데이터 플로우 구별에 의한 네트워크 주소 변환

윤승용° 이광희 최창국 전우직
충 남 대 학 교 컴 퓨 터 공 학 과
{syyoon, leekh, ckchoi, chun}@ce.cnu.ac.kr

Network Address Translation By Flow Separation

Seung-Yong Yoon° Kwang-Hee Lee Chang-Kook Choi Woo-Jik Chun
Dept. of Computer Engineering, Chungnam National University

요 약

현재 인터넷이 직면하고 있는 IP 주소 부족 문제 해결을 위한 새로운 방안으로서 **데이터 플로우 구별에 의한 네트워크 주소 변환(NAT-FS : NAT by Flow Separation)** 기법을 제안하고 기술한다. 이 방식은 기존의 NAPT와 같이 단 하나의 글로벌 IP 주소에 모든 로컬 호스트가 할당되면서도 Basic NAT 방식처럼 DNS와 연동하여 Full Access 기능도 지원할 수 있다.

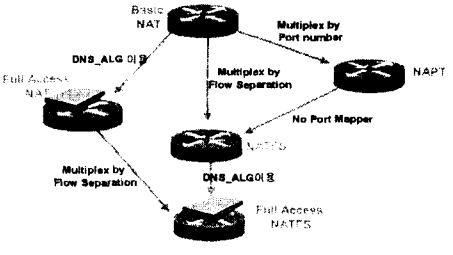
1. 서론

현재 인터넷에서 가장 심각하게 대두되고 있는 IP 주소 부족 문제 해결을 위해 제안된 NAT(Network Address Translation) 기법[1]은 로컬 네트워크내의 호스트들에게 로컬 IP 주소를 부여하고, 이들이 외부의 글로벌 네트워크와 통신할 때 글로벌 IP주소로 변환하여 통신하는 기법이다. 기존의 NAT기법은 IP 주소만을 변환하는 Basic NAT와 주소와 함께 포트번호까지 변환하는 NAPT(Network Address & Port Translation) /PAT(Port Address Translation)로 나뉘어 진다[2]. Basic NAT는 하나의 글로벌 IP 주소를 하나의 로컬 호스트에 할당하므로 IP 주소의 이용 효율이 떨어진다. 이 문제를 해결하기 위하여 NAPT는 포트번호를 서로 다르게 변환하여 단 하나의 글로벌 IP 주소에 모든 로컬 호스트를 동시에 할당하여 IP 주소 효율을 극대화 시키는 기법이다[3]. 그러나 이 방식은 로컬 호스트가 항상 통신을 시작해야하는 Client Access방식만이 가능하다. 따라서 DNS(Domain Name Server)와 연동하여[4] 글로벌이나 로컬이나 구분 없이 통신을 시작할 수 있는 Full Access방식은 현재 Basic NAT에서만 가능하다. 본 논문에서 제안하는 데이터 플로우 구별에 의한 네트워크 주소 변환 (NAT-FS : NAT by Flow Separation) 기법은 Basic NAT가 갖는 Full Access방식과 NAPT가 갖는 IP 주소 이용 효율의 극대화라는 장점을 모두 갖춘 IP 주소 부족 문제 해결을 위한 새로운 방안이다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안한 데이터 플로우 구별에 의한 네트워크 주소 변환 방법에 대해 자세히 기술하고, 3장에서는 설계 및 구현에 대해 다룬다. 4장에서는 기존의 NAT방식들과 비교하여 NAT-FS의 우수성을 검증한다. 마지막으로 5장에서 결론을 맺는다.

