



RESOLUCIÓN DE NOMBRES

Nombres de dominio

DNS

Utilidades DNS

DNS spoofing

Resolución de nombres

Nombre de dominio (domain name)

Un **dominio** es una colección de computadoras que pueden ser accedidas usando un nombre en común.

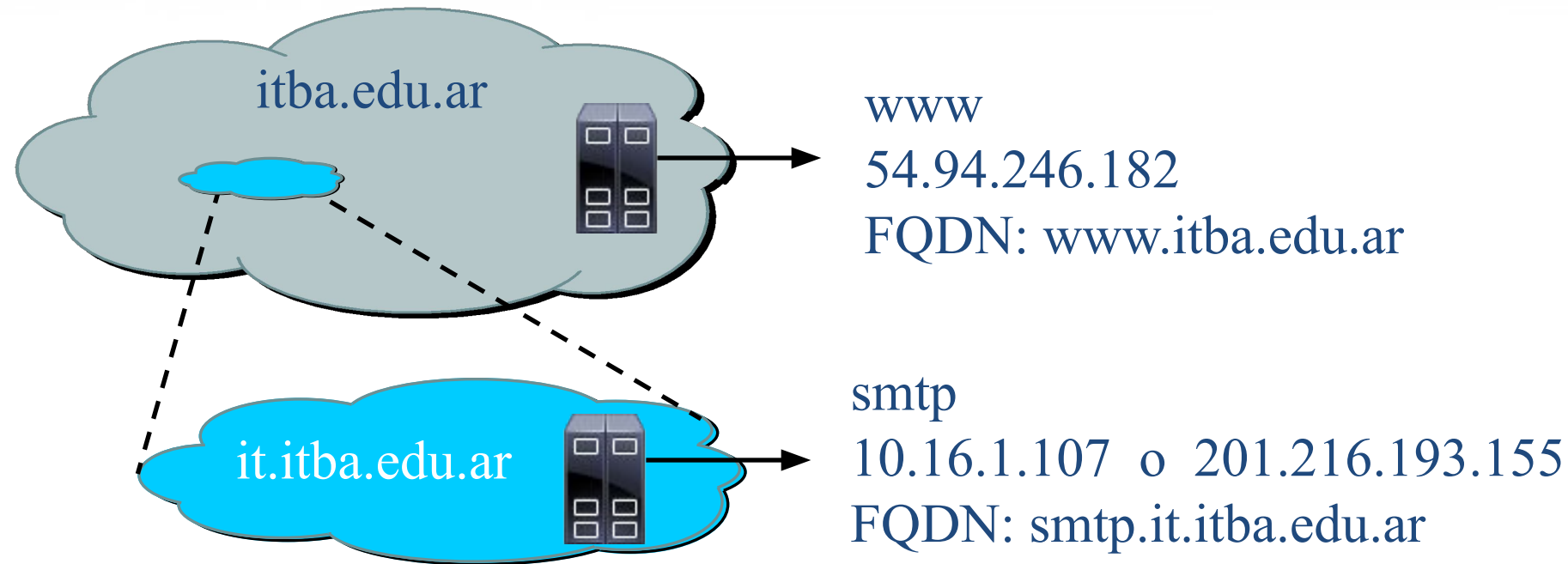
Un **nombre de dominio** hace referencia al nombre de múltiples hosts que son referenciados colectivamente (itba.edu.ar, ibm.com, etc.)

Los dominios tienen distintos niveles, siendo **.com** el dominio *top-level* más conocido de ellos. Ver RFC 1591 y RFC 3071.

Resolución de nombres

Dentro de un *top-level domain*, una organización tiene su propio dominio o dominios. A su vez dentro del dominio puede haber sub-dominios. Y cada host tiene su nombre propio (*hostname*).

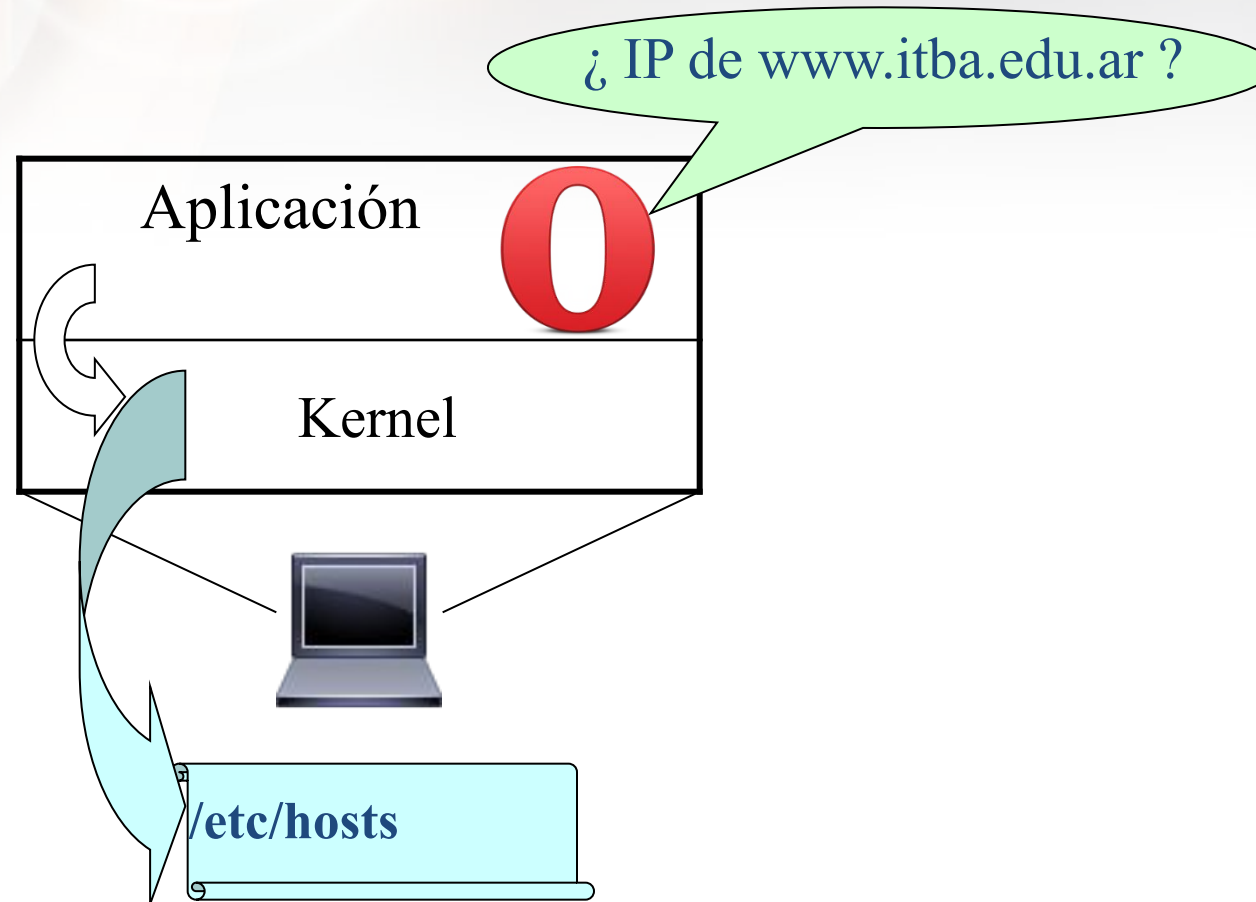
Uniando el nombre del host con el dominio al cual pertenece se forma el **FQDN** (*fully qualified domain name*).



