**인터넷 프로토콜 HW1**

12161756 윤성호

**< ipconfig >**

: 현재 컴퓨터의 TCP/IP 네트워크 설정 값을 표시하고 DHCP와 DNS 설정을 확인 및 갱신하는데 이용한다.



1. 이더넷 어댑터 이더넷 : 유선랜 인터페이스 정보를 말한다.

1) 미디어 상태 : 현재 사용 중인 노트북에는 유선랜이 연결되어 있지 않아 ‘미디어 연결 끊김’으로 표시된다.

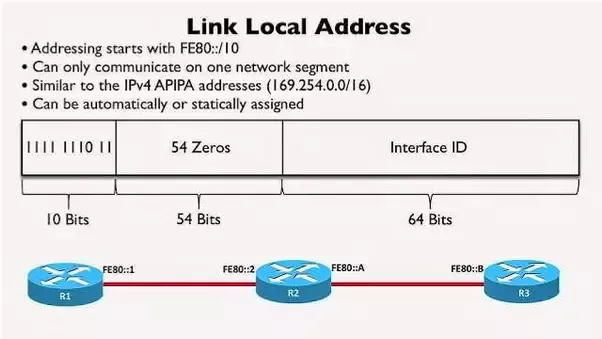
2) 연결별 DNS 접미사 : 현재 네트워크에 할당된 DNS 접미사를 말한다. 이 네트워크에 할당된

DNS 접미사는 존재하지 않는 것으로 나온다.

2. 이더넷 어댑터 VirtualBox Host-Only Network : 가상머신 프로그램인 ‘VirtualBox’에서 사용되는 가상의 네트워크 인터페이스 정보이다.

1) 링크-로컬 IPv6 주소 : 링크-로컬 IPv6 주소는 하나의 네트워크 세그먼트에서만 통신할 수 있는

128비트 주소 체계를 말한다. ‘fe80::/10’로 시작하며 EIGRP 및 OSPF와 같은 라우팅 프로토콜에서 다음 홉을 나타내는 주소로 이용된다. 이 인터페이스의 IPv6 주소는 fe80::6565:ff74:babb:cec7%20이다.



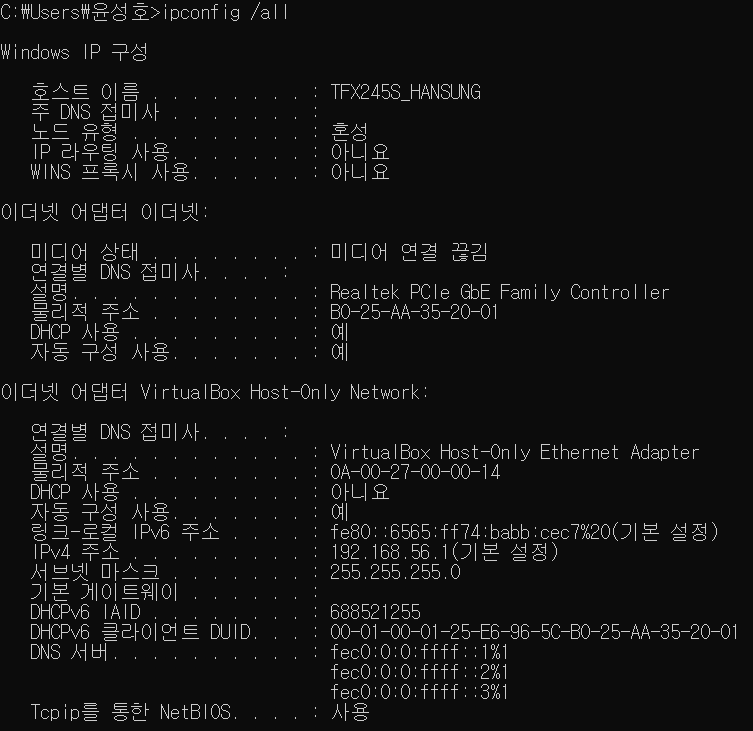
3) IPv4 주소 & 서브넷 마스크 : 각각 192.168.56.1, 255.255.255.0으로 표기되었다. 이를 통해 192.168.56까지가 Network ID이며 뒤의 1이 Host ID 부분임을 알 수 있다.

4) 기본 게이트웨이 : 현재 사용자가 위치한 네트워크에서 다른 네트워크로 이동하기 위해 반드시 거쳐야 하는 거점을 말한다. 이 인터페이스에서는 표기되지 않았다.

3. 무선 LAN 어댑터 Wi-Fi 2 : 무선랜 연결 정보이다. 현재 이 노트북은 Wi-Fi를 이용 중이며 노트북에 할당된 IPv4 주소는 192.168.0.25이다. 노트북이 속해 있는 192.168.0.0 네트워크에서는 192.168.0.1이 게이트웨이 주소이며 이는 사용 중인 iptime사의 공유기 IP주소이다. 공유기는 192.168.0.0 네트워크에 단말이 연결되면 DHCP서버를 이용해 자동으로 할당해주고 연결이 종료되면 다시 회수한다. iptime사 공유기 기준 현재 네트워크에 있는 모든 단말들의 IP할당 정보를 비롯한 공유기 설정은 게이트웨이 주소이자 공유기 주소인 192.168.0.1을 웹브라우저 도메인창에 입력해 제어할 수 있다.

**< ipconfig /all >**

: MAC 주소, DNS 서버 주소 등을 포함한 전체 구성 정보를 표시한다.

1. 호스트 이름 : 현재 컴퓨터 이름이 출력된다.

2. 설명 : 인터페이스(랜카드 등) 품명 및 제조사 정보가 출력된다.

3. 물리적 주소 : 인터페이스별 고유하게 할당된 하드웨어 주소를 말한다.

4. DHCPv6 : IPv6 네트워크에서 작동하는 데 필요한 IP주소, IP 접두사 및 기타 구성 데이터를 사용하여 IPv6 호스트를 구성하는데 사용하는 네트워크 프로토콜이다. DHCPv4와 기본적으로 동일한 체계를 사용하지만 클라이언트 ID가 필수이다. DHCPv6의 클라이언트 ID는 DUID(DHCP Unique Identifier)과 IAID(Identify Association Identifier)로 구성된다. DUID는 클라이언트 시스템을 IAID는 해당 시스템의 인터페이스를 식별한다.

5. NetBIOS : LAN 내에서 서로 다른 컴퓨터의 응용 프로그램들이 통신할 수 있게 허용하는 네트워크 인터페이스 체계 프로그램을 말한다.

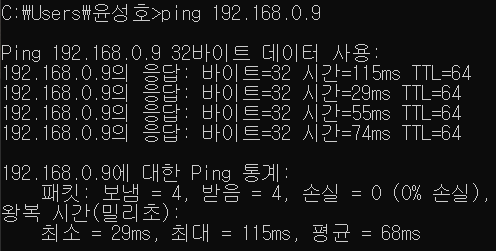
6. 무선 LAN 어댑터 로컬 영역 연결\* 11, 12 : 단순 ipconfig에서는 해당 인터페이스에 대해 알 수 없었지만 /all 옵션을 통해 Wi-Fi Direct의 인터페이스임을 알 수 있었다.

7. 임대 시작/만료 날짜 : DHCP서버를 통해 IP를 할당 받은 시간과 만료 시간을 표기한다. 현재의 192.168.0.0 네트워크에서 일반 단말에 할당 가능한 호스트 수는 192.168.0.0과 255, 1(공유기)를 제외한 253개로 한정돼 있기에 사용 중이지 않는 IP는 회수한다.

