# 주소 변환 프로토콜 (ARP : Address Resolution Protocol) - arp.pcap

ARP는 가장 간단한 프로토콜 중의 하나이고, 동작을 하기 위해 필요한 패킷의 수가 가장 적은 프로토콜이다.

ARP(RFC 826)는 계층 3(IP)의 주소를 계층 2(MAC)로 바꾸고 그럼으로 해서 스위치나 라우터 같은 장비들이 어떤 포트에 어떤 장비가 연결되는지 결정하게 한다.

ARP의 재미있는 점은 OSI 모델의 각기 다른 네트워크 계층과 데이터 링크 계층에게 서비스를 제공한다는 것이다.

컴퓨터가 다른 컴퓨터로 데이터를 전송하고자 할 때 당연히 전송하고자 하는 컴퓨터가 어디에 있는지 알아야 하는데, 이 작업은 두 대의 컴퓨터를 연결 하는 스위치나 라우터, ARP 프로토콜에 의해서 이뤄지는 것이다.

스위치나 라우터는 자신의 도메인 상에 있는 모든 컴퓨터들 중에 해당 아이피가 누구의 맥주소인지 알고자 할때 ARP 브로드캐스트(Broadcast) 패킷을 보내서 클라이언트 계층 3 주소를 찾게 하는 기능을 가지고 있다. 이 브로드캐스트는 계층 2의 주소 (ff:ff:ff:ff:ff:ff)로 보내는 패킷으로, 스위치의 브로드캐스트 도메인에 연결되어 있는 모든 컴퓨터로 전송됩니다.

이 패킷의 유일한 기능을 모든 컴퓨터에게 192.168.0.1이라는 IP 주소를 가지고 있는지 물어보는 것뿐이라, 이 요청을 받은 컴퓨터들 중 위의 IP 주소와 다르면 패킷을 버릴 것이고, 자신의 IP와 일치한다면 계층 2의 주소를 포함해서 다시 패킷을 보낸 컴퓨터에게 응답할 것입니다.



위의 사진을 보면 192.168.35.43이 누군지 브로드 캐스팅 중이고, 자신은 자신의 맥주소를 브로드 캐스팅 중이다. 원래는 자신의 맥주소를 192.168.35.1에게 주어야 하지만, 왜 브로드 캐스팅 하는지 이유를 찾아보니 아래 출처의 답변이 보였다.

<https://ask.wireshark.org/questions/5178/why-gratuitous-arps-for-0000>

DHCP의 팬딩때문이라고 하는거 같다. 좀더 공부해야 겠다.

# 동적 호스트 구성 프로토콜 (DHCP : Dynamic Host Configuration Protocol)

DHCP(RFC 2131)는 자동으로 클라이언트에게 도메인 이름, NTP 서버 주소, 특별한 계층 3(IP) 주소와 같은 네트워크 관련된 설정 정보들을 제공한다. TCP 통신 프로세스는 클라이언트/서버 통신 형태로, 클라이언트 컴퓨터가 DHCP 서버에게 IP 주소를 요청하면 서버가 응답하는 방식이다.

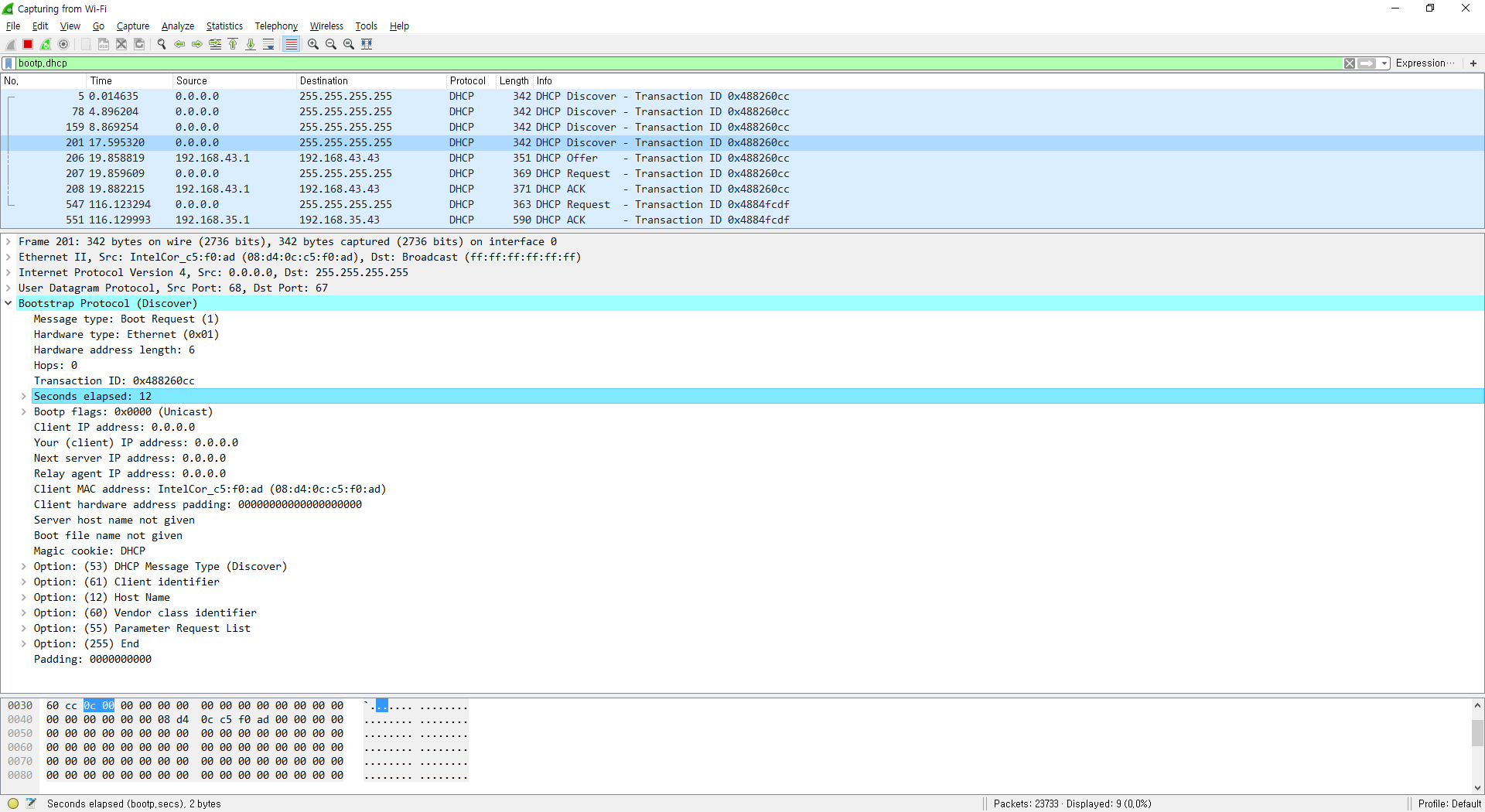
DHCP는 클라이언트 IP 주소와 설정 정보를 ‘동적인’ 방법으로 획득 할 수 있게 한다. BOOTP에서 BHCP는 주소/설정 할당에 대한 표준입니다.

