Repaso de DNS

Vista General

- Metas de esta sesión
- Qué es DNS ?
- Cómo se construye el DNS y cómo funciona?
- Cómo funcionan las peticiones?
- Tipos de Récords
- Cachés y autorizados
- Delegación: dominios vs zonas
- Cómo encontrar problemas

Metas de esta sesión

- Revisaremos los conceptos básicos de DNS, incluyendo los mecanismos de peticiones, delegaciones, y caching.

- La meta es saber suficiente DNS para configurar un servidor caché, y resolver problemas típicos de DNS, tanto locales como remotos (en la Internet)

Qué es DNS?

- Sistema para traducir nombres a direcciones:

```
nsrc.org          →   128.223.157.19
www.afrinic.net → 2001:42d0::200:80:1
```

- ... y viceversa:

```
128.223.157.19  →   nsrc.org
1.0.0.0.0.8.0.0.0.0.2.0.0.0.0.0.0.0.0.0
.0.0.0.0.0.d.2.4.1.0.0.2.ip6.arpa. →
www.afrinic.net.
```

Qué es DNS?

- Otra información que se puede hallar en DNS:

  Dónde enviar e-mail para un dominio
  Quién es responsable de este sistema?
  Información geográfica
  etc...

- Cómo buscamos esta información?

Herramientas básicas de DNS

- El comando host:

```
# host nsrc.org.
nsrc.org. has address 128.223.157.19
# host 128.223.157.19
19.157.223.128.in-addr.arpa domain name
pointer nsrc.org.
```

Herramientas básicas de DNS

- Host con IPv6:

```
# host www.afrinic.net

www.afrinic.net has IPv6 address
2001:42d0::200:80:1

# host 2001:42d0::200:80:1

1.0.0.0.0.0.8.0.0.0.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.0.0.d.2.4.1.0.0.2.ip6.arpa domain name
pointer www.afrinic.net.
```

Herramientas básicas de DNS

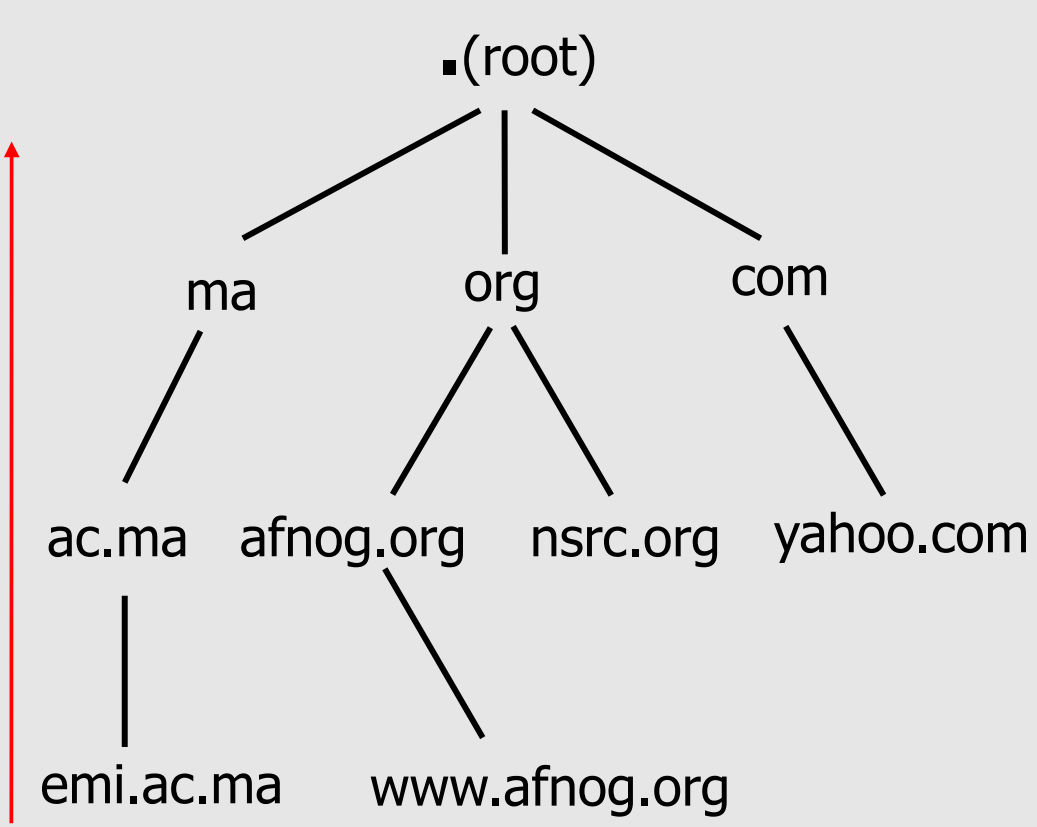
- Pruebe esto con otros nombres – primero busque estos nombres, y luego las direcciones que obtenga:

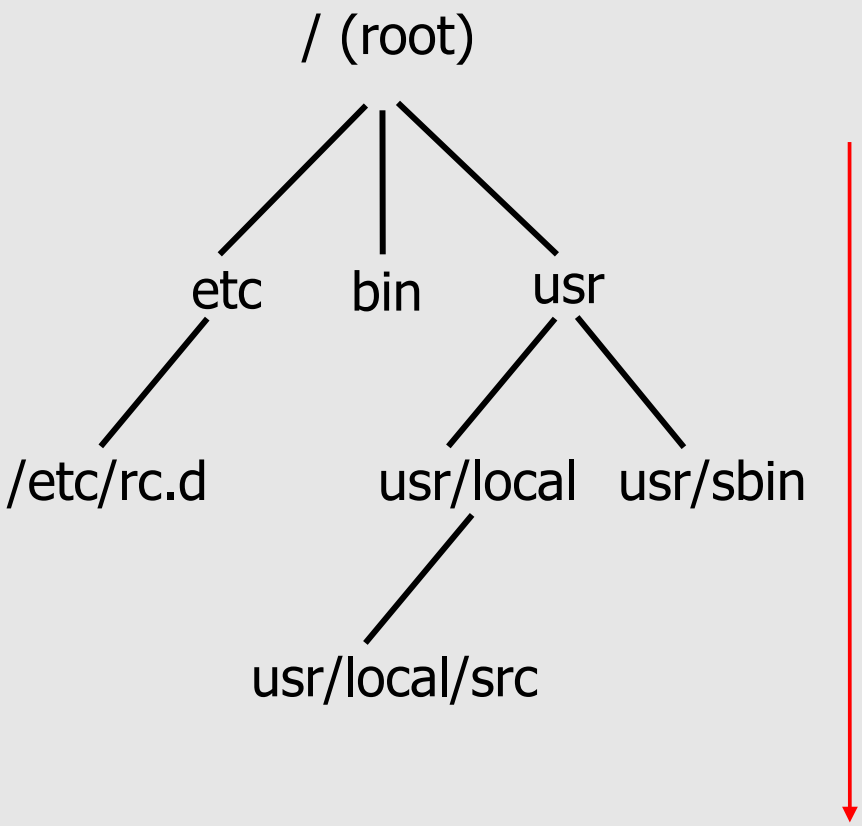
```
www.yahoo.com
www.nsrc.org
ipv6.google.com
```

- Concuerda el nombre al buscar la dirección? Por qué?

- De dónde sacó el comando 'host' esta información ?

Cómo se construye el DNS?





Base de datos DNS

Sistema de archivos Unix

... es una estructura de árbol invertido

Cómo se construye el DNS?

- El DNS es jerárquico
- La administración es compartida – No hay entidad central que administre todos los datos de DNS
- La distribución de la administración se llama ”delegación”

