

[IT Essential] Network #3 - L3 Router

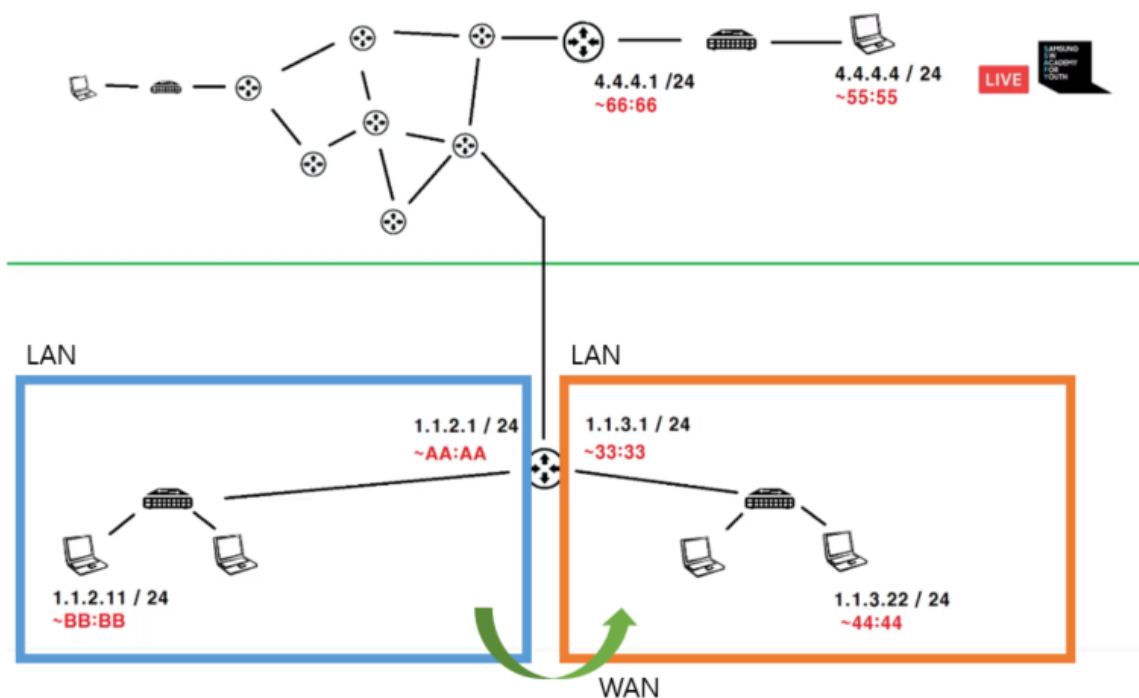
진행자: 최인국 컨설턴트님

날짜: 2021-02-03

목차

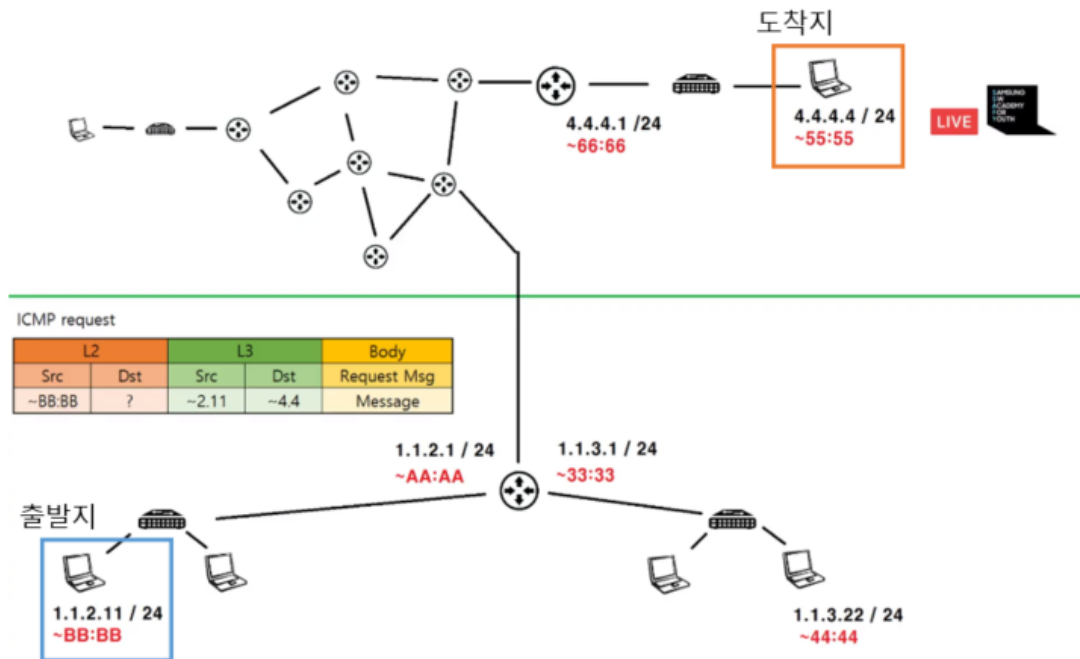
1. [L3 Router 패킷 전달 과정](#)
 - 1-1. [WAN으로 ICMP request 보내기](#)
 - 1-2. [WAN으로 ICMP response 보내기](#)
2. [네트워크 분리하기](#)
3. [IPv4 고갈 문제](#)
4. [Wireshark](#)

