CE3005: Computer Networks/CZ3006 Netcentric Computing

Student Name : Ng Chi Hui

Group : FDDP1

Date : 04/10/2021

**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:AC:8F | 172.21.151.141 | 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:AC:8F | 172.21.151.141 | DNS Response |
| 3. | 00:4E:01:BD:AC:8F | 172.21.151.141 | FF:FF:FF:FF:FF:FF | 172.21.148.202 | ARP  Request |
| 4. | 96:58:1E:57:DA:A4 | 172.21.148.202 | 00:4E:01:BD:AC:8F | 172.21.151.141 | ARP Response |
| 5. | 00:4E:01:BD:AC:8F | 172.21.151.141 | 96:58:1E:57:DA:A4 | 172.21.148.202 | UDP Request |
| 6. | 96:58:1E:57:DA:A4 | 172.21.148.202 | 00:4E:01:BD:AC:8F | 172.21.151.141 | UDP Response |
| Last | QOTD server |  | Your QotdClient |  | Quote of the day reply |

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]

# EXERCISE 3B: DATA ENCAPSULATION

|  |  |
| --- | --- |
| Complete Captured  Data    (please fill in ONLY 8 bytes in a row, in hexadecimal) | 96:58:1E:57:DA:A4:00:4E |
| 01:BD:AC:8F:08:00:45:00 |
| 00:3E:3B:CF:00:00:80:11 |
| 7A:5D:AC:15:97:8D:AC:15 |
| 94:CA:F5:27:00:11:00:2A |
| A9:C8:4E:67:20:43:68:69 |
| 20:48:75:69:2C:20:46:44 |
| 44:50:31:20:2C:20:31:37 |
| 32:2E:32:31:2E:31:35:31 |
| 2E:31:34:31 |

# EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

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

* The Ethernet frame is carrying the **Internet Protocol (IPv4).**

How do you know?

* By expanding Ethernet under 2nd window, we see 2 bytes captured before the frame data is 0x0800.
* This means that the frame is carrying an IPv4 packet.
* Thus, it must be carrying the internet protocol within its captured data.

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

|  |  |
| --- | --- |
| Destination Address | 96:58:1e:57:da:a4 |
| Source Address | Dell\_bd:ac:8f (00:4e:01:bd:ac:8f) |
| Protocol | IPv4 (0x0800) |
| Frame Data    (8 bytes in a row, in hexadecimal) | 45:00:00:3E:3B:CF:00:00 |
| 80:11: 7A:5D:AC:15:97:8D |
| AC:15:94:CA:F5:27:00:11 |
| 00:2A:A9:C8:4E:67:20:43 |
| 68:69:20:48:75:69:2C:20 |
| 46:44:44:50:31:20:2C:20 |
| 31:37:32:2E:32:31:2E:31 |
| 35:31:2E:31:34:31 |

# EXERCISE 3D: NETWORK PDU - IP DATAGRAM

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

* The IP packet is carrying the **User Datagram Protocol**.
* In the Internet Protocol, the field protocol is identified as UDP (0x11), thus it must be carrying the User Datagram Protocol.

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

No Options + Padding, no zeros observed.

There are no options present because the Internet Header Length is 5 (20 bytes), which is the minimum IHL. Options cannot be present as they require an additional offset to the IHL, causing it to be larger than 20 bytes. Since IHL is 20 bytes, no options are present as there is no space to include them in the header.

No padding because the IP header is 160 bits long, whichis a factor of 32 bits and thus doesn’t require any additional padding. Padding is only required when the header is not a multiple of 32 bits. Moreover, since we know that options field is not present, there will not be any varying length of options field in the IP header thus padding will not be needed.

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

|  |  |
| --- | --- |
| Version | 4 (0x4) |
| Total Length | 62 (00x3E) |
| Identification | 0x3BCF (15311) |
| Flags  (interpret the meanings) | 0x00  **First Bit (Reserved Bit):** Reserved bit always set to 0  **Second Bit (Do Not Fragment):** Represents whether or not the packet can be fragmented. Since the second bit is zero here, it means the packet is not allowed to be fragmented.  **Third Bit (More Fragments):** Represents more fragment which is not set. Since it is 0, it indicated that the packet is not fragmented. |
| Fragment Offset | 0 (0x0000) |
| Protocol | UDP (0x17) |
| Source Address | 172.21.151.141 (0 X AC 15 97 8D) |
| Destination Address | 172.21.148.202 (0 X AC 15 94 CA) |
| Packet Data    (8 bytes in a row, in hexadecimal) | F5:27:00:11:00:2A:A9:C8 |
| 4E:67:20:43:68:69:20:48 |
| 75:69:2C:20:46:44:44:50 |
| 31:20:2C:20:31:37:32:2E |
| 32:31:2E:31:35:31:2E:31 |
| 34:31 |

# EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

|  |  |
| --- | --- |
| Source Port | 62759 (0xF5 27) |
| Destination Port | 17 (0x00 11) |
| Length | 42 (0x00 2A) |
| Data  (8 bytes in a row, in hexadecimal) | 4E:67:20:43:68:69:20:48 |
| 75:69:2C:20:46:44:44:50 |
| 31:20:2C:20:31:37:32:2E |
| 32:31:2E:31:35:31:2E:31 |
| 34:31 |

# EXERCISE 3F: APPLICATION PDU

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

|  |  |
| --- | --- |
| Message | Ng Chi Hui, FDDP1, 172.21.151.141 |

**Is this the message that you have sent?**

Yes, Indeed