



Tópicos sobre DNS e o seu provedor na ICANN.



Daniel Fink daniel.fink@icann.org

IX Fórum Regional – SJRP SP
Setembro 2019

O que é a ICANN?

Corporação
da Internet
para Designação
de Nomes

Missão da ICANN

A missão da Corporação da Internet para Designação de Nomes e Números (ICANN) é garantir a operação estável e segura dos sistemas de identificadores exclusivos da Internet.

Especificamente, a ICANN:

- 1  Coordena atribuições na **zona-raiz** do DNS
- 2  Coordena políticas para nomes de domínio de **segundo nível** em gTLDs
- 3  Facilita a coordenação da operação e evolução dos servidores raiz do DNS
- 4  Coordena a distribuição de blocos IP e números de AS
- 5  Colabora com outras entidades para prover registros necessários para o funcionamento da Internet de acordo com especificações.

Estrutura da ICANN



O grupo dos provedores na ICANN

ICANN | ISPCP

Internet Service Providers & Connectivity Providers

Representa o setor de conectividade, contribui nas diversas discussões técnicas e macropolíticas:

- Impacto do lançamento de novos nomes de domínio genéricos
- Universal Acceptance
- SSR de DNS

Se você é um provedor de Internet, participe da ISPCP na ICANN. Não há custos, simplesmente cadastre-se e receberá todas as novidades e oportunidades para participar nas atividades do grupo. Ademais, você poderá antecipar-se às oportunidades de negócios quando surgirem.

Visite: <http://www.ispcp.info>

O que é DNSSEC?



- DNSSEC = “**DNS Security Extensions**”
- É um protocolo que está sendo implantado atualmente para proteger o Sistema de Nomes de Domínio (DNS).
- O DNSSEC adiciona segurança ao DNS ao incorporar criptografia de chave pública na hierarquia do DNS, resultando em uma PKI (Public Key Infrastructure, infraestrutura de chave pública) única e aberta para nomes de domínio.
- Resultado de mais de uma década de desenvolvimento de padrões abertos

THE ORIGINS OF DNSSEC

5000 BC



This is Ugwina. She lives in a cave on the edge of the Grand Canyon...



This is Og. He lives in a cave on the other side of the Grand Canyon...



It's a long way down and a long way round. Ugwina and Og don't get to talk much...



On one of their rare visits, they notice the smoke coming from Og's fire



...and soon they are chatting regularly using smoke signals



until one day, mischievous caveman Kaminsky moves in next door to Ug and starts sending smoke signals too...

