“La mala práctica del uso de localhost en dominios”

Hugo Salgado, .CL

Foro Técnico LACNIC 35, Online.

nic chile
SOMOS EL PUNTO CL

¿Qué es “localhost”?

- Se trata de incluir en una zona pública un registro de nombre “localhost” con tipo A y dirección IP de *loopback*:

```
$ cat example.com.zone
[ … ]

localhost.example.com.    IN     A     127.0.0.1
```

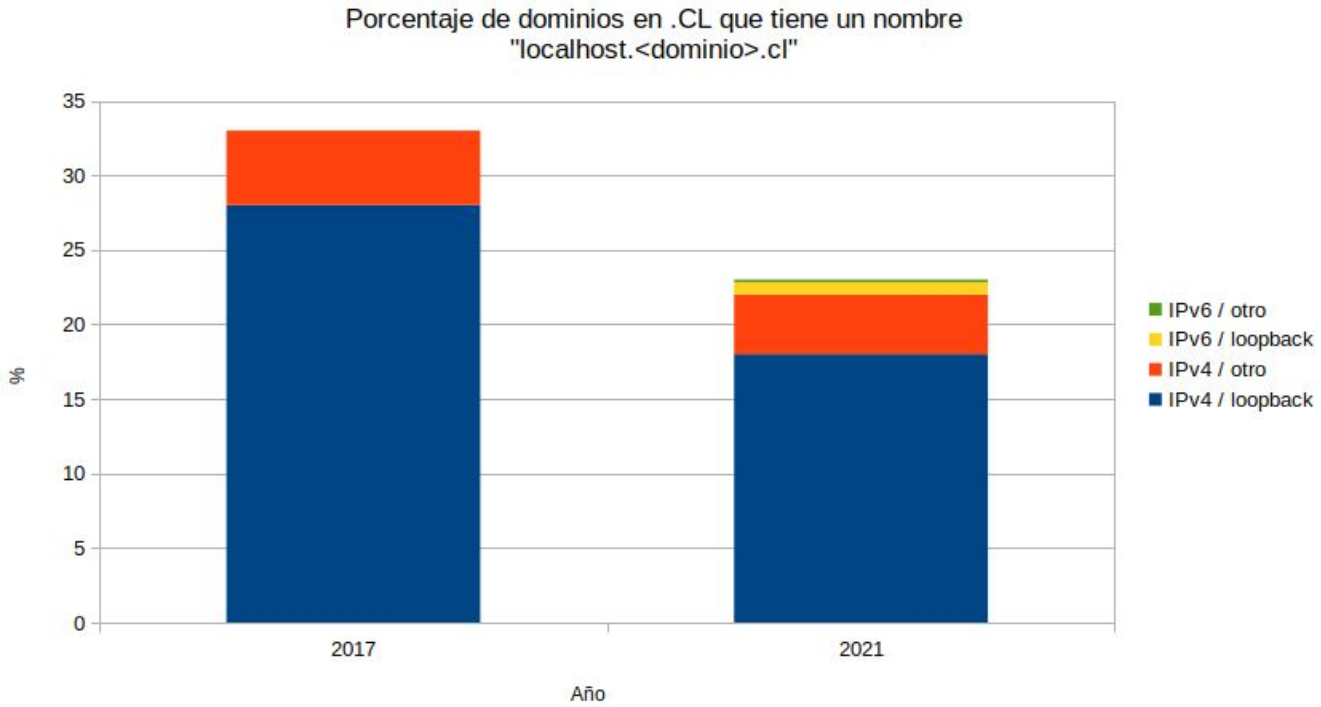
Fue una “buena práctica”...

- En el año 1993 (RFC1537) se instauró como buena práctica el incluir registros “localhost” en todas las zonas.
- Se puso por defecto en algunos softwares DNS, en templates y ejemplos.
- El intento era evitar que al usar “*search list*” con nombres locales, estos fueran respondidos con NXDOMAIN, o direcciones IPs públicas.

… por tres años.

