Student Name : _____Ferguson Chiew_____

Group : _____SCS1_____

Date : _____14/03/2024_____

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.	A4:BB:6D:61:CF:D0 (ME)	10.96.185.255	00:00:0C:9F:F0:F0	155.69.3.8	DNS request
2.	00:00:0C:9F:F0:F0	155.69.3.8	A4:BB:6D:61:CF:D0 (ME)	10.96.185.255	DNS response
3.	A4:BB:6D:61:CF:D0 (ME)	10.96.185.255	FF:FF:FF:FF:FF:FF	Broadcast	ARP request
4.	CC:B6:C8:85:5A:37 (QOTD Server)	155.69.100.96	A4:BB:6D:61:CF:D0 (ME)	10.96.185.255	ARP reply
5.	A4:BB:6D:61:CF:D0 (ME)	10.96.185.255	CC:B6:C8:85:5A:37 (QOTD Server)	155.69.100.96	Quote of the day request
Last.	QOTD server CC:B6:C8:85:5A:37	155.69.100.96	Your QotdClient A4:BB:6D:61:CF:D0 (ME)	10.96.185.255	Quote of the day reply

Determine the IP address of DNS server. 155.69.3.8
Determine the IP address of the QoD server 155.69.100.96
What is the MAC address of the router? 00:00:0C:9F:F0:F0

EXERCISE 3B: DATA ENCAPSULATION

Complete Captured Data (please fill in ONLY 8 bytes in a row, in hexadecimal)	00 00 0c 9f f0 f0 a4 bb
	6d 61 cf d0 08 00 45 00
	00 3a 3c d0 00 00 80 11
	80 9e 0a 60 b9 ff ac 15
	94 ca d6 d2 00 11 00 26
	46 65 72 67 75 73 6f 6e
	2c 20 53 43 53 31 2c 20
	31 30 2e 39 36 2e 31 38
	35 2e 32 35 35

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

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

IPv4. It is found in the Ether Protocol Type (Type:IPv4) in the Ethernet Frame (Ethernet II)

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

Destination Address	00:00:0C:9F:F0:F0
Source Address	A4:BB:6D:61:CF:D0
Protocol	IPv4(0x8000)
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 3a 3c d0 00 00
	80 11 80 9e 0a 60 b9 ff
	ac 15 94 ca d6 d2 00 11
	00 26 46 65 72 67 75 73
	6f 6e 2c 20 53 43 53 31
	2c 20 31 30 2e 39 36 2e
	31 38 35 2e 32 35 35

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

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

UDP. It is found in the Protocol (UDP) of the IP Datagram.

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

No. There are no bits in between the destination address and the packet data, so no bits are used for Options + Padding.

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

Version	4
Total Length	58 bytes
Identification	0x3CD0 (15568)
Flags (interpret the meanings)	Flags: 0x00 1st bit: Reserved Bit, Not Set 2nd bit: Don't Fragment, Not Set 3rd bit: More Fragment, Not Set
Fragment Offset	0
Protocol	UDP (17)
Source Address	10.96.185.255
Destination Address	155.69.100.96
Packet Data (8 bytes in a row, in hexadecimal)	94 ca d6 d2 00 11 00 26
	46 65 72 67 75 73 6f 6e
	2c 20 53 43 53 31 2c 20
	31 30 2e 39 36 2e 31 38
	35 2e 32 35 35

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	54994
Destination Port	17
Length	38
Data	46 65 72 67 75 73 6f 6e
	2c 20 53 43 53 31 2c 20

(8 bytes in a row, in hexadecimal)	31 30 2e 39 36 2e 31 38
	35 2e 32 35 35

EXERCISE 3F: APPLICATION PDU

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

Message	Ferguson, SCS1, 10.96.185.255

Is this the message that you have sent? Yes