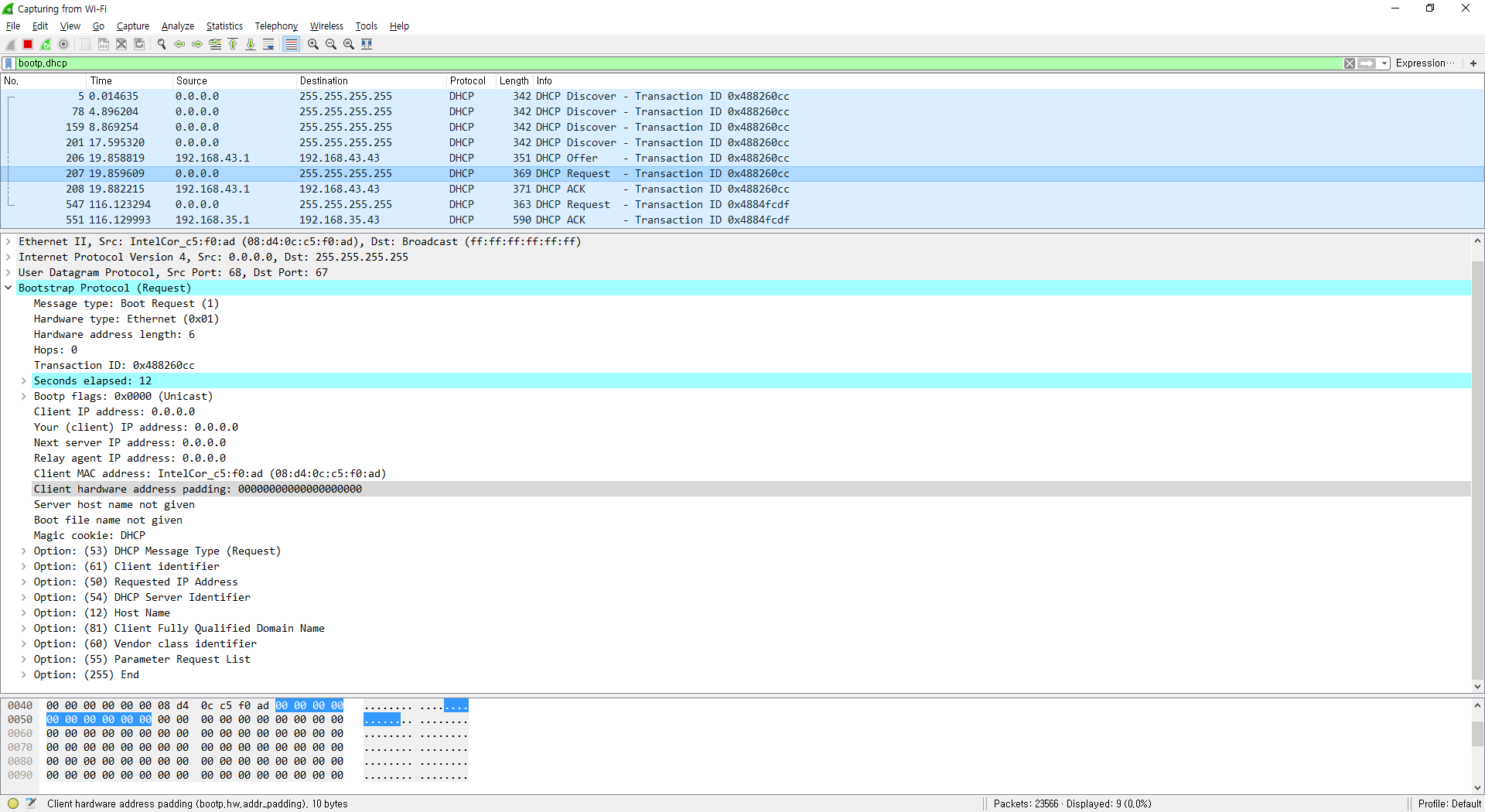
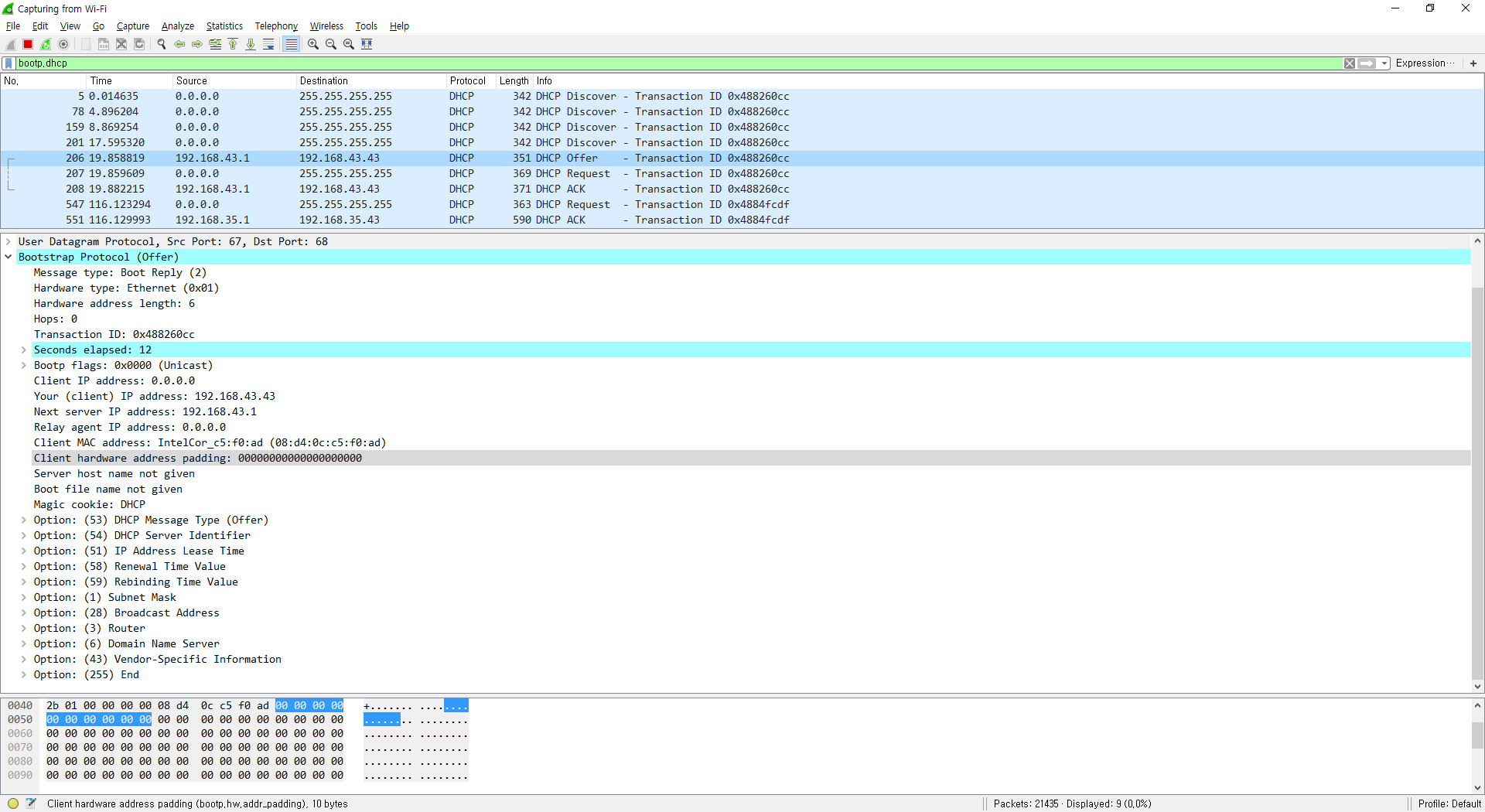
DHCP는 다양한 설정 옵션에 대한 비연결형 서비스를 제공하기 위한 전송으로 UDP를 사용합니다. (TCP를 통해 실행도 가능합니다)