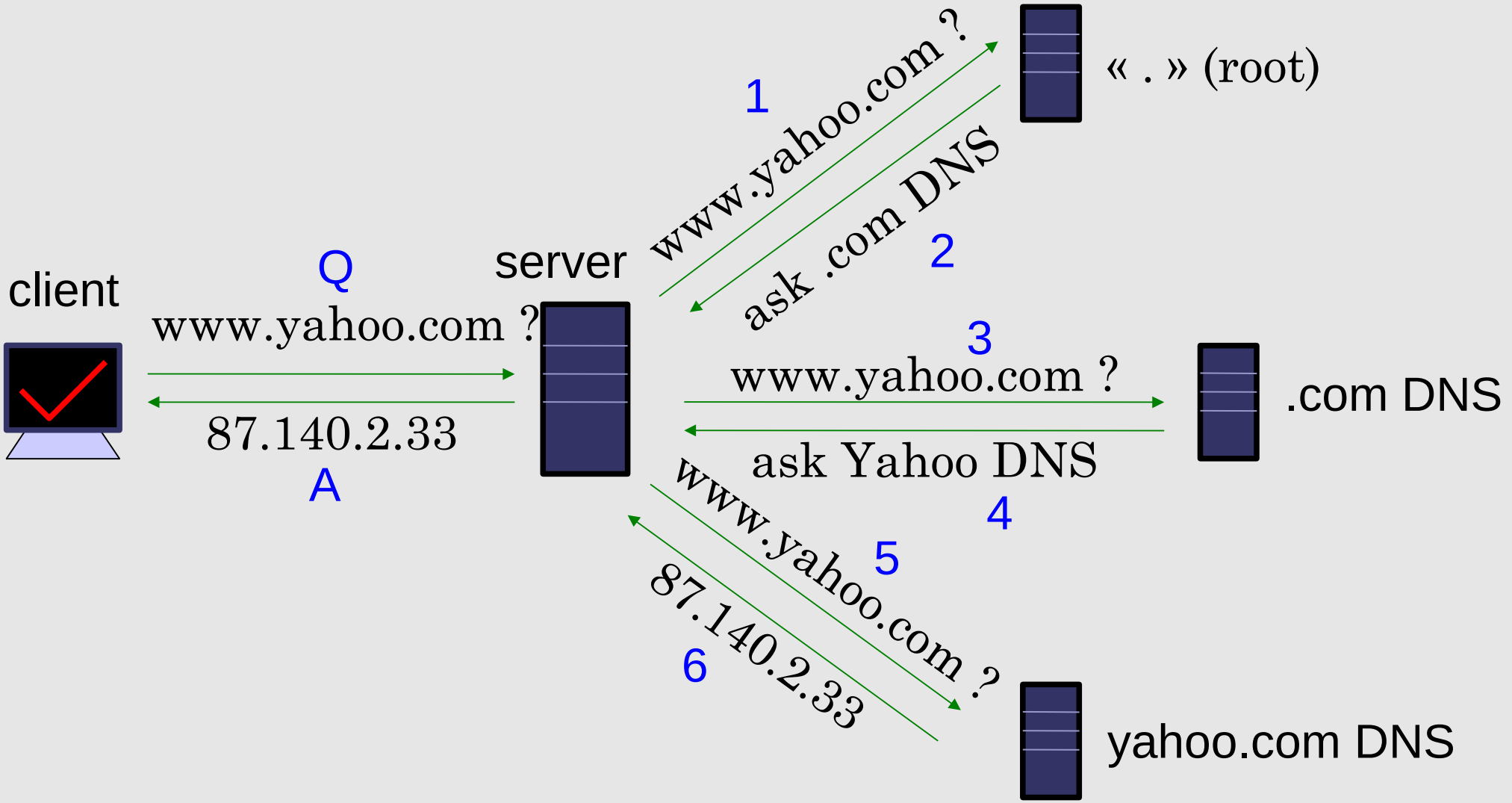
Cómo funciona el DNS?

- **Los clientes** usan un mecanismo llamado **resolver** y preguntan a los **servidores** – esto se llama una **query (pregunta)**
- El servidor cuestionado intentará encontrar la respuesta de parte del cliente
- El servidor opera recursivamente, desde el tope (raíz) hasta que encuentra una respuesta, preguntando a otros servidores según atraviesa el árbol – el servidor recibe referencias de otros servidores

Cómo funciona el DNS?

- El cliente (navegador web, cliente de correo ...) utiliza el “resolver” del sistema operativo para encontrar la dirección IP.
- Por ejemplo, si vamos a la página www.yahoo.com:
  El navegador pregunta al OS « Necesito la IP de www.yahoo.com »
  El OS busca en la configuración del resolver a quién preguntar, y envía la pregunta
- En UNIX, la configuración está en /etc/resolv.conf.

