안정적인 IPv6 리커시브 DNS 서비스를 위한 애니캐스트 기반의 실패 복구 방안 연구

학생회원 서 유 화*, 김 경 민*, 정회원 신 용 태*, 송 관 호**, 김 원**, 박 찬 기**

Fail-over Mechanisms based on Anycast for Stable IPv6 Recursive DNS Services

Yuhwa Suh*, Kyungmin Kim** *Student Members*
Yongtae Shin*, Kwanhoo Song**, Weon Kim**, Chanki Park** *Regular Members*

요 약

리커시브 DNS(Recursive DNS)는 사용자 PC환경에서 1,2차 DNS로 설정되어 사용자의 1차적인 DNS 질의에 대한 도메인 네임 레졸루션(Domain Name Resolution)을 수행하는 중요한 DNS이다. 현재 전체 인터넷의 트래픽 중 DNS 트래픽은 많은 양을 차지하고 있으며 IPv6로의 전이에 따라 DNS 질의·응답 실패에 따른 불필요한 트래픽이 매우 증가할 것으로 예상된다. 또한 리커시브 DNS의 경우 악의적인 공격에 따른 DNS 서버의 불능 상태가 발생 시 이를 복구하고 사용자에게 신뢰적인 DNS 서비스를 제공할 수 있는 메커니즘이 부족한 상태이다. 이를 해결하기 위해 본 논문은 애니캐스트(Anycast) 전송 기술을 리커시브 DNS에 적용하여 IPv6 DNS 도입에 따라 발생할 수 있는 불필요한 트래픽과 지연을 최소화한다. 또한 사용자에게 1차로 설정된 리커시브 DNS로의 질의·응답 실패 시에 실패 복구를 위한 리커시브 DNS로써 애니캐스트 리커시브 DNS를 설정하도록 하여 사용자에게 투명하고 공격에 안정적인 도메인 네임 서비스를 제공할 수 있는 방안을 제안한다.

Key Words : Recursive DNS, DNS fail-over mechanism, domain name resolution, Anycast, IPv6

ABSTRACT

Recursive DNS is configured as primary or secondary DNS on user PC and performs domain name resolution corresponding user's DNS query. At present, the amount of DNS traffic is occupied high rate in the total internet traffic and the internet traffic would be increased by failure of IPv6 DNS queries and responses as IPv6 transition environment. Also, existing Recursive DNS service mechanisms is unstable on malicious user's attack same as DoS/DDoS Attack and isn't provide to user trust DNS service fail-over.

In this paper, we propose IPv6 Recursive DNS service mechanisms for based on anycast for improving stability. It is that fail-over Recursive DNS is configured IPv6 Anycast address for primary Recursive DNS's fail-over. this mechanisms increases reliability and resiliency to DoS/DDoS attacks and reduces query latency and helps minimize DNS traffic as inducing IPv6 address.

Ⅰ. 서 론

DNS(Domain Name System)는 도메인 네임과 그에 해당하는 IP 주소를 변환하는 거대한 분산 데이터베이스로써 웹, 이메일 등 인터넷 응용 서비스

※ 본 연구는 한국 인터넷 진흥원의 URI 프로토콜 표준화 사업의 일환으로 위탁연구과제 "IPv6 리커시브 DNS 도입 모델 및 표준화 연구"의 지원으로 수행되었음.
* 숭실대학교 컴퓨터학과 통신연구실 (zzarara@cherry.ssu.ac.kr), ** 한국인터넷진흥원 (ckp@nida.or.kr)
논문번호 : #KICS2006-12-547, 접수일자 : 2006년 12월 26일, 최종논문접수일자 : 2007년 1월 15일

를 제공하는 핵심적인 요소이다.

2002년 10월, 루트 네임서버에 대한 DDoS 공격 발생으로 13개 루트 DNS 서버 중 8개의 서버가 서비스 불능 상태에 빠진 사건과 2003년 1월, SQL Slammer 웜 바이러스에 의한 DDoS 공격으로 13개 루트 DNS 서버 중 5개의 서버가 다운되는 사건이 발생한 이후 DNS의 안정성 문제는 매우 중요한 이슈로 등장하기 시작하였다.

리커시브 DNS는 사용자 PC환경에서 설정되어 사용자의 1차적인 DNS 질의·응답을 처리하는 DNS로써 공격에 노출될 위험이 매우 높으나 DoS/DDoS 공격 등과 같은 악의적인 공격에 대한 대비가 미비한 실정이다. 또한 현재 DNS의 안정성 확보를 위한 연구는 루트 DNS 및 TLD급 상위 DNS에 편중되어 있으며 이에 대해서도 아직 안정성이 보장되어 있지 못하기 때문에 리커시브 DNS의 특성을 고려한 방안 연구가 더욱 필요하다고 할 수 있다.

DNS 트래픽은 전체 인터넷 트래픽의 매우 많은 양을 차지하고 있으며 DNS 트래픽 중 1/3이상이 응답 실패가 발생하여 재질의 되는 것으로 연구된 바 있다.[4] 이러한 상황에서 IPv6 망으로의 완전한 전이까지 빈번한 IPv6 DNS 질의·응답 실패가 발생할 것이며 이에 따르는 인터넷의 트래픽과 지연의 증가는 매우 클 것으로 예상된다.

본 논문에서는 IP 애니캐스트 리커시브 DNS를 기존의 운영체제에서 제공하는 DNS 실패 복구 메커니즘에 적용하여 리커시브 DNS 질의·응답 실패에 의한 트래픽을 감소시키고 DoS/DDoS 공격에 대비하여 공격 발생 시 피해 범위를 최소화하고 국지화할 수 있는 방안을 제안한다.

본 논문의 2장에서는 리커시브 DNS의 개념을 살펴보고 3장에서는 IPv6를 지원하는 운영체제의 리커시브 DNS 실패 복구 메커니즘의 구조와 그에 따른 문제점을 분석한다. 4장에서는 IP 애니캐스트의 개념을 설명하고 5장에서는 애니캐스트 리커시브 DNS를 적용한 리커시브 DNS 실패 복구 메커니즘을 제안한다. 6장에서는 본 제안의 성능을 분석하고 7장에서는 결론을 맺도록 한다.

