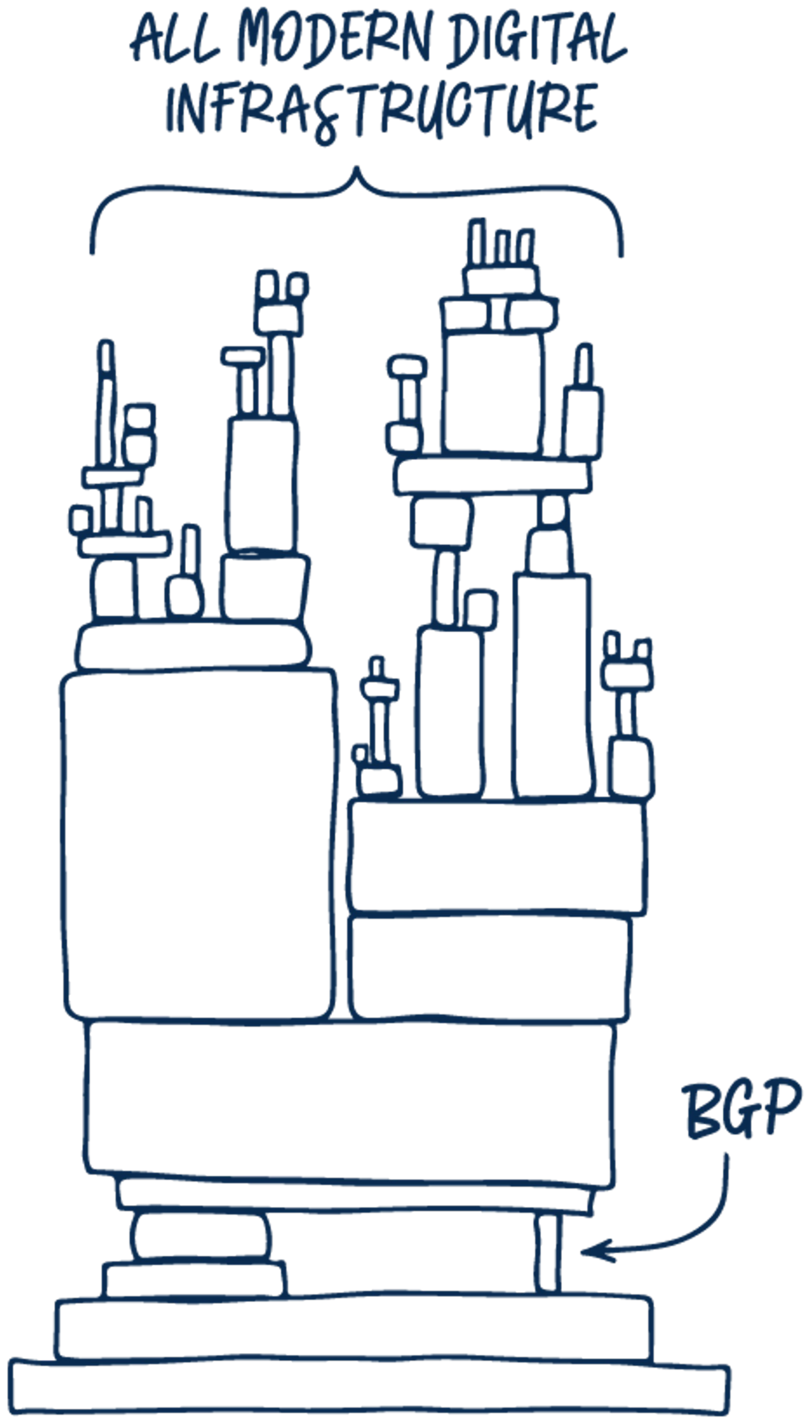
Lefteris Manassakis

COO & co-founder | Code BGP

✉ lefteris@codebgp.com

🌐 https://manassakis.net/

BGP hijacks, leaks & misconfigurations affect your network



- BGP events critically affect **reliability, security, and performance**
- Only the **tip of the iceberg** gets known

