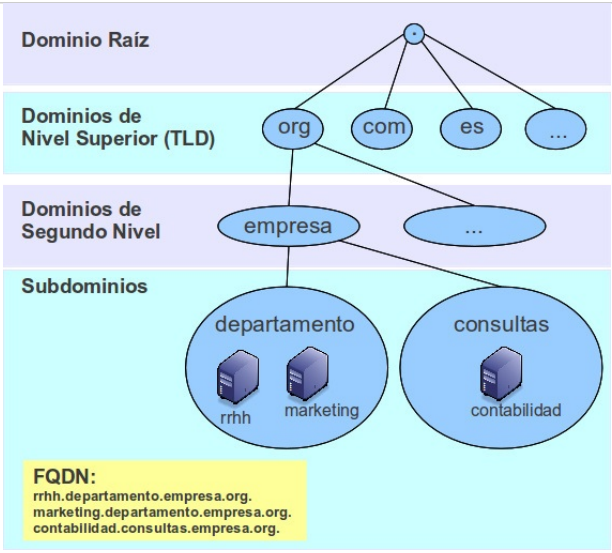
DNS (Domain Name Server)



Nomenclatura DNS

DNS: O sistema DNS é unha base de datos distribuída, que permite a administración local de segmentos que xuntos compoñen toda a base de datos local. Os datos de cada segmento están dispoñibles para toda a rede a través dun esquema cliente-servidor xerárquico.

Servidor DNS: Permite resolver hostnames a IPs e viceversa.

/etc/hosts: Ficheiro que soe ter preferencia (ver `/etc/nsswitch.conf`) na resolución de nomes sobre o servidor DNS. Permite alias de nomes de dominios, é dicir, unha mesma IP pode apuntar a nomes distintos. Cada liña do ficheiro comezará con unha IP e na mesma liña separados por espazos ou tabuladores podes escribir os nomes de dominios correspondentes. O primeiro nome, o máis preto á IP, é considerado o principal, os demais son alias de éste.

/etc/resolv.conf: Ficheiro de configuración que permite definir os servidores DNS a empregar mediante a directiva nameserver.

/etc/nsswitch.conf: Ficheiro de configuración das Bases de Datos do Sistema e do sistema de Conmutación dos Servizos de Nomes (Name Service Switch - NSS), é dicir, establece a orde de búsqueda das bases de datos que ten definidas. A base de datos que corresponde á resolución DNS é hosts. Así, se neste ficheiro atopamos: `hosts: files dns` na resolución DNS prevalece o existente en /etc/hosts(files) sobre o ficheiro /etc/resolv.conf(dns).

Zona DNS: É aquela parte do DNS para a cal se delegou a administración. é dicir, cando se configura un dominio nun servidor DNS este debe pertencer a unha zona. Así, nos arquivos de configuración de zona indicarase que IP vai co servizo web www, o servizo de correo mail, etc.

Zona de Procura Directa: As resolucións desta zona devolven a dirección IP correspondente ao recurso solicitado. Realiza as resolucións que esperan como resposta a dirección IP dun determinado recurso.

Zona de Procura Inversa: As resolucións desta zona buscan un nome de equipo en función da súa dirección IP; unha procura inversa ten forma de pregunta, do estilo: Cal é o nome DNS do equipo que utiliza a dirección IP `192.168.100.10`?.

DNS Dinámico: É un sistema que permite a actualización en tempo real da información sobre nomes de dominio situados nun servidor de nomes, sendo usado maioritariamente para asignar un nome de dominio da internet a un computador con dirección IP variable (dinámica). O DNS dinámico, así, pode ofrecer servizos na internet en hosts que posúan conexión con dirección IP dinámica, a típica configuración que os ISP ofrecen para conectarse a Internet.

Servidores primarios (primary name servers): Estes servidores almacenan a información da súa zona nunha base de datos local. Son os responsables de manter a información actualizada e calquera cambio debe ser notificado a este servidor.

Servidores secundarios (secundary name servers): Tamén chamados escravos, aínda que tamén poden ser mestres doutros servidores secundarios. Son aqueles que obteñen os datos da súa zona desde outro servidor que teña autoridade para esa zona. O proceso de copia da información denomínase transferencia de zona.