Ⅱ. 리커시브 DNS의 개념

DNS 네임 서버는 두 가지 동작 모드로 동작할 수 있는데 비리커시브 모드와 리커시브 모드이다. 리커시브 모드는 네임 서버가 기본적으로 동작하는 모드로써 모든 네임 서버는 이 동작 모드를 구현하여야 한다. 비리커시브 모드 네임서버는 자신이 갖고 있는 도메인 데이터베이스 영역의 정보에 대해서만 권한을 지니고 응답한다. 리커시브 모드는 네임 서버가 옵션 기능으로 구현, 동작할 수 있는 모드이며 이는 주로 클라이언트 호스트의 리커시브 질의 요청에 응답하기 위한 것이다.

그림 1의 (a)와 같이 리커시브 모드로 동작하는 네임 서버는 클라이언트에서 리커시브 질의 요청이 있는 경우, 자신이 포함하고 있는 리졸버 루틴을 사용하여 리졸버의 질의 절차를 수행하고 최종 응답 결과를 클라이언트로 응답한다. 즉, 리커시브 네임 서버는 본래의 네임 서버 기능에 리졸버의 역할까지 포함하여 동작하는 네임 서버라 할 수 있다. 비리커시브 모드로 동작하는 네임 서버는 리커시브 모드로 동작하는 네임 서버가 도메인 네임에 대한 정보를 가지고 있지 않을 경우 네임 질의 요청에 대한 응답을 수행하기 위한 것이며 자신이 관리하는 도메인 영역에 대한 질의 요청에 대해 응답한다. 이러한 네임 서버를 이터레이티브(iterative) 네임 서버라고 한다. 일반적으로 클라이언트로부터 요청되는 질의를 리커시브 질의, 리커시브 네임 서버의 상위 도메인 영역에 대한 질의를 이터레이티브 질의라고 한다.

DNS는 네임 체계 방식 중 도메인 네임을 사용하는 시스템 체계를 통칭하며 그림 1의 (b)와 같이 계층적인 트리로 이루어진다. 리커시브 네임 서버는 클라이언트의 도메인 네임 질의에 대해 상위 네임 서버로 이터레이티브 질의를 통해 도메인 네임 레졸루션을 수행한다. 그림 1의 (a)와 같이 이터레이티브 네임서버는 자신이 보유한 도메인 데이터베이스 영역에 대해서만 DNS 응답을 한다. 해당 도메인 데이터베이스 영역을 벗어난 영역의 도메인 네임에 대한 질의에 대해서는 현재 보유한 도메인 영역으로부터 가장 근접한 위임 영역의 네임서버 정보를 참조정보로 응답한다. 즉, 리졸버가 다음 단계

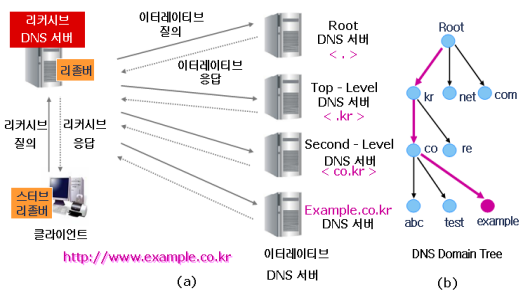

그림 1. DNS의 계층 구조

의 네임서버로 탐색을 계속할 수 있도록 다음 네임 서버 정보를 제공하는 역할만 한다.

Ⅳ. 기존의 리커시브 DNS 실패 복구 메커니즘의 문제점

현재 호스트의 운영체제에서는 GUI를 통해 1차와 2차 리커시브 DNS 서버를 설정하도록 지원하며 수동 설정에 의해 그 이상의 리커시브 DNS 서버 설정이 가능하다. 그러나 DoS/DDoS와 같은 공격이 리커시브 DNS에 발생할 경우 호스트 뿐 만 아니라 호스트가 속해 있는 네트워크에 무수히 많은 패킷이 유입되게 되어 네트워크 자체가 정상적인 작동을 할 수 없게 된다. 이러한 경우 1차 리커시브 DNS의 실패에 대비하기 위한 2차 리커시브 DNS 또한 서비스 불능 상황이 발생할 가능성이 매우 크다. 이를 위해 수동으로 그 이상의 리커시브 DNS를 설정할 수 있지만 사용자의 대부분이 해당 지식의 비전문가라는 점을 고려해 볼 때 해당 PC의 리커시브 DNS 서버 설정을 특정한 위험 요소를 피해서 적용하거나, 수동으로 변경하는 일, 설정된 리커시브 DNS 서버의 문제 발생 여부를 판단하는 등의 행동을 기대하는 것은 현실적이지 못하다.

안정적인 IPv6 리커시브 DNS 서비스를 저해하는 주요 요인 중 하나는 호스트의 운영체제의 스터브 리졸버 라이브러리에서 제공하는 DNS 실패 복구 메커니즘의 문제이다. 현재 호스트의 DNS 스터브 리졸버 라이브러리는 대부분 하나 이상의 리커시브 DNS를 설정할 수 있도록 하며 IPv6를 지원하는 윈도우 및 리눅스 계열의 많은 운영 체제의 경우 설정 가능한 리커시브 DNS의 수의 제안은 없다. 그림 2는 기존의 운영 체제에서 동작하는 리커시브 DNS 실패 복구 동작 과정을 나타낸다. 운영 체제의 스터브 리졸버 라이브러리는 설정된 리커시브 DNS 리스트를 따라 1차 리커시브 DNS 응답 실패 시 질의에 대한 원하는 응답이 올 때까지 리스트의 마지막까지 질의 메시지를 재전송 한다.

이러한 리커시브 DNS 실패 복구 메커니즘의 문제는 1차 리커시브 DNS의 장애 발생 시 그에 대한 히스토리를 저장하지 않고 새로운 리커시브 DNS 질의가 수행될 때마다 리커시브 DNS 리스트의 처음부터 질의를 전송한다는 것이다. 로컬 네트워크 상에서 1차 리커시브 DNS와 2차 리커시브 DNS를 설정할 경우 두 개의 리커시브 DNS가 모두 공격의

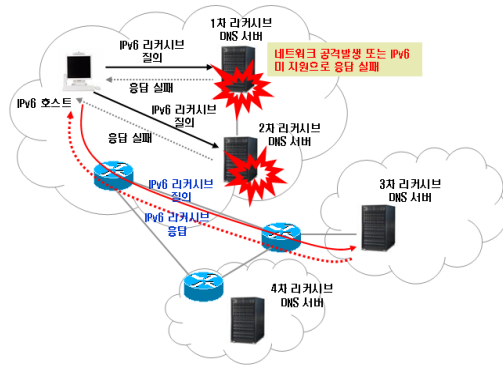

그림 2. 기존 리커시브 DNS의 실패 복구 동작 과정

대상이 될 가능성이 높으며 공격 발생 시에는 1차 DNS가 복구되기까지 인터넷 상에 불필요한 트래픽과 지연이 발생하게 된다.

현재 IPv6를 지원하는 많은 운영체제의 DNS 리졸버 라이브러리는 하나의 리커시브 DNS에 대해 6to4 터널을 통해 IPv6 질의와 IPv4 질의를 모두 수행하도록 구현되어 있다. 전체 인터넷 트래픽의 DNS 트래픽은 매우 큰 비중을 차지하며 실제 DNS 질의에 대한 응답의 매우 많은 양이 응답 실패로 처리된다. IPv6 DNS 도입이 안정화되기까지 IPv6 질의에 대한 응답 실패는 매우 빈번할 것이며 그에 따라 현재의 DNS 실패 복구 메커니즘은 인터넷에 과도한 트래픽과 지연을 발생시킬 것이다.

따라서 리커시브 DNS의 실패 복구 메커니즘은 사용자의 리커시브 DNS의 불능 시 사용자에게 연속적이고 투명하게 리커시브 DNS 서비스를 제공할 수 있도록 공격에 대한 복원력을 지원하도록 하여야 한다. 또한 IPv6 DNS 전이 기간 동안 사용자의 IPv6 리커시브 DNS 질의·응답의 실패에 따른 네트워크의 트래픽 발생을 최소화하면서 IPv6 DNS 서비스의 연속성의 보장할 것을 고려하여야 한다.

Ⅳ. IP 애니캐스트의 개념

IP 애니캐스트는 단일 IP를 다수의 호스트가 공유하여 사용할 수 있는 기술로 라우터에 의해 패킷이 사용자의 IP와 가장 가까운 단일 호스트로 라우팅 된다. 이는 마치 미러링(mirroring)과 같은 효과를 얻을 수 있는 방식으로 분산 서비스 거부 공격(DDoS 공격)에 효과적인 대응이 가능하다. 또한 장애 범위를 국지화하여 DNS 서비스의 안정성을, 다수의 DNS 서버에 의한 서비스 분산 및 다중화와,

DNS 서비스의 복원력 강화 효과를 얻을 수 있다.

애니캐스트는 단일 송신자와 다중 수신자 사이의 통신인 멀티캐스트, 그리고 단일 송신자와 단일 수신자 사이의 통신인 유니캐스트와 대비하여 정의되었다. 애니캐스트는 멀티캐스트와 같이 일-대-다 전송을 지원한다. 그러나 그룹 내의 모든 수신자에게 보내어지는 것이 아니라 가장 가까운 서버 또는 사용자에게 서비스 할 수 있는 최선의 한 노드로만 전송하므로 결과적으로는 일-대-일 전송 방식이라고도 볼 수 있다.

하나의 애니캐스트 주소는 다수의 호스트에 할당되며, 발신 노드가 해당 애니캐스트 주소를 목적지로 하여 패킷을 전송하게 되면, 라우터가 라우팅 테이블에서 같은 애니캐스트 주소를 갖는 호스트 중 가장 근접한 호스트로 라우팅하게 된다. 이때 라우팅 거리는 설정되어 있는 라우팅 프로토콜에 따르게 된다. 사용자는 가장 가까운 서비스 호스트로부터 서비스를 제공 받을 수 있음으로서 서비스의 품질 향상을, 애니캐스트 서비스 호스트는 부하 분산과 장애 시 서비스의 연속성 효과를 기대할 수 있다. 애니캐스트 주소는 유니캐스트 주소의 구조를 그대로 사용하며, 유니캐스트 주소 공간으로 부터 할당되어졌다. 그러므로 애니캐스트 주소는 유니캐스트 주소와 구문적으로 구분되지 않는다.

Ⅴ. 제안하는 리커시브 DNS 실패복구 메커니즘

5.1 애니캐스트 리커시브 DNS

애니캐스트 DNS는 서버 분산 구성 및 안정성 향상을 위해 IP 애니캐스트 기술을 적용한 DNS이다. 일반적으로 애니캐스트 주소는 같은 서비스를 제공하는 서버들의 그룹을 정의하는데 사용되며 비연결형 서비스에 적합하다. 호스트는 애니캐스트 주소를 통해 같은 애니캐스트 주소를 가진 서버 그룹 중에 서비스를 받고자 하는 사용자에게 가장 최선인 서버와 통신을 하게 된다. 정의되어 있는 특정 애니캐스트 DNS 서버의 주소를 사용자 시스템에 설정함으로써 별도의 프로토콜, 사용자 설정 또는 확장 메시지 없이 애니캐스트 DNS를 사용할 수 있다.

그림 5와 같이 여러 개의 서비스 노드에 1대 이상의 서버 설치, 해당 서버 그룹에 대하여 동일한 IP를 부여하면 해당 IP 주소를 라우팅 프로토콜을 통해 전달되고 동일 IP 주소에 대한 여러 개의 경로가 존재하게 된다. 각각의 라우터는 여러 개의 경로 중 라우팅 프로토콜에 의해 정의되는 최적의 경로를 선택하여 라우팅 테이블에 설정하게 되면 서비스 이용자의 서비스 요청 시 이용자가 최초로 접속된 라우터에서 라우팅에 의해 서비스 노드를 선택하여 서비스 처리를 하고 서버 장애 또는 네트워크 변경 시 라우팅 프로토콜의 라우팅 정보 전달 기능을 통해 정상적인 노드 및 경로를 자동 선택하게 된다.

IP 애니캐스트 기술에 의해 사용자의 리커시브 DNS 질의 트래픽은 라우팅 상의 가장 인접한 리커시브 DNS 서버로 라우팅 되어 DNS 서비스를 받게 되는데, 이 때 기존 설정된 서버에 장애가 발생한다면 사용자는 차선의 리커시브 DNS 서버를 통해 서비스를 받을 수 있도록 설정되어야 할 것이다.

