

네트워크 개론 Part 8

: PAT (Port Address Translation)

글. 조인준 KBS 미디어기술연구소 차장

지난 연재에서는 로컬 네트워크의 사설 IP 주소를 인터넷에서 사용 가능한 공인 IP 주소로 바꾸는 NAT(Network Address Translation)에 대해 다루며 NAT을 구현하는 몇 가지 방식 중 Static NAT과 Dynamic NAT에 관한 설명해 드렸습니다. 이번 연재에서는 사설 IP 주소를 공인 IP 주소로 바꾸는 또 다른 방법인 PAT(Port Address Translation)에 대해 이야기해보겠습니다.

이전에 간단히 설명해 드린 대로 하나의 공인 IP 주소를 하나의 사설 IP 주소에 맵핑하는 NAT과 달리 PAT은 포트 번호를 이용하여 하나의 공인 IP 주소를 다수의 사설 IP 주소로 맵핑할 수 있습니다. 포트 번호는 네트워크 서비스나 관련 프로세스를 구분하는 식별자라고 알려드렸으며, 하나의 IP 주소를 통해 받은 여러 종류의 데이터들을 각각의 처리 가능한 해당 프로세스로 전달할 수 있는 것이 데이터들이 포트 번호를 통해 처리 프로세스와 연결되기 때문입니다. PAT에도 NAT과 유사하게 Static PAT과 Dynamic PAT이 있습니다.

• Static PAT

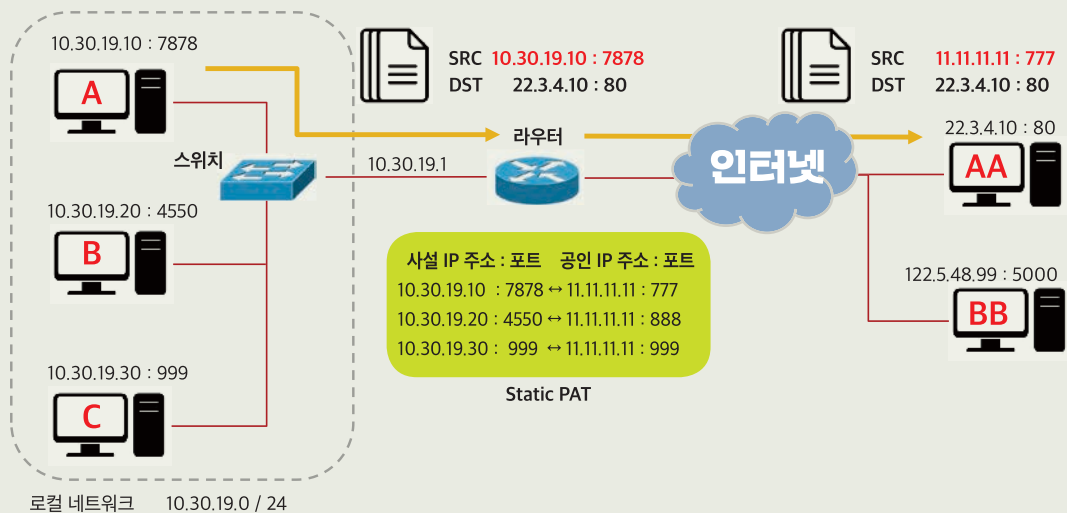


그림 1. Static PAT에 의한 호스트 디바이스 'A' 패킷의 IP 주소 정보 변환

Static PAT은 [그림 1]의 녹색으로 표시한 블록과 같이 동일한 공인 IP 주소에 포트 번호(IP 주소 뒤 ':' 표시 다음에 위치)를 달리하여 사설 IP 주소를 가진 로컬 호스트 디바이스들에 공인 IP 주소를 고정적으로 매칭하는 방식이며 NAT과 달리 IP 주소만을 맵핑하는 것이 아니라 'IP 주소 + 포트 번호'를 맵핑합니다. [그림 1]의 녹색 블록을 보시면 로컬 호스트 디바이스 'A'의 사설 IP 주소 10.30.19.10의 7878번 포트(10.30.19.10:7878)는 공인 IP 주소 11.11.11.11의 777번 포트(11.11.11.11:777), 로컬 호스트 디바이스 'B'의 사설 IP 주소 10.30.19.20의 4550

