碩士學位論文

터널링에 기반한 IPv6의 구축과 트래픽 모니터링

指導敎授 宋旺暾

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

濟州大學校 産業大學院

電子電氣工學科

梁德性

2005년 6월

터널링에 기반한 IPv6의 구축과 트래픽 모니터링

指導敎授 宋旺暾

이 論文을 工學 碩士學位 論文으로 提出함

2005年 6月 日

濟州大學校 産業大學院

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

電子電氣工學科

컴퓨터工學專攻

梁德性

梁德性의 工學 碩士學位 論文을 認准함

2005年 6月 日

審査委員長 安 基 中 印

審 査 委 員 金 壯 亨 印

審 査 委 員 宋 旺 暾 印

목 차

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

[표 차례]

[그림 차례]

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Deployment IPv6 based on Tunneling and traffic monitoring

Duk-Sung Yang

Department of Electrical and Electronic Engineering
Graduate School of Industry
Cheju National University

Supervised by Professor Wang-Cheol Song

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

ABSTRACT

With current IPv6 activities It is needed to study IPv6 address architecture in the viewpoint of the end user. It should be deployed before IPv6 is commonly used. Currently in order to deploy IPv6 architecture in the existing network, IPv4/IPv6 tunneling is commonly deployed and used as the testbed for IPv6 for the end user. In this thesis, the IPv4/Ipv6 tunneling is considered to deploy the IPv6 network in the Internet. And, in the tunneled network various network architecture is considered to monitor and analyze the IPv6 traffic. The considered tunneling mechanism are ISATAP, 6to4, Teredo and Wireless IPv6. And, the tunneled network is deployed in the real network such as campus network, ADSL, and so on.

Ⅰ. 서론

1994년부터 IP부족 문제 등으로 하여 시작되었던 IPv6주소체계의 연구성과는 이제 실용화의 단계로 접어들었다.[1] 하지만 IPv6망은 즉각적으로 모든 네트워크에 반영되지 못하며, IPv4망과 일정기간 혼재되어 사용되어야 한다. 기존의 IPv4망과 IPv6망의 연동을 터널링을 통하여 해결하고자 하는 시도는 이러한 상황을 반영한다. [2][3] Sisco, Juniper, Microsoft 등도 자체 개발 장비나 소프트웨어에 IPv4체계와 IPv6주소체계를 혼용하고 있는 추세이다. [4][5][6] 한편 이를 반영하듯 IPv6 주소 기반에서의 실험들은 다수 나오고 있으나, 일상화된 인터넷기반을 통한 Enduser 차원에서의 각종의 프로토콜 아래에서의 실제적인 실험과 분석은 그리 많지 않은 듯하다. 본 논문은 그러한 점에 착안하여 인터넷 기반에서 IPv4/IPv6 터널링 망을 실제로 구축하고 Enduser가 일상적으로 흔히 사용하고 있는 응용계층에서의 패킷흐름을 분석하여 보고자 한다. 이러한 시도는 IPv4/IPv6주소체계를 혼용한 장비들의 점차적인 보급 확대에 맞추어 IPv6주소체계로의 접근에 대한 기초 자료로 활용하는 데에도 의미가 있다 할 것이다. 그러한 맥락에서 본 논문은 2장에서 IPv6 터널에 관련한 연구를 진행하고, 3장에서 실제적인 터널을 구축한다. 이어 4장에서 여러 환경에 따른 IPv4/IPv6 터널 기반의 트래픽을 모니터링하고 5장에서 결론을 맺고자 한다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Ⅱ. 관련 연구

1. IPv6의 개요

1) IPv6의 개요

IPv6는 1996년에 IETF (Internet Engineering Task Force)에 의해서 표준화된 차세대 주소체계이다.[7] IPv6의 등장은 128비트 주소길이를 사용함으로써 주소 고갈 문제를 근본적으로 해결하게 되는 한편, 보안강화, 라우팅 효율성문제, QoS(Quality of Service)보장, 무선 인터넷 지원 등의 다양한 기능을 제공할 수 있을 것으로 기대되고 있다.(Table. 1참조)

제주대학교 중앙도서관 JEJU NATIONAL UNIVERSITY LIBRARY

구분	IPv4	IPv6
주소길이	32비트	128비트
표시방법	8비트씩 4부분으로 10진수로 표시 ex) 203.24.78.63	16비트씩 8부분으로 16진수로 표시 ex)2001:0230:abod:ffff:oooo:oooo:ffff:1111
주소개수	약 43억개	약 43억 X 43억 X 43억 X 43억 (거의 무한대)
주소할당	A,B,C,D 등 class 단위의 비 순차적 할당(비효율적)	네트워크 규모 및 단말기 수에 따른 순차적 할당(효율적)
품질제어	Best Effort 방식으로 품질 보장이 곤란(Type of Service에 의한 QoS 일분 지원)	등급별, 서비스별로 패킷을 구분할 수 있어 품질보장이 용이 (Traffic Class, Flow Label에 의한 QoS 지원)
보안기능	IPsec 프로토콜 별도설치	확장기능에서 기본으로 제공
Plug&Play	없음	있음(자동 네트워킹 가능)
Mobile IP	곤란(비 효율적)	용이 (효율적)
웹 캐스팅	곤란	용이 (Scope Field증가)

Table. 1. IPv4와 IPv6 주소체계의 비교

2) IPv6의 특징

IPv6 주소체계가 가지고 있는 특징들을 대략적으로 살펴보면 먼저, 주소공간이 3.4×10^{28}개로 늘어나, 현재 주소공간의 부족으로 인한 서비스 확대의 어려움을 대부분 해소할 것으로 보이며, 다양한 개인 단말기에도 주소를 부여할 수 있을 것으로 추측되고 있다. IPv6의 다음 특징으로는 IP 헤더를 간략화 했다는 것이 될 것이다. 헤더의 단순화는 라우터 측면에서 볼 때에도 헤더를 분석하는 부하를 줄이게 되어 결국 패킷 처리를 위한 속도의 향상을 얻게 되고, 필요할 때에만 Next Header를 통하여 사용하게 되어 패킷 처리 과정에 효율성을 높이게 된다.[8] IPv6의 새로운 주소체계는 QoS(Quality of Service)에도 많은 변화를 주고있다. IPv6는 QoS 지원을 위해 IP 패킷의 연속적인 흐름을 Flow로 정의하고, 이것을 IPv6 패킷 헤더의 Flow Label 필드로 식별하게 하고 있다. 이를 통해 서비스의 수준을 조정할 수 있다.[9] 그리고 보안과 개인정보 보호에서의 IPv6에서는 보안에 관련된 인증절차, 데이터 무결성 보호, 선택적인 메시지 발신자 확인 기능 등을 프로토콜 차원에서 지원하고 있고, 확장 헤더를 이용하여 종단 간 암호화 기능을 지원할 수 있기 때문에 패킷 변조를 방지할 수 있다.[10] IPv6의 또 하나의 특징은 IPv4와 달리 Interface에 대한 주소를 자동으로 설정할 수 있다는 것이다.[11] IPv6 에서는 자동으로 Local IPv6 주소를 생성할 수 있다.

제주대학교 중앙도서관

2. IPv6 주소의 구조

1) IPv6 헤더구조

(1) 개요

IPv6 헤더는 40바이트의 고정 크기를 갖는 기본 헤더구조(Fig. 1참조)와 Payload로 구성되어 있다.[12]

Fig. 2에 IPv6 형식을 도시하였다.

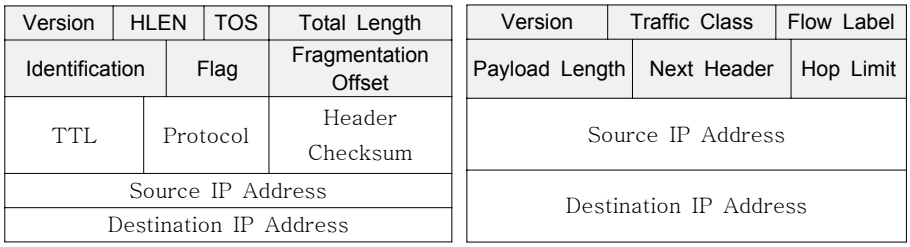


Fig. 1. IPv4, IPv6 Header

이 중, Traffic Class(8비트)는 QoS에서 사용되는 필드로 패킷의 우선순위 등을 나타내고, Flow Label(20비트)은 IPv6에 신설된 필드로서 Flow를 구분해 Flow 별 패킷 처리를 가능하게 해주는 QoS 관련 필드로 사용될 수 있다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Destination Address	6
Source Address	6
EtherType=0x86DD	2
Ver=6	4bits
Traffic class	1
Flow Label	20bits
Payload length(전체40)	2
Next Header	1
Hop Limit	1
Source IP Address	16
Dest IP Address	16
Payload=Extension Header(선택)+상위계층 패킷	Payload length
FCS	4

Fig. 2. IPv6의 형식

Flow Label 영역은 보통 실시간 서비스를 위하여 정의되어져 있고 표준화가 진행 중이다. 확장 헤더는 라우터에서의 처리를 높이고 다양한 옵션을 처

리할 수 있다.

IPv6의 모든 확장 헤더들은 Fig. 3에서 보듯이 자신을 지칭하는 Next Header 값을 가지고 있으며, UDP나 TCP 등의 상위 계층 프로토콜들은 IPv4에서 protocol 영역에서 사용되던 값들을 그대로 사용한다.

Next Header Type	Header name	
0	Hop-by-Hop options	확장헤더
2	ICMP v4	
4	IPv4	
6	TCP	
17	UDP	
41	IPv6	
43	Routing Header	확장헤더
44	Fragment Header	확장헤더
45	IDRP	
46	RSVP	
50	ESP	
58	ICMPv6	
59	Null=No Next Header	
60	Destination Option Header	확장헤더
62	Mobility Header	

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Fig. 3. Next header code

2) IPv6 주소체계

(1) 주소표기

IPv6 주소는 Prefix Interface ID로 구성된다. Prefix는 주소의 종류 및 subnet을 판별할 때 사용하는 필드영역이고 Interface ID는 네트워크에 연결되어 있는 각 인터페이스들을 구별해 주는 64비트의 필드영역이다. IPv6주소 배분은 IPv4와 달리 인터페이스를 기점으로 한다. IPv6 주소의 표기는 128비트로 구성되어 가독성을 높이기 위하여 아래와 같은 주소표기법을 따른다.

● 기본표기법

16비트씩 콜론(:)으로 나누고 각 필드를 16진수로 표현하는 방법이다.

'hexadeximal colon notation'이라고 한다.

● 주소 생략법

기본 표기된 주소 중 0이 자주 나타나는 경우 에 사용되는 표기법이다. 이는 나누어진 각 필드에서 0이 연속되어 나나날 경우 상위 0을 생략하는 상위 0 생략법, 필드안의 0을 모두 생략하는 연속 필드 생략법, IPv4 주소를 하위 32비트에 그대로 쓰고, 상위 모든 필드를 0으로 표현하는 IPv6표기법이 사용되고 있다.

