IPv6 환경에서 Anycast DNS를 이용한 안전한 DNS 구성

김경민° 김진석 서유화 김승홍 신용태
숭실대학교 컴퓨터학과
{kmkim°, smics, zzarara, liontail, shin}@cherry.ssu.ac.kr

Safe DNS Formation Using Anycast DNS in IPv6 Environment

Kyungmin Kim° Jinseok Kim Youhwa Seo Seunghong Kim Yongtae Shin
Dept. of Computing, Soongsil University

요 약

본 논문은 IPv6 환경에서 보다 안전한 DNS 구성에 대해 제안한다. DNS 서버는 도메인 네임을 해당하는 IP 주소로 맵핑하여 주는 시스템으로 IPv6 환경에서는 늘어나는 IP 주소의 길이로 인해 직접적인 사용이 힘들고, 현재 거의 모든 인터넷 응용 서비스들이 DNS를 이용하고 있다는 점에서 앞으로 그 중요성은 더욱 높아질 전망이다. 현재 사용되고 있는 DNS 서버의 구성은 1차, 2차 서버를 통해 1차 서버의 장애 발생 시 그 역할을 2차 DNS가 수행하는 방식이다. 그러나 이는 DNS 서버가 속해 있는 네트워크를 대상으로 하는 공격이나 장애에 대응하기 어렵고, DNS 서버의 이용자 또한 서비스의 연속성을 보장받기 어렵다. 이를 해결하기 위해 본 논문은 Anycast 전송 기술을 DNS 서버에 적용하여 재구성함으로써 장애 발생 시에도 안정적으로 도메인 네임 서비스를 사용자에게 제공할 수 있는 방안을 제시하였다.

1. 서 론

DNS(Domain Name System)란 도메인 네임과 그에 해당하는 IP 주소를 전환하고 변환하는 메커니즘으로서 웹, 이메일 등 다양한 응용 프로그램이 사용자에게로 서비스가 이루어지기 위해서 핵심적인 역할을 담당하고 있는 거대한 분산 데이터베이스이다.[1]

현재 IPv4 환경에서 32bit의 IP 주소를 사용하는 것과 다르게 IPv6 환경에서의 DNS 서버는 128bit의 IP 주소를 사용하는 환경으로 인해 월등히 늘어난 수의 주소 전환 처리를 해야 하고 IPv4 주소에 비해 수치상으로 4배 길어진 주소체계를 사용해야 한다. 이러한 환경은 사용자의 IP 주소 사용에 대해 실수 발생 여지를 높이기 때문에 IPv6 환경에서 IP 주소와 도메인 네임간의 전환 서비스를 제공하는 DNS의 중요성은 더욱 부각되어진다.

도메인 네임 서비스의 중요성으로 인해 서비스 제공자는 DNS 서버가 최대의 가용성을 유지하도록 하기 위하여 일반적으로 1차(primary) DNS 서버와 함께 2차(secondary) DNS 서버를 서비스 제공자의 망에 구성한다. 이러한 구성을 통해 사용자는 일반적으로 자신의 PC에 설정한 1차 DNS 서버를 통해 서비스를 이용하게 되고, 1차 DNS 서버가 응답하지 않을 경우 함께 설정한 2차 DNS 서버로 전환하여 DNS 쿼리를 전송함으로 목적하는 서비스를 이용할 수 있게 된다. 하지만 1차, 2차 DNS 서버를 일반적으로 동일한 망에 구성하게 되는 방식은 악의적인 목적을 가진 공격자의 다음과 같은 공격에 의해 보안상의 문제를 나타내게 된다. 공격자의 타깃이 되는 호스트로 무수히 많은 패킷을 전송하여 타깃의 서비스를 중단시키는 DDoS(Distributed Denial of Service) 공격의 경우 호스트뿐만 아니라 호스트가 속해 있는 네트워크에 무수히 많은 패킷이 유입되게 되어 타깃 호스트의 네트워크 자체가 정상적인 작동을 할 수 없게 된다. 그 외의 타깃 호스트가 포함되어 있는 네트워크를 불안정하게 만드는 각종 네트워크 기반 공격들로부터 위의 방식은 안전하지 못하다.

이를 해결하기 위해 사용자는 1차 DNS 서버와 2차 DNS 서버 설정을 각각 다른 서비스 제공자의 DNS 서버 주소로 하거나, 현재 설정된 DNS 서버에 문제가 발생했다고 판단되어 질 때, 해당 설정을 수동으로 바꾸는 방법을 생각할 수 있다. 하지만 DNS 서버 설정은 거의 모든 PC에서 적용되어야 하는 반면에 그 사용자의 대부분은 해당 지식의 비전문가라는 점을 고려할 때, 해당 PC의 DNS 서버 설정을 특정한 위험요소를 피해서 적용하거나, 수동으로 변경 하는 일, 그리고 설정된 DNS 서버의 문제 발생여부를 판단하는 등의 행동을 기대하는 것은 현실적이지 못하다.

본 논문은 IPv6 환경에서 DNS 서버를 구성할 때 1차, 2차 DNS 서버로 이루어진 환경의 보안적인 문제점들을 극복하면서 일반 사용자가 DNS 서버 이상 시 별다른 조치 없이도 서비스 연속성을 유지할 수 있도록 하기 위해 IPv6의 구조적 특징과 Anycast 기술을 적용한 DNS 서버를 이용하여 그 해결책을 제안한다.

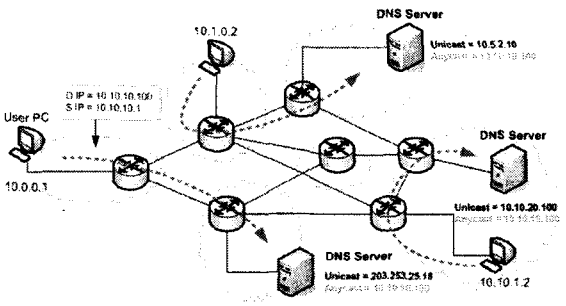
2. 관련연구

2.1 Anycast 전송방식

Anycast는 단일 송신자와 다중 수신자 사이의 통신인 Multicast, 그리고 단일 송신자와 단일 수신자 사이의 통신인 Unicast와 대비하여 정의되었다. Anycast는 멀티캐스트와 같이 일-대-다 전송을 지원한다. 그러나 그룹 내

의 모든 수신자에게 보내어지는 것이 아니라 가장 가까운 서버 또는 사용자에게 서비스 할 수 있는 최선의 한 노드로만 전송하므로 결과적으로는 일-대-일 전송방식이라고도 볼 수 있다.

하나의 Anycast 주소는 다수의 호스트에 할당되며, 발신 노드가 해당 Anycast 주소를 목적지로 하여 패킷을 전송하게 되면, 라우터가 라우팅 테이블에서 같은 Anycast 주소를 갖는 호스트 중 가장 근접한 호스트로 라우팅 하게 된다. 이때 라우팅 거리는 설정되어 있는 라우팅 프로토콜에 따르게 된다. 사용자는 가장 가까운 서비스 호스트로 부터 서비스를 제공 받을 수 있음으로서 서비스의 품질 향상을, Anycast 서비스 호스트는 부하분산 효과와 장애 시 서비스의 연속성 효과를 기대할 수 있다. 또한 Anycast 주소는 Unicast 주소와 구문적으로 차이가 없기 때문에 Anycast 호스트에 추가적인 수정사항이 발생하지 않는다.[2]



[그림 1] Anycast DNS

2.2 Anycast DNS 서버의 효과

계층적인 구조의 분산 데이터베이스 체계로 운용되는 DNS는 각 계층의 영역에 대해 1개의 1차(primary) 서버와 12개의 2차(secondary) 서버로 구성되는 13개까지의 서버로 구성이 가능한데 이는 한 개의 네임서버 응답 메시지인 UDP 패킷의 최대 크기인 512바이트 내에 모든 네임서버 이름과 IP주소를 포함하기 위함이다. 이를 극복하기 위하여 Anycast 기술을 적용하여 사용되기 시작하였으며, 각 계층의 DNS 서버 운용기관은 자신이 관리하고 있는 서버의 미러 사이트를 설치해 분산·관리 하게 된다. Anycast 기술의 DNS 적용을 통해 몇 가지 기대효과를 얻을 수 있다.[3] [그림 1]은 Anycast 전송방식을 이용하여 DNS 서버로 접근하는 모습을 보여준다.

● DNS 서비스 안정성(Robustness)
지역적으로 분산된 다수의 Anycast DNS 서버를 통해 DNS 트래픽의 지역적 분산 처리가 이루어지며, 분산 서비스 거부 공격(DDoS) 발생 시 공격을 분산함으로써 장애 지역의 범위를 최소화함으로 DNS 서비스의 연속성을 유지할 수 있다.

● DNS 서비스 다중화(Redundancy)
다수의 Anycast DNS 서버를 통한 서비스 분산 및 서비스 다중화 효과를 기대할 수 있으며, 사용자는 가장 인접한 지역 서버에서 DNS 서비스 받을 수 있게 되어 DNS 질의·응답 시 서비스 성능 개선 및 전체 인터넷 자원의 효율적 사용이 가능하다.

● DNS 서비스 복원력 강화(Resiliency)
Anycast DNS 서버 간에 자동 서비스 전환 기술을 통해 일부 호스트의 장애 발생 시 중단 없는 DNS 서비스 제공이 가능하다

2.3 IP Anycast DNS 이용현황

현재까지 Anycast는 안정성과 서비스 분산효과를 얻기 위하여 도메인 네임 질의수가 많은 상위 DNS 서버인 root DNS와 TLD 네임 서버에 적용이 되고 있다. 2006년 6월 9일 업데이트 된 Root Server Technical Operations Assn(www.root-servers.org)의 자료에 따르면 현존하는 13개의 root DNS 서버 중 6개(C, F, I, J, K, M)의 root DNS 서버가 다수의 미러링 서버를 갖추고 Anycast 주소를 할당받아 운영되고 있으며, 그 중 F, J, M-root DNS가 국내에서 미러링 되어 운영 중이다.

국내에 미러링 되어 있는 root DNS 서버 중 Internet Systems Consortium, Inc.에서 운영 중인 F-root DNS 서버는 미러링 서버를 포함하여 총 37개의 DNS 서버가 하나의 Anycast 주소(192.5.5.241/2001:500::1035)를 통해 서비스 되고 있다. 국내에 미러링 되어 있는 다른 root-DNS 서버 중 J-root DNS 서버는 veriSign Naming and Directory Services에서 운영 중이며 총 21개의 Anycast DNS 서버를 가지고 IPv4로 서비스 되고 있으며, M-root DNS 서버는 일본의 대표적인 차세대 인터넷 관련연구 프로젝트인 WIDE 프로젝트에서 운영 중이며 4개의 Anycast DNS 서버를 통해 서비스 되고 있다.[4]

Anycast DNS 기법은 인터넷 사용자가 여러 네트워크 중에 라우팅 경로가 가장 가까운 쪽과 통신을 하게 되는 라우팅 기법을 이용한 것으로 현재 전 세계 13개 루트 DNS 운용기관 중 ISC와 RIPE-NCC가 본 기술을 이용한 미러 사이트 확대에 적극적이다.

3. IPv6 환경에서 Anycast DNS를 이용한 DNS 구성

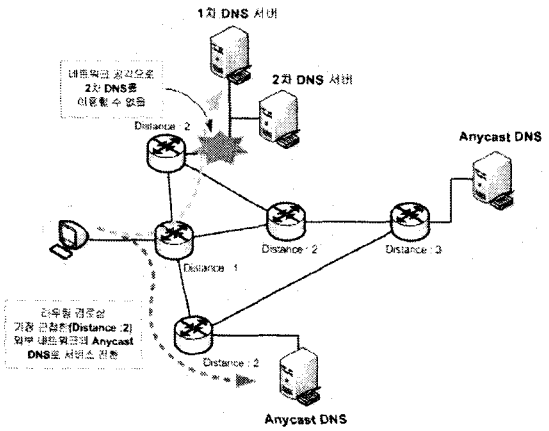
3.1 IPv6 인터페이스에 Anycast 주소 할당

본 논문에서 제안하고자 하는 안전한 DNS 서버의 구성을 위해서는 Anycast DNS 서버의 네트워크 인터페이스에 2개의 IP 주소를 할당해야 한다. IPv6 주소체계에서 하나의 네트워크 인터페이스는 다수의 IPv6 주소를 가질 수 있다는 점을[2] 이용하여 Anycast DNS 서버의 네트워크 인터페이스에 Global Unicast 주소와 Anycast 주소를 함께 할당한다. 이 중 Global Unicast 주소는 1차 DNS 서버의 역할을 가지는 IP 주소로 각각의 서버마다 다른 IP 주소가 할당되어 서비스 이용자에게 공개되어야 한다. 반면에 Anycast 주소는 2차 DNS 서버로의 이용을 위한 IP 주소로서 Anycast 서비스를 위해 예약된

주소 범위 내에서 선택 된다. 여기서 Anycast 서비스를 위해 예약된 주소 범위의 사용을 위해서는 IP 주소의 관리 기관인 ICANN을 통해 해당 주소 범위의 예약이 필요한데 이것은 앞으로 정의될 수 있는 Anycast 주소를 활용한 다양한 응용 프로그램 및 서비스를 위한 목적으로 예약될 수 있을 것이다.

3.2 Anycast DNS를 이용한 안전한 DNS 구성

사용자는 1차 DNS 서버 설정에 기존의 Global Unicast 주소 설정을 유지하고 2차 DNS 서버 설정에 Anycast 주소를 등록하여 [그림 2]와 같은 DNS 구성을 만들 수 있다.

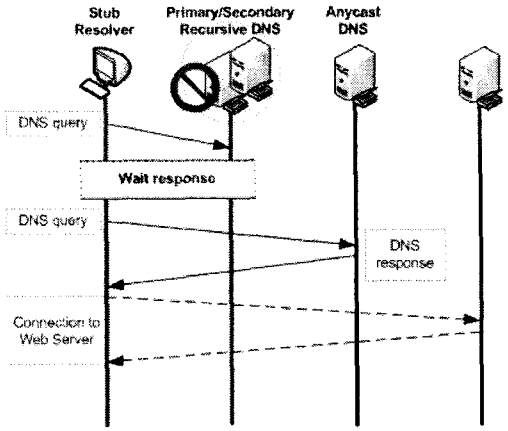


[그림 2] 제안하는 DNS 서버의 구성

[그림 2]에서 지금까지의 2차 DNS 서버는 1차 DNS 서버와 같은 네트워크에 위치하며, 1차 DNS 서버가 서비스를 제공할 수 없는 상황에 빠졌을 때 1차 DNS 서버의 서비스를 대체하기 위해 사용된다.

이러한 구성을 통하여 1차 DNS 서버에 대한 물리적인 단절이나 보안 위협 문제가 발생하여 1차 DNS 서버가 사용자의 질의에 대한 응답을 돌려주지 못하는 상황에 처했을 경우, 2차 DNS 서버를 통해 해당 DNS 서비스의 가용성을 유지하려 했다. 하지만 이는 1차, 2차 DNS 서버 중 어느 하나의 서버에 국한된 문제 발생에만 대응할 수 있는 구조이기 때문에, DDoS 공격이나 DNS 서버가 설치되어 있는 네트워크 자체에 대한 공격으로 인해 양쪽 서버가 정지하거나 해당 네트워크가 그 기능을 충분히 수행하지 못할 경우에는 효과적으로 대응할 수 없다. 따라서, 2차 DNS 서버는 1차 DNS와는 다른 네트워크에 위치하며 사용자가 높은 접근성을 확보 할 수 있어야 한다. 또한 서비스를 제공받는 사용자는 문제가 발생한 상황이 DNS 서비스에 의해 발생한 것인지를 판단하고 적절히 대응을 하기는 어렵다. 제안하는 DNS 서버의 구성은 1차 DNS 서버가 위치하고 있는 네트워크에 문제가 발생하였을 경우 Anycast 라우팅의 특성에 따라 자동으로 최선의 접근성을 가지고 있는 다른 네트워크의 Anycast DNS 서버를 2차 DNS 서버로 전환하여 서비스 가용성을 유지한다. 이를 통해 사용자는 1차, 2차 DNS 서버 설정 외의 부수적인 설정 없이 Unicast DNS 서버에 장애 발생 시에도 서비스를 유지할 수 있다.

대부분의 일반상황에서 사용자는 Global Unicast 주소를 통해 DNS 서비스를 제공받게 되며 DNS 서버에 대한 위협이나 네트워크 문제가 발생했을 때 Anycast 주소가 설정된 다른 DNS를 통해 서비스를 받게 된다.



[그림 3] 1차 DNS 서버의 장애 시 Anycast DNS의 이용 과정

제안하는 DNS 서버 구성에서 사용자가 특정 서비스를 이용하기 위해 DNS 서버로 질의를 하게 되는 과정에 대한 순서를 [그림 3]을 통해 보여준다. 장애가 없는 상황에서 1차 DNS를 이용하여 웹서버의 IP 주소로 접근하던 사용자가 1차 DNS로 부터 질의에 대한 응답을 받지 못하게 되면 서비스는 라우팅 경로상 인접한 Anycast DNS로 전환되고 사용자는 전환된 Anycast DNS를 이용하여 서비스를 받을 수 있다. 기존의 1차, 2차 DNS 서버로만 이루어진 구성에서 [그림 3]과 같은 문제가 발생한다면 사용자는 자신의 질의가 실패했음을 확인하기 위해 1차, 2차 DNS로 부터 정해진 시간만큼 응답을 기다리게 됨으로 제안하는 구성에 비해 약 2배의 확인시간이 소요되고 요청한 서비스는 실패하게 된다.

3.3 Anycast DNS의 2차 DNS 서버로의 적용

제안하는 DNS 서버 구성에서 Anycast 주소를 1차 DNS로 설정한다면 앞에서 언급한 장점들을 이용할 수 있으면서도 2차 DNS 서버 설정과정을 요구하지 않아 전체적으로 DNS 서버 설정을 간소화 할 수 있다. 하지만 사용자가 PC의 DNS 설정을 Anycast DNS 서버의 주소로 할당하게 되면 사용자에게 인터넷 서비스를 제공하고 있는 서비스 제공자나 사용자의 의도와는 상관없이 사용자의 PC는 라우팅 경로상의 가장 가까운 DNS 서버의 자원을 사용하게 된다. 이는 DNS 서비스의 제공자 입장에서는 의도하지 않은 사용자 또는 계약되지 않은 사용

자가 서비스 제공자의 DNS 시스템 자원을 어떠한 허가 절차도 없이 소모하게 되는 결과를 가져오며, 서비스 제공자로 부터 안정적이고 높은 성능의 서비스를 받아야 하는 정식 사용자의 입장에서는 허가 절차 없이 접근한 사용자들로 인해 DNS 서버와 서비스 제공자의 네트워크 자원을 나누어 사용하게 된다. 이러한 문제점은 많은 사용자를 보유하고 뛰어난 접근성과 질 높은 네트워크 서비스를 제공하는 서비스 제공자의 DNS 서비스 일수록 높은 확률로 빈번하게 발생하게 된다. 그러므로 본 논문은 Anycast 주소를 2차 DNS 서버에 적용하여 구성하는 것을 제안한다.

4. 결 론

DNS는 인터넷 서비스를 이용하는데 핵심적인 요소 중 하나로 안전하게 보호 되어야 한다. 최근 DNS를 대상으로 하는 공격이 증가하고 다양해짐에 따라 DNS 서비스의 가용성을 유지하는 문제의 중요성이 부각되고 있다.

본 논문에서는 Anycast DNS를 이용하여 DNS를 구성함으로써 DNS의 장애 상황 발생 시 근접한 다른 DNS 서버로 서비스를 전환한다. 이를 통해 서비스 제공자는 서비스의 연속성을 기대할 수 있고 서비스 이용자는 DNS 서비스가 이루어지지 않는 상황에서 부가적인 설정 없이 근접한 다른 DNS 서버를 이용할 수 있다.

그러나, Anycast 전송기법에 의해 선택된 DNS는 검증되지 않은 임의의 DNS 서버 일 수 있다. 검증되지 않은 DNS 서버는 같은 DNS 질의에 대해 서로 다른 응답을 전송하거나 잘못된 응답을 반환함으로 인해 사용자에게 보안상의 문제를 발생시킬 수 있다는 점은 추가로 보안되어야 할 것이다. .

참고문헌

[1] P. Albitz, and C. Liu, "DNS and BIND 2nd Ed.", O'Reilly, January 1997.

[2] R. Hinden, and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006

[3] 한국인터넷진흥원, "차세대 인터넷주소자원 기술 동향보고서", 2005.12

[4] Root Server Technical Operations Assn, "www.root-servers.org", 2006.06

[5] J. Jeong, Ed., "IPv6 Host Configuration of DNS Server Information Approaches", RFC 4339, February 2006

[6] S. Weber, and L. Cheng, "A Survey of Anycast in IPv6 Networks", IEEE Communications Magazine, January 2004

[7] Y. Morishita, and T. Jinmei, "Common Misbehavior Against DNS Queries for IPv6 Addresses", RFC 4074, May 2005.

[8] S. Thomson, and C. Huitema, "DNS Extensions to support IP version 6", RFC 1886, December 1995.