Student Name : Jden Goh

Group : SCS4

Date : 26 Feb 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:C9:AE	10.96.184.132	00 00 0C 9F F0 F0	155.69.3.8	DNS request
2.	CC:B6:C8:85:4E:CB	155.69.3.8	A4:BB:6D:61:C9:AE	10.96.184.132	DNS reply
3.	A4:BB:6D:61:C9:AE		FF:FF:FF:FF:FF:FF		ARP request
4.	00 00 0C 9F F0 F0		A4:BB:6D:61:C9:AE		ARP reply
5.	A4:BB:6D:61:C9:AE	10.96.184.132	00 00 0C 9F F0 F0	155.69.100.96	Quote of the day request
Last.	CC:B6:C8:85:5A:37	155.69.100.96	A4:BB:6D:61:C9:AE	10.96.184.132	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 c9 ae 08 00 45 00
	00 44 bb a3 00 00 80 11
	00 00 0a 60 b8 84 9b 45
	03 08 d0 08 00 35 00 30
	83 04 09 e2 01 00 00 01
	00 00 00 00 00 00 06 68
	77 6c 61 62 31 04 73 63
	73 65 03 6e 74 75 03 65
	64 75 02 73 67 00 00 01
	00 01

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
It carries the IPv4 protocol.

How do you know?
The ethernet protocol type frame has value of 0x0800, which indicates that the frame is carrying an IPV4 packet.

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

Destination Address	00:00:0c:9f:f0:f0
Source Address	a4:bb:6d:61:c9:ae
Protocol	08 00 (IPv4)
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 35 f0 fc 00 00
	80 11 00 00 0a 60 b8 84
	9b 45 64 60 f8 85 00 11
	00 21 37 cf 4a 64 65 6e
	2c 20 53 43 53 34 2c 20
	31 30 2e 39 36 2e 31 38
	34 2e 31 33 32

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?
It carries the User Datagram Protocol (UDP).
The field protocol has value 0x11, which is UDP protocol.

Does the captured IP header have the field: Options + Padding? How do you know?
No. There are no bits after destination address in the IP datagram, before the data packet. This shows no bits were used for Options + Padding.

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

Version	4
Total Length	53
Identification	0xf0fc (61692)
Flags (interpret the meanings)	0x0 1st bit -> reserved bit, not set 2nd bit -> don't fragment, not set
Fragment Offset	0
Protocol	UDP (17)
Source Address	10.96.184.132
Destination Address	155.69.199.96
Packet Data (8 bytes in a row, in hexadecimal)	4a 64 65 6e 2c 20 53 43
	53 34 2c 20 31 30 2e 39
	36 2e 31 38 34 2e 31 33
	32

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	63621 (0xf885)
Destination Port	17 (0x0011)
Length	33 (0x0021)
Data (8 bytes in a row, in hexadecimal)	4a 64 65 6e 2c 20 53 43
	53 34 2c 20 31 30 2e 39
	36 2e 31 38 34 2e 31 33
	32

EXERCISE 3F: APPLICATION PDU

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

Message	Jden, SCS4, 10.96.184.132

Is this the message that you have sent? Yes!