

네트워크 개론 Part 7

: NAT

글. 조인준 KBS 미디어기술연구소 차장

지난 '네트워크 개론 Part 6'에서는 로컬 네트워크의 IP 주소를 가진 호스트 디바이스들이 어떻게 공인 IP 주소를 사용하여 인터넷을 통해 데이터를 보내고 받을 수 있는지에 관한 소개가 주된 내용이었으며 로컬 네트워크의 사실 IP 주소를 공인 IP 주소로 바꾸는 NAT(Network Address Translation)과 PAT(Port Address Translation)에 관한 간략한 설명도 덧붙였습니다. 하지만, 독자 여러분의 직장 등에서 쓰는 로컬 네트워크와 인터넷이 어떻게 연결되는지에 관해 조금 더 자세히 설명 드린다면, 이후의 여러 IP 네트워크 관련 기술들의 이해에 관해서도 도움이 될 수 있을 것 같아서 NAT과 PAT에 관한 더 자세한 설명을 이어가 볼까 합니다.

지난 연재 말미에서 NAT을 Static NAT, Dynamic NAT으로 나누고 PAT은 별다른 구분 없이 하나로 설명하며 마무리했습니다. 하지만, PAT도 Static PAT과 Dynamic PAT으로 구분되며 NAT 또한 앞서 소개한 두 가지 방식 외에 Policy NAT과 Twice NAT 등도 있습니다. 이런 관계로 우리가 일상적으로 네트워크를 활용하고 이해하는데 필요한 범위 내에서 Static NAT, Dynamic NAT, Static PAT, Dynamic PAT, Policy NAT, Twice NAT 등을 설명하는 연재를 이어가 보도록 하겠습니다.

• Static NAT (Network Address Translation)