Types of BGP prefix hijacks

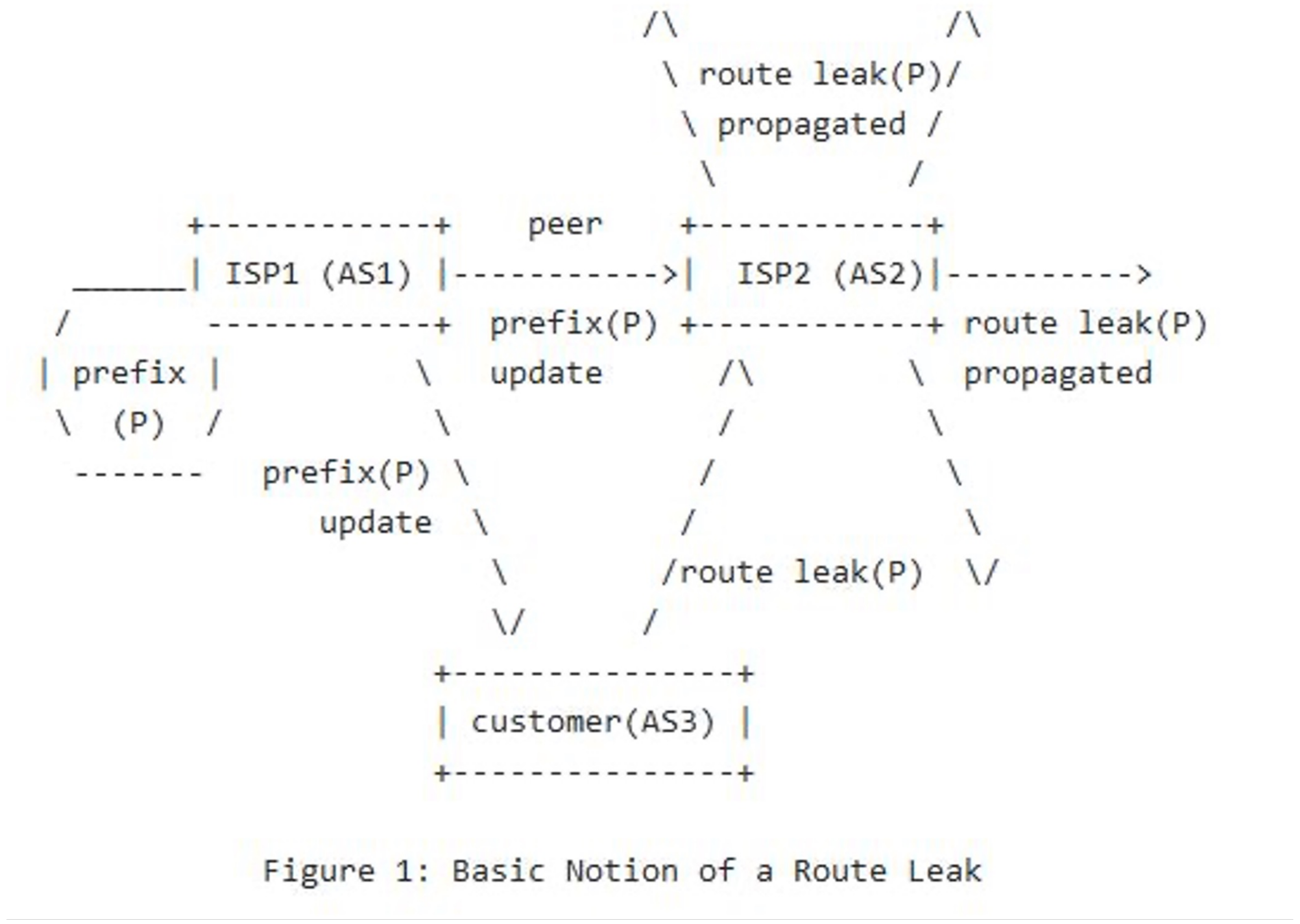
- **Classification by Announced AS-Path**
    - **Origin-AS (or Type-0):** The hijacker AS announces – as its own – a prefix that it is not authorized to originate. This is the most commonly observed hijack type.
    - **Type-N (N ≥ 1):** The hijacker AS announces an illegitimate path for a prefix it does not own. The announced path contains the ASN of the victim (first AS in the path) and hijacker, e.g., {AS50414, ASx, ASy, AS1 – 212.46.55.0/24}, while the sequence of ASes in the path is not a valid route, e.g., AS50414 is not an actual neighbor of ASx.

Types of BGP prefix hijacks

- **Classification by Affected Prefix**
  - **Exact Prefix Hijacking:** The hijacker announces a path for exactly the same prefix announced by the legitimate AS. Since shortest AS-paths are typically preferred, only a part of the Internet that is close to the hijacker (e.g., in terms of AS hops) switches to route towards the hijacker.
  - **Sub-Prefix Hijacking:** The hijacker AS announces a more specific prefix of the prefix of the legitimate AS. Since the more specific prefixes are preferred, the entire Internet routes traffic towards the hijacker to reach the announced sub-prefix.
  - **Squatting:** The hijacker AS announces a prefix owned but not (currently) announced by the owner AS.
  - For a comprehensive prefix hijack taxonomy please check the ARTEMIS paper.

Route Leaks

- **Definition:** A route leak is the propagation of routing announcement(s) beyond their intended scope.



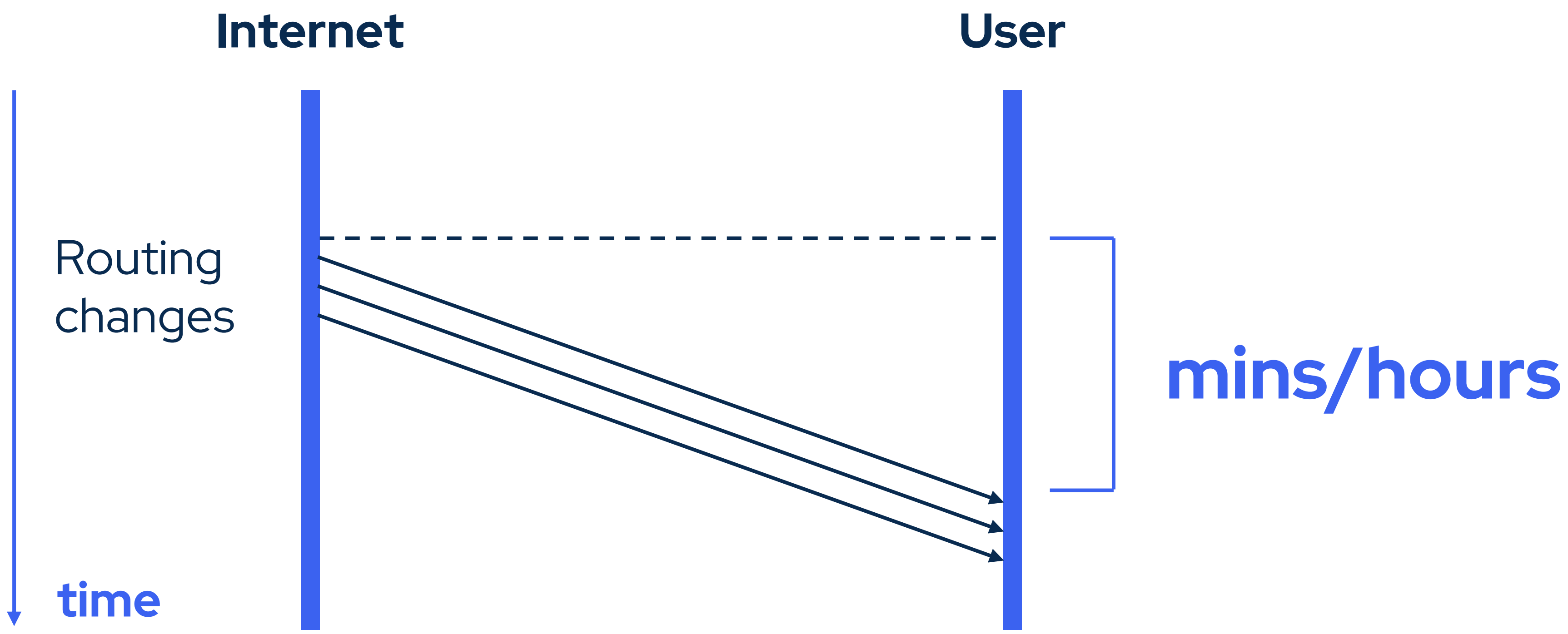
```
                              /\              /\
                               \ route leak(P)/
                                \ propagated /
                                 \          /
      +------------+    peer    +------------+
______| ISP1 (AS1) |----------->|  ISP2 (AS2)|---------->
/       ------------+  prefix(P) +------------+ route leak(P)
| prefix |          \   update        /\        \  propagated
\  (P)  /            \               /           \
 -------   prefix(P)  \             /             \
           update      \           /               \
                        \         /route leak(P)   \/
                        \/       /
                       +---------------+
                       | customer(AS3) |
                       +---------------+
```

Figure 1: Basic Notion of a Route Leak

  - ○ For different types of route leaks please check RFC 7908.