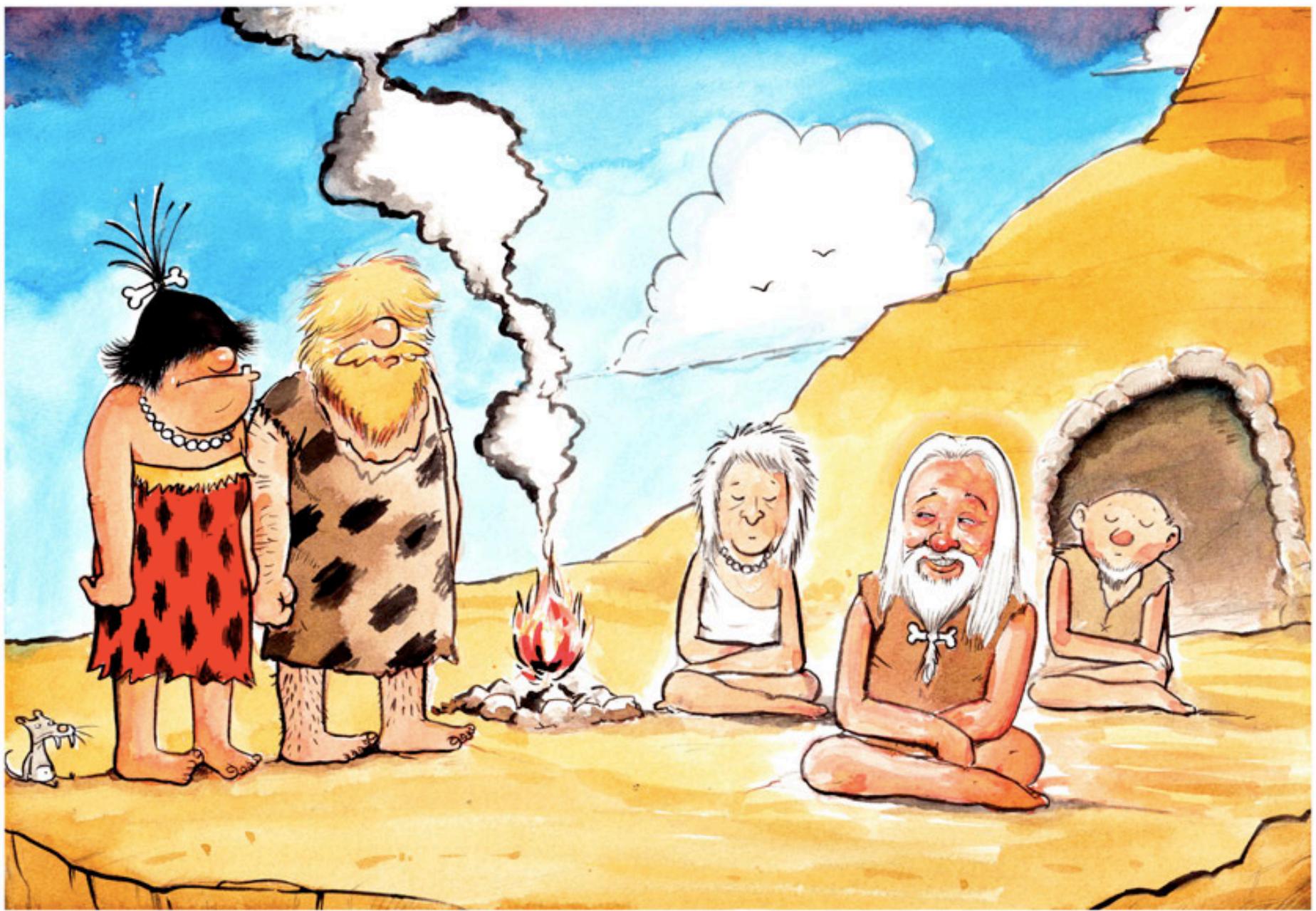
nominet



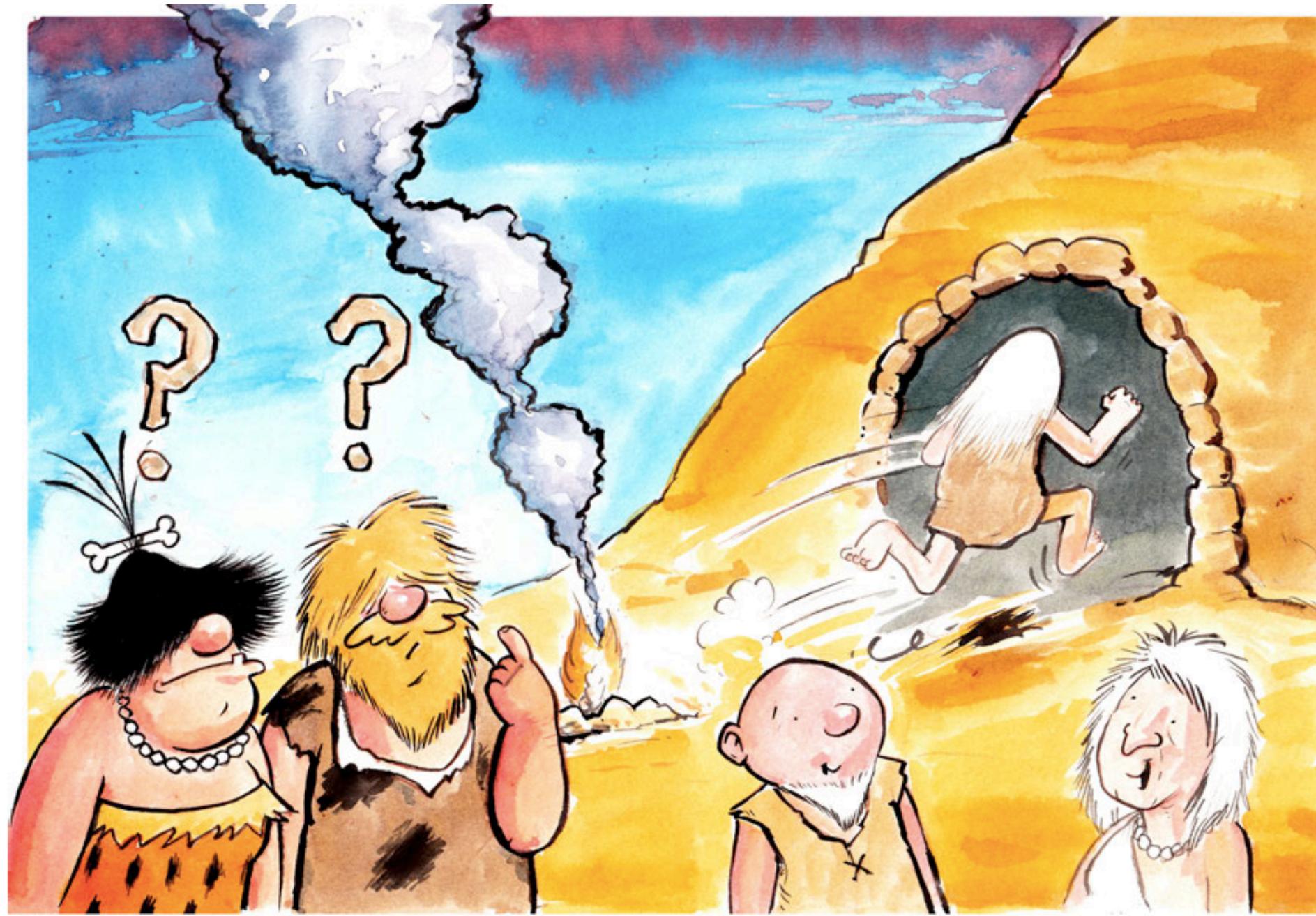
Now Ugwina is really confused. She doesn't know which smoke to believe...



