

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.

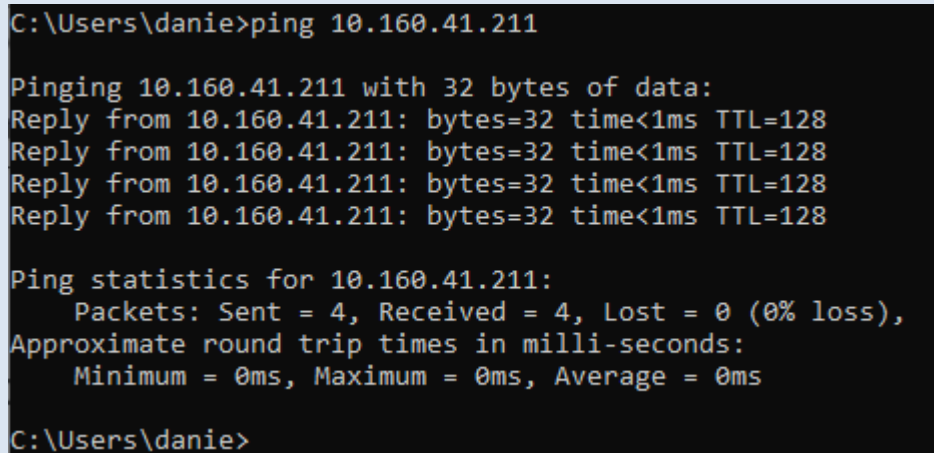
- i. To check your DNS server setting, open up the command line terminal on the PC and input the command:

ipconfig /all

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

10.160.41.211

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



```
C:\Users\danie>ping 10.160.41.211

Pinging 10.160.41.211 with 32 bytes of data:
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128
Reply from 10.160.41.211: bytes=32 time<1ms TTL=128

Ping statistics for 10.160.41.211:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\danie>
```

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

nslookup

The prompt should change to ">"

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

- i. Enter the following commands:

```
set type=SOA
delta.dlsu.edu.ph
```

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

delta.manila.dlsu.edu.ph

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

responsible mail address, serial number, refresh in seconds, retry in seconds, expire in seconds, default TTL in seconds.

4. 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	delta.manila.dlsu.edu.ph
edu.ph	gomez.ph.net
ph	ph-tld-ns.dot.ph
.	a.root-servers.net

5. 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
```

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

Domain	Number of DNS servers
dlsu.edu.ph	3
edu.ph	4
ph	4
.	13

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

There would be a need for multiple name servers for a domain because it helps domains remain available and perform well under all conditions.

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

A DNS server needs to contain NS type of resource records to ensure the proper delegation and management of the domain name system hierarchy.

7. Run Wireshark and set it to capture on your Ethernet/WLAN connection. Set the filter to capture only DNS (UDP port 53)
8. 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?

Answer RRs: 0

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

No.	Time	Source	Destination	Protocol	Length	Info
971	17.861521	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0x7ff7 A mtalk.google.com CNAME mobile-gtalk.l.google.com A 64.233.187.188
972	17.861521	10.128.128.128	10.160.41.211	DNS	105	Standard query response 0x8449 A connectivitycheck.gstatic.com A 142.251.220.195
973	17.861521	10.128.128.128	10.160.41.211	DNS	90	Standard query response 0xd5f1 A www.google.com A 142.251.220.228
974	17.865000	10.128.128.128	10.160.41.211	DNS	102	Standard query response 0x8d0a AAAA www.google.com AAAA 2404:6800:4017:801::2004
975	17.871022	10.128.128.128	10.160.41.211	DNS	133	Standard query response 0x03a6 AAAA mtalk.google.com CNAME mobile-gtalk.l.google.com AAAA 2404:6800:4008:c...
983	17.894878	10.128.128.128	10.160.41.211	DNS	117	Standard query response 0xb46a AAAA connectivitycheck.gstatic.com AAAA 2404:6800:4017:801::2003
1042	18.410833	10.160.41.211	10.128.128.128	DNS	71	Standard query 0x57b7 A dlsu.edu.ph
1043	18.411147	10.160.41.211	10.128.128.128	DNS	71	Standard query 0xac16 HTTPS dlsu.edu.ph
1048	18.415798	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0x57b7 A dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1050	18.420012	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0xac16 HTTPS dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1052	18.421153	10.160.41.211	10.128.128.128	DNS	71	Standard query 0x8ebd A dlsu.edu.ph
1053	18.425917	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0x8ebd A dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1104	19.495238	10.160.41.211	10.128.128.128	DNS	75	Standard query 0x855c A www.dlsu.edu.ph
1105	19.495668	10.160.41.211	10.128.128.128	DNS	75	Standard query 0xc923 HTTPS www.dlsu.edu.ph
1107	19.499865	10.128.128.128	10.160.41.211	DNS	91	Standard query response 0x855c A www.dlsu.edu.ph A 103.231.241.180
1108	19.500993	10.128.128.128	10.160.41.211	DNS	135	Standard query response 0xc923 HTTPS www.dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1180	19.657233	10.160.41.211	10.128.128.128	DNS	76	Standard query 0x4c94 A assets.juicer.io
1181	19.657502	10.160.41.211	10.128.128.128	DNS	76	Standard query 0x4e83 HTTPS assets.juicer.io


