
DNS: Instalación, Configuración, Herramientas y Errores Comunes

Por:
David Soltero-Lugo, david@nic.pr



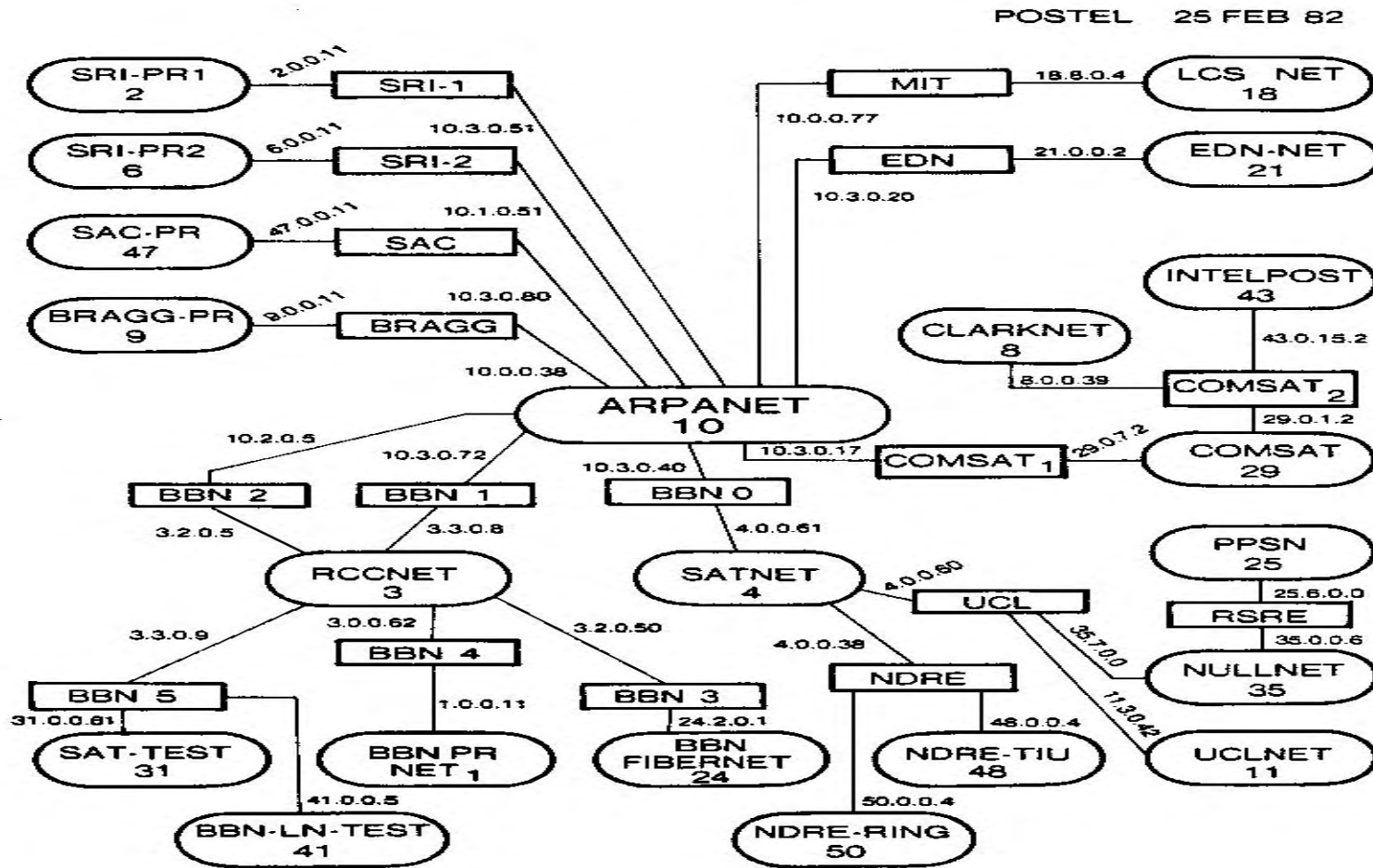
Objetivos de este Workshop

- Al final de este workshop podrás contestar las siguientes preguntas:
 - ¿ Que es el sistema de Dns y cual es su uso principal?
 - ¿ Cual es la estructura del sistema de Dns ?
 - ¿ Cuales son los tipos de record básicos para configurar una zona en el DNS ?
 - ¿ Cuales son 2 programas mas comunes para hacer "debug" a un sistema de DNS ?
 - ¿ Cuales son los problemas mas comunes en la configuración de un DNS server?

¿ Que es IP?

- Una dirección de IP (dirección de Protocolo de Internet) es un numero único que se asigna a devices con el propósito de identificarlos y que se comuniquen unos con los otros dentro de una red, utilizando el standard del Protocolo de Internet.
 - 136.145.251.60

Precursor del Internet (ARPANET)



