

ARP 패킷 캡처 후 분석

23.10.26

My IPv4 Address : 192.168.0.18

(cmd의 'ipconfig' 명령어를 통해 게이트웨이의 주소를 알아내었다. -> 192.168.0.18)

My MAC Address : b0:60:88:0c:51:39

(cmd의 'getmac' 명령어를 이용하여 알아내었다.)

① Direct Delivery : Host to Host ARP 해보기

192.168.0.18 ~> 192.168.0.16으로 ping을 하였다.

다음은 54번 packet(ARP Request)을 확인한 사진이다.

54	4.990776	IntelCor_0c:51:39	Broadcast	ARP	42	Who has 192.168.0.16? Tell 192.168.0.18
55	5.099518	EFMNetwo_f1:aa:50	IntelCor_0c:51:39	ARP	42	192.168.0.16 is at 70:5d:cc:f1:aa:50
56	5.099546	192.168.0.18	192.168.0.16	ICMP	74	Echo (ping) request id=0x0001, seq=315/15105, ttl=128 (reply in 57)
57	5.101519	192.168.0.16	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=315/15105, ttl=128 (request in 56)
58	5.998758	192.168.0.18	192.168.0.16	ICMP	74	Echo (ping) request id=0x0001, seq=316/15361, ttl=128 (reply in 59)
59	6.000962	192.168.0.16	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=316/15361, ttl=128 (request in 58)
60	7.015127	192.168.0.18	192.168.0.16	ICMP	74	Echo (ping) request id=0x0001, seq=317/15617, ttl=128 (reply in 61)
61	7.017371	192.168.0.16	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=317/15617, ttl=128 (request in 60)

> Frame 54: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8F3F2FA1-D467-4B23-A353-0AC0664AF5E1}, id 0

✓ Ethernet II, Src: IntelCor_0c:51:39 (b0:60:88:0c:51:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: IntelCor_0c:51:39 (b0:60:88:0c:51:39)

Type: ARP (0x0806)

✓ Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: IntelCor_0c:51:39 (b0:60:88:0c:51:39)

Sender IP address: 192.168.0.18

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.0.16

- 목적지 주소 : Broadcast

- Source 주소 : b0:60:88:0c:51:39(My MAC Address)

- Type : ARP (0x0806)

- 밑의 4줄을 통해 MAC 주소를 알아내기 위한 과정을 볼 수 있다. Sender의 IP, MAC 주소는 알고 있지만, Target (192.168.0.16)의 MAC 주소는 아직 모르고 있다.

다음은 55번(ARP Reply) packet을 확인한 사진이다.

53	3.906251	20.191.166.80	192.168.0.18	TCP	54	443 → 12424 [ACK] Seq=1 Ack=39 Win=501 Len=0
54	4.990776	IntelCor_0c:51:39	Broadcast	ARP	42	Who has 192.168.0.16? Tell 192.168.0.18
55	5.099518	EFMNetwo_f1:aa:50	IntelCor_0c:51:39	ARP	42	192.168.0.16 is at 70:5d:cc:f1:aa:50
56	5.099546	192.168.0.18	192.168.0.16	ICMP	74	Echo (ping) request id=0x0001, seq=315/15105, ttl=128 (reply in 57)
57	5.101519	192.168.0.16	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=315/15105, ttl=128 (request in 56)
58	5.998758	192.168.0.18	192.168.0.16	ICMP	74	Echo (ping) request id=0x0001, seq=316/15361, ttl=128 (reply in 59)
59	6.000962	192.168.0.16	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=316/15361, ttl=128 (request in 58)
60	7.015127	192.168.0.18	192.168.0.16	ICMP	74	Echo (ping) request id=0x0001, seq=317/15617, ttl=128 (reply in 61)
61	7.017371	192.168.0.16	192.168.0.18	ICMP	74	Echo (ping) reply id=0x0001, seq=317/15617, ttl=128 (request in 60)

> Frame 55: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8F3F2FA1-D467-4B23-A353-0AC0664AF5E1}, id 0 > Ethernet II, Src: EFMNetwo_f1:aa:50 (70:5d:cc:f1:aa:50), Dst: IntelCor_0c:51:39 (b0:60:88:0c:51:39) > Destination: IntelCor_0c:51:39 (b0:60:88:0c:51:39) > Source: EFMNetwo_f1:aa:50 (70:5d:cc:f1:aa:50) Type: ARP (0x0806) > Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: EFMNetwo_f1:aa:50 (70:5d:cc:f1:aa:50) Sender IP address: 192.168.0.16 Target MAC address: IntelCor_0c:51:39 (b0:60:88:0c:51:39) Target IP address: 192.168.0.18	0000 0010 0020
--	----------------------

- 목적지 주소 : b0:60:88:0c:51:39 (나의 MAC 주소)
- Source 주소 : 70:5d:cc:f1:aa:50 (target의 MAC 주소)
- Type : ARP (0x0806)
- 밑의 4줄에는 sender(알고자 하는 host), target(나의) IP, MAC 주소가 나열되어있다. 이전 packet과 다르게 이번에는 상대 host의 MAC 주소를 알기 때문에 1번째 줄에 MAC 주소가 나와 있는 것을 볼 수 있다. 이를 통해 상대 host의 MAC 주소를 알 수 있게 되었다.

