Quick Savajiyani(A20451378)
Ninad Parikh(A20427382)
Jay Rodge(A20418613)

CS 542
HW2

1.(4 points) Consider the three hosts A, B and C, and a router running a proxy ARP for them (see the table below). The router has received an ARP request for host C from a host with IP address 114.5.7.89, and physical address 457342ACAE32. Show an ARP reply packet. <u>Fill in all its required fields.</u> Consider the Ethernet as a hardware type.

	IP address	Physical address
Host A	141.23.56.21	A46EF45983AB
Host B	141.23.56.22	A46EF45983BC
Host C	141.23.56.23	A46EF45983CD
Router	114.5.7.95	A46EF45983DE

Ans:

ARP Reply Packet:

<table>
<tr><td colspan="2">0x0001</td><td>0x0800</td></tr>
<tr><td>0x06</td><td>0x04</td><td>0x0002</td></tr>
<tr><td colspan="3">0xA46EF45983DE</td></tr>
<tr><td colspan="3">0x8D173817 (141.23.56.23)</td></tr>
<tr><td colspan="3">0x457342ACAE32</td></tr>
<tr><td colspan="3">0x72050759 (114.5.7.89)</td></tr>
</table>

DATA FRAME:

Preamble and SFD	0x457342ACAE32	0xA46EF45983DE	0X0806	ARP Reply Packet (As shown above	CRC

https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/13718-5.html -- As per the site, the target logical address does not need to be changed to the proxy router's logical address. It should be that of the host C.

Quick Savajiyani(A20451378)
Ninad Parikh(A20427382)
Jay Rodge(A20418613)

2.(6 points) Consider the just updated ARP cache table (see below) at time t. At *t*+65 s the input module received an ARP reply from the host with IP address 19.1.7.82. The ARP package received only 2 packets in the interval (*t, t+68* s). Identify these packets and give the updated cache table at time *t*+68 s. The cache table is updated every 4 seconds. Assume *MAX_ATTEMPTS*=21, and the initial value of *TIME_OUT*=1000. Explain your answer.

State	*Queue*	*Attempt*	*Time-Out*	*Protocol Addr.*	*Hardware Addr.*
R	5		900	180.3.6.1	ACAE32457342
P	2	2		129.34.4.8	
P	14	5		201.11.56.7	
R	8		450	114.5.7.89	457342ACAE32
P	12	1		220.55.5.7	
F					
R	9		60	19.1.7.82	4573E3242ACA
P	18	3		188.11.8.71	

Ans:
a) Since the cache table is updated every 4 seconds, the last update would have been at t+68 within the timeframe (t, t+68). The total number of updates would have been 68/4 =17.
b) For all the pending records in the cache table, the number of attempts would increase by 17. Since the record for 201.11.56.7, the time-out exceeds the max value of 21, it turned to free state.
c) For all the resolved records in the cache table, the time-out would decrease by 68 seconds. For the record 19.1.7.82, the time-out would have been 0 at t+60 s which would have turned to free state.
d) Since the above record would not be there at t + 65 s, the ARP reply from 19.1.7.82 would have created a new record entry in the cache table with resolved state and reinitialized time-out.
e) Since the ARP Package received only two packets in the interval (t, t+68), one could have been an IP packet for destination 19.1.7.82 at the output module for address resolution which could have been sent out after t+60 s while the other would be the ARP reply it got at t+65 s.
f) Below is the updated cache table at t+68 s.

State	Queue	Attempt	Time-Out	Protocol Address	Hardware Address

Quick Savajiyani(A20451378)
Ninad Parikh(A20427382)
Jay Rodge(A20418613)

R	5		832	180.3.6.1	ACAE32457342
P	2	19		129.34.4.8	
F					
R	8		382	114.5.7.89	457342ACAE32
P	12	18		220.55.5.7	
R	23		997	19.1.7.82	4573E3242ACA
F					
P	18	20		188.11.8.71	

3.(2 points) In an IP packet, the value of HLEN is C, and the value of Total Length is 00AA. How many bytes of data is this packet carrying? Are there any options? If so,what is the length of these options? (The above values are given in the hexadecimal format.)

Ans: HLEN $(C)_{16} = (12)_{10}$ = 12*4 = 48 bytes
Total Length: $(00AA)_{16} = (170)_{10}$

Data = Total Length - Header
= 170 - 48
= 122 bytes

Therefore, it is carrying 122 bytes of data

Header Length = 48 = (20+28)
= (Base Header + Options)
Yes, there are options and 28 bytes is the length of these options

4.(3 points) An IP fragment has arrived with the first few hexadecimal digits shown below:

4500002C03B12367......

What is the offset of the next fragment?

For This question we will need header length, total length and the offset of this fragment.
Header Length - 5 * 4 = 20
Total length = 002C in Hexadecimal to Decimal - 44
Offset is 367 in hexadecimal the last 13 bits. which is 871 in decimal.

