

2018037356 – 안동현

1. ARP 명령어를 찾아보고 스스로 학습한 뒤, 다음의 과정을 실행 후 해당 화면을 스크린샷으로 저장한 뒤 보고서로 작성하세요.

arp 테이블은 네트워크 장치 상에서, IP주소와 MAC주소 간의 매핑 정보를 저장하는 데이터베이스입니다. 이러한 매핑 정보를 사용하여, 데이터 패킷을 송수신하는 동안 IP주소를 해당 라우터, 스위치, 컴퓨터 등의 네트워크 장치 상에서 관리됩니다. 또한 캐시 돼 있는 arp 테이블은 주기적으로 정보가 업데이트되며, 직접 관리자 권한으로 윈도우에서 명령 프롬프트를 통해 삭제, 추가가 가능합니다.

(1) 현재의 ARP table을 출력하세요.

```

C:\Windows\System32> arp -a

인터페이스: 192.168.72.1 --- 0x8
  인터넷 주소      물리적 주소      유형
  192.168.72.255    ff-ff-ff-ff-ff-ff  정적
  224.0.0.2         01-00-5e-00-00-02  정적
  224.0.0.22        01-00-5e-00-00-16  정적
  224.0.0.251       01-00-5e-00-00-fb  정적
  224.0.0.252       01-00-5e-00-00-fc  정적
  239.255.255.250   01-00-5e-7f-ff-fa  정적

인터페이스: 192.168.45.129 --- 0x10
  인터넷 주소      물리적 주소      유형
  192.168.45.1      50-46-ae-38-91-b1  동적
  192.168.45.255    ff-ff-ff-ff-ff-ff  정적
  224.0.0.2         01-00-5e-00-00-02  정적
  224.0.0.22        01-00-5e-00-00-16  정적
  224.0.0.251       01-00-5e-00-00-fb  정적
  224.0.0.252       01-00-5e-00-00-fc  정적
  239.255.255.250   01-00-5e-7f-ff-fa  정적
  255.255.255.255   ff-ff-ff-ff-ff-ff  정적

인터페이스: 192.168.20.1 --- 0x12
  인터넷 주소      물리적 주소      유형
  192.168.20.255    ff-ff-ff-ff-ff-ff  정적
  224.0.0.2         01-00-5e-00-00-02  정적
  224.0.0.22        01-00-5e-00-00-16  정적
  224.0.0.251       01-00-5e-00-00-fb  정적
  224.0.0.252       01-00-5e-00-00-fc  정적
  239.255.255.250   01-00-5e-7f-ff-fa  정적
  
```

테이블을 확인해보면 인터페이스3개에, 각각에 IP, MAC, Type이 출력되고 있습니다.

| | |
|----------|----------------|
| IPv4 주소: | 192.168.45.129 |
|----------|----------------|

저의 컴퓨터의 네트워크 설정을 찾아보면 현재 IP주소가 이러한 것과,

| | |
|---------|----------------|
| IP 주소 | 192.168.45.218 |
| 서브넷 마스크 | 255.255.255.0 |
| 라우터 | 192.168.45.1 |

개인 스마트 폰의 와이파이 설정을 본 결과 192.168.45.xxx 구조인 것을 확인할 수가 있었습니다. 따라서 두번째 인터페이스가 저의 개인 서브넷에서 동작하는 인터페이스인 것을 추측할 수가 있었습니다. 그러한 만큼 유일하게

192.168.45.1 IP 주소를 가진 부분만 유일하게 Type이 ‘동적’임을 확인 할 수 있었습니다.

또한 255로 끝나는 IP는 브로드캐스트 용 주소로 그 MAC 주소가 ff:ff:ff:ff:ff:ff로 되어있는 것을 확인 할 수 있고, 멀티 캐스트 용의 224 주소 등을 확인하는 것도 가능합니다.

(2) ARP table에 존재하는 하나의 entry를 삭제한 뒤 ARP table을 출력하세요.

```

C:\Windows\System32> arp -d 192.168.72.255
C:\Windows\System32>arp -a

인터페이스: 192.168.72.1 --- 0x8
  인터넷 주소      물리적 주소      유형
224.0.0.2          01-00-5e-00-00-02  정적
224.0.0.22         01-00-5e-00-00-16  정적
224.0.0.251        01-00-5e-00-00-fb  정적
224.0.0.252        01-00-5e-00-00-fc  정적
239.255.255.250    01-00-5e-7f-ff-fa  정적

인터페이스: 192.168.45.129 --- 0x10
  인터넷 주소      물리적 주소      유형
192.168.45.1       50-46-ae-38-91-b1  동적
192.168.45.255     ff-ff-ff-ff-ff-ff  정적
224.0.0.2          01-00-5e-00-00-02  정적
224.0.0.22         01-00-5e-00-00-16  정적
224.0.0.251        01-00-5e-00-00-fb  정적
224.0.0.252        01-00-5e-00-00-fc  정적
239.255.255.250    01-00-5e-7f-ff-fa  정적
255.255.255.255     ff-ff-ff-ff-ff-ff  정적

인터페이스: 192.168.20.1 --- 0x12
  인터넷 주소      물리적 주소      유형
192.168.20.255     ff-ff-ff-ff-ff-ff  정적
224.0.0.2          01-00-5e-00-00-02  정적
224.0.0.22         01-00-5e-00-00-16  정적
224.0.0.251        01-00-5e-00-00-fb  정적
224.0.0.252        01-00-5e-00-00-fc  정적
239.255.255.250    01-00-5e-7f-ff-fa  정적

C:\Windows\System32>

