

네트워크 개론 Part 5

: 네트워크에서의 IP 패킷 이동

글. 조인준 KBS 미디어기술연구소 차장

C군의 네버엔딩 스토리

지난 연재까지는 IP 주소에 관해 다루었습니다. 그렇다면 이제 IP 주소를 이용하여 네트워크에서 패킷이 어떻게 호스트 디바이스 간에 이동하는지 [그림 1]을 통해 설명 드리겠습니다. [그림 1]의 각 장치는 IP 주소와 MAC 주소를 가지고 있고, 네트워크 스위치나 라우터 주변의 ①, ②, ③ 등의 숫자는 다른 장치와 연결된 포트 번호이며, 네트워크마다 네트워크 주소와 서브넷 마스크를 CIDR(네트워크 개론 Part 4 참조)로 표기하였습니다.

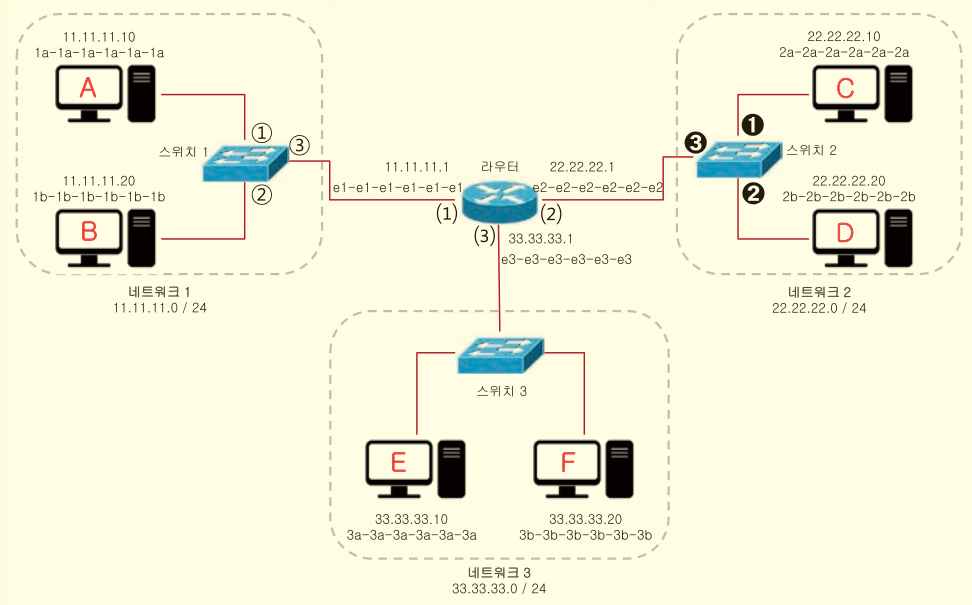


그림 1. 라우터로 연결된 세 개의 네트워크

[그림 1]의 장치들에 IP 주소와 MAC 주소가 함께 적혀있는 이유는 IP 네트워크를 구현하는 이더넷을 통해 데이터를 전달할 경우 수신 장치의 IP 주소와 MAC(Media Access Control) 주소를 모두 알아야 전송이 가능하기 때문입니다. MAC 주소는 16진수를 이용하여 e5-30-2b-ff-d8-a2 또는 e5:30:2b:ff:d8:a2 등과 같이 표시되며 IP 주소와 같은 논리적 주소가 아닌 하드웨어에 할당된 고유 식별 주소입니다. 적절한 비유일지 모르겠지만, 사람으로 이야기하면 사람과 사람을 구분하기 위한 정보 중에 지문이 MAC 주소, 이름이나 아이디 등이 IP 주소와 비슷하다고 보셔도 될 것 같습니다

니다. 지문은 사람이 생체적으로 지니고 태어나 변경할 수 없지만, 이름이나 아이디 등은 필요에 따라 절차 등을 거쳐 바꿀 수 있습니다. 마찬가지로 MAC 주소는 하드웨어가 제조될 때 하드웨어에 심어져 변경이 불가능한 반면, IP 주소는 네트워크의 변경 등 필요에 따라 바꿀 수 있습니다.

IP 패킷의 전송은 같은 네트워크 내에서의 전송과 서로 다른 네트워크 간의 전송으로 나누어 설명하겠습니다.