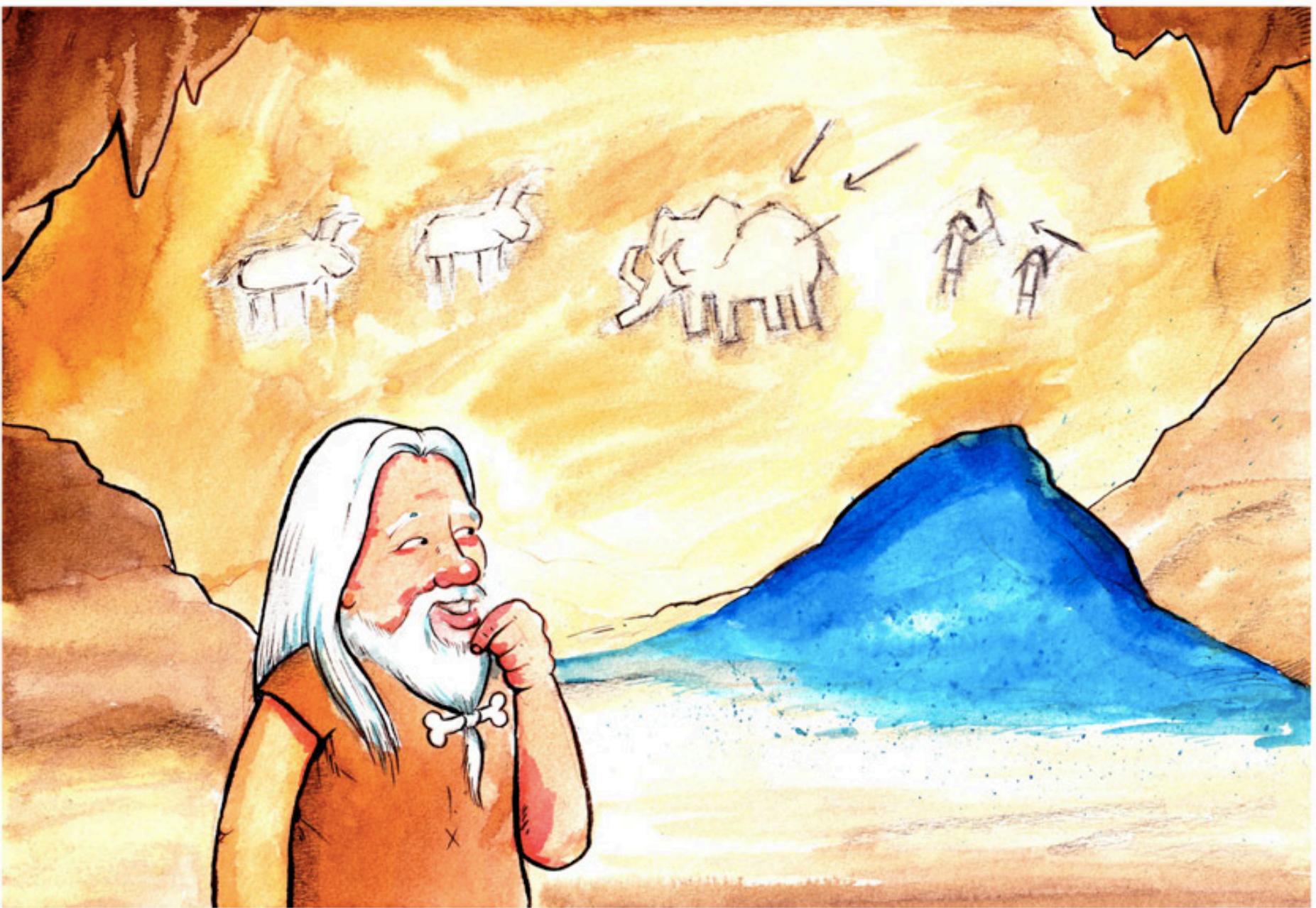
So Ugwina sets off down the canyon to try and sort out the mess...



Ugwina and Og consult the wise village elders. Caveman Diffie thinks that he might have a cunning idea...



And in a flash, jumps up and runs into Ug's cave...!



Right at the back, he finds a pile of strangely coloured sand
that has only ever been found in Ug's cave...



