



LACNIC's RDAP Service

GTER 41 - Uberlândia
May 2016

Agustín Formoso

@aguformoso | agustin@lacnic.net

The RDAP Protocol

- “The new whois”
- Drafts started in early 2012
 - WEIRDS WG
- IETF standard since March 2015
 - RFCs 7480-7485
- Usage of HTTP response codes
 - 200, 4XX, 3XX
- Standardized formats
 - Query
 - RESTful interface
 - Response
 - JSON format

The RDAP Protocol: RESTful Interface

Lookup

Object	URL
IP	<code>/ip/<ip_adress></code>
Entity (users & orgs)	<code>/entity/<entity_handle></code>
AS	<code>/autnum/<as_number></code>
Nameserver	<code>/nameserver/<nameserver></code>
Domain	<code>/domain/<domain></code>

Searches

Object	URL
Entities	<code>/entities/<ip_adress></code>
Nameservers	<code>/entity/<entity_handle></code>
Domains	<code>/autnum/<as_number></code>

RDAP deployment

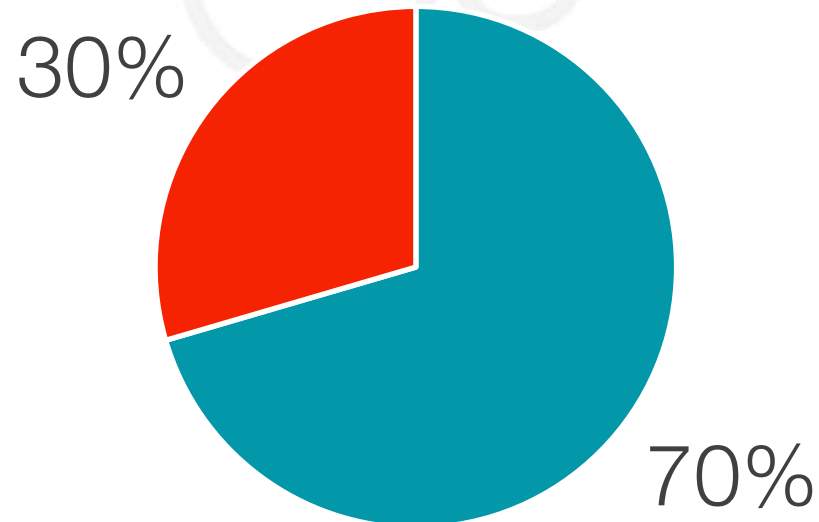
- RIRs
 - All five RIRs
- The LAC region
 - NIC BR
 - Any others?