Resolución de nombres

¿Cómo se obtiene, dado un FQDN, su número de IP?

Opción 1:



Archivo /etc/hosts

- ◆ Contiene una línea por cada número de IP y el o los nombres asociados a dicho IP.
- ◆ Por defecto se consulta primero este archivo y luego DNS
- ◆ Se puede cambiar el orden en /etc/nsswitch.conf

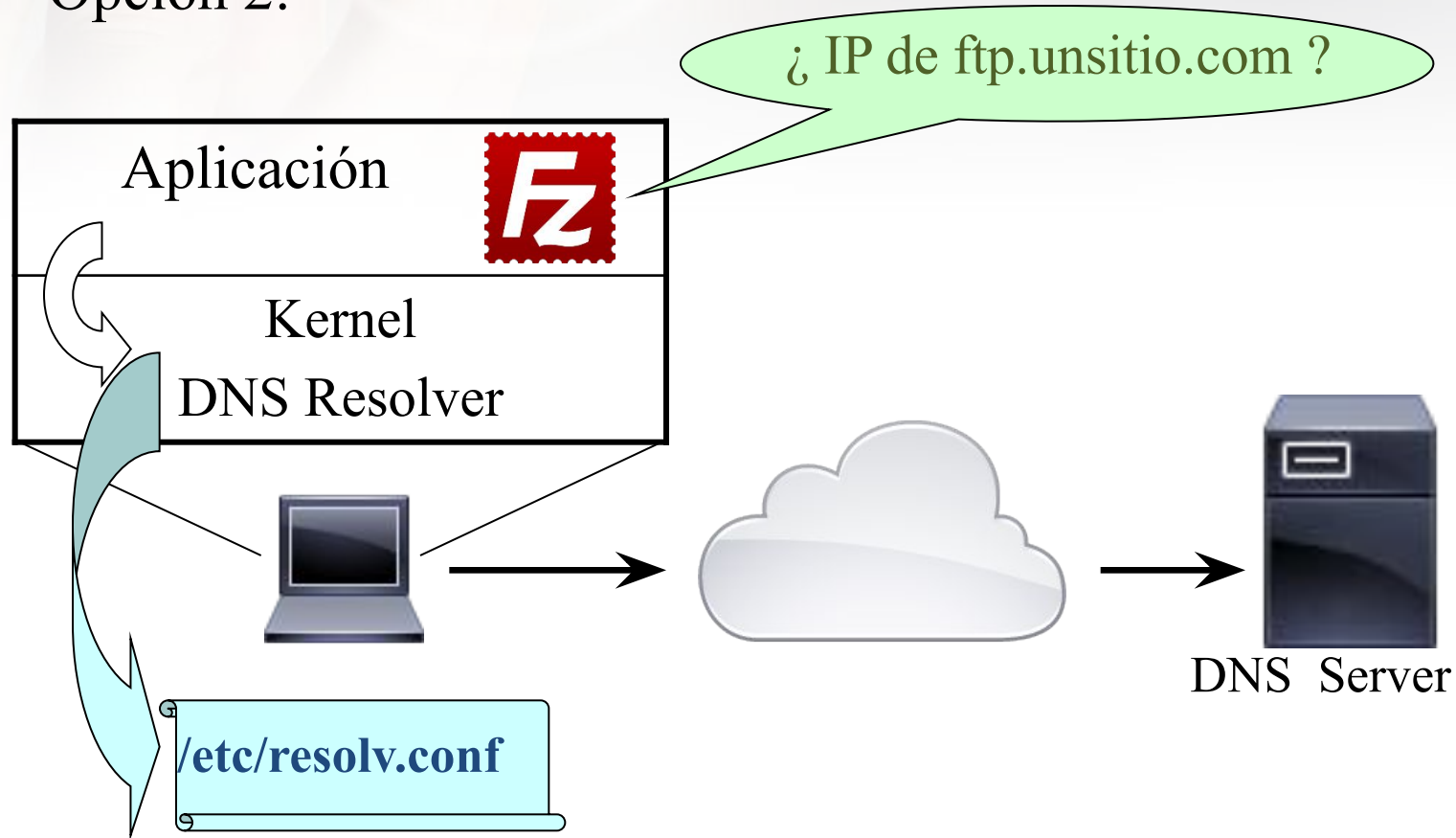
```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1    localhost mihost mihost.com
::1          localhost
192.168.2.2  printserver
127.0.0.1    pagina12.com.ar
127.0.0.1    clarin.com

# End of hosts.
```

Resolución de nombres

¿Cómo se obtiene, dado un FQDN, su número de IP?