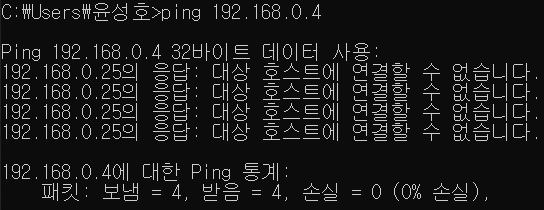
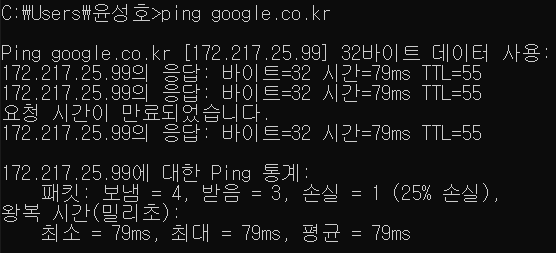
8. DNS 서버 : 현재 사용 중인 인터넷 공급 기관의 IP주소가 출력된다.



**< ping >**  
: IP 네트워크를 통해 특정한 호스트가 도달할 수 있는지를 테스트하는 데 사용되는 명령어이다.



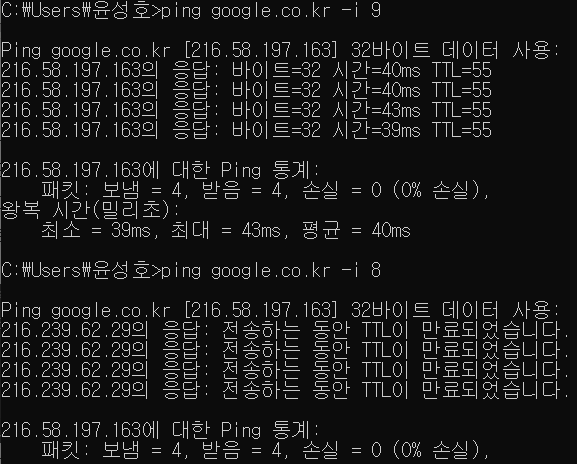
1. 유무선 공유기의 웹 설정창으로 접속하여 같은 Wi-Fi를 사용 중인 스마트폰의 IP 주소를 확인하였다. 192.168.0.9로 확인되었으며 캡쳐 이미지는 이 IP 주소로 ping test를 한 결과를 보여주고 있다. 기본적으로 패킷을 보내고 다시 받는 과정을 4번 실행한 후 이에 따른 손실율과 최소, 최대, 평균 왕복 시간을 보여준다.

2. DHCP 서버 상 존재하지 않는 IP주소로 ping 테스트를 하였더니 ‘대상 호스트에 연결할 수 없습니다.(Destionation host unreachable)’라는 메시지가 출력된다.

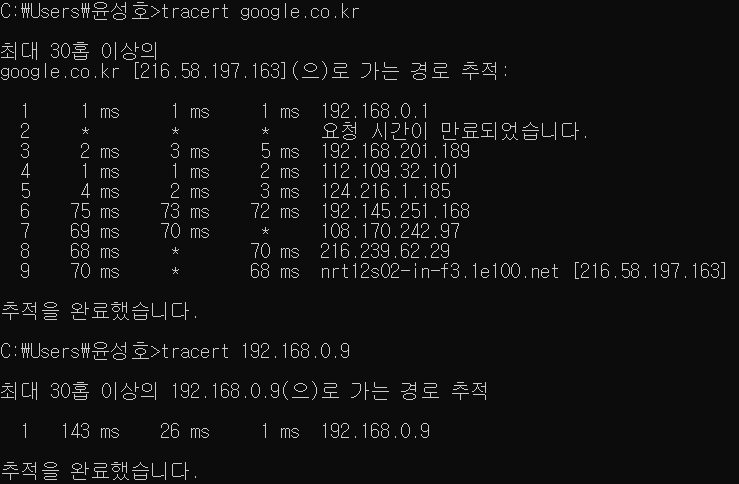
3. google.co.kr로 ping 테스트를 한 결과 3번째 패킷은 ‘요청 시간이 만료되었습니다.(Request timed out)’ 메시지를 통해 다시 받지 못한 것을 확인할 수 있었다. 4개 중에 1개의 패킷이 돌아오지 못해 손실율은 25%로 표기되었다.

