12주차 3차시 VPN 보안 및 미래

【학습목표】

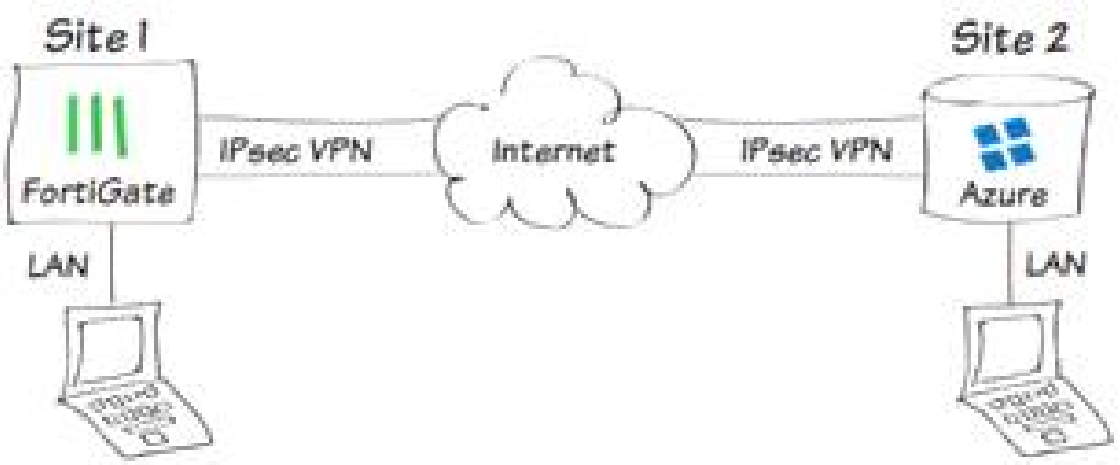
1. VPN의 대표적인 보안방법인 IPSec에 대해 설명할 수 있다.
2. VPN의 미래에 대해 논의할 수 있다.

학습내용1 : VPN의 보안방법인 IPSec

1. IPSec (IP Security)

1) 정의

- IETF가 IP 계층 보안을 위하여 개방형 구조로 설계한 표준
- 네트워크 계층의 보안에 대해서 안정적이고 표준화된 기초를 제공
- IP 계층에서 직접 보안 서비스를 제공함에 따라 상위 계층 프로그램의 변경이 필요 없음
  - 암호화된 패킷은 보통의 IP 패킷과 동일한 형태를 갖기 때문에 네트워크 장비의 내부 변경 없이 IP 네트워크를 통해서 쉽게 라우팅 가능
  - 암호화에 관련된 유일한 장비는 종단점
  - 구현과 관리 비용을 모두 크게 줄일 수 있음
- 차세대 인터넷 프로토콜인 IPv6에서는 IPSec을 기본적으로 포함
- IPv4에서도 IPSec을 사용하는 것이 보안을 위해 필요
- 인터넷의 기초적인 보안을 튼튼하게 할 수 있는 방법을 제공
- 방화벽이나 VPN등의 응용에 도입

