네트워크 도달성 모니터링을 위한 DNS 서버 수집 방법

[1]홍성철, [2]김태영, [2]권동우, [2]김현우, [2]주홍택, [1]홍원기
[1]포항공과대학교 컴퓨터공학과, [2]계명대학교 컴퓨터공학과

[1]{pluto80, jwkhong}@postech.ac.kr, [2]{arsenic, dwkwon, khw2890, juht}@kmu.ac.kr

A Method Collecting DNS Servers for Network Reachability Monitoring

[1]Seongcheol Hong, [2]Taeyoung Kim, [2]Dongwoo Kwon, [2]Hyeonwoo Kim, [2]Hongtaek Ju,
[1]James W. Hong
[1]Department of Computer Science and Engineering, POSTECH
[2]Department of Computer Science and Engineering, Keimyung University

요 약

인터넷은 수많은 AS 들이 상호 연결되어 이루어진 거대한 통신망으로써, 이들 간의 라우팅 프로토콜로 BGP 를 사용한다. BGP 라우팅은 분산 라우팅 방법으로 일부의 오류나 고장에 의하여 도달성이 보장되지 않는다. 본 논문에서는 인터넷 수준에서 한 지점에서 다른 네트워크로의 도달성 모니터링을 위한 DNS 서버 수집 방법을 제시한다. 네트워크 도달성은 네트워크의 고장위치 확인, SLA 정보 수집, 라우팅 상태 검증 등 다양한 목적을 위해 필요한 정보이며, 네트워크 관리자에게 유용하게 활용될 수 있다.

Ⅰ. 서 론

인터넷은 BGP (Border Gateway Protocol) [1] 를 사용하여 라우팅 정보를 교환하는 AS (Autonomous System)들로 이루어진 거대한 분산 시스템이다. 라우팅의 기본 목적은 직접 연결되지 않은 호스트들 사이에 통신이 가능하도록 연결 경로를 설정하는 것이다. 라우터(Router)가 패킷을 전달할 때는 그 패킷을 목적지까지 보내기 위해 어느 경로로 보내야 하는지를 선택하게 된다. 여기서 도달성 (Reachability) 이란 라우팅에 의하여 설정된 경로로 실제 데이터를 전달할 수 있는가에 대한 판단 결과이다. BGP 라우팅은 분산 라우팅 방법으로 일부의 오류나 고장에 의하여 도달성이 보장되지 않는다. 즉, AS 경로와 데이터 경로와의 불일치는 다양한 이유로 인해 존재하며 [2, 3, 4], 따라서 라우팅 정보만으로는 도달성이 확보되지 않는다. 그러므로, 도달성은 실제 검증을 통하여 확인할 필요성이 있으며, 이 정보는 네트워크의 고장위치 확인, SLA 정보 수집, 라우팅 상태 검증 등 다양한 목적을 위하여 필요하다.

본 논문에서는 인터넷 수준에서 한 지점에서 다른 네트워크로의 도달성 여부를 DNS 서버를 이용하여 모니터링 하는 방법을 제안한다. 즉, BGP 라우팅 정보에 근거하여 한 AS 에서 다른 AS 에 대한 도달성을 검증하는 것이다. 주기적으로 수집되는 도달성 유무에 대한 정보는 관리자 입장에서 유용하게 활용될 수 있다.

Ⅱ. 본론

BGP 는 AS 와 AS 가 만나는 경계 간의 라우팅 프로토콜로써, 조직 간의 문제를 해결하기 위한 여러 가지 정책을 다루는 프로토콜이다. 현재는 인터넷의 보편화와 더불어 AS 의 숫자가 크게 늘어가면서, IX (Internet eXchange)나 ISP (Internet Service Provider) 뿐만 아니라 일정 규모 이상의 네트워크에서 많이 사용하는 라우팅 프로토콜이 되었고 서로 간의 정책은 점점 복잡해지고 있다.

인터넷에서 서로 다른 기관 사이의 라우팅은 BGP 를 이용하여 주고 받는 IP prefix 와 AS path 정보로 이루어진다. 라우터는 목적지에 대한 정보를 CIDR (Classless Inter-Domain Routing) 형태의 IP prefix 별로 다양한 경로 정보를 인접한 라우터들로부터 입수한다. 즉, BGP 라우팅은 인접한 곳으로부터만 정보를 받는 분산 라우팅 방법으로 목적지로의 도달성이 항상 보장되지 않는다. 따라서 도달성을 실제 검증을 통하여 주기적으로 확인함으로써 안정적인 라우팅을 제공할 수 있다.