● Prefix 표기방법

IPv6의 주소 네트워크 프리픽스 표기법은 IPv4의 CIDR(Classless Inter-Domain Routing) 표기법과 유사하여 IPv6의 주소 뒤에 "/"를 표기하고 네트워크 프리픽스를 10진수로 넣어 사용한다. 아래는 그 예이다.

3ffe:831f:cbc9:9a0a:0:fbd9:3419:53f7/64

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

웹 브라우저에서 IP주소와 일대일 관계에 있는 FQDN(Fully Qualified Domain Names)을 URL(Uniform Resource Locator)로 표기하는 것 대신에 상대방 IP 주소와 응용 포트를 직접 명기할 수도 있다. 이 경우, IPv4에서는 포트를 IP 주소와 구분하여 표기하기 위해 콜론(:)을 사용한다. IPv6는 콜론을 이미 다른 용도로 사용하고 있기 때문에, 중괄호()를 이용해서 이 문제를 해결한다. 아래는 그 예이다.

http://2001:2e3f::1:2:3:80/just.html

3. IPv4/IPv6 망 연결 형태

1) IPv4/IPv6 Dual stack 구조에 의한 연결

Dual satck 기술은 하나의 호스트 혹은 라우터가 두개의 주소체계(IPv4/IPv6)를 가지고 해당 프로토콜을 동시에 처리하는 기술이다.[13] 따라서 듀얼스택 기술을 지원하는 시스템은 물리적으로 하나의 시스템이지만 논리적으로는 IPv4와 IPv6를 지원하는 두 개의 시스템(interface)을 가지는 것이다. Fig. 4는 듀얼스택 호스트의 일반적인 구조이다.

<table>
<tr><td colspan="2">Application</td></tr>
<tr><td colspan="2">TCP, UDP</td></tr>
<tr><td>IPv4</td><td>IPv6</td></tr>
<tr><td colspan="2">Link layer, Phisical layer</td></tr>
</table>

Fig. 4. Dual stack

위 Fig. 4에서처럼 Dual stack에서 IP stack 아래는 IPv4 인터페이스와 IPv6 인터페이스를 설정하여, 하나의 LAN 카드로 IPv4와 IPv6 통신을 모두 함께 하게 된다. 대부분의 PC나 서버 시스템에 대한 OS(Windows 2000, Windows 2003, XP, Linux 2.4.X 등)들은 현재 IPv4/IPv6 Dual stack을 지원하고 있다.

(1) 주소설정

IPv4/IPv6 듀얼스택 노드는 IPv4 주소로의 설정과 IPv6주소로의 설정이 모두 가능하다. IPv4주소는 IPv4의 주소 할당 방식(예 : DHCP)을 사용하며, IPv6 주소는 IPv6의 주소 할당 방식을 사용하여 얻게 된다.

(2) DNS 이름 해석

IPv4/IPv6 듀얼스택 노드는 IPv4 및 IPv6 노드와 직접 호환될 수 있어야 하므로 IPv4 A 레코드는 물론이고, IPv6 AAAA 레코드도 처리할 수 있는 DNS Resolver Library가 있어야 한다. DNS resolver는 IPv4 또는 IPv6에 대

한 순서를 정할 수 있다.[14]

2) IPv4/IPv6 변환

(1) 변환기술의 개요

변환 기술은 IPv4 망과 IPv6 망 사이에 연동을 하기위한 기술로 IPv6 client가 IPv4 서버에 접속할 때 또는 IPv4 클라이언트가 IPv6 서버에 접속할 때 사용되며, IPv4/IPv6 네트워크 간의 Gateway에 사용한다. 변환 기술은 어떤 계층을 거쳐서 변환하는지에 따라서 헤더변환방식, 수송계층 릴레이 방식, 응용계층 게이트웨이 방식으로 구분할 수 있으며, 이에 따라 NAT-PT, SIIT, TRT, SOCKS 게이트웨이, BIS, BIA 등의 기술이 사용되어져 왔다.[15] [16][17]

(2) 변환방식

가. 헤더 변환방식

헤더변환방식은 IPv6 패킷 헤더를 IPv4 패킷 헤더로, 또는 그 반대로 변환하고, 필요하다면 체크섬을 조정한다. 헤더 변환은 IP 계층에서의 변환을 의미하며 헤더변환에서 IPv4 패킷을 IPv6로 또는 그 반대로 변환하는 것에 대한 정의는 SIIT(Stateless IP/ICMP Translation)에서 정의하고 있다. NAT-PT(Network Address Translation - Protocol Translation)은 SIIT방식에 기반한 헤더 변환 방식의 대표적인 예이다. 헤더 변환 방식의 가장 큰 장점은 IP계층에서만 변환하기 때문에 속도가 매우 빠르다. 하지만 NAT(Network Address Translation)와 마찬가지로 IP 계층 변환에 따른 단점을 가지고 있는데 대표적인 것이 DNS, FTP와 같이 응용 프로토콜에 내장된 IP 계층 주소를 변환하는 것이 어렵다. 이러한 점을 해결하기 위해서 DNS-ALG, FTP-ALG와 같은 별도의 응용 게이트웨이를 추가한다. 또한 IPv4/IPv6 헤더 변환시에 IPv4의 패킷이 여러 개의 IPv6 패킷으로 분할되게 되는데, 이는 IPv6의 헤더길이가 IPv4보다 20바이트 더 크기 때문이다. 그 외

제주대학교 중앙도서관

전환 기술로 BIS(Bump In the Stack) 등이 있다.

나. 수송계층 릴레이 방식

수송계층 릴레이 방식은 TCP, UDP/IPv4 세션과 TCP, UDP/IPv6 세션을 중간에서 릴레이 하는 방식을 의미한다. 이 방식에서의 전형적인 TCP 릴레이 서버는 다음과 같은 동작으로 수송계층에서의 전환을 이루게 된다. 즉, TCP에 대한 요청이 릴레이 서버에 도착하게 되면, 네트워크 계층은 목적지가 서버의 주소가 아니더라도 TCP 요청을 TCP 계층으로 전달하고, 서버는 TCP 패킷을 받아서 발신 호스트와 TCP를 연결하게 된다. 그 다음 서버는 실제 목적지로 TCP 연결을 하나 더 만든 후에 두 연결이 구축되게 되면 서버는 두 연결 중 하나에서 데이터를 읽어서 데이터를 나머지 하나의 연결에 기록하게 된다.

수송 릴레이 에서는 각 세션이 IPv4와 IPv6에 각각 밀폐되어 있기 때문에 헤더변환방식처럼 Fragments 나 ICMP 변환의 문제가 없으며, 헤더 변환 방식에 비하여 상대적으로 빠르다는 장점이 있다. 하지만 응용 프로토콜에 내장된 IP 주소에 대한 변환의 문제는 여전히 남아 있게 된다. 수송계층 릴레이 방식의 기술로는 TRT(Transport Relay Translator)와 Socks 게이트웨이 등이 있다.

제주대학교 중앙도서관

다. 응용계층 게이트웨이 방식

응용 계층 게이트웨이 방식은 트랜잭션 서비스를 위한 ALG(Application Level Gateway)로 사이트 정보를 숨기고 캐시 매커니즘으로 서비스의 성능을 향상시키기 위해 사용된다. ALG가 IPv4 및 IPv6 두 프로토콜을 동시에 지원하는 경우에 두 프로토콜간에 변환 방식이 사용될 수 도 있다. 이 방법은 응용 계층에서 변환하는 방식으로, 각 서비스가 IPv4와 IPv6에 밀폐되어 있기 때문에 헤더 변환에서 나타나는 단점은 없지만, 각 서비스를 위한 ALG가 IPv4와 IPv6 상에서 모두 실행 될 수 있어야 한다. 응용 계층 게이트웨이 방

식으로는 Squid가 있다.

3) IPv4/IPv6 tunnel

IPv4/IPv6 tunnel은 IPv6망에서 IPv4망을 거쳐서 IPv6 망으로 이동할 때 IPv4 망에 터널을 만들어 IPv6 패킷이 지나갈 수 있도록 하는 것이다. IPv4/IPv6 듀얼 스택 호스트와 라우터는 IPv6 데이터그램을 IPv4 패킷에 캡슐화하여 IPv4 라우팅 토폴로지 영역을 통해 터널링 할 수 있다. 다음 절에서 별도로 다룬다.

4. IPv4/IPv6망 연동을 위한 터널링

1) IPv4/IPv6 tunnel

제주대학교 중앙도서관

IPv6 도입 초기에는 섬 형태의 IPv6 망들이 IPv4망과 공존하게 될 것이므로 IPv4망을 경유하기 위하여 터널링을 통한 연결이 필요할 것이다. 지금까지 다양한 터널링 기술이 표준으로 제안 된 바, 그 중 대표적인 것을 살펴보면 Configured tunnel, 6to4, 6over4, ISATAP(Intra-Site Automatic Tunnel Addressing Protocol), Teredo, IPv6 over MPLS 등이 있다.

IPv6 in IPv4 터널링 기술은 크게 설정 터널링(Configured Tunneling)과 자동 터널링(Automatic Tunneling)으로 구분할 수 있다. 아래에서 다시 살펴본다.

(1) 설정 터널링(configured tunneling)

실제 통신이 일어나기 전에 터널 종단간의 라우터를 미리 설정하는 방식으로 발신 호스트에서 생성된 IPv6 패킷의 목적지 주소는 최종 목적지의 IPv6 호스트 주소를 포함하고 있게 된다.

(2) 자동터널링(Auto tunneling)

자동 터널링은 설정 터널링과 달리 실제 통신이 일어나면 자동으로 터널 종단을 설정하는 방식이다. 이때 발신 호스트에서 생성된 IPv6 패킷은 IPv4 주소를 포함하는 IPv4 호환의 IPv6 주소 패킷을 사용한다.

(3) 향상된 터널링 방식

기본적으로는 터널링 기술을 이용하면서 추가적인 기술을 통하여 기능을 향상시킨 터널링이다. 현재의 IPv4 망에 의해 격리된 IPv6 섬들과의 연동을 위해서 IPv6 패킷이 IPv4 망을 지나갈 때 IPv4 망에서는 IPv6 패킷을 인식 못하여 패킷 라우팅을 할 수 없게 되는 점을 터널링을 통해서 이용이 가능하도록 하는 것이다.

가. IPv6 터널브로커

IPv6 네트워크에 안정적이고 지속적인 IPv6 주소와 DNS 이름을 중계하기 위해 도입된 개념으로 터널 브로커라는 전용 서버를 구축하여 사용자의 터널 요구를 자동으로 관리하는 방법이다.[18] IPv6- over - IPv4 터널들을 관리하기 위한 터널브로커(Tunnel Broker)는 아래 Fig.5에서처럼 IPv4 인터넷에 연결된 사용자 또는 기관들이 IPv6 over IPv4 터널을 통해 IPv6 네트워크에 접속할 수 있도록 터널구성서비스를 제공할 수 있다.