Servidores mestres (master name servers): Os servidores mestres son os que transfiren as zonas aos servidores secundarios. Cando un servidor secundario arrinca busca un servidor mestre e realiza a transferencia de zona. Un servidor mestre para unha zona pode ser á vez un servidor primario ou secundario desa zona. Así, evítase que os servidores secundarios sobrecarguen ao servidor primario con transferencias de zonas. Os servidores mestres extraen a información desde o servidor primario da zona

Servidores só caché (caching-only servers): . Os servidores só caché non teñen autoridade sobre ningún dominio: limítanse a contactar con outros servidores para resolver as peticións dos clientes DNS. Estes servidores manteñen unha memoria caché coas últimas preguntas contestadas. Cada vez que un cliente DNS formúlalle unha pregunta, primeiro consulta na súa memoria caché. Se atopa a dirección IP solicitada, devólvella ao cliente; se non, consulta a outros servidores, apunta a resposta na súa memoria caché e comunícalle a resposta ao cliente. Se o noso caché DNS almacena a gran maioría de peticións que se realizan desde a rede local, as respostas dos clientes satisfaranse practicamente de forma instantánea proporcionando ao usuario unha sensación de velocidade na conexión. Todos os servidores DNS gardan na caché as consultas que resolveron.

Transferencia de zona: O proceso de copia da información de zonas entre servidores DNS denomínase transferencia de zona. Unha transferencia de zona pode darse: cando vence o intervalo de actualización dunha zona, cando un servidor mestre notifica os cambios da zona a un servidor secundario, cando se inicia o servizo Servidor DNS nun servidor secundario da zona, cando se utiliza o comando rndc nun servidor secundario da zona para iniciar manualmente unha transferencia desde o seu servidor mestre

Servidores raíz: Os servidores de raíz son entidades distintas. Hai 13 servidores raíz ou, máis precisamente, 13 direccións IP na internet nas que poden atoparse aos servidores raíz (os servidores que teñen unha das 13 direccións IP poden atoparse en ducias de localizacións físicas distintas). Todos estes servidores almacenan unha copia do mesmo arquivo que actúa como índice principal das axendas de direccións da internet. Enumeran unha dirección para cada dominio de nivel principal (.com, .es, etc.) na que pode atopase a propia axenda de direccións dese rexistro. Os trece servidores raíz DNS denomínanse polo primeiras trece letras do alfabeto latino, da **A ata a M (`A.ROOT-SERVERS.NET., B.ROOT-SERVERS.NET., ... , M.ROOT-SERVERS.NET.`)**, e están en mans de 12 organizacións independentes.

Rexistros DNS: Cada zona DNS mantén un conxunto de rexistros de recursos (RR) estruturados.

Recursividade: Un servidor DNS tamén pode consultar ou poñerse en contacto con outros servidores DNS en nome do cliente DNS solicitante para resolver o nome por completo e, a continuación, enviar unha resposta ao cliente. Este proceso chámase recursividade.

Iteración: Un cliente DNS pode tentar poñerse en contacto con servidores DNS adicionais para resolver un nome. Cando un cliente fai isto, utiliza consultas adicionais e independentes en función de respostas de referencia dos servidores. Este proceso chámase iteración.

Xerarquía de nomes de dominio

O espazo de nomes de dominio (o universo de todos os nomes de dominio) está organizado de forma xerárquica. O nivel máis alto na xerarquía é o dominio raíz, que se representa como un punto (".") e o seguinte nivel na xerarquía chámase dominio de nivel superior (**TLD**). Só hai un dominio raíz, pero hai moitos TLDs e cada TLD chámase dominio secundario do dominio raíz. Neste contexto, o dominio raíz é o dominio principal, xa que está un nivel por encima dun TLD e cada TLD, á súa vez, poden ter moitos dominios fillos. Os fillos dos dominios de nivel superior chámanse de segundo nivel, os do segundo nivel chámanse de terceiro nivel, os do terceiro nivel de cuarto, e así sucesivamente.
Por tanto o DNS, organiza os nomes de máquina (hostname) nunha xerarquía de dominios separados polo carácter punto '.'. Un dominio é unha colección de nodos relacionados dalgunha forma -porque están na mesma rede, tal como os nodos dunha empresa-. Por exemplo:

rrhh.departamento.empresa.org
marketing.departamento.empresa.org
contabilidade.consultas.empresa.org

onde:

- A empresa agrupa as súas nodos no dominio de primeiro nivel `org`. Este é un TLD.
- A empresa ten un subdominio, dominio de segundo nivel `empresa` baixo `org`. Así `empresa` é un dominio de segundo nivel, fillo do TLD `org`.
- Á súa vez podes atopar novos subdominios dentro, neste caso: `departamento` e `consultas`. É dicir, dominios de terceiro nivel, fillos á súa vez do dominio de segundo nivel `empresa`.
- Finalmente, un nodo que terá un nome completo coñecido como totalmente cualificado ou FQDN, que é a concatenación de: TLD, dominio de segundo nivel, dominio de terceiro nivel, etc., tal como:
  - `rrhh.departamento.empresa.org.`
  - `marketing.departamento.empresa.org.`
  - `contabilidade.consultas.empresa.org.`

Na figura podes ver unha parte do espazo de nomes. A raíz da árbore, que se identifica cun punto sinxelo, é o que se denomina dominio raíz e é a orixe de todos os dominios. Para indicar que un nome é FQDN, ás veces termínase a súa escritura nun punto, aínda que polo xeral se omite. Este punto significa que o último compoñente do nome é o dominio raíz. Así, por exemplo no nome de dominio:

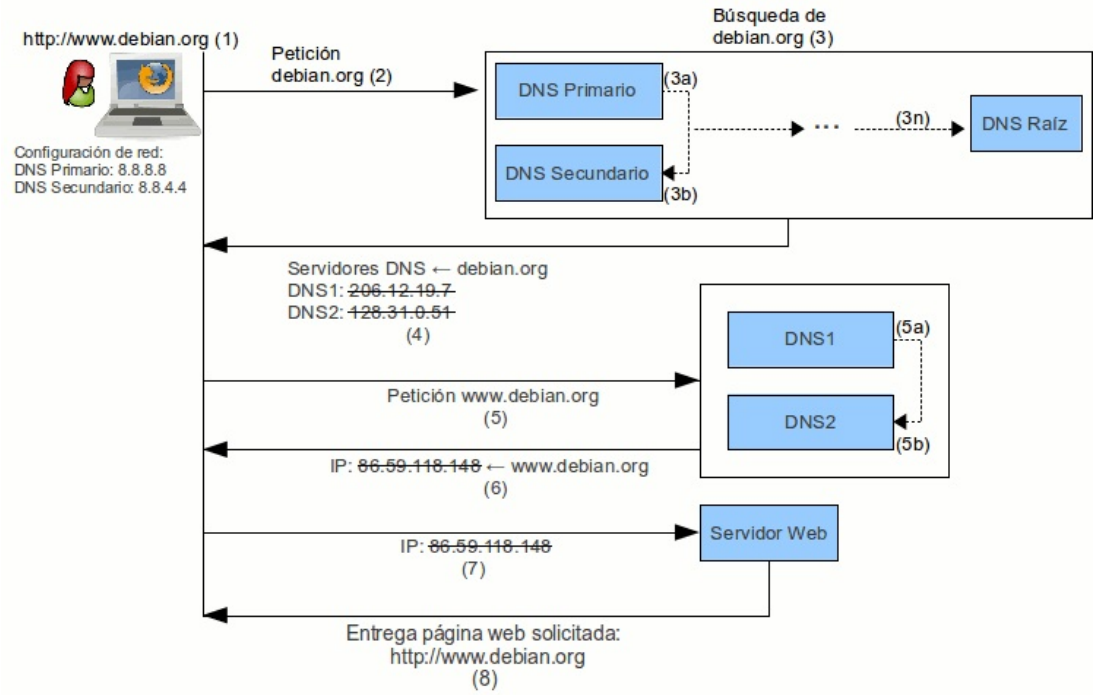
rrhh.departamento.empresa.org.

