Student Name : ________Lim Xin Yi____________________

Group : ___________TCCA____________

Date : ___________16 Oct 2023________

## LAB 3: SNIFFING AND ANALYSING NETWORK PACKETS

## EXERCISE 3A: PACKETS CAPTURING

List the sequence of all relevant network packets sent and received by your laboratory PC from the time your Rfc865UdpClient initiated a request to the DNS server to resolve the QoD server name till it received the quote of the day. Fill in the MAC and IP address of the packets where appropriate/available.

| Packet | Source MAC | Source IP | Dest. MAC | Dest. IP | Purpose of Packet |
|---|---|---|---|---|---|
| 1. | 00:4e:01:bd:a8:41 | 172.21.150.191 | 00:08:e3:ff:fc:a0 | 155.69.3.8 | DNS request |
| 2. | 00:08:e3:ff:fc:a0 | 155.69.3.8 | 00:4e:01:bd:a8:41 | 172.21.150.191 | DNS reply |
| 3. | 00:4e:01:bd:a8:41 | | ff:ff:ff:ff:ff:ff<br>(Broadcast) | | Address Resolution Protocol request |
| 4. | 96:58:1e:57:da:a4 | | 00:4e:01:bd:a8:41 | | Address Resolution Protocol reply |
| 5. | 00:4e:01:bd:a8:41 | 172.21.150.191 | 96:58:1e:57:da:a4 | 172.21.148.202 | Quote of the day request |
| 6. | 96:58:1e:57:da:a4 | 172.21.148.202 | 00:4e:01:bd:a8:41 | 172.21.150.191 | Quote of the day reply |

Determine the IP address of DNS server.
155.69.3.8

Determine the IP address of the QoD server
172.21.148.202

What is the MAC address of the router?
96:58:1e:57:da:a4

## EXERCISE 3B: DATA ENCAPSULATION

| | |
|---|---|
| Complete Captured Data<br>(please fill in ONLY 8 bytes in a row, in hexadecimal) | 96581e57daa4004e |
| | 01bda84108004500 |
| | 003c7bfe00008011 |
| | 3afeac1596bfac15 |
| | 94cae13b00110028 |
| | 7af64c696d205869 |
| | 6e2059692c205443 |
| | 43412c203137322e |
| | 32312e3134382e32 |
| | 3032 |
| | |
| | |
| | |
| | |
| | |

## EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
How do you know?
Network PDU
In the TCP/IP model, Ethernet belongs to layer 2 – Data link layer. Hence, its frame data should contain packet data passed from the Network layer. Additionally, from the frame data, we can see that it contains the source and destination IP addresses (Network-header, Internet Protocol), the source and destination ports (Transport-header, User Datagram Protocol) and the actual Application layer data.

Determine the following from the captured data in Exercise 3B:

| | |
|---|---|
| Destination Address | 96581e57daa4 |
| Source Address | 004e01bda841 |
| Frame Data<br>(8 bytes in a row, in hexadecimal) | 4500003c7bfe0000 |
| | 80113afeac1596bf |
| | ac1594cae13b0011 |
| | 00287af64c696d20 |
| | 58696e2059692c20 |
| | 544343412c203137 |
| | 322e32312e313438 |

| | |
|---|---|
| | 2e323032 |
| | |
| | |
| | |

## EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?
Transport PDU
In the TCP/IP model, IP belongs to layer 3 – Network layer. Hence, its packet data should contain data passed from the Transport layer. Additionally, from the packet data, we can see that it contains the source and destination ports (Transport-header, User Datagram Protocol) and the actual Application layer data.

Does the captured IP header have the field: Options + Padding? How do you know?
No
In the captured packet, the source port data follows right after the destination IP address, there is no data bytes representing the Options + Padding field.

Determine the following from the Frame Data field in Exercise 3C:

| | |
|---|---|
| Version | 4 |
| Total Length | 60 |
| Identification | 0x7bfe (31742) |
| Flags<br>(interpret the meanings) | 0x0<br>Reserved bit: Not set<br>Don’t fragment: Not Set<br>More fragsment: Not set |
| Fragment Offset | 0 |
| Source Address | 172.21.150.191 |
| Destination Address | 172.21.148.202 |
| Packet Data<br>(8 bytes in a row, in hexadecimal) | e13b001100287af6 |
| | 4c696d2058696e20 |
| | 59692c2054434341 |
| | 2c203137322e3231 |
| | 2e3134382e323032 |
| | |
| | |
| | |
| | |

## EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

Determine the following from the Packet Data field in Exercise 3D:

| | |
|---|---|
| Source Port | 57659 |
| Destination Port | 17 |
| Length | 40 |
| Data<br>(8 bytes in a row, in hexadecimal) | 4c696d2058696e20 |
| | 59692c2054434341 |
| | 2c203137322e3231 |
| | 2e3134382e323032 |

**EXERCISE 3F: APPLICATION PDU**

Interpret the application layer data from the Data field in Exercise 3E:

| | |
|---|---|
| Message | Lim Xin Yi, TCCA, 172.21.148.202 |

Is this the message that you have sent?
Yes.