INSTALACIÓN Y CONFIGURACIÓN BÁSICA DEL SERVICIO DNS EN *WINDOWS SERVER 2022*. ZONA DE BÚSQUEDA DIRECTA

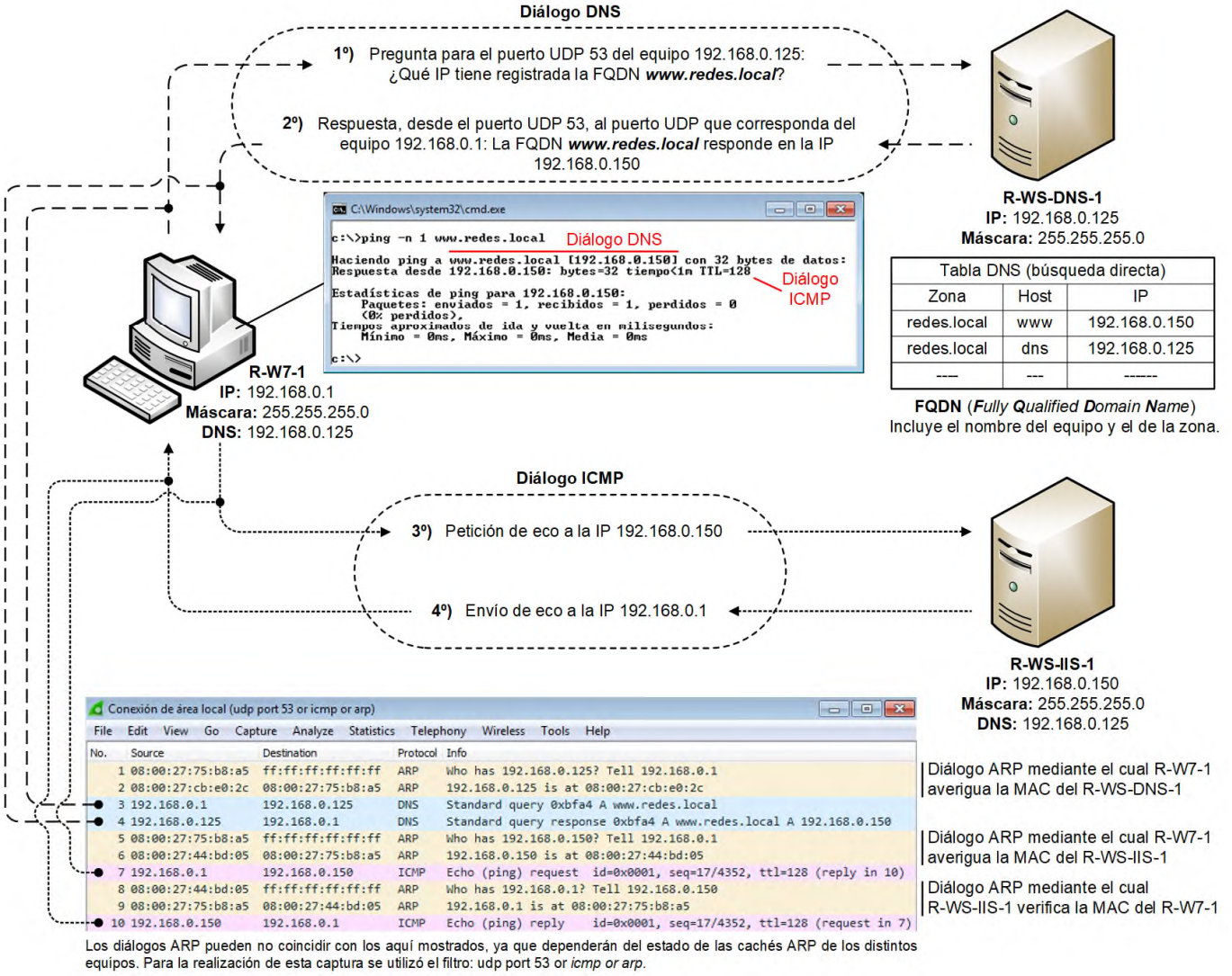


Figura 1

1.- CONFIGURACIÓN TCP/IP DE LOS EQUIPOS.

Dotar a cada máquina de la configuración TCP/IP indicada en el esquema de la Figura 1 y disponerlas en la red interna R-192. Comprobar que todos los equipos se "ven" entre sí.

2.- INSTALACIÓN DEL SERVICIO DNS EN EL *WINDOWS SERVER 2022*.

Lanzamos el administrador del servidor, Figura 2, y en la herramienta que se abre, en el bloque "Configurar este servidor local", seleccionamos "Agregar roles y características", Figura 3.

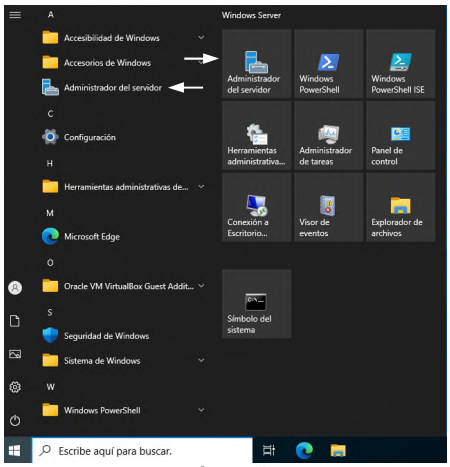


Figura 2

Figura 3

En el panel de información que se abre, pulsamos el botón “Siguiente” y en el nuevo formulario, Figura 4, habilitamos la opción “Instalación basada en características o en roles”, tal y como se muestra en la Figura 4. A continuación, pulsamos el botón “Siguiente”.

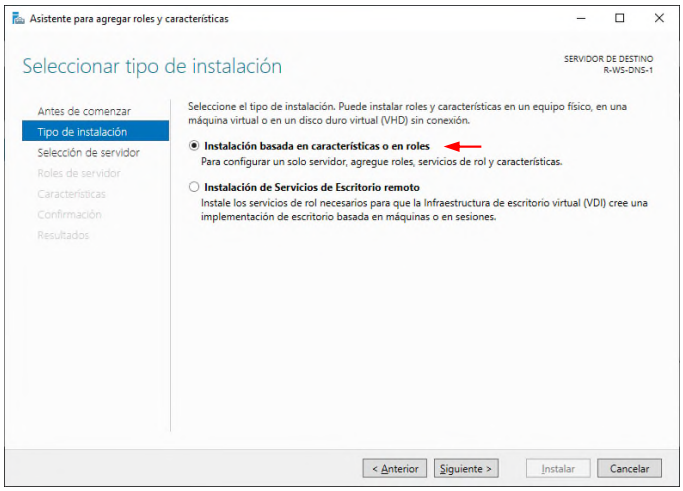


Figura 4

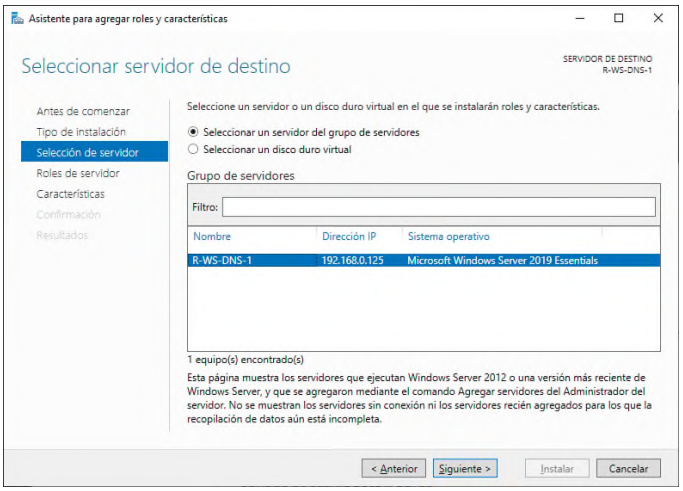


Figura 5

En el nuevo formulario, Figura 5, comprobamos que se encuentra seleccionado el servidor en uso y pulsamos el botón “Siguiente”.

En la lista de roles, del siguiente formulario, habilitamos “Servidor DNS”, Figura 6, que inmediatamente nos presenta un nuevo formulario, Figura 7, en el que se nos indica que para la administración del servicio DNS es necesario instalar las herramientas de administración específicas, y nos pide que le indiquemos si las deseamos instalar en el mismo servidor. Pulsamos le botón “Agregar características”, para indicarle que sí. Lo que nos devuelve al formulario anterior, Figura 6, en donde pulsamos el botón “Siguiente”.

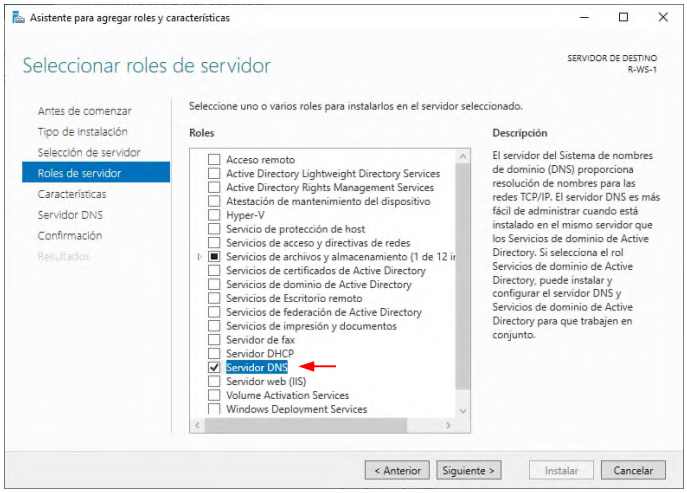


Figura 6

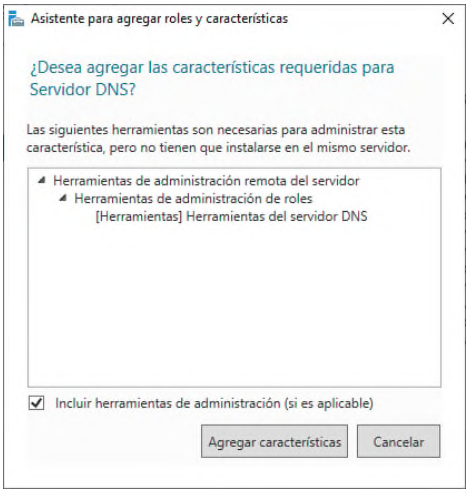


Figura 7

En el nuevo formulario de selección de características, Figura 8, pulsamos el botón “Siguiente”, sin seleccionar ninguna nueva característica para instalar.

