Wireshark Lab 5: Ethernet and ARP

Group Details:

Leting Ni 1006255446 Yuhe Chen 1005689480

Mark:

	Question	Answer
1	What is the 48-bit Ethernet address	00:d0:59:a9:3d:68
	of your computer?	
Annotated	Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9 > Destination: LinksysG_da:af:73 (00:06:25:da:a-	:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Screenshot (if needed)	> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	
	Type: IPv4 (0x0800)	00.06.25.1£.72
2	What is the 48-bit destination	00:06:25:da:af:73
	address in the Ethernet frame?	Triada addisor of man Triadassa acceptan
	X714 -1	It is the address of my Linksys router
	What device has this as its Ethernet address?	(gateway to get off my subnet).
	Ethernet address?	
Annotated	Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)	
Screenshot	> Destination: LinksysG_da:af:73 (00:06:25:da:a	f:73)
(if needed)	<pre>> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Type: IPv4 (0x0800)</pre>	
3	Give the hexadecimal value for the	0x0800
	two-byte Frame type field.	
		It corresponds to IPv4.
	What upper layer protocol does this	
	correspond to?	
Annotated Screenshot	> Destination: LinksysG_da:af:73 (00:06:25:da:a-	:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73) f:73)
(if needed)	> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)	
4	How many bytes from the very start	54 bytes
'	of the Ethernet frame does the	3 Toytes
	ASCII "G" in "GET" appear in the	
	Ethernet frame?	
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
Annotated		3d 68 08 00 45 00 ··%··s·· Y·=h··E·
Screenshot		c0 a8 01 69 80 77 ····@··· ···i·w ac a5 3f b4 50 18 ···"·Pe· ····?·P·
(if needed)		2f 65 74 68 65 72 ···~O·· GE T /ether
	0040 65 61 6c 2d 6c 61 62 73 2f 48	54 54 50 2d 65 74 eal-labs /HTTP-et
	0050 68 65 72 65 61 6c 2d 6c 61 62	2d 66 69 6c 65 33 hereal-l ab-file3

5	What is the value of the Ethernet source address? What device has this as its Ethernet	00:06:25:da:af:73 It is the address of my Linksys router (gateway to get onto my subnet).
	address?	
Annotated Screenshot (if needed)	Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da: > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68 (00:d0:59:a9:a9:3d:68 (00:d0:59:a9:a0:a0:d0:59 (00:d0:59:a9:a0:d0:59 (00:d0:59	af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
6	What is the destination address in the Ethernet frame?	00:d0:59:a9:3d:68 Yes, it is the Ethernet address of my
	Is this the Ethernet address of your computer?	computer.
Annotated Screenshot (if needed)	Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da: > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3c) > Source: LinksysG_da:af:73 (00:06:25:da:af:73) Type: IPv4 (0x0800)	
7	Give the hexadecimal value for the two-byte Frame type field.	0x0800
	What upper layer protocol does this correspond to?	It corresponds to IPv4.
Annotated Screenshot (if needed)	Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da: > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d: > Source: LinksysG_da:af:73 (00:06:25:da:af:73) Type: IPv4 (0x0800)	af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
8	How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?	67 bytes
Annotated Screenshot (if needed)	0010 05 dc 8f 2f 40 00 37 06 76 f7 0020 01 69 00 50 04 22 ac a5 3f b4 0030 1b 28 5e d0 00 00 48 54 54 50 0040 30 30 20 4f 4b 0d 0a 44 61 74 0050 2c 20 32 38 20 41 75 67 20 32	af 73 08 00 45 60Y.=h%sE` 80 77 f5 0c c0 a8/@.7. vw 65 14 9c 1f 50 10 .i.P."?.eP. 2f 31 2e 31 20 32 .(^HT TP/1.1 2 65 3a 20 53 61 74 00 0KD ate: Sat 30 30 34 20 31 37 , 28 Aug 2004 17 0d 0a 53 65 72 76 :19:37 G MTServ
9	Write down the contents of your computer's ARP cache.	Contents: see screenshot below.
	What is the meaning of each column value?	Internet Address: IP address Physical Address: MAC address Type: protocol type