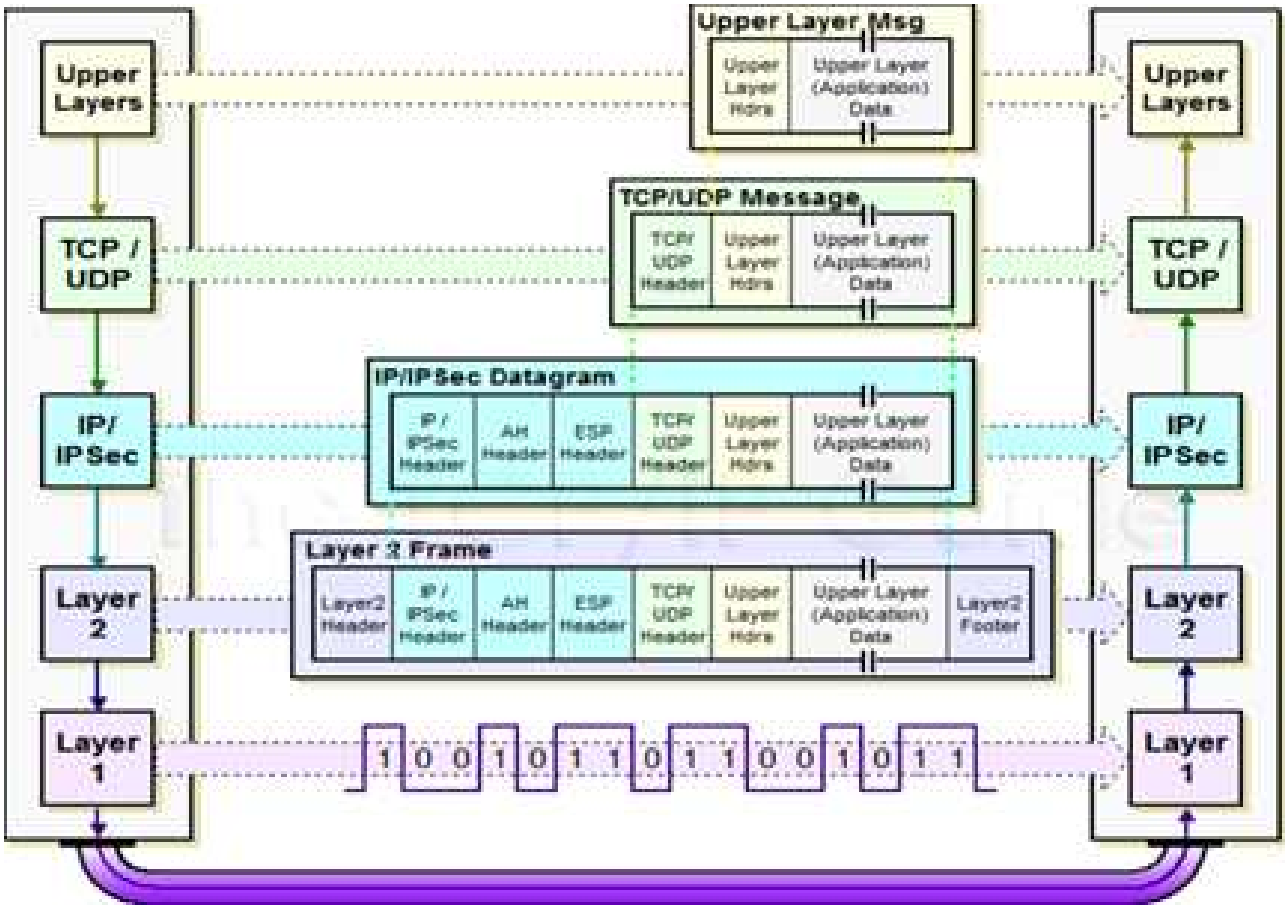


2) IPSec 제공 기능

- 데이터 원본 인증(Data source authentication)
  - 요청한 수신인에 의해서 각각의 데이터가 원본인가를 확인
- 데이터 무결성(Data integrity)
  - 데이터의 내용들이 이동 중 제 3자의 고의적 파괴나 네트워크 내에서 발생될 수 있는 오류들에 의해서 변화되지 않았다는 것을 확인
- 데이터의 기밀성(Data confidentiality)
  - 암호를 사용해서 메시지의 내용을 은폐
- Replay 보호(Protection against replay attacks)
  - 제 3자가 데이터를 가로채어 분석 후 그 정보를 이용한 불법 침입 방지

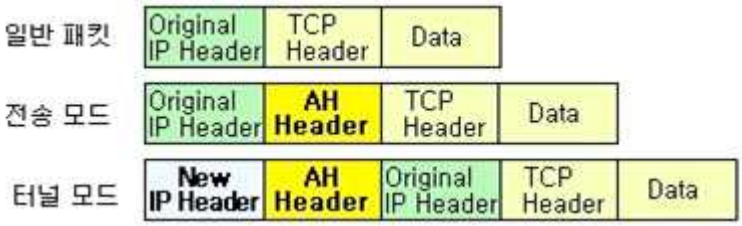
3) SA (Security Association)

- IPSec으로 통신 할 때 송·수신측은 공개키를 교환
- 인증 및 암호화 알고리즘과 암호키에 대한 정보를 교환
- 위와 같은 암호관련 프로파일(profile)을 SA(Security Association)라고 함
- 애플리케이션(application)마다 독립적으로 생성
- SA가 단 방향이기 때문에 양단간의 통신이 필요한 경우 각 방향에 대해 하나씩의 SA를 정의