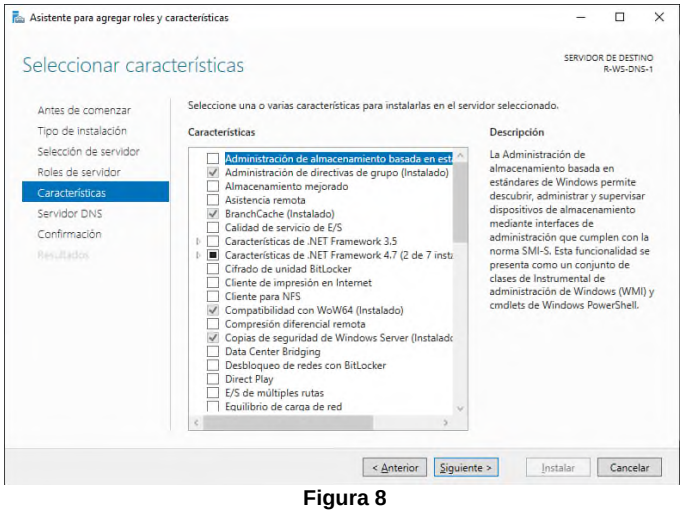


Figura 8

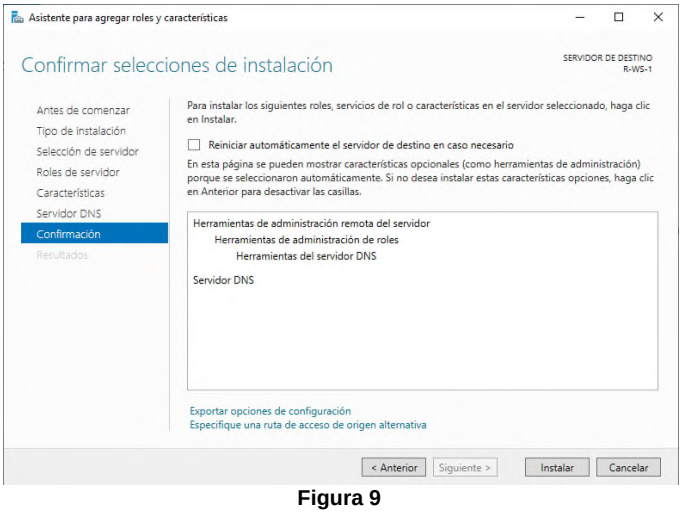


Figura 9

En el panel de información sobre el servicio DNS que se presenta, pulsamos le botón “Siguiente” y en el formulario de confirmación de la instalación, Figura 9, pulsamos el botón “Instalar”.

Una vez concluida la instalación del servicio DNS, nos indicará, en su caso, que la instalación fue correcta tal y como se muestra en la Figura 10. En donde pulsaremos el botón “Cerrar”; para concluir la instalación del servicio DNS cerraremos la herramienta de administración del servidor.

Antes de dar por concluida la instalación del servicio DNS, comprobaremos que su arranque está configurado como automático. Para ello, obraremos de la forma siguiente:

Icono Iniciar → Herramientas administrativas de Windows, Figura 11 → Servicios → En la lista de servicios buscamos el “Servidor DNS”, Figura 12, y hacemos doble clic sobre él. En el formulario que se abre, Figura 13, comprobamos que el tipo de arranque se encuentra configurado como “Automático”, en caso de no estarlo, seleccionarlo en el combo y pulsar el botón “Aceptar”.

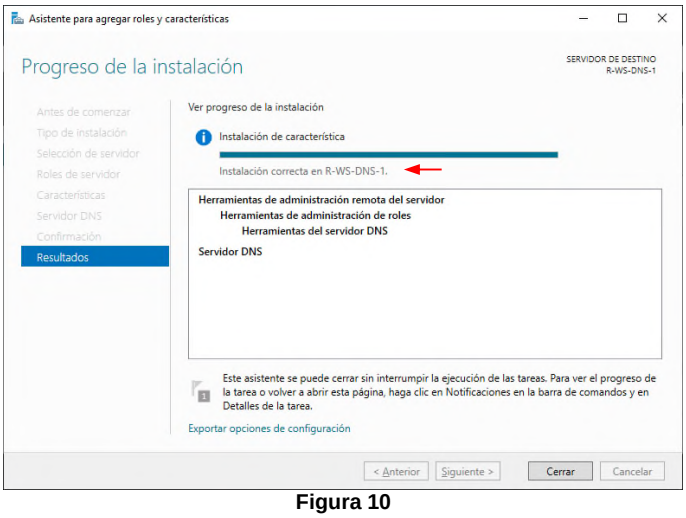


Figura 10

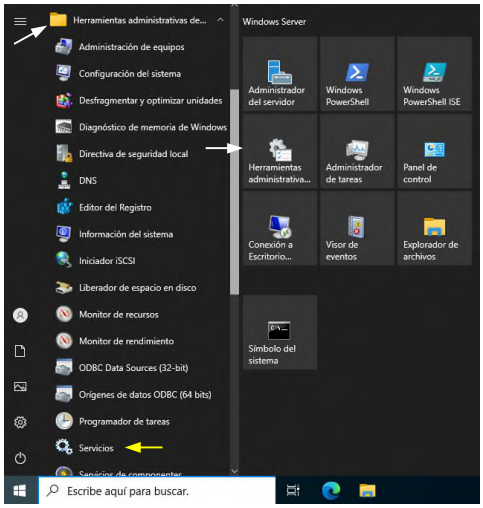


Figura 11

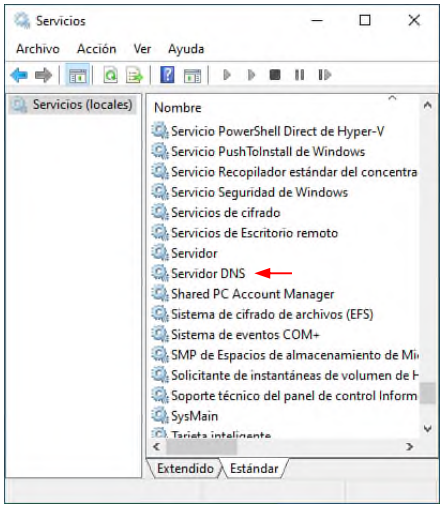


Figura 12

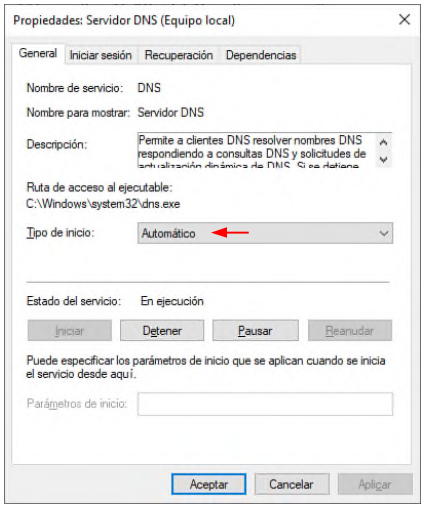


Figura 13

Una vez instalado el servicio DNS y verificado su arranque, reiniciaremos la máquina.

Una buena forma de saber si el servicio DNS se encuentra en funcionamiento, es verificar que el puerto que tiene asignando se encuentra levantado, para ello ejecutaremos la orden (requiere elevación): ***netstat -ap UDP | find ":53 "***, a través de la cual le indicamos que deseamos un listado de los puertos abiertos (***-a***) correspondientes al protocolo UDP (***-p UDP***) y que solo muestra aquellas líneas, de la salida (*pipeline* **|**), que contengan (***find***) el texto indicado entre comillas (***“53 ”***), recuerde que el servicio DNS escucha en el puerto UDP:53. Nótese que después del número 53 aparece un espacio en blanco, para evitar que nos muestre, por ejemplo, un puerto UDP:53…..

El resultado de la ejecución de este comando se muestra en la Figura 14, en ella se constata que el servicio DNS está escuchando en el bucle local (*socket* 127.0.0.1:53) y sobre la interfaz del equipo (*socket* 192.162.0.125:53), tal y como se esperaba. En breve haremos uso del *socket* sobre el bucle local, al configurar el cliente DNS del R-WS-DNS-1 sobre esa IP.

```
c:\>netstat -ap UDP | find ":53 "
  UDP    127.0.0.1:53           *:*
  UDP    192.168.0.125:53       *:*

c:\>
```

Figura 14

Si en lugar de preguntar por los puertos UDP, lo hiciéramos sobre los TCP (***netstat -ap TCP | find ":53 "***), obtendríamos una salida pareja, tal y como se muestra en la Figura 15. Es necesario recalcar que el puerto TCP:53 solo lo utiliza, el servicio DNS, para diálogos de transferencia de zonas, entre servidores DNS maestros y esclavos. En los diálogos DNS cliente DNS ⇆ servidor DNS, como el que estamos estudiando, solo utiliza el puerto UDP:53. Esta es la razón por la cual el puerto TCP:53 debe cerrase siempre en el cortafuegos siempre, salvo, claro está, que dispongamos de servidores DNS esclavos y, como consecuencia, se realicen transferencias de zonas.

```
c:\>netstat -ap TCP | find ":53 "
  TCP    127.0.0.1:53           R-WS-DNS-1:0           LISTENING
  TCP    192.168.0.125:53       R-WS-DNS-1:0           LISTENING

c:\>
```

Figura 15

3.- CONFIGURACIÓN BÁSICA DEL SERVICIO DNS. ZONA DE BÚSQUEDA DIRECTA[1].

Para realizar la configuración del servicio DNS obraremos de la forma siguiente:

Icono Iniciar → Herramientas administrativas de Windows, Figura 16 → Herramienta DNS → Desplegamos el árbol del servidor, haciendo clic en el carácter “>” que aparece a su izquierda → Seleccionamos “Zona de búsqueda directa” → Botón derecho, seleccionamos “Zona nueva” → Botón “Siguiente” → Seleccionamos la opción “Zona principal” → Botón “Siguiente” → En el campo de texto introducimos el nombre de la zona que deseamos crear, en este caso *“redes.local”* → Botón

"Siguiente" ➔ Aceptamos la opción por defecto de creación del fichero *"redes.local.dns"* para guardar los registros de la zona y Botón "Siguiente" ➔ Aceptamos la opción por defecto de "No admitir actualizaciones dinámicas" y Botón "Siguiente" ➔ Botón "Finalizar".

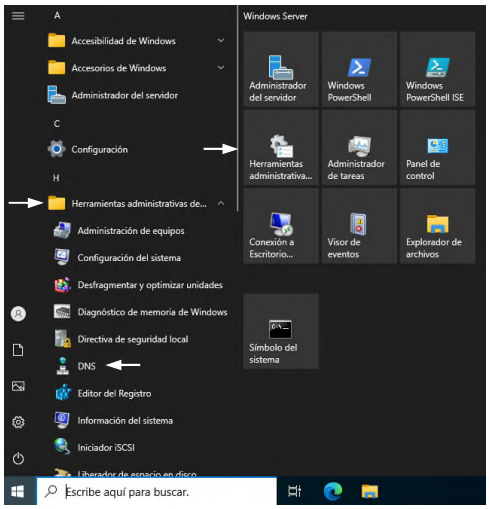


Figura 16

Si todo funcionó en la forma debida, debemos estar en una circunstancia idéntica a la que se muestra en la Figura 17.

En ella puede verse el contenedor de la zona de búsqueda directa, recién creada, *"redes.local"* (panel de la izquierda) y el contenido del mismo (panel de la derecha).

Las dos líneas que, de momento, componen la zona (a cada línea de una zona DNS se le denomina registro) se crean automáticamente y guardan información vital para el correcto funcionamiento del servicio DNS con respecto a esa zona.

Antes de analizar el contenido y alcance de cada uno de estos registros, sería interesante aclarar el significado de algunas de las expresiones que se utilizan para referirse a los servidores DNS, de manera que, en adelante, las utilizaremos de acuerdo con lo que a continuación se explica.

Servidor DNS primario: Será único y obligatorio para cada zona, y se corresponderá con el servidor DNS sobre el cual se defina una zona específica; siendo el único en el cual se podrá administrar, dando altas, bajas o modificando los registros correspondientes. Será, por así decirlo, el poseedor de la información original de la zona, ya que el resto de los servidores DNS, que tengan información de esa zona, tendrán una "copia de solo lectura" de la misma.