동일 네트워크 내에서의 IP 패킷 전송

앞서 말씀드렸듯이 다른 장치에 IP 패킷을 전송하기 위해서는 해당 장치의 IP 주소와 MAC 주소를 모두 알아야 합니다. 이 때문에 데이터를 보낼 장치의 IP 주소만 알고 MAC 주소를 모르는 경우에는 ARP(Address Resolution Protocol)를 이용하여 수신 장치의 MAC 주소를 알아내고 이를 ARP 테이블로 관리하여 추후 IP 패킷 전송에 사용합니다. ARP를 이용하여 데이터를 수신할 장치의 MAC 주소를 알아내는 과정의 설명을 위해 [그림 1] '네트워크 1'의 A 장치로부터 B 장치에 IP 패킷을 전송해야 하는 상황을 가정합니다.

A 장치는 서브넷 마스크와 B 장치의 IP 주소를 통해 두 장치 모두 같은 '네트워크 1'에 속해 있음을 알 수 있으나 B 장치의 MAC 주소는 모릅니다. B 장치의 MAC 주소를 알기 위해 A 장치는 '네트워크 1'에 연결된 모든 장치에 ARP Request를 보냅니다. A 장치가 보내는 ARP Request는 [표 1]의 정보를 포함하는 ARP 패킷에 이더넷 헤더를 붙인 [그림 2]의 패킷으로 전송이 됩니다. [그림 2]의 이더넷 헤더에 들어있는 송신 장치 MAC 주소와 수신 MAC 주소를 주목해주세요.

구분	내용
A 장치(송신) 관련 정보	MAC 주소 : 1a-1a-1a-1a-1a-1a IP 주소 : 11.11.11.10
B 장치(수신) 관련 정보	IP 주소 : 11.11.11.20

표 1. ARP Request 포함 정보 (A → 네트워크 1의 모든 장치)



그림 2. A 장치에서 송신하는 ARP Request

A 장치가 ARP Request를 '네트워크 1'의 모든 장치에 전달하기 위해서는 우선 '스위치 1'에 보내어 네트워크 내에 브로드캐스팅(Broadcasting) 해야 합니다. 이를 위해 [그림 2]와 같이 ARP 패킷의 이더넷 헤더에 수신 MAC 주소를 ff-ff-ff-ff-ff-ff로 설정합니다. ff-ff-ff-ff-ff-ff는 예약되어 있는 MAC 주소로써 네트워크 스위치에 연결된 모든 장비에 해당 패킷을 전송하게 합니다. '스위치 1'은 A 장치가 보낸 ARP Request 패킷을 받으면 이더넷 헤더를 검사하여 ARP Request를 보낸 A 장치의 MAC 주소는 1a-1a-1a-1a-1a-1a이며 자신의 ①번 포트에 연결되어 있다는 것을 자신의 MAC 테이블에 없으면 기록하고 ①번 포트를 제외한 모든 포트로 A 장치의 ARP Request를 발송합니다.

이때 '스위치 1'은 A 장치가 보낸 패킷이 ARP 관련 패킷인지 아닌지 아무런 관심이 없으며 송신 MAC 주소와 수신 MAC 주소만 보고 패킷을 MAC 테이블에 의해 적절한 포트로 보냅니다. 이렇게 '네트워크 1' 전체로 전파된 ARP Request는 B 장치와 라우터에 전달되고, ARP Request에 포함된 수신 장치 IP 주소를 보고 자신에게 온 Request임을 확인한 B 장치는 A 장치의 IP 주소와 MAC 주소를 자신의 ARP 테이블에 기록한 후 A 장치에 ARP Reply를 보냅니다. ARP Request를 받은 라우터는 자신에게 온 것이 아님을 확인 후 해당 ARP Request를 버립니다.

