White Paper

NSLOOKUP, herramienta para la gestión de los servidores de DNS

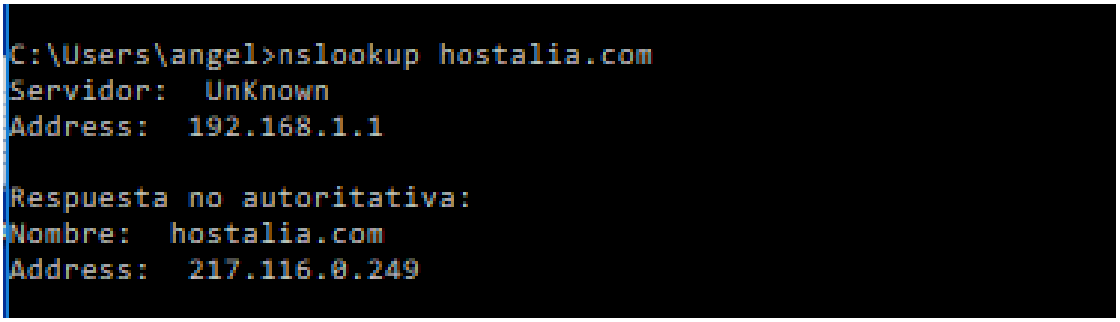
Hostalia.

Como mucho de vosotros ya sabréis, parte importante del buen funcionamiento de Internet se lo debemos al sistema de nombres de dominios, también conocido por las siglas DNS. Este sistema, que se encuentra distribuido por todo el mundo, es el encargado de convertir los nombres de dominio en direcciones IP que hacen referencia a las máquinas donde están hospedadas las páginas web. Esto es lo que hace que los usuarios no tengan que recordar complejas direcciones IP para visitar sus páginas favoritas. Lo que pasa es que en ocasiones esta resolución de nombres de dominio puede dar problemas, de ahí que pueda ser interesante conocer alguna herramienta que nos permita realizar de forma manual la dirección IP asociada a un dominio. Esto lo podemos conseguir gracias a la herramienta NSLOOKUP, una aplicación que está disponible tanto en Windows como Linux y en MacOS. A lo largo de nuestro White Paper nos centraremos en hablar más sobre esta interesante herramienta.

¿Qué es NSLOOKUP?

NSLOOKUP es una herramienta de línea de comandos cuya función básica es consultar, obtener información, probar y solucionar problemas de los servidores DNS que usa una conexión, así como realizar una resolución inversa de una dirección IP. Aunque el uso de la herramienta es mediante línea de comando, su funcionamiento resulta muy sencillo y nada complicado. Como ya hemos comentado, suele estar instalada por defecto en los principales sistemas operativos. En sistemas operativos Windows podremos iniciar el servicio a través del

símbolo del sistema (CMD), mientras que en UNIX o MacOS se hará desde un terminal.



Cuando hagamos una consulta mediante NSLOOKUP, veremos de forma frecuente estos dos términos:

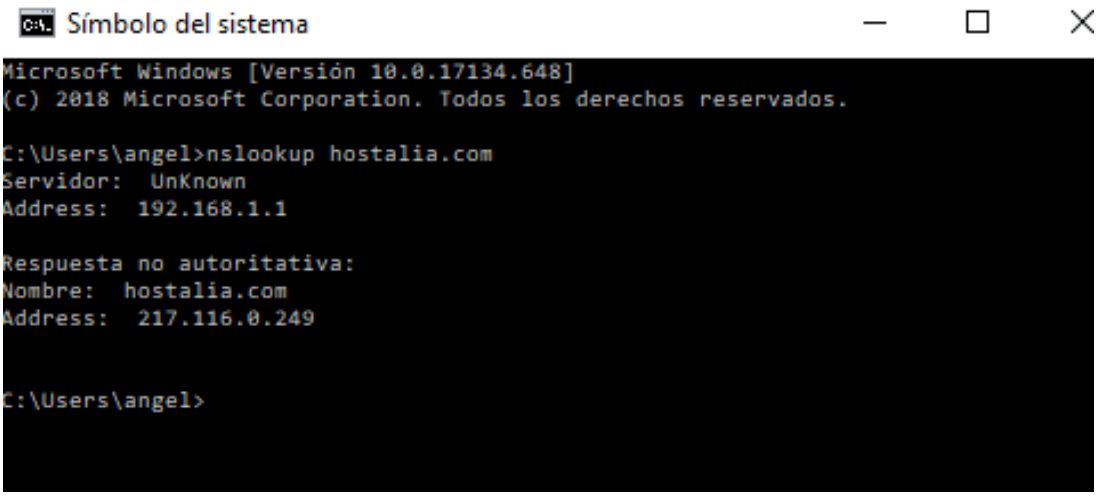
- **Authoritative Answer:** significa que la respuesta DNS se ha producido desde el servidor DNS que tiene todo el archivo de información disponible para esa zona.
- **Non Authoritative Answer:** significa que la respuesta DNS se ha producido desde un servidor DNS que tiene en caché una copia de las consultas realizadas para esa zona, al servidor que tiene la Autoridad para responder (el que tiene el archivo de zona). Por esto veremos muy a menudo la respuesta desde servidores que son Non Authoritative.

Funcionamiento de NSLOOKUP

Como ya hemos comentado anteriormente, para utilizar esta herramienta es necesario abrir el programa de líneas de comando del sistema operativo en cuestión. Una vez realizado esto, encontramos dos métodos diferentes a la hora de utilizar esta herramienta.

Modo normal o no interactivo

En este caso, en la línea de consola se introduce el nombre del comando, seguido de las opciones que queremos ejecutar. Finalmente se pulsa “Enter” para que se ejecute la petición.

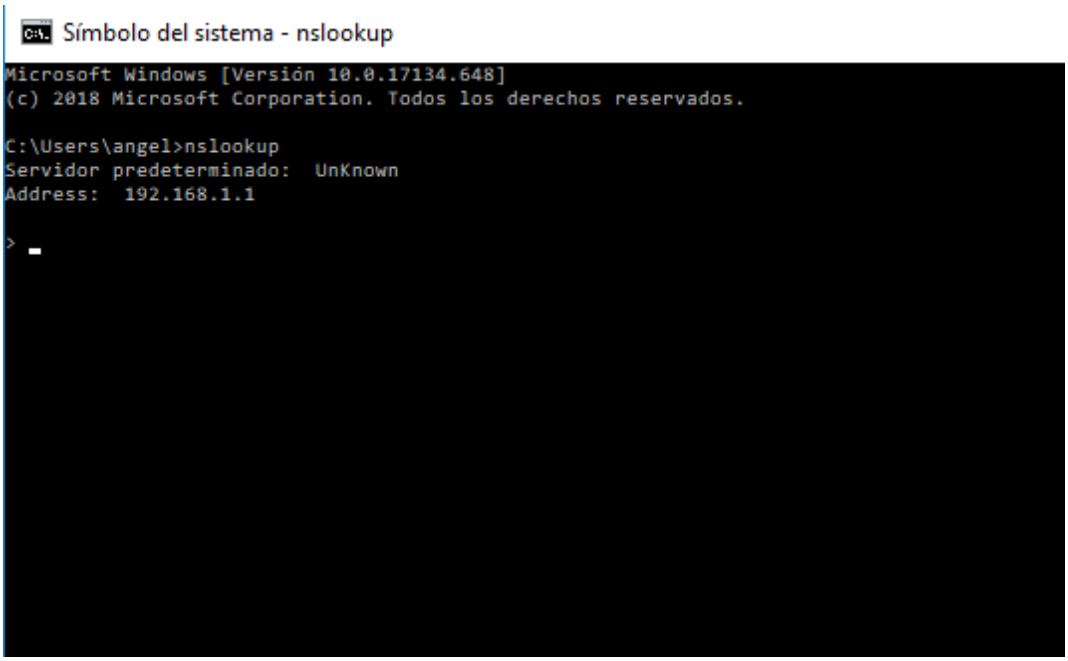


En la imagen se puede observar como la instrucción ejecutada ha sido “nslookup hostalia.com”. En este resultado, observamos los siguientes componentes:

- **Servidor**: Aquí nos indica el nombre del servidor DNS que utilizará la herramienta para hacer las consultas
- **Address**: Nos indica la dirección IP del servidor DNS que estamos usando
- **Respuesta no autoritativa**: Nos indica un servidor DNS que no es dueño del dominio que estamos buscando pero al que se puede consultar para obtener más información.
- **Nombre**: Es el nombre del dominio que estamos buscando.
- **Addresses**: Nos indica las direcciones IP que responden a este dominio (registro A).

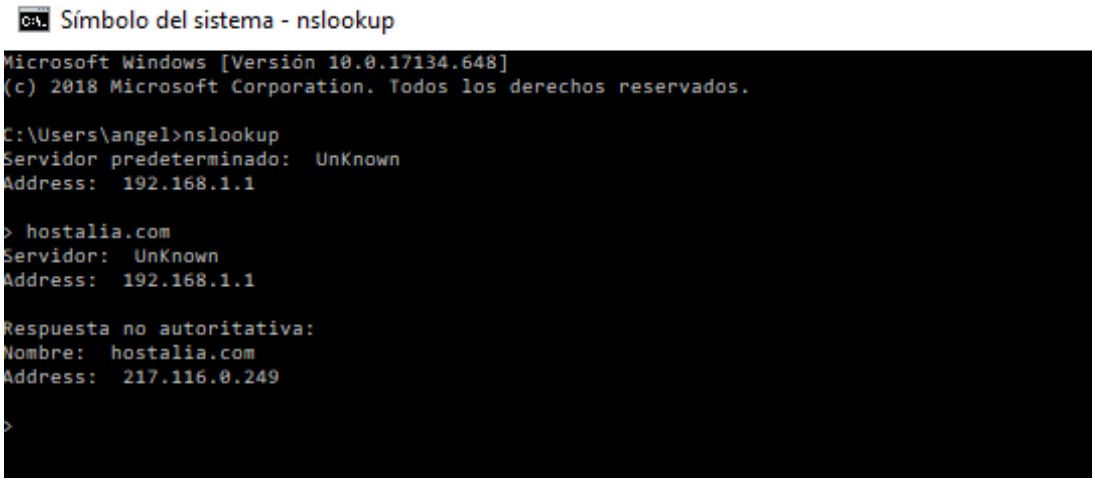
Modo interactivo

En el caso de que queramos buscar registros más específicos, es recomendable utilizar la herramienta NSLOOKUP en su forma interactiva, es decir, iniciamos el comando y después se añaden los argumentos.



En este caso, obtenemos una respuesta como se muestra en la figura anterior. Ahí se muestra el servidor de DNS que estamos utilizando para hacer nuestras consultas, así como su dirección IP. También se muestra el prompt que nos permitirá ingresar información sobre la consulta que queremos realizar.

Por defecto se buscarán siempre registro tipo A, es decir, se nos devolverá la dirección IP asociada al dominio que indiquemos, aunque esto lo podemos cambiar como veremos en el siguiente apartado.



En este caso, la respuesta que hemos obtenido cuando ejecutamos el comando en su modo normal.

Ejemplos de aplicación de NSLOOKUP

Veamos algunos ejemplos de uso que podemos hacer con la herramienta NSLOOKUP.

Peticiones de diferentes registros de DNS

Como hemos comentado en el punto anterior, por defecto las búsquedas se llevan a cabo sobre el registro A del dominio. Si queremos obtener registros diferentes, debemos especificarlo primero mediante alguna de las opciones que ofrece:

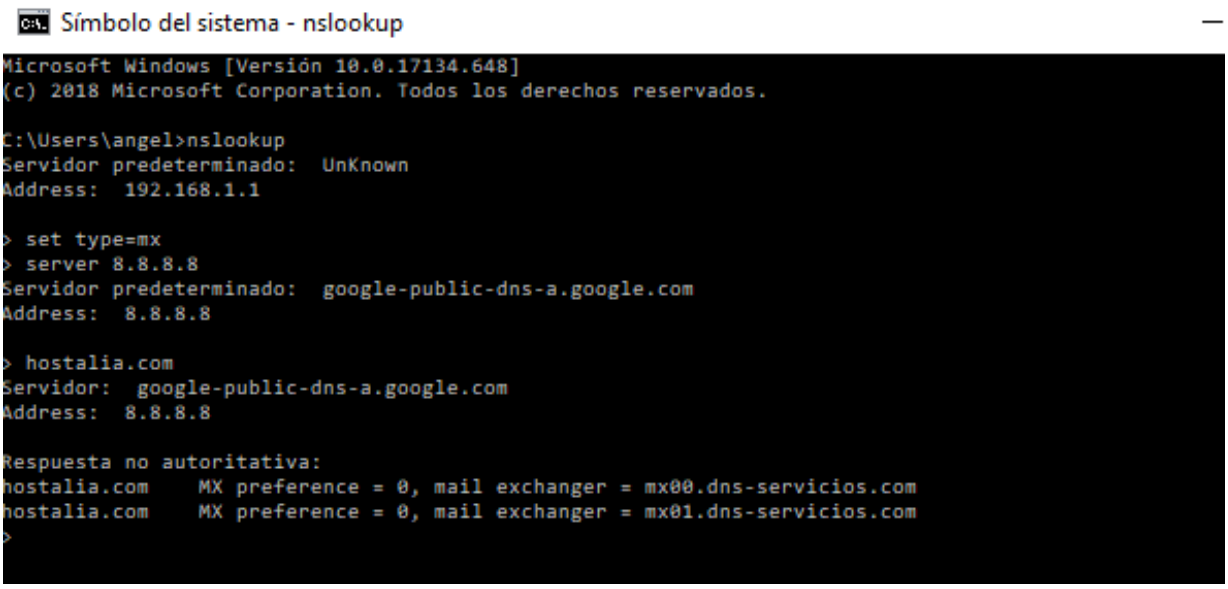
- **set type=A**, para buscar registros A.
- **set type=PTR**, para buscar registros reversos.
- **set type=MX**, para buscar los registros Mail Exchange del correo.
- **set type=TXT**, para buscar registros de texto como SPF o DKIM.
- **set type=CNAME**, para buscar alias del dominio.

En este ejemplo, primero hemos configurado la herramienta para buscar registros MX tecleando “set type=mx”, seguido del nombre del dominio del cual queremos conseguir la información.

Estado de los cambios realizados en nuestros registros DNS

Otro uso común de esta herramienta es conocer el estado en el que se encuentra los cambios que hayamos hecho en nuestros registros de DNS públicos. Cualquier cambio que se realice sobre los registros de DNS, puede tardar horas en propagarse. Para saber si tu DNS local ya aplicó los cambios, puedes ejecutar los comandos que hemos visto anteriormente.