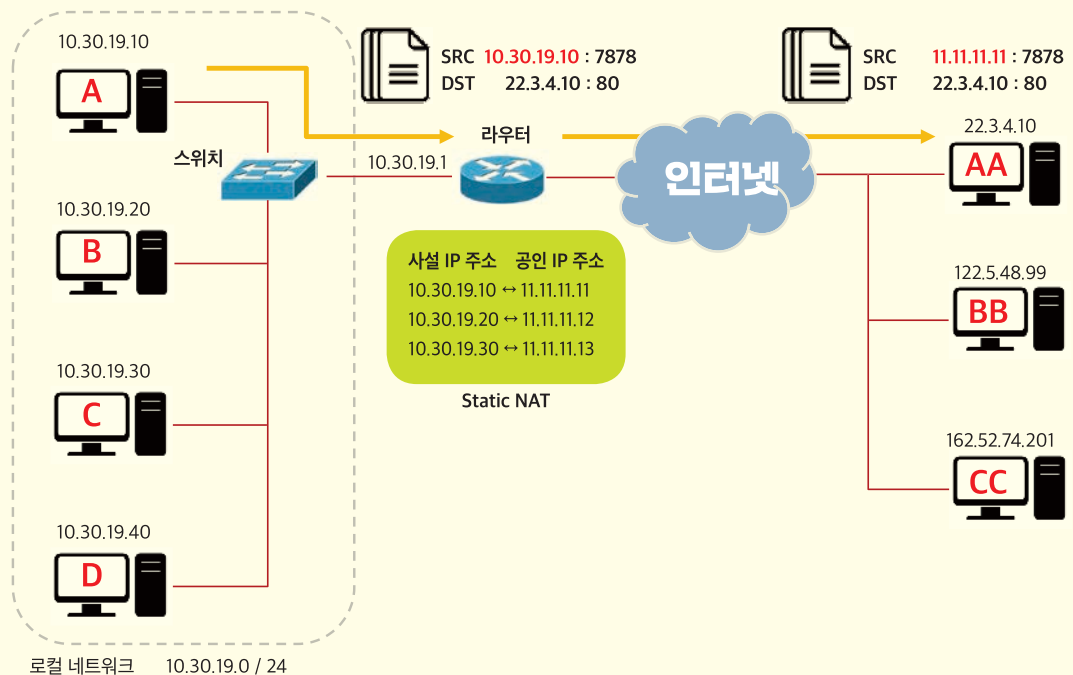


그림 1. Static NAT에 의한 호스트 디바이스 'A' 패킷의 주소 정보 변환

Static NAT은 [그림 1]의 녹색으로 표시한 블록과 같이 필요한 수만큼 공인 IP 주소를 할당받아 사설 IP 주소를 가진 호스트 디바이스에 라우터를 통해 1:1로 고정적 매핑을 하는 방식입니다. [그림 1]의 녹색 블록을 보시면 사설 IP 주소(로컬 네트워크에서 호스트 디바이스에 할당된 IP 주소)들인 10.30.19.10, 10.30.19.20, 10.30.19.30은 각각 인터넷과 연결 시 공인 IP 주소인 11.11.11.11, 11.11.11.12, 11.11.11.13으로 라우터에서 변환이 되도록 설정되어 있습니다. [그림 1]의 노란색 화살표로 표시된 것과 같이 사설 IP 주소 10.30.19.10을 갖는 호스트 디바이스 'A'가 인터넷상의 공인 IP 주소를 갖는 서버 'AA'에 IP 패킷을 보내는 상황을 가정해 보겠습니다. IP 패킷에는 패킷을 보내는 호스트 디바이스의 IP 주소(SRC: Source), 패킷을 받는 호스트 디바이스의 IP 주소(DST: Destination) 및 호스트 디바이스들이 실제로 IP 패킷을 처리하는 프로세스 등을 구분하기 위한 포트번호(IP 주소 뒤 ':' 이후의 번호)가 포함되어 있습니다. [그림 1]의 호스트 디바이스 'A'가 인터넷상의 호스트 디바이스 'AA'의 공인 IP 주소 22.3.4.10 및 자신의 패킷을 받아주는 포트번호 80을 알고 있다면, 'AA'에게 패킷을 보내거나 받기 위한 자신의 포트번호 7878을 통해 송신 장치의 IP 주소 및 포트번호(SRC) 10.30.19.10 : 7878, 수신 장치의 IP 주소 및 포트번호(DST) 22.3.4.10:80이 담긴 패킷을 라우터로 보냅니다. 외부의 IP 주소를 목적지로 갖는 패킷이 왜 라우터로 전달되는 지는 이전의 연재를 보시면 알 수 있습니다. 라우터로 보내진 패킷은 이제 공인 IP 주소만 허용되는 인터넷으로 나가야 합니다. 이를 위해 라우터는 패킷의 송신 장치 주소를 미리 설정된 Static NAT을 통해 10.30.19.10 → 11.11.11.11로 수정합니다. 이제 인터넷에서 바라보면 [그림 1]의 패킷은 공인 IP 주소 11.11.11.11로부터 송신된 패킷이 됩니다. 여기서 눈여겨보실 것은 IP 패킷에 포함된 IP 주소 및 포트 정보 중, IP 주소만 라우터를 통해 수정된다는 것입니다. NAT에서는 패킷 내부의 포트 번호 정보는 그대로 유지된다는 점을 꼭 기억하시기 바랍니다.