그림 3은 정상 상태의 애니캐스트 리커시브 DNS 서비스 전환 메커니즘을 나타낸다. 그림 3과 같이 호스트 A, B는 애니캐스트의 특성에 따라 라우팅 경로 상 가장 가까운 리커시브 DNS 서버인 A로 포워딩되어 서비스를 받게 된다. 그림 4는 라우팅이나 서비스 공격에 의한 장애 발생 시 즉각적인 DNS 장애 극복 과정에서 일어나는 자동 전환 메커니즘을 보여준다. 리커시브 DNS 서버 A에 장애가 발생하자 애니캐스트 특성에 따라 응답이 없는 리커시브 DNS 서버 A로의 라우팅을 중단하고 차선책으로 리커시브 DNS 서버 B로 트래픽의 경로가 전환되었다.

최근까지 세계적으로 꾸준히 증가하고 있는 DNS에 대한 보안, 운영상의 외부 장애 요인에 독립성을 높이고 인터넷 기반 안정성을 강화할 수 있는 방안의 하나로 루트 DNS 서버에 애니캐스트 기술을 적용하는 것에 대한 관심이 높아지고 있으며, 이미 일부 루트 DNS 서버는 애니캐스트 기술이 적용되어 운영 중에 있다.

IP 애니캐스트는 IPv6 DNS 도입 지연의 주요 요인인 DNS UDP 패킷 사이즈의 한계에 관계없이 DNS 수를 증가시킬 수 있고 다양한 네트워크 토폴로지 상에 또는 지리적으로 다양한 장소에 리커시브 DNS 노드를 분산시켜 구축할 수 있다. 따라서 DoS/DDoS 공격에 대한 대비책이 될 수 있으며 공격 발생 시 피해의 범위를 최소화하고 국지화할 수 있어 안정적인 리커시브 DNS 서비스 제공이 가능하다. 또한 애니캐스트를 이용하여 리커시브 DNS를 구축할 경우 사용자로부터의 1개의 IP 질의 패킷으로 호스트로부터 가장 가까운 라우팅 경로 상

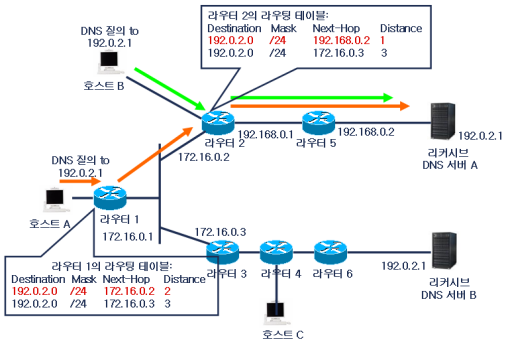

그림 3. 애니캐스트 DNS 서비스 전환 메커니즘(정상 상태)

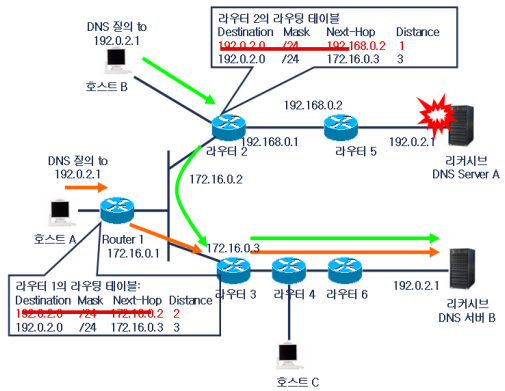

그림 4. 애니캐스트 DNS 서비스 전환 메커니즘(장애 상태)

의 리커시브 DNS로 전달되고 질의를 받은 리커시브 DNS가 불능 상태일 경우 같은 애니캐스트 주소를 가지는 그룹 내의 다음 차 순의 리커시브 DNS로 라우팅 된다. 따라서 호스트에게 투명하게 DNS 질의·응답 실패를 복구할 수 있으며 DNS 트래픽 부하를 줄이고 호스트에게 최소의 지연으로 연속적인 리커시브 DNS 서비스를 제공할 수 있다.

5.2 애니캐스트 리커시브 DNS 실패 복구 메커니즘

본 논문에서는 호스트의 PC에서 설정한 1차 리커시브 DNS가 IPv6를 지원하지 못할 경우 또는 악의적인 공격에 의해 서비스 불능 상태일 경우에 대비한 DNS 실패 복구를 위한 리커시브 DNS로써 애니캐스트 리커시브 DNS를 설정할 것을 제안한다.

기존의 DNS 실패 복구 메커니즘에서는 1차 IPv6 리커시브 DNS의 불능 시 IPv6를 지원하고 질의에 대한 적합한 응답을 받을 때까지 설정된 리커시브 DNS 리스트를 따라 반복적인 질의를 수행한다. 이러한 방식은 인터넷 상에 많은 트래픽과 유발시키고 호스트의 DNS 질의에 대한 응답이 오기까지 오랜 지연을 발생시키며 안정적인 IPv6 DNS 서비스를 보장하지 않는다.

DNS 질의·응답 실패 복구를 위한 리커시브 DNS의 주소 설정을 위해 윈도우 계열 운영체제의 경우에는 GUI DNS 주소 설정 창을 통해 1차와 2차의 리커시브 DNS를 설정하도록 되어 있으며 2차 이상의 리커시브 DNS를 설정을 원할 경우 사용자의 수동 설정을 요구한다. 일반적으로 로컬 네트워크상에 존재하는 1차와 2차 리커시브 DNS는 동일한 공격 위협에 노출될 가능성이 높기 때문에 1차 리커시브 DNS가 불능 상태일 경우 2차 리커시브 DNS도 불능 상태일 경우가 많다. 또한 1,2차 리커시브 DNS가 동일하게 관리 운영될 경우 1차 리커시브 DNS가 IPv6 지원을 하지 않을 경우 2차 리커시브 DNS도 IPv6를 지원하지 않을 가능성이 높다. 따라서 애니캐스트 리커시브 DNS가 DNS 실패 복구 리스트의 상위에 위치할수록 DNS 서비스의 복원력과 안정성이 높아지며 불필요한 트래픽의 발생은 감소한다. 2차 리커시브 DNS의 가용성을 높이고 안정적이고 연속적인 리커시브 DNS 서비스를 보장하기 위해 호스트는 2차 리커시브 DNS 주소로써 애니캐스트 리커시브 DNS를 설정할 것을 제안한다. 이를 통해 호스트는 부수적인 설정 없이 DNS 서버 장애 발생 시에도 서비스를 유지할 수 있다.