Opción 2:



Resolución de nombres

Las opciones de configuración de **/etc/resolv.conf** son:

nameserver *direcciones*

Números IP de los servidores de nombres que consultará el resolver (hasta 3). Si no hay ningún nameserver utilizará al propio host como servidor de nombres.

domain *nombre*

Dominio local por defecto. El resolver agrega este nombre a todo hostname que no contenga un punto antes de resolverlo.

search *dominios*

Similar al anterior pero pueden ser varios dominios (no se usan ambas opciones en simultáneo)

Resolución de nombres

sortlist *red[/mascara]*

En caso de recibir múltiples direcciones IP para un nombre, reordena las direcciones en base a las redes listadas en esta opción.

options *opción*

Usada para seteos opcionales. Las posibles opciones son:

- debug
- ndots:*n*
- timeout:*n*
- attempts:*n*
- rotate
- no-check-names
- inet6

Resolución de nombres

Ejemplo de `/etc/resolv.conf` del host 192.168.2.20

```
domain    itba.edu.ar
nameserver 192.168.2.1
nameserver 8.8.8.8
nameserver 200.49.159.69
```

Linux incluye las utilidades **dig** y **host** para resolver nombres, ya sea para obtener el IP en base a un nombre o el nombre en base a un IP (*reverse DNS*).

Resolución de nombres

Por defecto se consulta primero el archivo `/etc/hosts` y luego –de ser necesario– al DNS resolver. Esto puede cambiarse editando el archivo `/etc/host.conf`, el que típicamente contiene una sola línea

```
order hosts, bind
```

En caso de querer que se consulte siempre al DNS resolver sólo hay que cambiar el orden, como el ejemplo siguiente:

```
order bind, hosts
```

Para más opciones consultar *man host.conf*

Un host mantiene en su cache los nombres que ha podido resolver

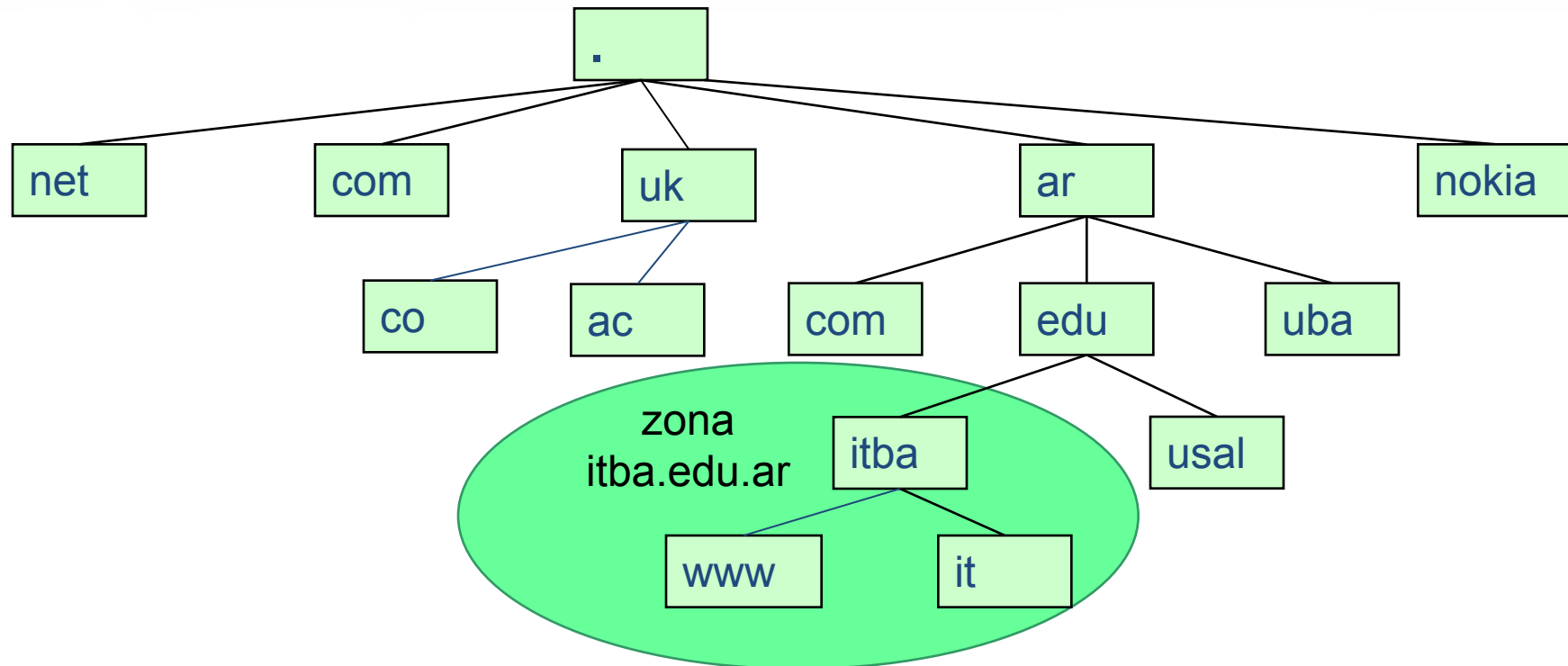
DNS

Algunos nombres de dominio a resolver se pueden encontrar en /etc/hosts, pero en la mayoría de los casos deberán ser resueltos preguntando a un **servidor DNS**.

