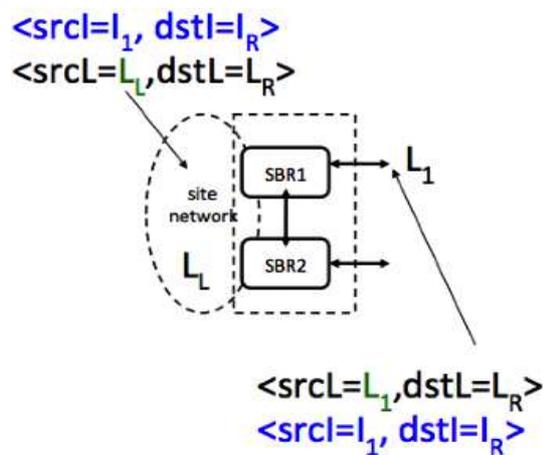


ILNP와 NAT

김대영 (충남대학교)

ILNP(Identifier-Locator Network Protocol; RFC6740)는 IRTF(Internet Research Task Force) RRG(Routing Research Group)에서 백본 라우팅 테이블 폭발을 야기하는 멀티호밍을 개선하고자 내어 놓은 새로운 프로토콜이다. ILNP는 위치자/식별자 분리(locator/identifier separation: LIS) 방법의 하나인데 특이한 것은 위치자에 대해 주소변환기(Network Address Translator: NAT)를 적극적으로 활용한다는 점이다. 더구나 ILNP가 IPv6의 아류라는 것을 감안하면 끝대끝 유일한 주소를 지향하는 IPv6와 달리 국부 위치자 및 주소변환기를 사용하는 것은 주목해야 할 매우 특이한 사항이다.

<그림 1>은 ILNP에서 국부망(site)이 두 개의 게이트웨이 SBR1(site border router 1) 및 SBR2에 의해 글로벌 망에 멀티호밍(multi-homing)으로 연결된 모양을 보이고 있다. 이때 국부망에 있는 호스트 1은 자기와 상대방의 식별자 및 위치자를 각각 $\langle I_1, IR \rangle$ 및 $\langle L_L, LR \rangle$ 로 인식하고 있다고 하자. 여기서 L_L 은 호스트 1이 붙어 있는 국부망(site) 내의 특정 IP 부속망(subnetwork)을 가리킨다. 라우터는 위치자만 보고 동작하므로, 국부망 내에서는 호스트 1에 대한 길찾기(라우팅)는 L_L 에 의해 결정된다. 여기까지는 특이할 것이 없다.



<그림 1: INLP 멀티호밍>

문제는 패킷이 국부망을 떠나 글로벌 망으로 들어가는 경우이다. 예를들어 패킷이 SBR1을 통해 밖으로 나가는 경우를 보자. 이때 패킷의 출발지와 목적지의 식별자는 그대로 변함없이 $\langle I_1, IR \rangle$ 로 유지되지만, 위치자는 $\langle L_1, LR \rangle$ 로 바뀐다. 곧, 출발지의 위치자가 L_L 에서 L_1 로 바뀌는 것이다.

여기에서 든 보기는 국부망에서 출발한 모든 패킷에 공통적으로 적용되는 것이다. 곧, 국부망에서의 위치자가 무엇이든 상관없이 글로벌 망으로 들어갈 때에는 국부망 안에 있는 모든 호스트에 대해 위치자가 L_1 으로 대체되는 것이다. 거꾸로 말하면 글로벌 망 길찾기에서는 국부망 전체가 L_1 하나의 위치자로 파악되는 셈이다.

이것은 전형적인 주소변환(NAT) 동작이다. IETF(Internet Engineering Task Force)가 발간한 프로토콜 중에서 이렇게 주소변환을 기본동작으로 정의하는 것은 매우 드문 경우이다. IPv6로의 전환을 공식 정책으로 채택하고 있는 IETF로서 NAT를 기본동작으로 하는 프로토콜 규격을 발행한 것은 매우 특이할 만한 사항이다.