전통적으로 특정 호스트로의 도달성 검증은 Ping 혹은 Traceroute 등의 프로그램을 이용하였다. 이들 프로그램은 ICMP 패킷을 이용한 가장 직접적인 방법이다. 그러나 이 방법들은 인터넷 보안 강화로 인하여 ICMP 패킷이 방화벽을 통과하기 힘들고 많은 네트워크 장치들이 ICMP 패킷에 대한 Reply 를 보내지 않도록 설정되어 있어 사용하기 힘들다. 따라서 ICMP 뿐만 아니라 TCP 및 UDP 등 다양한 프로토콜을 활용할 필요가 있다. 여기서 TCP 나 UDP 를 사용하여 도달성을 정확하게 확인할 때는 살아있는 호스트(Live Host)여야 한다는 조건이 붙는다. 이러한 살아있는 호스트가 모든

이 논문은 2009 년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업 연구 (NRF-2009-0089825)

AS 내에 존재해야 하고 손쉽게 IP 주소를 얻어낼 수 있어야 하는데, 그 중 가능한 것이 DNS 서버이다. 대부분의 기관은 자신만의 도메인 이름(Domain Name)을 가지고 있고, 기관 내에 DNS 서버를 운영하여 네트워크를 관리하기 때문이다. AS 별로 가지고 있는 DNS 서버에 대한 정보가 있으면 이를 이용하여 해당 AS 로의 도달성 검증을 수행할 수 있다. DNS 서버는 해당 기관이 보유한 도메인 네임에 대한 응답을 담당하기 때문에 항상 살아있는 호스트이고, 안정성을 위해 대부분의 기관이 보조 DNS 서버를 같이 운영하기 때문에 AS 별 살아있는 호스트로 활용하기에 매우 적합하다. 모든 AS 가 가진 DNS 서버로의 도달성 검증을 주기적으로 수행함으로써 관리자는 모든 목적지로의 라우팅이 제대로 이루어지고 있는지 알 수 있다.

AS 별로 DNS 서버를 찾아내기 위하여 다음과 같은 과정을 거친다. 우선 AS 별로 IP prefix 를 알기 위해 라우팅 테이블 정보를 분석하는데, RouteViews [5]에서 가져온 RIB (Routing Information Base) 데이터가 여기에 활용될 수 있다. RIB 에는 특정 IP prefix 로 가기 위한 AS path 정보가 포함되어 있고, 최종 목적지 AS 를 보면 해당 IP prefix 를 소유한 AS 번호를 알 수 있다. 다음으로 해당 IP prefix 를 담당하는 DNS 서버를 찾기 위해 DNS 역방향 질의(Reverse lookup)를 수행한다. 역방향 질의를 통하여 해당 IP prefix 에 대한 DNS 서버의 이름을 알 수 있다. 마지막으로 찾아진 DNS 서버 이름을 가지고 DNS 질의를 수행하면 DNS 서버의 IP 주소를 얻을 수 있으며, 추가적으로 해당 DNS 서버와 함께 운영되는 보조 DNS 서버들 정보까지 얻어낼 수 있다. 그림 1 은 AS 별 DNS 서버 수집 과정에서 발생하는 데이터 간의 관계를 보여준다.

