Lab 3 - Domain Name System (DNS)

Learning objectives

- Use nslookup to perform DNS queries.
- Use Wireshark to capture, analyse DNS query and response messages.

Introduction

Domain Name System (DNS) is a distributed network of hierarchical DNS servers that translates the domain names such as www.leedsbeckett.ac.uk to an IP address. Every time you open the web browser on your computer and enter the domain name of a website, you are using the Domain Name System (DNS). In this lab, you will use the 'nslookup' program to perform DNS queries and obtain DNS information. You will also use Wireshark to capture, examine DNS query and response messages.

Download Windows **CCOM** template image on Desktop PC.

Tasks

Note – **Use the bottom PC to complete task1.**

1. Using nslookup

- Logon on bottom PC.
- Open a command prompt on your PC by typing **cmd** in the search box (bottom left-hand-corner).
- At command prompt, type the **nslookup** and press Enter.
- What is the default DNS server used by your PC?

```
Microsoft Windows [Version 10.0.26100.3037]
(c) Microsoft Corporation. All rights reserved.

C:\Users\imper>nslookup
Default Server:  bthub.home
Address:  fe80::f286:20ff:[redacted]

>
```

You noticed the command prompt changed to a greater than **>** symbol. This is the nslookup prompt. You are now in nslookup command mode and can enter commands without typing 'nslookup.'

- Type **?** and press Enter.

You should see a list of **nslookup** commands/options that you can use.

- Type **www.leedsbeckett.ac.uk** and press Enter.

When using nslookup to query a domain name such as above, it provides two main pieces of information:

  - The name and IP address of the DNS server that provided the answer.
  - The answer itself, which is the domain name (you entered) and IP address of domain name (e.g., www.leedsbeckett.ac.uk).

Although the response came from the local DNS server at Leedsbeckett University, it is quite likely that the local DNS server contacted several other DNS servers to get the answer.

- At nslookup prompt, type **exit** to return to the regular PC command prompt.

By default, nslookup uses type '**A**' query and sends the query to the default DNS server. We can use the **'-type'** option to specify how the query should be interpreted.

For example, we can use type '**NS**' to find the name of authoritative DNS for www.leedsbeckett.ac.uk.

- At the prompt, type **nslookup -type=NS www.leedsbeckett.ac.uk** and press return.

Now, it is your turn to experiment using **nslookup**.

Use **nslookup** to find the following:

- IP address of amazon.co.uk Web server.
- Authoritative DNS server(s) for amazon.co.uk.
- Authoritative DNS server(s) for google.co.uk.

- Authoritative DNS server(s) for ox.au.uk.

```
C:\Users\imper>nslookup -type=soa ox.au.uk
Server:  bthub.home
Address:  fe80::f286:20ff:fe6e:275b

Non-authoritative answer:
ox.au.uk
        primary name server = ns1.dan.com
        responsible mail addr = dns.jomax.net
        serial  = 2024111500
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)

C:\Users\imper>nslookup ox.au.uk ns1.dan.com
3.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.2.1.2.5.0.0.0.3.0.6.2.ip6.arpa
        primary name server = ns1.dan.com
        responsible mail addr = dns.jomax.net
        serial  = 2024111500
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
Server:  Unknown
Address:  2603:5:2125::43

Name:    ox.au.uk.home
Addresses:  13.248.169.48
          76.223.54.146
```

IPV6

IPV4

- Authoritative DNS server(s) for www.leedsbeckett.ac.uk.
- Leedsbeckett University mail server(s).

```
C:\Users\imper>nslookup -type=soa leedsbeckett.ac.uk
Server:  bthub.home
Address:  fe80::f286:20ff:fe6e:275b

Non-authoritative answer:
leedsbeckett.ac.uk
        primary name server = dns-a.leedsbeckett.ac.uk
        responsible mail addr = hostmaster.leedsbeckett.ac.uk
        serial  = 2015104822
        refresh = 1200 (20 mins)
        retry   = 180 (3 mins)
        expire  = 1209600 (14 days)
        default TTL = 6400 (1 hour 46 mins 40 secs)

C:\Users\imper>nslookup leedsbeckett.ac.uk dns-a.leedsbeckett.ac.uk
Server:  dns-a.leedsbeckett.ac.uk
Address:  160.9.151.150

Name:    leedsbeckett.ac.uk
Addresses:  18.171.30.181
          18.134.81.66
```

-

2. Capturing DNS messages

Note – Use Desktop PC to complete task2.

Make sure Windows **CCOM** template image is downloaded on Desktop PC and ready to complete the following tasks.

- Open a command prompt on your PC by typing **cmd** in the search box (bottom left-hand-corner).
- At command prompt, type **ipconfig/all** and press Enter. Fill in the following information for Ethernet Network Interface Card (NIC) on your PC.