- Base de datos distribuida implementada en una jerarquía de servidores de nombre
- Protocolo de aplicación que permite consultar dicha base

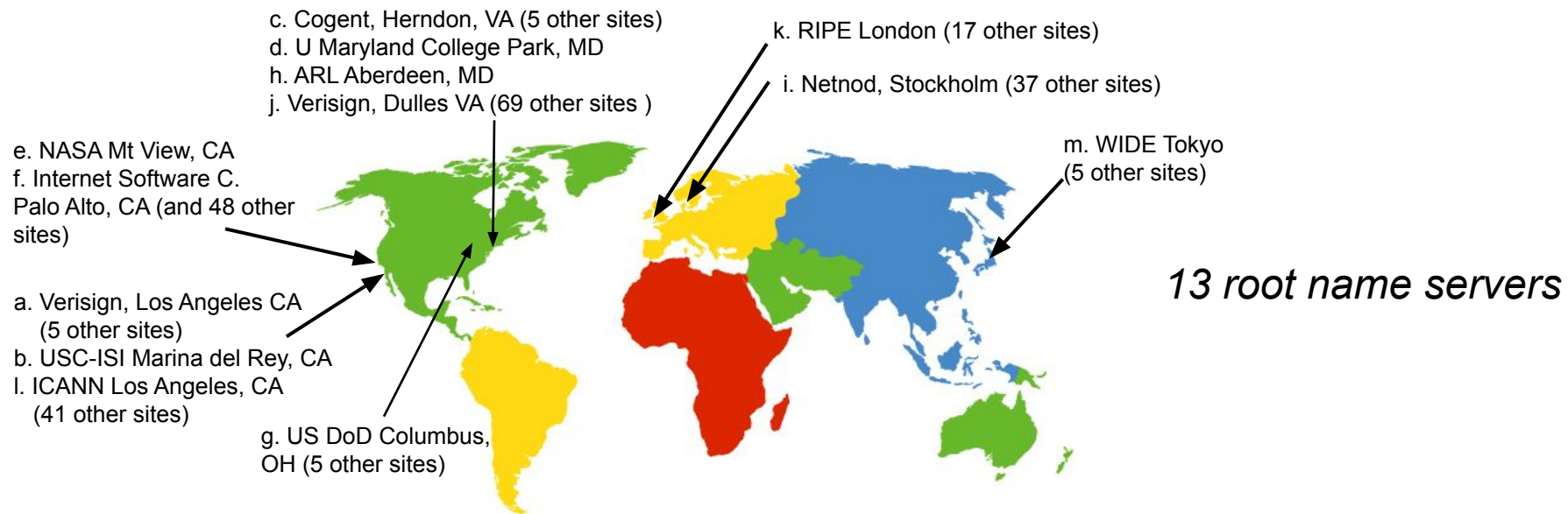
DNS

DNS es un sistema jerárquico distribuido para traducir nombres de hosts a direcciones IP. La información en DNS puede ser vista como un árbol invertido donde la raíz hace referencia a servidores de nombres raíz (*root name servers*).



DNS: root name servers

- usados cuando el servidor de nombres local no puede resolver un nombre
- root name server:
 - contacta name server autorizado si no conoce la respuesta
 - almacena
 - retorna respuesta al servidor de nombres local



TLD, servidores autorizados

top-level domain (TLD) servers:

- responsables de com, org, net, edu, aero, jobs, museums, y todos los países (ar, uk, uy, tv, etc.)
- Verisign para .com TLD, Educause para .edu TLD

authoritative DNS servers:

- Cada organización mantiene su propio servidor(es) DNS
- Puede ser mantenido por la misma organización o un proveedor

Para un listado completo de TLD y sus responsables ver <https://www.iana.org/domains/root/db>

Servidor DNS local

- No necesariamente pertenecen a la jerarquía
- Cada ISP tiene uno, conocido como “default name server”
- Cuando un host realiza una consulta DNS, es enviada al servidor DNS local
 - Busca en la caché si tiene el par nombre-dirección y no caducó
 - Actúa como un proxy

Resolución de nombres

Ejemplos

```
user@server:~$ host www.dc.uba.ar
```

```
www.dc.uba.ar is an alias for www-1.dc.uba.ar.
```

```
www-1.dc.uba.ar is an alias for dc.uba.ar
```

```
dc.uba.ar has address 157.92.27.127
```

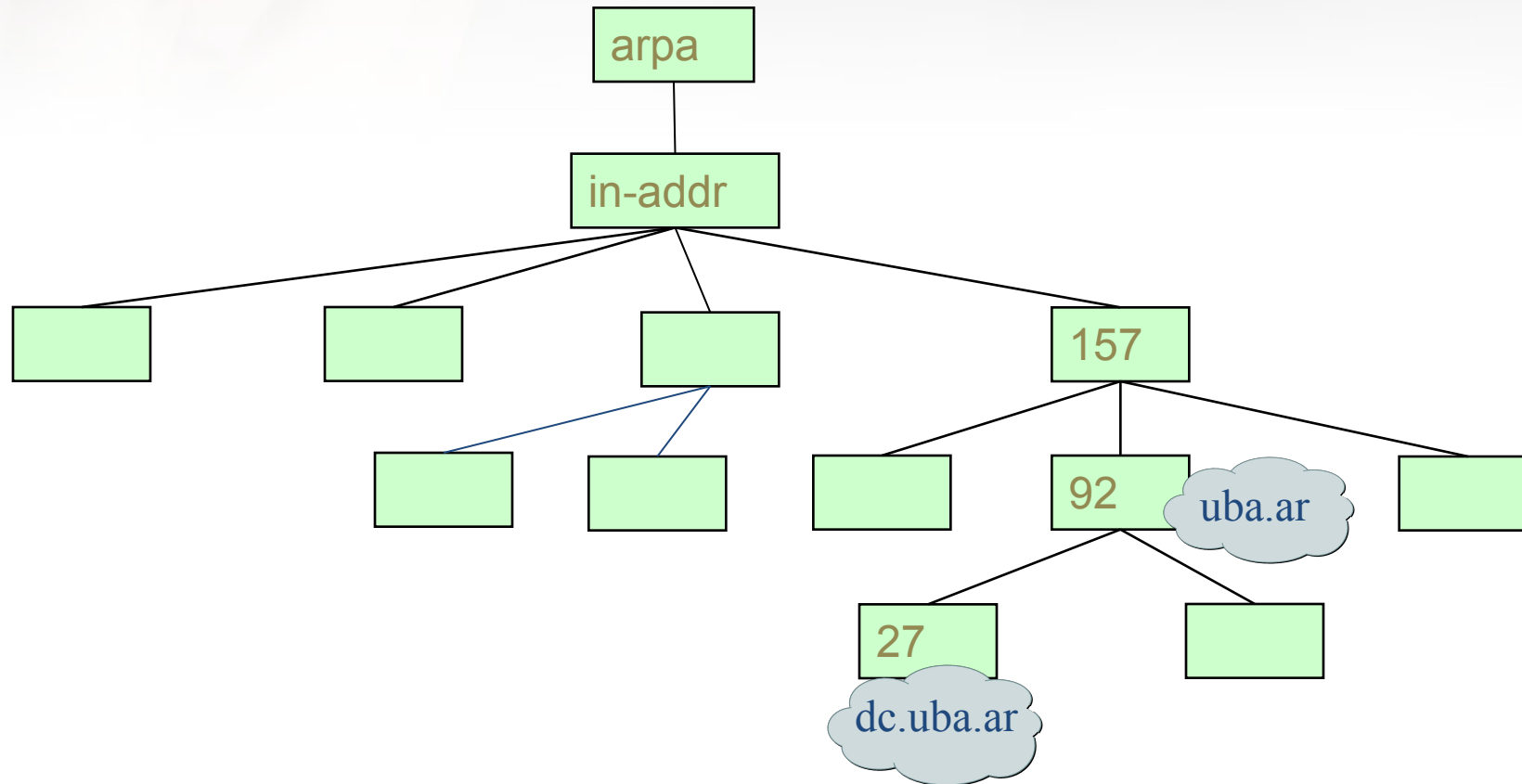
```
user@server:~$ host 157.92.27.21
```

```
21.27.92.157.in-addr.arpa domain name pointer
```