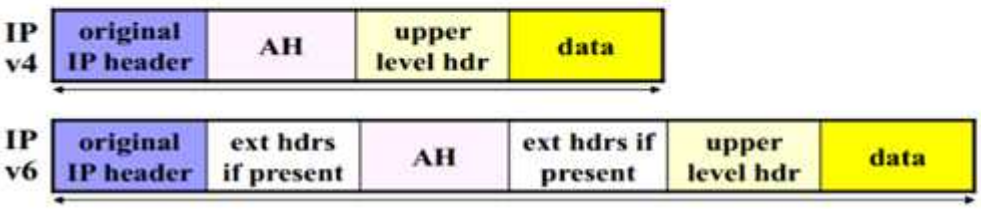


4) AH (Authentication Header)

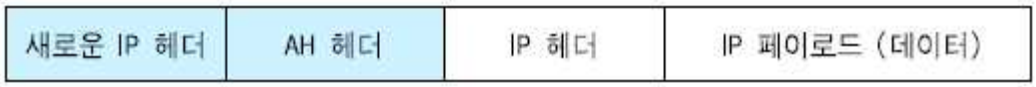
- AH는 IP 패킷에 대해서 무결성과 데이터 원본 인증을 제공
- Replay에 대한 보호를 제공
- 데이터 무결성
  - 메시지 인증 코드(MD5: Message Digest 5)에 의해서 생성되는 검사 합(checksum)에 의해서 보증
- 데이터 원본 인증
  - 인증된 데이터 안에 있는 공유된 비밀키에 의해서 보증
- Replay 보호는 AH 헤더의 필드에서 일련번호를 사용
- 모드별 데이터 포맷

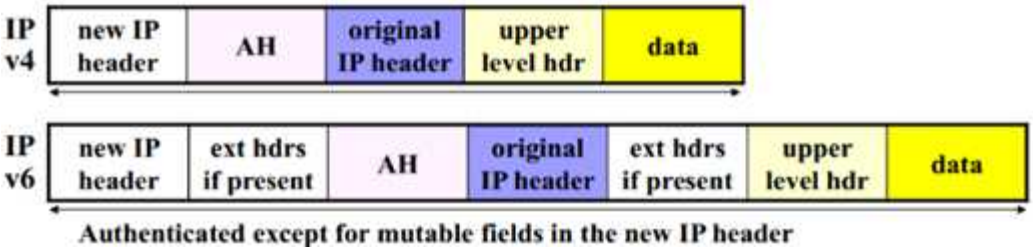


- 전송모드
  - 원래 IP헤더의 출발지, 목적지를 그대로 유지하는 방법이며, 터널모드는 새로운 IP헤더를 만들어서 원래의 IP 패킷 모두를 AH의 페이로드로 만드는 방법
  - IP 페이로드 부분만을 암호화
  - 두 개의 호스트간 통신에 사용
  - 데이터 원본 인증은 지원하지만 헤더부분의 모든 정보는 평문으로 되어 있어 노출 가능성 있음



- 터널모드
  - IP 헤더까지 모든 패킷을 암호화 하여 페이로드에 포함
  - 암호화된 IP 헤더이외의 부가적인 IP헤더가 필요
  - 통신 주체인 양단 중 하나가 게이트웨이일 경우에는 터널모드를 사용해야 함



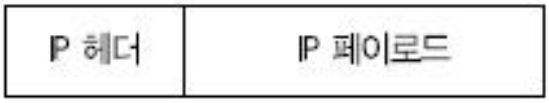


5) 캡슐 보안 페이로드 (ESP: Encapsulation Security Payload)