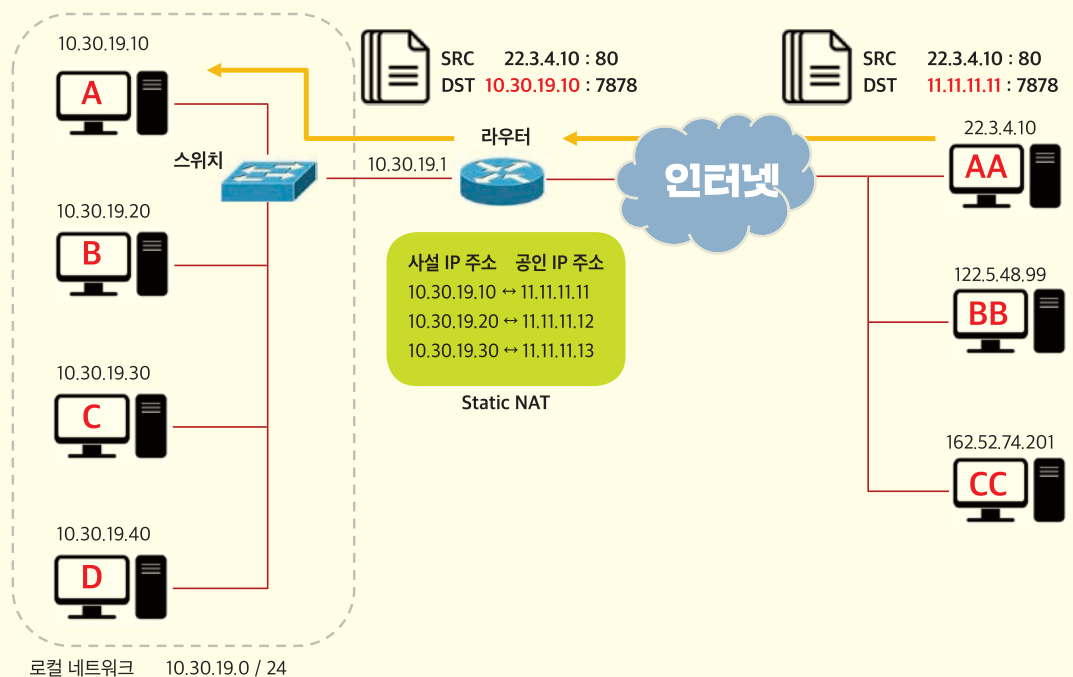


그림 2. Static NAT에 의한 호스트 디바이스 'AA' 패킷의 주소 정보 변환

[그림 1]과 같이 라우터를 통한 '사설 IP → 공인 IP' 수정을 통해 'A'로부터 'AA'에 패킷이 전달되고 그 처리 결과에 대해서 'AA'가 'A'에게 패킷으로 회신하는 경우를 [그림 2]와 같이 가정해 보겠습니다. 'AA'는 'A'로부터 패킷을 받아서 처리 후에 그 결과를 회신하는 패킷을 보낼 때 송신 장치 IP 주소 및 포트번호(SRC) 22.3.4.10:80, 수

신 장치 IP 주소 및 포트번호(DST) 11.11.11.11:7878이 패킷에 담깁니다. 이 패킷이 인터넷을 통해 공인 IP 주소 11.11.11.11을 사용하는 [그림 2]의 라우터에 도달하면 라우터는 녹색 블록과 같이 설정된 Static NAT을 통해 패킷의 공인 IP 주소 11.11.11.11을 사설 IP 주소 10.30.19.10으로 변환하여 로컬 네트워크의 호스트 디바이스 'A'에게 보냅니다. 이때도 포트번호는 그대로 유지되며 패킷 내부의 '공인 IP → 사설 IP' 수정만 일어납니다. 이렇게 라우터에서 미리 설정된 사설 IP와 공인 IP의 매칭을 통해 로컬 네트워크의 호스트 디바이스가 인터넷상의 호스트 디바이스와 통신할 수 있게 하는 방식이 Static NAT이며 사설 IP와 공인 IP의 매칭이 미리 설정되어 있기 때문에 'A'가 먼저 인터넷상의 호스트 디바이스에 연결을 시작하던지, 인터넷상의 호스트 디바이스가 'A'에게 먼저 연결을 시작하던지 상관없이 작업을 진행할 수 있습니다. 그러나 [그림 1], [그림 2]의 호스트 디바이스 'D'와 같이 공인 IP 주소와의 매칭이 정의되지 않은 사설 IP 주소를 가진 경우는 인터넷상의 호스트 디바이스와 통신을 할 수 없습니다. 마지막으로 Static NAT은 공인 IP 주소에 대응되는 사설 IP 주소를 1:1로 설정하여 라우터에서 변환하는 방식이므로 공인 IP 주소를 절약할 수 있는 방식은 아닙니다.