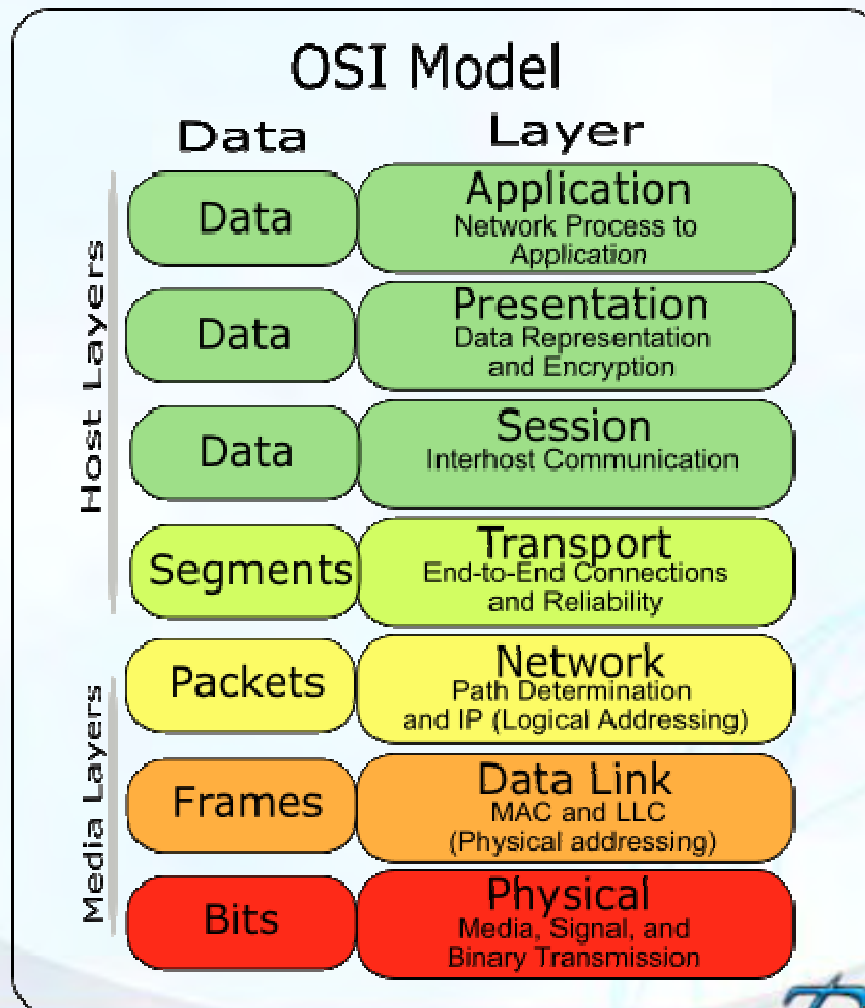
Clases IP

- Justo antes de la proliferación de las redes locales (Lan's), cuando solo existían pocas y grandes redes (ARPANET) no existían clases, esto limitaba el internet a solo 256 redes posibles. Para solucionar este problema se crean las clases.
- El objetivo para clasificar las redes de esta forma fue el de decidir cual es la parte que se encarga de la red, y que partes se dedican para los nodos.

Tipos de Clases

- Clase A
 - Numero total de redes posibles = 126
 - Numero total de direcciones por red = 16,777,214
 - 1.0.0.0 - 127.0.0.0 (Netmask /8)
- Clase B
 - Numero total de redes posibles = 16,384
 - Numero total de direcciones por red = 65,534
 - 128.0.0.0 - 191.255.0.0 (Netmask /16)
- Clase C
 - Numero total de redes posibles = 2,097,152
 - Numero total de direcciones por red = 254
 - 192.0.0.0 - 223.255.255.0 (Netmask /24)

Modelo OSI



¿Qué es el DNS?

- Domain Name System (DNS)
 - DNS es la base de datos distribuida mas grande del mundo, comprometiando mas de 1 millón de servidores operando como un database global.
 - DNS es un sistema jerárquico con estructura de árbol donde el "." se denomina como la raíz.
 - Bajo la raíz se hallan los dominios de más alto nivel TLD (Top Level Domains)

