VPN 서비스를 위한 Layer Two Tunneling Protocol (L2TP)의 구현

정미라 , 최종원
숙명여자 대학교 전산학과

An Impelementation of Layer Two Tunneling Protocol (L2TP) for VPN Service

Jung Mira, Choi Jong Won
Dept. of Computer Science, Sookmyung Women's University

요 약

최근 이동 사용자가 늘어나고 기업간의 사내망 구축이 증가하면서 Virtual Private Network(VPN) 서비스에 대한 요구가 많아지게 되었다. VPN 서비스를 위한 표준으로 제안된 L2TP는 PPTP·L2F와 호환이 가능하며, IPx, Appletalk등 다중 프로토콜 지원이 가능하다는 장점을 가진다. L2TP는 다중 터널, 다중 세션을 지원하며 터널의 보안을 위해 터널 인증 시 CHAP과 유사한 기법으로 상대 시스템 인증이 가능하고 제어 메시지 암호화와 같은 기능을 통해 외부의 침입자로부터 터널을 안전하게 보호한다. 또한 확장성을 위해 제어 메시지에 사용되는 속성 값들을 각각의 고유한 속성과 그 값들의 가변적인 집합으로 구성하여 전송하는 기법을 사용하고 있다. 본 논문에서는 L2TP의 특징을 다른 터널링 프로토콜들과 비교, 분석하고 주요 기능을 구현하는 것을 주 목적으로 한다.

1 서론

최근 사내망에 접속하는 원거리 사용자가 증가하고 사내 지점망을 통합하는 기업이 많아지면서 설치비용이 많이 드는 전용선을 이용한 사내망과 비교할 때 전화망이나 인터넷 등의 공중망을 이용하여 보다 저렴하게 가상 사내망을 구축할 수 있는 가상 사설망(VPN) 서비스가 증가하고 있다. 전형적인 다이얼 업 네트워크 서비스가 등록된 IP 주소만 사용 가능하고 패킷 전송 시 보안성이 떨어지는 것에 비하여 가상 사설망 서비스는 IP에 국한되는 것이 아닌 다중 프로토콜의 지원과 등록되지 않은 IP 주소의 사용을 허락하며 인증과 암호화 등을 통해 전송 시의 보안도 제공한다. 이러한 다중 프로토콜을 지원하는 가상 사설망 서비스는 최종 사용자, 기업, 그리고 인터넷 서비스 제공자들이 코어 하부구조를 공유할 수 있게 해주며 IP 프로토콜을 사용하지 않는 응용 프로그램들을 이용할 수 있게 해준다.

가상 사설망 서비스에 사용되는 프로토콜로는 마이크로 소프트사에서 개발한 PPTP[4], 시스코 사에서 개발된 L2F와, 마이크로 소프트사와 시스코사가 공동 개발중인 L2TP[8], 그리고 IP 기반에서 가상 사내망 서비스를 제공하는 IPSec[5,6,7]이 있다. PPTP는 마이크로 소프트사에서 개발된 가상 사설망 서비스를 위한 소프트웨어이고 L2F는 시스코사에서 개발된 라우터를 사용하여 VPN 서비스를 제공하는 프로토콜이다. 이들은 다른 제품과의 호환성이 부족하다는 단점이 있다. IPsec은 IP 기반에서의 패킷 전송 시에 보안성 높이기 위해 제안된 프로토콜로 최근에는 가상 사설망 서비스에도 많이 쓰이고 있으나 IP 기반의 서비스만을 제공할 수 있다는 단점을 가지고 있다. 반면 최근 들어 IETF의 PPP extension 워킹 그룹에서 VPN을 위한 표준으로 제안한 L2TP는 PPTP와 L2F의 통합 버전으로 두 가상 사내망 서비스 프로토콜의 특징을 취합하였으며 더 발전된 부분도 포함하고 있다. 또한 IP 기반에서만 서비스가 가능한 IPSec에 비해서도 높은 호환성을 가지고 있다. 따라서 본 논문에서는 L2TP를 PPPT나 L2F, IPsec과 비교 분석하고 L2TP의 주요 기능을 구현한다.

본 논문의 구성은 다음과 같다. 2장에서는 PPTP와 L2F, IPsec을 소개하고, 3장에서는 L2TP의 개요와 특징을 설명한다. 그리고 4장에서는 구현 환경과 중점을 두어 구현한 부분에 대하여 기술하고 5장에서 결론을 맺도록 한다.

2. 관련 연구

마이크로 소프트사에 의해 개발된 PPTP는 공통 키 인프라구조가 없는 두 개의 게이트웨이 사이 또는 사용자와 게이트웨이 사이에서 사용자 패스워드 확인을 통한 인증과 암호화된 통신을 지원 하기 위해 1996년 처음 개발되었다. PPTP 디자인 목적은 단순하면서도 다중 프로토콜 전송이 가능한 터널링 프로토콜의 개발이었다. PPTP는 터널 설정 시에 TCP를 사용하며 터널을 통한 PPP 패킷 전송시에는 GRE 헤더를 사용한다. 또한 사용자 인증이나 암호화, IP 주소 할당 서비스 등을 제공하고 있다. 사용자 암호 확인을 통한 인증과 암호화를 제공하기 때문에 관리자가 사용하기 쉽고 비용이 저렴하지만 소프트웨어 기반으로만 작동하기 때문에 하드웨어 기반으로 작동하는 터널링 프로토콜과는 호환이 어려운 단점이 있다.

시스코에서 개발된 L2F는 시스코가 라우터를 판매하는 하드웨어 업체라는 점에서 같은 터널링 프로토콜인 PPTP와 차이점을 가진다. L2F를 이용하려면 인터넷 서비스 업체가 반드시 L2F를 지원해주는 원거리 억세스 서버와 라우터를 사용해야만 한다. L2F는 3계층에서 작동하는 프로토콜이므로 2계층에서 작동하는 PPTP가 IP 기반의 라우팅을 필요로 하는 것과 달리 특정한 프로토콜에 구애받지 않고 큰 오버헤드 없이 네트워크 계층의 낮은 부분에서 수행이 가능하다. 또한 L2F는 단순한 사용자 계정과 패스워드 확인 외에도 옵션을 사용하여, 양 끝 점 간의 인증을 위한 보안이 PPTP 보다 철저하다. 그러나 L2F를 사용하기 위해서는 반드시 라우터를 구입해야하므로 비용이 비싸며 PPTP와 마찬가지로 다른 터널링 프로토콜과 호환성이 떨어지는 문제점이 있다.

IPSec은 현재 표준화가 진행중인 패킷 계층 보안 기술로, IPSec 이전의 모든 보안에 대한 고려는 응용 프로그램에서 적용되었으나 IPSec이 개발되면서 응용 프로그램과 독립적으로 네트워크 보안이 가능해졌다. IPSec 패킷에는 인증과 프라이버시, 패킷의 무결성을 제공하는 ESP 포맷과, 인증과 무결성을 제공하지만 프라이버시는 제공하지 않는 AH 포맷의 두 가지 종류가 있다. 또한 전송 시에도 양 끝 지점간에 보안이 강화된 IP 전송을 제공하는 전송 모드와 기존의 IP 패킷을 새로운 IP 패킷 내에 캡슐화하여 전송하는 터널 모드가 있으며, 이 터널 모드를 이용하여 가상 사설망 구축이 가능하다. IPSec은 IP를 기반으로 하는 망에서는 안전한 가상 사내망 연결이 가능하지만 IP를 사용하

지 않는 망에서는 호환성이 떨어지는 단점이 있다.

3. L2TP 프로토콜

최근 VPN 서비스를 위한 표준으로 제안된 L2TP는 PPTP와 L2F의 호환성 문제를 보완하기 위해 개발된 터널링 프로토콜로서 PPTP와 L2F의 통합 버전이라고 할 수 있으며 두 프로토콜 보다 더욱 발전된 프로토콜이다. L2TP는 전화를 이용한 사내망으로의 접속과 인터넷을 통한 사내망으로의 접속을 모두 지원한다.

3.1 개요 및 구조

L2TP는 2계층의 종단 점과 PPP 연결의 종단 점이 패킷망으로 상호 연결된 서로 다른 장치에 존재할 수 있도록 PPP 모델을 확장한 프로토콜이다. 사용자는 L2TP를 사용하여 연결 집중 장치로 2계층의 연결이 가능하고, 연결 집중 장치는 사내망 등의 기반 랜에 연결된 터널링 장치인 네트워크 접근 서버에게로 각각의 PPP 프레임을 터널링하여 전송함으로서 2계층 터널의 종단에서는 실제 PPP 프레임 패킷이 기반 랜으로 전송된다. 이렇게 2계층의 종단 점과 PPP 연결의 종단 점을 분리시킴으로써 PPP 연결이 지역 회선 집중 장치에서 종결될 수 있어 망 연결 서버까지 원거리로 연결하는 경우보다 저렴한 비용으로 서비스를 제공 할 수 있다. 또한 L2TP에서는 양 끝 점간의 다중 터널과 다중 세션을 지원한다.

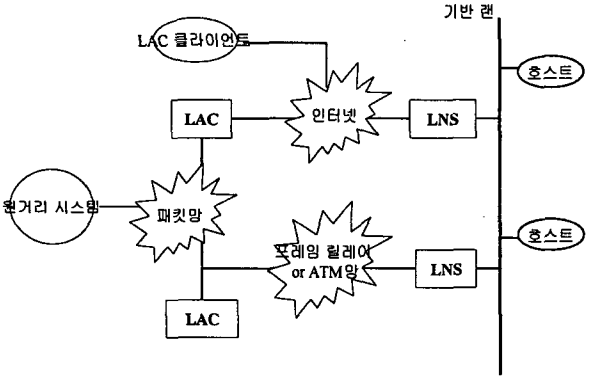

그림 1 L2TP 구조

L2TP에는 그림1과 같이 전화망을 통한 비동기 PPP를 사용한 접근과 ISDN이나 인터넷· ATM망 등의 동기 PPP를 이용한 접근 방법, 2가지가 있다. LAC(L2TP Access Concentrator)는 원거리 시스템이 접속되는 연결 집중 장치로서 L2TP 서비스를 제공하는 인터넷 서비스 업체 상에서 동작하며 LNS로의 터널링을 담당한다. 기반 랜에 연결된 네트워크 서버인 LNS (L2TP Network Server)는 원거리 시스템에 연결된 L2TP 네트워크 서버 장치로 LAC로부터 터널링 된 패킷을 전송받아 처리 후 기반 랜으로 접속을 하거나 기반 랜으로부터 전송 받은 PPP 프레임을 터널링하여 LAC로 전송하는 기능을 수행한다. 즉 2계층의 터널은 LAC와 LNS 사이에 설정된다. 외부 시스템에서 기반 랜으로 터널을 구축하는 경우 우선 LAC로의 PPP 연결을 생성하면 LAC는 원거리 시스템에서의 PPP 연결을 터널링하여 공중망을 통해 LNS에게 전송한다. 기반 랜에서 외부 시스템으로의 연결이 필요한 경우 사내망에 연결된 호스트들은 LNS로 PPP 연결을 하고 LNS는 해당 외부 시스템이 연결된 적절한 LAC로의 터널을 설정한 후 기반 랜에서 전송되는 패킷들을 터널링 하여 LAC로 전송한다. LAC 클라이언트는 L2TP가 동작하고 있는 호스트로서 별도의 LAC없이 LNS로의 터널링을 수행하며 이 경우 LAC 클라이언트 소프트웨어가 동작하는 호스트는 이미 인터넷망에 접속이 되어 있는 상태라야 한다. 접속이 되어 있는 경우 가상의 PPP 연결이 생성되고 호스트의 LAC 클라이언트 소프트웨어는 LNS로의 터널을 생성한다. 두 경우 모두 주소 할당과 인증, 회계 기능은 기반 랜의 관리 도메인에서 담당한다.

3.2 프로토콜의 동작

L2TP에는 터널과 세션을 설정, 관리하는 제어 메시지와 데이터 전송을 위한 데이터 메시지의 두 가지 메시지 형태가 있다. L2TP는 제어 메시지와 데이터 메시지에 공통 헤더를 사용한다. L2TP에서는 터널의 흐름 제어와 혼잡 제어를 위한 순서 번호 필드의 사용이 중요한 부분을 차지하는데, 데이터 전송 시는 순서 번호 사용이 선택적이지만 제어 메시지에는 반드시 순서 번호를 사용해야 한다. 또한 제어 메시지는 신뢰성 있는 데이터 전송이 가능하지만 데이터 메시지는 패킷이 손실되었을 때 재전송을 지원하지 않는다. IP 기반에서 L2TP가 동작할 때는 UDP 포트 1701번을 사용한다. L2TP의 제어 메시지 전송 형태는 그림 2와 같고 PPP 데이터 전송 시 L2TP 데이터 메시지 전송 형태는 그림 3과 같다.

UDP	L2TP 헤더	제어 메시지

그림 2. L2TP 제어 메시지

UDP	L2TP 헤더	PPP 헤더	데이터

그림 3. L2TP 데이터 메시지

L2TP는 호환성을 지원하면서도 확장성을 최대화하기 위해 제어 메시지에 사용되는 속성 값이나 속성 타입을 하나의 동일한 형태로 구성하는 AVP라는 인코딩 방법을 사용한다. AVP는 제어 메시지에 사용되는 속성과 그 값들의 가변 길이 집합을 의미하는 것으로 여러 AVP가 모여 터널의 구축과 관리, 터널 해제 등에 사용되는 제어 메시지를 구성한다. 각각의 제어 메시지에 따라 적절한 AVP를 사용하도록 지정되어 있으며 각 AVP는 속성의 타입을 나타내는 필드와 그 속성의 실제 값을 저장하고 있는 필드로 구성되고 보안이 필요한 AVP는 MD5를 이용한 암호화가 가능하다. 원격지의 사용자가 다이얼 업 서비스를 이용하여 기반 랜으로의 접근을 시도하는 경우 처리 과정은 그림 4와 같다.

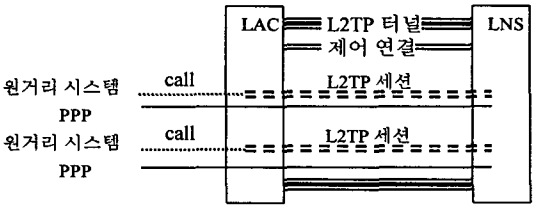

그림 4 PPP 터널링

PPP 터널링이 시작되기 전에 LAC와 LNS 사이에는 터널 구축을 위한 제어 메시지 교환이 이루어져야 한다. 먼저 원거리의 사용자가 PSTN이나 다른 망을 통하여 인터넷 서비스 업체에 PPP 연결을 시도한다. 인터넷 서비스 업체의 LAC가 연결을 받아들이면 PPP 링크가 설정되게 된다. 만약 인터넷 서비스 업체의 LAC에서 적절한 LNS로의 터널이 존재하지 않는다면 터널이 초기화된다. 일단 터널이 존재하면 터널 내 사용하지 않는 슬롯에 대하여 call 번호가 할당된 후 이 내용이 LNS에 알려지고 LNS가 연결을 받아들이면 터널이 설정된다. 설정 작업이 끝나면 원격 사용자로부터의 PPP 프레임을 인터넷 서비스 업체의 LAC가 수신하여 L2TP에 담아서 적당한 터널로 전송한다. LNS는 이 프레임을 수신한 뒤 L2TP 헤더를 벗겨내고 처리를 시작한다.

제어 메시지는 일반 데이터 메시지 전송 시 사용되는 터널과 같은 터널을 통하여 전송된다. 제어 메시지는 터널에 관한 상태 정보뿐 아니라 터널을 통하여 운송되어 지는 세션에 대한 설정과 해제, 그리고 관

리에 대한 책임을 가진다. 세션의 양 사용자들은 각각 독립적인 call 번호를 사용하므로 해당 세션의 송신자는 송신하고자 하는 패킷 헤더의 call 번호 필드에 수신자 측에서 사용하는 call 번호 값을 설정해야만 한다.

터널의 keep alive 메카니즘은 상위 계층에 의하여 이루어진다. 일정 기간동안 제어 메시지나 데이터 메시지가 교환되지 않는 경우 Hello 제어 메시지를 보낸 후 확인 메시지를 기다린다. 확인 메시지가 일정 시간동안 수신되지 않는 경우 재전송을 한다. 몇 번의 재전송 시도에도 불구하고 확인 메시지가 도착하지 않은 경우에는 해당 터널이 다운된 것으로 간주되고 터널 재설정이 시작된다. 일단 터널이 구축되고 제어 메시지가 터널 설정을 끝마치면 터널은 세션을 위한 PPP 패킷을 전송하는데 사용된다.

L2TP는 해당 LAC와 LNS 사이에 다중 터널을 설정하여 사용 할 수 있다. 이는 하나의 사용자 세션을 위하여 하나의 터널이 사용되는 경우 터널 미디어가 주어진 사용자에게 특정한 QoS 속성을 제공해 줄 수 있다는 점에서 매우 유용한 특성이다. 또한 L2TP는 터널의 보안을 위해 터널 구축 시에 선택적으로 CHAP[3]과 유사한 형태의 단순한 터널 인증 시스템의 사용이 가능하다. L2TP 헤더의 세션 번호 필드는 PPP 패킷이 속해있는 세션을 지정하며, 버전 필드는 같은 UDP 포트 1701번을 사용하는 L2F와 L2TP 패킷을 구분하는 용도로 사용된다.

4. 구현

본 절에서는 L2TP의 구현 환경과 중점 구현 사항에 대해 기술한다. L2TP 구현도구로는 자바 (JDK1.2)를 사용하였다. LNS를 수행하는 시스템은 SUN Enterprise 3000 server를 사용하였으며, 운영체제는 Solaris 2.6을 사용하였다. LAC 클라이언트는 LAN을 통해 인터넷에 연결된 windows98 운영체제의 Pentium II 300Mhz PC를 이용하였다.

VPN 서비스는 특성상 보안이 크게 중요시되므로 L2TP 터널 설정 시에 challenge AVP와 challenge response AVP를 사용하여 상대 시스템 인증을 반드시 수행하도록 하였다. 상대 시스템 인증을 이용한 터널 설정 메시지, SCCRQ의 처리 과정 의사 코드는 그림 5와 같다.

```
// 제어 연결 상태가 idle 상태일 때 제어 메시지 처리 과정
while (state = idle)
    receive(L2TP)
    processing(L2TP_header)
    parsing_AVP(message_type)
    If (message type =SCCRQ)
        parsing_AVP(protocol_version)
        parsing_AVP(host_name) // get peer's host name
        Parsing_AVP(framing_capabilities)
        parsing_AVP(tunnel_id)  // tunnel_id should be 0 in SCCRQ
        parsing_AVP(challenge_AVP) // get challenge
        secret = get_secret()
        challenge_response=calcaulate_MD5(secret,value of challeng AVP)
        // SCCRP 메시지 구성
        make_L2TPheader(
        make_AVP(SCCRP)
        make_AVP(protocol_version)  // protocol version =1
        make_AVP(framing_capability)
        make_AVP(host_name)
        make_AVP(tunnel_id) // tunnel_id should be randomized
        make_AVP(challenge_respnse)
        combine(L2TPheader, AVP)
        send(SCCRP)
        // SCCN 메세지를 기다리는 상태로 이동
        state = wait_ctl_conn
    else
        state = idle
```

그림 5. 터널 설정 시 SCCRQ 처리 의사 코드

challenge AVP를 이용한 상대 시스템 인증이 실패할 경우 터널 설정은 취소된다. 또한 외부 시스템으로부터 기반 랜으로의 세션 설정 시, 대리 LCP AVP와 대리 인증 AVP를 사용하였고 대리 인증 프로토콜로는 PPP CHAP을 이용한다. 이러한 AVP들의 사용으로 외부 시스템과 LAC와의 LCP · PPP 협상을 L2PT 제어 메시지에 실어 LNS로 전송함으로써 LNS와는 별도의 LCP · PPP 재협상을 할 필요가 없도록 하였다.

CHAP은 상대 시스템 인증을 위해 사용되는 프로토콜로서 서버와 클라이언트 사이에 3번의 메시지 교환을 하는 핸드쉐이킹 방식으로 수행된다. 서버 측인 LNS에서 랜덤 스트링과 호스트 이름으로 구성된 challenge를 LAC로 전송하면 LAC에서는 공유 비밀 키를 습득한 뒤 MD5 암호화를 수행, calllenge response를 계산하여 LNS로 전송한다. LNS에서 공유 비밀키와 challenge를 이용해 계산된 MD5의 결과와 전송받은 challenge response가 일치하는 경우 상대 시스템 인증이 성공한 것이다.

L2TP 서비스를 사용하는 형태로는 3.2에서 밝힌 것처럼 사용자가 LAC를 수행하는 인터넷 서비스 업체에 연결하여 해당 업체와 기반 랜에 접속된 LNS와 터널을 구축하여 L2TP 서비스를 받는 경우와 호스트에서 직접 L2TP가 수행되어 LNS로의 터널링을 수행하는 두 가지 경우가 있다. 본 논문에서는 그중 호스트에서 직접 L2TP를 수행하여 LNS로 터널링을 수행하는 부분에 중점을 두어 구현하였다.

5. 결론

원거리 사용자가 기반 랜에 접근하기 위한 VPN 서비스가 증가하면서 VPN 서비스를 위한 PPTP, IPSec, L2TP, L2F등의 프로토콜 개발이 활발해지고 있다. 최근 들어 VPN 서비스를 위한 표준으로 제안되는 L2TP는 다른 제품과의 호환이 어려운 L2F나 PPTP와는 달리 높은 호환성을 제공하고 있으며 IP 기반으로만 동작이 가능한 IPSec과 비교할 때 다중 프로토콜을 지원하는 장점을 지니고 하나의 양 끝점간에 다중 터널을 구축할 수 있기 때문에 QoS 서비스를 지원할 수 있다는 장점을 가지고 있다.

본 논문에서는 자바를 이용하여 L2TP의 주요 기능을 구현하였으며 터널 설정 시 상대 시스템 인증을 수행하고 세션 설정 시에 CHAP을 이용한 대리 인증을 수행하도록 하여 보안 강화에 중점을 두었다.

현재로는 인터넷 상의 다른 부분을 접근하려는 사용자의 터널에 대한 접근을 제한하는 등 부족한 점이 있지만 호환성과 확장성, 다양한 보안, 인증 사용 기법, IPSec과의 연동을 통해 향후 VPN 서비스의 표준이 될 것이다.

References

[1] C. McGregor, "The PPP Internet Protocol Control Protocol (IPCP)", Internet-Draft: RFC 1332, May 1992

[2] W. Simpson, " The Point-to-Pont Protocol(PPP)", STD 51,RFC 1661,July 1994

[3] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996

[4] Kory Hamzeh, Gureep Pall, William Verthein, "Point-to-Point Tunneling Protocol(PPTP)", Internet-Draft, July 1997

[5] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", Internet-Draft: RFC 2401,November 1998

[6] S. Kent, R. Atkinson, "IP Authentication Header (AH)", Internet-Draft: RFC 2402, November 1998

[7] S. Kent, R. Atkinson, "IP Encapsulation Security Payload (ESP)", Internet-Draft: RFC 2406, November 1998

[8] W. M. Townsley, A. Valencia, A. Rubens, G. S. Pall, G. Zorn and B. Palter,"Layer Two Tunneling Protocol (L2TP)", Internet-draft, June 1999