- 데이터 기밀성, 패킷 단위의 무결성, 데이터 원본 인증 및 Replay에 대한 보호를 제공
- 암호화를 제공(AH는 제공하지 않음)
- 암호화는 공유된 대칭키 사용
  - 양단 사이에서 교환되는 데이터를 암호화/복호화하기 위해서 사용
  - 인증기능을 제공하기 위해 AH와 같은 알고리즘 이용
- 전송모드
  - ESP의 인증기능들은 오직 고유 IP 페이로드만을 보호, 고유 IP 헤더는 보호하지 않음
- 터널모드
  - 인증은 고유 IP 헤더와 IP 페이로드를 보호한다.
  - 새로운 IP 헤더는 보호하지 않음
  - 일반적으로 ESP 터널모드는 두 방화벽 사이에 터널을 만들고 통신하는 동안 방화벽 뒤의 실제 통신에 참여하는 호스트들에 대한 내부 주소정보를 숨기기 위해서 사용
  - ESP는 단독으로 혹은 AH와 함께 사용 가능
  - 두 개의 프로토콜을 사용하면 호스트와 호스트 사이, 방화벽과 방화벽 사이 또는 호스트와 방화벽 사이에 인증이

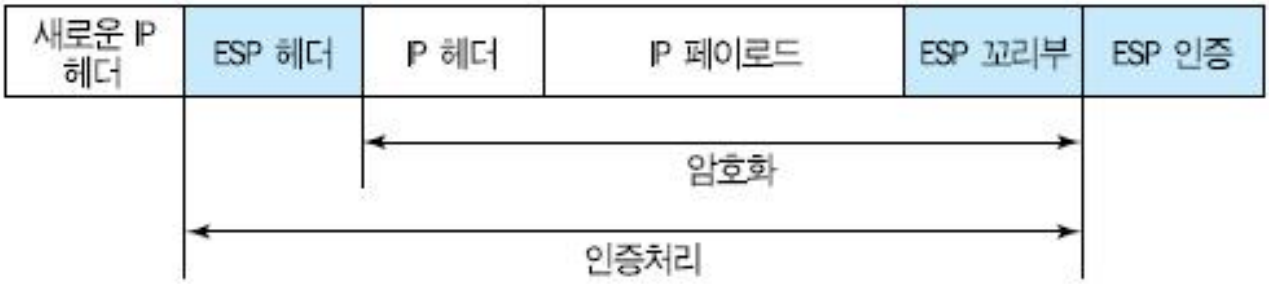
- ESP 전송모드, 터널모드별 삽입형태

원본 데이터

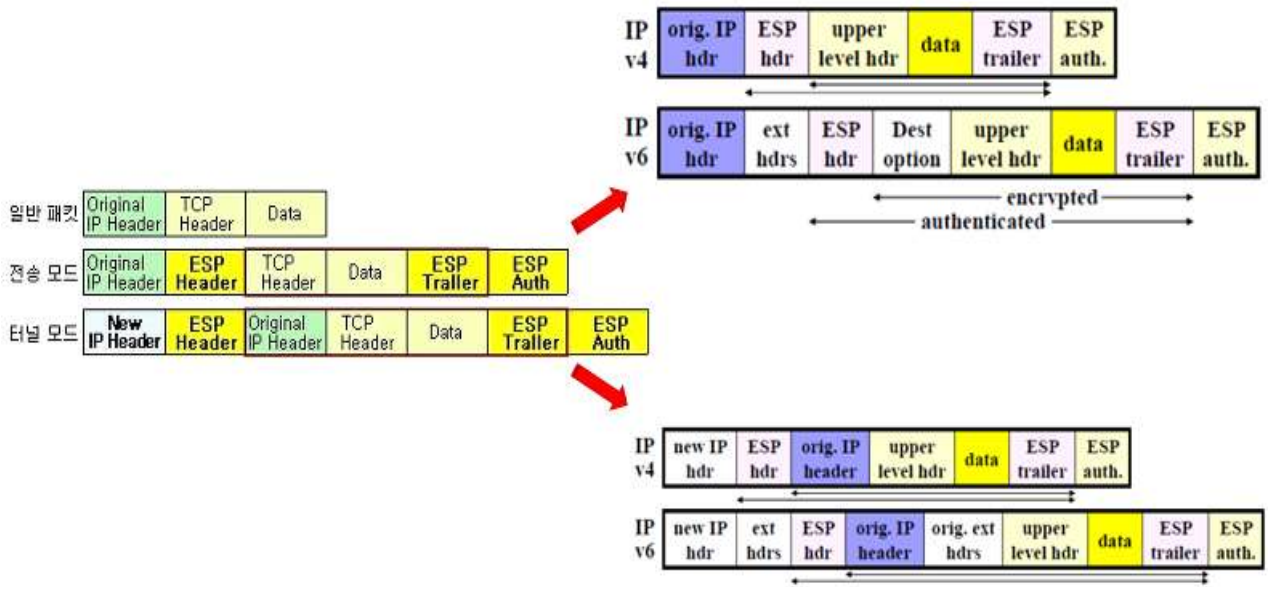


ESP - 전송 모드에 의해 보장된 원본 데이터

ESP - 터널 모드에 의해 보장된 원본 데이터



- ESP 전송모드, 터널모드별 삽입형태



학습내용2 : VPN의 미래

1. MPLS

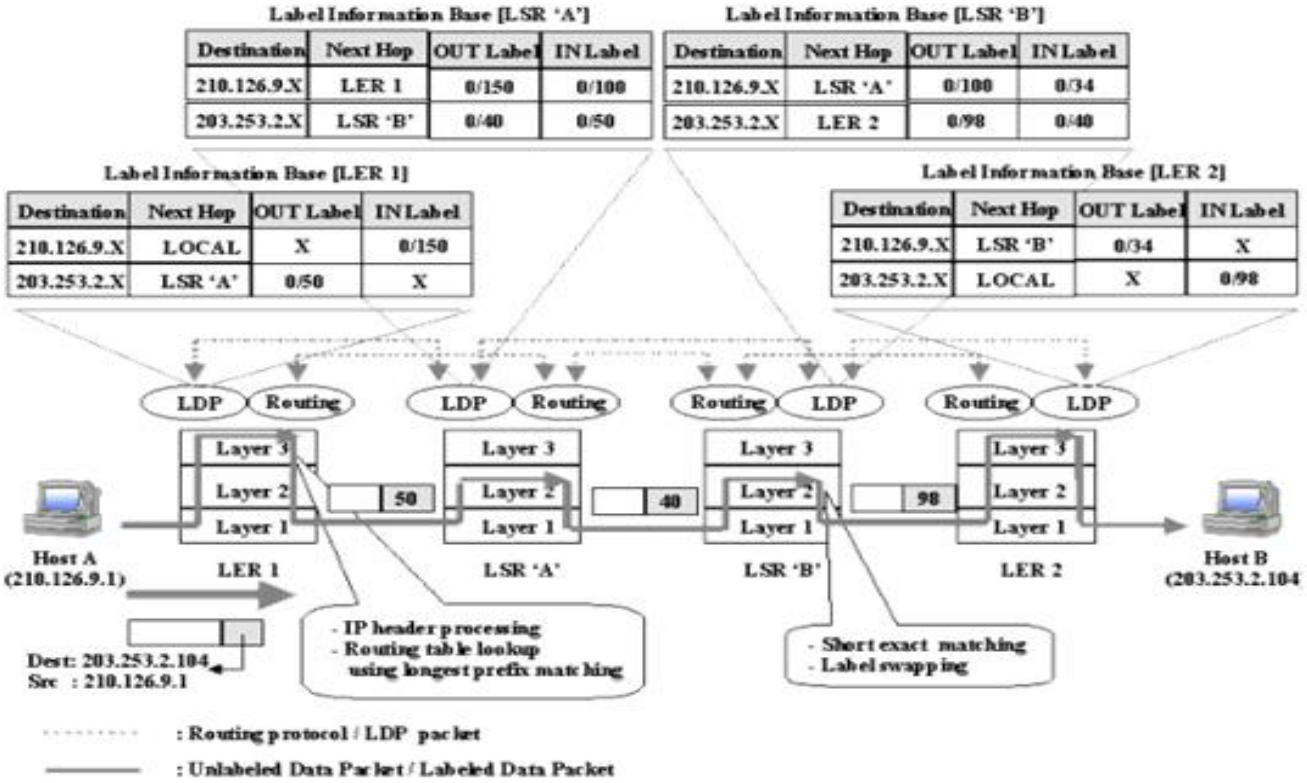
1) 개요

- 자체적인 터널링 기능
- 대다수의 링크 계층 프로토콜을 지원
- 기존 IP 네트워크의 비효율적인 라우팅 방식과, 속도를 개선
- QoS(Quality of Service) 측면에서도 상당한 이점