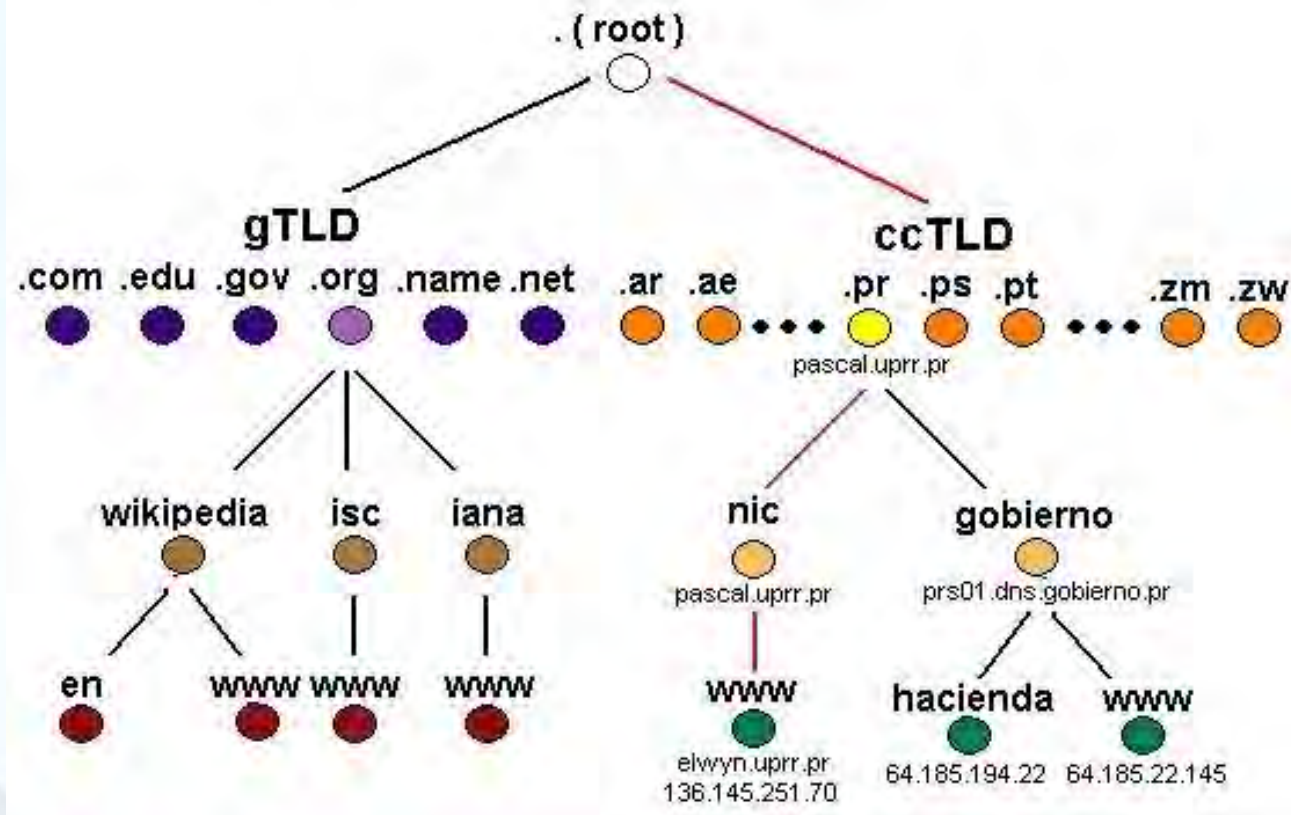
- gTLD

- .com
- .net
- .org
- .edu
- .info

- ccTLD

- .pr
- .us
- .uk
- .ar
- .mx

¿Qué es el DNS? Cont..



Historia del DNS

En los 1970 el ARPANET, el precursor del Internet, era una comunidad de unos cientos de nodos. Para que dos nodos se comunicaran se usaba un solo archivo "HOSTS.txt" que contenía toda la información sobre un host o nodo. El file era mantenido por el Standford Research Laboratory Network Information Center y era distribuido desde una solo servidor a través de FTP (file transfer protocol).

Todo empeoró cuando el ARPANET comenzó a usar TCP/IP y el network creció exponencialmente. Este esquema tenia varios problemas como: problemas de tráfico, colisiones de nombre, consistencia, y la lentitud de las actualizaciones por lo que poco después se volvió inmanejable.

El cuerpo administrador del ARPANET decidió investigar un sucesor a HOSTS.txt que permitiera redundancia, edición local y consistencia. Paul Mockapetris, del USC Information Sciences Institute, fue el responsable de la arquitectura del nuevo sistema. En 1984 Mockapetris publicó la especificación del sistema de DNS.



¿Para que se usa el DNS?

- El DNS es el corazón del internet, actuando como un directorio que convierte host names a direcciones de IP y viceversa. Básicamente, cada vez que accedas al internet desde un web browser, un cliente de FTP o una aplicación de email, estas dependiendo de un DNS. Sin el DNS el internet no podía ser tan robusto como lo es hoy día.
- Domain Name System (DNS)
 - Por una parte, traducir una dirección canónica en una dirección IP. Por Ejemplo:
 - **"pascal.uprr.pr has address 136.145.251.60"**
 - Por otra parte, traducir una dirección IP en una o varias direcciones canónicas. Es lo que se conoce como traducción inversa. Por ejemplo:
 - **"60.251.145.136. in-addr.arpa domain name pointer pascal.uprr.pr."**
 - Obtener información sobre servicios.
 - Mail Exchange Records
 - VoIP SIP (Voice over IP Session Initiation Protocol)

¿Para que se usa el DNS? Cont...

- Facilita el uso del *Internet*.
 - <http://136.145.251.70>
 - [http://\[2001:468:1300:101:206:5bff:fef8:41e1\]](http://[2001:468:1300:101:206:5bff:fef8:41e1])
 - <http://www.nic.pr>
- Se puede utilizar para Redundancia en los Servicios.
- Otros.

Algunas Implementaciones de DNS Servers

- ISC Bind (Internet System Consortium)
 - <http://www.isc.org/sw/bind/bind9.3.php>
- PowerDNS
 - <http://www.powerdns.com>
- Djbdns
 - <http://tinydns.org>
- Microsoft DNS
- Otros...

Requisitos Técnicos para correr un DNS Server

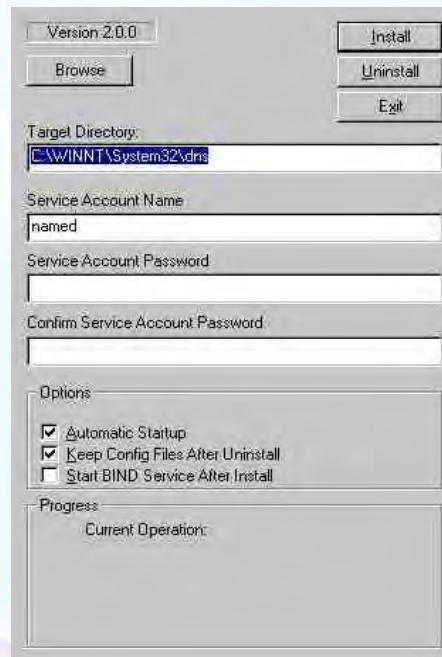
- 1 servidor que utilicé uno de los siguientes:
 - Sistemas Operativos:
 - Linux/Unix
 - Mac OS
 - Solaris
 - BSD
 - Windows
 - Conexión a la Internet

Instalando ISC Bind9.3.x

- Linux/Unix/BSD
 - Bajar el source
 - <http://www.isc.org/sw/bind/>
 - ./configure
 - make
 - make install

Instalando Bind9.3.x cont...

