ELEC-5220

Info. Networks

FROM: Jacob Howard

TO: Dr. Yihan Li & Chao Yang,

DUE DATE: 11/29/21

Lab 8

Ex1

```
C:\Users\Authorized User>arp -a

Interface: 128.238.66.101 --- 0x6
  Internet Address      Physical Address      Type
  128.238.66.102        98-ee-cb-57-51-09     dynamic
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\Authorized User>
```

Host 1: arp -a After Ping

```
Interface: 128.238.66.102 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\WINDOWS\system32>arp -a

Interface: 128.238.66.102 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.101        98-ee-cb-57-54-1c     dynamic
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Host 2: arp -a before and after ping

No.	Time	Source	Destination	Protocol	Length	Info
13	12:36:34.238911	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
14	12:36:36.238648	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
15	12:36:38.238647	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
16	12:36:39.884739	WistronI_57:54:1c	Broadcast	ARP	60	Who has 128.238.66.102? Tell 128.238.66.101
17	12:36:39.884755	WistronI_57:51:09	WistronI_57:54:1c	ARP	42	128.238.66.102 is at 98:ee:cb:57:51:09
18	12:36:39.885451	128.238.66.101	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3914/18959, ttl=128 (reply in
19	12:36:39.885508	128.238.66.102	128.238.66.101	ICMP	74	Echo (ping) reply id=0x0001, seq=3914/18959, ttl=128 (request i
20	12:36:40.238505	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
21	12:36:40.892903	128.238.66.101	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3915/19215, ttl=128 (reply in
22	12:36:40.892961	128.238.66.102	128.238.66.101	ICMP	74	Echo (ping) reply id=0x0001, seq=3915/19215, ttl=128 (request i
23	12:36:41.908606	128.238.66.101	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3916/19471, ttl=128 (reply in
24	12:36:41.908665	128.238.66.102	128.238.66.101	ICMP	74	Echo (ping) reply id=0x0001, seq=3916/19471, ttl=128 (request i
25	12:36:42.238364	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
26	12:36:42.924347	128.238.66.101	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3917/19727, ttl=128 (reply in
27	12:36:42.924407	128.238.66.102	128.238.66.101	ICMP	74	Echo (ping) reply id=0x0001, seq=3917/19727, ttl=128 (request i
28	12:36:44.238229	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
29	12:36:44.856605	WistronI_57:51:09	WistronI_57:54:1c	ARP	42	Who has 128.238.66.101? Tell 128.238.66.102
30	12:36:44.857501	WistronI_57:54:1c	WistronI_57:51:09	ARP	60	128.238.66.101 is at 98:ee:cb:57:54:1c
31	12:36:46.238087	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001
32	12:36:48.237959	Cisco_f6:a7:b8	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8001

Host 2 Wireshark Ping

Q1: Is there any new entries in the ARP tables from after Ping process? If yes, which network interfaces are they for?

Yes, from the host we pings as shown below in the screenshot.

```
Interface: 128.238.66.102 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\WINDOWS\system32>arp -a

Interface: 128.238.66.102 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.101        98-ee-cb-57-54-1c     dynamic
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Q2: Is ARP request sent before or after the Ping request? Who sends the ARP request and whose MAC address is queried? Who is supposed to receive the ARP request?

Before. Host2 sends request and Host1's MAC address is queried as shown in the wireshark screenshot below. The wourter is supposed to receive the ARP request.

```
16 12:36:39.884739 WistronI_57:54:1c    Broadcast           ARP         60 Who has 128.238.66.102? Tell 128.238.66.101
17 12:36:39.884755 WistronI_57:51:09    WistronI_57:54:1c   ARP         42 128.238.66.102 is at 98:ee:cb:57:51:09
```

Q3: Who sends the ARP reply as a respond to the ARP request in Q2? Who is supposed to receive the ARP reply?

The router sends replay and Host2 recievess it.

```
16 12:36:39.884739 WistronI_57:54:1c    Broadcast           ARP         60 Who has 128.238.66.102? Tell 128.238.66.101
17 12:36:39.884755 WistronI_57:51:09    WistronI_57:54:1c   ARP         42 128.238.66.102 is at 98:ee:cb:57:51:09
```

Q4: List the source IP address, destination IP address, source MAC address, and destination MAC address of the ping request packet.

