Servicios de directorio de Internet

Fernando Gont
UTN/FRH, Argentina

Congreso Internacional de Ingeniería en Computación
23 al 26 de septiembre de 2008, Ixtlahuaca, Mexico

Breve presentación

- Realizo trabajos para el Centre for the Protection of National Infrastructure (CPNI) del Reino Unido, en el área de seguridad en protocolos de comunicaciones.
- Soy miembro del Centro de Estudios de Informática (CEDI) de la Universidad Tecnológica Nacional/Facultad Regional Haedo (UTN/FRH) de Argentina en el área de ingeniería de Internet, con participación activa en la Internet Engineering Task Force (IETF).
- Como resultado de estas actividades he publicado una variedad de trabajos en el área de protocolos de comunicaciones.
- Para mas información: http://www.gont.com.ar

Agenda

- El Servicio de Nombres de Dominio
  - Teoría de funcionamiento
  - Ejemplos
  - Acceso al mismo mediante la herramienta dig
- El Servicio Whois
  - Teoría de funcionamiento
  - Ejemplos
  - Acceso al mismo mediante la herramienta telnet

El Servicio de Nombres de Dominio (DNS)

Breve historia del DNS

- Una de las tantas diferencias entre las máquinas y los seres humanos tiene que ver con el tipo de información que uno y otro pueden manejar con mayor confidencia.
- Los maquinas pueden manejar perfectamente valores númericos (por ej., direcciones IP), mientras que al hombre le es mas conveniente utilizar nombres mas descriptivos (por ej., nombres como www.google.com).
- Es por ello que surgió la necesidad de proveer algún mecanismo que, a partir de un nombre, permitiera obtener su dirección IP correspondiente.
- Originalmente, se mantenía un único archivo global (“HOSTS.TXT”), que debía ser modificado cada vez que algún sistema de la Internet cambiaba su configuración, así como también debía ser “descargado” por cada sistema de la red, para que dichos cambios tomaran efecto.

Breve historia del DNS

- Este mecanismo de traducción funcionó hasta mediados de los ’80, cuando la cantidad de sistemas conectados a la red era reducida.
- A medida que se comenzaron a incorporar cada vez mayor cantidad de sistemas, el archivo HOSTS.TXT se torno un mecanismo inconveniente:
  - El ancho de banda del equipo que contenía el archivo en cuestión se convertía en un cuello de botella.
  - Se debía descargar el archivo entero, por mas que solo se hubieran realizado pequeños cambios.
  - A medida que mas y mas equipos se conectaban a Internet, se empezó hacer cada vez mas difícil que la actualización de dicha base de datos (el archivo HOSTS.TXT) fuera centralizado.
- Como era de esperar, se decidió que la información necesaria para realizar la traducción entre nombres y direcciones IP estuviera almacenada en una base de datos distribuida: el DNS.

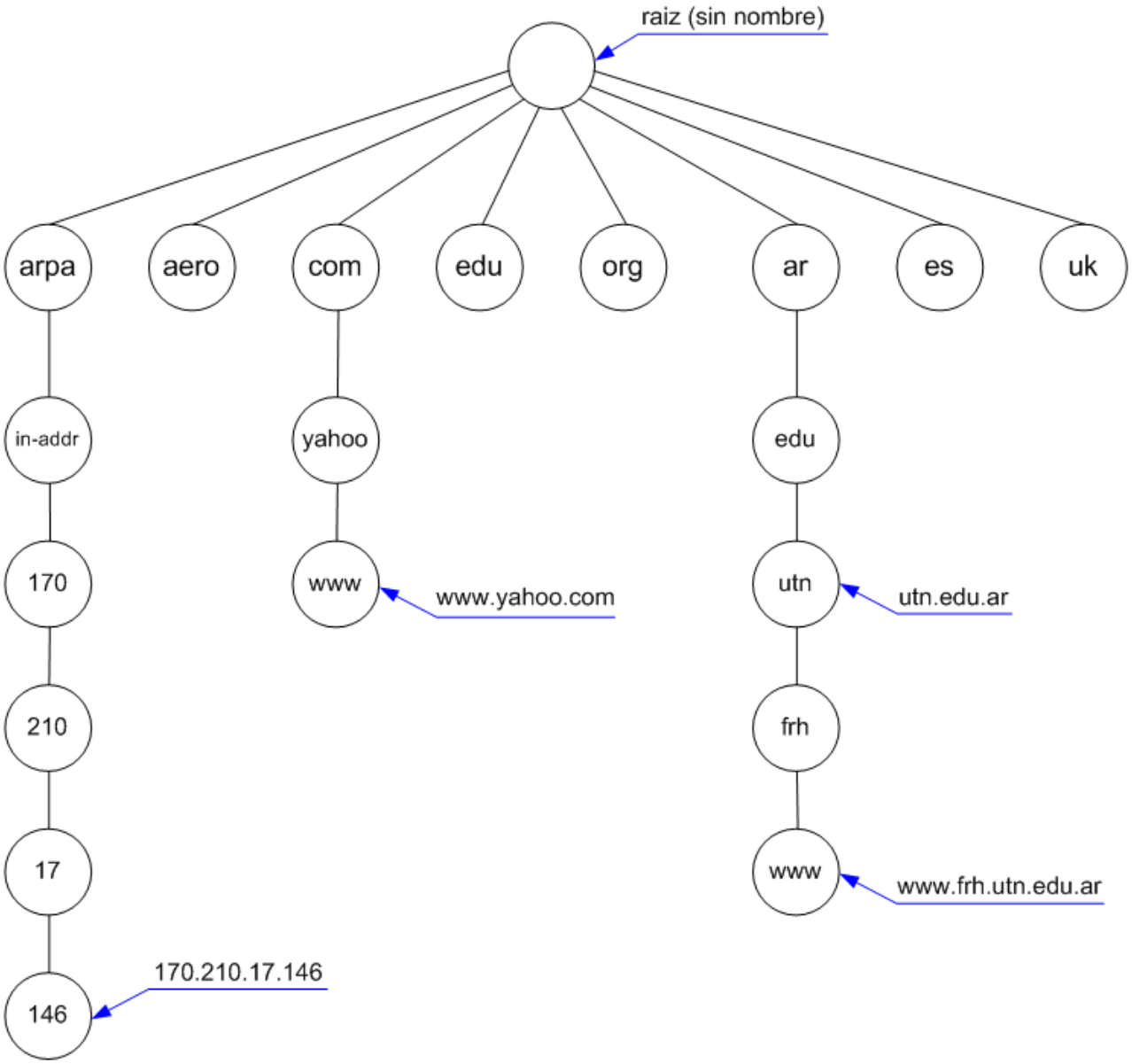
El Sistema de nombres de dominio (DNS)

