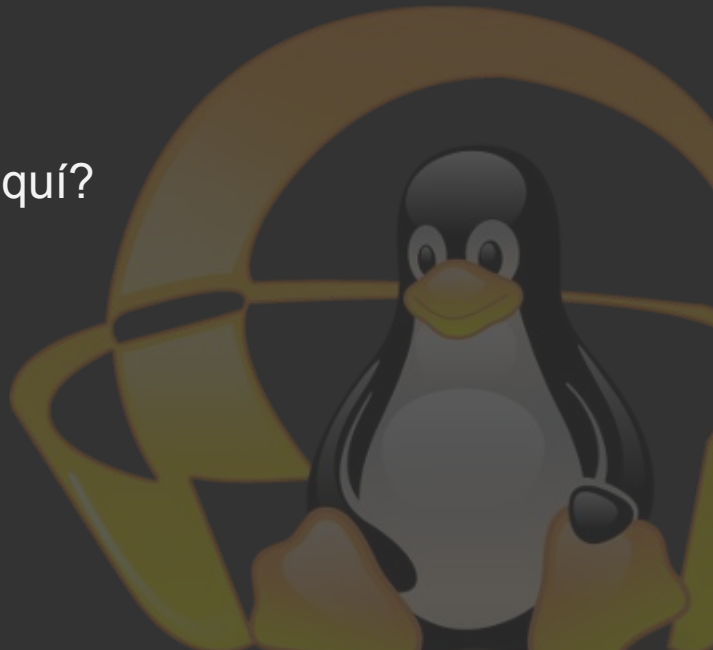
DNS y BIND

Por: Jesús Godínez (@tonymoyoy)
Grupo de Usuarios de GNU/Linux de Tijuana
Sábado 18 de Junio, 2016

Introducción

¿Quien soy y por qué estoy aquí?



¿Qué es DNS?

- DNS = Domain Name Server
  - Jerarquía
  - Distribuido
  - Delegación

¿Cómo funciona DNS?

Query

Root Servers

TLD

NameServer

Respuesta

foro.gultij.org?

