Tópicos sobre DNS e o seu provedor na ICANN.

Daniel Fink daniel.fink@icann.org

IX Fórum Regional – Manaus AM
Julho 2019

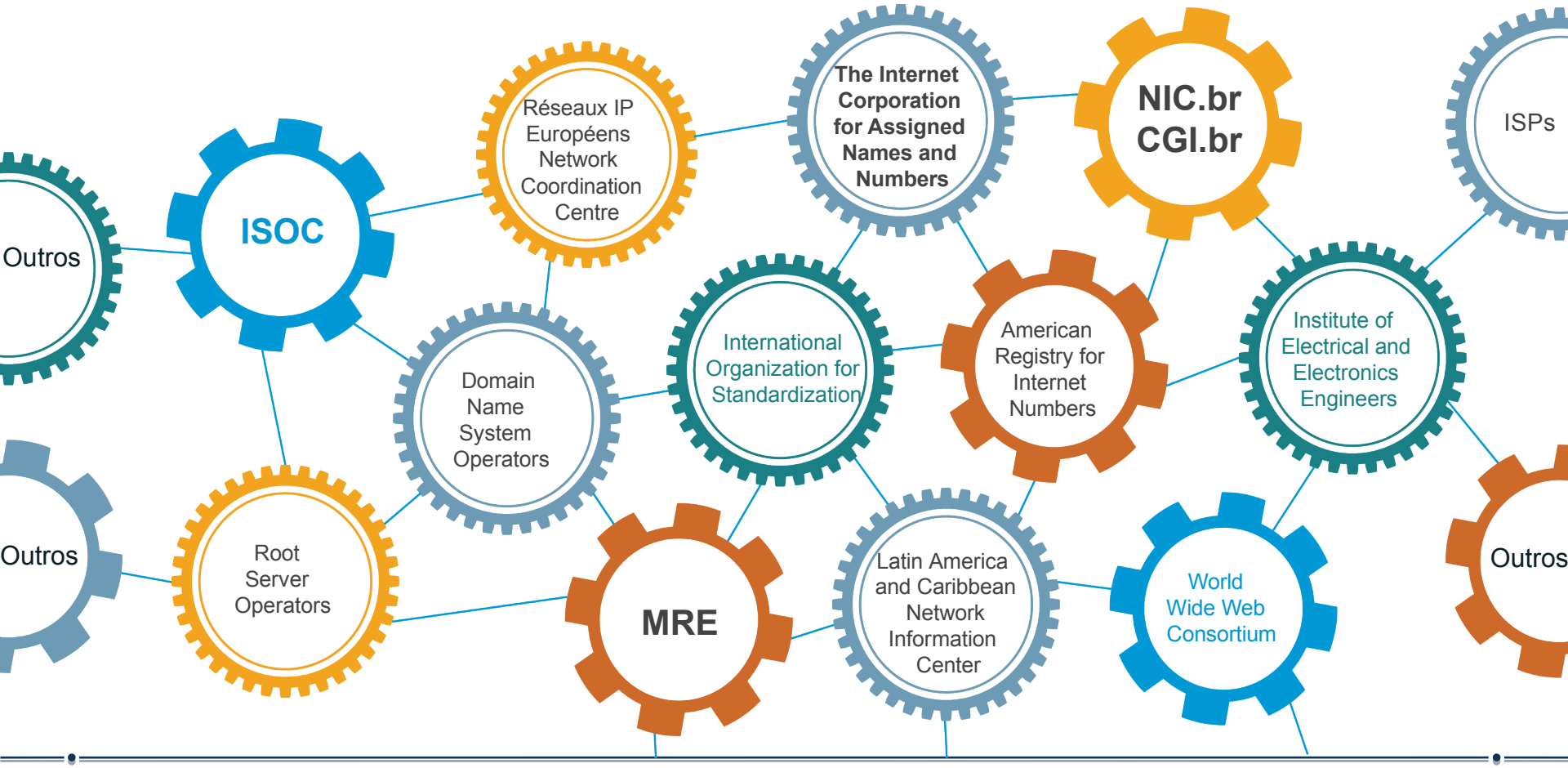
O que é a ICANN?

ICANN

Corporação da Internet para Designação de Nomes e Números

Nossos parceiros

Em coordenação com nossos parceiros, ajudamos a fazer a Internet funcionar.