```

192.168.72.255 entry를 삭제해 보았습니다. 테이블에서 없어진 것을 확인할 수 있었습니다.

(3) ARP table의 모든 엔트리를 삭제하는 명령어를 실행한 뒤 ARP table을 출력하세요.

```
C:\Windows\System32>arp -d *
C:\Windows\System32>arp -a

인터페이스: 192.168.72.1 --- 0x8
  인터넷 주소      물리적 주소      유형
  224.0.0.22        01-00-5e-00-00-16  정적

인터페이스: 192.168.45.129 --- 0x10
  인터넷 주소      물리적 주소      유형
  192.168.45.1      50-46-ae-38-91-b1  동적
  224.0.0.2         01-00-5e-00-00-02  정적

인터페이스: 192.168.20.1 --- 0x12
  인터넷 주소      물리적 주소      유형
  224.0.0.22        01-00-5e-00-00-16  정적

C:\Windows\System32>
```

모든 엔트리를 삭제하고 다시 테이블을 출력해본 결과, 엔트리들이 남아있는 것을 볼 수 있는데, 아마 삭제 후 엔트리가 업데이트 되어 다시 추가된 것 같습니다. 이 경우에도 192.168.45.1 엔트리만 동적임을 볼 수 있습니다.

(4) ARP table에 다음의 엔트리를 추가한 뒤 ARP table을 출력하세요.

```
C:\Windows\System32>arp -s 12.34.56.75 11-22-33-cc-dd-ff
C:\Windows\System32>arp -a

인터페이스: 192.168.72.1 --- 0x8
  인터넷 주소      물리적 주소      유형
  224.0.0.22        01-00-5e-00-00-16  정적
  239.255.255.250   01-00-5e-7f-ff-fa  정적

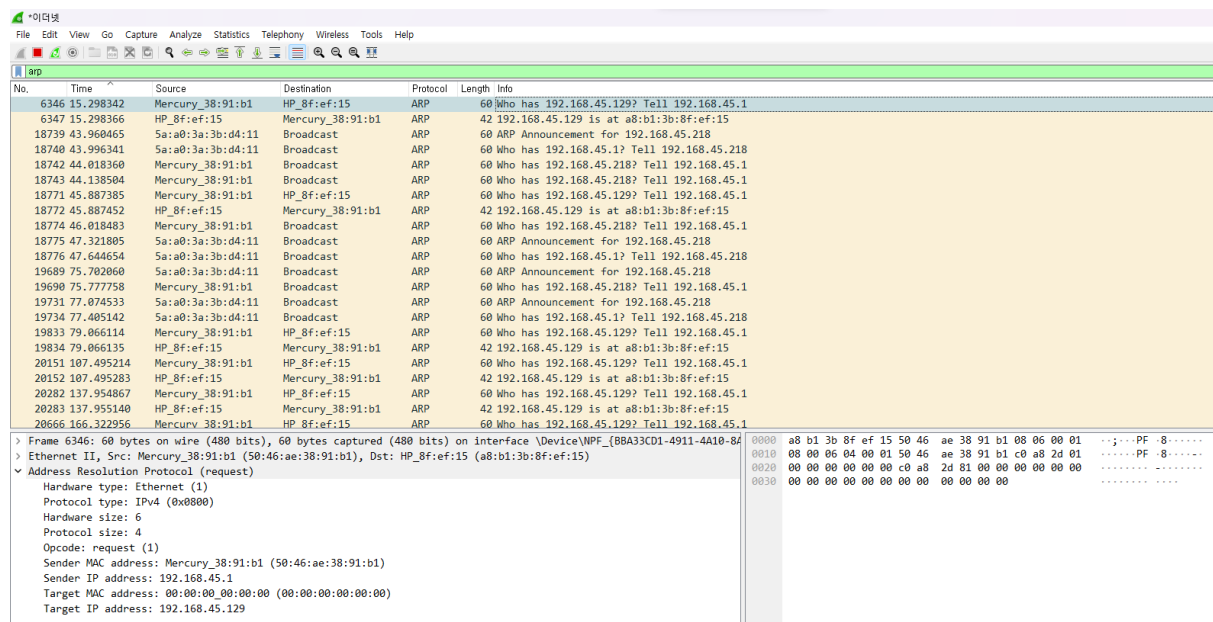
인터페이스: 192.168.45.129 --- 0x10
  인터넷 주소      물리적 주소      유형
  192.168.45.1      50-46-ae-38-91-b1  동적
  224.0.0.2         01-00-5e-00-00-02  정적
  224.0.0.251       01-00-5e-00-00-fb  정적
  224.0.0.252       01-00-5e-00-00-fc  정적
  239.255.255.250   01-00-5e-7f-ff-fa  정적

인터페이스: 192.168.20.1 --- 0x12
  인터넷 주소      물리적 주소      유형
  12.34.56.75       11-22-33-cc-dd-ff  정적
  224.0.0.22        01-00-5e-00-00-16  정적
  239.255.255.250   01-00-5e-7f-ff-fa  정적

C:\Windows\System32>
```