O símbolo do dominio raíz é o punto situado máis á dereita do nome do dominio.
Só hai unha raíz de dominio, pero **hai máis de 1500 dominios de nivel superior**, clasificados no seguintes tres tipos:

- TLD de código de país (ccTLD): dominios asociados con países e territorios. Hai máis de 240 ccTLD. Están formados por 2 letras, por exemplo: `es`, `uk`, `en`, e `jp`.
- Dominios de nivel superior xenéricos (gTLD): Están formados por 3 ou máis letras. Á súa vez se subdividen en:
  - Dominios da internet patrocinados (sTLD): Representan unha comunidade de intereses, é dicir, detrás existe unha organización ou organismo público que propón o dominio e establece as regras para obtar ao devandito dominio. Por exemplo: `edu`, `gov`, `int`, `mil`, `aero`, `museum`.
  - Dominios da internet non patrocinados (uTLD). Sen unha organización detrás que estableza as regras para obtar ao devandito dominio. A lista de gTLD inclúe: `com`, `net`, `org`, `biz`, `info`.

Funcionamento do DNS

A seguinte imaxe presenta graficamente o funcionamento do DNS, tomando como exemplo a páxina web `www.debian.org` e considerando que a información da petición do dominio para buscar non se atopa no teu computador ou nun servidor DNS local existente na túa rede ou no teu computador.



1. A través do teu navegador queres consultar a páxina web oficial de Debian escribindo na barra de direccións a URL `http://www.debian.org`.
2. O navegador busca a información das DNS do dominio `debian.org`.
3. Internet está ordenada en forma de árbore invertida, se non atopa a información no teu computador, irá buscala aos servidores DNS que posúes na configuración de rede do teu computador, tipicamente os proporcionados polo teu Provedor de Servizos a Internet (ISP): `DNS Primario (3a)` ou `DNS Secundario (3b)`. De non estar, seguirá buscándoa a niveis superiores, e en último lugar atoparao no Servidor de Nomes Raíz: `DNS Raíz (3n)`.
4. A información buscada: as IP correspondentes ao servidor DNS que goberna o dominio `debian.org`, chega ao teu computador: `DNS1` → ~~`206.12.19.7`~~ e `DNS2` → ~~`128.31.0.51`~~. Adoitan ser dous porque as especificacións de deseño de DNS recomendan que como mínimo deben existir dous servidores DNS para aloxar cada zona, á que pertence cada dominio.

O teu computador agora tentará conectar co servidor `DNS1 (5a)` ou ante calquera problema de conexión con este tentarao co servidor `DNS2 (5b)`. Estes son os servidores de nomes onde se atopa información acerca de onde se pode buscar a páxina web (servidor da web), unha dirección de correo electrónico (servidor de correo), etc.

5. O teu computador recibirá a información acerca da localización da páxina web, ou sexa, a dirección IP do servidor web onde está aloxada a páxina.
6. O teu computador dirixirase logo ao servidor web e buscará a páxina web en éste.
7. Por último, o servidor web devolve a información pedida e ti recibes a páxina web, visualizándoa no navegador.

Pero, e se volves consultar a páxina web oficial de Debian escribindo na barra de direccións a URL `http://www.debian.org`, repetirase de novo todo o proceso? Para contestar este pregunta hai que establecer dúas situacións:

1. O host desde o que volves realizar a consulta é o mesmo: Se non o é, antes de repetir todo o proceso tentaríase co exposto no seguinte punto, pero se é o mesmo, ao facer a consulta desde este host, a resolución dominio-IP se garda durante algún tempo na memoria caché do mesmo, polo cal non será necesario repetir todo o proceso de novo. Se o tempo no que a memoria caché garda a resolución expirou volverá repetir o proceso de novo.
2. Existe un servidor DNS caché na túa rede ou no teu host: por tanto, se un segundo cliente, que ten configurado este servidor DNS, volve realizar a mesma petición, como este servidor ten a resposta almacenada na súa memoria caché, responderá inmediatamente sen ter que cursar a petición a ningún servidor DNS da internet. Se o tempo no que a memoria caché garda a resolución expirou volverá repetir o proceso de novo.

