



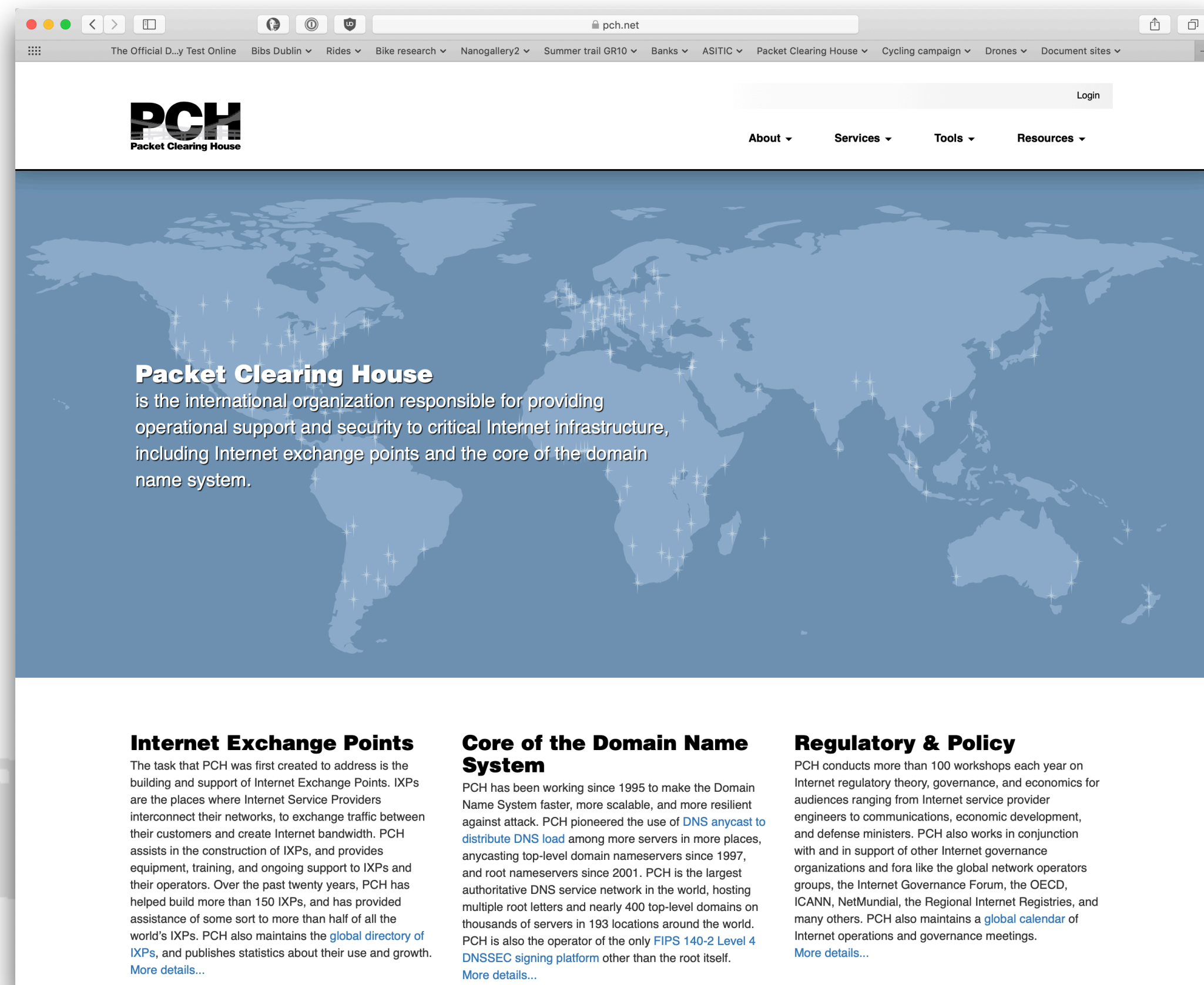
Recursos y herramientas para ISPs y IXPs/PITs



Packet Clearing House
AS42 & AS3856

¿Quienes somos?

