Presentación disponible con animaciones en **https://aspath.app/lacnic35-presentation**

ASPATH Project

Software open-source para monitoreo de colectores de rutas BGP.

Presenta:

Rodrigo Peña
Software Engineer

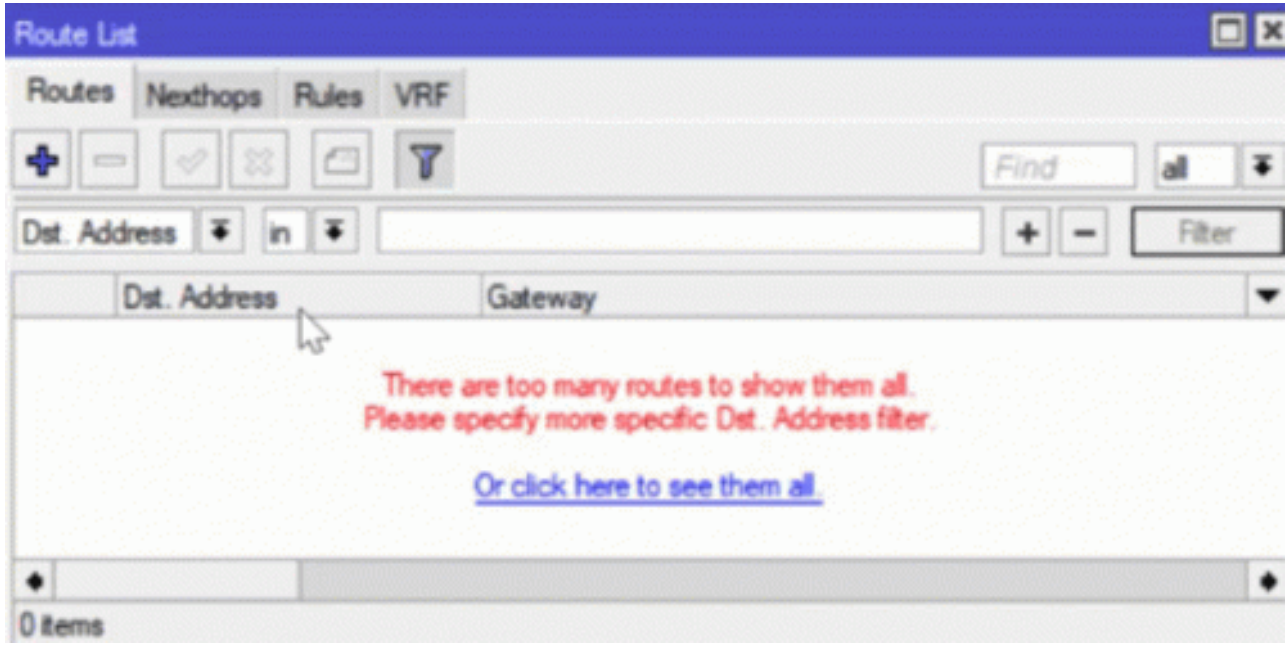
ASPATH

Problemas comunes

- "Cierta página no carga/funciona 🤔"
- "A que proveedor corresponde una dirección IP?"
- Búsqueda de causa
  - DNS ok? `dig lacnic.net`
  - Ping destino? `ping -f -c 100 lacnic.net`
  - **Problemas de ruteo**? bgp.he.net / BGPlay / `show ip bgp` / `traceroute` / ...