LACNIC's RDAP service

- Out of beta since December 2014
- Based on RIPE NCC RDAP
- Rising traffic 😊

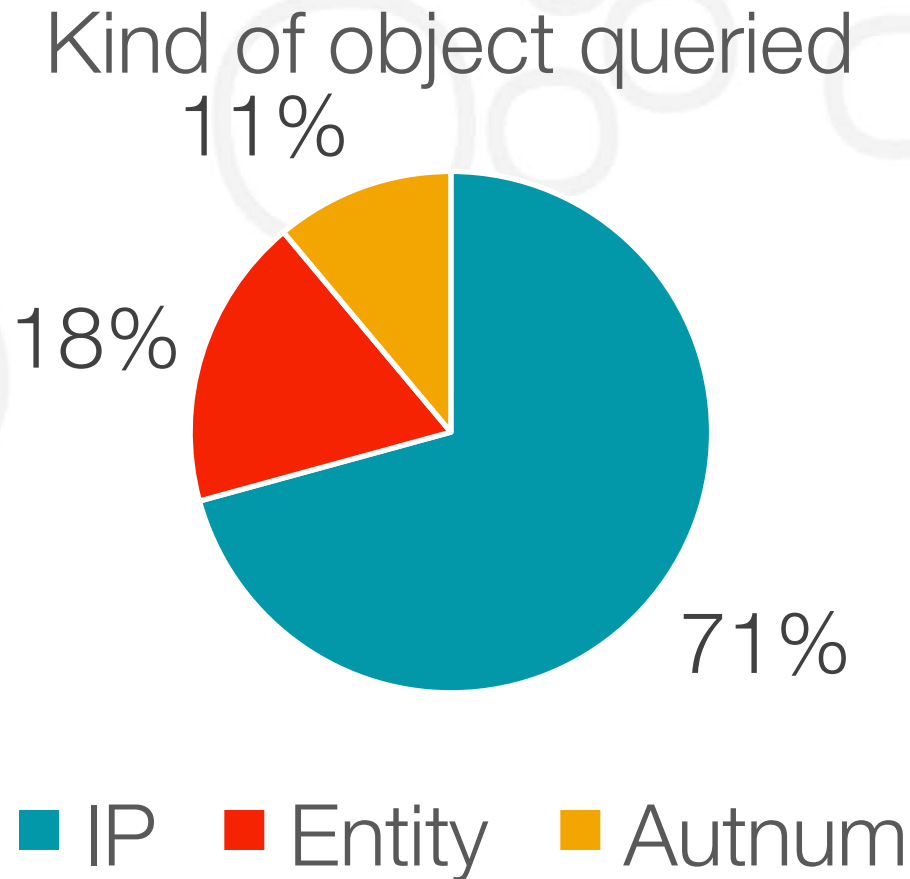
LACNIC's RDAP service

IP version traffic seen



■ v4 ■ v6

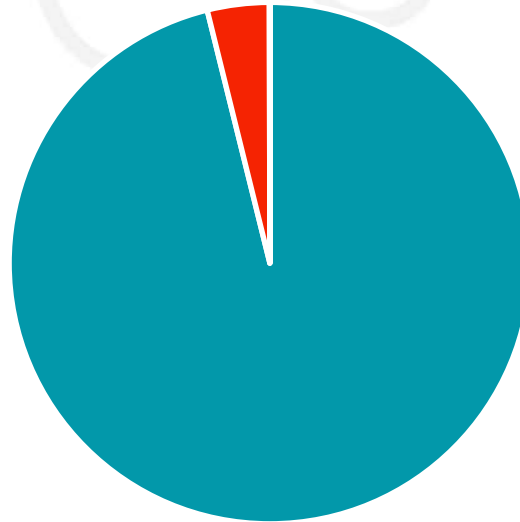
LACNIC's RDAP service



**Very little
search!**

LACNIC's RDAP service

Kind of HTTP method seen
4%



POST...?
(780 queries so far)