PCH es una organización internacional sin ánimo de lucro que proporciona apoyo operacional y seguridad a la infraestructura crítica de Internet, como los IXPs y el núcleo del Sistema de Nombres de Dominio.



The screenshot shows the PCH website homepage. At the top left is the PCH logo. A navigation menu includes 'About', 'Services', 'Tools', and 'Resources'. A 'Login' button is in the top right. The main content area features a world map with a blue overlay and the text: 'Packet Clearing House is the international organization responsible for providing operational support and security to critical Internet infrastructure, including Internet exchange points and the core of the domain name system.' Below this are three columns of text: 'Internet Exchange Points', 'Core of the Domain Name System', and 'Regulatory & Policy', each with a brief description and a 'More details...' link.

- **Internet Exchange points:** PCH apoya la construcción de puntos neutros de intercambio de tráfico a través de donación de equipamiento, asesoría, acompañamiento y formación. PCH mantiene el IXP Directory y herramientas para ISPs e IXPs.
- **Core of the Domain Name System:** PCH trabaja para hacer el Sistema de Nombre de Dominio (DNS) más rápido, escalable y más resiliente ante ataques. PCH fue pionero en el uso de anycast para distribuir la carga DNS en un mayor número de servidores por el mundo, haciendo anycast de servidores DNS autoritativos desde 1997 y servidores DNS root desde 2001.
- **Regulatory and Policy:** PCH participa en talleres, seminarios y formaciones sobre políticas regulatorias, gobernanza y economía de Internet. PCH trabaja y colabora con instituciones afines como ICANN, ISOC, ARIN, LACNIC, AFRINIC, APNIC y RIPE, así como los grupos de operadores de red (NOGs).

Servicios, recursos y herramientas PCH

PCH tiene puntos de presencia en 193 puntos de intercambio de trafico, en los cinco continentes. Política de peering abierta, peering bilateral con todos los ASNs.