번 포트(10.30.19.20:4550)는 공인 IP 주소 11.11.11.11의 888번 포트(11.11.11.11:888), 마지막으로 로컬 호스트 디바이스 'C'의 사설 IP 주소 10.30.19.30의 999번 포트(10.30.19.30:999)는 공인 IP 주소 11.11.11.11의 999번 포트(11.11.11.11:999)로 변환이 되어 인터넷상의 다른 호스트 디바이스에 데이터를 보낼 수 있게 됩니다.

조금 더 자세히 [그림 1]의 'A'가 'AA'에 IP 패킷을 보내는 경우를 생각해보겠습니다. IP 패킷에는 패킷을 보내는 호스트 디바이스의 IP 주소와 포트 번호(SRC: Source), 패킷을 받는 호스트 디바이스의 IP 주소와 포트 번호(DST: Destination)가 포함되어 있습니다. [그림 1]의 'A'가 인터넷상의 'AA'의 공인 IP 주소와 해당 데이터를 보낼 포트 번호인 22.3.4.10:80을 알고 있다면, 자신의 포트 번호 7878을 통해 송신 장치의 IP 주소 및 포트 번호 (SRC) 10.30.19.10 : 7878, 수신 장치의 IP 주소 및 포트 번호(DST) 22.3.4.10:80이 담긴 패킷을 라우터로 보냅니다. 라우터로 보내진 패킷은 이제 공인 IP 주소만 허용되는 인터넷으로 나가야 합니다. 이를 위해 라우터는 패킷의 송신 장치 IP 주소와 포트 번호를 미리 설정된 Static PAT을 통해 10.30.19.10:7878 → 11.11.11.11:777로 수정합니다. 이제 인터넷에서 바라보면 [그림 1]의 패킷은 공인 IP 주소 11.11.11.11의 777번 포트(11.11.11.11:777)로부터 송신된 패킷이 됩니다.

여기서 중요한 점은 Static PAT에서는 정해진 IP 주소 및 포트 번호만 라우터를 통해 수정된다는 것입니다. 예를 들면 [그림 1]의 'A'에서 7878이 아닌 8484 같은 다른 포트 번호를 이용하여 라우터로 IP 패킷을 보내면 라우터는 Static PAT에 10.30.19.10:8484가 정의되어 있지 않으므로 이를 포트 번호가 달린 공인 IP 주소로 변환하지 않습니다. 이것이 NAT과 PAT이 다른 점입니다. NAT은 IP 주소만을 맵핑하는 방식이므로 어떤 포트 번호를 쓰든 상관하지 않고 같은 포트 번호로 '사설 IP 주소 ↔ 공인 IP 주소' 맵핑을 합니다. 하지만 PAT은 '사설 IP 주소 및 포트 번호 ↔ 공인 IP 주소 및 포트 번호'를 맵핑하므로 Static PAT에 설정되지 않은 포트 번호를 쓰면 같은 로컬 호스트 디바이스에서 IP 패킷을 송신하더라도 인터넷으로 나가지 못합니다. 다시 강조하자면 [그림 1]의 녹색 블록으로 표시된 Static PAT에서 10.30.19.30:999 ↔ 11.11.11.11:999도 'C'의 999번 포트에만 해당하는 변환이고, 'C'가 다른 포트 번호를 쓴다면 공인 IP 주소 맵핑이 일어나지 않습니다.

