Wireshark Lab 5: Ethernet and ARP

Group Details: Bikramjit Narwal (1005242300), Chao Glen Xu (1004274634)

Mark:

	Question	Answer
1	What is the 48-bit Ethernet address of your computer?	00:d0:59:a9:3d:68
Annotated Screenshot (if needed)	Wirehark: Packet 4- ethermet-ethereal-trace-1	
2	What is the 48-bit destination address in the Ethernet frame? What device has this as its Ethernet address?	00:09:25:da:af:73
Annotated Screenshot (if needed)	Wirshark - Packet 4 - ethernet - ethereal-trace-1	
3	Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?	The hexadecimal value for the two- byte Frame type field is 0x0800. It corresponds to Internet Protocol version 4.

	■ 100 1 1 10 11 11 11 11 11 11 11 11 11 1		
Annotated Screenshot	> Frame 4: 62 bytes on wire (496 bits)), 62 bytes captured (496 bits)	
(if needed)	V Destination: LinksysG_da:af:73 (@ Address: LinksysG_da:af:73 (@	0:06:25:da:af:73)	
	0 V Source: AmbitMic_a9:3d:68 (00:d0:		
	Address: AmbitMit_m3:346(80:d0:99:a9:3468)o. = LG bit: Globally unique address (factoryo = T6 bit: Individual address (unicast)		
	Type: IPV4 (0x0800) > Data (46 bytes)		
4	How many bytes from the years start	After 122 hits (54 haytes) the C in set	
4	How many bytes from the very start of the Ethernet frame does the	After 432 bits (54 bytes) the G in get	
	ASCII "G" in "GET" appear in the	appears.	
	Ethernet frame?		
	Butternet frame.		
Annotated			
Screenshot			
(if needed)	What is the value of the Ethernet	The value of the Ethernet source	
	source address?	address is 00:06:25:da:af:73.	
	source address.	address is 00.00.23.da.ai.73.	
	What device has this as its Ethernet	The device that has this as its	
	address?	Ethernet address is my router.	
		,	
Annotated		(00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68	
Screenshot (if needed)	✓ Destination: AmbitMic_a9:3d:68 (00 Address: AmbitMic_a9:3d:68 (00	:d0:59:a9:3d:68)	
(II liceded)	0		
	0 = LG bit: Globally unique address (factory0 = IG bit: Individual address (unicast) Type: IPv4 (0x0800)		
	> Data (48 bytes)		
6	What is the destination address in	The destination address is	
	the Ethernet frame?	00:d0:59:a9:3d:68. It is the address of	
	Is this the Ethernet address of your	my computer.	
	Is this the Ethernet address of your		
	computer?		
Annotated	> Frame 8: 62 bytes on wire (496 bits)		
Screenshot	✓ Destination: AmbitMic_a9:3d:68 (0		
(if needed)	Address: AmbitMic_a9:3d 68 (00:d0:59:a9:3d:68)0 = LG bit: Globally unique address (factory0 = TG bit: Individual address (unicast)		
	✓ Source: LinksysG_da:af:73 (00:06: Address: LinksysG_da:af:73 (00	25:da:af:73)	
	0	= LG bit: Globally unique address (factory = IG bit: Individual address (unicast)	
	Type: IPv4 (0x0800) > Data (48 bytes)		
7	Give the hexadecimal value for the	The hexadecimal value for the two-	
	two-byte Frame type field.	byte Frame type field is 0x0800. It	
		corresponds to Internet Protocol	
	What upper layer protocol does this	version 4.	
	correspond to?		

Annotated Screenshot (if needed)	> Frame 8: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) > Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 > Destination: 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?	It appears after 52 bytes from the start of the Ethernet frame.
Annotated Screenshot (if needed)		
9	Write down the contents of your computer's ARP cache. What is the meaning of each column value?	The meaning of each column: Internet Address column contains the IP address, the Physical Address contains the MAC address, and the type indicates the protocol type.
Annotated Screenshot (if needed)	192.168.2.1 b8 192.168.2.255 ff 224.0.0.22 01 224.0.0.251 01 224.0.0.252 01 239.255.255.250 01	- 0xe ysical Address
10	What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?	Source: 00:80:ad:73:8d:ce Destination: ff:ff:ff:ff:ff
Annotated Screenshot (if needed)	Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) * Ethernet II	
11	Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this	The hexadecimal value for the two- byte Ethernet Frame type field is 0x0806. Refers to ADP.
	correspond to?	