Una pregunta DNS



Detalle de pregunta con tcpdump

- En el servidor, hágase root:

```
$ su
passwd:
# tcpdump -s1500 -n port 53
```

- En otra ventana, ejecute:

```
# host … (cualquier cosa)
```

Detalle de pregunta - tcpdump

- 1: 18:40:38.62 IP 192.168.1.1.57811 > 192.112.36.4.53: 29030 [1au] A? h1-web.hosting.catpipe.net. (55)
- 2: 18:40:39.24 IP 192.112.36.4.53 > 192.168.1.1.57811: 29030- 0/13/16 (540)

- 3: 18:40:39.24 IP 192.168.1.1.57811 > 192.43.172.30.53: 7286 [1au] A? h1-web.hosting.catpipe.net. (55)
- 4: 18:40:39.93 IP 192.43.172.30.53 > 192.168.1.1.57811: 7286 FormErr- [0q] 0/0/0 (12)

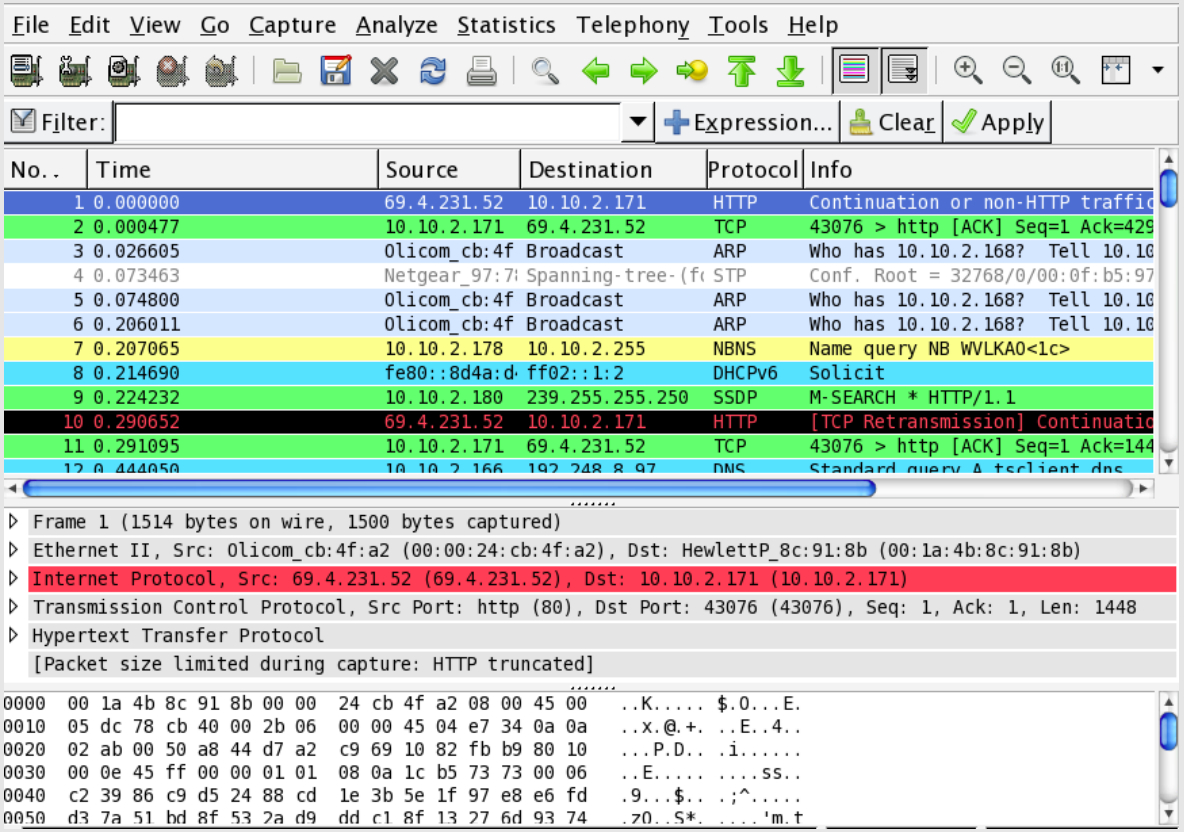
- 5: 18:40:39.93 IP 192.168.1.1.57811 > 192.43.172.30.53: 50994 A? h1-web.hosting.catpipe.net. (44)
- 6: 18:40:40.60 IP 192.43.172.30.53 > 192.168.1.1.57811: 50994- 0/3/3 (152)