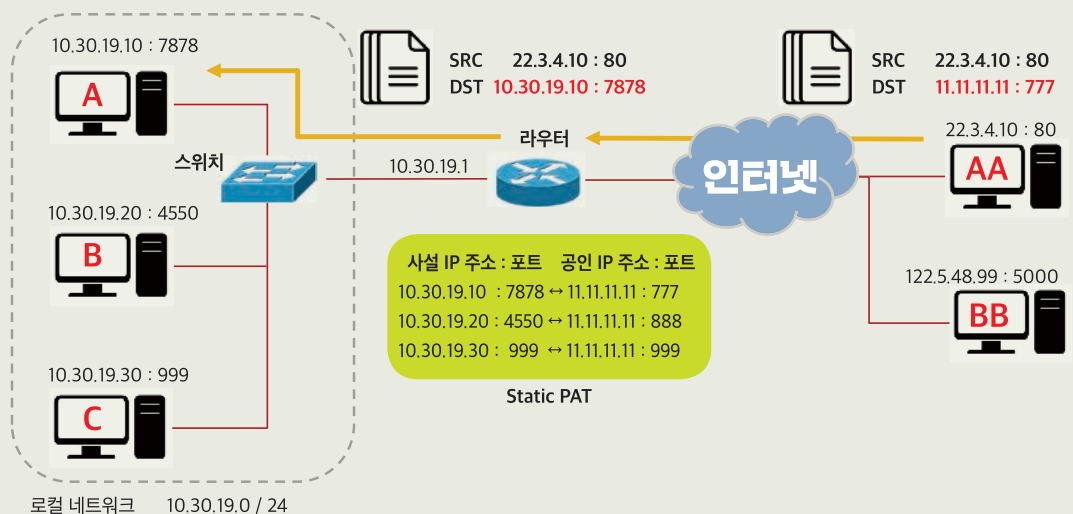


그림 2. Static PAT에 의한 호스트 디바이스 'AA' 패킷의 IP 주소 정보 변환

[그림 2]는 [그림 1]과 반대로 'AA'에서 'A'로 패킷을 보내는 경우입니다. 'AA'에서 'A'로 패킷을 보낼 때 송신 장치 IP 주소 및 포트 번호(SRC) 22.3.4.10:80, 수신 장치 IP 주소 및 포트 번호(DST) 11.11.11.11:777이 패킷에 담깁니다. 이 패킷이 [그림 2]의 라우터에 도달하면 라우터는 녹색 블록과 같이 설정된 Static PAT을 통해 패킷의

공인 IP 주소 및 포트 번호 11.11.11.11:777을 사설 IP 주소 및 포트 번호 10.30.19.10:7878로 변환하여 로컬 네트워크의 호스트 디바이스 'A'에 보냅니다.

Static PAT은 포트 번호를 포함한 '사설 IP 주소 및 포트 번호 ↔ 공인 IP 주소 및 포트 번호' 매핑을 고정적으로 정의하고 있으므로 로컬 네트워크의 호스트 디바이스들과 인터넷상의 호스트 디바이스 중 어느 쪽이 먼저 연결하든 상관 없이 데이터를 주고받을 수 있습니다. 또한 [그림 1]과 [그림 2]처럼 하나의 공인 IP 주소만을 사용하는 것이 아니라 복수의 공인 IP 주소를 사용해도 Static PAT은 가능합니다. 하나의 공인 IP 주소를 포트 번호를 통해 여러 로컬 네트워크의 호스트 디바이스가 사용 가능하므로 Static NAT과 달리 Static PAT은 공인 IP 주소 절약효과가 있습니다.