Quick Savajiyani(A20451378)
Ninad Parikh(A20427382)
Jay Rodge(A20418613)

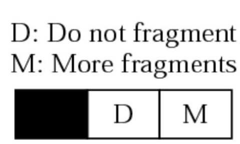
To get the starting value of the fragment we need to multiply the offset by 8
871 *8 = 6968
And to get the last value of the fragment we will add the total data to the starting value of fragment which is 6968
Total data = Total length - Header length
= 44-20 = 24
6968 + 24 - 1 = 6991
So the range of data in this fragment is 6998 to 6991
To get the offset of the next segment we will need the first data value of that segment which is 6992 and we divide it by 8
6992/8 = 874 is the offset of the next fragment.

5.(2 points) An IP packet has arrived with a *D* bit value of 1. What is an *M* bit value of this packet? What is the fragmentation offset value?
Ans: The D bit with 1 signifies, ‘Do not Fragment’ i.e the data is continuous, therefore the value of M bit will be 0. Since this is single fragment and would be starting from 0, the offset value will also be 0.

6.(2 points) What is the difference between a socket address and an IP address? We can identify a host by an IP address. Do we need a socket address?
Ans: A Socket address is a combination of IP address and port number of client or server, and it is used to uniquely identify client and server processes. While IP address is used for representing a host or client/server in a network.
If we need to communicate with a client/server process, then socket address is required, since IP address in socket address will help to getting to the host and port number in socket address will help us to get to the specific required process.

7.(2 points) Which protocol is faster: TCP or UDP? Why?
Ans: UDP is faster than TCP, and the reason is that its non-existent acknowledgement packet (ACK) that allows to make a continuous packet stream, rather than TCP accepting a set of packets, measured using the TCP window size and round trip time (RTT).

8.(3 points) Which fields change in an IP base header due to fragmentation?
Ans: The following field change in IP base header
Flags (3 bits):



Quick Savajiyani(A20451378)
Ninad Parikh(A20427382)
Jay Rodge(A20418613)

Total Length: As we fragment the main packet the total length gets distributed among the fragments. The total length will change accordingly and its is suppose to be less than or equal to the value mentioned in the MTU.

More fragments (MF = 1 bit) it tells if more fragments ahead of this fragment i.e. if MF = 1, more fragments are ahead of this fragment and if MF = 0, it is the last fragment.

Fragmentation Offset (13 bits):
It is used to identify sequence of fragments in the frame. It generally indicates the number of data bytes preceeding or ahead of the fragment.
Maximum fragment offset possible = (65535 – 20) – 1 = 65514
{where 65535 is maximum size of datagram and 20 is minimum size of IP header}
So, we need ceil(log265514) = 16 bits for fragment offset but fragment offset field has only 13 bits. So, to represent efficiently we need to scale down fragment offset field by 216/213 = 8 which acts as a scaling factor. Hence, all fragments except the last fragment should have data in multiples of 8 so that fragment offset ∈ N.

9.(2 points) Can an original IP datagram reach the destination if one of its fragments is lost?
Ans: The different fragments of a single IP datagram can arrive in any order to the destination system. When one of its fragments of an IP datagram are lost, then the entire IP datagram is discarded after a timeout period.

10.(2 points) What is the importance of the TCP sequence number and acknowledgment number?
Ans: The fields of sequence and acknowledgment are two of the many features that allow us to define TCP as a connection-oriented protocol. As such, when data is sent via a TCP connection, they help remote hosts keep track of the connection and make sure that no packet is lost on the way to their destination.
The sequence number defines the number assigned to the first data byte contained in that segment whereas the acknowledgement number defines the number of the next byte a party expects to receive, and it’s cumulative.

11.(2 points) Why does the *rwnd* change during a TCP data transfer phase?
Ans: To achieve flow control, TCP forces the sender and the receiver to adjust their window sizes, although the size of the buffer for both parties is fixed when the connection is established. The receive window closes (move it’s right wall to the right) when more bytes are pulled by the process.
The send window closes (move its left wall to the right) when the receive window size(rwnd) advertised by the receiver allows it to do so.

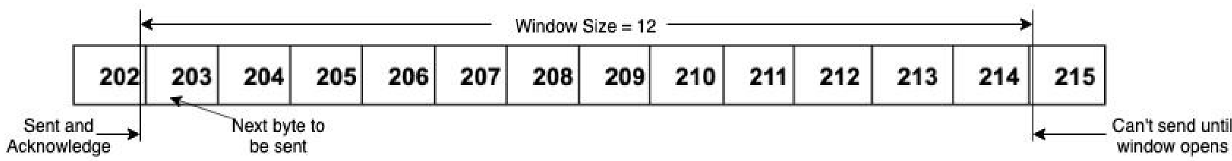
Quick Savajiyani(A20451378)
Ninad Parikh(A20427382)
Jay Rodge(A20418613)

The receiver window cannot shrink. But he send window can shrink (it's right wall moves to the left) if the receiver defines a value for rwnd that results in shrinking the window.

12.(3 points) The TCP values of *rwnd* and *cwnd* are 15 and 12, respectively. The acknowledgment number received is 203. Draw a diagram showing this window. Then a segment with new acknowledgment number 207 and a new *rwnd* size was received. What is the minimum of this new rwnd size to avoid shrinking the window? *cwnd* is still 12.

Ans:

ACK = 203, Window Size = min(rwnd,cwnd) = min(15,12) = 12



The minimum size of the new rwnd is 12 to avoid shrinking the window.

If the new minimum size for **rwnd** is 12, following diagram shows this window: