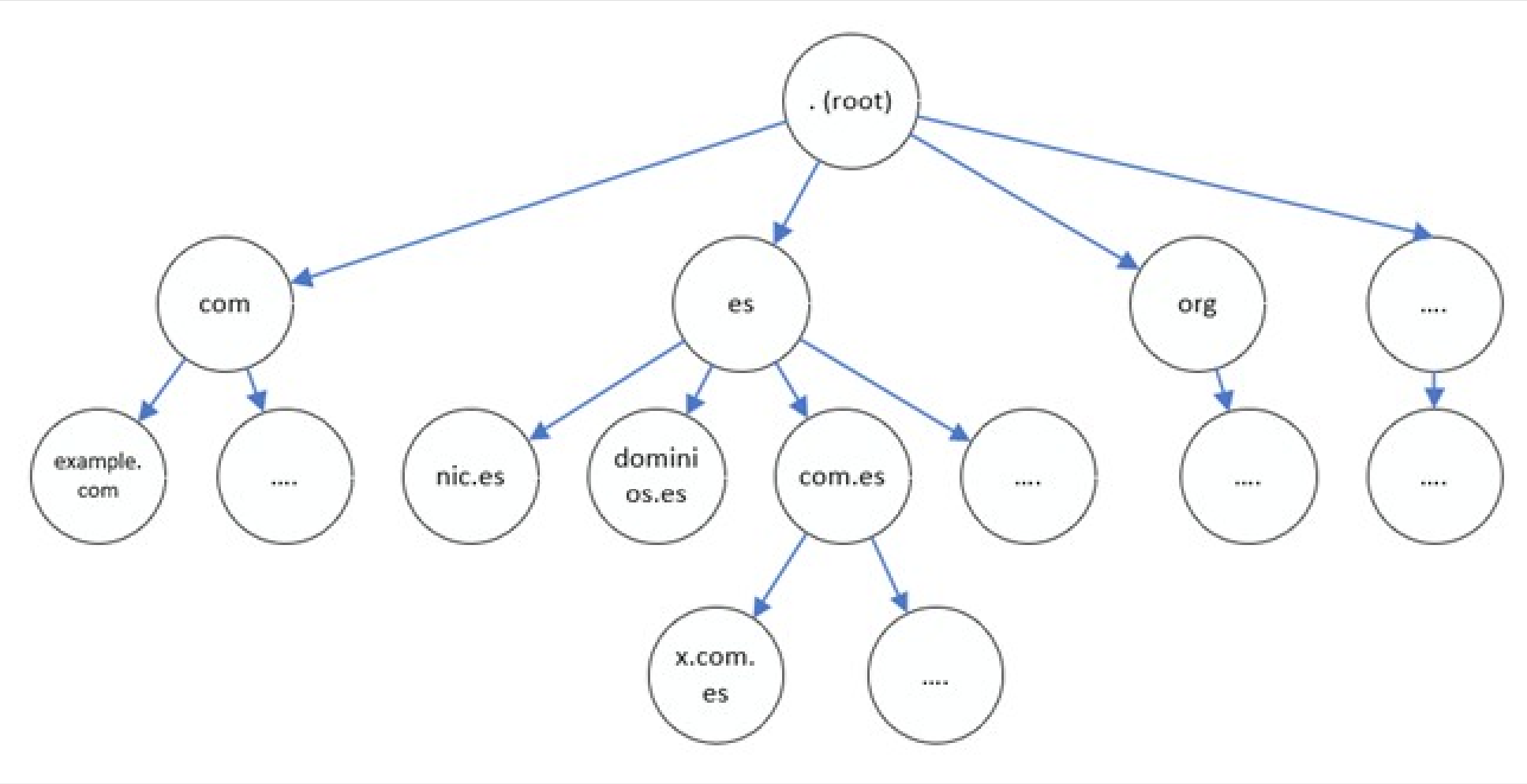
Apresentação
DNS

- Introdução
- Conceitos e Definições
- Ferramentas
- Configuração exemplo
- Problemas & Aspectos de segurança
- Laboratório
- Atividade extra

Intro

- Domain name system é um sistema mundial para registo de nomes em relação aos endereços IP. Mecanismo para tradução de IPv4 ou IPv6 em hostnames.
- Sistema mantido em estrutura hierarquica onde todo nome (FQDN) tem origem no “.” raiz da hierarquia.
- Espaço de nomes gerido pelo ICANN e registos regionais (ARIN, RIPE NCC, APNIC, LACNIC e AfriNIC).
- Primeiras utilizações em 1984.
- RFC 1034 e 1035.
- Tipicamente utiliza UDP 53, e alternativamente TCP 53
- DNSsec é a extensão do DNS para garantir criptogragia e mais segurança na comunicação DNS.

Conceitos e Definições



https://www.dominios.es/en/plataforma-dns

Conceitos

- https://root-servers.org

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	170.247.170.2, 2801:1b8:10::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Conceitos e Definições

- Tipos de servidores

- Root Server
- TLD
- Authoritative
- Resolver.

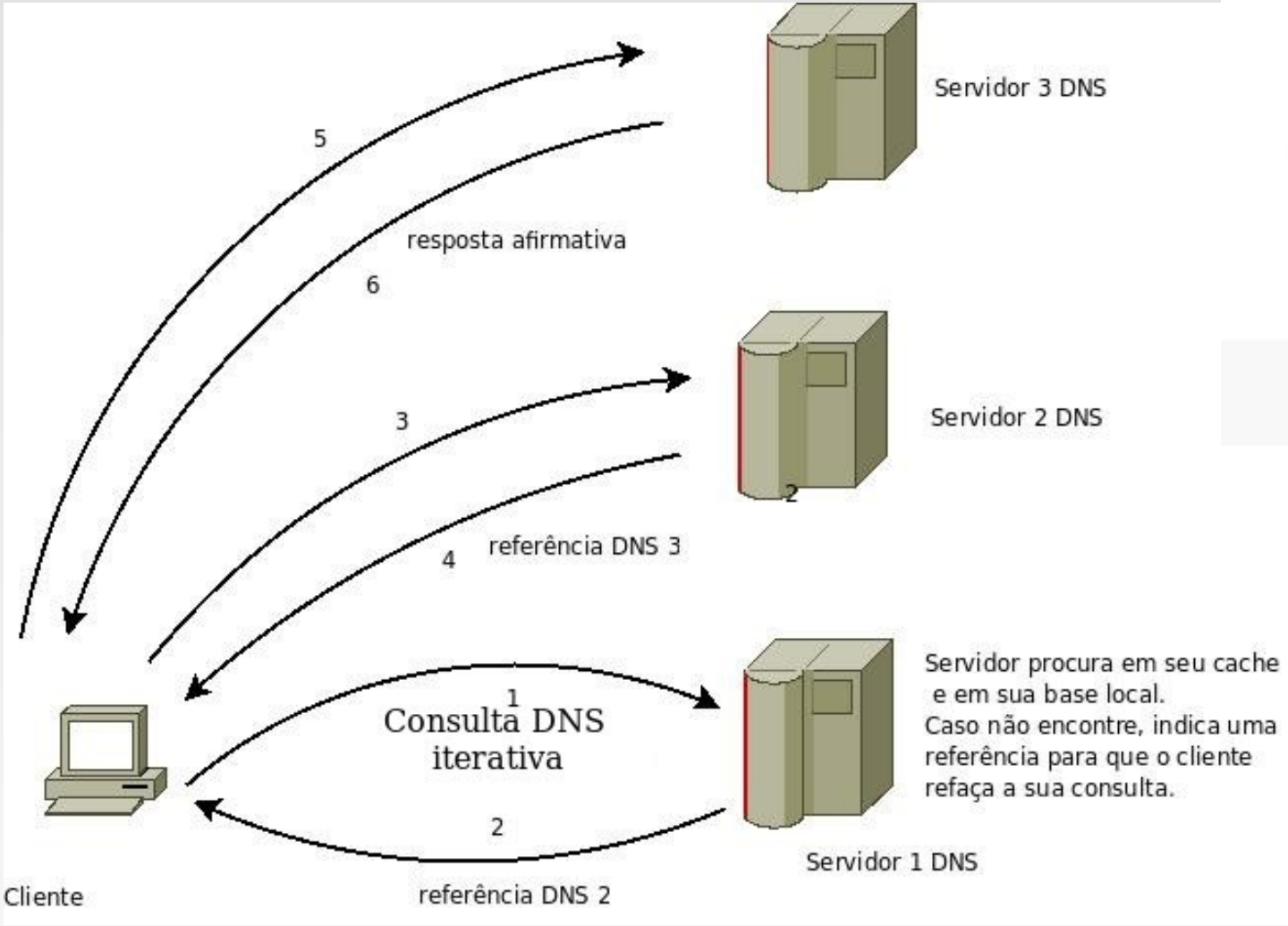
- Cache local (clientes e servers).

Conceitos e Definições

Consulta recursiva.

Conceitos e Definições

Consulta iterativa.