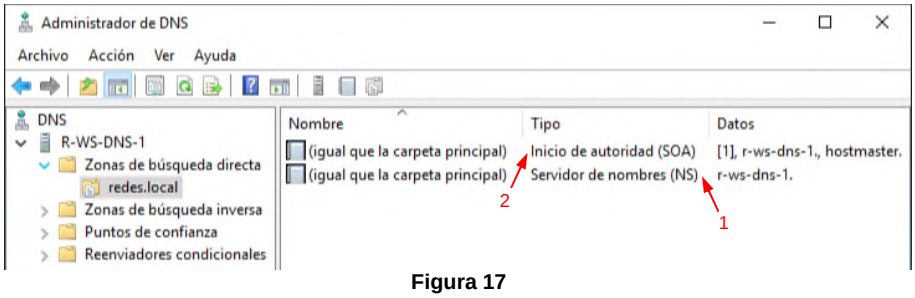


Figura 17

Obligatoriamente, todo servidor DNS primario, de una zona, dispondrá de un registro NS (***N**ames **S**erver*), Figura 17-1, en dicha zona. Con lo cual todo servidor DNS primario, de una zona, será un servidor autoritativo de la misma.

Servidor DNS secundario o esclavo: Serán todos aquellos servidores DNS que tenga una copia completa, no administrable, de la zona determinada, en su servicio DNS. La copia se actualizará, automáticamente, a partir de la información de un DNS maestro. Si el servidor DNS secundario dispone de un registro NS, en la zona en cuestión, será un servidor DNS secundario autoritativo de esa zona.

Un servidor DNS, que tan solo disponga de la información de una zona, aunque sea completa, a través de la caché de su servicio DNS, y no disponga de una copia activa en su propio servicio DNS, no será un servidor secundario de esa zona, será, en su caso, un servidor DNS caché.

No es obligatoria la existencia de servidores DNS secundarios y, de existir, su número puede ser ilimitado. Se utilizan como medida de seguridad, frente a un fallo del DNS primario, y para la distribución de la carga del servicio DNS de la zona en cuestión.

Servidor DNS maestro: Será todo aquel servidor que sirva de fuente para transferir una zona a otro servidor DNS, denominado esclavo. Un servidor DNS maestro, puede ser un servidor primario o un servidor secundario, esclavo, que actúe como maestro para un tercero.

Servidor DNS autoritativo: A parte del servidor DNS primario de una zona; tendrá la consideración de DNS autoritativo, todo aquel servidor DNS secundario que se encuentre en condiciones de ser promocionado a DNS primario de dicha zona, para lo cual debe de disponer del correspondiente registro NS definido en la zona en cuestión.

La promoción de un servidor DNS secundario autoritativo de una zona, a servidor DNS primario de la misma, podría venir provocada por la pérdida irrecuperable del servidor DNS primario original y la necesidad de seguir gestionando la zona concreta.

Una vez vistos estos conceptos, que nos harán falta a continuación, analizaremos los registros vistos en la zona creada.

Inicio de autoridad (SOA - *Start **O**f **A**uthority*):**

El registro SOA, Figura 17-2, es único y obligatorio, para cada una de las zonas que se definan en cualquier servidor DNS, y en él se establece qué DNS es el responsable único de la zona (DNS primario) y las condiciones temporales en las cuales cualquier otro servidor DNS secundario, o cliente DNS, puede hacer uso de la información (registros) obtenida de esta zona. La realidad, es que quizá se vea la auténtica utilidad de este registro cuando se trabaje con DNS secundarios y se transfiera la zona a alguno de ellos, ya que este es uno de los registros que se le transfieren y constituye una especie de contrato de condiciones de uso de la información que se le suministra, tal y como se muestra en la captura de la Figura 18. Pero, en cualquier caso, aquí también se define información de utilidad para los clientes normales, como puede ser, en nuestro ejemplo, el R-W7-1, tal y como se verá más adelante y se muestra en la Figura 31.

En entornos *Windows* es muy fácil que estos parámetros pasen absolutamente desapercibidos y aceptados, como valores por defecto, para cumplimiento del estándar DNS. Sin embargo, resulta muy interesante conocerlos ya que en sistemas *GNU/Linux* deben declararse de forma explícita, en el correspondiente fichero de zona, y mediante la sintaxis específica.

Para ver el contenido de ese registro, hacemos doble clic sobre él o bien lo seleccionamos → Botón derecho → Propiedades → Lengüeta "Inicio de autoridad (SOA)". Y veremos el formulario de la Figura 19.

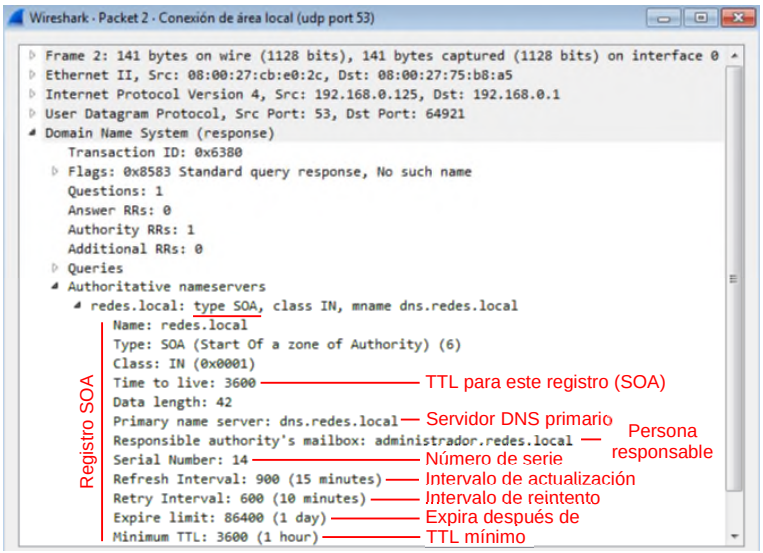


Figura 18

Número de serie: Indica el número de actualizaciones que se han hecho en la información de la zona, se modifica de forma incremental automáticamente. Se utiliza en las transferencias de zona, entre servidores DNS maestros y esclavos, para comprobar si la información que tienen ambos servidores es la misma o no y, en su caso, actualizar la del servidor DNS esclavo. De hecho, cuando un servidor secundario solicita una actualización de una zona, al correspondiente DNS maestros, lo que hace es pedir una copia del registro SOA, y si comprueba que el valor del campo "Número de serie" es mayor que el que tiene la copia de la zona que él posee, solicita una copia de la zona actualizada, al DNS maestro (Figura 19 y Figura 18).

Servidor primario: Muestra el DNS primario de la zona, que es el que posee la información original de la misma (a través de él se administra, dando bajas, altas, etc.). En una zona solo puede existir un DNS primario. Por defecto, toma el nombre *NetBIOS* del servidor DNS en el cual se define la zona, en nuestro caso: R-WS-DNS-1 (Figura 19), algo que habrá que corregir en la configuración del servicio DNS, tal y como consta en la Figura 18.

Persona responsable: Corresponde a la dirección de correo electrónico del administrador de la zona, que, por defecto, hace referencia al *hostmaster*, Figura 19. En este caso, el símbolo "@" que separa el identificador de usuario, del dominio, en una cuenta de correo electrónico, debe reemplazarse por un punto, ya que la arroba no está soportada. Así por ejemplo, si se deseara declarar la cuenta de correo *administrador@redes.local*, en el campo "Persona responsable" figuraría como: *administrador.redes.local*, tal y como se muestra en la Figura 18.

Si se dispusiera de un servidor de correo electrónico y una cuenta en él, se utilizaría un registro DNS especial (de tipo RP, ***R**esponsible **P**erson*) para incorporar la dirección de la persona de contacto. Es este caso, una vez creado el registro RP, se utilizaría el botón "Examinar" para localizarlo y configurar la información de la persona responsable.

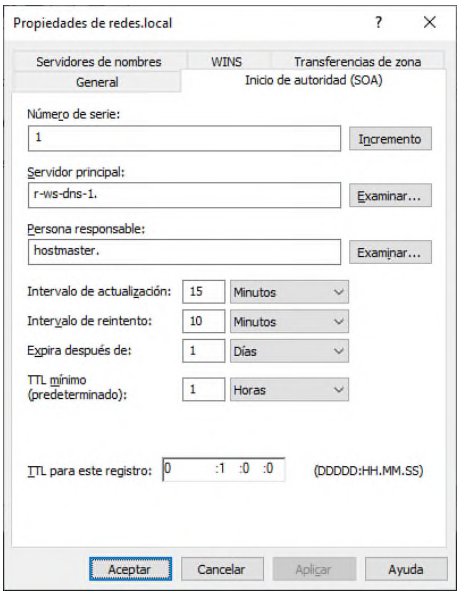


Figura 19

Los siguientes parámetros se utilizan como valores de caducidad para los servidores DNS secundarios y cachés DNS.

Intervalo de actualización: Es el intervalo de tiempo que debe esperar, un DNS esclavo de esta zona, antes de realizar una nueva solicitud de actualización de la zona a su DNS maestro. En nuestro caso, los DNS esclavos de la zona *redes.local*, solicitarán una actualización de la zona, a su correspondiente DNS maestro, cada 15 minutos, Figura 19 y Figura 18.

Intervalo de reintento: Es complementario del anterior, y en él se establece que si una vez solicitada la actualización de la zona, al DNS maestro, no se obtiene respuesta de él. Debe intentarse de nuevo, pero -en nuestro caso- en lugar de cada 15 minutos, se hará cada 10 minutos, hasta que se obtenga la respuesta correspondiente, Figura 19 y Figura 18.

Expira después de: Corresponde al tiempo máximo que un DNS esclavo puede dar por buena la información que posee, sin contactar con su DNS maestro de la zona. Transcurrido este período, el DNS esclavo, dejará de responder a las peticiones que reciba, sobre esta zona, por tener su información caducada. En nuestro ejemplo, transcurrido un día sin que algún DNS esclavo pudiera contactar con su servidor maestro, automáticamente dejaría de servir la información correspondiente a la zona *redes.local*. (Figura 19 y Figura 18).

TTL mínimo: Indica el tiempo que una caché DNS puede almacenar cualquier registro de esta zona. Este TTL no es de aplicación para los DNS secundarios, sino para las cachés de clientes y servidores DNS, que no sean DNS secundarios de esta zona. En nuestro caso, las cachés DNS deben considerar la información de esta zona, a la que tengan acceso, con una caducidad de máxima de 1 hora, transcurrida la cual deben eliminarla de su correspondiente caché DNS. (Figura 19 y Figura 18).

TTL para este registro: Es el TTL del registro de SOA, y por lo tanto establece el tiempo máximo que cualquier caché DNS pueden dar por válida la información del propio registro SOA, Figura 19 y Figura 18.

Servidor de nombres (NS):

A diferencia del SOA el registro NS, Figura 17-1, puede no ser único, ya que debe existir uno por cada DNS secundario autoritativo de la zona, más el correspondiente al DNS primario, que sí es obligatorio en cada zona. De acuerdo con esto, en cualquier zona debe haber al menos un registro NS, el correspondiente al DNS primario.

Para ver el contenido de ese registro, hacemos doble clic sobre él o bien lo seleccionamos ➔ Botón derecho ➔ Propiedades ➔ Lengüeta "Servidores de nombres". Y veremos el formulario que se muestra en la Figura 20.