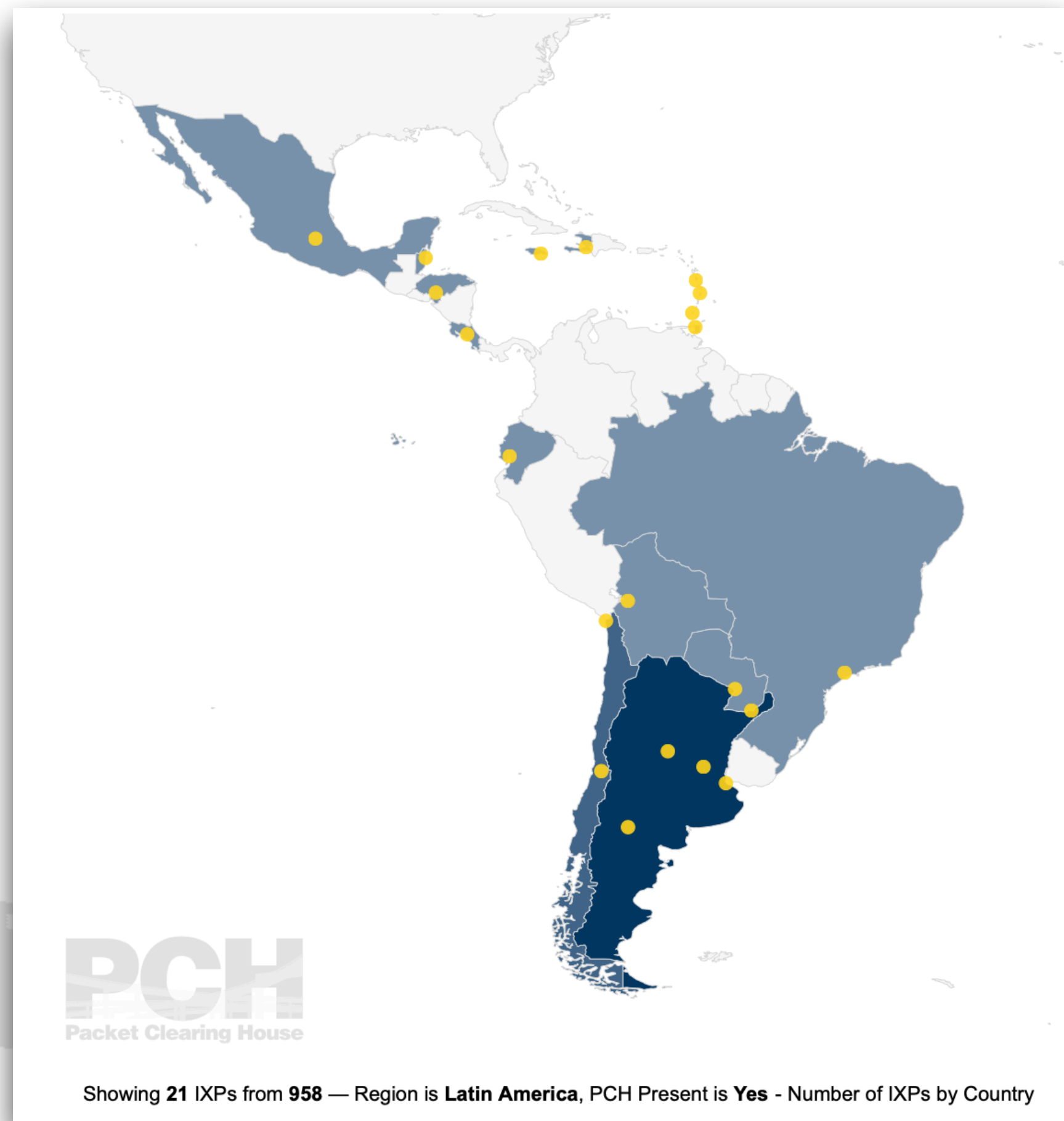


The screenshot shows the PCH website's 'Point of Presence Locations' page. The page title is 'Packet Clearing House Point of Presence Locations'. Below the title, it states: 'As of May 2019, PCH has Points of Presence (PoPs) in 193 Internet Exchange Points. The 10 most recently added PoP locations are:'. A list of 10 locations follows, each with a number and a link to more information: 1. Baltimore, United States (BaltIX), 2. Arica, Chile (PIT Chile Arica), 3. Tel Aviv, Israel (IIX), 4. Marseille, France (France-IX Marseille), 5. Marseille, France (DE-CIX Marseille), 6. Madrid, Spain (DE-CIX Madrid), 7. Lisbon, Portugal (GIGA-PIX), 8. Belgrade, Serbia (SOX), 9. Madrid, Spain (ESpanix), 10. Dakar, Senegal (SENIX). Below the list, it says 'All 193 are shown on this map:'. A world map is displayed with numerous yellow dots representing PoP locations across all continents. The PCH logo is visible in the bottom left corner of the page content, and the footer contains a Creative Commons license notice, 'PRIVACY', and 'DONATE' links.

- Replicas de D-Root and E-Root
- Servidores DNS autoritativos para 400+ TLDs, incluyendo 100+ ccTLDs, entre ellos diversos en la region como .ar, .bo, .cl, .cr, .do, .ec, .gt, .mx, .pe, .py
- Servidores DNS autoritativos de zonas reversas (in-addr.arpa, ip6.arpa)
- Resolver recursivo publico Quad9 (9.9.9.9)
- Route collectors para recopilación y archivo de información de enrutamiento
- Looking-glass interactivo

Nodos PCH en la region LAC

21 nodos repartidos en 16 países.



