LAB Assignment Part 3

Domain Name System (DNS) Assignment

Introduction

The operation to translate a host name to its IP address is fundamental to most Internet services and applications. Therefore, it's valuable to know how the DNS system works and how to explicitly check how a translation is done.

There are a number of programs, including ***dig***, ***host***, and ***nslookup***, which provide line commands to help the user contact a name server and ask for the information. In this lab, you should use ***dig*** (***d***omain ***i***nformation ***g***roper) in order to study the services of DNS by executing commands via a terminal.

Report & Hand-In

All the following assignments shall be carried out. Answers, outcomes and comments shall be written down in a concise manner and handed in as an assignment on the Canvas course page. There is no strict formatting rules, but try to avoid lengthy screen dumps and pages of unprocessed command output. Focus on the relevant parts of the command results and the analysis, and that the answer shows understanding of the question (where so is needed). Make sure that you answer all questions in the assignments and use the correct numbering of the questions for your answers.

Assignments

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

Using dig, how can you find out your computer's name according to the DNS system? If your home router has it's own DNS system going (e.g. using .local TLD) that answer is accepted, if not then you might consider viewing your home router as your computer and provide the name given by the ISP.

Provide your computer's IPv4 address, its hostname and the dig command to translate an IP to a hostname.

192.168.1.83, 192.168.1.1, dig 192.168.1.1 ……

Consider comparing the answer to the host command of *nix or what is shown in Windows by ipconfig /all

a. Now use ***dig*** to look up the IP address corresponding to the host name of your lab partner's computer (your neighbor will do the similar lookup about your computer). Examine the output to make sure the answer is correct.

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

……

……

……

Inspect the different fields of the header, what does the flag "**ra**" indicate? .....

……

Verify that you and your neighbor have gotten the right answer each.

What is the IP address of your neighbor's computer?
……...

What is the IP address of the server that you get answer from? ……

b. Examine the content of the hosts file of your system. In *nix systems it would most probably be the file **/etc/hosts** using any text editor or just view it by issuing the command: **cat /etc/hosts**. This file exists partly due to historical reasons, but also to help during bootstrapping.

What do the mappings in the file tell you? …….

……

……

c. Use ***dig*** to look up a host name that does not exist in the DNS system, choose anything you want but an example would be misspelling chalmers web server (wwww.chalmers.se)

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

Is there any answer section? …….. Why? .....

……

2. Local cache, cache-only DNS Servers

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

……

b. 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? ..192.168.1.1#53(192.168.1.1)……

c. Is the answer authoritative? …….Why or why not and what does that mean?

……

……

……

3. Using Authoritative DNS Servers

Looking at the output of previous lookups you will find that the official (authoritative) name servers for Chalmers domain are listed in the "AUTHORITY SECTION" and they are four: {**ns1**, **ns2**, **ns3**}**.chalmers.se** and **sunic.sunet.se**. These are DNS servers which give authoritative answers for Chalmers, but on the other hand they normally do not provide recursion.

By default, you will be using your local name server for translations as you have learned in previous tasks. That is usually acceptable, but there are cases where you want to verify that a specific name server has delivered correct information. In this case, you can tell ***dig*** to use an authoritative name server.

a. Run ***dig*** to look up the IP address for any Chalmers computer of your choice by querying one of the official (authoritative) name servers of the Chalmers domain to see that you get authoritative answer.

How can you verify that the answer is authoritative? ……

……

b. Try now to ***dig*** a name of well-known server abroad (not belonging to Chalmers) of your choice using **ns1.chalmers.se** where we need to have recursion, and note the results to verify whether recursion will be available or not.

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

……

……

……

c. Now in order to find the authoritative DNS servers at domain **kth.se** you may perform a recursive lookup for any of the domain computers (e.g. www.kth.se). However, you can use ***dig*** to ask explicitly for the Resource Records of type **NS**.

Provide the command you used ……..……

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

……..……..…….

d. You will now query one of these **kth.se** NS servers **ns2.chalmers.se** (which is also NS of Chalmers). Use ***dig*** to get information about a KTH computer and compare the results with those when using one of the official name servers at Chalmers **sunic.sunet.se** to get information about the same KTH computer.

In both cases the server you ask is authoritative, are there differences? Explain.

……..…….

……..…….

……..…….

4. Survival time for cached information

a. Look up again the translation for the web server **www.kth.se** using the cache-only server and repeat few times by doing successive lookups to see that the TTL value is counted down and after few minutes it becomes zero. Then you will get a new time-to-live value since your local server has to ask the KTH name server for a new translation.

For DNS, what is the TTL value used for? What does it mean? Why is it needed?

……..…….

b. Repeat the same command but direct the DNS question to an authoritative server of KTH.

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

……..…….