- Windows
 - Bajar el binario
 - <http://www.isc.org/sw/bind/>
 - Doble click en BindInstall.exe, luego de haber bajado el paquete y haberlo descomprimido
 - Click Install



The screenshot shows the Bind 9.3.x installation wizard window. It has a title bar that says "Version: 2.0.0". There are buttons for "Install", "Uninstall", "Exit", and "Browse". The "Target Directory:" field is set to "C:\WINNT\System32\dns". The "Service Account Name:" field is set to "named". The "Service Account Password:" and "Confirm Service Account Password:" fields are empty. The "Options:" section has three checkboxes: "Automatic Startup" (checked), "Keep Config Files After Uninstall" (checked), and "Start BIND Service After Install" (unchecked). The "Progress:" section shows "Current Operation:".

Configurando el named.conf

Servidor Autoritario (Conf. Recomendada)

```
# 134.202.2.10
acl servers { 134.202.0.10;134.202.1.10; };
options {
    directory "/var/lib/named";
    dump-file "/var/log/named_dump.db";
    statistics-file "/var/log/named.stats";
    #listen-on port 53 { any; };
    listen-on-v6 { any; };
    recursion no;
    allow-transfer {servers; };
    version "no version";
    transfer-format many-servers;
};
zone "." in {
    type hint;
    file "root.hint";
};
zone "isc.org.pr" in {
    type master;
    file "isc.org.pr.zone";
};
zone "0.0.202.134.IN-ADDR.ARPA" in {
    type master;
    file "0.0.202.134.IN-ADDR.ARPA.zone";
};
```

Configurando el named.conf

Servidor Autoritativo/Recursivo

```
# 134.202.2.10
acl servers {134.202.0.10;134.202.1.10; };
acl internals {134.202.0.0/16; servers; };
options {
    directory "/var/lib/named";
    dump-file "/var/log/named_dump.db";
    statistics-file "/var/log/named.stats";
    #listen-on port 53 { 127.0.0.1; };
    listen-on-v6 { any; };
    allow-recursion {internals; };
    allow-transfer {servers; };
    version "no version";
    transfer-format many-servers;
};
zone "." in {
    type hint;
    file "root.hint";
};
zone "isc.org.pr" in {
    type master;
    file "isc.org.pr.zone";
};
zone "0.0.202.134.IN-ADDR.ARPA" in {
    type master;
    file "0.0.202.134.IN-ADDR.ARPA.zone";
};
```

Configurando el named.conf Servidor Autoritario "Slave"

```
# 134.202.1.10, 134.202.0.10
options {
    ...
    ...
    ...
};
zone "." in {
    type hint;
    file "root.hint";
};
zone "isc.org.pr" in {
    type slave;
    file "isc.org.pr.zone";
    masters {134.202.2.10; };
};
zone "0.0.202.134.IN-ADDR.ARPA" in {
    type slave;
    file "0.0.202.134.IN-ADDR.ARPA.zone";
    masters {134.202.2.10; };
};
```

Archivo de la Zona "isc.org.pr.zone"

```

$ORIGIN .
$TTL 86400      ; 1 day
pr              IN SOA ns1.isc.org.pr. root.isc.org.pr. (
                2006022700 ; serial
                1200       ; refresh (20 minutes)
                900        ; retry (15 minutes)
                1209600    ; expire (2 weeks)
                3600       ; minimum (1 hour)
                )
@               IN      NS       ns1.isc.org.pr.
@               IN      NS       ns2.isc.org.pr.
@               IN      NS       ns3.isc.org.pr.
@               IN      MX       5          MTA01      ; SMTP Server Principal
@               IN      MX       10         MTA02      ; SMTP Server Secundario
@               IN      A        134.202.3.1      ; Webserver
@               IN      AAAA     2001:468:1300:1011:1205:5bff:fef8:451e
www             IN      A        134.202.3.1      ; Webserver
www             IN      AAAA     2001:468:1300:1011:1205:5bff:fef8:451e
MTA01          IN      A        134.202.3.2
MTA02          IN      A        134.202.4.2
ns1            IN      A        134.202.2.10      ; DNS's
ns2            IN      A        134.202.1.10      ; DNS's
ns3            IN      A        134.202.0.10      ; DNS's
Sip            IN      A        134.202.5.1       ; SIP Server
ftp            IN      CNAME     www
.              IN      A        134.202.3.1      ;Wildcard DNS
@              IN      TXT     "v=spf1 ip4:134.202.0.0/16 mx:mta01.isc.org.pr mx:mta02.isc.org.pr
~all"
_sip._udp      IN      SRV      0          0          5060      sip

```

Archivo de la Zona "0.0.202.134.IN-ADDR.ARPA.zone"

```
$ORIGIN .
$TTL 86400 ; 1 day
0.0.202.134.IN-ADDR.ARPA IN SOA ns1.isc.org.pr. root.isc.org.pr. (
    2005080600 ; serial
    1200 ; refresh (20 minutes)
    900 ; retry (15 minutes)
    1209600 ; expire (2 weeks)
    3600 ; minimum (1 hour)
)
0.0.202.134.IN-ADDR.ARPA IN NS ns1.uprr.pr.
0.0.202.134.IN-ADDR.ARPA IN NS ns2.uprr.pr.
0.0.202.134.IN-ADDR.ARPA IN NS ns3.uprr.pr.
10.1.202.134.in-addr.arpa. IN PTR ns2.isc.org.pr.
10.2.202.134.in-addr.arpa. IN PTR ns1.isc.org.pr.
10.0.202.134.in-addr.arpa. IN PTR ns3.isc.org.pr.
2.3.202.134.in-addr.arpa. IN PTR mta01.isc.org.pr.
2.4.202.134.in-addr.arpa. IN PTR mta02.isc.org.pr.
1.3.202.134.in-addr.arpa. IN PTR www.isc.org.pr.
```

