QRATOR LABS

QRATOR.RADAR

Real-time BGP Monitoring

qrator.net

Your unique tool to find and fix network anomalies

The Internet is based on the interaction between autonomous systems (AS). AS constantly exchange routing information through the BGP protocol that makes it possible to choose traffic routes between cities and countries all around the world.

However, the fragility of the Internet lies in the lack of security mechanisms and limitations within the specifications of the Border Gateway Protocol.

Therefore, different routing anomalies may occur during the exchange process caused by errors in the network equipment configuration or attacks by cyber-criminals.

In 2022 only,

○ 29% of different telecom operators triggered global network anomalies, which they did not even realize in some cases,

○ 86% of Autonomous Systems were affected by BGP Incidents

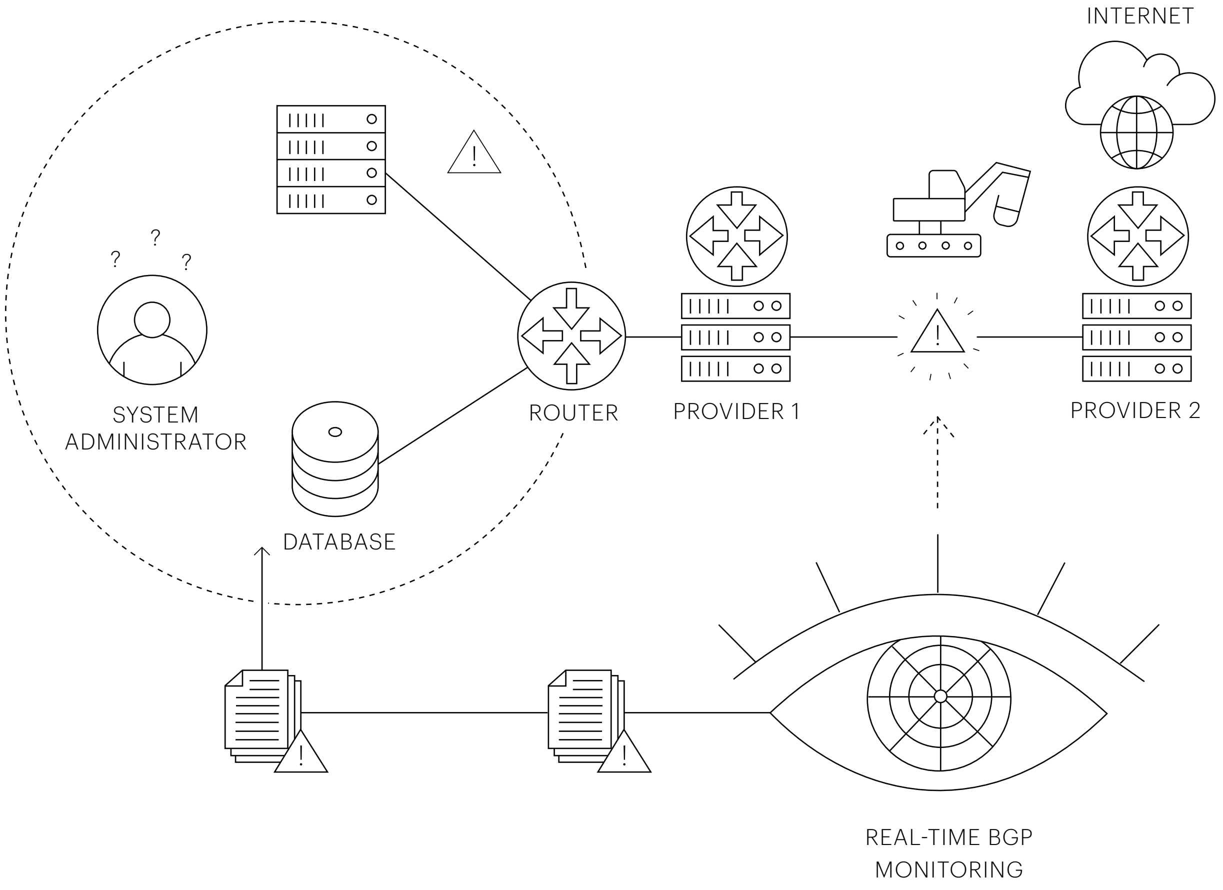
Why do you need BGP monitoring?

It is almost impossible to detect BGP anomalies once inside the customer's network, so troubleshooting BGP incidents is a significant challenge for network engineers.

To monitor traffic and detect anomalies just in time, you need an external professional tool that functions at the cross-domain routing level.

Qrator.Radar

Qrator.Radar from Qrator Labs is a unique platform designed to analyze routing information, detect incidents and changes in network connectivity in realtime.