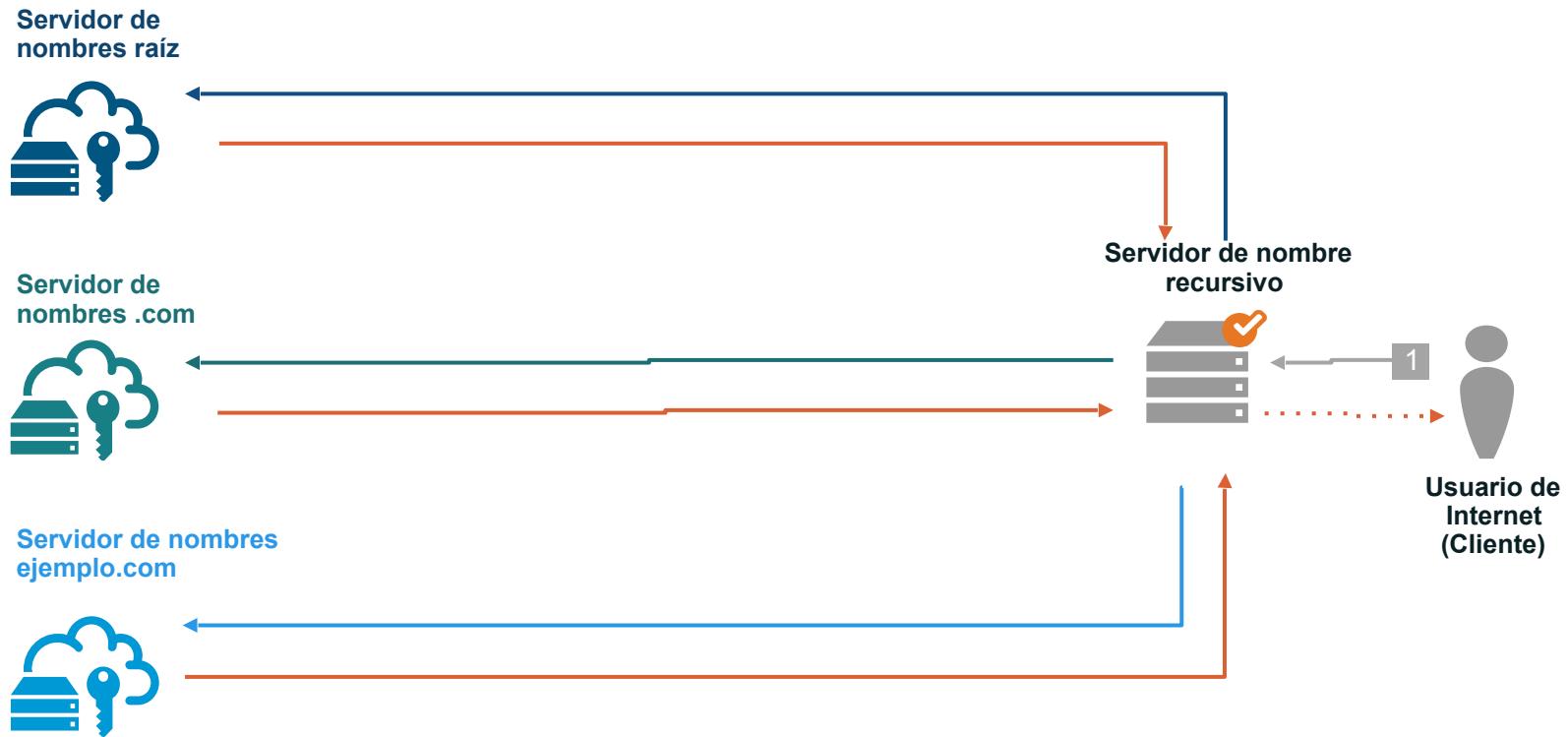
And with a skip, he rushes out and throws some of the sand onto the fire. The smoke turns a magnificent blue...



