IPv6를 위한 비쥬얼 이더넷 트래픽 발생기의 설계 및 구현

황재민*, 정인상, 정인환
한성대학교 컴퓨터 공학과
jem inad, insnag, ihjung@ hansung.ac.kr

Design and Implementation of Visual Ethernet Traffic Generator for IPv6

Jem in Hwang*, Insang Jung, Inhwan Jung
School of Computer Engineering, Hansung Univ.

요 약

본 논문에서는 이더넷의 네트워크 진단과 분석을 위해 필수적인 트래픽 발생기를 IPv6주소체계를 지원하는 네트워크 환경을 고려하여 설계하고 구현한다. 인터넷주소의 고갈과 IPv4프로토콜의 비효율성을 개선하기 위해 IPv6프로토콜에 대한 연구가 활발하게 진행되고 있다. 또, 이더넷 트래픽은 패킷의 양과 프로토콜의 종류 그리고 패킷의 길이에 영향을 받는다. 본 연구에서 설계하고자 하는 트래픽 발생기는 이 세가지 항목을 조정하여 다양한 네트워크 트래픽을 발생하는 것을 목표로 한다. 설계된 트래픽 발생기는 허브, 라우터등의 네트워크 장비의 성능 평가와 패킷을 모니터링하는 소프트웨어들인 네트워크 진단 시스템과 침입탐지 시스템 등의 성능 평가 및 검증을 위해 사용될 수 있다.

1. 서 론

현재 이더넷(Ehternet)은 가장 널리 사용되는 근거리 통신망의 형태이며 PC 를 통한 인터넷망으로 널리 사용되는 통신망 형태이다. 그러나 인터넷망에서 주소를 구분하는 현재의 IPv4는 컴퓨터의 증가에 따라 새로운 단말기, 네트워크에 할당할 주소가 부족한 상태에 이르고 있다. 앞으로의 인터넷도 지금과 같은 컴퓨터 시장에 의해 계속 성장할 것으로 예상되고 IPv4의 고갈을 예상하여 새로운 주소체계인 IPv6[1]에 대한 연구가 활발히 진행되고 있다. 또한 이더넷 네트워크의 물리계층(physical layer)은 많은 종류의 네트워크 장비와 컴퓨터들이 접속되어 사용되며 각각의 장비들 간에는 다양한 데이터가 오고 가고 있다. 물리적으로 하나의 네트워크를 공유하기 때문에 네트워크의 트래픽은 예측되기 어려운 면이 있고, 더욱이 IPv6를 주소로 하는 패킷들에 대한 네트워크 트래픽을 검증하는 도구가 필요할 것이다. 이와 같은 문제를 검증하기 위한 방편으로 네트워크 트래픽을 사용하여 이더넷에 접속되어 있는 IPv6 주소체계를 사용하는 네트워크 장비들의 성능 평가를 시도할 수 있는 트래픽 발생기(traffic generator)가 요구된다.

본 논문에서는 IPv6 주소체계[2]를 사용하는 이더넷 네트워크의 진단과 분석을 위해 필수적인 트래픽 발생기를 설계하고 구현하였다. 구현된 트래픽 발생기 VTGv6(Visual Ethernet Traffic Generator Version 6)는 윈도우 환경 하에서 수행되는 프로그램으로 편리한 사용자 화면을 제공하며, 다양한 방법으로 IPv6 이더넷 패킷을 발생함으로써 네트워크의 성능을 다양한 각도에서 검사할 수 있게 해 준다.

본 논문의 구성은 다음과 같다. 2장 관련연구에서는 이더넷 패킷을 직접 처리할 수 있는 환경과 IPv6의 헤더내용과 주소체계에 대하여 설명한다. 3장에서는 VTGv6의 설계 및 구현에 대하여 설명한다. 마지막으로 4장에서는 결론 및 향후 연구에 대하여 기술한다.

2. 관련연구

2.1 저수준 패킷 처리 환경

본 논문에서는 이더넷에 패킷을 직접 읽고 쓸 수 있는 환경인 Winpcap[3] 을 사용하여 트래픽 발생기를 구현하였다.

이더넷에서 네트워크 인터페이스를 통해 패킷을 직접 읽거나 쓰는 연구는 대표적으로 BPF[4] 와 Winpcap 이 있다. BPF 는 Unix 환경 하에서 패킷 감시 라이브러리인 libpcap 의 형태로 제공되며 Unix 또는 Linux 환경 아래에서 효과인 패킷감시기능을 제공하였다. BPF 는 사용자가 정의한 조건(filter)을 운영체제 내부에서 검사하여 조건에 맞는 패킷만 사용자 버퍼에 복사하는 구조를 가지고 있다. Winpcap 은 기존의 BPF 와 libpcap 의 호환성을 유지하면서 윈도우에서 패킷을 감시할 수 있는 환경을 제공한다. Winpcap 은 BPF가 2단계 버퍼를 사용하는 것과 달리 원형 버퍼를 사용하고, 커널에서 사용자 버퍼로 데이터가 복사되는 도중에도 패킷을 수집하여 저장할 수 있다. 따라서 Winpcap 이 BPF 에 비해 높은 성능을 보였다[3].