가. 리커시브 DNS 서버의 애니캐스트 IP 할당

애니캐스트 리커시브 DNS 서버를 사용하기 위해, 해당 리커시브 DNS 서버의 네트워크 인터페이스에는 기존의 IP 주소를 유지한 상태로 애니캐스트 IP 주소를 추가 할당한다. 애니캐스트 IP 주소가 할당 된 리커시브 DNS 서버는 두 개의 IP 주소를 가지고 이 중 글로벌 유니캐스트 주소는 1차 리커시브 DNS 서버의 역할을 가지는 IP 주소로 기존 리커시브 DNS 서버의 서비스를 유지하는데 사용하며, 글로벌 애니캐스트 주소는 2차 리커시브 DNS 서버로의 이용을 위한 IP 주소로서 애니캐스트 DNS 서버로서의 서비스를 위해 사용한다. 이 때, 할당되는 애니캐스트 주소는 예약된 주소 범위 내에서 선택하게 되는데, 애니캐스트 서비스를 위해 예약된 주소 범위를 사용을 위해서는 IP 주소의 관리 기관인 ICANN을 통해 해당 주소 범위의 예약이 필요하다. 이것은 앞으로 정의될 수 있는 애니캐스트 주소를 활용한 다양한 응용 프로그램 및 서비스를 위한 목적으로 예약될 수 있을 것이다.

하나의 인터페이스에 두개의 IP 주소를 할당하는 방법은 IP 주소체계에 따라 다르다. IPv4 환경에서

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=203.253.21.136
NETMASK=255.255.255.0
GATEWAY=203.253.21.254
```

(a) ifcfg-eth0 file