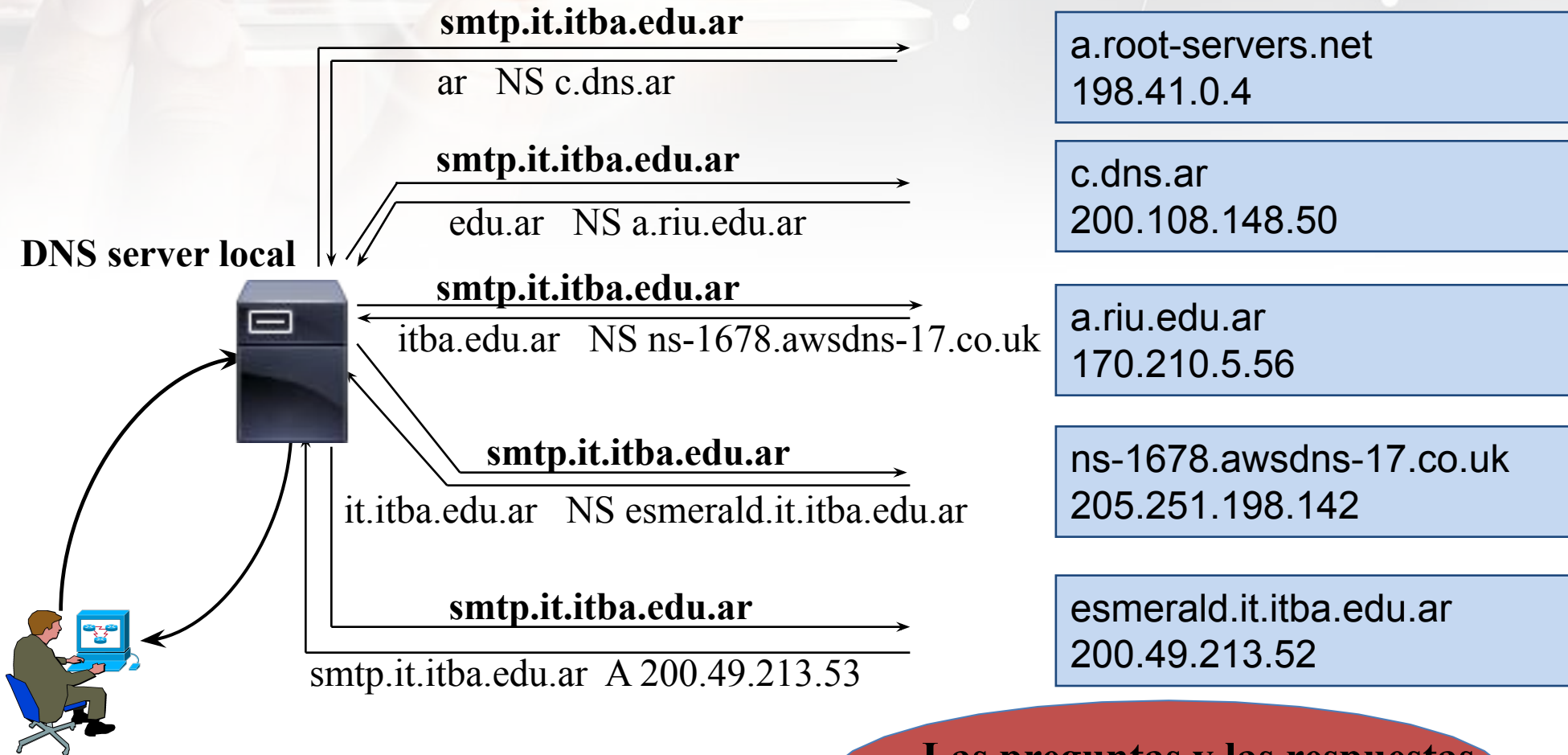
```
dc.uba.ar.
```

DNS

Para poder responder un *DNS reverse* se usa un árbol especial en base a los números IP.



DNS: consultas



¿Cuál es el IP de
`smtp.it.itba.edu.ar` ?