- El Servicio de Nombres de Dominio (DNS) nos permite acceder a los distintos servicios de Internet mediante nombres fácilmente identificables por los seres humanos.
- Asimismo, permite obtener una variedad de información sobre nombres de dominio y direcciones IP.
- Es, por ejemplo, quien nos permite acceder al sitio web de Google mediante el nombre www.google.com, evitandonos utilizar valores tales como “74.125.95.103”
- Se trata de una base de datos distribuida:
  - No hay ningún sistema que posea el total de la información
  - Distintos sistemas se encargan de la administración de distintas partes de dicha base de datos
  - No hace falta descargar la totalidad de la información contenida en dicha base de datos para poder acceder a alguna información en particular.

Nombres de dominio

- Las “entidades” sobre las que almacena información el DNS son los “nombres de dominio” (de ahí el nombre del sistema).
- Dichos nombres de dominio tienen una estructura bien definida, de tipo jerárquico.
- Están compuestos por distintas “partes” que se se separan entré si por un punto. Por ej.,
  - www.google.com
  - www.gont.com.ar
  - www.mit.edu
- Cada “parte” componente de un nombre de dominio tendrá una importancia o significado que dependerá de la posición que dicha parte ocupe en el nombre en cuestión.
- Una misma “parte” (por ej., “www”) podrá repetirse en distintos nombres de domino, o incluso en un mismo nombre, con tal de que el **conjunto** de partes sea único.

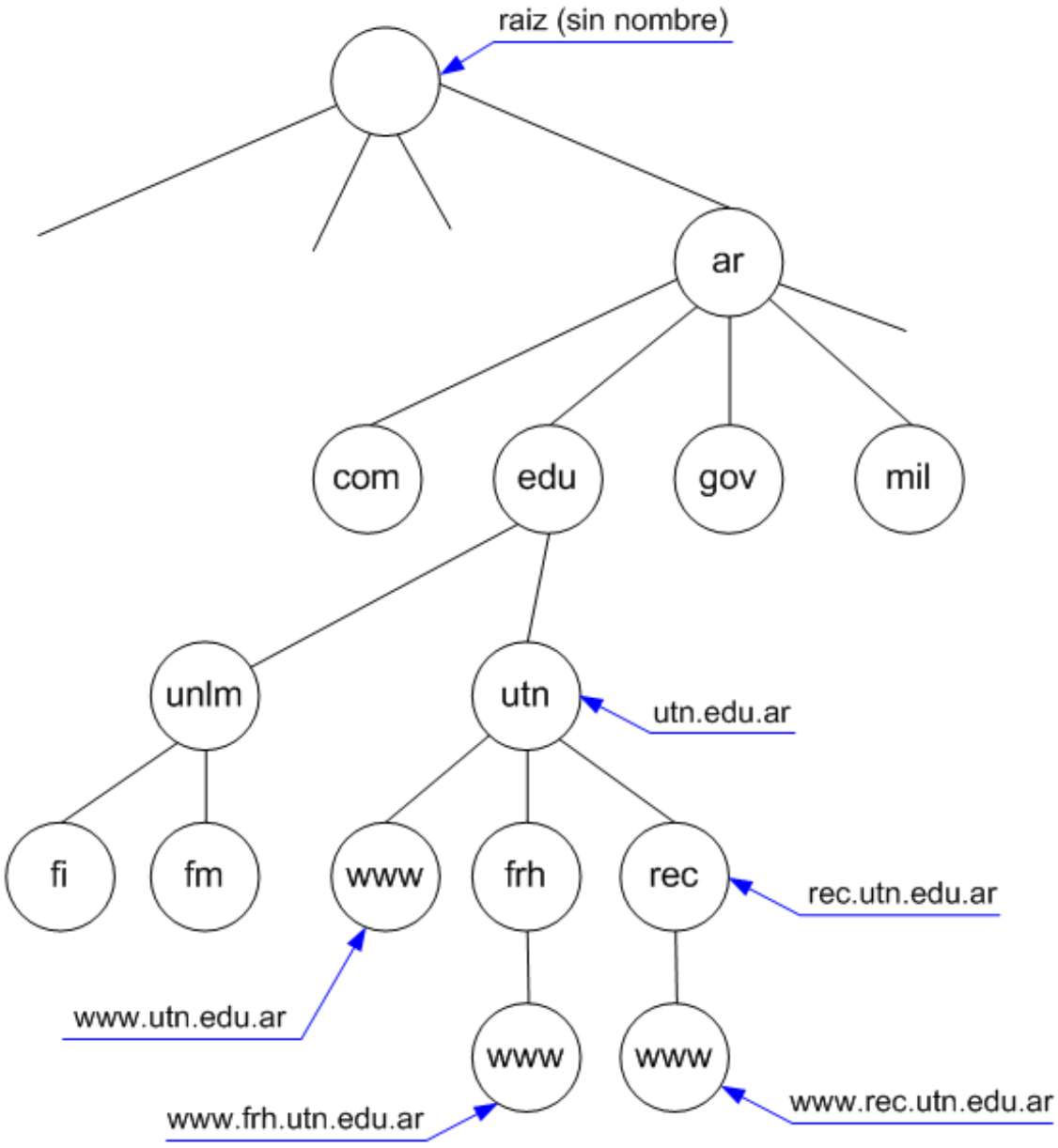
Estructura jerarquica de los nombres de dominio



