

hw8

1. a) I will assume that the host has received its IP address and knows the IP address of the router since this process is usually done before ARP and the table is already filled
 1. Host looks at ARP table to get the MAC address for the first router (router 2) based on the IP address (MAC is 77-77-77-77-77-77 and dest IP is 182.162.3.1). The host then creates and sends an ethernet frame for the aforementioned MAC address
 2. The router (2) gets the frame. It unwraps it to get the datagram and determines the next step to be Router 1 (182.168.2.1). It checks the ARP table and determines this is MAC 33-33-33-33-33-33. It then creates the ethernet frame and sends it there accordingly
 3. Router 1 then gets the frame and follows a similar process. From the datagram it gets the next destination host B with IP 182.168.1.003. From there the ARP table says it is MAC 22-22-22-22-22-22 where the frame is then created and sent.
 4. Host B gets the frame and unwraps it to get the message
- b) Once again, assume DHCP is done and the address of the router is known
 1. The first step is to send an ARP query to FF-FF-FF-FF-FF-FF. This will broadcast that we are looking for where to send the packets to because we do not know where so we need to find the MAC address for Host E to send the packet to. From there, Router 2 will receive this packet and send a response to Host B saying to send the packets to 77-77-77-77-77-77. This response will go to the sender of the query which is 88-88-88-88-88-88.
 2. After that everything is the same

2.

Action	Known MACs	Links sent to	Explanation
A->D	A	B, C, D	Initially the table is empty. When the packet is received, A is added to the ARP table. From there since the destination B is not known, the links are "flooded" or in other words the info is sent to all the links.
D->A	A, D	A	The switch receives the packet and adds D to the ARP table. From there the packet is forwarded to A since A is already in the ARP table
C->A	A, D, C	A	The switch receives the packet and adds C to the ARP table. From there the packet is forwarded to A since A is already in the ARP table
A->C	A, D, C	C	The switch receives the packet. A is in the ARP table so it doesn't change. From there the packet is forwarded to C since C is already in the ARP table

3. Facebook updated their border gateway protocol which withdrew their IP addresses from global routing tables. Since their authoritative DNS was now unreachable, facebook.com was impossible to resolve so you could no longer access the website. This was propagated by a lot of Facebook internal servers being down so it took forever for it to come back.

Part 2

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=
2	0.002091700	138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0
3	0.002870917	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029390199	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031464845	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ac
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232896589	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ac
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (te
11	0.233703166	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ac
12	5.189772327	PcsCompu_82:36:d7	PcsCompu_89:c7:7c	ARP	42	Who has 192.168.10.11? Tell
13	5.191799501	PcsCompu_89:c7:7c	PcsCompu_82:36:d7	ARP	60	192.168.10.11 is at 08:00:2
14	5.234545253	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=1
15	5.234709589	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=5
16	5.236143161	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ac
17	5.238048528	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1038 A
18	5.241721585	PcsCompu_89:c7:7c	PcsCompu_82:36:d7	ARP	60	Who has 192.168.10.254? Tel
19	5.241747598	PcsCompu_82:36:d7	PcsCompu_89:c7:7c	ARP	42	192.168.10.254 is at 08:00:

Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330
Source Port: 53924
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 330]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2729789995
[Next Sequence Number: 331 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2574368014
1000 = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)

1. Source Port (tcp.srcport), 2 bytes Packets: 19 · Displayed: 19 (100.0%) Profile: Default

The source is 192.168.10.11:53924

The dest is 138.76.29.8:80

2. .030672101

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.10.11	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=
2	0.002091700	138.76.29.8	192.168.10.11	TCP	74	80 → 53924 [SYN, ACK] Seq=0
3	0.002870917	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=
4	0.027362245	192.168.10.11	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029390199	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1 Ack=
6	0.030672101	138.76.29.8	192.168.10.11	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031464845	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ac
8	0.231407421	192.168.10.11	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232896589	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=548 Ac
10	0.233074462	138.76.29.8	192.168.10.11	HTTP	555	HTTP/1.1 404 Not Found (te
11	0.233703166	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ac
12	5.189772327	PcsCompu_82:36:d7	PcsCompu_89:c7:7c	ARP	42	Who has 192.168.10.11? Tell
13	5.191799501	PcsCompu_89:c7:7c	PcsCompu_82:36:d7	ARP	60	192.168.10.11 is at 08:00:2
14	5.234545253	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [FIN, ACK] Seq=1
15	5.234709589	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=5
16	5.236143161	192.168.10.11	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ac
17	5.238048528	138.76.29.8	192.168.10.11	TCP	66	80 → 53924 [ACK] Seq=1038 A
18	5.241721585	PcsCompu_89:c7:7c	PcsCompu_82:36:d7	ARP	60	Who has 192.168.10.254? Tel
19	5.241747598	PcsCompu_82:36:d7	PcsCompu_89:c7:7c	ARP	42	192.168.10.254 is at 08:00:

Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547	
Source Port: 80	
Destination Port: 53924	
[Stream index: 0]	
[Conversation completeness: Complete, WITH_DATA (31)]	
[TCP Segment Len: 547]	
Sequence Number: 1 (relative sequence number)	
Sequence Number (raw): 2574368014	
[Next Sequence Number: 548 (relative sequence number)]	
Acknowledgment Number: 331 (relative ack number)	
Acknowledgment number (raw): 2729790325	
1000 = Header Length: 32 bytes (8)	
Flags: 0x018 (PSH, ACK)	
Frame (613 bytes) Uncompressed entity body (511 bytes)	
Source Port (tcp.srcport), 2 bytes	
Packets: 19 · Displayed: 19 (100.0%) Profile: Default	

3. Same image as 2

The source is 138.76.29.8:80

The dest is 192.168.10.11:53924

4. .027356291

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=
2	0.002058086	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK] Seq=0
3	0.002853940	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029338911	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1 Ack=
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ac
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863610	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=548 Ac
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (te
11	0.233687113	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ac
12	5.189837924	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253? Tell 16
13	5.191700729	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:00:27:2
14	5.231662506	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 16
15	5.231707677	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:4
16	5.234487950	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [FIN, ACK] Seq=1
17	5.234707098	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=5
18	5.236144683	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ac
19	5.238001105	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1038 A

Frame 4: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface eth0, id 0	
Ethernet II, Src: PcsCompu_43:65:cd (08:00:27:43:65:cd), Dst: PcsCompu_22:fd:74 (08:00:27:22:fd:74)	
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 138.76.29.8	
Transmission Control Protocol, Src Port: 53924, Dst Port: 80, Seq: 1, Ack: 1, Len: 330	
Source Port: 53924	
Destination Port: 80	
[Stream index: 0]	
[Conversation completeness: Complete, WITH_DATA (31)]	
[TCP Segment Len: 330]	
Sequence Number: 1 (relative sequence number)	
Sequence Number (raw): 2729789995	
[Next Sequence Number: 331 (relative sequence number)]	
Acknowledgment Number: 1 (relative ack number)	
Source Port (tcp.srcport), 2 bytes	
Packets: 19 · Displayed: 19 (100.0%) Profile: Default	

5. Same pic as 4

The source is 10.0.1.254:53924

The dest is 138.76.29.8:80

Interestingly, the source IP is different but the source port is not. The rest are the same

6. .030625966

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.1.254	138.76.29.8	TCP	74	53924 → 80 [SYN] Seq=0 Win=
2	0.002058086	138.76.29.8	10.0.1.254	TCP	74	80 → 53924 [SYN, ACK] Seq=6
3	0.002853940	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=1 Ack=
4	0.027356291	10.0.1.254	138.76.29.8	HTTP	396	GET / HTTP/1.1
5	0.029338911	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1 Ack=
6	0.030625966	138.76.29.8	10.0.1.254	HTTP	613	HTTP/1.1 200 OK (text/html)
7	0.031448670	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=331 Ac
8	0.231400190	10.0.1.254	138.76.29.8	HTTP	317	GET /favicon.ico HTTP/1.1
9	0.232863610	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=548 Ac
10	0.233043313	138.76.29.8	10.0.1.254	HTTP	555	HTTP/1.1 404 Not Found (te
11	0.233687113	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=582 Ac
12	5.189837924	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	Who has 10.0.1.253? Tell 10
13	5.191700729	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	10.0.1.253 is at 08:00:27:2
14	5.231662506	PcsCompu_22:fd:74	PcsCompu_43:65:cd	ARP	60	Who has 10.0.1.254? Tell 10
15	5.231707677	PcsCompu_43:65:cd	PcsCompu_22:fd:74	ARP	42	10.0.1.254 is at 08:00:27:4
16	5.234487950	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [FIN, ACK] Seq=1
17	5.234707098	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [FIN, ACK] Seq=5
18	5.236144683	10.0.1.254	138.76.29.8	TCP	66	53924 → 80 [ACK] Seq=583 Ac
19	5.238001105	138.76.29.8	10.0.1.254	TCP	66	80 → 53924 [ACK] Seq=1038 A

Frame 6: 613 bytes on wire (4904 bits), 613 bytes captured (4904 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_22:fd:74 (08:00:27:22:fd:74), Dst: PcsCompu_43:65:cd (08:00:27:43:65:cd)

