

Vanessa Ulloa

Daniel Kushner

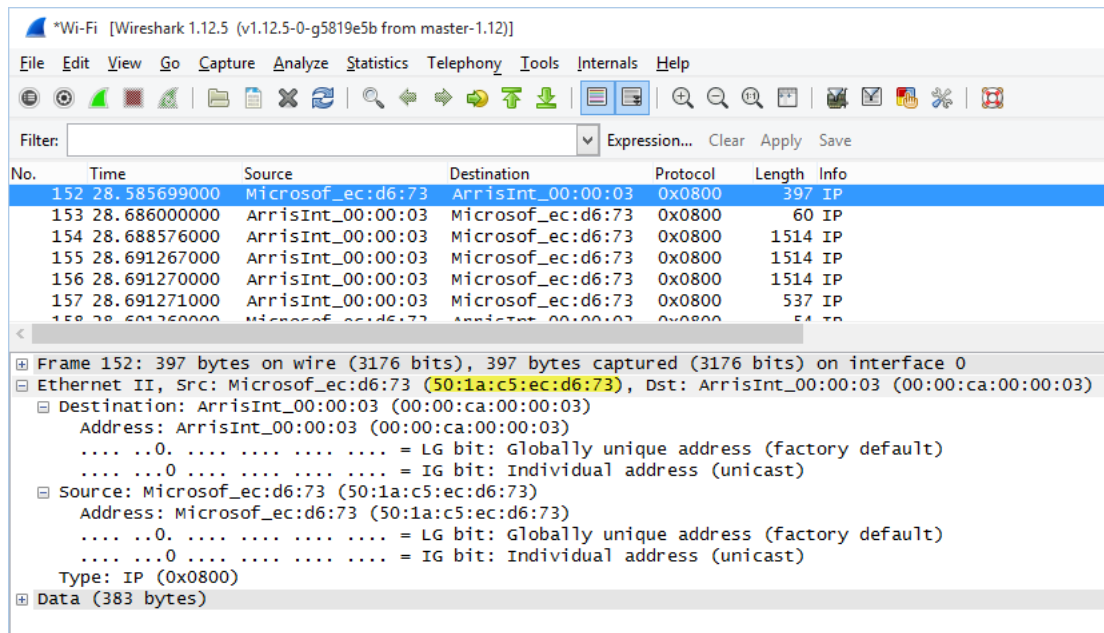
CST 311

16 June 2015

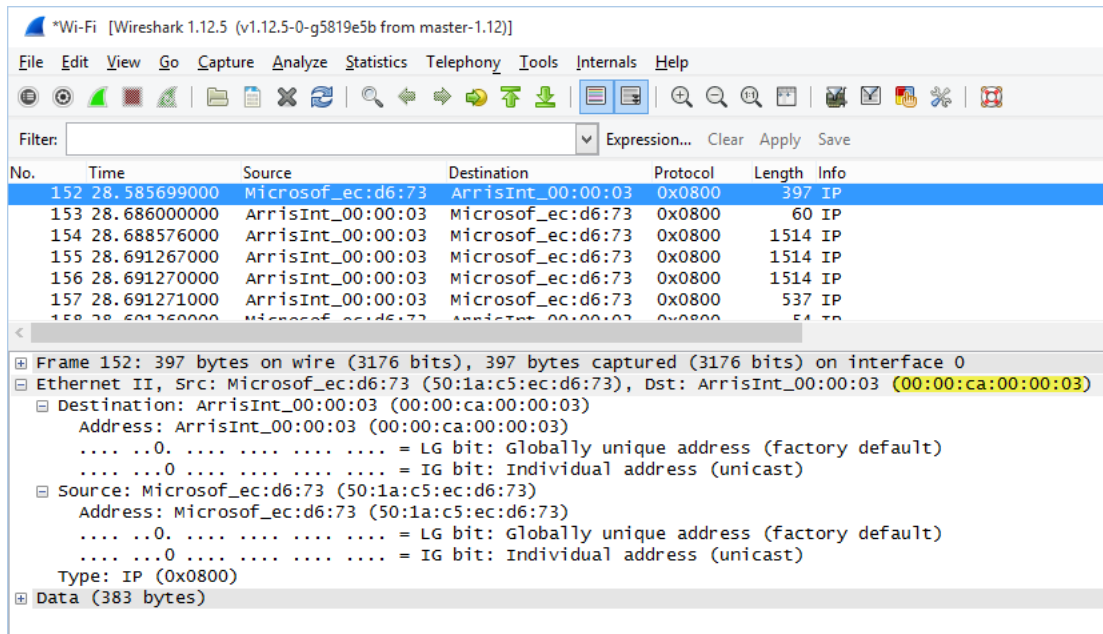
Lab 8

Capturing and analyzing Ethernet frames

1. What is the 48-bit Ethernet address of your computer?



- a. 50:1a:c5:ec:d6:73
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]