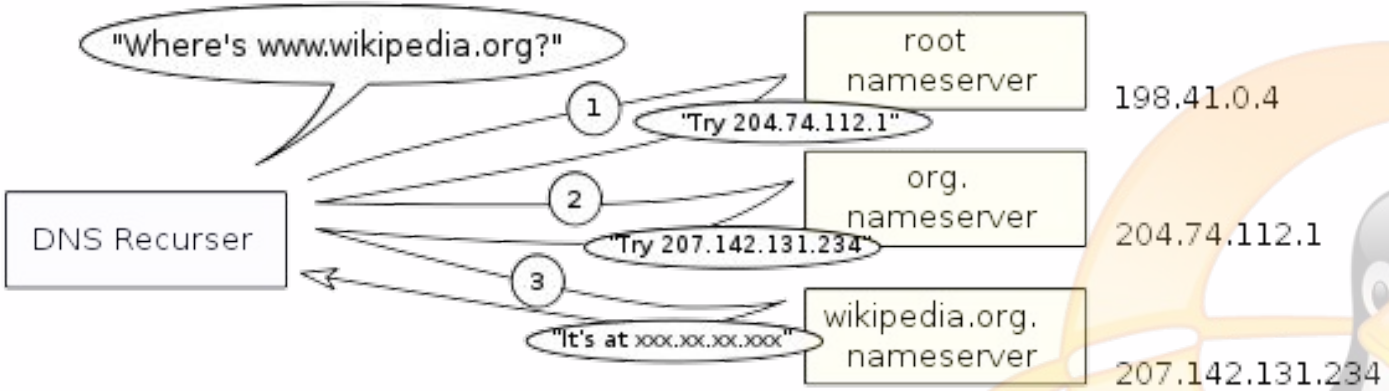
.org

gultij.org

foro.gultij.org

207.210.217.159

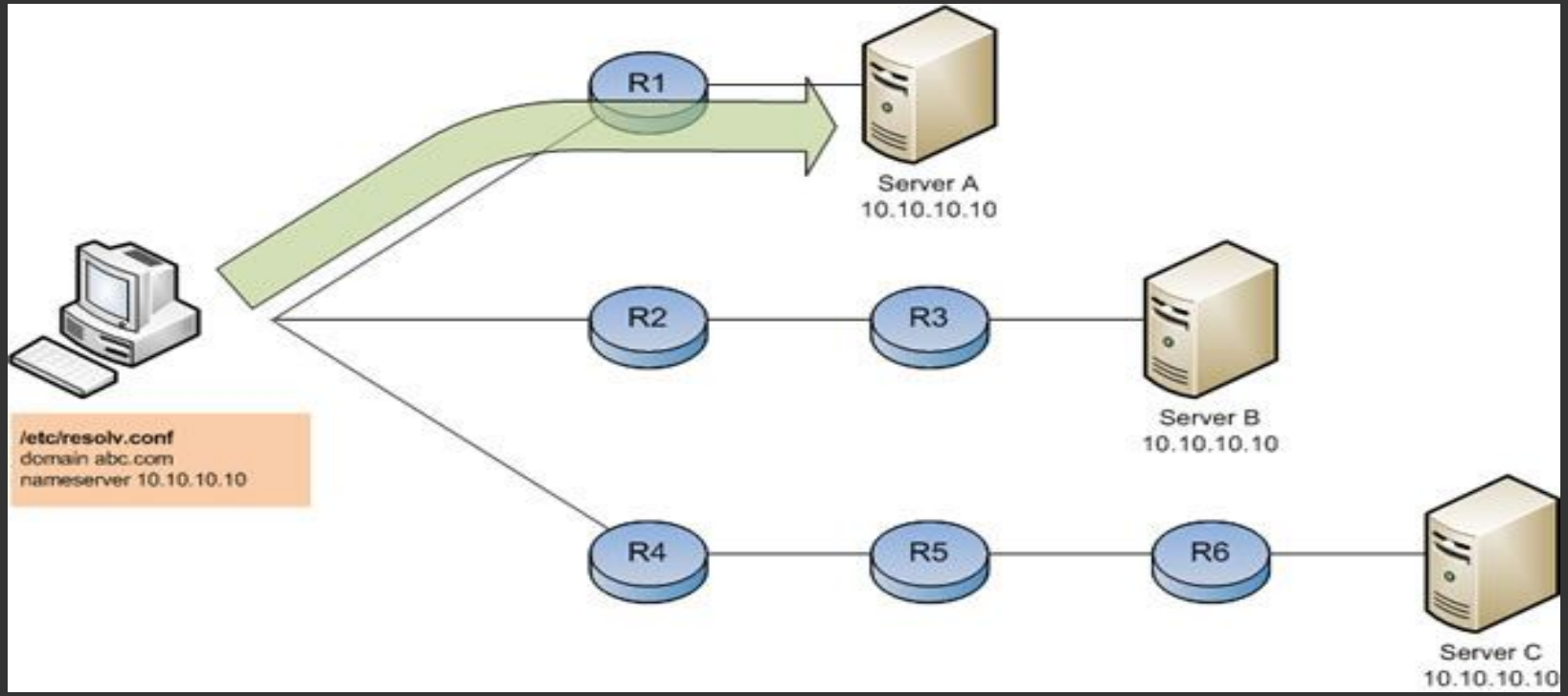
¿Cómo funciona DNS?



Root Servers

- Responsabilidad de ICANN
- Root Server System Advisory Committee (RSSAC) ← How To Administrar estos servidores
- Server A-M
- Operadores: Universidades, Verisign, NASA, etc
- Distribuidos
- Se encargan de referir a los servidores autoritarios para los dominios
- “13” servers, en realidad son más ya que usan anycast
- Software: NSD

