Virtual Group 네트워크 서비스 제공을 위한 IP 주소 변환 시스템 개발

최 진 영† · 이 승 표†

요 약

본 고에서는 Virtual Group 네트워크 서비스 제공을 위한 IP 주소 변환 시스템의 개발과 이를 초고속 시범 서비스에 적용한 예에 관하여 다루었다. 이러한 방법은 전용 망에 접속된 지역 망 내의 제한된 가상 그룹에 대해 별도의 전용 네트워크 서비스를 제공할 수 있는 방안이 될 수 있으며, 향후 관심이 부각되고 있는 인트라넷 환경에서 폐쇄 그룹 내부에서의 모든 업무를 인터넷 관련 기술로 처리하는 새로운 개념의 네트워크 환경을 제공하는데 이용될 수 있다.

Development of IP address translator for Virtual Group network service

Jin Young Choi† · Seung Pyo Lee†

ABSTRACT

In this paper, we present a development of IP address translator for virtual group network service and an application to Korea Information Infrastructure Pilot projects in Daeduk science town network. This method can be a way to provide network service for limited virtual groups which are connected to a specialized network. Also this can be used to provide a new network environment for closed user groups in Intranet applications.

1. 개 요

기존의 그룹웨어 서비스와 함께 최근 인터넷이 활성화되면서, 인터넷의 웹 기술을 이용하여 기업 업무에 활용하는 인트라넷 서비스가 새롭게 나타나고 있다. 인트라넷이란 기업체, 연구소 등 조직 내부의 모든 업무를 인터넷 관련 기술로 처리하는 새로운 개념의 네트워크 환경을 말한다. 따라서, 인트라넷은 TCP/IP를 지원하는 LAN 환경에서 구축될 수 있으며, 인터넷과 동일한 브라우저 상에서 그룹 웨어 개념의 업무들을 처리할 수 있게 된다. 이것은 LAN 환경의 인터넷이라고 할 수 있으며, 이를 통해 조직은 전자 메일 시스템, 전자 결재 시스템 등 각각 별도 시스템을 통해 주고 받던 다양한 형태의 정보를 인터넷의 웹 환경으로 통합하여 업무의 효율성을 기할 수 있다.

또한, 인터넷과 같은 공중망 및 별도의 전용망을 통하여 인트라넷 환경을 구축하고, 각 기업의 요구에 따라 인트라넷 서비스를 대행하는 가상 인트라넷 서비스도 생겨났다. 가상 인트라넷 서비스 제공자는 기업 업무에 필요한 기본적인 서비스 기능을 제공함은 물론이고, 각 기업에게 신뢰성 있는 서비스를 제공하기 위하여 백본 망의 고품질 및 고 신뢰도와 기업 내부 정보의 보호 등을 확실하게 보증할 수 있어야 하며, 이를 위해

† 정 회 원 : 한국전자통신연구원 선임연구원
논문접수 : 1997년 10월 21일, 심사완료 : 1998년 3월 19일

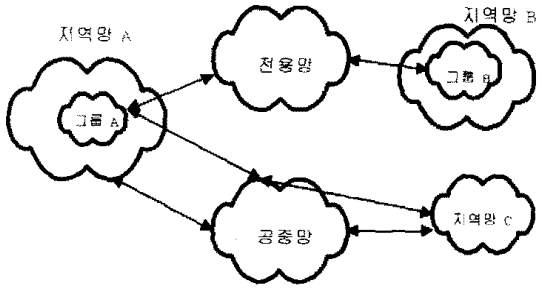
인트라넷 환경에서는 기업 내부의 자원을 보호하기 위하여 일반적으로 방화벽을 설치하고 있다. 그러나, 인터넷 백본 상에서 제한된 사용자들만이 가상적인 네트워크를 형성하여 기업의 그룹웨어 서비스를 구축하는 가상 인트라넷 서비스에서는 네트워크 차원의 방화벽 기능만으로는 불충분하며, 응용 서비스 차원에서 보다 안전하고 유용한 보안 기능이 요구된다.

본 고에서는 이러한 폐쇄된 사용자들에 대해 제한된 네트워크 서비스를 제공하기 위하여 적용될 수 있는 IP 주소 변환을 이용한 서비스 제공 방안에 관하여 기술하고자 한다. 2절에서는 각 단위 지역 망 내에서 특정 네트워크 백본 망을 이용한 제한된 네트워크 서비스를 요구하는 그룹에 대한 서비스 제공 방안을 제안하고, 3절에서는 이를 위해 필요한 IP 변환 시스템의 구현에 관하여 논한다. 4절에서는 제안된 IP 주소 변환 시스템이 초고속 시범망에서의 시범 가입자를 위한 시범 서비스 제공을 위해 적용된 사례에 관하여 기술한다.

2. Virtual Group 네트워크 서비스 제공 방안

2.1 Virtual Group 네트워크 서비스

인터넷 기술이 활성화 되면서 기존의 그룹웨어 서비스를 인터넷의 웹 환경으로 통합하여 업무의 효율성을 기하고자 하는 노력들이 지속적으로 이루어지고 있으며, 이를 위해 인터넷과 같은 공중망 및 별도의 전용망을 통하여 인트라넷 환경을 구축하고, 사용자에게 제한된 네트워크 서비스를 제공해야 하는 요구가 발생하였다. 그러나, 각 단위 지역 망 내에서의 특정 그룹만이 어느 특정한 네트워크를 전용해야 하는 요구 사항은 지금까지의 단순한 라우팅만으로는 불충분하며, 추가의 처리 기술이 필요하다.

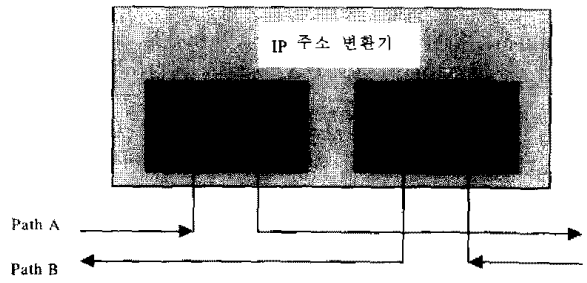


(그림 1) Virtual Group 네트워크 서비스
(Fig. 1) Virtual Group Network Service

(그림 1)은 Virtual Group 네트워크 서비스의 개념을 나타낸다. 그림에서와 같이 특정 그룹에 속한 사용자 간의 통신은 별도의 전용망을 통해서 이루어지며, 이 전용 네트워크는 그 이외의 사용자에게는 폐쇄되어 있다. 즉, 지역망 A의 그룹 A에 속하는 사용자들은 전용망을 이용하여 지역망 B의 그룹 B 사용자들과 통신을 하는 것이 필요하며, 이 그룹 이외의 사용자들은 기존의 공중망을 이용하여 각 그룹 또는 그 외의 사용자들과 통신하게 된다. 물론, 그룹에 속한 사용자가 일반 사용자와 통신을 하기 위해서는 기존의 공중망을 이용하게 된다. 본 고에서는 이를 Virtual Group 네트워크 서비스라 정의하고, 이러한 서비스를 제공하기 위한 방안을 제안하고자 한다.

2.2 Virtual Group 네트워크 서비스 제공 방안

본 절에서는 앞에서 언급한 Virtual Group 네트워크 서비스 요구 사항을 만족시키도록 구현된 IP 변환 시스템에 관하여 기술하고자 한다. 제안된 방식에서는 Virtual Group에 속한 가입자들에게 전용망에 속한 IP 주소를 가상으로 부여하고, Virtual Group 간의 통신 시에 이 가상 주소를 이용하도록 하였다. 따라서 Virtual Group에 속한 각 사용자는 고유의 주소와 함께 임의로 할당된 주소를 동시에 갖는다. 물론 각 지역망의 게이트웨이 라우터에는 전용망의 도메인 주소가 등록되어 있어야 한다. IP 변환 시스템이 IP 패킷을 수신하면 목적지 주소가 Virtual Group에 속한 주소인가를 확인하여 주소 변환 여부를 결정한다. 또한 소스 주소는 가상의 할당된 IP 주소로 변환된다. 실제로 본 고에서 제안된 IP 주소 변환기는 초고속 시범망에서 제한된 시범 가입자에게 초고속 시범망을 통한 전용 네트워크 서비스를 제공하는데 이용되었다.



(그림 2) IP 주소 변환기의 소프트웨어 개념적 구조
(Fig. 2) Conceptual structure of IP address translator software

지금까지 제안되었던 지역 망과 외부 망간의 접속 서비스 제공을 위한 방법으로는 한 지역 망 내에서 외부와 직접 접속이 가능한 노드를 몇 개로 제한한 경우 원격 소켓의 관리를 통해 외부 망으로의 중계를 제공하는 소켓를 이용하는 방안과 더불어, 가장 단순한 방법으로 프록시 서버를 통하여 외부로의 접속을 제공하는 방안, 지역 망에서 전역 망으로의 접속을 허용하기 위해 망 주소 변환기(Network Address Translator)를 이용하는 방안 등이 있다.[1][2][3][4]

3. IP 주소 변환 시스템의 구현

3.1 IP 주소 변환 시스템의 개념적 구조

IP 주소 변환 시스템의 기능은 Unix 워크스테이션에서 구현되었으며, 전체적인 소프트웨어 개념적 구조는 (그림 2)와 같다. 2개의 path A, B에 대하여 각각 대응되는 프로세스가 수행된다. 즉 하나의 프로세스는 Virtual Group에서 전용망으로의 트래픽에 대하여 IP 주소를 변환하며, 다른 하나는 전용망에서 Virtual Group으로의 트래픽에 대하여 IP 주소를 변환한다. 이러한 IP 변환 시스템의 세부적인 기능은 다음과 같다.

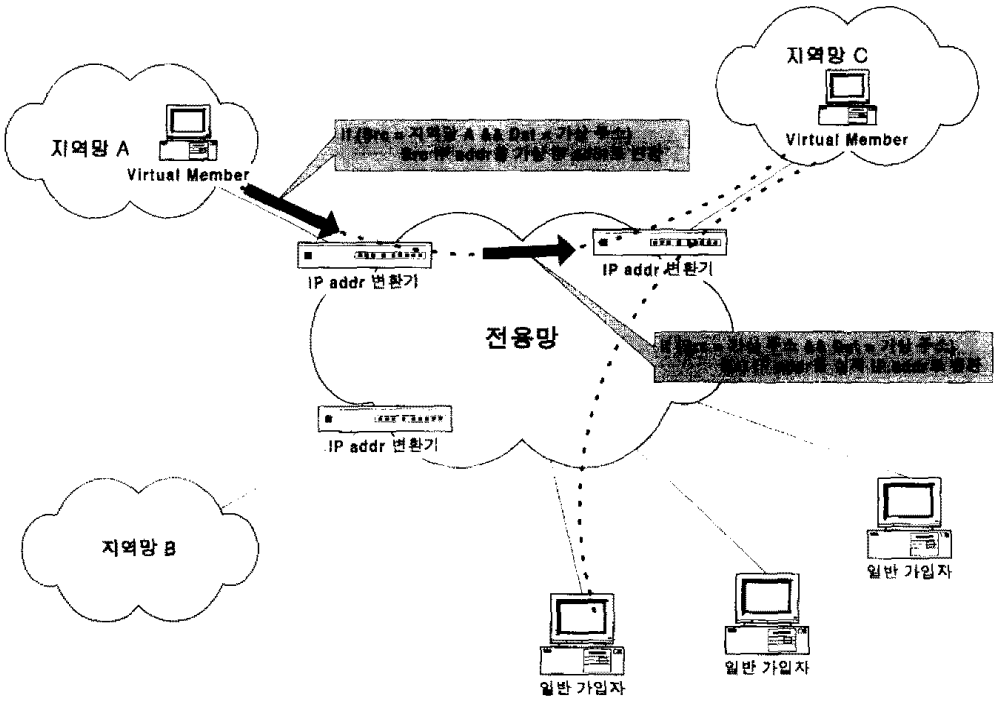
- IP 패킷 소스 주소를 대응하는 가상의 전용망 IP 주소로 변환
- 전용망에 속하는 가상의 IP 패킷 목적지 주소를 원래의 목적지 주소로 변환
- IP 헤더 Checksum 재 계산
- TCP Checksum 재 계산
- UDP Checksum 재 계산