Annotated	<pre>C:\Users\nilet>arp -a</pre>	
Screenshot (if needed)	Interface: 100.64.75.69 0x11 Internet Address Physical Add 100.64.64.1 70-b3-17-c4- 100.64.64.19 08-35-71-ee- 100.64.71.227 70-bc-10-d1- 224.0.0.22 01-00-5e-00- 224.0.0.251 01-00-5e-00- 224.0.0.252 01-00-5e-00- 239.255.255.250 01-00-5e-7f- 255.255.255.255 ff-ff-ff-ff-	55-9f dynamic cd-87 dynamic cb-dd dynamic 00-16 static 00-fb static 00-fc static ff-fa static
10	What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?	Source: 00:d0:59:a9:3d:68 Destination: ff:ff:ff:ff:ff
Annotated Screenshot (if needed)	Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff) > Destination: Broadcast (ff:ff:ff:ff:ff) > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Type: ADD (0:0000)	
11	Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?	0x0806 It corresponds to ARP.
Annotated Screenshot (if needed)	Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff) > Destination: Broadcast (ff:ff:ff:ff:ff) > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Type: ARP (0x0806)	
12.a	How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?	20 bytes
Annotated Screenshot (if needed)		3d 68 08 06 00 01
12.b	What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?	0x0001

Annotated	∨ Address Resolution Protocol (request)		
Screenshot	Hardware type: Ethernet (1)		
(if needed)	Protocol type: IPv4 (0x0800)		
	Hardware size: 6		
	Protocol size: 4		
	Opcode: request (1)		
	0000 ff ff ff ff ff oo do 59 a9 3d 68 08 06 00 01 ······ Y·=h····		
	0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 ···································		
10 -	 		
12.c	Does the ARP message contain the Yes.		
	IP address of the sender? 192.168.1.105		
Annotated	Address Resolution Protocol (request)		
Screenshot	Hardware type: Ethernet (1)		
(if needed)	Protocol type: IPv4 (0x0800) Hardware size: 6		
	Protocol size: 4		
	Opcode: request (1)		
	Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		
	Sender IP address: 192.168.1.105		
	Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)		
	Target IP address: 192.168.1.1		
12.d	Where in the ARP request does the The Target MAC address is set to		
	"question" appear – the Ethernet 00:00:00:00:00. This will query		
	address of the machine whose the machine whose corresponding IP		
	corresponding IP address is being address is 192.168.1.1.		
	queried?		
	querieu.		
Annotated	Address Resolution Protocol (request)		
Screenshot	Hardware type: Ethernet (1)		
(if needed)	Protocol type: IPv4 (0x0800)		
	Hardware size: 6		
	Protocol size: 4		
	Opcode: request (1)		
	Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Sender IP address: 192.168.1.105		
	Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00)		
	Target IP address: 192.168.1.1		
13.a	How many bytes from the very 20 bytes		
	beginning of the Ethernet frame		
	does the ARP opcode field begin?		
	does the rife opeode field begin.		
Annotated	∨ Address Resolution Protocol (reply)		
Screenshot	Hardware type: Ethernet (1)		
(if needed)	Protocol type: IPv4 (0x0800) Hardware size: 6		
(== === 3 4 2 4)			
	Protocol size: 4		
	Opcode: reply (2)		
	0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01 ··Y·=h·· %··s···		
	0010 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01 ································		
	0030 00 00 00 00 00 00 00 00 00 00 00 00		
L	1		

13.b	What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?	0x0002
Annotated Screenshot (if needed)	<pre> Address Resolution Protocol (reply Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) </pre>	
13.c	Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?	The Sender MAC address 00:06:25:da:af:73 and the Sender IP address 192.168.1.1 is the answer to the earlier ARP request.
Annotated Screenshot (if needed)	Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73) Sender IP address: 192.168.1.1 Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Target IP address: 192.168.1.105	
14	What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?	Source: 00:06:25:da:af:73 Destination: 00:d0:59:a9:3d:68
Annotated Screenshot (if needed)	Ethernet II, Src: Linksys6_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) > Source: Linksys6_da:af:73 (00:06:25:da:af:73) Type: ARP (0x0806) Padding: 000000000000000000000000000000000000	
15	Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?	The ARP request is broadcast, but the ARP reply is not broadcast and sent directly to the computer that sent the request. Therefore, we cannot see the ARP reply in this trace.
Annotated Screenshot (if needed)		