1. L3 Router 패킷 전달 과정



- 초록선 아래는 사내망, 위는 인터넷이다. 그림과 같이 LAN들은 L3 Router로 연결되어있으며, **WAN**으로 가기 위해서는 **L3 Router**를 반드시 거쳐야한다.
- 저번 시간에는 LAN 내에서 호스트 간에 ICMP request를 보내는 방법에 대해 알아보았다.
- 이번에는 **ICMP request**를 LAN이 아닌 외부, 즉 **WAN**으로 보내는 방법을 알아보자.

1-1. WAN으로 ICMP request 보내기



- 왼쪽 아래의 1.1.2.11/24 에서 4.4.4.4/24 로 ICMP request 패킷을 보낸다고 가정하자.

ICMP request

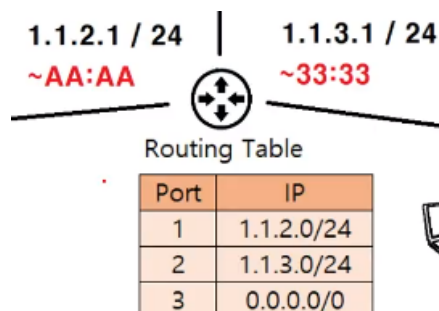
L2		L3		Body
Src	Dst	Src	Dst	Request Msg
~BB:BB	?	~2.11	~4.4	Message

- 출발지에서 보낼 ICMP request 패킷의 모습이다. L2 계층에는 출발지와 도착지의 MAC 주소, L3 계층에는 출발지와 도착지의 IP 주소 정보가 들어가야한다. 그러면 L2 계층의 도착지 MAC 주소는 어떤 것이 들어가야할까?