Herramientas para “troubleshooting”

Nslookup

- nslookup es un comando de windows y unix el cual se utiliza para hacer una consulta a un DNS server para obtener el nombre y dirección de una maquina. Para usar nslookup escribimos en el command line: "nslookup" seguido por la dirección de Ip de una maquina o por su nombre.
- Esta herramienta es obsoleta en plataformas LINUX, UNIX, BSD, etc

Ejemplo nslookup

- Z:\>nslookup www.wikipedia.org
Server: welch.uprr.pr
Address: 136.145.251.80

Non-authoritative answer:

Name: rr.pmtpa.wikimedia.org

Addresses: 207.142.131.202, 207.142.131.203,
207.142.131.204, 207.142.131.205, 207.142.131.206,
207.142.131.210, 207.142.131.213, 207.142.131.214,
207.142.131.235, 207.142.131.236, 207.142.131.245,
207.142.131.246, 207.142.131.247, 207.142.131.248

Aliases: www.wikipedia.org, rr.wikimedia.org

Dig

- Dig es una herramienta para hacer consultas a Servidores de Nombres de Dominios (DNS server queries) para obtener información sobre direcciones de web, mail exchanges records y name servers entre otros.
- Esta herramienta se encuentra dentro del paquete de Bind.

Veamos una consulta sencilla...

- \$ dig www.isc.org

Observemos de manera detallada

```
; <<>> DiG 9.3.1 <<>> www.isc.org
;; global options: printcmd

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;www.isc.org.                IN      A

;; ANSWER SECTION:
www.isc.org.                600     IN      A      204.152.184.88

;; AUTHORITY SECTION:
isc.org.                    2191    IN      NS     ns-ext.lga1.isc.org.
isc.org.                    2191    IN      NS     ns-ext.nrt1.isc.org.
isc.org.                    2191    IN      NS     ns-ext.sth1.isc.org.
isc.org.                    2191    IN      NS     ns-ext.isc.org.

;; Query time: 210 msec
;; SERVER: 136.145.251.80#53(136.145.251.80)
;; WHEN: Mon Feb 13 12:21:42 2006
;; MSG SIZE rcvd: 144
```

Continuación...

```
; <<>> DiG 9.3.1 <<>> www.isc.org  
;; global options: printcmd
```

```
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
www.isc.org.
```

```
IN A
```

```
;; ANSWER SECTION:  
www.isc.org.
```

```
600 IN A 204.152.184.88
```

```
;; AUTHORITY SECTION:
```

```
isc.org. 2191 IN NS ns-ext.lga1.isc.org.  
isc.org. 2191 IN NS ns-ext.nrt1.isc.org.  
isc.org. 2191 IN NS ns-ext.sth1.isc.org.  
isc.org. 2191 IN NS ns-ext.isc.org.
```

```
;; Query time: 210 msec  
;; SERVER: 136.145.251.80#53(136.145.251.80)  
;; WHEN: Mon Feb 13 12:21:42 2006  
;; MSG SIZE rcvd: 144
```

Continuación...

```
; <<>> DiG 9.3.1 <<>> www.isc.org  
;; global options: printcmd
```

```
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
;www.isc.org.
```

```
IN A
```

```
;; ANSWER SECTION:  
www.isc.org.
```

```
600 IN A 204.152.184.88
```

```
;; AUTHORITY SECTION:
```

```
isc.org. 2191 IN NS ns-ext.lga1.isc.org.  
isc.org. 2191 IN NS ns-ext.nrt1.isc.org.  
isc.org. 2191 IN NS ns-ext.sth1.isc.org.  
isc.org. 2191 IN NS ns-ext.isc.org.
```

```
;; Query time: 210 msec  
;; SERVER: 136.145.251.80#53(136.145.251.80)  
;; WHEN: Mon Feb 13 12:21:42 2006  
;; MSG SIZE rcvd: 144
```

Continuación...

```
;; <<>> DiG 9.3.1 <<>> www.isc.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0
```

;; QUESTION SECTION:

```
;;www.isc.org.          IN      A
```

;; ANSWER SECTION:

```
www.isc.org.          600     IN      A      204.152.184.88
```

;; AUTHORITY SECTION:

```
isc.org.              2191    IN      NS      ns-ext.lga1.isc.org.
isc.org.              2191    IN      NS      ns-ext.nrt1.isc.org.
isc.org.              2191    IN      NS      ns-ext.sth1.isc.org.
isc.org.              2191    IN      NS      ns-ext.isc.org.
```

```
;; Query time: 210 msec
;; SERVER: 136.145.251.80#53(136.145.251.80)
;; WHEN: Mon Feb 13 12:21:42 2006
;; MSG SIZE rcvd: 144
```

Continuación...

```
; <<>> DiG 9.3.1 <<>> www.isc.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;www.isc.org.
```

```
;; ANSWER SECTION:
www.isc.org. 600
```

```
IN A
```

```
IN A
```

```
204.152.184.88
```

```
;; AUTHORITY SECTION:
```

```
isc.org. 2191 IN NS
isc.org. 2191 IN NS
isc.org. 2191 IN NS
isc.org. 2191 IN NS
```

```
ns-ext.lga1.isc.org.
ns-ext.nrt1.isc.org.
ns-ext.sth1.isc.org.
ns-ext.isc.org.
```

```
;; Query time: 210 msec
;; SERVER: 136.145.251.80#53(136.145.251.80)
;; WHEN: Mon Feb 13 12:21:42 2006
;; MSG SIZE rcvd: 144
```

