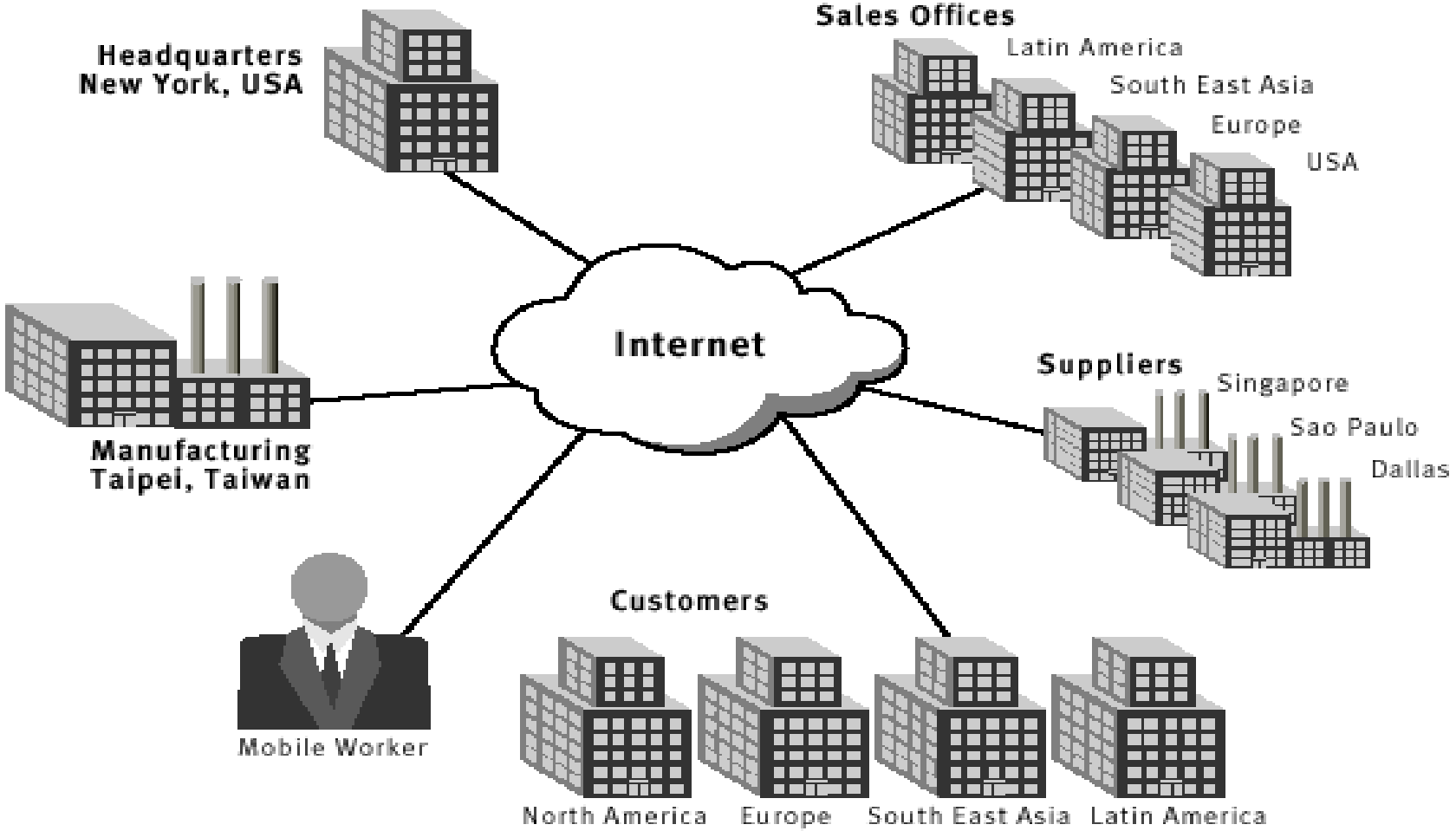
VPN (가상사설망) 기술의 이해

차례

VPN이란?

- VPN
  - **Virtual Private Network** : 가상 사설망
  - 공중망을 통한 연결을 전용선처럼 사용하는 것
  - 기존의 인터넷 서비스를 통해 하나의 사설 네트웍처럼 사용하는 가상 사설망
  - 터널링 프로토콜과 보안 과정을 거쳐 내부 기밀을 유지
  - 단일 회사만 사용하는 전용선의 개념과 대비
  - 공중망을 공유하기에 낮은 비용으로 동일한 네트웍 성능을 제공
  - Extranet과 광범위한 Intranet 지원

VPN이란?


Headquarters
New York, USA
Sales Offices
Latin America
South East Asia
Europe
USA
Internet
Manufacturing
Taipei, Taiwan
Suppliers
Singapore
Sao Paulo
Dallas
Customers
Mobile Worker
North America
Europe
South East Asia
Latin America

VPN의 확산 배경(기업측면)

- 컴퓨터의 도입
  - 정보 공유의 확산
  - 신속한 의사 결정
- 근무환경 변화, 또 다른 제한 발생
  - 업무 범위의 확대
  - 재택 근무의 확산
  - 사외 network구성의 필요성 대두
- 기업내의 사내 network의 사외로 확대 요구
  - 외부로의 network 구성에 막대한 시설 투자비 요구
  - 구성 network 운영, 관리 비용 증가

VPN의 확산 배경(ISP측면)

- 단순 Network 접속 서비스의 한계
- 고부가가치 수익 창출 요구
- 다양한 응용서비스 제공을 위한 기반 서비스 필요
  - 전자 상거래
  - interactive한 교육(화상 교육, 멀티미디어 서비스)
  - contents hosting
  - 전화서비스와 음성,데이터 통합 관리 서비스
- 새로운 형태의 관리형 네트워크 서비스 필요

VPN의 확산 배경

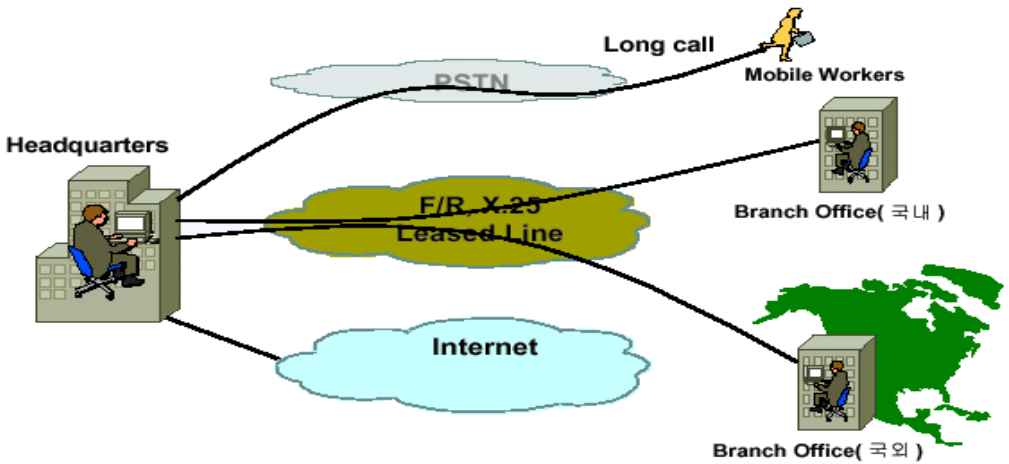
- 컴퓨터의 도입

- 인터넷
  - 구조상 정보 체계, 보안구축 불가능
    - 보안(인증, 무결성, 비밀성 보장…)
  - 자원(resource)의 공유
    - QoS의 불확실성
    - 최선형(best-effort) 패킷 전달 방식, 단일 QoS
    - 액세스점의 병목현상, 응답 속도의 불균일, 패킷 비순서성
- 전용선(Leased Line) 사용
  - 문제점 해결, 비용의 증가

- VPN + 인터넷
  - 비용 절감, 자원의 효율성

VPN의 확산 배경

- 기존의 기업 WAN 환경
  - network사업자의 Leased Line, FrameRelay망을 이용한 자체적 intranet 구축
  - 단점
    - 운영 및 관리 비용 증가
    - 국외 지사의 경우 가격대비 효율성 떨어짐
    - 재택근무자의 증가로 원격 사용자 통신비용 증가



VPN의 확산 배경

- 가상 사설망(VPN)의 대두
  - 기존의 ISP의 인터넷망 이용 가상의 사설망 구축
  - 가상 사설망의 관리운영은 ISP 담당
  - ISP의 POP을 이용하여 기업 내부 network 접근 가능
  - 암호화를 통한 정보 보호 제공
  - 인터넷의 일정 대역폭 할당, QoS 보장 필요

pop : points of presence로 가입자가 ISP에 접속하는 지점

VPN의 확산 배경

- VPN의 이용 분야
  - 재택 근무자, mobile user, telecommuter
  - 본사와 지사, 지사와 지사
  - 협력 업체와 네트워크를 통한 extranet 구성
  - 모 기업과 협력 업체간의 연결
  - 동종 기업간의 자료 공유
  - 전자 상거래와 보안

VPN의 확산배경

⌘ VPN의 장단점(기존의 전용망에 비해)

	내 용
장점	저비용 network 관리 및 운영 비용 절감 기업 network의 유동성 확보 기업의 통신 비용 절감
단점	보안성 VPN 장비간의 호환성 관리 편의성 QoS보장 표준화 인터넷의 성능 불안정

VPN의 종류

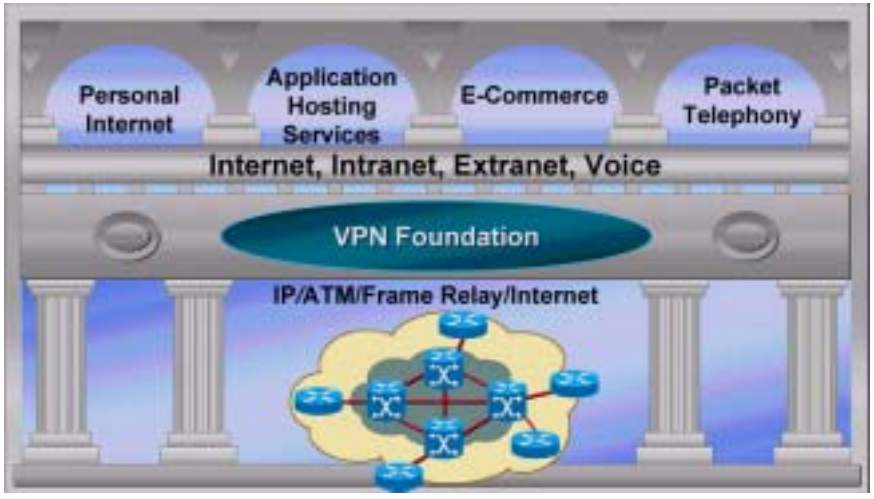
⌘ 구조에 따른 분류

- intranet VPN : 공중망을 통한 원격지와의 LAN 연결.

- Extranet VPN : Intranet VPN과 Remote Access VPN이 결합된 총체적인 형태.

- Remote Access VPN :
  원격지의 사용자가 해당 지역의 ISP 가 제공하는 인터넷에 접속후 서버쪽과 접속하는 형태.

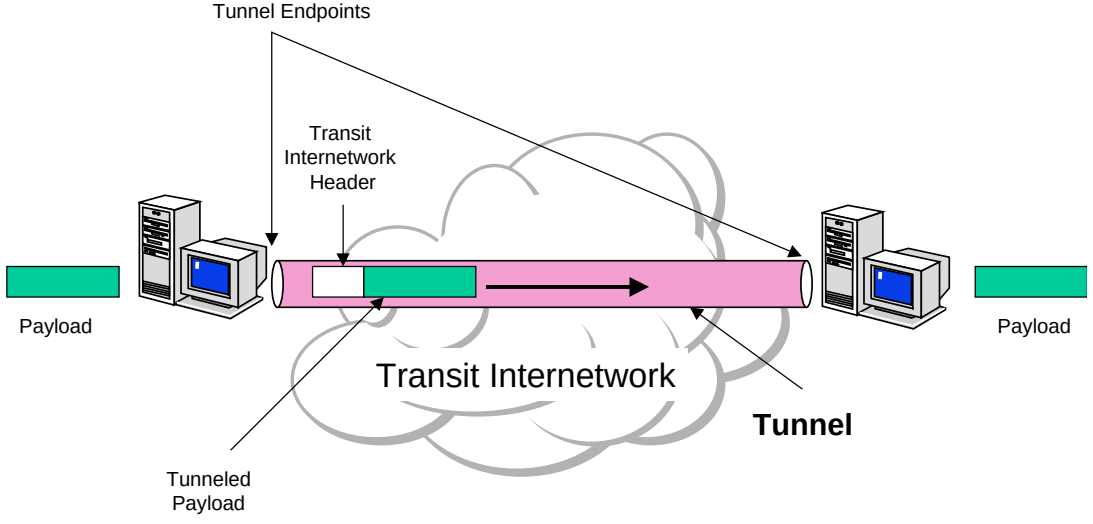
VPN Service & Architecture



Service	Architecture	Technologies
Access VPN	Client-Initiated NAS-Initiated	Layer 2F/2TP, IPSec Dial, ISDN, DSL, Mobile IP, Cable
Intranet VPN	IP Tunnel Virtual Circuit MPLS	GRE, IPSec Frame Relay, TM IP or IP + ATM
Extranet VPN	IP Tunnel Virtual Circuit MPLS	GRE, IPSec Frame Relay, ATM IP or IP + ATM

VPN 구성 필수 요소

- 터널링 기법을 이용한 네트워크 보안 및 데이터보안 지원
- 암호화 알고리즘을 통한 DATA의 손실 및 변형 방지
- 압축기법 활용을 통한 네트워크 속도 저하 문제 해결
- Key management 기능을 통한 LAN to LAN 혹은 Dial-up to LAN의 신뢰성 확보
- VPN 표준 프로토콜인 IPSec(IP Security) 지원



VPN의 종류

구현 방식

VPN 전용 server

- VPN client와 내부 네트워크 보안이 필요한 곳에 독립적 설치
- 대역폭 증가, 고속 통신 필요
- 확장성 용이
- 고비용 - 장비 구입
- checkpoint, radguard, vpnet, shiva

Router 형

- 전송경로상에 있는 router나 access server에 VPN 기능 추가
- router의 성능에 따라 VPN성능 좌우
- point-to-point tunneling
- 보안문제 취약 - router
- cisco, shiva, intel,...

firewall 형

- firewall에 VPN기능 추가
- bottleneck현상 발생 가능
- checkpoint, 퓨쳐시스템, 시큐어소프트

VPN의 종류

- VPN 서비스 형태
  - Remote Access VPN
    - PSTN, ISDN, DSL, Cable Modem...
  - LAN to LAN VPN(Site-to-site VPN)
  - 기업에서의 LAN to LAN VPN
  - 기업에서의 LAN to Client VPN
  - ISP에서의 VPN

Remote Access VPN

- Mobile Worker, Telecommuter, 재택근무자

- Client Initiated VPN
  - 국내외 가능
  - PC에서 구현 가능
  - QoS 지원 어려움
- NAS(Network Access Server) Initiated VPN
  - 국내끼리만 가능
  - 타 ISP와의 연동 안됨