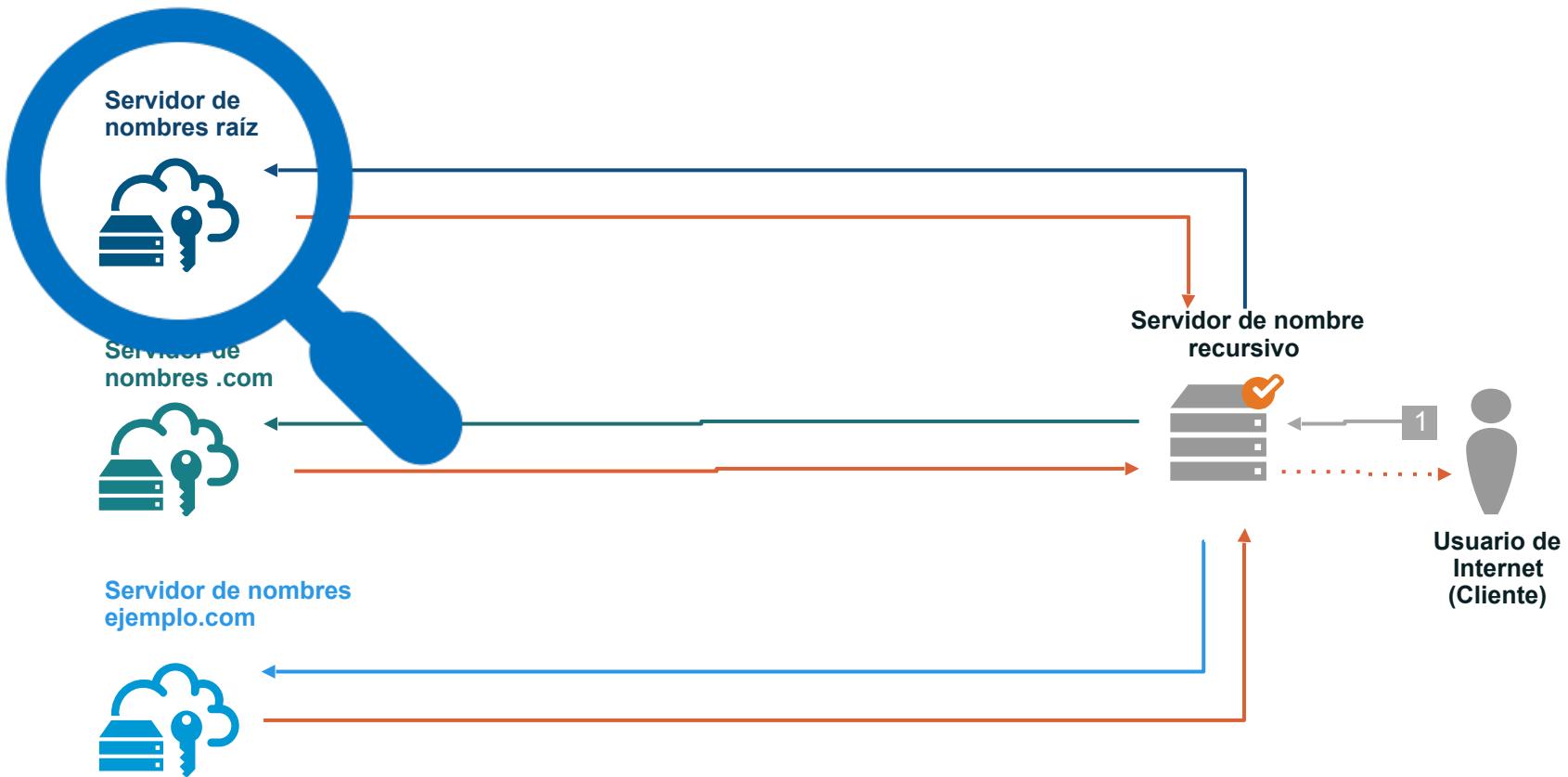
Now Ugwina and Og can chat happily again, safe in the knowledge that nobody can interfere with their conversation...