제주대학교 중앙도서관

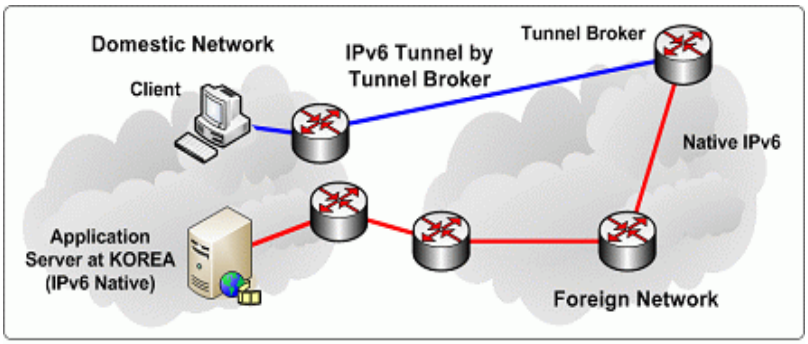


Fig. 5. Tunnel broker

위 그림에서 독립적으로 분리되어 있는 IPv4/IPv6 Dual-Stack 호스트는 터널 브로커를 통하여 IPv6 망에 대한 IPv6-over-IPv4 tunnel을 구성한다. 사용자 호스트는 터널브로커에 접속하여 터널서비스 등록절차를 수행하여 계정을 받는다. 계정 발급 후 터널 브로커 인증을 통해 터널브로커는 사용자 호스트, DNS 서버, 터널 서버 등을 구성하여 사용자 호스트와 터널 서버사이의 터널이 동작하고 사용자 호스트는 IPv6 네트워크에 연결이 된다. 개개인의 IPv6 접속을 위한 터널들은 터널브로커로 통합되어 운영된다.

나. 6to4 터널링

6to4는 명시적인 터널의 설정 없이 IPv6 네트워크 사이에 IPv4 네트워크를 통해 상호간에 통신하기 위한 방식으로 하나 이상의 유일한 IPv4 주소를 가지고 있는 IPv6 전용 사이트에 “2002:IPv4 주소::/48” 단일 IPv6 프리픽스를 할당하여 외부 IPv6 네트워크와 자동 터널링을 가능하도록 하는 기술이다.[19] 6to4 터널링은 IPv6-over-IPv4에서의 터널설정을 사용자가 직접 해야 한다는 번거로움을 해소하고 체계적인 터널관리가 필요 없도록 자동 주소 할당 및 격리된 IPv6 사이트를 서로 연결시켜 준다.(Fig. 6)

제주대학교 중앙도서관

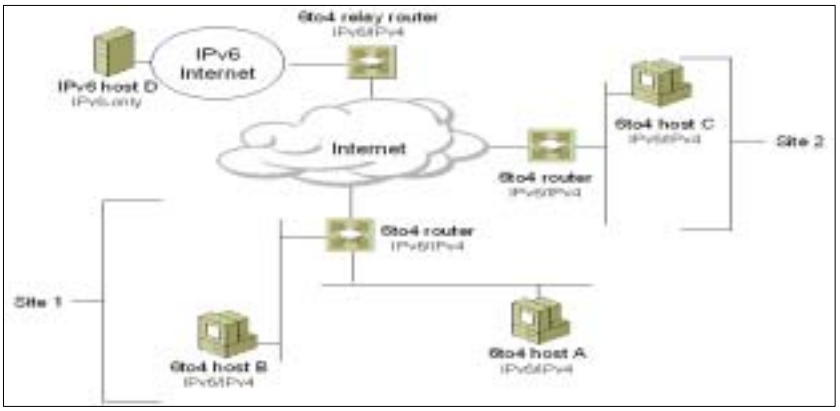


Fig. 6. 6to4 tunnel

그러나 6to4 터널링은 이를 지원하는 라우터를 각 사이트에 추가적으로 설치해야 하는 비용의 문제가 발생한다. 현재까지는 이러한 추가 장비들이 PC로 에뮬레이션(Emulation)되어 프로토콜 동작과 그 모듈의 안정성 테스트를 점검하고 있다.

다. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)

ISATAP(Intra Site Automatic Tunnel Addressing Protocol)은 듀얼스택 호스트와 듀얼스택 라우터들을 IPv4 네트워크 상에서 연결하기 위한 방식으로 IPv6 게이트웨이와 공통 데이터 링크를 공유하지 않는 듀얼스택 노드가 사이트 내에서 IPv4라우팅 인프라를 통해 IPv6 메시지를 자동으로 터널링 함으로서 글로벌 IPv6 네트워크에 결합할 수 있도록 한다.[20] 6to4 와 함께 사용자가 IPv6 망으로의 접속을 위한 터널 세팅을 쉽게 이루어주기 위한 방안으로 ISATAP는 IETF에서 정식 거론되어 논의 중에 있다. ISATAP는 터널 주소를 사용자가 직접 자신의 호스트에 설정 하지 않고 ISATAP 라우터를 통해서 사용자가 IPv6 망에 접속을 요청하게 되는 경우 자동으로 접속을 위한 IPv6 주소를 할당해 준다.(Fig. 7 참조)

제주대학교 중앙도서관

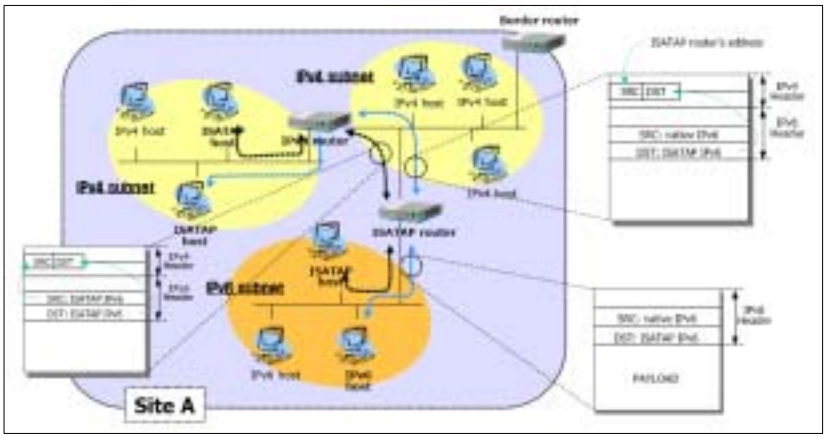
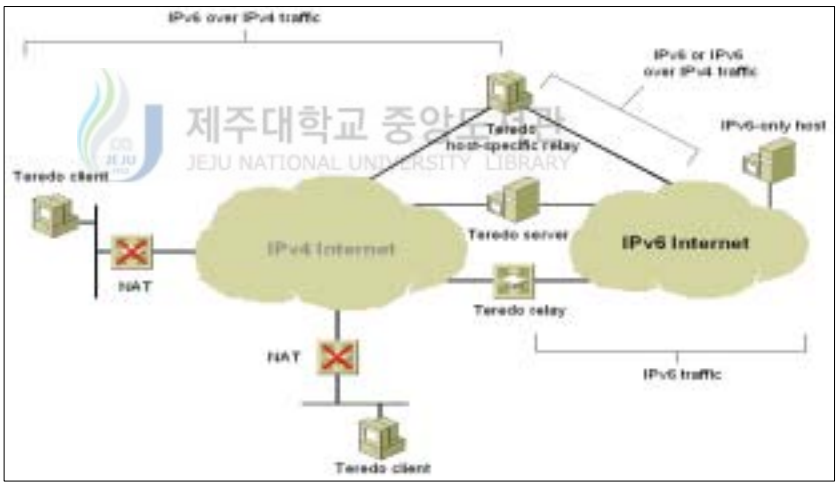


Fig. 7. ISATAP tunnel

라. Teredo

IPv4 NAT 상에서 위치한 노드에 UDP 상의 터널링 패킷을 통하여 IPv6 연결성을 제공하는 기술이다.[21] Teredo 서버는 각 Teredo Client의 정보를 관리하며, Teredo Relay는 PC에서 전달된 IPv6 데이터를 공식 IPv6 네트워크로 전달하고, 공식 IPv6 네트워크에서 전달된 IPv6 데이터를 다시 PC로 전달해주는 역할을 한다.(Fig. 8 참조) Teredo IPv4-IPv6 전환기술은 아직 표준화가 진행중이기 때문에, 일반인을 위한 Teredo 서버 및 릴레이의 운영은 6to4 릴레이 및 ISATAP 릴레이에 비해 활발하지는 않다.



제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Fig. 8. Teredo infrastructure

Microsoft, 6Wind, 한국전산원에서 Teredo 서버와 릴레이를 운영하고 있다. 본 논문에서는 한국전산원 6NGIX에서 운영중인 Teredo 서버와 릴레이를 이용하여 실험한다. 한국전산원 6NGIX의 Teredo 서버는 릴레이 역할을 함께 수행하고 있다.

Ⅲ. 터널링 기반 IPv6 네트워크

1. IPv6 호스트 설계

IPv4/IPv6 터널링을 구축해 보기 위해서 다음과 같이 망을 배치하였다.

1) 망 구성도

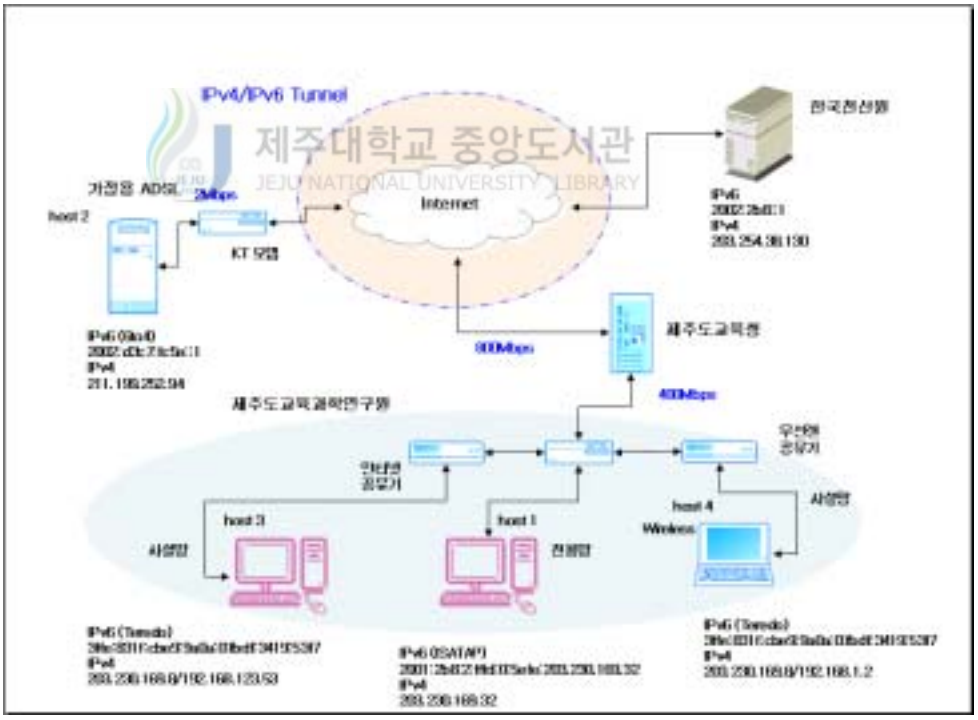


Fig. 9. 실험망 구성도

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

2) 망 구성에 대한 설명

본 실험에서는 교육전용망아래에서 IPv6터널링을 통한 트래픽을 모니터링하여 보고자 위 Fig. 8의 Host1을 구축하였다. Host1은 ISATAP방식의 터널링을 통하여 IPv6망에 접속한다. Host2는 KT 등의 ISP에서 제공하는 인터넷 접속망에서의 IPv6터널링 트래픽을 분석하여 보고자 구축하였다. 이 호스트는 6to4 방식의 터널링을 통하여 IPv6망에 접속한다. Host3은 일반적으로 흔히 쓰는 IP(인터넷)공유기를 통한 IPv6 터널링을 구축하고 트래픽을 분석하고자 설치하였다. 이 호스트는 Teredo 방식의 터널링을 통하여 IPv6망에 접속한다. 마지막으로 Host4는 Wireless Access Point를 통한 무선인터넷 기반의 호스트로서 이 호스트는 Wireless 기반에서의 IPv6 터널링을 실험하여 보고자 구축하였다. 이 호스트도 역시 Teredo 기반의 IPv6 터널링 방식을 사용하여 트래픽을 측정한다. 한국전산원은 IPv6 선도기관 중 하나로 본 실험에서 IPv6 전용 홈페이지 접속, IPv6 속도 측정 및 IPv6기반 파일 등의 서비스를 제공하고 있음으로 하여 본 실험환경에 넣게 되었다.