Continuación...

```
;; <<>> DiG 9.3.1 <<>> www.isc.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;www.isc.org.                IN      A

;; ANSWER SECTION:
www.isc.org.                600     IN      A      204.152.184.88

;; AUTHORITY SECTION:
isc.org.                    2191    IN      NS      ns-ext.lga1.isc.org.
isc.org.                    2191    IN      NS      ns-ext.nrt1.isc.org.
isc.org.                    2191    IN      NS      ns-ext.sth1.isc.org.
isc.org.                    2191    IN      NS      ns-ext.isc.org.

;; Query time: 210 msec
;; SERVER: 136.145.251.80#53(136.145.251.80)
;; WHEN: Mon Feb 13 12:21:42 2006
;; MSG SIZE rcvd: 144
```

Continuación...

```
;; <<>> DiG 9.3.1 <<>> www.isc.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;www.isc.org.                IN      A

;; ANSWER SECTION:
www.isc.org.                600     IN      A      204.152.184.88

;; AUTHORITY SECTION:
isc.org.                    2191    IN      NS      ns-ext.lga1.isc.org.
isc.org.                    2191    IN      NS      ns-ext.nrt1.isc.org.
isc.org.                    2191    IN      NS      ns-ext.sth1.isc.org.
isc.org.                    2191    IN      NS      ns-ext.isc.org.

;; Query time: 210 msec
;; SERVER: 136.145.251.80#53(136.145.251.80)
;; WHEN: Mon Feb 13 12:21:42 2006
;; MSG SIZE rcvd: 144
```

Tipos de Consultas

- **A** (Dirección de IP)
 - dig www.isc.org.pr A
- **MX** (Mail Exchanges)
 - dig isc.org.pr mx
- **NS** (Name Servers)
 - dig isc.org.pr ns
- **ANY** (*Cualquier record*)
 - dig isc.org.pr any
- **AAAA** (*Dirección de IPv6*)
 - dig www.isc.org.pr aaaa
- **TXT** (*Texto*)
 - dig www.isc.org.pr txt

Consulta corta

- *dig www.isc.org +short*
 - *Desplega como resultado de la consulta solo la direccion de IP.*

Como hacer un reverse lookup?

- La opción `-x` te permite hacer un reverse lookup.

```
dig -x 204.152.184.167 +short  
mx-1.isc.org
```

```
dig 60.251.145.136.in-addr.arpa ptr +short  
pascal.uprr.pr
```

Hacer consultas a Nameservers Expecificos...

- Con dig es posible consultar a un servidor especifico

dig @ns-ext.isc.org www.isc.org

dig @upr1.upr.clu.edu www.isc.org

Búsqueda en masas (bulk lookups)...

- Para hacer bulk lookup's solo basta con crear un archivo .txt con los nombres de los host a buscar y utilizar la opción **-f**

dig -f /dirección/del/archivo.txt

Como hacer un Trace...

- Si deseas hacer un trace y observar como dig va del punto A al punto B usamos la opción *+trace*.

dig isc.org +trace

Trace Cont

```
; <<>> DiG 9.3.1 <<>> isc.org +trace  
;; global options: printcmd
```

```
.      166388      IN          NS          I.ROOT-SERVERS.NET.  
.      166388      IN          NS          J.ROOT-SERVERS.NET.  
.      166388      IN          NS          K.ROOT-SERVERS.NET.  
.      166388      IN          NS          L.ROOT-SERVERS.NET.  
.      166388      IN          NS          M.ROOT-SERVERS.NET.  
.      166388      IN          NS          A.ROOT-SERVERS.NET.  
.      166388      IN          NS          B.ROOT-SERVERS.NET.  
.      166388      IN          NS          C.ROOT-SERVERS.NET.  
.      166388      IN          NS          D.ROOT-SERVERS.NET.  
.      166388      IN          NS          E.ROOT-SERVERS.NET.  
.      166388      IN          NS          F.ROOT-SERVERS.NET.  
.      166388      IN          NS          G.ROOT-SERVERS.NET.  
.      166388      IN          NS          H.ROOT-SERVERS.NET.  
;; Received 292 bytes from 136.145.251.80#53(136.145.251.80) in 1 ms
```

```
org.    172800      IN          NS          TLD2.ULTRADNS.NET.  
org.    172800      IN          NS          TLD3.ULTRADNS.org.  
org.    172800      IN          NS          TLD4.ULTRADNS.org.  
org.    172800      IN          NS          TLD5.ULTRADNS.INFO.  
org.    172800      IN          NS          TLD6.ULTRADNS.CO.UK.  
org.    172800      IN          NS          TLD1.ULTRADNS.NET.  
;; Received 283 bytes from 192.36.148.17#53(I.ROOT-SERVERS.NET) in 157 ms
```

```
isc.org. 86400      IN          NS          ns-ext.sth1.isc.org.  
isc.org. 86400      IN          NS          ns-ext.nrt1.isc.org.  
isc.org. 86400      IN          NS          ns-ext.lga1.isc.org.  
isc.org. 86400      IN          NS          ns-ext.isc.org.  
;; Received 188 bytes from 204.74.113.1#53(TLD2.ULTRADNS.NET) in 121 ms
```

```
isc.org. 3600      IN          A           204.152.184.88  
isc.org. 3600      IN          NS          ns-ext.lga1.isc.org.  
isc.org. 3600      IN          NS          ns-ext.nrt1.isc.org.  
isc.org. 3600      IN          NS          ns-ext.sth1.isc.org.  
isc.org. 3600      IN          NS          ns-ext.isc.org.  
;; Received 232 bytes from 192.228.89.19#53(ns-ext.sth1.isc.org) in 208 ms
```