Winpcap 의 또다른 특징은 저 수준 패킷 전송 기능을 제공한다는 것이다. Windows 계열의 OS 에서도 저 수준 소켓을 제공하지만 제한적인 기능만 가능하다. 따라서 본 연구에서는 트래픽 발생기를 구현하기 위하여 Winpcap 의 패킷 전송 기능을 이용하였다.

2.2 비쥬얼 이더넷 트래픽 생성기(VTG)

기존 연구[5]는 비쥬얼 이더넷 트래픽 생성기(이하 VTG)를 구현하였다. VTG는 이더넷 과 IPv4 주소를 입력하고 UDP 와 TCP 프로토콜 형태 등을 지정하여 트래픽을 생성하는 도구이다. VTG는 패킷량, 전송시간, 전송량과 전송속도를 조정하는 다양한 전송방식을 가진다. 특히 전송속도를 조정하는 것은 불안정한 네트워크의 상태를 고려할 때에 절대적인 수치를 유지하는 것이 필요하다. 다음은 이에 필요한 알고리즘이다. 본 논문에서도 이와 같은 알고리즘을 사용한다.

```
do {
  very_last_time = clock(); // 현재 시간
  do {
    process_other_event(); // 속도 등기화를 위한 지연
  } while (clock() < (very_last_time + delay_time));
  total_sent_bytes += SendPacket(); // 1개의 패킷을 전송
  cur_time = clock(); // 현재 시간
  run_time = cur_time - start_time; // 총 실행 시간 계산
  cur_speed = (total_sent_bytes*8) / run_time // 속도
  if (cur_speed > requested_speed)// 목표 속도와 비교
    delay_time ++; // 속도가 따르면 지연시간 증가
  else if (cur_speed <requested_speed)
    delay_time--; // 속도가 느리면 지연시간 감소
} while (run_time < requested_time_duration)
```

2.3 IPv6 헤더

IPv6 기본 헤더는 그림 1과 같이 IP version 정보, 데이터그램 우선순위부, 흐름제어부, Payload 길이부, Next header, Hop limit 와 주소부로 되어있다.

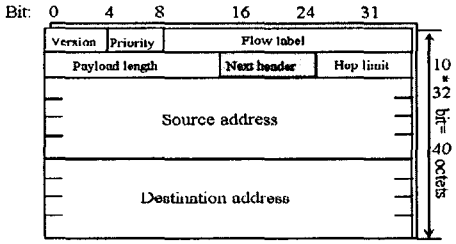

그림 1 IPv6 기본 헤더

그림 1에서 보는 것과 같이 IPv6는 IPv4에 비해 기본 헤더의 정보가 줄어들었으며, 총 헤더 길이는 40옥텟으로 정해져있다. 추가적으로 필요한 헤더 정보에 대해서는 Next header 옵션을 통해 지정할 수 있다.

추가적으로 지정할 수 있는 확장 헤더들은 hop-by-hop 옵션, 라우팅, Flagmentation, Authentication 와 목적지 옵션 헤더 등이 있다.

2.4 IPv6 주소

2.4.1 IPv6 주소표현 방식

IPv6 주소는 일반적으로 다음과 같이 128비트 의 길이를 가진다. 주소를 표현하는 방식은 4개의 16진수를 ":" 으로 구분한 8개의 필드로 나타낸다.

```
FEDC : BA48 : 7554 : 3210 : FEDC : BA48 : 7554 : 3210
```

주소를 표현하는 방식은 '0' 의 숫자열을 압축할 수 있으며 다음과 같이 "::" 으로 표현하여 '0' 의 16비트 그룹이 이어진 것을 나타낸다.

```
FF01 : 0 : 0 : 0 : 0 : 0 : 0 : 38
=> FF01 : : 38
```

IPv4와 IPv6 node의 혼합환경을 취급하는 표현방식은며 다음과 같이 마지막 4바이트를 IPv4 주소형식으로 대치하여 표현한다.

```
0 : 0 : 0 : 0 : 0 : FFFF : 128.134.165.1
=> : : FFFF : 128.134.165.1
```

본 논문에서는 위와 같은 IPv6의 표현방식을 제공하는 사용자 인터페이스를 설계하였다.