제주대학교 중앙도서관

호스트	터널 방식	구성된 네트워크
Host 1	ISATAP	전용망
Host 2	6to4	ADSL
Host 3	Teredo	전용망에서의 사설
Host 4	Teredo	전용망에서의 Wireless

Table. 2. 실험에 사용된 각 호스트의 터널방식

3) 사용된 각 장비의 명세

본 실험에서는 아래 Table. 3에 표시된 바와 같이 장비를 준비하였다. Host1에 사용된 장비는 P4 PC이다. 일반 사무용 장비로 많이 사용하는 기종이다.

구분	제조자(장비명)	OS	CPU	MEMORY	NIC
Host1	Samsung 멀티캡	XP home	2.8GHz	128M	intel pro 100
Host2	LGIBM X 210	Linux 2.6.11	2.4GHz	512M	intel pro 100
Host3	DELL 4600	XP pro	2.8GHz	256M	intel pro 100
Host4	Samsung Sens	XP pro	M 1.3GHz	512M	3com 10/100
E 1	Unicorn 800	Linux Embeded			54MHz
E 2	Linksys(AP)	Linux Embeded			2.4GHZ

Table. 3. 실험 장비 명세

Host 2 에 사용된 장비는 일반 사무실에서 워크스테이션용으로 사용이 가능한 기종으로 본 실험에서는 Linux 운영체제를 탑재하여 실험하였는데 소규모 네트워크에서는 워크스테이션으로 무리 없이 사용된다. Host 3 장비는 Dell 컴퓨터의 일반 사무용PC이다. 최근 들어 사무용으로 무리없이 사용되고 있는 기종이다. Host4에 사용된 장비는 센트리노 노트북으로 학생 및 직장인들이 많이 쓰는 기종으로서 무선 환경에 적절하게 사용되고 있다. E1 및 E2 게이트웨이용 장비는 일반사무환경에서 많이 쓰는 장비라 이번 실험에 채택하였다.

제주대학교 중앙도서관

2. 터널링 호스트 구축

본 논문에서 터널링 기반의 IPv6망을 구축하고 트래픽을 분석하여 보고자 전용망에서는 IPv6망에 정확히 IPv6주소로 접속하기 위하여 ISATAP방식의 터널링을 구축하였고, ADSL기반의 인터넷망에서는 Linux운영체제에서 구성하기에 편리한 6to4 터널링 방식을 사용하였다. IPv4 방화벽을 가진 사설망에서 여타 IPv6 터널링 방식을 사용하면 접속이 되지 않는다. 이런 이유로 하

여 사설망에서의 터널링 방식은 Teredo 를 사용하였다.

1) 전용망에서의 IASTAP 터널링 호스트 구축

본 실험에 사용된 전용망에서의 Host 1 호스트는 Windows XP 운영체제를 가지고 실험하였다. Windows XP에서의 IPv6 터널링 구축은 Windows XP SP2 또는 SP1 + 고급네트워킹팩이 설치되어 있어야 하고, 6to4 터널링 방식을 사용하게 되면 IPv4/IPv6 Dual stack 웹사이트를 IPv4 주소로 우선 접속하는 현상이 발생하고, IASTAP 터널링은 항상 IPv6로 우선 접속하기 때문에 본 논문에서는 IASTAP 터널링을 구축하여 실험하게 되었다.

Microsoft Windows XP 및 2003에는 기본적으로 IPv6 스택(프로토콜)이 내장되어 있다. 이때 사용되는 프로토콜은 “Microsoft TCP/IP Version6″이다.

Windows XP와 2003에서의 IASTAP 터널링을 설정은 netsh 명령을 이용하며 터널링을 형성할 IASTAP 라우터를 지정해야 한다. 본 논문에서는 한국전산원의 IASTAP 터널링 라우터를 활용하여 실험하였다. 한국전산원 IASTAP 라우터의 주소는 isatap.ngix.ne.kr 이다. 다음과 같은 명령을 이용하여 IPv6 스택을 활성화하였다.

제주대학교 중앙도서관

```
netsh interface ipv6 isatap set router isatap.ngix.ne.kr enabled
netsh interface ipv6 isatap set state enabled
```

위 명령은 ‘netshell’을 통해 대상 interface에 IASTAP 방식의 터널링을 구성하고 Router는 isatap.ngix.ne.kr로 활성화 하라는 명령이다. 명령 수행후 Fig. 10에서 보는 바와 같이 시스템에 설정된 IPv6 주소를 확인하였다.

Fig. 10 설치된 IPv6 주소확인

이어서 IPv6의 ISATAP 터널링이 활성화 된 것을 확인하기 위하여 ping6명령으로 http://ipv6.vsix.net과 통신을 시도하였다. http://ipv6.vsix.net는 IPv6 전용 서버이다. Fig. 11은 이를 보여주고 있다.

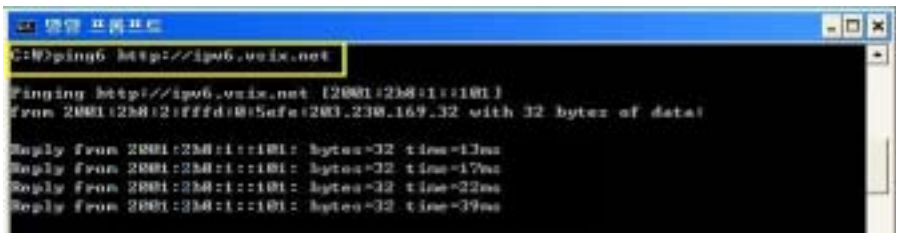


Fig. 11. Host1 ping6

아래의 Fig. 12는 IPv6 터널링을 통한 IPv6 전용홈페이지에 접속하여본 그림이다.

Fig. 12. IPv6 전용 홈페이지

Fig. 12에서 보는 바와 같이 IPv6주소를 가진 호스트들만이 접속가능한 IPv6 전용 웹페이지에 성공적으로 접속됨을 확인하였고 접속 IP가 IPv6 주소체계를 가지고 있음도 알 수 있다. 같은 사이트에서 제공하는 IPv6를 위한 품질테스트를 아래Fig. 13처럼 수행하였다.

Fig. 13. 한국전산원 속도 측정기

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

위 그림은 아래 Fig. 14에 보이는 IPv6 터널링 경로에서 IPv6 주소체계로 ipv6.vsix.net에 접속하였을 때 ipv6.vsix.net 서버가 접속자와 ipv6.vsix.net과의 트래픽을 의도적으로 발생시켜 망의 성능을 시각적으로 알 수 있게 서비스 해주는 시스템이다. 이 그림으로 보면 다운로드와 업로드 테스트시에 지연율, 손실율, 총 데이터/Sec 전송 결과 등을 보여주고 있다.

위 설계에 제시되었던 Host 2 IPv6 Linux 호스트에 ping6 테스트를 다음의 Fig. 14와 같이 실험해 보았다.

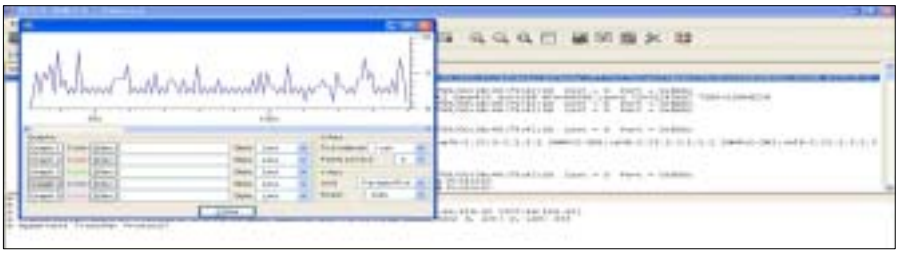


Fig. 14. Host 2와 접속

위 Fig. 14는 교육전용망에 속하여 있는 Host 1이 원격지의 ADSL 기반의 네트워크에 속하여 있는 Host 2와 Ping6 를 통해 패킷을 주고 받는 것을 나타내주는 그림이다.

이상과 같이 하여 Windows XP에 IPv6 ISATAP 터널링을 구축하였다.

2) 사설망에서의 IPv6 터널링 구축

본 논문에서는 설계상에 제시된 인터넷공유기 기반의 사설망의 Windows XP가 설치된 PC에 IPv6 터널 호스트를 구축하여 트래픽 측정을 시도하였다. 본 논문에서 제안한 사설망의 IPv4/IPv6간 연동을 위한 터널링 방식은 Teredo 방식을 사용하였고. Windows IPv6 Stack 설치는 ISATAP 방식과 다르지 않아 여기에서는 생략한다. 'Tunnel adapter Teredo Tunneling Pseudo-Interface:'로 표시되는 프로토콜 설치 확인 창을 통하여 IP Address는 fe80::5445:5245:444f%4로 나타나고 있는 것을 확인할 수 있다.(Fig. 15. 참조) 이때 Teredo 가상 인터페이스는 있지만, 관련된 설정이 되어 있지 않아, fe80으로 시작하는 Link Local 주소만 보이고 있음을 알 수 있다.

Fig. 15. 사설망 IPv6 주소

Teredo 데이터를 처리해줄 Teredo 서버와 릴레이를 지정하였다. 릴레이 지정명령은 아래와 같다.

netsh interface ipv6 set teredo client teredo.ngix.ne.kr

위 명령은, 본 실험재료인 해당 PC를 클라이언트로 등록시키고, 'teredo.ngix.ne.kr' 호스트를 Teredo 릴레이서버로 지정하도록 Teredo 터널을 설정하는 것이다. Host 3의 주소를 확인하였다. 아래 Fig. 16에 그 결과를 보인다.