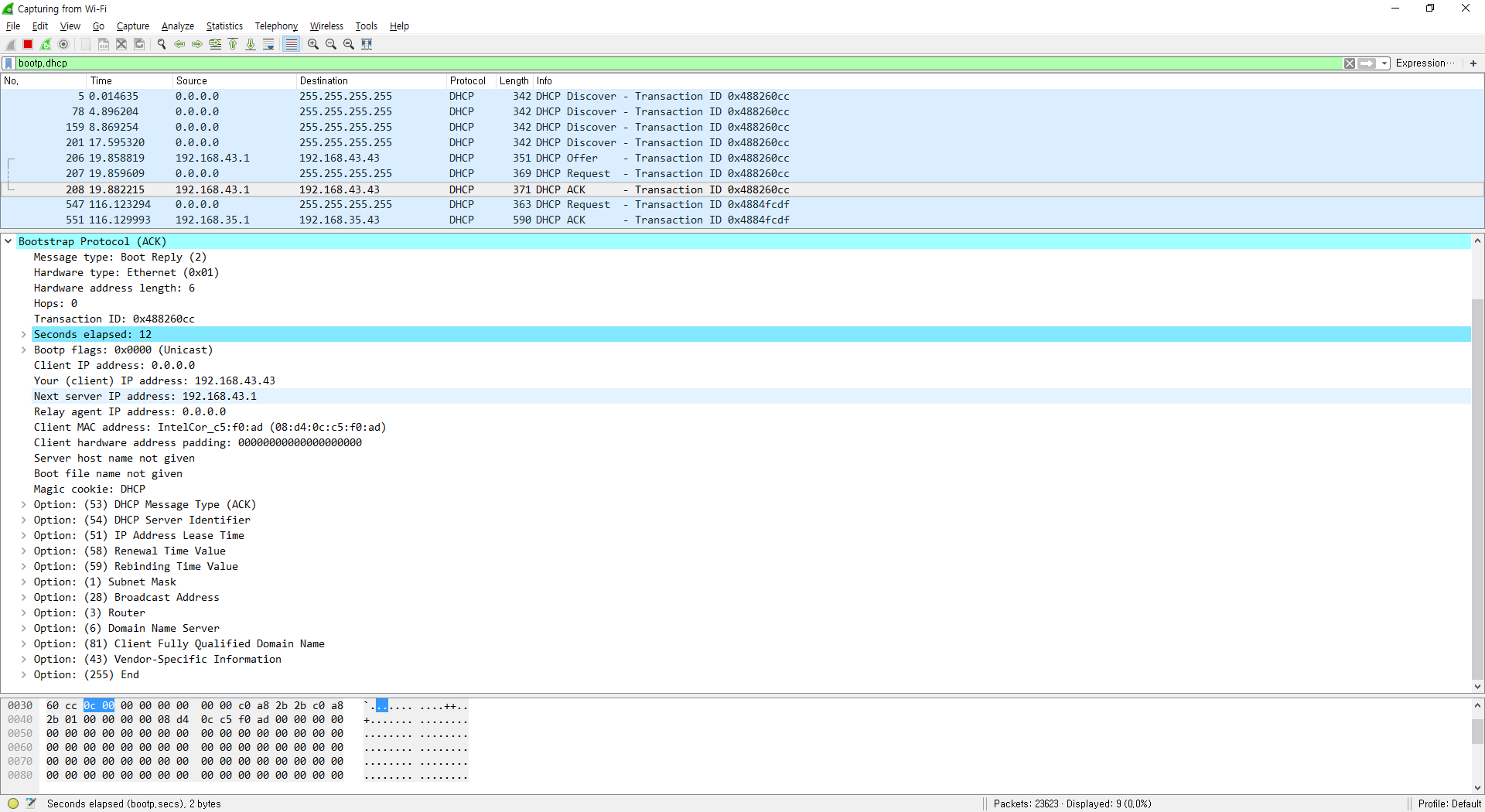
% 일반적인 DHCP 트래픽 분석

DHCP 통신을 위한 디폴트 포트는 68번 포트(클라)와 67번(서버) 포트입니다.

Discover-Offer-Request-Acknowledgement는 주소 임대 시간 외인 DHCP 클라이언트의 디폴트 시작에 사용되는 순서이다. 클라이언트가 주소 임대 시간 내에 있다면 Request-Acknowledgement 순서가 사용된다. 만일, 클라이언트가 주소 임대 시간 내에 있다면 Request-Acknowledgement 순서가 사용됩니다.







DHCP 메시지 유형에는 8가지가 있습니다.

1. DHCP Discover = 사용 가능한 DHCP 서버를 찾기 위한 클라이언트 브로드캐스트
2. DHCP Offer = 설정 파라미터를 제공하는 DHCP Discover에 대한 서버로부터 클라이언트에 대한 응답
3. DHCP Request = (a). 한 서버로부터 요청된 파라미터에 대해 응답하고 다른 서버로부터의 offer를 감소, (b). 시스템 재부팅 후 이미 할당된 주소의 정확성 확인, (c). 특정 네트워크 주소에서 임대 확장 같은 서버에 대한 클라이언트 메시지
4. DHCP Decline = 클라이언트는 제공된 네트워크 주소를 수용할 수 없다는 것을 서버에게 알림. (아마 클라이언트는 무료 ARP 테스트 프로세스를 통해 이미 사용 중인 주소를 발견했을 것)
5. DHCP Acknowledgment = 허용 네트워크 주소를 포함하는 설정 파라미터를 갖는 클라이언트에 대한 서버 응답
6. DHCP Negative Acknowledgment = 서버는 클라이언트의 네트워크 주소가 잘못되었거나(예를 들면 클라이언트가 새로운 서브 넷으로 이동했을 때) 클라이언트의 임대가 만료되었음을 알림
7. DHCP Release = 클라이언트는 서버에서 네트워크 주소를 포기하거나 남은 임대 취소를 알림
8. DHCP Informational = 클라이언트는 서버에서 지역 설정 파라미터만을 요청, 클라이언트는 이미 외부적으로 네트워크 구성을 마쳤음

DHCP의 가장 일반적인 사용은 ‘동적 주소 할당’입니다. 호스트가 시작 할 때 주소 임대와 파라미터를 획득하는 4개의 패킷 프로세스를 보여준다. DHCP 클라이언트가 DHCP 서버로부터 확인 응답과 IP 주소를 성공적으로 수신하면 클라이언트는 ‘바운드bound’상대로 진입한다.

주소 요청과 할당 프로세스 동안 클라이언트는 다음과 같은 3개의 시간 값을 얻는다.

1. 임대 시간 (LT:Lease Time)
2. 재설정 시간(T1)
3. 재연결 시간(T2)

임대 시간LT은 클라이언트가 얼마나 오랫동안 할당된 IP 주소를 사용하는지 정의한다. 재설정 시간은 5.0xLT이며, 재연결 시간은 87xLT이다.

재설정 시간T1에서 클라이언트는 재설정 상태가 되고, 임대 시간을 연장하기 위하여 DHCP 서버로 유니캐스트 DHCP 요청Request을 합니다. DHCP 서버가 확인 응답을 가지고 응답하면 클라이언트는 바운드 상태로 돌아갑니다.

클라이언트가 재연결 시간T2가 될 때까지 확인 응답을 받지 못하면 클라이언트는 재연결 상태rebinding state가 됩니다. 재연결 상태에서 클라이언트는 임대를 확장하기 위해 브로드캐스트 DHCP 요청을 전송합니다. 클라이언트가 확인 응답을 수신한다면 클라이언트는 바운드 상태로 되돌아갑니다.

클라이언트는 LT 종료까지 남은 시간의 절반이 될 때 까지 DHCP 요청을 시도한다.

