IPv6를 이용한 NAT 대체 방법에 관한 연구

양진석*, 김현구*, 임형진*, 이승윤**, 정태명*
*성균관대학교 컴퓨터공학과
**한국전자통신 연구원
e-mail:*{jsyang, hkkim, hjlim}@imtl.skku.ac.kr,
**syl@etri.re.kr, *tmchung@ece.skku.ac.kr

A Study on Replacing NAT using IPv6 Functionality

Jin-Seok Yang*, Hyoun-Ku Kim*, Hyoung-Jin Lim*,
Seung-Yun Lee** and Tai-Myoung Chung*

*Dept. of Computer Engineering, SungKyunKwan University

**Electronics and Telecommunications
Research Institute

요 약

IPv6는 최신 장치에 대한 추가기능요구와 사용할 수 있는 인터넷 주소의 고갈이 임박해옴에 따라 만들어졌다. 기존의 IPv4 환경에서는 주소 부족에 대한 단기 해결책으로 NAT 등 여러 가지 메커니즘이 제시되었다. IPv6의 등장으로 IPv4의 주소 부족이라는 문제를 해결하였으나 NAT는 계속해서 사용되고 있으며 이로 인해 보안 서비스측면, 인터넷 및 통신 아키텍처 투명성 등의 문제들이 제기되고 있다. NAT 관련 문제를 해결하기 위한 기존의 접근 방법은 NAT와 상호운용성을 전제로 하고 있으나, 본 논문은 NAT를 대체할 수 있는 IPv6의 기능을 기술한다. NAT가 없어지면 각종 보안 서비스에 있어서 문제가 되고 있는 많은 복잡한 문제들도 해결된다. IPv6는 NAT를 대체를 위해 주소 공간, 자동설정메커니즘, 멀티캐스팅 범주(scope), 흡별 처리의 기능들이 존재한다. 각 기능들은 NAT의 장점을 대체할 수 있다.

1. 서론

IPv4 기반의 문제들에 대한 단기 해결책인 Renumbering, CIDR(Classless Inter-Domain Routing), NAT(Network Address Translator), DHCP(Dynamic Host Configuration Protocol)들은 IPv6의 등장으로 IP 주소 공간 및 구조나 DHCPv6 메커니즘으로 일부 해결 및 보완되었으나, NAT 문제는 아직까지 해결되지 않고 이슈가 되고 있다[1, 2, 6, 19]. 특히, NAT는 인터넷뿐만 아니라 VPN 환경에서 많은 문제점을 내포하고 있고 이를 해결하기 위한 또 다른 복잡한 메커니즘을 요구하고 있다[3, 9, 10, 12, 15]. 이러한 복잡한 메커니즘은 IPv6의 특징을 살리지 못하고 NAT 자체의 단점을 해결하기 위하여 또 다른 메커니즘을 도입함으로써 관리에 대한 복잡성을 높이는 결과를 낳고 있다.

최근에 열린 IETF의 IPv6 ops와 ngtrans 워킹그룹의 미팅에서조차 NAT와 관련하여 문제가 있음을 언급하고 있으나 근본적인 해결책을 제시하고 못하고 있다[7, 19].

NAT 관련 문제에 대한 기존의 해결 방법은 NAT와 상호운용성을 전제로 하므로 근본적인 해결책이 될 수 없다. 본 논문에서는 IPv6의 기능 중 NAT를 완전히 대체할 수 있는 특징들을 제시한다.

본 논문의 2장은 NAT와 IPv6에서 제공하는 새로운 기능들을 분석하고, 3장은 IPv6에서 제공하는 NAT의 대체 기능을 구체적으로 기술한다.

2. 관련 연구

본 장에서는 NAT의 장점 및 단점에 대해 기술하고 IPv6를 기능적 측면에서 분석을 한다.

2.1 NAT의 장단점

NAT는 기존의 IPv4 공용 주소의 부족으로 인해 제안된 메커니즘이다. NAT는 주소 부족 등의 문제를 단기적으로 해결할 수 있는 장점이 있지만, NAT가 사용될 때 야기되는 단점은 다음과 같이 요약될 수 있다[6].

- single point of failure
- end-to-end 인터넷 아키텍처의 투명성을 저해
- end-to-end 인증 및 보안문제
- end-to-end 커뮤니케이션 아키텍처를 복잡성
- peer-to-peer 모델의 저해요소

위의 단점뿐만 아니라 키관리 프로토콜의 표준으로 추진되는 IKE의 경우 NAT 존재 시 적용할 수 없는 큰 단점이 있다[6]. 그럼에도 불구하고 NAT가 쓰이는 이유는 다음과 같다[11].

■ 모자라는 공용 IP 주소의 대체

주소 변환 방법은 정적인 방법과 동적인 방법이 있다. 정적인 방법은 테이블을 설정해서 일대일 대응시켜 변환하는 방법이다. 동적인 방법은 공용 IP 주소들을 풀(pool)로 등록해 놓고, 요청이 올 때마다 풀 내의 IP 주소들로 돌아가며 할당하는 방식이다.

■ 보안성 향상

라우터를 기준으로 내부 네트워크에서는 사설 IP 주소를 사용하기 때문에 인터넷에 대해 내부 네트워크를 숨길 수 있다.

■ 설정의 편의성

어떤 조직에서 ISP 업체를 옮길 경우가 있는데 컴퓨터의 수가 많은 경우 컴퓨터의 IP 주소 세팅을 일일이 바꾸어야 한다. 그러나, NAT를 사용하면 내부에서는 네트워크를 변경하지 않고 NAT에서만 바뀐 ISP 주소로 변환하도록 설정해주면 된다.

■ 부하 공유(Load sharing)

아주 많은 사용자들이 이용을 하는 사이트의 경우 서버의 사양을 높이는 방법도 있지만 여러 대의 서버를 사용하여 부하를 줄이는 방법이 있다. 이럴 때 NAT를 이용하여 로드를 분산하는 방법이 있다.

2.2 IPv6의 새로운 기능

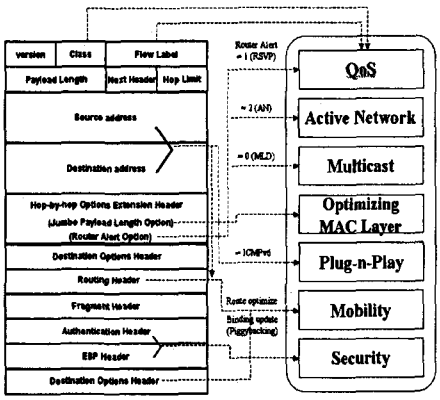
IPv6의 기능별 새로운 서비스는 [그림 1]에서 보는 바와 같이 크게 7가지로 분류할 수 있다. IPv6는 이러한 기능을 지원하기 위해 주소 체계 및 헤더 형식을 설계하였다. IPv6가 제공하는 새로운 서비스는 다음과 같다[16].

■ 주소 공간 및 구조

IPv6가 만들어진 목적인 IP 주소 공간은 무한대라고 할 수 있을 만큼 풍부하다. 또한, IPv6의 주소 공간은 인터넷 백본부터 조직 내의 개별 서브넷까지 여러 수준의 서브네팅과 주소 할당이 가능하도록 만들어졌다[13].

■ 서비스 품질(QoS)

IPv6 헤더의 흐름 레이블 필드나 트래픽 클래스를 사용한 트래픽 확인을 통해 라우터는 원본과 대상 사이에서 일련의 패킷 흐름에 속하는 패킷의 특수한 처리를 식별하고 제공할 수 있다. IPv6 헤더에서 트래픽이 식별되기 때문에 IPsec를 통해 패킷 페이로드가 암호화될 때에도 QoS를 지원할 수 있다. 또한, 홉-바이-홉 옵션 헤더의 라우터 경고 옵션의 RSVP(Resource reSerVation Protocol) 메세지을 이용할 수도 있다[16].



[그림 1] IPv6의 기능별 매핑(mapping)

■ 액티브 네트워크(Active Network)

홉-바이-홉 옵션에 포함되는 라우터 경고 옵션은 라우터에서 사용자가 원하는 어떠한 처리가 가능하도록 한다[4].

■ MAC 계층 최적화(Optimizing MAC layer)

홉-바이-홉 옵션 헤더에서 제공하는 이 기능은 헤더에서 다른 옵션의 위치를 이동시키는 것을 제공한다. 적절한 정렬은 IP 데이터그램의 가장 효율적인 처리를 위해 중요하다[16].

■ 플러그-앤-플레이(Plug-n-Play)

플러그-앤-플레이는 ICMPv6 프로토콜을 이용하여 주소의 자동 생성, 인접 노드 탐색, 사이트 주소재지정의 기능을 제공한다[20].

■ 이동성(Mobility)

이동성의 경우, 모바일 장치들(devices)에 대해서 적용 가능하다. 이웃 탐색(Neighbor Discovery),

자동설정, 경로 최적화 기능은 IPv4에서 보다 효과적으로 이동성을 제공한다[5].

