

Servicio de nombres de dominio

Álvaro González Sotillo

Rey Fernando VI

29 de septiembre de 2015



- 1 Introducción
- 2 Componentes y funcionamiento
- 3 Espacio de nombres de dominio
- 4 Servidores DNS
- 5 Clientes DNS
- 6 Registros de recursos
- 7 Resolución inversa



Motivación

- En una red TCP/IP se utilizan direcciones numéricas (MAC, IP, puertos)
 - Fácil para los ordenadores
 - Complicado para las personas
- Para las personas es más simple recordar nombres:
`www.google.com`

Servicios de resolución de nombres

- Asocian direcciones (numéricas) a nombres
 - Dirección a partir del nombre
 - Nombre a partir de la Dirección
 - **Resuelven** nombres
- **DNS:** Domain Name Server
 - Principal servicio de resolución de nombres en TCP/IP, y por tanto en Internet
 - Modelo cliente-servidor
 - Modelo distribuido

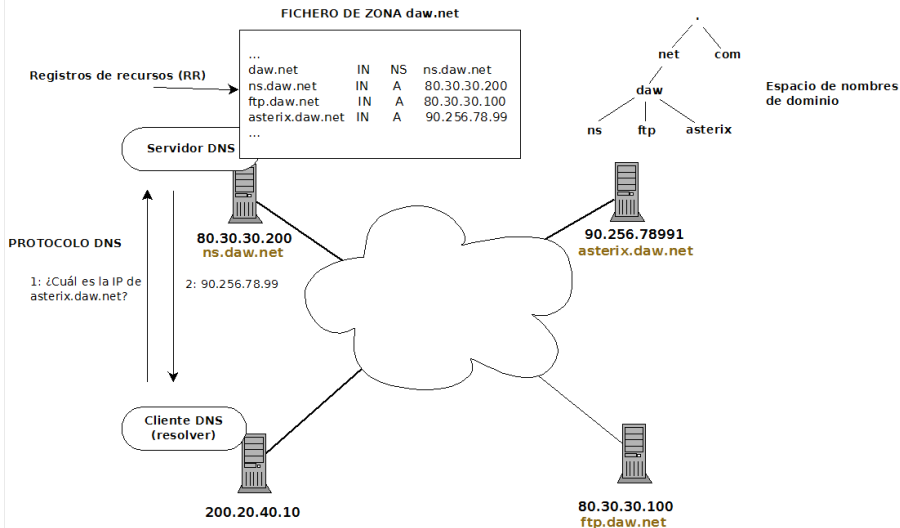
DNS: Base de datos

- Es un servicio de almacenamiento y consulta de información
- Posibles consultas:
 - Resolución directa: ¿Cuál es la IP de `www.daw.net`?
 - Resolución inversa: ¿Cuál es el nombre de `100.200.30.45`?
 - Correo: ¿Dónde se envía el correo de `gmail.com`?
 - Balanceo de carga: ¿Qué servidor de nombres tiene información de `gmail.com`?
 - Descubrimiento: ¿Qué servidores hay en el dominio `gmail.com`?
 - Claves públicas

Componentes y funcionamiento

- Domain Name Space: Espacio de nombres de dominio
- Name Servers: Servidores de nombres
- Resolvers: Clientes de DNS
- Protocolo DNS
- Base de datos distribuida: Registros de recursos (**RR**) organizados en **zonas**

Componentes y funcionamiento



Componentes y funcionamiento

- Los clientes (resolvers) preguntan a los servidores de nombres
- Los servidores de nombres se comunican entre si:
 - Si no tienen información por la que les han preguntado
 - Para intercambiar información sobre sus zonas (transferencias de zona)
- <http://www.youtube.com/embed/dIGxJCqLJlY>

Ejercicios

Configura DNS en *Debian*


Usa el fichero `/etc/resolv.conf` para configurar el servidor DNS del resolver en *Debian*

Usa el resolver en *Debian*

Usa el comando **nslookup** (*Windows* o *Debian*) o **dig** (*Debian*) para conocer:

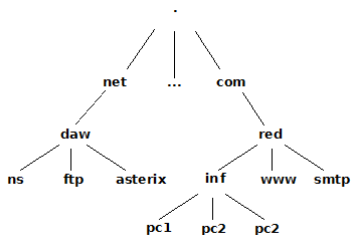
- El nombre de la dirección 8.8.8.8
- La dirección de `www.gmail.com`

Nombres de dominio

- Uno o varios nombres separados por puntos, con un punto final
- En total, menos de 256 caracteres
- Cada nombre, menor de  caracteres
- Ejemplos
 - com.
 - google.com.
 - iesreyfernando.educa.madrid.org.
 - .