이렇게 12.34.56.75에 대한 엔트리가 테이블에 추가된 것을 볼 수 있습니다.

2. Wireshark을 설치 한 뒤 wireshark을 활용하여 ARP packet을 캡쳐하세요. 해당 화면을 스크린 샷으로 저장한 뒤 보고서로 작성하세요.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|-------------------|------------------|----------|--------|-------------------------------------------|
| 6346 | 15.298342 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 6347 | 15.298366 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18739 | 43.960465 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 18740 | 43.960341 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 18742 | 44.018360 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18743 | 44.138504 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18771 | 45.887385 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 18772 | 45.887452 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18774 | 46.018483 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18775 | 47.321805 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 18776 | 47.644654 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 19689 | 75.702060 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 19690 | 75.777758 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 19731 | 77.074533 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 19734 | 77.405142 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 19833 | 79.066114 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 19834 | 79.066135 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20151 | 107.495214 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 20152 | 107.495283 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20282 | 137.954867 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 20283 | 137.955140 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20666 | 166.322956 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |

> Frame 6346: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{BBA33CD1-4911-4A10-84-00} Ethernet II, Src: Mercury_38:91:b1 (50:46:ae:38:91:b1), Dst: HP_8f:ef:15 (a8:b1:3b:8f:ef:15)

> Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x8000)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Mercury_38:91:b1 (50:46:ae:38:91:b1)

Sender IP address: 192.168.45.1

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

Target IP address: 192.168.45.129

0000 a8 b1 3b 8f ef 15 50 46 ae 38 91 b1 00 06 00 01 : : : : PF 8 : : : :
0010 00 00 06 04 00 01 50 46 ae 38 91 b1 c0 a8 2d 01 : : : : PF 8 : : : :
0020 00 00 00 00 00 00 c0 a8 2d 81 00 00 00 00 00 00 : : : : : : : :
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : : : : : : : :

와이어 샤크로 이더넷 프레임을 캡처했을 때 첫번째 프레임으로 라우터(192.168.45.1) 에서 저의 컴퓨터(192.168.45.129)의 MAC 주소를 묻는 내용의 프레임입니다. 하나 특이한 점은 MAC주소를 묻는 ARP 프로토콜인데 왜 Broadcast가 아닌 것이지? 하고 의문을 품었을 때 이미 라우터는 저의 IP 주소를 알고있어서 그렇다는 결론이 나왔습니다. 계속해서 인터넷 선을 꼽고 있었기 때문 입니다.

이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|-------------------|------------------|----------|--------|-------------------------------------------|
| 6346 | 15.298342 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 6347 | 15.298366 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18739 | 43.960465 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 18740 | 43.996341 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 18742 | 44.018360 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18743 | 44.138504 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18771 | 45.887385 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 18772 | 45.887452 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18774 | 46.018483 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18775 | 47.321805 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 18776 | 47.644654 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 19689 | 75.702060 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 19690 | 75.777758 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 19731 | 77.074533 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 19734 | 77.405142 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 19833 | 79.066114 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 19834 | 79.066135 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20151 | 107.495214 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 20152 | 107.495283 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20282 | 137.954867 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 20283 | 137.955109 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20666 | 166.322956 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |

> Frame 6347: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{BBA33CD1-4911-4A10-84-00} Ethernet II, Src: HP_8f:ef:15 (a8:b1:3b:8f:ef:15), Dst: Mercury_38:91:b1 (50:46:ae:38:91:b1)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: HP_8f:ef:15 (a8:b1:3b:8f:ef:15)
Sender IP address: 192.168.45.129
Target MAC address: Mercury_38:91:b1 (50:46:ae:38:91:b1)
Target IP address: 192.168.45.1

0000 50 46 ae 38 91 b1 a8 b1 3b 8f ef 15 08 06 00 01 PF-8-... ;.....
0010 08 00 06 04 00 02 a8 b1 3b 8f ef 15 c0 a8 2d 81 ;.....
0020 50 46 ae 38 91 b1 c0 a8 2d 01 PF-8-... ..