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 dominio 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

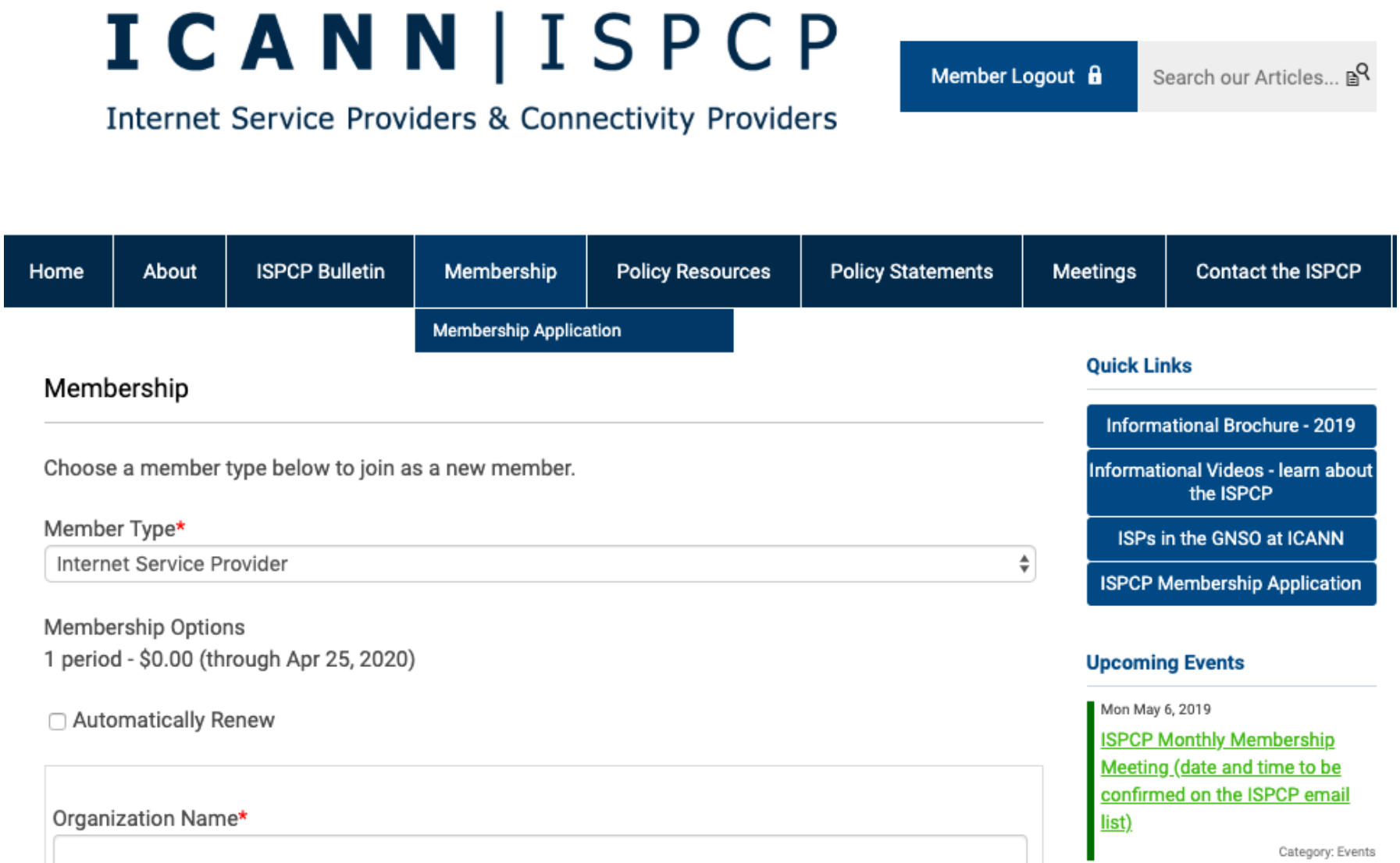
Representa o setor de conectividade, contribui nas diversas discussões técnicas e macropolíticas:

- 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

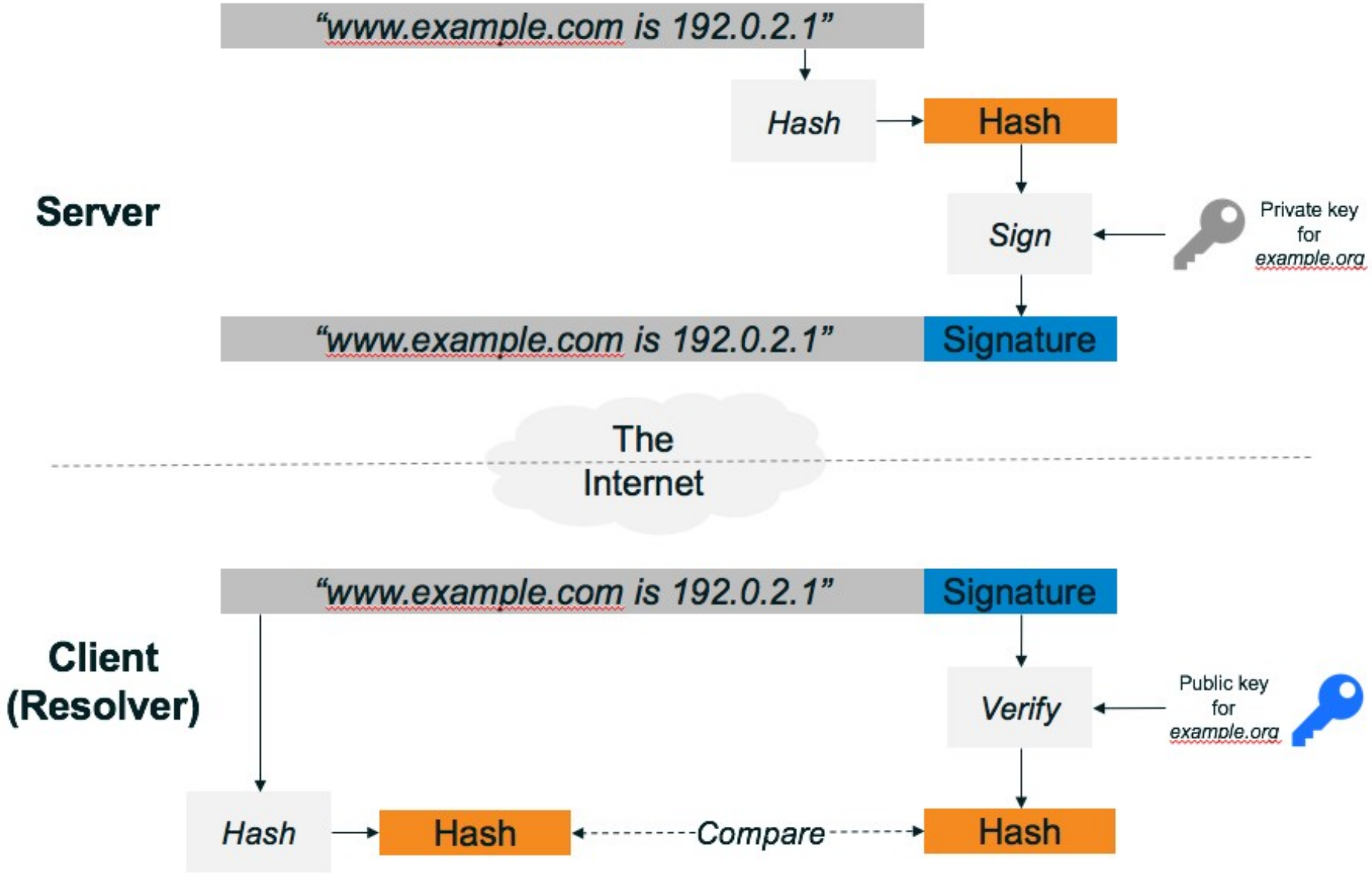
Seja um membro: www.ispcp.info



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

Criptografia de Chave Pública e DNSSEC



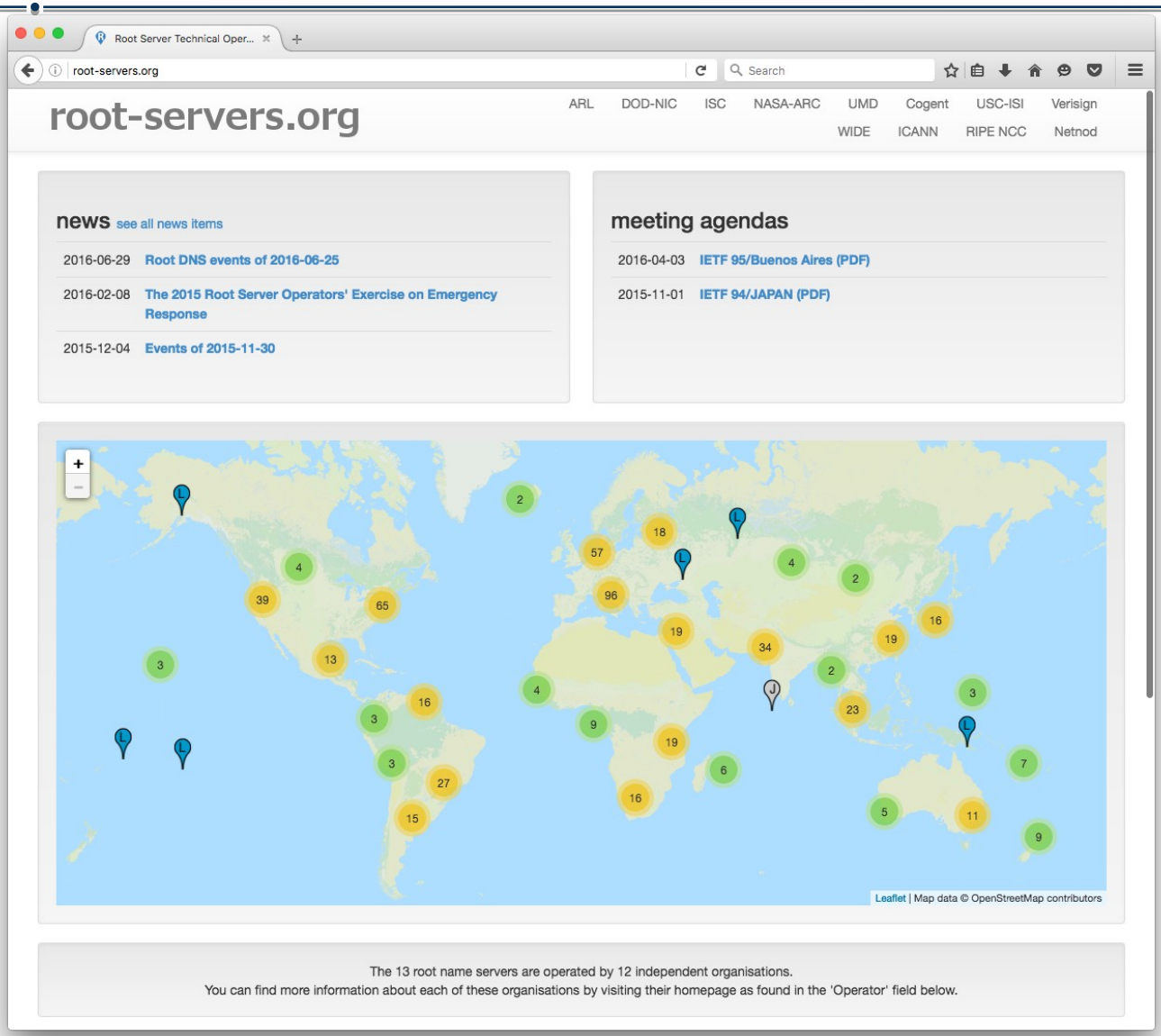
Hyperlocal

Alternativa ao IMRS

Servidores Raiz e Operadores

- **A** Verisign
- **B** University of Southern California Information Sciences Institute
- **C** Cogent Communications, Inc.
- **D** University of Maryland
- **E** United States National Aeronautics and Space Administration (NASA) Ames Research Center
- **F** Information Systems Consortium (ISC)
- **G** United States Department of Defense (US DoD) Defense Information Systems Agency (DISA)
- **H** United States Army (Aberdeen Proving Ground)
- **I** Netnod Internet Exchange i Sverige
- **J** Verisign
- **K** Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- **L** Internet Corporation For Assigned Names and Numbers (ICANN)
- **M** WIDE Project (Widely Integrated Distributed Environment)

Instâncias Anycast (aprox. 1000 cópias)



RFC 1546 1993

→ No Brasil: 14 instaladas pelo NIC.br

E se mesmo assim algo der errado?