2.4.2 IPv6 주소체계

IPv6 주소는 인터페이스들과 인터페이스들의 집합을 지정하며 Unicast, Anycast 와 Multicast 주소와 같은 3가지 유형을 갖는다. Unicast 주소는 단일 인터페이스를 지정하는 형식으로 Unicast 주소로 보내진 패킷은 어드레스에 해당하는 인터페이스에 전달된다.

Anycast 주소는 특정 그룹으로 된 노드들의 인터페이스를 지정하며 Anycast 주소로 보내진 패킷은 라우팅 프로토콜의 거리 측정에 의해 그 어드레스에 해당하는 인터페이스 중 거리가 가장 짧은 하나의 인터페이스에 전달된다. Anycast 주소는 Unicast 주소 공간으로 부터 할당되어졌고, Unicast 주소 구조를 갖는다. 그러나 IPv6 Anycast 주소는 다음의 제한이 따른다. Anycast 주소는 IPv6 패킷의 소스 주소로 사용될 수 없고, 호스트에 할당될 수 없다. 단지 IPv6 라우터에만 할당된다.

Multicast 주소는 특정 그룹으로 된 노드들의 인터페이스를 지정하며 Multicast 주소로 보내진 패킷은 그 어드레스에 해당하는 모든 인터페이스들에 전달된다. IPv6는 Broadcast 주소가 없고, Multicast 주소가 이에 해당하는 기능을 대체한다. Multicast 주소의 형식은 그림 2와 같다.

8 bits	4 bits	4 bits	112 bits
11111111	flag	scop	group ID

그림 2 Multicast 주소 형식

그림 2는 Multicast 주소가 Unicast 주소와 구별되는 FF(11111111) 의 상위 옥텟 값을 가진 것을 보여준다.

본 논문에서는 위와 같은 IPv6 주소체계를 적용한 인테페이스를 설계하여 사용자가 쉽게 패킷을 생성할 수 있도록 하였다.

3. 설계 및 구현

본 논문에서 구현한 VTGv6는 패킷을 생성하고 전송하는 기능을 담당하는 커널 레벨 수준의 모듈과 IP 주소와 전송방식을 지정하는 응용프로그램 레벨 수준의 구조를 그림 3과 같이 가지고 있다.

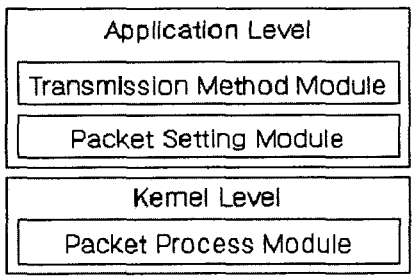

그림 3 VTGv6의 구조

그림 3의 주소 모듈은 패킷을 생성하기 위한 헤더 정보와 데이터를 직접 지정할 수 있다. 패킷을 위해 지정되는 헤더 정보는 이더넷 주소와 IP주소가 있고, 추가적으로 옵션부를 지정할 수 있다. 전송방법 모듈은 기존 연구에서 제안한 것과 같이 패킷량, 전송시간, 전송속도와 전송량 등을 조정하여 패킷을 전송할 수 있는 기능을 구현하였다.

IPv6의 주소체계는 주소가 사용되는 방법에 따라 여러 가지 형식을 취하게 된다. 따라서 사용자는 주소를 쉽게 입력할 수 있는 인터페이스가 필요하게 된다. 그림 4는 사용자가 IPv6 주소를 지정하기 위해서 필요한 인터페이스의 선택 흐름을 나타낸 것이다.

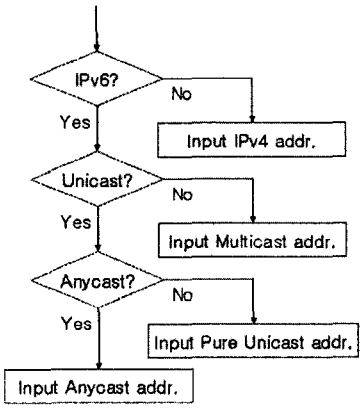

그림 4 주소 입력 인터페이스 흐름도

그림 4와 같은 순서는 사용자가 생성하고자 하는 주소 형태를 결정한다. 주소를 입력할 때에는 0'압축을 비롯하여 :'을 이용한 주소 구분을 해석할 수 있다. 또한 IPv4를 적용한 IPv6 주소도 해석이 가능하도록 하였다.

설정된 주소정보와 옵션정보를 가지고 생성된 패킷은 다양한 방식으로 전송될 수 있다. 이러한 기능은 네트워크에 접속되어 있는 라우터와 같은 네트워크 장비들의 성능테스트나 프로토콜 분석기[6]와 같은 네트워크 모니터링 도구를 테스트 할 경우에 유용하게 사용된다. VTGv6에서 지원되는 전송방식은 패킷수, 전송시간, 전송량, 전송속도 등을 조정할 수 있다.

다음 그림 5는 구현된 VTGv6 프로그램의 실행화면이다.

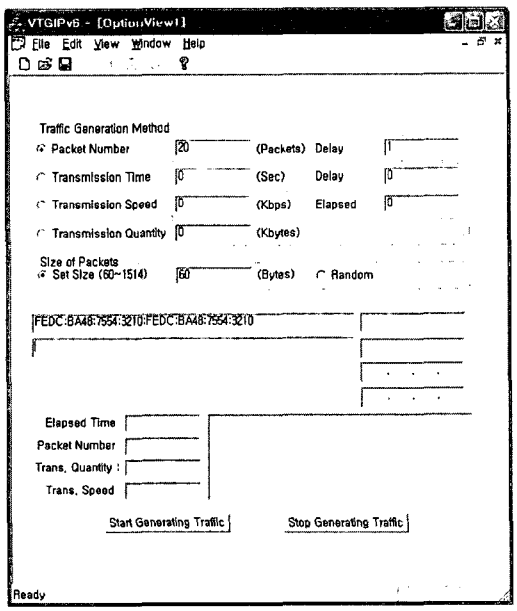

그림 5 VTGv6 실행화면

그 밖에 프로그램의 기능은 다음과 같다

■ IPv6의 기본 헤더 크기는 40Bytes 로 고정되어있으며, 기존 IPv4와 달리 옵션이 간소화 되어있다. 따라서 기본적인 옵션 이외의 추가적인 옵션을 제공하기 위해서는 기본 헤더의 뒷부분에 추가적인 옵션을 설정할 수 있는 기능이 필요하다. 프로그램의 인터페이스로서 이것을 고정시킬 수도 있지만, 패킷의 세부적인 부분까지 수정할 수 있는 상황을 고려하여 데이터 영역에 직접적으로 필요한 내용을 지정할 수 있도록 하였다.

■ IPv6 Nextheader 는 IP헤더의 옵션이나 상위계층의 프로토콜에 관한 정보를 지정하는 부분이다. VTGv6에서는 이를 위하여 옵션이나 상위계층 프로토콜을 쉽게 설정할 수 있는 인터페이스를 제공한다. 해당하는 옵션과 프로토콜 이름을 Nextheader 코드와 매칭시켜 해당하는 사항의 입력 인터페이스를 동적으로 재생성할 수 있도록 하였다.

■ IPv6의 옵션에는 Hoplimit 옵션이 있다. 이는 패킷이 몇 개까지의 노드를 거칠 것인가를 지정하는 옵션이다. 이 Hoplimit의 지정과 함께 ICMPv6 패킷을 생성할 경우에는 간단한 Ping 프로그램이 생성된다. VTGv6에서는 이를 이용하여 생성된 패킷이 네트워크 상에서 유효한지를 테스트하는 간단한 Ping 프로그램을 구현하였다.

4. 결론 및 향후 연구

본 논문에서는 다양한 방법으로 IPv6를 주소체계로 가지는 네트워크 트래픽을 발생할 수 있는 비쥬얼 이더넷 트래픽 발생기 VTGv6를 설계하고 구현하였다. 구현된 트래픽 발생기는 IPv6의 주소형식을 적절히 반영한 인터페이스를 가지고 있다.

본 논문에 이은 향후 연구로는, 구현된 VTGv6를 사용한 성능평가를 수행하고, 상위 계층의 프로토콜에 대한 트래픽 발생과 IPv6의 옵션헤더를 조정한 트래픽 발생에 대에 연구하는 것이다.

참고문헌

[1] IETF, The Recommendation for the IP Next Generation Protocol, RFC1752

[2] DSN, IPv6 기술 동향, http://database.sarang.net/study/ipv6/ipv6.html

[3] F. Risso and L. Degioanni, An Architecture for High Performance Network Analysis, Proceedings of the Sixth IEEE Symposium on Computers and Communications, pp. 686 693., 2001.

[4] S. McCanne and V. Jacobson, The BSD Packet Filter: A New Architecture for User-level Packet Capture., Proceedings of the 1993 Winter USENIX Technical Conference (San Diego, CA, Jan. 1993), USENIX.

[5] Inhwan Jung and Jinhwan Kim, Design and Implementation of Visual Ethernet Traffic Generator, 제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

[6] F. Risso and L. Degioanni, Analyzer: a public domain protocol analyzer, http://analyzer.polito.it/