Student Name : Toh Kok Soon

Group : SCSI

Date : 24/09/2025

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.	-	-	-	-	DNS request
2.	-	-	-	-	DNS reply
3.	a4:27:a5:5b:ba:20	-	a4:bb:6d:61:d6:81	-	Arp Request
4.	a4:bb:6d:61:d6:81	-	ff:ff:ff:ff:ff:ff	-	Arp reply
5.	Your QotdClient	10.96.182.202	QOTD server	10.96.189.96	Quote of the day request
Last.	QOTD server	10.96.189.96	Your QotdClient	10.96.182.202	Quote of the day reply

Determine the IP address of DNS server. N/A
Determine the IP address of the QoD server 10.96.189.96
What is the MAC address of the router? N/A

EXERCISE 3B: DATA ENCAPSULATION

Complete Captured Data (please fill in ONLY 8 bytes in a row, in hexadecimal)	a4 27 a5 5b f4 20 a4 bb
	6d 61 d6 81 08 00 45 00
	00 3d a2 04 00 00 80 11
	00 00 0a 60 b6 ca 0a 60
	bd 60 22 b8 00 11 00 29
	89 25 54 6f 68 20 4b 6f
	6b 20 53 6f 6f 6e 2c 20
	53 43 53 49 2c 20 31 30
	2e 39 36 2e 31 38 32 2e
	32 30 32

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

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

IPv4, the type field in wireshark shows 08 00 which correspond to IPv4 protocol

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

Destination Address	a4 27 a5 5b f4 20
Source Address	a4 bb 6d 61 d6 81
Protocol	08 00
Frame Data (8 bytes in a row, in hexadecimal)	45 00
	00 3d a2 04 00 00 80 11
	00 00 0a 60 b6 ca 0a 60
	bd 60 22 b8 00 11 00 29
	89 25 54 6f 68 20 4b 6f
	6b 20 53 6f 6f 6e 2c 20
	53 43 53 49 2c 20 31 30
	2e 39 36 2e 31 38 32 2e

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

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

UDP, the protocol field is 17 which corresponds to UDP

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

No, Wireshark did not show a field for Options+Padding. It can also be seen that from wireshark that the header length is 20 which is the size of the header without any padding and options

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

Version	4
Total Length	61
Identification	41476
Flags (interpret the meanings)	00 0 (None Set)
Fragment Offset	0
Protocol	UDP (17)
Source Address	10.96.182.202
Destination Address	10.96.189.96
Packet Data (8 bytes in a row, in hexadecimal)	22 b8 00 11 00 29
	89 25 54 6f 68 20 4b 6f
	6b 20 53 6f 6f 6e 2c 20
	53 43 53 49 2c 20 31 30
	2e 39 36 2e 31 38 32 2e

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	8888
Destination Port	17
Length	41
Data (8 bytes in a row, in hexadecimal)	54 6f 68 20 4b 6f
	6b 20 53 6f 6f 6e 2c 20
	53 43 53 49 2c 20 31 30
	2e 39 36 2e 31 38 32 2e

EXERCISE 3F: APPLICATION PDU

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

Message	Toh Kok Soon, SCSI, 10.96.182.202

Is this the message that you have sent? Yes