• Dynamic NAT

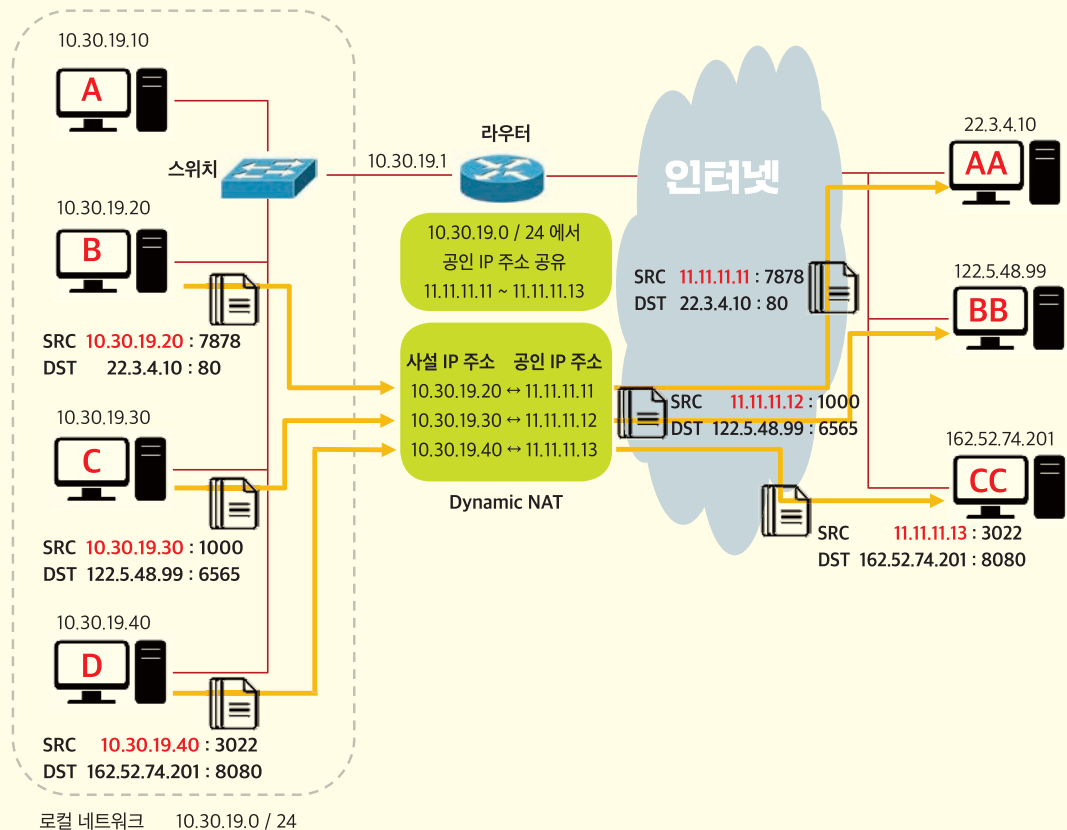


그림 3. Dynamic NAT에 의한 공인 IP 주소 배정 및 패킷의 주소 정보 변환

Dynamic NAT은 [그림 3]의 녹색으로 표시한 블록의 내용과 같이 몇 개의 공인 IP 주소를 할당받은 후 라우터를 통해 동적으로 로컬 네트워크의 호스트 디바이스에 할당된 사설 IP 주소에 매핑하여 로컬 네트워크의 호스트 디바이스들이 인터넷에 연결될 수 있게 하는 방식입니다. 설명을 위해 [그림 3]과 같이 라우터에 11.11.11.11 ~ 11.11.11.13 세 개의 공인 IP 주소가 할당되어 있고 이 공인 IP 주소들을 Dynamic NAT으로 로컬 네트워크의 호스트 디바이스들에 할당하는 상황을 생각해 보겠습니다. Dynamic NAT은 Static NAT과 달리 라우터가 사설 IP 주소와 공인 IP 주소를 고정적으로 매핑하지 않고 그때그때 필요에 따라 매핑하게 되므로 로컬 네트워크