두번째 프레임에서 reply로 00:00:00:00:0000 이던 MAC 주소가 채워지는 것을 확인할 수 있었습니다.

이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|------------|-------------------|------------------|----------|--------|-------------------------------------------|
| 6346 | 15.298342 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 6347 | 15.298366 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18739 | 43.960465 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 18740 | 43.996341 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 18742 | 44.018360 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18743 | 44.138504 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18771 | 45.887385 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 18772 | 45.887452 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18774 | 46.018483 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 18775 | 47.321805 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 18776 | 47.644654 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 19689 | 75.702060 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 19690 | 75.777758 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 19731 | 77.074533 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 19734 | 77.405142 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 19833 | 79.066114 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 19834 | 79.066135 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20151 | 107.495214 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 20152 | 107.495283 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20282 | 137.954867 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 20283 | 137.955140 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20666 | 166.322956 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |

> Frame 18739: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{BBA33CD1-4911-4A10-84-00} Ethernet II, Src: 5a:a0:3a:3b:d4:11 (5a:a0:3a:3b:d4:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Address Resolution Protocol (ARP Announcement)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
[Is gratuitous: True]
[Is announcement: True]
Sender MAC address: 5a:a0:3a:3b:d4:11 (5a:a0:3a:3b:d4:11)
Sender IP address: 192.168.45.218
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.45.218

0000 ff ff ff ff ff 5a a0 3a 3b d4 11 08 06 00 01Z ;:.....
0010 00 00 06 04 00 01 5a a0 3a 3b d4 11 c0 a8 2d daZ ;:.....
0020 00 00 00 00 00 c0 a8 2d da 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| *이더넷 | | | | | |
|----------------------------------------------------------------------------|------------|-------------------|------------------|----------|----------------------------------------------|
| File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help | | | | | |
| arp | | | | | |
| No. | Time | Source | Destination | Protocol | Length Info |
| 6346 | 15.298342 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 Who has 192.168.45.129? Tell 192.168.45.1 |
| 6347 | 15.298366 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18739 | 43.960465 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 ARP Announcement for 192.168.45.218 |
| 18740 | 43.996341 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 Who has 192.168.45.1? Tell 192.168.45.218 |
| 18742 | 44.018360 | Mercury_38:91:b1 | Broadcast | ARP | 60 Who has 192.168.45.218? Tell 192.168.45.1 |
| 18743 | 44.138504 | Mercury_38:91:b1 | Broadcast | ARP | 60 Who has 192.168.45.218? Tell 192.168.45.1 |
| 18771 | 45.887385 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 Who has 192.168.45.129? Tell 192.168.45.1 |
| 18772 | 45.887452 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 18774 | 46.018483 | Mercury_38:91:b1 | Broadcast | ARP | 60 Who has 192.168.45.218? Tell 192.168.45.1 |
| 18775 | 47.321805 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 ARP Announcement for 192.168.45.218 |
| 18776 | 47.644654 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 Who has 192.168.45.1? Tell 192.168.45.218 |
| 19689 | 75.702060 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 ARP Announcement for 192.168.45.218 |
| 19690 | 75.777758 | Mercury_38:91:b1 | Broadcast | ARP | 60 Who has 192.168.45.218? Tell 192.168.45.1 |
| 19731 | 77.074533 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 ARP Announcement for 192.168.45.218 |
| 19734 | 77.405142 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 Who has 192.168.45.1? Tell 192.168.45.218 |
| 19833 | 79.066114 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 Who has 192.168.45.129? Tell 192.168.45.1 |
| 19834 | 79.066135 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20151 | 107.495214 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 Who has 192.168.45.129? Tell 192.168.45.1 |
| 20152 | 107.495283 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20282 | 137.954867 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 Who has 192.168.45.129? Tell 192.168.45.1 |
| 20283 | 137.955140 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 20666 | 166.322956 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 Who has 192.168.45.129? Tell 192.168.45.1 |

| | | | |
|---------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------|----------------|
| > Frame 18740: 60 bytes captured (480 bits) on interface \Device\NPF_{8BA33CD1-4911-4A10-8000-000000000000} [ethernet II] | 0000 | ff ff ff ff ff ff 5a a0 3a 3b d4 11 00 06 00 01 |Z ;:..... |
| > Ethernet II, Src: 5a:a0:3a:3b:d4:11 (5a:a0:3a:3b:d4:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff) | 0010 | 00 00 06 00 00 01 5a a0 3a 3b d4 11 c0 a8 2d da |Z ;:..... |
| > Address Resolution Protocol (request) | 0020 | 00 00 00 00 00 00 c0 a8 2d 01 00 00 00 00 00 | |
| > Hardware type: Ethernet (1) | 0030 | 00 00 00 00 00 00 00 00 00 00 00 00 | |
| > Protocol type: IPv4 (0x0800) | | | |
| > Hardware size: 6 | | | |
| > Protocol size: 4 | | | |
| > Opcode: request (1) | | | |
| > Sender MAC address: 5a:a0:3a:3b:d4:11 (5a:a0:3a:3b:d4:11) | | | |
| > Sender IP address: 192.168.45.218 | | | |
| > Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) | | | |
| > Target IP address: 192.168.45.1 | | | |

저의 스마트폰에 대한 프레임 역시 확인할 수 있었습니다.

