UD3 – SERVICIO DNS

1.- INTRODUCCIÓN

Hemos visto que el elemento básico de las comunicaciones que se producen en redes TCP/IP es la dirección IP, con la que se identifica unívocamente al emisor y receptor de la información. Sin embargo, lo que le resulta tan sencillo al ordenador, para el ser humano es súmamente difícil; para nosotros es mucho más sencillo recordar cadenas de texto que una tupla formada por dígitos.

En redes locales con pocos ordenadores es común el uso de **nombres planos**, formados por una única palabra. Este nombre recibe múltiples denominaciones como el nombre de computadora, nombre de máquina, nombre de red, nombre **NETBIOS** o nombre **SMB**. Todos estos términos significan lo mismo con la excepción de nombre netbios que también puede aplicarse al nombre del grupo de trabajo.

Este método de identificar a equipos no es adecuado en grandes redes locales o para Internet, ya que exigiría la existencia de grandes ficheros con todos los nombres de los computadores y sus IPs. Para solucionar este problema, existen los nombres **DNS** (**Domain Name System, sistema de nombres de dominio**); es un sistema de articulación de nombres para nodos TCP/IP que intenta organizar de modo jerárquico el nombre de todos los nodos conectados a Internet. Cada nombre DNS consta de dos partes. La primera parte identifica al nodo dentro de una subred. La segunda parte identifica a la subred. La proliferación de nodos en Internet ha creado la necesidad de fraccionar los dominios en subdominios de uno o varios niveles. Cada uno de los niveles (dominio, subdominio y nodos) va separado del siguiente nivel en la escritura del nombre por un punto.

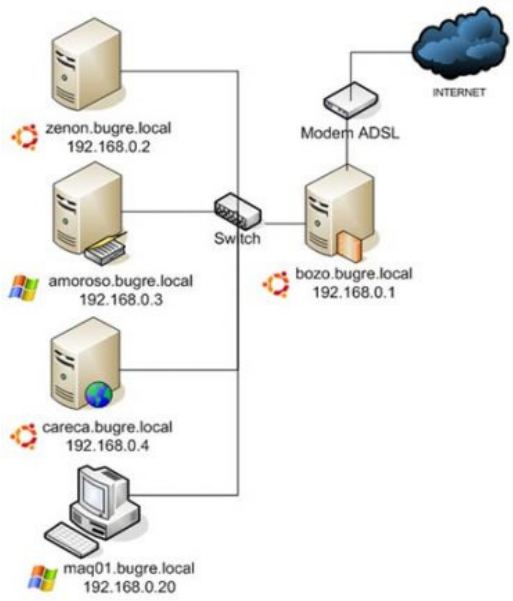
Nombres DNS en RAL

En la actualidad es comun encontrar servicios propios de Internet (http, ftp, smtp,ssh ...) implementados en las redes locales de algunas organizaciones. Las ventajas principales del uso de estos servicios en RAL son la reducción de costes y el aumento de la eficiencia, ya que:

- Facilitan de acceso a la información.
- Mejoran la comunicación entre empleados.
- Mejoran la automatización de procesos de negocio (aplicaciónes web).
- Facilitan trabajar desde cualquier lugar.
- Archivos centralizados. No se duplican.
- Control de acceso a los archivos.

Como todos sabéis, en Internet es comun el acceso a los servicios por nombres DNS, y aunque no sería necesario para la implantación de la mayoría de los servicios TCP/IP en las RALs, es comun utilizarlos tambien debido a:

- Los nombres DNS generan una agrupación lógica, independiente a la estructura de la red (los ordenadores de contabilidad podrían agruparse en el dominio contabilidad.local, los de ventas en ventas.local, dirección.local...)
- La estructura jeraquica de los nombres DNS facilitan identificar el origen/destino de los datos (carpeta compartida proveedores.contabilidad.local o impresora de red lpt1.marketing.local)



2.- ESPACIO DE NOMBRES DE DOMINIO

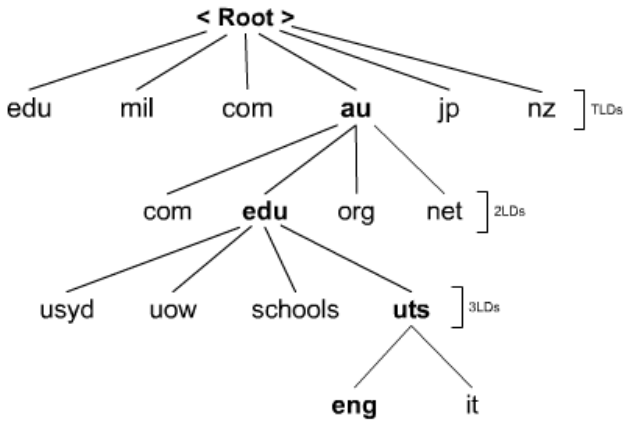
El servicio de DNS permite que un equipo cliente de la red registre y resuelva nombres de dominio de DNS. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet. Los tres componentes principales de DNS son los siguientes:

- **Espacio de nombres de dominio**.
- **Registros de recursos (RR) asociados**. Una base de datos distribuida de información de nombres.
- **Servidores de nombre de DNS.** Servidores que mantienen el espacio de nombres de dominio y los RR y responden a las peticiones de los clientes de DNS.

El **espacio de nombres de dominio** está estructurado de manera jerárquica en un árbol que empieza en una raíz sin nombre para todas las operaciones de DNS.

Cada nodo en el árbol de DNS tiene un nombre distinto llamado etiqueta (label). Cada etiqueta de DNS puede tener entre 1 y 63 caracteres y el dominio raíz no tiene caracteres. Un nombre de dominio concreto es la lista de etiquetas, desde el nodo nombrado hasta la raíz del árbol de DNS. La convención de DNS es que las etiquetas que componen un nombre de dominio se leen de izquierda a derecha, desde lo más concreto hasta la raíz, por ejemplo, www.midominio.com. Este nombre completo también se denomina nombre de dominio completo, **FQDN (Fully Qualified Domain Name).**

En la siguiente imagen se muestra el espacio de nombres DNS de Internet.



En el caso de Internet, un dominio superior es un dominio de DNS directamente debajo de la raíz. Resulta difícil crear nombres adicionales, al menos en Internet. Las tres categorías de dominios superiores son las siguientes:

- **<ARPA>**. Es un dominio especial, se usa en la actualidad para búsqueda inversa de nombres.
- TLD (Top Level Domain o dominio de nivel superior): son los dominios genéricos de primer nivel.
  - Por una parte, los *gTLD* o dominios de nivel superior genéricos. Inicialmente eran siete: `com`, `net`, `info`, `gov`, `mil`, `edu`, `int`.
  - Por otra parte, los *ccTLD* o *country code top level domain*. Estos serían los dominios territoriales, que tendrían por nombre la abreviatura de cada país según la norma ISO-3166.

Internet ha crecido mucho desde los años 80 y, en consecuencia, han crecido. Según Wikipedia, en 2012 **existen 22 gTLD y 293 ccTLD**.

Principales TLD

De los genéricos, podríamos destacar, por ejemplo:

- *.biz*, para negocios.
- *.com*, para propósitos comerciales.
- *.info*, para información general.
- *.int*, para organizaciones internacionales.
- *.mobi*, para sites móviles
- *.name*, para páginas personales y para individuales.
- *.net*, para lo que sea, si bien su propósito original era apuntar a sitios "paraguas" (portal para acceder a sitios más pequeños).
- *.org*, para organizaciones sin ánimo de lucro.
- *.pro*, para profesionales.
- *.tel*, para datos de contacto (se almacena directamente en el DNS).

3.- ZONAS

En Internet, el espacio de nombres está dividido en varias zonas que están almacenadas, distribuidas y replicadas en distintos servidores DNS. Hay dos tipos de zonas de búsqueda: zonas de búsqueda directa y zonas de búsqueda inversa.

Zonas de búsqueda directa.

Una zona de búsqueda directa permite consultas de búsqueda directa (dado un nombre DNS obtener la IP que le corresponde). En los servidores de nombres se debe configurar al menos una zona de búsqueda directa para permitir el funcionamiento del servicio de DNS.

Zonas de búsqueda inversa.

Un zona de búsqueda inversa permite las consultas de búsqueda inversa (dada una IP obtienen el nombre DNS que le corresponde). Las zonas de búsqueda inversa no son necesarias. Sin embargo, una zona de búsqueda inversa es imprescindible para ejecutar herramientas de reparación de problemas, como `nslookup` o `dig`.

4.- REGISTROS DE RECURSOS DNS

Un registro de recurso (RR) es un registro que contiene información relacionada con un dominio que puede contener la base de datos de DNS y que puede solicitar y usar un cliente de DNS. Por ejemplo, el RR de host de un dominio concreto mantiene la dirección de IP de tal dominio (host); un cliente de DNS podrá utilizar este RR para conseguir la dirección de IP para el dominio.

Cada servidor de DNS contiene los RR relacionados con aquellas porciones del espacio de nombre de DNS para el que es autoridad, o para el que puede responder las solicitadas por un host. Cuando un servidor de DNS es autorizado para una porción del espacio de nombres de DNS, dichos administradores del sistema son los responsables de asegurar que la información sobre esa porción del espacio de nombres de DNS es correcta. Para aumentar la eficiencia, un servidor de DNS dado puede hacer caché de los RR relativos a un dominio de cualquier parte del árbol de dominios.

Cada RR contendrá un conjunto de información común:

- **Propietario**. Indica el dominio de DNS en el que se encuentra el registro de recurso.
- **TTL**. Tiempo que utilizan otros servidores de DNS para determinar durante cuanto tiempo se hace caché de la información de un registro antes de descartarla. Para la mayoría de los RR, este campo es opcional. El valor de TTL se mide en segundos, con un valor de 0 que indica que el RR contiene datos volátiles que no se deben guardar en caché. Por ejemplo, los registros SOA tienen un valor de TTL predeterminado de 1 hora, de esta forma se evita que otros servidores mantengan en caché estos registros durante largos períodos de tiempo, lo que podría retrasar la propagación de cambios.
- **Clase**. Para la mayoría de los RR, este campo es opcional. Cuando se utiliza, contiene un texto mnemónico que indica la clase de un RR. Por ejemplo, una clase con IN indica que el registro pertenece a la clase Internet (IN).
- **Tipo**. Este campo es requerido y mantiene un texto mnemónico estándar que indica el tipo del RR. Por ejemplo, el mnemónico A indica que el RR guarda la información de dirección (Address) del host.
- **Datos** específicos del registro. Es un campo de tamaño variable que contiene información que describe elrecurso. Este formato de información varía de acuerdo con el tipo y clase del RR.

Los archivos de zona de DNS estándar contienen el conjunto de RR de dicha zona en un archivo de texto. En este archivo de texto, cada RR se encuentra en una línea separada y contiene todos los elementos de datos anteriores, como un conjunto de campos de texto separados por espacios en blanco. En el archivo de zona, cada RR consta de los elementos de datos anteriores, aunque diferentes registros pueden contener registros con formatos ligeramente diferentes para datos específicos.

Los RR usados más habitualmente, son:

- **Dirección de host (A) [Adress 32 bits]**

Este RR contiene un RR dirección de host que hace corresponder un nombre de dominio de DNS con una dirección de IPv4 de 32 bits.

Tipo. A

Sintaxis. Propietario A dirección_IPv4

Ejemplo. kona A 10.10.2.200

- **Nombre canónico (CNAME) [canonical name]**

El RR nombre canónico (CNAME) permite a los administradores de red crear un alias de otro nombre de dominio. El uso de RR CNAME se recomienda para su uso en los siguientes escenarios:

- Cuando un host especificado en un RR (A) de la misma zona necesita cambiar de nombre. Por ejemplo, si necesita cambiar el nombre de kona.midominio.com a hilo.midominio.com, crearía una entrada CNAME para kona.midominio.com que apuntase a hilo.midominio.com.
- Cuando un nombre genérico de un servicio conocido, como ftp o www, se necesita resolver a un grupo de equipos individuales, cada uno con un RR (A) individual. Por ejemplo, podría querer que www.midominio.com fuese un alias de kona.midominio.com y hilo.midominio.com. Un usuario que accediese a www.midominio.com normalmente no advertiría qué equipo realmente sirve la solicitud.

Este RR hace corresponder un alias o nombre de dominio de DNS alternativo en el campo Propietario (Owner) con un nombre canónico, real, de DNS. Debe haber también un RR (A) para el nombre de dominio de DNS canónico, que se debe resolver a un nombre de dominio de DNS válido en el mismo espacio de nombres. El nombre canónico completo debería terminar con un punto («.»).

Tipo. CNAME

Sintaxis. Alias CNAME Nombre_canónico o alias

Ejemplo. ns1 CNAME alias.midominio.com.

- **Puntero (PTR) [Pointer reverse]**

Este RR que se usa para los mensajes de búsqueda inversa de nombre apunta en la dirección de IP del campo Propietario (Owner) otra ubicación en el espacio de nombres de DNS como especifica el nombre_de dominio_objetivo. Normalmente, se usa sólo el árbol de dominio in-addr.arpa para la búsqueda inversa de la correspondencia dirección-nombre. En la mayoría de los casos, cada registro proporciona información que apunta a otra ubicación de un nombre de dominio de DNS, como un RR A de dirección de host en una zona de búsqueda inversa.

Tipo. PTR

Sintaxis. Propietario PTR nombre_de_dominio_objetivo

Ejemplo. 200 PTR kona.midominio.com

- **Servidor de nombres (NS)**

El registro de tipo NS indica quien es el servidor de nombres para el dominio. Es necesario que a dicho nombre se le asocie una dirección IP mediante un registro de tipo A.

Ejemplo. NS severoochoa.ies.

- **Inicio de autoridad (SOA)**

En primer lugar al describir un dominio siempre aparece el denominado registro SOA, que describe una zona de autoridad, es decir, una zona donde los datos que aparecen el fichero maestro son los que tienen prioridad y deben ser tomados como referencia.

El registro contiene distintos parametros:

- **Serie**: el primer parámetro numérico conocido como número serie se debe ir incrementando cada vez que se cambia algo en el servidor de nombres, de cara a que el servidor secundario sepa que debe actualizarse.
- **Refresco**: indica cada cuantos segundos el servidor secundario ha de actualizarse con los datos del servidor primario.
- **Reintento**: indica cada cuantos segundo el servidor secundario debe intentar reconectarse al primario para actualizar los datos en caso de error.
- **Expiración**: indica cuanto tiempo ha de pasar para que el servidor secundario deseche toda la información que tenía del primario.
- **TTL**: tiempo de vida de los registros que no lo indiquen explícitamente.

Los RR se pueden asociar a cualquier nodo del árbol de DNS, aunque los RR no existirán en algunos dominios; por ejemplo, los RR Puntero (PTR) se encuentran sólo en los dominios debajo del dominio in-addr.arpa. Por ello, los dominios superiores, como microsoft.com, pueden tener RR individuales, así como disponer de subdominios que también podrían disponer de RR individuales; por ejemplo, eu.microsoft.com, que tiene un registro de host www.eu.microsoft.com.

Ejemplo de RR con Bind.

Prácticamente el único software utilizado en los servidores de nombres de *Internet* es **bind** ("*Berkeley Internet Name Domain*"), creado originalmente en la *Universidad de California*, y actualmente propiedad del *Internet Systems Consortium*.

Este programa, distribuido bajo una licencia libre, es utilizado en prácticamente todos los sistemas *Unix* del mundo. Esto ha sido considerado un problema de seguridad, al punto que se ha propuesto la migración de algunos *root servers* a otro sistema, ya que la aparición de algún problema de seguridad en **bind** podría implicar la caída de todo el **DNS** de *Internet*.

Para instalarlo, podemos hacerlo con apt-get desde una consola de root:

```
// Instalación del servidor DNS bind
# apt-get install bind9
```

Ejemplo de configuración del dominio severoochoa.ies

```
// Añadir en /etc/bind/named.conf.local
// Archivo para búsquedas directas
zone "severoochoa.ies" {
type master;
file "/etc/bind/severoochoa.db";
};

// Archivo para búsquedas inversas
zone "0.168.192.in-addr.arpa" {
type master;
file "/etc/bind/192.rev";
};
```

Supongamos que en nuestra red local tenemos un aula llamada aula5 con 12 PCs con IPs que van desde la 192.168.0.101 hasta 112 y cuyos nombres van desde aula5pc1 hasta aula5pc10, luego un servidor web (pc11) y un servidor de correo electrónico que además es servidor DNS (pc12). El archivo de configuración DNS de nuestro dominio podría ser así:

```
// Archivo /etc/bind/severoochoa.db
;
; BIND data file for severoochoa.ies
;
@ IN SOA severoochoa.ies. root.severoochoa.ies. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Default TTL

IN NS severoochoa.ies.
IN MX 10 mail.severoochoa.ies.

aula5pc1 IN A 192.168.0.101
aula5pc2 IN A 192.168.0.102
aula5pc3 IN A 192.168.0.103
aula5pc4 IN A 192.168.0.104
aula5pc5 IN A 192.168.0.105
aula5pc6 IN A 192.168.0.106
aula5pc7 IN A 192.168.0.107
aula5pc8 IN A 192.168.0.108
aula5pc9 IN A 192.168.0.109
aula5pc10 IN A 192.168.0.110
```

```
www IN A 192.168.0.111
dns IN A 192.168.0.112
mail IN A 192.168.0.112
```

Las primeras líneas son unos parámetros relacionados con la actualización del DNS (número de serie y periodos de actuación). Las dos siguientes líneas indican quién es el servidor primario (NS = Name Server) y quien procesa el correo electrónico del dominio (MX = Mail eXchange). Las siguentes líneas especifican las IPs de los distintos PCs componentes del dominio (A = Address).

Para poder realizar consultas inversas (de IP a nombre) será necesario crear el siguiente archivo:

```
// Archivo /etc/bind/192.rev
;
; BIND reverse data file for 192.168.0.0
;
@ IN SOA severoochoa.ies. root.severoochoa.ies. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Default TTL

IN NS dns.severoochoa.ies.

101 IN PTR aula5pc1.severoochoa.ies.
102 IN PTR aula5pc2.severoochoa.ies.
103 IN PTR aula5pc3.severoochoa.ies.
104 IN PTR aula5pc4.severoochoa.ies.
105 IN PTR aula5pc5.severoochoa.ies.
106 IN PTR aula5pc6.severoochoa.ies.
107 IN PTR aula5pc7.severoochoa.ies.
108 IN PTR aula5pc8.severoochoa.ies.
109 IN PTR aula5pc9.severoochoa.ies.
110 IN PTR aula5pc10.severoochoa.ies.
111 IN PTR www.severoochoa.ies.
112 IN PTR dns.severoochoa.ies.
112 IN PTR mail.severoochoa.ies.
```

5.- TIPOS DE SOLICITUDES

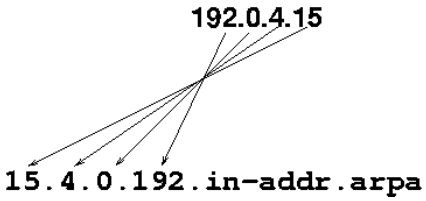
Un cliente efectúa una operación de solicitud a un servidor de DNS para conseguir parte o toda la información de RR relacionada con un determinado dominio, por ejemplo, para determinar qué registro o registros de hosts (A) se mantienen sobre el dominio llamado midominio.com. Si el dominio existe y también el RR solicitado, el servidor de DNS devolverá la información solicitada en un mensaje de respuesta a la solicitud. El mensaje de respuesta devolverá tanto la solicitud inicial como la respuesta con los registros relevantes, suponiendo que el servidor de DNS pueda conseguir los RR necesarios.

Solicitud inversa.

Una solicitud inversa es aquella en la que se solicita a un servidor de DNS el nombre de dominio de DNS de un host con una determinada dirección de IP. Los mensajes de Solicitud de búsqueda inversa son, realmente, solicitudes estándar, pero relacionadas con las zonas de búsqueda inversa. Para la resolución inversa fueron creados nombres de dominio especiales: **in-addr.arpa** para bloques IPv4 e ip6.arpa para bloques IPv6 y contienen principalmente los RR de **PTR**.

Para poner la dirección IP dentro de la jerarquía de nombres DNS, es necesario hacer una operación para crear un nombre que represente la dirección IP dentro de esa estructura.

En la jerarquía de nombres del sistema DNS la parte más a la izquierda es la más específica y la parte a la derecha la menos específica. Pero en la numeración de direcciones IP eso está invertido, es decir, lo más específico es lo que está más a la derecha en una dirección IP, por lo que para resolver eso se debió hacer una operación invirtiendo cada parte de la dirección IP y luego añadir el nombre de dominio reservado para la resolución inversa (in-addr.arpa o ip6.arpa) Por ejemplo, considerando la dirección IPv4 192.0.4.15. Para colocarla en el formato necesario, se debe invertir cada byte (Un byte es lo mismo que 8 bits) y añadir el dominio para resolución inversa al final: **15.4.0.192.in-addr.arpa**