Zonas

- Cada nodo define, implicitamente, una **zona**.
- Llamaremos zona al conjunto de nombres de dominio que depende de un mismo nodo.
- Ejemplos:
  - La zona raiz (“.”) está compuesta por los nombres de domino “org”, “com”, “edu”, cada uno de los códigos de países (por ej., “ar”), etc.
  - La zona “ar.” estará compuesta por los nombres “com.ar”, “org.ar”, “edu.ar”, etc.
  - A su vez, la zona “edu.ar.” estará compuesta por los nombres “utn.edu.ar”, “unlm.edu.ar.”, etc.
- En principio, cada zona podrá estar administrada por una entidad diferente, que puede incluso delegar la administración de zonas anidadas.

Ejemplo de zonas



Administración de zonas

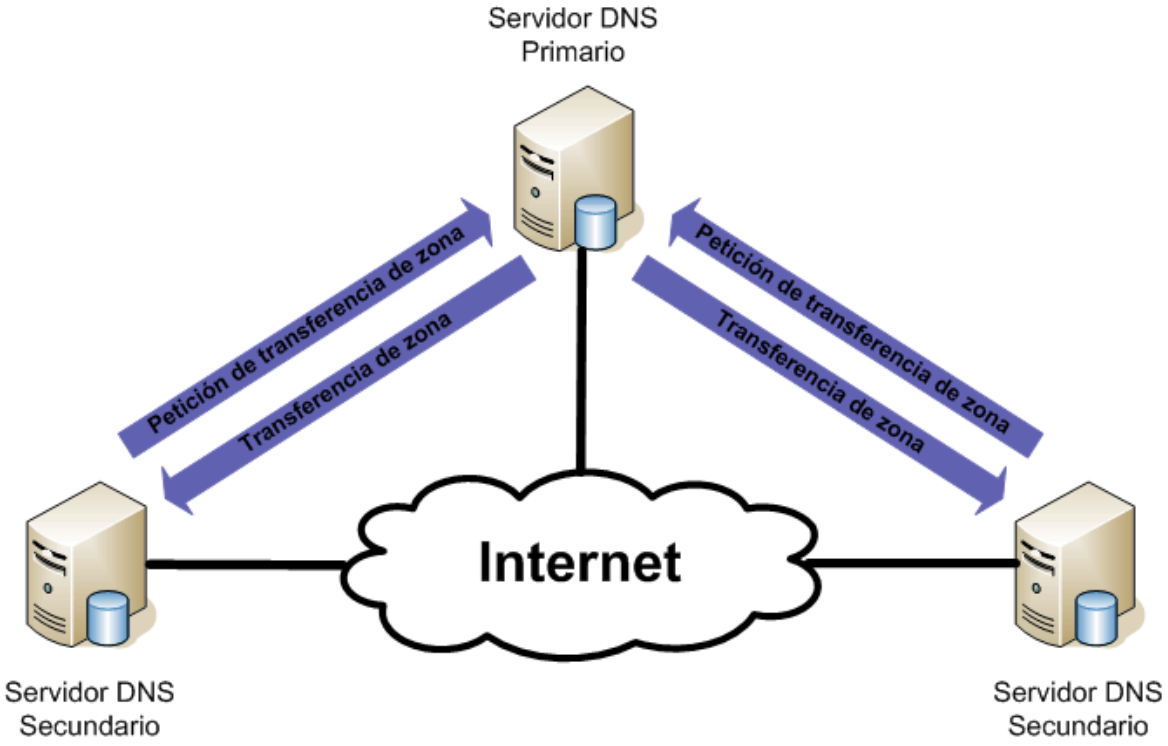
- Cada zona puede estar administrada por una entidad diferente, que puede a su vez delegar la administración de zonas “anidadas” en la misma.
- En nuestro ejemplo,
  - La zona raiz (“.”) se encuentra adminsitrada por ICANN (Internet Corporation for Assigned Names and Numbers”), quien en consecuencia administra nombres como “com.”, “edu.”, “ar.”, etc.
  - ICANN delega la administración de “ar.” a NIC Argentina, un organismo gubernamental de la República Argentina creado para tal fin. NIC Argentina administra también las zonas “com.ar.”, “edu.ar.”, etc., y delega la administración de “utn.edu.ar.” a la Universidad Tecnológica Nacional.
  - UTN delega la administración de “frh.utn.edu.ar” a la “Facultad Regional Haedo” de dicha universidad
  - Y el proceso continua…..

Servidores primarios y secundarios

- Cada zona del DNS poseerá un **servidor DNS** encargado de proveer a la comunidad la información correspondiente a los nombres de dominio pertenecientes a dicha zona.
- Dado que el funcionamiento del DNS es crucial para la operación de Internet, usualmente se utiliza un **servidor primario**, y uno o mas **servidores secundarios**, encargados de proveer redundancia.
- Los servidores secundarios se encargarán de mantener una copia actualizada de la información almacenada en el servidor primario, para poder brindar esta información a la comunidad en caso que el servidor primario fallara.

Servidores primarios y secundarios (II)

- Para tal fin contactarán al servidor primario con una frecuencia determinada (configurable) para comprobar si hubieran habido cambios en al información del primario.
- En caso de que hubieran, el servidor secundario descargará del primario toda la información correspondiente a la zona en cuestión, mediante una operación denominada “transferencia de zona”



Servidores primarios y secundarios (III)

- Normalmente los servidores secundarios se conectan en redes distintas a la del servidor primario y a la de otros servidores secundarios de la misma zona, con el fin de evitar lo que se conoce como “único punto de falla” (“single point of failure”).
- La idea es evitar que el fallo de un único equipo o sistema deje fuera de servicio a todos los servidores de una misma zona, haciendo inefectiva la “redundancia” provista por los mismos.