```
DEVICE=eth0:1
ONBOOT=yes
BOOTPROTO=static
IPADDR=203.253.21.137
NETMASK=255.255.255.0
```

(b) ifcfg-eth0:1 file

그림 5. IP Aliasing
(/etc/sysconfig/network-script/ifcfg-eth0)

는 IP Aliasing('multi-homing') 기술[16]을 통해 그림 5와 같이 각각의 IP 주소를 할당할 수 있고, IPv6 환경에서는 다수 IP 주소의 사용을 허용하고 있다.

나. 애니캐스트를 이용한 리커시브 DNS 서버구성

1차 리커시브 DNS 서버 설정에 기존의 글로벌 유니캐스트 주소 설정을 유지하고 2차 리커시브 DNS 서버 설정에 예약된 범위의 애니캐스트 IP 주소를 모두 할당한 리커시브 DNS 서버들을 적용한 리커시브 DNS 서버 구성은 기존의 리커시브 DNS의 실패 복구 방식의 문제를 해결한다.

그림 6은 애니캐스트 리커시브 DNS를 적용한 리커시브 실패 복구 방식의 개선을 나타낸다. 호스트에 1차 리커시브 DNS 서버로 설정되어 있던 리커시브 DNS 서버가 호스트의 질의에 대해 응답 불능 상태이거나, 리커시브 DNS 서버가 속한 라우터의 네트워크에 문제가 발생한다면 호스트는 2차 리커시브 DNS 서버로 설정되어 있는 애니캐스트 IP 주소로 리커시브 DNS 패킷을 전송한다. 이 리커시브 DNS 패킷은 애니캐스트 라우팅에 의해 가장 근접한 애니캐스트 DNS 서버로 전환된다.

제안하는 리커시브 DNS 서버 구성에서 애니캐스트 리커시브 DNS 서버를 1차 리커시브 DNS로 설정한다면 2차 리커시브 DNS 서버 설정 과정 없이 리커시브 DNS 서버 설정을 간소화 할 수 있다. 하지만 클라이언트의 리커시브 DNS 서버 설정을 애니캐스트 리커시브 DNS 서버의 주소로 할당할 경우 일부 애니캐스트 그룹의 리커시브 DNS로 DNS 트래픽이 집중될 수 있다. 그러나 현실적으로 네트워크상의 모든 리커시브 DNS의 트래픽을 일부의 애니캐스트 리커시브 DNS 그룹이 수용하기에는 무리가 있으며 애니캐스트 리커시브 DNS가 범용적으로 사용되고 IPv6 DNS 서비스가 안정화 될 때까지는 1차 리커시브 DNS의 경우 로컬 네트워크에서 제공하는 리커시브 DNS를 사용할 것을 권고 한다. 기본적으로 IPv6 망이 안정화되기까지는 IPv4/IPv6

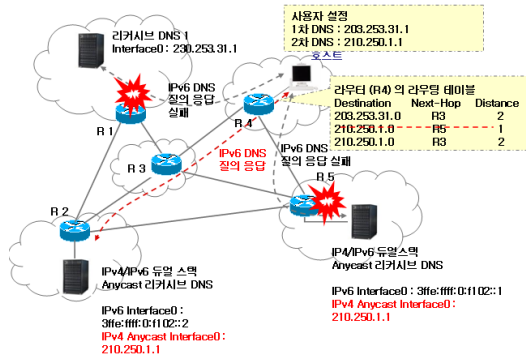

그림 6. 애니캐스트 DNS 서버를 이용한 DNS 서버 구성

듀얼 스택으로 구성된 리커시브 DNS를 IPv4 애니캐스트 그룹으로 구축하며 향후 점진적으로 IPv6 애니캐스트 주소를 할당하고 IPv6 애니캐스트 리커시브 DNS 구룹을 구성하는 방향으로 추진할 것을 제안한다.

Ⅶ. 성능 평가

본 논문에서는 일반적인 운영체제에서 제공하는 기존의 리커시브 DNS 실패 복구 메커니즘과 제안하는 애니캐스트 리커시브 DNS 실패 복구 메커니즘의 성능을 비교 평가한다. 비교 평가를 위한 실험 환경은 표 1과 같다. 기존의 실패 복구 메커니즘을 사용할 경우 일반적인 리커시브 DNS 사용 환경과 동일하게 사용자 PC에 설정되는 1차와 2차 리커시브 DNS는 사용자 PC가 위치한 네트워크와 동일한 네트워크 환경에 존재한다. 제안하는 애니캐스트 리커시브 DNS 실패 복구 메커니즘을 사용할 경우 사용자 PC와 1차 리커시브 DNS는 동일한 네트워크 환경에 존재하나 2차 리커시브 DNS는 애니캐스트 주소를 가지는 애니캐스트 그룹 내의 리커시브 DNS로써 사용자 PC와 다른 네트워크 상에 존재한다.

기존의 리커시브 DNS 실패 복구 메커니즘을 사용하는 경우 사용자의 로컬 네트워크 상에 문제로 인해 사용자 PC에 설정되어 있는 두 대의 리커시브 DNS 서버들이 모두 응답을 하지 않을 경우, WindowsXP 운영체제의 리커시브 DNS 질의 재전송 과정과 반복과정, 그리고 해당 과정에 소요되는 시간을 측정하고, 이 때 사용자에게 요구되는 응답 대기시간을 측정한다. 비교 대상이 되는 애니캐스트 DNS 적용 환경에서의 DNS 질의 재전송은 사용자 PC(Stub Resolver)는 1차로 설정되어있는 Unicast DNS 서버로의 질의가 실패한 후, 2차로 설정되어

있는 애니캐스트 그룹에서 이용 가능한 DNS 서버를 찾는다. 두 개의 실패 복구 메커니즘을 적용한 각각의 성능은 Ethereal을 통해 리커시브 DNS 서버 전환 과정에서 일어나는 패킷 전송 과정과 애니캐스트 DNS 적용을 통해 얻을 수 있는 비용을 측정하였다.

6.1 기존의 리커시브 DNS 실패 복구 메커니즘

사용자 PC에 설정되어 있는 리커시브 DNS 서버들이 불능 상태일 경우 때, 호스트에서의 재질의 과정을 알아보기 위해 100회의 질의를 수행한 결과 그 패턴은 표 2와 같다. 이를 통해 클라이언트는 매 질의마다 설정된 리커시브 DNS 리스트 내에서 서버를 변경한다는 것을 확인할 수 있다.

표 2를 그래프로 나타내면 그림 9와 같으며 7번째, 14번째, 7의 배수 회에서 큰 폭의 지연 시간을 갖게 된다. 이것은 표 2의 7번째 질의에서 타임 아웃되어 질의 구조를 바꾸어 재전송을 수행하기 때문이다. 리커시브 DNS 질의가 실패할 경우 운영체제가 질의의 형태를 표 3과 같은 형태로 바꾸어 재전송을 시작한다. 표 3에서 볼 수 있듯, 총 7가지 형태의 도메인명으로 IPv4/IPv6 도메인네임 포맷으로 질의를 바꿔가며 질의를 성공 할 때까지 시도한다. 하나의 질의 형태는 다시 표 2의 과정을 거치

표 1. 실험 환경

요소	환경
시스템	Intel Pentium4 3.0Ghz, 1024Mb
운영체제	Windows XP SP2
사용 툴	Ethereal 0.99.0, Visual C++
사용 언어	C++, PHP
라이브러리	WinPcap, IPHelper API, Mysql API
통신 패킷	UDP(512byte)
1차 리커시브 DNS	203.253.25.138 (Unicast, Linux, BIND9)
2 차 리 커 시 브 DNS	168.126.63.1 (애니캐스트, KT)

표 2. Windows XP 환경에서 재질의 시 타임 아웃 값

n	타임아웃(msec)	도메인	목적지
1	1000	www.ssu.ac.kr	1차
2	1000	www.ssu.ac.kr	2차
3	2000	www.ssu.ac.kr	1차