① Case 2 : Indirect mapping : 게이트웨이로 ARP 해보기

첫 번째 ARP packet을 확인한 사진이다.

No.	Time	Source	Destination	Protocol	Length	Info
73	11.924520	IntelCor_0c:51:39	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.18
74	11.929796	EFMNetwo_ca:68:70	IntelCor_0c:51:39	ARP	42	192.168.0.1 is at 70:5d:cc:ca:68:70
94	16.590120	22:d8:a5:09:af:2c	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.4 (Reply)
95	16.966367	EFMNetwo_ca:68:70	IntelCor_0c:51:39	ARP	42	Who has 192.168.0.18? Tell 192.168.0.1
96	16.966390	IntelCor_0c:51:39	EFMNetwo_ca:68:70	ARP	42	192.168.0.18 is at b0:60:88:0c:51:39

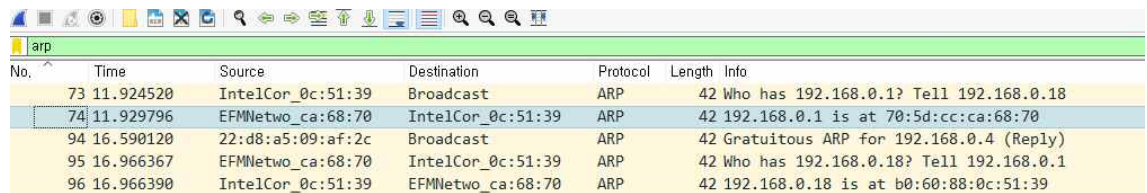
```

<
> Frame 73: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8F3F2FA1-D467-4B23-A353-0AC06
v Ethernet II, Src: IntelCor_0c:51:39 (b0:60:88:0c:51:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_0c:51:39 (b0:60:88:0c:51:39)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: IntelCor_0c:51:39 (b0:60:88:0c:51:39)
  Sender IP address: 192.168.0.18
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.1

```

- 목적지 주소 : Broadcast (ff:ff:ff:ff:ff:ff)
- source 주소(나) : 보낸 나의 mac 주소가 표시된다.
- Type : ARP (0x0806)
- 밑의 4줄에는 sender(나)와 target(게이트웨이)의 IP, MAC 주소가 나열되어있다. (ARP request) 게이트웨이의 MAC 주소는 아직 모르기 때문에 0으로 되어있는 것을 볼 수 있다.

두 번째 ARP packet을 확인한 사진이다.



No.	Time	Source	Destination	Protocol	Length	Info
73	11.924520	IntelCor_0c:51:39	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.18
74	11.929796	EFMNetwo_ca:68:70	IntelCor_0c:51:39	ARP	42	192.168.0.1 is at 70:5d:cc:ca:68:70
94	16.590120	22:d8:a5:09:af:2c	Broadcast	ARP	42	Gratuitous ARP for 192.168.0.4 (Reply)
95	16.966367	EFMNetwo_ca:68:70	IntelCor_0c:51:39	ARP	42	Who has 192.168.0.18? Tell 192.168.0.1
96	16.966390	IntelCor_0c:51:39	EFMNetwo_ca:68:70	ARP	42	192.168.0.18 is at b0:60:88:0c:51:39

```

<
> Frame 74: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8F3F2FA1-D467-4B23-A353-0AC06}
Ethernet II, Src: EFMNetwo_ca:68:70 (70:5d:cc:ca:68:70), Dst: IntelCor_0c:51:39 (b0:60:88:0c:51:39)
  Destination: IntelCor_0c:51:39 (b0:60:88:0c:51:39)
  Source: EFMNetwo_ca:68:70 (70:5d:cc:ca:68:70)
  Type: ARP (0x0806)
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: EFMNetwo_ca:68:70 (70:5d:cc:ca:68:70)
    Sender IP address: 192.168.0.1
    Target MAC address: IntelCor_0c:51:39 (b0:60:88:0c:51:39)
    Target IP address: 192.168.0.18

```

- 목적지 주소 : b0:60:88:0c:51:39 (나의 MAC 주소)
- Source 주소 : 70:5d:cc:ca:68:70 (게이트웨이의 MAC 주소)
- Type : ARP (0x0806)
- 밑의 4줄에는 sender(게이트웨이), target(나)의 IP, MAC 주소가 나열되어있다. 첫 번째 packet과 다르게 이번에는 게이트웨이의 MAC 주소를 알기 때문에 1번째 줄에 MAC 주소가 나와 있는 것을 볼 수 있다. 이를 통해 게이트웨이의 MAC 주소를 알 수 있게 되었다.