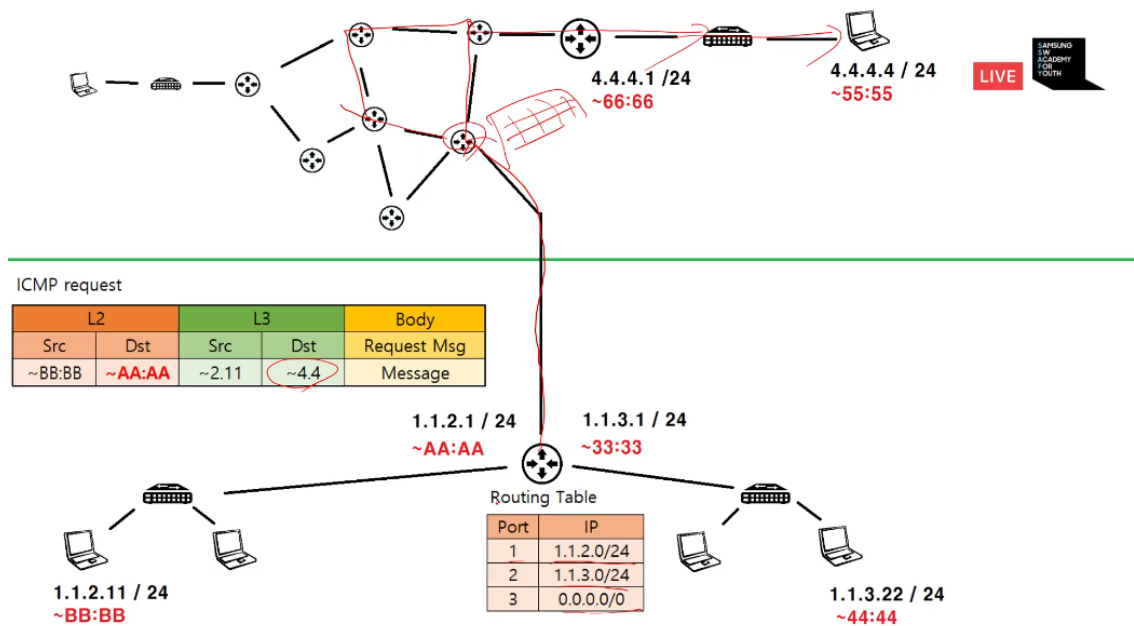
ICMP request

L2		L3		Body
Src	Dst	Src	Dst	Request Msg
~BB:BB	~AA:AA	~2.11	~4.4	Message

- 보내진 패킷은 먼저 L2 Switch를 거친다. 최종 도착지의 MAC 주소는 ~55:55지만 다른 LAN에 있는 호스트이기 때문에 L2 Switch가 가지고 있는 **forwarding** 테이블에 최종 도착지 정보가 있을 수 없다. 따라서 패킷의 L2 계층에는 도착지 정보에 LAN 상에서 최종 목적인 gateway의 MAC 주소가 들어간다.



- 패킷을 받은 L3 Router는 어디로 보내야할지 결정하기 위해 **Routing 테이블**을 본다. Routing 테이블에는 Port 정보와 IP 주소 정보가 담겨있는데, 예를 들어 1번 포트에는 1.1.2에 해당하는 네트워크를 가진 LAN이 연결되어있는 것이다. 3번 포트는 0.0.0.0/0이 등록되어 있는데, 이는 1과 2번 포트에 속하지 않는 모든 패킷이 해당되는 **default router**다. 우리가 보내려는 패킷은 3번 포트를 통해 보낸다.



- WAN으로 나간 Router는 계속해서 L3 Router들을 거쳐서 최종 도착지까지 도달한다. 패킷을 받은 호스트는 다시 **ICMP response** 패킷을 보낸다.

1-2. WAN으로 ICMP response 보내기

ICMP response

L2		L3		Body
Src	Dst	Src	Dst	Response Msg
~55:55	~66:66	~4.4	~2.11	Message

- ICMP response 패킷의 도착지도 역시 **L2 계층에 LAN 상에서 최종 목적지인 gateway의 MAC 주소가 기입**되고, 패킷은 L3 Router를 거쳐서 도착지가 속한 LAN의 L3 router까지 도달한다.

ICMP response

L2		L3		Body
Src	Dst	Src	Dst	Response Msg
~AA:AA	~BB:BB	~4.4	~2.11	Message

- 도착지가 있는 LAN의 L3 Router에서 response 패킷은 위와 같이 L3 계층의 정보는 이전과 동일하지만 **L2 계층의 정보가 바뀐다**. 출발지는 gateway의 MAC 주소, 도착지는 최종 도착지의 MAC 주소 정보를 가지게 된다. L3 Router도 **ARP 테이블**을 가지고 있는데, 이를 이용해서 최종 도착지의 MAC 주소를 찾는다. 경우에 따라서는 MAC 주소를 알아내기 위해 ARP request(broadcast)를 먼저 보내야 할 수도 있다.

업체들에게 준다. 국가별로 어떤 IP 대역을 할당 받을지를 정하는 곳은 **IANA(Internet Assigned Numbers Authority)**다.

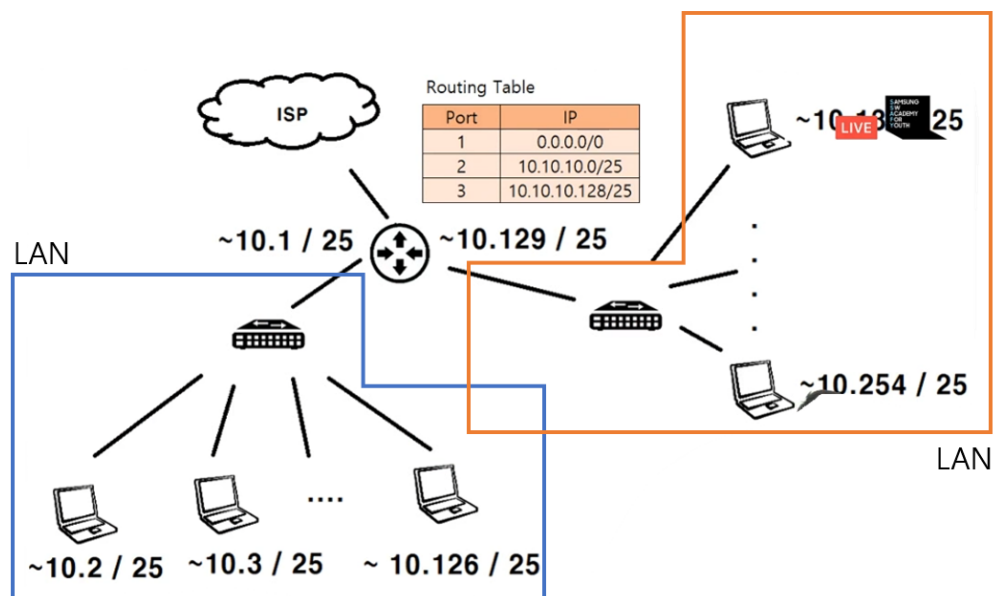
- 만약 부여 받은 IP를 사용하는 그룹 또는 사용 목적에 따라 네트워크 분리를 하고 싶으면 어떻게 할까?

Network				Host	
00001010	00001010	00001010	00000000		10.10.10.0
11111111	11111111	11111111	00000000		255.255.255.0
Network				Host	
00001010	00001010	00001010	00000000		10.10.10.0
11111111	11111111	11111111	10000000		255.255.255.128
Network				Host	
00001010	00001010	00001010	10000000		10.10.10.128
11111111	11111111	11111111	10000000		255.255.255.128

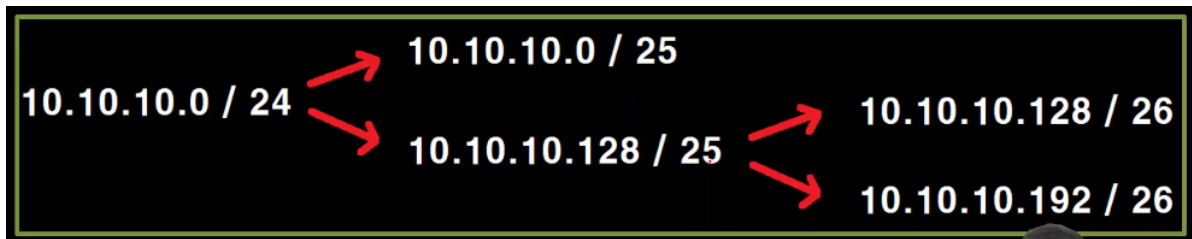
- IP 주소는 서브넷 마스크에 의해 네트워크 영역과 호스트 영역으로 나뉘는데, 보통은 가장 위와 같이 네트워크 영역의 비트 개수는 24다. 하지만 부여 받은 IP를 두 개의 네트워크로 분리하고 싶으면, **네트워크 영역의 비트 수를 하나 늘리면 된다.** 즉, 끝자리를 0으로 하는 네트워크와 끝자리를 1로 하는 네트워크로 나누면 된다.



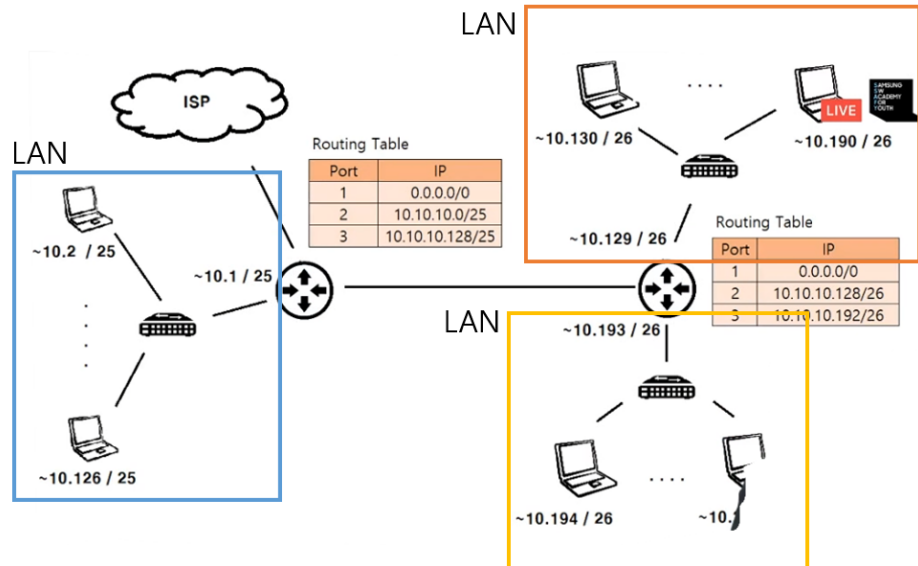
- 결국 10.10.10.0/25와 10.10.10.128/25로 나눌 수 있으며, 서브넷 마스크는 24에서 비트가 하나 늘어난 25가 된다.