더 중요한 것은 ILNP의 개발이 애초에 백본 라우팅 테이블 폭발을 막을 방법으로 제시되었었다는 점이다. 그 논리의 맥락은 이러하다:

1. 백본 라우터의 라우팅 테이블이 폭발하는 것은 IP로는 멀티호밍이 효과적으로 이루어지지 않기 때문이다.
2. 멀티호밍이 잘 안되는 이유는 IP 주소가 식별자와 위치자의 두 기능을 중복적으로 갖고 있기 때문이다.
3. 따라서 수송 연결에 사용할 식별자와 길찾기에 사용할 위치자를 분리하는 것, 곧 LIS가 필요하다.

위 논리에서 묵시적으로 가정된 것은 식별자와 위치자 모두 글로벌 유일(globally unique) 값을 갖는다는 것이다. 따라서 ILNP의 초안에서는 IP 주소만을 가리키는 위치자도 글로벌 유일값을 갖는 것으로 되어 있었다. 현대 최종본에는 위치자는 국부값을 갖고 글로벌로 들어갈 때에는 NAT를 사용하도록 하고 있다.

그 이유를 이해하기 위해 <그림 1>의 멀티호밍을 다시 들여다보면 기실 위치자의 입장에서 보면 INLP는 IP 주소에서 상황과 하나도 다른 것이 없다는 것이다. 따라서 인터넷에서 나타났던 똑같은 문제가 ILNP 위치자에도 그대로 계승되고 만다. 결국 ILNP에서도 위치자를 저장하는 백본 라우팅 테이블이 폭발하기는 마찬가지라는 것이다. (*이 점을 설명하기 위해 위의 3단 논법의 제1단계에서 왜 현재의 인터넷에서 멀티호밍으로 라우팅 테이블이 폭발하는지를 이해할 필요가 있는데, 이 글에서는 그 상세한 내용은 생략한다.) 곧, INLP가 애초 목표로 했던 백본 라우팅 테이블 폭발 제어 문제가 식별자/위치자 분리로 해결되지 않은 것이며, 이는 위 논법 2단계에서 멀티호밍 문제의 원인을 식별자/위치자 중복 문제로 지목한 진단 자체가 잘못됐음을 의미한다.

ILNP가 제시하는 방법은 글로벌 유일 위치자가 아니라 국부(local) 위치자를 쓰자는 것이다. 곧, IP로 말하자면 사설(private) 또는 공급자독립(provider-independent; PI) 주소를 쓰자는 것이다. 그리고 글로벌 망에 들어갈 때에야 비로서 글로벌 유일 위치자로 주소변환 하자는 것이다. 이런 상황에서는 통상 인터넷에서 악으로 간주되는 주소변환기(NAT)가 ILNP에서는 오히려 반전되어 중요한 네트워크 인프라로 인정되는 꼴이 된다.

만일 애초에 이런 결론에 이를 것을 알았다면 번거롭게 멀티호밍 문제 해결을 할 목적으로 식별자/위치자 분리 작업을 할 필요가 없다는 결론이 된다. 이것은 마찬가지로 애초에 멀티호밍을 해결하려고 시작한 LISP(Locator-Identifier Separation Protocol)등 모든 LIS 계열 프로토콜에 마찬가지로 적용될 수 있는 비판이다.

ILNP의 규격은 NAT에 대한 새로운 인식을 제시한다고 할 수 있다. NAT를 긍정적인 시각에서 들여다볼 필요가 있다는 것이다. 이미 NAT는 인터넷에 만연해 있고 IPv6로의 진행을 막는 가장 큰 걸림돌로 인식되고 있다. 사실 모든 사이트에서 같은 종류의 중간자(middle box)인 방화벽(firewall)이 설치돼 운영되고 있는 것을 생각하면 NAT의 사용은 보안등의 문제를 위해서라도 오히려 더 권장되어야 할 장치일 수도 있다. 이제까지 인터넷을 논할 때에 끝대끝법칙(end-to-end principle)를 금과옥조처럼 떠받들었으나, 인터넷이 앞으로는 오히려 중간자(middle box) 통신 패러다임으로 진화할 지도 모른다는 점이 시사된다.