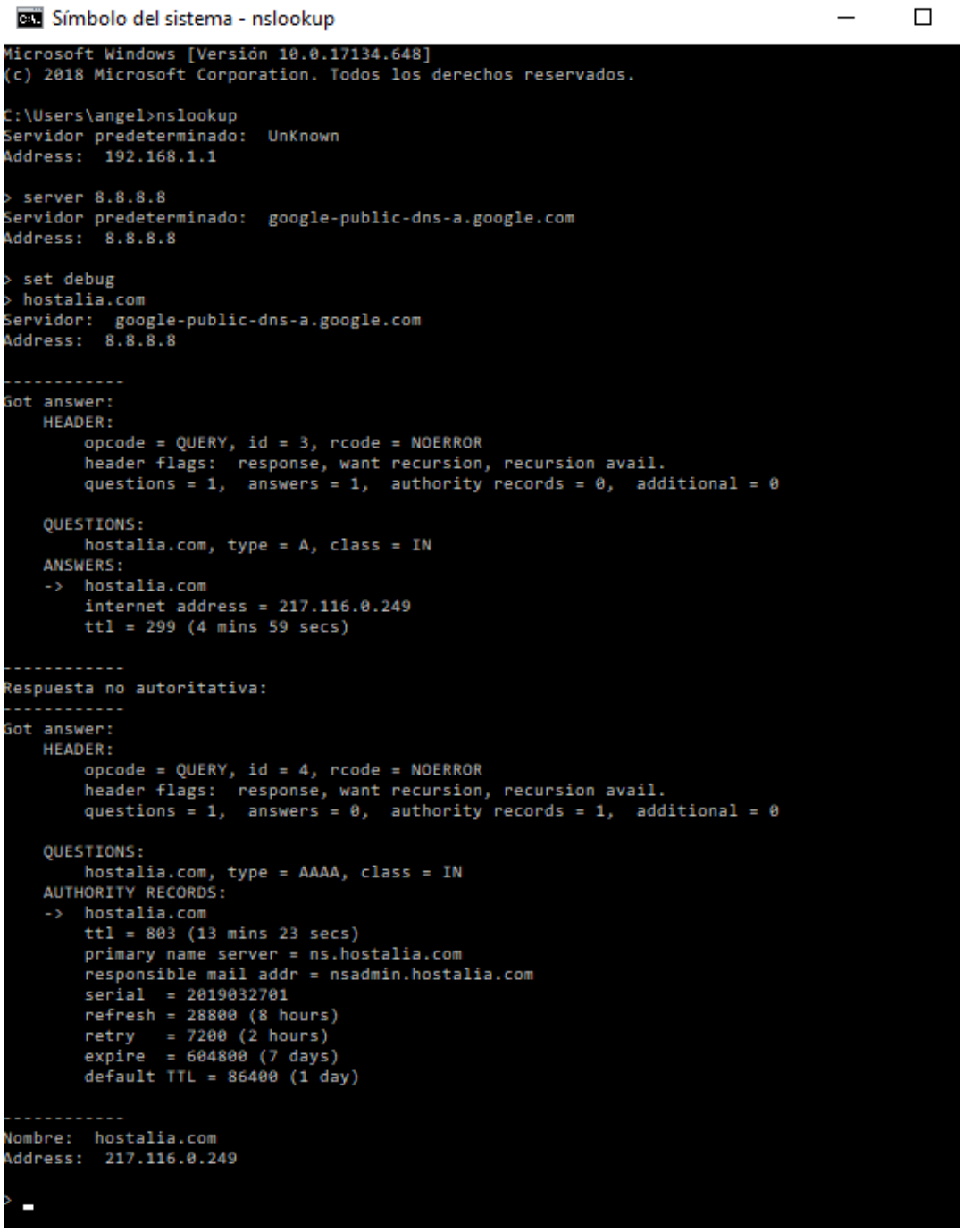
En el caso de que quieras saber si los cambios han sido ya efectivos en algún país, es necesario cambiar el servidor DNS desde donde realizamos la consulta e indicar el nuevo. Para realizar este cambio, debemos utilizar la opción “server” seguida de la dirección IP que queremos utilizar.



Si nos fijamos, por defecto la IP de nuestro servidor de DNS es 192.168.1.1, pero al indicar la opción de "server" lo hemos cambiado por 8.8.8.8 y ahora todas nuestras consultas serán resueltas desde ese servidor de DNS.

Extraer toda la información sobre un dominio

Mediante esta herramienta, también es posible conseguir toda la información que esté disponible de un dominio. Para ello es necesario utilizar la opción "set debug" que se encargará de ello.



Resolución inversa de una dirección IP

Cuando hablamos de resolución inversa de una dirección IP, nos estamos refiriendo a la posibilidad de conocer a que dominio o servidor apunta una determinada dirección. Para poder conocer esta información, tan solo debemos indicar la dirección IP de la

que queremos conocer su inversa después del comando NSLOOKUP.

Si nos fijamos, podemos observar en la imagen anterior como la dirección IP 8.8.8.8 está asociada a un subdominio de Google.