Hyperlocal Alternativa ao IMRS

Resolução de nomes

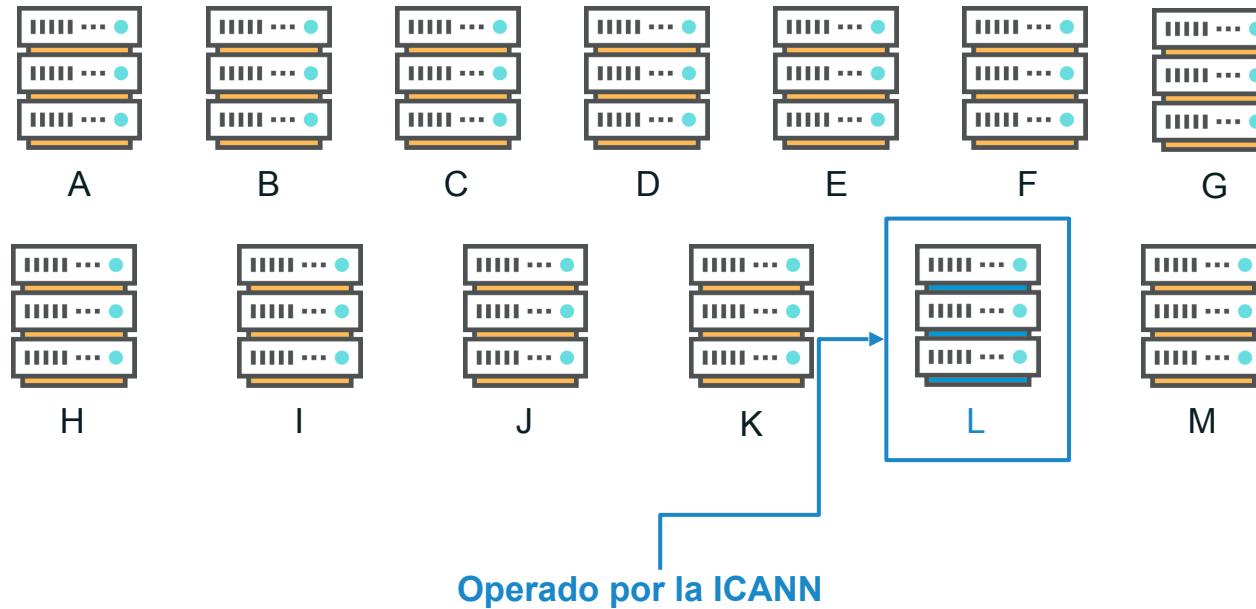


Resolução de nomes



Servidores raíz

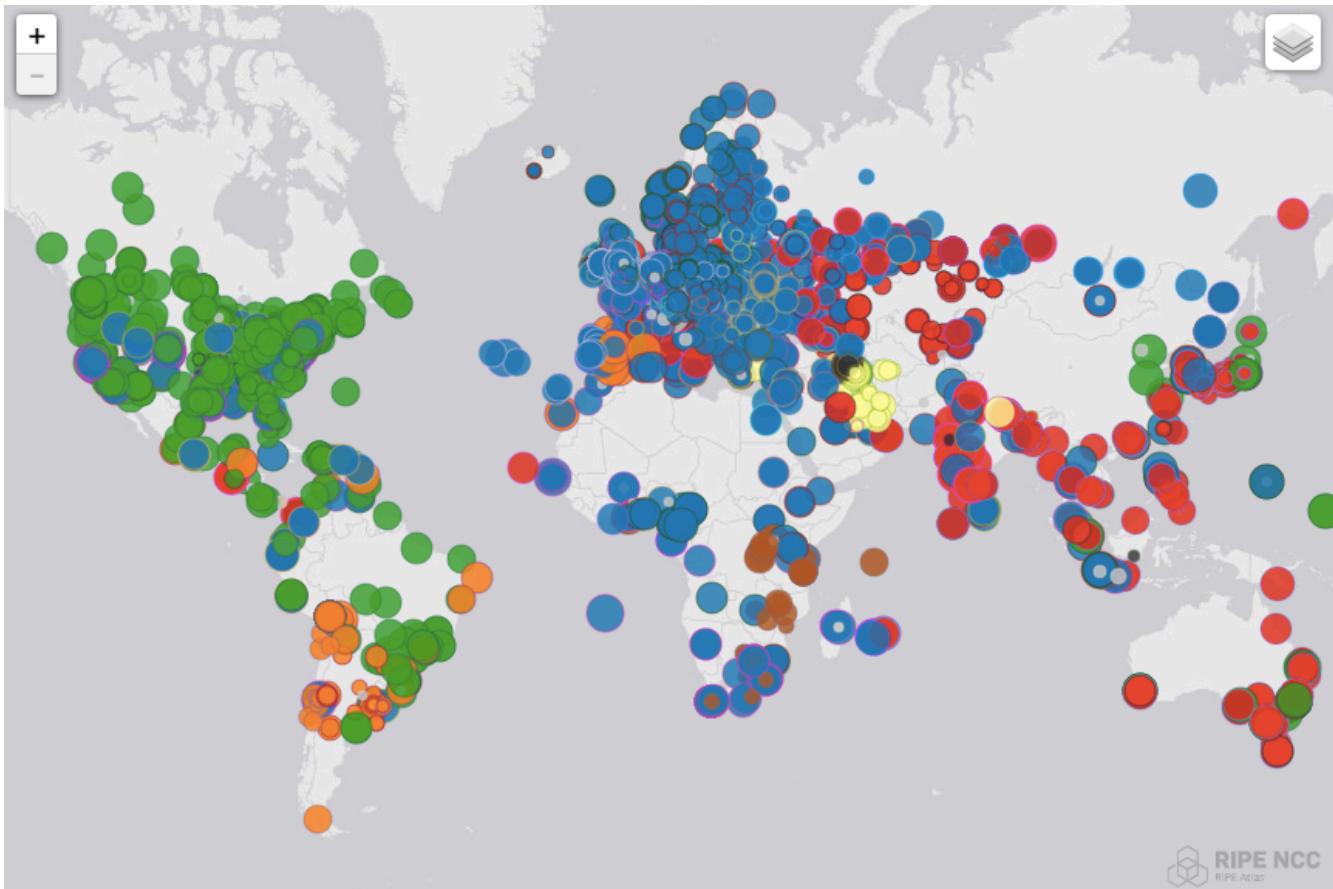
Los servidores raíz se identifican desde la A hasta la M



La Raíz L es uno de los 13 servidores raíz
operados independientemente; todos sirven a la
misma zona raíz del DNS.

Cópias de servidor raíz

Anycast instances of authoritative name servers serving the root zone at almost **1,000** locations spread around the globe.



<https://atlas.ripe.net/results/maps/root-instances/>

O que é Hyperlocal?

Adiciona resiliência ao recursivo

- Provedor mantém uma cópia local da zona raiz.
- RFC7706

[\[Docs\]](#) [\[txt|pdf\]](#) [\[draft-ietf-dnsop-00\]](#) [\[Tracker\]](#) [\[Diff1\]](#) [\[Diff2\]](#) [\[IPR\]](#) [\[Errata\]](#)