- 7: 18:40:40.60 IP 192.168.1.1.57811 > 83.221.131.7.53: 58265 [1au] A? h1-web.hosting.catpipe.net. (55)
- 8: 18:40:41.26 IP 83.221.131.7.53 > 192.168.1.1.57811: 58265* 1/2/3 A 83.221.131.6 (139)

Pregunta - analisis

- Usamos una analizador de paquetes (wireshark) para ver los contenidos de la pregunta...

  http://www.wireshark.org/



Configuración del Resolver

- Indica al sistema a qué servidor preguntar
- En UNIX: `/etc/resolv.conf`
- Busque este fichero, y verifique que tiene una instrucción 'nameserver' así:

  ```
  nameserver a.b.c.d
  ```

  o

  ```
  nameserver ip:v6:ad:dr:es:ss
  ```

  ... donde a.b.c.d es la IP/IPv6 de un servidor operativo (debería).

Encontrar la raíz

- La primera pregunta se dirije a:

  192.112.36.4 (G.ROOT-SERVERS.NET.)

- Cómo sabe el servidor en dónde encontrar los servidores raíz ?
- Problema de *la gallina y el huevo*
- Cada servidor necesita una lista de los servidores raíz (A – M.ROOT-SERVERS.NET) y sus direcciones IP
- En BIND, `named.root`

Usar 'dig' para saber más detalles

- El comando 'host' es limitado – bueno para resolver, pero no para depurar problemas.
- Usamos 'dig' para obtener más detalles
- dig muestra muchas cosas interesantes

Usar 'dig' para saber más detalles

```
ns# dig @147.28.0.39 www.nsrc.org. a

; <<>> DiG 9.3.2 <<>> @147.28.0.39 www.nsrc.org
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4620
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4,
ADDITIONAL: 2

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

;; ANSWER SECTION:
www.nsrc.org.           14400   IN      A       128.223.162.29

;; AUTHORITY SECTION:
nsrc.org.               14400   IN      NS      rip.psg.com.
nsrc.org.               14400   IN      NS      arizona.edu.

;; ADDITIONAL SECTION:
rip.psg.com.            77044   IN      A       147.28.0.39
arizona.edu.             2301   IN      A       128.196.128.233

;; Query time: 708 msec
;; SERVER: 147.28.0.39#53(147.28.0.39)
;; WHEN: Wed May 10 15:05:55 2007
;; MSG SIZE  rcvd: 128
```

```
noc# dig www.afrinic.net any

; <<>> DiG 9.4.2 <<>> any www.afrinic.net
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36019
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 10

;; QUESTION SECTION:
;www.afrinic.net.         IN   ANY

;; ANSWER SECTION:
www.afrinic.net. 477     IN   AAAA     2001:42d0::200:80:1
www.afrinic.net. 65423   IN   A        196.216.2.1

;; AUTHORITY SECTION:
afrinic.net.     65324   IN   NS       sec1.apnic.net.
afrinic.net.     65324   IN   NS       sec3.apnic.net.
afrinic.net.     65324   IN   NS       ns1.afrinic.net.
afrinic.net.     65324   IN   NS       tinnie.arin.net.
afrinic.net.     65324   IN   NS       ns.lacnic.net.
afrinic.net.     65324   IN   NS       ns-sec.ripe.net.

;; ADDITIONAL SECTION:
ns.lacnic.net.   151715  IN   A        200.160.0.7
ns.lacnic.net.   65315   IN   AAAA     2001:12ff::7
ns-sec.ripe.net. 136865  IN   A        193.0.0.196
ns-sec.ripe.net. 136865  IN   AAAA     2001:610:240:0:53::4
ns1.afrinic.net. 65315   IN   A        196.216.2.1
tinnie.arin.net. 151715  IN   A        168.143.101.18
sec1.apnic.net.  151715  IN   A        202.12.29.59
sec1.apnic.net.  151715  IN   AAAA     2001:dc0:2001:a:4608::59
sec3.apnic.net.  151715  IN   A        202.12.28.140
sec3.apnic.net.  151715  IN   AAAA     2001:dc0:1:0:4777::140

;; Query time: 1 msec
;; SERVER: 196.200.218.1#53(196.200.218.1)
;; WHEN: Tue May 27 08:48:13 2008
;; MSG SIZE  rcvd: 423
```

Salida de dig

- Campos interesantes:

  flags section: qr aa ra rd
  status
  answer section
  authority section
  TTL (numbers in the left column)
  query time
  server

- Fíjese en los records tipo 'A' y 'AAAA' en la salida.