2. NAT-FS (NAT by Flow Separation) 기법

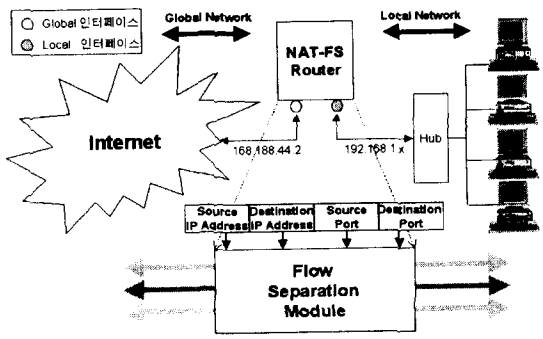
NAT-FS는 기존의 NAT방식들과 달리 데이터 플로우를 구분하여 이를 바탕으로 주소만을 변환하는 특징을 가지고 있다. 따라서 이 방식은 기존의 NAPT와 같이 단 하나의 글로벌 IP 주소에 모든 로컬 호스트가 할당되면서도 Basic NAT 방식처럼 DNS와 연동하여 Full Access 기능도 지원할 수 있다는 장점을 가지고 있다. [그림 1]은 다른 NAT기법들과의 관계를 그림으로 보여주고 있다.



[그림 1] 다른 NAT기법들과의 관계

위 그림에서 알 수 있듯이 Full Access NAT-FS 방식은 기존 NAT 방식들의 장점을 모두 가지고 있는 가장 진화된 형태

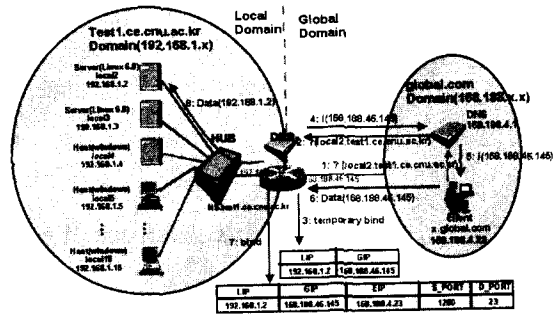
의 NAT 기법이라고 할 수 있다.



[그림 2] 데이터 플로우 구분에 의한 네트워크 주소 변환

[그림 2]는 데이터 플로우 구분에 의한 네트워크 주소 변환에 대한 기본적인 동작 과정을 나타낸 그림이다. 위 그림에서 로컬 네트워크와 인터넷은 데이터 플로우 구분에 의한 네트워크 주소 변환 기능을 가진 라우터(NAT-FS)에 의해 연결되어 있다. 로컬 네트워크의 한 호스트가 인터넷의 호스트와 통신하려면 로컬 네트워크의 호스트에 부여되어 있는 로컬 IP 주소(RFC 1918)를 인터넷에서 사용 가능한 글로벌 IP로 변환해야 한다. NAT-FS 기법에서는 NAPT와 같이 단 하나의 글로벌 IP 주소에 모든 로컬 호스트를 할당하나 각각의 데이터 플로우는 <발신지 주소, 목적지 주소, 발신지 포트번호, 목적지 포트번호>로 구분한다. 그러나 NAPT 방식과 달리 포트번호를 변환하지는 않는다. 즉, NAT-FS 라우터는 로컬 네트워크에서 인터넷으로 가는 모든 Outgoing 데이터 플로우의 <발신지 주소, 목적지 주소, 발신지 포트번호, 목적지 포트번호>를 변환 테이블에 기록하고 패킷의 로컬 발신지 IP 주소를 글로벌 IP 주소로 변환한다. Incoming시에는 <발신지 주소, 목적지 주소, 발신지 포트번호, 목적지 포트번호>로 변환 테이블을 검색하여 패킷의 글로벌 목적지 IP 주소를 로컬 IP로 변환한다. 이때 인터넷으로부터 로컬 네트워크로 들어오는 Incoming 패킷은 목적지 IP 주소(Outgoing시 변환되었던 글로벌 IP 주소)가 같은 경우에도 그 패킷이 속한 데이터 흐름, 즉 Outgoing시 기록해 둔 <발신지 주소, 목적지 주소, 발신지 포트번호, 목적지 포트번호>에 의해 구분된다. 이런 방식으로 NAT-FS는 Basic NAT기법과 같이 IP 주소만을 변환하면서도 NAPT에서와 같이 단 하나의 글로벌 IP 주소에 모든 로컬 호스트를 할당하여 IP 주소 이용 효율을 극대화시킬 수 있다.