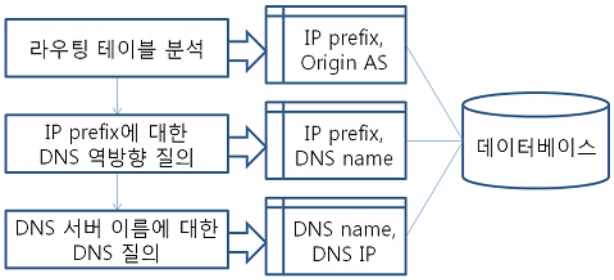

그림 1 AS 별 DNS 서버 주소 수집 과정

RouteViews 에서 가져온 2010 년 3 월 1 일 0 시의 RIB 데이터를 가져와서 분석한 결과, 현재 인터넷 상에는 33,641 개의 AS 가 있으며, IP prefix 와 AS path 쌍이 총 11,103,319 개인데, 이를 IP prefix 와 최종 목적지 AS 로만 모으면 316,873 개가 나왔다. 이는 현재 인터넷 라우터의 포워딩 테이블(Forwarding Table)의 크기가 30 여 만 개가 넘음을 알 수 있다. IP prefix 에 대하여 역방향 질의를 하였을 때 88.4%의 IP prefix 만이 응답이 오고 나머지 11.6%는 응답이 없었다. 그림 2 는 응답이 오지 않는 IP prefix 의 네트워크 주소 크기 별로 개수를 표로 나타낸 것이다. 상대적으로 네트워크 주소가 더 상세할수록 응답이 오지 않는 경우가 많음을 알 수 있다. 이는 DNS 서버를 가지지 않고 자신의 상위 AS 에 의존하는 규모가 작은 네트워크 혹은 IX 등 도메인 네임 서비스가 필요하지 않은 AS 임을 확인하였다.

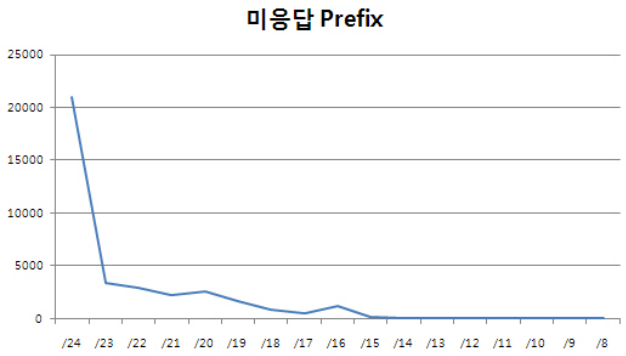

그림 2. 응답이 오지 않은 IP prefix 에 대한 네트워크 주소 크기 별 분포

다음으로 역방향 질의의 응답으로 온 DNS 서버 이름에서 중복되는 것을 제외하여 37,821 개의 DNS 서버를 알아내었다. 이 중에서 질의를 통해 32,398 개의 주 DNS 서버 정보를 얻어내었고, 각각의 주 DNS 서버와 같이 운영되는 보조 DNS 서버들을 확인할 수 있었다. AS 개수와 주 DNS 서버 개수를 비교해 보면 대부분의 AS 에 대하여 DNS 서버 정보를 얻을 수 있음을 알 수 있다. DNS 서버 정보를 얻어내지 못한 AS 들은 다른 방식으로 살아있는 정보를 얻어내야 하는데, 상대적으로 규모가 작은 네트워크이기 때문에 전통적인 스캐닝 방법으로도 가능할 수 있다.

Ⅲ. 결론

현재의 인터넷은 수많은 AS 들이 상호 연결되어 있고 이들 간의 라우팅은 BGP 를 사용한다. 그러나 BGP 라우팅은 분산 라우팅 방법이기에 목적지로의 도달성이 항상 보장되지 않는다. 본 논문에서는 인터넷 상의 모든 AS 로의 도달성을 검증하기 위하여 DNS 서버를 이용하는 방법을 제안하였다. 이를 위해 각 AS 별로 운영하는 DNS 서버를 찾는 방법과 사용되는 데이터 간의 관계를 제시하고 실제 라우팅 테이블 데이터를 분석하여 결과를 보여주었다.

향후 연구로는 DNS 서버를 가지지 않은 AS 들에 대하여 다른 살아있는 호스트를 찾아내는 방법을 고안하는 것이다. 또한 도달성 검증 과정의 성능 측정과 정확도에 대한 비교 분석도 이루어져야 할 것이다.

참 고 문 헌

[1] A Border Gateway Protocol 4 (BGP-4), http://www.ietf.org/rfc/rfc4271.txt.

[2] Chang, H., Jamin, S., Willinger, W., "Inferring AS-level Internet topology from router-level path traces," In SPIE ITCom, 2001.

[3] Hyun, Y., Broido, A., kc claffy, "Traceroute and BGP AS path incongruities," Tech. rep., CAIDA, 2003.

[4] Mao, Z.M., Rexford, J.,Wang, J., Katz, R.H., "Towards an accurate AS-level traceroute tool," In Proc. of ACM SIGCOMM, 2003.

[5] Route Views Project Page, http://www.routeviews.org/.