클라이언트가 LT 종료 전까지 확인 응답을 받지 못하면 클라이언트는 반드시 초기화되지 않은 상태로 돌아가야만 하고, 가능하면 자신의 IP 주소를 반납하고 지역 DHCP 서버에게 DHCP 브로드캐스트를 전송해야 한다. 대부분의 DHCP 소프트웨어는 클라이언트가 마지막에 할당된 IP 주소를 기억해 해당 주소를 다시 사용하기 위해 ‘sticky IP address’를 사용한다. 동적 IP 주소 지정은 이름만큼 동적이지 않다. ( 그래서 내 공유기가 정해진 IP만을 준다 )

% DHCP 문제점 분석

DHCP가 적절히 동작하지 않으면 클라이언트는 IP 주소나 다른 클라이언트 설정을 획득하거나 유지할 수 없게 됩니다. 네트워크 상의 호스트가 정적으로 할당된 주소를 가졌는데 DHCP 서버가 이를 인식하지 못한다면 중복 주소 테스트(일반적으로 ICMP의 에코 요청 사용)를 하지 않는다면 이미 사용 중인 주소를 무심코 제공할 수 있다. ( 예를 들어 어떤 컴퓨터가 정적으로 ip를 할당 받았는데, 그 아이피를 동적으로 할당 해줄 때…)

대신 클라이언트는 중복 주소 테스트를 수행할 수 있다. 클라이언트가 다른 호스트와 동일한 주소를 가진다면 DHCP 클라이언트는 반드시 DHCP Offer에서 제공된 IP 주소를 감소시켜야 합니다.

% DHCP 패킷 구조 분석 : DHCP 패킷은 가변 길이다.

* 메시지 유형

연산 필드Opcode field라고도 불리며, 1은 DHCP 요청을 나타내고 2는 DHCP 응답을 나타낸다.

* 하드웨어 유형

이 필드는 사용되는 하드웨어 주소 유형을 정의하고, ARP 하드웨어 주소 유형 정의와 일치한다. 0x0001 값은 하드웨어 주소가 이더넷 주소임을 나타낸다.

* 하드웨어 길이

이 필드는 하드웨어 주소 길이를 나타내고, 이더넷 주소는 6이다.

* 홉

이 필드는 DHCP 서버에 도착하기 위해 통과하는 네트워크 수를 정의하는 DHCP 중계 에이전트에 의해 사용된다.

* 트랜잭선 식별자

이 필드는 DHCP 요청과 응답 패킷을 일치하는 데 사용된다.

* 초 단위 경과 시간

이 필드는 클라이언트가 새 주소를 요청하거나 갱신 주소 요청을 시작했을 때부터 경과한 초를 나타낸다.

* BOOTP 플래그

이 플래그는 IP 스택이 완전히 구성되기 전에 클라이언트가 유니캐스트나 브로드캐스트 MAC 패킷을 받아들일지를 나타낸다.

* 클라이언트 IP 주소

DHCP 서버에 의해 할당된 후 클라이언트는 클라이언트 IP 주소로 채운다.

* 사용자(클라이언트) IP 주소

이 필드는 DHCP 서버에 의해 제공된 주소를 나타낸다. DHCP 서버만 이 필드를 채운다.

* 다음 서버 IP 주소

이 필드는 중계 에이전트가 사용될 때 DHCP 서버의 주소를 포함한다.

* 중계 에이전트 IP 주소

이 필드는 사용 중일 때 DHCP 중계 에이전트 주소를 보여준다.

* 클라이언트 MAC 주소

이 필드는 클라이언트 MAC 주소를 포함한다. 이 필드는 사용자가 부팅 과정에 대해 불평하고 DHCP 문제일거라고 예상할 대 매우 유용한 필드다.

* 서버 호스트 이름

이 필드의 DHCP 서버의 이름(옵션)을 포함할 수 있다.

* 부트 파일 이름

이 필드는 부트 파일 이름(옵션)을 나타낸다.

* 매직 쿠키

이 필드는 다음 데이터 유형을 나타낸다. 0x63825363 값은 데이터가 DHCP임을 나타낸다.

* 옵션

옵션은 IP 주소와 설정 요청을 DHCP 서버에 제공하는 데 사용하고 클라이언트에 응답한다.

더 자세한 목록은 [www.iana.org](http://www.iana.org) 에서 볼 수 있다.

1 – 서브넷 마스크

3 – 라우터

4 – 시간 서버

5 – 이름 서버

6 – 도메인 서버

12 – 호스트 이름

15 – 도메인 이름

31 – 라우터 발견

# DHCP 트래픽 필터

DHCP 트래픽에 대한 캡처 필터 구문은 port 67 or port 68 이다.

DHCP는 BOOTP에서 파생됐고, bootp 디스플레이 필터 스트링을 사용한다.

Bootp.option.value == 0

DHCP Discover 메시지

Bootp.option.value == 04

DHCP Decline 메시지

Bootp.hw.mac\_addr == xx:xx:xx:xx:xx:xx

MAC 주소 xx:xx:xx:xx:xx:xx를 포함하는 DHCP 메시지

Bootp.option.type == 12

호스트 이름 값(옵션 유형 12)을 포함하는 메시지

!bootp.ip.relay == 0.0.0.0

DHCP 중계 에이전트 값을 포함하는 메시지

(bootp.ip.your == 192.168.0.104) && (bootp.option.value == 05)

IP 주소 192.168.0.104를 사용하는 클라이언트로부터의 DHCK ACP 메시지

Bootp.option.type == 55 && bootp.option.value contains 1F

Perform Router Discover(0x1F)를 포함하는 DHCP 파라미터 요청 목록

# BOOTP – DHCP 통계 디스플레이

BOOTP-DHCP 통계 윈도우는 추적 파일에서 DHCP 메시지 유형을 요약한다. 다음 목록은 일반적으로 나타나는 DHCP 메시지 유형 53 값이다.

# DNS의 목적

DNS (Domain Name System)는 [www.wiresharkU.com](http://www.wiresharkU.com) 같은 문제로 된 호스트 이름은 숫자로 된 IP 주소로 결정하는 데 사용한다. DNS는 또한 DNS 서버 간에 이름 정보를 전송하기 위해 사용하고, IP 주소와 관련된 호스트 이름을 식별하는 데 사용하며, MX 레코드 같이 다른 이름을 검색하는 데 사용한다.

DNS는 네트워크에서 가장 중요한 애플리케이션 중 하나다. DNS가 고장 나면 호스트들은 서로의 위치를 알아낼 수 없다.

DNS 요청/응답은 UDP와 TCP 존 전송에서 사용한다.

결정 프로세스는 DNS 이름을 결정하기 위해 실행된다.

DNS는 UDP나 TCP를 통해 실행할 수 있다. 일반적으로 UDP를 이용하는 DNS 쿼리와 응답을 볼 수 있다. 지역zone 전달이나 커다란 DNS 쿼리들은 TCP 상에서 실행될 수도 있다. DNS에 대한 기본 포트는 53번이다.

RFC 1035의 ‘도메인 이름: 구현과 상세’는 UDP를 통한 패킷 페이로드를 512바이트로 제한한다. 이것은 일반적으로 DNS 쿼리에 대해 충분한 수치다. 그러나 응답이 512바이트 이상의 공간을 요구하면 응답으로 단편 플래그 비트가 전송된다.

이것은 더 큰 패킷 크기를 허용하는 TCP를 사용해 DNS 쿼리를 다시 전송하기 위해 결정자를 작동시킨다.

RFC 2671의 ‘DNS(EDNS0)에 대한 메커니즘 확장’은 UDP를 통해 512바이트 이상을 허용한다. 이 추가된 기능은 마이크로소프트 DNS 사가 EDNS0에 대한 추가 지원을 할 때 많은 사람에 의해 문제가 제기되었지만, Cisco PIX Firewall 6.3이전 버전은 그렇지 않았다. PIX Firewall은 최대 구성된 길이(기본 값은 512바이트)보다 더 큰 DNS 패킷은 삭제할 것이다.

멀티캐스트 DNS(mDNS)는 DNS 서버가 설치되어 있지 않은 작은 네트워크에 대해 이름 결정 프로세스를 지원한다. 최상위 mDNS 이름 수준은 ‘.local’로 끝난다. ‘local’로 끝나는 모든 DNS 쿼리는 mDNS 멀티캐스트 주소로 전송되어야 한다. 멀티캐스트 DNS에 대한 자세한 정보는 [www.multicastdns.org](http://www.multicastdns.org)를 참조

% 일반적인 DNS 쿼리/응답 분석

네트워크 이름 결정 DNS 쿼리와 응답 프로세스들은 아주 간단하다. 클라이언트는 호스트에 대한 IP 주소를 얻기 위해 DNS 서버에 DNS 쿼리를 전송한다. DNS 서버는 정보에 대해 즉각적으로 응답하거나, 클라이언트를 대신해 다른 DNS 서버에 요청한다.