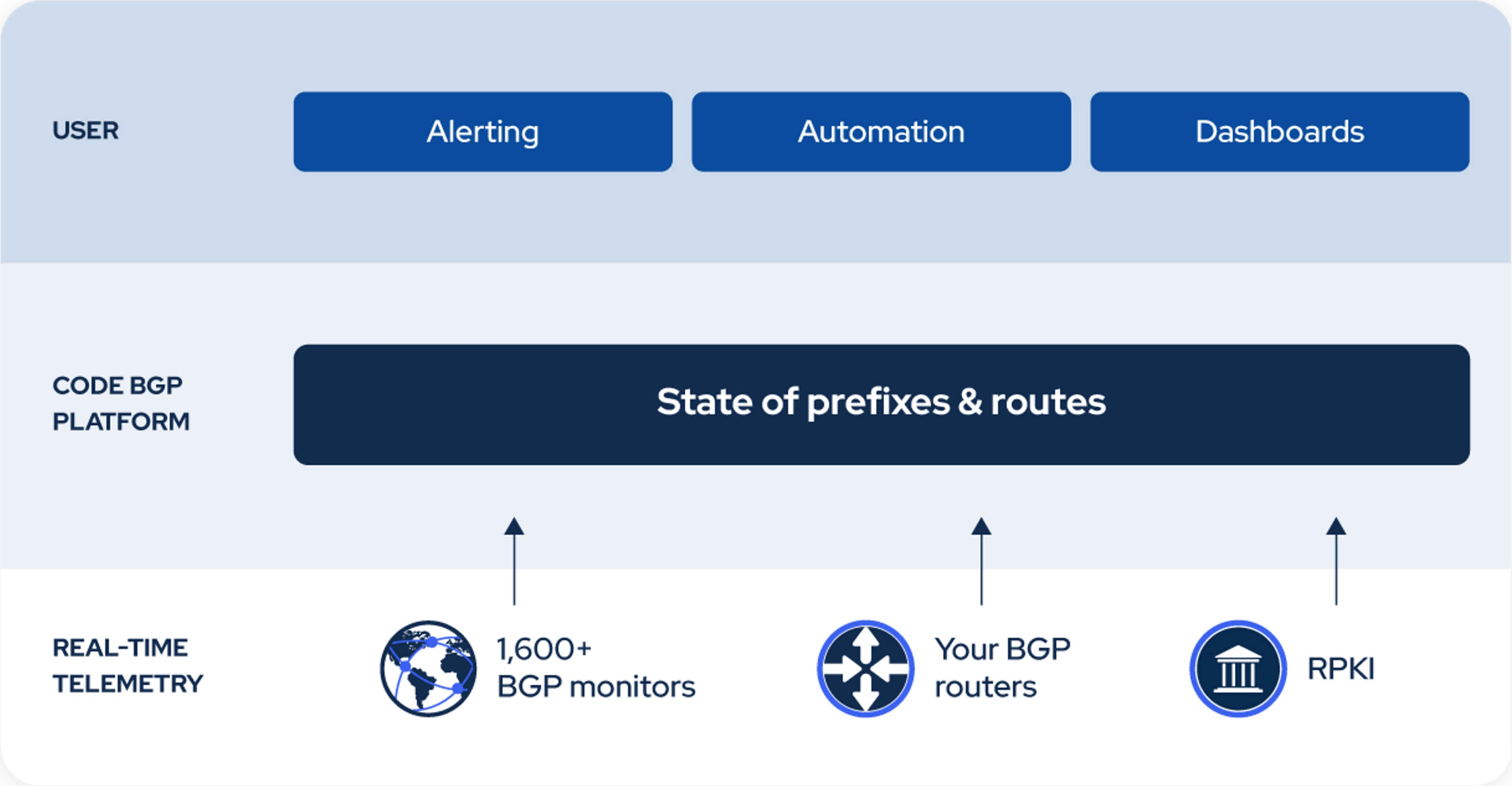
Challenges of hijack and route leak detection