Pais	Ciudad	Nombre IXP	IATA
Argentina	Buenos Aires	CABASE IXP Buenos Aires	bue
Argentina	Córdoba	CABASE IXP Córdoba	cor
Argentina	Neuquén	CABASE IXP Neuquén	nqn
Argentina	Posadas	CABASE IXP Posadas	pos
Argentina	Rosario	CABASE IXP Rosario	ros
Belize	Belize City	Belize Internet Exchange Point	bze
Bolivia	La Paz	IXP MegaLink	lpb
Brazil	São Paulo	Ponto de Troca de Tráfego Metro São Paulo	gru
Chile	Arica	PIT Chile Arica	ari
Chile	Santiago	PIT Chile - Santiago	scl
Costa Rica	San Jose	Punto de Intercambio Neutro de Internet	sjo
Dominica	Roseau	Dominica National Internet Exchange Point	dom
Ecuador	Guayaquil	IXP Ecuador	gye
Grenada	St. Georges	Grenada Internet Exchange	gnd
Haiti	Port au Prince	AHTIC Internet Exchange Point	pap
Honduras	Tegucigalpa	IXP-HN Puntos de Intercambio de Tráfico – Honduras	tgu
Jamaica	Kingston	Jamaica Internet Exchange Point	kin
Mexico	Mexico DF	Mexico IXP	mex
Paraguay	Asunción	Punto de Intercambio de Tráfico de Paraguay	asu
Saint Lucia	Castries	Saint Lucia IXP	slu
Trinidad and Tobago	Barataria	Trinidad and Tobago Internet Exchange	pos

Looking-glass interactivo

Herramienta disponible para detección de incidentes, averías, etc. a través de consultas en tiempo real en todos los IXPs en los que PCH se encuentra hospedado.

The screenshot shows the PCH Looking Glass web interface. At the top, there is a navigation bar with the PCH logo and links for About, Services, Tools, and Resources. Below this is the 'Looking Glass' section, which contains a list of IXPs, a query selection menu, and an input field for arguments. The IXP list includes locations like RomandIX, A-IX, AAIX, AIX, AIXP, AMS-IX, ANGONIX, AO-IXP, APE, and ARMIX. The query menu offers options such as 'show ip bgp summary', 'show ipv6 bgp summary', and 'show ip bgp <prefix> [netmask|prefix|length]'. A 'Submit' button is located at the bottom right of the form area.

Consultas:

- show ip bgp summary
- show ipv6 bgp summary
- show ip bgp <prefix> [netmask|prefix|length]
- show ipv6 bgp <prefix>
- show ip bgp regex <regex>
- ping
- traceroute

Ejemplo de uso looking-glass

```
Result
BGP router identifier 66.102.32.68, local AS number 3856
RIB entries 682725, using 42 MiB of memory
Peers 77, using 189 KiB of memory
Peer groups 8, using 128 bytes of memory
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
200.23.206.4	4	22850	16283	16280	0	0	0	01w4d07h	4
200.23.206.12	4	52411	25541	23862	0	0	0	4d03h27m	1
200.23.206.3	4	64112	410170	359001	0	0	0	04w1d18h	4
200.23.206.37	4	266826	83210	72866	0	0	0	31w1d11h	Idle (Admin)
200.23.206.38	4	266866	456087	400011	0	0	0	01w0d01h	3
200.23.206.39	4	266866	455522	398922	0	0	0	2d19h36m	1
200.23.206.44	4	265675	358540	313933	0	0	0	06w2d22h	4
200.23.206.67	4	28096	294209	178994	0	0	0	01w0d10h	6
200.23.206.91	4	13381	0	0	0	0	0	never	Connect
200.23.206.29	4	266801	490877	429916	0	0	0	07w2d14h	4
200.23.206.209	4	32934	481472	461040	0	0	0	10w1d06h	36
200.23.206.227	4	13335	67066	64189	0	0	0	03w1d06h	211
66.102.32.65	4	42	560224	508674	0	0	0	17:26:06	127
200.23.206.55	4	21765	167468	160586	0	0	0	46w6d22h	Active
200.23.206.57	4	266713	568583	497521	0	0	0	01w0d07h	Active
200.23.206.60	4	262237	1063069	1014421	0	0	0	6d13h49m	81
200.23.206.70	4	263237	142714	273137	0	0	0	37w6d23h	Active
200.23.206.78	4	265703	114171	220139	0	0	0	38w6d21h	Active
200.23.206.90	4	13381	588485	508289	0	0	0	02w3d23h	40
200.23.206.93	4	265662	746451	508389	0	0	0	01w0d19h	5