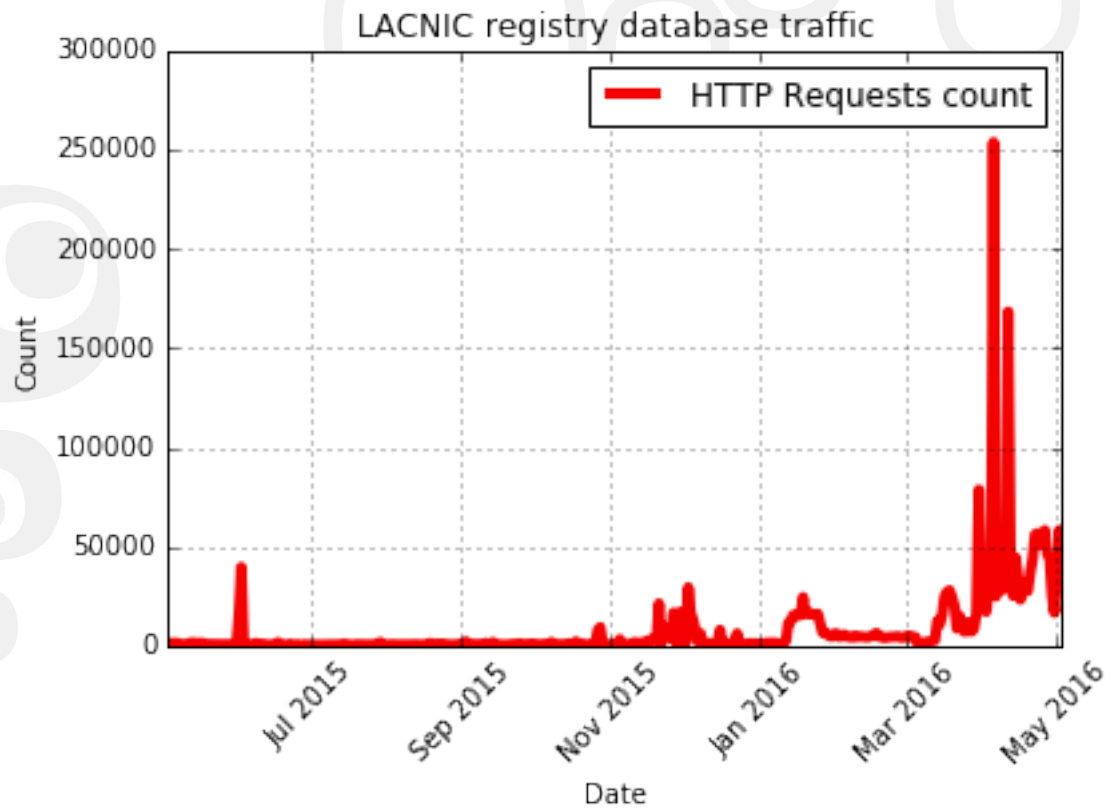
■ GET ■ HEAD ■ POST ■ OPTIONS

LACNIC's RDAP service

- Last 12 months:
 - 13 M queries
- Last April
 - 1.4 M queries
 - Daily avg.: 46 K queries
 - Some *suspicious* traffic spikes

