**CS3506 Lab 1: Worksheet**

**DNS / IP**

1. Which version of the IP protocol is being used for the DNS packets?

IPv4

2. What is the IP address of the DNS server?

128.238.29.23

3. The DNS server returns two IP addresses for [www.ietf.org](http://www.ietf.org). Why two rather than one? What are the two IP addresses?

Some websites use multiple IP addresses to support redundancy, load balancing, or geographic distribution.

* Redundancy ensures that if one IP is unavailable, the other can still handle requests.
* Load balancing distributes traffic to multiple servers for efficiency and reliability.

4. What field is used to indicate to the receiver that the IP payload contains a UDP packet? What value is that field (in decimal and hexadecimal)?

In the IP header, the "Protocol" field indicates the type of payload.

* For UDP, the value is 17

**UDP**

1. Select one DNS packet. From the packet bytes field, identify and determine the length (in bytes) of each of the four main UDP header fields.

The four main fields of the UDP header are:

1. Source Port (2 bytes)
2. Destination Port (2 bytes)
3. Length (2 bytes)
4. Checksum (2 bytes)

2. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

The Length field specifies the total length of the UDP datagram, including the header (8 bytes) and the DNS payload. You can verify this by checking the length field in the UDP header.

3. Based on information in the UDP header alone, what is the highest possible source port number?

The UDP source port is 16 bits long, so the highest possible port number is 65535.

4. Examine the pair of DNS/UDP packets. Describe the relationship between the port numbers in the two packets.

In a typical DNS query-response exchange:

* The source port of the request (from the client) becomes the destination port of the response (from the server), and vice versa.

This is what happens here:

* The client sends the request using a random high-numbered source port (in this case, 3163).
* The DNS server responds using port 53 as the source port, and the client's source port (3163) becomes the destination port in the response packet.

5. Consider a system using Ethernet/IP/UDP, with a maximum Ethernet Frame *payload* of 500 bytes + the three last digits of your student number. What is the maximum number of bytes of UDP payload supported?

**DHCP**

1. Draw a time sequence diagram illustrating the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicate the source and destination port numbers and the time they were sent.

DHCP Discover

DHCP Offer

DHCP Request

DHCP ACK

Discover:

Source IP: 0.0.0.0 -> this is 0.0.0.0 as the client does not yet have an IP address assigned when it first reaches out to the DHCP server

Destination IP: 255.255.255.255

Source Port: 68 (client port)

Destination Port: 67 (server port)

Offer:

Source IP: 192.168.1.1 (DHCP server)

Destination IP: 255.255.255.255 (broadcast)

Source Port: 67

Destination Port: 68

Request:

Source IP: 0.0.0.0

Destination IP: 255.255.255.255

Source Port: 68

Destination Port: 67

ACK:

Source IP: 192.168.1.1

Destination IP: 192.168.1.102

Source Port: 67

Destination Port: 68

2. What is the link-layer (i.e., Ethernet) address of the host sending the DHCP Discover message?

From the Ethernet II section for the DHCP Discover packet (visible in the image), the Source MAC address is listed as Dell\_48:f5:23 (which translates to the full MAC address 00:08:74:48:f5:23).

3. What is the purpose of the Transaction-ID field? Using the packet bytes pane, how many bytes in length is this field?

- Purpose: The Transaction-ID is used to match incoming DHCP messages with ongoing communication between the client and the server. It ensures that the DHCP server’s Offer, ACK, and other messages are correctly associated with the client's Discover and Request messages.

- Length: From the packet bytes pane in your image, the Transaction-ID field is visible and it is 4 bytes long. This field appears in both the Discover and Offer messages.

4. Complete the address values in the table below, for the first four DHCP messages.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Message | Src IP | Dst IP | Src Port | Dst Port |
| Discover |  |  |  |  |
| Offer |  |  |  |  |
| Request |  |  |  |  |
| Ack |  |  |  |  |

5. What IP address is the DHCP server offering to the host in the DHCP Offer message? Indicate which DHCP message field contains the offered DHCP address.

- Look at the DHCP Offer packet.

- In the Bootstrap Protocol section (within the DHCP message), look for the Your (Client) IP Address field.

- The offered IP address is typically in this field, and in your case, it is likely 192.168.1.102, but you should verify by checking that specific field in Wireshark.

6. Explain the purpose of the Router line in the DHCP offer message? Compare to the IP address of the DHCP server and what can you conclude?

The Router (Gateway) Option in the DHCP Offer provides the client with the default gateway (router) that it should use to reach other networks (outside its subnet).

7. Explain the purpose of the DHCP lease time? What value is it set to in this exchange?

The DHCP Lease Time indicates how long the client can use the assigned IP address before it needs to request a renewal or a new IP address.

8. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client’s DHCP request? What would happen if the client’s DHCP release message is lost?

* The DHCP Release message is sent by the client to inform the DHCP server that it is giving up the assigned IP address. The server can then make this IP available for other clients.
* If the release message is lost, it is not critical because the server will reclaim the IP address after the lease time expires.