% DNS 문제 분석

가장 일반적인 DNS 문제는 네임 서버 데이터베이스에 이름이 존재하지 않아 오류가 발생하는 것이다. 이것은 잘못된 이름을 입력하거나 인터넷 네임 서버를 통해 아직 제공되지 않은 새로운 이름으로 입력했기 때문에 발생한다.

사용자는 이것이 유효한 주소라는 것을 알지만 (예를 들어 [www.naver.com](http://www.naver.com) ) DNS는 확인 할 수 없을 때도 있다. DNS 문제 때문에 그 사이트에 접근할 수가 없는 것이다.

DNS 문제의 원인을 찾는 것은 해당 위치에서 프로세스를 검색하기 위해 DNS 서버의 와이어 샤크 업 스트림 이동을 요구할 것이다.

% DNS 패킷 구조 분석

단일 전송 메커니즘(UDP나 TCP)을 사용하는 다른 애플리케이션과 다르게 DNS는 UDP와 TCP 모두를 사용한다. DNS는 일반적으로 이름 요청과 응답에 대해 UDP 53번 포트를 사용하고, 전송 대역과 더 큰 이름 요청이나 응답에 대해 TCP 53번 포트를 사용한다. 모든 DNS 패킷은 단일 기본 구조를 사용한다. 4개의 기본 섹션으로 구성되어 있다.

1. 질문
2. 응답 Resource Records
3. 권한 Resource Records
4. 추가 Resource Records

* Transaction ID

사용자는 이 필드에서 DNS 요청/응답과 관련된 모든 것을 보기 위한 값(dns.id==0x4269)을 필터링할 수 있다. Transaction ID필드는 DNS 쿼리와 응답에 연관된다.

* Flags

플래그 바이트는 쿼리 특성을 정의하는 수많은 필드로 구성되어 있다.

* + Query/Response

쿼리/응답 비트 패킷이 요청인지(0), 응답인지(1) 표시한다. DNS 요청(dns.flags.response == 0)이나 응답(dns.flags.response == 0)을 표시하기 위해 와이어샤크 필터를 작성할 수 있다.

* + Opcode

Opcode 필드는 쿼리의 유형을 지정한다. 가장 일반적으로 이 필드는 일반적인 요청에 대해 0000을 포함하고, 필드는 응답에 대해 0000으로 나타난다.

* + Authoritative Answer

응답에 사용되는 Authoritative Answer 필드는 도메인 이름에 대해 믿을 수 있는 서버로부터의 응답임을 표시한다.

* + Truncation

Truncation 필드는 DNS 응답이 길이 때문에 잘렸다는 것을 표시한다. 클라이언트가 잘린 DNS 응답을 보게 되면 TCP를 통해 쿼리를 재전송한다. 이것은 TCP 기반의 요청/응답에서 자주 볼 수 없는 광경이다.

* + Recursion Desired

재귀Recursion는 서버가 재귀 쿼리 프로세스인지 표시하기 위해 DNS 요청에서 정의될 수 있다. 재귀는 클라이언트의 관점에서 응답에 대해 다른 서버에 요청하기 위한 DNS 서버를 허용한다. 로컬 네임 서버가 응답을 보내면 즉시 응답할 것이다. 응답이 없으면 이것은 클라이언트를 대신해 프로세스 검색을 시작할 것이다. 재귀가 요구되지 않으면 요청은 반복 요청으로 간주된다. 반복 요청을 이용해 지역적으로 사용 가능할 경우 DNS 서버는 정보를 반환할 것이다. 그렇지 않으면 DNS 서버는 요청을 위한 다른 DNS 서버의 IP 주소를 반환할 것이다. DNS 요청은 재귀를 사용한다.

* + Recursion Available

응답에서 정의된 이 설정은 재귀가 DNS 서버에서 사용 가능한지를 표시한다.

* + Reserved

이 필드는 0으로 설정된다.

* + Rcode(Response Code)

Rcode 필드는 응답에서 오류가 존재하는지 표시한다. 아래는 가능한 Rcode값을 보여준다.

0 – 오류 없음

1 – 형식 오류 – 쿼리를 설명할 수 없음

2 – 서버 실패 – 서버가 네임 서버에 대한 무제 때문에 쿼리를 실행할 수 없음

3 – 네임 오류 – 도메인 이름이 존재하지 않음

4 – 실행되지 않음

1. – 거부 – 네임 서버가 규정 때문에 제 기능을 수행하지 못함

* Question Count

Question Count 필드는 질문 절에서 질문의 숫자를 표시한다. 일반적으로 쿼리 패킷당 하나의 질문을 볼 수 있을 것이다.

* Answer Resource Record(RR) Count

이 필드는 Answer RRs 섹션에서 응답의 수를 표시한다. 응답이 CNAME 정보를 포함하면 Answer RR Count 영역에서 2개를 볼 수 있을 것이다. 하나는 CNAME에 대한 것이고, 다른 하나는 CNAME 레코드의 IP 주소에 대한 것이다. ( 감염된 봇 호스트는 DNS 응답으로 큰 수의 응답 RR을 수신할 수 있다. )

* Authority RRs Count

Authority RRs Count 필드는 Authority RRs 섹션에서 응답 수를 표시한다. 이런 응답은 명명 계층 구조에서 대상 이름에 더 가까운 서버로부터 수신된다.

* Additional RRs Count

Additional RRs Count 필드는 Additional RRs 섹션에서 응답 수를 나타낸다. 이 영역에서 Additional RRs 섹션의 서버에 대한 A 레코드를 발견할 것이다.

* Questions

이 가변 길이 필드는 결정 중인 이름을 정의한다.

* + Name

이 필드는 결정 중인 이름을 포함한다. 형식은 이름에서 영문자 바이트의 숫자를 표시하기 위해 숫자 구분 문자를 이용하는 가변 길이다.

Ex) 06 G o o g l e 03 c o m

봐보니 06, 03 은 .이다.

* + Type

이 필드는 쿼리의 유형을 나타낸다. 등록된 숫자에 대한 전체 목록은 www.iana.org/assignments/dns -parameters

A – 호스트 주소

NS – Authoritative 네임 서버

CNAME – 별칭에 대한 표준 이름

SOA – 권한 영역의 시작

MX – 메일 교환

AAAA – IPv6 주소

* + Class

이 필드는 TCP/IP 통신에 대한 인터넷 클래스 주소를 표시하기 위해 1로 설정된다.

* Answer RRs

Questions 필드에서와 같은 형식이다.

* + RR Time to Live

이 필드는 DNS 응답에 사용되고 클라이언트가 캐시에서 DNS 응답을 얼마나 오래 유지하는지 표시하는 RR Time to Live 값을 포함한다.

* + Authority RRs

Questions 필드에서와 같은 형식이다.

* + Additional RRs

Questions 필드에서와 같은 형식이다.

# DNS/MDNS (멀티플랙스) 트래픽에서 필터링

Tcpdump 필터 형식이 문자 형태의 dns를 이해할 수 없기 때문에 DNS 트래픽에 대한 캡처 필터 구문은 포트 번호를 기반으로 한다. 이것은 업데이트된 liibpcap와 WinPcap로 결정될 것이다.

mDNS가 포트 5353을 사용하고 캡처 구문이 port 5353인 것에 비해, UDP 또는 TCP에서의 표준 DNS 트래픽에 대한 캡처 필터는 port 53이다.

디스플레이 필터 구문은 간단한 dns이다. 이 필터는 DNS와 mDNS 트래픽을 모두 표시한다. 아래 리스트는 추가 DNS 디스플레이 필터다.