Key benefits

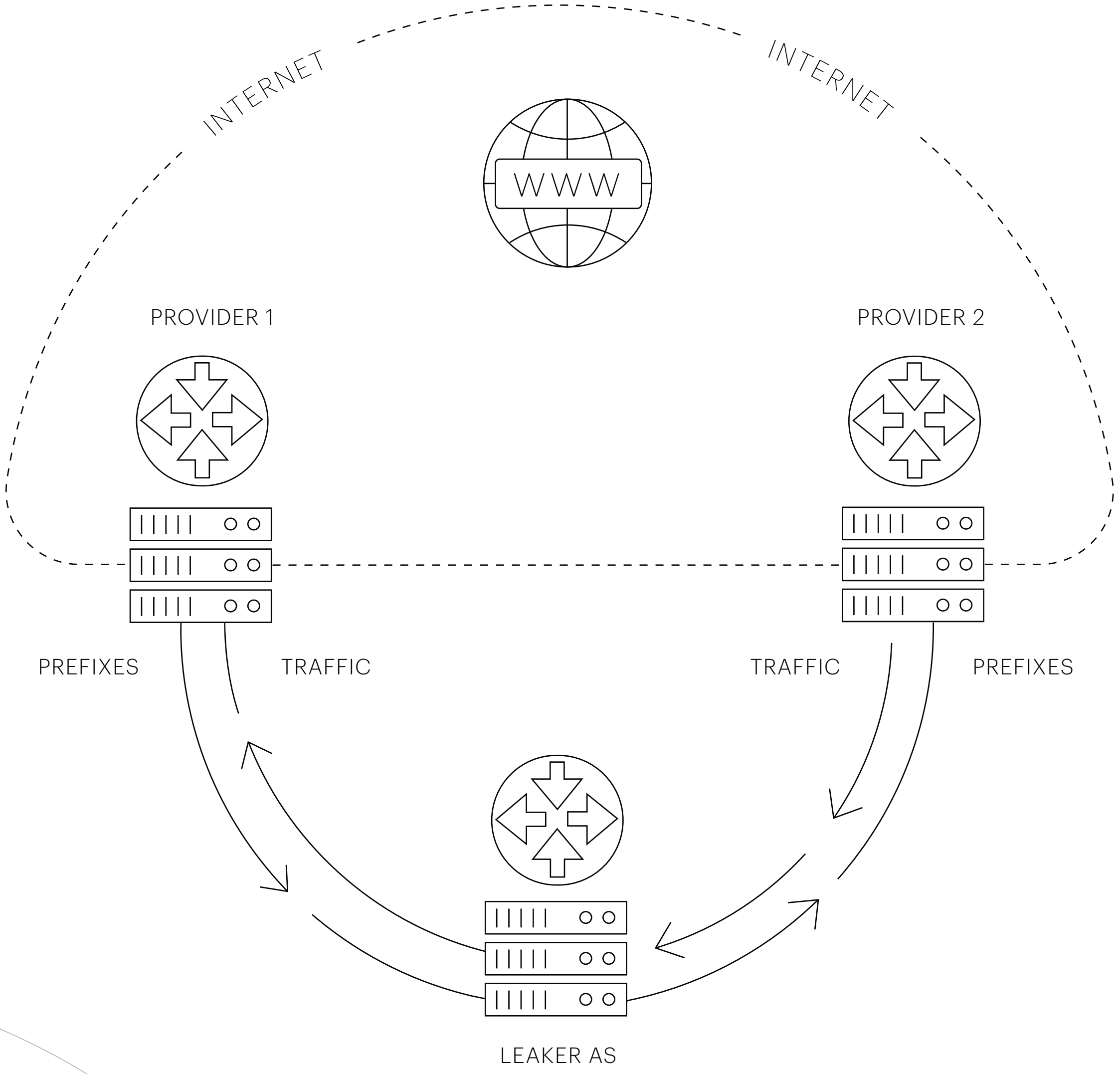
- One of the world's largest traffic data collectors — over 850 BGP sessions with major ISPs globally;
- The unique mathematical model that defines the relationships between AS's;
- Large number of types of BGP incidents detected;
- Historical routing data recorded since 2017;
- A platform to detect network anomalies and recognize their conditions and consequences in real-time;
- Seamless integration with other network monitoring systems through syslog, e-mail or API.

Operating Principles:

- Data is delivered to the Qrator.Radar collector in the form of route tables of all the Internet subnets available to operators (full view).
- Qrator Labs' specially developed algorithms are used to analyze the received full view.

Qrator.Radar monitors the following types of network anomalies:

BGP Route Leaks



BGP Route Leak is the redirection of traffic through an autonomous system that should not be on the route.