```

Frame 1104: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF...
Ethernet II, Src: HonHaiPrecis_8e:6d:c3 (40:49:0f:8e:6d:c3), Dst: CiscoMeraki_c7:e5:db (ac:17:
Internet Protocol Version 4, Src: 10.160.41.211, Dst: 10.128.128.128
User Datagram Protocol, Src Port: 49669, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x855c
  Flags: 0x0100 Standard query
  Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.dlsu.edu.ph: type A, class IN
    [Response in: 1107]
  
```

1 question

- ii. 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.

No.	Time	Source	Destination	Protocol	Length	Info
971	17.861521	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0x7ff7 A mtalk.google.com CNAME mobile-gtalk.l.google.com A 64.233.187.188
972	17.861521	10.128.128.128	10.160.41.211	DNS	105	Standard query response 0x8449 A connectivitycheck.gstatic.com A 142.251.220.195
973	17.861521	10.128.128.128	10.160.41.211	DNS	90	Standard query response 0xd5f1 A www.google.com A 142.251.220.228
974	17.865000	10.128.128.128	10.160.41.211	DNS	102	Standard query response 0x8d0a AAAA www.google.com AAAA 2404:6800:4017:801::2004
975	17.871022	10.128.128.128	10.160.41.211	DNS	133	Standard query response 0x03a6 AAAA mtalk.google.com CNAME mobile-gtalk.l.google.com AAAA 2404:6800:4008:c...
983	17.894878	10.128.128.128	10.160.41.211	DNS	117	Standard query response 0xb46a AAAA connectivitycheck.gstatic.com AAAA 2404:6800:4017:801::2003
1042	18.410833	10.160.41.211	10.128.128.128	DNS	71	Standard query 0x57b7 A dlsu.edu.ph
1043	18.411147	10.160.41.211	10.128.128.128	DNS	71	Standard query 0xac16 HTTPS dlsu.edu.ph
1048	18.415798	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0x57b7 A dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1050	18.420012	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0xac16 HTTPS dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1052	18.421153	10.160.41.211	10.128.128.128	DNS	71	Standard query 0x8ebd A dlsu.edu.ph
1053	18.425917	10.128.128.128	10.160.41.211	DNS	131	Standard query response 0x8ebd A dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1104	19.495238	10.160.41.211	10.128.128.128	DNS	75	Standard query 0x855c A www.dlsu.edu.ph
1105	19.495668	10.160.41.211	10.128.128.128	DNS	75	Standard query 0xc923 HTTPS www.dlsu.edu.ph
1107	19.499865	10.128.128.128	10.160.41.211	DNS	91	Standard query response 0x855c A www.dlsu.edu.ph A 103.231.241.180
1108	19.500993	10.128.128.128	10.160.41.211	DNS	135	Standard query response 0xc923 HTTPS www.dlsu.edu.ph SOA delta.manila.dlsu.edu.ph
1180	19.657233	10.160.41.211	10.128.128.128	DNS	76	Standard query 0x4c94 A assets.juicer.io
1181	19.657502	10.160.41.211	10.128.128.128	DNS	76	Standard query 0x4e83 HTTPS assets.juicer.io