- 결과적으로 위의 그림과 같이 **두 개의 LAN**으로 나뉘어지며, Routing 테이블도 그에 맞게 정보가 변경된 것을 볼 수 있다.



- 만약 네트워크를 또 나누고 싶으면 아까처럼 네트워크 영역의 비트 수를 하나 더 늘리면 된다. 넷마스크는 25에서 비트 수 하나 늘어난 26이 된다.



- 결국 위의 그림과 같이 3개의 LAN으로 나뉘어진 것을 볼 수 있다.

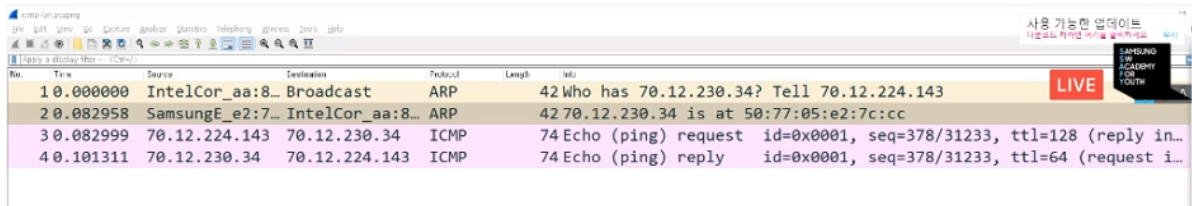
3. IPV4 고갈 문제

- $2^{32} \approx$ 약 46억개(특수 용도 제외, 약 36억 개)
- 국가별 IP 주소 대역 할당
- IPV4 이미 고갈
- NAPT 기술 연명
- 근본적인 해결책 : IPV6

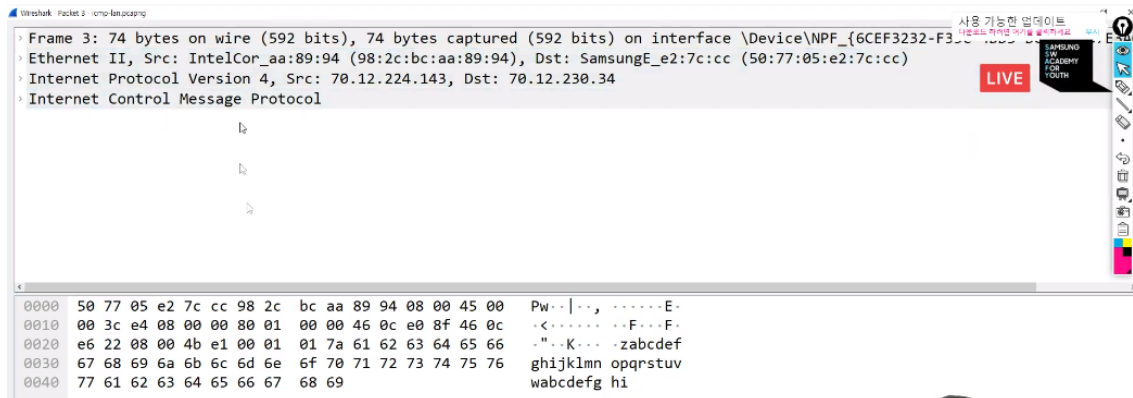
- IPV4는 4바이트로, 약 36억 개의 IP를 전세계가 나눠서 사용한다. IANA가 국가별로 사용할 수 있는 IP 주소 대역을 할당해준다.
- IPV4는 이미 국가들에게 나눠 줄 수 있는 IP 주소가 모두 고갈되었다. 한국은 약 1억 개 정도의 IPV4 주소를 할당 받았는데, 아직 한국은 할당 받은 주소가 모두 고갈되지는 않았다. NAPT 기술 활용과 같은 방식으로 연명하고 있지만 언젠가는 IPV4 주소가 고갈 될 것이며, 근본적인 해결책은 IPV6를 사용하는 것이다.

4. Wireshark

- [Wireshark](#)는 오픈 소스 패킷 분석 프로그램으로, 네트워크 분석, 소프트웨어 및 통신 프로토콜 개발, 교육 등에 사용된다.



- 상단의 노란색 부분은 **ARP request, ARP response**, 아래의 분홍색 부분은 **ICMP request, ICMP response**에 대한 정보다. Wireshark를 이용하면 위와 같이 패킷의 정보를 자세히 살펴볼 수 있다.



- 위의 그림은 wireshark를 통해서 본 **ICMP request** 패킷의 세부 모습이다. 두번째 줄은 L2 계층, 세번째 줄은 L3 계층의 정보를 보여주고 있다.