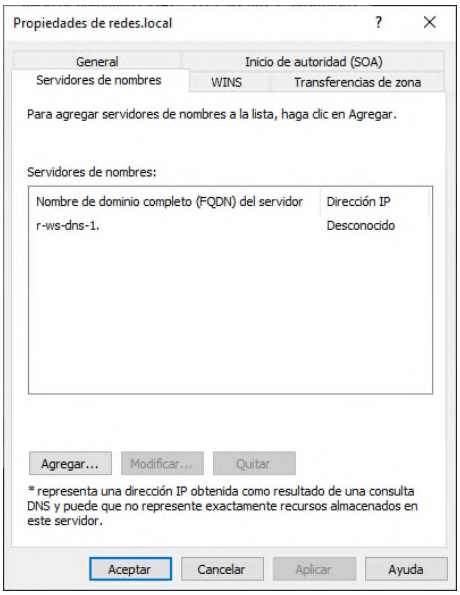


Figura 20

Este registro hace referencia al propio servidor DNS primario de la zona, es obligatorio en la definición de cualquier zona. Obsérvese que, por defecto, toma el nombre *NetBIOS* del equipo. Este registro de tipo NS (***N**ames **S**erver*), no permite resolver el nombre del *host*, es decir, si hiciéramos un ***ping r-ws-dns-1.redes.local*** el servidor DNS respondería que no tiene registrado ningún equipo con ese nombre, tal y como se muestra en la Figura 21.

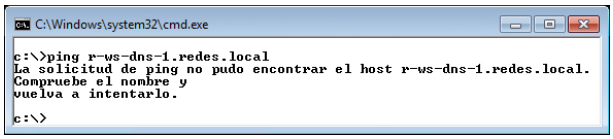


Figura 21

La finalidad de los registros tipo NS es conocer qué servidores DNS disponen de una copia veraz de la información de la zona en cuestión.

4.- DAR DE ALTA UN EQUIPO EN LA ZONA DE BÚSQUEDA DIRECTA *REDES.LOCAL*.

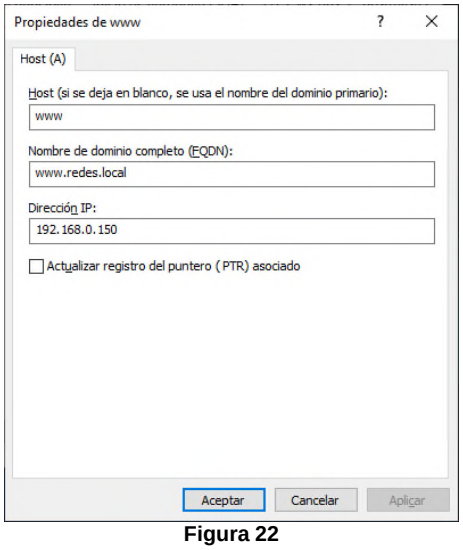


Figura 22

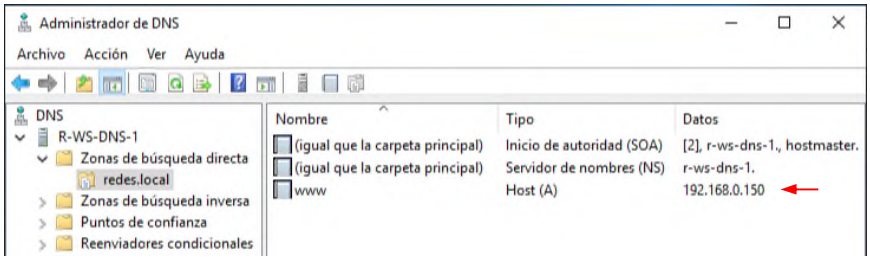


Figura 23

Para ello seleccionamos el contenedor de la zona *redes.local* (panel izquierdo) o nos situamos bajo el último registro (panel derecho) ➔ Botón derecho ➔ Opción "*Host* nuevo (A o AAAA)..." y cubrimos el formulario poniendo en el primer campo el nombre del equipo, en nuestro caso *www* y en el segundo de los campos la dirección IP del equipo al que deseamos asignar el nombre anterior, en el ejemplo que estamos desarrollando sería la IP 192.168.0.150 (tal y como se muestra en la Figura 22) ➔ Botón "Agregar *host*" ➔ Botón "Realizado".

Si todo funcionó correctamente, debemos obtener el resultado que se muestra en la Figura 23. En donde puede verse que aparece un nuevo registro, correspondiente al *host www* de la zona *redes.local*, de tipo A. Se denominan registros de tipo A (registros de *hosts*), a aquellos registros DNS que incorporan la información necesaria para que el servicio pueda devolver la IP sobre la que responde el *host* de que se trate, es decir, relaciona IP y nombre simbólico DNS de un *host*. Los registros de tipo A corresponden a *hosts* con IPv4 y los de tipo AAAA a equipos con IPv6[2].

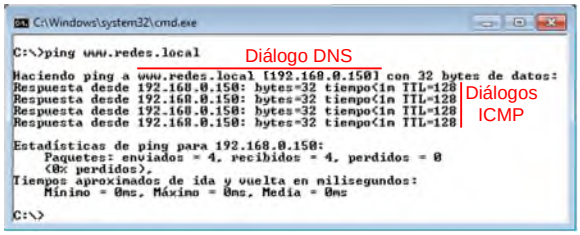


Figura 24

Figura 25

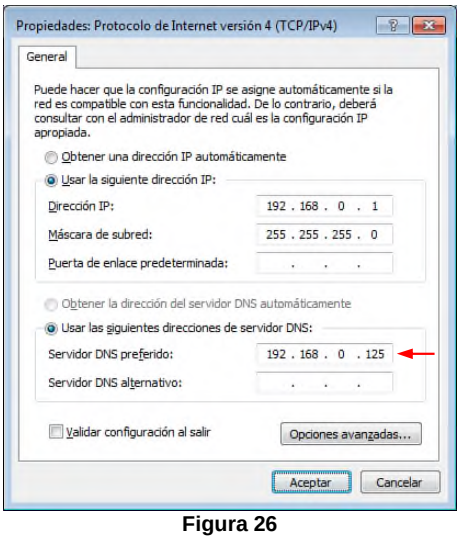


Figura 26

Una vez dado de alta el equipo de nombre *www*, en la zona *redes.local*, debe ser posible hacer una petición de eco al nombre simbólico *www.redes.local*, tal y como se recoge a continuación, Figura 24. Para que el R-W7-1 pueda solicitar la información necesaria, para resolver la FQDN (en la Figura 25 se muestran las partes de una FQDN), al servidor DNS, es necesario que lo tenga incorporado, como tal, en su configuración TCP/IP. En la Figura 26 se muestra la configuración TCP/IP del R-W7-1.

En la ventana de la consola en la que se recoge el resultado del ***ping***, deben singularizarse las partes que corresponden al diálogo DNS y al ICMP. Obsérvese, en la Figura 24, que tan solo la primera línea del resultado corresponde a la consulta DNS, ya que es en ella en donde se plasma la resolución hecha (IP

192.168.0.150) para la FQDN *www.redes.local*. El resto corresponde al diálogo ICMP entre el R-W7-1 (192.168.0.1) y la máquina de IP 192.168.0.150 y para nada interviene el servidor DNS.

La captura realizada por el *sniffer*, correspondiente al ***ping –n 1 www.redes.local***, es la que se muestra en la Figura 27 (en las capturas hechas para este ejercicio se utiliza el siguiente filtro de captura en el *sniffer: icmp or (udp port 53)*, adviértase que no se capturan los posibles diálogos ARP).

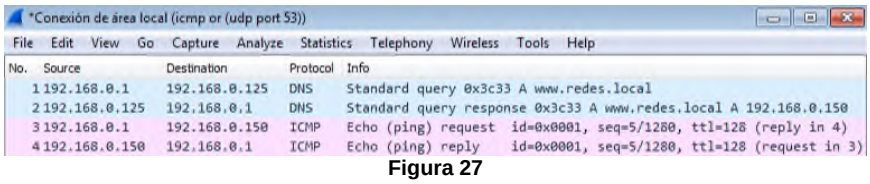
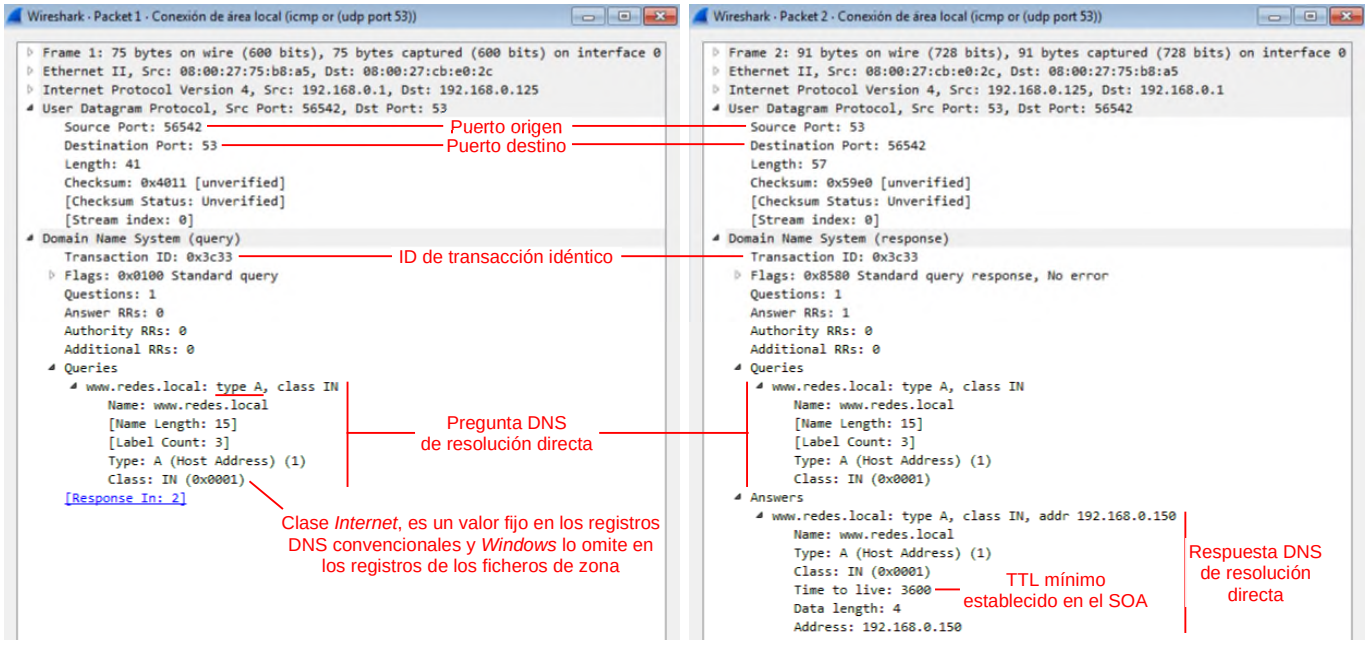


Figura 27

Recuérdese que las dos primeras tramas, de la captura, corresponden al diálogo DNS y las dos últimas al diálogo ICMP, tal y como se muestra en la columna *protocol* de la Figura 27.

En la Figura 28 se muestra el contenido de las tramas del diálogo DNS, capturadas por el *sniffer*.



Pregunta DNS de resolución directa (trama 1)

Respuesta DNS de resolución directa (trama 2)

Figura 28

Obsérvese, en la pregunta DNS de la Figura 28, que el cliente especifica que se solicita la búsqueda del registro tipo A correspondiente a la FQDN *www.redes.local*.

Adviértase que el ID de transacción es el mismo en la pregunta que en la respuesta, esto permite, por un lado, que el cliente DNS empareje correctamente cada pregunta con su respuesta y, por otro, que el servidor pueda detectar preguntas duplicadas de un cliente DNS. También puede comprobarse el direccionamiento del nivel de transporte, observándose como el cliente DNS utiliza un puerto UDP efímero, generado de forma aleatoria entre los puertos no asignados (en la Figura 28 el 56542), y dirige sus mensajes al puerto del servidor DNS UDP:53. Obviamente, el servidor envía la respuesta al puerto del cliente que recibe como puerto origen en la pregunta, transcurriendo los diálogos tal y como se muestra en la Figura 29.