위에서 스마트폰에서 현재 IP가 192.168.45.218이라고 언급한 적이 있는데, 와이파이기가 계속 풀렸다가 다시 잡히며 자신의 IP 주소를 Broadcast로 알리고 있는 모습과, 라우터의 MAC 주소를 묻는 프레임을 확인할 수 있었습니다.

답장이 보이지 않는 이유는?

MAC 주소를 묻는 ARP 프레임은 Broadcast로 보내기에 저의 개인 스마트폰 외에도 저의 데스크탑에서 수신이 되고있지만. 라우터가 자신의 MAC 주소를 스마트폰에 보내주거나, 저의 스마트폰이 라우터에게 MAC 주소를 보내주는건 Unicast이기 때문에 수신이 불가능한걸로 추측됩니다.

거기에 와이파이 특성상 계속 끊겼다가 잡히는 탓인지 끊임없이 다시 자신의 IP 주소를 보내주고, MAC 주소를 묻는 등 여러 프레임들이 보입니다.

아까 전에 인터넷 선이 끊혀 있어서 저의 개인 데스크톱과 라우터 사이에서 Broadcast를 하지 않는 것 같다고 언급했었는데, 따라서 인터넷 선을 제거했다가 다시 꼽아봤습니다.

이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-------------|-------------------|------------------|----------|--------|-------------------------------------------|
| 41013 | 2281.388253 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 41014 | 2281.388319 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 41139 | 2303.829681 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41141 | 2303.936274 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 41142 | 2303.947766 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 41145 | 2305.273985 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41151 | 2305.603428 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 41156 | 2308.497442 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 41157 | 2308.497464 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 41198 | 2320.883779 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41199 | 2320.937187 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 41203 | 2322.254648 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41204 | 2322.581191 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 41224 | 2372.277126 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.1? Tell 192.168.45.129 |
| 41225 | 2372.280689 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | 192.168.45.1 is at 50:46:ae:38:91:b1 |
| 41229 | 2372.368310 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.1? Tell 192.168.45.129 |
| 41230 | 2372.371787 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | 192.168.45.1 is at 50:46:ae:38:91:b1 |
| 41231 | 2372.568356 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.129? (ARP Probe) |
| 41340 | 2373.534994 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 41341 | 2373.535059 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 41342 | 2373.576535 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.129? (ARP Probe) |
| 41581 | 2374.578869 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.129? (ARP Probe) |

> Frame 41224: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{8BA33CD1-4911-4A10-8...}

> Ethernet II, Src: HP_8f:ef:15 (a8:b1:3b:8f:ef:15), 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: HP_8f:ef:15 (a8:b1:3b:8f:ef:15)

Sender IP address: 192.168.45.129

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

Target IP address: 192.168.45.1

이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-------|-------------|-------------------|------------------|----------|--------|-------------------------------------------|
| 41013 | 2281.388253 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 41014 | 2281.388319 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 41139 | 2303.829681 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41141 | 2303.936274 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 41142 | 2303.947766 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 41145 | 2305.273985 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41151 | 2305.603428 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 41156 | 2308.497442 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 41157 | 2308.497464 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 41198 | 2320.883779 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41199 | 2320.937187 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.218? Tell 192.168.45.1 |
| 41203 | 2322.254648 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | ARP Announcement for 192.168.45.218 |
| 41204 | 2322.581191 | 5a:a0:3a:3b:d4:11 | Broadcast | ARP | 60 | Who has 192.168.45.1? Tell 192.168.45.218 |
| 41224 | 2372.277126 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.1? Tell 192.168.45.129 |
| 41225 | 2372.280689 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | 192.168.45.1 is at 50:46:ae:38:91:b1 |
| 41229 | 2372.368310 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.1? Tell 192.168.45.129 |
| 41230 | 2372.371787 | Mercury_38:91:b1 | HP_8f:ef:15 | ARP | 60 | 192.168.45.1 is at 50:46:ae:38:91:b1 |
| 41231 | 2372.568356 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.129? (ARP Probe) |
| 41340 | 2373.534994 | Mercury_38:91:b1 | Broadcast | ARP | 60 | Who has 192.168.45.129? Tell 192.168.45.1 |
| 41341 | 2373.535059 | HP_8f:ef:15 | Mercury_38:91:b1 | ARP | 42 | 192.168.45.129 is at a8:b1:3b:8f:ef:15 |
| 41342 | 2373.576535 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.129? (ARP Probe) |
| 41581 | 2374.578869 | HP_8f:ef:15 | Broadcast | ARP | 42 | Who has 192.168.45.129? (ARP Probe) |