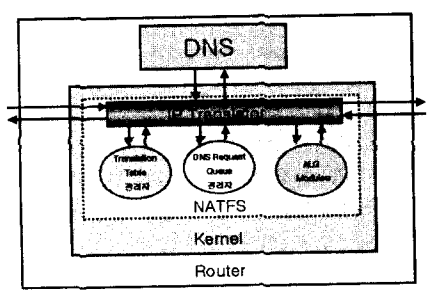
또한 NAT-FS 기법은 DNS 기술을 접목시켜 NAPT에서 불가능한 양방향 주소변환 기능을 구현할 수 있다. [그림 3]은 NAT-FS 기술에 DNS 기술을 접목시켜 Full Access의 네트워크 주소 변환기능을 가진 라우터를 나타낸 그림이다. 그림에서는 글로벌 네트워크의 사용자(168.188.4.23)가 로컬 네트워크의 서버로 어떤 서비스를 요청할 때 일어나는 과정을 보여주고 있



[그림 3] DNS 기술을 적용한 양방향의 NAT-FS

다. 사용자는 서버의 도메인 주소만을 알고 있고 이를 이용해 서버에 서비스를 요청한다(1). 서버와 통신하기 위해 서버의 IP 주소를 알아야 하므로 지정된 DNS(168.188.4.1)에게 질의를 하고 이 질의는 NAT-FS의 DNS에 도착된다(2). NAT-FS의 DNS는 앞으로 자신에게 도착할 데이터 패킷의 주소 변환을 위해 글로벌 IP(168.188.46.145)를 할당하고 DNS Request Queue에 임시적으로 엔트리를 생성한 후, 글로벌 IP 주소를 DNS에게 알려준다((3), (4)). 글로벌 호스트는 DNS에 의해 서버의 IP 주소를 알고 나서 데이터를 전송한다((5), (6)). 이때 NAT-FS에 처음 도착한 패킷의 발신지 주소(168.188.4.23), 발신지 포트번호(1200), 목적지 포트번호(23) 정보를 이용하여 변환 테이블 엔트리의 EIP, S_PORT, D_PORT 필드를 채워 완전한 변환 테이블 엔트리를 생성한다(7). 그 후, 패킷의 글로벌 목적지 주소(168.188.46.145)가 로컬 IP 주소(192.168.1.2)로 변환되어 전달된다(8).

3. NAT-FS 의 설계 및 구현



[그림 4] NAT-FS의 기본 구조

[그림 4]는 NAT-FS의 기본 구조를 나타낸다. IP Translator는 로컬 네트워크에서 글로벌 네트워크로 또는 글로벌 네트워크에서 로컬 네트워크로 데이터를 전송할 때, IP 패킷의 발신지 주소 또는 목적지 주소를 변환한다. 로컬 네트워크에서 글로벌 네트워크로는 일반적인 DNS처리 루틴을 따르며 글로벌

네트워크에서 로컬 네트워크로는 DNS Request Queue관리자와 연동 DNS_ALG(Application Level Gateway)처럼 작동하여 Full Access를 지원한다. Translation Table 관리자는 IP 주소 바인딩 정보를 관리하여 로컬 네트워크에서 글로벌 네트워크로 또는 글로벌 네크워크에서 로컬 네트워크로 Access할 수 있도록 한다. DNS Request Queue 관리자는 DNS와 연동하여 외부에서 DNS 질의시 임시적 바인딩 정보를 유지하여 Full Access를 지원한다. ALG Modules는 페이로드 부분에 IP 주소 정보를 담아가거나 컨트롤과 데이터 세션이 상호 의존적인 프로토콜등을 위한 모듈로서 다양한 서비스 지원을 위한 것이다. [그림 5]는 Translation Table 관리자, [그림 6]은 DNS Request Queue 관리자를 위해 구현된 기본적인 구조체 내용이다.

```
struct ip_trans{
        __u32 lip, gip, eip;
        __u16 dport;
        short sport_cnt;
        struct sport_list *sport_head;
        struct timer_list timer;
        struct ip_trans *link;
};
struct sport_list{
        __u16 sport;
        struct sport_list *link;
};
```