Registros de información

- Para cada nombre de dominio existente podrán existir una variedad de registros de información (“Resource Records”)

Nombre	Descripción	Petición	Respuesta
A	Dirección IP	●	●
NS	Servidor DNS	●	●
CNAME	Nombre canónico	●	●
PTR	Puntero a nombre de dominio	●	●
MX	Servidor de correo electrónico	●	●
AXFR	Petición de transferencia de zona	●	
ANY	Petición de todos los registros	●	

Registros A

- Cada registro “A” proporciona una dirección IP correspondiente al nombre de dominio en cuestión.
- Si un determinado nombre de dominio pudiera ser accedido mediante mas de una dirección IP, entonces dicho dominio contendría mas de un registro “A”.
- Es interesante notar las distintas direcciones IP proporcionadas por distintos registros “A” de un determinado dominio, no tienen porqué corresponder necesariamente a un mismo sistema físico.
- Ejemplo:
  - Cuando deseamos visitar el sitio www.gont.com.ar, lo que hacemos es primeramente buscar registros “A” del nombre de dominio www.google.com, para saber qué dirección IP se debe enviar nuestra petición.

Registros CNAME

- Los registros CNAME contienen un nombre de dominio, y sirven para especificar que un determinado nombre de dominio es en realidad un alias de otro dominio.
- Se utilizan con frecuencia para evitar tener que repetir la configuración de un sistema, innecesariamente.
  - Ejemplo:
    - Supongamos que el nombre “smtp.gont.com.ar” tiene 5 registros “A”
    - Si ahora quiero que el nombre pop3.gont.com.ar sea accesible por las mismas direcciones IP que en el caso anterior, podría:
      - repetir la configuración del caso anterior, para el nombre “pop3.gont.com.ar”
      - Definir un registro CNAME apra el nombre “pop3.gont.com.ar”, cuyo contenido sea “smtp.gont.com.ar”

Registros AXFR

- Estos “registros” se utilizan Únicamente en **peticiones** DNS, para indicar que se desea realizar una “transferencia de zona”
- En la respuesta a dicha petición no se incluyen registros “AXFR”, sino que se incluyen todos los registros disponibles para todos los nombres de dominio de la zona en cuestión.
- El tipo “AXFR”, al ser especificado en una petición DNS, se puede interpretar como “dame todos los registros de todos los nombres de dominio correspondiente a ésta zona”.

Registro ANY

- Estos “registros” se utilizan Únicamente en **peticiones** DNS, para indicar que se desean recibir todos los registros correspondientes a un determinado nombre de dominio.
- En la respuesta a dicha petición no se incluyen registros “ANY”, sino que se incluyen todos los registros disponibles para el nombre de dominio en cuestión.
- El tipo “ANY”, al ser especificado en una petición DNS, se puede interpretar como “dame todos los registros del siguiente nombre de dominio”.

Registros NS

- Los registros NS contienen un nombre de dominio, y se utilizan para especificar un servidor autoritativo (ó “responsable”) de la zona en cuestión.
- Si dicha información de la zona en cuestión estuviera siendo brindada por mas de un servidor DNS, entonces existirán varios registros “NS”.
- A modo de ejemplo, si quisieramos averiguar que servidores tienen la información de la zona “frh.utn.edu.ar”, tendríamos que buscar registros “NS” del nombre “frh.utn.edu.ar”

Registros MX

- Los registros MX permiten especificar él o los sistemas que se encargarán de recibir el correo electrónico para un determinado nombre de dominio.
- Contienen un nombre de dominio (el del encargado de recibir el correo electrónico) junto con un valor numérico que establece la prioridad del sistema en cuestión.
- Si mas de un “sistema” se encargara de recibir el correo electrónico para un determinado nombre de dominio, dicho dominio tendría mas de un registro MX.

Registros PTR

- Estos registros contienen un nombre de dominio, y son utilizados para la resolución inversa de dirección IP en nombre de dominio.