> Frame 41225: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{8BA33CD1-4911-4A10-8...}

> Ethernet II, Src: Mercury_38:91:b1 (50:46:ae:38:91:b1), Dst: HP_8f:ef:15 (a8:b1:3b:8f:ef:15)

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: Mercury_38:91:b1 (50:46:ae:38:91:b1)

Sender IP address: 192.168.45.1

Target MAC address: HP_8f:ef:15 (a8:b1:3b:8f:ef:15)

Target IP address: 192.168.45.129

결과적으로 다시 Broadcast로 라우터의 MAC 주소를 묻고, 그걸 라우터가 Unicast로 답장해주는 모습을 볼 수 있었습니다! 여기서 의문점을 하나 확인할 수 있는데.

이더넷 프레임의 최소 데이터 용량은 46바이트(패딩 18바이트 포함)으로 알고 있는데 저 개인의 데스크톱에서 보내는 프레임에는 60바이트(CRC 제외) 가 아니라 42바이트(패딩18 바이트 제외 + CRC 제외) 인 것을 확인할 수 있었습니다.

인터넷에서 여러 정보를 수집하고 판단해본 결과,

와이어 샤크는 OS 커널 어딘가에서 프레임을 캡처하지만, 패딩이 다뤄지는 부분은 H/W 단위의 NIC임을 생각해서, Application 계층에서부터 내려와서 물리계층까지 데이터를 보낼 때 캡처되는 프레임에는 패딩이 아직 들어가있지 않아 보이지 않는 것이고 해당 캡처 이후 패딩이 추가될 것

이라고 예측이 됩니다. 반대로 저에게 들어오는 프레임에서는 NIC를 거치고 들어오기에 패딩이 추가되어 60바이트로 표시된다고 판단이 됩니다.

3. Wireshark을 통해 sniff한 모든 packet은 각각의 header를 볼 수 있지만 CRC는 확인 할 수 없는데 그 이유를 작성하세요.

위에서 언급했듯, wireshark는 os 커널의 한 부분에서 데이터들을 캡처합니다. 그러나 CRC는 패딩과 마찬가지로 하드웨어 수준에서 생성되거나, 이미 FCS 검사를 통과한 상태로 wireshark에서 캡처되어 확인이 불가능합니다.

4. Wireshark에서 CRC를 포함한 모든 header의 정보를 볼 수 있는 방법을 찾아보고 직접 수행한 뒤 스크린샷으로 저장 후 문서에 작성하세요.

여러 방법과 문서를 찾아보고, 설정을 건드려 보았지만 결국 실패하고 말았습니다.


첫번째로 NIC 설정을 건드려보기 위해서 윈도우 레지스트리 영역을 건드려봤습니다.

[My Sniffer Isn't Seeing VLAN, 802.1q, or QoS Tagged Frames \(intel.com\)](#) 해당 글을 참고하여

Place the new key (dword) at:

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\00nn
```

Where nn is the physical instance of the network port where you want to capture the VLAN tags. ControlSet001 might need to be Current Control Set or another 00x number.

| | |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Caution Changes to the registry can disable your system. Have a skilled technician make the changes to the registry. This change is only for promiscuous mode/sniffing use. |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

When creating or changing registry dword MonitorModeEnabled, set the dword value to one of the following:

- **0**—disabled (Do not store bad packets, Do not store CRCs, Strip 802.1Q vlan tags)
- **1**—enabled (Store bad packets. Store CRCs. Do not strip 802.1Q vlan tags)

When creating or modifying registry dword MonitorMode, set the dword value to one of the following options:

- **0**—disabled (Do not store bad packets, Do not store CRCs, Strip 802.1Q vlan tags)
- **1**—enabled (Receive bad/runt/invalid CRC packets. Leave CRCs attached to the packets. Do not strip VLAN tags and ignore packets sent to other VLANs as per normal operation.)

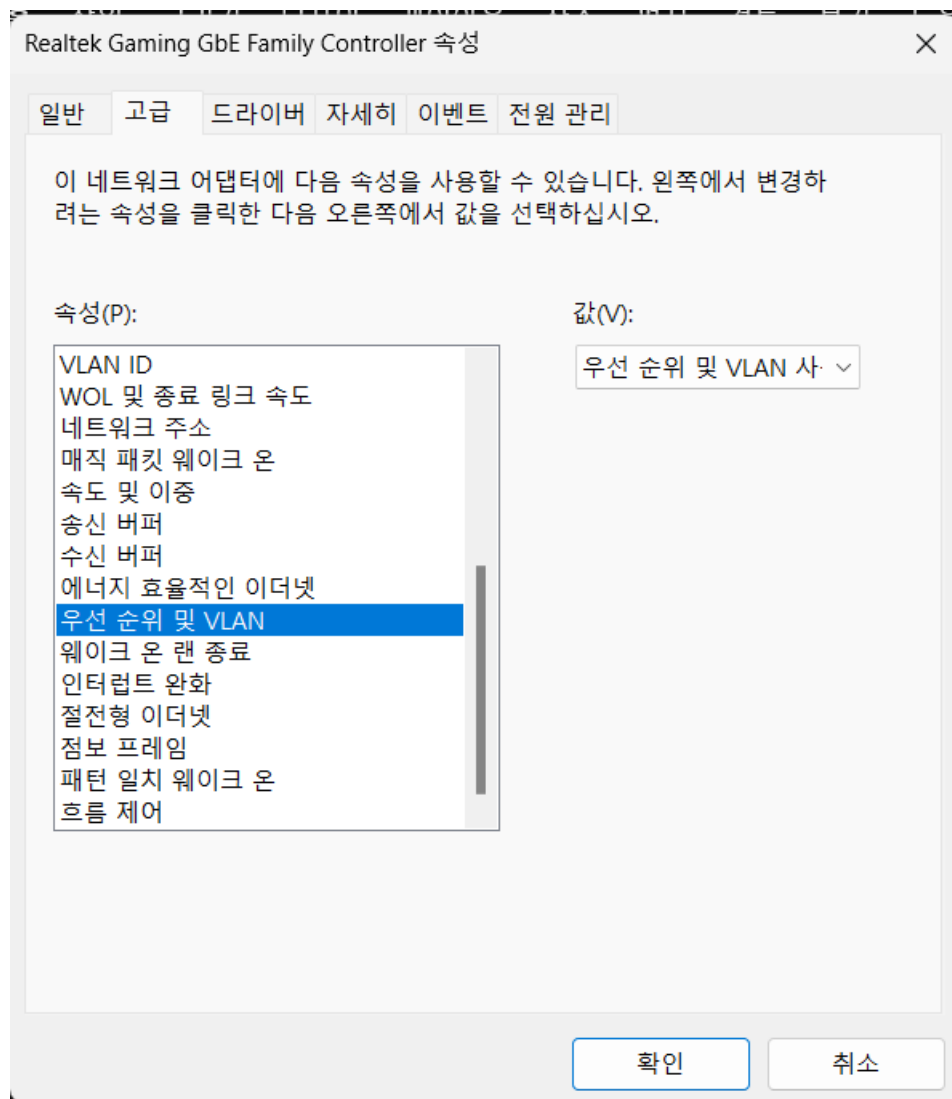
| | |