■ 보안성(Security)

AH(Authentication Header)와 ESP(Encapsulating Security Payload)는 IP 레벨에서 데이터의 기밀성, 무결성, 가용성을 제공하기 위해 정의되었으며 터널링 기술을 통해 보안 서비스를 제공한다[17, 18].

위의 기능들 중 몇 가지 기능은 NAT를 대체하기 위한 솔루션을 제공한다.

3. NAT 대체를 위한 IPv6 솔루션

2.1절에서 분석한 NAT는 IPv6가 제공하는 새로운 서비스로써 대체가 가능하다. 첫 번째, IPv6는 모자라는 공용 주소를 모두 대체할 수 있다. 두 번째, 설정의 편의성은 자동설정(Autoconfiguration)의 기능 중 사이트 주소재지정(Site renumbering)과 라우터 주소재지정(Router renumbering)으로 해결할 수 있다. 부하 공유는 IPv6의 멀티캐스트 주소 scope 필드와 홉-바이-홉 옵션 헤더를 이용한 서비스 품질을 보장함으로써 대체가 가능하리라 예상한다. 각 기능들을 자세하게 살펴보면 다음과 같다.

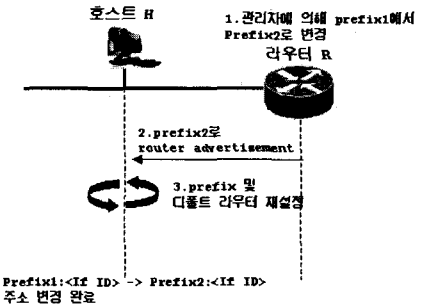
3.1 주소 공간

최신 장치에 대한 추가 기능 요구와 사용할 수 있는 인터넷 주소의 고갈이 임박해옴에 따라 IPv4의 업그레이드 버전인 IPv6가 만들어졌다. IPv6는 128비트로 표현되는 주소를 갖음으로써 3.4×1038개 이상 결합되어 표시될 수 있다. IPv6의 주소 공간은 인터넷 백본부터 조직 내의 개별 서브넷까지 여러 수준의 서브네팅과 주소 할당이 가능하도록 크게 만들어졌다. 현재는 소수의 주소만 호스트에서 사용하도록 할당되어 있지만 앞으로는 많은 수의 주소를 사용할 수 있게 될 것이고 사용 가능한 주소가 매우 많기 때문에 더 이상 NAT의 구축과 같은 주소 변환 기술이 필요하지 않다.

3.2 사이트 주소재지정

사이트 주소재지정은 사이트 전체의 주소 변경 시 수작업에 의한 주소 변경이 불필요하여 네트워크의 재설정을 용이하게 한다.

[그림 2]에서 보는바와 같이 라우터 R의 prefix 1이 prefix 2로 변경되었을 때, 라우터는 prefix 2를 가지고 광고(advertisement) 한다. 호스트는 prefix 및 default router를 재설정한다. 이 과정에서 기존의 맺어진 세션에 대해 고려해야한다. 세션은 유효주소를 "preferred" 와 "deprecated"로 구분하여 관리하며 연결은 "preferred" 주소에서만 시작 가능하도록 하였다. 또한, "preferred" 생존시간을 두어 각 주소의 사용 기간을 명시할 수 있도록 하였다.



[그림 2] 사이트 주소재지정

관리자는 주소를 재지정할 때 통신 실패를 최소화하기 위해서 적당한 prefix 생존시간 설정이 가능하다. "deprecation period"는 기존 주소가 무효 되었을 때 대부분의 통신이 새 주소를 사용할 수 있을 만큼 길어야 한다[20]. 사이트 주소재지정은 NAT의 장점 중 하나인 설정의 편의성 측면에서 대체가 가능하리라 예상된다.

3.3 라우터 주소재지정

라우터 주소재지정은 상위 라우터가 하위 라우터의 prefix를 설정할 수 있는 메커니즘을 제공한다[8]. 이와같은 기능은 관리자가 사이트 전체의 주소 변경 시 편리한 재설정과 원격에서 상위 라우터를 이용하여 하위 라우터를 편리하게 제어할 수 있어 설정의 편의성 측면에서 NAT가 제공하는 기능을 대체할 수 있다.

3.2와 3.3과 같은 기능은 관리자가 사이트 전체의 주소 변경 시 설정의 편의성 측면에서 NAT가 제공하는 기능을 대체할 수 있으며 특히, 관리 네트워크의 범위가 커졌을 경우 효율적인 솔루션이 될 수 있다. 관리 측면에서 볼 때 관리자의 부담뿐만 아니라 비용도 최소화할 수 있다.