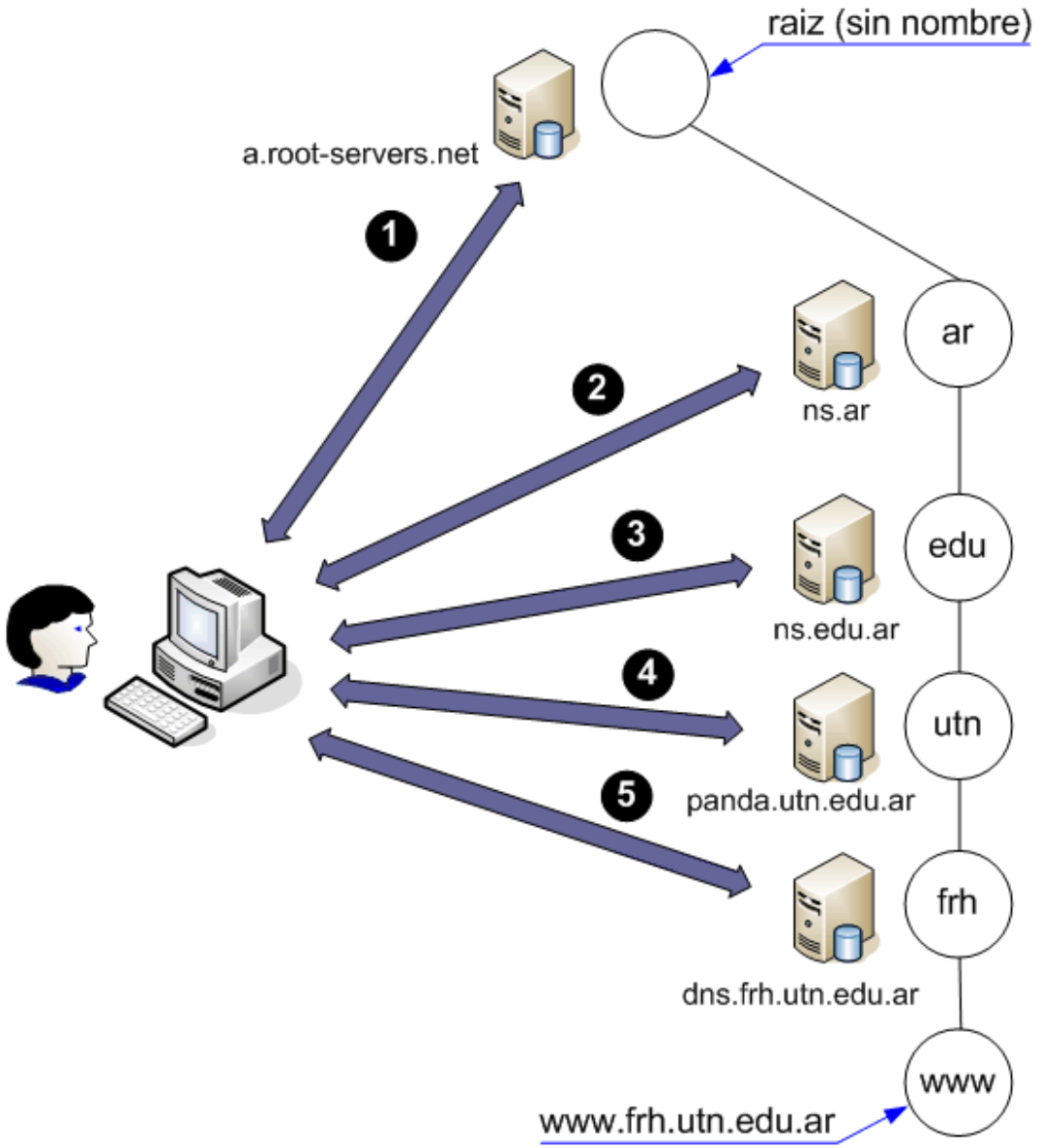
Tiempo de Vida (TTL)

- Aparte de la información específica mencionada anteriormente, junto con cada registro de información se incluye un valor denominado “TTL” (“Time To Live”, ó “Tiempo de Vida”).
- Este valor especifica el tiempo en segundos durante el cual la información en cuestión puede considerarse válida.
- Así cuando un sistema realiza una petición, podrá almacenar los resultados correspondientes, para evitar tener que volver a realizar la petición en caso de volver a necesitar dicha información.
- Sin embargo, cumplido el plazo estipulado por el campo TTL de un registro, dicho registro deberá ser descartado.

El proceso de resolución

- El proceso de resolución es un proceso iterativo.
- Se comenzará interrogando a alguno de los servidores responsables de la zona raíz, quien nos brindará el nombre de un servidor DNS que nos dará información mas precisa acerca de la información buscada.
- Este proceso se repetirá sucesivamente, hasta que logremos interrogar a aquél servidor DNS que pueda brindar exactamente la información buscada.

El proceso de resolución (II)

