Wireshark를 이용한 DHCP 패킷 분석

24.03.21

1. 과정

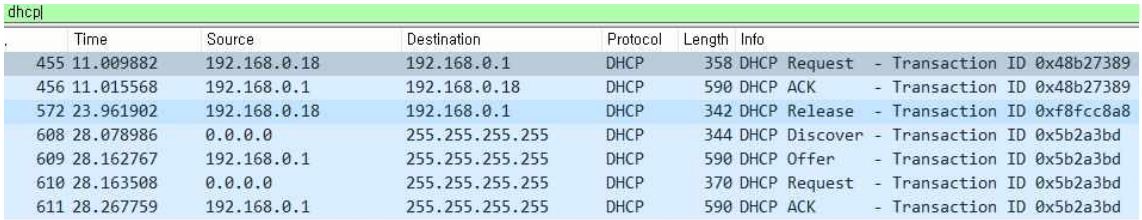
Wi-Fi 환경에서는 이미 IP가 자동 할당되어 있어 다른 방법을 사용해야 했습니다. 그래서 명령 프롬프트(cmd)를 이용하여 DHCP 과정을 보았습니다.

(1) ipconfig/renew 입력

(2) ipconfig/release 입력

(3) ipconfig/renew 다시 입력

2. 결과



dhcp

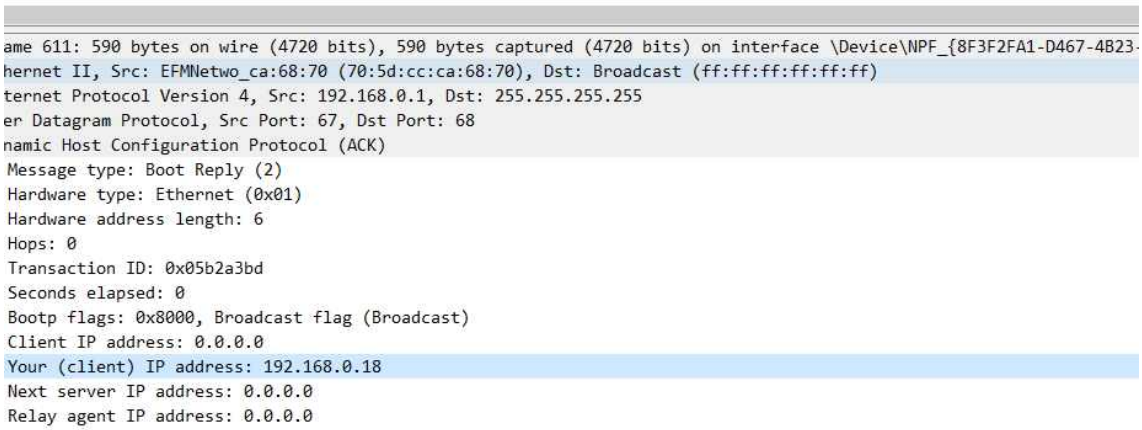
	Time	Source	Destination	Protocol	Length	Info
455	11.009882	192.168.0.18	192.168.0.1	DHCP	358	DHCP Request - Transaction ID 0x48b27389
456	11.015568	192.168.0.1	192.168.0.18	DHCP	590	DHCP ACK - Transaction ID 0x48b27389
572	23.961902	192.168.0.18	192.168.0.1	DHCP	342	DHCP Release - Transaction ID 0xf8fcc8a8
608	28.078986	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x5b2a3bd
609	28.162767	192.168.0.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x5b2a3bd
610	28.163508	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x5b2a3bd
611	28.267759	192.168.0.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x5b2a3bd

No. 455~456: DHCP 갱신을 시도합니다. 이때는 Unicast 방식으로 송수신됩니다.

No. 572 : IP를 반환합니다. 이후 인터넷 연결이 끊기게 됩니다.

No. 608~611 : 현재 할당받은 IP가 없으므로 Lease를 시도합니다. Discover -> Offer -> Request -> ACK 순서로 수행됩니다. 이 과정은 모두 Broadcast로 진행됩니다.

611 28.267759 192.168.0.1 255.255.255.255 DHCP 590 DHCP ACK - Transaction ID 0x5b2a3bd



```
ame 611: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{8F3F2FA1-D467-4B23-
hernet II, Src: EFMNetwo_ca:68:70 (70:5d:cc:ca:68:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
ternet Protocol Version 4, Src: 192.168.0.1, Dst: 255.255.255.255
er Datagram Protocol, Src Port: 67, Dst Port: 68
namic Host Configuration Protocol (ACK)
 Message type: Boot Reply (2)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x05b2a3bd
 Seconds elapsed: 0
 Bootp flags: 0x8000, Broadcast flag (Broadcast)
 Client IP address: 0.0.0.0
 Your (client) IP address: 192.168.0.18
 Next server IP address: 0.0.0.0
 Relay agent IP address: 0.0.0.0
```

마지막 Packet을 보면 IP 주소가 다시 할당된 것을 볼 수 있습니다.