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.	00:4e:01:bd:b4:cf	172.21.150.205	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:b4:cf	172.21.150.205	DNS response
3.	00:4e:01:bd:b4:cf	172.21.150.205	98:be:94:63:5d:52	172.21.147.9	ARP request
4.	98:be:94:63:5d:52	172.21.147.9	00:4e:01:bd:b4:cf	172.21.150.205	ARP response
5.	00:4e:01:bd:b4:cf	172.21.150.205	96:58:1e:57:da:a4	172.21.148.202	Quote of the day request
Last.	(QOTD server) 96:58:1e:57:da:a4	172.21.148.202	(Your QotdClient) 00:4e:01:bd:b4:cf	172.21.150.205	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? [172.21.147.9]

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 b4 cf 08 00 45 00
	00 40 2b 8f 00 00 80 11
	8b 5b ac 15 96 cd ac 15
	94 ca fe fb 00 11 00 2c
	cb d4 59 6f 6e 67 20 57
	65 6e 20 53 68 69 75 61
	6e 2c 20 54 53 37 2c 20
	31 37 32 2e 32 31 2e 31
	35 30 2e 32 30 35

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). The packet data is contained within the Network PDU. 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	96:58:1e:57:da:a4
Source Address	00:4e:01:bd:b4:cf
Protocol	IPv4 (0x0800)
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 40 2b 8f 00 00
	80 11 8b 5b ac 15 96 cd
	ac 15 94 ca fe fb 00 11
	00 2c cb d4 59 6f 6e 67

	20 57 65 6e 20 53 68 69
	75 61 6e 2c 20 54 53 37
	2c 20 31 37 32 2e 32 31
	2e 31 35 30 2e 32 30 35

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. The next bytes directly after the destination address is the data, so no bytes are used for Options + Padding.

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

Version	4
Total Length	64
Identification	0x2b8f (11151)
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 (17)
Source Address	172.21.150.205
Destination Address	172.21.148.202
Packet Data (8 bytes in a row, in hexadecimal)	fe fb 00 11 00 2c cb d4
	59 6f 6e 67 20 57 65 6e
	20 53 68 69 75 61 6e 2c
	20 54 53 37 2c 20 31 37
	32 2e 32 31 2e 31 35 30
	2e 32 30 35

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	65275
Destination Port	17
Length	44
Data (8 bytes in a row, in hexadecimal)	59 6f 6e 67 20 57 65 6e
	20 53 68 69 75 61 6e 2c
	20 54 53 37 2c 20 31 37
	32 2e 32 31 2e 31 35 30
	2e 32 30 35

EXERCISE 3F: APPLICATION PDU

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

Message	Yong Wen Shiuan, TS7, 172.21.150.205

Is this the message that you have sent?

Yes