크의 각 장비가 인터넷상의 호스트 디바이스에 연결되지 않으면 라우터 내부에 정해진 매핑이 존재하지 않습니다. 11.11.11.11 ~ 11.11.11.13이 특정 사설 IP 주소에 배정되지 않은 상황에서 [그림 3]의 'B'가 공인 IP 주소 22.3.4.10을 갖는 인터넷상의 호스트 디바이스 'AA'의 포트번호 80으로 패킷을 보낸다고 가정합니다. 이때 라우터는 현재 배정되지 않은 공인 IP 주소 중의 하나인 11.11.11.11을 'B'의 사설 IP 주소에 배정하여 라우터를 통과하는 'B'의 패킷의 송신 장치 IP 주소(SRC)를 11.11.11.11로 바꿉니다. 이후 'C'가 또 공인 IP 주소 125.5.48.99를 갖는 인터넷상의 호스트 디바이스 'BB'에 포트번호 6565로 패킷을 보내면 라우터는 남아 있는 공인 IP 중의 하나인 11.11.11.12를 'C'의 사설 IP 주소에 배정하여 라우터를 통과하는 'C'의 패킷의 송신 장치 IP 주소(SRC)를 11.11.11.12로 바꿉니다. 'D'의 경우에도 같은 방식으로 사설 IP 주소에 공인 IP 주소를 배정합니다.

