Student Name : Shen Chihao

Group : SCS4

Date : 26/02/2024

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:d7:9f	10.96.181.107	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:d7:9f	10.96.181.107	DNS response
3.	a4:bb:6d:61:d7:9f	-	ff:ff:ff:ff:ff:ff	-	ARP request
4.	cc:b6:c8:85:5a:37	-	a4:bb:6d:61:d7:9f	-	ARP response
5.	a4:bb:6d:61:d7:9f	10.96.181.107	00:00:0c:9f:f0:f0	155.69.100.96	UDP request
6.	cc:b6:c8:85:5a:37 QOTD server	155.69.100.96	a4:bb:6d:61:d7:9f Your QotdClient	10.96.181.107	UDP response: 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 d7 9f 08 00 45 00
	00 3c c5 39 00 00 80 11
	00 00 0a 60 b5 6b 9b 45
	64 60 d8 d5 00 11 00 28
	68 02 53 68 65 6e 20 43
	68 69 68 61 6f 2c 20 53
	43 53 34 2c 20 31 30 2e
	39 36 2e 31 38 31 2e 31
	30 37

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
The type of upper layer data is IPv4.

How do you know?
Because the Ether Protocol Type captured in the frame is 0x0800, which is corresponding to the IPv4 protocol.

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

Destination Address	00:00:0c:9f:f0:f0
Source Address	a4:bb:6d:61:d7:9f
Protocol	0x0800
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 3c c5 39 00 00
	80 11 00 00 0a 60 b5 6b
	9b 45 64 60 d8 d5 00 11
	00 28 68 02 53 68 65 6e
	20 43 68 69 68 61 6f 2c
	20 53 43 53 34 2c 20 31
	30 2e 39 36 2e 31 38 31

	2e 31 30 37

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?
The type of upper layer data is UDP. Since the Protocol field captured in the IP packet is 0x11, which is corresponding to the UDP protocol.

Does the captured IP header have the field: Options + Padding? How do you know?
No Options + Padding field. Because the IHL field is 0x5, which means the IP header is 20 bytes long. The Options field requires extra offset, which needs IP header to be larger than 20 bytes, so no space for the Options field. Since 20 bytes is 160 bits, which is the multiple of 32 bits, so no need for additional Padding field.

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

Version	4
Total Length	0x003c (60 bytes)
Identification	0xc539
Flags (interpret the meanings)	0x0 Meanings:
Fragment Offset	0x000
Protocol	0x11 (17 (UDP))
Source Address	0a 60 b5 6b (10.96.181.107)
Destination Address	9b 45 64 60 (155.69.100.96)
Packet Data (8 bytes in a row, in hexadecimal)	d8 d5 00 11 00 28 68 02
	53 68 65 6e 20 43 68 69
	68 61 6f 2c 20 53 43 53
	34 2c 20 31 30 2e 39 36
	2e 31 38 31 2e 31 30 37

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	d8 d5 (Port 55509)

Destination Port	00 11 (Port 17)
Length	00 28 (40 bytes)
Data (8 bytes in a row, in hexadecimal)	53 68 65 6e 20 43 68 69
	68 61 6f 2c 20 53 43 53
	34 2c 20 31 30 2e 39 36
	2e 31 38 31 2e 31 30 37

EXERCISE 3F: APPLICATION PDU

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

Message	Shen Chihao, SCS4, 10.96.181.107

Is this the message that you have sent?
Yes.