Source address: 128.238.66.102, Destination address: 128.238.66.101, Source MAC address: 98:ee:cb:57:51:09, Destination MAC address: 2c:5a:0f:f6:a7:ba

Q5: List the source IP address, destination IP address, source MAC address, and destination MAC address of the ping reply packet.

Source address: 128.238.66.101, Destination address: 128.238.66.102, Source MAC address: 2c:5a:0f:f6:a7:ba, Destination MAC address: 98:ee:cb:57:51:09

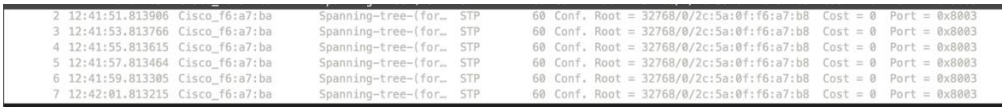
Ex2

Q6: When host 1 pings host 2, is the Ping process successful? Do you observe any ARP packets and what is the purpose of them? Explain what has happened.

The ping is unsuccessful because they're on different subnets. There are some ARP packets, which serve to find the route to the desired IP address but it can't find it since they're on different subnets.

```
Interface: 128.238.66.120 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.127        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\WINDOWS\system32>arp -a

Interface: 128.238.66.120 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.101        98-ee-cb-57-54-1c     dynamic
  128.238.66.127        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Host 2: arp -a Before and After Ping



2	12:41:51.813906	Cisco_f6:a7:ba	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8003
3	12:41:53.813766	Cisco_f6:a7:ba	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8003
4	12:41:55.813615	Cisco_f6:a7:ba	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8003
5	12:41:57.813464	Cisco_f6:a7:ba	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8003
6	12:41:59.813305	Cisco_f6:a7:ba	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8003
7	12:42:01.813215	Cisco_f6:a7:ba	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/2c:5a:0f:f6:a7:b8 Cost = 0 Port = 0x8003

Host 1 Wireshark Ping

Q7: When host 2 pings host 1, is the Ping process successful? Do you observe any ARP packets and what is the purpose of them? Explain what has happened.

No, unsuccessful. There are 2 ARP packets which help Host2 identify the location of Host1.

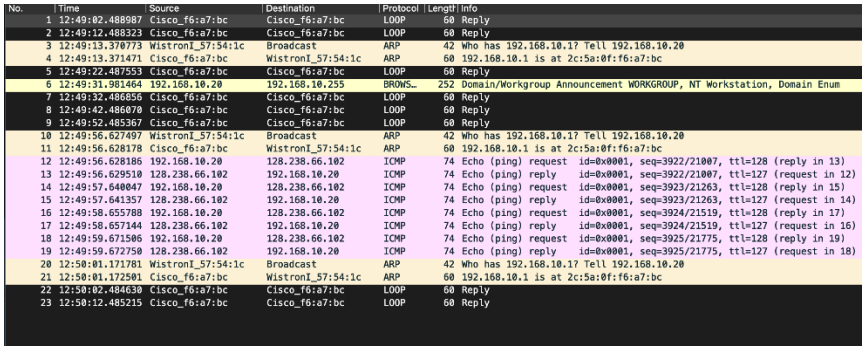
Ex3

```
Interface: 192.168.10.20 --- 0x6
  Internet Address      Physical Address      Type
  192.168.10.1          2c-5a-0f-f6-a7-bc     dynamic
  192.168.10.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\WINDOWS\system32>
```

Host 1: arp -a After Ping

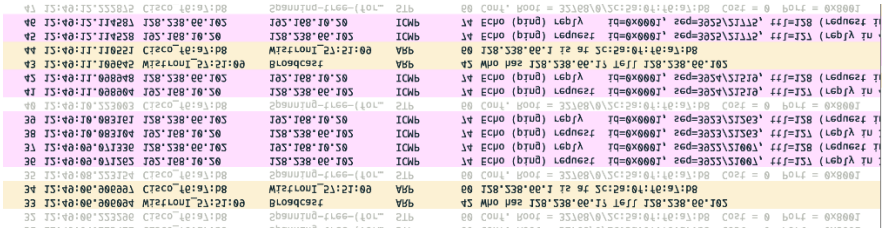
```
Interface: 128.238.66.102 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