Mikrotik way

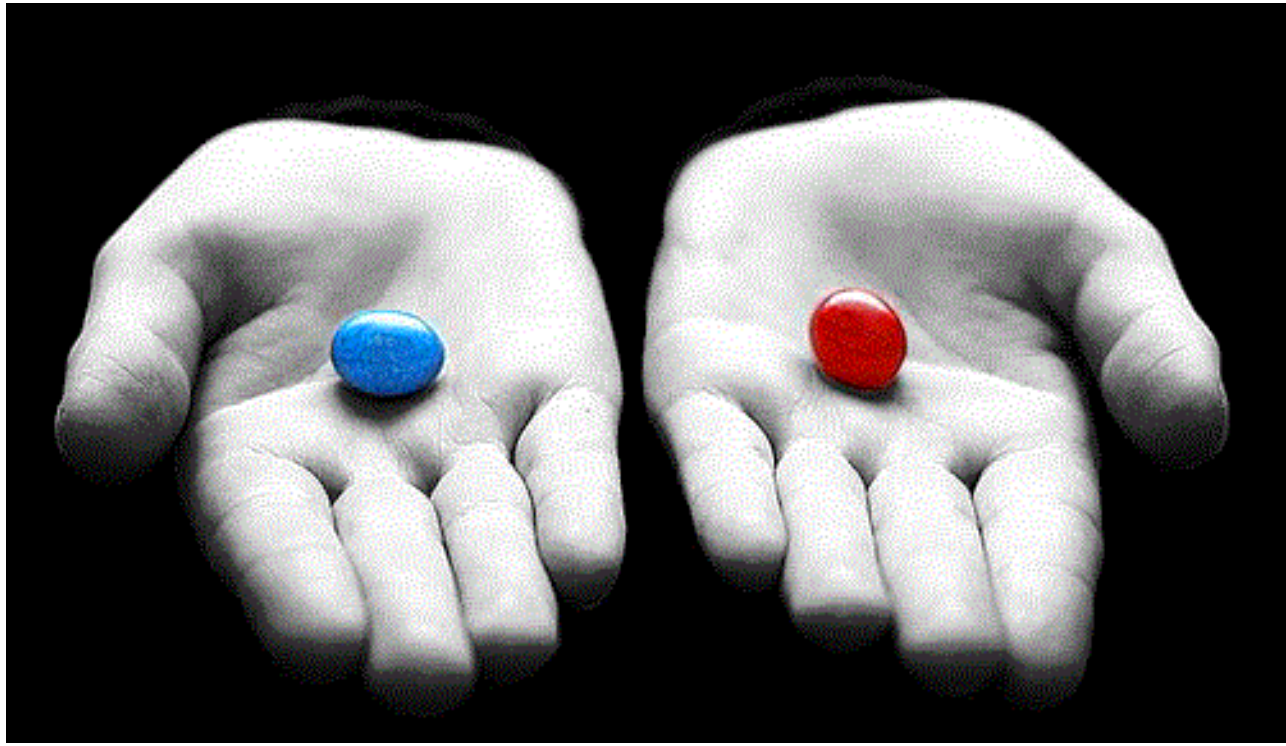
La tentación existe, pero estás poniendo mucho en juego por querer visualizar la tabla de rutas