• Dynamic PAT

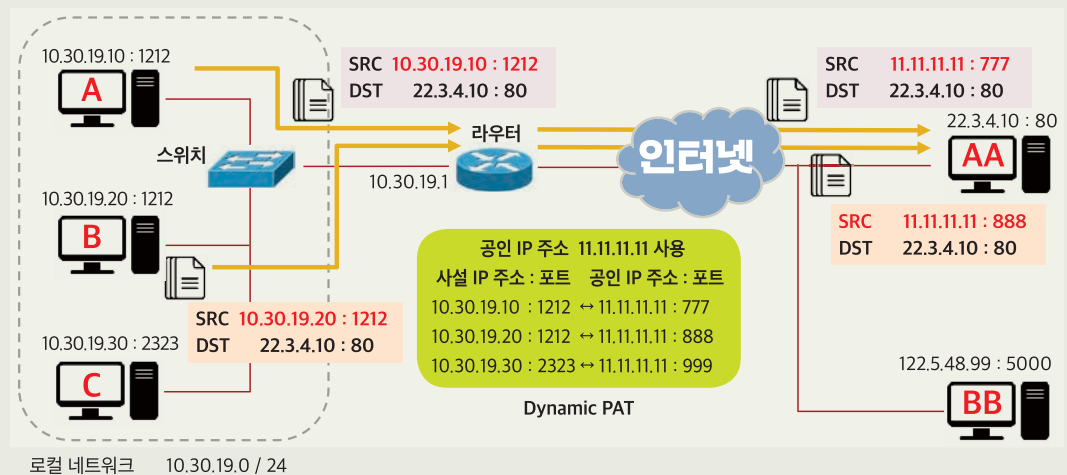


그림 3. Dynamic PAT에 의한 IP 주소 및 포트 번호 정보 변환

Dynamic PAT은 [그림 3]의 녹색으로 표시한 블록과 같이 라우터에서 중첩되지 않는 임의의 포트 번호를 공인 IP 주소에 붙인 후 로컬 네트워크의 사설 IP 주소 및 포트 번호에 할당하여 로컬의 호스트 디바이스들이 인터넷에 연결될 수 있게 하는 방식입니다.

조금 더 자세한 설명을 위해 [그림 3]과 같이 라우터에 공인 IP 주소 11.11.11.11이 할당되어 있고 이 공인 IP 주소에 임의의 포트 번호를 할당하여 로컬 호스트 디바이스들의 사설 IP 주소 및 포트 번호에 동적으로 매칭하는 과정을 살펴보겠습니다. Dynamic PAT은 Static PAT과 달리 라우터가 '사설 IP 주소 및 포트 번호 ↔ 공인 IP 주소 및 포트 번호'의 매핑을 고정해 놓지 않고 그때그때 필요에 따라 동적으로 포트 번호를 매핑하게 되므로 로컬 네트워크의 각 장비가 인터넷상의 호스트 디바이스에 연결되지 않으면 라우터 내부에 정해진 매핑이 존재하지 않습니다.

특정 매핑이 존재하지 않는 상황에서 [그림 3]의 'A'가 1212번 포트를 사용하여 공인 IP 주소 22.3.4.10을 갖는 인터넷상의 호스트 디바이스 'AA'의 포트 번호 80으로 패킷을 보낸다고 가정합니다. 이때 라우터는 배정받은 공인 IP 주소 11.11.11.11에 포트 번호 777을 동적으로 할당하여 'A'의 사설 IP 주소 및 포트 번호 10.30.19.10:1212에 매칭합니다. 이로써 라우터 내부에 '10.30.19.10:1212 ↔ 11.11.11.11:777' 매핑이 생성됩니다. 이어서 'B'가 'A'와 똑같이 1212번 포트로 'AA'의 80번 포트에 패킷을 보내면 라우터에서 777과 중첩되지 않는 888번 포트를 동적으로 할당하여 '10.30.19.20:1212 ↔ 11.11.11.11:888' 매핑이 추가되고, 마지막으로 'C'

가 2323번 포트를 사용하여 인터넷 어딘가로 패킷을 보내면 라우터는 또 중첩되지 않는 포트 번호인 999번 포트 번호를 동적으로 할당하여 '10.30.19.30:2323 ↔ 11.11.11.11:999' 맵핑을 추가합니다.

보시는 것처럼 임의로 포트 번호를 할당하기 때문에 'A'와 'B'가 같은 포트 번호로 'AA'에 데이터를 보내더라도 'AA'에서는 서로 다른 포트 번호로 'A'와 'B'를 구분할 수 있습니다. Dynamic PAT의 '사실 IP 주소 및 포트 번호 ↔ 공인 IP 주소 및 포트 번호' 맵핑은 'A'와 'AA' 같이 로컬 호스트 디바이스와 외부 호스트 디바이스의 연결이 유지되는 동안 유효하며 연결이 해지되면 같이 소멸하고, 새 연결이 생기면 다시 임의로 생성된 포트 번호를 공인 IP에 붙여서 할당해 줍니다. 또한, Dynamic PAT도 Static PAT과 같이 인터넷상의 호스트에서 로컬 네트워크의 호스트에게 패킷을 보낼 수 있지만, 이는 로컬 네트워크의 호스트가 먼저 연결을 시작했을 때만 가능합니다.