	(400 bits) C0 bits and (400 bits)	-:	
Annotated	> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bytes) Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst:		
Screenshot	<pre>Destination: Broadcast (ff:ff:ff:ff:ff) Address: Broadcast (ff:ff:ff:ff:ff:ff)</pre>		
(if needed)	1 = LG bit: Locally administ		
	1		
12.a	How many bytes from the very	20 bytes from the very beginning of	
12.0	beginning of the Ethernet frame	the Ethernet frame.	
		the Ethernet Irame.	
1	does the ARP opcode field begin?		
Annotated			
Screenshot			
(if needed)	XXII		
12.b	What is the value of the opcode	The value of the opcode field within	
	field within the ARP-payload part	the ARP-payload part of the Ethernet	
	of the Ethernet frame in which an	frame in which an ARP request is	
	ARP request is made?	made is 1.	
Annotated	' Address Resolution Protocol (r		
Screenshot	Hardware type: Ethernet (1)		
(if needed)	Protocol type: IPv4 (0x0800 Hardware size: 6	9)	
(=======)	Protocol size: 4		
	Opcode: request (1)		
	Sender MAC address: CnetTec Sender IP address: 192.168.	ch_73:8d:ce (00:80:ad:73:8d:ce)	
		00 00:00:00 (00:00:00:00:00)	
	Target IP address: 192.168.		
12.c	Does the ARP message contain the	192.168.1.104	
12.0	IP address of the sender?	1,2.100.1.101	
Annotated	' Address Resolution Protocol (r	request)	
Screenshot	Hardware type: Ethernet (1)		
(if needed)	Protocol type: IPv4 (0x0800)		
(II liceded)	d) Hardware size: 6 Protocol size: 4		
	Opcode: request (1)		
	<u> </u>	ch_73:8d:ce (00:80:ad:73:8d:ce)	
	Sender IP address: 192.168.		
	Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.117		
12.d	Where in the ARP request does the	The field "Target Mac Address" is	
12.0		_	
	"question" appear – the Ethernet	00:00:00:00:00:00 to question the	
	address of the machine whose	machine whose corresponding IP	
	corresponding IP address is being	address is being queried.	
	queried?		
Annotated	' Address Resolution Protocol (r		
Screenshot	Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800		
(if needed)	Protocol type: IPv4 (0x0800) Hardware size: 6		
	Protocol size: 4		
	Opcode: request (1) Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)		
Sender IP address: 192.168.1.104			
	Target MAC address: 00:00:00:00 (00:00:00:00:00:00)		
	Target IP address: 192.168.1.117		
13.a	How many bytes from the very	20 bytes from the very beginning of	
	beginning of the Ethernet frame	the Ethernet frame.	
	does the ARP opcode field begin?		
Annotated	and the operation regime.	<u> </u>	
	I .		

Screenshot			
(if needed)			
13.b	What is the value of the opcode	It is 2.	
	field within the ARP-payload part		
	of the Ethernet frame in which an		
	ARP response is made?		
Annotated	Address Resolution Protocol (reply)		
Screenshot	Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800)		
(if needed)	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		
13.c	Where in the ARP message does the	192.168.1.1	
13.0	"answer" to the earlier ARP request	1/2.106.1.1	
	appear – the IP address of the		
	machine having the Ethernet		
	address whose corresponding IP		
	address whose corresponding if address is being queried?		
Annotated	Address Resolution Protocol (reply)	
Screenshot	Hardware type: Ethernet (1)	
(if needed)	Protocol type: IPv4 (0x0800 Hardware size: 6	0)	
	Protocol size: 4 Opcode: reply (2)		
	Sender MAC address: Linksy	sG_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	<u>Γ</u>	
14	What are the hexadecimal values	Source:	
	for the source and destination	00:06:25:da:af:73	
	addresses in the Ethernet frame	Destination:	
	containing the ARP reply message?	00:d0:59:a9:3d:68	
	Ethonnot II Specilinkeyes doubt.72 (00:06:25:do	35.72\ Det. AmbitMic 30.24.69 (AB.40.50.30.24.69)	
Annotated Screenshot	✓ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d	af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) l:68)	
(if needed)	Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:0= LG bit: Glo		
(ii needed)	0 = IG bit: Individual address (unicast)		
15	V Source: LinksysG_da:af:73 (00:06:25:da:af:73) Why is there no ARP reply (sent in	Why is there no ARP reply (sent in	
	response to the ARP request in	response to the ARP request in	
	packet 6) in the packet trace?	packet 6) in the packet trace because	
	packet of in the packet trace:	we are not in the machine that sent	
		the request. In addition, the ARP	
		=	
		request is broadcast. It's also known	
		that the ARP reply is sent back	
		straight to the senders (source's)	
Annotated		Ethernet address.	
Screenshot			
(if needed)			