

Aprendiendo un poco más de DNS

El presente documento es complementario a lo visto en las clases teóricas y el laboratorio de protocolos de capa de aplicación. El curso de Redes de Datos 1 es autocontenido entre el teórico y los laboratorios, el material complementario busca ofrecer herramientas para que los alumnos puedan profundizar o complementar sus conocimientos por cuenta propia.

Introducción: Sin necesidad de utilizar un resolver (cliente DNS) en una computadora es posible realizar consultas DNS, por tipo de registro de un dominio y a un determinado servidor.

Existen varias alternativas para realizar consultas DNS desde un navegador web, a continuación, presentaremos una de ellas con la finalidad de que puedan realizar el ejercicio.

Kloth.net:

<http://www.kloth.net/services/dig.php>

The screenshot shows a web browser window with the URL www.kloth.net/services/dig.php. The page has a blue header with navigation links: Services, Radio, Internet, Software, Support, Aircraft, and Links... The main content area is titled "DIG: look up DNS domain IP address information". Below the title, there is a form with the following fields and options:

- Domain:** A text input field with a placeholder "... the name of the machine to look up."
- Server:** A dropdown menu currently set to "localhost" with a placeholder "... the DNS nameserver you want to handle your query (just start with this site's default server if you don't know better)".
- Query:** A dropdown menu currently set to "A (IPv4 address)".
- Checkboxes for "Trace" and "Dnssec".
- A "Look it up" button.

Below the form, there is a paragraph of text explaining the service: "DIG is a service to look up information in the DNS (Domain Name System [RFC1034, RFC1035]), just like nslookup. Basically, DNS maps domain names to IP addresses. Although this service can query a specific DNS server, in most cases it may be sufficient and convenient just to use the KLOTH.NET default nameserver 'localhost/127.0.0.1'. The default querytype is A. You may check the 'Trace' option to trace the delegation path down from the root name servers for the name being looked up. dig makes iterative queries to resolve the name being looked up. It will follow referrals from the root servers, showing the answer from each server that was used to resolve the lookup. To resolve an IP V4 address by reverse lookup (get a computer's name if you only have its IP address), try a PTR query instead of ANY. This reverse lookup will only work if the IP address owner has inserted a PTR record in the DNS. If you don't get a PTR information about a specific computer from a DIG query, you may want to try our whois service to find out the owner of this IP address. The DIG utility (domain information proper) is a unix tool, which can be used to gather information from the Domain Name System servers. It is part of the ISC bind nameserver software package. If you want to learn more about dig, here is the Linux dig man page."

At the bottom of the page, there is a "PayPal DONATE" button with the text "If you like this service, please, consider to make a small donation to fund and continue this site. Thank you." and a footer with copyright information: "Copyright © 2003-2020 Ralf D. Kloth, Ludwigsb. DE (QRQ software). < hostmaster at kloth net > (dont send spam) Created 2003-10-20. Last modified 2011-01-30. Your visit 2020-08-26 23:57:56. Page created in 0.1378 sec."

Domain: Nombre de dominio por el cual se desea obtener la información.

Server: Seleccionar a que servidor deseamos realizar la consulta, localhost utilizar servidores que estan definido de forma estática. Es posible especificar el servidor destino o bien por dirección IPv4 o bien como nombre de dominio.

Query: Seleccionar el tipo de registro de queremos averiguar, correspondiente al nombre de dominio expresado en *Domain*.

Look it up: Realiza la consulta DNS con los parámetros especificados en *Domain*, *Server* y *Query*.

Desafío: Realiza una consulta DNS por algún sitio web que normalmente navegue, observe la respuesta a intente identificar los 5 valores que definen un registro: *name*, *type*, *class*, *tll* y *value*.

Se desea obtener la lista de servidores de nombres autoritativos del dominio uy, se realizan las siguientes pruebas:

a) domain = uy
server = a.root-server.net (uno de los 13 root servers)
query = NS

Se observa que se retorna la lista de nombre de servidores autoritativos para el dominio uy, y retorna en *Additional Section* las direcciones IP de cada uno de ellos.

b) domain = uy
server = a.nic.uy (uno de los servidores autoritativos del uy)
query = NS

Se puede observar que retorna en *Additional Section* solamente las direcciones IP de los NS autoritativos del uy, a.nic.uy, b.nic.uy y d.nic.uy.

c) domain = ns1.anteldata.com.uy
server = a.nic.uy
query = A

Se puede observar que retorna el registro A asociado a los nombres de los servidores de DNS autoritativos del uy. Repita la consulta varias veces, confirme que el valor de TTL se mantiene inalterado.

d) domain = ns1.anteldata.com.uy
server = localhost
query = A

Se puede observar que retorna el registro A asociado a los nombres de los servidores de DNS autoritativos del uy. Repita la consulta varias veces, confirme que el valor de TTL difiere entre las consultas.

Pregunta1: ¿Por qué es importante obtener las direcciones IPs de los NS autoritativos de un dominio?

Pregunta2: Investigue el por qué ocurren las diferencias en los valores de TTL de las respuestas obtenidas en c) y d).