Servizo DNS

Sumario

Introdución

DNS ou *Domain Name System* é o sistema estándar en Internet para asociar nomes a direccións IP. Estas direccións identifican máquinas, por exemplo a dirección 10.22.1.10, pero para as persoas é máis doado traballar con nomes, como www.iessanclemente.net. Ademais, é máis probable que cambie unha dirección IP que un nome. Por contra, o sistema implica un certo retardo asociado á ?tradución? de nomes a direccións IP, na maior parte dos casos, despreciable para o usuario.

Os RFC 1034 e o RFC 1035 especifican a implementación e configuración do DNS para a versión 4 do IP. As extensións para admitir a versión 6 do protocolo están no RFC 1886.

O DNS úsano outros protocolos do nivel de aplicación (HTTP, SMTP, etc.) pero non os usuarios directamente (salvo os administradores da rede que usan ferramentas como `dig` ou `nslookup` para facer consultas directas aos servidores).

Nomes de dominio

Para entender o servizo que proporciona o DNS pódese establecer unha analoxía co sistema telefónico, onde unha persoa pode saber uns cantos números de teléfono, pero se descoñece algún chama a un teléfono de información. No DNS é similar, xa que existe o Servidor de Nomes de Dominio que ten unha IP á cal os clientes DNS "chaman" para averiguar cal é a IP asignada a un nome de dominio.

Os clientes DNS configúranse indicando a IP do servidor de DNS que pode resolver as súas consultas. Tal e como xa vimos na unidade 2 isto realízase en GNU/Linux a través do ficheiro `/etc/resolv.conf`, onde se definen dous tipos de servidores:

- **Servidor DNS primario** ou preferido. É ó primeiro servidor ao que se lle vai consultar.
- **Servidor DNS secundario** ou alternativo. Este servidor é consultado no caso de que falle o primeiro.

INTERÉSACHE

Dominio ou nome de dominio. É o nome que identifica a unha máquina, frecuentemente un sitio web. O dominio ten que ser único, aínda que un servidor pode aloxar dominios distintos.

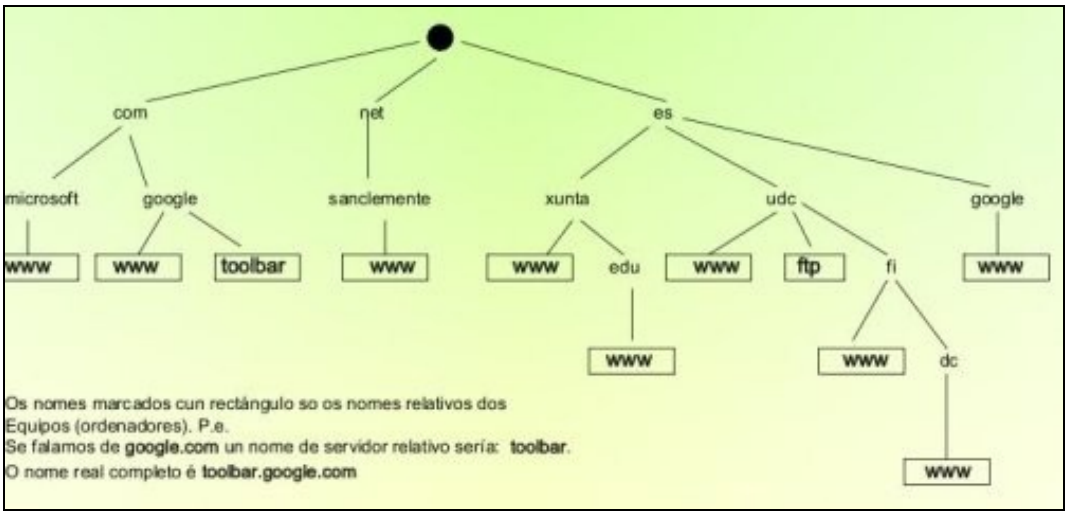
Algúns exemplos de nomes de dominio son:

- **xunta.es**. É un dominio, e ao mesmo tempo xunta é un subdominio de .es
- **edu.xunta.es**. É un dominio, e ao mesmo tempo edu é un subdominio de xunta.es
- **www.xunta.es**. É o equipo que executa o servizo Web (www) dentro do dominio xunta.es
- **www.edu.xunta.es**. É o equipo que executa o servizo Web (www) dentro do dominio edu.xunta.es

Estrutura xerárquica

Os nomes de dominio están estruturados en forma de árbore desde a raíz (representada por un ? . ?,) ata o nivel inferior. A esta estrutura chámaselle **espazo de nomes de dominio**. Cada nivel sepárase do superior por un punto ?. ?.

Aos dominios que se atopan xusto debaixo do dominio raíz ? . ? chámaselles **dominios de primeiro nivel**.



Cada nodo da árbore é unha etiqueta de **63 caracteres como máximo**. Entón, podemos redefinir agora un nome de dominio como a secuencia formada polas etiquetas existentes no camiño entre un nodo e a raíz. Este nome de dominio completo chámase **nome de dominio completamente cualificado** ou *Fully Qualified Domain Name* (**FQDN**).

Dominios de primeiro nivel

Son os que están xusto debaixo do nodo raíz. Tamén se lles chama *Top Level Domains* ou **TLD**. Hai varios tipos: organizativos, xeográficos e de recente creación.

Dominios Organizativos (gTLD)

Creáronse inicialmente para organizar Internet en EE.UU e son os seguintes:

- **.COM**. Inicialmente era para empresas, hoxe está aberto a calquera cousa.
- **.NET**. Inicialmente era para empresas e organismos relacionados coa Rede, hoxe tamén está aberto a outras organizacións.
- **.ORG**. Inicialmente era para organismos de EE.UU. sen ánimo de lucro, hoxe está aberto a calquera cousa.
- **.MIL**. Inicialmente era para organismos militares de EE.UU. e hoxe séguео sendo.
- **.EDU**. Inicialmente era para universidades de EE.UU. e hoxe está aberto ao ámbito educativo.
- **.GOV**. Inicialmente era para organismos relacionados co goberno de EE.UU. e hoxe séguео sendo.
- **.INT**. Inicialmente era para organismos internacionais, p.e. www.eu.int, e hoxe séguео sendo.

Dominios xeográficos (ccTLD)

Xurdiron cando Internet se expandiu alén dos EE.UU e son os dominios que representan a organismos, empresas, etc. dun determinado país, como por exemplo, **.ES** (España), **.UK** (Reino Unido), **.BR** (Brasil), **.DE**, (Alemaña), **.PT** (Portugal), etc.

España, como outros países, non fixo control sobre os dominios secundarios ao contrario que Reino Unido (i.e. co.uk, gov.uk, org.uk) ou Brasil.

Dominios de recente creación

Son dominos creados para atender ás novas necesidades como, por exemplo, **.MAIL**, **.INFO**, **.MUSEUM**, etc. En http://www.internic.net ou en http://www.icann.org están todos.

Funcionamento

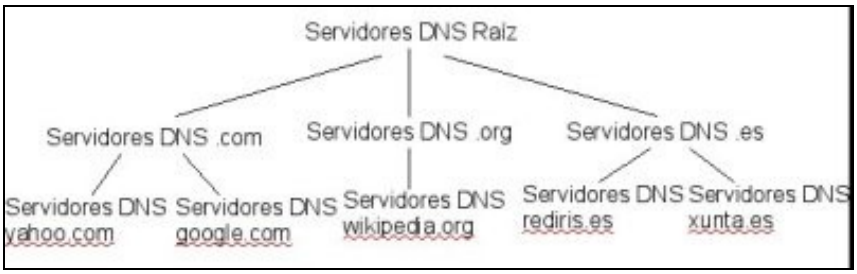
O DNS funciona como unha base de datos (BBDD) distribuída e xerarquizada que se consulta para achar a IP asociada a un nome de dominio. Os motivos para descentralizar a BBDD, principalmente, son:

- Evitar ter un único punto de fallo.
- Balancear a carga xa que o volume de tráfico é importante.
- Evitar retardos derivados da distancia que pode existir a unha única BBDD centralizada.
- Favorecer a escalabilidade do sistema.

Ao proceso de averiguar a IP asociada a un nome de dominio coñéceselle co nome **resolución DNS** ou **resolución de nomes**.

Tipos de servidores

Os servidores DNS non saben todas as IP e nomes de dominio existentes. Os servidores organízanse en forma de árbore, de tal xeito que se un servidor non é quen de resolver un nome de dominio, reenvía a pregunta a outro servidor ata atopar o nome de dominio ou obter unha resposta negativa, como se verá máis adiante.