Fig. 16. Teredo tunnel(Host 3)

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

위 Fig. 16에서 3ffe:831f:cbe9:9a0a:0:fbd9:3419:53f7이라는 주소가 생성된 것이 보인다. Fig. 17은 Host 2로의 접속 테스트이고, Fig. 18은 2001:2b8:1에 접속 테스트이다. IPv6 주소로 터널링이 되고 있다.

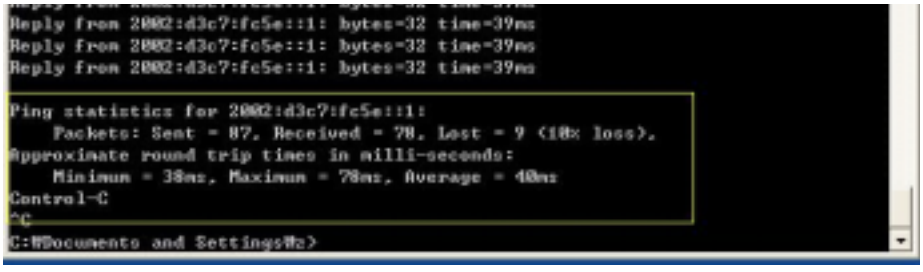


Fig. 17. Host2 ping6(Host 3)

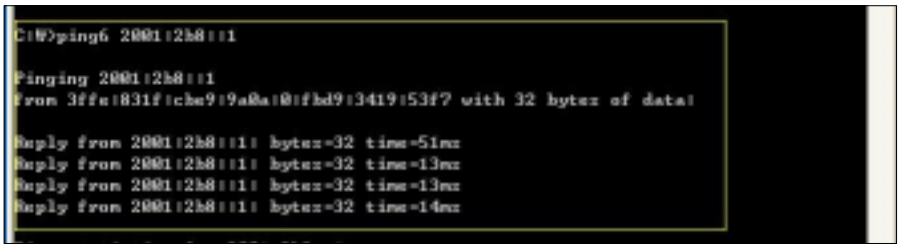


Fig. 18. 한국전산원 Ping6(Host 3)

아래 Fig. 19는 IPv6전용 홈페이지에 접속한 것을 나타낸 것이다. 상단에 접속한 IPv6주소가 표시되어 Teredo 터널 방식을 활용한 IPv6 터널링이 진행되었음을 알 수 있다.

Fig. 19. IPv6 전용 홈페이지(Host 3)

이상과 같이 하여 인터넷공유기를 사용하는 환경에서 Teredo 터널 방식을 이용한 IPv6터널링 방식을 구축하였다.

3) Wireless 환경에서의 터널링 구축

Wireless 환경에서의 IPv6 터널링 트래픽 모니터링을 수행하고자 네트워크를 구축하였다. 이는 위의 사설망 네트워크 구축과 다르지 않아 생략한다.

4) ISP 제공 ADSL 기반에서의 호스트 터널링 구성

본 실험을 위하여 재료로 사용한 시스템은 Linux kernel 2.6.11 Fedora 3.0 이다. 본 실험 수행을 위한 Linux 시스템의 설치 및 kernel Compile 과정은 생략한다. 본 Linux 운영체제에서 IPv6 Tunne 구축을 위한 호스트 구성은 6to4 터널링 방식을 활용하여 구축하였다. 여기에서 실험하게 될 6to4 터널 방식은 global IPv4 주소를 가진 단말의 주소를 Dual stack 으로 구성하여 원격지의 IPv6 네트워크에 이르기까지의 구간을 터널을 형성하여 통신 하는 것이다. 6to4 터널링은 하나의 IPv6 주소를 생성하는 것이 아니고, "/64"에 해당되는 Prefix를 생성하는 것으로서 6to4 Prefix 생성을 필요로 한다. 6to4 터널을 이용하면 내부적으로 별도의 IPv6 네트워크를 생성할 수 있다. 6to4 Prefix는 16진수로 변경한 IPv4 주소를 2002 뒤에 4자리씩 나열한 값이다.

IPv6 터널 프로토콜을 사용하기 위하여 아래의 명령으로 IPv6 스택이 설치되어 있는지 확인할 수 있다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

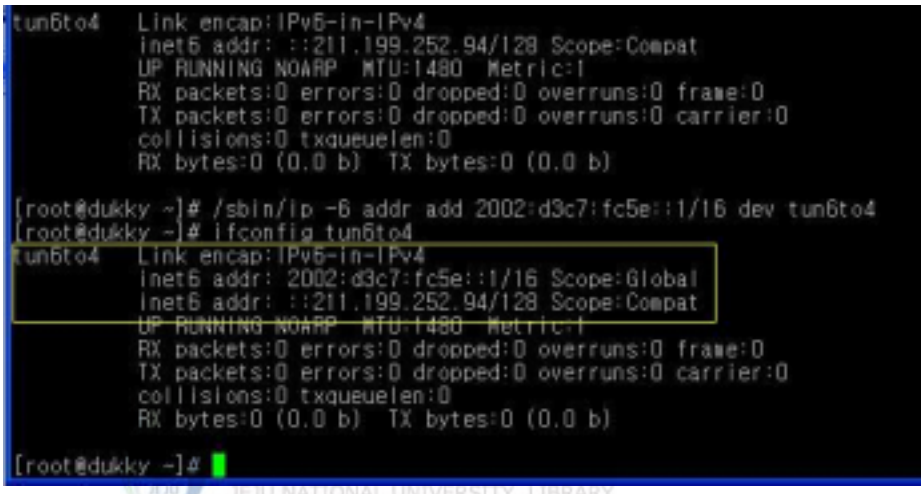
```
/sbin/ip -6 tunnel show
```

Linux에서 터널을 설정하기 위해서는 별도로 가상 인터페이스를 만든 다음 이 인터페이스에 주소를 할당하고, 라우팅 처리를 해야 한다. 6to4 터널링을 구축하기 위해 tun6to4 라는 가상 인터페이스를 생성시켜야 한다. 6to4 터널 인터페이스 생성은 다음과 같이 IP 명령으로 생성시켰다.

```
# /sbin/ip -6 tunnel add tun6to4 mode sit ttl 64 remote any local 211.199.252.94
```

이어 생성된 tun6to4 인터페이스를 활성화 시켰다. 활성화 명령은 아래와 같다. Fig. 20은 이에 대한 결과를 보여주고 있다.

```
# /sbin/ip link set dev tun6to4 up
```



JEJU NATIONAL UNIVERSITY LIBRARY

Fig. 20. 6to4 interface(Host2)

다음으로 외부 통신을 위한 라우팅 설정을 하였다. 라우터 설정을 통하여 Global IPv6와 연결이 가능하다. 6to4 라우팅 설정은 ip 명령을 이용하여 처리하였다. ip 명령어는 아래와 같다.

```
# /sbin/ip -6 route add 2000::/3 via ::203.254.38.130 dev tun6to4 metric 1
```

위 명령에서 203.254.38.130은 IPv4 Anycast 주소로서, host2가 속한 네트워크에서 가장 가까운 6to4 릴레이라우터를 찾아서 통신하기 위한 것이다. 위의 주소는 한국전산원의 라우터 주소이다.

지금까지 리눅스 호스트에 IPv4/IPv6간 연동을 위한 6to4 터널링을 구축하였다. 지금까지의 결과를 ping명령으로 확인하였다. 아래의 Fig. 21은 위에서 구축한 Host 1 호스트로 실행한 것이다.

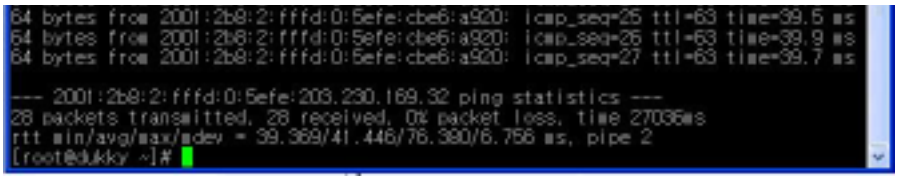


Fig. 21. Ping Host1 (host 2)

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Ⅳ. 트래픽 측정 실험

본 논문에서의 실험은 IPv4/IPv6 터널링 기반 하에서의 트래픽을 모니터링 하여 IPv6 터널링 트래픽의 특성을 파악하는데 있다. 본 실험에서는 IPv6 터널링으로 구성된 IPv6망의 Bandwidth, Time delay, 패킷손실을 측정하고자 ICMP, FTP, HTTP 프로토콜을 모니터링한다. 본 실험을 위하여 사용된 도구는 Ethereal, PRTG, MRTG, Sniffer, Analyzer이다. 실험방법으로는 Advanced Tunneling을 통하여 구성된 IPv6 네트워크 단말기에서 각각의 단말로 패킷을 전송한다. 실험의 결과는 그림과 표로 나타내고, 필요한 경우 설명을 추가한다. 기술순서는 전용망에서의 모니터링, 사설망에서의 모니터링, Wireless 기반에서의 모니터링, ISP 기반 ADSL 망에서의 모니터링순으로 한다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

1. 전용망에서의 실험

1) Ping

Ping은 ICMP나 ICMPv6프로토콜의 응용계층 프로토콜로 네트워크를 진단하거나 특정 목적지에 대한 도달을 알아보고자 할 때 메시지 응답을 요구하여 활용한다. 이번 실험에서는 host1에서 host2로 ping test를 하였다. 실험은 Bandwidth, 패킷의 손실, Delay Time을 측정하고자 하였다. 먼저 대역폭에 대한 실험은 Host1에서 host2로의 ping6 테스트를 통하여 수행하였다. 아

래의 Fig. 22는 1024Byte/sec의 데이터를 10분간 송출한 것이다. 그림에서 알 수 있듯이 순간적인 변화파형이 발생하였지만 대체로 안정적으로 대역폭이 유지되고 있다.

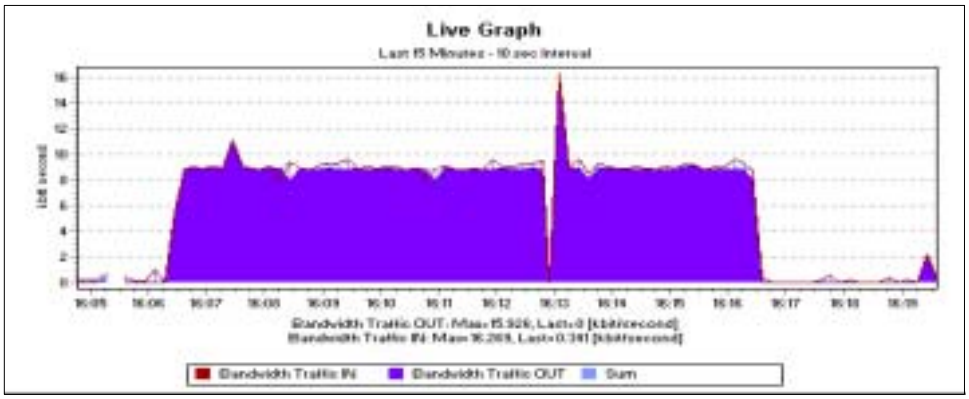


Fig. 22. IGMP Bandwidth (Hsot 1)

제주대학교 중앙도서관

패킷 손실 실험은 아래 Fig. 23에서 보는 것처럼 Host1에서 Host2로의 Ping6 테스트를 통해서 알아보았다. 이 Fig. 23은 1200초간 1024바이트의 크기를 가진 패킷을 전송하고 받아들인 결과를 보여준다. 이 실험의 수행은 패킷을 분석할 수 있는 Ethereal로 실험하였다. 이 Fig. 23에서 붉은 막대그래프가 Packets/sec을 나타낸다. 여기에서 알 수 있는 것은 패킷손실 여부인데, 패킷분석을 하여본 결과 공히 1024바이트의 데이터를 받고 있음으로 하여 데이터 패킷손실은 없다고 보여진다.