Ameaça de DDoS

Capacidade de ataque > mecanismos de defesa

Alternativa

Diminuir dependência dos servidores recursivos aos servidores raiz.

Como?

Manter e usar uma cópia local da zona raiz

→ **Hyperlocal** **RFC 7706**

Hyperlocal

1. Cópia da Zona Raiz junto ao recursivo.
2. Consultas mais rápidas e discretas.
3. DNSSEC cada vez mais importante.
4. Como baixar a zona raiz de forma segura.
5. ‘Framework’ será apresentado 2019
6. Arquivos de zona não são confidenciais

RFC 7706

1. BIND 9.9
   - Recursivo e Autoritativo
2. Unbound 1.4 and NSD 4
   - Softwares diferentes
3. Microsoft Windows Server 2012
   - Recursivo e Autoritativo

https://tools.ietf.org/html/draft-ietf-dnsop-root-loopback-05

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

```
[root@master ~]# dig @8.8.8.8 domaininvalid.rrrrrrrrrrrrrrrrrrrr

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @8.8.8.8 domaininvalid.rrrrrrrrrrrrrrrrrrrr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 17346
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;domaininvalid.rrrrrrrrrrrrrrrrrrrr. IN        A

;; AUTHORITY SECTION:
.                       86398   IN      SOA     a.root-servers.net. nstld.verisign-grs.com.

;; Query time: 70 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Qui Jun 06 12:53:34 -03 2019
;; MSG SIZE  rcvd: 139
```

Teste do Hyperlocal na RLINE Telecom, Planalto-PR

2 - recursivo local 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 local para um dominio invalido

```
[root@master ~]# dig @[redacted].4 domaininvalid2.rrrrrrrrrrrrrrrrrrr

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @[redacted].4 domaininvalid2.rrrrrrrrrrrrrrrrrrr
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 20333
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;domaininvalid2.rrrrrrrrrrrrrrrrrrr. IN A

;; AUTHORITY SECTION:
.                       637     IN      SOA     a.root-servers.net. nstld.verisign-grs.com.

;; Query time: 2 msec
;; SERVER:[redacted].4#53([redacted].4)
;; WHEN: Qui Jun 06 12:59:35 -03 2019
;; MSG SIZE  rcvd: 140
```

```
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+zrSlu47rt8SNNVZGy83YvSB3
CMrLhVAutCpuIHQTaqxOr2yZXyxCNyV0T7we4YXCrnc/+nz/V8DeMdEw F7MDSQPEXXKIQPlicjRQcnJXildYInCmS52CtFgZ5JEhcNKdHMqUH/Sh MtYNYaA3Zy97njc9D
GeGby7YMQrXE3fpW2qYnPQ//DXGF6OHaxaxQn+SaoQwBMr0dHCfur/+A zaOOiPmt/DxO9wZGJ228Fhj9Hn+716fzFy3QXFo/wZeK0xdXbSMcimqX s5DicA==
bridgestone.            86400   IN      NSEC    broadway. NS DS RRSIG NSEC
bridgestone.            86400   IN      RRSIG   NSEC 8 1 86400 20180409050000 20180327040000 41824 . kVQgn9+pRVu8QLY4LZdU9mAdNFqSl8
BnGL72oc3T7ec4E/hqcQFVn3Iu+X/nxnHMsXxTixWDvQFy/+RtGHhZ6E Han6HhAYD1p0X5eT6DZR5eSyLzL/m9RaMZ3JHVAtw09Gk4UiPe9PI8Ub rrVb3g/Vt5n/K2MRZ
pTn6mQCp6XWWtEj6zDb4r8nflWScjgXkaL4ldXHC5Z9KFuUw1UFY6gSE pOzJ44DY8Xs6desRd21n5txMEFxP+JugYx8gvPqzo+r/dwpZdk3zFVdz 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 CCC4CE45AACB1C0ECD8181D968B86BEFF3B34D1A71576F137CA43529 FF8F12BB
broadway.               86400   IN      RRSIG   DS 8 1 86400 20180409050000 20180327040000 41824 . en0qUbYprYYSvW/Lq4Y/4PSIqfmrjbBK
```

Muito obrigado ! **daniel.fink@icann.org**

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