```
[...]
Total number of neighbors 43
```

- **Troubleshooting:**

- Qué prefijos esta anunciando el ASN XXXX ?

- **Optimización:**

- Cuál es el AS_PATH para llegar al ASN YYYY?

- **Dimensionamiento:**

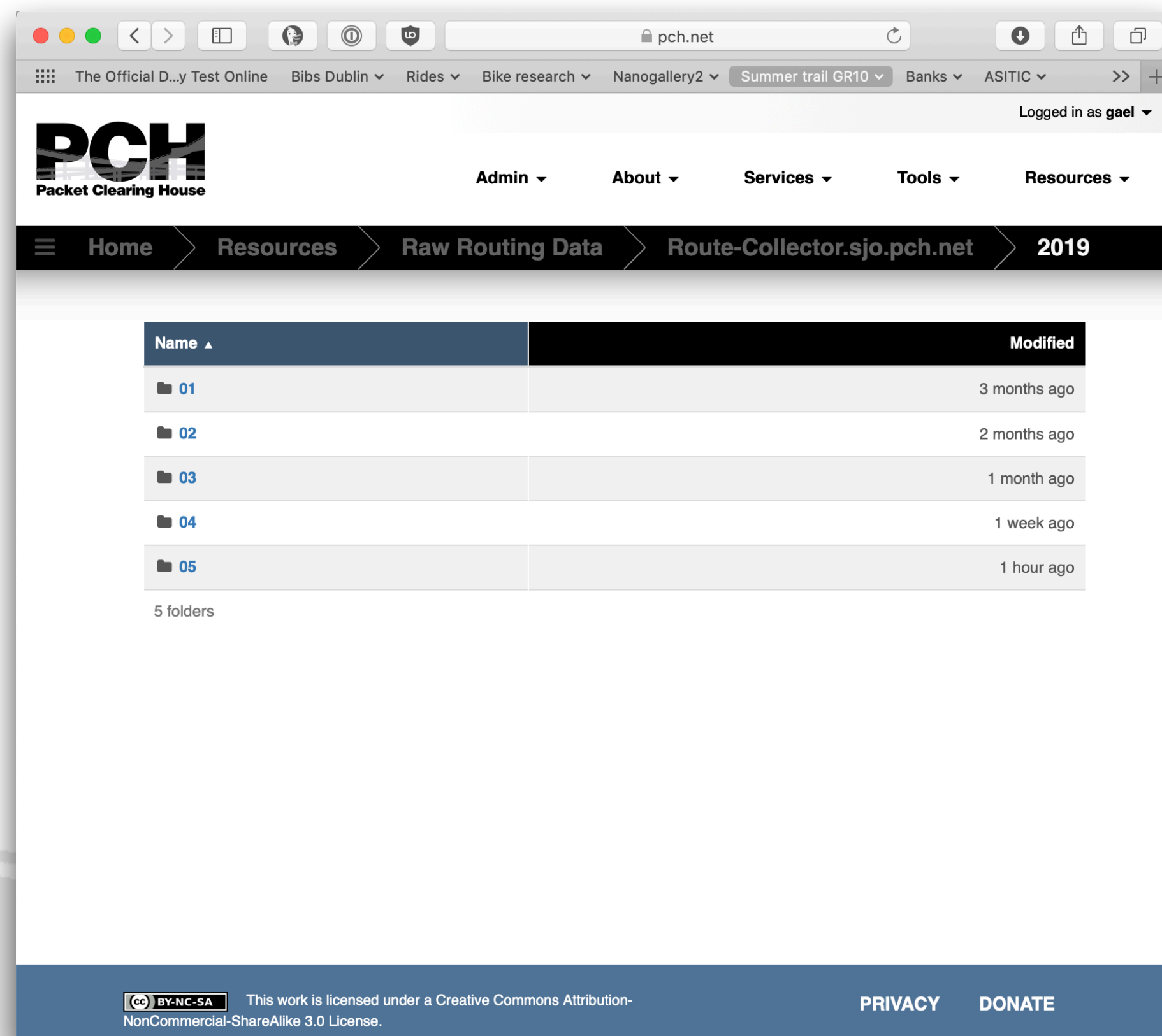
- Filtros: cuántos prefijos esta anunciando el route-server?