여기서 IP 헤더, TCP와 UDP Checksum 등은 전용망을 이용한 트래픽에 대한 분석 자료로 이용될 수 있다.[6]

3.2 IP 주소 변환 방식

(그림 3)은 복수 개의 IP 망이 하나의 전용망에 접속되어 있고, 접속된 IP 망들의 호스트 중 특정한 호스트 들만이 전용망을 통한 통신을 가능하게 하는 IP 변환 시스템의 주소 변환 방식을 나타낸다. 그림에서는 각 IP 망과 전용망 사이에 IP 변환 시스템이 필요한 것처럼 나타나 있으나, 그림처럼 각각 별도의 시스템으로 구현될 수도 있고, 하나의 시스템에 모두 구현될 수도 있다.[5][7]

(그림 3)에서 전용망에 접속된 지역 망에 속한 호스



(그림 3) IP 주소 변환 방식
(Fig. 3) IP address translation scheme

트에서 전용망으로 전송되는 트래픽에 대해서는 목적지가 전용망에 접속된 다른 지역 망의 Virtual Group에 속하는 호스트인가 또는 전용망에 직접 접속된 호스트인가에 관계 없이, 소스 주소가 접속된 지역 망의 도메인에 속하고 목적지 주소가 전용망 도메인에 속하면, 소스 주소가 그에 대응하는 가상의 주소로 변환된다. 또한, 전용망에서부터 접속된 지역 망으로 향하는 트래픽에 대하여는 소스가 전용망에 직접 접속된 호스트인가 또는 어떤 지역 망의 Virtual Group에 속하는 호스트인가에 관계 없이 소스 및 목적지 주소가 모두 전용망 도메인에 속하면 목적지 주소가 그에 대응하는 원래의 주소로 변환된다. 위의 조건에 해당되지 않는 모든 패킷은 폐기된다.

4. 초고속 시범 서비스에의 적용

본 절에서는 이러한 IP 주소 변환 시스템을 초고속 시범 망에서의 시범 서비스 제공을 위해 적용한 예에 관하여 기술하고자 한다.

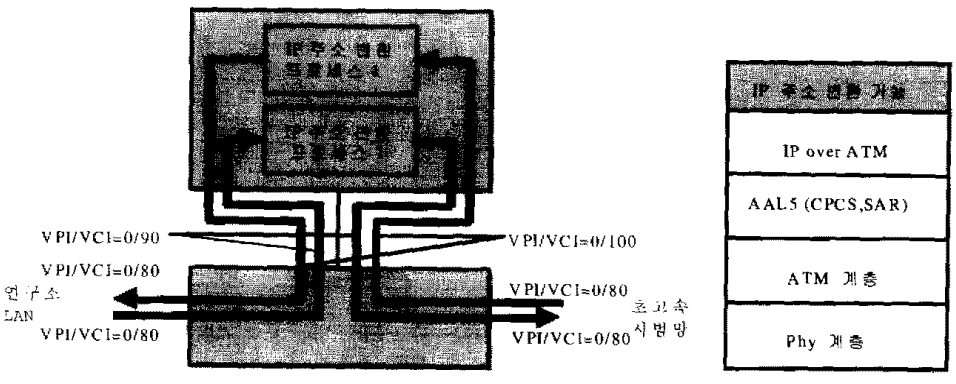
4.1 초고속 시범 서비스 가입자 수용에 대한 요구 사항

현재 초고속 시범 서비스는 대전 광역시 둔산 전화국에 설치된 ATM MSS(MAN Switching System) 교환기를 중심으로 약 300 가입자 정도의 규모로 운영되고 있다. 제공되는 서비스는 IP over ATM을 약간 변형한 형태의 서비스를 제공하고 있다. 초고속 시범 망은 비연결형 서비스만을 제공할 수 있도록 구성되어 있으며, 이를 위하여 connectionless 서버와 유사한 기능을 갖는 IP 서버를 두고 있다. 시범 가입자는 크게 연구소 가입자와 일반 가입자로 구성되며, 조선 일보, 하이텔 PC 통신 등의 정보 제공자들로부터의 서비스를 이용할 수 있다. 그러나, 연구소 가입자는 연구소 내의 특정한 호스트들을 선정하여 이들 호스트(연구소 내의 Virtual Group)만이 초고속 시범망을 통하여 정보 제공자의 서버 또는 초고속 시범망에 연결된 다른 연구소의 호스트에 접속할 수 있도록 해야 하는 요구 사항을 가지고 있었다.