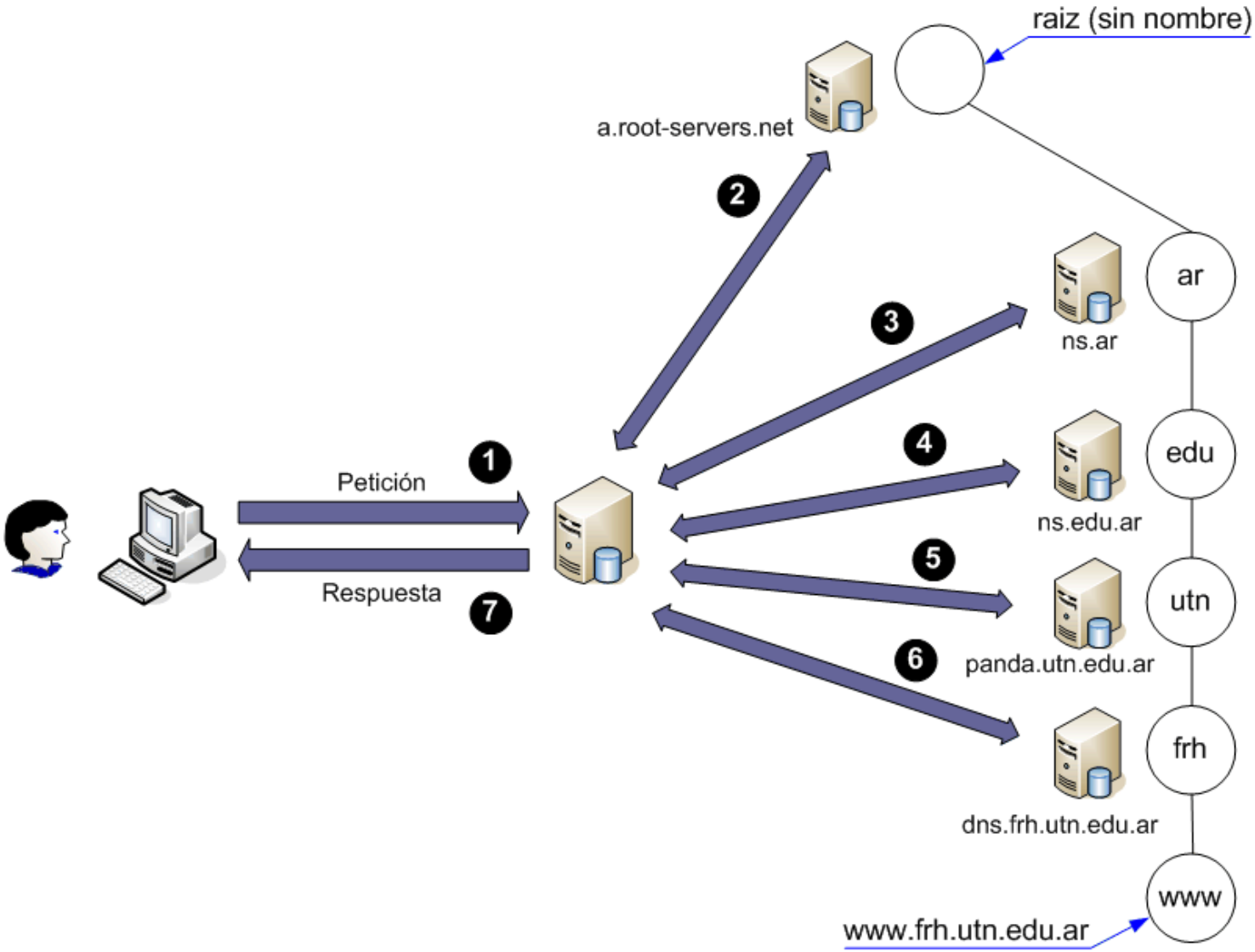


- Ejemplo de resolución del nombre de dominio www.frh.utn.edu.ar

Peticiones recursivas y no recursivas

- En el ejemplo anteriormente visto, la resolución de un nombre de dominio implica un cierto trabajo por parte del “usuario” del DNS, consistente en interrogar a una variedad de servidores DNS, hasta conseguir la información buscada.
- Se dice que cada una de las peticiones enviadas en dicho ejemplo son con “recursividad no deseada”.
- Sin embargo, existe una manera de simplificar el trabajo del cliente, mediante lo que se conoce como “peticiones con recursividad deseada”.
- Dicha modalidad consistirá en tener un servidor DNS intermediario, a quien el cliente le enviará sus peticiones.
- Y será entonces este servidor DNS quien tendrá la responsabilidad de realizar e proceso iterativo descripto anteriormente.
- Este “servidor intermediario” suele ser compartido por una variedad de usuarios.

Peticiones con “recursividad deseada”



Servidores DNS de tipo caché

- El proceso de resolución de nombres es un proceso costoso:
  - Utiliza recursos de comunicaciones
  - Utiliza recursos de procesamiento de los sistemas involucrados
  - Requiere de un determinado tiempo para completarse, que puede volverse indeseable
- Con el fin de mitigar estos problemas, el “servidor DNS intermediario” almacenará todas aquellos registros de información que haya obtenido hasta el momento (teniendo en cuenta el TTL de cada registro). Por este motivo se lo denominará “servidor DNS caché” (ó “caching DNS server”)
- De este modo, si la información solicitada por un usuario/cliente se encontrara almacenada en dicho servidor, se podría

Respuestas autoritativas y no autoritativas

- Al realizarse una petición, la misma podría ser respondida por algún servidor autoritativo (“responsable”) de la zona en cuestión, o bien por algún servidor que simplemente tenía almacenada (“cacheada”) la respuesta a nuestra petición.
- En el primero de los casos, se dice que la respuesta es “autoritativa”
- En el segundo, se dice que la respuesta es “no autoritativa”.

Resolución inversa

- Para la resolución inversa de direcciones IP en nombres de dominio se utilizarán nombres de dominio finalizados en “in-addr.arpa”
- Básicamente, dada una dirección IP “*w*.*x*.*y*.*z*” lo que haremos será realizar una petición de registros “PTR” del dominio “*z*.*y*.*x*.*w*.in-addr.arpa.”
- Dichas peticiones se realizarán exactamente de la misma manera que para resolver nombres de dominio en direcciones IP, ya sea realizando el proceso iterativo anteriormente visto, o bien delegando la responsabilidad de dicho proceso a un servidor DNS de tipo cache.
- Ejemplo:
  - Para obtener el nombre de dominio correspondiente a la dirección IP 170.210.17.150, deberemos buscar registros PTR del dominio “150.17.210.170.in-addr.arpa.”

Uso de la herramienta `dig` para acceder al DNS

La herramienta `dig`

- La herramienta dig es una herramienta libre, que se distribuye usualmente con el softwate BIND (Berkeley Internet Name Domain).
- La misma nos permite interactuar directamente con el DNS, ya sea para poder obtener información nombres de dominio y direcciones IP.
- Su sintaxis es:

`dig` [*@server*] ***domain*** [*query-type*] [*query-class*] [*+qoption*] [*-digoption*]

Resolviendo nombres

- Para obtener la dirección IP del dominio www.gont.com.ar, ejecutaremos dig de la siguiente manera
  - dig www.gont.com.ar A
- Las características de esta petición serán:
  - Petición con recursividad deseada (por defecto)
  - Query-type: “A” (el especificado)
  - Query-class: “IN” (por defecto)
  - Servidor DNS caché: El configurado en el sistema (ver */etc/resolv.conf*)

Posible respuesta obtenida

```
1:  ; <<>> DiG 9.2.3 <<>> www.gont.com.ar
2:  ;; global options:  printcmd
3:  ;; Got answer:
4:  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3235
5:  ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4
6:
7:  ;; QUESTION SECTION:
8:  ;www.gont.com.ar.              IN      A
9:
10:  ;; ANSWER SECTION:
11:  www.gont.com.ar.       2400    IN      A       170.210.17.146
12:
13:  ;; AUTHORITY SECTION:
14:  gont.com.ar.           86400   IN      NS      ns1.mydomain.com.
15:  gont.com.ar.           86400   IN      NS      ns2.mydomain.com.
16:  gont.com.ar.           86400   IN      NS      ns3.mydomain.com.
17:  gont.com.ar.           86400   IN      NS      ns4.mydomain.com.
18:
19:  ;; ADDITIONAL SECTION:
20:  ns1.mydomain.com.      52902   IN      A       64.94.117.195
21:  ns2.mydomain.com.      52902   IN      A       216.52.121.233
22:  ns3.mydomain.com.      52902   IN      A       66.150.161.130
23:  ns4.mydomain.com.      52902   IN      A       63.251.83.74
24:
25:  ;; Query time: 2330 msec
26:  ;; SERVER: 170.210.17.150#53(170.210.17.150)
27:  ;; WHEN: Tue Sep  6 13:55:30 2005
28:  ;; MSG SIZE  rcvd: 197
```