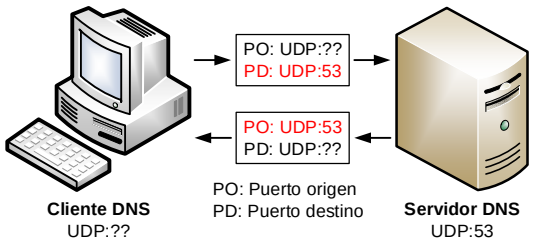


Figura 29

En la pregunta DNS aparece una referencia a la clase IN (Internet), que es un valor fijo en los registros DNS convencionales, y que se omite en los ficheros de zona generados por *Windows*. Por el contrario, en los ficheros de zona usados en sistemas *GNU/Linux*, suele incorporarse la referencia a la clase IN en cada registro de la zona.

Una vez realizada esta petición de ***ping*** a *www.redes.local*; si la repetimos, obtenemos la captura mostrada en la Figura 30. En la que no aparecen las tramas correspondientes al diálogo DNS. ¿Cuál es la razón de esta diferencia?, tratándose de la misma petición de eco.

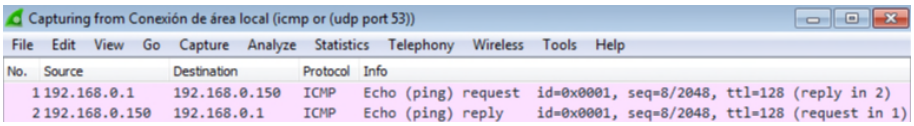


Figura 30

La causa debemos buscarla en el cliente, en este caso en el R-W7-1. De la misma manera que cuando se hablaba del diálogo ARP se veía que existía una caché dinámica y volátil ARP, en el cliente; de forma que antes de lanzar una petición ARP se consultaba esa caché y si se encontraba la respuesta en ella, ya no se generaba petición ARP. También existe una caché DNS dinámica y volátil en cada cliente (no todas las implementaciones de clientes DNS utilizan caché DNS, los sistemas *Windows* sí la utilizan en todas sus versiones actuales), de forma que en ella se almacenan los resultados de las últimas peticiones DNS que

hizo el cliente DNS, según esto, antes de lanzar alguna petición al servidor DNS, se comprueba la caché DNS y si ya tenemos la información en ella, no se molesta al servidor DNS con una pregunta cuya respuesta ya se conoce. Para ver el contenido de la caché DNS de una máquina *Windows*, se utiliza el comando ***ipconfig /displaydns*** que, en nuestro caso, mostrará el contenido que se ve en la Figura 31, en la que se aprecia la resolución hecha para *www.redes.local*.

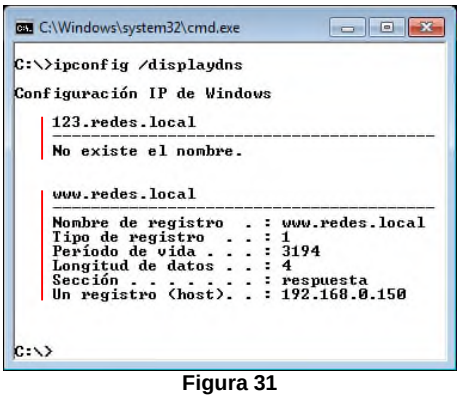


Figura 31

El valor que aparece en la caché DNS como período de vida, es un valor, dinámico, que corresponde al número de segundos que le restan, al registro, antes de ser eliminado. El valor inicial de este parámetro corresponde al valor que recibe en el campo TTL de la respuesta del DNS para esa entrada (Figura 28), que a su vez lo toma del valor del campo TTL mínimo del registro SOA de la zona de que se trate, Figura 19.

Es importante destacar, que de la misma manera que en la caché DNS se guarda el resultado positivo de una resolución DNS, también se recuerdan las peticiones DNS no resueltas, en la Figura 31 se muestra el ejemplo correspondiente a una supuesta máquina *123.redes.local*, lo cual, en algunos casos, pueda dar lugar a equívocos y problemas.

Para limpiar el contenido de la caché DNS del cliente, en entornos *Windows*, se utiliza el comando ***ipconfig /flushdns***.

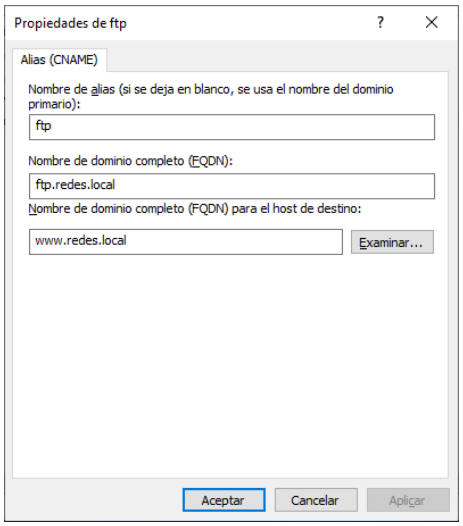


Figura 32

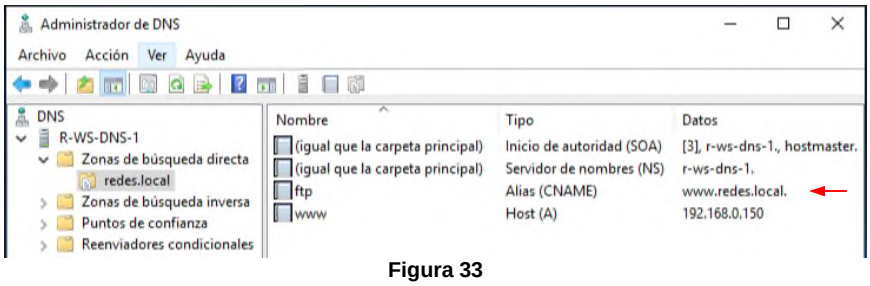


Figura 33

En muchas ocasiones se instalan varios servicios en una misma máquina, y para facilitar el acceso a los usuarios, mediante nombres que le sean sencillos y próximos al servicio que demandan, resulta interesante que esa máquina responda a distintos nombres DNS (alias). Por ejemplo, imagine que en un mismo servidor instala un servidor web y un servidor *FTP*, quizá lo más razonable sea indicarle al usuario que la empresa dispone de un sitio web en la dirección *www.redes.es* y de un servidor *FTP* en la *ftp.redes.local*, al usuario se le facilita el recordar cómo acceder a ambos servicios, ya que nos ajustamos a los convencionalismos *-de facto-* en los nombres de los servidores, sin importarle si responden en el mismo servidor físico o distintos. Corresponderá al administrador resolver esta cuestión en la definición de los registros DNS correspondientes al equipo, o equipos, que presta, o prestan, dichos servicios.

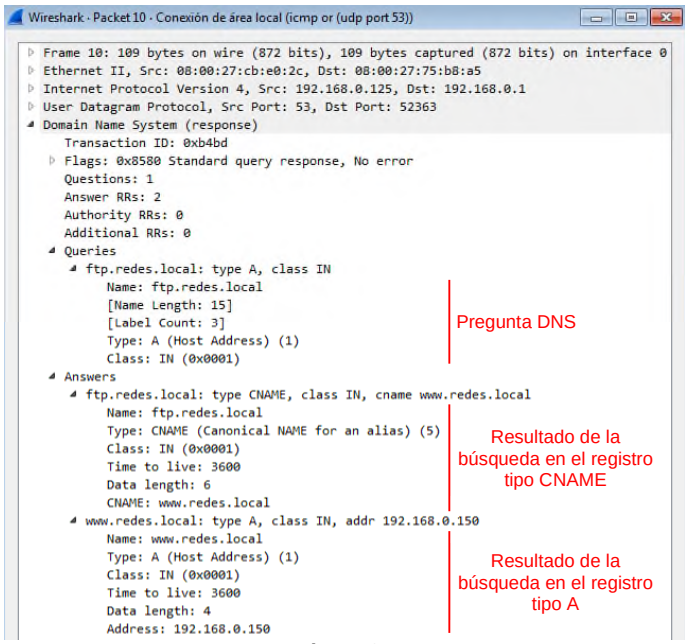


Figura 34

Siguiendo con nuestro ejemplo, vamos a dar de alta, en el servicio DNS, el alias *ftp* para nuestra máquina *www*, de forma que responda, correctamente, a ambas FQDN: Icono Iniciar → Herramientas administrativas → DNS → Desplegamos el árbol del servidor, haciendo clic en el signo "+" que aparece a su izquierda → Desplegamos el árbol de "Zona de búsqueda directa", haciendo clic en el signo "+" que aparece a su izquierda → Seleccionamos la zona "*redes.local*" → Botón derecho → Seleccionamos la opción "Alias nuevo (CNAME)..." → Y cubrimos el pequeño formulario de la siguiente forma: Nombre de alias: *ftp*; Nombre de dominio completo para el *host* de destino (FQDN): escribimos *www.redes.local* o bien le damos al botón "Examinar" y buscamos su registro en la zona del servidor DNS correspondiente. Quedando el formulario como se muestra en la Figura 32 → Botón "Aceptar".

Concluido el proceso de dar de alta el alias *ftp* para la máquina *www*, debemos encontrarnos en la situación reflejada en la Figura 33.

En donde se aprecia la incorporación del nuevo registro correspondiente al nombre *ftp*, obsérvese que es de tipo "Alias" (CNAME, ***Canonical NAME***) y que referencia el nuevo nombre al otro nombre simbólico de la máquina (*www.redes.local*), en lugar de a su IP, lo cual facilita la gestión, ya que si se desea cambiar la IP del servidor, el alias (o los alias, ya que pueden ser varios) no sufrirá ningún problema, pues apunta al registro original de la máquina y se podrá leer la nueva IP sin dificultades.

A la vista de lo comentado anteriormente, es sencillo deducir que las búsquedas, en un servidor DNS, sobre un alias, conllevan dos búsquedas consecutivas. En primer lugar, se localizará el registro correspondiente a la FQDN solicitada (en nuestro caso *ftp.redes.local*), que corresponderá al registro del alias (registro CNAME), una vez localizado tal registro se extraerá del mismo la FQDN del registro de referencia (en nuestro caso *www.redes.local*), tras lo cual se buscará el registro de *host* correspondiente, en donde se encuentra la IP que se necesita, en nuestro ejemplo la 192.168.0.150, enviándose el resultado de ambas búsquedas al cliente, tal y como se muestra en la Figura 34.

Según todo lo anterior, tanto el *host www*, como el *ftp* deben responder en la IP 192.168.0.150, tal y como se aprecia en la Figura 35. Obsérvese que cuando al servidor DNS se le pregunta por el alias, *ftp.redes.local*, lo resuelve como *www.redes.local*.

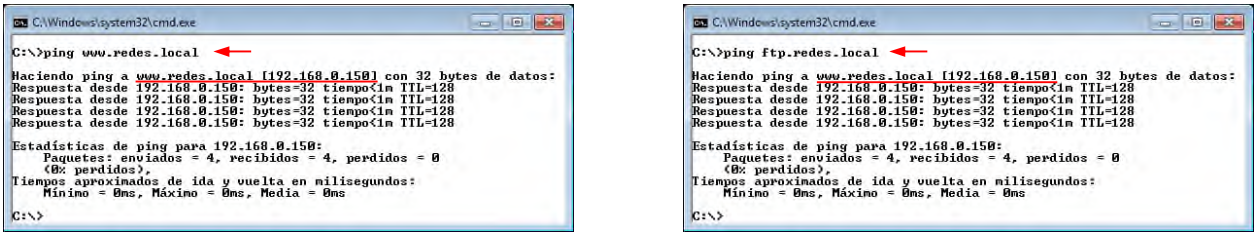


Figura 35

La pregunta que surge inmediatamente, es si sería posible utilizar un registro de tipo A para definir el *host ftp*, sin necesidad de usar el alias (CNAME), la respuesta es que sí. Aunque se prefiere utilizar el alias para evitar multiplicidades de IP en el registro DNS, lo que en el caso de un servidor con varios nombres complica la administración del servicio DNS, y es una posible fuente de errores por olvidar la actualización de la IP en alguno de los registros DNS del servidor con múltiples nombres registrados.