Resolución de nombres

Las preguntas y las respuestas
utilizan UDP

DNS: cache

- ✦ Una vez que el servidor de nombres aprende el mapeo, lo almacena en cache
- ✦ Expiran tras un tiempo (TTL)
- ✦ Servidores de nombre generalmente cachean la dirección de los servidores TLD
- ✦ Los Root Servers no suelen visitarse

¿Qué sucede si cambio el IP de un host conocido o migro una aplicación?

DNS

Los servidores raíz DNS son operados por IETF (*Internet Engineering Task Force*). Cuando alguien obtiene un nombre de dominio es el responsable de mantener, en un servidor DNS ~~master~~**primary** , actualizado ese dominio.

En Unix y Linux DNS es implementado generalmente con BIND (*Berkeley Internet Name Domain*).

Configuración de un servidor DNS

Existen cuatro niveles de configuración:

- Resolver only systems
- Caching-only servers
- ~~Master~~ Primary servers
- ~~Slave~~ Secondary servers

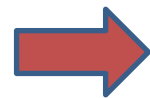
DNS Caching-only Server

- Aprende las respuestas acerca de los nombres de dominios de otro servidor. Una vez que aprende esa respuesta, la almacena para futuras preguntas.
- Todos los servidores utilizan esta técnica pero un caching-only server es la única técnica que utiliza.
- No es considerado un server autorizado porque su información es de segunda mano.

El programa **dnscache** funciona solo como cache de servidores de nombre, y puede ser usado en caching-only servers.



Resolución de nombres



DNS Caching-only Server

DNS Primary Server

- ◆ Es la fuente autorizada para toda la información de una zona específica.
- ◆ Lee la información sobre el dominio desde un archivo construido por el administrador.
- ◆ Es un server autorizado para un dominio o parte de un dominio pues puede responder con autoridad preguntas sobre ese dominio.

DNS Secondary Server

- ◆ Transfiere información completa de una zona desde un master server y la almacena en un archivo en el disco local.
- ◆ Mantiene información completa y actualizada de una zona y puede responder preguntas sobre zona en forma autorizada.

Registros DNS

DNS: base de datos distribuída de "resource records" (RR)

formato RR : (name, value, type, ttl)

type	name	value
A	nombre del host	IP
NS	dominio	nombre del host autorizado a resolver nombres del dominio
CNAME	alias para el nombre canónico	nombre canónico
MX	dominio	nombre del servidor de mails para el dominio

Registros DNS

DNS: base de datos distribuída de "resource records" (RR)

formato RR : (name, value, type, ttl)

type	name	value
AAAA	nombre del host	IPv6
SOA	Start of Authority	Inicio de información autorizada
SRV	Localizador de servicios	Para no crear registros tipo MX
RP	Persona responsable	Normalmente el mail del responsable

Registros DNS

DNS: base de datos distribuída de "resource records" (RR)

formato RR : (name, value, type, ttl)

type	value
TXT	un texto libre
SPF	Lista de IPs de hosts autorizados para enviar mails en nombre de este dominio

DNS: ejemplo parcial de configuración

\$ORIGIN example.com.

@ IN SOA ns1.example.com. hostmaster.example.com. (
 zone-admin.example.com. ; address of responsible party
 2016072701 ; serial number
 3600 ; refresh period
 600 ; retry period
 1w ; expire time
 3h) ; minimum ttl

IN NS ns1.example.com. ; DNS in the domain

IN NS ns.outsider.com. ; external to domain

IN NS ns2.example.com.

IN MX 10 mail.example.com.

IN MX 20 smtp.example.com.

ns1 IN A 192.168.0.1

ns2 IN A 201.13.248.106

mail IN A 204.13.248.106

smtp CNAME mail.example.com.

www IN A 192.168.0.3

Ver apunte "Understanding DNS—anatomy of a BIND zone file" en Material Didáctico / Prácticas / 03.-DNS

reverse-zone

```
$ORIGIN 1.0.10.in-addr.arpa.
```

```
$TTL 86400
```

```
@ IN SOA dns1.example.com. hostmaster.example.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.example.com.
```

```
IN NS dns2.example.com.
```

```
20 IN PTR alice.example.com.
```

```
21 IN PTR betty.example.com.
```

```
22 IN PTR charlie.example.com.
```

```
23 IN PTR doug.example.com.
```

```
24 IN PTR ernest.example.com.
```

```
25 IN PTR fanny.example.com.
```

Utilidades DNS

Para poder testear si la configuración es correcta se suelen usar 3 utilidades de línea de comandos:

- ◆ `host`
- ◆ `nslookup`
- ◆ `dig`

Para obtener información sobre el responsable de un dominio se puede utilizar `whois`.

whois: ejemplo

ITBA.edu.ar - Instituto Tecnológico de Buenos Aires

Dirección Postal: Av. E. Madero 399 (1106) - Capital Federal

Teléfonos: +54-11-4314-7778

Incumbencia Principal: Instituto Universitario

DATOS DEL CONTACTO TECNICO:

Nombre: Lo Nigro Miguel Martín

Dirección Postal: Av. Eduardo Madero 399

Teléfonos: +54 11 21504800 interno 5926 Fax:

Dirección de e-mail: mlonigro@itba.edu.ar

Horario de disponibilidad para contacto telefónico: 13 - 17 Hs

...