Nesa estrutura de árbore hai tres tipos de servidores:

- **Servidores DNS raíz**. Cando o Servidor de DNS primario, que actúa como caché, non atopa información nas súas bases de datos locais nin na súa caché pregunta a un servidor DNS raíz. Por defecto o servidor de DNS primario ven configurado cunha lista de servidores raíz (13 servidores) aos que preguntar para estes casos.

- **Servidores DNS de primeiro nivel** ou *Top Level Domain*. Son os responsables dos dominios .com, .org, .net, .edu, etc., e de todos os dominios de primeiro nivel dos países: es, uk, fr, ca, jp, etc.
- **Servidores de zona autorizados**. Son os servidores de DNS das empresas, universidades ou calquera outra insitución que teña un dominio propio, por exemplo, xunta.es, e equipos dentro dese dominio coas súas IP asociadas (por exemplo, www.xunta.es ou ftp.xunta.es). Pode estar administrado pola mesma organización ou por un ISP.

Existe outro tipo de servidor DNS que estaría fóra da xerarquía propiamente dita. Son os **servidores de DNS caché** que unicamente fan consultas a outros servidores para resolver nomes, por exemplo, o servidor DNS primario do instituto.

Proceso de resolución de nomes

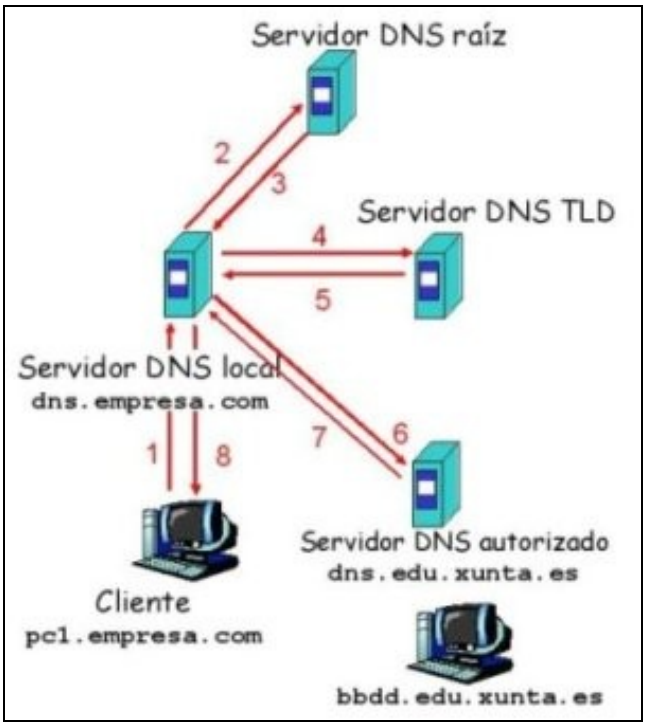
Hai dúas formas de resolver os nomes, en **modo iterativo** e en **modo recursivo**.

Modo iterativo

Supoñamos que un cliente quere a IP de www.google.com. O proceso para resolver un nome, grosso modo, sería o seguinte:

1. O cliente consulta un **servidor DNS raíz** para atopar un servidor DNS para **.com** (servidor Top Level Domain).
2. O cliente consulta un **servidor DNS .com** para obter un servidor DNS para **google.com** (servidor autorizado).
3. O cliente consulta o servidor **DNS de google.com** para obter a dirección de **www.google.com**.