구분	내용
B 장치(송신) 관련 정보	MAC 주소 : 1b-1b-1b-1b-1b-1b IP 주소 : 11.11.11.20
A 장치(수신) 관련 정보	MAC 주소 : 1a-1a-1a-1a-1a-1a IP 주소 : 11.11.11.10

표 2. ARP Reply 포함 정보 (B → A)



그림 3. B 장치에서 송신하는 ARP Reply

B 장치가 A 장치로 보내는 ARP Reply는 [표 2]의 정보를 포함하는 데이터에 이더넷 헤더를 붙인 [그림 3]의 패킷으로 전송이 됩니다. B 장치는 A 장치의 IP 주소와 MAC 주소를 모두 알고 있으므로 브로드캐스팅 된 ARP Request와 달리 이더넷 헤더와 ARP 패킷에 A 장치의 MAC 주소와 IP 주소를 특정하여 ARP Reply를 보냅니다. B 장치가 보낸 ARP Reply 패킷을 수신한 ‘스위치 1’은 이더넷 헤더로부터 ARP Reply를 보낸 B 장치의 MAC 주소는 1b-1b-1b-1b-1b-1b이며 ②번 포트에 연결되어 있다는 것을 자신의 MAC 테이블에 없으면 기록하고, 패킷을 수신하는 A 장치의 MAC 주소는 ①번 포트를 통해 연결되어 있다는 것을 MAC 테이블 조회를 통해 알아낸 후 해당 포트인 ①번 포트에 패킷을 전달합니다. 이렇게 ARP Reply가 ARP Request를 보낸 A 장치에 수신되면 A 장치는 자신의 ARP 테이블에 IP 주소 11.11.11.20과 MAC 주소 1b-1b-1b-1b-1b-1b를 기록합니다. 이로써 B 장치의 MAC 주소를 알게 된 A 장치는 [그림 4]와 같은 이더넷 헤더를 붙인 IP 패킷으로 B 장치에 보낼 데이터를 ‘스위치 1’로 전송하고, A 장치와 B 장치의 MAC 주소와 해당 포트 번호를 MAC 테이블로 갖고 있는 ‘스위치 1’은 이더넷 헤더 정보를 보고 해당 포트에 패킷을 전송하여 A 장치와 B 장치 사이에 IP 패킷을 이용한 데이터 통신이 이루어지게 됩니다.



그림 4. A 장치에서 B 장치로 보내는 패킷

서로 다른 네트워크 간의 IP 패킷 전송

그렇다면 서로 다른 네트워크에 속하는 장치들 간의 IP 패킷 전송은 어떻게 이루어질까요? [그림 1] ‘네트워크 1’의 A 장치가 ‘네트워크 2’의 D 장치에 데이터를 보내는 경우를 생각해보겠습니다. 앞서와 같이 A 장치는 D 장치의 IP 주소는 알고 있으나 MAC 주소는 모른다고 가정합니다. A 장치는 자신의 서브넷 마스크와 D 장치의 IP 주소 22.22.22.20을 보고 D 장치가 자신이 속한 네트워크(11.11.11.0)와는 다른 네트워크(22.22.22.0)에 속한 장치라는 것을 알 수 있습니다. 다른 네트워크로 IP 패킷을 내보내기 위해서는 게이트웨이 역할을 하는 라우터를 통과해야 합니다. 이때, A 장치가 라우터의 ‘네트워크 1’ 포트 (1)의 IP 주소만 알고 MAC 주소는 모른다면 라우터로 IP 패킷을 보낼 수 없으므로 라우터의 ‘네트워크 1’ 포트 (1)의 IP 주소 11.11.11.1을 적어 ARP Request를 보냅니다. ARP Request가 ‘스위치 1’을 통해 ‘네트워크 1’에 브로드캐스팅 되고 ‘스위치 1’의 MAC 테이블에 ARP Request를 수신한 A 장치와 연결된 포트 번호 ①과 A 장치의 MAC 주소가 기록되는 등의 절차는 앞서의 예와 같습니다.

라우터가 아닌 다른 장치들에서 A 장치의 ARP Request는 버려지고 라우터만이 A 장치의 IP 주소와 MAC 주소를 ARP 테이블에 기록한 후 ARP Reply를 보냅니다. 라우터의 ARP Reply를 통해 라우터의 '네트워크 1' 포트 (1)의 MAC 주소를 알게 된 A 장치는 자신의 ARP 테이블에 라우터의 '네트워크 1' 포트 (1)의 IP 주소와 MAC 주소를 기록하고 [그림 5]와 같이 D 장치에 보낼 IP 패킷을 만들어 라우터의 '네트워크 1' 포트 (1)의 MAC 주소로 보냅니다.