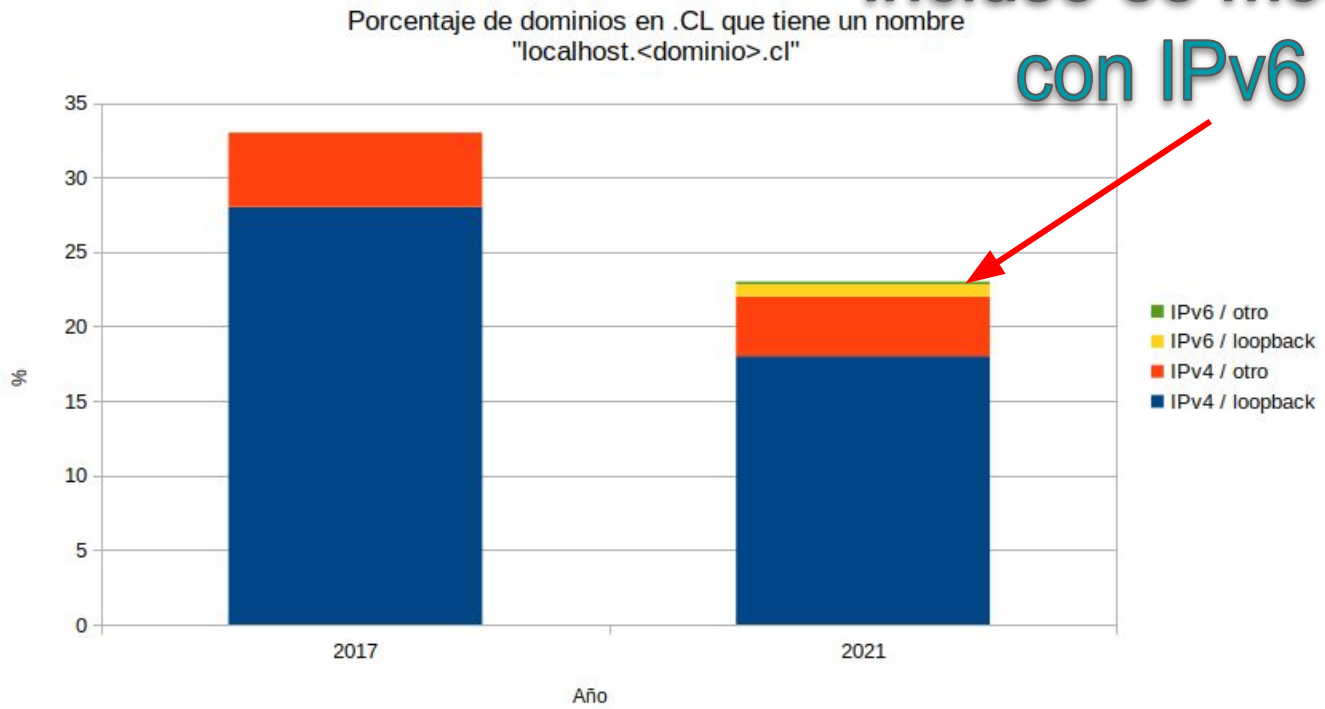
- Rápidamente se vieron los problemas. Tres años después, en el RFC1912, se recomienda DEJAR DE HACERLO.
- El problema es que lo que está en Internet… se queda para siempre en Internet :(
  - por “costumbre”
  - zonas arrastradas desde siempre
  - “templates” o ejemplos históricos

Veintiséis años después...



Veintiséis años después...

Incluso se moderniza con IPv6 ! :(



¿Por qué es mala idea hoy? Usabilidad

- El mismo “search list” es problemático
  - No hay una forma única de hacerlo
    - consistencia en la experiencia de usuario

¿Por qué es mala idea hoy? Usabilidad

- El mismo “search list” es problemático
  - No
    -

System	Absolute *server.*	Relative Single Label *server*	Relative Multi-Label *www.server*
MAC OSX 10.9	never	always	never
Windows XP	never	always	post
Windows Vista	never	always	never
Windows 7	never	always	never
Windows 8	never	always	never
FreeBSD 9.1	never	pre	post
Ubuntu 13.04	never	pre	post

Table 1 – Application of Search Lists in Name Resolution for various Operating Systems

Estudio “Dotless”, Geoff Huston, octubre 2013. Aparecido en “The ISP Column”.

¿Por c…bilidad

- El misn…
  - N…
    - …

MacOS OSX 10.9

Browser\Query	Absolute *server.*	Relative Single Label *server*	Relative Multi-Label *name.server*
Chrome (31.0.1650.39 beta)	never	always	pre
Opera (12.16)	never	always	never
Firefox (25.0)	post*	always	post*
Safari (7.0 9537.71)	none**	none**	none**

* Firefox looked up the base name, then added prefix of "www.", then tried prefixing the "www." and also appending the search list. If the base name starts with "www." it will look up the base name, then lookup the base name with the search list appended

** Safari seems to be aware of TLDs and does not perform DNS lookups when the name is not a known delegated TLD, irrespective of the local search list. Safari is also aware of SLD-restricted TLDs and will not perform queries when the SLD is restricted, unless the SLD matches the restricted list. In known TLDs Safari will query <name>.tld and then www.<name.tld>, unless the query name already starts with "www."

Windows 8.1

Browser\Query	Absolute *server.*	Relative Single Label *server*	Relative Multi-Label *name.server*
Chrome (30.0.1599.101 m)	never	always	never
Opera (17.0)	none	none	none*
Firefox (25.0)	never**	always	never**
Safari (5.1.7 7534.57.2)	never***	always****	never***
Explorer (11.0.900.16384)	never	none	never

* Opera is aware of delegated tlds, and only queries the DNS when the last label is a known TLD. In that case it does not use the local search list

Estudio "Dotless", Geoff Huston, octubre 2013. Aparecido en "The ISP Column".