이와 같은 요구 사항을 충족시키기 위해서는 연구소 내에서 초고속 시범망에 연결된 서버로 향하는 IP 패킷에 대한 라우팅을 그 패킷의 소스 주소가 시범망 가입자인 경우와 아닌 경우로 분리하여 처리해야 하며, 또한 서비스 제공자들의 LAN에서도 연구소로 향하는 패킷인 경우에는 목적지 주소가 시범망의 가입자인 경우와 아닌 경우로 분리하여 처리해야 한다. 그러나, 기본적으로 인터넷의 라우터들은 목적지 주소에 의해 IP 패킷을 라우팅하므로 연구소 LAN에서 소스 주소에 따라 라우팅 경로를 결정한다는 것은 불가능하다.

4.2 IP 주소 변환기를 이용한 Virtual Group 네트워크 서비스

초고속 시범 서비스에서는 앞에서 언급한 요구 사항을 해결하기 위해서 본 고에서 제안된 IP 주소 변환 시스템을 적용하였다. IP 주소 변환 시스템은 연구소 게이트웨이 라우터와 초고속 망 사이에 위치한다. 제안된 방식에서는 연구소 내 시범 가입자들 및 초고속 시범망에 연결된 정보 제공자들에게 초고속 시범망 도메인에 속한 IP 주소를 가상으로 부여하고, 연구소 가입자가 서비스 제공 서버에 접근할 때는 그 서버에 가상으로



(그림 4) IP 주소 변환 시스템의 구성과 프로토콜 구조
(Fig. 4) Structure of IP address translator and Protocol stack

부여된 IP 주소를 이용하여 접근하도록 하였다. 이때 물론 연구소 게이트웨이 라우터의 라우팅 테이블에 초고속 망 도메인 주소가 등록되어 있어야 한다. IP 주소 변환 시스템은 IP 패킷을 연구소 LAN으로부터 수신하면 목적지 주소가 가상 주소인가를 조사하여 가상 주소이면 원래 그 서버에 할당된 인터넷 주소로 변환하고, 가상 주소가 아니면 변환하지 않는다. 소스 주소는 연구소 LAN 도메인에 속한 원래의 IP 주소에서 가상 IP 주소로 변환된다. 정보 제공 서버에서 연구소 가입자 호스트로 향하는 IP 패킷도 연구소에서 정보 제공 서버로 향하는 패킷과 마찬가지로 처리한다. (그림 4)는 구현된 IP 주소 변환 시스템의 구성과 프로토콜 구조를 나타낸다. 그림에서처럼 연구소 LAN에서 ATM 스위치, IP 주소 변환 시스템, 초고속 시범 망 사이에는 VPI/VCI=0/80, VPI/VCI=0/90, VPI/VCI=0/100, VPI/VCI=0/80의 PVC가 설정되어 있으며, 이러한 IP 주소 변환 시스템은 물리 계층, ATM 계층, AAL5 계층 위에 IP over ATM상의 IP 주소 변환 기능이 구현되어 있다.

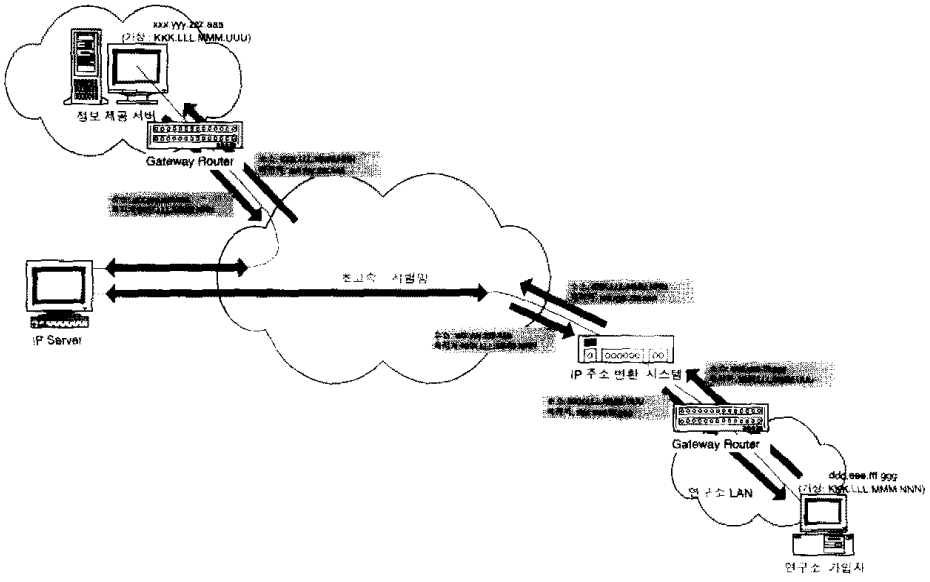
IP 주소 변환 시스템을 이용한 IP 패킷의 흐름을 (그림5)에 나타내었다. 그림에서 IP 주소 ddd.eee.fff.ggg를 갖는 연구소 가입자는 초고속 망에 속하는 IP 주소 KKK.LLL.MMM.NNN을 가상으로 부여받고, IP 주소 xxx.yyy.zzz.aaa인 정보 제공 서버는 초고속 망에 속하는 IP 주소 KKK.LLL.MMM.UUU를 가상으로 부여 받았다고 가정해 보자. 이때 연구소 가입자와 정보 제공 서버 간의 패킷 전송 절차는 다음과 같다.

① 연구소 가입자가 초고속 망을 통하여 정보 제공 서버에 접근하고자 할 때는 정보 제공 서버에 가상으로 부여된 주소 KKK.LLL.MMM.UUU를 이용하여 접속한다. 따라서 연구소 가입자에서 정보 제공 서버로 향하는 패킷은 소스 주소는 ddd.eee.fff.ggg이고, 목적지 주소는 KKK.LLL.MMM.UUU가 된다.

② 연구소 게이트웨이 라우터의 라우팅 테이블에는 KKK.LLL.MMM.0 네트워크에 대하여 초고속 망으로 라우팅 되도록 사전에 설정되어 있으므로 이 패킷은 초고속 망으로 라우팅되게 된다.

③ 위와 같은 소스 및 목적지 주소를 갖는 IP 패킷을 IP 주소 변환 시스템이 수신하면, 소스 주소를 그에 대응하는 가상의 주소로 변환한다. 목적지 주소는 가상으로 부여된 주소에서 그에 대응하는 원래의 주소로 변환된다.

④ IP 패킷을 수신한 IP 서버는 그 패킷의 목적지 주소에 따라 그에 대응하는 가상 채널로 그 패킷을 전송한다.



(그림 5) IP 주소 변환 시스템을 이용할 때 IP 패킷의 주소 변환 과정
(Fig. 5) IP address translation process

⑤ 위와 같은 패킷을 전달 받은 정보 제공 서버는 소스 주소를 원래의 주소인 xxx.yyy.zzz.aaa로, 목적지 주소는 수신한 패킷의 소스 주소 KKK.LLL.MMM.NNN으로 하여 응답 패킷을 초고속 망으로 전송한다.

⑥ 다시 와 같은 패킷을 수신한 IP 서버는 목적지 주소 KKK.LLL.MMM.NNN에 대하여 연구소 측으로 전송하도록 사전에 설정되어 있으므로 연구소 측으로 전송한다.

⑦ 초고속 망으로부터 IP 패킷을 전달 받은 IP 주소 변환 시스템은 '의 절차와 같이 소스 주소는 가상 주소로 변환하고, 목적지 주소는 원래 주소로 변환한다.

⑧ 연구소 LAN 내부에서는 목적지 주소에 따라 라우팅 되어 (그림5)의 연구소 가입자에게 전달되게 된다.