Básicamente, en una información de zona DNS, de búsqueda directa, podemos encontrarnos registros de tipo[2] SOA, NS, A, AAAA, CNAME, RP (***R**esponsible **P**erson*, persona responsable, se utiliza para incorporar la cuenta de correo electrónico en el SOA) y MX (***M**ail e**X**change Record, registro de intercambio de correo*), siendo este último especial para servidores de correo electrónico.

5.- Optimización de la configuración del servidor DNS.

Hasta aquí todo ha funcionado correctamente; sin embargo, la configuración del servidor DNS dista mucho de estar completa y optimizada. Lo primero que debemos solucionar es el hecho de que nuestro servidor DNS carece de servidores DNS en su configuración TCP/IP, no tiene configurado su cliente DNS, lo que impide, por ejemplo, que desde él sea posible lanzar un ***ping*** a *www.redes.local*, tal y como se muestra en la Figura 36, a pesar de ser él, el servidor DNS primario de esa zona. Es muy importante tener claro que nada tiene que ver la configuración del cliente DNS del servidor, que es la que nos falta, con la configuración del servicio DNS que se ejecuta en el mismo servidor, que es la que tenemos a medio hacer. Es más, en ocasiones, el propio servicio DNS hace uso del cliente DNS del servidor para solicitar resoluciones de nombres simbólicos DNS.

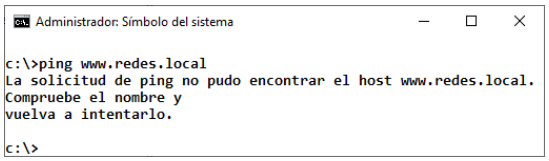


Figura 36

Para configurar el servidor DNS del cliente DNS, dado que será él mismo, podemos utilizar la propia IP del servidor (192.168.0.125) o bien la correspondiente al bucle local (127.0.0.1), ya que en ambos casos se obtiene el mismo resultado. En este caso sería una buena idea utilizar la referencia al bucle local, ya que en el supuesto de que nos viéramos en la necesidad de cambiar la IP del servidor, no necesitaríamos acordarnos de cambiar, también, la IP del servidor DNS del cliente, pues la referencia al bucle local es independiente de la IP configurada en la máquina. Según esto, la configuración TCP/IP de nuestro servidor DNS sería la que se muestra en la Figura 37.

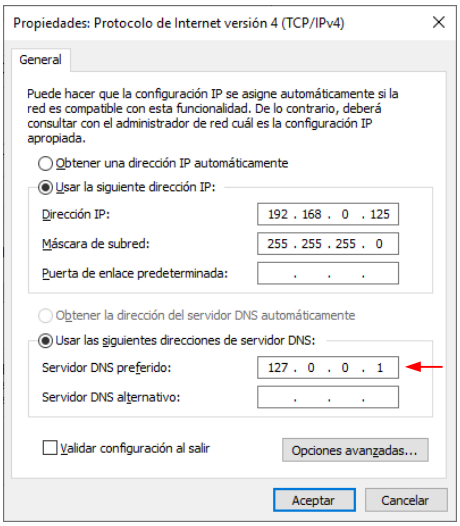


Figura 37

Nótese que es posible utilizar el bucle local porque sabemos que el servicio DNS también abre el puerto UDP:53 sobre el bucle local, tal y como se pone claramente de manifiesto en la Figura 14. Si este servicio no configurara el *socket* UDP 127.0.0.1:53, no sería posible utilizar la IP del bucle local para configurar el cliente DNS del servidor DNS, ya que el servicio DNS nunca recibiría las preguntas DNS enviadas a esa IP.

Una vez configurado el cliente DNS del servidor, haciendo un ***ping*** a *www.redes.local* debemos obtener el mismo resultado que el mostrado en la Figura 35, para el lanzado desde el R-W7-1.

6.- Optimización de la configuración de la zona de búsqueda directa *redes.local*.

Pasaremos, ahora, a optimizar la configuración de la zona de búsqueda directa *redes.local* empezando por solventar una pequeña, pero importante, incongruencia que tenemos. Estudiando la Figura 18, la Figura 19 y la Figura 20 advertiremos que siempre se hace referencia al DNS primario con el nombre *NetBIOS* de la máquina (R-WS-DNS-1), la opción por defecto que toma el servicio DNS en *Windows* cuando se crea una zona. Pero además, ese será el nombre que circule por la red para identificar al servidor DNS primario de la zona *redes.local*, dándose la paradoja de que tal nombre no lo resuelve ningún servidor DNS, tal y como se demostró en la Figura 21.

Empezaremos por discutir que nada tiene que ver el nombre *NetBIOS* con el nombre que daremos al *host*, en la FQDN correspondiente, a cada servicio que instalemos. Por ejemplo, si en un único servidor instalásemos el servicio DNS, un servidor

web y un servidor FTP, lo habitual sería asignarle el identificador *ftp.redes.local*, para el servicio FTP, *www.redes.local*, para el servicio web y para el servidor DNS *¿r-ws-dns-1.redes.local*?. No, no parece coherente. Lo lógico sería asignarle un nombre simbólico del tipo *dns.redes.local*, de manera que fuera sencillo de recordar y además que fuera posible resolverla a través del propio servicio DNS. Los nombres *NetBIOS* de las máquinas suelen ser muy particulares de cada red, e incluso de cada administrador, y nada significativos fuera de ese entorno. Razón por la cual, no tienen por qué coincidir.

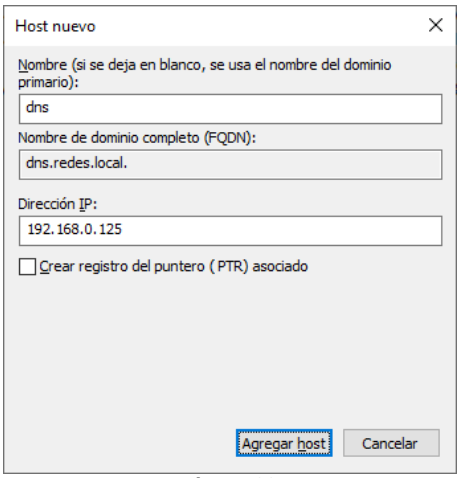


Figura 38

Definitivamente a nuestro servidor DNS le asignaremos el identificador *dns.redes.local* y además le crearemos un registro de *host* (tipo A) para que se pueda resolver.

Para ello seleccionamos el contenedor de la zona *redes.local* (panel izquierdo) o nos situamos bajo el último registro (panel derecho) → Botón derecho → Opción "*Host* nuevo (A o AAAA)..." y cubrimos el formulario poniendo en el primer campo el nombre del equipo, en nuestro caso "dns" y en el segundo de los campos la dirección IP del equipo al que deseamos asignar el nombre anterior, en el ejemplo que estamos desarrollando sería la IP 192.168.0.125 (tal y como se muestra en la Figura 38) → Botón "Agregar *host*" → Botón "Realizado".

Incorporado el registro de *host* para el nombre simbólico *dns.redes.local*, debe ser posible hacer un ***ping*** a ese nombre de *host* y obtener la respuesta que se muestra en la Figura 39.

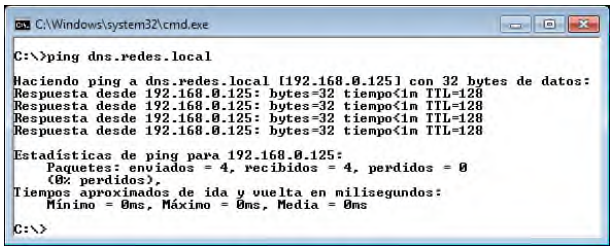


Figura 39

Con el nuevo registro, el contenido de la zona *redes.local* será el mostrado en la Figura 40.

Es interesante destacar que, así como en la configuración TCP/IP del servidor utilizamos el bucle local (127.0.0.1) como IP del DNS, no es posible hacer lo mismo a la hora de crear el registro de *host* para el nombre simbólico *dns.redes.local*, ya que, en este caso, es información para uso externo a la propia máquina y lo que se conseguiría sería que todas la máquinas, que solicitaran la resolución de esa FQDN, obtuvieran como respuesta que eran ellas mismas (se resolvería como la IP 127.0.0.1). Lo cual es claramente incorrecto.

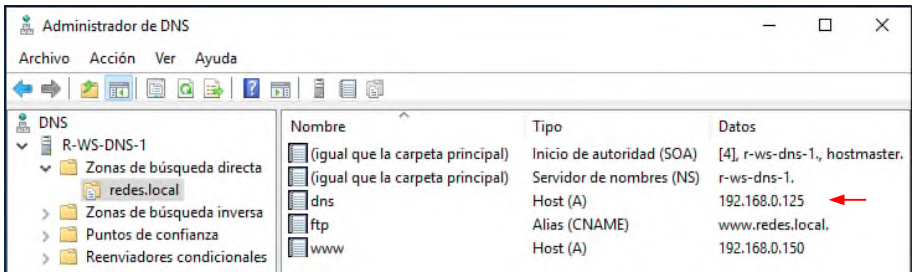


Figura 40

Tal y como ya se discutió, la misma información que acabamos de incorporar en el registro de *host* debería ser la que se distribuyera en la red como DNS primario, y la que se recogiera en el correspondiente registro NS del servidor DNS.

Empezaremos por incorporarlo como DNS primario en el SOA, para ello haremos doble clic sobre el registro SOA de la zona *redes.local* y pulsaremos el botón "Examinar" correspondiente al campo "Servidor primario" → Doble clic sobre el servidor que se muestra → Doble clic sobre la carpeta "Zonas de búsqueda directa" → Doble clic en la zona *redes.local* → Seleccionamos la entrada correspondiente al nombre "dns" → Botón "Aceptar". Aprovecharemos, también, para cambiar el contenido del campo "Persona responsable", incorporando la cuenta de correo del administrador del sistema *administrador@redes.local*, asumiendo la existencia de la misma. Recuérdese que no se soporta el carácter @ y que se debe sustituir por un punto, quedando el identificador de la cuenta como *administrador.redes.local*. Quedando, finalmente, el formulario del SOA tal y como se muestra en la Figura 41. Botón "Aceptar".