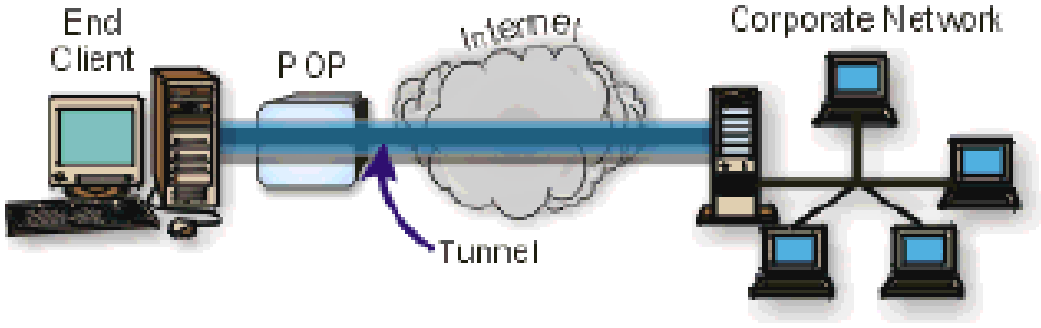
Remote Access VPN

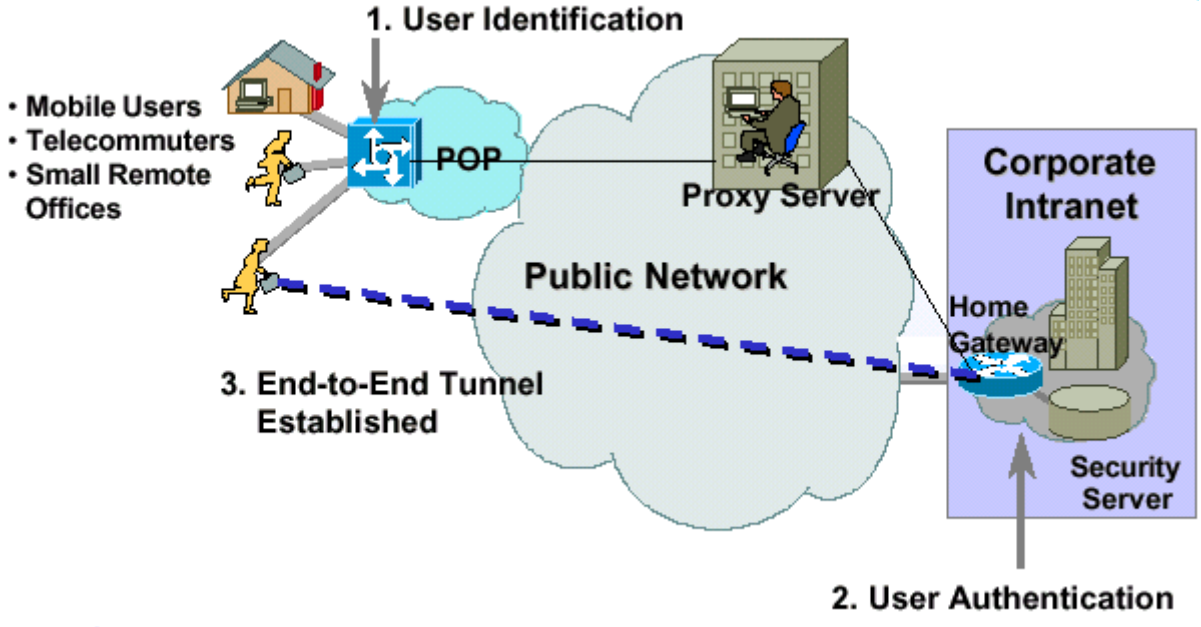
⌘ Client Initiated VPN

- PC등 사용자 장비에서 VPN전용 S/W를 이용하여 본사의 server(gateway)까지 tunnel 형성
- 특징
  - public IP 주소 사용
    - public IP : internet 접속
    - private IP : 사내 network 접속
  - 사용자 장비 관리 필요 : VPN S/W 관리, upgrade
- 사용 Tunneling 방식
  - IPSec
  - PPTP, L2TP

Remote Access VPN

⌘ Client Initiated VPN





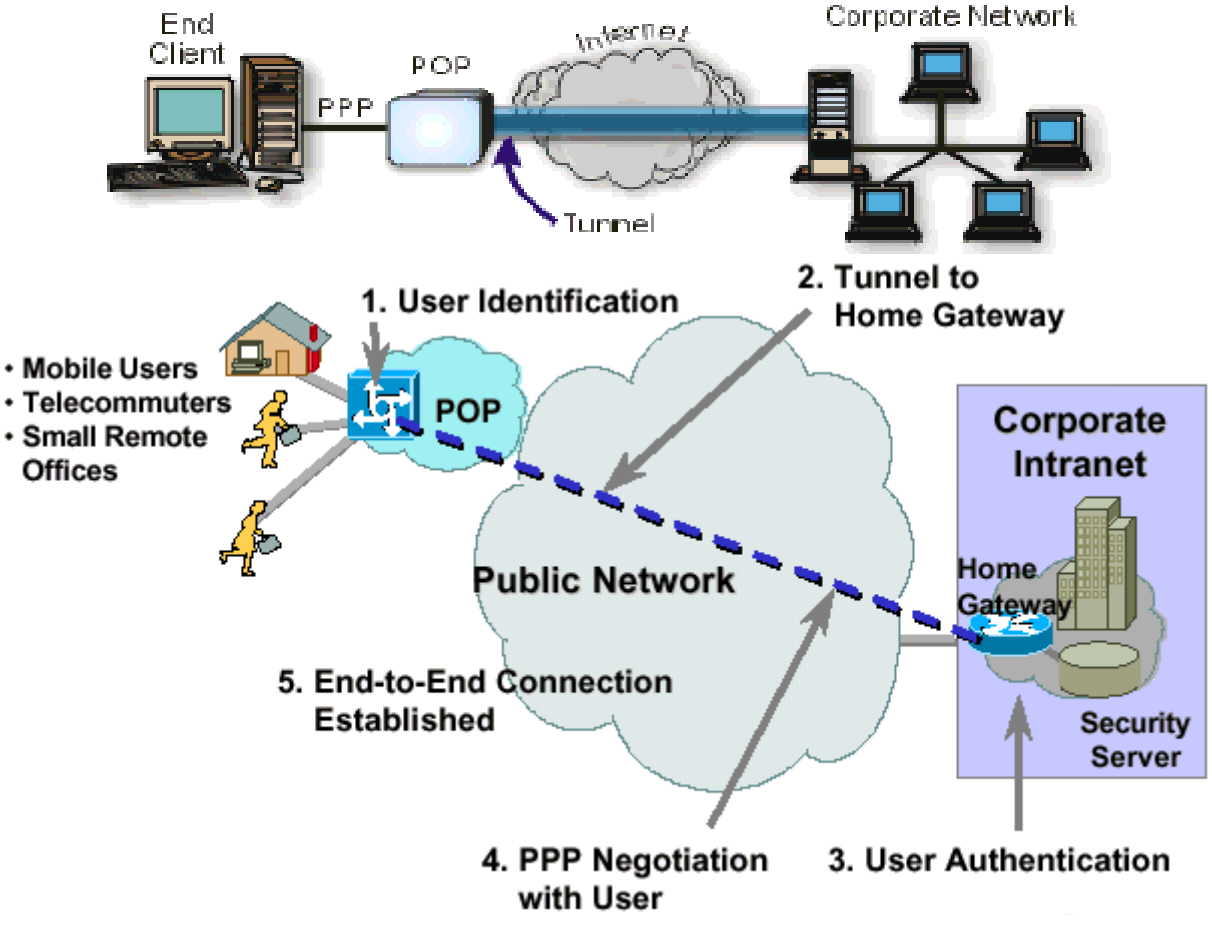
Remote Access VPN

⌘ NAS Initiated VPN

- ISP의 NAS(Network Access Server)에서 본사의 server(Gateway)까지 tunnel 형성
- 특징
  - NAS에 VPN제공을 위한 추가 기능 지원
  - private IP 사용
    - 직접적으로 internet 접속 불가, 사내 network 통한 접속가능
    - client에 VPN s/w 설치할 필요 없음
- 사용 Tunneling 방식
  - L2TP, L2F
- 제공업체
  - cisco, Lucent, 3Com

Remote Access VPN

⌘ NAS Initiated VPN



LAN to LAN VPN

- 본사 network와 지사 network 간의 연결

- IP VPN
  - CPE based VPN
    - 국내외 연결 가능
    - 기업 site에서 VPN 실행
  - Core based VPN
    - 국내만 가능
    - ISP에서 대신 VPN 수행
    - MPLS 이용

* CPE : Customer Promise Equipment

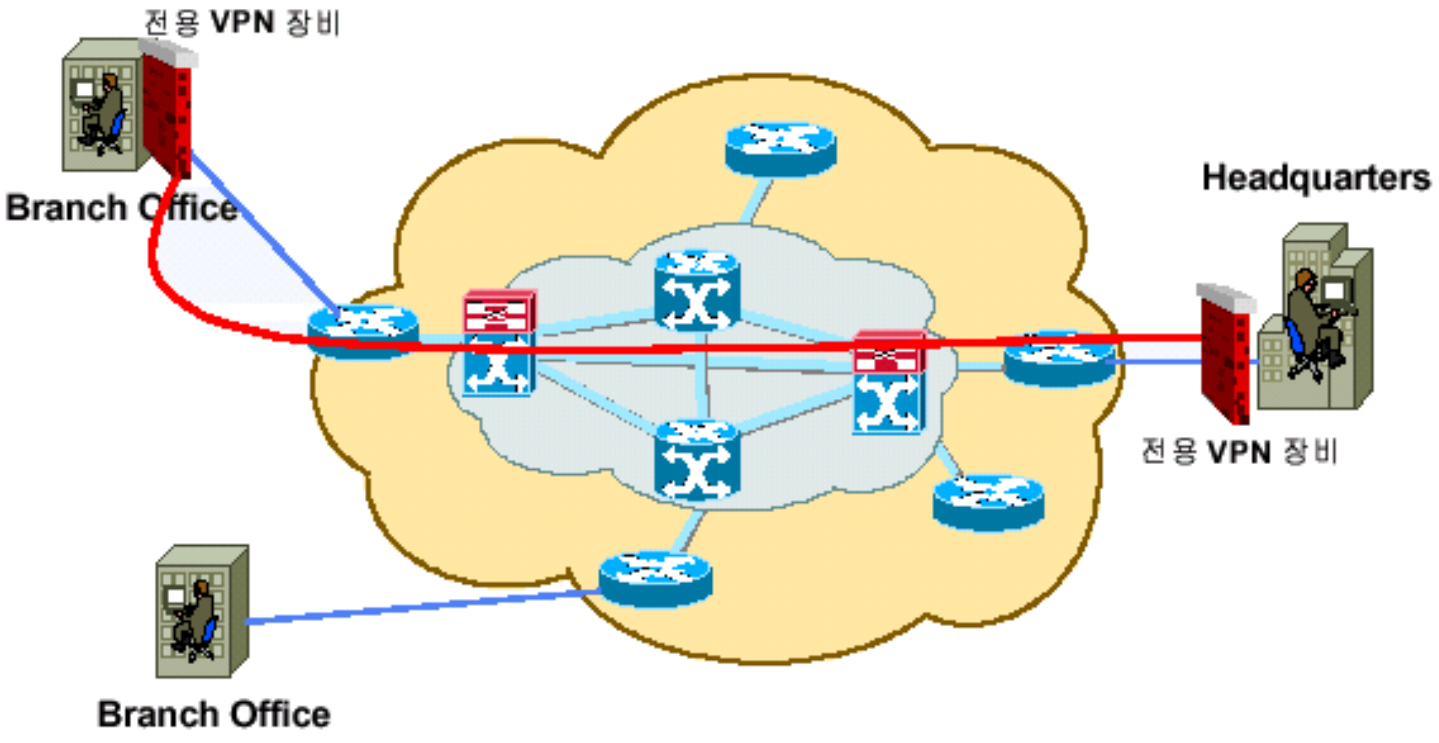
LAN to LAN VPN

⌘ CPE based VPN

- 다양한 VPN 전용 장비 제공
  - Microsoft, Novell, Checkpoint,…
  - VPNet, Lucent, Cisco, 3Com,…
- 특징
  - 기업의 CPE에서 VPN 기능 수행
  - 기업이 독자적으로 구축 및 운영
  - ISP가 VPN management 대행
    - network manage
    - Firewall manage
    - VPN manage
- 사용 Tunneling 방식
  - IPSec

LAN to LAN VPN

⌘ CPE based VPN



LAN to LAN VPN

⌘ Core based VPN

- ISP의 장비(Router 등..)에 VPN 기능 탑재
- 특징
  - VPN 서비스 처리를 위한 기능 추가 필요
  - Core network의 성능 향상에 따라 QoS 서비스 보장 가능
- 체계적인 관리를 위한 Service Management 필요
- 사용 Tunneling 방식
  - IPSec
  - MPLS

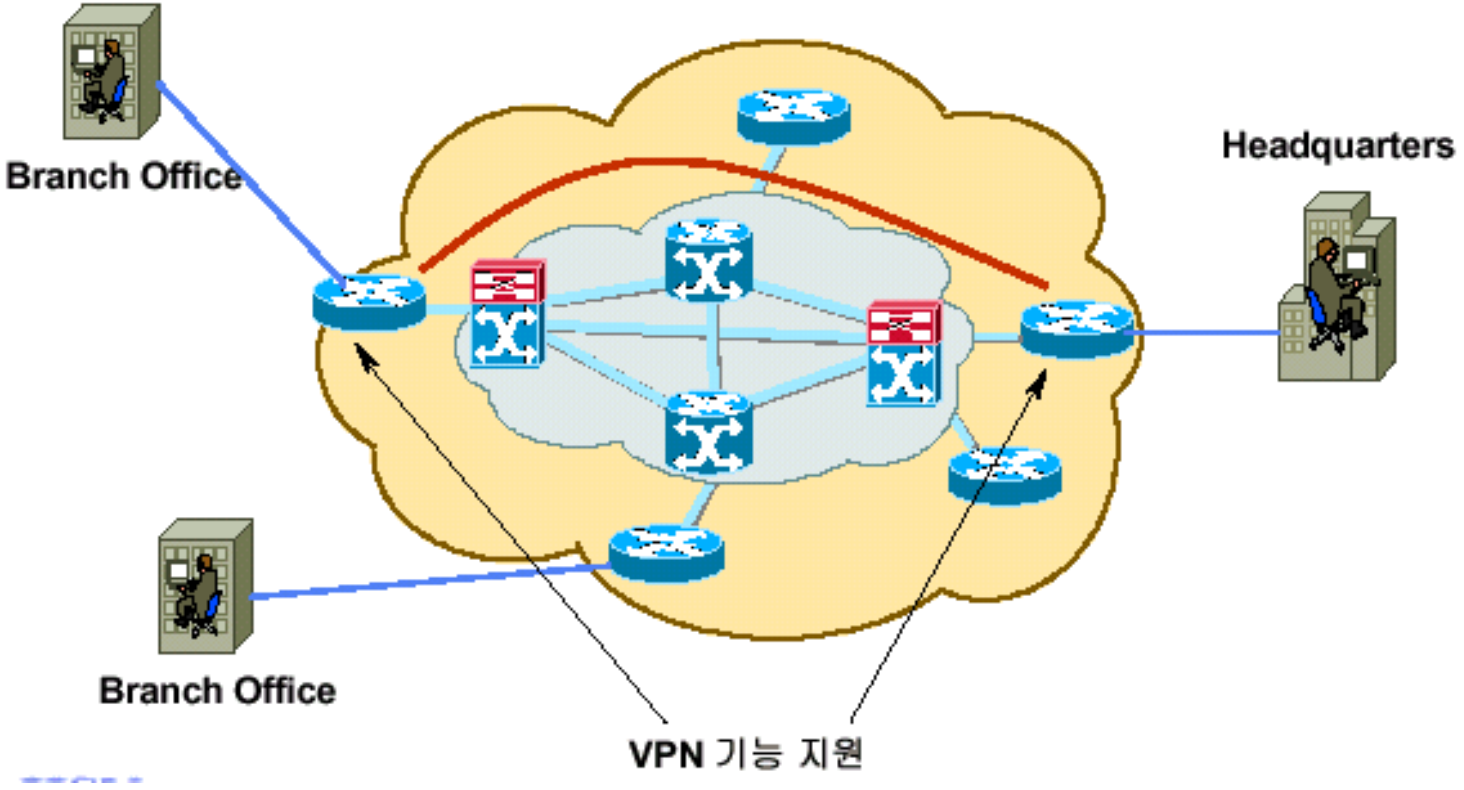
LAN to LAN VPN

⌘ Core based VPN

- MPLS (Multi-Protocol Label Switching)
  - Cisco Tag switching 기반
- ATM, FrameRelay 적용 가능
- Label을 이용한 packet forwarding load 감소
- Traffic Engineering을 이용한 QoS service 제공 가능