Dns.flags.response == 0

DNS 쿼리

Dns.flags.response == 1

DNS 응답

Dns.flag.rcode != 0

DNS 응답이 오류를 포함

Dns.count.answer >= 5

DNS 응답이 5개 이상의 응답을 포함

Dns.qry.name == [www.abc.com](http://www.abc.com)

DNS 쿼리가 [www.abc.com](http://www.abc.com)에 대한 것임

Dns contains “abc”

DNS 쿼리나 응답이 문자열 ‘abc’를 포함

Dns.qry.type == 0x0001

DNS 쿼리가 호스트 이름에 대한 것임

Dns.qry.type == 0x000c

DNS 쿼리가 도메인 이름 포인터 쿼리임(역쿼리)

Dns.resp.type == 0x0005

DNS 응답이 CNAME 값을 포함(표준 이름)

Dns.resp.type == 0x0005

DNS 응답이 SOA(권한의 시작) 정보를 포함

Dns.flags.recdesired == 1

요구된 재귀에 대한 DNS 쿼리

Dns.flags.recavail == 1

DNS 응답 상태가 재귀가 가능

# 주소 결정 프로토콜 (ARP : Address Resolution Protocol)

ARP는 로컬 네트워크에서 IP 주소와 물리 주소를 연관 짓고, IP 주소(불필요한 ARP 프로세스)의 중복을 테스트하기 위해 사용한다. ARP 같은 단순한 프로토콜은 네트워크 주소 지정이나 구성에 대한 신호 문제를 가진 프로토콜이 될 수 있다. ARP는 RFC 826, ‘이더넷 주소 결정 프로토콜’에 정의되어 있다.

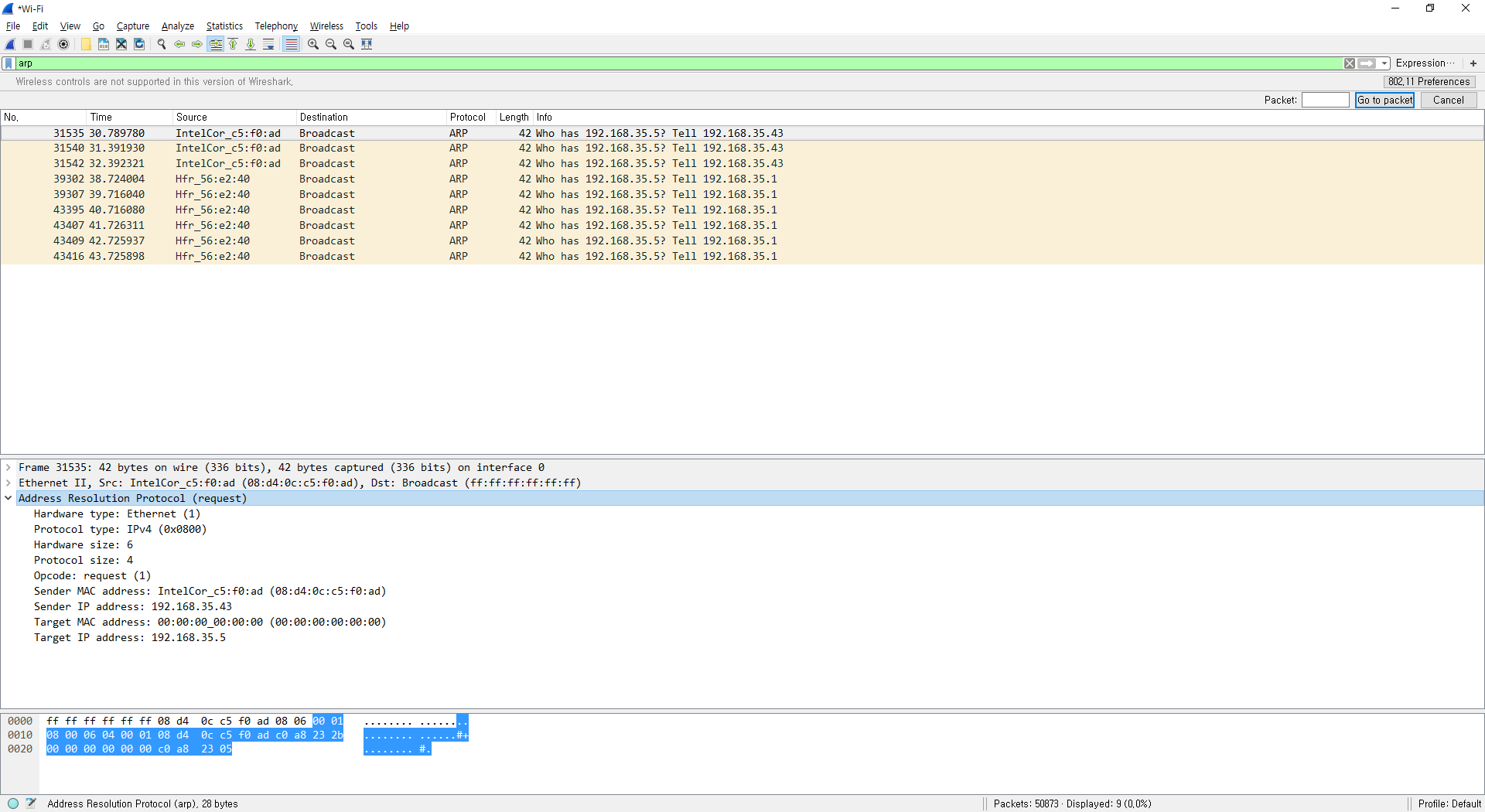
ARP 패킷은 IP 헤더를 포함하지 않기 때문에 TCP 네트워크 트래픽에 있는 대부분의 패킷과 비교할 때 상대적으로 고유한 값을 갖는다. 이런 특징은 ARP 패킷이 라우팅되지 않는 패킷이라는 의미이다.

* ARP는 오직 로컬이다.

ARP 패킷을 캡처하기 위해 호스트가 ARP 패킷을 전송하는 동안 반드시 같은 네트워크 세그먼트에 있어야 한다.

# 일반적인 ARP 요청/응답 분석

일반적인 ARP 통신은 간단한 요청과 응답으로 구성된다. 호스트는 대상 IP 주소를 포함하는 ARP 브로드캐스트를 전송한다.



# 쓸모 없는 ARP 분석

쓸모없는 ARP들은 주로 네트워크에서 다른 호스트나 발신지와 같은 IP 주소를 가졌는지 식별하기 위해 사용한다. 모든 호스트는 IP 주소가 정적이나 동적으로 할당되는지 여부에 상관없이 쓸모없는 ARP를 전송한다. 시도마다 1초를 기다리는데, 3번의 시도 후에 다른 1초 동안 응답이 없으면 IP 스택을 초기화 하기 위해 새로 시작할 수 있다. 쓸모없는 ARP가 응답을 받으면 다른 호스트는 이상적인 IP 주소를 사용한다. 이것은 일반적으로 IP 주소 개시 작업을 정지하라는 ‘IP 주소 중복’ 경고를 생성한다.

# 프로토콜 유형

이 필드는 프로토콜 주소 유형을 정의한다. 이 필드는 이더넷 II 프레임 구조에 사용되는 표준 프로토콜 ID 값을 사용한다. 이 프로토콜 유형은 [www.iana.org/assignments/protocol-numbers](http://www.iana.org/assignments/protocol-numbers)에 정의되어 있다.

* 하드웨어 주소 길이

이 필드는 해당 패킷에 사용되는 물리 주소의 길이(Byte)를 정의한다. 이 필드는 물리 유형 필드에 의해 결정된 값이기 때문에 여분의 필드다.

* 프로토콜 주소 길이

이 필드는 패킷에 사용되는 프로토콜(네트워크) 주소의 길이(바이트)를 정의한다. 이 필드는 프로토콜 유형 필드에 의해 결정된 값이기 때문에 여분의 필드다.