2) MPLS

- 시스코사의 태그 스위칭(Tag Switching)과 IBM의 ARIS(Aggregate Route-based IP Switching)를 결합해 IETF에서 정한 표준
- 유입되는 패킷을 진입부분에서 3계층 주소를 이용해서 해당 라우터가 갖고 있는 레이블 정보와 비교하여 부가적인 MPLS 레이블정보를 덧붙임
- 레이블이 부가된 패킷은 이제 MPLS 네트워크 내에서는 오직 레이블로만 스위칭 됨
- 레이블 스와핑(Label swapping): 현재 부여 받은 레이블이 다음 라우터에서 새로운 레이블로 변경되는 작업
- 레이블 스와핑이 반복되면서 목적지로 스위칭 됨

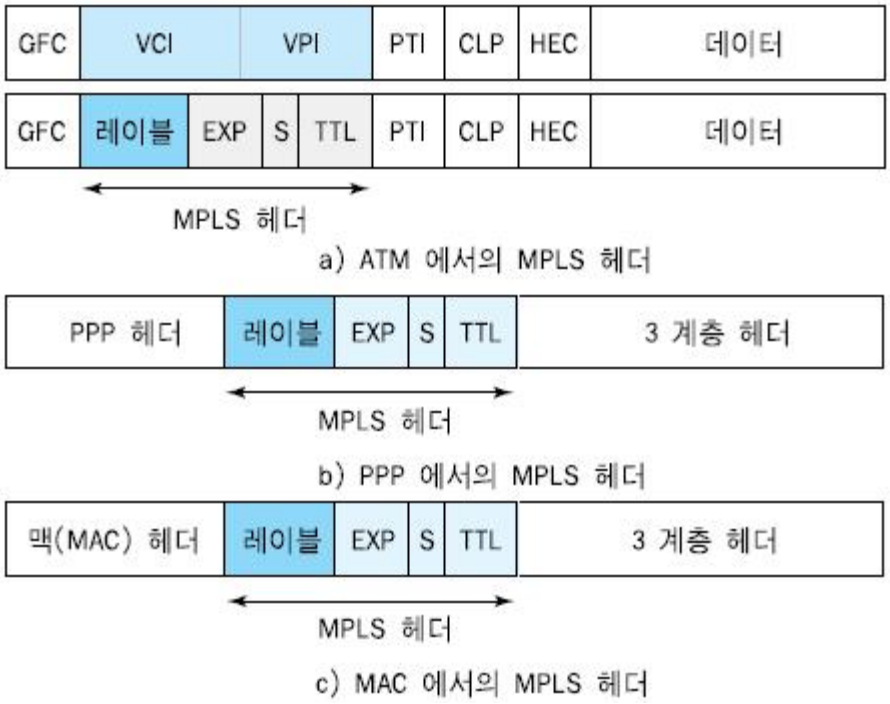
3) MPLS 전송 동작



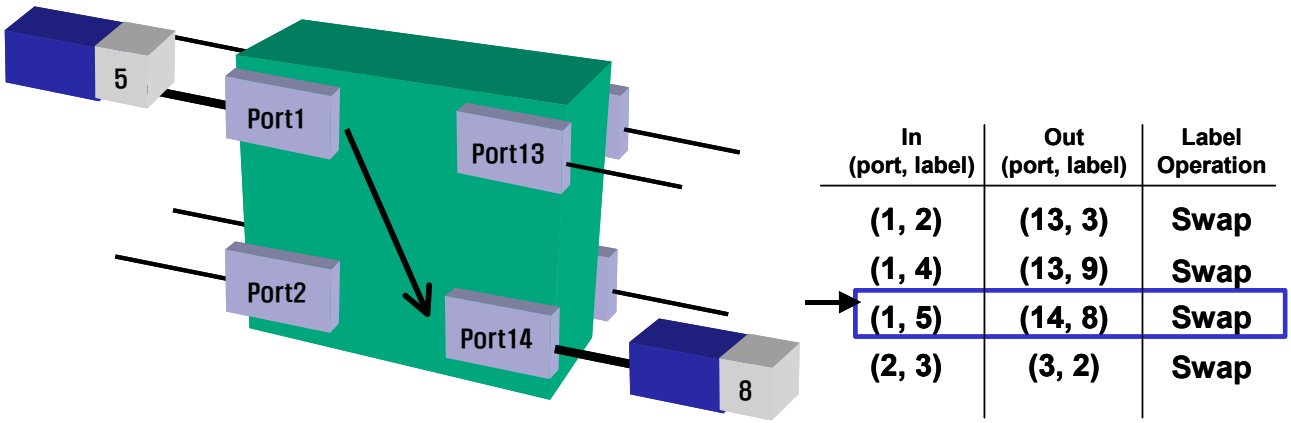
4) MPLS 기본 용어

용 어	의 미
Label	3계층 주소 대신 스위칭에 이용되는 정보
Label binding	특정 데이터의 흐름과 label을 대응
Label swapping	유입된 데이터의 레이블과 전달할 레이블을 교환
Label distribution	인접 라우터들과스위칭을 위한 레이블 정보 교환