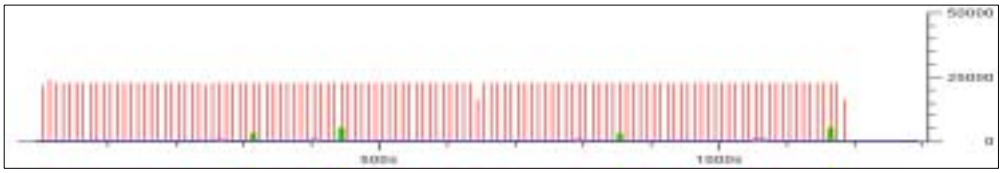


Fig. 23. Host2로의 Ping (Host1)

이때의 Ping test의 결과를 다음의 표에 나타내었다.

section	send packet	receive packet	lost packet (%)	Minimum (ms)	Maximum (ms)	Average (ms)
IPv4	1200	1200	0(0)	58	119	59
IPv6	1200	1200	0(0)	62	109	64

Table. 4. Host1에서 host2로의 ping 결과(1200sec)

다음의 Fig. 24는 600초간의 Host1에서 Host2로의 ping 결과를 ICMP와

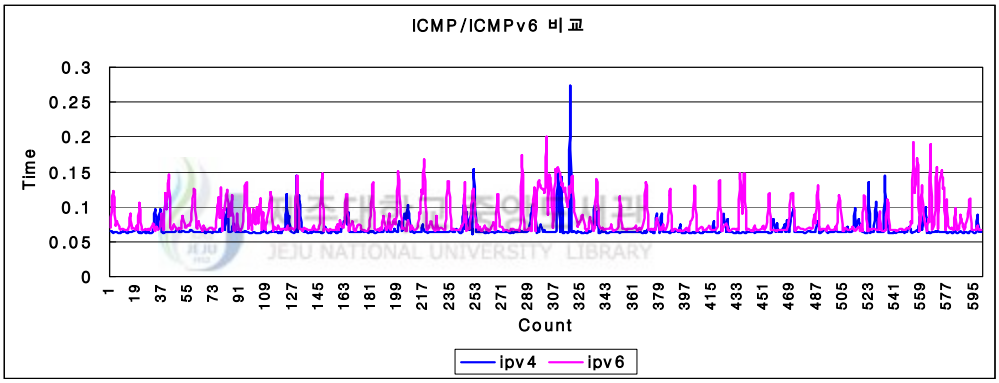


Fig. 24. ICMP/ICMPv6 Ping (host1)

ICMPv6와의 delay Time결과를 비교하여 보여주고 있다. 이 Fig. 24에서는 IPv4의 delay Time이 IPv6의 그것보다 적게 발생하고 있다. IPv6는 곳곳에서 delay Time이 발생하고 있는 것을 알 수 있다. 아래 Table. 5에 그 결과를 나타내었다. 다만 여기에서 밝혀두고 싶은 것은 측정시점에 따라 트래픽 발생이 다소 변화가 있었다는 점이다.

section	send packet	receive packet	lost packet (%)	Minimum (ms)	Maximum (ms)	Average (ms)
IPv4	600	600	0(0)	62	273	67
IPv6	600	600	0(0)	60	255	72

Table. 5. Host1에서 host2로의 ping 결과(600 sec)

Host 1에 MRTG를 설치하고 호스트와 호스트간의 실시간 트래픽 측정을 하였다. Host 1 호스트에서 Host 2호스트로 Ping6 패킷을 보내었고, 실험 후 해당 프레임을 보면 패킷 프레임의 크기는 일정하게 유지되고 있었다. 전체 트래픽을 측정하기 위하여 설치한 Host 1의 MRTG 측정량(Fig. 25 참조)을 보면 평균 11.1Mb의 패킷을 받아 들였고 2,343KB 패킷이 터널링을 통하여 나가고 있었다.

Fig. 25 Host 1과의 MRTG

2) Streaming

IPv6 터널링 기반에서 데이터 스트리밍 관련 트래픽을 측정하여 보고자

스트리밍 데이터 전송실험을 수행하였다. 이 실험을 통하여 IPv6 Streaming 트래픽을 대역폭, 지연, 패킷손실을 기술한다. 아래 Fig. 26은 동영상 데이터를 RTSP(Real Time Streaming Protocol) 전송에 대한 대역폭 측정을 그림으로 나타낸 것이다. 이 실험은 PRTG 패킷 툴 분석기를 통하여 대역폭을 측정하였다. 측정 시 마다 다소의 차이는 있었지만 그림에서도 알 수 있는 바와 같이 대략 3,800kbps의 대역폭을 보여주었다.

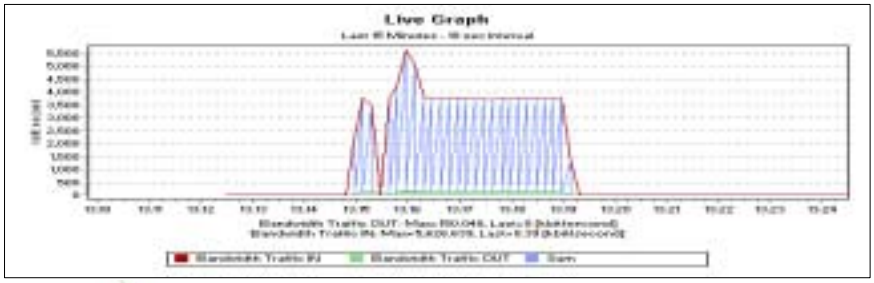


Fig. 26. 동영상데이터의 다운로드 대역폭 (IPv6-실험1)

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

아래의 Fig. 27은 동영상 데이터 패킷들을 보여주고 있다. 동영상의 크기는 총 75MByte이고, 내려 받은 패킷 프레임은 50,899개 이다. 이 Fig. 26은 스트리밍 전송이 IPv6 터널링을 통한 패킷전송으로 Payload length를 1440으로 정하여 패킷을 전송받고 있다는 것을 보여준다. RTSP 데이터의 크기는 1420 바이트이다.

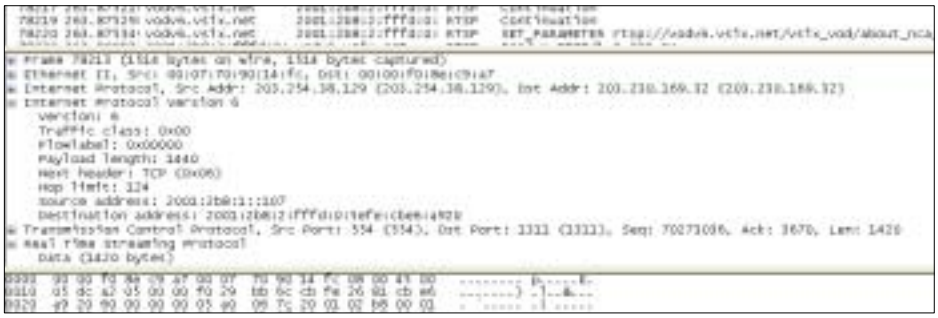


Fig. 27. RTSP IPv6 패킷

이번 실험에서 RTSP 프로토콜 패킷은 패킷 마다 평균 1475바이트의 멀티미디어 데이터를 가지고 있고, 매초마다. 평균 175개의 패킷을 전송받고 있었다는 것을 볼 수 있다. 터널링 기반 IPv6 환경에서의 스트리밍 데이터 전송과 IPv4 네트워크에서의 스트리밍 전송을 비교하면 Table. 6과 같다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

section	packets	E/R	Rx (MByte)	Avg. packets (packets/sec)	Avg. RX (Byte/packet)	Avg. Bytes (KBytes/sec)	Time(s)
IPv4	49344	0	73.6	291	1490	434	206
IPv6	50899	0	75.1	173	1475	255	233

Table. 6. Hsot1의 스트리밍 데이터 패킷

3) ftp

이번에는 응용계층에서의 트래픽을 모니터링하기 위하여 파일전송실험을 하였다. 실험은 한국전산원으로부터 262MByte의 압축파일을 내려받기 함으로써 수행하였다. 이 실험에 사용된 파일 내려받기에 관련된 사항은 아래 와 같다.

다운로드 시간	**7분 26초**
패킷 수/sec	**667.4개**

평균 패킷사이즈	1456.317바이트
총 바이트 수	287986590바이트
바이트/sec	971945.925바이트

아래의 Fig. 28은 대역폭을 보여주고 있다. 이 실험 역시 측정시간에 따라 많은 변동이 나타나고 있지만 일반적으로 250kb/sec에 가까이 이르고 있다.

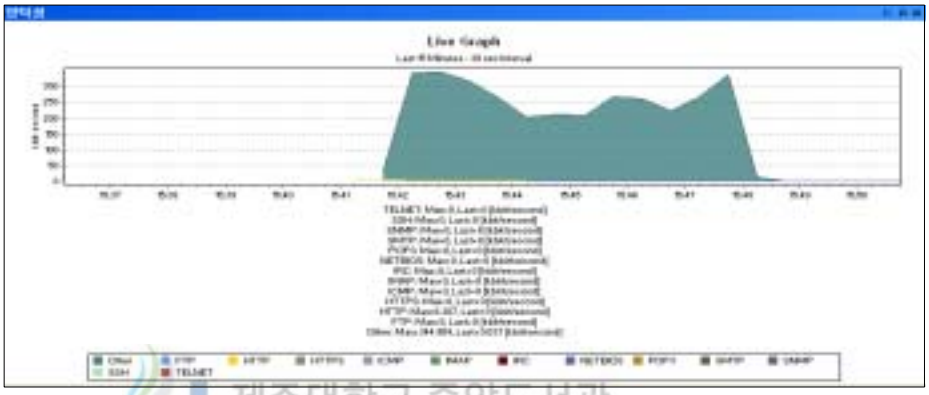


Fig. 28. 파일 다운로드 패킷 대역폭 측정

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

4) 트래픽 분석기를 이용한 다운로드, 업로드 분석

다음은 한국전산원에서 제공하고 있는 IPv6 전용 트래픽 측정 툴을 사용하여 Host 1과의 트래픽을 측정하였다. Fig. 29는 host1과 한국전산원과의 트래픽을 분석하는 분석기를 보여주고 있다.