Internet Protocol Version 4, Src: 138.76.29.8, Dst: 10.0.1.254

Transmission Control Protocol, Src Port: 80, Dst Port: 53924, Seq: 1, Ack: 331, Len: 547

Source Port: 80

Destination Port: 53924

[Stream index: 0]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 547]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2574368014

[Next Sequence Number: 548 (relative sequence number)]

Acknowledgment Number: 331 (relative ack number)

Frame (613 bytes) Uncompressed entity body (511 bytes)

Source Port (tcp.srcport), 2 bytes

Packets: 19 · Displayed: 19 (100.0%) Profile: Default

7. Same image as above

The source is 138.76.29.8:80

The dest is 10.0.1.254:53924

8. Since the NAT protocol essentially replaces the headers at the router with what they're supposed to be, it will be exactly how the host expects

The source is 138.76.29.8:80

The dest is 192.168.10.11:53924

Lab 2

This lab was a bit confusing because there was only one response to any of the ARP messages. I will assume the sender who got a response is the computer

1. c4:41:1e:75:b1:52

Packet list	Narrow & Wide	Case sensitive	String	is at	Find	Cancel
No.	Time	Source	Destination	Protocol	Length	Info
108	6.344929	BelkinIn_75:b1:52	Broadcast	ARP	42	Who has 128.119.247.1? Tell 128.119.247.66
109	6.347010	3ComEuro_7e:d9:01	BelkinIn_75:b1:52	ARP	60	128.119.247.1 is at 00:1e:c1:7e:d9:01
113	6.366804	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.59? Tell 128.119.247.1
116	6.459026	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.41? Tell 128.119.247.1
117	6.626891	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.111? Tell 128.119.247.1
118	6.643177	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.49? Tell 128.119.247.1
119	6.643178	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.19? Tell 128.119.247.1
120	6.645401	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
121	6.743138	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
122	6.743142	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
138	6.968905	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.53? Tell 128.119.247.1
145	7.146524	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.94? Tell 128.119.247.1
146	7.228363	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.63? Tell 128.119.247.1
147	7.327735	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.20? Tell 128.119.247.1
148	7.374264	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.104? Tell 128.119.247.1
150	7.651855	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.39? Tell 128.119.247.1
151	7.653103	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.117? Tell 128.119.247.1
152	7.752467	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
153	7.753640	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
Frame 108: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en9, id 0						
Ethernet II, Src: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
Sender MAC address: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)						
Sender IP address: 128.119.247.66						
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)						
Target IP address: 128.119.247.1						
Ethernet (eth), 14 bytes						
Packets: 268 · Displayed: 179 (66.8%)						
Profile: Default						

2. ff:ff:ff:ff:ff:ff (above picture)

3. 128.119.247.66 (above pic)

4. 128.119.247.1 (above pic)

5. 00:1e:c1:7e:d9:01

Packet list	Narrow & Wide	Case sensitive	String	128.119.247.66	Find	Cancel
No.	Time	Source	Destination	Protocol	Length	Info
108	6.344929	BelkinIn_75:b1:52	Broadcast	ARP	42	Who has 128.119.247.1? Tell 128.119.247.66
109	6.347010	3ComEuro_7e:d9:01	BelkinIn_75:b1:52	ARP	60	128.119.247.1 is at 00:1e:c1:7e:d9:01
113	6.366804	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.59? Tell 128.119.247.1
116	6.459026	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.41? Tell 128.119.247.1
117	6.626891	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.111? Tell 128.119.247.1
118	6.643177	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.49? Tell 128.119.247.1
119	6.643178	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.19? Tell 128.119.247.1
120	6.645401	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
121	6.743138	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
122	6.743142	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
138	6.968905	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.53? Tell 128.119.247.1
145	7.146524	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.94? Tell 128.119.247.1
146	7.228363	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.63? Tell 128.119.247.1
147	7.327735	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.20? Tell 128.119.247.1
148	7.374264	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.104? Tell 128.119.247.1
150	7.651855	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.39? Tell 128.119.247.1
151	7.653103	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.117? Tell 128.119.247.1
152	7.752467	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.4? Tell 128.119.247.1
153	7.753640	3ComEuro_7e:d9:01	Broadcast	ARP	60	Who has 128.119.247.9? Tell 128.119.247.1
Frame 109: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en9, id 0						
Ethernet II, Src: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01), Dst: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)						
Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						
Sender MAC address: 3ComEuro_7e:d9:01 (00:1e:c1:7e:d9:01)						
Sender IP address: 128.119.247.1						
Target MAC address: BelkinIn_75:b1:52 (c4:41:1e:75:b1:52)						
Target IP address: 128.119.247.66						
Sender IP address (arp.src.proto_ipv4), 4 bytes						
Packets: 268 · Displayed: 179 (66.8%)						
Profile: Default						