EDA387: Computer Networks - Lab 3
Domain Name System (DNS) Assignment

Group 5: Haitham Babbili and Olalekan Peter Adare

23rd October 2020

1. Translation between computer's host name and its IPv4 address

By using dig -x ip address of your computer, My computer's IPv4 address is: 192.168.10.237

Output of the command is shown below:
;; ANSWER SECTION: 237.10.168.192.in-addr.arpa. 0 IN PTR LEKSIDE-PC.lan.
Therefore, its host name is **L**EKSIDE-PC
By using dig -x "ip address " of my computer will translate its IP address to its host name.

In reverse, when we ran dig LEKSIDE-PC, it gave the translated IP address as well.
;; ANSWER SECTION: LEKSIDE-PC. 0 IN A 192.168.10.237

A: What are the sections of the output you get? Describe with your own words and NOT copy of the outcome.

peter@LEKSIDE-PC: $ *dig − x*192.168.10.131

; ¡¡¿¿ DiG 9.16.1-Ubuntu ¡¡¿¿ -x 192.168.10.131 ;; global options: +cmd ;; Got answer: ;; -¿¿HEADER¡¡- opcode: QUERY, status: NOERROR, id: 64975 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;131.10.168.192.in-addr.arpa. IN PTR

;; ANSWER SECTION: 131.10.168.192.in-addr.arpa. 0 IN PTR Haithams-MBP.lan.

;; Query time: 2 msec ;; SERVER: 192.168.10.153(192.168.10.1) ;; WHEN: Fri Oct 23 23:35:07 EEST 2020 ;; MSG SIZE rcvd: 81

My colleague's IP address 192.168.10.131. The host name is Haithams-MBP

- global options: +cmd It shows the version and the global options of the dig command. Also, the number of answer, and if there is error in request, id of the request, number of query needed in this order, and the authority.
- OPT PSEUDOSECTION: It is related to Extended mechanisms for DNS,where we can see the version number, flags, and the udp port number.
- QUESTION SECTION: This section shows information about what is being requested for from the DNS server, with the IP address reverse DNS lookup information, 131.10.168.192.in-addr.arpa. . It also shows which DNS record is record we are accessing. For example, this can be **A**, for IPv4 addresses, or **NS** for the authoritative server,or **CNAME** for canonical name, or **PTR** which is a pointer to a canonical name.
- ANSWER SECTION: This section shows the response to our request, with the reverse loop-up information of the queried IP address. It also shows the DNS record that is offering the answer, the time-to-live value, the class (IN), and the resolved host name
- The last section shows the Query time in milliseconds, the DNS server responding to the request, the time stamp detail, and the message size, in bytes

RA: This means Recursion Available. It is a response from the DNS server to the **rd**, Recursion Desired request, from the DNS client. Recursion is a solution that makes the DNS server to save the entries that has been queried into its cache to speed up the response time to clients that are requesting for the same information later on within the network.

Recursion Desired is a request from the client to the server when making a DNS request. It is a request to be able to use the server's cache subsequently. Recursion available is the response from the server to the client if the option is available for it, or not

What is the IP address of your neighbor's computer?
My colleague's IP address 192.168.10.131

What is the IP address of the server that you get answer from?
SERVER: 192.168.10.153(192.168.10.1)
The IP address of the server responding is 192.168.10.1.

B: What do the mappings in the file tell you?

It is the default DNS record that the client will query first in the local DNS flow.
This file shows that the OS supports IPv4 and IPv6, and shows the mapping between to the hostname and the local ip address.

It shows the link-local IP addresses that will be used by the OS in case there is no DHCP or a manual assignment of ip addresses

C: Identify the field in the header that is indicating error, which one is it?

;;-¿¿HEADER¡¡- opcode: QUERY, status: NXDOMAIN, id: 8347
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

The **NXDOMAIN** is a DNS message type received by the DNS client when a request to resolve a domain is sent to the DNS, and it cannot be resolved to an IP address. This is the major indicator that the DNS resolution failed, or the record was not found.

An NXDOMAIN error message means that the domain does not exist.

Is there any answer section?Why?

No, there was no answer section.
This is because the domain request could not be found by the DNS server. In other words, the DNS server did not get an answer which means that probably the domain does not exist.

2. Local cache, cache-only DNS Servers

How can you find out which DNS server your computer are configured to use?

The last section that contains the statistics data includes the server IP address and the popular DNS port number 53. This is the DNS server that the PC is using. We can also verify by checking the network interface card details.

Using dig look up a well-known Chalmers computer. Give the name of the computer and its IP address.

remote11.chalmers.se. 14400 IN A 129.16.29.50
What is the IP address of the server that you get answer from?
192.168.10.153(192.168.10.1)
Therefore IP address of the server we got this information from is 191.168.10.1, using the A record.

C: Is the answer authoritative?why or why not and what does that mean?

No , this is not authoritative.
By default, since the dig command, without any specified type information, will use the A record to fulfil the request, if it is IPv4, and AAAA record if it is IPv6. Since, dig command did not specify the use of an authoritative server, then the A record will be used for this request.

Running dig ns remote11.chalmers.se will return with the Authoritative section (NS records) with all the authoritative server details.

3. Using Authoritative DNS Servers

A: How can you verify that the answer is authoritative?

This can be verified using the command $ dig remote11.chalmers.se ns .
This will return with one authoritative section and the detail of one of the authoritative server.
If we run $ dig remote11.chalmers.se @ns1.chalmers.se, then it will show us all the authoritative servers of chalmers, and additional information. From the output, there are 4 authoritative servers in answers section including, ns1.chalmers.se. This is because they are labelled as NS resource records.

B: What is the response of the DNS server? Explain why?

The response is: WARNING: recursion requested but not available.
The client requests RD but the server can accept or reject this request. The DNS server, ns1.chalmers.se, is an authoritative server. We tried for google site (www.google.com) and there was no answer section. This probably means that it cannot find googles detail in all the records accessible to it. It used A records by default and its server could not connect to external networks.
Furthermore, the server did not accept the recursion request. Hence, the warning message: WARNING: recursion requested but not available

C: Provide the command you used

dig kth.se NS
What are the authoritative DNS servers of the domain kth.se?
Make sure that the answer RR is of the expected type!

- (kth.se 1566 IN NS nic2.lth.se)
- (kth.se. 1566 IN NS ns2.chalmers.se)
- (kth.se. 1566 IN NS b.ns.kth.se)
- (kth.se. 1566 IN NS a.ns.kth.se.)

The resource record is the displays the NS record.
In both cases the server you ask is authoritative, are there differences? Explain.
The dig operation using @ns2.chalmers.se, there was no error and we got the answer section and an authoritative section displaying NS records.
Query performed using @sunic.sunet.se was refused. This is because sunic.sunet.se is not an authoritative server for kth.se. Although, it is an authoritative server for chalmers.

4. Survival time for cached information

A: For DNS, what is the TTL value used for?

TTL: Time-To-Live
The set TTL value is set for the DNS record that defines how long a resolver should cache the DNS query before the query expires.

What does it mean?
TTL is Time-To-Live. It is a count down set on a cached query. After, this time expires, the record is updated.

Why is it needed?
It is needed to typically reduce the response load on the authoritative name servers. This will speed up the DNS queries for clients. The main goal of DNS caching is to speed up internet load times, and thereby decreasing the load on the DNS servers.

B: Repeat the command several times and notice the TTL value. Is there any difference? If so, try to give an explanation of why.

$ dig kth.se @ns2.chalmers.se
There was a difference. The TTL value seems to remain the same; unchanging. These records are on the authoritative servers and they have longer TTL time in the cache. This is a practice to positive for a quick turnaround time on DNS lookups, thus speeding up your internet browsing experience overall. It is much faster to check a cached version against your local resolver than it is to perform a DNS record lookup.
Generally, there is a need to create a perfect balance between quick update and efficient resource usage.