Student Name : Chew Di Heng

Group : SCS2

Date : 28/2/2024

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:d6:5e	10.96.187.27	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:d6:5e	10.96.187.27	DNS response
3.					
4.					
5.	a4:bb:6d:5f:cb:63	10.96.178.43	00:00:0c:9f:f0:f0	155.69.100.96	Quote of the day request
Last.	cc:b6:c8:85:4e:cb	155.69.100.96	a4:bb:6d:61:d6:5e	10.96.178.43	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 d6 5e 08 00 45 00
	00 34 ec 64 00 00 80 11
	00 00 0a 60 bb 1b 9b 45
	64 60 f4 0b 00 11 00 20
	c6 fa 48 65 6c 6c 6f 20
	53 65 72 76 65 72 31 30
	2e 39 36 2e 31 38 37 2e
	32 37

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying? IPv4.
How do you know? Row 2 of EXERCISE 3B "08 00" represents the ether type field to be IPv4.

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

Destination Address	a4:bb:6d:61:d6:5e
Source Address	00:00:0c:9f:f0:f0
Protocol	IPv4
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 2e fa d0 00 00
	80 11 00 00 0a 60 b2 2b
	9b 45 64 60 cf 55 00 11
	00 1a 6e 6b 53 43 53 33
	2c 20 31 30 2e 39 36 2e
	31 37 38 2e 43 33

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?
UDP, 0x11 refers to the UDP protocol used.

Does the captured IP header have the field: Options + Padding? How do you know?
The IHL field is set to 5 which represents 20 bytes, this is the minimum size length of a ip datagram without options and padding added.

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

Version	0x4 (Version 4)
Total Length	0x0034 (52)
Identification	0xec64 (60516)
Flags (interpret the meanings)	0x00 Reserved Bit: Not Set, this bit is used for future expansion and by setting it to 0, it ensures that the bit is not misused. Don't fragment bit: Not set, this means that the packet can be fragmented if necessary if it exceeds the MTU size. More fragment bit: Not set, this could mean that the packet is the last fragment or the only packet.
Fragment Offset	0x00
Protocol	0x11
Source Address	10.96.187.27
Destination Address	155.69.100.96
Packet Data (8 bytes in a row, in hexadecimal)	f4 0b 00 11 00 20 c6 fa
	48 65 6c 6c 6f 20 53 65
	72 76 65 72 31 30 2e 39
	36 2e 31 38 37 2e 32 37

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	0xf40b (62475)
Destination Port	0x0011 (17)
Length	0x0020 (32)
	48 65 6c 6c 6f 20 53 65

Data (8 bytes in a row, in hexadecimal)	72 76 65 72 31 30 2e 39
	36 2e 31 38 37 2e 32 37

EXERCISE 3F: APPLICATION PDU

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

Message	Hello Server 10.96.187.27

Is this the message that you have sent?

Yes