Student Name : Bryan Lu We Zhern

Group : A52

Date : 16/3/2023

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:D7:65	172.21.144.251	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:D7:65	172.21.144.251	DNS Response
3.	A4:BB:6D:61:D7:65	172.21.144.251	FF:FF:FF:FF:FF:FF	172.21.148.201	ARP Request
4.	FE:96:8F:0F:DC:64	172.21.148.201	A4:BB:6D:61:D7:65	172.21.144.251	ARP Response
5.	A4:BB:6D:61:D7:65	172.21.144.251	FE:96:8F:0F:DC:64	172.21.148.201	UDP Request
6.	FE:96:8F:0F:DC:64 *QOTD Server*	172.21.148.201	A4:BB:6D:61:D7:65 *Your QotdClient*	172.21.144.251	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: 172.32.248.201

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 D7 65 08 00 45 00
	00 42 E5 AD 00 00 80 11
	00 00 AC 15 90 FB AC 15
	94 C9 DA 26 00 11 00 2E
	A0 8F 42 72 79 61 6E 20
	4C 75 20 57 65 20 5A 68
	65 72 6E 2C 20 41 35 32

	2C 20 31 37 32 2E 32 31
	2E 31 34 34 2E 32 35 31

EXERCISE 3C: DATA LINK PDU - ETHERNET FRAME

What type of upper layer data is the captured ethernet frame carrying?
The Ethernet Frame is carrying IPv4 Protocol

How do you know?
The 2 bytes captured at the ethernet protocol type frame is 0x0800. This means that the frame is carrying an IPv4 packet. Hence, it must be carrying the internet protocol.

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

Destination Address	FE:96:8F:0F:DC:64
Source Address	A4:BB:6D:61:D7:65
Protocol	0x0800 (IPv4)
Frame Data (8 bytes in a row, in hexadecimal)	45 00 00 42 E5 AD 00 00
	80 11 00 00 AC 15 90 FB
	AC 15 94 C9 DA 26 00 11
	00 2E A0 8F 42 72 79 61
	6E 20 4C 75 20 57 65 20
	5A 68 65 72 6E 2C 20 41
	35 32 2C 20 31 37 32 2E
	32 31 2E 31 34 34 2E 32
	35 31

EXERCISE 3D: NETWORK PDU - IP DATAGRAM

What type of upper layer data is the captured IP packet carrying? How do you know?

It is carrying the User Datagram Protocol (UDP). The field protocol is identified as UDP (0x11), hence UDP.

Does the captured IP header have the field: Options + Padding? How do you know?
No Options & Padding field

No options because the Internet Header Length (IHL) is 5 (20 bytes). Having options require an additional offset to the IHL, which then needs to be larger than 20 bytes. Since IHL is 20 bytes, so there is no space to include them in the header.

No padding because the IP header is 160 bits long, which is a factor of 32 bits and thus doesn’t require any additional padding.

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

Version	4
Total Length	66

Identification	0xE5AD
Flags (Interpret the meanings)	0b000 MSB bit: Reserved Bit not set Middle bit: Don't Fragment not set LSB bit: More Fragments not set
Fragment Offset	0
Protocol	UDP (17)
Source Address	AC 15 90 FB (172.21.144.251)
Destination Address	AC 15 94 C9 (172.21.148.201)
Packet Data (8 bytes in a row, in hexadecimal)	DA 26 00 11 00 2E A0 8F
	42 72 79 61 6E 20 4C 75
	20 57 65 20 5A 68 65 72
	6E 2C 20 41 35 32 2C 20
	31 37 32 2E 32 31 2E 31
	34 34 2E 32 35 31

EXERCISE 3E: TRANSPORT PDU - UDP DATAGRAM

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

Source Port	0xDA26 (55846)
Destination Port	0x0011 (17)
Length	0x002E (46)
Data (8 bytes in a row, in hexadecimal)	42 72 79 61 6E 20 4C 75
	20 57 65 20 5A 68 65 72
	6E 2C 20 41 35 32 2C 20
	31 37 32 2E 32 31 2E 31
	34 34 2E 32 35 31

EXERCISE 3F: APPLICATION PDU

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

Message	Bryan Lu We Zhern, A52, 172.21.144.251

Is this the message that you have sent? Yes