Student Name : Keh Jing Xiang

Group : SCSE

Date : 11-3-2025

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.	00:4E:01:BD:C2:0B	-	FF:FF:FF:FF:FF:FF	-	ARP request
2.	A4:27:A5:5B:BA:20	-	00:4E:01:BD:C2:0B	-	ARP reply
3.	A4:27:A5:5B:F4:20	-	00:4E:01:BD:C2:0B	-	ARP reply
4.	00:4E:01:BD:C2:0B	10.96.178.254	A4:27:A5:5B:BA:20	10.96.189.98	Quote of the day request
5.	A4:27:A5:5B:BA:20	10.96.189.98	00:4E:01:BD:C2:0B	10.96.17.254	Quote of the day reply
Last.	QOTD server		Your QotdClient		Quote of the day reply

Determine the IP address of DNS server. -
Determine the IP address of the QoD server 10.96.189.98

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)	A4 27 A5 5B BA 20 00 4E
	01 BD C2 0B 08 00 45 00
	00 3F A2 42 00 00 80 11
	13 4B 0A 60 B2 FE 0A 60
	BD 62 FF 16 00 11 00 2B
	B2 DC 4B 65 68 20 4A 69
	6E 67 20 58 69 61 6E 67
	2C 20 53 43 53 45 2C 20
	31 30 2E 39 36 2E 31 37
	38 2E 32 35 34

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
How do you know?
The captured ethernet frame is carrying IPv4 because the Ether Protocol Type bit is 0x0800.

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

Destination Address	A4 27 A5 5B BA 20
Source Address	00 4E 01 BD C2 0B
Protocol	IPv4 (0x0800)
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 3F A2 42 00 00
	80 11 13 4B 0A 60 B2 FE
	0A 60 BD 62 FF 16 00 11
	00 2B B2 DC 4B 65 68 20
	4A 69 6E 67 20 58 69 61
	6E 67 2C 20 53 43 53 45
	2C 20 31 30 2E 39 36 2E
	31 37 38 2E 32 35 34

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?
It is UDP because it is found in the Protocol section of the IP datagram.

Does the captured IP header have the field: Options + Padding? How do you know?
No, because there wasn't any extra bits between the destination address and the packet data.

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

Version	4
Total Length	63
Identification	0xa242 (41538)
Flags (interpret the meanings)	0x00 Bit 1: Reserved bit (Not set) Bit 2: Don't fragment (Not set) Bit 3: More fragments (Not set)
Fragment Offset	0
Protocol	UDP (17)
Source Address	10.96.178.254
Destination Address	10.96.189.98
Packet Data (8 bytes in a row, in hexadecimal)	FF 16 00 11 00 2B B2 DC
	4B 65 68 20 4A 69 6E 67
	20 58 69 61 6E 67 2C 20
	53 43 53 45 2C 20 31 30
	2E 39 36 2E 31 37 38 2E
	32 35 34

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	65302
Destination Port	17
Length	43
Data	4B 65 68 20 4A 69 6E 67
	20 58 69 61 6E 67 2C 20
	53 43 53 45 2C 20 31 30

(8 bytes in a row, in hexadecimal)	2E 39 36 2E 31 37 38 2E
	32 35 34

EXERCISE 3F: APPLICATION PDU

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

Message	Keh Jing Xiang, SCSE, 10.96.179.254

Is this the message that you have sent?

Yes