4. TTL은 ‘Time to Live’의 약어로 패킷이 경유할 수 있는 최대 홉 수를 의미하며 라우터 1개를 통과할 때마다 값이 1씩 감소한다. 운영체제별로 기본 TTL값은 다르며 윈도우 : 128, 리눅스 : 64, 시스코 : 255 등의 기본 값을 가진다. 따라서 TTL값을 통해 대략적인 OS를 유추할 수 있으나 변경이 가능하기에 맹신할 수는 없다. 만약 google.co.kr 서버의 기본 TTL값이 64이라고 가정하면 9개의 라우터를 지난 것으로 풀이할 수 있다.



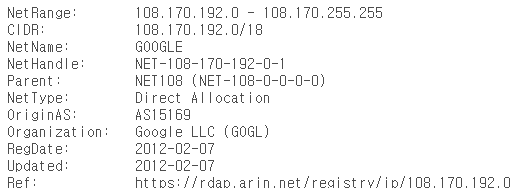
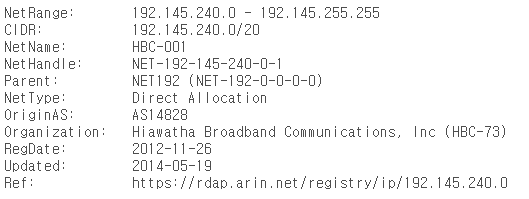
5. TTL을 임의로 제한하여 ping을 보내는 <-i> 옵션을 이용하여 4번에서 추측한 내용을 검증해보았다. TTL을 9로 제한했을 때는 google.co.kr에 도달이 가능했지만 8로 제한하자 전송 중에 TTL이 만료되었다는 메시지가 출력된다. TTL이 0이 되면 패킷을 폐기하고 ICMP를 통해 송신자에게 보고한다.

**< Tracert >**  
: 지정된 호스트에 도달할 때까지 통과하는 경로의 정보와 각 경로에서의 지연 시간을 추적하는 명령어이다.



1. 192.168.0.1(공유기 ip)를 지난 후 216.58.197.163까지 총 9개의 라우터를 거쳐 도달하는 것을 확인할 수 있다. 한 경로 당 세 개의 응답시간이 출력되는데 세 개 모두 \*로 나타난 경우는 해당 장비에서 ip 노출을 막아 놓은 것이다.

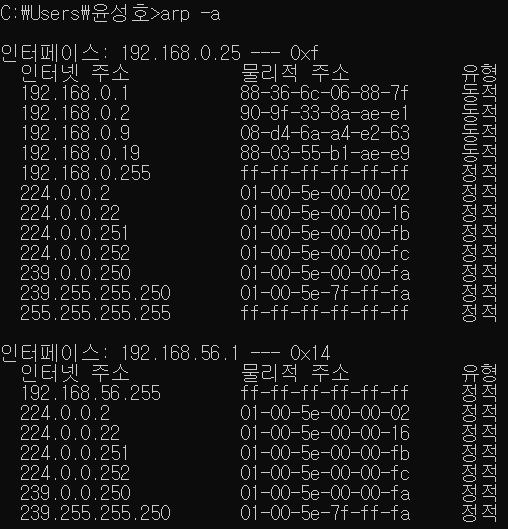
2. ip를 조회해보니 112.109.32.101과 124.216.1.185(인터넷 공급사), 192.145.251.168( Hiawatha Broadband Communication)를 거쳐 google 서버에 도달했다.



**< Arp >**  
: arp(주소 확인 프로토콜)에서 사용하는 IP 주소에서 물리적 주소로의 변환 표를 표시하고 수정한다.

**< arp -a >**

: 현재 프로토콜 데이터를 질문하여 현재 ARP 항목을 표시한다.



무선랜 인터페이스를 통해 통신한 IP 주소와 MAC 주소, 유형이 표기된다. 192.168.0.1~192.168.0.19는 DHCP를 통해 동적할당된 IP이기 때문에 유형에 ‘동적’으로 표시된다.