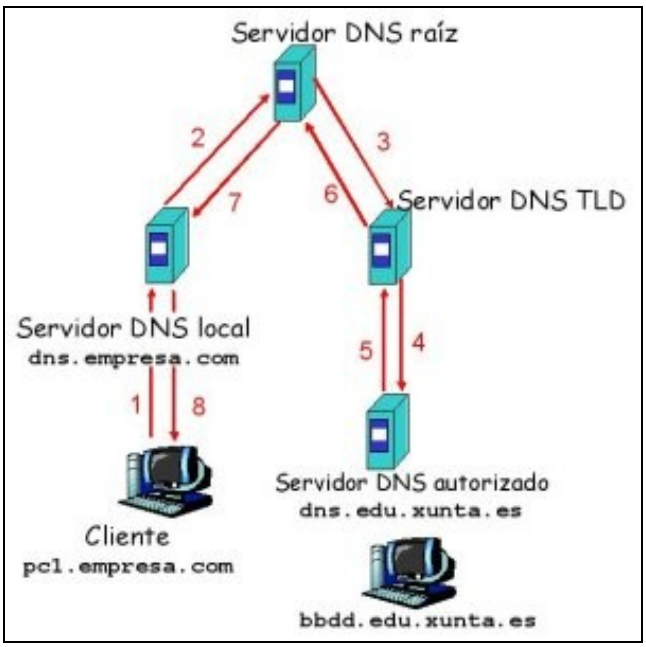
Vexamos, máis en detalle, outro exemplo de funcionamento en modo iterativo. O computador pc1.empresa.com necesita a dirección IP de bbdd.edu.xunta.es. O proceso sería como se amosa na seguinte figura:



Cando se contacta cun servidor de DNS que non sabe a resposta, este envía o nome doutro servidor: ?Non coñezo ese nome. Pregúntalle a este servidor?.

Modo recursivo

O modo recursivo é máis custoso para o sistema de DNS xa que delega totalmente nos servidores o proceso. Por iso, frecuentemente, os servidores teñen esta funcionalidade deshabilitada. Vexámolo cun exemplo: o computador pc1.empresa.com necesita a dirección IP do nome de dominio bbdd.edu.xunta.es.



O modo recursivo pode supoñer moita carga para os servidores de niveis superiores, polo que non sempre está soportado.

Na seguinte ligazón pódese explorar os distintos funcionamentos do DNS (recursivo e iterativo).

Reenvío

Os servidores de DNS poden funcionar en modo iterativo ou recursivo. Con todo, cando se configura un servidor de DNS pode interesar que este pregunte a outro/s servidor/es de DNS concreto/s antes de comezar o proceso de recursividade ou iterativo. É dicir, un servidor de DNS pode reenviar a consulta a un servidor DNS concreto.

Por exemplo, a Xunta é a Provedora de Servizos de Internet (ISP) dos IES. Como tal, ofrécelles dous servidores de DNS aos que os programas clientes dos centros poden facer as súas peticións de resolución DNS. Estes servidores xestionan o dominio xunta.es. Agora ben, o centro ten a súa propia intranet local co seu servidor de DNS local (10.0.0.36). Os clientes do centro preguntan a 10.0.0.36, o cal está configurado para reenviar aos servidores de DNS da Xunta as consultas que non poida resolver (que non teña en cache). No caso de que os servidores de DNS da Xunta non atopen nada na súa cache usarán o modo iterativo ou recursivo, en función de como estean configurados. Unha vez que teñan unha resposta almacenaraa na cache respostaranlle ao servidor local. O servidor DNS local almacenará na cache, á súa vez, as respostas e enviaraas ao cliente.

Zonas DNS

Para facer manexable a xestión e administración do sistema de nomes de dominio os seus nodos están agrupados en zonas. Cada zona está formada por un nodo chamado superior e todos os que se atopen nos niveis xerarquicamente inferiores, ata chegar aos nodos terminais.

Por exemplo, unha zona pode corresponder a un país e as súas subzonas poden corresponder a organizacións deste país. Cara organización á súa vez pode crear subzonas para diferentes departamentos, etc.

O obxectivo de agrupar nodos en zonas consiste en asignar a un **servidor autorizado** a responsabilidade sobre todos os nodos da súa zona. O administrador encargado dese servidor autorizado pode engadir ou borrar nodos dentro da súa zona, modificar a información dos seus nodos, crear subzonas, etc.

Un servidor autorizado para unha zona pode contestar directamente as consultas que reciba sobre os nodos da súa zona, sen necesidade de acceder a outros servidores. Neste caso dise que o servidor enviará **respostas con autoridade**.

Se unha consulta se refire a outra zona, o servidor DNS empregará o modo recursivo ou iterativo para xerar a resposta. Os servidores de DNS engaden a información obtida á cache para que, se se lles solicita a mesma información, non sexa necesario pedila de novo a outros servidores. Se os datos se modificaron no servidor de orixe desde que se solicitaron por primeira vez o servidor debe avisar ao cliente de que lle envía unha **resposta sen autoridade**.