¿Por qué es mala idea hoy? Usabilidad

- El mismo “search list” es problemático
  - No hay una forma única de hacerlo
    - consistencia en la experiencia de usuario)

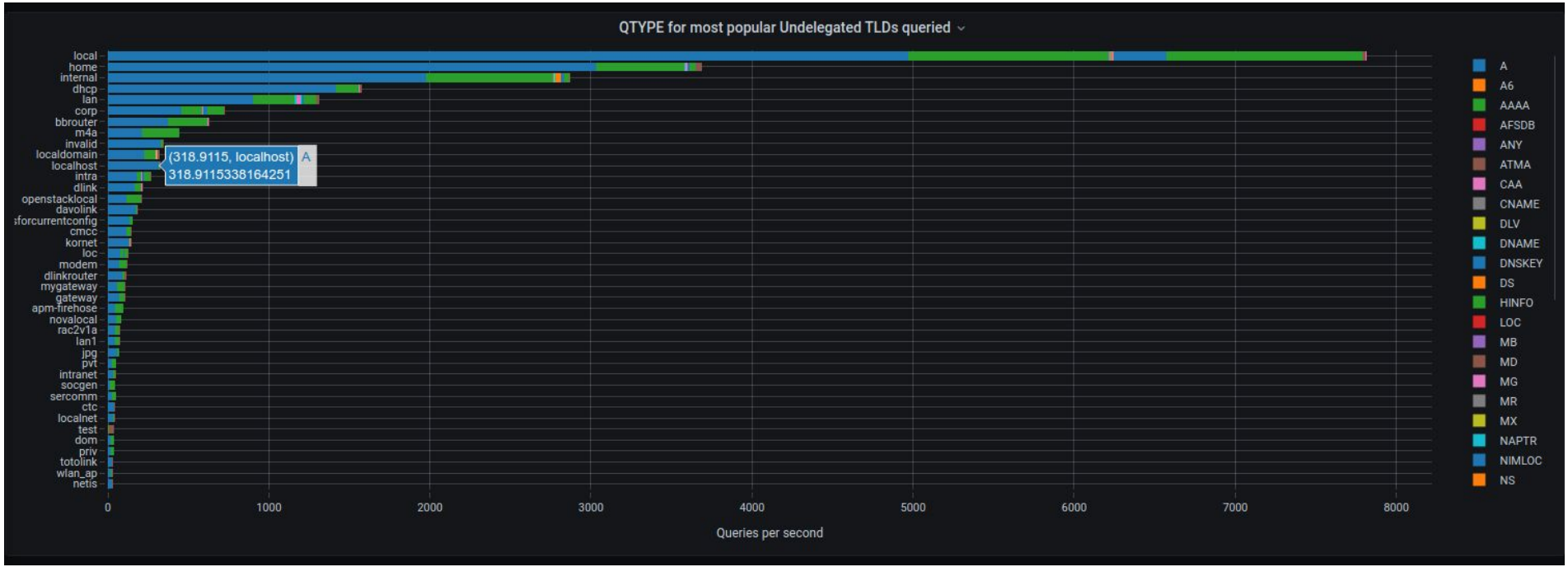
- Es mejor hacerlo “lo más cercano al usuario” posible
  - interfaces, front-end
  - a la altura de “aplicaciones a OS” y sobre todo “OS a resolver”, deben ser “*fully qualified domains*”.

¿Por qué es mala idea hoy? Localidad

- Las direcciones “localhost” deben ser… bueno… ¡**locales**! No tienen sentido en la internet pública.
- El soporte correcto a localhost ya viene en el software DNS:
  - stub debe responder con loopback
  - full resolvers deben responder NXDOMAIN

“Let 'localhost' be localhost.” IETF draft, M. West, December 18, 2017

¿Por qué es mala idea hoy? Localidad



Estadísticas root server L (stats.dns.icann.org)

¿Por qué es mala idea hoy? Seguridad

- Por último, hay/hubo riesgos de seguridad
  - ambientes multiusuario
  - envío de cookies por dominio
- (Y de paso, es muy buena idea revisar sus zonas y eliminar cualquier registro CNAME/A/AAAA que no esté en uso)

```
$ cat example.com.zone
[ … ]
api.staging.example.com.  IN  CNAME …s3-website-us-west-2.amazonaws.com.
```

¡Elimine los nombres “localhost” (superfluos) de sus zonas!

¡Gracias!

Hugo Salgado, hsalgado@nic.cl

Grupo DNS de LACNOG
https://www.lacnog.org

nic chile
SOMOS EL PUNTO CL