Y si reenviáramos la petición?

```
 ; <<>> DiG 9.2.3 <<>> www.gont.com.ar
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56223
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.gont.com.ar.               IN      A

;; ANSWER SECTION:
www.gont.com.ar.        2337    IN      A       170.210.17.146

;; AUTHORITY SECTION:
gont.com.ar.            86337   IN      NS      ns2.mydomain.com.
gont.com.ar.            86337   IN      NS      ns3.mydomain.com.
gont.com.ar.            86337   IN      NS      ns4.mydomain.com.
gont.com.ar.            86337   IN      NS      ns1.mydomain.com.

;; ADDITIONAL SECTION:
ns1.mydomain.com.       52839   IN      A       64.94.117.195
ns2.mydomain.com.       52839   IN      A       216.52.121.233
ns3.mydomain.com.       52839   IN      A       66.150.161.130
ns4.mydomain.com.       52839   IN      A       63.251.83.74

;; Query time: 2 msec
;; SERVER: 170.210.17.150#53(170.210.17.150)
;; WHEN: Tue Sep  6 13:56:33 2005
;; MSG SIZE  rcvd: 197
```

Resolución con “recursividad no deseda”

- Podrámos obtener la misma información que en el ejemplo anterior, realizando nosotros mismos el proceso iterativo que habíamos descripto.
- Para tal fin, enviaremos nuestra petición con “recursividad no deseada” comenzando por alguno de los servidores raíz, y repitiendo el proceso hasta lograr interrogar al servidor autoritativo de la zona gont.com.ar
- Para tal fin, ejecutaremos la herramienta dig de la siguiente manera:
  - `dig @a.root-servers.net www.gont.com.ar +norecurse`

Respuesta de a.root-servers.net

```
; <<>> DiG 9.2.3 <<>> @a.root-servers.net www.gont.com.ar +norecurse
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46248
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 9

;; QUESTION SECTION:
;www.gont.com.ar.               IN      A

;; AUTHORITY SECTION:
ar.                     172800  IN      NS      ATHEA.ar.
ar.                     172800  IN      NS      CTINA.ar.
ar.                     172800  IN      NS      MERAPI.SWITCH.CH.
ar.                     172800  IN      NS      NS.UU.NET.
ar.                     172800  IN      NS      UUCP-GW-1.PA.DEC.COM.
ar.                     172800  IN      NS      UUCP-GW-2.PA.DEC.COM.
ar.                     172800  IN      NS      NS1.RETINA.ar.
ar.                     172800  IN      NS      NS-AR.RIPE.NET.

;; ADDITIONAL SECTION:
ATHEA.ar.               172800  IN      A       200.16.98.2
CTINA.ar.               172800  IN      A       200.16.97.17
MERAPI.SWITCH.CH.       172800  IN      AAAA    2001:620::5
MERAPI.SWITCH.CH.       172800  IN      A       130.59.211.10
NS.UU.NET.              172800  IN      A       137.39.1.3
UUCP-GW-1.PA.DEC.COM.   172800  IN      A       204.123.2.18
UUCP-GW-2.PA.DEC.COM.   172800  IN      A       204.123.2.19
NS1.RETINA.ar.          172800  IN      A       200.10.202.3
NS-AR.RIPE.NET.         172800  IN      A       193.0.12.11

;; Query time: 238 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net)
;; WHEN: Tue Sep  6 16:23:01 2005
;; MSG SIZE  rcvd: 390
```

Respuesta de athea.ar

- `dig @athea.ar www.gont.com.ar A +norecurse`

```
; <<>> DiG 9.2.3 <<>> @athea.ar www.gont.com.ar +norecurse
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10729
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;www.gont.com.ar.            IN      A

;; AUTHORITY SECTION:
gont.com.ar.        14400   IN      NS      ns1.mydomain.com.
gont.com.ar.        14400   IN      NS      ns2.mydomain.com.
gont.com.ar.        14400   IN      NS      ns3.mydomain.com.
gont.com.ar.        14400   IN      NS      ns4.mydomain.com.

;; Query time: 271 msec
;; SERVER: 200.16.98.2#53(athea.ar)
;; WHEN: Tue Sep  6 16:24:20 2005
;; MSG SIZE  rcvd: 117
```

Respuesta de ns1.mydomain.com

```
; <<>> DiG 9.2.3 <<>> @ns1.mydomain.com www.gont.com.ar
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11811
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.gont.com.ar.            IN      A

;; ANSWER SECTION:
www.gont.com.ar.       2400    IN      A       170.210.17.146

;; AUTHORITY SECTION:
gont.com.ar.           86400   IN      NS      ns1.mydomain.com.
gont.com.ar.           86400   IN      NS      ns2.mydomain.com.
gont.com.ar.           86400   IN      NS      ns3.mydomain.com.
gont.com.ar.           86400   IN      NS      ns4.mydomain.com.

;; ADDITIONAL SECTION:
ns1.mydomain.com.      1800    IN      A       64.94.117.195
ns2.mydomain.com.      1800    IN      A       216.52.121.233
ns3.mydomain.com.      1800    IN      A       66.150.161.130
ns4.mydomain.com.      1800    IN      A       63.251.83.74

;; Query time: 29 msec
;; SERVER: 64.94.117.195#53(ns1.mydomain.com)
;; WHEN: Tue Sep  6 16:25:01 2005
;; MSG SIZE  rcvd: 197
```

