Redes de ordenadores

DNS

Grupo de sistemas y comunicaciones
Juan Jesús Muñoz Esteban
jjmunoz@gsyc.inf.uc3m.es

4.DNS

El servicio de nombres permite que los humanos usemos nombres de máquina y sean los ordenadores (resolver-named) quienes los traduzcan a direcciones IP.

El fichero /etc/hosts asocia direcciones IP a nombres de máquinas conocidas:

```
127.0.0.1       localhost                       /* Para pruebas. Siempre está */
163.117.128.84  maquinita nombreoficial.uc3m.es  www.uc3m.es
```

Se utiliza al arrancar (antes de conectarse al servicio de nombres), en combinación con NIS y en pequeñas instalaciones sin Internet.

El NIC registra nombres de máquina en un fichero accesible por ftp anónimo: ftp://nic.ddn.mil/netinfo/hosts.txt. Obviamente era enorme e inmantenible (cada modificación debería difundirse a todos los posibles interlocutores, lo que casi siempre sería un trabajo inútil y la tarea como tal, una quimera).

El DNS (Domain Name Service) forma un base de datos distribuida(repartida), fácilmente ampliable, de mantenimiento descentralizado y jerárquico. Data de 1984, cuando Paul Mockapetris escribe las primeras RFCs sobre name servers, siendo las actuales las RFCs 1034 y 1035.

Los nombres se descomponen en dominios independientes, sin que haya relación entre dominios y rangos de direcciones IP (gestionadas por www.iana.org).

Cada vez que se delega un subdominio, se delega su gestión (incluyendo su sucesiva subdivisión). Una dirección IP en su dominio padre indica dónde está su Name Server, con lo que un sencillo cambio permite moverse a otro proveedor sin que el usuario lo perciba, y sin más retardo que la actualización de los cachés.

El sistema escala muy bien. Si en 1995 eran 180.000 los dominios registrados, el 4 de mayo 1998 han superado los 2.000.000.

4.1 Organización en dominios

Se organiza en una jerarquía de dominios, como un árbol:

Dominio raiz (root): Grupo de root servers, conocidos por todo el mundo (hay varias direcciones donde traerse un fichero con todos ellos, y se emplea para cargar inicialmente el caché del servidor). Lo gestiona InterNIC por delegación de IANA.

Dominios de nivel máximo:

com: comercial	net: network support center
edu: educación	org: otros
gov: gobierno	arpa: ARPANET (obsoleto)
mil: militar	int: organización internacional

o el pais correspondiente: es, de, uk, us... (ISO 3166)

En España, www.nic.es gestiona los nombres de todos los dominios, y no hay organización de segundo nivel (empresa.co.uk, empresa.co.jp, midominiovalido.es)

Dominios secundarios, terciarios (uc3m.es, inf.uc3m.es, gsyc.inf.uc3m.es...)

Un nombre es pues: máquina.subdominio*.dominio

No distingue mayúsculas de minúsculas. Si termina en punto se llama fully quallified o absoluto. Cada componente puede tener hasta 63 caracteres, y la cadena 255.

No tiene por qué haber una asociación directa entre los dominios y las direcciones de red-subred. Una misma máquina puede tener varios interfaces, cada uno con varios nombres (alias).

Además para ciertos servicios se crea un alias (www.map.es puede cambiar de máquina, incluso dinámicamente (Round Robin DNS)).

4.2 Dominio inverso

Direcciones IN-ADDR.ARPA (dominio inverso). Permite obtener el nombre conociendo la dirección IP. Se construye invirtiendo los números que componen la dirección de red, y terminando en in-addr.arpa

Ejemplo: Red 138.117.0.0:

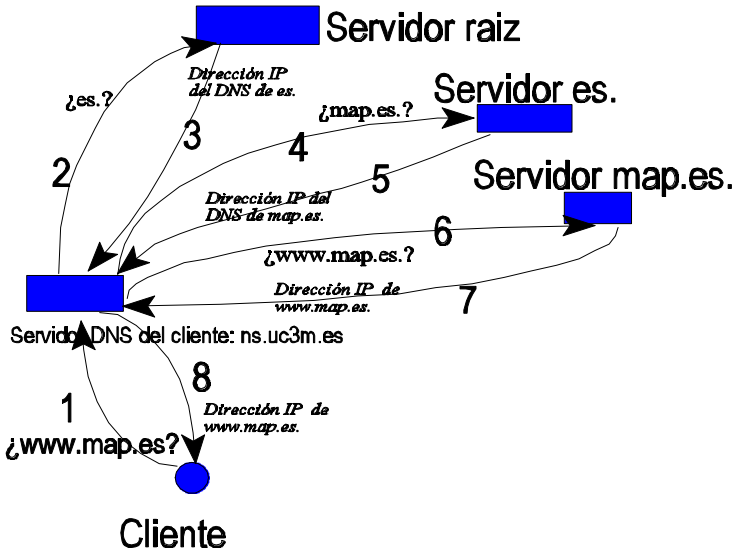
117.138.in-addr.arpa

Se emplea para seguridad: algunos servidores de ftp-anonimous comprueban que realmente esa máquina es quien dice ser (al menos está en DNS), y otros incluso comprueban el dominio (MIT no exporta kerberos fuera de USA por estar clasificado como armamento).

Los servidores WWW lo emplean para obtener sus estadísticas de accesos a sus páginas. Así pueden saber de qué nacionalidad son sus clientes.

4.3 Resolución de direcciones

El cliente conoce su(s) servidores, y les consulta cuando quiere algo:



El comando nslookup permite consultar la información del DNS:

nslookup www.map.es -> 197.4.5.6

Se puede especificar el tipo de datos que se solicitan, de forma interactiva. Así puede especificarse set domain dominio.de.interés, y sobre el realizar distintas consultas (set type=any te da toda la información sobre un objeto, ls toda la información sobre una zona). Con view puedes ver el contenido de un fichero

4.4 Configuración del cliente

Al cliente hay que especificarle a quién consultar (y por orden de preferencia: el primero debería estar en su LAN, ya que va a consultarlo frecuentemente).

Ejemplo (resolv.conf):

```
domain      uc3m.es
server      163.117.137.150
server      163.117.137.151
server      163.117.13.31
```

domain indica el dominio cuando se especifica una dirección no completamente cualificada (que no termina en .) Pueden probarse alternativas a esta cadena para completar el nombre de máquina (search).

El cliente puede tener uno o varios servidores (por tolerancia fallos: si el primero no le contesta, usará el siguiente. En todo caso, solo uno simultáneamente).

Se puede especificar que se use DNS antes o después de mirar al fichero hosts o a las páginas amarillas.

La consulta se hace habitualmente de forma recursiva: la implementación del cliente puede mantenerse muy simple, asumiendo que siempre tendrá una respuesta definitiva pasado un plazo. El servidor tendrá que realizar por él tantas gestiones sean necesarias hasta obtener lo pedido.

Su rendimiento se basa mucho en la utilización de cachés: el cliente almacena las últimas respuestas para próximas consultas. Los servidores actúan de forma similar con la ventaja de poder favorecer al cliente por una consulta previa de otro.

En la consulta los nombres de subdominios se codifican de manera que en lugar del punto se pone un caracter con el número de letras que componen la cadena de la siguiente parte del nombre: 3www4gsyc3inf4uc3m2es

4.5 Configuración de un servidor DNS

Los servidores pueden dar respuestas:

(Authoritative)

Servidor primario: Origen de todos los datos del dominio.

Servidores secundarios: Se copian periódicamente la base de datos del primario, y son su respaldo (RedIris prohibe ser secundario de un subdominio sin que exista delegación: podría emplearse para spoofing).

(Non-authoritative)

Servidores caching-only: Hacen preguntas a otros servidores, manteniendo una cache con las respuestas. Solo les preguntan sus clientes, y dan esta respuesta almacenada en su caché en lugar de ir en ese momento a resolverlo por la red (acelera y consume menos ancho de banda).

El funcionamiento del servidor suele ser iterativo: consulta a raíz por el nombre del dominio (salvo que ya lo tenga en su caché de una reciente consulta anterior), y como respuesta obtendrá la dirección de un servidor de nombres del dominio, al que enviará la siguiente consulta para volver a obtener la dirección de otro “name server” del subdominio o la respuesta final.

