Domain Name System

In this exercise, you will be observing different DNS resource records through **nslookup** and inspecting DNS packets to explore their content and relate these to the protocol specifications defined in the DNS RFC.

* 1. Ensure that your PC has connectivity to a DNS server.

To check your DNS server setting, open up the command line terminal on the PC and input the command:

**ipconfig /all**

Look for the DNS server setting under your Ethernet/WLAN adapter connection and copy the IP address here:

|  |
| --- |
|  |

Ping the DNS server IP address and ensure that you can contact it. Attach the screenshot.

|  |
| --- |
| Screenshot |

* 1. On the PC command line, start the nslookup tool by entering the command.

**nslookup**

The prompt should change to “>”

* 1. Determine the administrative zone of the server by querying for Start of Authority (SOA) records:

Enter the following commands:

set type=SOA

delta.dlsu.edu.ph

From the output, identify the domain name administered by this server:

|  |
| --- |
|  |

What other information about a domain can you get from an SOA record?

|  |
| --- |
|  |

* 1. Try to trace the DNS tree structure up to the root server for the branch where your DNS server belongs. Query for the DNS servers of the domains listed below. You may input the domain name directly. No need to set the record type again.

|  |  |
| --- | --- |
| Domain | Primary DNS server name or IP address |
| dlsu.edu.ph |  |
| edu.ph |  |
| ph |  |
| **.** |  |

* 1. Determine the name servers of a domain querying for name server (NS) records: Set ‘NS’ as the record type to be queried using the command

set type=NS

* 1. Query the following domains and fill in the number of name servers serving each of them.

|  |  |
| --- | --- |
| Domain | Number of DNS servers |
| dlsu.edu.ph |  |
| edu.ph |  |
| ph |  |
| **.** |  |

Why would there be a need for multiple name servers for a domain?

|  |
| --- |
|  |

Why would a DNS server need to contain NS type of resource records?

|  |
| --- |
|  |

* 1. Run Wireshark and set it to capture on your Ethernet/WLAN connection. Set the filter to capture only DNS (UDP port 53)
  2. Get DNS host records by setting query type to ‘A’, then query for the host www.dlsu.edu.ph.

What is the response of the server?

|  |
| --- |
|  |

* 1. Go to Wireshark and check captured packets, there should be a query and reply packet for www.dlsu.edu.ph

Look for the DNS query packet of the client then expand the DNS message details. Observe the data within the query

How many questions are included in the message? Attach the screenshot of the captured packet.

|  |
| --- |
|  |

Look for the DNS reply packet of the server then expand the DNS message details. Observe the flag values and data within the query

How many answers are included in the message? Based on the flag value, is the answer considered authoritative? Attach the screenshot of the captured packet.

|  |
| --- |
|  |

What does it mean if the server returns an authoritative answer in the DNS response?

|  |
| --- |
|  |

* 1. Using nslookup, query for ‘www.up.edu.ph’ this time then check Wireshark for the server reply for ‘www.up.edu.ph’.

What is the value of the ‘Authoritative’ flag? Attach the screenshot of the captured packet.

|  |
| --- |
|  |

Why is the authoritative flag different for this response?

|  |
| --- |
|  |

* 1. Stop the packet capture on Wireshark.
  2. Try querying for ‘dlsu.instructure.com’, which is the URL for Animospace. Notice that the result includes a different name. This is an indication that the name is an alias rather than the real name of the server.
  3. Set the nslookup query type to ‘cname’ to query the DNS for canonical names.

Query for ‘dlsu.instructure.com’. What is its canonical name? Attach a screenshot.

|  |
| --- |
|  |

* 1. Query for the canonical name of the result obtained in #13.

What is its canonical name? Attach a screenshot.

|  |
| --- |
|  |

Based on the result, which provider do you think is hosting Animospace?

|  |
| --- |
|  |

* 1. Get mail exchange records by setting query type to ‘MX’, then query for the domain dlsu.edu.ph.

How many mail servers are used by DLSU?

|  |
| --- |
|  |

Based on the results, which provider is hosting the mail services for DLSU?

|  |
| --- |
|  |