* Opcode

이것은 요청이나 응답 패킷인지와 발생하는 주소 해결 유형을 정의한다. RARP는 MAC 주소로부터 네트워크 주소를 얻게 해주는 프로세스다. RARP는 RFC 903, ‘역방향 주소 변환 프로토콜’에 정의되어 있다.

1 – ARP request

2 – ARP reply

3 – RARP request

4 – RARP reply

* 발신자 하드웨어 주소

이 필드는 요청과 응답을 전송하는 장치의 물리 주소를 나타낸다.

* 발신자의 프로토콜 주소

이 필드는 프로토콜이나 네트워크, 요청과 응답을 전송하는 장치의 주소를 나타낸다.

* 대상 하드웨어 주소

이 필드는 요구되는 대상 하드웨어 주소를 표시한다. ARP 요청에서 이 필드는 일반적으로 0으로 채워진다. ARP 응답에서 이 필드는 ARP 요청을 전송하는 장치의 물리 주소를 함께 포함한다.

* 대상 프로토콜 주소

이 필드는 요청에 있는 요구되는 대상의 프로토콜이나 네트워크 주소를 표시한다. 응답에서 이것은 요청이 발생한 주소를 포함한다.

# ARP 트래픽 필터링

ARP 트래픽을 위한 캡처 필터 구문은 간단하게 arp다. 이 디스플레이 필터 구문은 간단하게 arp다.

Arp.opcode == 0x0001

ARP 요청

Arp.opcode = 0x0002

ARP 응답

Arp.src.hw\_mac == xx:xx:xx:xx:xx:xx

ARP 발신 물리 주소는 xx:xx:xx:xx:xx:xx (요청 혹은 응답)이다.

(arp.src.hw\_mac == xx:xx:xx:xx:xx:xx) && (arp.opcode == 0x0001)

발신 물리 주소 xx:xx:xx:xx:xx:xx에 대한 ARP 요청

(arp.src.hw\_mac == xx:xx:xx:xx:xx:xx) && !(arp.src.proto\_ipv4 == 192.168.1.1)

Xx:xx:xx:xx:xx:xx에 호스트에 있는 ARP 패킷은 자신의 IP 주소(192.168.1.1)를 알리지 않는다.

(arp.opcode == 0x0002) && !(arp.src.proto\_ipv4 == 192.168.0.1/16)

할당된 주소 ARP 패킷은 원격 장치(ARP proxy 응답)에 대한것이다. Proxy ARP를 조심하라.

# IPv4

IPv4는 RFC 791에 정의되어 있고, IP는 연결된 시스템에 대한 데이터그램 전송 서비스뿐만 아니라, 낮은 MTU 네트워크에 대한 단편화와 재조립 기능을 제공합니다. 또한 IP는 특정 트래픽에 대한 우선순위를 매기기 위해 서비스 품질 지정 기능을 제공한다.

IP는 비연결형이고 신뢰할 수 없는 프로토콜이며, IP 호스트 간에 데이터 그램을 위한 최선의 전달 서비스를 제공한다. IP는 스스로 대상 위치에 패킷이 도착한 경우를 확인하기 위한 방법을 제공하지 않는다. 전달 보장을 요하는 애플리케이션은 IP를 통한 TCP를 사용해야 한다.

IP 헤더는 대개 20바이트의 길이를 갖지만, IP 헤더 길이를 늘일 수 있는 옵션 필드를 포함한다. ( 4바이트 씩 증가)

# 일반적인 IPv4 트래픽 분석

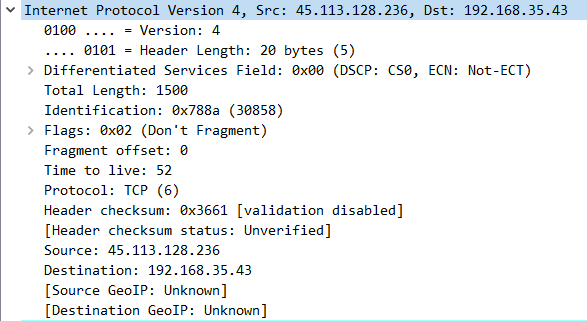
일반적인 IPv4 통신은 가장 효과적인 패킷 크기를 이용해 한 장소에서 다른 장소로 패킷을 옮긴다.

IP 패킷들이 라우터에 의해 전송됨으로써 대상 IP 주소는 경로를 결정하기 위해 검사되고, MTU 크기는 다음 링크의 MTU 크기(단편화가 필요하고, 허용된 경우를 확인하기 위해)를 검사한다. MAC 헤더는 분석되고 다음 네트워크에 대해 새로운 값이 적용 되며, IP 헤더의 time to live 값은 감소한다. 또한 IP 헤더는 우선순위를 전달하기 위해 검사된다.

IPv4 통신에서 모든 동작이 잘 작동하면 트래픽은 IP 주소로부터 송/수신될 것이다. 헤더에 IP 주소는 NAT/PAT 장치가 트래픽을 가로채고 주소를 수정하지 않는 한 바뀌지 않아야 한다.

패킷이 경로상에서 다음 링크에 전송되기까지 너무 먼 경우에 라우터는 IP 헤더의 단편화 설정을 조사한다. 단편화 비트가 설정되지 않으면 패킷은 전송될 수 없다. 라우터는 MTU 제한을 정의하는 ICMP 유형 3, 코드 4 메시지를 패킷 발기인(생성자)에게 전송해야 한다. 발기인(생성자)은 작은 패킷 크기로 패킷을 재전송해야 한다. 단편화가 허용된다면 라우터는 하나의 커다란 패킷을 두개 이상의 작은 패킷으로 분할하고, 단편화 오프셋을 정의하며, 그 패킷들이 단편화되었음을 지정한 후에 전송한다.

# IPv4 패킷 구조 분석



* 버전 필드

IP 헤더의 첫 번째 필드는 버전Version 필드다. IPv4는 Version 값이 4이다.

* 헤더 길이 필드

이 필드는 ‘인터넷 헤더 길이’ 필드나 IHL에도 언급되어 있다. 이 필드는 오직 IP 헤더의 길이를 나타낸다. IP 헤더는 옵션을 지원하기 때문에 이는 필수적이며 다양한 길이를 가질 수 있다. 이 필드 값은 4바이트 배수로 제공된다.

* 차별화된 서비스 필드와 명시적 혼잡 알림



6비트의 차별화된 서비스 필드(DiffServ)는 트래픽의 우선순위를 결정하고, 일정 수준의 서비스 품질Qos을 제공하고자 사용된다. 이 필드는 차별화된 패킷을 다루는 방법(per-hop behavior, 홉당 동작)을 경정하는 데 사용되는 차별화된 서비스 코드 포인트(DSCP, Differentiated Services Code Point) 값을 포함한다.

<http://www.ktword.co.kr/abbr_view.php?m_temp1=2578>

DSCP 자세한 사이트

* + 보증된 전달과 홉당 신속한 전달 동작

Assured Forwarding PHB Group인 RFC 2597은 Assured Forwarding을 DiffServ 공급자가 DiffServ 고객으로부터 수신한 IP 패킷들을 대한 전달 보장에 대한 서로 다른 레벨을 제공하는 수단으로서 정의했다. RFC2598에서는, 신속한 전송 PHB를 낮은 손실, 낮은 지연, 낮은 지터, 보증된 대역폭, DS(DiffServ) 도메인을 통한 종단-대-종단 서비스를 구축하기 위해 사용할 수 있다. 이런 서비스는 점-대-점 연결이나 ‘가상 임대 회선’ 같은 종단점에 나타난다. 또한 이런 서비스는 프리미엄 서비스로서 서술된다고 정의한다. 빠른 전송을 제공하기 위해 46의 DSCP 값을 검색하는 DiffServ를 제공한다..