- 00:00:ca:00:00:03
 - Not the same address as gaia.cs.umass.edu but the router instead.
- Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
 - Type field: 0x0800
 - How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?
 - 54 bytes
 - What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

*Wi-Fi [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
157	28.691271000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	537	IP
158	28.691369000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	54	IP
159	28.789766000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	365	IP
160	28.796879000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	66	IP
161	28.814671000	Raspberr_62:f1:fe	IPv4mcast_fb	0x0800	170	IP
162	28.886000000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	540	IP

Frame 157: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0

Ethernet II, Src: ArrisInt_00:00:03 (00:00:ca:00:00:03), Dst: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)

- Destination: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
 - Address: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: ArrisInt_00:00:03 (00:00:ca:00:00:03)
 - Address: ArrisInt_00:00:03 (00:00:ca:00:00:03)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Type: IP (0x0800)
- Data (523 bytes)
 - Data: 4500020b9fc140002f066ef68077f50cc0a805090050f205...
 - [Length: 523]

a. 00:00:ca:00:03

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

*Wi-Fi [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
157	28.691271000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	537	IP
158	28.691369000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	54	IP
159	28.789766000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	365	IP
160	28.796879000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	66	IP
161	28.814671000	Raspberr_62:f1:fe	IPv4mcast_fb	0x0800	170	IP
162	28.886000000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	540	IP

Frame 157: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0

Ethernet II, Src: ArrisInt_00:00:03 (00:00:ca:00:00:03), Dst: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)

- Destination: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
 - Address: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Source: ArrisInt_00:00:03 (00:00:ca:00:00:03)
 - Address: ArrisInt_00:00:03 (00:00:ca:00:00:03)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
- Type: IP (0x0800)
- Data (523 bytes)
 - Data: 4500020b9fc140002f066ef68077f50cc0a805090050f205...
 - [Length: 523]

a. 50:1a:c5:ec:d6:73

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

a. 0x0800

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?

No.	Time	Source	Destination	Protocol	Length	Info
150	28.585188000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	66	IP
151	28.585347000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	54	IP
152	28.585699000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	397	IP
153	28.686000000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	60	IP
154	28.688576000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	1514	IP
155	28.691267000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	1514	IP
156	28.691270000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	1514	IP
157	28.691271000	ArrisInt_00:00:03	Microsof_ec:d6:73	0x0800	537	IP
158	28.691369000	Microsof_ec:d6:73	ArrisInt_00:00:03	0x0800	54	IP

Frame 154: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

Ethernet II, Src: ArrisInt_00:00:03 (00:00:ca:00:00:03), Dst: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)

Destination: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
Address: Microsof_ec:d6:73 (50:1a:c5:ec:d6:73)
.....0. = LG bit: Globally unique address (factory)
.....0. = IG bit: Individual address (unicast)

Source: ArrisInt_00:00:03 (00:00:ca:00:00:03)

Address: ArrisInt_00:00:03 (00:00:ca:00:00:03)
.....0. = LG bit: Globally unique address (factory)
.....0. = IG bit: Individual address (unicast)

Type: IP (0x0800)

Data (1500 bytes)

Data: 450005dc9f9be40002f066b288077f50cc0a805090050f205...

[Length: 1500]

0000	50 1a c5 ec d6 73 00 00	ca 00 00 03 08 00 45 00	P...S... ..E.
0010	05 dc 9f be 40 00 2f 06	6b 28 80 77 f5 0c c0 a8	...@./ k(w...
0020	05 09 00 50 f2 05 9a 24	af da b8 c5 cd d0 50 10	...P...\$P.
0030	00 7b 12 96 00 00 48 54	54 50 2f 31 2e 31 20 32	...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 54 75 65	00 OK..D ate: Tue
0050	2c 20 31 36 20 4a 75 6e	20 32 30 31 35 20 32 30	,_16_Jun 2015 20

a. 53 bytes

The Address Resolution Protocol

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

Administrator: Command Prompt

Microsoft Windows [Version 10.0.10130]
(c) 2015 Microsoft Corporation. All rights reserved.