Fig. 29. 한국전산원 트래픽 분석

위의 트래픽 분석기를 이용하여 아래의 Table. 7, Table. 8과 같은 IPv4/IPv6 터널망의 트래픽 측정 결과를 얻을 수 있다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

section	Time(s)	Data (Mbps)	speed (KB/s)
IPv4	10	5.07	750
IPv6	10	7.05	881

Table. 7. 트래픽 분석기를 이용한 downloading 트래픽 측정

section	Time(s)	Data (Mbps)	speed (KB/S)
IPv4	10	0.77	96.3
IPv6	10	9.56	1228

Table. 8. 트래픽 분석기를 이용한 uploading 트래픽 측정

이번 측정 실험에서 10초동안에 7.05Mpps의 데이터를 IPv6 단말기에서 881kB/s 로 다운로드 받을 수 있었고, 같은 시간 동안 IPv4 단말기에서는 5.07Mbps의 데이터를 750kB/s의 속도로 전송 받았음을 알 수 있다. 업로드 실험에서는 Table. 8과 같이 IPv4와 IPv6간의 격차는 현격하게 드러났다.

2. 사설망에서의 실험

1) ping

사설망을 통한 실험에서는 사설망에서 Teredo 방식을 통한 터널링을 구축하고 실제로 글로벌망에 접속하여 트래픽 모니터링을 수행하고자 하였다. 먼저 IPv6 글로벌망인 ipv6.vsix.net에 접속하여 Ping6 테스트를 진행하였다. 이번 실험 측정과 관련된 사항을 아래에 보였다.

시간(sec)	600
총 패킷 수	1240개
평균 패킷 수/sec	2.055개
평균 패킷 사이즈	121.277바이트
총 바이트 수	150384바이트
평균 바이트 수/sec	249.234바이트

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

아래 Fig. 29는 ICMPv6 프로토콜 트래픽 중 일부를 보여주고 있다.

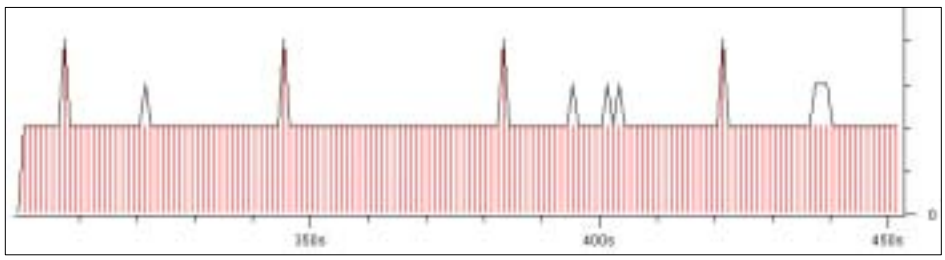


Fig. 30 Global ping traffic

이 실험은 10분간 32바이트의 패킷을 전송하고 받은 것으로 전체적으로 고르게 트래픽이 형성되고 있다.

다음 실험으로 host 2로의 ping6 테스트를 진행하고 이를 ICMP 트래픽과 비교하였다. 아래 Fig. 31에서 보는 바와 같이 전반적으로 IPv6 터널링 에서 보다 IPv4 망에서 더 안정적인 트래픽을 보여주고 있다.

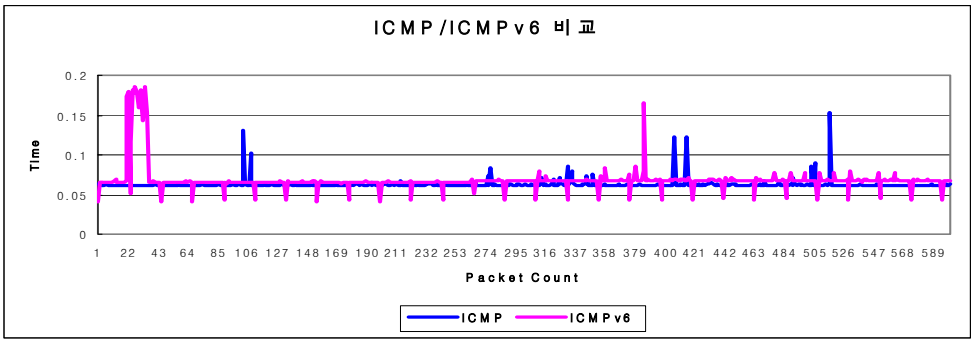


Fig. 31. Host2 와의 ping 트래픽 비교

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

2) ftp

사설망에서 IPv6 터널링을 통한 파일 다운로드 트래픽을 측정하기 위하여 ftp 프로토콜을 측정하였다. 다음의 Fig. 32는 한국전산원에서 200MByte 파일을 내려 받은 트래픽을 측정하여 본 것이다.

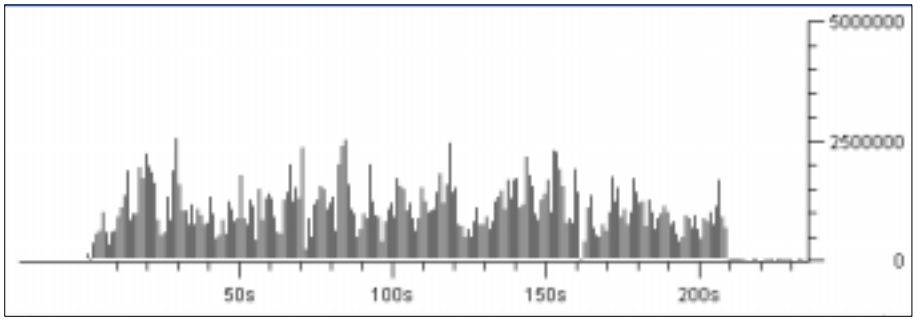


Fig. 32. 파일 다운로드 패킷 트래픽

위 Fig. 32에서 FTP 프로토콜이 매우 불규칙하고 급격한 피크를 보이고 있으나 여러 번의 실험으로 이는 회선상의 문제로 인한 것으로 보이고 있지만 매 실험마다 트래픽이 달라지고 있다.(Fig. 33 참조) 또한 다운로드 시간도 매우 불규칙하여 위 Fig. 32의 경우 210초 내외이지만, 아래 Fig. 33의 경우 70초정도에 파일의 다운로드가 완수 된 것을 알 수 있다. 이러한 점은 IPv6 터널링 환경에 있어서 트래픽의 적절한 측정을 어렵게 하는 요인이 된다.

Fig. 33. 파일다운로드 패킷 트래픽 2

위 Fig. 33 실험에서 얻어진 결과는 아래와 같다.

시간(sec)	234
총 바이트	219,676,549바이트
평균 패킷 사이즈	940,569바이트
평균 바이트/sec	935,180.93바이트
총 패킷 수	233,557개
평균 패킷 수/sec	994.271개

3. Wireless 기반에서의 실험

Wireless 기반 아래에서 IPv6 터널링 트래픽을 모니터링 하고자 이번 실험을 수행하였다. 이번 실험에서는 IPv6 터널링을 Teredo 방식으로 구축하고 ICMP 및 ICMPv6를 진행함으로써 패킷 트래픽을 살펴보았다. 이번 실험은 사설망 네트워크 상에서 수행하였기 때문에 네트워크 망 구축 형태는 위 사설망에서의 트래픽 모니터링 실험과 크게 다르지 않다.

아래의 Fig. 34는 Wireless 네트워크에서의 ICMPv6의 트래픽을 측정한 것이다. 그림에서 알 수 있듯이 전체적으로 고른 트래픽을 보여주고 있다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Fig. 34. Wireless ICMPv6 Traffic

다음은 ICMP와 ICMPv6의 트래픽을 비교하여 보았다.

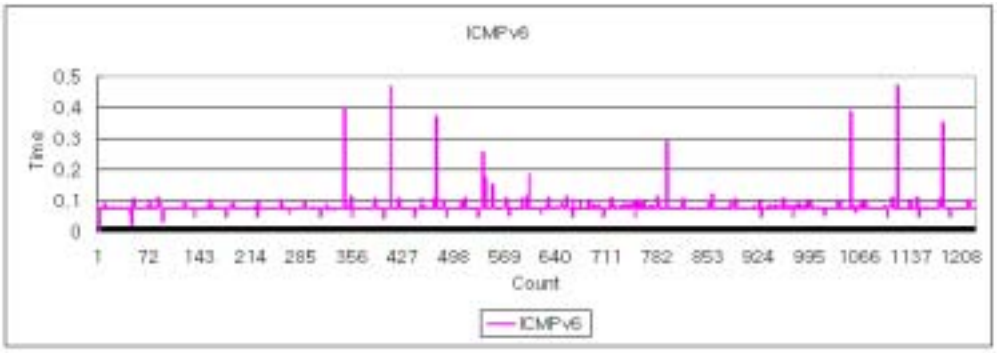


Fig. 35. Wireless ICMP/ICMPv6 traffic

아래의 그림은 한국전산원에서 200MByte의 파일을 다운로드 받고 그 트래픽을 모니터링한 것이다.

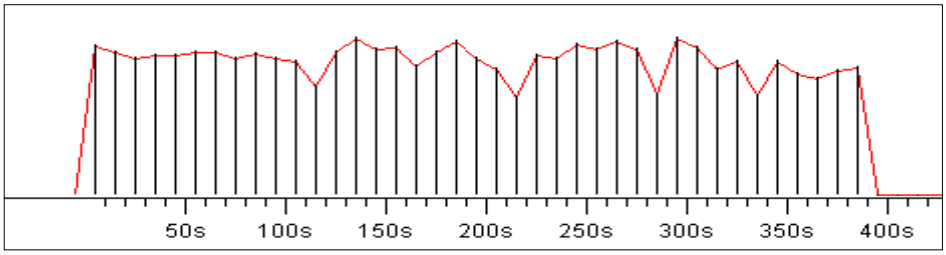


Fig. 36. Wireless - download file traffic

이 실험의 결과는 위 사설망에서의 실험과 비교해 보면 Wireless 기반의 실험 결과가 트래픽이 더 안정적으로 보이는데 이 점은 측정시간에 따른 특별한 특성으로 보여지고 있다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

4. ADSL망에서의 실험

IPv4/IPv6 터널링을 Linux에 구축하고 웹페이지 접속 및 FTP, IGMP 등의 실험을 하였다. 아래 Fig. 37은 트래픽 모니터링에 앞서 tracert 명령을 사용하여 IPv6 터널을 확인하였다.

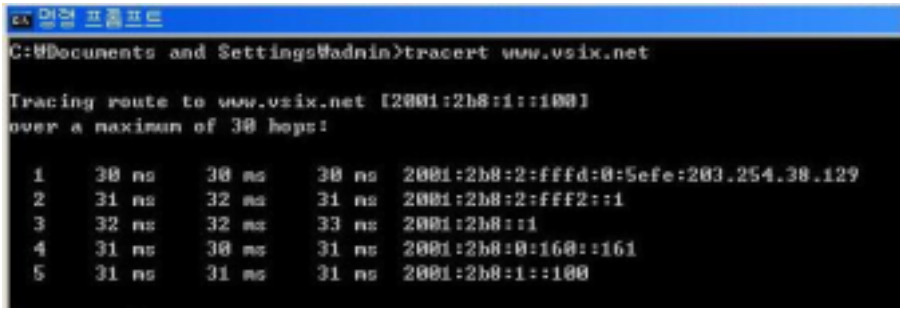


Fig. 37. tracert를 통한 터널링 확인

1) ftp

아래 Fig. 38은 IPv4/IPv6 터널링 망에서의 트래픽의 흐름을 모니터링 하고자 한국전산원에 올려놓은 200MByte의 zip 파일을 다운로드하여 그 트래픽을 모니터링 한 것이다.