3.4 멀티캐스트 주소 scope 필드

<표 1>에서 보는바와 같이 멀티 캐스트 주소의

scop 필드는 멀티캐스트 그룹의 범주를 제한하는 필드를 제공한다[14].

<표 1> 멀티캐스트 scope 필드 값

scope 필드	범 주
0	예약됨
1	인터페이스-로컬 범주
2	링크-로컬 범주
3	서브넷-로컬 범주
4	관리-로컬 범주
5	사이트-로컬 범주
6	미할당
7	미할당
8	조직-로컬 범주
9	미할당
A	미할당
B	미할당
C	미할당
D	미할당
E	글로벌 범주
F	예약됨

멀티 캐스트 패킷의 경우 많은 노드에게 패킷을 보내는 통신이므로 관리자는 적절한 범위로 멀티 캐스트 범주를 설정하여 사용한다면 네트워크 내부의 트래픽을 줄일 수 있을 것이라고 예상된다.

3.5 홉-바이-홉 옵션 헤더

홉-바이-홉 옵션 헤더는 전송 경로상의 모든 노드마다 처리할 옵션 정보를 포함한다. 이 옵션은 라우터 경고 옵션, 점보 페이로드 옵션을 포함하고 있다. 라우터 경고 옵션은 타입에 따라 다시 3가지로 나뉘어 지는데, MLD(Multicast Listener Discovery), RSVP, 액티브 네트워크 메시지가 있다. RSVP와 액티브 네트워크는 서비스 품질을 위한 메커니즘을 제공한다. 그러나, 이 옵션들은 서비스 품질을 제공하기 위한 기반구조가 필요하다.

3.4절과 3.5절은 사용자 서비스를 보장한다는 측면에서 NAT에서 제공하는 부하 공유 기능을 대체할 수 있으리라 예상된다.

4. 결론 및 향후 과제

NAT는 IPv4 환경뿐만 아니라 IPv6 전환 시 서비스 측면에서 큰 장애물이다. 본 논문에서는 NAT가 IPv6에서 제공하는 솔루션으로 대체될 수 있음을 제시하였다. NAT의 대체는 서비스 측면, 종단간 커뮤니케이션 모델이나 아키텍처 투명성의 문제를 해결할 수 있을 뿐만 아니라 관리 측면에서도 많은 장점이 있다.

향후에는 본 논문에서 제시한 IPv6 솔루션과 기존의 솔루션에 대한 관리 측면에서의 장·단점을 정성적으로 비교 분석하는 연구가 필요하다.

참고문헌

[1] 홍진표, "IPv6 네트워크로의 전환을 위한 과제", 한국정보통신기술협회 IT Standard Weekly, Nov. 2001.

[2] A. Durand, "NAT Issues", v6ops meeting, Mar. 2003.

[3] B. Aboba and W. Dixon, "IPsec-NAT Compatibility Requirements", Internet draft, Aug. 2003.

[4] C. Partridge and A. Jackson, "IPv6 Router Alert Option", RFC 2711, Oct. 1999.

[5] D. Johnson, C. Perkins, "Mobility Support in IPv6", Internet draft, Jun. 2003.

[6] IEEE Internet computing, "Network Address Translators : Effects on Security Protocols and Applications in the TCP/IP stack", Dec. 2000.

[7] J. Bound, et al., "IPv6 Enterprise Networks Scenarios", Internet draft, Jun. 2003.

[8] M. Crawford, "Router Renumbering for IPv6", RFC 2894, Aug. 2000.

[9] M. Stiemerling, et al., "MIDCOM Protocol Semantics", Internet draft, Aug. 2003.

[10] Nortel Networks, "NAT Traversal", Mar. 2002.

[11] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, Aug. 2001.

[12] P. Srisuresh, et al., "Middlebox communication architecture and framework", RFC 3303, Aug. 2002.

[13] R. Hinden and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, Apr. 2003.

[14] R. Hinden and S. Deering, "IPv6 Multicast Address Assignments", RFC 2375, Jul. 1998.

[15] R. Swale, et al., "Middlebox Communications (midcom) Protocol Requirements", RFC 3304, Aug. 2002.

[16] S. Deering and B. Hinden, "Internet Protocol, Version 6 (IPv6) specification", RFC 2460, Dec. 1998.

[17] S. Kent, and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Nov. 1998.

[18] S. Kent, and R. Atkinson, "IP Authentication Header", RFC 2402, Nov. 1998.

[19] S. Satapati, "NAT Issues", v6ops meeting, Mar. 2003.

[20] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Dec. 1998.