Tipos de Récords

- Tipos básicos:

- A, AAAA: Dirección IPv4, IPv6
- NS: Name Server
- MX: Mail eXchanger
- CNAME: Nombre canónico (alias)
- PTR: Información inversa

Caching vs Autorizado

- En la salida de dig, y en las salidas siguientes, notamos un decremento en el tiempo de respuesta si repetimos la pregunta.
- Las respuestas están siendo **cached** (almacenadas temporalmente) por el servidor que pregunta, para ahorrar ancho de banda y mejorar el tiempo de respuesta
- El valor TTL controla el tiempo que el servidor puede almacenar cada respuesta
- Los servidores DNS se pueden poner en dos categorías: **caching** y **autorizados**.

Caching vs Autorizado

- Los servidores autorizados típicamente sólo responden a peticiones de información para la cual ellos tienen la autoridad, ej.: datos para los cuales tienen un respaldo permanente (ficheros, base de datos)
- Si no la tienen, enviarán una lista de servidores que sí son autorizados, pero no procesarán la petición recursivamente

Caching vs Autorizado: caching

- Los servidores caching actúan como intermediarios para los clientes, y almacenan las respuestas para después.
- Puede ser el mismo software (suele serlo), pero mezclar estas funciones (recursivo/caching y autorizado) no es recomendable (riesgos de seguridad + confuso)
- El TTL de la respuesta se usa para determinar cuánto tiempo se puede almacenar la respuesta antes de preguntar de nuevo.

Valores TTL

- Los valores TTL decrementan y caducan
- Pruebe a pedir repetidamente el récord A de www.yahoo.com:

```
# dig www.yahoo.com
```

- Qué puede observar acerca del tiempo de respuesta y el TTL?

SOA

- Vamos a pedir el récord SOA de un dominio:

```
# dig SOA <domain>
...
;; AUTHORITY SECTION:
<domain>. 860 IN SOA ns.<domain>. root.<domain>.
                          200702270 ; serial
                          28800       ; refresh
                          14400       ; retry
                          3600000   ; expire
                          86400       ; neg ttl
...
```

SOA

- Los primeros dos campos resaltados son:

  El SOA (Start Of Authority), en el cual el administrador el nombre del servidor “fuente” para el dominio en cuestión (no siempre es el caso)

  El RP (Responsible Person), que es la dirección de correo electrónico (con el @ cambiado por un '.') a contactar en caso de que haya problemas con el dominio.

SOA

- Los campos oficiales son:
  serial: El número de serie de la zona: útil para la replicación entre servidores
  refresh: qué tan frecuentemente los servidores esclavos deben verificar con el master si hay una versión nueva de la zona
  retry: Con qué frecuencia reintentar el contacto con el master si éste no responde a un refresh.
  expire: Cuando el servidor maestro ha dejado de responder por mucho tiempo, no responder a peticiones de clientes.
- Por qué es necesario caducar una zona ?

Cómo implementar un servidor caché

- Tener un servidor caché local puede ser muy útil
- Fácil de instalar, por ejemplo en FreeBSD:

```
Agregar named_enable="YES" a /etc/rc.conf
Cargar named:
   /etc/rc.d/named start
```

- Cómo se puede verificar que named está corriendo ?

Cómo implementar un servidor caché

- Cuando esté seguro de que su servidor caché está corriendo, configure so resolver para utilizarlo (/etc/resolv.conf):

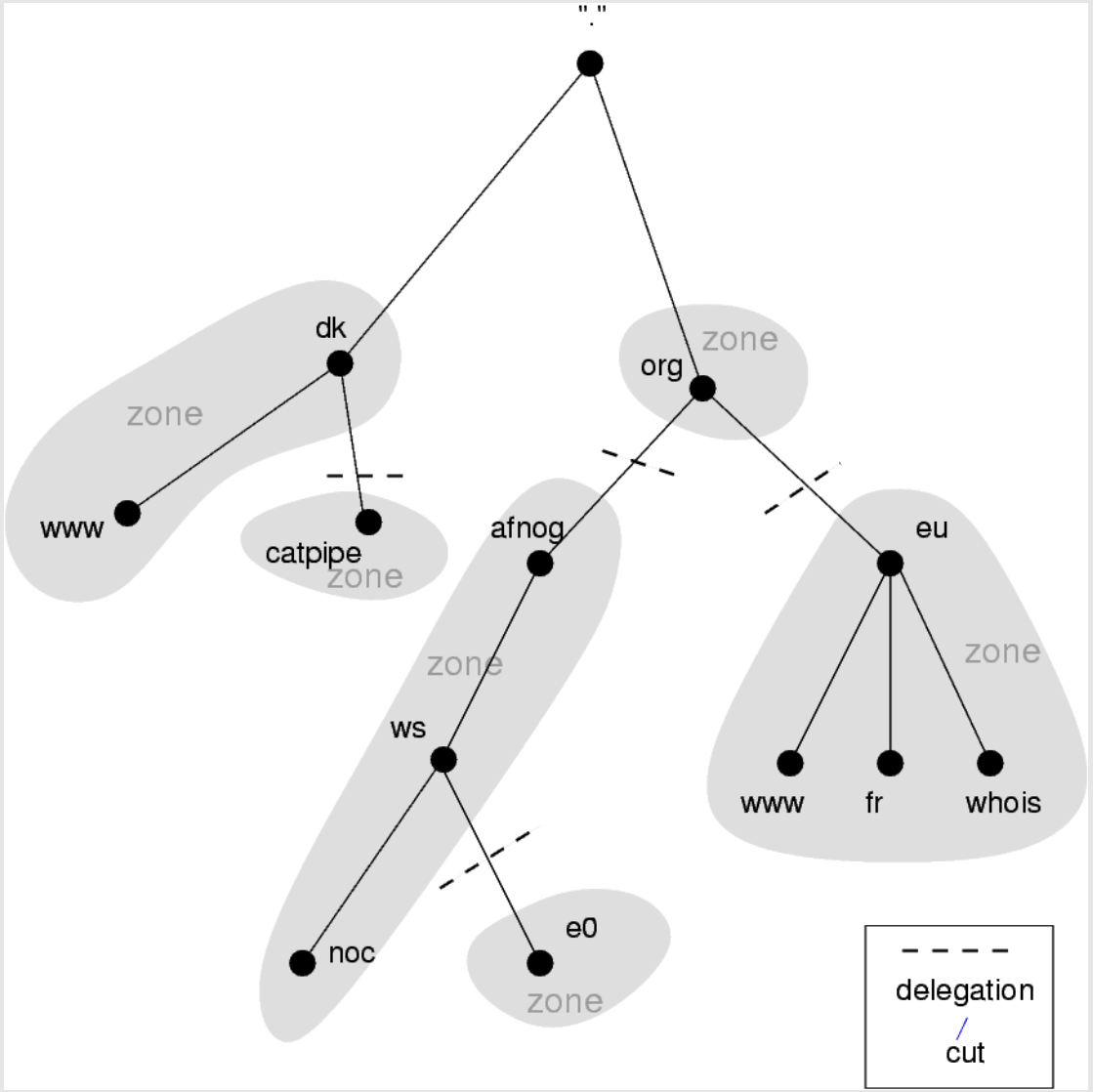
```
nameserver 127.0.0.1
```

Delegación

- Mencionamos que una de las ventajas de DNS era que su administración es distribuída. Esto se llama delegación.

- Hacemos una delegación cuando hay una separación administrativa y queremos dar el control de un sub-dominio a:
  - Un departamento de una organización grande
  - Una empresa de un país
  - Una entidad que representará el dominio de un país