Conceitos e Definições

- Tipos mais comuns de registos

- A record
- AAAA record
- CNAME
- MX record
- PTR record
- NS record

- HFIFO, TXT, SRV, SOA, etc

Ferramentas

- nslookup

```
> set q=mx
> uol.com.br
Server:    200.144.145.9
Address:  200.144.145.9#53

Non-authoritative answer:
uol.com.br     mail exchanger = 10 mx.uol.com.br.

Authoritative answers can be found from:
uol.com.br     nameserver = eliot.uol.com.br.
uol.com.br     nameserver = charles.uol.com.br.
uol.com.br     nameserver = borges.uol.com.br.
mx.uol.com.br      internet address = 200.147.36.15
eliot.uol.com.br     internet address = 200.221.11.98
borges.uol.com.brinternet address = 200.147.255.105
charles.uol.com.br       internet address = 200.147.38.8
```

- host

- whois

Ferramentas

- dig

```
dig -q www.uol.com.br

; <<>> DiG 9.6.1-P2 <<>> -q www.uol.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4002
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.uol.com.br.     IN      A

;; ANSWER SECTION:
www.uol.com.br.      291    IN      A       200.147.67.142
www.uol.com.br.      291    IN      A       200.221.2.45

;; AUTHORITY SECTION:
uol.com.br.     2554    IN      NS      borges.uol.com.br.
uol.com.br.     2554    IN      NS      charles.uol.com.br.
uol.com.br.     2554    IN      NS      eliot.uol.com.br.

;; ADDITIONAL SECTION:
eliot.uol.com.br.       2554    IN      A       200.221.11.98
borges.uol.com.br.      2554    IN      A       200.147.255.105
charles.uol.com.br.     290     IN      A       200.147.38.8

;; Query time: 3 msec
;; SERVER: 200.144.145.9#53(200.144.145.9)
;; WHEN: Mon Oct 10 12:22:34 2011
;; MSG SIZE  rcvd: 175
```

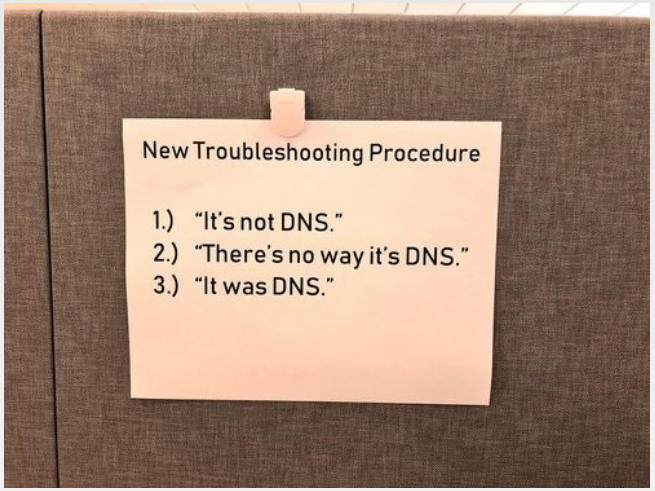
Configuração (bind)

```
$ORIGIN domain.com
$TTL 86400
@     IN     SOA    dns1.domain.com.     hostmaster.domain.com. (
                    2001062501 ; serial
                    21600      ; refresh after 6 hours
                    3600       ; retry after 1 hour
                    604800     ; expire after 1 week
                    86400 )    ; minimum TTL of 1 day
      IN     NS     dns1.domain.com.
      IN     NS     dns2.domain.com.
      IN     MX     10     mail.domain.com.
      IN     MX     20     mail2.domain.com.
             IN     A       10.0.1.5
server1      IN     A       10.0.1.5
server2      IN     A       10.0.1.7
dns1         IN     A       10.0.1.2
dns2         IN     A       10.0.1.3
ftp          IN     CNAME   server1
mail         IN     CNAME   server1
mail2        IN     CNAME   server2
www          IN     CNAME   server2
```

Problemas


Me, waiting for effects after changing DNS records


HE WHO CONTROLS DNS
CONTROLS EVERYTHING
makeameme.org


New Troubleshooting Procedure
1.) "It's not DNS."
2.) "There's no way it's DNS."
3.) "It was DNS."


0 DAYS SINCE IT WAS DNS
(It's always DNS)

Aspectos de segurança

- Propagar https://www.whatsmydns.net/
- Envenenamento de hosts local.
- Envenenamento do cache do DNS.

http://www.youtube.com/watch?v=1d1tUefYn4U

- Implementação de DNSsec para evitar que respostas ilegítimas atinjam ao servidor e possivelmente seu cache.

Laboratório

- Configurar um DNS server local que resolve nomes e Ips para os hosts da rede da sala.

Atividade Extra

- Faça o exercício extra em http://rzuolo.com/2025/grs/atividade-extra-06-DNS.pdf

The End