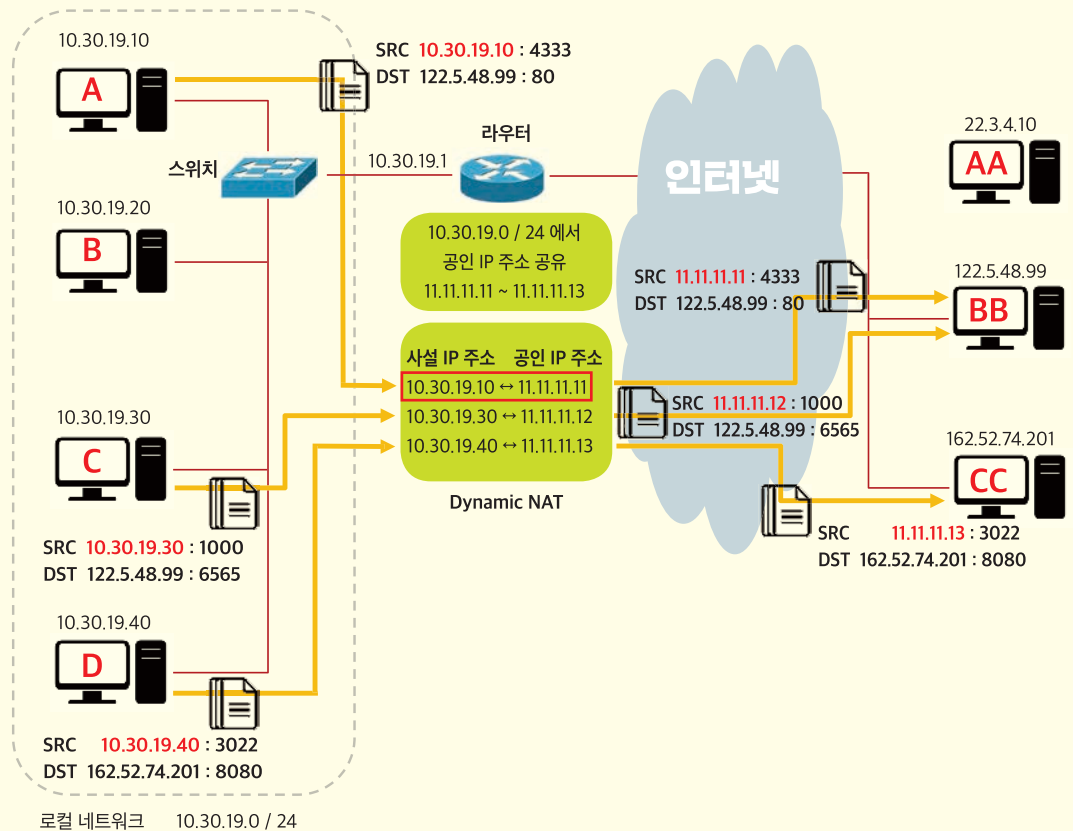


그림 4. Dynamic NAT에 의한 공인 IP 주소 배정 변화

그런데 'B', 'C', 'D'의 사설 IP 주소에 3개의 공인 IP 주소가 모두 배정되면 더 이상 공인 IP 주소를 배정할 수 없어서 'B', 'C', 'D' 중 하나가 연결을 끝내어 풀려난 공인 IP 주소가 'A'에게 배정될 때까지 'A'는 인터넷상의 호스트 디바이스와 연결될 수 없습니다. [그림 4]에 공인 IP 주소를 사용하던 'B'가 연결을 종료하여 공인 IP 주소 11.11.11.11이 사용 가능해지고 이를 'A'가 다시 배정받아 인터넷상의 호스트 디바이스에 패킷을 보내는 상황을 표시하였습니다. 'B'가 인터넷과의 연결을 종료하면 라우터는 공인 IP 주소 11.11.11.11을 회수하여 배정 가능한 상태로 둡니다. 이 상황에서 'A'가 공인 IP 주소 122.5.48.99를 갖는 인터넷상의 호스트 디바이스 'BB'에 포트번호 80으로 패킷을 보냅니다. 이때 라우터는 현재 배정되지 않은 공인 IP 주소 중의 하나인 11.11.11.11을 'A'의 사설 IP 주소에 배정하여 라우터를 통과하는 'A'의 패킷의 송신 장치 IP 주소(SRC)를 11.11.11.11로 바꾸어 줍니다. 지면 관계상 [그림 2]와 같이 반대 방향으로 패킷이 전달되는 설명을 포함하지는 않았지만 Dynamic NAT에서도 Static NAT과 같이 인터넷상의 호스트에서 로컬 네트워크의 호스트에게 패킷을 보낼 수 있습니다.

하지만, Dynamic NAT을 사용하면 한 가지 유의할 점이 있습니다. 지금까지의 설명과 같이 그때그때 공인 IP 주소를 사용하는 호스트 디바이스가 바뀌므로 인터넷상의 호스트 디바이스가 먼저 로컬 네트워크의 호스트 디바이스에 새로운 연결을 생성하여 패킷을 보낼 수는 없습니다. 그 이유를 가장 단적인 예인 [그림 5]를 통해 설명하겠습니다. 로컬 네트워크상의 호스트 디바이스들이 외부와의 연결을 모두 종료한 시점에서는 라우터에 할당된 모든 공인 IP 주소들이 배정 대기상태에 들어갑니다. 이 경우 인터넷상의 호스트 디바이스 'BB'가 라우터에 배정된 공인 IP 주소 중의 하나인 11.11.11.11로 패킷을 보낸다면 라우터는 'A'~'D' 중 어느 호스트 디바이스에 패킷을 전달해야 하는지 알 수가 없습니다. 이러한 이유로 Dynamic NAT의 경우 모든 연결은 로컬 네트워크의 호스트 디바이스들이 시작해야 하며, 인터넷상의 호스트 디바이스들이 연결을 시작할 수는 없습니다. 하지만 인터넷상의 호스트 디바이스들이 연결을 시작할 수 없다는 것이 로컬 네트워크의 호스트 디바이스에 회신으로 패킷을 보낼 수 없다는 이야기는 아닙니다. 로컬 네트워크의 호스트 디바이스들이 연결을 시작하고 이 연결이 유지되는 동안은 해당 사설 IP 주소와 공인 IP 주소의 매칭은 유효하기 때문에 인터넷상의 호스트 디바이스들이 로컬 네트워크의 호스트 디바이스에 패킷을 보내고, 로컬 네트워크의 호스트 디바이스들이 이를 정상적으로 수신할 수 있습니다.