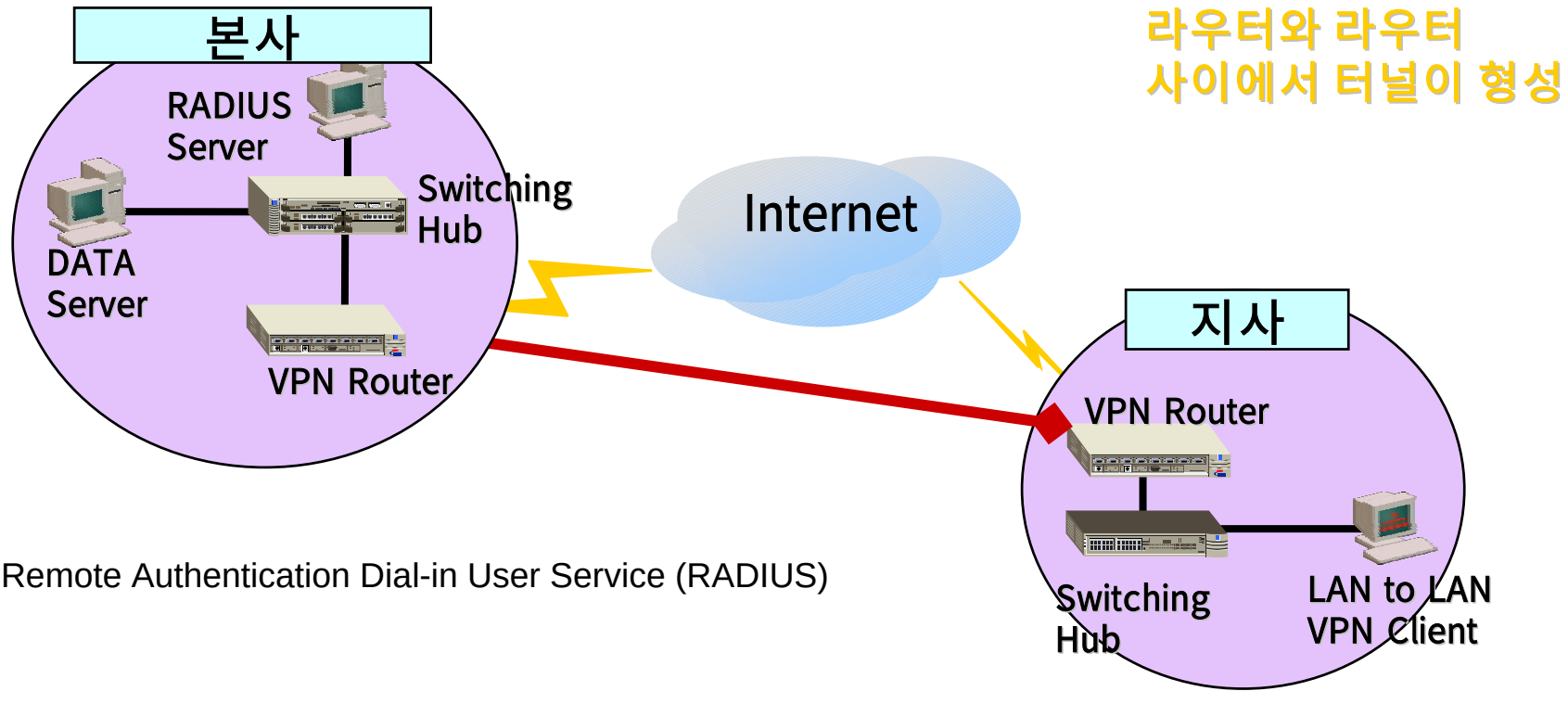
LAN to LAN VPN

⌘ Core based VPN



LAN to LAN VPN

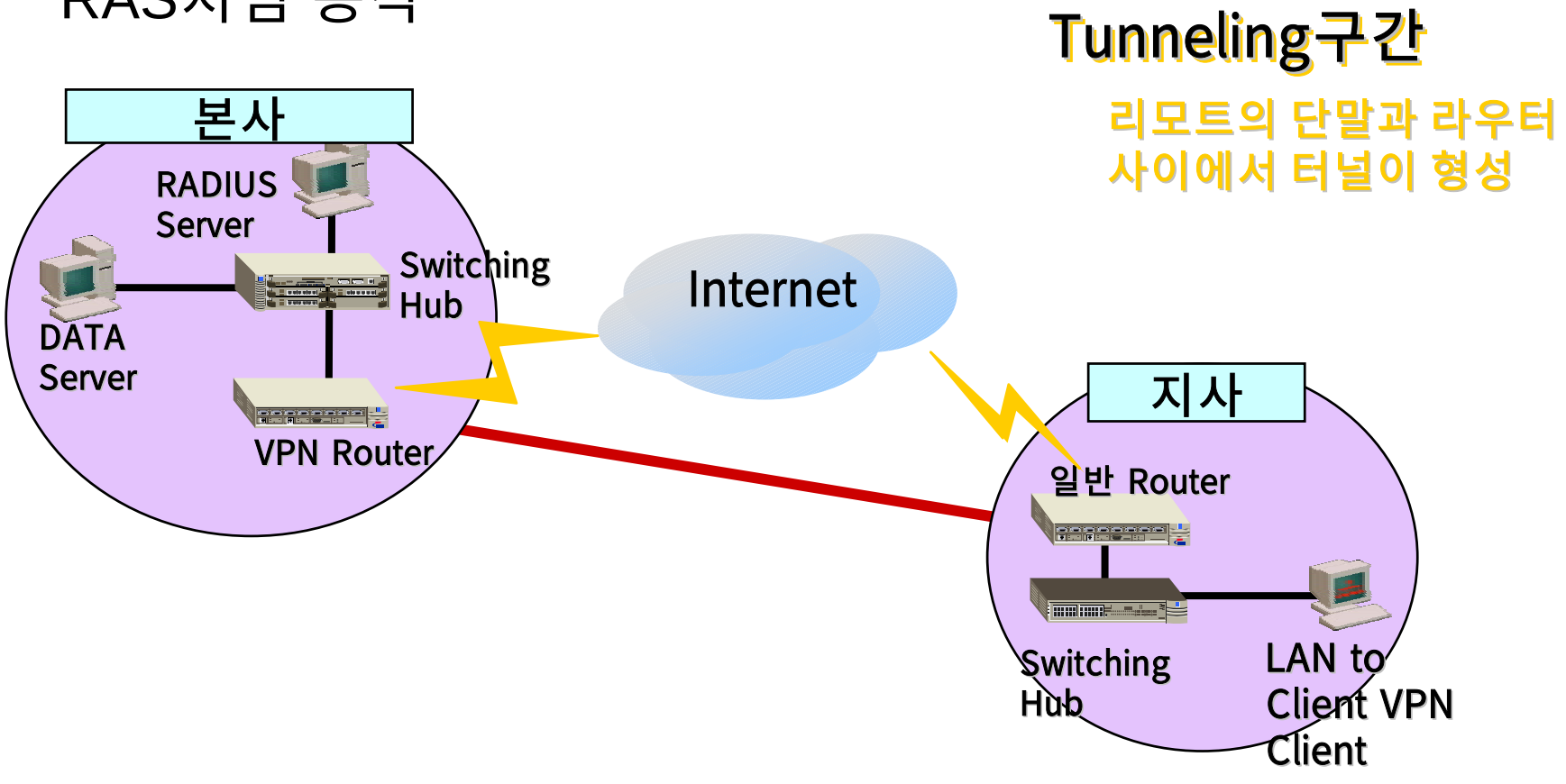
⌘ 기업의 본사와 지사간 연결을 인터넷을 통해 하면서도 마치 라우터 끼리 전용선으로 연결한 것과 같은 동작을 하는 VLL(Virtual Leased Line)



Remote Authentication Dial-in User Service (RADIUS)