4	0.1	www.ssu.ac.kr	1차
5	3999	www.ssu.ac.kr	2차
6	0.1	www.ssu.ac.kr	1차
7	7009	www.ssu.ac.kr	2차

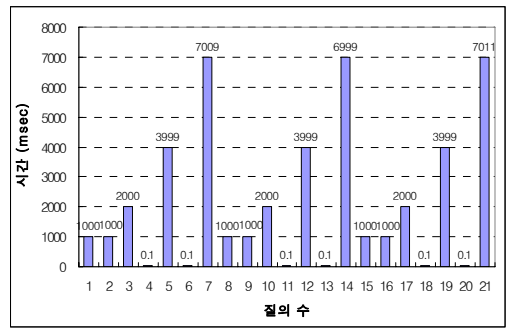

그림 9. Windows XP 환경에서 리커시브 DNS 재질의 시 타임 아웃 값 패턴

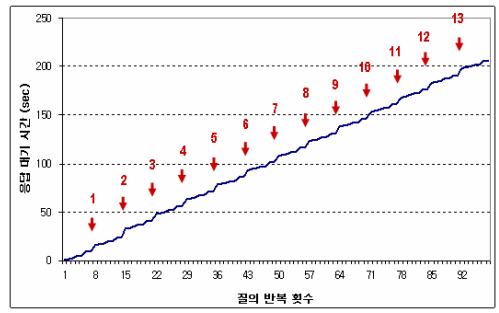

그림 10. 기존의 리커시브 DNS 실패 복구 메커니즘 상에서 사용자의 응답 대기 시간

표 3. DNS 질의 실패 후 질의 형태의 변화

k	도메인	포맷
1	www.ssu.ac.kr	A
2	www.ssu.ac.kr	AAAA
3	auto.search.msn.com	A
4	auto.search.msn.com	AAAA
5	www.www.ssu.ac.kr.co.kr	A
6	www.www.ssu.ac.kr.co.kr	AAAA
7	www.www.ssu.ac.kr.com	A
8	www.www.ssu.ac.kr.com	AAAA
9	www.www.ssu.ac.kr.org	A
10	www.www.ssu.ac.kr.org	AAAA
11	www.www.ssu.ac.kr.net	A
12	www.www.ssu.ac.kr.net	AAAA
13	auto.search.msn.com	A
14	auto.search.msn.com	AAAA

므로 호스트에 설정된 DNS 서버의 서비스가 정지되었을 때 지연이 매우 큼을 알 수 있다. 그림 10은 기존 실패 복구 메커니즘 상에서의 사용자의 응답 대기 시간을 나타낸다.

6.2 제안하는 애니캐스트 리커시브 DNS 실패 복구 메커니즘

2차 리커시브 DNS 서버를 애니캐스트 리커시브

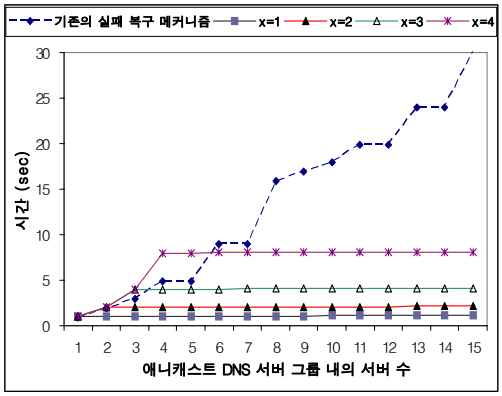

그림 11. 애니캐스트 리커시브 DNS 서버 적용을 통해 단축되는 응답 대기 시간

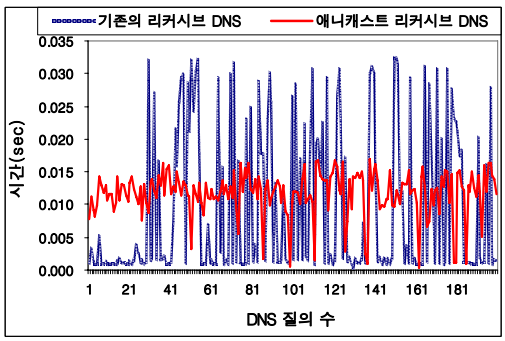

그림 12. 리커시브 DNS 서버 주소 방식에 따른 질의 시간

DNS 서버로 적용할 경우 애니캐스트 그룹의 주소로 설정된 2차 DNS 서버는 1차 DNS 서버의 서비스가 정지되면 애니캐스트 주소를 할당받은 서버 중 라우팅 거리 상 가장 가까운 서버를 선택하여 서비스를 시도한다. 이 시도가 실패한다면 같은 애니캐스트 그룹의 주소를 가지는 다른 애니캐스트 리커시브 DNS 서버를 찾아 질의를 시도하게 된다.

애니캐스트 리커시브 DNS를 실패 복구 메커니즘을 적용할 경우 설정한 애니캐스트 DNS 서버가 속한 애니캐스트 그룹의 리커시브 DNS 수가 6 이상이라면, 그룹 내에서 최대 6대의 다른 애니캐스트 DNS 서버들에 임의로 질의를 전송하며 해당 그룹의 모든 애니캐스트 DNS 서버가 사용할 수 없는 상황이라면 해당 질의는 실패임을 확인하게 된다.

그림 11은 기존의 실패 복구 메커니즘과 제안한 애니캐스트 리커시브 실패 복구 메커니즘 상에서 1차 리커시브 DNS가 불능 상태일 경우 실패 복구 과정 동작 시 응답 대기 시간을 비교한 것이다. 그림 11의 그래프를 통해, 기존의 리커시브 실패 복구 메커니즘보다 애니캐스트 DNS 서버 적용 환경의 예상되는 응답 대기시간이 짧다는 것을 알 수 있다. 그림 11에서 x값은 서비스 가능한 2차 애니캐스트 리커시브 DNS를 만나게 되는 홉 수이다. 2차로 설정된 애니캐스트 주소를 가진 서버 중 선택된 첫 번째 서버가 서비스 가능하다면 x=1, 첫 번째로 선택된 서버 역시 서비스를 할 수 없는 상태라 두 번째로 서비스 전환된 서버를 이용하게 되는 상황의 그래프가 x=2의 그래프 이다.

그림 10에서 볼 수 있듯, 기존의 실패 복구 메커니즘 상에서는 설정된 리커시브 DNS 서버들이 서비스를 할 수 없을 경우, 총 98회의 질의를 수행한 후 해당 서비스를 유지할 수 없음을 확인하게 되는 반면, 애니캐스트 DNS 적용을 한 그림 11에서는 서비스 중인 다른 애니캐스트 DNS 서버를 만나는 시점까지만 질의를 하여 질의 횟수가 눈에 띄게 감소하며, 기존 환경처럼 설정된 소수의 리커시브 DNS 서버를 대상으로 하는 질의가 아닌, 동일한 애니캐스트 주소를 사용하는 다수의 DNS 서버로 질의를 시도함에 따라 서비스 중인 리커시브 DNS 서버를 찾을 확률을 높일 수 있다.

그림 12는 일반적으로 리커시브 DNS 서비스에 문제가 없는 상황에서 기존의 유니캐스트 실패 복구 메커니즘을 사용하는 경우와 제안한 애니캐스트 리커시브 DNS 실패 복구 메커니즘을 그림 12 리커시브 DNS 서버 주소 방식에 따른 질의 시간 사용했을 경우 질의·응답을 수신할 때까지의 시간을 나타낸다. 애니캐스트 리커시브 DNS 서버를 사용하는 방식은 평균 2 msec 늦은 반응속도를 보여주었지만 대체적으로 고른 질의 시간을 보여주었고, 유니캐스트 DNS 서버는 목적지가 되는 사이트에 따라 심한 편차를 보여주었다.

Ⅶ. 결 론

DNS는 인터넷 상의 도메인 네임을 그에 해당하는 IP 주소로 전환하여 주는 역할을 하는 기술로 현재 대부분의 인터넷 응용 프로그램을 통한 서비스가 이루어지기 위해 반드시 필요한 분산 데이터베이스로서 그 중요성이 커지고 있다. 하지만 현재 운영체제에서 제공하는 리커시브 실패 복구 메커니즘은 네트워크를 목적으로 하는 공격이나 DoS/DDoS 공격 등으로 백업 DNS 서버까지 서비스를 제공할 수 없는 상황에서는 적절하게 대응할 수 없다. 또한 기존의 리커시브 DNS 실패 복구 메커니즘에는 IPv6 도입에 따른 도메인 네임의 질의·

응답 실패로 인한 트래픽 부하와 지연의 증가에 따른 문제를 해결하기 위한 대책이 미흡하였다.

이러한 문제를 해결하기 위해 본 논문에서는 애니캐스트 주소 체계를 이용하여 리커시브 DNS 서버를 지역적으로 분산하고 그룹화 하며, 서버에 문제가 발생했을 경우 그룹 내의 다른 서버로 전환할 수 있도록 하였다. 그리고 제안한 기법의 성능 분석을 위해 구현물을 이용한 테스트와 패킷 분석을 이용하여 기존의 방식에서 DNS 서비스의 성능을 최대한 유지하면서 생존력을 향상 시켰음을 증명하였다.