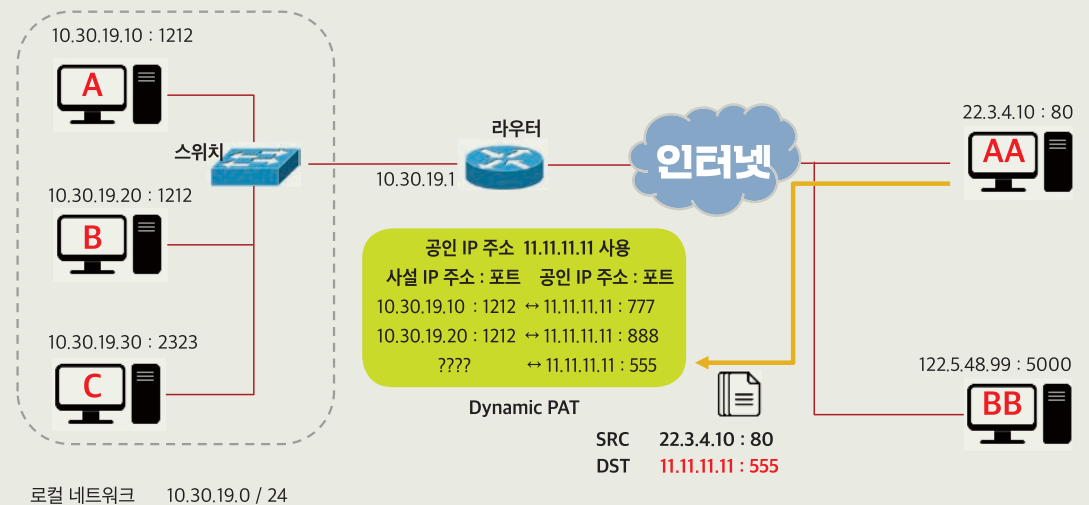


그림 4. 인터넷상의 호스트 디바이스가 연결 시작 시 Dynamic PAT의 문제

그 이유는 자명하지만, 노파심에 좀 더 설명을 추가하면, 앞의 내용을 보시며 Dynamic PAT도 Dynamic NAT과 유사하게 로컬 네트워크의 호스트 디바이스가 먼저 외부와 연결을 시도해야 라우터 내부에 '사실 IP 주소 및 포트 번호 ↔ 공인 IP 주소 및 포트 번호'의 매핑이 생성된다는 것을 알아차리셨을 것 같습니다. 이런 이유로 [그림 4]와 같이 인터넷상의 호스트 디바이스 'AA'에서 먼저 11.11.11.11:555 등과 같이 맵핑이 생성되지 않은 공인 IP 주소 및 포트 번호로 [그림 4]의 로컬 네트워크와 연결을 시도한다면 라우터는 11.11.11.11:555를 어디에 맵핑해야 할지 알 길이 없으므로 아무런 연결이 성립할 수 없습니다.

참고로 포트 번호는 0~65535까지 사용할 수 있습니다. Static PAT은 공인 IP 주소 하나로 약 65,000개 정도의 로컬 호스트 디바이스가 인터넷을 통해 데이터를 주고받을 수 있게 합니다. Dynamic PAT은 공인 IP 주소 하나당 동시에 65,000개 정도의 로컬 호스트 디바이스가 인터넷과 연결을 할 수 있으므로, 모든 로컬 호스트 디바이스가 동시접속만 하지 않는다면 Static PAT보다 더 많은 수의 로컬 호스트 디바이스들에 인터넷 접속을 지원할 수 있습니다. Dynamic PAT도 65,000개 이상의 인터넷 동시접속을 제공해야 한다면 공인 IP 주소를 추가하면 됩니다.

지금까지 PAT에 관해 설명해 드렸습니다. 다음 연재에서는 NAT의 나머지 다른 방식들인 Policy NAT과 Twice NAT에 관한 설명해 드리고 NAT과 PAT 관련 내용을 마무리하겠습니다. 📖