Determinando el TTL

```
; <<>> DiG 9.3.1 <<>> www.isc.org
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34429
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;www.isc.org. IN A

;; ANSWER SECTION:
www.isc.org. 600      IN      A      204.152.184.88

;; AUTHORITY SECTION:
isc.org. 2191     IN      NS     ns-ext.lga1.isc.org.
isc.org. 2191     IN      NS     ns-ext.nrt1.isc.org.
isc.org. 2191     IN      NS     ns-ext.sth1.isc.org.
isc.org. 2191     IN      NS     ns-ext.isc.org.

;; Query time: 210 msec
;; SERVER: 136.145.251.80#53(136.145.251.80)
;; WHEN: Mon Feb 13 12:21:42 2006
;; MSG SIZE rcvd: 144
```

Otras Herramientas



DNS Report for isc.org

Generated by www.DNSReport.com at 11:49:08 GMT on 11 Feb 2006.

Category	Status	Test Name	Information
Parent	PASS	Missing Direct Parent check	OK. Your direct parent zone exists, which is good. Some domains (usually third or fourth level domains, such as example.co.us) do not have a direct parent zone ('co.us' in this example), which is legal but can cause confusion.
	INFO	NS records at parent servers	Your NS records at the parent servers are: ns-ext.sth1.isc.org. [192.228.85.19] [TTL=86400] [US] ns-ext.nrt1.isc.org. [192.228.90.19] [TTL=86400] [US] ns-ext.lgal.isc.org. [192.228.91.19] [TTL=86400] [US] ns-ext.isc.org. [204.152.184.64] [TTL=86400] [US] [These were obtained from flc1.ultradns.net]
	PASS	Parent nameservers have your nameservers listed	OK. When someone uses DNS to look up your domain, the first step (if it doesn't already know about your domain) is to go to the parent servers. If you aren't listed there, you can't be found. But you are listed there.
	PASS	Glue at parent nameservers	OK. The parent servers have glue for your nameservers. That means they send out the IP address of your nameservers, as well as their host names.
	PASS	DNS servers have A records	OK. All your DNS servers either have A records at the zone parent servers, or do not need them (if the DNS servers are on other TLDs). A records are required for you' hostnames to ensure that other DNS servers can reach your DNS servers. Note that there will be problems if your DNS servers do not have these same A records.
NS	INFO	NS records at your nameservers	Your NS records at your nameservers are: ns-ext.lgal.isc.org. [192.228.91.19] [TTL=3600] ns-ext.nrt1.isc.org. [192.228.90.19] [TTL=3600] ns-ext.sth1.isc.org. [192.228.85.19] [TTL=3600] ns-ext.isc.org. [204.152.184.64] [TTL=3600]
	PASS	Matched glue	OK. The DNS report did not detect any discrepancies between the glue provided by the parent servers and that provided by your authoritative DNS servers.
	PASS	No NS A records at nameservers	OK. Your nameservers do include corresponding A records when asked for your NS records. This ensures that your DNS servers know the A records corresponding to all your NS records.
	PASS	All nameservers report identical NS records	OK. The NS records at all your nameservers are identical.
	PASS	All nameservers respond	OK. All of your nameservers listed at the parent nameservers responded.
	PASS	Name server name validity	OK. All of the NS records that your nameservers report seem valid (no IPs or partial domain names).
	PASS	Number of nameservers	OK. You have 4 nameservers. You must have at least 2 nameservers (RFC2182 section 5 recommends at least 3 nameservers), and preferably no more than 7.
	PASS	Same nameservers	OK. All the nameservers listed at the parent servers answer authoritatively for your domain.
	PASS	Missing (stealth) nameservers	OK. All 4 of your nameservers (as reported by your nameservers) are also listed at the parent servers.
	PASS	Missing nameservers 2	OK. All of the nameservers listed at the parent nameservers are also listed as NS records at your nameservers.
	PASS	No CNAMEs for domain	OK. There are no CNAMEs for isc.org. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
	PASS	No NSs with CNAMEs	OK. There are no CNAMEs for your NS records. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
	PASS	Name servers on separate class Cs	OK. You have nameservers on different Class C (technically, /24) IP ranges. You must have nameservers at geographically and topologically dispersed locations. RFC2182 3.1 goes into more detail about secondary nameserver location.
	PASS	All NS IPs public	OK. All of your NS records appear to use public IPs. If there were any private IPs, they would not be reachable, causing DNS delays.
	INFO	Name servers versions	Your nameservers have the following versions: 192.228.85.19: "S.3.1" 192.228.90.19: "S.3.1"



ZoneCheck: isc.org.

Zone information

isc.org.
1 ns-ext.nrt1.isc.org. 192.228.90.19
2 ns-ext.sth1.isc.org. 192.228.89.19
2 ns-ext.isc.org. 204.152.184.64, 2001:4F8:02::13
2 ns-ext.lga1.isc.org. 192.228.91.19

Test results

— warning —

Host doesn't reply to ICMP requests (firewall?)

→ ns-ext.isc.org /2001:4F8:02::13

— fatal —

The 'expire' period should be between 1W and 6W

Adv: default registry policy
The registry requires the SCA fields to be inside a defined range: the 'expire' should be between 1W and 6W, the 'minimum' between 3M and 1W, the 'refresh' between 1H and 2D, and at last the 'retry' between 15M and 1D.

The expire value is 41W and should be between 1W and 6W.