**< arp -s >**

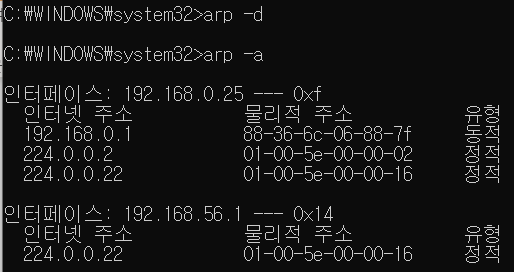
: IP주소와 MAC 주소를 정적으로 추가한다.



**< arp -d>**

: arp cache를 모두 제거한다.



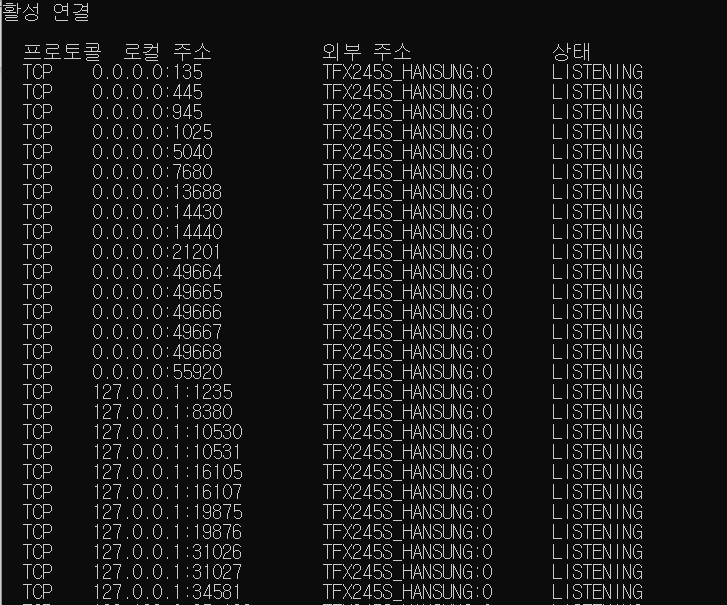


그냥 cmd창에서 실행할 경우 권한 상승이 필요하다. 관리자 권한으로 실행 후 arp -a를 입력하였더니 기본적인 목록을 제외하고는 제거된 것을 확인할 수 있다.

**< Netstat >**  
: 전송 제어 프로토콜, 라우팅 테이블, 수많은 네트워크 인터페이스, 네트워크 프로토콜 통계를 위한 네트워크 연결을 보여주는 명령 줄 도구이다. 네트워크의 문제를 찾아내고 성능 측정으로 네트워크 상의 트래픽의 양을 결정하기 위해 사용된다.

**< Netstat -a >**

: 모든 연결과 수신 대기 포트를 표시한다.



사용 중인 프로토콜과 포트번호, 상태가 출력된다.

1. LISTENING : 연결 요구를 기다리는 상태이다.

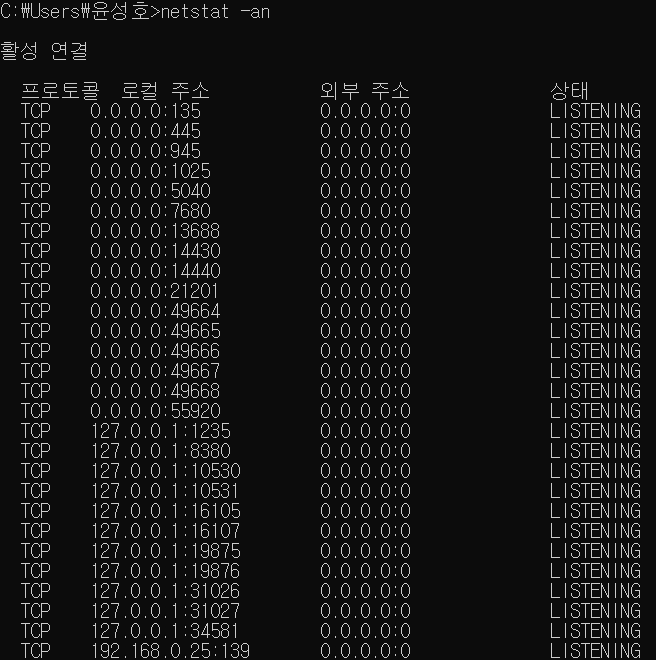
2. ESTABLISHED : 서로 연결되어 있는 상태이다.