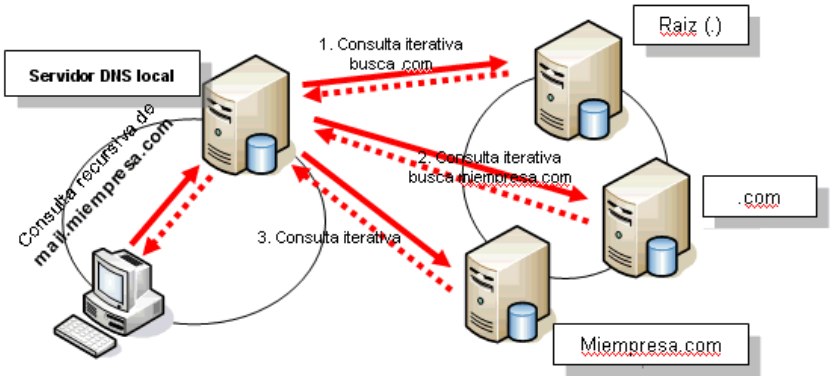
Solicitud recursiva

Es una solicitud de DNS que se envía a un servidor de DNS en la que el host solicitante pregunta al servidor de DNS para que le proporcione una **respuesta completa a la solicitud**, aunque ello signifique que tenga que ponerse en contacto con otros servidores para obtener la respuesta. Cuando se envía una solicitud recursiva, el servidor de DNS usa un conjunto de solicitudes iterativas a otros servidores de DNS como intermediario del host solicitante para conseguir la respuesta a la solicitud.

Para resolver este tipo de solicitudes el servidor DNS dispone de los nombres y direcciones de servidores DNS del dominio raíz(.) Al conjunto de estos servidores se denominan sugerencias raíz.

Solicitud iterativa.

Es una solicitud de DNS que se envía a un servidor de DNS en el que el host solicitante pide que se devuelva la mejor respuesta que el servidor de DNS pueda proporcionar sin buscar ayuda adicional de otros servidores de DNS.



6.- TIPOS DE SERVIDORES DNS

Hay tres tipos de servidor de nombres:

Primario

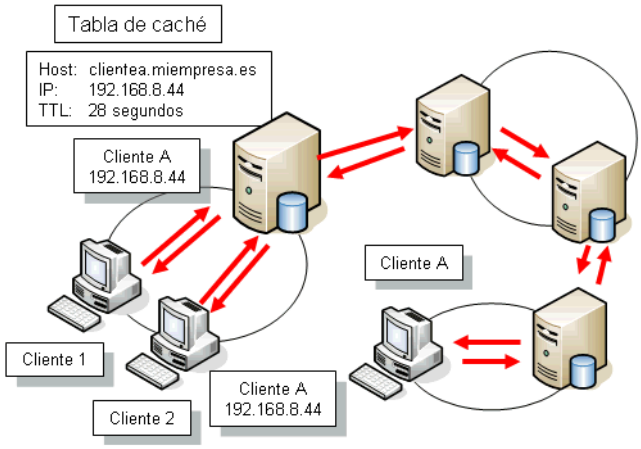
Un servidor de nombres primario carga de disco la información de una zona, y tiene autoridad sobre ella.

Secundario

Un servidor de nombres secundario tiene autoridad sobre una zona, pero obtiene la información de esa zona de un servidor primario utilizando un proceso llamado transferencia de zona. Para permanecer sincronizado, los servidores de nombres secundarios consultan a los primarios regularmente y reejecutan la transferencia de zona si el primario ha sido actualizado. Un servidor de nombres puede operar como primario o secundario para múltiples dominios, o como primario para unos y secundario para otros. Un servidor primario o secundario realiza todas las funciones de un servidor caché.

Caché

Un servidor de nombres que no tiene autoridad para ninguna zona se denomina servidor caché.



7.- DNS Dinámico

El DNS dinámico (DDNS) es un servicio que permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres. El uso más común que se le da es permitir la asignación de un nombre de dominio de Internet a un dispositivo con dirección IP variable (dinámica). Esto permite conectarse con la máquina en cuestión sin necesidad de tener conocimiento de que dirección IP posee en ese momento.

El uso más común de **DDNS** es el acceso remoto a cámaras IP, NAS, routers, dispositivos de domótica o cualquier dispositivo conectado a Internet.

Muchos ISP tienen esta opción, incluso algunas lo ofrecen gratuitamente, como es el caso de DynDNS.com, No-IP.com…