Tipos de rexistros DNS

Todos os rexistros de recursos (RR) teñen un formato definido que utiliza os mesmos campos de nivel superior, segundo descríbese na táboa seguinte:

Formato dos rexistros de recursos DNS	
Campo	**Descrición**
Propietario	Indica o nome de dominio DNS que posúe un rexistro de recursos. Este nome é o mesmo que o do nodo da árbore da consola onde se atopa un rexistro de recursos.
Tempo de vida (TTL)	Para a maior parte dos rexistros de recursos, este campo é *opcional*. Indica o espazo de tempo utilizado por outros servidores DNS para determinar canto tarda a información en caché en caducar un rexistro e descartalo. Por exemplo, a maior parte dos rexistros de recursos que crea o servizo do servidor DNS herdan o TTL mínimo (predeterminado) de 1 hora desde o rexistro de recurso de inicio de autoridade (SOA) que evita que outros servidores DNS almacenen en caché durante demasiado tempo. Nun rexistro de recursos individual, pode especificar un TTL específico para o rexistro que suplante o TTL mínimo (predeterminado) herdado do rexistro de recursos de inicio de autoridade. Tamén se pode utilizar o valor cero (0) para o TTL nos rexistros de recursos que conteñan datos volátiles que non estean na memoria caché para o seu uso posterior unha vez complétese a consulta DNS en curso.
Clase	Contén texto nemotécnico estándar que indica a clase do rexistro de recursos. Por exemplo, o valor "IN" indica que o rexistro de recursos pertence á clase Internet. Este campo é *obligatorio*.
Tipo	Contén texto nemotécnico estándar que indica o tipo de rexistro de recursos. Por exemplo, o texto nemotécnico "A" indica que o rexistro de recursos almacena información de direccións de host. Este campo é *obligatorio*.
Datos específicos do rexistro	Un campo de lonxitude variable e *obrigatorio* con información que describe o recurso. O formato desta información varía segundo o tipo e clase do rexistro de recursos.