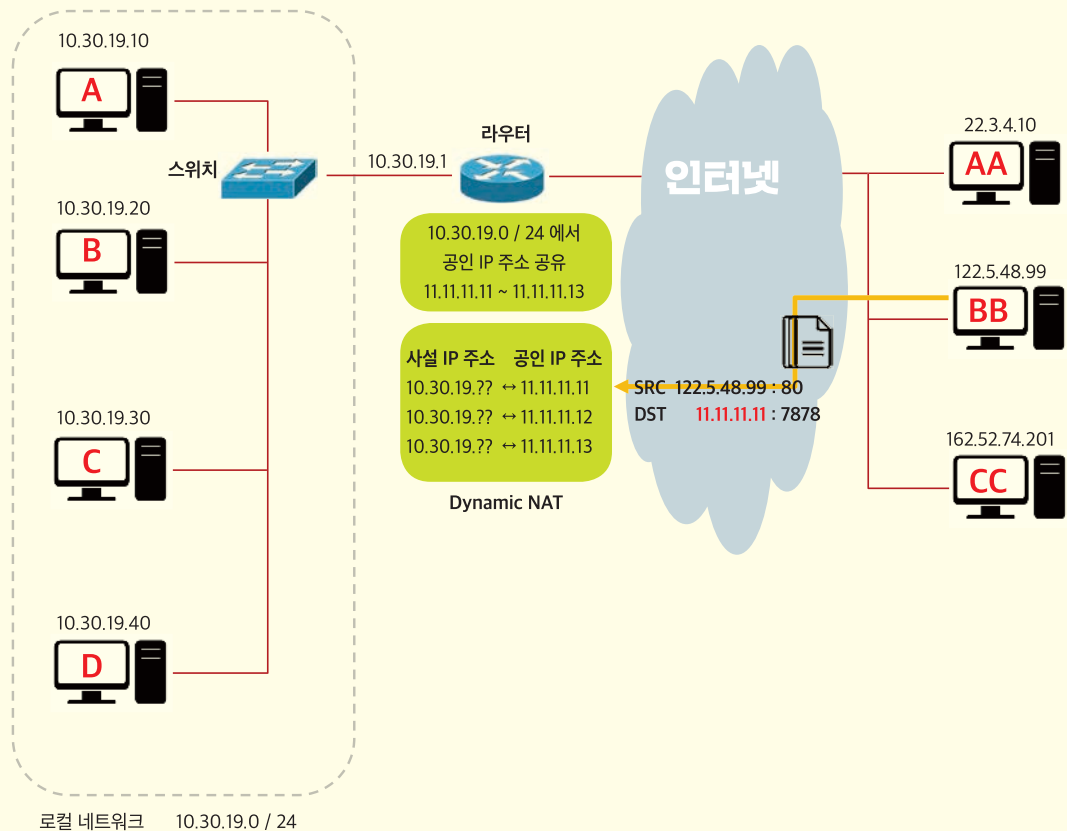


그림 5. 인터넷상의 호스트 디바이스가 연결 시작 시 Dynamic NAT의 문제

지금까지 Static NAT과 Dynamic NAT에 관해 설명해 드렸습니다. 다음 연재에서는 PAT에 관해 조금 더 깊이 들어가 보도록 하겠습니다. ☺