이더넷 헤더	IP Packet
A 장치(송신) MAC 주소 : 1a-1a-1a-1a-1a-1a 라우터(수신) MAC 주소 : e1-e1-e1-e1-e1-e1	A 장치(송신) IP 주소 : 11.11.11.10 D 장치(수신) IP 주소 : 22.22.22.20

그림 5. A 장치에서 D 장치로 보내는 패킷(송신 : A 장치, 수신 : 라우터 포트 (1))

그런데 [그림 5]를 유심히 보신다면 흥미로운 점을 발견하실 수 있습니다. '네트워크 1'의 A 장치에서 '네트워크 2'의 D 장치로 보내는 패킷의 이더넷 헤더의 수신 MAC 주소는 라우터의 '네트워크 1' 포트 (1)의 MAC 주소인데, IP 패킷의 수신 주소는 라우터 포트 (1)의 IP 주소가 아닌 최종적으로 IP 패킷을 수신할 D 장치의 IP 주소입니다.

A 장치로부터 [그림 5]의 패킷을 받은 라우터는 수신 IP 주소가 22.22.22.20인 것을 보고 자신의 (2)번 포트에 연결된 '네트워크 2'에 속하는 장치로 전달되어야 할 패킷이라는 것을 알 수 있습니다. 만약 라우터가 IP 주소 22.22.22.20을 갖는 D 장치의 MAC 주소를 모른다면 자신의 (2)번 포트를 통해 '네트워크 2'에 D 장치의 IP 주소를 적은 ARP Request를 보냅니다. ARP Request가 '스위치 2'를 통해 '네트워크 2'에 브로드캐스팅 되고 '스위치 2'의 MAC 테이블에 ARP Request를 송신한 라우터와 연결된 스위치 포트 번호 ❹과 라우터 '네트워크 2' 포트 (2)의 MAC 주소가 기록되는 등의 절차는 역시 앞서와 같습니다. D 장치가 아닌 다른 장치에서 라우터의 ARP Request는 버려지고 D 장치만이 라우터의 '네트워크 2' 포트 (2)의 IP 주소와 MAC 주소를 자신의 ARP 테이블에 기록한 후 라우터에 ARP Reply를 보냅니다. D 장치의 ARP Reply를 통해 D 장치의 MAC 주소를 알게 된 라우터는 자신의 ARP 테이블에 D 장치의 IP 주소와 MAC 주소를 기록하고, A 장치가 D 장치로 보내기 위해 자신에게 보낸 [그림 5]의 패킷에서 이더넷 헤더의 송신/수신 MAC 주소를 [그림 6]과 같이 교체하여 '스위치 2'를 통해 D 장치의 MAC 주소로 보냅니다.

이더넷 헤더	IP Packet
라우터(송신) MAC 주소 : e2-e2-e2-e2-e2-e2 D 장치(수신) MAC 주소 : 2b-2b-2b-2b-2b-2b	A 장치(송신) IP 주소 : 11.11.11.10 D 장치(수신) IP 주소 : 22.22.22.20

그림 6. A 장치에서 D 장치로 보내는 패킷(송신 : 라우터 포트 (2), 수신 : D 장치)

[그림 6]을 보시면 A 장치가 라우터로 보낸 [그림 5]의 전체 패킷 중에 IP Packet은 바뀌지 않았고 이더넷 헤더의 송신 → 수신 MAC 주소만 [A 장치 MAC 주소 → 라우터 포트 (1)]에서 [라우터 포트 (2) → D 장치 MAC 주소]로 바뀌었습니다. 다소 복잡해 보이지만 정리하면 다른 네트워크로 IP 패킷을 전송할 때에는 수신 장치의 MAC 주소로 직접 데이터를 보내는 것이 아니라, 자신의 네트워크와 연결된 라우터 포트의 MAC 주소로 데이터를 보낸 다음 라우터가 수신 장치가 있는 네트워크와 연결된 포트를 통해 데이터를 다시 보내는 방식으로 처리가 됩니다.

이상 같은 네트워크 내에서의 IP 패킷 전송 및 서로 다른 네트워크 간의 IP 패킷 전송에 대해 알아보았습니다.

다음 연재도 더욱 유익한 IP 네트워크 관련 내용으로 찾아뵙겠습니다. 📺