3. CLOSE\_WAIT : 원격의 연결 요청을 받고 연결이 종료되기를 기다리는 상태이다.

4. TIME\_WAIT : 연결은 종료되었으나 원격의 수신 보장을 위해 기다리고 있는 상태이다.

**< netstat -an >**

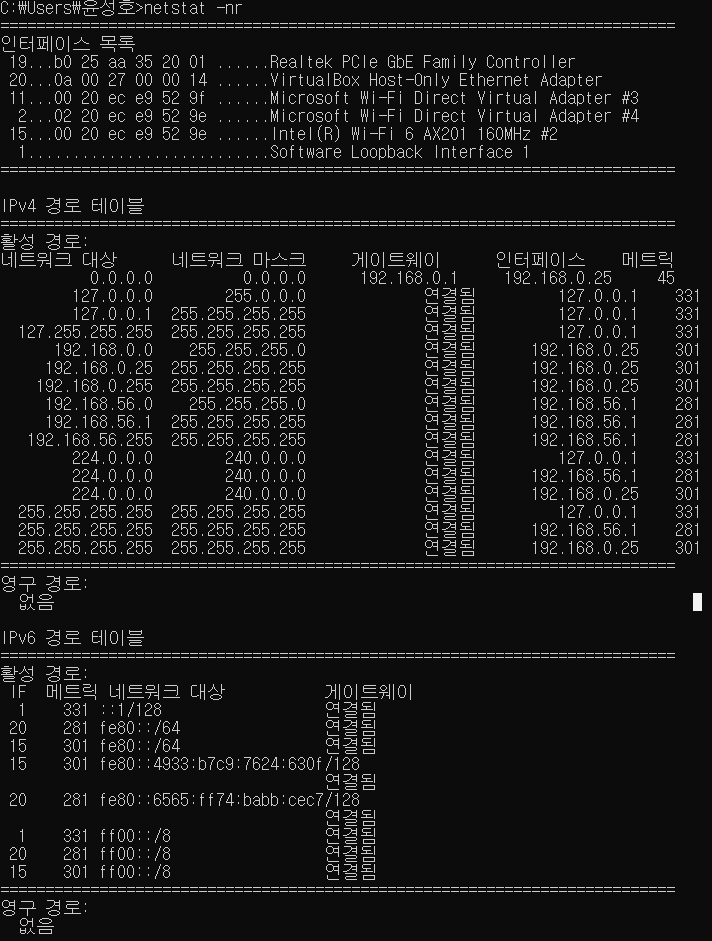
: 모든 연결과 수신 대기 포트를 표시한다. 주소와 포트 번호를 숫자 형식으로 표시한다.(-n)



‘TFX245S~’로 표시되었던 외부 주소가 숫자(0.0.0.0)으로 표시된 것을 확인할 수 있다.

**< netstat -nr >**

: 라우팅 테이블을 표시한다 (-r)



인터페이스 목록과 IPv4 경로 테이블, IPv6 경로 테이블을 보여준다. 메트릭은 우선순위를 나타내며 값이 작을수록 우선순위가 높다.

**< Nslookup >**

: 도메인 네임을 얻거나 IP 주소 매핑 또는 다른 특정한 DNS 레코드를 DNS에 질의할 때 사용한다. (name server lookup)



nslookup을 입력하자 현재 인터넷 공급자인 jcntv의 도메인명과 주소가 표기된다. 도메인명인google.co.kr을 입력하자 해당 서버 주소인 172.217.25.67이 출력되었다.