2 비트의 명시적 혼잡 알림ECN 필드는 경로를 통한 네트워크 혼잡을 식별하기 위해 전송자나 경로에 따른 라우터로 사용된다.

IP 헤더의 DiffServ와 ECN 섹션은 예전에는 서비스 유형(TOS, Type of Service) 필드로 사용됬다.

* 전체 길이 필드

이 필드는 IP 헤더의 길이와 유효한 데이터의 길이를 정의한다(이것은 모든 데이터 링크 채워 넣기는 포함하지 않음).

* 식별 필드

각 개별 IP 패킷은 전송되었을 때 유일한 ID 값을 할당받는다. 패킷이 작은 패킷 크기를 지원하는 네트워크에서 크기를 맞추기 위해 단편화되는 경우 같은 ID 번호는 이런 단편화들이 같은 원본 패킷의 일부라는 것을 나타내기 위해 각 단편화에 위치 될 것이다.

* + 무한 반복되는 패킷을 찾기 위해 IP ID 필드를 사용

동일한 패킷들로 반복 실행 중인 네트워크를 분석할 때 IP 헤더 ID 필드와 단편화 설정을 조사해야 한다. IP ID 필드가 각 패킷마다 다르다면 패킷은 반복될 수 없다. 호스트는 분할 패킷에 대한 네트워크로 가득찰 것이다. 따라서 호스트를 찾아야 하고 닫아야 한다. 하지만 IP ID 필드가 같고 패킷이 단편화되지 않으면(모든 단편화 설정은 같은 IP ID값을 포함한다) 사용자는 네트워크를 반복하는 같은 패킷이라고 가정할 수 있다. 문제의 원인은 기반 구조 순환을 살펴보라.

* 플래그 필드

플래그 필드는 실제로 3비트의 길이이며, 아래와 같은 할당된 비트 값을 가진다.

Bit 0 – 예약됨, 0으로 설정

Bit 1 – 단편화 비트가 아님 (0=단편화, 1=단편화가 아님)

Bit 2 – 더 단편화된 비트 (0=마지막 조각, 1=전송될 조각이 더 있음)

<http://egloos.zum.com/tokyoiron/v/237368>

* Fragment 오프셋 필드

패킷이 단편화된다면 Fragment 오프셋 필드는 조각이 단일 패킷에서 재조립될 때 이런 패킷의 데이터를 어디에 위치시켜야 하는지 표시한다. Fragment 오프셋 필드는 8바이트 값으로 오프셋을 제공한다. 예를 들어 첫 번째 조각은 0의 오프셋을 가지며, 1400바이트의 데이터를 포함할 것이다. 두 번째 조각은 175(175\*8 = 1400)의 오프셋 값을 가진다. 이 필드는 패킷이 단편화된 경우에만 사용된다. 그렇지 않으면 0으로 설정된다.

* Time to Live 필드

이 필드는 패킷의 남은 수명(라우터를 통과할 때마다 초로 표시)을 표시한다. 일반적으로 TTL 초기 값은 32, 60, 128이다.

기본 TTL 값들은 공급 업체의 TCP/IP 스택에 포함되어 있다. 애플리케이션(traceroute 같은)은 이런 기본 값들을 원하는 값으로 재정의할 수 있다. 라우터에 의해 패킷이 전송되는 시간마다 라우터는 TTL 필드를 1씩 감소시킨다. 라우터가 확장된 주기(1초 이상)에 대해 큐에 패킷을 보관해야 한다면 그 시간만큼 TTL 값을 감소시켜야하고, 패킷은 큐에 보관될 뿐만 아니라 한 홉당 TTL 값을 감소시켜야 한다.

패킷이 라우터에 TTL =1로 도착하면 TTL 값을 0으로 감소시킨 후 패킷을 전송할 수 없기 때문에 라우터는 패킷을 폐기해야 한다. 라우터는 패킷이 Time to Live 값 때문에 전송될 수 없다고 나타내는 ICMP 유형 11, 코드 0 응답을 수신자에게 전달할 것이다. ( 시간 초과, Time To Live 전송 시간이 초과됨).

패킷이 단편화된 경우 모든 조각은 같은 TTL 값을 할당받는다. 네트워크를 통해 다른 경로를 받는다면 다양한 TTL 값으로 목적지에 도착할 것이다. 하지만 첫 번째 조각이 목적지에 도착할 때 목적지 호스트는 매 초 패킷의 TTL 값을 1씩 감소시킬것이다. 모든 조각은 시간이 만료되거나 조각 설정이 ‘미완성’과 사용할 수 없다고 간주되기 이전에 도착해야 한다. 목적지는 패킷의 수명이 재조립 과정 중에 만료되었다고 표시하기 위해 ICMP 유형 11, 코드 1 응답(시간 초과, 단편화 재조립 시간 초과)을 목적지에 전송한다. 이것은 원래 단편화되지 않은 패킷을 재전송하기 위해 클라이언트에 알려준다.

* 프로토콜 필드

모든 헤더는 다음에 어떤 것이 수신될지 정의하는 필드를 가진다. 예를 들어 TCP/IP 패킷에서 이더넷 II 헤더는 다음으로 IP가 수신된다는 것을 표시하기 위한 유형 필드를 가진다. IP 헤더는 무엇이 다음에 수신될지 표시하기 위한 프로토콜 필드를 가진다.

1 – ICMP

2 – IGMP

6 - TCP

8 – EGP

9 – Cisco의 IGRP 같은 사설 내부 게이트웨어

17 – UDP

45 – IDRP

88 – Cisco EIGRP

89 – OSPF

* 헤더 체크섬 필드

IP 헤더 체크섬 필드는 IP헤더에만 구성되어 있는 오류 검출 기능을 제공한다. 이 필드는 IP 헤더에만 존재한다. 이 체크섬은 계산을 할 때 자기 자신을 포함하지 않는다.

* 발신지 주소 필드

이것은 패킷을 전송한 장치의 IP 주소다. DHCP 재시작 작업 같은 일부 경우에 클라이언트는 이 IP 주소를 모를 것이며, 따라서 이 필드에서 0.0.0.0을 사용할 것이다. 이 필드는 멀티캐스트나 브로드캐스트 주소를 포함할 수 없다.

* 목적지 주소 필드

이 필드는 유니캐스트, 멀티캐스트, 브로드캐스트(IPv6의 경우에도) 주소를 포함할 수 있다. 이 주소는 패킷의 최종 목적지이다.

* 옵션 필드

IP 헤더는 옵션의 수에 따라 확장될 수 있다. 헤더가 옵션에 의해 확장된 경우 인터넷 헤더 길이(IHL) 필드가 헤더 길이를 4바이트 단위로 정의하기 때문에 이런 옵션들은 4바이트 단위로 끝나야 한다. [www.iana.org](http://www.iana.org)

0 – 옵션 목록의 종료 ( IP 옵션이 종료될 때 정의)

3 – 느슨한 발신지 경로( 일부 경로 정보 제공)

4 – 타임스탬프( 경로에 따른 타임스탬프)

7 – 경로 기록( 라우터가 통과한 경로 표시)

9 – 엄격한 발신지 경로( 상세 경로 정보 제공)

# 브로드캐스트/멀티캐스트 트래픽

네트워크에는 브로드캐스트/멀티캐스트의 2가지 기본 유형이 있다. 검색과 공지가 그것이다. 시스템이 부팅되고 새로운 IP 주소를 필요로 할 때 DHCP 클라이언트가 디스커버리 브로드캐스트를 전송하고, DHCP 서버를 찾는 것이 바로 조회의 한 예이다. 검색의 다른 예는 ARP MAC-대-IP 주소 결정 브로드캐스트다.

* 일반 브로드캐스트 255.255.255.255
* 서브넷 브로드캐스트 10.2.255.255
* 멀티캐스트 224.X.X.X – 239.X.X.X