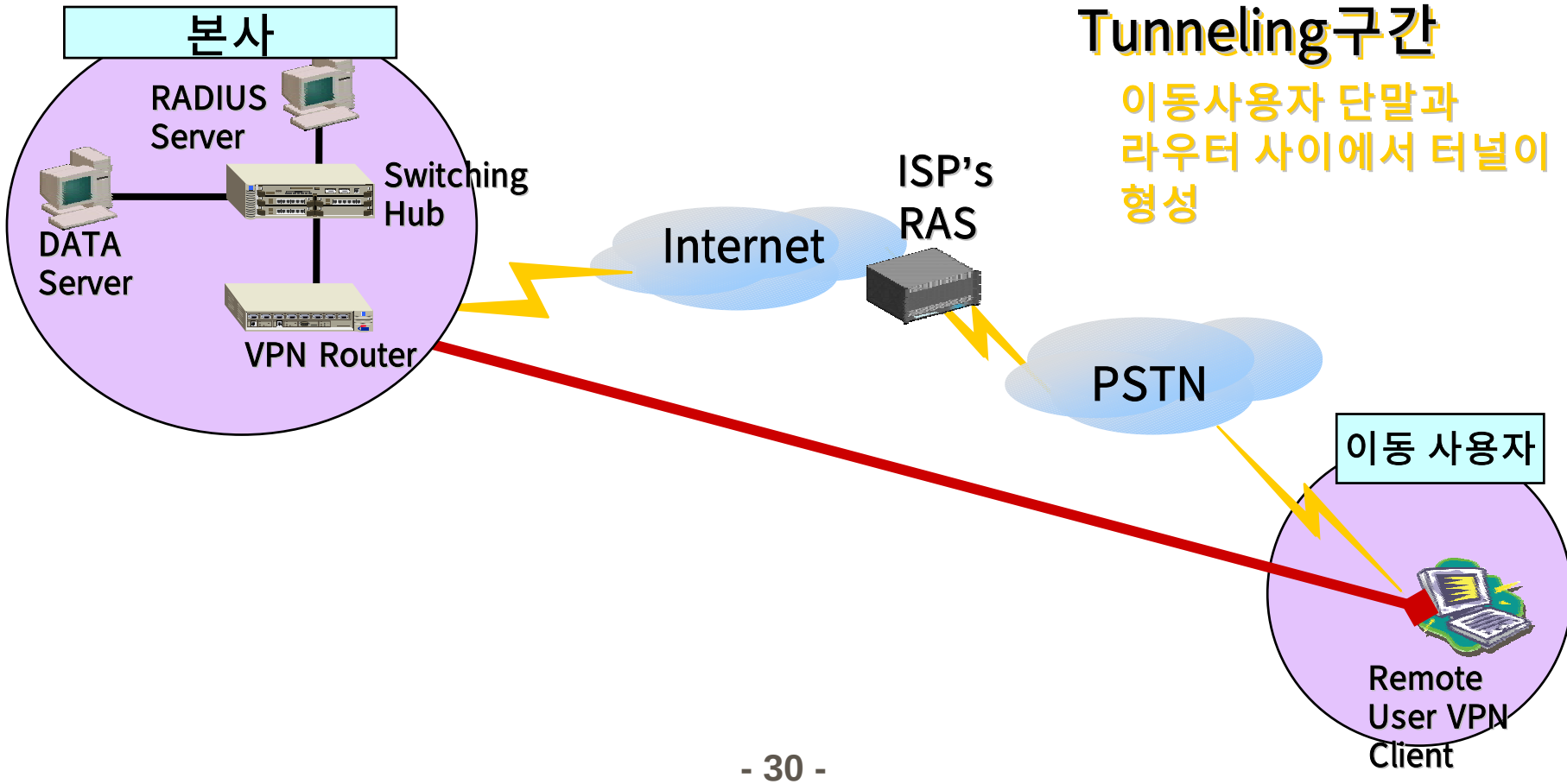
LAN to Client VPN

⌘ 리모트 지역의 PC에서부터 터널이 형성되어 본사의 VPN 라우터에서 터널이 종료되어 본사의 라우터는 마치 RAS처럼 동작

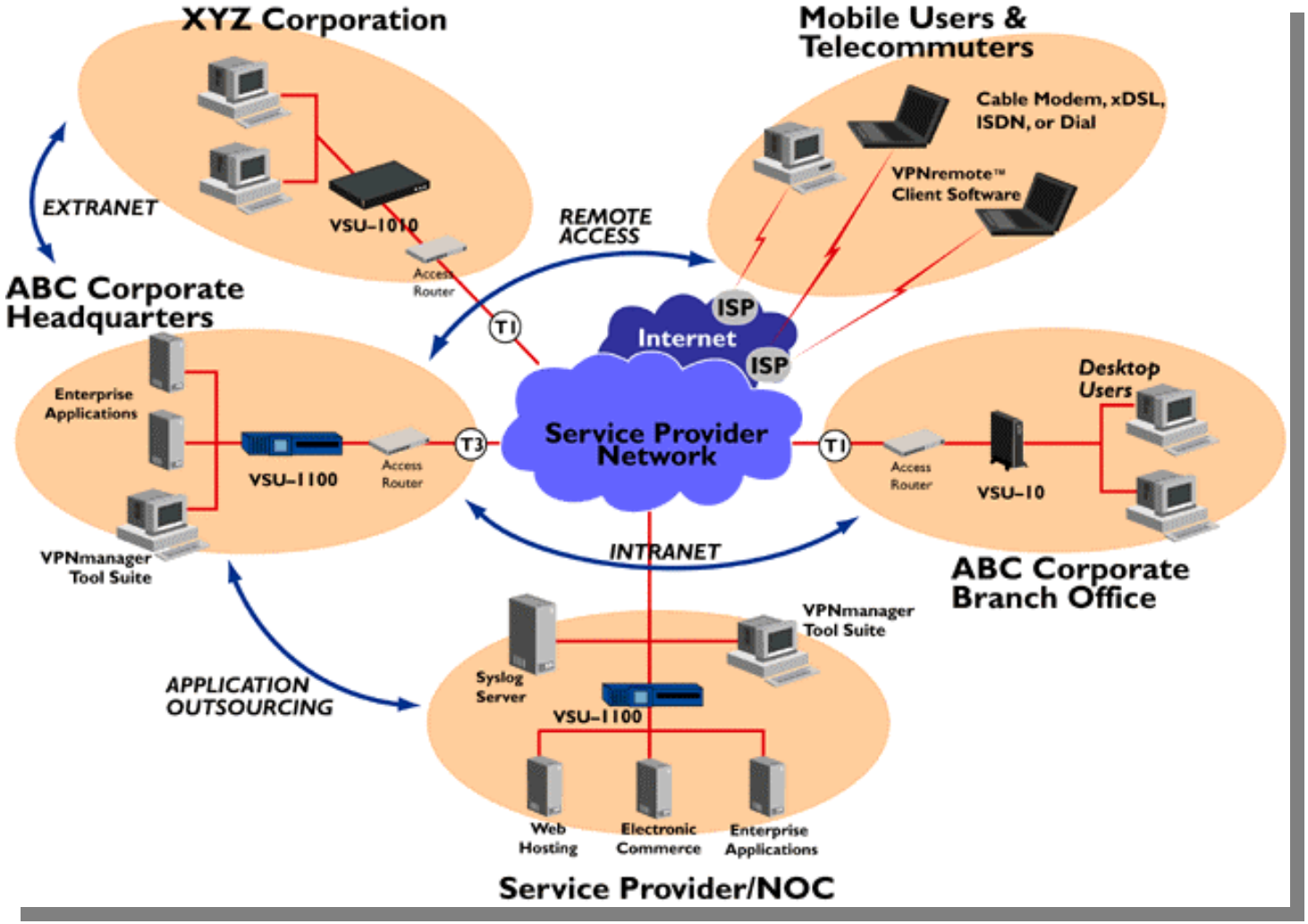


ISP에서의 VPN

⌘ 이동 사용자가 ISP로 전화 접속하여 본사의 라우터로부터 인증을 획득한 후 VPN 터널 형성



VPN 구성 예


XYZ Corporation
Mobile Users &
Telecommuters
Cable Modem, xDSL,
ISDN, or Dial
VPNremote™
Client Software
EXTRANET
VSU-1010
Access
Router
REMOTE
ACCESS
ABC Corporate
Headquarters
T1
ISP
Internet
ISP
Desktop
Users
Enterprise
Applications
VSU-1100
Access
Router
T3
Service Provider
Network
T1
Access
Router
VSU-10
VPNmanager
Tool Suite
INTRANET
ABC Corporate
Branch Office
VPNmanager
Tool Suite
APPLICATION
OUTSOURCING
Syslog
Server
VSU-1100
Web
Hosting
Electronic
Commerce
Enterprise
Applications
Service Provider/NOC

VPN의 핵심 구성 요소

- Tunneling
  - 전용망 환경에서 point-to-point으로 연결한 것과 같은 효과를 얻기 위해 두 종단사이에 가상의 tunnel을 형성하는 것
- Security
  - 암호화
  - 인증
- Quality of Services
  - 기존의 Leased Line, FR망을 사용할 때의 Bandwidth를 보장

VPN의 핵심 구성 요소

- Tunneling
  - Layer2
    - L2F(layer 2 Forwarding)
    - PPTP(Point-to-Point Tunneling Protocol)
    - L2TP(Layer 2 Tunneling Protocol)
  - Layer 3
    - IPSEC(Internet Protocol Security)
    - ATMP(Ascend Tunnel Management Protocol)
    - VTP(Virtual Tunneling Protocol)

VPN의 핵심 구성 요소

⌘ Tunneling 기술의 비교

Exhibit 4 **VPN Technology Standards Compared**

	PPTP	L2TP	IPSec
Mode	Client-server	Client-server	Host-to-host
Purpose	Remote access via tunneling	Remote access via tunneling	Intranets, extranets, remote access via tunneling
OSI Layer	Layer-2	Layer-2	Layer-3
Protocols Encapsulated	IP, IPX, AppleTalk, etc.	IP, IPX, Appletalk, etc.	IP
Security:			
User authentication	None (use PAP, CHAP, Kerberos, Token ID, etc.)	None (use PAP, CHAP, Kerberos, Token ID, etc.)	None (use PAP, CHAP, Kerberos, Token ID, etc.)
Packet authentication	None"	None"	AH header
Packet encryption	None"	None"	ESP header
Key management	None"	None"	ISAKMP/Oakley, SKIP
Tunnel Services	Single point-to-point tunnel, no simultaneous Internet access	Single point-to-point tunnel, no simultaneous Internet access	Multipoint tunnels; simultaneous VPN and public access

Notes

1. Not in standard, not offered
2. Vendor-specific implementation only
3. Refers to IPSec for implementation

VPN의 핵심 구성 요소

⌘ Security

- authentication(인증)
- Integrity(무결성)
- encryption(암호화)
- 방법
  - DES (Data Encryption Standard) : CPU intensive
  - 3DES
  - RC5
  - MPPE

VPN의 핵심 구성 요소

⌘ Quality of Service(QoS)

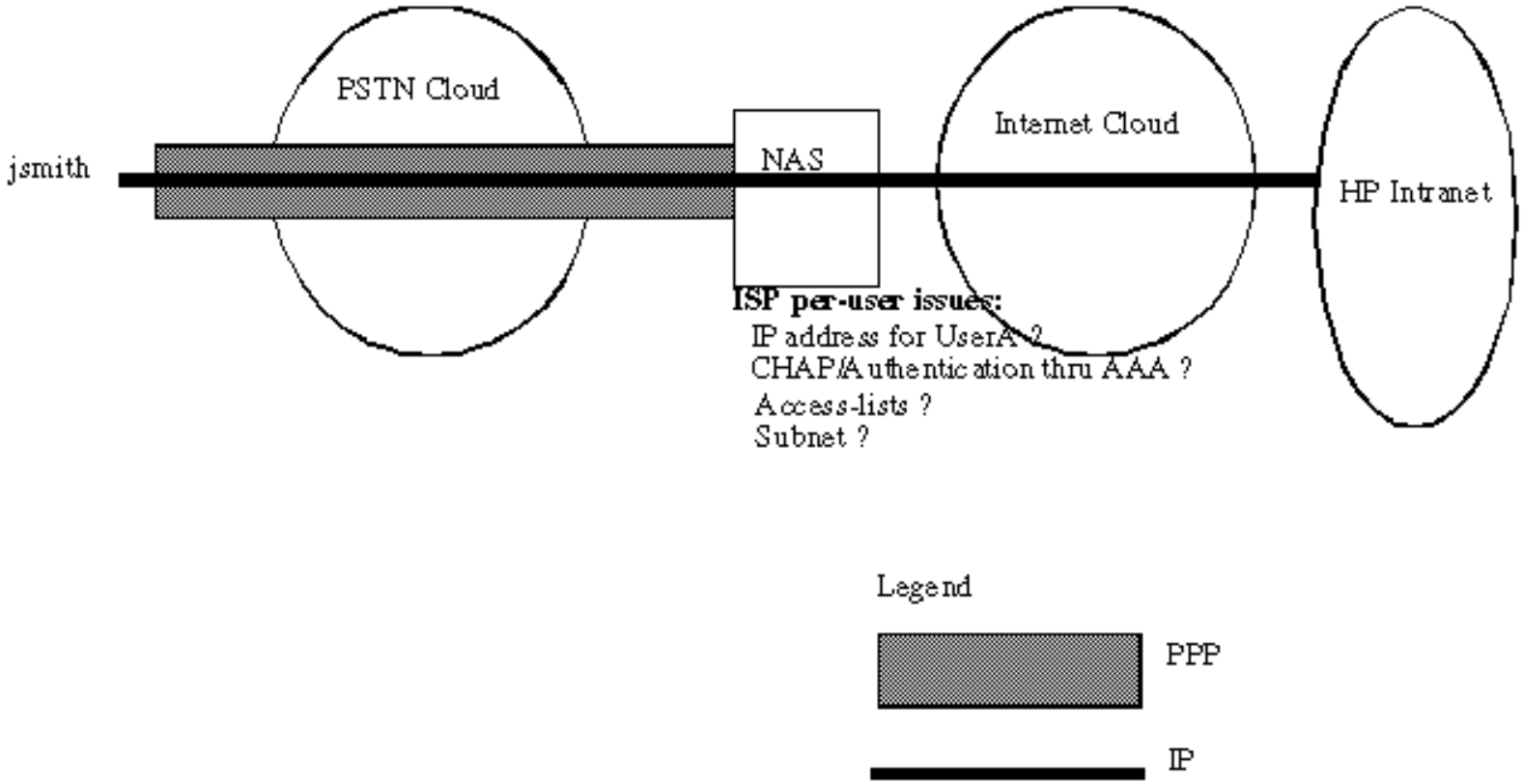
- 기존의 사설망을 사용할 때의 Bandwidth를 보장해야 함
- RSVP : cisco
- CR-LDP : nortel
- diffserv (Differentiated Service)
  - RFC 2474
  - RFC 2475

Tunneling Protocol : L2F

- L2F(Layer 2 Forwarding)
  - Cisco, Nortel, Shiva
    - 원격지의 ISP 장비에서 접근 server측의 tunnel server로 L2F 터널 생성
    - 가상 tunnel은 direct-dial PPP/RAS세션 생성
  - 원격지 사용자의 home site에서 주소 할당이 이루어짐
  - 사용자 인증은 home site의 gateway에서 이루어짐
  - 접근 server는 주어진 domain과 사용자 ID를 가지고 인증
  - FrameRelay나 ATM과 같은 물리적 미디어와 작동 가능 (tunneling이 IP에 의존하지 않음)
  - PPP(point-to-point) 사용
  - 인증 : TACACSA+, RADIUS