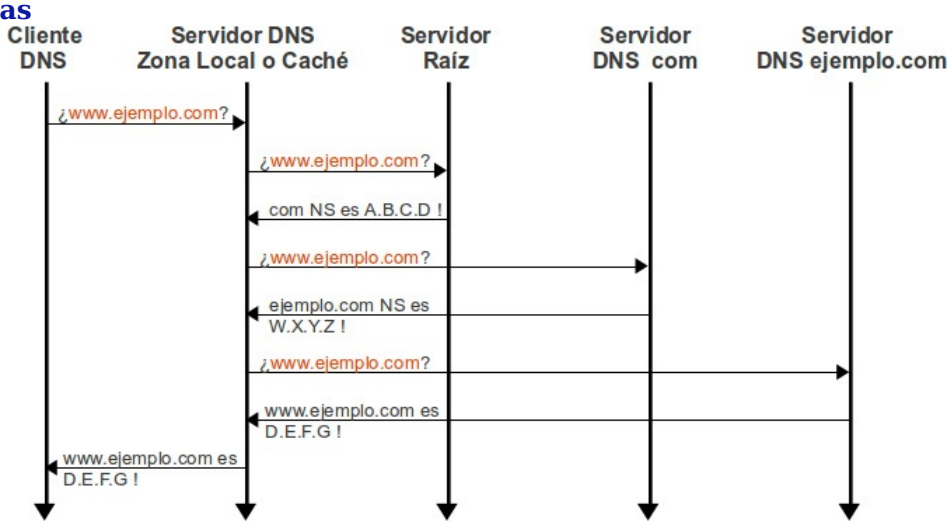
Tipos de rexistros DNS (O campo TTL *se omite en caso de ser opcional*. O campo TTL incluíuse na sintaxe de cada rexistro para indicar onde pode agregarse)	
Rexistro	**Descrición, Sintaxe e Exemplo**
A	**Descrición:** Address (Dirección). Este rexistro úsase para traducir nomes de hosts a direccións IP versión 4. **Sintaxe:** *propietario clase ttl* **A** *IP_version4* **Exemplo: host1.exemplo.com IN A 127.0.0.1**
AAAA	**Descrición:** Address (Dirección). Este rexistro úsase para traducir nomes de hosts a direccións IP versión 6. **Sintaxe:** *propietario clase ttl* **AAAA** *IP_version6* **Exemplo: host1ipv6.exemplo.com. IN AAAA 1234:0:1:2:3:4:567:89ab**
SRV	**Descrición:** Service Record (Rexistro de servizo). Este rexistro úsase para identificar os hosts que prestan servizos específicos. **Sintaxe:** *_servizo._proto.nome ttl clase* **SRV** *prioridade peso porto destino* **Exemplo: _ldap._tcp.exemplo.com. SRV 0 1 389 old-host1.exemplo.com** **_ldap._tcp.exemplo.com. SRV 0 5 389 new-host1.exemplo.com** Os servidores old-host1 e new-host1 teñen a mesma prioridade pero como new-host1 ten maior peso a conexión por defecto establecerase co servidor new-host1
CNAME	**Descrición:** Canonical Name (Nome Canónico). Úsase para crear nomes de hosts adicionais, ou alias. Hai que ter en conta que o nome de host ao que o alias referencia debe ser definido previamente como rexistro tipo "A". Comunmente usado cando un servidor cunha soa dirección IP executa varios servizos, como: ftp, web... e cada servizo ten a súa propia entrada DNS. Tamén é utilizado cando o servidor web aloxa distintos dominios nunha mesma IP (virtualhosts). **Sintaxe:** *propietario ttl clase* **CNAME** *nomeCanónico* **Exemplo: nomealias.exemplo.com CNAME nomeverdadeiro.exemplo.com** Como se comentou anteriormente **nomeverdadeiro.exemplo.com** previamente debe estar definido como rexistro tipo **A.**
NS	**Descrición:** Name Server (Servidor de Nomes). Indica que servidores de nomes teñen total autoridade sobre un dominio concreto. Cada dominio pódese asociar a unha cantidade calquera de servidores de nomes. **Sintaxe:** *propietario ttl IN* **NS** *nomeServidorNomeDominio* **Exemplo: exemplo.com. IN NS nomeservidor1.exemplo.com**
MX	**Descrición:** Mail eXchange (Rexistro de Intercambio de Correo). Asocia un nome de dominio a unha lista de servidores de intercambio de correo para ese dominio. **Sintaxe:** *propietario ttl clase* **MX** preferencia hostIntercambiadorDeCorreo **Exemplo: exemplo.com. MX 10 servidorcorreo1.exemplo.com** O número, neste caso 10, indica a preferencia, e ten sentido en caso de existir varios servidores de correo. A menor número maior preferencia.
PTR	**Descrición:** Pointer (Indicador). Traduce direccións IP en nomes de dominio. Tamén coñecido como 'rexistro inverso', xa que funciona á inversa do rexistro "A". **Sintaxe:** *propietario ttl clase* **PTR** *nomeDominioDestino* **Exemplo: 1.0.0.10.in-addr.arpa. PTR host.exemplo.com**
SOA	**Descrición:** Start Of Authority (Autoridade da zona). Proporciona información sobre o servidor DNS primario da zona. **Sintaxe:** *propietario clase servidorNomes persoaResponsable (numeroSerie intervaloActualización intervaloReintento caducidadetempoDeVidaMínimo)* **Exemplo: @ IN SOA nomeServidor.exemplo.com. postmaster.exemplo.com. (** **1 ; número de serie** **3600 ; actualizar [1h]** **600 ; reintentar [10m]** **86400 ; caducar [1d]** **3600) ; TTL mínimo [1h]** O propietario (servidor DNS principal) especifícase como "@" porque o nome de dominio é o mesmo que a orixe de todos os datos da zona (exemplo.com.). Trátase dunha convención de nomenclatura estándar para rexistros de recursos e utilízase máis a miúdo nos rexistros SOA. O número de serie é o número de versión desta base de datos. Debes incrementar este número cada vez que modificas a base de datos.
TXT	**Descrición:** TeXT (Información textual). Permite aos dominios identificarse de modos arbitrarios. **Sintaxe:** *propietario ttl clase* **TXT** *cadenaDeTexto* **Exemplo: exemplo.com. TXT "Exemplo de información de nome de dominio adicional."**
SPF	**Descrición:** Sender Policy Framework. É un rexistro de tipo TXT que vai creado nunha zona directa do DNS, na cal se pon as informacións do propio servidor de correo coa sintaxe SPF. Utilízase para evitar o envío de correos suplantando identidades. Por tanto, axuda a combater o SPAM, xa que, neste rexistro especifícase cal ou cales hosts están autorizados a enviar correo desde o dominio dado. O servidor que recibe, consulta o SPF para comparar a IP desde a cal lle chega, cos datos deste rexistro. **Sintaxe:** *propietario ttl clase* **IN SPF** *cadenaDeTexto* **Exemplo: exemplo.com IN SPF "v=spf1 a:mail.exemplo.com -all"**