Utilidades DNS: host

host informa, dado un nombre de host, el número IP que le corresponde.

```
user@server:~$ host clarin.com
```

```
www.clarin.com has address 200.42.136.212  
clarin.com mail is handled by 0  
clarin-com.mail.protection.outlook.com.
```

```
user@server:~$ host upa
```

```
upa.midominio.com has address 172.16.12.4
```

```
user@server:~$ host -n 127.0.0.1
```

```
1.0.0.127.in-addr.arpa domain name pointer localhost.
```

```
user@server:~$ host localhost
```

```
localhost has address 127.0.0.1  
localhost has IPv6 address ::1
```

Utilidades DNS: dig

dig permite ver los registros para un dominio

```
user@server:~$ dig www.itba.edu.ar
; <<>> DiG 9.12.0 <<>> www.itba.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 499

;; QUESTION SECTION:
;www.itba.edu.ar.      IN A

;; ANSWER SECTION:
www.itba.edu.ar.      172800 IN      CNAME    AWS-S-BAL04.itba.edu.ar.
AWS-S-BAL04.itba.edu.ar. 172800 IN      CNAME
AWS-S-BAL04-248295998.sa-east-1.elb.amazonaws.com.
AWS-S-BAL04-248295998.sa-east-1.elb.amazonaws.com. 60 IN A 54.94.221.168
AWS-S-BAL04-248295998.sa-east-1.elb.amazonaws.com. 60 IN A 54.94.246.182
```


Utilidades DNS: dig

Ejemplo: **dig www.itba.edu.ar** (*cont.*)

```
;; AUTHORITY SECTION:
```

```
sa-east-1.elb.amazonaws.com. 67 IN NS ns-632.awsdns-15.net.  
sa-east-1.elb.amazonaws.com. 67 IN NS ns-2034.awsdns-62.co.uk.  
sa-east-1.elb.amazonaws.com. 67 IN NS ns-1276.awsdns-31.org.  
sa-east-1.elb.amazonaws.com. 67 IN NS ns-291.awsdns-36.com.
```

```
;; ADDITIONAL SECTION:
```

```
ns-291.awsdns-36.com. 12086 IN A 205.251.193.35  
ns-291.awsdns-36.com. 9492 IN AAAA 2600:9000:5301:2300::1  
ns-632.awsdns-15.net. 34682 IN A 205.251.194.120  
ns-632.awsdns-15.net. 84172 IN AAAA 2600:9000:5302:7800::1  
ns-1276.awsdns-31.org. 8938 IN A 205.251.196.252  
ns-1276.awsdns-31.org. 8938 IN AAAA 2600:9000:5304:fc00::1  
ns-2034.awsdns-62.co.uk. 9492 IN AAAA 2600:9000:5307:f200::1
```

Utilidades DNS: dig

Ejemplo: **dig www.itba.edu.ar** (*cont.*)

```
;; Query time: 2 msec
;; SERVER: 10.1.0.10#53(10.1.0.10)
;; WHEN: Tue Aug 22 09:31:59 -03 2017
;; MSG SIZE rcvd: 462
```

```
~$ dig www.itba.edu.ar +nocomments +noquestion +noauthority +noadditional +nostats
; <<>> DiG 9.14.10 <<>> www.itba.edu.ar +nocomments +noquestion +noauthority +noadditional
+nostats
;; global options: +cmd
www.itba.edu.ar.      59    IN     CNAME  aws-s-bal04.itba.edu.ar.
aws-s-bal04.itba.edu.ar. 39    IN     CNAME  aws-s-bal04-248295998.sa-east-1.
elb.amazonaws.com.
aws-s-bal04-248295998.sa-east-1.elb.amazonaws.com. 59 IN A 54.233.177.225
aws-s-bal04-248295998.sa-east-1.elb.amazonaws.com. 59 IN A 52.67.10.227
```

Utilidades DNS: dig

- `dig host +noall +answer`
- `dig host MX +noall +answer`
- `dig -t NS host +noall +answer`
- `dig host ANY +noall +answer`
- `dig host ns +short`
- `dig -x 13.227.69.6`
- `dig host +trace`

Utilidades DNS: nslookup

nslookup puede ser utilizado en forma interactiva o en forma similar a dig.

```
user@server:~$ nslookup www.itba.edu.ar
Server:      10.16.1.102
Address:     10.16.1.102#53
Non-authoritative answer:
www.itba.edu.ar canonical name = aws-s-bal04.itba.edu.ar
aws-s-bal04.itba.edu.ar canonical name =
aws-s-bal04-248295998.sa-east-1.elb.amazonaws.com.
Name:      aws-s-bal04-248295998.sa-east-1.elb.amazonaws.com
Address:   54.233.98.53
Name:      aws-s-bal04-248295998.sa-east-1.elb.amazonaws.com
Address:   54.94.246.182
```

Utilidades DNS: nslookup

Si se lo ejecuta sin parámetros ingresa al modo interactivo

```
user@server:~$ nslookup
```

```
> clarin.com
```

```
Server:      192.168.2.1
```

```
Address:     192.168.2.1
```

```
Non-authoritative answer:
```

```
Name:  clarin.com
```

```
Address: 200.42.136.212
```

```
>dns.itba.edu.ar
```

```
*** Can't find dns.itba.edu.ar: No answer
```

Intento adivinar el
servidor DNS

Utilidades DNS: nslookup

Ahora la consulta será
por registros NS

```
> set type=NS
```

```
> itba.edu.ar
```

```
Server: 192.168.2.1
```

```
Address: 192.168.2.1
```

Non-authoritative answer:

```
itba.edu.ar      nameserver = ns-888.awsdns-47.net.
```

```
itba.edu.ar      nameserver = ns-1287.awsdns-32.org.
```

```
itba.edu.ar      nameserver = ns-90.awsdns-11.com.
```

```
> server ns-888.awsdns-47.net
```

```
Default server: ns-888.awsdns-47.net
```

```
Address: 205.251.198.142#53
```

```
Default server: ns-888.awsdns-47.net
```

```
Address: 2600:9000:5306:8e00::1#53
```

Le pregunto al server
autorizado

Utilidades DNS: nslookup

```
> itba.edu.ar
```

```
Server:      ns-1678.awsdns-17.co.uk
```

```
Address:     205.251.198.142#53
```

```
itba.edu.ar      nameserver = ns-1678.awsdns-17.co.uk.
```

```
itba.edu.ar      nameserver = ns-888.awsdns-47.net.
```

```
itba.edu.ar      nameserver = ns-1287.awsdns-32.org.
```

```
itba.edu.ar      nameserver = ns-90.awsdns-11.com.
```

DNS: Split-horizon

Split-Horizon: un nombre se resuelve con distintas IP dependiendo del origen de la consulta

```
$ host crystal.it.itba.edu.ar  
crystal.it.itba.edu.ar has address 10.16.1.103
```

```
$ host crystal.it.itba.edu.ar  
crystal.it.itba.edu.ar has address 200.5.121.139
```

DNS dinámico

DDNS (RFC 2136) permite actualizar en forma dinámica un servidor DNS. Introducido en BIND a partir de la versión 8.