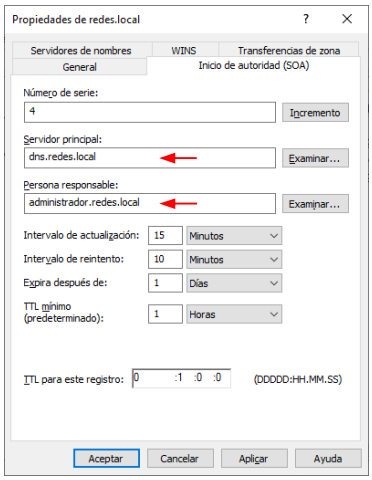


Figura 41

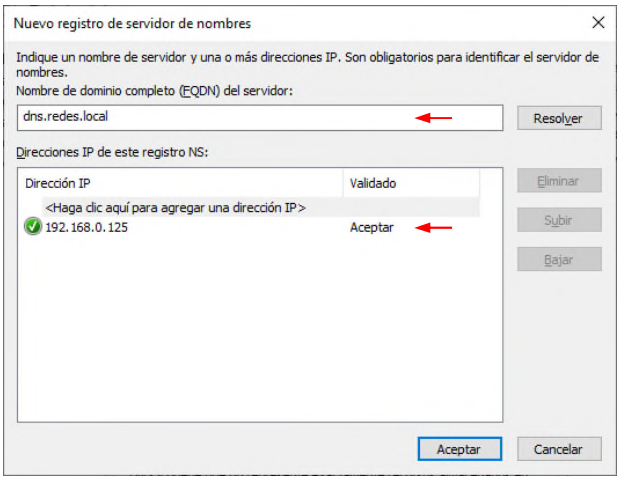


Figura 42

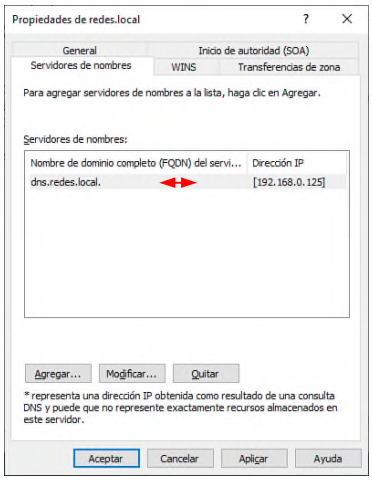


Figura 43

A continuación cambiaremos la información del registro NS, para lo cual haremos doble clic sobre él ➔ Seleccionamos la línea correspondiente al nombre *NetBIOS* del servidor que deseamos eliminar ➔ Botón "Quitar" ➔ Botón "Agregar" ➔ En el campo "Nombre de dominio completo (FQDN) del servidor", escribimos la URL del servidor, *dns.redes.local* ➔ Botón "Resolver", tras lo cual debe mostrarnos el contenido de la Figura 42 (esta resolución solo funcionará si el servidor tiene correctamente configurado el DNS, en su configuración TCP/IP, ya que la realiza a través del propio cliente DHCP) ➔ Botón "Aceptar", tras lo cual ya debe aparecer *dns.redes.local* en el registro NS, Figura 43.

Es importante destacar que cuando se da de alta un servidor de nombres para una zona determinada, Figura 42, el servidor DNS lo valida pidiéndole una copia del registro SOA de la zona en cuestión, si no la recibe permite configurarlo como tal, pero advierte que no fue posible validar la existencia de la zona correspondiente en el servidor DNS indicado.

También es posible incorporar el nombre simbólico *dns.redes.local*, en el registro NS, introduciendo la IP asociada en el campo "Dirección IP" del formulario mostrado en la Figura 42. Concluidos estos cambios, la zona *redes.local* debe tener el contenido que se muestra en la Figura 44.

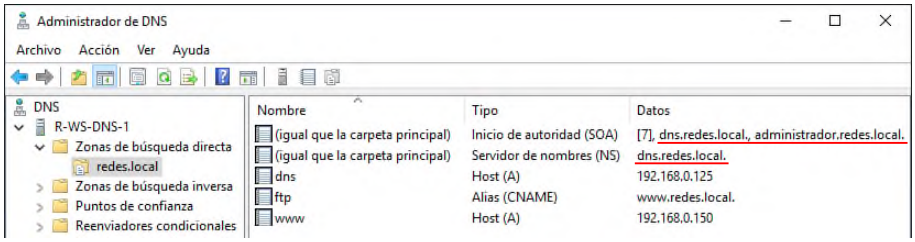


Figura 44

En muchas ocasiones se desea que de la misma manera que se resuelve el *host* de un domino, por ejemplo el *host www* del dominio *cesga.es*, *www.cesga.es*, (***CE**ntro de **S**upercomputación de **GA**licia*[3]) en la IP 193.144.34.248, tal y como se muestra en la Figura 45-1, se pueda resolver el propio dominio, *cesga.es*, Figura 45-2, asociándolo a una IP. Esto permitirá, por ejemplo, alcanzar el sitio web del CESGA utilizando cualquiera de los siguientes localizadores: *www.cesga.es* o *cesga.es*; lo que facilita el acceso a los usuarios, ya que solo deben recordar el nombre del dominio y no la denominación del *host* más la del dominio.

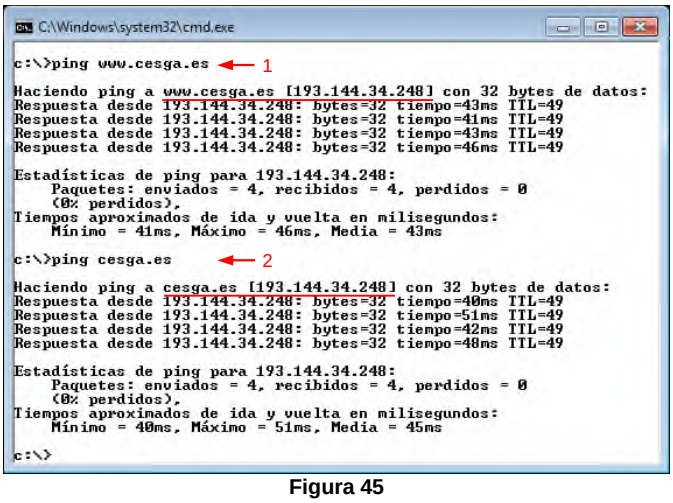


Figura 45

En nuestro caso, por ejemplo, podríamos resolver el *host www* del dominio, con la FQDN *www.redes.local*, en la IP 192.168.0.150, y asociar el propio dominio, *redes.local*, a la misma IP, de manera que sea posible hacer un ***ping*** a *redes.local* y que nos responda el equipo de IP 192.168.0.150.

Para ello crearemos un registro de *host* para la zona, asociado a la IP 192.168.0.150. Seleccionamos el contenedor de la zona *redes.local* (panel izquierdo) o nos situamos bajo el último registro (panel derecho) ➔ Botón derecho ➔ Opción "*Host* nuevo (A o AAAA)..." y cubrimos el formulario dejando el campo "Nombre" en blanco e incorporando en el segundo de los campos la dirección IP del equipo al que deseamos asociar la zona, en el ejemplo que estamos desarrollando sería la IP 192.168.0.150 (tal y como se muestra en la Figura 46) ➔ Botón "Agregar *host*" ➔ Botón "Realizado".

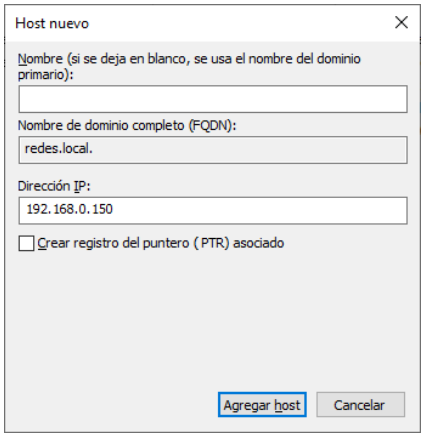


Figura 46

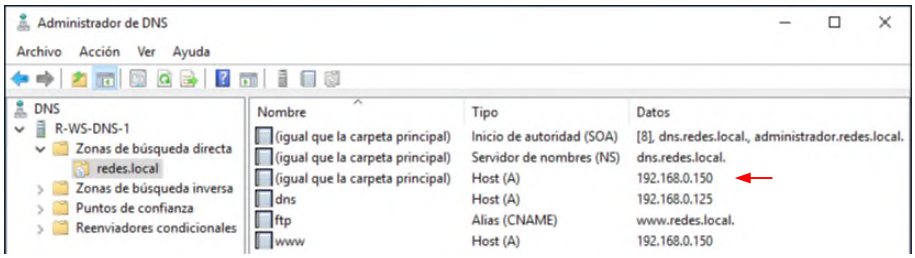


Figura 47

El contenido actual de la zona *redes.local* será el mostrado en la Figura 47.

Ahora será posible lanzar un ***ping redes.local*** y recibir la respuesta desde la IP 192.168.0.150, tal y como se muestra en la Figura 48.

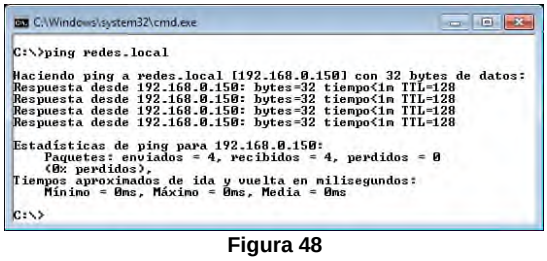


Figura 48

Adviértase que esta configuración obliga a duplicar la IP 192.168.0.150, ya que la tenemos en el registro de la propia zona y en la del *host www*. Esta duplicidad, tal y como ya se comentó, no suele ser aconsejable ya que puede ser una fuente de errores. Para evitar esta repetición lo que debe hacerse es definir el servidor *www* como alias de la zona, tal y como se muestra en la Figura 49. Para incorporar la FQDN, en el campo correspondiente de la Figura 49, puede pulsarse le botón "Examinar" y seleccionar el registro que aparece como "(igual que la carpeta principal)", Figura 50.

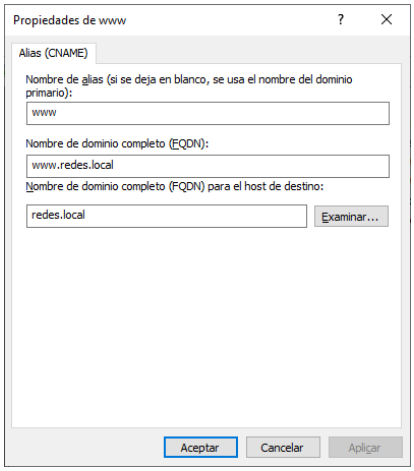


Figura 49

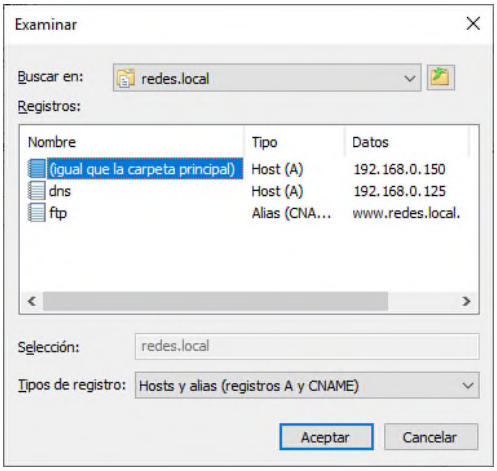


Figura 50

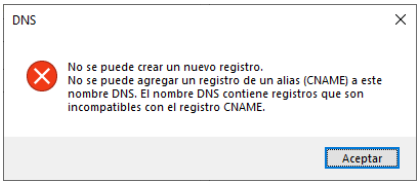


Figura 51

Es importante destacar que, a la hora de crear el registro, para la propia zona, no puede utilizarse un registro tipo CNAME. Es decir, no puede definirse la propia zona como un alias de cualquier otro registro. En el caso de que se intentará configurarlo de esta manera, el propio sistema lo impide, e informa mediante el aviso mostrado en la Figura 51.

Tras los últimos cambios, quedará la zona tal y como se muestra en la Figura 52.

Tal y como puede apreciarse, en la Figura 52, hemos conseguido que, en la zona *redes.local*, no haya ni una sola IP duplicada pero, sin embargo, hemos creado una condición que siempre debe procurar evitarse.

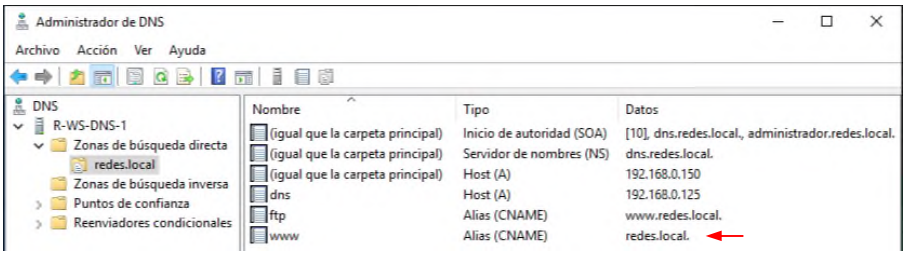


Figura 52

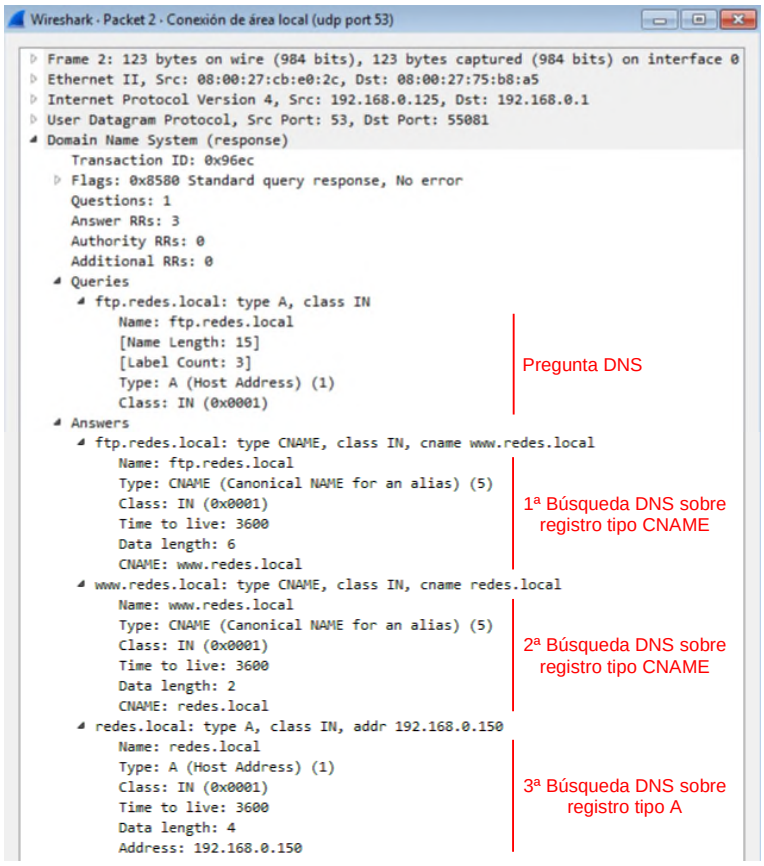


Figura 53

Si nos fijamos en el registro del equipo *ftp*, advertiremos que lo tenemos referenciado como un alias del equipo *www*, que, a su vez, es un alias de la propia zona. De acuerdo con esto, cuando algún cliente DNS solicite, del servidor DNS, la resolución de la FQDN *ftp.redes.local*, se obligará al servicio DNS a realizar tres búsquedas, hasta obtener la respuesta solicitada. La primera búsqueda nos llevará a la FQDN *www.redes.local*, la segunda nos llevará a la propia zona, *redes.local*, y la tercera relacionará la FQDN *redes.local* con la IP 192.168.0.150, que es la respuesta buscada. Todo ello puede comprobarse en la Figura 53, en la que se muestra una captura correspondiente a la resolución de la FQDN *ftp.redes.local*.

Para evitar esta búsqueda innecesaria, tan solo debemos declarar la FQDN *ftp.redes.local* como un alias de la propia zona, quedando, finalmente, como se muestra en la Figura 54.

En el servidor DNS toda la información de la zona *redes.local* se guarda en el fichero:

C:\Windows\System32\dns\redes.local.dns

Recuérdese que durante la creación de la zona se nos indicó si queríamos usar ese fichero o preferíamos seleccionar otro.

A efectos prácticos, resultará muy interesante conocer su contenido, ya que será idéntico al que se generará en las plataformas *GNU/Linux* (Se eliminaron algunas líneas de comentario -son las que empiezan por el carácter ";" en el contenido original del fichero- para ganar en claridad de código):

```
; Database file redes.local.dns for Default zone scope in zone redes.local.
; Zone version: 15

@       IN      SOA        dns.redes.local.   administrador.redes.local. (
                               15      ; serial number
                              900      ; refresh
                              600      ; retry
                            86400      ; expire
```

```
                    3600 )   ;  default TTL
; Zone NS records
@             NS        dns.redes.local.

; Zone records
@             A         192.168.0.150
dns           A         192.168.0.125
ftp         CNAME       redes.local.
www         CNAME       redes.local.
```

Como puede apreciarse, en estas pocas líneas está todo lo que hemos configurado en esta primera práctica. La configuración de una zona de búsqueda directa en sistemas *GNU/Linux* nos obligará a generar, manualmente, un fichero prácticamente igual que este.

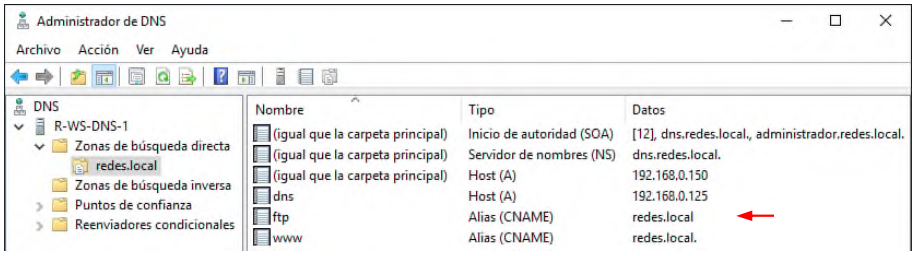


Figura 54

Indicar, por último, que el carácter "@", que aparece en el fichero, hace referencia a la propia zona (en nuestro caso, *redes.local*).

7.- EJEMPLO PRÁCTICO DE LA UTILIZACIÓN DEL SERVICIO DNS.

Hasta ahora, hemos intentado desentrañar el funcionamiento básico de las búsquedas directas en el servicio DNS (el cliente envía una FQDN y obtiene la IP asociada), utilizando diálogos ICMP perfectamente conocidos y sencillos.

Sin embargo, a nadie se le escapa que no es ésta la utilidad más práctica, y usada, del servicio DNS, ya que, sin duda alguna, la más común es la resolución de nombres simbólicos propiciada por los clientes web (navegadores).

Figura 55

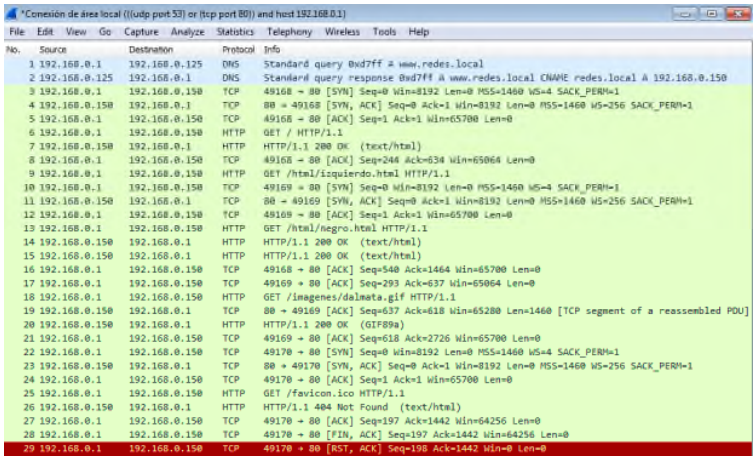


Figura 56

Para comprobar los diálogos DNS generados por un navegador web, empezaremos por limpiar la caché DNS del R-W7-1, ejecutando la orden ***ipconfig /flushdns***. A continuación, levantaremos un *sniffer*, en la subred correspondiente, y utilizaremos el siguiente filtro para realizar la captura: *((udp port 53) or (tcp port 80)) and host 192.168.0.1*. Lo que nos permitirá capturar, únicamente, el tráfico DNS (puerto UDP 53[4]) y el tráfico HTTP (puerto TCP 80[5]) que tenga su origen, o su destino, en el R-W7-1 (IP 192.168.0.1).

Acudiendo al R-W7-1 abriremos el *Internet Explorer* y en el campo de direcciones escribiremos *www.redes.local*, tal y como se muestra en la Figura 55.

Si todo funcionó en la forma debida, el navegador debe mostrarnos la web de la Figura 55, y el *sniffer* debió de capturar el tráfico mostrado en la Figura 56, en el cual las dos primeras tramas corresponden a la pregunta DNS propiciada por el cliente web para averiguar la IP asociada a la FQDN *www.redes.local*, y, una vez conocida esta dirección IP, comenzar el diálogo HTTP, con el servidor de IP 192.168.0.150, para obtener la página web deseada, tramas 3 a 29.

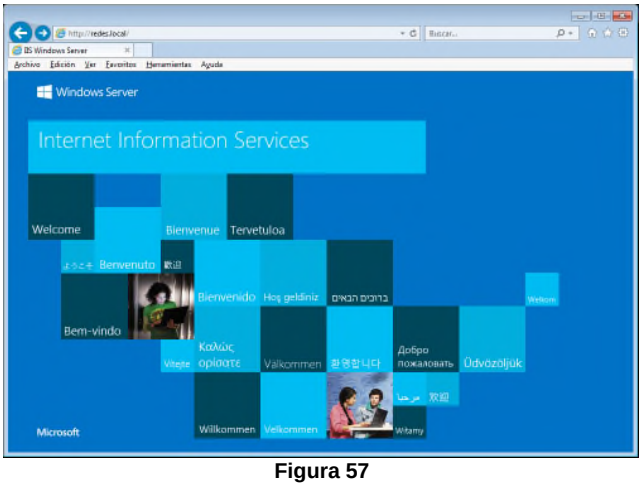


Figura 57

Como puede comprobarse, y es natural, se reproduce el diálogo DNS visto a lo largo del ejercicio.

Adviértase, que en este caso sería posible solicitar la resolución de la FQDN *redes.local*, ya que se dispone, en el servicio DNS, del registro tipo A correspondiente y, por lo tanto, se resolverá como respondiendo en la IP 192.168.0.150; que nos devolverá, con la configuración actual del servidor web, la web por defecto del IISv10 (***I**nternet **I**nformation **S**ervices*, servidor web de *Microsoft*) mostrada en la Figura 57.

8.- NOTAS FINALES.

[1] Con la única finalidad de ganar en claridad, se tratarán de forma independiente las zonas de búsqueda directa y las de búsqueda inversa. Pero es obligado aclarar, desde el comienzo, que nunca debe configurarse una zona de búsqueda directa sin su correspondiente, o correspondientes, zona de búsqueda inversa.

[2] Para los distintos tipos de registros DNS, véase: https://www.redeszone.net/tutoriales/internet/que-es-registros-dns/

[3] Para CESGA, véase: https://www.cesga.es/

[4] El servicio DNS también utiliza el puerto TCP 53, pero solo en diálogos, entre servidores DNS, de transferencia de zona. Véase: https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio

[5] Para el puerto TCP 80, véase: https://es.wikipedia.org/wiki/Anexo:Puertos_de_red