```

Frame 1107: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF...
Ethernet II, Src: CiscoMeraki_c7:e5:db (ac:17:c8:c7:e5:db), Dst: HonHaiPrecis_8e:6d:c3 (40:49:
Internet Protocol Version 4, Src: 10.128.128.128, Dst: 10.160.41.211
User Datagram Protocol, Src Port: 53, Dst Port: 49669
Domain Name System (response)
  Transaction ID: 0x855c
  Flags: 0x8500 Standard query response, No error
  Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.dlsu.edu.ph: type A, class IN
  Answers
    [Request in: 1104]
    [Time: 0.004627000 seconds]
  
```

The answer is not authoritative.

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

it means that the DNS server providing the response has the original records of the domain because it is directly responsible for that domain

10. 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.

NSCOM01 Lab – Domain Name System

No.	Time	Source	Destination	Protocol	Length	Info
7	3.851401	10.160.41.211	10.128.128.128	DNS	79	Standard query 0xbff A clients4.google.com
8	3.851564	10.160.41.211	10.128.128.128	DNS	79	Standard query response 0x48fa HTTPS clients4.google.com
9	3.895185	10.128.128.128	10.160.41.211	DNS	153	Standard query response 0x48fa HTTPS clients4.google.com CNAME clients1.google.com SOA ns1.google.com
10	3.938365	10.128.128.128	10.160.41.211	DNS	119	Standard query response 0xbff A clients4.google.com CNAME clients1.google.com A 142.251.220.142
32	4.028034	10.160.41.211	10.128.128.128	DNS	95	Standard query 0x5f07 A optimizationguide-pa.googleapis.com
33	4.028327	10.160.41.211	10.128.128.128	DNS	95	Standard query response 0xc86e HTTPS optimizationguide-pa.googleapis.com
34	4.044231	10.160.41.211	10.128.128.128	DNS	83	Standard query 0x571e A safebrowsing.google.com
35	4.044534	10.160.41.211	10.128.128.128	DNS	83	Standard query response 0x7e86 HTTPS safebrowsing.google.com
36	4.050448	10.160.41.211	10.128.128.128	DNS	69	Standard query 0x7334 A up.edu.ph
37	4.050695	10.160.41.211	10.128.128.128	DNS	69	Standard query response 0xc606 HTTPS up.edu.ph
38	4.065839	10.128.128.128	10.160.41.211	DNS	152	Standard query response 0xc86e HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
39	4.069429	10.128.128.128	10.160.41.211	DNS	239	Standard query response 0x5f07 A optimizationguide-pa.googleapis.com A 64.233.188.95 A 142.251.221.42 A 14...
43	4.084379	10.128.128.128	10.160.41.211	DNS	166	Standard query response 0x571e A safebrowsing.google.com CNAME sb1.google.com A 64.233.187.93 A 64.233.18...
44	4.089659	10.128.128.128	10.160.41.211	DNS	152	Standard query response 0x7e86 HTTPS safebrowsing.google.com CNAME sb1.google.com SOA ns1.google.com
48	4.111689	10.128.128.128	10.160.41.211	DNS	181	Standard query response 0x7334 A up.edu.ph A 192.0.78.156 A 192.0.78.250
130	4.941877	10.160.41.211	10.128.128.128	DNS	77	Standard query 0x8ae1 A fonts.gstatic.com
131	4.942200	10.160.41.211	10.128.128.128	DNS	77	Standard query response 0x9bac HTTPS fonts.gstatic.com
132	4.947672	10.128.128.128	10.160.41.211	DNS	93	Standard query response 0x8ae1 A fonts.gstatic.com A 142.251.220.163

▶ Frame 36: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF...
 ▶ Ethernet II, Src: HonHaiPrecis_8e:6d:c3 (40:49:0f:8e:6d:c3), Dst: CiscoMeraki_c7:e5:db (ac:17:00:00:00:00:00)
 ▶ Internet Protocol Version 4, Src: 10.160.41.211, Dst: 10.128.128.128
 ▶ User Datagram Protocol, Src Port: 56179, Dst Port: 53
 ▶ Domain Name System (query)
 Transaction ID: 0x7334
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 ▶ up.edu.ph: type A, class IN
 [Response in: 48]

0

Why is the authoritative flag different for this response?

The authoritative flag is same because it uses the same DNS query.

- Stop the packet capture on Wireshark.
- 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.
- 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.

```

> dlsu.instructure.com
Server: UnKnown
Address: 10.128.128.128

Non-authoritative answer:
dlsu.instructure.com canonical name = cluster396.instructure.com
  
```

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

What is its canonical name? Attach a screenshot.

```

Non-authoritative answer:
dlsu.instructure.com canonical name = cluster396.instructure.com
cluster396.instructure.com canonical name = canvas-sin-prod-c396-1782718951.ap-southeast-1.elb.amazonaws.com
  
```

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

Amazon Web Services

- 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?

```
Can't find address for server dlsu.edu.ph. Non-authoritative answer
> set type=mx
> dlsu.edu.ph
Server: UnKnown
Address: 10.128.128.128

dlsu.edu.ph      MX preference = 2, mail exchanger = aspmx.l.google.com
aspmx.l.google.com  internet address = 108.177.97.27
aspmx.l.google.com  AAAA IPv6 address = 2404:6800:4008:c19::1b
\
```

2 mail servers

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

Google