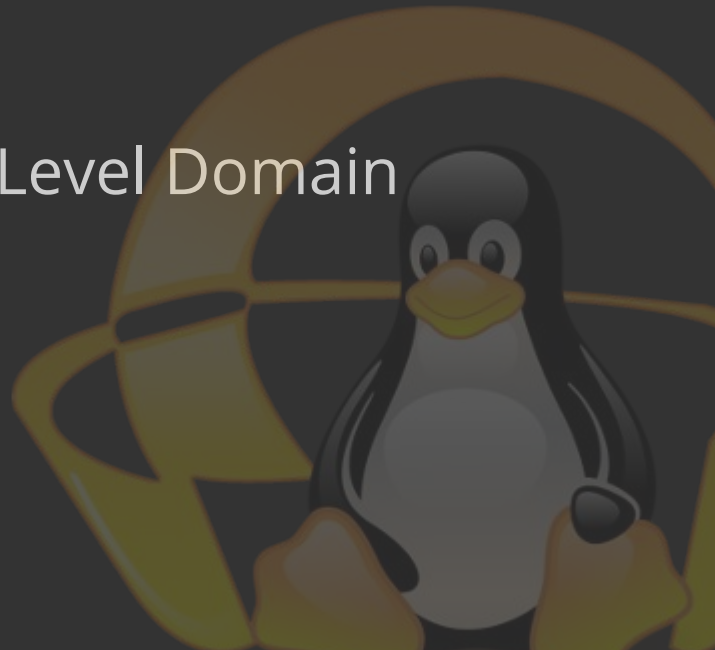
Anycast?


R1
Server A
10.10.10.10
R2
R3
Server B
10.10.10.10
/etc/resolv.conf
domain abc.com
nameserver 10.10.10.10
R4
R5
R6
Server C
10.10.10.10

GTLDs y CCTLDs

- TLD = Top Level Domain
- GTLD = Generic Top Level Domain
  - .com, .net, .org

- CCTLD = Country Code Top Level Domain
  - .fr, .mx, hu, jp, ca, etc
  - Reglas propias :)
  - Comercial CCTLD
    - .tv, .fm, .am, etc



BIND

- Berkeley Internet Name Domain
- Bind 9 – The Standard
- Bind 10 – Reestructuracion

DNS Software

- Fuentes de Datos
- Complejidad
- Administración
- Datos Dinámicos

Anatomía de una Zona de DNS (BIND)

```
$TTL 1800
@ IN SOA example.com. root.example.com. (
20160616001       ; serial
                  8H              ; refresh
                  2H              ; retry
                  4W              ; expire
                  900 )            ; minimum

NS lala1.com.
NS lala1.com.
MX 10 example.com.
TXT "Test"
router            A 192.168.177.1
printer.example.com. A 192.168.177.2
ns       IN    A 192.168.177.3
www               A 192.169.141.192

ftp CNAME ww.example.com.
mail CNAME gmail.com.
```

Tipos de Registros

- A
- CNAME
- PTR
- NS
- TXT
- SRV
- MX

named.conf (parte 1)

```
options {
directory "/var/named";
Version "2.0 Fake";
allow-transfer {"none";};
  allow-recursion {192.168.3.0/24;};

};

logging{
channel example_log{
file "/var/log/named/example.log" versions 3 size 2m;
severity info;
print-severity yes;
print-time yes;
print-category yes;
};
category default{
example_log;
};
```

named.conf (parte 2)

```
zone "." {
type hint;
file "root.servers";
};
zone "example.com" in{
type master;
file "master/master.example.com";
allow-transfer {192.168.23.1;192.168.23.2;);
};
```

Forwarders

- Proxy
- Caching
- Defensa Perimetral
- Control Administrativo
- Balance de Carga
- Forwarder para zonas específicas

Delegations

- NS Record
- Delegación de Zonas

- whois
- Delegación de Subzonas

Dig

- Domain Information Groper
- $dig gultij.org +short
- $dig gultij.org axfr
- $dig -x 192.168.1.1
- $dig @dns-slave5 gultij.org

DNS Riesgos y Ataques

- Zonas
- Actualizaciones Dinámicas
- Transferencias de Zonas

  - Slave Spoofing

  - Zonas pueden contener información interna

Preguntas y Comentarios

Créditos