Resolviendo direcciones IP en nombres

- `dig 146.17.210.170.in-addr.arpa ptr`

```
; <<>> DiG 9.2.3 <<>> 146.17.210.170.in-addr.arpa PTR
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11596
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;146.17.210.170.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
146.17.210.170.in-addr.arpa. 21600 IN   PTR     server.frh.utn.edu.ar.

;; AUTHORITY SECTION:
17.210.170.in-addr.arpa. 21600  IN      NS      dns.frh.utn.edu.ar.

;; ADDITIONAL SECTION:
dns.frh.utn.edu.ar.     21600   IN      A       170.210.17.150

;; Query time: 6 msec
;; SERVER: 170.210.17.150#53(170.210.17.150)
;; WHEN: Tue Sep  6 16:21:41 2005
;; MSG SIZE  rcvd: 114
```

Servidores de correo electrónico

- `dig gont.com.ar mx`

```
; <<>> DiG 9.2.3 <<>> gont.com.ar MX
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53521
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
;gont.com.ar.                IN      MX

;; ANSWER SECTION:
gont.com.ar.          2400    IN      MX      10 m1.dnsix.com.
gont.com.ar.          2400    IN      MX      5 server.frh.utn.edu.ar.

;; AUTHORITY SECTION:
gont.com.ar.          86085   IN      NS      ns4.mydomain.com.
gont.com.ar.          86085   IN      NS      ns1.mydomain.com.
gont.com.ar.          86085   IN      NS      ns2.mydomain.com.
gont.com.ar.          86085   IN      NS      ns3.mydomain.com.

;; ADDITIONAL SECTION:
server.frh.utn.edu.ar.  21600   IN      A       170.210.17.146
ns1.mydomain.com.       52587   IN      A       64.94.117.195
ns2.mydomain.com.       52587   IN      A       216.52.121.233
ns3.mydomain.com.       52587   IN      A       66.150.161.130
ns4.mydomain.com.       52587   IN      A       63.251.83.74

;; Query time: 372 msec
;; SERVER: 170.210.17.150#53(170.210.17.150)
;; WHEN: Tue Sep  6 14:00:45 2005
;; MSG SIZE  rcvd: 253
```

Información de una zona

- Para poder obtener información de una zona, deberemos peticionar el registro “SOA” correspondiente a dicha zona.
- El formato del registro SOA será:

```
dominio             ttl    IN      SOA     servidor_primario e-mail_administrador
                                           serial
                                           REFRESH
                                           RETRY
                                           EXPIRE
                                           MINIMUM
```

Información de la zona gont.com.ar

- `dig gont.com.ar soa`

```
; <<>> DiG 9.2.3 <<>> gont.com.ar SOA
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;gont.com.ar.                IN      SOA

;; ANSWER SECTION:
gont.com.ar.          86400   IN      SOA     ns1.mydomain.com.
                              hostmaster.gont.com.ar.
                              2005090704 16384 2048 1048576 2560

;; AUTHORITY SECTION:
gont.com.ar.          68229   IN      NS      ns3.mydomain.com.
gont.com.ar.          68229   IN      NS      ns4.mydomain.com.
gont.com.ar.          68229   IN      NS      ns1.mydomain.com.
gont.com.ar.          68229   IN      NS      ns2.mydomain.com.

;; ADDITIONAL SECTION:
ns1.mydomain.com.     34731   IN      A       64.94.117.195
ns2.mydomain.com.     34731   IN      A       216.52.121.233
ns3.mydomain.com.     34731   IN      A       66.150.161.130
ns4.mydomain.com.     34731   IN      A       63.251.83.74

;; Query time: 239 msec
;; SERVER: 170.210.17.150#53(170.210.17.150)
;; WHEN: Tue Sep  6 18:58:22 2005
;; MSG SIZE  rcvd: 224
```

Manos a la obra!

1. Cuáles son los servidores DNS de la zona “gont.com.ar”?
2. Existe redundancia?
3. Cuál es la dirección IP del servidor web www.gont.com.ar
4. Que sistemas reciben el correo de gont.com.ar?
5. Con que dirección de correo debería contactar al administrador de la zona “gont.com.ar”?
6. Cuales son los parámetros de la zona gont.com.ar? (en lo que respecta a los servidores secundarios)
7. Que contiene el registro “TXT” del nombre de dominio “fernando.gont.com.ar”?

Manos a la obra! (II)

- Cuáles son los servidores de nombres responsables de la zona ceui.com.mx?
- Cuál es la dirección IP del servidor web www.ceui.com.mx?
- Que sistemas reciben el correo de las cuentas @ceui.com.mx?

Manos a la obra! (III)

1. Cuáles son los servidores DNS de la zona “yahoo.com”?
2. Cuál es la dirección IP del servidor web www.yahoo.com?
3. Que sistemas reciben el correo de yahoo.com?
4. Con que dirección de correo debería contactar al administrador de la zona “yahoo.com”?
5. Cuales son los parámetros de la zona yahoo.com? (en lo que respecta a los servidores secundarios)

El servicio whois

Introducción al servicio whois

- A menudo suele necesitarse obtener información sobre el registro de nombres de dominio o sobre la asignación de direcciones IP.
- Por ejemplo, si una de mis redes estuviera siendo atacada por la dirección IP “170.210.17.150”, podría interesarme identificar a la organización a quien dicha dirección IP le fue asignada, para contactar al responsable para que “tome cartas en el asunto”.
- Asimismo, podría interesarme saber quien registró el dominio www.ceui.com, para hacerle una oferta de compra, etc.
- Todo este tipo de información se puede acceder mediante loq eu se conoce como el servicio whois.
- El servicio whoisestá especificado por el RFC 3912 de la IETF, y básicamente proporciona una interfaz de acceso a la información mencionada.

Acceso al servicio whois

- Se puede acceder mediante dos maneras distintas:
  - telnet *servidorwhois* whois
  - jwhois *dominio*
- La primera opción require que conozcamos los distintos servidores whois existentes.
- La segunda de las opciones accede al servicio utilizando una herarmineta especifica, que incluye una base da datos