INFORMATIONAL

Errata Exist

W. Kumari

Google

P. Hoffman

ICANN

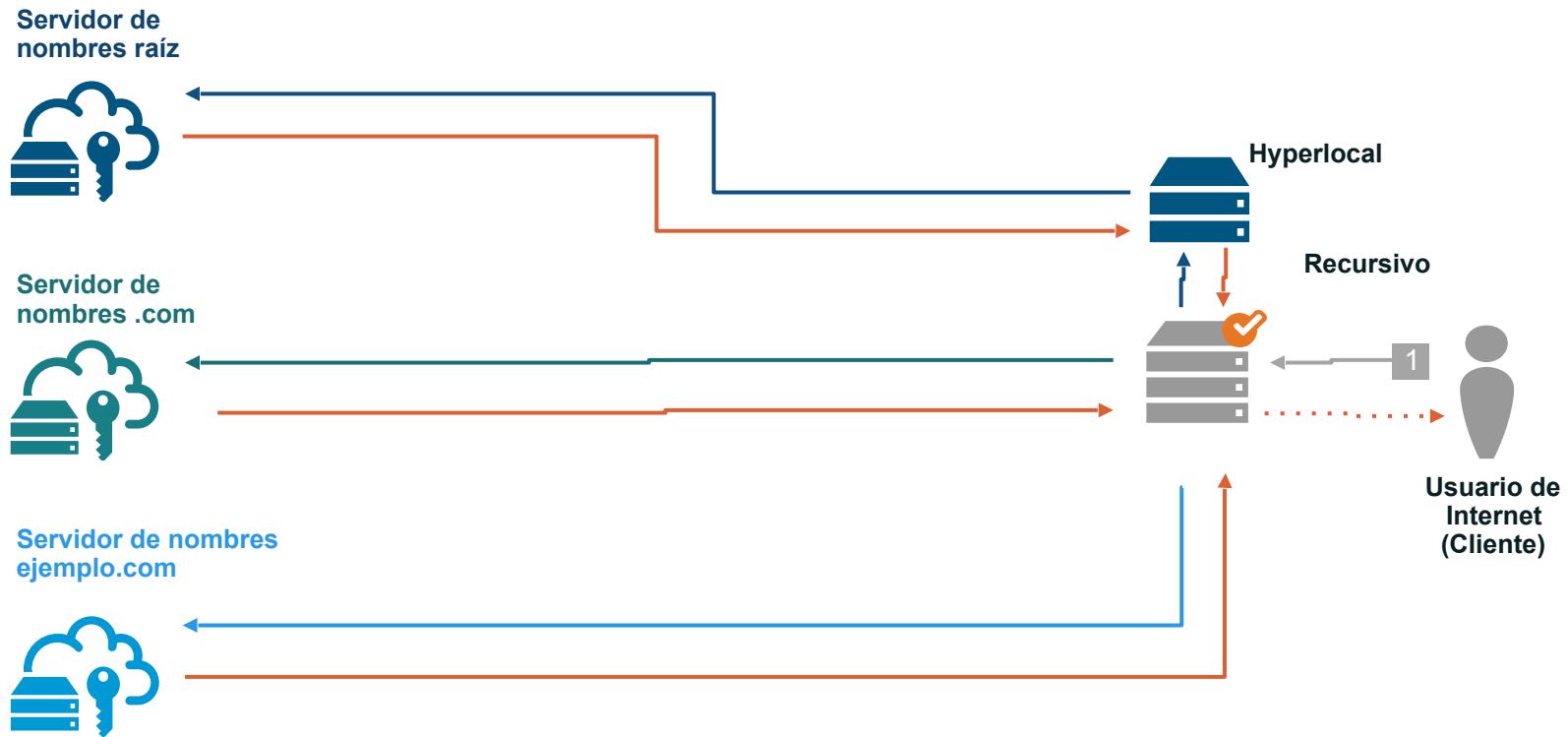
November 2015

Decreasing Access Time to Root Servers by Running One on Loopback

Abstract

Some DNS recursive resolvers have longer-than-desired round-trip times to the closest DNS root server. Some DNS recursive resolver operators want to prevent snooping of requests sent to DNS root servers by third parties. Such resolvers can greatly decrease the round-trip time and prevent observation of requests by running a copy of the full root zone on a loopback address (such as 127.0.0.1). This document shows how to start and maintain such a copy of the root zone that does not pose a threat to other users of the DNS, at the cost of adding some operational fragility for the operator.

Resolução de nomes com Hyperlocal



Benefícios

- Respostas de DNS mais rápidas
 - Respostas negativas imediatas
 - Consultas mais resistentes a snooping
 - Alternativa de baixo custo em relação ao IMRS
 - Contribui para uma operação mais segura, estável e resiliente.
-

Teste do Hyperlocal na RLINE Telecom, Planalto-PR



Rosauro Baretta



Fabio Ortlieb

Maquina virtualizada VMware

4 x Intel(R) Xeon(R) CPU E5-2620 v2 @ 2.10GHz

8G Memoria

Disco 16G SSD

Não ocupada nada de recursos, foi instalado em uma maquina com CentOS7, Bind na versão 9.

Teste do Hyperlocal na RLINE Telecom, Planalto-PR

- 1 - recursivo da google (8.8.8.8) para dominio uol.com.br

```
[root@master ~]# dig @8.8.8.8 uol.com.br
; <>> DiG 9.9.4-RedHat-9.9.4-72.el7 <>> @8.8.8.8 uol.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22386
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;uol.com.br.          IN      A
;; ANSWER SECTION:
uol.com.br.          47      IN      A      200.147.35.149
;; Query time: 27 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Qui Jun 06 12:53:12 -03 2019
;; MSG SIZE  rcvd: 55
```

Teste do Hyperlocal na RLINE Telecom, Planalto-PR

- 1 - recursivo da google (8.8.8.8) para um dominio invalido

Teste do Hyperlocal na RLINE Telecom, Planalto-PR

2 - recursivo hyperlocal para o dominio uol.com.br

```
[root@master ~]# dig @[REDACTED].4 uol.com.br
; <>> DIG 9.9.4-RedHat-9.9.4-72.el7 <>> @[REDACTED].4 uol.com.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65160
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uol.com.br.                      IN      A
;; ANSWER SECTION:
uol.com.br.                      27      IN      A      200.147.3.157
;; Query time: 0 msec
;; SERVER: [REDACTED].4#53([REDACTED].4)
;; WHEN: Qui Jun 06 12:55:40 -03 2019
;; MSG SIZE  rcvd: 55
```