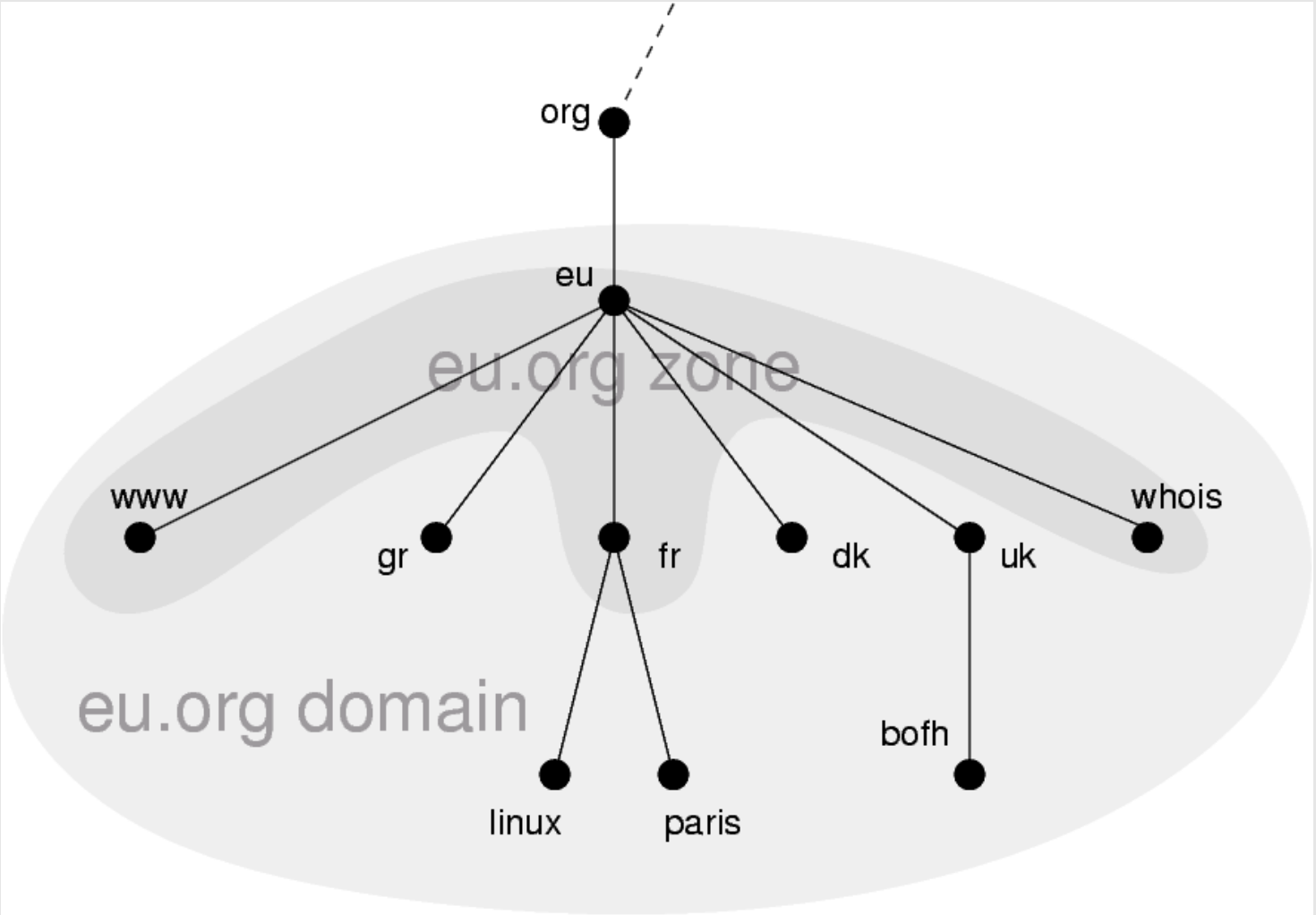
Delegación


"."
dk
org
zone
zone
www
catpipe
zone
afnog
eu
zone
zone
ws
www
fr
whois
e0
noc
zone
delegation
cut

Delegación: Dominios vs Zonas

- Cuando hablamos de un sub-árbol completo, nos referimos a *dominios*
- Cuando hablamos acerca de parte de un dominio administrado por una entidad, nos referimos a *zonas*

Delegación: Dominios vs Zonas



Encontrar errores con doc

- Cuando hay problemas en la red, servicio e-mail o web, no siempre se sospecha de DNS.
- Pero en caso de que sí, no siempre es obvio – El DNS puede ser confuso.
- Una gran herramienta para detectar problemas es 'doc'
- /usr/ports/dns/doc – Instálelo ahora!
- Hagamos algunas pruebas con doc...

Conclusión

- El tema de DNS es amplio
- Requiere mucha práctica el detectar problemas con exactitud a la primera – la recursión y el caching son particularmente confusos
- Recuerde que hay varios servidores para la misma información, y no siempre se está interrogando al mismo
- Practique, practique, practique!
- No tenga miedo de preguntar

Questions ?

?