Nombres de dominio

- El conjunto de nombres es el espacio de nombres de dominio
- Los nombres cuelgan de nombres de nivel superior
- El nivel más alto es . (punto)



Nombres de dominio

- Subdominio: Nombres que dependen de un dominio
 - El subdominio aparece a la izquierda del dominio
- Nombres absolutos: Indican todos los dominios y subdominios
 - Acaban en .
 - Son nombres FQDN (*Fully Qualified Domain Name*)
- Nombres relativos: Desde el nombre actual
 - Se intentan resolver quitando dominios desde el actual
 - Hasta llegar a . (por eso `www.google.com` suele acabar siendo `www.google.com.`)

Nombres de dominio

- El “dueño” de los nombres de dominio es la ICANN
- Existe un número limitado de TLD
 - Asociados a países: es, pt, it, tv ...
 - Asociados a la función de la organización: com, biz, gov, edu, net ...
 - Otros: tienda, soy, pizza ...
 - https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains
- Existen varios servidores DNS que “poseen” la raíz de los nombres (Root Hints)
 - No es posible publicar un nombre de forma mundial sin contar con ellos
 - Los agentes registradores permiten “alquilar” nombres a partir de estos Root Hints

Ejercicios

Root Hints

Localiza una lista de los nombres de dominio de los servidores DNS que poseen el dominio “.”

Servidores DNS

- Almacenan información sobre nombres de dominio
- Solo tienen una parte de la información total (una o varias zona)
- Responden a preguntas de otros servidores y resolvers con el protocolo DNS
- Puertos:
 - 53 TCP
 - 53 UDP

Zonas

- Parte contigua del espacio de nombres de dominio
- Ejemplo del fichero de zona del dominio daw.org en un servidor con IP 192.168.1.100

```
1  ...
2  daw.org      IN NS      ns.daw.org
3  ns.daw.org   IN A       192.168.1.100
4  www.daw.org  IN A       192.168.1.200
5  smtp.daw.org IN A       192.168.1.220
6  ftp.daw.org  IN CNAME   www.daw.org
7  zipi.daw.org IN CNAME   smtp.daw.org
8  ...
```

Listado 1 : Ejemplo de fichero de zona del dominio daw.org

Zonas

- Los ficheros de zona contienen registros de recursos (RR, Resource Records).
- Pueden almacenarse en ficheros de texto, bases de datos, servicios de directorio,...
- Si un servidor de nombres contiene una zona es autorizado para esa zona (authoritative)
 - ¿Qué pasaría si el servidor de una zona deja de estar activo?
 - ¿De qué forma los clientes DNS podrían seguir consiguiendo información?

Zonas

- Balanceo de carga: Para ofrecer rapidez y una mayor tolerancia a fallos
- una misma zona se almacena en varios servidores DNS
 - Servidor maestro o primario
 - Servidor esclavo o secundario: Recibe sus datos por una transferencia de zona

Tipos de servidores DNS

- Por su función
 - Servidor maestro o primario
 - Servidor esclavo o secundario: Transferencias de zona
 - Servidor cache : Cache y TTL (Time To Live)
 - Servidor reenviador (forwarding)
 - Servidor solo autorizado
- **IMPORTANTE** : Un mismo servidor DNS puede combinar varias de estas funciones simultáneamente