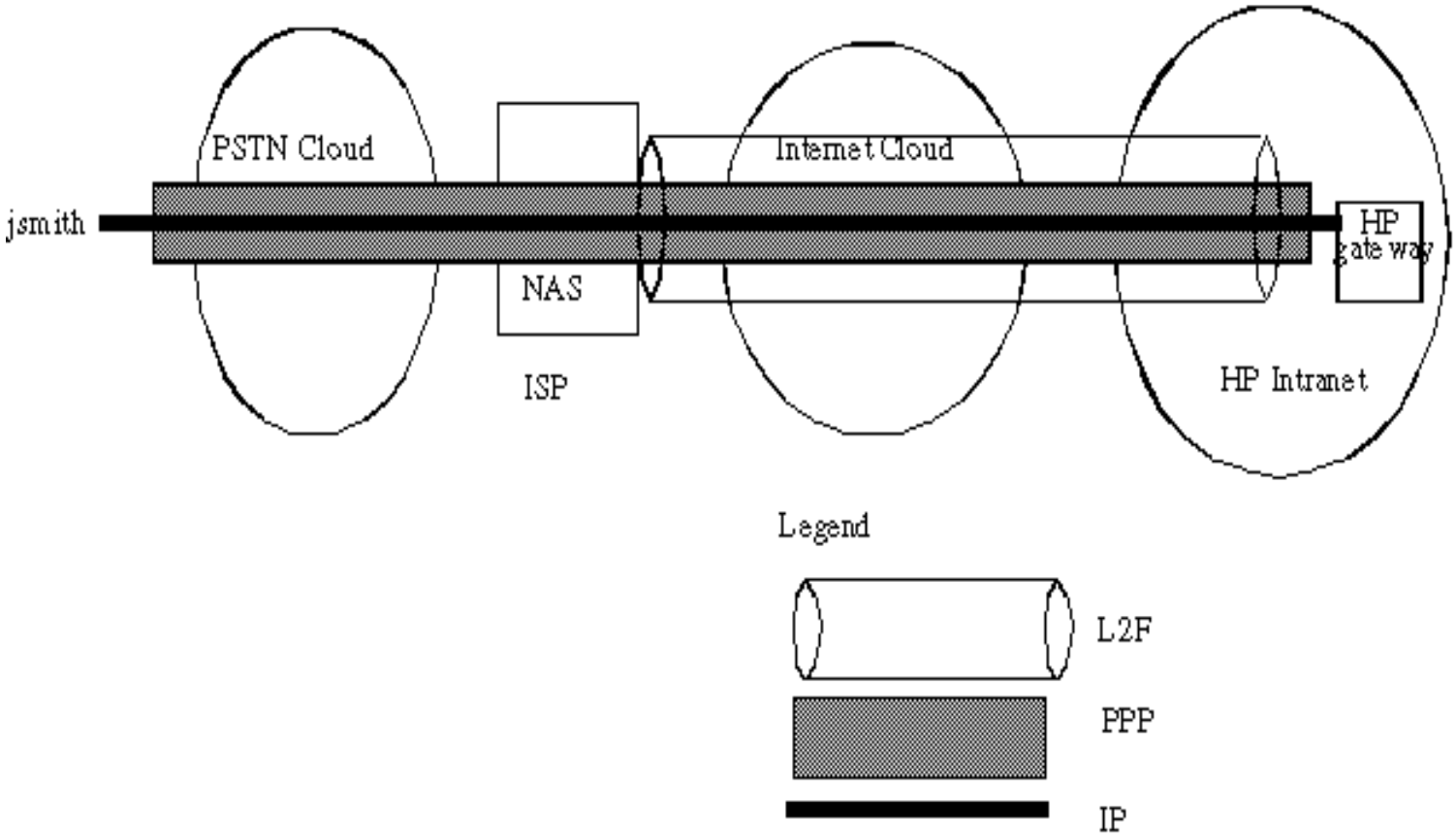
Tunneling Protocol : L2F

⌘ 고전적 접근 방법



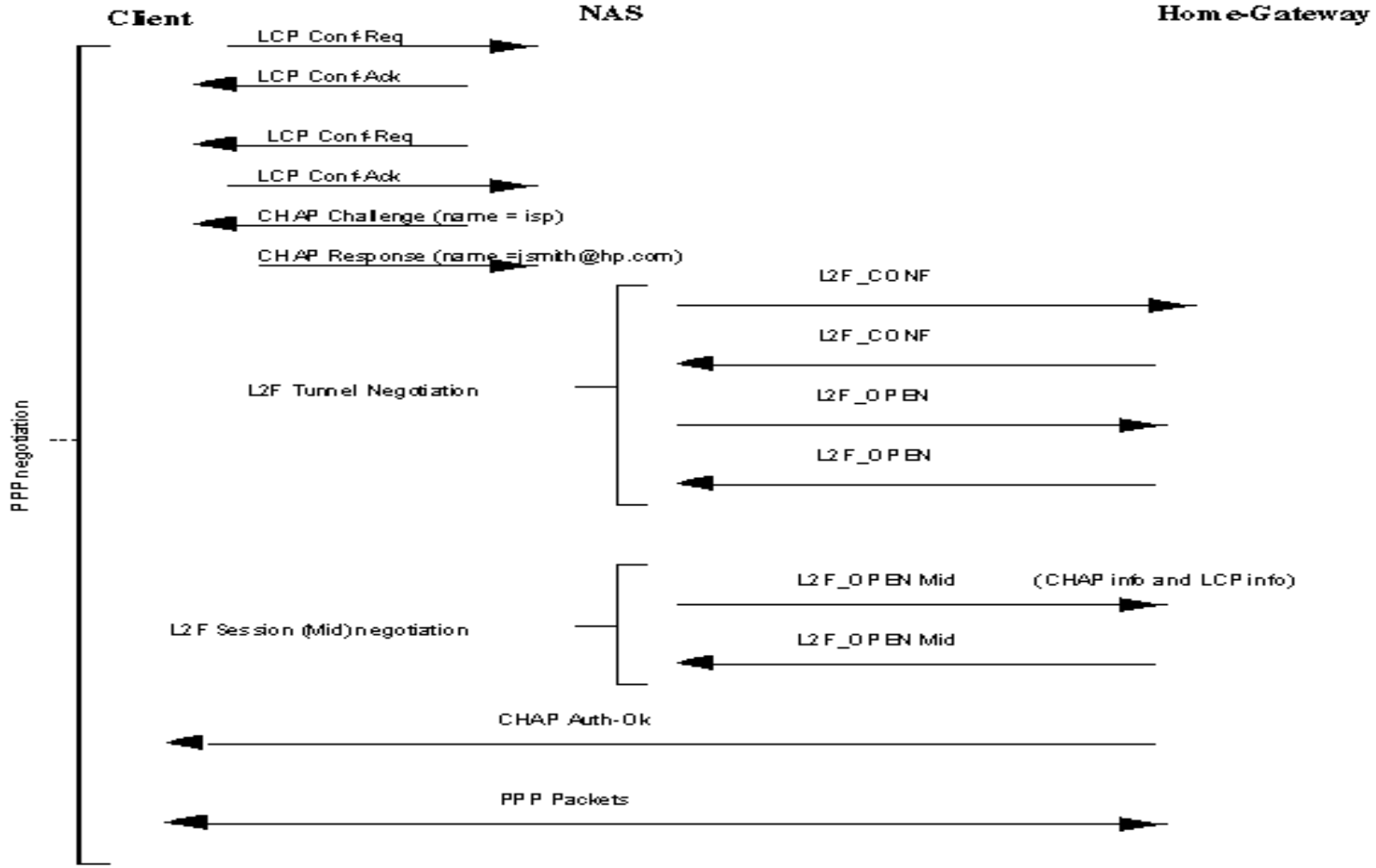
Tunneling Protocol : L2F

- L2F(Layer 2 Forwarding)



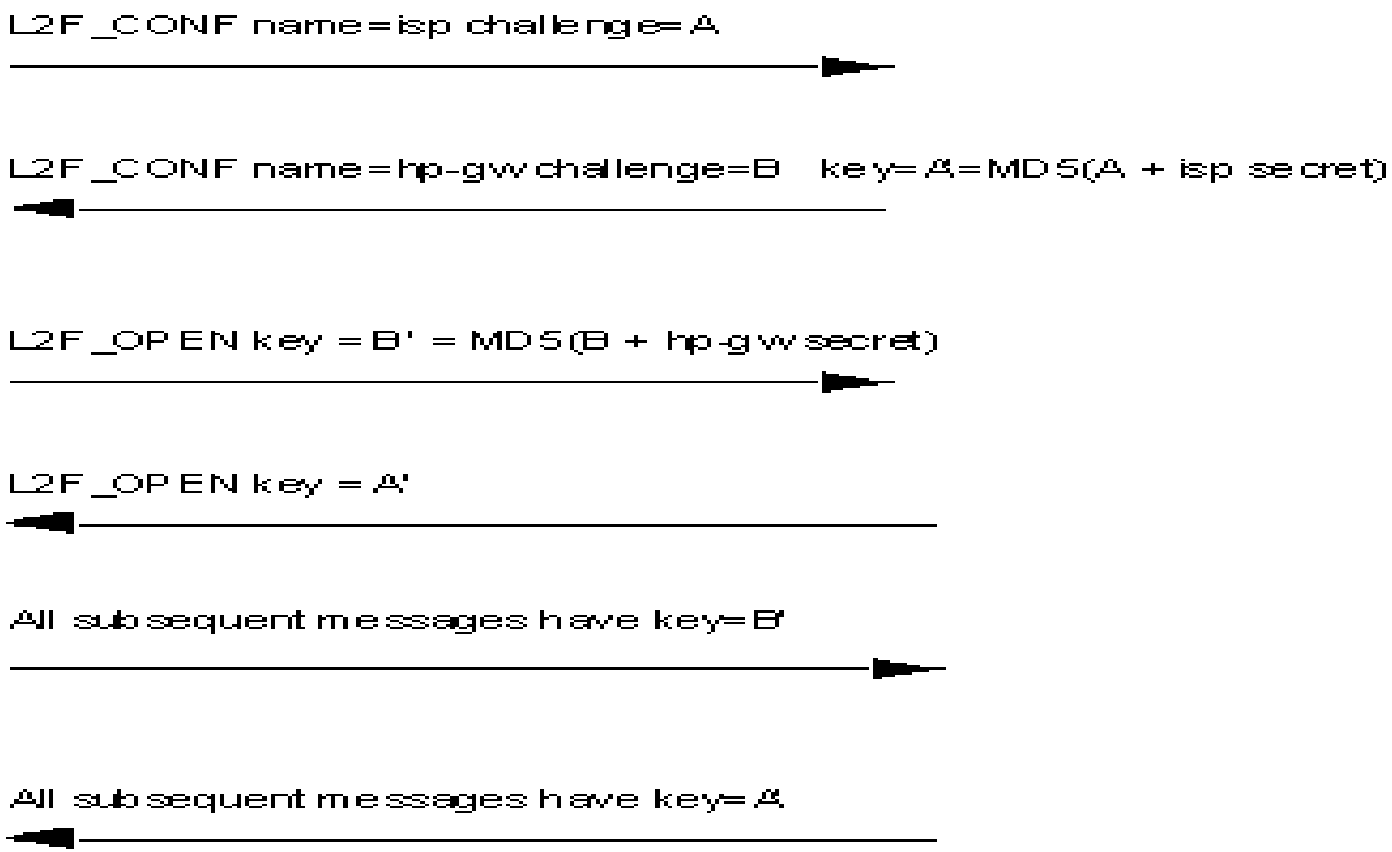
Tunneling Protocol : L2F

- L2F Flow (PPP authentication)



Tunneling Protocol : L2F

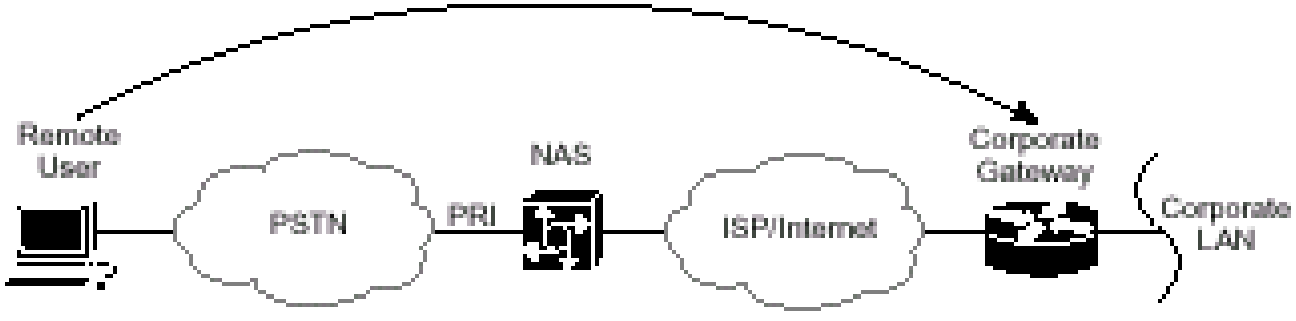
- L2F Tunnel Authentication



Tunneling Protocol : L2F

Frame 형식

IP/UDP	L2F	PPP (Data)
Carrier Protocol	Encapsulating Protocol	Passenger Protocol



Tunneling Protocol : PPTP

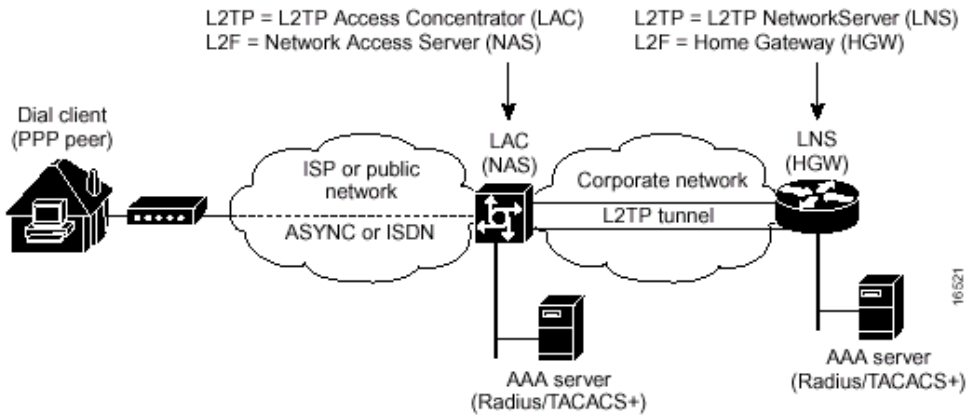
- PPTP (Point-to-Point Tunneling Protocol)
  - 3COM, Microsoft, Ascend, US Robotics
  - first popular tunneling standard,
  - PPP의 확장형으로 개발
  - Client/Server 동작
- Windows 95 와 Windows NT 4.0에 적용
- Mobile user가 home site에 접속 가능하도록 구성
- 인증기능 취약
- Allows you to tunnel or encapsulate IPX and NetBEUI packets in a standard TCP/IP dial-up connection or a dedicated Internet connection
- PPTP uses the security policy you already have set up on the network
- Over 90 million PCs are PPTP-enabled--unlike other protocols

Tunneling Protocol : PPTP

- Bi-directional Tunnel
- Two mode
  - client enabled
  - ISP enabled
- Non IP protocol 지원 : IPX, Appletalk
- PAP, CHAP, MS-CHAP
- RC4(40bits/128bits) 암호화 지원
- Microsoft dependent (Windows NT필요)
- 일반적으로 RAS vendor가 지원

Tunneling Protocol : L2TP

- L2TP : Layer2 Tunneling Protocol
  - remote에서 모뎀등을 통해 LAC(L2TP Access Server)에 접근하고 Home gateway의 LNS(L2TP Network Server)를 통해 접근
  - 기존의 remote access 에 비해
    - cost overhead 줄임
    - flexibility
    - scalability
  - client initiated VPN

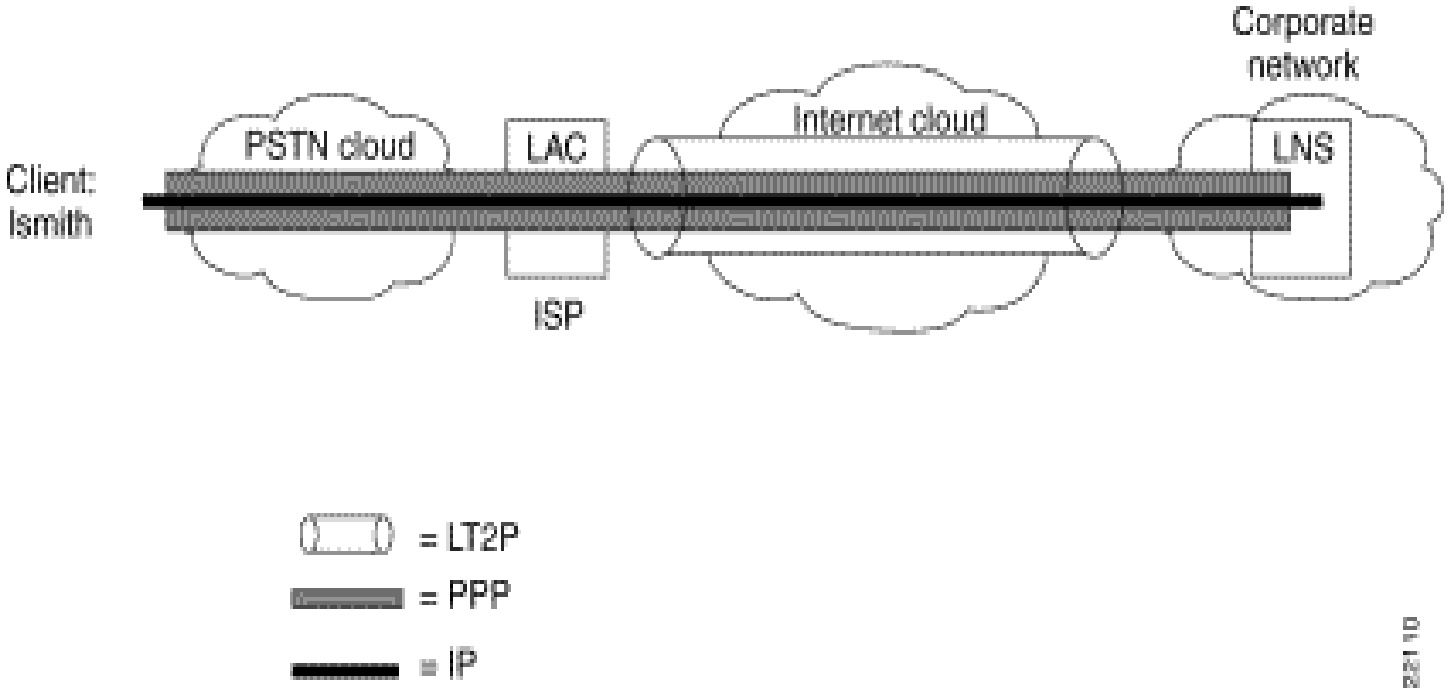


Tunneling Protocol : L2TP

- 특징
  - Hybrid of L2F and PPTP
  - Emerging standard for VPN tunneling
  - Multiple protocol 지원: IP, IPX, AppleTalk
  - non-IP network 환경에서도 가능
    - LAN-to-LAN VPN
  - 다양한 WAN 지원: X.25, ATM, Frame Relay, SONET
  - network traffic 감소할 수 있게 해 줌
  - flow control : server가 congestion handling 가능하도록 함 (network access system 과 home gateway간)
  - LAC (L2TP Access Concentrator)
    - 사용자가 전화를 거는 ISP의 NAS
  - LNS (L2TP Network Server)
    - 접속하고자 하는 edge 장비(router, firewall)

Tunneling Protocol : L2TP

⌘ L2TP Tunnel Structure



Tunneling Protocol : L2TP

⌘ L2TP Incomming Call Flow

Remote user는 ISP로 PPP 접속을 초기화 한다.