본 논문에서 제안하는 애니캐스트 리커시브 DNS 실패 복구 메커니즘은 리커시브 DNS 이용하여 기존의 리커시브 DNS 서비스의 성능을 유지하면서 리커시브 DNS의 위험 상황에서 더욱 안정적인 리커시브 DNS 서비스를 제공할 수 있을 것이다. 이를 위해 향후에는 본 제안에 대해 보다 확장된 범위의 애니캐스트 리커시브 DNS 그룹을 구성하였을 경우와 다양한 환경 상에서 애니캐스트 커시브 DNS 실패 복구 메커니즘을 적용하였을 경우의 성능에 대한 연구를 진행할 필요가 있다.

참 고 문 헌

〔1〕 S. Lee, Y. Ju, W. Kim, "Default Well-known DNS Resolver IPv6 Address Using Anycast", Internet Draft, October 2005

〔2〕 Yasuhiro Orange Morishita, Masato Minda, "An Approach for Increasing Root And TLD DNS Servers" Internet Draft, Jul 2004

〔3〕 Kevin Miller "Three Pracitical Ways to Improve Your Network", in proc. Large Installation Systems Administration Conference San Diego, CA, USA October 26, 2003

〔4〕 Jaeyeon Jung, Emil Sit, Hari Balakrishnan, Member, "DNS Performance and the Effectiveness of Caching", IEEE/ACM Transactions on networking, Vol.10, No. 5, October 2002, pp. 589-603

〔5〕 Satoshi Doi, Shingo Ata, Hiroshi Kitamura, Masayuki Murata, "IPv6 Anycast for Simple and Effective Service-Oriented Communications", IEEE Communications Magazine May, 2004

〔6〕 Ching-Yu Lin, Jung-Hua Lo, Sy-Yen Kuo, "Load-Balanced Anycast Routing", in proc. ICPADS'04

〔7〕 Sandeep Sarat, Vasileios Pappas, Andreas Terzis, " On the Use of Anycast in DNS", in proc. SIGMETRICS'05, June 6-10, 2005

〔8〕 Tony Bonanno, HyoungJun Kim, Jungsoo Park, "Design and Implementation of Recursive DNS Server", ICACT'06, Feb. 20-22. 2006

〔9〕 C. Partridge, T. Mendez, and W. Milliken, ''Host Anycasting Service,'' RFC1546, November, 1993

〔10〕 Niall Mansfield, "IP aliasing ("multi-homing") on Linux", addison Wesley Professional 2003Qiangfeng Jiang, D. Manivannan, "Routing Protocols for Sensor Networks," *CCNC* 2004, Jan, 2004.

서 유 화 (Yuhwa Suh) 학생회원

2003년 2월 숭실대학교 컴퓨터학부 졸업

2005년 8월 숭실대학교 컴퓨터학과 공학석사

2006년 3월~현재 숭실대학교 컴퓨터학과 박사과정

<관심분야> 애드혹/센서 네트워크, 모바일 IP, 멀티캐스트, 휴대인터넷

김 경 민 (Kyungmin Kim) 학생회원

2004년 한경대학교 컴퓨터공학과 졸업

2005년 9월~현재 숭실대학교 컴퓨터학과 석사과정

<관심분야> 멀티캐스트, DNS

신 용 태 (Yongtae Shin) 정회원

1985년 한양대학교 산업공학과 졸업
1990년 Univ. of Iowa 전산학과 석사
1994년 Univ. of Iowa 전산학과 박사
1994년~1995년 Michigan State Univ. 전산학과 객원 교수
1995년 3월~현재 숭실대학교 컴퓨터학부 부교수
<관심분야> 멀티캐스트, 실시간 프로토콜, 이동통신, DRM

송 관 호 (Kwanhoo Song) 정회원

1973년~1980년 서울대학교 공과대학 전자공학과 졸업
1981년~1984년 한양대학교 산업대학원 전자공학과 졸업 공학석사
1990년~1995년 광운대학교 대학원 전자통신공학과 졸업 공학박사
1996년~1997년 서울대학교 행정대학원 정보통신정책과 수료
1998년~1999년 Visiting Professor University of Maryland
2005년~2005년 글로벌 최고경영자과정 수료
1997년~1985년 LG전선(주) 정보시스템 과장
1979년~1985년 금성전선연구소 정보시스템 과장
1985년~1987년 데이콤(주) 미래연구실장
1987년~1994년 한국전산원 정보통신표준담당 연구위원
1995년~1995년 한국전산원 초고속국가망구축실장
1996년~1997년 한국전산원 표준본부 본부장
1999년~1999년 한국전산원 국가정보화센터 단장
1998년~2002년 APAN(Asia Pacific Advanced Network) 부회장
1999년~2004년 한국인터넷정보센터 초대 원장
2000년~2000년 실버넷운동 운영위원장
2002년~2002년 건국대학교 정보통신대학 겸임교수
2002년~현재 한국통신학회 이사(산학협동위원장)
2002년~현재 한국인터넷정보학회 부회장
2003년~현재 한국해양정보통신학회 부회장
2003년~현재 URI표준화포럼 의장
2004년~현재 한국인터넷진흥원 초대 원장
2005년~현재 사이버명예시민운동 추진위원
2005년~현재 국회 과학기술정보통신위원회 정보통신 정책자문위원

김 원 (Weon Kim) 정회원

1980년~1984년 한양대학교 전자공학과 졸업
1987년~1989년 한양대학교전자공학과 졸업 공학석사
1998년~2002년 경희대학교전자공학 (공학 박사)
1984년~1987년 국방과학연구소 연구원
1989년~1992년 (주)데이콤 대리
1992년~1999년 한국전산원 선임연구원
1999년~2003년 한국인터넷진흥원 부장
2003년~현재 한국인터넷진흥원 단장

박 찬 기 (Chanki Park) 정회원

1994년~1995년 선경정보시스템 사원
1995년~1999년 한국전산원 주임연구원
1999년~현재 한국인터넷진흥원 (NIDA) 기술연구팀 팀장