CE3005: Computer Networks/CZ3006 Netcentric Computing

Student Name : Yong Wen Shiuan

Group : TS7

Date : 23 / 9 / 2021

**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. |  | 172.21.150.205 |  |  | DNS request |
| 2. |  |  |  | 172.21.150.205 | DNS response |
| 3. |  | 172.21.150.205 |  |  | ARP request |
| 4. |  |  |  | 172.21.150.205 | ARP response |
| 5. |  | 172.21.150.205 |  | 172.21.148.202 | QoD request |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Last. | QOTD server | 172.21.148.202 | Your QotdClient | 172.21.150.205 | Quote of the day reply |

What is the IP address of DNS server? [\_\_\_\_\_\_\_\_\_\_\_\_]

What is the IP address of the QoD server? [ 172.21.148.202 ]

What is the MAC address of the router? [\_\_\_\_\_\_\_\_\_\_\_\_]

Page 3-1

# EXERCISE 3B: DATA ENCAPSULATION

|  |  |
| --- | --- |
| Complete Captured  Data    (please fill in ONLY 8 bytes in a row, in hexadecimal) |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

# EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?

How do you know?

The type of upper layer data is the packet data (Figure 3.2 in lab manual). This is because the ethernet frame here is the data link PDU, which receives / carries data from the upper Network layer.

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

|  |  |
| --- | --- |
| Destination Address |  |
| Source Address |  |
| Protocol | IPv4 (0x0800) |
| Frame Data  (8 bytes in a row, in hexadecimal) |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |  |
|  |

# EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?

The type of upper layer data is the Data from the Transport PDU (Figure 3.2 in lab manual). This is because the IP datagram here is the Network PDU, which carries/contains data from the upper Transport layer.

Does the captured IP header have the field: Options + Padding? How do you know?

No, it does not have the field: Options + Padding. Because there are no zeroes for padding.

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

|  |  |
| --- | --- |
| Version | 4 |
| Total Length |  |
| Identification |  |
| Flags  (interpret the meanings) | Flags: 0x00  0... .... = Reserved bit: Not set  .0.. .... = Don't fragment: Not set  ..0. .... = More fragments: Not set |
| Fragment Offset | 0 |
| Protocol | UDP (0x11) |
| Source Address | 172.21.150.205 |
| Destination Address | 172.21.148.202 |
| Packet Data    (8 bytes in a row, in hexadecimal) |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

# EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

|  |  |
| --- | --- |
| Source Port |  |
| Destination Port | 17 |
| Length |  |
| Data |  |
|  |
| (8 bytes in a row, in hexadecimal) |  |
|  |

# EXERCISE 3F: APPLICATION PDU

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

|  |  |
| --- | --- |
| Message |  |

Is this the message that you have sent?

Yes