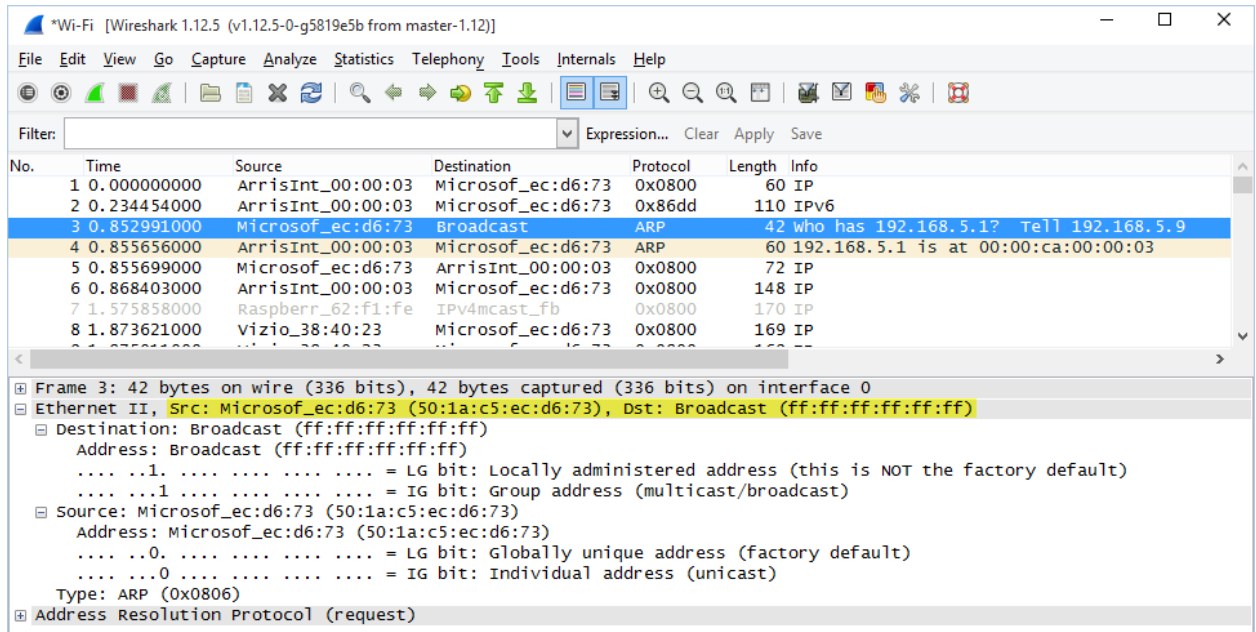
C:\WINDOWS\system32>arp -a

Interface: 192.168.5.9 --- 0xb		
Internet Address	Physical Address	Type
192.168.5.1	00-00-ca-00-00-03	dynamic
192.168.5.11	a4-ee-57-fe-3c-64	dynamic
192.168.5.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
224.0.0.253	01-00-5e-00-00-fd	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

C:\WINDOWS\system32>

a. Internet address = IP Address, Physical Address = MAC Address, type = protocol type.

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?



- a. Source: 50:1a:c5:ec:d6:73
 - b. Destination: ff:ff:ff:ff:ff:ff
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
 - a. 0x0806, ARP
 12. Download the ARP specification from <ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.
 - a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
 - i. 20 bytes
 - 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?
 - i. 0x0001
 - c. Does the ARP message contain the IP address of the sender?
 - i. Yes, the Sender IP Address (192.168.5.9)
 - d. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
 - i. The target MAC address = 00:00:00:00:00:00
 13. Now find the ARP reply that was sent in response to the ARP request.
 - a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
 - i. 20 bytes
 - 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?
 - i. 0x0002

- 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?
 - i. The Sender MAC address with the IP Address
- 14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
 - a. Source address: 00:00:ca:00:00:03
 - b. Destination address: 50:1a:c5:ec:d6:73
- 15. Open the ethernet-ethereal-trace-1 trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?
 - a. The reply is sent to the machine that sent the request, to the physical address.