

# 네트워크 간 VPN 지원 유무선 공유기 시스템

김창수\* · 양승의\* · 정희경\*

\*배재대학교 컴퓨터공학과

## Network-to-Network Router VPN Support System

Chang-Su Kim\* · Seung-Eui Yang\* · Hoe-kyung Jung\*

\*Department of Computer Engineering, Paichai University

E-mail : ddoja@pcu.ac.kr, alex@im.co.kr, hkjung@pcu.ac.kr

### 요 약

스마트 디바이스 활용영역이 시간과 장소의 제약을 뛰어넘어 사무실, 집, 학교 그리고 국내·외 출장 중 어디서든 자신이 하던 일을 계속 이어서 할 수 있게 되었다. 하지만 이러한 네트워크 간 인프라를 구축하기 위해서는 네트워크 전문가의 지원과 고가의 VPN전용장비가 필요한 이유로 중소기업에 까지 대중화가 되지는 못하는 실정이다.

본 논문에서는 저렴한 개방형 유무선공유기 H/W플랫폼에 개방형 네트워크전용 임베디드OS인 OpenWRT플랫폼을 기반으로 OpenVPN, OpenSSH, iproute 를 구현하여 네트워크 간 VPN을 지원하는 시스템을 설계 및 구현하였다.

### ABSTRACT

Take advantage of smart devices is time and place constraints beyond the Office, home, school and a Korean or foreign travel was being keep doing it yourself anywhere. But in order to build the infrastructure of these network-to-network VPN-only expert support and expensive equipment is needed for some reason does not go as far as small-to medium-sized institutions, popularised.

In this paper, H/W wired/wireless router a cheap, open platforms, open network-only embedded OS is based on OpenSSH, OpenVPN, OpenWRT platforms to implement network VPN iproute support system design and implementation.

### 키워드

OpenVPN, OpenSSH, iproute, 유무선공유기

## I. 서 론

두 개의 원격지 네트워크 간 VPN연동을 위해서는 양쪽에 VPN전용장비가 필요하다. 기존의 상용 VPN의 경우 라우터 기능, 터널링 기능 외에 IDS, IPS등 지능형 방화벽, QoS 기술, 다중 회선 지원, 로드 밸런싱등 다양한 고객의 요구에 적용할 수 있도록 구성하여 그 성능 및 가격이 수백만원에서 수천만원까지 형성이 되어있다. 또한, 이 장비를 설정하기 위해서는 라우터설정, 방화벽 설정, 터널링설정 등 네트워크 전문가의 지원이 필요한 어려움이 있다. 따라서 일반사용자, SOHO, 중소기업의 경우 네트워크간 VPN을 도입하기에는 소요 비용 측면에서 부담이 크다 할 수

있다. 즉, 유무선공유기 수준의 저렴한 가격과 손쉬운 설정으로 네트워크간 VPN을 구성하여 활용할 수 있는 장비에 대한 필요성이 대두되고 있다[1,2].

이에 본 논문에서는 유무선 공유기 수준의 저렴한 비용으로 네트워크간 VPN 연동이 가능한 장비를 제안하고자 한다. H/W플랫폼은 공개된 유무선공유기를 사용하고, S/W 플랫폼은 네트워크 전용 공개 임베디드OS인 OpenWRT를 기반으로 OpenVPN, easy-rsa, iproute등 관련 오픈소스들을 활용하여 구현한다. 여기에, 특허출원기술인 다중 큐잉 실시간 트래픽셰이핑 기술을 VPN터널에 적용시켜 회선품질의 변화가 빈번하더라도 최적의 네트워크 환경을 유지할 수 있도록 한다[3,4].

## II. 시스템의 구성

본 장에서는 논문에서 제안한 시스템에 대해 구현 절차와 시스템 구성을 기술한다.

### 2.1 OpenWRT 플랫폼 이식

타겟 H/W플랫폼은 상용 유무선 공유기에 가장 많이 사용되는 CPU인 Atheros, Broadcom 을 선택한다. 타겟 개발용 호스트 PC는 Linux 기반에 OpenWRT 개발환경을 준비한다. 타겟 CPU에 맞도록 커널설정을 하고 OpenVPN, openssl, iproute2, libpcap, 큐잉 등 관련 패키지들을 선택하여 컴파일한다. 이렇게 준비된 새 이미지는 tftp나 부트로더에서 펌업작업을 한다.

### 2.2 네트워크간 VPN - 브릿지 구현

두 개의 네트워크가 브릿지로 연결이 되었기 때문에 라우팅이 필요 없고 주소체계가 동일하고 동일 네트워크처럼 동작하기 때문에 이더넷 패킷까지 교환되고 모든 장비에 접근이 가능하다. DLNA, 인트라넷 등 동일 네트워크에서 동작하는 프로그램을 그대로 쓸 수 있는 장점이 있고, 이더넷 패킷까지 모두 전송되어 트래픽이 과도한 단점이 있다.

### 2.3 네트워크간 VPN - 라우팅 구현

두 개의 네트워크가 라우팅으로 연결이 되었기 때문에 주소체계가 다르고 다른 네트워크처럼 동작하기 때문에 명시적으로 라우팅 설정을 해서 사용을 해야 한다. 장단점은 브릿지 방법과 반대라고 할 수 있다.

### 2.4 브릿지 방법에서 다중큐잉 실시간 트래픽셰이핑 기술 구현

다중큐잉에는 밴드폭을 조절하기 쉬운 htb(Hierarchical Token Bucket) 와 우선순위 조절이 우수한 sfq(Stochastic Fairness Queuing)를 혼합하여 사용한다. 큐잉은 서비스포트별, IP주소별 PREROUTING, POSTROUTING 모두 설정할 수 있도록 구현한다. 디버깅 및 성능평가를 위해서 실시간 패킷모니터링이 가능하도록 하고 VPN터널링에 걸리는 CPU부하를 모니터링할 수 있도록 준비한다. VPN 터널링을 통해서 DLNA 동영상 플레이 및 제어가 되도록 하고, 동시에 ftp송수신과 ssh접속을 함께 할 수 있도록 하여 큐잉방법에 따라 그 성능의 변화를 모니터링 할 수 있도록 구현한다.

## III. 구현 및 실험결과

### 3.1 구현

정적인 방법으로 특정 IP, 특정 서비스포트별로 별도의 큐를 할당하고 밴드폭과 우선순위를 설정하고 테스트한 결과는 별도의 성능평가 리포트로 확인할 수 있다.

여기서는 2절에서 제시한 방법대로 현실의 DLNA 서버, 플레이어, 컨트롤러 그리고 ftp, ssh서버, 클라이언

트 장비를 VPN환경의 테스트베드로 구축하였다. 이렇게 구축된 동적인 테스트베드 환경에서 다중큐잉의 성능을 비교하기 위하여 다음과 같이 3가지 종류의 성능평가를 실시하였다. 실험 데이터의 우선순위는 원하는 대로 다양하게 적용할 수 있지만, 여기서는 동영상 끊김 효과를 바로 확인할 수 있도록 DLNA 스트림 데이터를 가장 높은 우선순위로 지정하여 테스트 하였다. 설명은 다음 그림 1과 같다.

- 트래픽셰이핑 없이 VPN 터널링만 동작
- 단일큐잉에서 트래픽셰이핑 동작
- 다중큐잉에서 트래픽셰이핑 동작

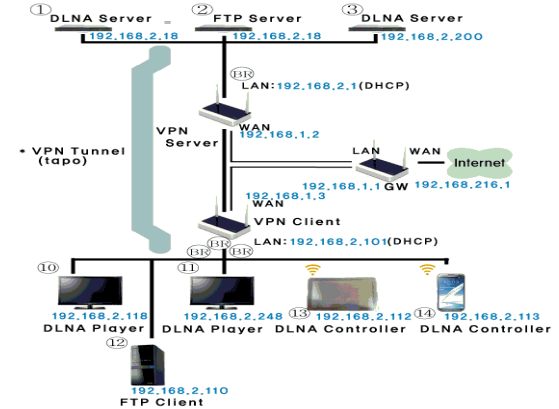


그림 1. VPN - 브릿지 - 다중큐잉 - 테스트베드

### 3.2 다중큐잉에서 트래픽셰이핑 동작

3개의 큐를 가지고 각 테스트 시나리오 마다 별도의 큐를 사용하게 한다. 동영상 스트림이 통과하는 큐1과 큐3은 우선순위와 대역폭을 동일하게 설정한다. FTP스트림이 통과하는 큐2는 큐1,3에 비해 우선순위가 낮고 대역폭도 좁게 설정한다.

#### 3.2.1 테스트 시나리오

가. 큐1: 번호⑬ --> 번호③ --> 번호⑩

큐1을 통해서 DLNA컨트롤러⑬로 DLNA서버③에 있는 동영상(3.5GB, 1920x800, 4508Kbps)을 DLNA플레이어⑩에 플레이시킨다.

나. 큐2: 번호②--> 번호⑫

큐2를 통해서 FTP서버②에 있는 파일(3.4GB)을 FTP클라이언트⑫에 다운로드한다.

다. 큐3: 번호⑭ --> 번호① --> 번호⑪

큐3을 통해서 DLNA컨트롤러⑭로 DLNA서버①에 있는 동영상(381MB, 1280x720, 7062Kbps)을 DLNA플레이어⑪에 플레이시킨다.

#### 3.2.2 테스트 결과

시나리오 “가”, “나”, “다” 순서로 동시실행한다.

- 공유기의 VPN프로세스 CPU점유율 : 86~93% 사이 안정적

- 시나리오 “가” : 전혀 버퍼링 없음.

- 시나리오 “나” : 900Kbps ~ 4000Kbps 가변적. 우선순위가 낮아 전체 트래픽이 올라가면 낮아짐.

- 시나리오 “다” : 속도체크를 위한 1~2번만 버퍼링만 발생.

#### IV. 결 론

본 논문에서는 특허출원기술인 다중큐잉 실시간 트래픽쉐이핑 기술을 VPN터널에 적용시켜 회선품질의 변화가 발생하더라도 최적의 네트워크환경을 유지할 수 있도록 하여 저렴한 장비지만 회선품질성능은 상용제품보다 우수하도록 하였다.

특히 실험결과와 같이, 전용 VPN장비에 비해 상대적으로 부족한 유무선공유기의 CPU성능을 실시간 다중큐잉 트래픽쉐이핑 기술로 네트워크 상황과 CPU상황 그리고 우선순위에 따라 대역폭을 조절함으로써 실제 운용성능을 최대로 끌어올린 것에 본 논문의 의미가 있다고 할 수 있다.

향후 과제로는 다중큐잉 방법과 병행하여 가중치가 다른 다중 터널링으로 확장하여 더욱 효율적인 성능을 끌어낼 수 있는 방법에 대한 연구가 필요하다. 또한, 응용과제로는 IoT 센서를 본 논문에서 개발한 플랫폼에 “센서-DLNA” 가상화 기술과 접목시켜 VPN을 통한 맥내 센서에 안전한 접근이 가능한 연구로 발전시킬 수 있다.

#### 감사의 글

본 논문은 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No.C0212853)의 연구수행으로 인한 결과물임을 밝힙니다.

#### 참고문헌

- [1] Min-seok Kye, Joon-Ki Min, Seung-Eui Yang, Sang-No Park, Hoe-kung Jung, “iOS-based Fitness Management System utilizing OpenWrt Server”, Journal of the Korea Institute of Information and Communication Engineering, vol. 18, no.2, Oct, 2014.
- [2] OpenWRT Web site: <http://openwrt.org>
- [3] I. Kotuliak, P. Rybár and P. Trúchly, “Performance Comparison of IPsec and TLS Based VPN Technologies”, ICETA 2011 9th IEEE International Conference on Emerging eLearning Technologies and Applications, Oct. 27-28, 2011.
- [4] “Introduction to iproute2”. The Linux Foundation. 2009-11-19. Retrieved 2014-06-30. <http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2>