LSR(Label Switch Router)	Label을 이용하여 스위칭 하는 라우터
LER(Label Edge Router)	MPLS 네트워크의 테두리에 있는 라우터
LDP(Label Distribution Protocol)	LSR간에 label 할당 정보를 교환하는 프로토콜
LIB(Label Information Base)	Label 할당에 관한 정보가 있는 표
Ingress LER	들어오는 것, ingress LER
Egress LER	나가는 것, egress LER

5) MPLS 데이터포맷



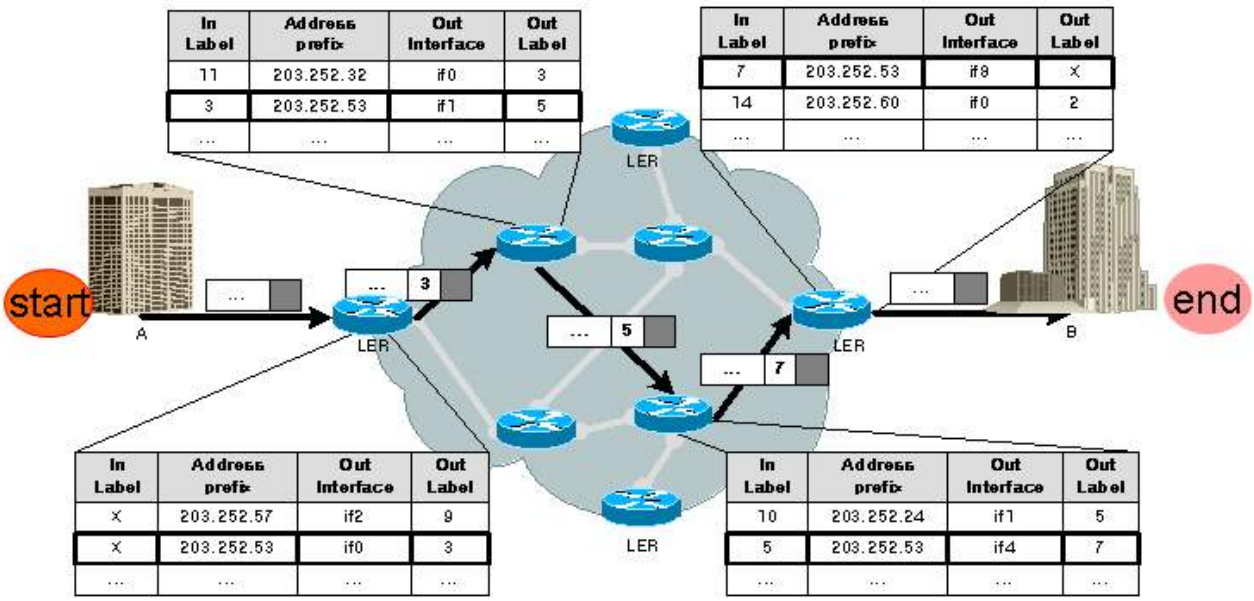
6) 레이블 스와핑(Label Swapping)



In (port, label)	Out (port, label)	Label Operation
(1, 2)	(13, 3)	Swap
(1, 4)	(13, 9)	Swap
(1, 5)	(14, 8)	Swap
(2, 3)	(3, 2)	Swap

- LSR은 입력 포트와 레이블을 보고 출력 포트와 레이블을 판단
- 이런 행동은 LER을 제외한 모든 LSR에서 수행
- LER은 레이블이 없는 패킷에 레이블을 부여하거나 외부 네트워크로 전송할 때 레이블을 삭제하는 역할