- Speed
- Accuracy
- Evasion
- Privacy and flexibility



Code BGP Platform

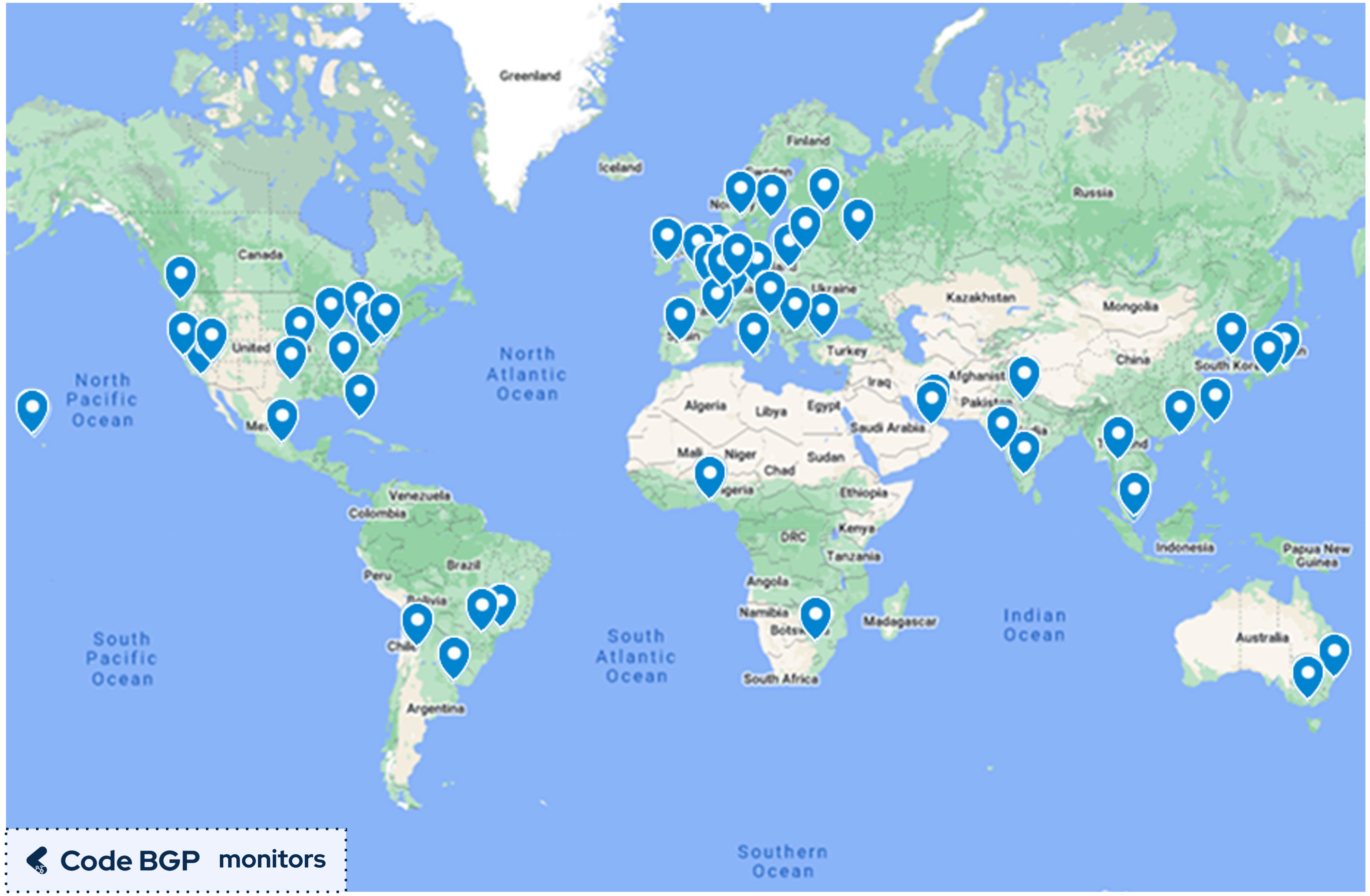
Monitor • Detect • Protect



Data service: Code BGP Monitor

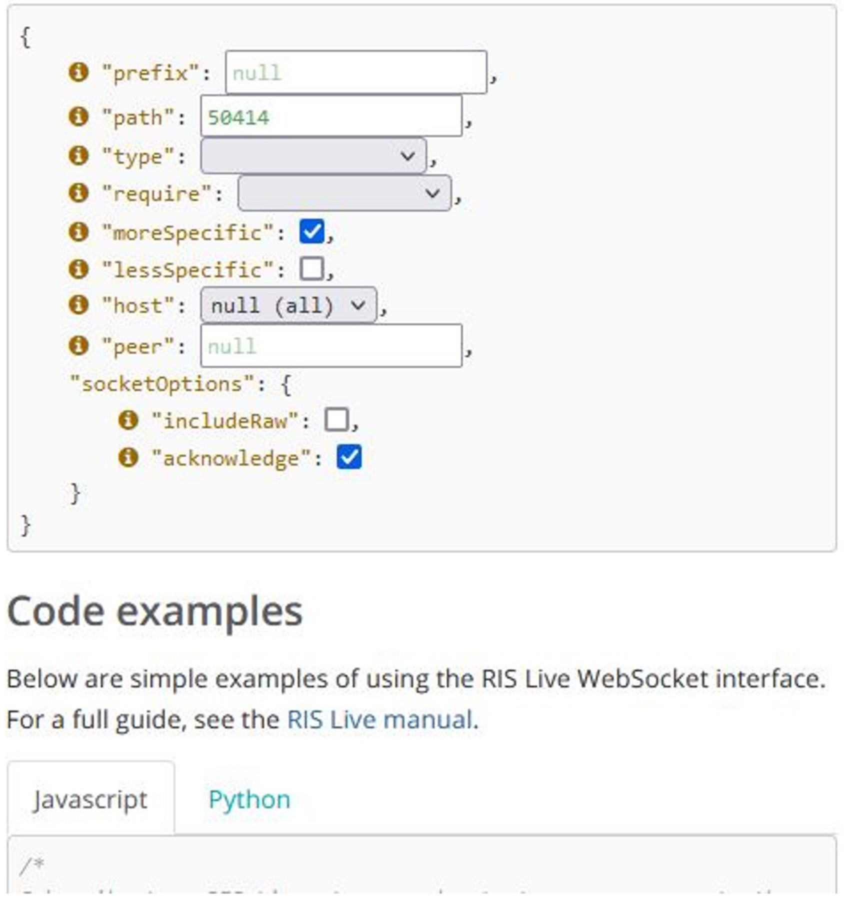
BGP Monitoring Service developed by Code BGP

- Route Reflection (RFC 4456)
- BGP Add-Path (RFC 7911)
- 186 full feed peerings (v4 & v6)
- 20 Upstreams
- Monitors in 37 countries, 62 cities



Data Service: RIS Live

Provides real-time JSON BGP messages via a fully filterable interactive WebSocket JSON API, and a full stream ("firehose") containing all of the messages generated by RIS. → https://ris-live.ripe.net/