[그림 5] Translation Table 엔트리 구조체

```
struct dns_request_list{
        __u32 lip, gip;
        struct timer_list timer;
        struct dns_request_list *next;
};
```

[그림 6] DNS Request Queue 엔트리 구조체

IP 패킷의 발신지 포트는 프로토콜 또는 서비스 종류에 따라 커넥션 동안에 동적으로 변화하므로 Linked-List로 관리되는데 sport_cnt로 List의 수를 기록해 놓고 일정한 수 이상이 되면 LRU(Least Recently Used) 알고리즘에 의해 새롭게 사용된 발신지 포트로 계속해서 수정해 나간다. 그리고 Expiration Timer를 두어 일정 시간 동안 데이터 전송이 없으면 변환 테이블에서 엔트리를 삭제한다. 변환 테이블 엔트리 검색 시 보다 빠른 검색을 위하여 해싱을 이용하는데, ip_trans구조체의 link 포인터는 eip로 해싱해서 나온 값으로 해당 테이블을 찾기 위해 사용되는 링크로 해싱값이 같은 다음 테이블을 가리킨다.

4. 기존 네트워크 주소 변환 기법과의 특성 비교

NAT-FS는 데이터 플로우 구별에 의한 IP 주소만 변환함으로서 포트 계층에 민감한 다양한 서비스들을 지원하며, 모든 로컬 호스트들을 위해 단 하나의 글로벌 IP 주소만 필요하므로 IP 주소 이용률이 매우 높다. 또한 DNS 기술과 접목하여 Full Access의 네트워크 주소 변환 기능을 제공할 수 있다. [표 1]은 이러한 장점들을 기존의 NAT 기법들과 비교하여 보여주고 있다.

	Basic NAT	NAPT	NAT-FS
Flow 구별	목적지 주소	TCP/UDP 계층의 포트	**발신지 주소, 목적지 주소, 발신지 포트, 목적지 포트**
서비스 지원도	좋다	나쁘다	**좋다**
IP 주소 이용률	낮다	높다	**높다**
Full Access 지원	지원 가능	지원 불가능	**지원 가능**

[표 1] 기존 NAT 기법과의 특성 비교

5. 결론

본 논문에서 제안한 NAT-FS(NAT by Flow Separation) 기법은 <발신지 주소, 목적지 주소, 발신지 포트, 목적지 포트>를 이용하여 데이터 플로우를 구별하고 포트가 아닌 주소만 변환함으로서 다양한 서비스를 지원할 수 있었다. 또한 단 하나의 글로벌 IP 주소를 모든 로컬 호스트에 할당함으로서 IP 사용률을 극대화 시켰으며 DNS 기술과 접목하여 Full Access 기능도 지원할 수 있었다. 이런 NAT-FS의 장점들은 Home/SOHO Network, Regional Network 구축에 활용될 수 있을 것이다.

6. 참조문헌

[1] P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663, August 1999

[2] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", Internet Draft <draft-ietf-nat-traditional-04.txt>, April 2000

[3] Michael Hasenstein, "IP Address Translation", http://www.csn.tuchemnitz.de/HyperNews/get/linux-ip-nat.html, 1997

[4] P. Srisuresh, G. Tsirtsis, P. Akkiraju, A. Heffernan, "DNS extensions to Network Address Translators (DNS_ALG)", RFC2663, September 1999

[5] 전우직, "발신지 주소를 이용한 네트워크 주소 변환 방법", 특허 출원중, August 1999