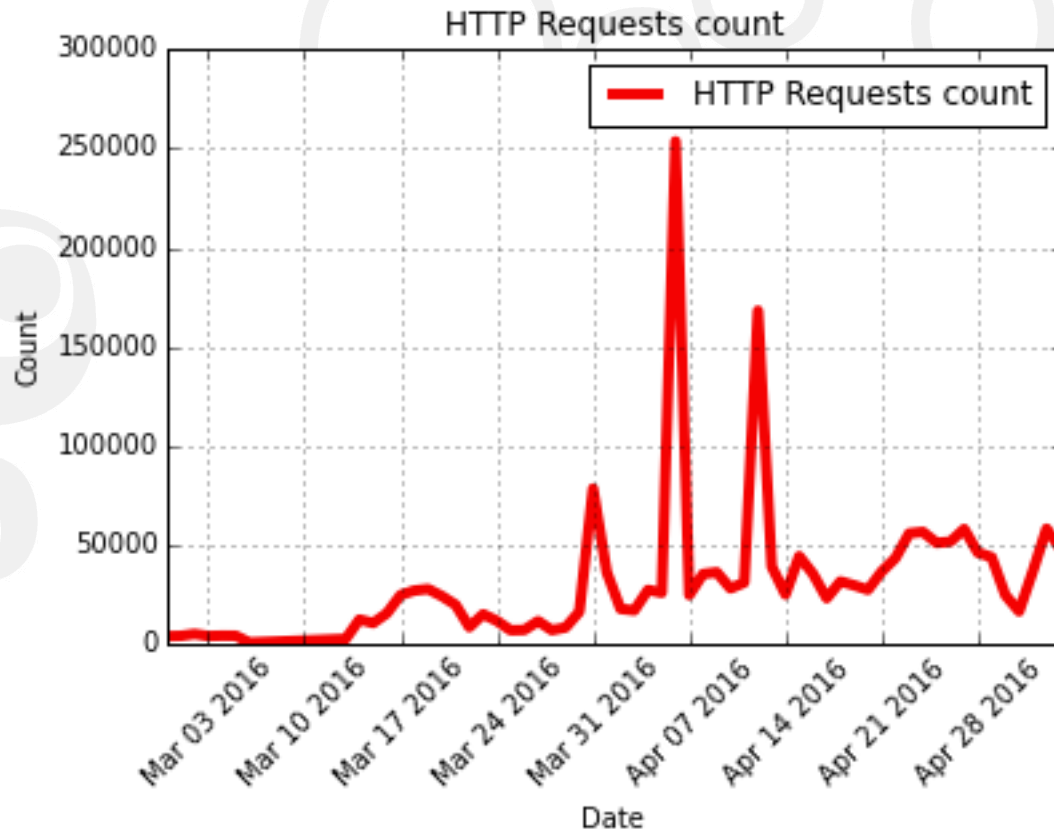
LACNIC's RDAP service

- Last 12 months



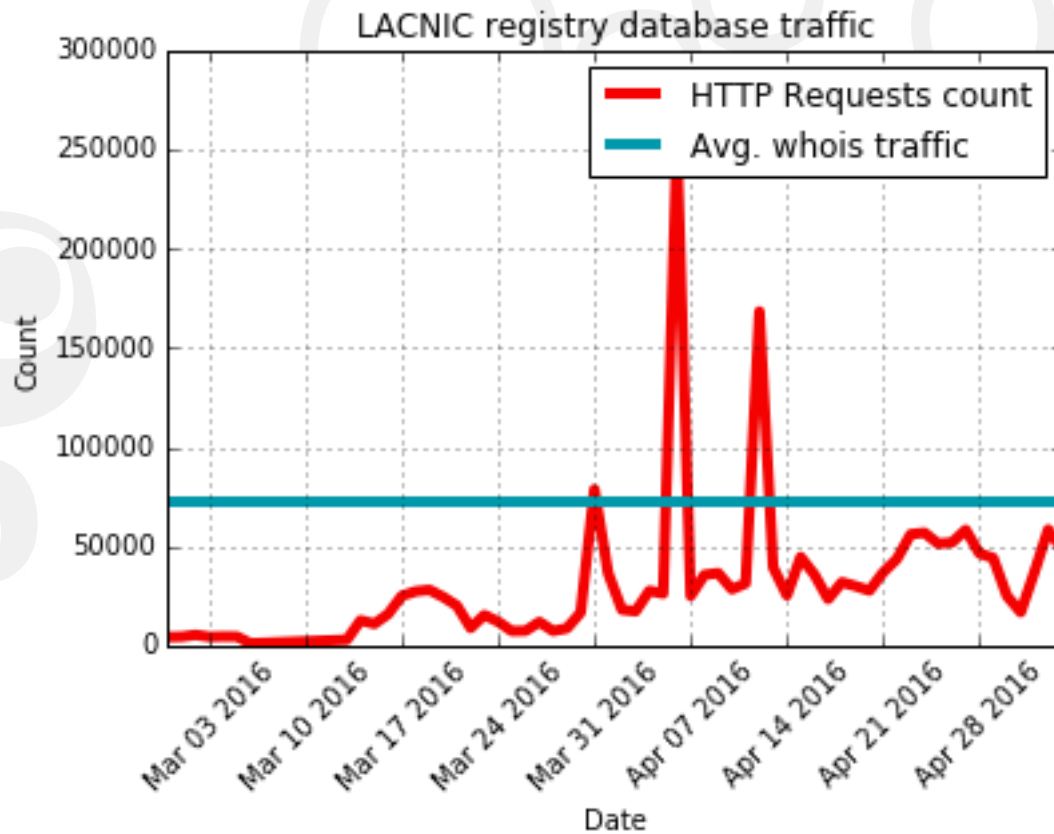
LACNIC's RDAP service

- Last 2 months



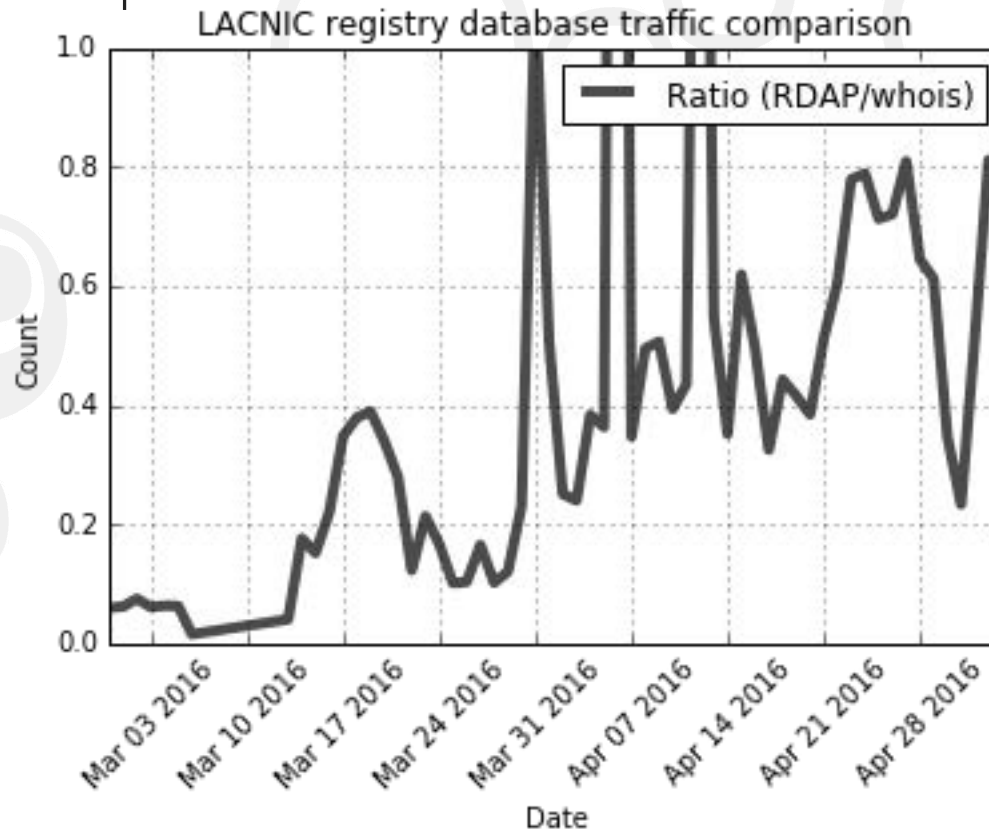
LACNIC's RDAP service

- Last 2 months



LACNIC's RDAP service

- Traffic comparison...not bad!



API Keys

**1,2% of LACNIC's
RDAP traffic uses
the API Keys
system**

- Additional query parameter
- Uses [LACNIC API Key](#) services
- API Key tokens used for rate limiting only
- Defaults to 2 rate limits: 10 per minute and 1000 per hour, whichever is violated first
- IP-based rate limits