En ocasiones puede configurarse para que no consulte al raíz, sino a otro servidor local (forwarder) que esté en la zona de Internet de la organización, de manera que la organización interna quede oculta.

4.6 Resource Records

La información en DNS se almacena en RRs, registros normalizados cuyo formato es, según la RFC 1033:

[nombre] [ttl] IN tipo datos

Nombre (del objeto): Nombre de máquina o de dominio.

nombre.de.dominio	relativo al dominio actual, que se concatena automáticamente.
nombre.de.dominio**.**	absoluto o fully quallified

Si está en blanco, se refiere al de la línea anterior.

ttl (time to live): Tiempo, en segundos, que se mantendrá ese dato en la cache. En el inicio del fichero se especifica su valor por defecto para ese dominio.

IN es la clase que se aplica en Internet. Hay otra, experimental, definida en el MIT.

Tipos de RRs : definen los valores que se pueden consultar:

-A	(Address)	dirección IP de una máquina
-MX	(Mail Exchange)	lista priorizada de dónde entregar el correo.
-SOA	(Start of Authority)	comienzo de los datos de esa zona.
-NS	(Name Server)	Indica un servidor de nombres.
-PTR	(Pointer)	alias para una dirección IP
-CNAME	(Canonical Name)	nombre del dominio (alias)
-HINFO	(Host Information)	descripción de las características.
-WKS	(Well Known Service)	puertos/servicios disponibles
-TXT		Cadena de texto sin mayor interpretación

4.7 Configuración

BIND (Berkeley Internet Name Domain) es la implementación más extendida en Unix. Puede encontrarse en www.isc.org, siendo la versión actual la 8.1.2 (Berkeley hasta la 4.8.3) . El cliente se llama resolver, y es una librería que se enlaza en el sistema operativo y captura las llamadas a gethostbyname() traduciendolas a consultas DNS en lugar de a búsquedas en el fichero hosts. El servidor named y tiene varios ficheros de configuración, donde se especifica de qué dominios es primario o secundario y en qué ficheros debe organizar la información.

Los ficheros que contienen la configuración tienen un formato similar, en forma de lista de Registros de Recursos escritos como tablas editables (internamente los codifica en binario por eficiencia)

/etc/named.boot:	Parámetros generales del servidor: nombres del resto de ficheros (En nuevas versiones puede llamarse named.conf, y su formato interno puede haber cambiado).
Y colgando de /etc/named	(Salvo que se haya especificado otro nombre)
named.db	Los datos del dominio (nombre genérico de una db)
named.ca	Cache. Inicialmente direcciones de servidores del dominio raíz.
named.hosts	Fichero de zona con las direcciones IP de nombres de host.
named.local	Resolución local de la dirección loopback.
named.rev	Fichero de zona del dominio inverso.

En definitiva, hay un fichero por cada dominio que se sirve (ya sea primario, creado en esta máquina con un editor, ya sea secundario, y DNS se lo trae al arrancar).

4.8 Ejemplo

```
gsyc.inf.uc3m.es    IN    SOA     ns.gsyc.inf.uc3m.es.
                                  root.gsyc.inf.uc3m.es. (
                      9810122200  ; Número de serie: actualizar en cada cambio
                                  ; rediris recomienda poner la fecha
                      28800       ; Refresco a las 8 horas
                      7200        ; Reintento tras 2 horas
                      604800      ; Expira después de una semana
                      86400 )     ; TTL mínimo de 1 día

gsyc.inf.uc3m.es      IN    NS      ns.gsyc.inf.uc3m.es
gsyc.inf.uc3m.es      IN    MX      10 ordago
localhost.            IN    A       127.0.0.1
ordago                IN    A       163.117.137.150
lareal                IN    A       163.117.137.151
ns                    IN    CNAME   ordago.gsyc.inf.uc3m.es.
www                   IN    CNAME   ordago.gsyc.inf.uc3m.es.
```

Ejemplos en ftp://ftp.isc.org/isc/bind

ÍNDICE