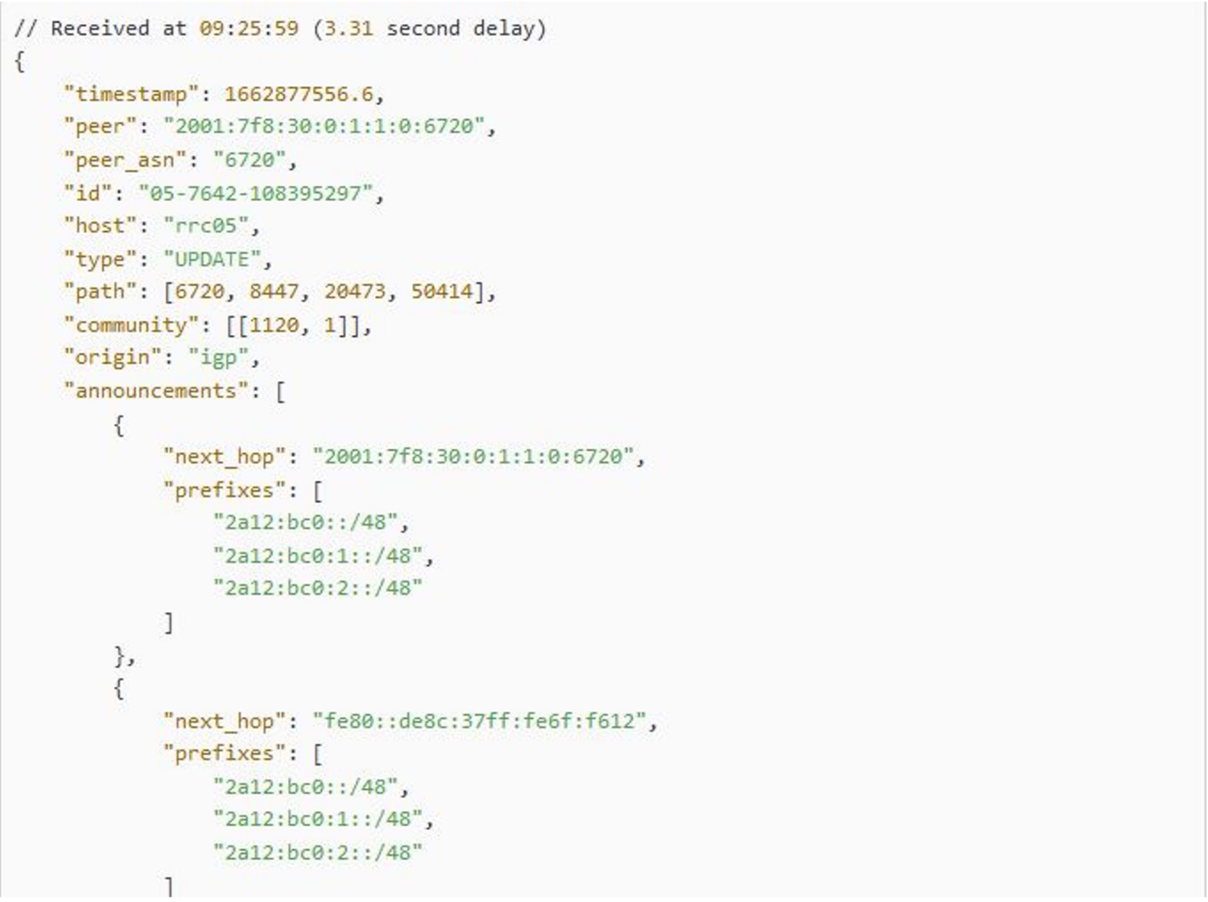


```
{
    "prefix": null,
    "path": 50414,
    "type": ,
    "require": ,
    "moreSpecific": ☑,
    "lessSpecific": □,
    "host": null (all),
    "peer": null,
    "socketOptions": {
        "includeRaw": □,
        "acknowledge": ☑
    }
}
```

Code examples

Below are simple examples of using the RIS Live WebSocket interface. For a full guide, see the RIS Live manual.

```
/*
```



```
// Received at 09:25:59 (3.31 second delay)
{
    "timestamp": 1662877556.6,
    "peer": "2001:7f8:30:0:1:1:0:6720",
    "peer_asn": "6720",
    "id": "05-7642-108395297",
    "host": "rrc05",
    "type": "UPDATE",
    "path": [6720, 8447, 20473, 50414],
    "community": [[1120, 1]],
    "origin": "igp",
    "announcements": [
        {
            "next_hop": "2001:7f8:30:0:1:1:0:6720",
            "prefixes": [
                "2a12:bc0::/48",
                "2a12:bc0:1::/48",
                "2a12:bc0:2::/48"
            ]
        },
        {
            "next_hop": "fe80::de8c:37ff:fe6f:f612",
            "prefixes": [
                "2a12:bc0::/48",
                "2a12:bc0:1::/48",
                "2a12:bc0:2::/48"
            ]
```

Total peerings (IPv4 & IPv6): **1448**

BGP full feeds:

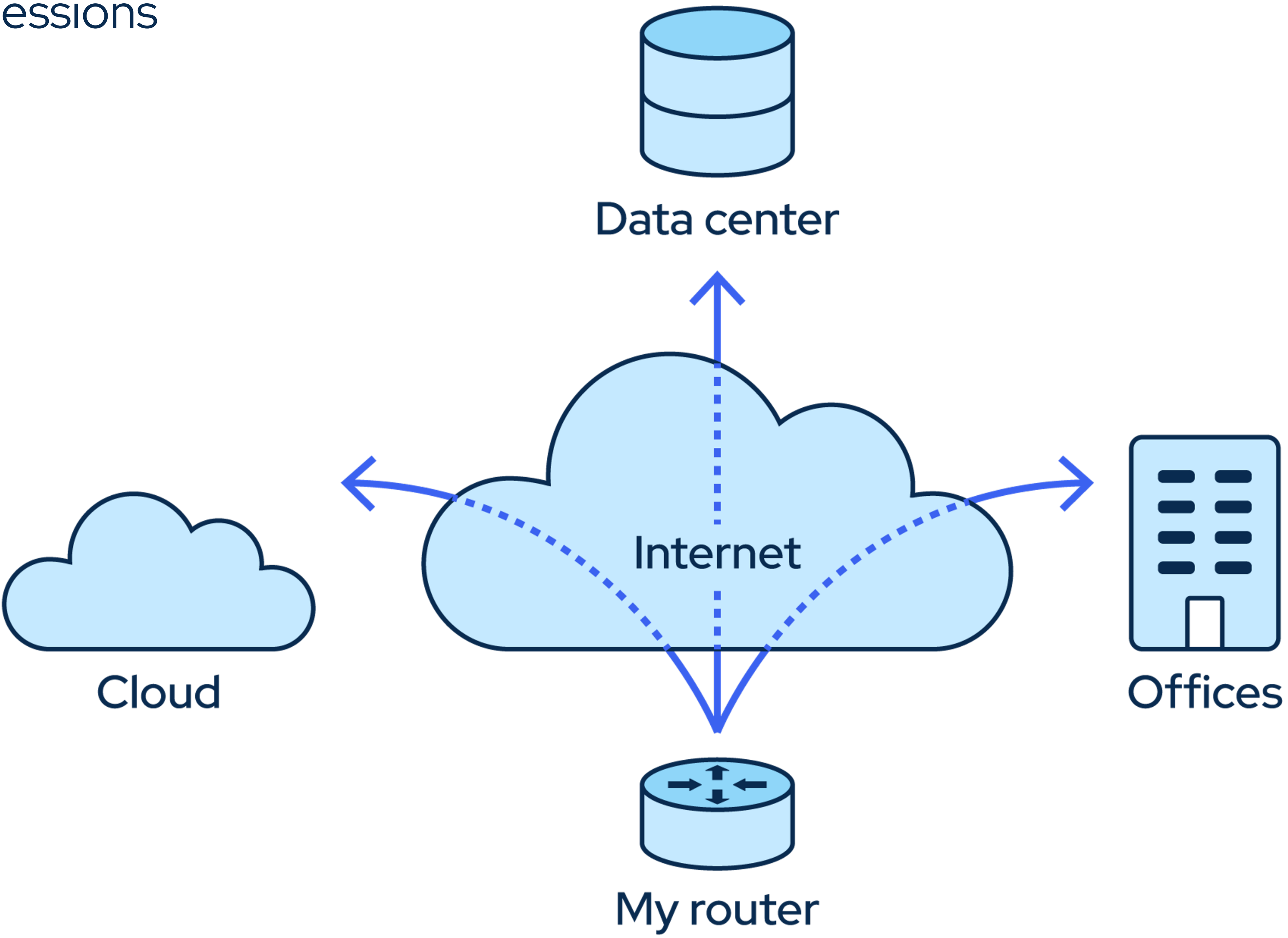
- IPv4: **366**
- IPv6: **401**

List of Route Collectors: https://ris.ripe.net/docs/10_routecollectors.html

List of Peers: https://www.ris.ripe.net/peerlist/all.shtml

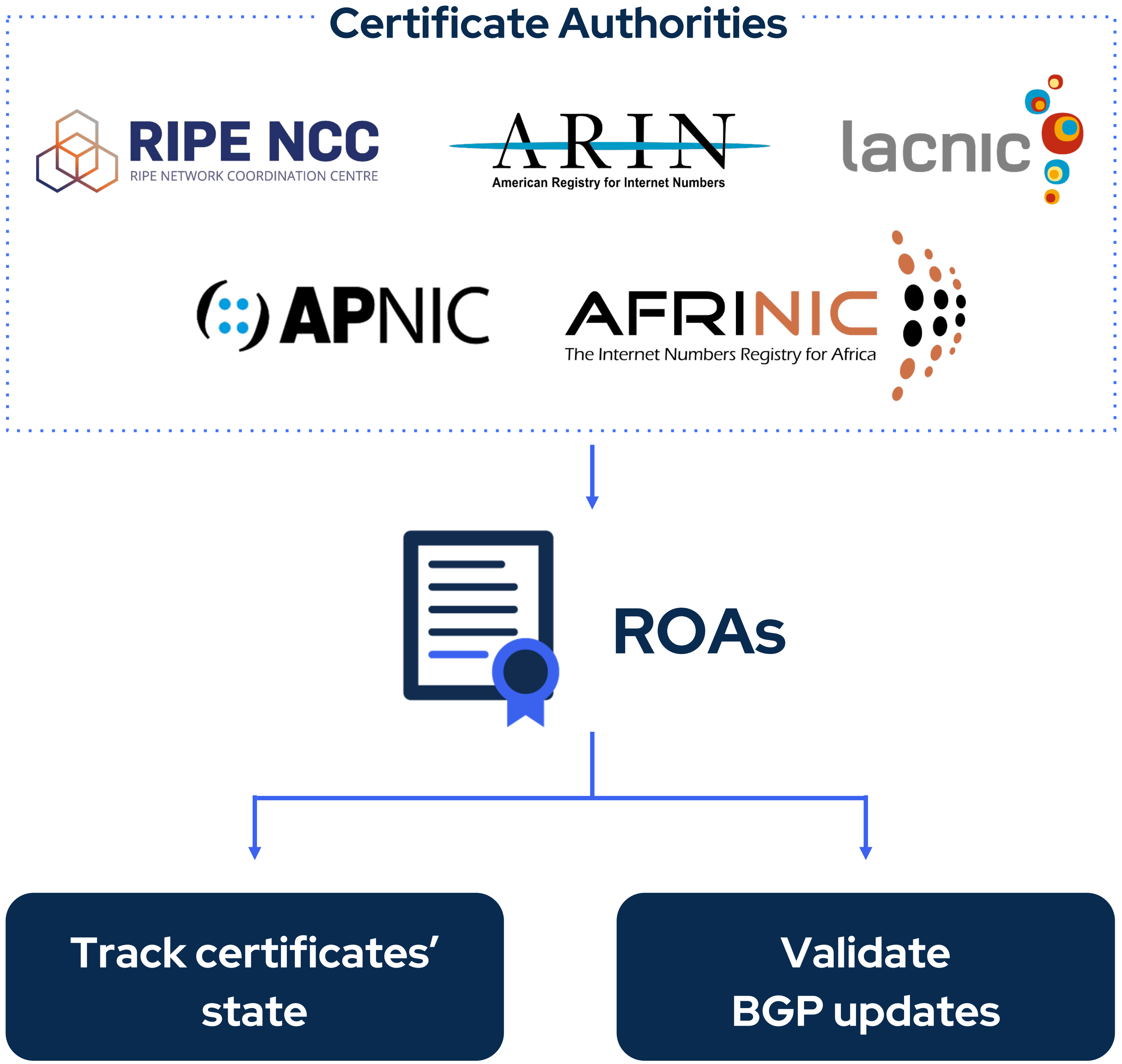
Data Service: Your routers

- **Multi-hop** BGP sessions



Data Service: RPKI

- Tracking the state of **ROA certificates**
- **Validating** BGP updates and detecting **invalids**



Certificate Authorities

RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ARIN
American Registry for Internet Numbers
lacnic
APNIC
AFRINIC
The Internet Numbers Registry for Africa

ROAs

Track certificates' state

Validate BGP updates

Alert Types

Supported Alert Types	Description
Exact Prefix Hijack	Illegal origin ASes that announce configured prefixes.
Sub-Prefix Hijack	Illegal origin ASes that announce subprefixes of configured prefixes.
Route Leak	Unexpected prefixes in the list of prefixes that are announced by configured ASes.
New Neighbor	New neighbors that appear to peer with configured ASes. Possible AS path manipulation.
Neighbor Leak/Hijack	New neighbors that not only appear to peer with configured ASes, but also propagate their prefixes.
Squatting	Illegal origin ASes announcing prefixes that are not currently announced by configured ASes.
Presence in AS Path	Presence of ASes in paths towards configured prefixes.
Invalid AS Path Pattern	Violation of valid pattern by AS paths towards configured prefixes.
Long AS Path	Paths towards configured prefixes exceed a specified length threshold.
Prefix Visibility Loss	Visibility of prefix falls below a configured data source count threshold.
Peering Visibility Loss	Visibility of peering falls below a configured data source count threshold.

Supported Alert Types	Description
RPKI-Invalid Detection	RPKI-Invalid announcements of configured prefixes by other ASes.
RPKI-Invalid Announcement	RPKI-Invalid announcements by configured ASes.
RPKI-Invalid Propagation	RPKI-Invalid routes propagated by configured ASes.
RPKI-NotFound Propagation	RPKI-NotFound routes propagated by configured ASes.
Bogon (Exact-)Prefix	Announcements of bogon prefixes by configured ASes.
Bogon (Sub-)Prefix	Announcements of bogon subprefixes by configured ASes.
Bogon AS	In-path presence of bogon ASes, in routes towards configured prefixes.
AS Path Comparison	Discrepancies in AS paths towards the same prefix, comparing between different Data Services, up to a terminating (end) AS.
Prefix Comparison	Discrepancies in prefixes announced by configured ASes, comparing between different Data Services.
Custom	User-defined

Root DNS Servers

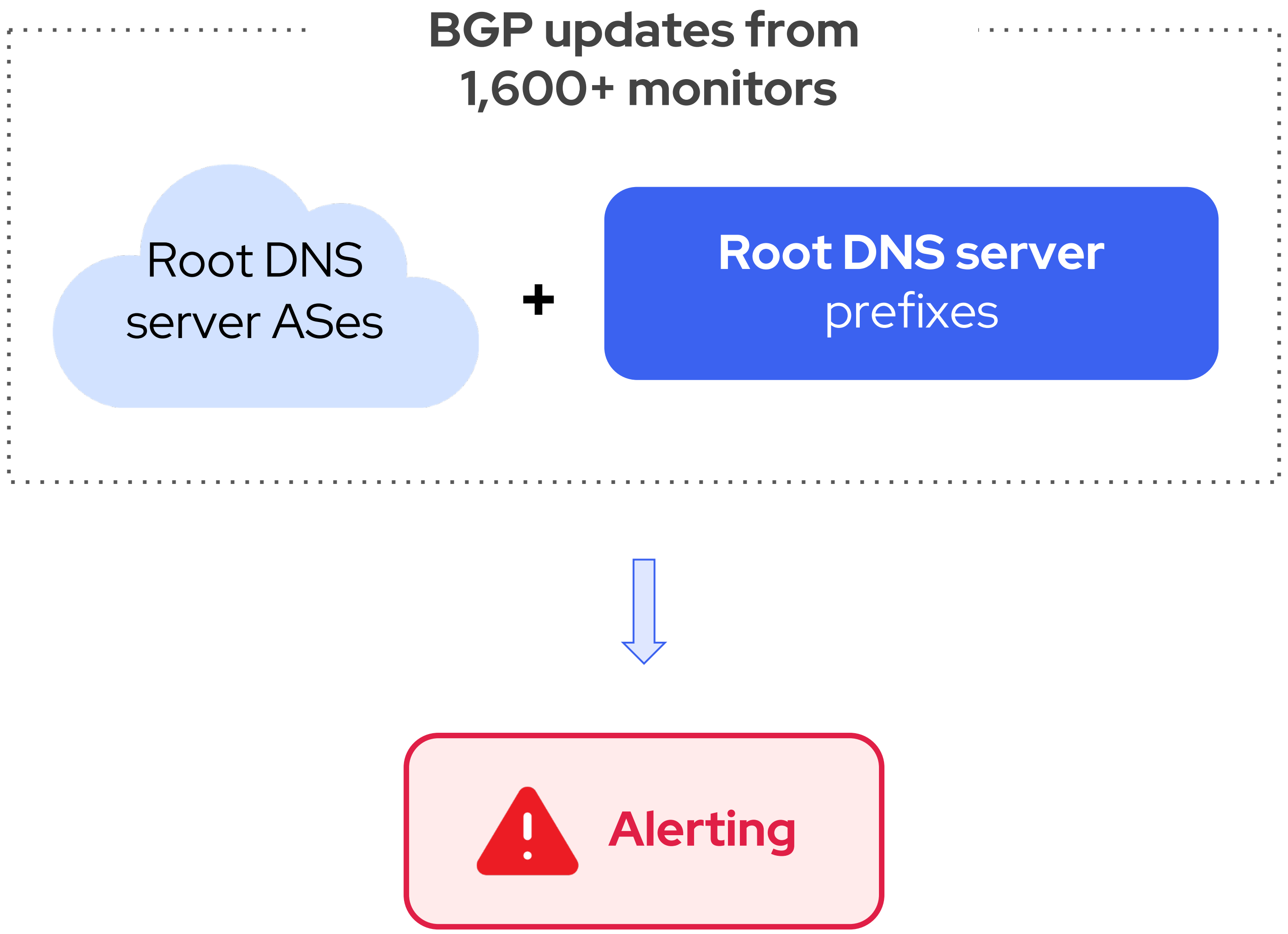
- The authoritative name servers that serve the DNS root zone