- ns-ext.sth1.isc.org./192.228.89.19
- ns-ext.lga1.isc.org./192.228.91.19
- ns-ext.isc.org./204.152.184.64
- ns-ext.nrt1.isc.org./192.228.90.19

Final status

FAILURE (and 1 warning(s))

Problemas Comunes

“lame delegation”

- Es cuando un NS Record apunta a un host incorrecto. Puede ser causado por:
 - Delegación de un zona a servidor que no es Authoritative de esta zona.
 - Un servidor Authoritative para la zona que tiene un record de otro servidor que no es Authoritative para la zona.
- Un dato importante es que $\frac{1}{4}$ de la zonas a nivel mundial poseen lame delegations.

Servidores Secundarios no son Actualizados

- Problemas Comunes:
 - Después del Cambio en el servidor principal no se actualizo el numero de serie de la zona.
 - No se le esta permitiendo la transferencia de zonas desde el servidor principal, ya sea por un ACL, o por el IP de donde se genera el request para el transfer.

Creación de A/AAAA/NS/MX Records

- Problemas comunes
 - Definimos un record sin tomar en cuenta el "."
 - EJ: (zona isc.org.pr)
 - ns1. IN A 134.202.2.10
 - ns2.isc IN A 134.202.1.10
 - ns3.isc.org.pr. IN A 134.202.0.10

Recursos online

- **The DNS Resources Directory**
 - <http://www.intac.com/%7Ecdp/cptd-faq/>
- **men&mice**
 - http://www.menandmice.com/online_docs_and_faq/glossary/index.htm
- **DNS HowTo**
 - <http://www.tldp.org/HOWTO/DNS-HOWTO.html>
- **Securing DNS with Transaction Signatures**
 - <http://www.linux.ie/articles/tutorials/dns-tsig.php>
- **All About DNS**
 - <http://www.linux.ie/articles/dns.php>
- **DNS Cómo**
 - <http://cauchy.bdat.net/dns/bind-9/DNS-HOWTO-9-es/>
- **Bulma.net**
 - <http://bulma.net/body.phtml?nIdNoticia=1334#queesunatsigyparaquesenecesita>

RFC's

- Los originales y definitivos estándares:
 - * 1034 - Domain Names: Concepts and Facilities.
 - * 1035 - Domain Names: Implementation and Specification.
- Estándares propuestos:
 - * 1995 - Incremental Zone Transfers in DNS.
 - * 1996 - A Mechanism for Prompt Notification of Zone Changes.
 - * 2136 - Dynamic Updates in the Domain Name System.
 - * 2181 - Clarifications to the DNS Specification.
- RFC de seguimiento de nuevos estándares:
 - * 2535 - Domain Name System Security Extensions.
 - * 2671 - Extension Mechanisms for DNS (EDNS0).
 - * 2672 - Non-Terminal DNS Name Redirection (DNAME).
 - * 2673 - Binary Labels in the Domain Name System.
- RFC diversos:
 - * 1535 - A Security Problem... with Widely Deployed DNS Software.
 - * 1536 - Common DNS Implementation Errors and Suggested Fixes.
 - * 1982 - Serial Number Arithmetic.
 - * 2536-2541 - Varios RFC sobre DNSSEC.

RFC's

- Tipos de registros de recursos:
 - * 1876 - A Means for Expressing Location Information in DNS.
 - * 2052 - A DNS RR for Specifying the Location of Services (SRV).
 - * 2168 - Resolution of Uniform Resource Identifiers using DNS.
 - * 2230 - Key Exchange Delegation Record for the DNS.
- DNS e Internet:
 - * 1101 - DNS Encoding of Network Names and Other Types.
 - * 1123 - Requirements for Internet Hosts: Application and Support.
 - * 1591 - Domain Name System Structure and Delegation.
 - * 2317 - Classless in-addr.arpa Delegation.
- Operaciones de DNS:
 - * 1537 - Common DNS Data File Configuration Errors.
 - * 1912 - Common DNS Operational and Configuration Errors.
 - * 2182 - Selection and Operation of Secondary DNS Servers.
 - * 2219 - Use of DNS Aliases for Network Services.
- Otros RFC relacionados con el DNS:
 - * 1713 - Tools for DNS debugging.
 - * 1794 - DNS Support for Load Balancing.

¿ Preguntas ?

Créditos:

- Carlos Rivera Silva, carlos@nic.pr
- Jose Ramon Villalon, villalon@nic.pr
- David Soltero-Lugo, david@nic.pr

Glosario

Algunos términos Comunes...

- A Record
 - Address Record, establece una relación entre un IP y un nombre de dominio
- Authoritative Server (Servidor Autoritario)
 - Adjetivo que describe un nameserver o una respuesta de un nameserver la cual se refiere a su propia data.

Términos comunes cont...

- Glue Record
 - Un glue record es un A record el cual es creado como parte de una delegación. Si una zona se delega a un nameserver cuyo hostname es un descendiente de esa zona particular, entonces se debe incluir un glue record para ese hostname en la delegación.
- MX Record
 - Mail Exchange Record, crea una ruta de correo para un nombre de dominio.

Términos comunes cont...

- NS Record
 - Name Server Record, define que servidor esta a cargo de una ruta.
- AAAA Record
 - Address Record, establece una relación entre un IPv6 y un nombre de dominio.
- PTR Record
 - Llamado Reverse Record, asocia un IP con un nombre de dominio.

Términos comunes cont...

- Serial Number (Numero de Serie)
 - Usado por los servidores secundarios para determinar si la zona requiere un transfer del servidor principal. Si el numero de serie es menor al numero de serie en el servidor primario, el secundario reconoce que la información que posee esta fuera de fecha. El formato recomendado es `yyyymmddnn` (2006022701).
- TTL
 - El Time To Live es el tiempo que permanecerá la información de esa consulta en el cache del name server, de esta manera si se le hace la consulta nuevamente puede contestar de una manera mas rápida. (segundos)