이러한 과정에서 IP 서버는 일종의 connectionless 서버로서 (IP 주소, PVC id) 테이블에 따라 IP 패킷을 수신하면, IP 패킷의 목적지 IP 주소와 대응하는 PVC id를 테이블에서 찾아 그 PVC로 IP 패킷을 전송하는 역할을 한다. 이와 같은 방식은 각 호스트에서 IP 서버로 하나의 PVC만을 설정하면 되므로 호스트들(라우터 포함) 사이를 Full mesh로 연결하는 것보다 PVC 수를 줄일 수 있다는 장점이 있다. 또한 IP 서버는 등록된 IP 주소에 따라 IP 패킷의 목적지 주소에 대한 PVC를 찾아 IP 패킷을 전송하므로 등록되지 않은 호스트로 향하는 IP 패킷은 처리되지 않는다. 그러나, IP 변환 시스템은 IP 서버의 유무에 관계 없이 이용될 수 있다.

5. 맺음말

지금까지 Virtual Group 네트워크 서비스 제공을 위한 IP 변역 시스템의 개발과 이를 초고속 시범 서비스에 적용한 예에 관하여 기술하였다. 이러한 방법은 제한된 가상의 그룹에 대해 별도의 전용 네트워크 서비스를 제공할 수 있는 방안이 될 수 있으며, 향후 관심이 부각되고 있는 인트라넷 환경에서 폐쇄 그룹 내부에서의 모든 업무를 인터넷 관련 기술로 처리하는 새로운 개념의 네트워크 환경을 제공하는데 이용될 수 있다.

그러나, 이러한 방식에서는 IP 주소를 이용하는 어플리케이션은 이용하지 못할 수도 있으며, 초고속 망의 관점에서 기관 가입자의 호스트는 원래의 ID가 숨겨져 있어 문제 발생시 추적을 어렵게 할 수도 있다. 또한, 만일 전용망이 인터넷과 연결된다면, 전용망에 연결된 IP 망의 특정한 호스트들 만이 전용망을 통하여 인터넷 상의 호스트들과 통신 할 수 있도록 해야 하는 방안이 추가로 필요하게 된다. 이러한 문제는 목적지 주소가 전용망에 접속된 IP 망의 특정한 호스트가 아니라 인터넷 상의 임의의 호스트일 수도 있기 때문에 IP 변환 시스템만으로는 해결이 불가능하다. 가장 간단한 해결 방안은 전용망 내에 프록시 서버를 두는 것이다. 또 다른 해결 방안은 다소 복잡하기는 하지만 인터넷의 특정한 경로로 IP 패킷을 라우팅하기 위하여 사용되는 터널링 기법을 이용할 수도 있다. 그 외에도 소스 라우팅을 이용하는 방식 등 여러 가지 대안이 가능하지만, 각각의 효율성 등 더 많은 검토가 요구된다.

참 고 문 헌

[1] K. egavang and P. Francis. The ip network address translator(NAT). RFC1631. May. 1994.

[2] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless inter-domain routing(CIRD) : An address assignment and aggregation strategy. RFC1519, Sep. 1993.

[3] D. Koblas and M.R. Koblas. SOCKS. In USENIX security symposium proceedings III, Sep. 1992.

[4] I. H. Kim and H. Y. Yeom. 투명한 포트-주소 변환기를 통한 IP 주소의 재사용. 한국통신학회논문지. Vol.20, No.12. pp.3277-3287. 1995.

[5] Y. Rekhter and B. Moskowitz. Address allocation for private internets. RFC1597. Mar. 1994.

[6] Transmission Control Protocol. RFC793, Sep. 1981.

[7] P.F. Tsuchiya and Tony Eng. Extending the ip internet through address reuse. ACM Computer Communication Review. Jan. 1993.

최 진 영

1991년 한양대학교 산업공학과 (학사)
1993년 한국과학기술원 산업공학과(석사)
1993년 2월 ~ 현재 한국전자통신연구원 선임연구원
관심분야 : B-ISDN, 프로토콜 적합성 시험, 인트라넷, Network Management

이 승 표

1983년 인하대학교 전자공학과 (학사)
1986년 인하대학교 전자계산학과(석사)
1986년 ~ 현재 한국전자통신연구원 선임연구원
관심분야 : Internet over ATM, LAN Switching, Network Management System