Name	IPv4	IPv6	Operator
A-Root	198.41.0.4	2001:503:ba3e::2:30	Verisign, Inc.
B-Root	199.9.14.201	2001:500:200::b	USC, Information Sciences Institute
C-Root	192.33.4.12	2001:500:2::c	Cogent Communications
D-Root	199.7.91.13	2001:500:2d::d	University of Maryland
E-Root	192.203.230.10	2001:500:a8::e	NASA (Ames Research Center)
F-Root	192.5.5.241	2001:500:2f::f	Internet Systems Consortium, Inc.
G-Root	192.112.36.4	2001:500:12::d0d	US Department of Defense (NIC)
H-Root	198.97.190.53	2001:500:1::53	US Army (Research Lab)
I-Root	192.36.148.17	2001:7fe::53	Netnod
J-Root	192.58.128.30	2001:503:c27::2:30	Verisign, Inc.
K-Root	193.0.14.129	2001:7fd::1	RIPE NCC
I-Root	199.7.83.42	2001:500:9f::42	ICANN
M-Root	202.12.27.33	2001:dc3::35	WIDE Project

Why Monitoring Root DNS Server Prefixes

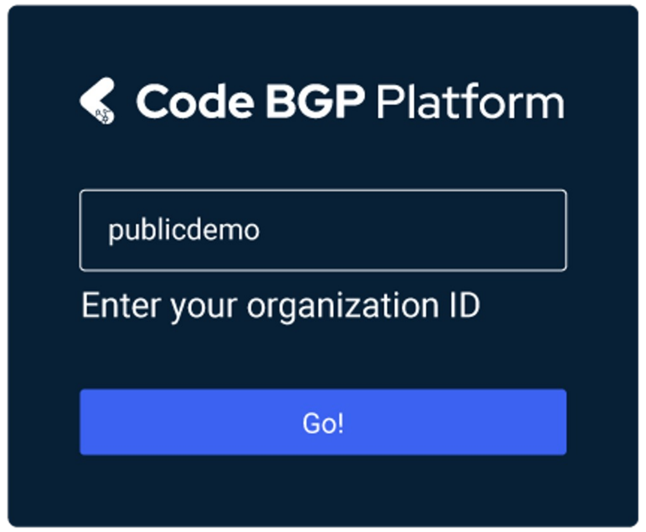
- Critical Internet infrastructure, worth protecting
- These prefixes are heavily anycasted
  - BGP anomalies (e.g. exact prefix hijacks) will go largely unnoticed, due to their limited impact on the data plane

We provide access for free to a Code BGP Platform instance which monitors the root DNS prefixes



How to get access to the Route DNS monitoring instance

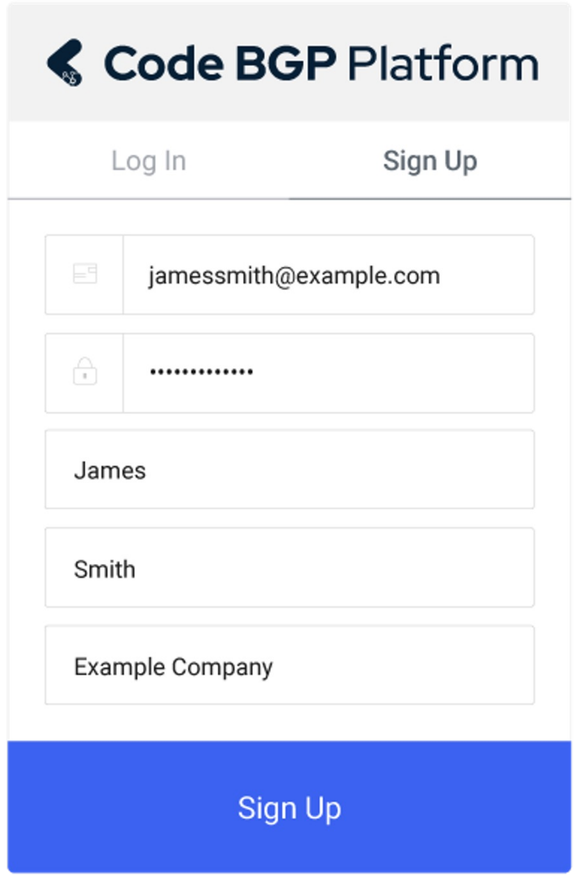
- Go to https://cloud.codebgp.com/ and in the Organisation ID type “publicdemo”
- Sign up
- Docs: https://docs.codebgp.com/



Code BGP Platform

publicdemo

Enter your organization ID



Code BGP Platform

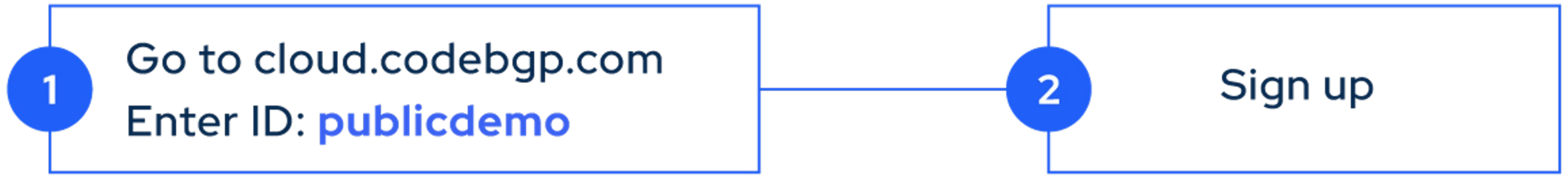
jamessmith@example.com

··············

James

Smith

Example Company



1 Go to cloud.codebgp.com
Enter ID: **publicdemo**

2 Sign up

Prefix Hijacking Demo

Code BGP Platform

Questions

✉ lefteris@codebgp.com

🌐 codebgp.com