IPv4 address
Physical (MAC) address
Default gateway IP address
Network (subnet) mask
DNS server IP address

(Table1)

```
Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Realtek RTL8
   Physical Address. . . . . . . . . : F8-54-F6-AF-
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2a00:23c8:95
   Temporary IPv6 Address. . . . . . : 2a00:23c8:95
   Link-local IPv6 Address . . . . . : fe80::8ee6:4
   IPv4 Address. . . . . . . . . . . : 192.168.1.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.
   Lease Obtained. . . . . . . . . . : 10 February
   Lease Expires . . . . . . . . . . : 11 February
   Default Gateway . . . . . . . . . : fe80::f286:2
                                       192.168.1.25
   DHCP Server . . . . . . . . . . . : 192.168.1.25
   DHCPv6 IAID . . . . . . . . . . . : 83383542
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-
   DNS Servers . . . . . . . . . . . : fe80::f286:2
                                       192.168.1.25
                                       fe80::f286:2
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       home
```

Displaying DNS cache on your PC.

- At command prompt, type **ipconfig /displaydns** and press Enter.

Clearing DNS cache on your PC.

- At command prompt, type **ipconfig /flushdns** and press Enter.

Make sure the DNS cache on your PC is empty.

```
C:\Users\imper>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\imper>ipconfig /displaydns

Windows IP Configuration
```

- Start Wireshark, click **Options…** menu (at top), select '**Ethernet**' interface and start a new capture.
- Open Chrome browser, in browser Window, enter URL **www.icann.org** and press return.
- Stop the Wireshark capture once your browser displays the page.

If you do not see any packets captured in Wireshark, repeat the above steps again. Alternatively, download '**DNS-trace-file**' from VLE and open it in Wireshark.

- Filter the packets displayed in the Wireshark window by entering '**dns**' (lowercase, no quotes), and press Enter.

Select '**www.icann.org**' DNS query packet in **Packets captured** Window and answer the following:

- Is the DNS query sent over UDP or TCP?

```
User Datagram Protocol, Src Port: 59589, Dst Port: 53
    Source Port: 59589
    Destination Port: 53
```

UDP (USER DATAGRAM PROTOCOL)

- What is the destination IP address of DNS query? Is this same as the IP address of your local DNS server? If so, explain why?

```
▸ Internet Protocol Version 6, Src: fe80::8ee6:412b:d1ae:cd3c, Dst: fe80::f286:20ff:fe6e:275b
```

Yes it is the same

- Is it an 'Iterative' or 'Recursive' DNS query?

```
Domain Name System (query)
    Transaction ID: 0xc1a5
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
```

-

- How many 'queries' are in the DNS query?

Mine came 3

```
fe80::8ee6:412b:d1ae:cd3c   fe80::f286:20ff:fe6e:275b   DNS   93 Standard query 0xc1a5 AAAA www.icann.org
fe80::8ee6:412b:d1ae:cd3c   fe80::f286:20ff:fe6e:275b   DNS   93 Standard query 0xc5b2 A www.icann.org
fe80::8ee6:412b:d1ae:cd3c   fe80::f286:20ff:fe6e:275b   DNS   93 Standard query 0xda61 HTTPS www.icann.org
```

- What is the DNS query **Type**? Explain.

A = Address Record = IPv4
AAAA = IPv6
HTTPS = HTTPS Protocol Binding

- How many 'answers' are in the DNS query? Should there be any 'answers' in the DNS query, if not why? **No answers – queries are requests, answers are responses.**

Select '**www.icann.org**' DNS response packet in **Packets captured** Window and answer the following:

- How many "answers" are provided?
  3 - the same number of queries

- What do each of these answers contain?

  A response for each query type (A,AAAA,HTPS)

```
▾ Queries
  ▸ www.icann.org: type A, class IN
▾ Answers
  ▸ www.icann.org: type CNAME, class IN, cname www.icann.org.cdn.cloudflare.net
  ▸ www.icann.org.cdn.cloudflare.net: type A, class IN, addr 104.18.3.93
  ▸ www.icann.org.cdn.cloudflare.net: type A, class IN, addr 104.18.2.93
  [Request In: 12718]
  [Time: 0.017618000 seconds]
```

- How many 'Authoritative Servers' are there?

*****************NEED TO ASK**********************

```
▾ Domain Name System (response)
    Transaction ID: 0xc1a5
  ▾ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.icann.org: type AAAA, class IN
  ▾ Answers
    ▾ www.icann.org: type CNAME, class IN, cname www.icann.org.cdn.cloudflare.net
        Name: www.icann.org
        Type: CNAME (5) (Canonical NAME for an alias)
        Class: IN (0x0001)
        Time to live: 879 (14 minutes, 39 seconds)
        Data length: 34
        CNAME: www.icann.org.cdn.cloudflare.net
    ▾ www.icann.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6812:25d
        Name: www.icann.org.cdn.cloudflare.net
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 16
        AAAA Address: 2606:4700::6812:25d
    ▾ www.icann.org.cdn.cloudflare.net: type AAAA, class IN, addr 2606:4700::6812:35d
        Name: www.icann.org.cdn.cloudflare.net
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 16
        AAAA Address: 2606:4700::6812:35d
    [Request In: 12717]
    [Time: 0.090377000 seconds]
```

3. Reflection and class discussion

- What is the fundamental purpose of DNS?
  translates domain names into IP addresses

- Do you need to have a DNS server to use the Internet?