7) MPLS 네트워크에서의 스위칭



① A에서 B로 향하는 패킷을 전송하였다고 가정

② Ingress LER은 A의 패킷을 받아 Address prefix를 검출하고 미리 할당된 값에 따라, 출력 인터페이스와(out interface) 레이블(out label)을 부가한다. LER 역시 레이블을 사용하는 라우터 이므로 LSR 임

③ LER은 label이 부가된 패킷을 MPLS망 내부의 LSR에게 출력 인터페이스로 전송한다. [그림 15-18]의 ingress LER의 LIB는 출력 인터페이스와 출력 레이블이 (if0, 3)로 설정 되어 있음

④ 해당 패킷을 전달받은 LSR은 이제 더 이상 Address prefix를 보지 않고, 입력 레이블(In label)만을 보고 스위칭 테이블에서 선택한다. 즉, (if0, 3)에서 (if1, 5)로 레이블 스와핑이 이루어 진 것을 확인할 수 있음

⑤ LSR은 이제 해당 패킷을 전송하고, 이를 받은 LSR은 레이블 5번을 갖는 패킷이 유입되고 있음을 알고 레이블을 할당하기 위해 테이블을 검색

⑥ (if4, 7) 이 입력 레이블 5에 대한 출력 정보이므로, 해당 패킷을 다음 LSR에게 전송

⑦ 패킷은 상대편인 B의 지점까지 가는 마지막 LSR인 egress LER에 도달

⑧ LER은 더 이상 레이블이 필요 없다는 것을 인지하고 레이블을 떼어낸 후 B에게 전송하게 된다. 이때는 보통의 패킷과 동일한 형태로 전달

2. MPLS VPN

1) 정의

- 기존 인터넷에 그대로 적용가능
- 2계층의 스위칭 속도와 3계층의 라우팅 기능을 접목
- 짧고 고정된 길이(4byte)의 레이블(label)을 이용하여 스위칭
- 패킷 전달(packet forwarding)은 레이블 스와핑(label swapping)으로 수행
- 패킷 지연시간 감소
- 레이블 부여는 LER에서만 수행
- 네트워크 내의 라우터와 스위치의 부담을 덜어준다
- 여러 가지 다양한 서비스 제공 가능: QoS(Quality of Service), VoIP(Voice over IP), TE(Traffic Engineering) 등
- 가입자에게 일정한 대역폭을 할당할 수 있어 높은 수준의 서비스 지원 가능
- 사설주소 체계 사용 지원(RFC1918)

2) 터널링

- MPLS VPN은 MPLS 자체가 터널링을 지원한다는 커다란 장점을 제공
- 레이블을 이용하여 터널링 수행
- 일단 LER에서 레이블을 부여하기 때문에 MPLS 네트워크 내부에서는 해당 레이블을 부여 받은 데이터의 흐름 내로 침입이 불가능

3) 문제점

- 라우팅 테이블의 수가 급격히 증가
- 터널링 IPSec VPN에 비해 가입자단 라우터의 부하를 줄일 수 있지만 MPLS VPN은 암호화 기능이 상대적으로 취약

3. VPN의 미래

- 현재 VPN은 VoIP와 같은 초고속 인터넷 기술을 이용한 응용 서비스의 밑거름이 되고 있음
- 보안성이 약하다는 단점을 보완
- 추세
  - IPSec의 강력한 보안, 인증기능 + MPLS의 강력한 네트워크 지원능력 및 기능
- IPSec와 MPLS의 혼용 시에는
  - IPSec은 원격접속 시에,
  - MPLS는 LAN-to-LAN에
  - 백본망과 기업망에는 IPSec+MPLS 구성이 예상되고 있음
- 앞으로 Mobile Security를 해결해야 할 것임

【학습정리】

1. IPSec은 데이터 원본 인증, 데이터 무결성, 데이터의 기밀성, Relay 보호 등의 기능을 제공한다.

2. MPLS는 자체적인 터널링 기능과 대다수의 링크 계층 프로토콜을 지원하며, 기존 IP 네트워크의 비효율적인 라우팅 방식과 속도를 개선하였다.