**CS3506 Lab 1 - Wireshark UDP/DHCP - Assignment**

NAME: Nathan Crowley

STUDENT NUMBER: 118429092.

**1. UDP**

* Select one UDP packet. From the packet content field, identify and determine the length (in bytes) of each of the UDP header fields.

UDP header has a fixed length of 8 bytes.

Each of the 4 header fields (sourcePort, destinationPort, Length, Checksum) is 2 bytes long.

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

The number of bytes of the UDP header and the UDP payload data.

UDP Length: 872. Data(872 bytes)**.**

* Input to the network interface is zeroes and ones. How does it know where the next frame starts? Based on the headers you see (Ethernet, IP, UDP), what is the maximum frame size?

Ethernet sends a **preamble** and then a **SoF**(start of frame). The next bit after this is the first bit of the frame.

- Max frame size: **1518 bytes**.

* Based on information in the UDP header alone, what is the highest possible source port number? Explain your answer.

The largest possible source port number is (2^16 -1) = 65535.

Since each UDP header field is 2bytes long (16 bits), we put 2 to the power of 16 bits to get how many port numbers can be represented. (65536)

With 65536 possible representations, we can have source ports 0 to 65535.

* Examine a pair of UDP packets in which the first packet is sent by your host and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

The packet being sent by host uses source port 56322 and destination port 443, which is used for secure web browser communicaiton.

The reply is then sent from this port 443 to the host at port 56322.

- Sent by host: source = 192.168.178.49, source port = 56322 desintaion port = 443.

- Reply: source = 74.125.193.103, source port = 443 desintaion port = 56322.

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

500 + 092 = 592 bytes.

header bytes = 8bytes.

So max number of bytes of UDP payload = 592 - 8 = **584 bytes**.

* **DHCP**

DHCP means Dynamic Host Configuration Protocol it is a service which assigns IP addresses automatically to devices (clients) whicha re connected in the network and requests for an IP address.

* 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. (Do not simply copy and paste this from another source).

*Client* *Sever*

|----------------**Discover -----------> |**

|<--------------**Offer**-----------------|

|----------------**Request**------------>|

|<--------------**AWK**-----------------|

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

Ethernet Source Address: IntelCor\_5c:7d:58

* What is the purpose of having a DHCP discover and a DHCP request message? (Why are they both needed?)

- **DHCP discover** request is used to broadcast that a DHCP client is looking fora DHCP server to user. The server recieves the discover packet and determines an appropriate address to give to the client. The server then temporarily reserves an address for the client and sends a **OFFER packet** asking client would it like to use this reservered address.

- **DHCP request** is then sent from the client to the server letting it know that it intends to use this address. The server then sends an **ACK packet** confirming that the client has been given a lease on this address for a server-specified period of time.

* What is the purpose of the Transaction-ID field?

Each DHCP message (DISCOVER/OFFER/REQUEST/ACK) has a Transaction-ID used to indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

All DHCP packets in a specific exchange between client and server carry this Transaction ID, this is how both ends know that the packets belong to the exchange rather than another concurrent DHCP operation.

* A host uses DHCP to obtain an IP address, among other things. But a host’s IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.
* 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.

The IP address its offering:

The DHCP field that contains the offered DHCP address is **yiaddr (Your Ip Address)**.

* Explain the purpose of the router and subnet mask lines in the DHCP offer message.

**Subnet Mask:** used to divide an IP address into two parks. One part identifies the host and the other identifies the network the host belongs to.

**Router:**

* Explain the purpose of the DHCP lease time.

**DHCP Lease Time is the amount of time a network device can use an IP address in a network. The IP address is reserved for the device until this lease time expires.**

**When the DHCP lease time expires, the device is atuomatically released from the IP address and the must ask the router to give out a new one.**

* 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 purpose of the DHCP Release is to tell the client to release the IP address it using and remove its configuration from the interface of the device.**

**-**

**- If the Release message is lost, the client releases the IP address but the server will not re-assign that adress until the clients DHCP lease time on that address expires.**