**LAB 23**

**DNS**

# DNS resolving in Windows

1. Make sure you don't run a VPN on your laptop. (No Howest, but no NordVPN or any other.)
2. Open the Windows command prompt on your laptop or on your Windows VM.

As you know, you need a DNS server to surf. What command can you use at the command prompt to retrieve the IPv4 address of the DNS servers used by your laptop? (command + option)

ipconfig /all

Paste below a screenshot of just those lines of the output of your command showing those addresses for your active NIC that you connect to the Internet. For some, this is wired at home, others via Wi-Fi and in your VM it is your virtual network adapter.

In addition to the IP addresses (IPv4 and possibly IPv6) that your NIC is assigned, you will also see the IP address(es) of the DNS server(s). Paste a screenshot of this output here.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

In what network is/are that/those DNS server(s) located (at your home network, ISP, etc.)?

It is the IP of the DNS-service of the home router and 2 optional DNS-servers

1. Now again retrieve the IP addresses of the DNS servers used by your laptop (or VM), but this time using the GUI.

Paste below a screenshot of the window in which you found this info.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Hint: You can quickly access all your network connections by typing ncpa.cpl (Network Control Panel Applet) in your command prompt window.

How did your NIC know this IP address of the DNS server?

With the DHCP-service on the home router

1. Your laptop has a local DNS cache in which name-to-IP address translations are temporarily stored. In this task you will learn how to work with this cache.

Execute the following commands on your host (or VM) using a legacy Windows command:

* With which **ipconfig** command (with additional option) can you clear the content of the local DNS cache? Do it!

Ipconfig /flushdns

* With which **ipconfig** command (with additional option) can you display the content of the local DNS cache? Do it!

Ipconfig /displaydns

Although you cleared the DNS cache, there might already be new entries in the cache (depends on whether you have other network applications open).

* You can also view the DNS cache with a PowerShell cmdlet. Which one? Try that one as well.

Get-DnsClientCache

* Surf to [www.howest.be](http://www.howest.be) . Afterwards, again show the content of your local DNS cache and paste below a screenshot of that part of the local DNS cache showing information about Howest’s website.

Hint: you can scroll through ipconfig’s output for displaying the DNS cache (or pipe it to findstr or Select-String to search for Howest record), but more convenient is to use the PowerShell cmdlet of previous question with a parameter.



* In the TTL line you see how long the name-to-address translation will stay in your local DNS cache? Write down this value below (number + unit)

3554 seconds

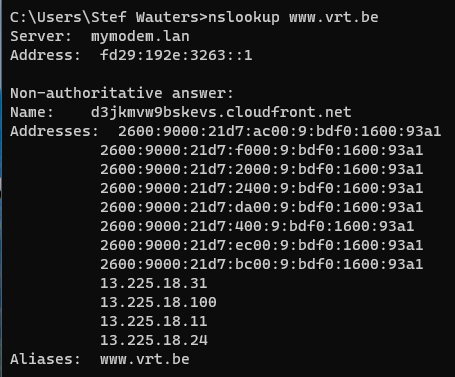
* Re-show the content of the local DNS cache showing information about the Howest web server.

What line has been changed to the previous screenshot? Explain why!

The ‘TTL’ line. This value is lower because this counts down for how long this will stay in the DNS cache.

1. Name-to-IP address translations are done automatically by the OS but can also be performed explicitly using the Windows ***nslookup*** command. This command can be used in both interactive and non-interactive mode.

You use the ***nslookup*** command **in non-interactive mode** by using an argument (e.g. a name or an IP address) immediately after the command. Test this non-interactive mode to locate the IP addresses of the VRT web server ([www.vrt.be](http://www.vrt.be)). Paste below a screenshot of your command and its output.



Did you use a forward or a reverse lookup query when you did this?

Forward lookup

The output consists of 2 parts:

* In the first 2 lines of the output of this command, you’ll see the name and IP address of the DNS server which did the translation.

This is by default the DNS server that is configured in your network configuration and which you’ve identified for your system via CLI and GUI in the first part of this lab.

* In the next line(s), the IP addresses corresponding to the requested name will be shown. Note that both IPv4 and IPv6 addresses are displayed (and possible other information).

1. Using nslookup, you can also use another DNS server than the default DNS server of your system, for one specific query only. You have to specify this as an additional argument in your nslookup command.

Test this by finding out the IP addresses of the www.google.com once using your default DNS server and once using ns1.google.com as DNS server (this is one of Google’s DNS servers).

Paste below a screenshot of your commands and its outputs.

Afbeelding met tekst

Automatisch gegenereerde beschrijvingAfbeelding met tekst

Automatisch gegenereerde beschrijving

Compare the output of both. There is one striking difference. Which one? Explain this!

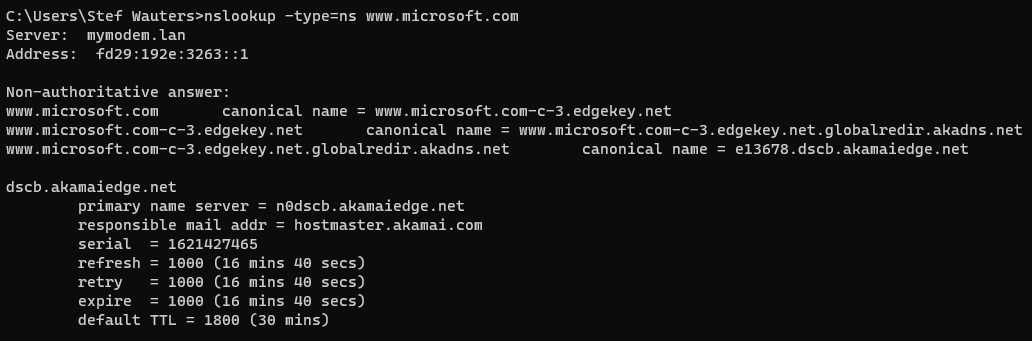
The second output doesn’t show the non-authoritative answer line because the lookup was done by their own DNS-server.

1. Using the nslookup command, request all DNS servers responsible for DNS from the google.com domain.

Hint: use the type-option for this.

You’ll notice that ns1.google.com is indeed one of the authoritative name servers for Google. Try the same with microsoft.com (we don’t want to always favor Google 😉)

Paste below a screenshot of your command and its output.



1. Also use the non-interactive mode of the nslookup command to find out the name of the computer with the IP address 8.8.8.8 and enter it below:

Nslookup 8.8.8.8

**Server name with IP address 8.8.8.8 =** dns.google

Notice the the toplevel domain of that host. It isn’t .com or .net. What is it?

.google is a gTLD or generic top level domain

Did you use a forward or a reverse lookup query for this?

Reverse lookup

1. You use the **nslookup** command **in interactive mode** by pressing the *Enter* button immediately after the *nslookup* command. You will then end up in the special nslookup prompt where you can enter special commands or just DNS names or IP addresses.

Also test this method for performing a forward and a reverse lookup for the website of some hostnames or IP addresses.

Then exit the interactive nslookup mode (e.g. exit command) and paste below a screenshot of the entire interactive nslookup session.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1. Now, to make life convenient (and/or more fun), suppose you want to make your Windows 10 VM (or your Linux VM) accessible using the name MyPreciousVM. You can do that without having to configure something at a DNS server. You can do that by changing the ‘hosts’ file on your laptop. (You did this for some other course module already at the start of the semester.)

If you have set this correctly, you should be able to ping from your laptop to the name MyPreciousVM. Test this and paste below a screenshot of your command and the output.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

# DNS resolving in Linux

1. Start your Linux-VM and sign in (with the *mickey* and password *mouse* account).

The IP address of the DNS server used by your Linux-VM NIC is located in the file ***/etc/resolv.conf***

A small Linux CLI recap: what command can you use to retrieve that IP address? Do this and find out the IP address of the DNS server for your Linux VM

Cat /etc/resolv.conf

And another Linux CLI recap: what command that restricts the output of your previous command to only that line that contains the requested address.

Grep nameserver /etc/resolv.conf

1. In your Linux-VM you could also use **nslookup**, but it is not installed by default with a minimal Debian installation. You can easily install it, but we will first use another tool here that is equally useful and is often available at your CLI by default: **host**.

Use this tool to resolve: google.be . What is the command output?

Afbeelding met tekst

Automatisch gegenereerde beschrijving

1. Just as with the nslookup command, you can give a second argument to the host command, to specify a specific DNS server for your query. To permanently change the DNS server that is used by your OS, you need to change the nameserver in resolv.conf. Let’s do that.

Place the line with the DNS server in /etc/resolv.conf in comments and add a similar line in order for your Linux to use DNS server 8.8.8.8 from now on.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Resolve now google.be again with the **host** tool. Are IPv4/IPv6 addresses the same now as in the previous question?

No, the addresses are different.

(You can now set /etc/resolv.conf to use the original DNS server again if you wish to do so.)

1. Now, install the **dnsutils** package (using ‘apt install’) . You’ll notice that now you also have ‘nslookup’ on your Linux. But even more powerful, you now also have the ‘**dig**’ tool. We won’t delve too deep into this, but try following command:

**dig +trace www.google.com**

You’ll see the different recursive steps to walk through the different DNS zones (root 🡪 .com 🡪 google.com 🡪 www.google.com) and you’ll e.g. see indeed ns1.google.com (and others) which is the authoritative DNS server for www.google.com

# Analyze DNS protocol messages

1. Open the capture file called “Lab 21 - HTTP capture.pcapng”, which we’ve used before.
2. Make sure only DNS packets are displayed.

You will notice that 2 types of DNS messages are shown: DNS queries and the corresponding DNS responses.

1. Check frame number 49 and replace the question marks with appropriate protocol names in the table below. Replace the question marks under the table by the size of the fields (in bytes).

Hint: if you add all the sizes together, you have to have the frame size shown in the first line of the Details window!

|  |  |  |  |
| --- | --- | --- | --- |
| **Ethernet** HEADER | **IP** HEADER | **UDP** HEADER | **DNS** MESSAGE |
| **14** bytes | **20** bytes | **8** bytes | **31** bytes |

1. In frame 16, we have a DNS request. You can see this by looking in the Info column, but you can also see it in black and white in the Details window.

What hostname is asked for the corresponding IP address?

www.google.be

Are you asking for an IPv4 or an IPv6 address here? You can also answer this question by looking in the Info column. It shows what kind of DNS record is requested (see also lecture slides).

A-record (IPv4)

1. At the bottom of the DNS protocol Details window you will see the number on which you will find the response to this request. By double clicking on that, you automatically go to that number. Do it!

So which IP address corresponds to the requested hostname? You can also answer this question by looking in the Info column or in the Details window...

74.125.136.94

1. Return to frame number 16. In the Details window you can see that the difference between a DNS query and a DNS response is indicated by the response flag: if it’s at 0, it’s a request, if it’s at 1, it’s a response.

Use this info to adjust your filter expression so that you can only see the DNS responses and note this filter expression below.

dns.flags.response eq 1

How many such DNS responses are there?

39

1. Show only the frames belonging to the same UDP stream as package number 16.

How many frames are there in this UDP stream?

2

Is such a stream initialized and finalized? Why (not)?

No, this doesn’t happen with UDP