|-------------|------------------------------------------------------------------|
| Note | You must restart Windows for the registry change to take effect. |
|-------------|------------------------------------------------------------------|

위 레지스트리 영역에 키를 추가하여 설정을 변경해보았습니다.

| | | |
|-------------------|-----------|------------------------|
| MatchingDevice... | REG_SZ | FCWVEN_T0EC&DEV_0100&S |
| MonitorMode | REG_DWORD | 0x00000001 (1) |
| MonitorModeEn... | REG_DWORD | 0x00000001 (1) |
| MDPCis... | REG_DWORD | 0x00000000 (0) |

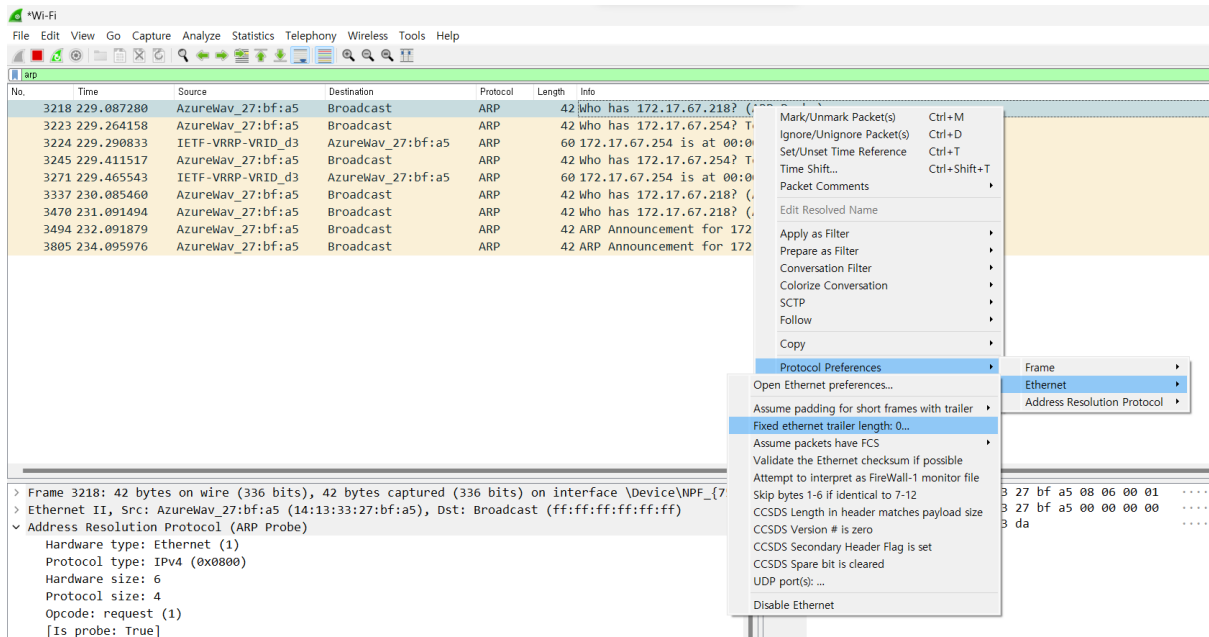
실제 사용중인 Realtek Gaming GbE Family Controller 부분 이더넷 위치를 변경해 보았고, DWORD 자료형 말고도 문자열로도 해보았지만 둘 다 실패하였습니다.

또한 wifi 네트워크를 통해서도 똑같이 진행해보았지만 실패하였습니다. 또한

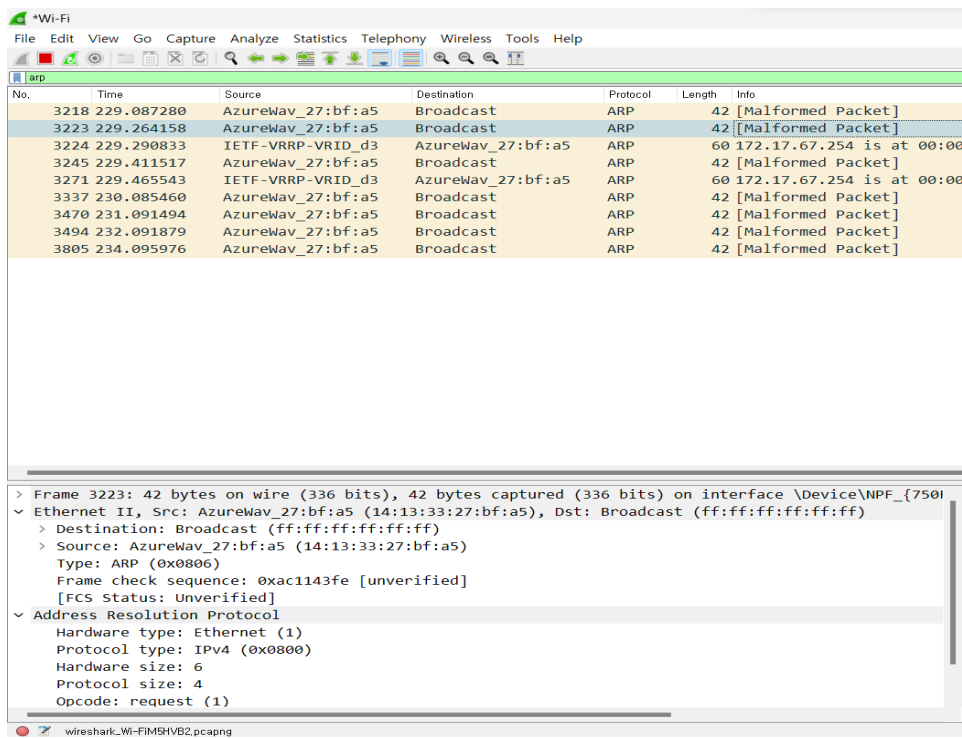


위와 같이 VLAN 설정 역시 건드려봤지만 실패하였습니다.

결국 가능했던 건



이곳의 설정을 건드려 보는 것인데



이와 같이 뒤쪽에 FCS 가 있도록 가정하여 보여주는 설정 뿐이었습니다. 해당 설정을 통하면 wireshark에서 보여주는 마지막 4비트를 FCS로 가정하는 설정인 것 같은데, 정확한 값은 아니라는 생각이 들어 매우 아쉬움이 남는 과제였습니다.

5. 후기

과제를 진행하면서 어려운 부분이 많았고, 특히 와이어 샤크로 이더넷 프레임들을 관찰하는 것들
것 어려웠습니다. 하지만 그 과정에서 데이터의 흐름을 추측하는 재미가 있어 유익한 시간이 들
었고, 그 과정에서 UniCast와 BroadCast가 몸에 와닿았습니다. 비록 완벽한 방법으로 CRC를 보는
방법까지 수행해내지는 못했지만 그 과정에서 네트워크의 설정을 직접 건드려보는 과정도 유익했
던 시간이었습니다.