Student Name : Jervis Chan Jun Yong

Group : TS8

Date : 24 March 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-C0-D7	172.21.149.77	00-08-E3-FF-FC-A0	155.69.5.54	DNS request
2.	00-08-E3-FF-FC-A0	155.69.5.54	00-4E-01-BD-C0-D7	172.21.149.77	DNS response
3.	00-4E-01-BD-C0-D7	172.21.149.77	FF-FF-FF-FF-FF-FF	Broadcast	ARP request
4.	FE-96-8F-0F-DC-64	172.21.145.187	00-4E-01-BD-C0-D7	172.21.149.77	ARP response
5.	00-4E-01-BD-C0-D7	172.21.149.77	FE-96-8F-0F-DC-64	172.21.145.187	UDP request to QoD server
6.	FE-96-8F-0F-DC-64	172.21.145.187	00-4E-01-BD-C0-D7	172.21.149.77	Quote of the day reply

Determine the IP address of DNS server. **155.69.5.54**
Determine the IP address of the QoD server **172.21.145.187**
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)	fe 96 8f 0f dc 64 00 4e
	01 bd c0 d7 08 00 45 00
	00 3b ad 0c 00 00 80 11
	0e 72 ac 15 95 4d ac 15
	91 bb db 00 00 11 00 27
	8b 55 4a 65 72 76 69 73
	20 43 68 61 6e 2c 20 54
	53 38 2c 20 31 37 32 2e
	32 31 2e 31 34 39 2e 37
	37

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
How do you know?
The Ethernet frame is carrying the data from the network PDU. In turn, the network PDU might hold upper layer data from the Transport and Application layer. This can be seen from the 08 00 Ether Protocol Type which corresponds to IPv4.

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

Destination Address	fe 96 8f 0f dc 64
Source Address	00 4e 01 bd c0 d7
Protocol	08 00
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 3b ad 0c 00 00
	80 11 0e 72 ac 15 95 4d
	ac 15 91 bb db 00 00 11
	00 27 8b 55 4a 65 72 76
	69 73 20 43 68 61 6e 2c
	20 54 53 38 2c 20 31 37
	32 2e 32 31 2e 31 34 39
	2e 37 37

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?
The captured IP packet contains Transport PDU. The protocol contains transport layer protocol (UDP) and there is additional data.

Does the captured IP header have the field: Options + Padding? How do you know?
No, there are no Options + Padding. The data does not contain multiples of 32 bits and the IP header length is 20.

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

Version	4
Total Length	0x003b (This translates to 59)
Identification	0xad0c
Flags (interpret the meanings)	000 (in bits) This shows that all three flags (reserved bit, don't fragment, more fragments) are not set
Fragment Offset	0
Protocol	UDP (0x11)
Source Address	172.21.149.77 (ac 15 95 4d)
Destination Address	172.21.145.187 (ac 15 91 bb)
Packet Data (8 bytes in a row, in hexadecimal)	db 00 00 11 00 27 8b 55
	4a 65 72 76 69 73 20 43
	68 61 6e 2c 20 54 53 38
	2c 20 31 37 32 2e 32 31
	2e 31 34 39 2e 37 37

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	db 00
Destination Port	00 11 (Port 17)
Length	00 27 (39 in decimal)
Data	4a 65 72 76 69 73 20 43
	68 61 6e 2c 20 54 53 38

(8 bytes in a row, in hexadecimal)	2c 20 31 37 32 2e 32 31
	2e 31 34 39 2e 37 37

EXERCISE 3F: APPLICATION PDU

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

Message	Jervis Chan, TS8, 172.21.149.77

Is this the message that you have sent? Yes