

Maryam khan

SP23-BSE-066

B

LAB ACTIVITY

QUESTION 1

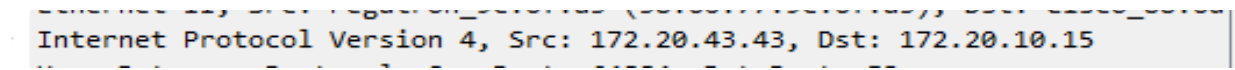
What is the destination port for the DNS query message? What is the source port of DNS response message?

Source Port: 64884

Destination Port: 53

QUESTION 2

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



```

Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : lab3a-03
    Primary Dns Suffix . . . . . : network.dcu
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : network.dcu

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : network.dcu
    Description . . . . . : Intel(R) 82579V Gigabit Network Connection
    Physical Address. . . . . : 38-60-77-9C-6F-A3
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::2ac1:acb2:e91f:1231%3(Preferred)
    IPv4 Address. . . . . : 172.20.43.43(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, March 1, 2025 7:06:22 AM
    Lease Expires . . . . . : Saturday, March 1, 2025 11:06:23 AM
    Default Gateway . . . . . : 172.20.43.2
    DHCP Server . . . . . : 172.20.10.10
    DHCPv6 IAID . . . . . : 54026359
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-3C-C9-B5-38-60-77-9C-6F-A3
    DNS Servers . . . . . : 172.20.10.15
                          1.1.1.1
    NetBIOS over Tcpip. . . . . : Enabled
    Connection-specific DNS Suffix Search List :
                                network.dcu

C:\Windows\system32>
  
```

DNS query message is send to IP: 172.20.10.15

Yes this the IP address of my default local DNS server.

QUESTION 3

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

```

* Domain Name System (query)
  Transaction ID: 0x2308
  ✓ 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
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ✓ Queries
    > arm-ring.msedge.net: type A, class IN
    [Response In: 400]

```

TYPE: A

Answer: 0

QUESTION 4

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

There are 3 answers in DNS response message it contains Name, type, class, time, data

UDP payload (110 bytes)

▼ Domain Name System (response)

Transaction ID: 0x2308

▼ 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

▼ arm-ring.msedge.net: type A, class IN

Name: arm-ring.msedge.net
 [Name Length: 19]
 [Label Count: 3]
 Type: A (1) (Host Address)
 Class: IN (0x0001)

▼ Answers

▼ arm-ring.msedge.net: type CNAME, class IN, cname arm-ring.arm-9999.arm-msedge.net

Name: arm-ring.msedge.net
 Type: CNAME (5) (Canonical NAME for an alias)
 Class: IN (0x0001)
 Time to live: 13 (13 seconds)
 Data length: 31

CNAME: arm-ring.arm-9999.arm-msedge.net

▼ arm-ring.arm-9999.arm-msedge.net: type CNAME, class IN, cname arm-9999.arm-msedge.net

.. ..