Student Name : Ernest Ang Cheng Han

Group : FDDP1

Date : 4 October 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. | 00:4e:01:bd:cb:93 | 172.21.151.236 | 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:cb:93 | 172.21.151.236 | DNS Response |
| 3. | 00:4e:01:bd:cb:93 | 172.21.151.236 | ff:ff:ff:ff:ff:ff (broadcast) | Null (broadcast) | ARP request |
| 4. | 96:58:1e:57:da:a4 | 172.21.148.202 | 00:4e:01:bd:cb:93 | 172.21.151.236 | ARP Response |
| 5. | 00:4e:01:bd:cb:93 | 172.21.151.236 | 96:58:1e:57:da:a4 | 172.21.148.202 | QOTD request |
| 6. | 96:58:1e:57:da:a4 | 172.21.148.202 | 00:4e:01:bd:cb:93 | 172.21.151.236 | QOTD response |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

What is the IP address of DNS server? 155.69.3.8

What is the IP address of the QoD server? 172.21.148.202

What is the MAC address of the router? 00:08:e3:ff:fc:a0

Page 3-1

# EXERCISE 3B: DATA ENCAPSULATION

**From client to server**

|  |  |
| --- | --- |
| Complete Captured Data  (please fill in ONLY 8 bytes in a row, in hexadecimal) | 96 58 1e 57 da a4 00 4e |
| 01 bd cb 93 08 00 45 00 |
| 00 45 80 80 00 00 80 11 |
| 35 46 ac 15 97 ec ac 15 |
| 94 ca e4 76 00 11 00 31 |
| 2c 6f 45 72 6e 65 73 74 |
| 20 41 6e 67 20 43 68 65 |
| 6e 67 20 48 61 6e 2c 20 |
| 54 53 34 2c 20 31 37 32 |
| 2e 32 31 2e 31 34 37 2e |
| 31 32 36 |
|  |
|  |
|  |
|  |

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

What type of upper layer data is the captured ethernet frame carrying? How do you know?

Ethernet is carrying data from the network layer, transport layer, and application layer. From Wireshark we can see that the contents of our request to the QOTD server on port 17 as well as the server’s requests to our computer. Hence, we know that the data from the upper layers above the data link layer which is the layer which Ethernet is operating on (i.e. the network layer since IP is being used, the transport layer since UDP is being used to transport the messages from our client to server, and application layer since we can actually see the contents of the quote of the day from the server as well as contents of the requester)

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

|  |  |
| --- | --- |
| Destination Address | 96 58 1e 57 da a4 (IP address: 172.21.148.202) |
| Source Address | 00 4e 01 bd cb 93 (IP address: 172.21.151.236) |
| Protocol Type | 08 00 (IPv4) |
| Frame Data  (8 bytes in a row, in hexadecimal) | 45 72 6e 65 73 74 |
| 20 41 6e 67 20 43 68 65 |
| 6e 67 20 48 61 6e 2c 20 |
| 54 53 34 2c 20 31 37 32 |
| 2e 32 31 2e 31 34 37 2e |
| 31 32 36 |
|  |
|  |
|  |

# EXERCISE 3D: NETWORK PDU - IP DATAGRAM

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

Transport layer and application layer data. From the contents of Wireshark, we can see that after the IP Protocol header, is the UDP protocol header and the actual data being transmitted from the client and the server. Hence, we can deduce that the data from transport and from the application layer is being encapsulated within the IP datagram.

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

No there is not. From Wireshark, we can observe that there is no options + padding and after the destination address, it is immediately the UDP protocol header. Also, the entire IP datagram is 20 + 8 + 41 = 69 bytes. It is long enough and does not require options + padding.

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

|  |  |
| --- | --- |
| Version | 0100 (Version 4) |
| Total Length | 0101 (20 bytes, (5)) |
| Identification | 8080 |
| Flags (interpret the meanings) | 00 (not set, not fragmented, not reserved)  Flags: 0x00  0... .... = Reserved bit: Not set  .0.. .... = Don't fragment: Not set  ..0. .... = More fragments: Not set |
| Fragment Offset | 00 00 (0) |
| Protocol | 11 (UDP) |
| Source Address | ac 15 97 ec (IP address: 172.21.151.236, MAC Address: 00:4e:01:bd:cb:93) |
| Destination Address | ac 15 94 ca (IP address: 172.21.148.202, MAC Address: 96:58:1e:57:da:a4) |
| Packet Data  (8 bytes in a row, in hexadecimal) | e4 76 00 11 00 31 2c 6f |
| 45 72 6e 65 73 74 20 41 |
| 6e 67 20 43 68 65 6e 67 |
| 20 48 61 6e 2c 20 54 53 |
| 34 2c 20 31 37 32 2e 32 |
| 31 2e 31 34 37 2e 31 32 |
| 36 |
|  |
|  |

# EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

|  |  |
| --- | --- |
| Source Port | e4 76 (port 58486) |
| Destination Port | 00 11 (port 17) |
| Length | 00 31 (length 49) |
| Data (8 bytes in a row, in hexadecimal) | 45 72 6e 65 73 74 20 41 |
| 6e 67 20 43 68 65 6e 67 |
| 20 48 61 6e 2c 20 54 53 |
| 34 2c 20 31 37 32 2e 32 |
| 31 2e 31 34 37 2e 31 32 |
| 36 |

# EXERCISE 3F: APPLICATION PDU

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

|  |  |
| --- | --- |
| Message | Ernest Ang Cheng Han, FDDP1, 172.21.151.236 |

Is this the message that you have sent?

Yes this is the data I have sent