Student Name : Singh Jasraj

Group : A29

Date : 07 March 2023

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:cc:f6	172.21.145.58	00:08:e3:ff:fc:a0	155.69.3.8	DNS request
2.	00:08:e3:ff:fc:a0	155.69.3.8	a4:bb:6d:61:cc:f6	172.21.145.58	Reply with IP of the Domain
3.	a4:bb:6d:61:cc:f6	172.21.145.58	ff:ff:ff:ff:ff:ff	Broadcast	ARP asking for 172.21.148.201
4.	fe:96:8f:0f:dc:64	172.21.148.201	a4:bb:6d:61:cc:f6	172.21.145.58	ARP reply with IP paired with MAC
5.	a4:bb:6d:61:cc:f6	172.21.145.58	fe:96:8f:0f:dc:64	172.21.148.201	UDP request
Last.	fe:96:8f:0f:dc:64	172.21.148.201	a4:bb:6d:61:cc:f6	172.21.145.58	Quote of the day reply

Determine the IP address of DNS server. 155.69.3.8
Determine the IP address of the QoD server. 172.21.148.201
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 a4 bb
	6d 61 cc f6 08 00 45 00
	00 3d 03 c8 00 00 80 11
	00 00 ac 15 91 3a ac 15
	94 c9 f4 46 00 11 00 29
	1f 06 53 69 6e 67 68 20
	4a 61 73 72 61 6a 2c 20
	41 32 39 2c 20 2f 31 37
	32 2e 32 31 2e 31 34 35
	2e 35 38

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying? Internet Protocol (IPv4)
How do you know? The 2 bytes captured before the frame data is 0x0800. This indicates that the frame is carrying an IPv4 packet. Thus, it must be carrying the internet protocol within its captured data.

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

Destination Address	fe:96:8f:0f:dc:64
Source Address	a4:bb:6d:61:cc:f6
Protocol	UDP
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 3d 03 c8 00 00
	80 11 00 00 ac 15 91 3a
	ac 15 94 c9 f4 46 00 11
	00 29 1f 06 53 69 6e 67
	68 20 4a 61 73 72 61 6a
	2c 20 41 32 39 2c 20 2f
	31 37 32 2e 32 31 2e 31
	34 35 2e 35 38

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know? User Datagram Protocol (UDP). In the Internet Protocol, the field protocol is identified as UDP (0x11), thus it must be carrying the User Datagram Protocol.

Does the captured IP header have the field: Options + Padding? How do you know? No, there are no options immediately after the destination address, just the data.

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

Version	4
Total Length	0x4500 (61 bytes)
Identification	0x03c8 (968)
Flags (interpret the meanings)	All flags unset
Fragment Offset	0
Protocol	UDP (17)
Source Address	172.21.145.58
Destination Address	172.21.148.201
Packet Data (8 bytes in a row, in hexadecimal)	f4 46 00 11 00 29 1f 06
	53 69 6e 67 68 20 4a 61
	73 72 61 6a 2c 20 41 32
	39 2c 20 2f 31 37 32 2e
	32 31 2e 31 34 35 2e 35
	38

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	0xf446 (63974)
Destination Port	0x0011 (17)
Length	0x0029 (41 bytes)
Data (8 bytes in a row, in hexadecimal)	53 69 6e 67 68 20 4a 61
	73 72 61 6a 2c 20 41 32
	39 2c 20 2f 31 37 32 2e
	2e 31 34 35 32 31 2e 35
	38

EXERCISE 3F: APPLICATION PDU

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

Message	Singh Jasraj, A29, /172.21.145.58

Is this the message that you have sent? Yes