```
BGP routing table entry for 50.31.196.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
Advertised to non peer-group peers:
206.220.231.55
6762 262287 30081
198.32.176.70 from 198.32.176.70 (195.22.206.253)
Origin IGP, metric 0, localpref 100, valid, external, best
Community: 3856:50800
Last update: Sat Apr 27 18:21:54 2019

2914 6762 262287 30081
129.250.10.57 from 129.250.10.57 (129.250.0.53)
Origin IGP, metric 0, localpref 100, valid, external
Community: 3856:50800
Last update: Sat Apr 27 12:23:57 2019
```

MRT Routing Updates & Daily snapshots

Representa un archivo histórico de información de enrutamiento recopilado en todos los IXPs en los que PCH esta hospedado.



- **Archivos MRT con updates BGP:** flujo de mensajes BGP recibidos por los route collectors de PCH. Representa los cambios en información BGP recibida a lo largo del día y que afecta a la composición de la tabla de enrutamiento. 1440 archivos al día, uno cada 10min. Archivo binario.
- **Daily snapshots:** estado de la tabla de enrutamiento del route-collector cuando se tomo el “snapshot” diario. Archivo de texto, uno al dia.

Ejemplo de uso archivos MRT

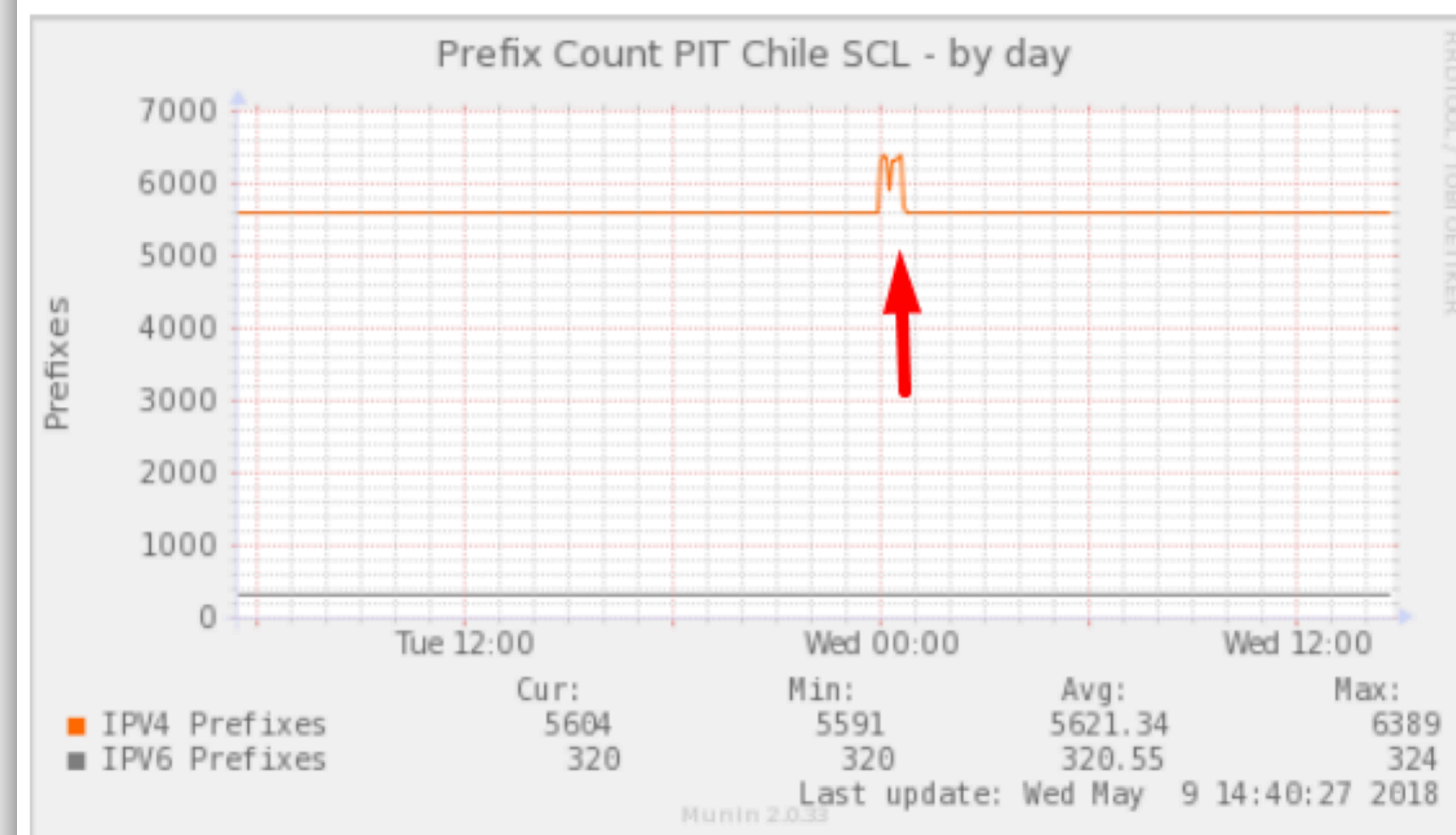
A diferencia de otras herramientas de medición y análisis, los archivos MRT registran la actividad local en el punto neutro de Internet.

Información histórica, algunos de ellos desde 2010.

- **Investigación y análisis del impacto de un evento:** por ejemplo, averiguar qué prefijos se anunciaron o retiraron en un determinado momento. Ejemplos: incidente PIT Chile, avería en DE-CIX.
- **Medición y monitoreo:** prefijos únicos, porcentaje de prefijos asignados al país visibles en el IXP, medición de prefijos anunciados por el route-server en el contexto de RPKI implementado (ejemplos proyecto ARDA en Africa, ISOC MANRS IXP Filter).
- **Investigación ámbito docente** en universidades que trabajan en enrutamiento inter-ASN

Quería hacerte una consulta específica. Ayer hubo un incidente con rutas en la red nacional donde “alguien” anunció unos 800 prefijos adicionales a lo regular y unos 20 ASN. Normalmente en la red nacional de Chile vemos del orden de 5300 prefijos y 250 ASN, este aumento repentino generó muchos problemas especialmente en quienes tenían un límite de prefijos recibidos para el nacional muy acotado y a consecuencia de eso sus sesiones BGP nacionales se cerraron.

Queremos averiguar quien fue ese “alguien” para poder entender por qué pasó esto y como evitarlo a futuro. Esto ocurrió entre las 00:00 y la 01:00 de hoy hora de Chile. Habrá quedado evidencia en el route collector de PCH?



Ejemplo de toolset para uso de archivos MRT

1. Descarga del fichero (curl, wget)

```
curl https://www.pch.net/resources/Raw_Routing_Data/route-  
collector.sjo.pch.net/2019/05/08/route-  
collector.sjo.pch.net-mrt-bgp-updates-2019-05-08-00-00.gz
```

2. Procesar el fichero MRT y exportar (bgpdump, bgpreader)

```
BGP4MP|03/14/19 03:34:08|A|206.126.225.20|6939|180.190.56.0/22|6939 40633 4775 132199|IGP  
BGP4MP|03/14/19 03:34:08|A|206.126.225.20|6939|180.190.56.0/24|6939 40633 4775 132199|IGP  
BGP4MP|03/14/19 03:34:08|A|206.126.225.253|53339|180.190.56.0/22|6939 40633 4775 132199|IGP  
BGP4MP|03/14/19 03:34:08|A|206.126.225.253|53339|180.190.56.0/24|6939 40633 4775 132199|IGP  
BGP4MP|03/14/19 05:09:34|A|206.126.225.20|6939|180.190.56.0/22|6939 40633 40633 40633 4775 132199|IGP
```

3. Operaciones específicas para completar el análisis deseado con la herramienta/lenguaje que desee (python, bash, mysql, etc.)

PCH Raw Routing Data, https://www.pch.net/resources/Raw_Routing_Data/

Bgpreader tool, <https://bgpstream.caida.org/docs/tools/bgpreader>

Bgpdump tool, <https://bitbucket.org/ripenc/bgpdump/wiki/Home>

RFC6396 Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format, <https://tools.ietf.org/html/rfc6396>