Servidor DNS
con soporte para
DDNS

registrar maria.no-ip.info, IP: 83.46.191.189

dominio: maria. no-ip.info, IP: 83.46.191.213

dominio: maria. no-ip.info, IP: 83.46.191.176



Usuario con
IP dinámica

DNS dinámico

Ejemplo

```
user@server:~$ dig carlos.no-ip.com

...
;; ANSWER SECTION:
carlos.no-ip.com. 55 IN A 69.208.210.116

;; AUTHORITY SECTION:
no-ip.com.      86330 IN NS nf2.no-ip.com.
no-ip.com.      86330 IN NS nf3.no-ip.com.
no-ip.com.      86330 IN NS nf1.no-ip.com.

;; ADDITIONAL SECTION:
nf1.no-ip.com.  84798 IN A 8.4.112.75
nf2.no-ip.com.  84797 IN A 63.208.74.227
nf3.no-ip.com.  84797 IN A 216.66.37.13
```


DNS spoofing

Es el arte de lograr que un registro DNS apunte a un IP que no sea el que debería apuntar.



¿Cuál es el ip de iol.itba.edu.ar ?

Rta: 24.232.138.9



Servidor DNS
local

La respuesta estaba en
la cache o la aportó
otro servidor DNS.

DNS spoofing

Método: enviar respuesta sin recibir una pregunta



Rta: El IP de campus.itba.edu.ar es
24.232.138.98



Servidor DNS
Víctima

Se debe verificar que la respuesta se corresponda con alguna pregunta. DNS establece que los mensajes de pregunta y respuesta tengan un mismo ID que los identifique

DNS spoofing

Método: *DNS sniffer*



¿IP de campus.itba.edu.ar?, ID=XYZ

sniffing



Servidor DNS

Rta falsa, ID = XYZ

Rta real, ID = XYZ

¿Sirve verificar el IP de origen de la respuesta?

DNS spoofing

Método: *DNS cache poisoning*



Formato de los mensajes

Ver también las capturas publicadas en Campus

DNS: formato de los mensajes

Message Header:

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
REQUEST ID																Q	Opcode				A	T	D	R	Rsvd				Rcode										
Count of Question Records																Count of Answer Records																							
Count of Authority Records																Count of Additional Records																							

Opcode

- ◆ 0: consulta estándar
- ◆ 1: consulta inversa
- ◆ 2: consulta por “server status”

Rcode

- ◆ 0: sin error
- ◆ 1: error de formato
- ◆ 2: error en el servidor
- ◆ 3: error en el nombre
- ◆ 4: sin implementar
- ◆ 5: rechazado

DNS: formato de los mensajes

Message Header:

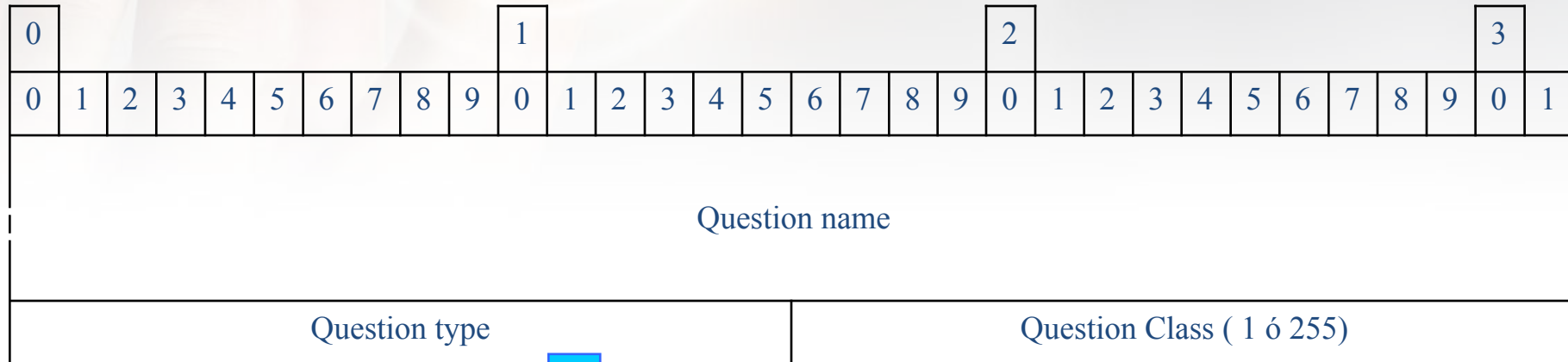
0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
REQUEST ID																Q	Opcode				A	T	D	R	Rsvd				Rcode										
Count of Question Records																Count of Answer Records																							
Count of Authority Records																Count of Additional Records																							


Bits

- ◆ Q: 0 (Query) / 1 (Response)
- ◆ A: Respuesta autorizada
- ◆ T: Respuesta truncada
- ◆ D: Pregunta con recursividad
- ◆ R: Recursión disponible

DNS: formato de los mensajes

Mensaje de pregunta (Question record):



- 
- ◆ 1: host
 - ◆ 2: name server autorizado
 - ◆ 5: nombre canónico de un alias
 - ◆ 15: mail exchange
 - ◆ 252: solicitud de transferencia de zona
 - ◆ etc.

DNS: formato de los mensajes

Mensaje de respuesta (Answer, Authority, Additional record):

0										1										2										3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
Name																																
Type																Class																
Time To Live (TTL)																																
Record data Length																																
Record data																																

Material de lectura

Capítulo 2.5 de la bibliografía