Para ofrecer unha alta fiabilidade no servizo, para cada zona pode haber dous servidores con autoridade:

- **Servidor primario**. Garda os ficheiros orixinais da base de datos correspondente á zona, é dicir, aqueles que o administrador debe actualizar directamente cada vez que haxa unha modificación nos seus nodos.
- **Servidor secundario**. Refrescan (actualizan automaticamente) as súas bases de datos a partir das do primario, por medio de consultas periódicas para saber se houbo algún cambio. A transferencia de zonas realízase mediante TCP.

Rexistros de recurso

A información asociada a unha zona consta dun conxunto de rexistros de recurso. Os rexistros de recurso de todos os nodos forman a base de datos DNS. Estes rexistros pódense consultar cos comandos dig ou co nslookup. Os principais rexistros de recurso son os seguintes:

- **Type=NS**. Nome do servidor DNS autorizado para ese dominio.
- **Type=A**. Dirección IP dun nome de dominio.
- **Type=SOA**. Información sobre o nodo superior dunha zona.
- **Type=CNAME**. Nome canónico (real) dun nome de dominio, por exemplo: www.ibm.com realmente é servereast.backup2.ibm.com.
- **Type=MX**. Nome do servidor de correo asociado a un dominio.

Así, se por exemplo tecleamos o seguinte:

```
nslookup
>set q=CNAME
>www.ibm.com
```

Obteremos como resposta:

```
Non-authoritative answer:
www.ibm.com     canonical name = www.ibm.com.cs186.net.
```

O proceso de refresco dunha zona nun servidor secundario consiste en pedir ao primario o seu rexistro SOA e comprobar se variou o campo SERIAL. Se variou, é preciso levar a cabo unha transferencia dos datos da zona cunha petición de transferencia total (AXFR) ou incremental (IXFR), e, se non, non é necesario facer nada. A transferencia entre servidores pode realizarse, por exemplo, por medio do protocolo FTP.

Zonas de busca inversa

Ás veces é interesante dada unha IP averiguar cal é nome de dominio que ten asignado. Isto é útil cando se ten un conflito IP (máis dunha máquina coa mesma IP) e se desexa averiguar quen é o causante. Así, faise un ping <IP en conflicto> e saberase o nome dos afectados.

Para elo é preciso dar de alta unha zona de busca inversa no servidor de DNS que teña asociadas IP a Nomes.

Estas zonas tamén as usas os servidores de correo smtp, como se verá máis adiante.

O ficheiro hosts

Todo cliente DNS ten un ficheiro HOSTS, onde se almacenan estaticamente asociacións de nomes de equipos (con ou sen o dominio) e as súas direccións IP. Este ficheiro sempre ten a entrada de loopback 127.0.0.1 asociada a localhost e só é modificable por administradores. O equipo consultará sempre o ficheiro hosts antes de facer unha consulta ao DNS.

Instalación e configuración do BIND

En Internet o paquete BIND (*Berkley Internet Naming Daemon*) é o servidor de DNS máis utilizado, aínda que existen outras alternativas.

Instalación

Para instalar o BIND só hai que teclear:

```
sudo apt-get install bind9
```

Os ficheiros de configuración do BIND en Ubuntu están no cartafol /etc/bind/. A instalación tamén crea un usuario bind.

BIND como DNS cache

Un servidor de nomes cache só ten configurada unha zona ou dominio que indica que é un servidor cache. Cando o servidor recibe unha solicitude de resolución, pregunta a outro con autoridade sobre a zona solicitada e este transmitiralle a información da mesma.

Para configurar o BIND como DNS cache habería que crear un ficheiro de configuración no cartafol /etc/bind/. Este ficheiro chámase named.conf e debería ter o seguinte contido:

```
zone "." {
        type hint; //Indica que é unha zona de tipo cache
        file "/etc/bind/db.root";
};
```

A configuración por defecto do servidor xa ten configurado este ficheiro, polo que xa permite resolver nomes de dominio dos computadores en Internet sen facer nada. O ficheiro /etc/bind/db.root trae configurados os servidores de DNS raíz aos que consultar o nome de calquera equipo. Ao instalar o bind9 o sistema xa realiza o seu arranque de xeito automático. Se non fose así, para arrancar o servidor DNS pódese facer como calquera outro servizo tecleando:

```
sudo /etc/init.d/bind9 start
```

Servidor de DNS con autoridade

Servidor de DNS escravo