- [Formal procedure](#) for requesting a new API Key (similar to bulk whois)

<https://apikey.lacnic.net>

<http://www.lacnic.net/documents/10834/1535064/solicitud-rdap-beta-es.pdf>

Temporary Cache

- Additional query parameter
- URL-based
- 24-hour object cache
- `cache=false` bypasses cache, hits the database, and refreshes the cache
- Cache notification is added to the `notices` attribute

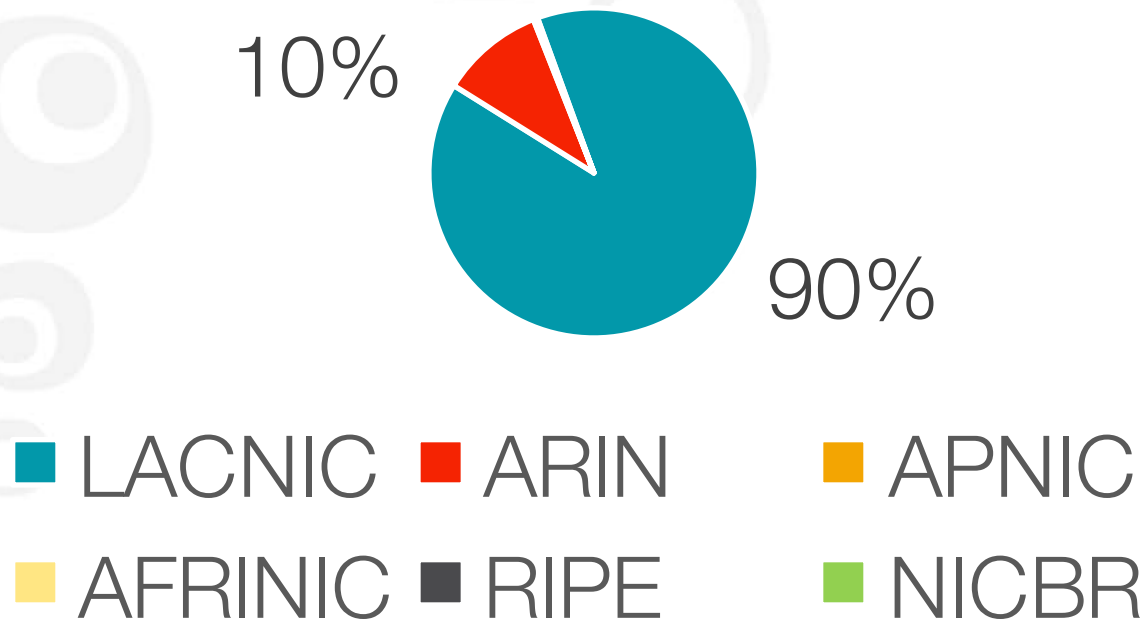
RDAP Bootstrap

- ARIN's bootstrap ([GitHub](#))
 - Out of the box Java application
 - Code collaboration from LACNIC
- HTTP redirects are based on
 - IANA json files
 - Other RIRs'
 - Custom LACNIC json files
 - Regional NICs (NIC.br)

