보안측면에서의 가상사설망과 전용회선망의 비교 연구

정은희*, 이병관**

A study on the comparison of VPN with Dedicated Line Network on security

Eun-Hee Jeong*, Byung-Kwan Lee**

요 약

통신망은 크게 누구든지 접속할 수 있는 공중망과 해당 조직 내의 사람들만이 접속할 수 있는 사설망으로 구분할 수 있는데, 공중망의 회선비용 절감과 사설망의 신뢰성 있는 보안 통신 지원이라는 장점만을 부각시킨 것이 VPN이라 할 수 있다. 본 연구에서는 3계층 터널링 기법을 사용하는 IPSec VPN과 2계층 스위칭 기법과 3계층 라우팅 기술을 접목한 새로운 스위칭 기법을 이용하는 MPLS(Multi Protocol Label Switching), 그리고 전용회선을 보안측면에서 비교 분석하였다. VPN이 비용면이나 보안측면에서 전용회선보다 우수하며, IPSec VPN과 MPLS VPN을 비교해보면 안전한 데이터 전송을 위한 보안 유지, 비용 절감, QoS 제공, 운영 및 관리의 유연성을 보장하고, 오히려 IPSec VPN의 문제점을 보완하는 MPLS VPN이 차세대 VPN이라 할 수 있다.

ABSTRACT

Communication is be classified into public network and private network. VPN is made by integrating the circuit cost reduction of public network and the reliable security support of public network. This paper analyzes the IPSec using three layer tunneling, MPLS(Multi Protocol Label Switching) integrating 2 layer switching and 3 layer routing techniques and dedicated line from the viewpoint of security. In conclusion, VPN is better than dedicated network line in cost and security. If IPSec VPN is compared with MPLS VPN, MPLS VPN is more excellent than IPSec VPN in safe data transmission, cost, QoS and management.

Key-words : VPN, IPSec VPN, MPLS VPN, 전용회선, VPN전용선

Ⅰ. 서 론

통신망은 크게 불특정 다수의 일반인에게 서비스할 수 있도록 통신업체들이 구축한 통신망인 공중망(public network)과 개인이나, 단체, 기업이 사적인 목적으로 구축한 네트워크로 내부적인 규정에 따라 관리, 운영되는 네트워크인 사설망(private network)의 2가지로 분류할 수 있다.

공중망은 일반 가입자뿐만 아니라 여러 기관의 컴퓨터나 단말기에서도 공유할 수 있어 통신자원을 절약함과 아울러 통신효율의 증대를 기대할 수 있다. 이러한 목적으로 많은 국가에서는 정보통신망을 구축하고 있는데, 이는 한 국가의 통신기반 설비로서 매우 중요한 요소가 되므로, 국가가 직접 이를 관장하고 있는 경우도 많다. 하지만, 공중망의 경우 많은 사람들이 사용하고 있고, 위험에 대한 노출이 크므로, 공중망을 사용할 경우 회사의 중요데이터는 공격자에 의하여 쉽게 노출 될 수 있다는 단점이 존재 한다.

사설망은 사설망에서 주고받는 정보들은 해당 조직의 사용자만이 접근할 수 있도록 보호되고 있다는 점과 IP주소 사용이나 네트워크 관련 규정들을 그 조직 내부의 임의대로 정의할 수 있다는 장점을 제공한다. 하지만 내부적 관리,

* 강원대학교 지역경제학과 조교수(jeongeh@kangwon.ac.kr)
** 관동대학교 컴퓨터학과 교수

운영 규정이 다른 사설망간의 연동은 어려운 문제일 뿐만 아니라 외부(공중망 : 인터넷)에서 사설망으로의 접근이 쉽지 않다. 또한 인터넷상에서 개별 조직을 위한 사설망 구축은 이중적인 비용부담을 안게 된다. 국내의 웬만한 기업들은 회선을 임대하여 지사나 공장 또는 해외지사와 연결한 사설 네트워크를 구축하여 필요한 데이터를 주고받고 있는데, 사설 네트워크를 구축한 업체들은 IMF시대를 맞아 회선비용을 절감할 수 있는 솔루션이 필요하게 되었다. 바로 이 절실한 필요성을 충족하기 위한 솔루션이 가상 사설망(VPN, Virtual Private Networks)이다.

VPN은 PSTN(Public Switched Telephone Network), IDSN(Integrated Services Digital Network), ADSL(Asymmetric Digital Subscriber Line) 같은 망 서비스 사업자의 공중망이나 인터넷을 자사의 WAN(Wide Area Network) 백본처럼 사용하는 네트워크를 말하며, 인터넷의 급격한 성장에 따라 급속히 발전해 왔다. VPN을 이용하면 기업의 본사와 지사, 또는 지사간의 원거리 통신망을 저렴한 비용으로 구축할 수 있으므로 기업 마케팅이나 영업활동에 있어서 최소 비용으로 최대 효과를 낼 수 있다.

최근에는 충분한 대역폭 확보와 기업내 정보보호를 위해 VPN 서비스가 급속히 보급되고 있는 추세로서 많은 기업들이 VPN의 조기 도입을 시도하고 있다. VPN은 보다 저렴한 비용으로 서비스 제공자와의 유연한 연결을 가능하게 함으로써 전통적인 WAN환경의 안전성과 성능향상 그리고 QoS(Quality of Service) 및 보안 확보를 가능하게 하는 네트워크 통합 솔루션이다. 또한 인트라넷 내에서 사용되어 보안강화, 중요정보나 시스템 및 자원에 대한 접속 제어, 회계시스템의 접속 제한, 기밀정보의 안전한 전송 등을 보장할 수 있다[1].

본 연구에서는 3계층 터널링 기법을 사용하는 IPSec(IP Security) VPN과 2계층 스위칭 기법과 3계층 라우팅 기술을 접목한 새로운 스위칭 기법을 이용하는 MPLS(Multi Protocol Label Switching) VPN을 비교 분석하고, 그리고 가상 사설망인 IPSec VPN, MPLS VPN과 전용회선을 비용 및 보안측면에서 비교 분석하였다.

II. VPN

2.1 VPN 정의

VPN은 인터넷과 같은 공중망을 이용해 사설 전용망의 효과를 얻는 기술로서, 이를 구현하기 위한 하드웨어 및 소프트웨어의 집합체라 정의할 수 있다. VPN은 현재 IT 기술 중에서 가장 주목받고 있는 기술 중 하나인데, 과거에는 각 제조사별로 독자적인 VPN 기술을 선보였기 때문에 표준화가 진행되지 않았고, 무엇보다 VPN 기술의 안정성과 성능이 충분히 검증되지 않아 그리 활발하게 도입되지 않았지만, 최근에는 VPN 기술이 IPSec 프로토콜로 표준화되고, 많은 도입 기업에서 VPN의 보안성과 신뢰성이 검증됨에 따라 원격지 네트워크를 안전하고 비용 효율적으로 연결할 수 있는 솔루션으로 인정받기 시작했다. VPN이 현재 시장에서 각광받으며 폭넓게 도입되고 있는 주요 이유는 다음과 같다.

① VPN은 낮은 비용으로 고비용의 전용회선을 대체함으로써 비용 절감 효과가 탁월하다.

② VPN은 표준화된 기술로서 개방적인 인터넷 하부 구조와 암호화 및 인증 프로토콜을 이용하여 전송되는 모든 데이터에 대해 신뢰성 있는 통신을 보장한다.

③ 기업의 비즈니스 영역이 확장됨에 따라 비즈니스 파트너나 고객과의 상호 접속 요구도 지속적으로 증대하고 있는데, 기업 네트워크가 인트라넷(Intranet), 엑스트라넷(Extranet)으로 확장되더라도 VPN은 유연한 적용이 가능하다.

④ VPN은 침입차단시스템(Firewall)이나 침입탐지시스템(Intrusion Detection System : IDS) 등의 타 보안 장비와 상호 운영성이 뛰어나며, 이들 솔루션과 통합되어 더 높은 수준의 보안체제를 구축할 수 있다.

2.2 VPN 보안 기술

VPN의 기본 개념은 터널링(Tunneling)으로 시작 지점에서 목표 지점까지 가상 터널을 생성

하고, 생성된 터널을 안전하게 관리하는 암호화/인증 프로토콜 및 키 관리 프로토콜이 VPN의 핵심 기술이라고 할 수 있다.

2.2.1 터널링 기술(Tunnelling)

VPN은 터널링 기법이라 대변될 만큼, VPN에 있어서 터널링 기술은 중요하다. 터널링이 중요한 이유는 어떠한 페이로드라도 수용할 수 있으며 GRE(Generic Routing Encapsulation)를 사용하여 여러 사용자가 동시에 다양한 형태의 페이로드(payload)를 액세스할 수 있다. 또한 VPN을 사용하는 기업은 그들의 IP 주소를 망에 알리지 않고 사용자가 기업에 액세스할 수 있도록 하며, 기업이 각각의 터널 연결을 필터링할 수 있게 한다.

VPN 터널링 기술의 가장 보편적인 형태는 네트워크 프로토콜(예: IP, IPX)을 PPP에 캡슐화한 다음 그 패킷을 다시 터널링 프로토콜에 캡슐화 하는 방법인데, 이 접근 방법은 터널링 프로토콜이 계층 2 프로토콜을 전송하므로 계층 2 터널링(L2T: Layer 2 Tunneling)이라고 한다.

또다른 방법은 네트워크 프로토콜을 직접 터널링 프로토콜로 캡슐화하는 방법으로서, 이 방법은 계층 3 터널링(Layer 3 Tunneling)이라고 한다[2].

표 1은 터널링 프로토콜을 OSI 계층에 따라 분류하고 특징을 비교 설명한 것이다[3].

표 1. 터널링 프로토콜 기술 비교
Table 1. The Comparison of Tunnel Protocol technology

	2계층	3계층	MPLS
프로토콜	PPTP, L2F, L2TP	IPSec	MPLS
모드	클라이언트-서버	호스트-호스트	호스트-호스트
캡슐화 프로토콜	IP, IPX, AppleTalk등	IP	IP
인증, 암호화	비표준화, 자체지원	IPSec	비표준화
특징	PPP 기술 활용	다중서비스 지원	QoS 제공

터널링은 캡슐화(Capsulation), 전송(Transmission), 그리고 디캡슐화(Decapsulation) 과정을 포함하며, 기본 개념은 그림 1과 같다.

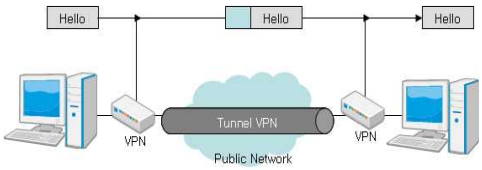


그림 1. VPN 터널링 개념
Fig. 1 VPN Tunneling Conception

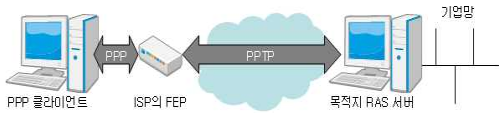
(1) 2계층 터널링

OSI 참조 모델에서 데이터링크 계층인 2계층 터널링 기법은 가장 보편적인 형태로 대부분 IPSec 이전의 VPN 기술로 IP나 IPX 패킷을 PPP에 캡슐화한 후, 다시 터널링 프로토콜로 캡슐화하는 형태를 사용한다. 2계층 터널링 기법은 비용면에서 효율적이며, 다중 프로토콜 전송, 원격 네트워크 접속 기능을 제공한다. 그러나 자체적으로 신뢰성 있는 보안 수준을 제공하지 못하므로, 다른 계층의 프로토콜과 복합적으로 사용되는 특성이 있다. 대표적인 예로 PPTP, L2TP, 그리고 L2F와 같은 프로토콜이 있다.

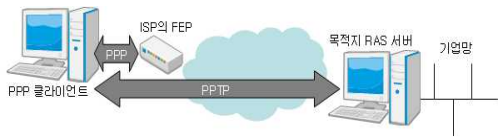
① PPTP(Point-to-Point Tunneling Protocol)

마이크로소프트사가 개발한 방법으로서, IP, IPX 또는 NetBEUI 트래픽을 암호화 하고, IP 헤더로 캡슐화하여 인터넷을 경유하여 전송한다. PPTP는 터널링을 유지하기 위해 TCP 연결을 사용한다.

PPTP는 그림 2와 같이 2가지의 터널링 방식이 있다[2].



(a) Voluntary 터널링



(b) Compulsory 터널링
그림 2. PPTP 터널링
Fig. 2 PPTP Tunneling

Voluntary 터널링은 PPP클라이언트가 ISP의 FEP(Front End Processor)와 PPP세션을 설정한다. 여기서, FEP는 원격사용자가 모뎀이나 ISDN을 사용하여 액세스하는 라우터나 브릿지를 말한다. FEP는 사용자로부터 RAS(Remote Access Server)로의 연결을 요청 받으면, RAS와 PPTP 세션을 열어 클라이언트로부터의 모든 데이터를 PPTP를 통해 전송한다.

Compulsory 터널링은 클라이언트가 PPTP 기능을 가진 경우로서, 먼저 사용자가 FEP로 다이얼업하여 PPP세션을 설정한다. 그리고 나서 RAS와 PPTP 연결을 설정하기 위해 PPP세션과 함께 RAS로 다시 2번째 다이얼업을 수행한다. 클라이언트와 서버간의 데이터는 새로 생성된 PPTP세션을 통해 전송된다.

L2TP와의 차이는 사용자가 PPP 협상이 끝난 후에 PPTP 서버를 선택하는 것이 가능하므로, 클라이언트의 변화없이 터널의 끝점이 자주 바뀔 때 유용하다. PPTP는 서비스제공자에게 투명하게 전송되므로 서비스 제공자는 PPTP서버를 가질 필요가 없고 진보적인 구성을 요구하지 않는다. 또한, 클라이언트는 어느 곳에서든지 터널을 생성하여 송신할 수 있어 On-Demand 가상회선처럼 보일 수 있다[2].

② L2F(Layer 2 Forwarding)

L2F는 시스코에서 독자적으로 제안한 기술로 IP나 ATM, 프레임릴레이 네트워크를 사용한다. 액세스 서버가 접속 트래픽을 PPP로 프레임화하고 WAN 접속을 통해 L2F 서버나 라우터로 전송하는 방식으로 동작하고, PPTP나 L2TP와는 달리 사용자가 별도의 소프트웨어를 필요로 하지 않다. 또한, L2F는 IP헤더가 아니라 전용헤더로 캡슐화하며, 특별한 인증절차를 규정하지 않으므로 액세스 서버는 단지 주어진 도메인과 사용자 ID가 VPN 사용자인지 여부만을 검증하는 특징을 가지고 있으나 데이터 암호화 기능이 미약하고, 상호 호환성이 떨어진다는 단점이 있다[4].

③ L2TP(Layer 2 Tunneling Protocol)

PPTP와 L2F의 장점만을 결합한 기술로 PPP를 기반으로 하고 있으며, IETF에서 산업표준(RFC 2661)으로 정의한 프로토콜이다. L2TP는 주로 IP, IPX, NetBEUI 트래픽을 암호화하고 IP 헤더로 캡슐화하여 인터넷이나 X.25, 프레임릴레이나 ATM 네트워크를 통해 전송한다. IP를 데이터그램 전송에 사용할 경우 인터넷에서 터널링 프로토콜로도 사용할 수 있다. 현재 RAS와 라우터를 비롯한 대부분의 NAS(Network Access Server) 장비는 기본적으로 L2TP 기능을 지원하며 프레임릴레이 네트워크에서도 사용이 가능하다[4].

L2TP는 NAS가 터널을 설정하는 방법을 제공하므로 먼저 클라이언트가 NAS에게 다이얼업하면 NAS는 성공적으로 인증을 받은 사용자에 대해 L2TP 터널을 미리 결정된 종단점으로 동적으로 설정한다. 서비스 제공자가 세션이 끝나는 곳을 제어하므로 서비스 제공자는 투명하게 데이터를 전송하여야 한다. 서비스 제공자는 모뎀풀을 제공하여 가입자별로 다른 목적지로 포워딩한다. 즉, 포워딩의 결정은 NAS에서 이루어지므로 가입자에게 정적으로 IP주소를 할당하는 것은 비효율적이다. L2TP 규격이 구체적이지 않아 많이 구현되어 있지 않은 단점이 있다.

PPTP와 L2TP는 모두 데이터를 PPP로 캡슐화하고 추가 헤더를 덧붙여 망으로 전송한다. 따라서 2개의 프로토콜은 매우 유사하지만 표 2와 같은 차이가 있다[2].

표 2. PPTP와 L2TP의 비교
Table 2. The Comparison of PPTP and L2TP

	PPTP	L2TP
지원 프로토콜	IP	IP, FR, X.25, ATM 등
엔드포인트 사이에 지원되는 터널 수	한개	여러 개
헤더 압축	지원안함	지원함
터널인증	지원안함	지원함

(2) 3계층 터널링(IPSec)

3계층 터널링의 대표적인 프로토콜은 IPsec, VTP 등이 있다. 특히, IPSec은 보안에 취약한 IP 프로토콜에서 안정성 있는 서비스를 제공하기 위해 IETF 워킹그룹에서 표준(RFC2401

-2412)으로 제정한 보안 프로토콜로 현재 VPN의 핵심 프로토콜이라 할 수 있다.

IPsec은 시스템으로 하여금 보안 프로토콜을 선택하고, 암호화 알고리즘을 결정하며, 또 암호화키를 결정할 수 있게 함으로써 IP계층에서 보안 서비스를 제공할 수 있도록 한다. IPsec은 두 호스트 사이, 두 보안 게이트웨이 사이, 또는 보안 게이트웨이와 호스트사이의 통신을 보호하기 위해 사용할 수 있다. IPsec이 제공할 수 있는 보안서비스는 접근제어, 무결성, 데이터 출처 인증, 재연된 패킷의 거부, 기밀성 그리고 제한된 트래픽 흐름 기밀성이다. 이 서비스들은 IP계층에서 제공되므로 TCP, UDP, ICMP, BGP 등과 같은 상위 계층 프로토콜에 의해 사용될 수 있다.

IPsec은 보안 서비스를 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)의 두 프로토콜을 사용하여 이들 프로토콜이 제공하는 보안 서비스들은 다음과 같다[2].

① AH는 무결성, 데이터 출처 인증을 제공하며 선택적으로 재연 공격에 대한 보호 서비스도 제공한다.

② ESP 프로토콜은 암호화를 통한 기밀성과 제한된 트래픽 흐름 기밀성을 제공한다. 또한, 기밀성, 데이터 출처 인증과 재연 공격에 대한 보호 서비스도 제공한다.

③ AH와 ESP는 함께 사용되었을 때 접근제어 서비스로 제공한다.

IPSec의 동작은 크게 Transport Mode와 Tunnel Mode로 나뉜다. Transport mode는 End-to-End Tunneling에, Tunnel Mode는 Gateway-to-Gateway Tunneling에 주로 사용되며, 각 모드는 Security Policy에 따라 AH alone, ESP alone 혹은 AH with ESP 등의 다양한 Security Protocol이 사용될 수 있다. 또한 필요에 따라서는 이 두 모드를 중첩 사용함으로써 다양한 Security Policy를 구현할 수도 있다.

그림 3은 IPSec의 Gateway-to-Gateway Tunneling인 Tunnel Mode의 AH와 End-to-End Tunneling인 Transport Mode인 ESP의 구조를 설명한 것이다.

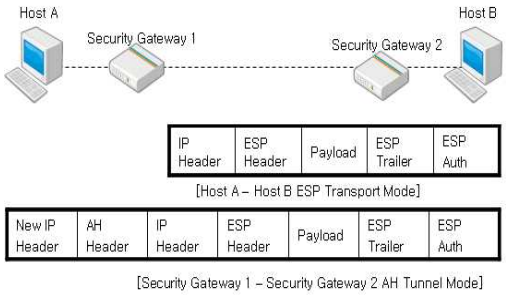


그림 3. IPSec Protocol
Fig. 3 IPSec Protocol

IPSec의 layer 3 tunneling과 PPTP/L2TP의 layer 2 tunneling의 장단점을 비교해 보면 다음과 같다.

① PPTP/L2TP는 Non-IP Traffic의 Tunneling도 가능하지만 IPSec은 IP Tunneling만을 지원한다. 따라서 IP 외의 다양한 Network Protocol을 사용하는 Intranet에 대한 Remote Access를 위해서는 PPTP/L2TP를 지원해야 한다.

② PPTP/L2TP는 Per-User-Authentication, Dynamic Address Allocation 등이 가능하나, IPSec은 기본적으로 Host-to-Host (Machine-to-Machine) Authentication을 지원하며, Fixed, Routable IP Address를 가정한다. Tight Access Control을 위해서는 User Authentication이 필수적이므로 대부분의 IPSec vendor들은 자체의 User Authentication Solution을 제공하고 있다. 표준화 작업이 계속 진행됨에 따라 IPSec에서도 User Authentication 및 다른 Token-based Authentication을 위한 표준을 지원할 가능성이 높다.

③ IPSec은 Per-Packet Encryption/Authenti-cation, Automated Key Management 등 Network Layer Security를 위한 Open Framework을 제공하지만, PPTP/L2TP는 단지 PPP Tunnel의 생성, 소멸, 관리를 주로 하며 PPP가 제공하는 외의 자체적인 Security 기능이 거의 없다. 따라서 PPTP/L2TP는 Security를 위해 IPSec과 함께 사용하는 것이 바람직하다.

2.2.2 인증

원격접속 VPN 사용자는 고정된 위치가 아닌

이동이 가능한 사용자로, 초기 VPN접속을 시도할 때 보안서버로부터 인증을 받아야 한다. 이를 위한 방식으로 상호 독립적인 Peer-Peer 방식과 주종의 관계를 갖는 Client-Server 방식이 있다[5].

(1) Peer-Peer 방식

독립적인 2개의 호스트 간에 요청 및 응답을 통한 사용자 인증을 수행하는 방식으로, PAP과 CHAP이 있다.

PAP(Password Authentication Protocol)은 two-way handshaking 방식으로 인증을 요청하는 호스트에서 사용자ID와 패스워드를 일반 텍스트 형태로 전달한다. 반면 CHAP(Challenge Handshake Authentication Protocol)은 three-way handshaking 방식으로 인증서버는 호스트로 challenge 메시지를 보내면, 호스트는 보안을 위해 해쉬 함수를 사용하여 계산한 값을 보내고 그런 다음 인증서버는 값이 일치하면 인증하는 방식이다.

(2) Client-Server 방식

보안 관리 기능에 대해 좀 더 편리하고 유연하게 제공하기 위한 방식으로 TACACS (Terminal Access Controller Access-Control System)와 RADIUS(Remote Access Dial-In User Service)가 있다. TACACS는 인증에 필요한 사용자ID, 패스워드, PINs 및 암호키 정보를 인증서버에서 데이터베이스 형태로 관리하며, 클라이언트로부터의 인증 요청을 처리한다.

RADIUS는 사용자 인증 이외에도 사용자 연결 관리를 위해 NAS와 연동하여 인증 시스템을 구성한다. NAS는 사용자가 네트워크로의 접속을 제공하는 서버 기능을 제공하면서 동시에 RADIUS에 대해 클라이언트 역할을 수행한다.

Client-Server방식은 PAP과 CHAP 인증을 지원하고, 다른 인증 시스템에 대해 Proxy 서버 역할도 지원함으로써, Peer-Peer방식에 비해 좀 더 유연하고 신뢰성 있는 인증 기능을 제공한다.

2.2.3 VPN 기술의 단점

지금까지 살펴본 VPN 기술들은 급속히 변하고 있는 기업 환경에 비추어 볼 때 다음과 같은 부족한 점이 있다.

① 기존의 VPN 터널링 기술들은 기업 외부에서 모뎀을 사용하여 홈 네트워크에 접속하는 Dial-up VPN 위주로 설계되었다. 그러나 시스템통합 산업이 활발해지면서 지사 또는 협력사들이 LAN 환경을 구축하고, 본사와 주고받는 트래픽이 증가함에 따라 기존의 Dial-Up VPN으로는 사용량을 감당하기 어려워졌다. 즉 LAN을 직접 연결할 수 있는 VPN 기술이 요구된다.

② 인터넷 망에서는 IP 헤더를 통해 QoS(Quality of Service)가 일부 가능하였다. 그러나 VPN 사용시 IP 패킷이 캡슐화되어 별도의 헤더를 통해 전송되므로 IP의 헤더에 있는 기능들을 사용할 수가 없다. 따라서 사용량이 많아져 전체적인 전송속도가 느려질 경우, 중요 패킷에 대한 우선권을 부여하는 QoS의 기능을 지원할 수 없다.

③ VPN 기술들을 공공망을 사설망처럼 사용하는 기술이니 무엇보다도 보안에 많은 신경을 써야 한다. 전송되는 IP 패킷에 대한 보안을 위해, 보내고자 하는 본래 IP 패킷을 캡슐화하여 다시 IP 헤더를 추가하여 전송함에 따라, 원시 데이터에 대한 전송 효율이 낮아지게 되고, IP패킷을 사용함에 따른 위험성은 여전히 남아 있다.

2.3 전용회선

전용 회선은 특정 목적을 위해서 사용되는 회선으로서, 통신회선의 일부를 특정업체나 개인이 독점적으로 사용하는 회선 서비스를 말한다.

전용 회선은 아날로그 전용회선과 디지털 전용회선으로 나눌 수 있다.

아날로그 전용회선은 전화나 광대역통신, 라디오 방송회선으로 분류한다. 특히, 전화급 회선은 음성통신을 위해 만들어진 회선으로 직통전화나 구내교환 설비 또는 FAX 회선으로 많이 사용하며, 모뎀 등을 연결하여 데이터 통신을 위해 사용할 수도 있다.

디지털 전용회선은 회선을 통한 데이터 전송

방식과 장비가 모두 디지털 방식으로 현재 사용하고 있는 전용회선 대부분이 디지털 전용회선을 이용하고 있다. 디지털 전용회선은 원거리 전송시에도 디지털 신호를 샘플링하여 에러를 정정 및 보상하기가 쉽고 기술이 간단하여 유지 및 관리가 쉬운 장점을 지니고 있다. 디지털 전용회선은 연결된 지점만이 전용회선을 사용할 수 있는 데이터 전용회선과 LAN에 연결된 모든 컴퓨터들은 언제든지 인터넷을 사용할 수 있도록 연결된 회선인 인터넷 전용회선을 나눌 수 있다.

전용회선은 다음과 같은 특징을 가지고 있다.

① 시간에 관계없이 24시간 사용할 수 있다.
② 지점과 지점이 직접 연결되어 있으므로 연결 장애가 발생하지 않는다.
③ 다수의 이용자가 공동으로 사용하는 공중망 서비스와 달리 특정 두 지점 간에 연결된 전송로를 독립적으로 사용하므로 보안성과 안정성이 높다.
④ 전송량과 관계없이 정액요금제를 적용하므로 이용 빈도가 많을 때 적합하다.
⑤ 고객의 통신 방법과 용도에 따라 독자적인 망 구축이 가능하다.
⑥ 전송하고자 하는 데이터의 종류에 따라 전화, FAX, 이미지전송, 인터넷 방송 등으로 사용자의 환경에 맞추어 사용할 수 있다.

2.3.1 전용회선 장비

전용회선에 사용되는 장비는 전용회선의 속도에 따라 분류하고, 전용회선의 종류는 IPS 업체의 속도에 따라 9.6Kbps, 56Kbps, 128Kbps, 256Kbps, 512Kbps, 1544Kbps(T1), 2048Kbps (E1) 으로 나누어진다.

장비 중에서 9.6Kbps~56Kbps에서는 DSU가 사용되지 않지만, 128Kbps 이상에서는 아래의 장비가 꼭 사용되는 것은 아니다. 특히, 요즘에는 HSM 장비가 단종되고 FDSU로 구성을 많이 하게 되는데, FDSU는 상당히 높은 속도까지 처리할 수 있다. 그리고 HDSL이나 O/R를 가지고 구성을 할 때에는 뒷단에 CSU 장비를 연결한 다음 라우터에 연결하여야 한다.

전용회선에 사용되는 장비를 전용회선의 속도에 따라 분류해보면 표 3과 같다.

표 3. 전용회선 장비
Table 3. Dedicated Lines equipment

속도	장비명
9.6Kbps ~ 56Kbps	DSU (Data Service Unit)
128Kbps ~ 256Kbps	HSM (High Speed Modem), FDSU(T1까지 수용)
384Kbps이상	CSU (Channel Service Unit), FDSU, HDSL, OR 등

(1) DSU(Data Service Unit)

DSU는 Digital Service Unit 또는 Data Service Unit이라고 한다. 보통 PC에서 많이 사용하는 MODEM은 아날로그 회선에서 사용하며 디지털 데이터를 아날로그 신호로 바꾸거나, 아날로그 신호를 디지털 신호로 바꾸는 기능을 하듯이, DSU는 디지털용 회선에 사용하는 장비로서 디지털 데이터를 디지털 신호로 변화해주는 역할을 한다. 그래서 Digital Service Unit이라고도 부르기도 한다.

(2) HSM(High Speed Modem)/FDSU(Flexible Data Service)

고객이 점차 많은 데이터 전송이 요구함에 따라 많은 데이터 전송이 필요해지면서 56K 이상의 전용회선을 사용하게 됨에 따라 고속 데이터 전송용으로 나온 것이 HSM이다.

HSM/FDSU는 최대 12개 채널, 즉 768Kbps까지의 속도를 지원할 수 있는 장비이며, 기본적인 전송 방법은 DSU와 같다. 그러나 동시에 다수의 채널을 이용할 수 있도록 제작되었기 때문에 속도를 768Kbps까지 낼 수 있다.

HSM은 에러의 보정 및 정정 기능이 없기 때문에 잘 사용되지 않으며, FDSU가 HSM을 거의 대체하고 있는 추세이다. 56/64Kbps에서도 사용이 가능하나, DSU에 비해 가격이 고가이므로 128Kbps 이상에서 사용하는 것이 보통이다.

(3) CSU(Channel Service Unit)

1 채널은 64Kbps의 전송속도를 가지는데 흔히 많이 사용하는 56K/64K는 1 채널을 사용하

는 것을 의미한다. 마찬가지로 128K는 64×2=128이므로 두 개의 채널을 사용하는 것이다. 256K, 512K도 마찬가지로 전송로에 할당된 채널이 4개, 8개 이다. 그래서 속도에 따라 몇 개의 채널을 사용하는가를 말할 수 있다.

실제로 전송할 때, 각각의 단 채널들이 따로 따로 전송되는 것이 아니라, 먹스라 불리 우는 집중장비가 여러 개의 채널을 모아서 하나의 대용량 전송로를 통해 한꺼번에 전송되는데 이것을 트렁크 방식이라 한다. CSU는 바로 이러한 트렁크 라인(T1이나 E1)을 그대로 수용할 수 있는 장비를 말한다. 전송방식의 차이로 T1은 24채널을 수용하고 E1은 30채널을 수용할 수 있다. 연결된 T1이나 E1 전송로는 CSU 옵션에 따라 채널수가 정해지고, 정해진 채널수에 따라 그에 따르는 전송로의 전송속도가 결정된다.

(4) HDSL(HighSpeed Digital Subscriber)

HDSL도 FDSU, CSU와 동일한 기능을 수행하며, FT1(Fractional T1)용, T1용, E1용 등으로 나누어져 있다.

2.3.2 전용회선 서비스 방식

전용회선을 통신사업자가 제공하고 있는 서비스 방식을 분류해보면 METRO ETHERNET, 무선랜 방식, LS방식, TDM 방식이 있는데, 특별히 보안을 강조하는 은행 같은 경우에는 FR 또는 LS와 같은 서비스를 사용한다[6].

(1) METRO ETHERNET 방식

기업이나 기관, 개인 사용자의 근거리 통신망과 지역 통신사업자의 공중 통신망을 광 케이블로 연결, 대도시 기반의 단일한 통신망을 구축하여 랜으로 데이터를 전송하는 방식입니다. TDM방식(E1, T1)과 가장 다른점은 1Mbps~1Gbps 대역까지 1M 단위로 라우터 없이 서비스 제공이 가능하다는 것이다.

METRO ETHERNET 방식을 제공하는 서비스는 DACOM 보라파워넷비즈와 KT-KORNET EXPRESS가 있다.

(2) 무선랜 방식

최근 무선 장비(AP, 랜카드 등) 기술 발전에 힘입어 기업에서 무선랜으로 구축하고자 하는 수용가 빠르게 증가하고 있다. 광케이블이 기업 내부까지 인입되고 AP를 통해 구내 무선랜이 하나로 통합되어 원스톱으로 제공되는 보다 편리하고 유용한 서비스이다. 이동이 잦은 기업, 회의실 활용이 많은 기업, 노트북 사용이 많은 기업, UTP 회선 관리가 힘든 기업, 이전 또는 신축 건물에 따른 신규 유선회선 구축이 필요한 기업 등에 유/무선 통합 서비스를 제공하는 서비스 방식이다.

무선랜 방식을 제공하는 서비스는 DACOM-AIRLAN POWER, KT-NESPOT BIZ INTRA가 있다.

(3) LEASED LINE 방식

LEASED LINE 방식은 고객이 원하는 두 지점간에 독립적으로 통신사업자로부터 회선을 임차하여 멀티미디어 정보(음성, 데이터, FAX, 영상)를 24시간 독점적으로 빠르고 정확하게 송수신할 수 있는 서비스이다. 다수의 이용자가 공동을 사용하는 공중망 서비스와 달리 특정 두 지점간에 연결된 전송로를 독립적으로 사용하므로 보안성과 안정성이 높은 서비스이다. 따라서 금융권이나 높은 보안 수준을 필요로 하는 기업이 국내 및 국제 구간 등에서 사용하고 있다.

LEASED LINE 방식을 제공하는 서비는 DACOM-DLS, KT-LS가 있다.

(4) TDM 방식

TDM(Time Division Multiplexing)이란 시분할 다중화를 의미하는 것으로 전송로의 자료 전송 시간을 일정한 시간으로 나누어 차례로 분배함으로써 몇 개의 저속 서브 채널이 1개의 고속 전송선을 나누어 이용하는 방식이다. 2002년 메트로이더넷 방식의 서비스 개시전까지 주로 사용해 오던 방식으로 현재는 56Kbps, 126Kbps 같은 저속급이나 45Mbps, 155Mbps와 같은 고속급에서 일부 사용하고 있다.

TDM 방식을 제공하는 서비스는 DACOM-보라넷, KT-KORENT HOTLIME이 있다.

Ⅲ. VPN과 전용회선의 비교 분석

3.1 IPSec VPN

IPSec VPN은 광대역 서비스를 기반으로 보안망을 구축하는 기업의 유일한 솔루션으로 확고한 위치를 확보한 상태며, 서비스의 형태는 사이트 투 사이트, 사이트 투 클라이언트로 분리할 수 있다. IPSec VPN은 다양한 암호화 기법(DES, 3DES, AES, RC4)과 데이터 무결성 기법(MD5, SHA-1)을 지원하며, 네트워크 레이어에서 암호화 서비스를 위해 터널링을 구축하는 기술이다.

그림 4는 IPSec VPN의 기본 구조를 설명한 것이다. 다만 일반적으로 IPSec VPN은 방화벽 기능을 함께 제공하는 제품이 많이 있기 때문에 별도의 방화벽을 설치하지 않는 경우가 많다.

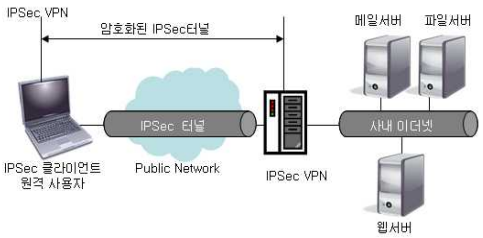


그림 4. IPSec VPN
Fig. 4 IPSec VPN

(1) IPSec VPN의 장점.

IPSec VPN의 장점을 살펴보면 다음과 같다.

① IPSec VPN은 IPSec 프로토콜을 사용하며, 정의된 암호화와 패킷 터널링 규격을 적용해 물리적인 네트워크에 대한 논리적 통신 오버레이를 제공한다. 즉, 다양한 암호화 기법(DES, 3DES, AES, RC4)과 데이터 무결성 기법(MD5, SHA-1)을 지원한다.

② IP 계층에 근접하는 IPSec VPN은 애플리케이션과 무관하게 동작하며 다양한 애플리케이션을 지원할 수 있다

③ IPSec VPN 게이트웨이는 일반적으로 네트워크 방화벽 기능과 통합되고, IPSec 클라이언트 솔루션은 개인 방화벽 및 다른 보안 기능을 통합할 수 있다.

④ IPSec VPN은 데이터의 기밀성을 유지하기 때문에 패킷이 도청되거나 잘못된 대상에게 전달된다해도 의도한 수신자만이 암호를 해독할 수 있다.

⑤ IPSec 인증 방식은 메시지 무결성을 제공하기 때문에 데이터가 네트워크 경로를 통과하는 동안 조작되거나 수정되지 않았음을 수신자가 확인할 수 있다.

(2) IPSec VPN 단점

IPSec VPN의 단점을 살펴보면 다음과 같다.

① 클라이언트 VPN은 데스크톱이나 노트북에 반드시 클라이언트 소프트웨어 설치가 필요하다.

② 클라이언트에 대한 패치 및 보안 관리가 필요하다.

③ 클라이언트의 각종 하드웨어에 대한 호환성에 문제가 있다.

④ 사내에 접근 가능한 자원들에 대해 방화벽에서의 추가적인 설정이 필요하다.

⑤ IPSec VPN을 이용한 구축은 사이트 투 사이트(Site-to-Site), 사이트 투 클라이언트(Site-to Client)의 두 가지 방식으로 이뤄지고 있으며, 사이트 투 사이트 경우는 매우 안정적인 보안 서비스를 제공한다. 반면 사이트 투 클라이언트는 원거리상의 모든 컴퓨터상에 VPN 클라이언트 소프트웨어를 설치, 관리 및 유지보수를 해야 하는 어려움으로 도입에 많은 걸림돌이 되고 있다.

3.2 MPLS VPN

MPLS는 IETF와 ATM 포럼을 중심으로 개발된 2계층 스위칭 기법과 3계층 라우팅 기술을 접목한 새로운 스위칭 기법으로 고정된 길이(4byte)의 레이블(Label)을 이용하여 고속 라우팅을 구현한다. 네트워크 송수신 패킷에 레이블을 부여하고 스위칭 장비에서 이 레이블을 읽어 패킷의 전송 경로를 결정함으로써, 패킷 지연 시간을 대폭 감소할 수 있다. 이외에 자체적으로 트래픽 관리 기법이나 VPN, 그리고 QoS 기

능 지원이 뛰어나다는 것이 특징이다.

MPLS VPN은 MPLS 기술을 IP VPN에 적용한 기술로서 라우터와 네트워크를 기반으로 VPN 서비스 제공이 가능하다. MPLS가 제공하는 트래픽 관리 기술을 기반으로 기존 IPSec VPN의 취약점인 서비스 품질과 안정성 문제를 극복할 수 있어 ISP에게는 새로운 부가 서비스로 주목받고 있다. 현재 MPLS 기술은 IETF가 주도하고 있으며, 이더넷을 중심으로 ATM 네트워크를 수용하는 방향으로 발전하고 있는데, 인터넷의 문제점인 대역폭 증가, 라우팅 증가, QoS 문제를 해결할 수 있는 현실적인 대안으로 인식되고 있다. 특히, MPLS 기반 VPN 서비스는 고정된 길이의 레이블을 이용하여 데이터를 전송하므로 ATM 셀과 IP 패킷 모두 수용 가능하며, 따라서 기존 ATM 기반 VPN에서의 IP와 ATM의 복잡한 주소 변환 체계가 필요 없다는 장점을 지니고 있다.

MPLS VPN은 기존의 IP VPN 방식이나 IP over ATM 방식에 비해 많은 장점을 가지고 있으므로, 향후에는 MPLS 네트워크가 점차 이들 기술을 흡수하거나 대체해 나갈 것이라는 전망이 우세하다.

MPLS VPN은 계층에 따라 터널링 중심의 L2 MPLS VPN과 BGP 기술이 중심인 L3 MPLS VPN으로 나뉘어진다. 각각의 특징을 살펴보면 다음과 같다[7].

① L2 MPLS VPN

기존의 Frame Relay, ATM VPN 가입자를 쉽게 수용할 수 있고 IP이외의 프로토콜 수용이 쉬우며, 망 제공자가 VPN 가입자들의 라우팅 정보를 관리하지 않으므로 구조가 단순해지고 관리가 쉬워지는 장점이 있다. 즉, L2 MPLS VPN은 단지 캐리어의 역할만 수행하던 망제공자가 네트워크의 고도화를 위해 MPLS 기술을 적용하고 VPN 서비스를 제공하는데 적합하지만, 확장성 측면에서는 L3 MPLS VPN에 비해 떨어지는 단점이 있다.

가입자의 장비가 접속되는 통신 사업자 측의 라우터를 PE (Provider Edge) 라우터라고 하며, 가입자의 라우터를 CE(Customer Edge) 라우터라고 한다. 다시 말하면 MPLS 네트워크를 경유해 패킷을 전달하는 것은 MPLS 레이블에 의존하고 PE 라우터에서 CE 라우터로 전달하는 것은 VPN 레이블에 의존하는 것이다.

그림 5는 L2 MPLS VPN 구조를 설명한 것이다.

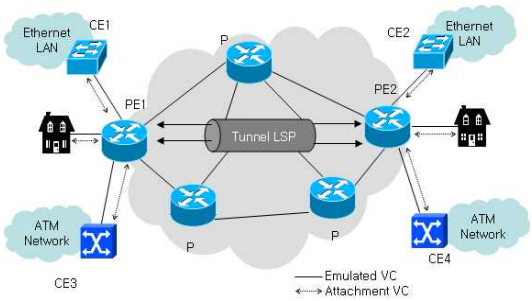


그림 5. L2 MPLS VPN
Fig. 5 L2 MPLS VPN

② L3 MPLS VPN

L3 MPLS VPN는 peer 모델로써 확장성이 뛰어나고, VPN을 동적으로 쉽게 생성할 수 있으며, 기존의 인터넷 고객을 거의 변화 없이 수용할 수 있는 장점을 가지는 반면, VPN 고객의 라우팅 정보를 관리해야 하고 공중망 전송시 암호화기능이 약한 단점을 갖는다. 즉, L3 MPLS VPN은 가입자들의 네트워크 관리 부담을 덜어주며 MPLS 기반으로 하기 때문에 VPN 확장성 및 유연성이 우수하다. 또한 망제공자들이 매우 뛰어난 부가 서비스를 제공할 수 있도록 해주며, 여러 망제공자들의 네트워크를 통해 VPN을 구축할 수 있는 장점을 갖는다.

그림 6은 L3 MPLS VPN의 구조를 설명한 것이다.

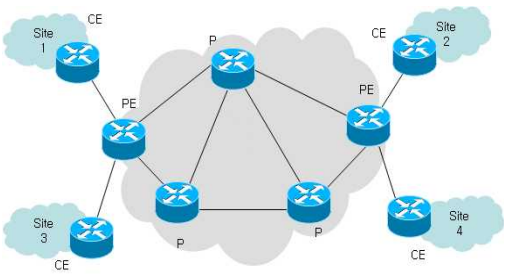


그림 6. L3 MPLS VPN
Fig. 6 L3 MPLS VPN

(1) MPLS의 장점

MPLS VPN은 가상랜 기반의 VPN이 갖는 제한 요인 대부분을 극복할 수 있는 해결책을 제공하며, 다음과 같은 장점을 갖는다.

① VPN 레이블은 20비트로 구성되어 있으므로 약 100만개 이상의 VPN을 서비스할 수 있다.

② MPLS 네트워크 안의 백본 라우터들이 VPN 가입자와 관계된 직접적인 정보들을 모두 관리하지 않아도 된다. 따라서 가입자가 많아지더라도 확장성이 큰 영향을 받지 않는다.

③ 링크 장애시 우회경로로 신속히 트래픽을 우회시킬 수 있으며, STP 운영에서 문제가 됐던 링크 대역의 낭비 현상이 발생하지 않게 된다.

④ 가입자의 가상랜 ID 혹은 네트워크 어드레스의 중복을 허용하므로 고객의 요구사항에 유연하게 대처할 수 있다.

⑤ 가입자간에 논리적인 회선과 유사한 레이블 스위치 패스(LSP)를 제공할 수 있고, 그것을 활용해 QoS 및 트래픽 엔지니어링 기능 등을 제공할 수 있다.

(2) MPLS VPN의 단점

MPLS VPN은 가상랜 기반의 VPN이 갖는 제한 요인 대부분을 극복할 수 있는 해결책을 제공하지만 MPLS VPN을 제공하는데 전혀 장애사항이 없는 것은 아니다. MPLS VPN 서비스의 문제점으로는 다음과 같다[8]

① 투자비용 : MPLS 기능을 제공할 수 있는 장비들은 MPLS 기능을 제공하지 못하는 장비에 비해 상대적으로 비싸기 때문이다. 그러나 2~3년 전까지만 하더라도 MPLS 기능을 가진 장비를 제공하는 회사가 많지 않았으나 최근 점차 증가하면서 투자비용 역시 크게 하락하고 있는 추세이다.

② 운영비용 : MPLS기반의 VPN을 서비스하기 위해 관리 소프트웨어 등을 재개발하고 운영 인력을 새롭게 교육해야 하기 때문이다. 그러나 MPLS 네트워크가 기반을 잡은 뒤에 그것을 이용하여 VPN, 전용 회선 서비스 및 기타 다른 서비스와 통합해 제공하게 된다면 오히려 별개의 네트워크를 운영하면서 요구되는 투입 비용을 절감할 수 있을 것이다.

③ 장비간의 호환성 문제 : 이미 MPLS와 관련한 기술 표준은 많이 완료되었고, MPLS 장비간의 호환성 시험도 이루어져 왔으나, 실제 복잡하게 얽혀있는 서비스 네트워크에서 테스트된 경우는 많지 않기 때문이다.

3.3 전용회선

(1) 인터넷 전용회선

인터넷 전용회선은 일반 가정이 아닌 게임방이나 사무실 등 컴퓨터의 대수가 많은 환경에서 안정적인 속도를 보장받기 위해 사용되고 있으며, 한국통신(KT)과 데이콤 등에서 전용회선 서비스를 제공한다. 인터넷 전용회선은 ISP업체와 사용자 사이를 전용회선으로 연결 후 가입자 측 컴퓨터에 CSU, 라우터, 허브/스위치로 연결해 사용하므로 컴퓨터가 많아도 안정적인 속도를 보장 받고, 일반 가정의 초고속 인터넷이 유동 IP를 부여하는 서비스인 반면 인터넷 전용회선은 고정 IP를 부여 받아 서비스를 이용하므로 웹 서버나 FTP 서버와 같은 여러 가지 하위 네트워크 구성도 가능하다. 또한 ISP와 가입자를 전용회선으로 연결하므로 주변의 다른 가입자의 사용유무에 관계없이 항상 일정한 속도의 서비스를 받을 수 있으며 고정 IP를 사용하므로 웹 서버나 FTP서버와 같이 여러 가지 하위 네트워크 구성도 가능하다[9].

그림 7은 인터넷 전용회선을 이용한 대표적인 망 구성을 설명한 것이다[9].

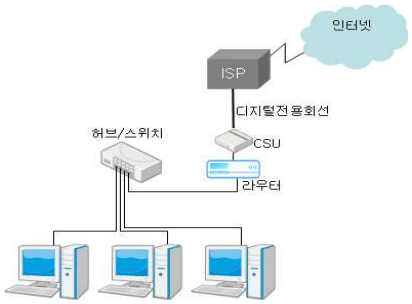


그림 7. 인터넷 전용회선 망
Fig. 7 Internet Dedicated Lines Network

(2) 케이블 모뎀 인터넷

케이블 모뎀 방식은 케이블 TV 방송을 위해 설치된 광케이블 망을 이용한 접속 방식이다. 그러다 보니 광케이블이 설치되지 않은 지역에서는 서비스를 받을 수 없다.

인터넷 서비스를 위한 케이블 TV 회선의 실제 대역폭은 하향으로 최고 27Mbps, 상향으로 2.5Mbps 정도이지만, 만약 지역 케이블 업체가 T-1(1.544Mbps) 정도의 회선으로 인터넷이 연결되어 있다면, 가입자 역시 최고 속도가 1.544Mbs 정도로 제한된다[10].

케이블 모뎀 인터넷은 가입자와 ISP가 일대일로 연결되는 방식이 아니라 하나의 광케이블에 여러명이 공유하는 방식이어서 가입자가 늘어나거나 사용자가 많은 시간대에는 속도가 느려지진다.

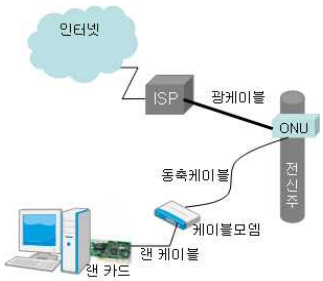


그림 8. 케이블모뎀방식의 망
Fig. 8 Cable Modem Network

(3) ADSL 서비스의 망

ADSL은 기존 전화선을 그대로 이용하면서 전화 통신에 사용되는 4KHZ의 주파수에서 남은 주파수 4KHz에서 1MHz의 대역폭을 이용해 인터넷을 서비스하는 것으로, 가장 많은 사용자층을 가지고 있는 인터넷 접속 방식으로 디지털 정보를 전송하기 위한 기술로서 사용자의 ADSL 모뎀과 전화국의 장비가 일대일로 연결되는 방식이기 때문에 주위 사용자 수에 상관없이 어느 정도 안정된 속도가 보장된다[9]. ADSL은 대부분의 채널을 사용자측으로 내려보내는 하향쪽으로 전송하는데 사용하고, 사용자로부터 받는 정보에는 아주 적게 할당하는 비대칭형 구조이며, 이론상의 전송속도는 상향 16Kbps~640Kbps, 하향 1.5Mbps~8Mbps이다. 또한, 회선에 디지털 정보 뿐 아니라 아날로그(음성) 정보도 동시에 수용할 수 있다.

따라서 마이크로 필터를 사용하여 전화선에서 음성 신호만 분리해 주는 장치를 반드시 연결해야 한다.

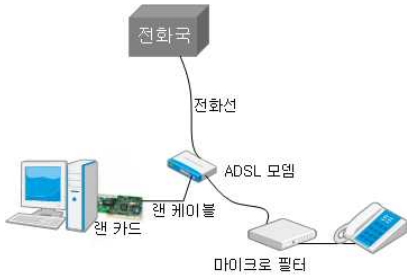


그림 9. ADSL 망
Fig. 9 ADSL Network

(4) VDSL 서비스 망

ADSL과는 달리 가입자에게 필요한 데이터만을 전송하고, 기존의 전화선을 그대로 이용하기 때문에 공급가격이 저렴할 뿐 아니라, 설치 공간도 덜 차지한다는 장점이 있다. 특히 이 전송기술이 상용화되면 대용량 멀티미디어 서비스를 수용할 수 있는 양방향 전송도 가능하다.

가입자측(하향) 전송 속도는 13~52Mbps, 교환국측(상향) 전송 속도는 1.5~2.3Mbps, 전송 거리는 0.3~1.5㎞이다. 그래서 ADSL에 비해서 2~10배 정도 넓은 대역폭을 사용한다[11].

그림 10을 보면 한국통신에서 가입자 근처의 집선 장치인 DSLAM 장비까지는 광케이블로 연결되며 DSLAM 장비에서 가입자까지의 선로는 기존 전화선을 그대로 사용하고 있다. 즉, VDSL의 경우 이 전화선 구간의 길이가 1Km가 넘게 되면 제대로 된 속도를 얻을 수 없다[9].

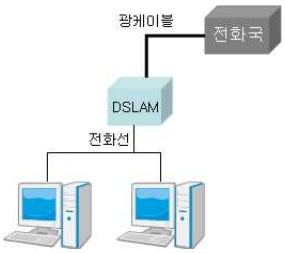


그림 10. VDSL 망
Fig. 10 VDSL Network

3.4 보안 강도의 차이

IPSec VPN은 IPSec 프로토콜을 이용해 인터넷 망내에 정보보안이 가능한 터널을 제공하는 VPN 서비스로써 뛰어난 보안성을 제공하지만 키 관리와 키 분배와 같은 기반 기술들이 필요하고, 사용자가 직접 VPN 서비스를 관리해 주어야 하며, QoS를 제한적으로 지원하는 문제가 있다. 또한, 암호화과정으로 인한 지연으로 인해 음성 또는 영상 트래픽에는 적합하지 않으며, Mesh 구조로 인한 확장성 제한도 단점으로 나타나고 있다. 이러한 문제점들을 개선한 구조가 MPLS VPN이다. MPLS VPN은 Mega-Scale로 확장성이 우수하고, 차별적 QoS 지원이 가능하며, IP만을 지원하는 IPSec VPN에 비해 다양한 프로토콜을 지원한다. 또한 멀티캐스트를 지원하기에도 용이하다.

표 4는 IPSec VPN과 MPLS VPN의 이러한 기능들을 비교하여 설명한 것이다.

표 4. IPSec VPN과 MPLS VPN 비교
Table 4. The comparison of IPSec VPN and MPLS VPN

구분	IPSec VPN	MPLS VPN
확장성	보통	매우 우수
QoS	보통	매우 우수
구축/유지비용	고가	저가
보안성	우수	보통

전용회선은 상향, 하향이 대칭이어서 일정한 트래픽 내에서는 안정적으로 사용할 수 있으나, 트래픽이 증가하면 속도가 느려지는 경향이 있다. 이때, 전용선은 트래픽을 분산하기위해 추가비용이 발생하지만 하지만 VPN 전용선은 트래픽을 IP별, PORT별로 분산하여 트래픽이 몰리는 현상을 줄이고, 추후 트래픽 증가로 속도 개선이 필요시에는 추가비용이 저렴하다. 전용회선은 초기설치비와 사용요금/ 속도증대 비용이 많이 필요하지만, VPN전용선은 전용선에 비해서 50%이상 저렴하고, 회사 이전시에도 간편하고, 유동적으로 이전이 가능하다. 전용회선은 장애 발생시 처리시간이 지연되나, VPN 전용선은 2~3회선의 인터넷회선을 이용하여 자체적으로 백업라인을 구축하고, NMS, 통합관제서비스, 24시간 모니터링 및 장애처리지원(NOC) 등 통합관제서비스를 통한 해킹시도 및 바이러스 침투관제도 등도 가능하다. 또한, VPN 전용선은 사설망을 통해 암호화된 데이터를 전송하므로 완벽한 보안을 제공하지만, 일반 전용회선의 경우에는 선에 접지하는 방식을 통해 간단히 해킹이 가능하다.

표 5는 이러한 VPN 전용선과 일반전용회선의 안정성과 보안성을 비교 설명한 것이다.

표 5. VPN 전용선과 일반전용회선의 비교
Table 5. The comparison of VPN Dedicated LIne and General Dedicated Line

구분	VPN 전용선	일반전용회선
IP	공인 IP	공인 IP
속도	4M이상(다운로드), VDSL 연결시 10M	E1(2MB), T1(1.5M)
안정성	다중회선 구성	단일회선으로 단선시 인터넷 끊김
비용	일반전용회선의 50%	고가
네트워크 관리	NMS, MRTG, Port별 제어 기능	NMS, MRTG(유료)
보안성	아주 높음	낮음

3.5 초기 구축비 및 유지보수 비용

전화국과 가입자간에 단일 회선의 광케이블이나 동선으로 구축되던 기존 인터넷전용회선과는 다르게 이중 회선의 ADSL과 케이블 망으로 종단 네트워크를 구성함으로써 회선의 안정성과 네트워크 유지비용을 절감한 새로운 개념의 인터넷전용회선 서비스인 VPN전용선의 초기구축비 및 유지보수비용을 비교해보면 다음과 같다.

표 6는 VPN 전용선과 기업 전용회선의 회선속도, 회선구성, 안정성, 이용료 등을 비교하여 설명한 것이다[12].

표 6. VPN전용선과 기업전용선 비교
Table 6. The comparison of VPN Dedicated Lines and Company Dedicated Lines

상품구분	회선속도	회선 구성	회선안 정성	이용료 (월)
VPN 전용선	공중망 회선속도	이중 회선	매우 우수	약45만원
기업 전용선	1.5M(T1)	단일 회선	우수	약130 만원

표 7. 기업용 인터넷전용회선 월 이용료(단위:천원[12])
Table 7. The company Internet dedicated lines fee per month

상품구분	기본 (월)	1년 약정	장비임대 (월)	비고
E1 (2.04Mbps)	1,750	1,645	국산:48 외산:88	동축 또는 광
T1 (1.5Mbps)	1,350	1,269	국산:48 외산:88	동축 또는 광
512Kbps	780	733	국산:48 외산:88	동축 또는 광
설치지역	전용선 개통이 가능한 전국			

표 8은 VPN과 전용회선의 회선구성, 대역폭, 보안, 안정성 등을 예를 들어 설명한 것이다. 안정성은 VPN과 전용회선 모두 안정적이지만 유동성에서는 VPN이 높으며, 확장성에서도 VPN이 더 유리하다는 것을 알 수 있다[13].

표 8. VPN과 전용회선 비교
Table 8. The comparison of VPN and Dedicated Lines

구분	D기업VPN Soho	기업 전용회선	PC방 전용회선
비교	ADSL 회선사용	5M	5M
회선구성	다중회선 (최대4회선)	단일회선 (1회선)	단일회선 (1회선)
대역폭	5M/512Kbps	5Mbps	5Mbps
보안 (방화벽)	O	X	X
안정성	안정적(백업)	안정적	안정적
유지비 (월)	20만원대	372만원	90만원
구성	VPN 라우터 + 회선	전용회선	전용회선
확장성	본지사간 확장 용이	구축 네트워크 내 한정	구축 네트워크 내 한정
유동성	높음	없음	없음
설치	인터넷사용 전지역	제한	제한
관제	O	X	X

3.6 국내 망 사업자 제공 서비스 현황

KT, 데이콤, 삼성 네트웍스 등 서비스 사업자를 중심으로 MPLS(Multi—protocol Label Switching) VPN 서비스가 본격화되고 있다. 또 9.11테러 이후 재해복구시스템의 중요성이 커지면서 금융권을 중심으로 가상사설망(VPN) 도입이 활발하다.

VPN 서비스가 최근 확산되는 이유는 기존 전용선보다 40~50% 저렴한 비용, VPN의 성능 향상과 QoS(Quality of Service) 및 보안 기능 보강, 인터넷을 이용한 인트라넷 및 엑스트라넷 구현 용이, 9·11테러 이후 금융권의 저비용 백업라인 도입 확산, 서비스사업자의 MPLS VPN 서비스 경쟁 등을 꼽을 수 있다.

VPN 서비스는 초기에 전용회선을 이용했으나 최근에는 인터넷의 확산으로 IP VPN으로 발전했다. IP VPN은 초기에 보안과 품질보장 등의 문제로 보급이 지체됐으나 보안은 IPSec 기술 이용이나 송수신되는 데이터의 암호화를 통해, 품질보장 문제는 MPLS VPN 등장으로

해소할 수 있게 됐다. 특히 VPN 서비스는 이제 모바일 VPN 및 PKI 기반의 VPN 등으로 확산되고 있다.

서비스 사업자를 중심으로 도입되는 MPLS VPN 장비는 대부분 외산인 반면, ADSL 등 초고속망을 이용한 VPN 장비는 국산이 강세를 보이고 있다. 관련업체를 살펴보면 서비스사업자에는 KT, 데이콤, 하나로통신, 비상장업체로는 삼성 네트웍스, 한솔아이글로브가 있다. 보안 업체 중 등록기업은 퓨처시스템, 어울림정보기술, 시그엔, 한국정보공학, 시큐어소프트가 있고 비상장기업은 사이젠텍, 이노크래프트, 시큐아이닷컴, 시큐어넥서스 등이 있다.

국내 IP VPN 서비스 시장은 2010년까지 연평균 성장률 15.1%로 약 2,612억 규모로 성장할 전망이다[14].

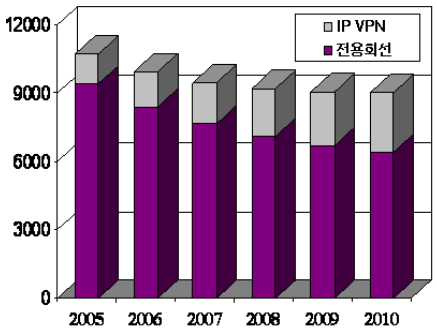


그림 11. 국내 IP VPN 서비스 시장 전망('06 ~ '10)
Fig. 11 The view of IP VPN Service Market('06 ~ '10)

2001년 LG데이콤이 국내 ISP 최초로 MPLS VPN을 제공한 이후 주요 사업자들이 서비스를 제공중이다. 표 9는 국내 VPN 서비스 제공 사업자 현황을 설명한 것이다[15].

표 9. VPN 서비스 제공 사업자 현황
Table 9. the operator status VPN Service offer

구분	LG Dacom	KT	삼성 네트웍스	하나로 텔레콤	SK 네트웍스
제공 서비스	MPLS, IPSec, VPLS	MPLS, IPSec	IPSec, MPLS	MPLS	MPLS
노드수	60	40	30	24	12
제공일	IPSec: '98년 MPLS: '01년 7월	IPSec: '98년 MPLS: '01년 10월	IPSec: '98년 MPLS: '02년 8월	MPLS : '06년	MPLS : '06년
특징	First Mover MVP, CADNET, WideLAN	최대 고객 규모, Managed 서비스	계열사 위주 고객	후발 사업자	후발 사업자

IV. 결 론

초기 금융권, 공공기관 등에서 백업 망으로 활용하기 위해 도입한 VPN은 차차 지사와 영업점 등을 많이 거느린 일반 기업으로 시장을 넓히고 있다. 또한 안정성이 검증됨에 따라 백업 외에 주 회선과 함께 전체 회선의 확장용으로 사용하는 사례가 점점 많아지고 있으며, 업계에 따라서는 아예 전용회선을 걷어내고 본·지사간 주요 회선으로 도입하고 있다.

IPSec 프로토콜을 이용하는 IPSec VPN은 인터넷 망내에 정보보안이 가능한 터널을 제공하여 뛰어난 보안성을 제공하지만 키 관리와 키 분배와 같은 기반 기술들이 필요하고, 사용자가 직접 VPN 서비스를 관리해주어야 하며, QoS를 제한적으로 지원하는 문제가 있다. 또한, 암호화과정으로 인한 지연으로 인해 음성 또는 영상 트래픽에는 적합하지 않으며, Mesh 구조로 인한 확장성 제한도 단점으로 나타나고 있다. 이러한 문제점들을 개선한 구조가 MPLS VPN이다. MPLS VPN은 확장성이 우수하고, IP만을 지원하는 IPSec VPN에 비해 다양한 프로토콜을 지원한다. 또한 멀티캐스트를 지원하기에도 용이하고, 차별적 QoS 지원이 가능하다. 따라서, MPLS VPN은 QoS를 적용해 트래픽을 제어할 수 있으므로 최근 심각한 문제로 부각되고

있는 웜(Worm) 바이러스 등의 유해 트래픽을 차단해 네트워크를 효율적으로 사용할 수 있다는 장점을 갖는다. 또한, QoS 기능은 네트워크의 과부하를 미연에 방지하고, 효율적 트래픽 분배와 처리 기능을 가지고 있으므로, 사용자나 애플리케이션 중요도에 따라 서비스 수준을 차별적으로 적용해 한정된 회선에서 중요한 트래픽의 우선 처리를 보장해 업무 효율을 증진시킬 수 있다.

지사에서 본사간의 통신은 VPN을 통해 암·복호화를 과정을 거쳐 보안상의 문제가 발생할 확률이 낮지만 지사에서 인터넷을 바로 접속하는 것은 늘 보안상의 문제점을 안고 있지만, NAT나 방화벽을 통하여 이러한 취약점을 제거할 수 있다. 이와 같이 VPN은 전용회선 보다 저 비용으로 강력한 보안과 고 효율을 가짐으로써 기업들에게 주목 받고 기업들이 선택하고 있으며, VPN은 현 시점에서 최고의 솔루션이라고 할 수 있다.

참고문헌

[1] 이윤철,"VPN 기술 및 국내외 시장 동향", 주간기술동향 1075호, 2002

[2] http://kidbs.itfind.or.kr/WZIN/jugidong/947/94703.html

[3] 이창호, "MPLS를 이용한 VPN 설계에 관한 연구", 경상대 산업대학원 석사학위논문, 2003

[4] 시사컴퓨터 2004년 4월호

[5] netmemo.tistory.com/attachment/jm247.doc

[6] http://www.it-line.biz/sub1.htm

[7] 안신혁, 허재두, 이형호, "L2/L3 MPLS 기반 VPN 기술동향", 주간기술동향, 1080호, 2003

[8] NETWORK TIMES 2002년 09월호

[9] http://user.chollian.net/~p4999/net.htm

[10] http://www.terms.co.kr

[11] http://ko.wikipedia.org/wiki/

[12] http://www.ok-net.net

[13] http://vpn.dotname.co.kr

[14] 한인규, "Korea IP VPN Services 2007-2011 Forcast and Analysis : 2006 Year-End Review", IDC코리아, 2006

[15] 김호성, "통신사업자 VPN 서비스 사례 및 이슈", LG텔레콤 인터넷사업부, 2007.11

[16] 한국전산원, "MPLS 망 고도화를 위한 기능 개선 방안 연구", 2003

[17] 유병일, 전병실, "MPLS 기반 VPN 제공을 위한 설계 및 성능분석", 전자공학회, 2002

저자약력

정 은 희(Eun-Hee Jeong)

1991년 강릉대학교 통계학과 이학사

1998년 관동대학교 전자계산공학과 공학석사

2003년 관동대학교 전자계산공학과 공학박사

2003년~현재 강원대학교 지역경제학과 조교수

<관심분야> 네트워크 보안, 전자상거래, 웹 프로그래밍

이 병 관(Byung-Kwan Lee)

1975년 부산대학교 기계설계학과 학사

1986년 중앙대학교 전자계산공학과 석사

1990년 중앙대학교 전자계산공학과 박사

1988년~현재 관동대학교 컴퓨터공학과 교수

<관심분야> 네트워크 보안, 전자상거래, 컴퓨터 네트워크