Teste do Hyperlocal na RLINE Telecom, Planalto-PR

2 - recursivo hyperlocal para um dominio invalido

box.	172800	IN	NS	a.nic.box.
box.	172800	IN	NS	b.nic.box.
box.	172800	IN	NS	c.nic.box.
box.	172800	IN	NS	d.nic.box.
box.	86400	IN	DS	32737 8 1 A637BE5E3CC2E079DFF2BD5BEFF84DB3CFB2E801
box.	86400	IN	DS	32737 8 2 2ABFC49F5DCD5655E7B32C6DCE32C11C8043AF5D31CD3C580B311D69 BFB161B9
br.	172800	IN	NS	a.dns.br.
br.	172800	IN	NS	b.dns.br.
br.	172800	IN	NS	c.dns.br.
br.	172800	IN	NS	d.dns.br.
br.	172800	IN	NS	e.dns.br.
br.	172800	IN	NS	f.dns.br.
br.	86400	IN	DS	45673 5 2 14369AD309CC59FD59C1A422BA93B71F2C522BF3672C2E067B2C53F5 3AE522DF
bradesco.	172800	IN	NS	dns1.nic.bradesco.
bradesco.	172800	IN	NS	dns2.nic.bradesco.
bradesco.	172800	IN	NS	dns3.nic.bradesco.
bradesco.	172800	IN	NS	dns4.nic.bradesco.
bradesco.	172800	IN	NS	dnsa.nic.bradesco.
bradesco.	172800	IN	NS	dnsb.nic.bradesco.
bradesco.	172800	IN	NS	dnsc.nic.bradesco.
bradesco.	172800	IN	NS	dnsd.nic.bradesco.
bradesco.	86400	IN	DS	44254 8 2 49F78D30A829D5D40A7671F9831DF0F056FC7F4E8E39906C905AFB8E B1B54100
bridgestone.	172800	IN	NS	a.gmoregistry.net.
bridgestone.	172800	IN	NS	b.gmoregistry.net.
bridgestone.	172800	IN	NS	k.gmoregistry.net.
bridgestone.	172800	IN	NS	l.gmoregistry.net.
bridgestone.	86400	IN	DS	27731 8 2 24BB0833FB1F67742592DF5123136A9B010B762390BC06077523A462 89F2F38C
bridgestone.	86400	IN	RRSIG	DS 8 1 86400 20180409050000 20180327040000 41824 . krkExWf+zrSlu47rt8SNNVZGv83YvSB3CMrLhVAutCpuTH0Taqx0r2yZXyxCNvV0T7we4YXCrnc/+nz/V8DeMdEw F7MDS0PEXXXKt0PlciR0cnJXildYInCmS52CtFg75J EhcnNKdHMqUH/Sh MtYNYaA3Zv97nic9DGeGby7YM0rXE3fpW2qYnPQ//DXGF60Haxax0n+Sao0wBMr0dHcfur/+A za00iPmt/Dx09wZGJ228Fhj9Hn+716fzFy30XFo/wZeK0xdXbSMcimoX s5DicA==
bridgestone.	86400	IN	NSEC	broadway. NS DS RRSIG NSEC
bridgestone.	86400	IN	RRSIG	NSEC 8 1 86400 20180409050000 20180327040000 41824 . kV0gn9+pRVu80LY4LZdU9mAdNFqS18BnGL72oc3T7ec4E/hac0FVn3Iu+X/nxnHMsXxTixWDvQFy/+RtGHhZ6E Han6HhAYD1p0X5eT6DZR5eSyLzL/m9RaM23JHVAtw09Gk4UiPe9PI8Ub rrVb3g/Vt5n/K2MR2pTn6mQcp6XWwtEi6zDb4r8nflWScigXkaL4ldXHC5Z9KFuUw1UFY6SE p0zJ44DY8Xs6desRd21n5txMEFxP+JugYx8qvPazo+r/dwpZdk3FVdz 184Zfg==
broadway.	172800	IN	NS	dns1.nic.broadway.
broadway.	172800	IN	NS	dns2.nic.broadway.
broadway.	172800	IN	NS	dns3.nic.broadway.
broadway.	172800	IN	NS	dns4.nic.broadway.
broadway.	172800	IN	NS	dnsa.nic.broadway.
broadway.	172800	IN	NS	dnsb.nic.broadway.
broadway.	172800	IN	NS	dnsc.nic.broadway.
broadway.	172800	IN	NS	dnsd.nic.broadway.
broadway.	86400	IN	DS	47576 8 2 CCC4CE45AACB1C0FCD8181D968B86BEFF3B34D1A71576F137CA43529 FF8F12BB
broadway.	86400	TN	RRSIG	DS 8 1 86400 20180409050000 20180327040000 41824 . en0n1hYnryYYCuW/ln4Y/4PSTnfmrhRk



Tutorial DNS Hyperlocal

Índice [ocultar]

- 1 [Introdução](#)
- 2 [Implementação - BIND \(CentOS\)](#)
- 3 [Implementação - Unbound](#)
- 4 [Implementação - Unbound + NSD](#)
- 5 [Implementação - Microsoft Windows Server 2012](#)
- 6 [Conclusão](#)
- 7 [Referências](#)

Introdução

A Zona Raiz do Sistema de Nomes de Domínios (DNS) é servida por 12 organizações que operam instâncias *anycast* de servidores de nomes autoritativos provendo respostas para a raiz do DNS. Estas instâncias estão distribuídas em mais de 1000 localidades ao redor do mundo. Apesar deste grande número de servidores e alta capacidade provisionada para a resolução da raiz de nomes, ainda existe a possibilidade de que um grande ataque coordenado de negação de serviço (DDoS) possa comprometer o acesso à internet para muitos usuários.

Para minimizar e prevenir esta ameaça, existe a possibilidade de adicionar um fator de resiliência na configuração dos servidores recursivos do provedor de internet através do uso de uma cópia local da zona raiz, chamada de **Hyperlocal**. Hyperlocal é apresentado em detalhes na [RFC7706](#) e, resumidamente, consiste em executar uma cópia da zona raiz no mesmo servidor de serviços de resolução recursiva. Desta forma, as consultas à zona raiz dos clientes são respondidas localmente sem necessidade comunicação externa entre os servidores. Isso resulta em maior robustez do serviço em caso de



One World, One Internet

Visit us at icann.org



@icann



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann