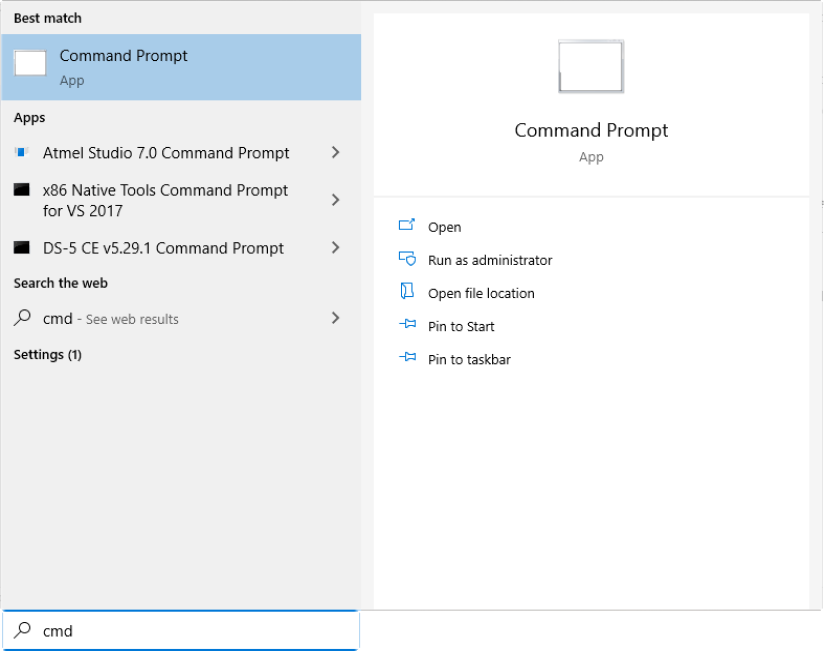
# ET4162 LAB 3 (Part 1): Command Line Networking tools and commands

In this lab we introduce some command line utilities that allow us to explore the TCP/IP configuration information on a PC running Windows. Similar tools are also found in Unix/Linux/MacOS computers. You will be asked to run several commands from the Windows command line, to capture the outputs and to extract some information about your computer and its network set-up. Fill in the appropriate boxes in this file and submit the file with answers filled in on Sulis.

## Getting started (Windows)

Step 1: Start a command prompt as an administrator



1. Use the Searchbox (above) or Right click the Windows icon and choose Run from the menu.

2. Type cmd in the prompt and press enter.

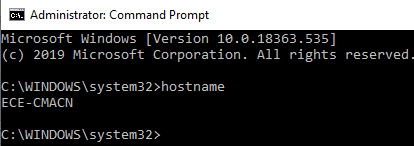
## Getting started (MAC)

This is a YouTube video showing how to open a terminal window on a MAC: <https://www.youtube.com/watch?v=RyabYbpsEBY>

## Lab Exercises (should also work for MAC and Linux computers)

**1. The hostname command**

This command simply displays the computer’s host name. Enter hostname at the command prompt.



Use the information you have found to fill in the following table:

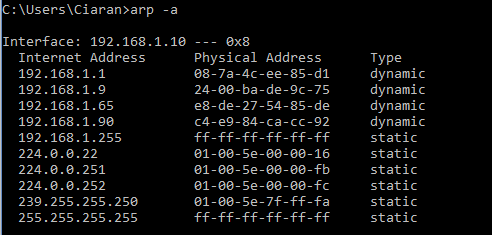
|  |  |
| --- | --- |
| Observed hostname | Olan-HP-Laptop |

**2. The arp command**

The Address Resolution Protocol (ARP) cache is a simple mapping of IP addresses to MAC addresses. When the computer’s TCP/IP stack uses ARP to determine the MAC address for an IP address it stores the mapping in the ARP cache to speed up future ARP lookup.

If you enter *arp* on its own you just get a list of the possible arp parameters. To see the complete ARP cache, enter arp -a as follows:

> arp -a



Note that the Physical Address here is the MAC address.

What is the name of the protocol used to assign IP addresses to hosts in a network?

DNS

**3. The ipconfig Command (Windows) or ifconfig (Linux/Unix/MacOSX)**

This command displays information about a computer’s TCP/IP configuration. In this exercise, first enter the ipconfig command on its own, without any parameters:

> ipconfig

(Use ifconfig in MAC OS).

Use the information from the command to obtain the following information:

What is the IP address of the computer or its NIC adapter?

What is the subnet mask being used?

What is the Default Gateway Address here?

Record the information below:

|  |  |
| --- | --- |
| IP address (IPv4) | 10.54.128.112 |
| Subnet mask | 255.255.244.0 |
| Default Gateway Address | 10.54.128.1 |

Enter the command

**>ipconfig /all**

(Mac: ifconfig –a, or possibly ip –a)

From the output of this command, find the IP address of the DNS Server used.

Find the time and date when the Lease was obtained and the time and date when the Lease Expires.

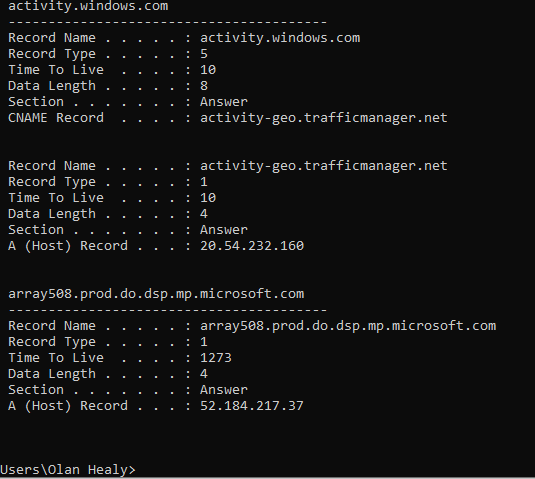
Record the information below:

|  |  |
| --- | --- |
| DNS Server IP address | 1.1.1.1  1.0.0.1 |
| Lease Obtained | Monday 14th of February 2022- 11:04:03 |
| Lease Expires | Thursday 17th of February 2022-15:06:45 |

Next enter the command

**ipconfig /displaydns**

Record, using a screen capture, the last few entries you see.

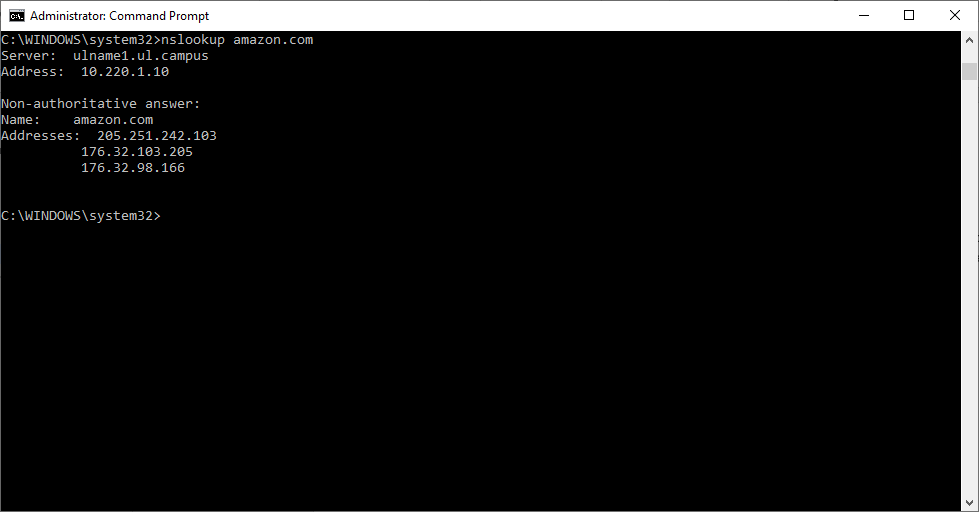


What do you think is meant by the entry ‘Time To Live’ here? Thats it’s limiting the data to the computer by l1273 packets

**4. The nslookup command**

This command gives the IP address for a given web address. *(Note that if you enter nslookup without parameters, this command puts the command window in a subcommand mode and you will need to enter exit to get back to the normal command line.)*

Enter nslookup followed by a web address (eg amazon.com)

****

Try this for ebay.com, rte.ie, youtube.com, google.com, ul.ie

|  |  |
| --- | --- |
| Name | Addresses |
| Ebay.com |  |
| Rte.ie |  |
| Youtube.com |  |
| Ul.com |  |

# Part 2

**Procedure (based on Kurose and Ross http lab)**

1. Start up your web browser.
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).
3. Wait a few moments and then begin Wireshark packet capture.
4. Enter the following in your browser  
   <http://www.theendofinternet.com/>   
   Your browser should display some text and a small gif.
5. Stop Wireshark packet capture.

If you prefer, you may use the simple HTML file used in Labs 1 and 2. <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

Click on the menu bar icon to halt capture of data. This is just to reduce the amount of data we will be looking at.

## TCP protocol frames

In the **packet list** pane, click on the GET frame and use the information from the packet list pane to fill in the answers in the following table.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Frame Number | Time | Source | Destination | Protocol | Length (Number of bytes) |
| 114 | Feb 15, 2022 15:35:32 | 90:b1:1c:a7:77:cd | 00:00:5e:00:01:71 | TCP (6) | 613 |

Move to the **packet details** pane. This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

Next Click on the Ethernet entry and expand it. Use the information here and in the packet bytes pane to fill in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| No of bytes in Ethernet header and trailer | Source MAC address | Destination MAC address | MAC address of your computer (as seen from ipconfig/all) |
| 14 bytes | 90:b1:1c:a7:77:cd | 00:00:5e:00:01:71 | B4:B6:76:33:6B:C9 |

Note that the bytes of the Ethernet header and trailer are highlighted in the packet bytes pane.

Next click on the Internet Protocol Row and expand it. Fill in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| No of bytes in IP header | Source IP Address | Destination IP Address | IP address of your computer |
| 20 bytes | 10.100.106.182 | 94.231.103.72 | 10.54.128.112 |

Finally Click on the TCP entry in the packet details pane and expand it. Fill in the details below. You can calculate the ‘No of bytes of data in the frame, as the difference between the total number of bytes in the frame and the total number of bytes in all the headers.

|  |  |  |  |
| --- | --- | --- | --- |
| Number of bytes in TCP header | TCP Source Port | TCP Destination Port | TCP Length or Payload Number of bytes |
| 20 bytes | 58269 | 80 | 559 |

## UDP Protocol Frames

Step 1

Replace the filter saying ‘http’ with ‘dns’

Click on a DNS packet in the captured frame.

Click on the Frame and use the information from the packet list pane to fill in the answers in the following table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Frame Number | Time | Source | Destination | Protocol |
| 1543 | Feb 15 2022 15:36:47 | 90:b1:1c:a7:77:cd | 00:00:5e:00:01:71 | UDP |

Move to the **packet details** pane. This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed. For the UDP frame, you should see 4 rows.

Click on the Frame Number in the pane and use the information you find to fill in the following table:

|  |  |
| --- | --- |
| Frame Number | Number of Bytes |
| 1543 | 8 bytes |

Use the Packet Details pane to see which Transport Layer Protocol is in use here?

|  |  |
| --- | --- |
| DNS Transport Layer Protocol (TCP or UDP?) | UDP |

Note that when you click on the Frame in the packet details pane, all the bytes of the packet bytes pane are highlighted.

Next Click on the Ethernet entry and expand it. Use the information here and in the packet bytes pane to fill in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| No of bytes in Ethernet header and trailer | Source MAC address | Destination MAC address | MAC address of your computer |
| 14 bytes | 90;b1;1c;a7;77;cd | 00;00;5e;00;01;71 | B4:B6:76:33:6B:C9 |

Note that the bytes of the Ethernet header and trailer are highlighted in the packet bytes pane.

Next click on the Internet Protocol Row and expand it. Fill in the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| No of bytes in IP header | Source IP Address | Destination IP Address | IP address of your computer |
| 20 bytes | 10.100.106.182 | 10.220.1.10 | 10.54.128.112 |

Finally Click on the UDP entry in the packet details pane and expand it. Fill in the details below.

|  |  |  |
| --- | --- | --- |
| Number of bytes in the UDP Segment | Number of bytes in UDP Payload | No of bytes in the UDP Header (No in Segment – Payload) |
| 8 bytes | 29 bytes | 29 bytes |