ISP Network LAC POP에서 접속을 받아들이고 PPP Link 성립

End User와 LNS가 LCP를 Negotiation 한 후에 LAC은 부분적으로 CHAP 또는 PAP으로 End User를 Authentication 함

User name, Domain name은 User가 VPDN client를 결정하는데 사용

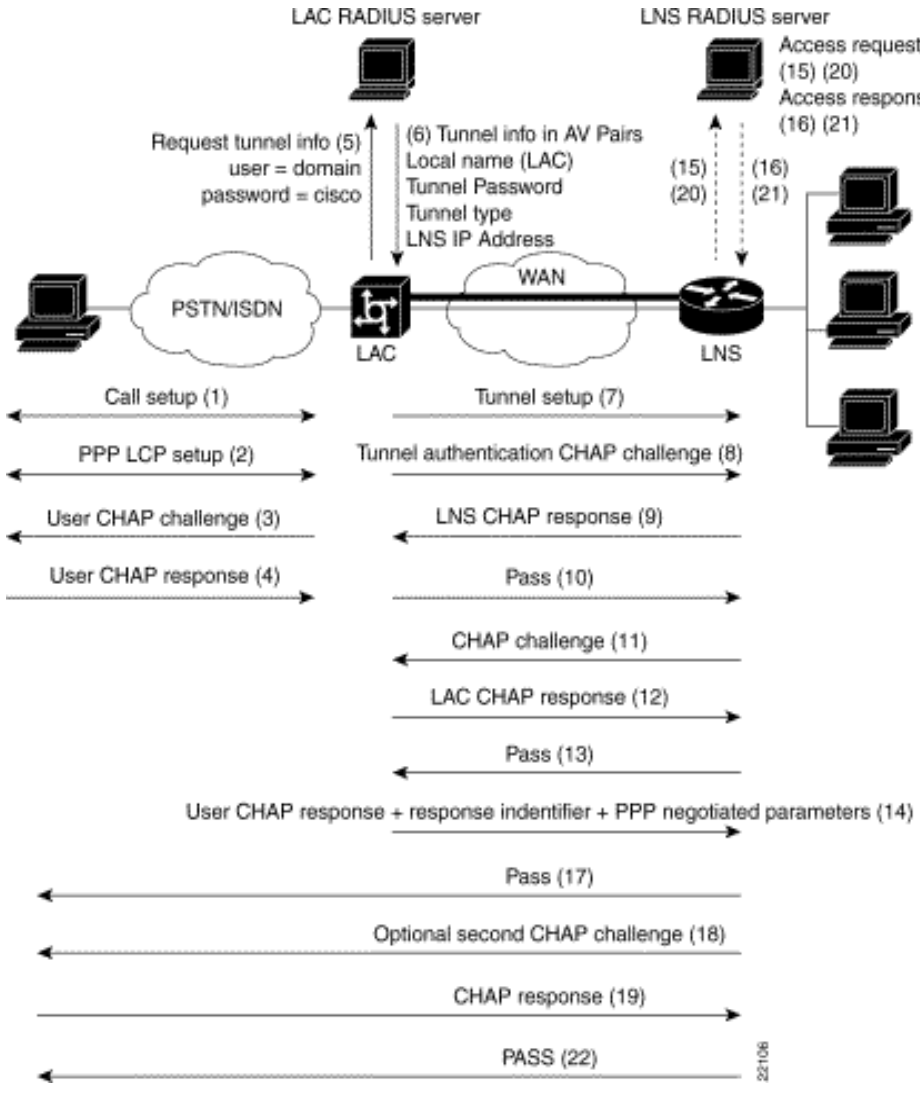
만약 User가 VPDN Client가 아니라면 인증은 계속되고 Client는 인터넷이나 다른 접속 서비스를 Access 할것이다.

만약 VPDN client user name 이라면 특별한 End Point로 mapping 한다 (The LNS)

Tunnel의 End Point에서 LAC과 LNS는 어떠한 Session 들이 Tunnel 안으로 들어오기 전에 인증이 이루어 진다.

Tunnel이 존재하면 L2TP Session 은 End User를 위해 생성된다.

LAC은 LCP 협상 옵션과 CAHP/PAP Authentication 정보를 LNS로 보낸다



Tunneling Protocol : L2TP

⌘ 특징

- 2개의 Message Type 존재 (터널을 통해 전송)
  - - Control message : 터널을 Establish, Maintenance, Clearing함. L2TP에 신뢰성있는 Control Channel 제공
  - - Data message : Encapsulation PPP를 터널로 전송. Packet Loss 시 Retransmit되지 않는다.

0 **L2TP 헤더** 32

T | L | X | X | S | X | O | P | X | X | X | X | Ver	Length(opt)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset size(opt)	Offset size(opt)

Tunneling Protocol : L2TP

- 각 필드의 설명

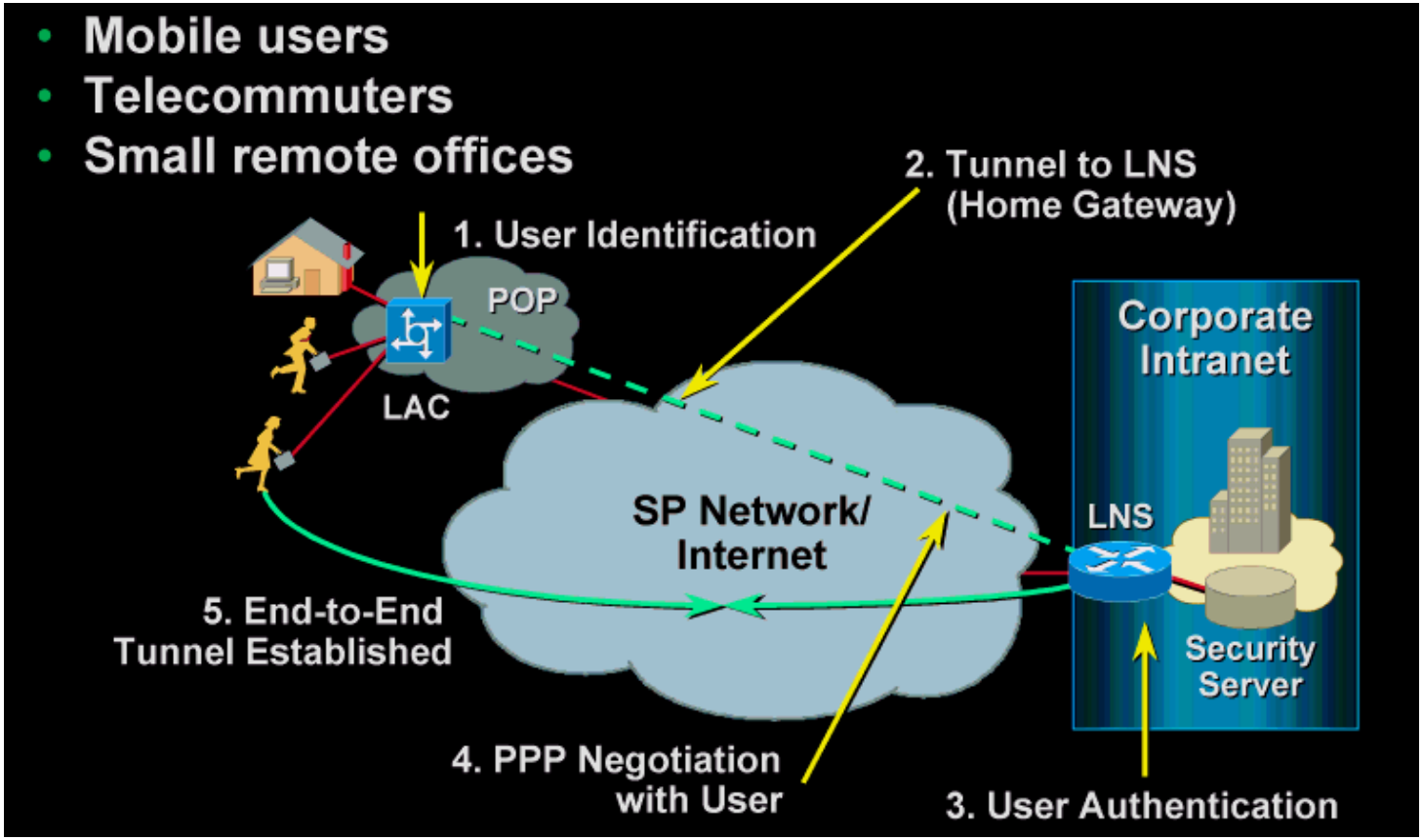
- T bit: Message 의 타입을 가리킴. 0은 Data message를 1은 Control message를 나타냄
- L bit : 1이면 Length 필드가 존재. Control message일 경우 반드시 1이어야 한다.
- X bit : 미래를 위해 예약
- S bit : 1이면 Ns 와 Nr 필드가 존재. Control message 일 경우 반드시 1이여야 한다.
- O bit : 1이면 Offset 필드가 존재. Control message 일 경우 0이어야 한다.
- P bit : 1은 이 Data message는 Local queuing이나 전송 시 우선적으로 처리하라는 의미. Data message 에서만 사용. Control message는 0의 값을 가짐
- Ver : 2는 L2TP를 1은 L2F를 가리킴
- Length : Message의 전체적인 길이를 나타냄
- Tunnel ID : Control Connection 을 위한 ID
- Session ID : 터널안의 Session ID
- Ns : Data 또는 Control Message를 위한 Sequence Number를 가리킴. 0에서 2^{16}까지 1씩 증가
- Nr : 다음에 오는 Control message의 Sequence Number를 나타냄. 0에서 2^{16}까지 1씩 증가
- Offset : Payload의 시작을 나타냄.

0 **L2TP 헤더** 32

T | L | X | X | S | X | O | P | X | X | X | X | Ver	Length(opt)
Tunnel ID	Session ID
Ns (opt)	Nr (opt)
Offset size(opt)	Offset size(opt)

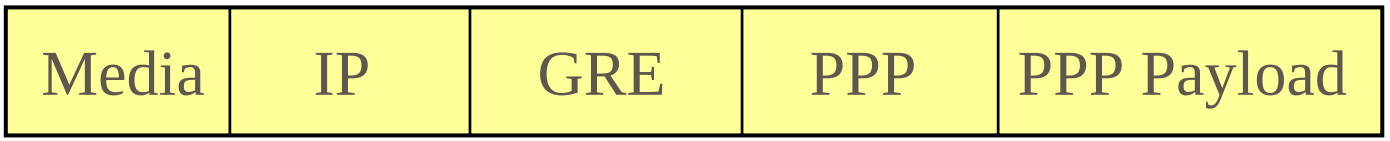
Tunneling : L2F/L2TP

⌘ L2F/L2TP opertation



Data Packet Format

- PPTP



draft-ietf-pppext-pptp-07.txt

- L2TP

draft-ietf-pppext-l2tp-12.txt

IPSec

- IETF IPSec working Group
- VPN tunneling의 업계 표준화
- 강력한 사용자 인증과 암호화가 layer 3에서 진행
- IPv6에 대한 충분한 고려
  - Non-IPSec에 비해 확장성 유리
- protocol
  - Authentication Header(AH) protocol : Packet Payload는 Encrypt하지 않아 완전한 기밀을 보장하지는 않는다.
  - Encapsulating Security Payload(ESP) protocol : Fully Encrypt를 시행하나 Overload 생김
  - 부가기능
    - Encryption Algorithms
      - DES(Data Encryt Standards), 3DES, RC5
    - Authentication Algorithms
      - MD(Message Digest)5->128bit , SHA(Secure Hash Algorithm)1->160 bit
    - IKE

IPSec

- 무결성과 인증을 보장하는 인증 헤더(Authentication Header)와 기밀성을 보장하는 ESP(Encapsulation Security Payload)를 사용하여 보안 서비스를 제공
- 두 가지 헤더의 사용으로 IP 프로토콜 처리 비용의 증가와 통신 지연으로 구현 시 성능 저하의 문제가 고려
- 키와 보안 연계(Security Association)의 안전한 사용을 위한 키 관리 메커니즘이 함께 제공
- 서로 다른 제품간의 호환성 극대화

IPSec

- Enables transmission of sensitive information over unprotected networks such as the Internet
- IPSec에서 제공
  - 기밀성(Confidentiality): packets encrypted before transmission
  - 무결성(Integrity): authenticates packets at the destination peer to ensure that data has not been tampered during transmission
  - 인증(Authentication): peers authenticate source of all IPSEC protected packets
  - 리플레이방지(Anti-replay): prevents capture and replay of packets

IPSec

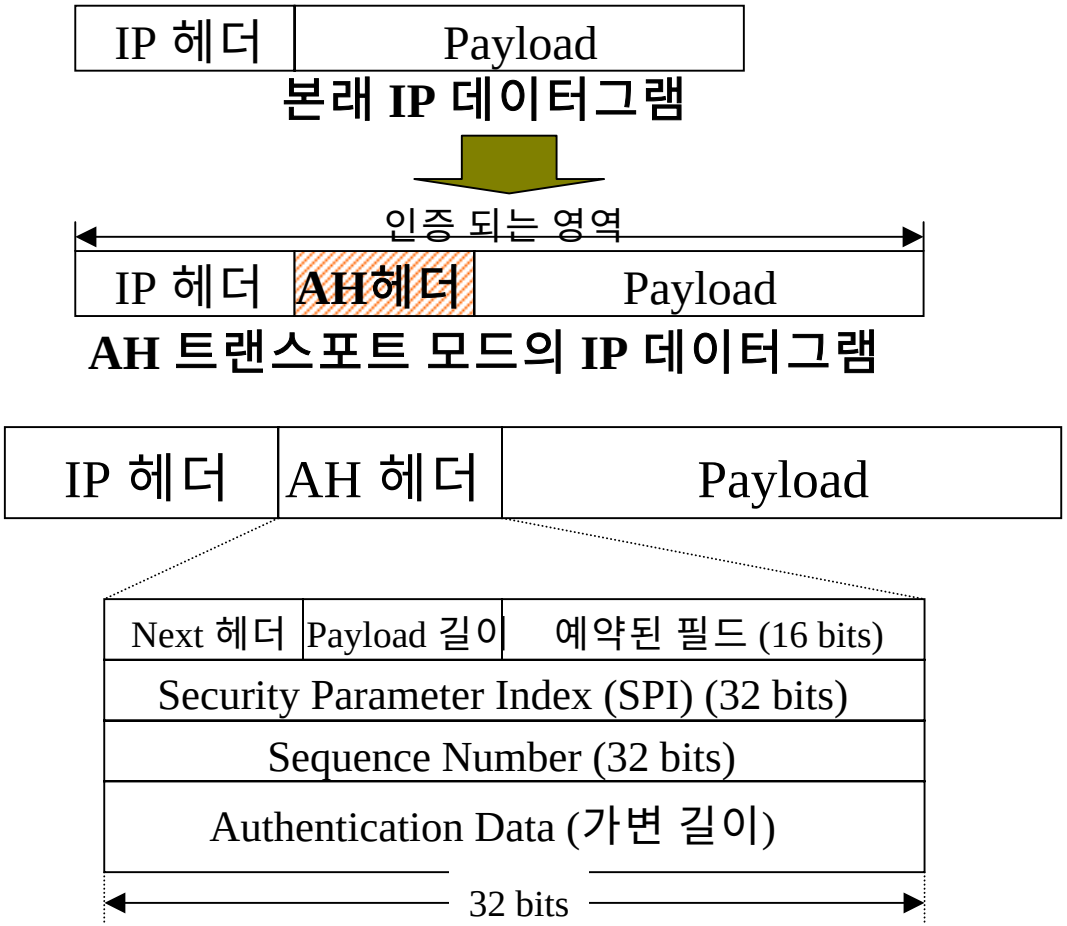
- 현재 표준화가 진행 중인 패킷 처리 레이어 보안 기술.
- IPSec 이전에는 모든 보안에 대한 고려는 어플리케이션에서 적용 됨.
- IPSec을 적용하면 어플리케이션과 독립적으로 네트워크 보안 가능
- 관련 RFC
  - RFC 1825 : Security Architecture for the Internet Protocol
  - RFC 1826 : IP Authentication Header
  - RFC 1827 : IP Encapsulating Security Payload (ESP)
  - RFC 1828 : IP Authentication Using Keyed MD5 (Message Digest)
  - RFC 1829 : The ESP DES-CBC Transform
  - RFC 2085 : HMAC-MD5 IP Authentication with Replay Prevention
  - RFC 2104 : HMAC: Keyed-Hashing for Message Authentication

IPSec header

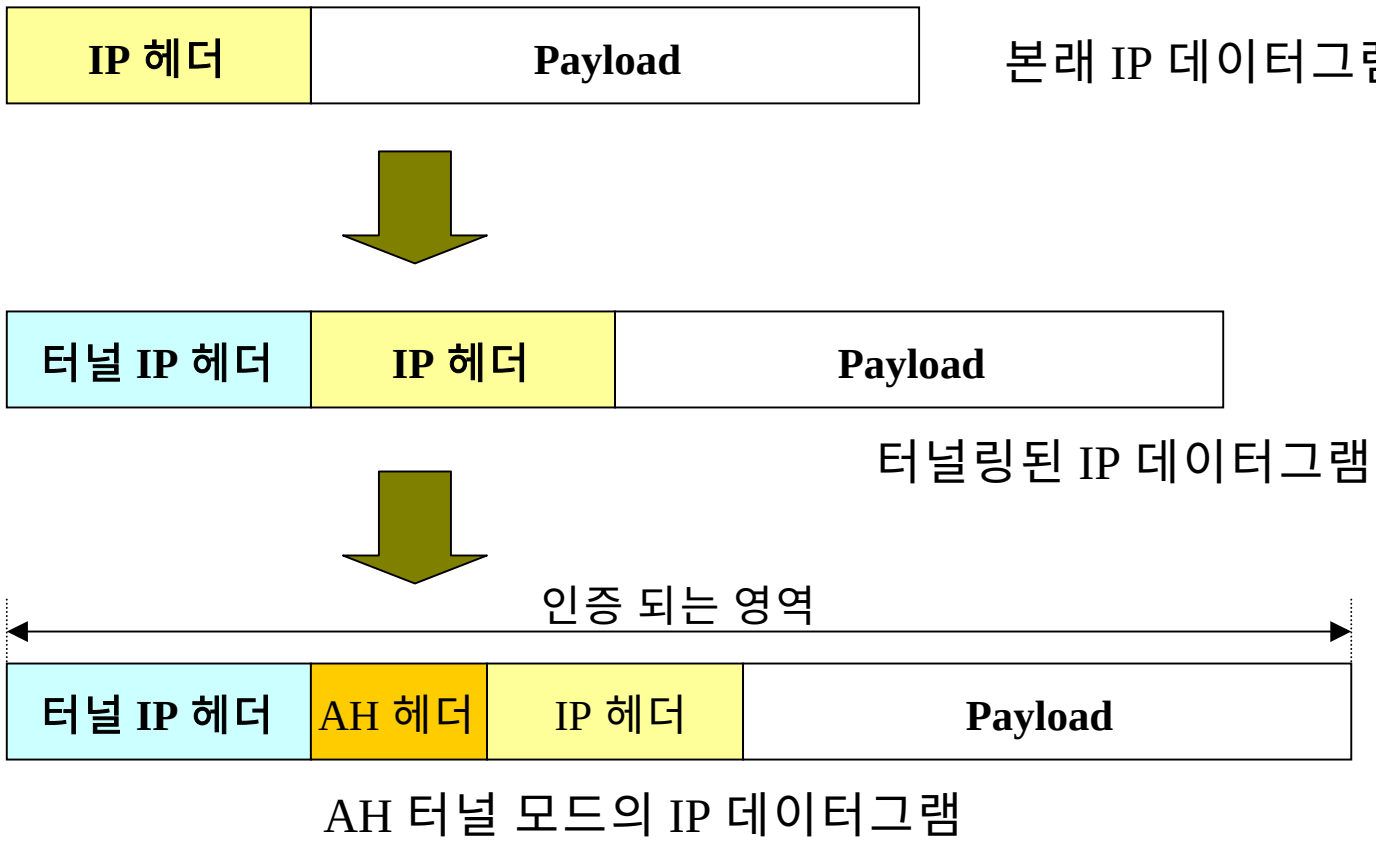
⌘ AH - Authentication Header

- IP datagram에 대해 authentication, integrity 보장
- data integrity, data origin authentication, optional Anti-replay protection를 제공 : RFC 2402
- inserted after the IP header and before any upper layer headers
- 데이터 무결성(integrity) 지원
  - MD5,SHA-1 와 같은 message checksum 활용
- IP 데이터그램에 대한 데이터의 근원지 인증 지원
  - 데이터에 비밀 공유키(secret shared key)을 심어서 활용
- Replay에 대한 보호 제공
  - AH header에 sequence number를 넣어서 활용

IPSec : AH Header



IPSec : AH Header

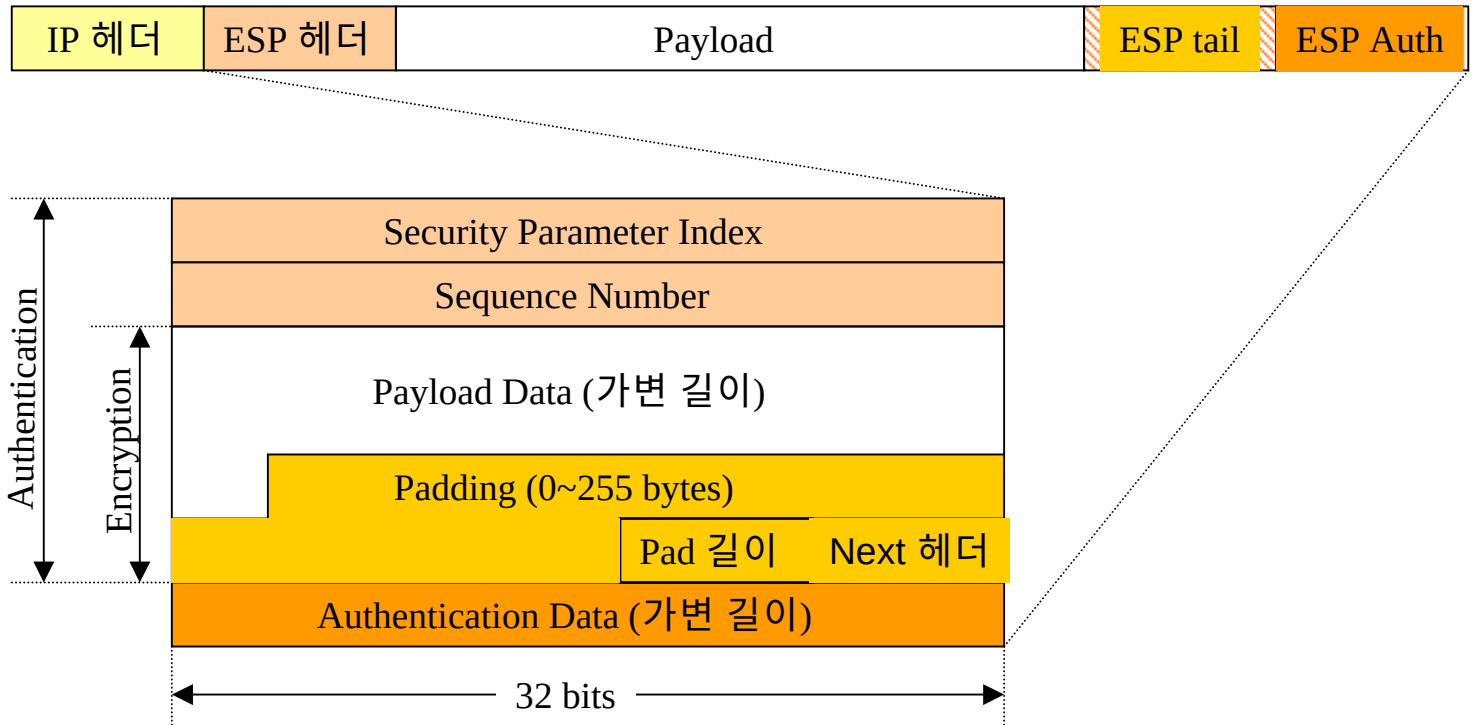


IPSec: ESP Header

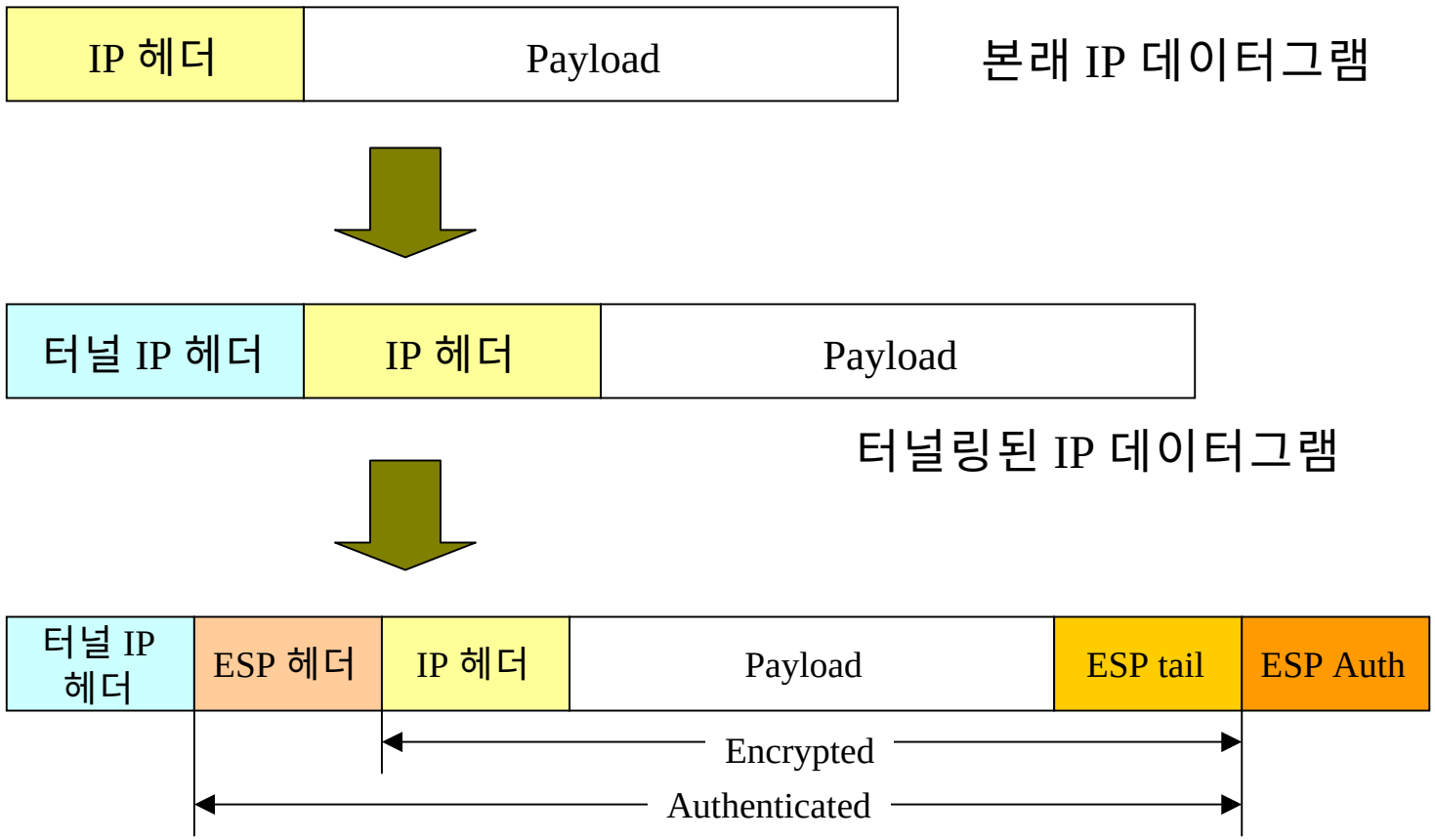
⌘ ESP - Encapsulating Security Payload

- Payload 까지 Encrypt -> AH보다 Overhead많음
- IP datagram에 대해 confidentiality, integrity 보장
- data confidentiality optional data integrity, peer authentication, anti-replay protection 제공 : RFC 2406
- Inserted after the IP header and before any upper layer headers
- 데이터 기밀성 제공
  - DES(Data Eecrytion Standard, 53bit)/3DES 등의 암호화 알고리즘 활용하여 IP packet 처리
- 선택적으로:
  - 패킷 단위의 무결성 제공
  - 데이터 근원지 인증 제공
  - Replay에 대한 sequence number를 이용하여 보호 제공

