<네트워크 해킹 hw2>

20160926 월 밤

ARP(Address Resolution Protocol)
- 배경 : 호스트의 IP를 아는 것만으론 MAC 주소를 이용해 통신하는 계층에서의 프레임 전달이 불가능 => ARP을 통해 IP와 MAC주소간의 동적 매핑을 제공
동적인 이유는 매핑이 자동으로 이뤄지며 변경이 발생하여도 시스템 관리자에 의해 재구성을 요구하지 않은채로 변경이 적용되기 때문입니다.

- IPv4에서만 사용이 됩니다. IPv6의 경우는 ICMPv6에 포함되있는 NDP사용

- 동일 브로드캐스트 도메인 내에서 브로드캐스트를 이용해 ARP Request를 송신합니다.

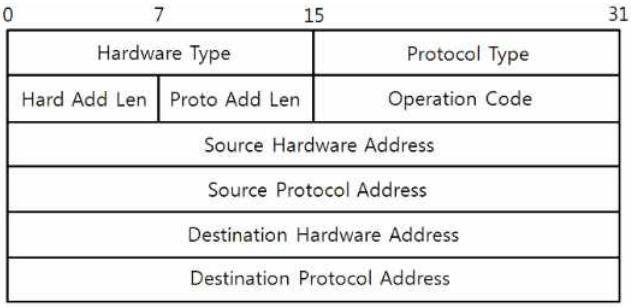
MAC주소
- 배경 : NIC제조업체에서 정해진 규칙에 의해 임의로 만들어진 주소를 장치 내부의 영구메모리에 저장한 값. 48bit(6bytes)로 구성

[그림 1] MAC 주소

ARP ex)
송신자A: 10.0.0.1 => 수신자B: 10.0.0.2 (실제 통신은 http://www.example.com으로 요청시 DNS 질의를 통해 알게된 10.0.0.1과 같은 32bit형식의 주소를 이용하여 진행하게 된다)

1. 송신자 A는 B의 MAC 주소를 알기 위해 ARP Request 패킷을 브로드캐스팅한다.
2. ARP Request 안에 지정된 IP주소를 가진 호스트B만이 자신의 MAC 주소를 입력한 ARP Reply 패킷을 송신자 A에게 유니캐스트로 응답한다. 이 때 수신자 B는 송신자 A의 IP와 MAC주소를 알게되며 나중에 사용하기 위해 ARP 테이블에 기록한다.
가정 : 송신자가 곧 패킷을 전송할 것이며, 그 패킷을 수신한 수신자 B의 시스템또한 A에게 응답 패킷을 전송할 것에 기초
cf. 수신자 B 이외의 다른 호스트는 ARP Requst 패킷을 무시한다.

ARP 구조



[그림 2] ARP 구조

Hardware Type : MAC주소의 유형을 나타내며 이더넷의 경우는 항상 1
Protocol Type : 매핑 대상인 프로토콜 주소의 유형을 나타내며 IPv4의 경우 0x0800(2048)

Hardware Address Length : MAC주소의 길이를 바이트로 나타낸다. 이더넷은 6
Protocol Address Len : 프로토콜 주소의 길이를 바이트로 나타낸다. IPv4는 4
Operation Code : ARP의 구체적인 동작을 나타냄 1 or 2

[표 1] Operation Code 값

값	동작
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply

Source Hardware Address : 송신자의 MAC주소

Source Protocol Address : 송신자의 IP주소

Destination Hardware Address : 수신자의 MAC 주소
(request시 FF:FF:FF:FF:FF:FF -> 브로드캐스팅)

Destination Protocol Address : 수신자의 IP 주소

gateway(게이트웨이)
현재 사용자가 위치한 네트워크에서 다른 네트워크로 이동하기 위해 반드시 거쳐야 하는 거점을 의미. 프로토콜이 다른 네트워크 상의 컴퓨터와 통신하려면 두 프로토콜을 적절히 변환해 주는 변환기가 필요한데, 게이트웨이가 그 역할을 한다. 라우터와 동일한 개념으로 이해가능, 공유기도 게이트웨이다. 공유기는 PC의 네트워크와 인터넷을 연결하여 유저가 웹사이트에 접근할 수 있도록 관문을 열어준다. 로컬 네트워크의 통신 프로토콜(ex netbios)와 인터넷의 통신 프로토콜(ex http)가 다르기 때문이다. LAN에선 게이트웨이없이 스위치나 허브만 있어도 되지만 인터넷에 접근하려면 게이트웨이가 필요. 게이트웨이에도 중복되지 않는 IP 주소가 필요하다. 보통 컴퓨터에 할당된 IP 주소중 끝자리만 다르고 1로 지정.

#
* victim ip는 인자
- 내 MAC주소& ip주소& 게이트웨이ip확인 : ipconfig -all 하면 나옴
=> 이 소스파일 찾아보자
- victim mac주소 확인 : by arp request
- gateway mac주소 확인 : by arp request <아직은 필요 x>

victim mac구하는건 ping [victim ip] 한후에
arp -a | findstr [victim ip]하면 나오네..

arp request로 victim mac을 알기위해선!

Ethernet	
Dst MAC	FFFFFF-FFFFFF
Src MAC	내 MAC<(ipconfig/all)로 알아낼것>
Protocol	0x0806
ARP	
Hardware Type	1
Protocol Type	2048 (0x0800)
HLen	6
PLen	4
Operation	1(Request)
Sender MAC	내 MAC
Sender IP	내 IP
Target MAC	000000-000000(모름)
Target IP	gateway IP

표 1 ARP request

Ethernet	
Dst MAC	victim MAC (유니캐스트이므로)
Src MAC	내 MAC<(ipconfig/all)로 알아낼것>
Protocol	0x0806
ARP	
Hardware Type	1
Protocol Type	2048 (0x0800)
HLen	6
PLen	4
Operation	2(Reply)
Sender MAC	내 MAC
Sender IP	게이트웨이 IP
Target MAC	Victim MAC?
Target IP	Victim IP?

표 2 ARP Reply