C:\WINDOWS\system32>arp -a

Interface: 128.238.66.102 --- 0xd
  Internet Address      Physical Address      Type
  128.238.66.1          2c-5a-0f-f6-a7-b8     dynamic
  128.238.66.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Host 2: arp -a Before and After Ping



No.	Time	Source	Destination	Protocol	Length	Info
1	12:49:02.488987	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
2	12:49:12.488323	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
3	12:49:13.370773	WistronI_57:54:1c	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.20
4	12:49:13.371471	Cisco_f6:a7:bc	WistronI_57:54:1c	ARP	60	192.168.10.1 is at 2c:5a:0f:f6:a7:bc
5	12:49:22.487553	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
6	12:49:31.981464	192.168.10.20	192.168.10.255	BROWS…	252	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
7	12:49:32.486856	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
8	12:49:42.486070	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
9	12:49:52.485367	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
10	12:49:56.627497	WistronI_57:54:1c	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.20
11	12:49:56.628178	Cisco_f6:a7:bc	WistronI_57:54:1c	ARP	60	192.168.10.1 is at 2c:5a:0f:f6:a7:bc
12	12:49:56.628186	192.168.10.20	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3922/21007, ttl=128 (reply in 13)
13	12:49:56.629510	128.238.66.102	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=3922/21007, ttl=127 (request in 12)
14	12:49:57.640047	192.168.10.20	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3923/21263, ttl=128 (reply in 15)
15	12:49:57.641357	128.238.66.102	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=3923/21263, ttl=127 (request in 14)
16	12:49:58.655788	192.168.10.20	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3924/21519, ttl=128 (reply in 17)
17	12:49:58.657144	128.238.66.102	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=3924/21519, ttl=127 (request in 16)
18	12:49:59.671506	192.168.10.20	128.238.66.102	ICMP	74	Echo (ping) request id=0x0001, seq=3925/21775, ttl=128 (reply in 19)
19	12:49:59.672750	128.238.66.102	192.168.10.20	ICMP	74	Echo (ping) reply id=0x0001, seq=3925/21775, ttl=127 (request in 18)
20	12:50:01.171781	WistronI_57:54:1c	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.20
21	12:50:01.172501	Cisco_f6:a7:bc	WistronI_57:54:1c	ARP	60	192.168.10.1 is at 2c:5a:0f:f6:a7:bc
22	12:50:02.484630	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply
23	12:50:12.485215	Cisco_f6:a7:bc	Cisco_f6:a7:bc	LOOP	60	Reply

Host 1 Ping Wireshark



Host 2 Ping Wireshark

Q8: A new entry appeared in host 1's ARP table after the ping process. Which network interface is it for?

192.168.10.1 is the new entry

Q9: A new entry appeared in host 2's ARP table after the ping process. Which network interface is it for?

128.238.66.1

Q10: Whose MAC address is queried in the ARP Request from host 1? Which network interface sends the ARP Reply to host 1?

The MAC address is ff:ff:ff:ff:ff:ff from Host1. The network interface that responds is 2c:5a:0f:f6:a7:bc.

Q11: List the source IP address, destination IP address, source MAC address, and destination MAC address of(1) the Ping Request packet captured on host 1 (2) the Ping Reply packet captured on host 1

1.

Source IP: 192.168.10.20

Destination IP: 128.238.66.102

Source MAC: 98:ee:cb:57:54:1c

Destination MAC: 2c:5a:0f:f6:a7:bc

2.

Source IP: 128.238.66.102

Destination IP: 192.168.10.20

Source MAC: 2c:5a:0f:f6:a7:bc

Destination MAC: 98:ee:cb:57:54:1c

Q12: List the source IP address, destination IP address, source MAC address, and destination MAC address of (1) the Ping Request packet captured on host 2 (2) the Ping Reply packet captured on host 2

1.

Source IP: 192.168.10.20

Destination IP: 128.238.66.102

Source MAC: 2c:5a:0f:f6:a7:bc

Destination MAC: 98:ee:cb:57:54:1c

2.

Source IP: 128.238.66.102

Destination IP: 192.168.10.20

Source MAC: 98:ee:cb:57:54:1c

Destination MAC: 2c:5a:0f:f6:a7:bc

Q13: Do you get the same MAC address results for Q11 and Q12? Explain why it happens.

The MAC addresses are the same because the network is on the same subnet.