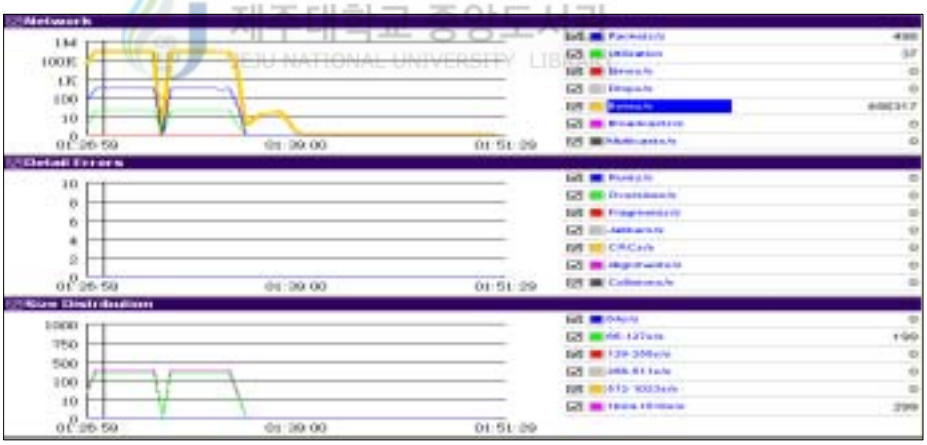


Fig. 38. Host 2에서의 다운로드 측정

위 Fig. 38에서 패킷 드롭이 없고, Packet/sec는 498개 초당 전송 바이트 수는 456,317바이트 임을 알 수 있다. 일반 가정에서 초고속 통신이 보통 T1 급이며, 다운로드 속도는 300kbps ~ 400kbps가 보통인 점을 감안하면 IPv6

터널링 방식에서의 파일 다운로드 속도 또한 거의 비슷한 양상을 보이고 있다.

2) ping

다음은 ping6 테스트를 통해서 패킷 드롭 및 딜레이를 측정하여 보았다. 테스트 대상호스트는 2001:2b8::1 이다. 실험은 1024 바이트의 패킷을 600초동안 전송하고 응답을 받는 것으로 진행하였다. 실험 결과는 다음과 같다.

시간(sec)	608
총 패킷	1,202
평균 패킷수/sec	2.003
평균 패킷 크기(Byte)	1104.336
총 바이트 수	1327412
평균 바이트 수/sec	2212.474

아래 Fig. 39의 그래프중 연속선은 IP 패킷 전체이며, 붉은 막대 그래프는 ICMPv6 패킷이다. 이 실험에서 패킷손실은 없었다. 600번의 호출로 같은 수의 응답을 받았다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

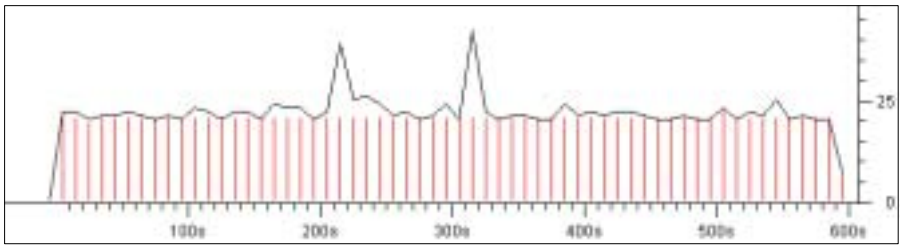


Fig. 39. ADSL 망에서의 Ping test

패킷에 대한 지연은 아래 Fig. 40에 ICMP와 같이 비교하였다. 실험을 통하여 ICMP 프로토콜을 통한 IPv4 네트워크일 때의 평균 응답속도는 0.049546초, IPv6일 때의 평균응답속도는 0.050527초로 나타났다.

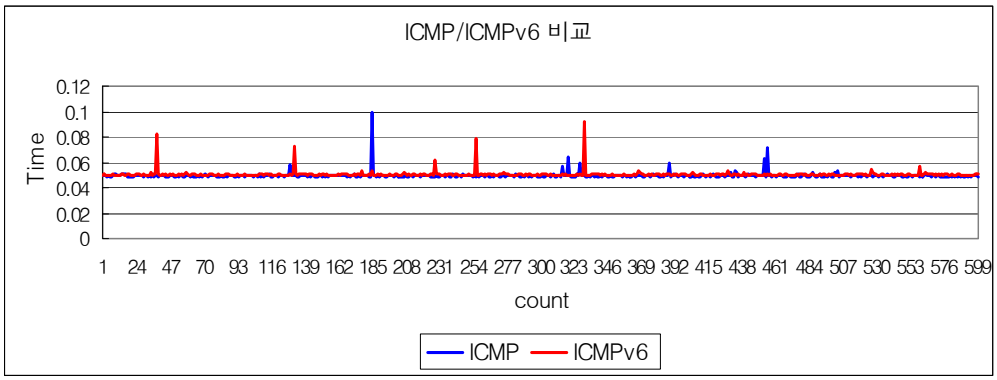


Fig. 40. ADSL 망 에서의 ICMP/ICMPv6 비교

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

Ⅴ 결론

IPv4/IPv6 연동을 위하여 전용망에서 ISATAP, 사설망에서 Teredo, ISP 기반의 ADSL 망에서 6to4, 방식의 터널을 구축하고 실제 망에 적용하여 ICMP, ICMPv6, 파일 다운로드, 멀티미디어 서비스 이용 등 격지자간의 트래픽을 발생하고 이에 대한 트래픽을 모니터링 하고자 하였다. 터널을 구성한 네트워크 망에서 "tracert"를 통하여 격지자간의 Router를 탐색한 결과는 터널을 구성한 구간에는 중간 노드가 보이질 않음으로 하여 터널이 설정되었다는 것을 알 수 있었다. 또한 단말기를 다른 네트웍크에 이식 시켜 보았을 때에도 기존의 네트워크와 무관하게 별 어려움 없이 주소가 호환되는 것을 알 수 있었다. 여러 번의 같은 실험을 통하여 일정한 트래픽 패턴이나 유사한 패턴을 찾으려 하였으나, 특별한 패턴이 발견되지는 않았고, IPv4 트래픽과 IPv6 트래픽을 비교 고찰한 실험 수행에서는 중간에 시차에 따른 회선의 트랙픽 변동이 심하게 발생하여 정확한 트래픽 측정이 쉽지 않았지만 대체적으로 IPv4 주소체계를 사용한 경우의 트래픽이 보다 안정적으로 나타났다. 전용망에서의 IPv4 접속인 경우 대역폭이 매우 우수하였지만 IPv6 터널을 통하여서는 그렇지 않았고, Ping test를 통한 패킷 지연은 IPv6 가 보다 많이 발생하였다. 패킷 손실을 측정한 결과는 IPv4나, IPv6에서 모두 0%의 결과를 나타내어 우수한 전송률을 나타내었다. 파일 다운로드를 통한 실험에서도 그 결과는 대체적으로 위와 같게 나왔다.

결과적으로 일반적인 사용자 수준에서의 IPv4/IPv6 터널을 통한 트래픽 측정에서 아직은 IPv4의 네트워크 트래픽이 IPv6의 트래픽 보다 안정적이라는 결과를 얻게 되었다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

참고문헌

[1] “IPv6 Status Report 2004”, 한국전산원, 1. 2005

[2] “공공기관을 위한 IPv6 도입 전략 수립 지침서” 정보통신부, 한국전산원, 12. 2004.

[3] 박성제, 이승종, “An IPv6 Introduction Strategy in The Defense Information System Network”, 1, 2002. 국방대학교 전산정보학과

[4] http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html

[5] http://www.ipv6.or.kr/archive/kripv6forum/html/att-0888/01-Juniper_IPv6_.pdf

[6] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/winsock/winsock/ipv6_guide_for_windows_sockets_applications_2.asp

[7] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 1883, 11. 1995.

[8] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture," RFC2373, 7. 1998.

[9] C. Partridge.“Using the Flow Label Field in IPv6”, RFC 1809, 6. 1995.

[10] R. Atkinson, "IP Encapsulating Security Payload (ESP)" RFC1827. 8. 1995.

[11] IAB, IESG, “IPv6 Address Allocation Management”, RFC 1881, 12. 1995.

[12] S. Kent, R. Atkinson, “IP Authentication Header”, RFC2402, 11. 1998.

[13] K. Tsuchiya, H. Higuchi, Y. Atarashi, “Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS)”, RFC2767, 2. 2000.

[14] M. Crawford, C. Huitema, “DNS Extensions to Support IPv6 Address Aggregation and Renumbering” RFC2874, 7. 2000.

[15] R. Coltun, D. Ferguson, J. Moy, “OSPF for IPv6”, RFC2740, 11.

제주대학교 중앙도서관 JEJU NATIONAL UNIVERSITY LIBRARY

1999.
[16] E. Nordmark, “Stateless IP/ICMP Translation Algorithm (SIIT)”, RFC2765, 2. 2000.
[17] “Network Address Translation - Protocol Translation (NAT-PT)”, RFC2766 G. Tsirtsis, P. Srisuresh 2. 2000
[18] A. Durand, P . Fasano, I. Guardini, D. Lento, ″ IPv6 Tunnel Broker“ , RFC3053, 1. 2001.
[19] B. Carpent er, K. Moore, ″Connection of IPv6 Domains via IPv4 Clouds″ , RFC3056, February 2001.
[20] F . Templin, T .Gleeson, M.T alwar , D. T haler , ″ Intra - Site Automatic Tunnel Addressing Protocol (ISATAP)″ , draft - ietf- ngtrans - isat ap, 2. 2002.
[21] http://support.microsoft.com/default.aspx?scid=kb;en-us;817778#10
[22] 정진욱 외, “TCP/IP 와 인터넷”, 생능출판사, 1. 2004.
[23] 윤종호 외,“TCP/IP 와 라우팅 프로토콜”, 교학사, 1. 2003.
[24] Wendell Odom, ″ Computer Network″, Cisco Press, 2004.
[25] William Stallings, ″Data & Computer Communications″, 7TH Edition. Prentice Hall, 2004.
[26] www.ipforumkorea.or.kr
[27] ipv6.vsix.net
[28] “on the NET”, 정보시대, 1. 2005.
[29] “on the NET”, 정보시대, 2. 2005.
[30] “on the NET”, 정보시대, 3. 2005.
[31] “on the NET”, 정보시대, 4. 2005.
[32] “on the NET”, 정보시대, 5. 2005.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY

감사의 말씀

오늘의 제가 있도록 온 마음으로 학문의 길을 열어주신 송왕철 지도교수님께 진심으로 깊은 감사를 드립니다.

제주대학교 중앙도서관
JEJU NATIONAL UNIVERSITY LIBRARY