Servidores de DNS

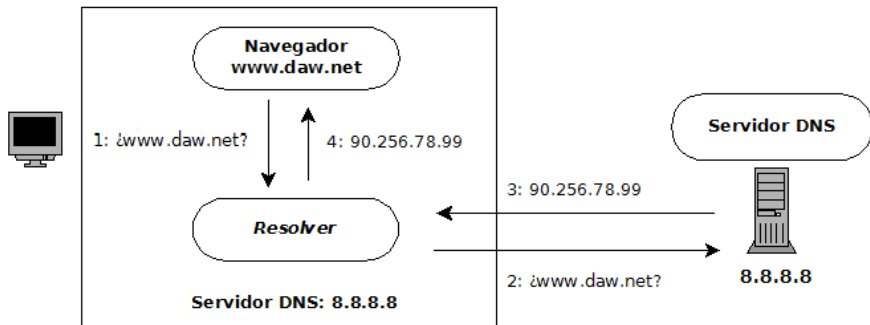
- BIND
- Servidor DNS de Microsoft
- PowerDNS
- NSD
- Simple DNS
- Cisco Network Registrar
- Dnsmasq



Clientes DNS (resolvers)

- Preguntan a los servidores de nombres.
- Integrados en los sistemas operativos.
- Invocados por las aplicaciones (navegadores, clientes FTP, ...)
- Pueden utilizar una cache de respuestas.

Clientes DNS (resolvers)



Clientes DNS (resolvers)

Funcionamiento básico

- El cliente DNS (resolver) consulta al servidor DNS.
- El servidor DNS
 - Si es autorizado (almacena la zona que contienen el nombre de dominio preguntado), responde.
 - Si no es autorizado (no contiene la información) pregunta a otros servidores DNS.
 - **Iterativamente:** Pregunta sucesivamente por los servidores de nombres de las zonas
 - **Recursivamente:** Pregunta a otro servidor DNS
 - El servidor puede *cachear* la respuesta por si otros clientes hacen la misma pregunta, durante un tiempo (TTL)

Registros de recursos

- SOA
- NS
- A
- CNAME
- MX
- PTR
- . . .

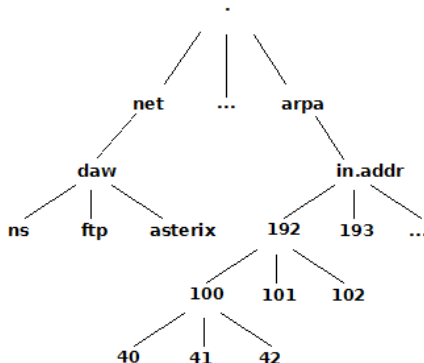


Resolución inversa

- ¿Cual es o cuales son los nombres de dominio asociados a la dirección IP 200.100.89.10?
- Motivos para preguntar por los nombres de dominio asociados a una IP
 - Resolver problemas de red.
 - Detectar spam en los servidores de correo
 - Seguir la traza de un ataque

Resolución inversa

- Espacio de direcciones para resoluciones inversas
 - **in-addr.arpa**: Direcciones IPv4
 - **ip6.arpa**: Direcciones IPv6



Resolución inversa

- Ejemplo Fichero de zona de resolución inversa del dominio 1.100.192.in.addr.arpa. que permite resolver consultas inversas sobre direcciones IP de la red 192.168.168.1.0/24

```
1 ...  
2 100.1.168.in.addr.arpa IN PTR ns.daw.org.  
3 200.1.168.in.addr.arpa IN PTR www.daw.org.  
4 200.1.168.in.addr.arpa IN PTR ftp.daw.org.  
5 220.1.168.in.addr.arpa IN PTR smtp.daw.org.  
6 220.1.168.in.addr.arpa IN PTR zipi.daw.org.  
7 ...
```

Listado 2 : Zona inversa

Resolución inversa

- Las zonas directas e inversas son independientes
 - Pueden estar en diferentes servidores DNS
 - Pueden ser responsabilidad de diferentes empresas
- Es responsabilidad de los administradores que contengan información coherente
- El proceso de resolución inversa es similar al de la directa (consultas recursivas/iterativas, caché ...)

Ampliación

- Transferencias de zona (completas/incrementales)
- DNS dinámico
- *whois*
- Para saber más
 - Servicios de Red e Internet (ISBN: 978-84-1622-832-4)
Editorial Garceta.