Al momento de diagnosticar el problema ya desapareció

-**Azul**: Ya se arregló, sigo con mi vida

-**Roja**: Quiero saber la verdad



Por qué es tan valioso investigar

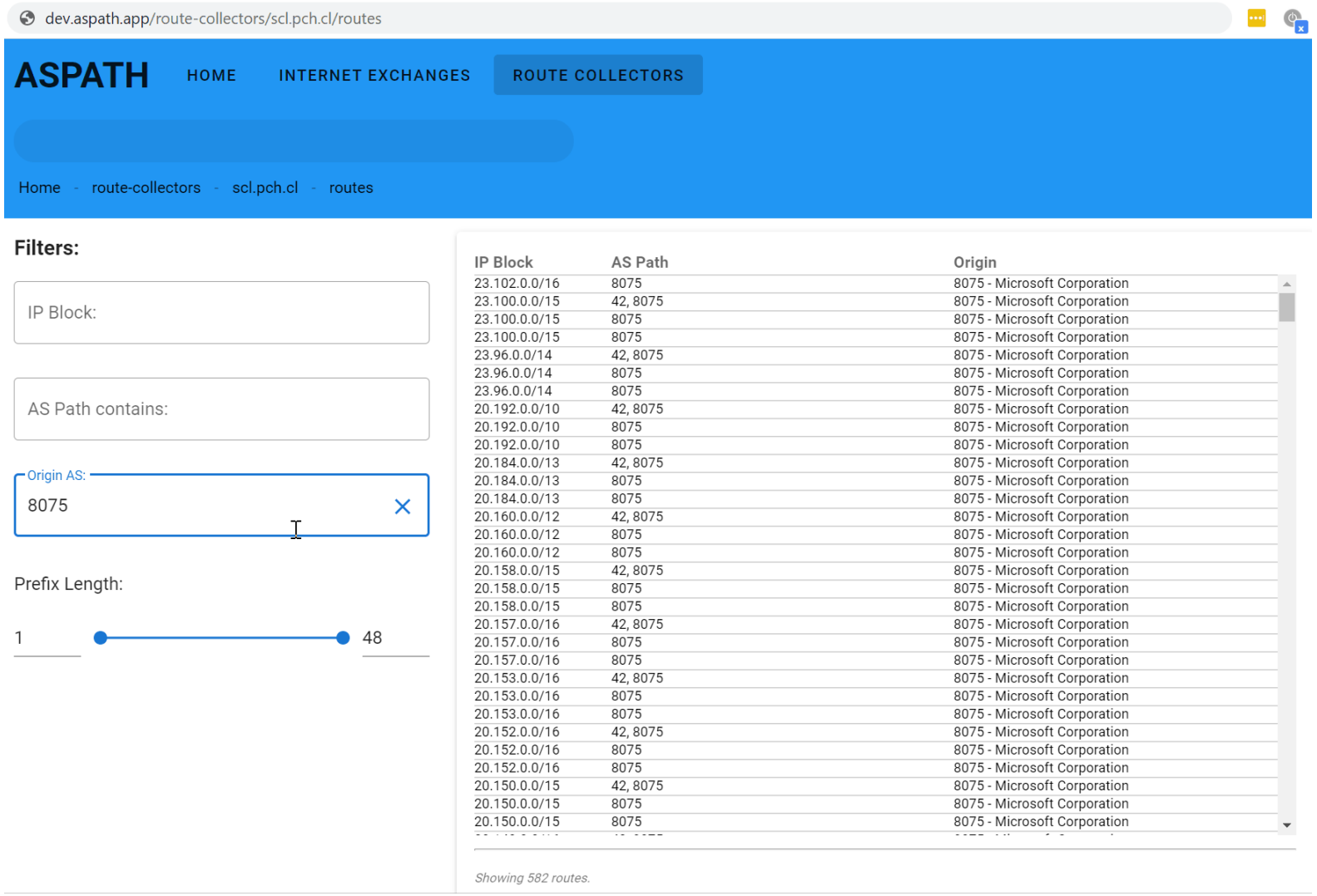
- Posible Hijack BGP
- Definir responsabilidades
- **Robustecer estabilidad de la red**

- Posibilidad de explorar la tabla de ruteo a lo largo del tiempo
- Desde la comodidad del navegador web
- Implementable con cualquier router o servidor de rutas

- Explorador de snapshots de tabla de ruteo con tecnologías web.
- Permite **almacenar y visualizar** tablas de ruteo de múltiples equipos a lo largo del tiempo.
- Desplegable de manera privada
- Código abierto bajo licencia MIT

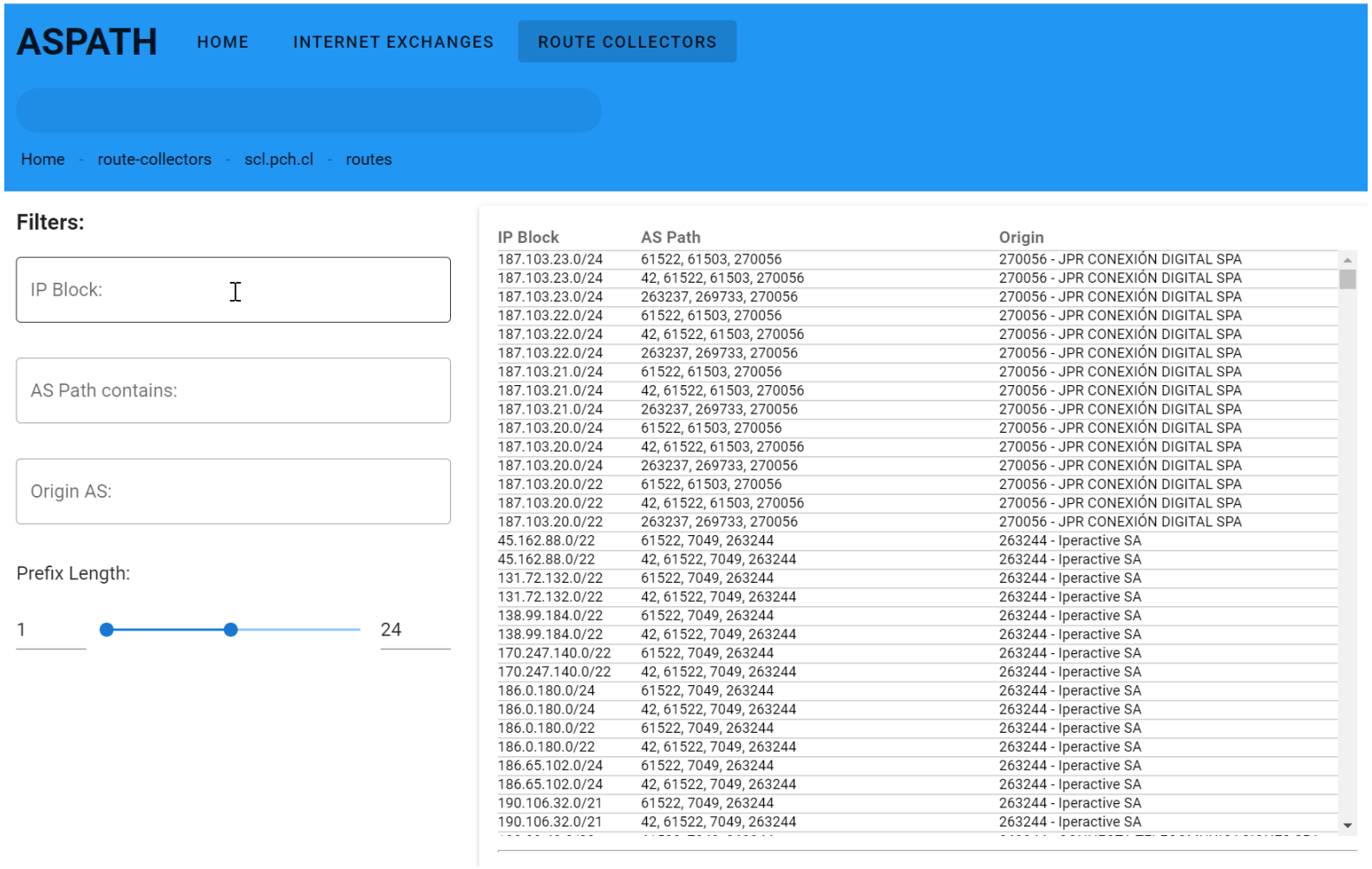
ASPATH

Cómo funciona



- Vista de snapshot proveniente de route collector de PCH.
- Filtros dinámicos para buscar dentro de tabla de ruteo.
- Lista de prefijos incluyendo otros datos como nombre de sistema autónomo.

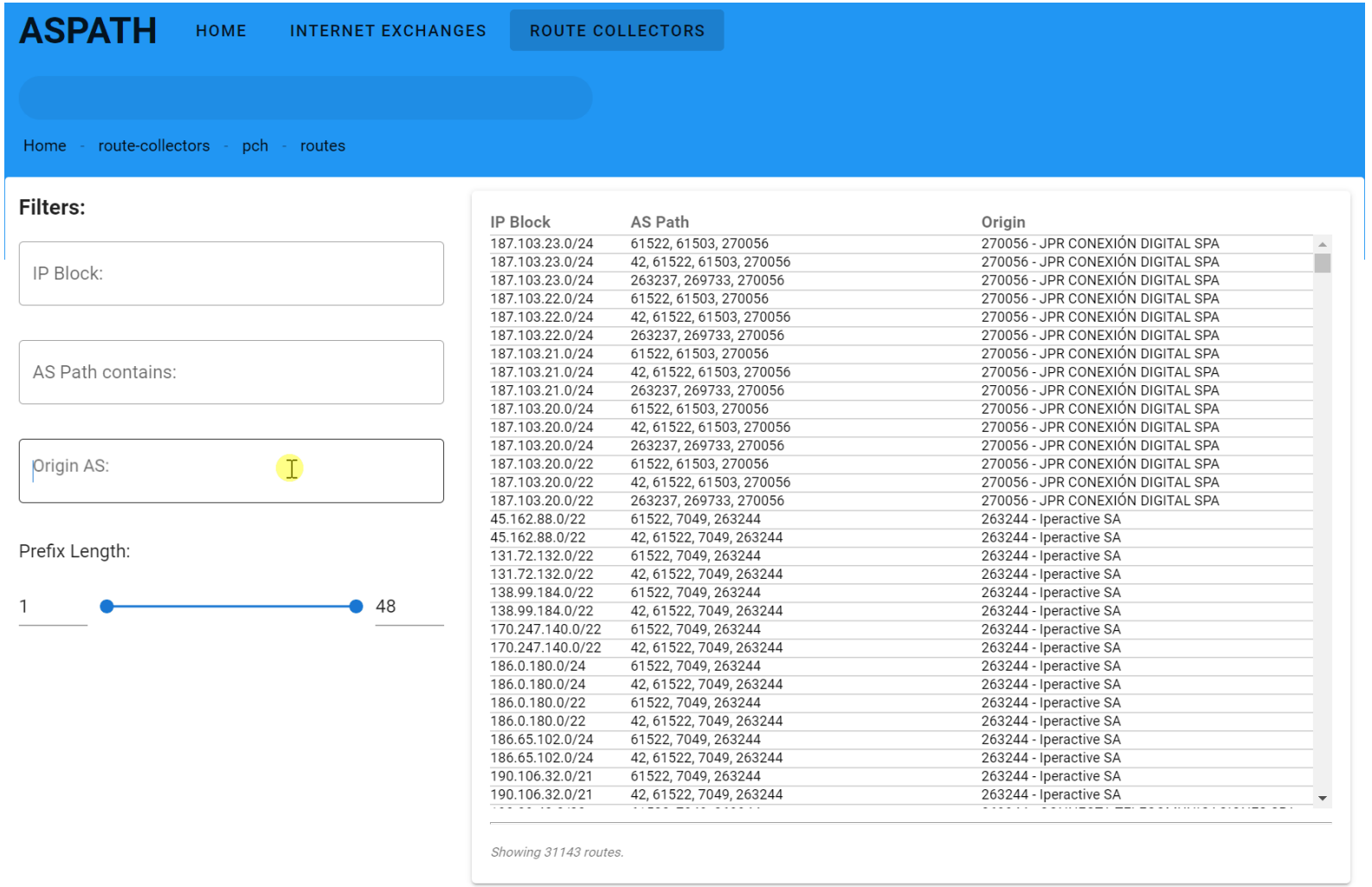
Caso práctico: buscando anuncios extraños en intercambio de tráfico



- Búsqueda rápida sobre bloques con incidentes típicos.
- Se logra encontrar hijack presente por largo tiempo.

ASPATH - Software código abierto para monitoreo de colectores de rutas https://aspath.app

Caso práctico: encontrando BGP Leaks en servidor de ruta



IP Block	AS Path	Origin
187.103.23.0/24	61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.23.0/24	42, 61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.23.0/24	263237, 269733, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.22.0/24	61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.22.0/24	42, 61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.22.0/24	263237, 269733, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.21.0/24	61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.21.0/24	42, 61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.21.0/24	263237, 269733, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.20.0/24	61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.20.0/24	42, 61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.20.0/24	263237, 269733, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.20.0/22	61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.20.0/22	42, 61522, 61503, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
187.103.20.0/22	263237, 269733, 270056	270056 - JPR CONEXIÓN DIGITAL SPA
45.162.88.0/22	61522, 7049, 263244	263244 - Iperactive SA
45.162.88.0/22	42, 61522, 7049, 263244	263244 - Iperactive SA
131.72.132.0/22	61522, 7049, 263244	263244 - Iperactive SA
131.72.132.0/22	42, 61522, 7049, 263244	263244 - Iperactive SA
138.99.184.0/22	61522, 7049, 263244	263244 - Iperactive SA
138.99.184.0/22	42, 61522, 7049, 263244	263244 - Iperactive SA
170.247.140.0/22	61522, 7049, 263244	263244 - Iperactive SA
170.247.140.0/22	42, 61522, 7049, 263244	263244 - Iperactive SA
186.0.180.0/24	61522, 7049, 263244	263244 - Iperactive SA
186.0.180.0/24	42, 61522, 7049, 263244	263244 - Iperactive SA
186.0.180.0/22	61522, 7049, 263244	263244 - Iperactive SA
186.0.180.0/22	42, 61522, 7049, 263244	263244 - Iperactive SA
186.65.102.0/24	61522, 7049, 263244	263244 - Iperactive SA
186.65.102.0/24	42, 61522, 7049, 263244	263244 - Iperactive SA
190.106.32.0/21	61522, 7049, 263244	263244 - Iperactive SA
190.106.32.0/21	42, 61522, 7049, 263244	263244 - Iperactive SA

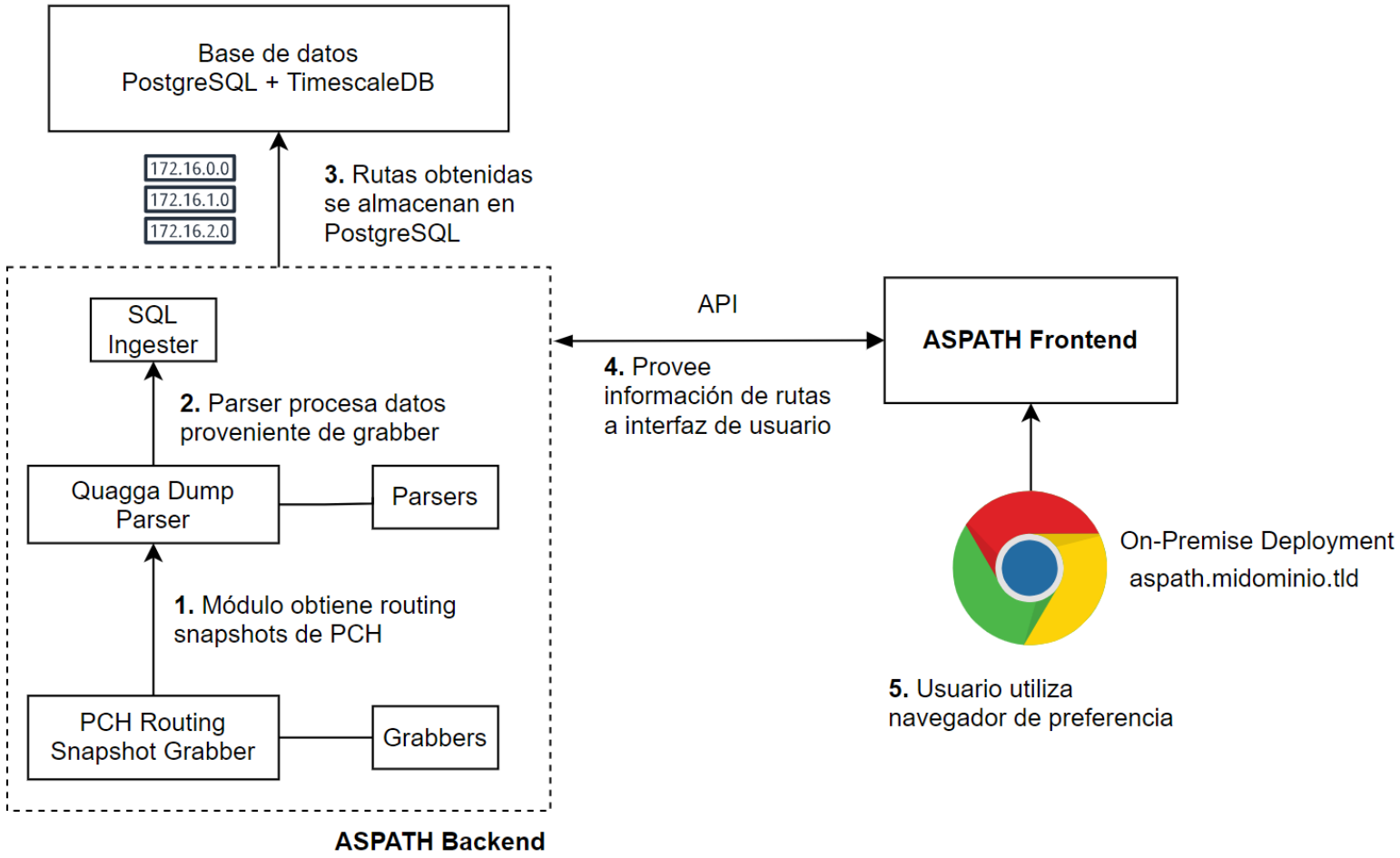
1. Búsqueda de rutas provenientes de microsoft.
2. Tras explorar tabla, se encuentran rutas con AS_PATH sospechosos.
3. Se detecta BGP leak proveniente de inyección de rutas de tránsito hacia IXP.

ASPATH - Software código abierto para monitoreo de colectores de rutas https://aspath.app

Cómo se implementa software ASPATH

- Actualmente, se consideran 2 métodos para agregar datos de ruteo al software:
  - **Quagga dump grabber**: Útil para trabajar con routing snapshots de proveído por terceros. **PCH provee routing snapshots diarios de sus colectores de rutas en este formato**.
  - **Colector GoBGP**: Implementación moderna de BGP. Se puede desplegar en una máquina virtual y hacer sesión multihop contra router de borde. **Implementación compatible con cualquier router que implemente BGP**.

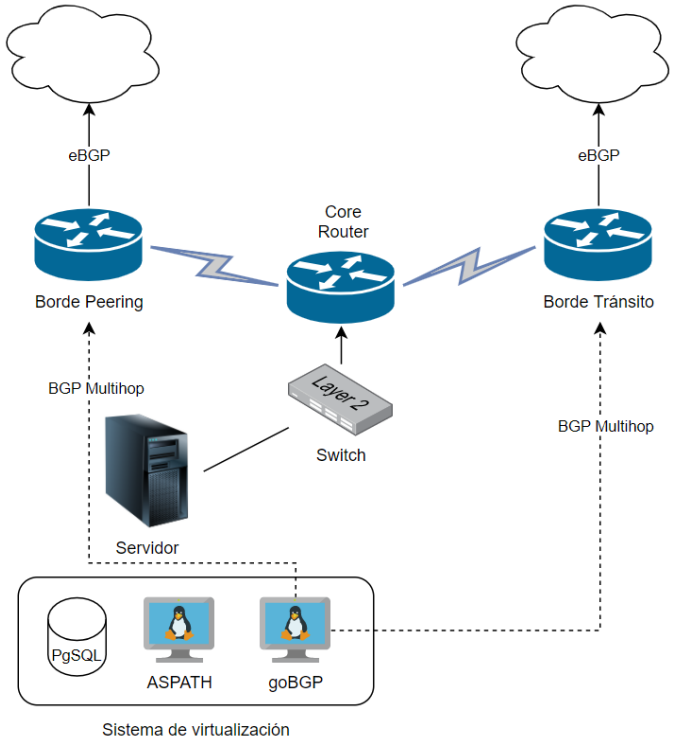
Diagrama de funcionamiento



- Proceso para alimentar al software con los Routing Snapshots disponibles desde Packet Clearing House.
- Este despliegue no requiere interacción con ningún router.

Diagrama de funcionamiento para ISP

Backbone de ejemplo



- Se instala goBGP como colector de rutas.
- goBGP mantendrá sesiones multihop contra routers de borde
- ASPATH extraerá periódicamente la tabla de ruteo de goBGP para alimentar la base de datos.

Roadmap

Q2 2021

- **Lanzamiento versión Beta**
- Explorador de rutas en progreso
- Ver snapshots pasados en progreso
- Grabber Quagga y goBGP

Q3 2021

- Lanzamiento versión estable
- Capacidad de compartir snapshots entre organizaciones

Te necesitamos

- Operadores de red que deseen implementar software
- Desarrolladores que quieran ser parte del proyecto
    - Python, Javascript, Ruby
- Interesados: https://aspath.app
- Otros: Suscribirse al newsletter para recibir noticias del proyecto

Proyecto bajo licencia MIT ¿🤔?

- Código abierto y disponible en https://aspath.app.
- Sin fees ni royalties.
- Se permite:
  - Uso comercial del software
  - Libre distribución y modificación de este.
  - Uso privado

¿Preguntas? 🤔

Software open-source para monitoreo de colectores de rutas BGP.

Presenta:

Rodrigo Peña
Software Engineer

ASPATH