https://github.com/arineng/rdap_bootstrap_server

RDAP Bootstrap

Authoritative RDAP server for IPv4 objects



Use case

- Analyzing our own logs file

IP address	Requests ▼	%	Organization	RDAP
193.252.242.15	2.7M	100	Gestion des Adresse IP France Telecom	RIPE
2001:19f0:7000:a0f9:5400:ff:fe1e:5b39	1.5M	55.5	Vultr Holdings, LLC	ARIN
200.7.84.2	530K	19.1	LACNIC - Latin American and Caribbean IP address	LACNIC
204.193.144.4	400K	14.7	Quality Tech	
2001:12ff:0:3::99	350K	12.6	Núcleo de Inf. e Coord. do Ponto BR - NIC.BR	NIC.BR
200.3.14.132	300K	10.7	LACNIC - Latin American and Caribbean IP address	LACNIC

RDAP Web

RDAP - WEB	
ENTITY : UY-LACN-LACNIC	
Source: https://rdap.lacnic.net/bootstrap/entity/UY-LACN-LACNIC	
ENTITY	
Handle	UY-LACN-LACNIC
Name	LACNIC - Latin American and Caribbean IP address
Country	UY
Roles	[REGISTRANT]
Address	Rambla República de México 6125
City	Montevideo
Postal Code	11400
E-mail	No data
Telephone	598 2 6042222
LAST_CHANGED	2015-08-04T17:07:24.000
Operator	LACNIC Hostmaster
Inetnums	➔
CONTACTS	
[ADMINISTRATIVE]	
Handle	AIL
Name	Carlos M. Martínez
Address	Rambla Rep. Mexico 6125
City	Montevideo
Country	UY
Postal Code	11400
E-mail	ipadmin@LACNIC.NET
Telephone	598 2 6042222
Registration	No data
Last Changed	No data
[REGISTRANT]	
Handle	LAH

RDAP Web

The screenshot shows the LACNIC website in a web browser. The browser's address bar displays 'lacnic.net'. The website features the LACNIC logo, a navigation bar with links for 'sugerencias / suggestions', 'português', 'english', and 'español', and a large blue banner for the 'CFE BANCO DE DESARROLLO DE AMÉRICA LATINA' and 'lacnic'. A yellow sticky note with the text 'WHOIS textbox at the LACNIC home page' is placed over the main content area, with an arrow pointing to the 'WHOIS' search box. The search box contains the IP address '200.7.84.80'. Below the search box is a button labeled 'Solicita tu bloque IP'. To the right, there is a section for IPv4 addresses, showing 'Direcciones IPv4 disponibles' as '1451264' and '/8s' as '0.087'. The date 'Fecha de agotamiento: 10 de Junio de 2014' is also displayed. The footer includes the text 'Contáctenos. Contate-nos. Contact us!' and a plus sign icon.

lacnic

200.7.84.80

Solicita tu bloque IP

Direcciones IPv4 disponibles 1451264

/8s 0.087

Fecha de agotamiento: 10 de Junio de 2014

Contáctenos. Contate-nos. Contact us! +

[RDAP](https://rdap.lacnic.net/rdap) https://rdap.lacnic.net/rdap

[RDAP Bootstrap](https://rdap.lacnic.net/bootstrap) https://rdap.lacnic.net/bootstrap

[RDAP Web](https://rdap.lacnic.net/rdap-web/) https://rdap.lacnic.net/rdap-web/

[RDAP NIC.BR](https://rdap.registro.br/) https://rdap.registro.br/

[RFCs \(IETF Tools\)](https://tools.ietf.org/wg/weirds/) https://tools.ietf.org/wg/weirds/

THANKS!