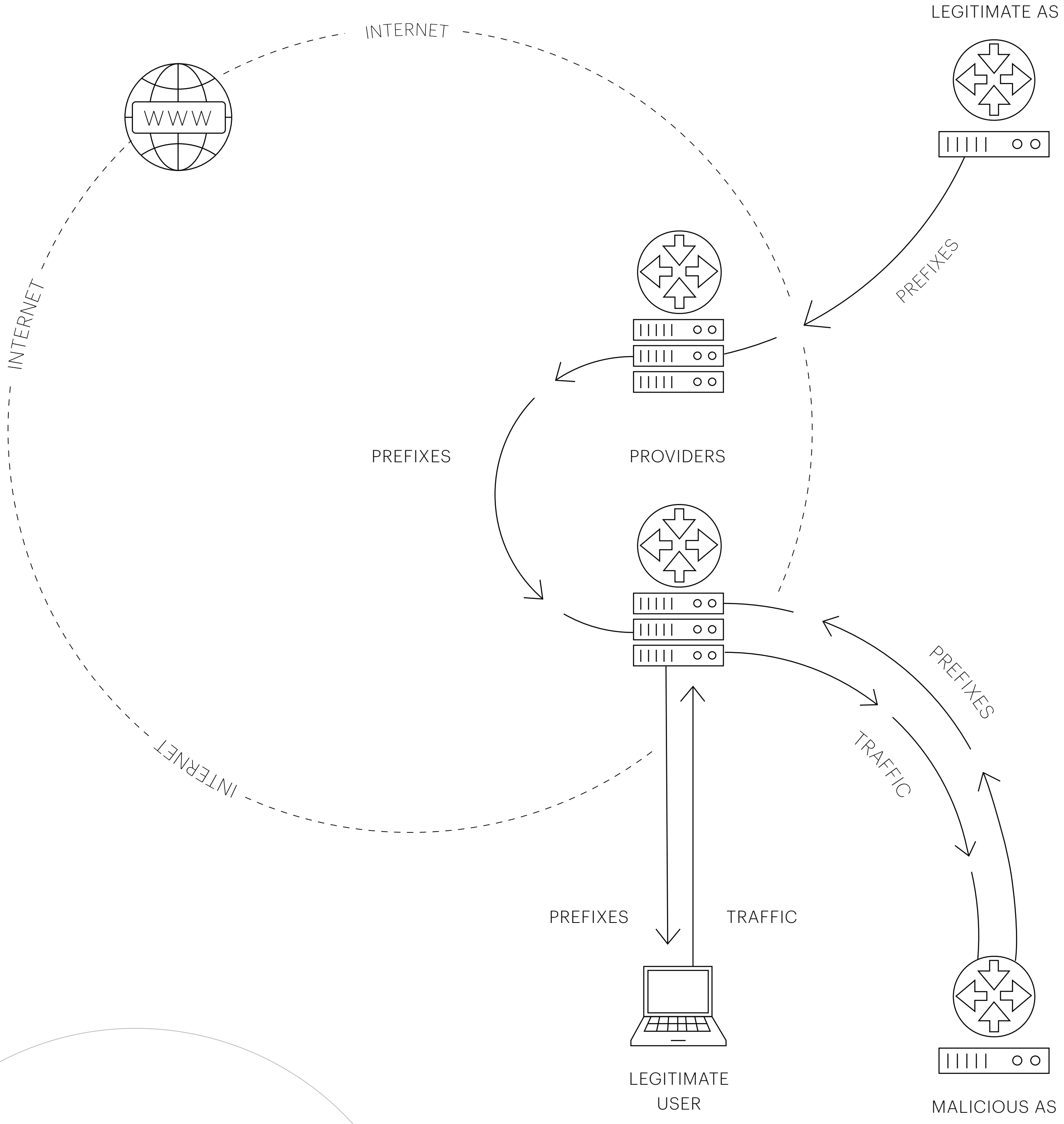
○ Increased network latency (RTT). In some cases, the delay to an affected service increases by 8 times and reaches several seconds during an incident;

○ Equipment failures and traffic losses (up to complete loss — DoS);

○ Man-in-the-Middle attacks.

BGP Hijacks

BGP Hijack is an illegitimate prefix announcement (traffic hijacking).



Impact:

- Traffic diversion to phishing sites and arranging Man-in-the-Middle attacks;
- Searching for passwords, financial and personal data in transmitted data;
- Deliberate organization of resources lockouts;
- DoS due to configuration errors.

Bogons

Bogon is announcing prefixes and Autonomous System Numbers (ASNs) that should not occur in routing tables.

Impact:

- Network unavailability due to invalid route filtering;
- Disclosing information about the local network to third parties.

Qrator.Radar captures several thousand routing incidents worldwide every day.

Feedback on anomalies is sent to customers in real-time.

This helps respond to network incidents immediately, mitigating possible adverse effects on the business and ensuring better network performance.

QRATOR LABS

+420 602 558 144
radar@qrator.net

qrator.net
radar.qrator.net