Funcionamento do cliente DNS

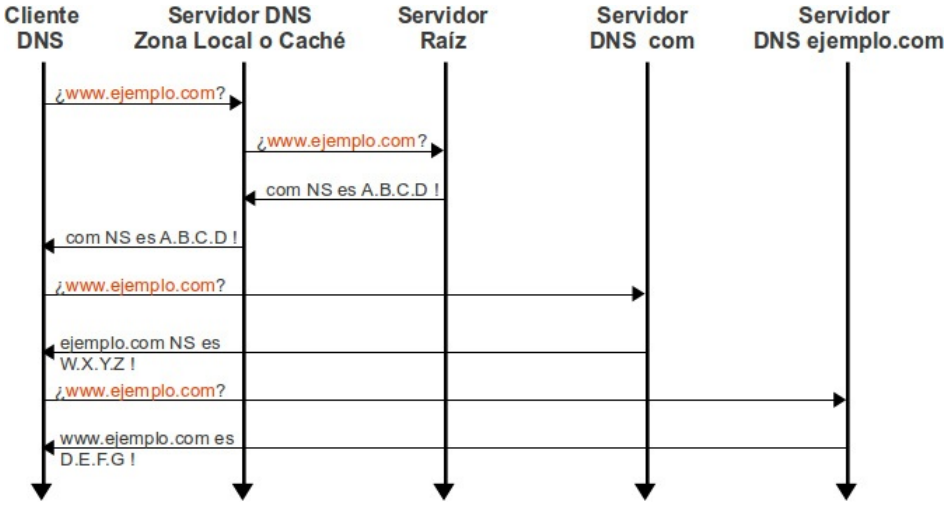
O proceso de consulta DNS realízase en dous partes:

- A consulta dun nome comeza nun equipo cliente e pásase ao solucionador (resolver), o servizo Cliente DNS, para proceder á súa resolución.
- Cando a consulta non se pode resolver localmente, pódese consultar aos servidores DNS segundo sexa necesario para resolver o nome.

Consultas recursivas

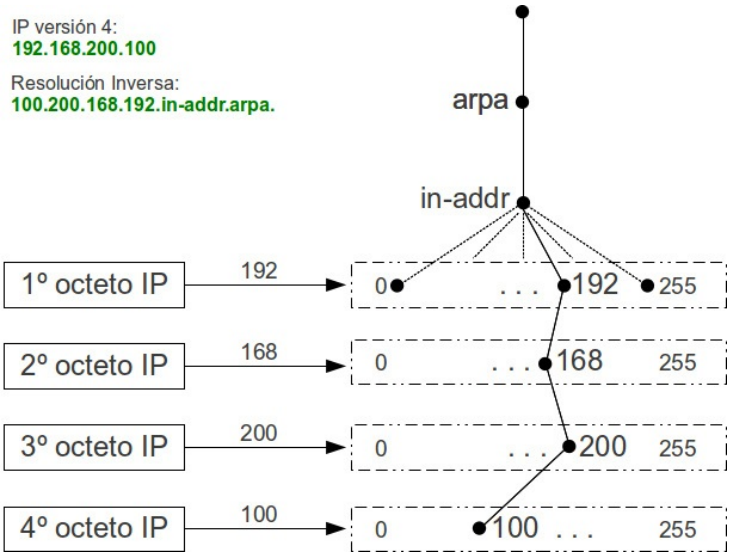


Consultas iterativas



Consultas inversas

O dominio `in-addr.arpa` úsase en todas as redes TCP/IP que se basean no direccionamiento do Protocolo da internet versión 4 (IPv4). Para o Protocolo da internet versión 6 (IPv6) úsase un nome de dominio especial diferente, o dominio `ip6.arpa`.



Ricardo Feijoo Costa