IPSec : ESP Header



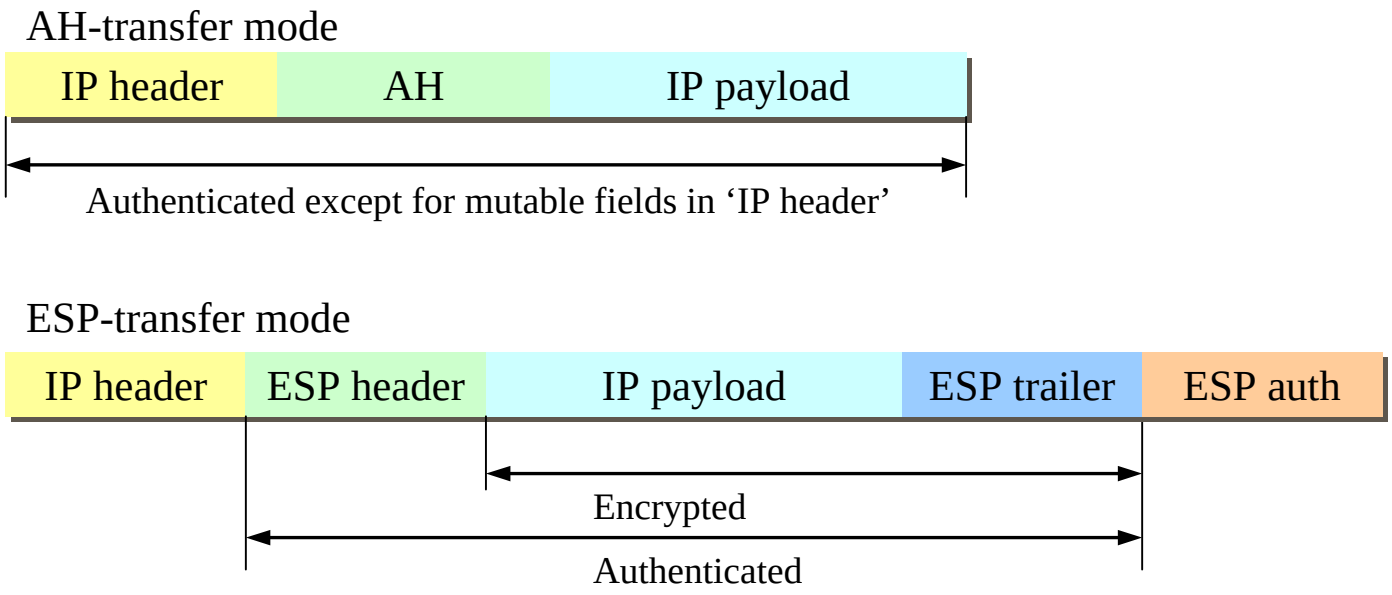
IPSec: ESP Header



IPSec:Transport Mode vs Tunnel Mode

Transport Mode

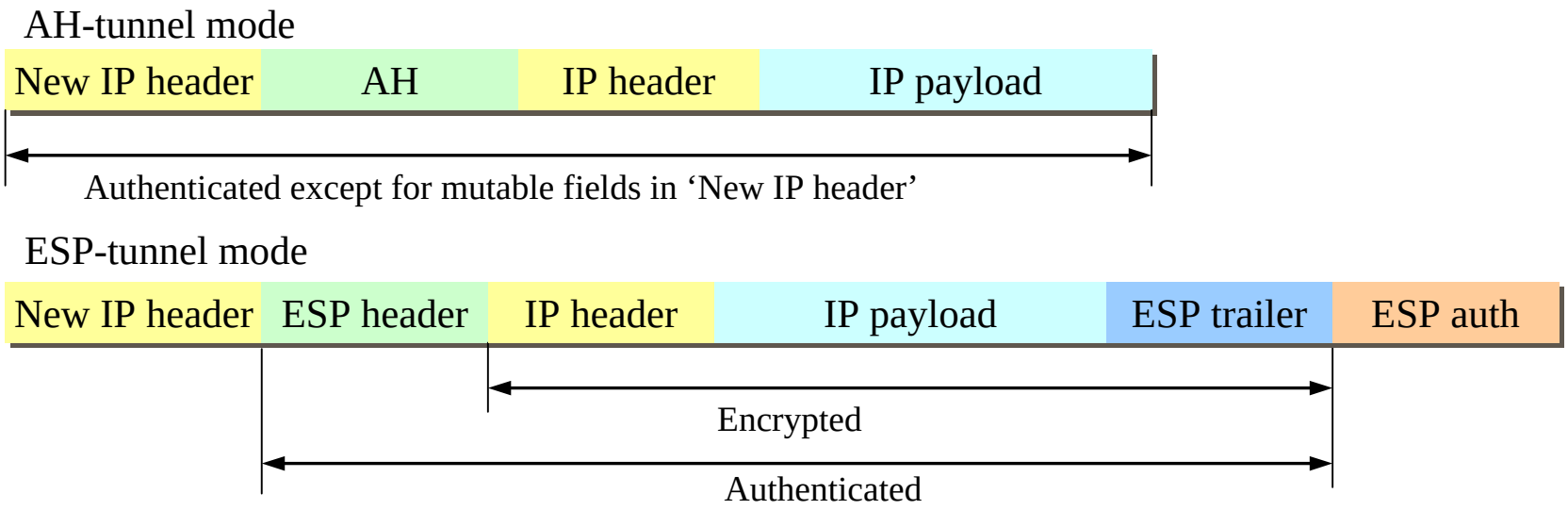
- IP payload만 Encrypt 되고 original IP header는 변하지 않고 남아있음.
- 각 패킷에 작은 byte만 더해지는 잇점이 있음.
- 이것은 Public network 상에서 device가 패킷의 마지막 Source/Destination을 볼 수 있게 해줌.
- 따라서 QoS같은 특별한 Processing을 가능하게 해줌.
- 그러나 IP header가 clear하기 때문에 4계층이상에서 Traffic을 분석할 수 있는 단점이 생김.



IPSec:Transport Mode vs Tunnel Mode

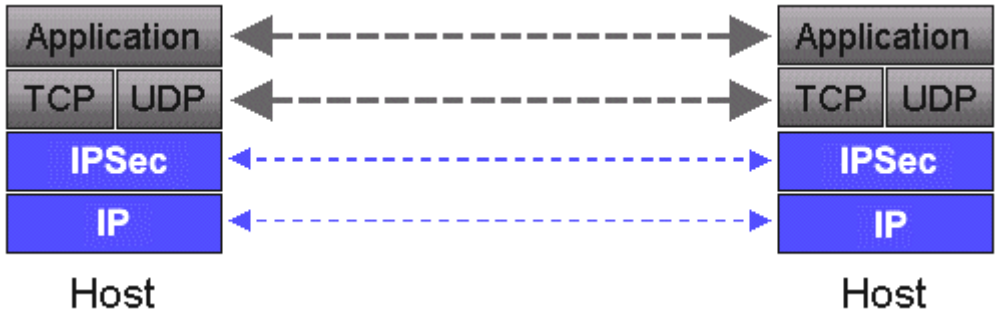
Tunnel Mode

- 모든 Original IP datagram이 Encrypt 되어지고 이것은 New IP 패킷의 Payload가 됨.
- 이 모드는 Router에게 Ipsec proxy 처럼 동작하게 하고 Router는 Hosts대신에 Encryption을 수행
- Source의 Router 는 패킷을 Encrypt하고 Ipsec을 통해서 Forwarding한다.
- Destination Router는 반대의 과정을 수행한다.
- 이 모드의 잇점은 End system은 Ipsec을 modyfi할 필요가 없다는 점이다. 그리고 Traffic을 분석할 수 없다는 점이다.

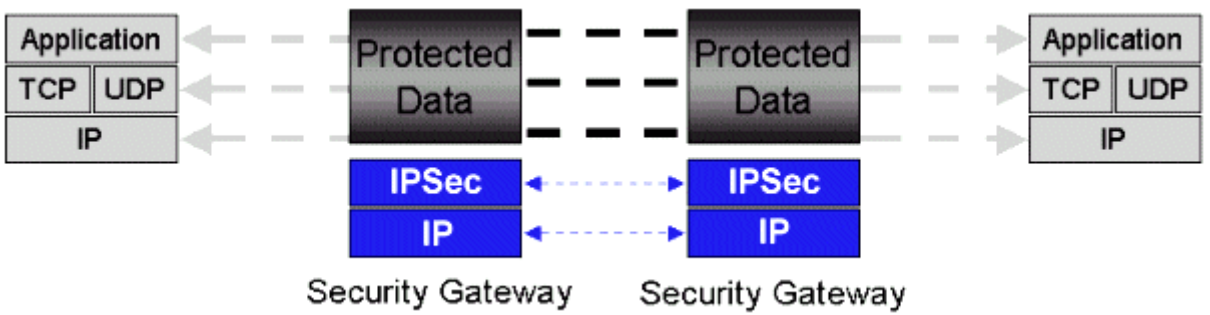


IPSec:Transport Mode vs Tunnel Mode

⌘ Transport Mode

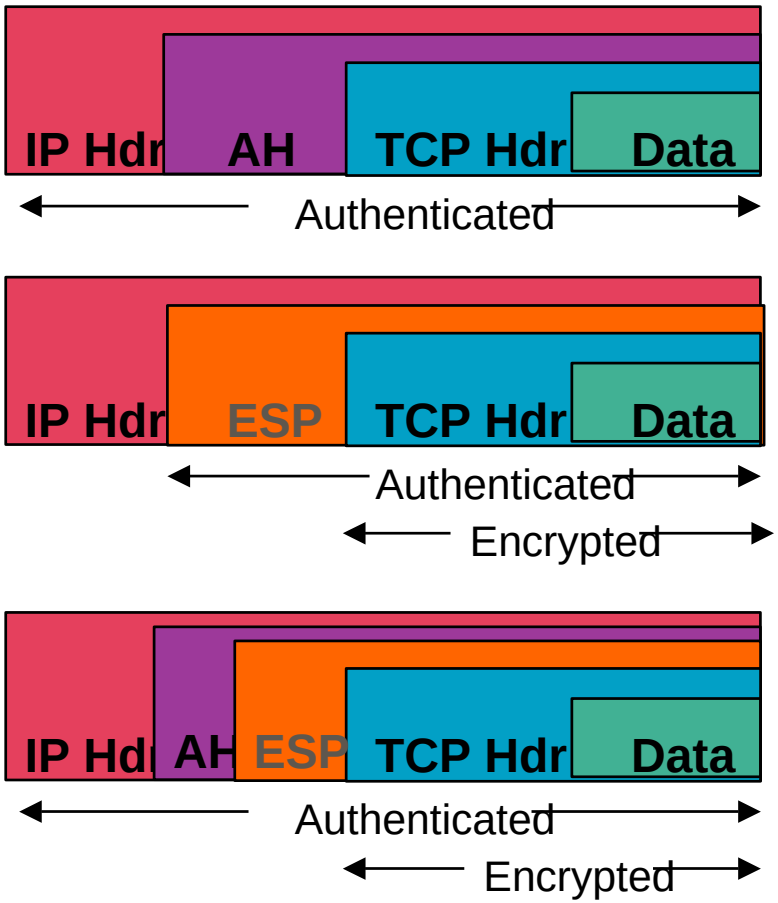


⌘ Tunnel Mode

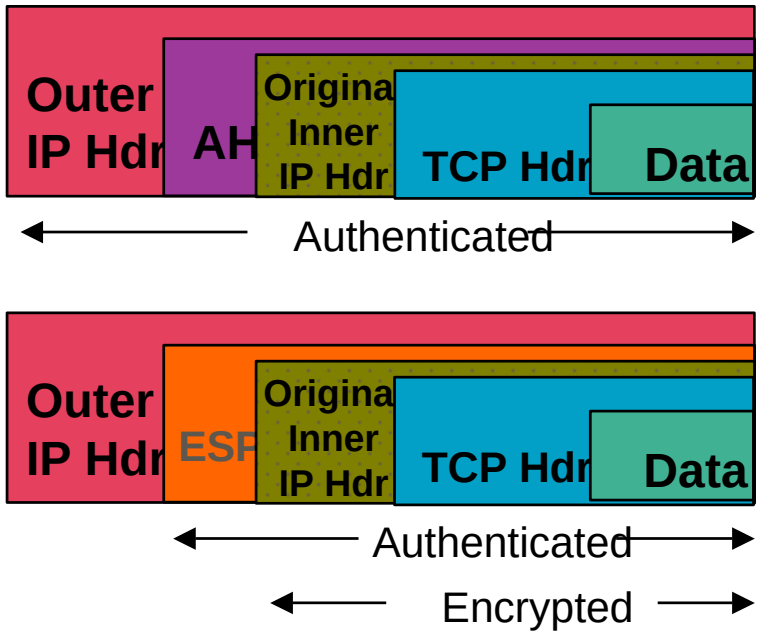


IPSec:Transport Mode vs Tunnel Mode

Transport Mode

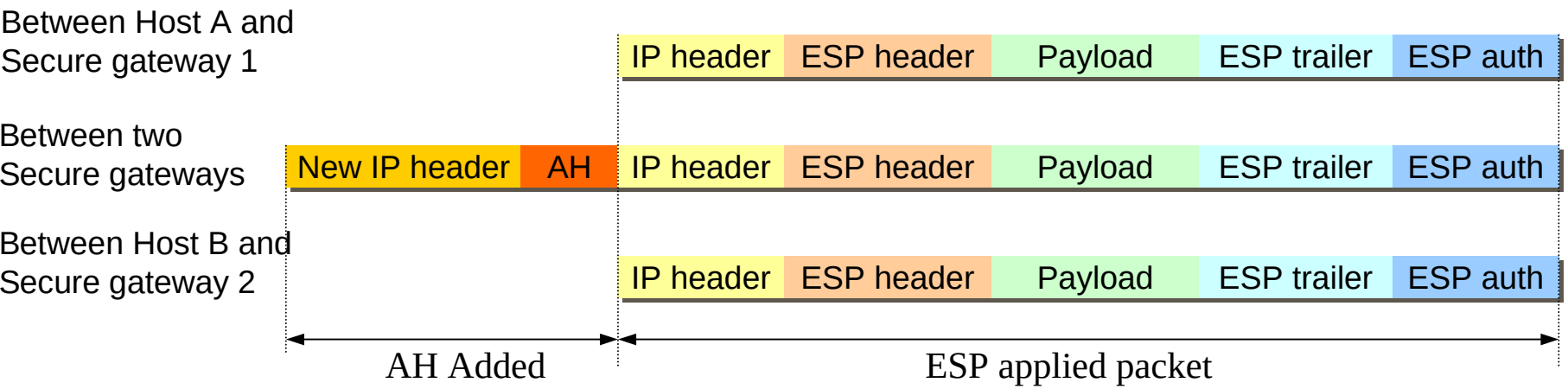


Tunnel Mode



IPSec:Transport Mode vs Tunnel Mode

- ESP : 두 host간에 적용
- AH : 두 secure gateway간에 적용



IPSec vs Non-IPSec

- IPSec 방식
  - IP 기반 프로토콜만 지원
  - Certificate Authority 필요
  - 서로 다른 제품 간 호환성 및 확장성 고려 됨

- Non-IPSec 방식
  - 여러 프로토콜 지원
  - VPN 구성을 위해 한 업체에서 제작한 프로토콜을 사용하므로 한 업체 제품으로 VPN 구성
  - L2F, L2TP, PPTP, SOCKS 등이 있음

VPN을 위한 IPSec의 역할

- 특정 그룹(장비 제작사 등)에 의해 지배되는 VPN 표준 기술 지향
- LAN-to-LAN 방식의 VPN과 Dialup-to-LAN 방식의 VPN을 동시에 지원 가능
- IPv6에 대한 충분한 고려로 Non-IPSec에 비해 확장성 유리
- 서로 다른 제품간의 호환성 극대화

Key management와 exchange

- Security association(SA)
- 인증과 암호화 서비스를 이용한 통신을 위한 조건
  - 상대방과의 nego : protocol, 암호화 알고리즘, key값
  - key 교환 용이성
  - 위 조건의 준수 및 유지
- SA under IPSEC specifies next things
  - the mode of the authentication algorithm used in AH and the keys to that authentication algorithm
  - the ESP encryption algorithm mode and the keys to that encryption algorithm.
  - the presence and size of(or absence of) any cryptographic synchronization to be used in that encryption algorithm.
  - how you authenticate your communications(using what protocol, what encrypting algorithm, and what key).
  - how you make your communication private(what algorithm, and what key).
  - how often those keys are to be changed.
  - the authentication algorithm mode, and transform for use in ESP plus the keys to be used by that algorithm.
  - the key lifetimes.
  - the lifetime of the SA itself.

Key management와 exchange

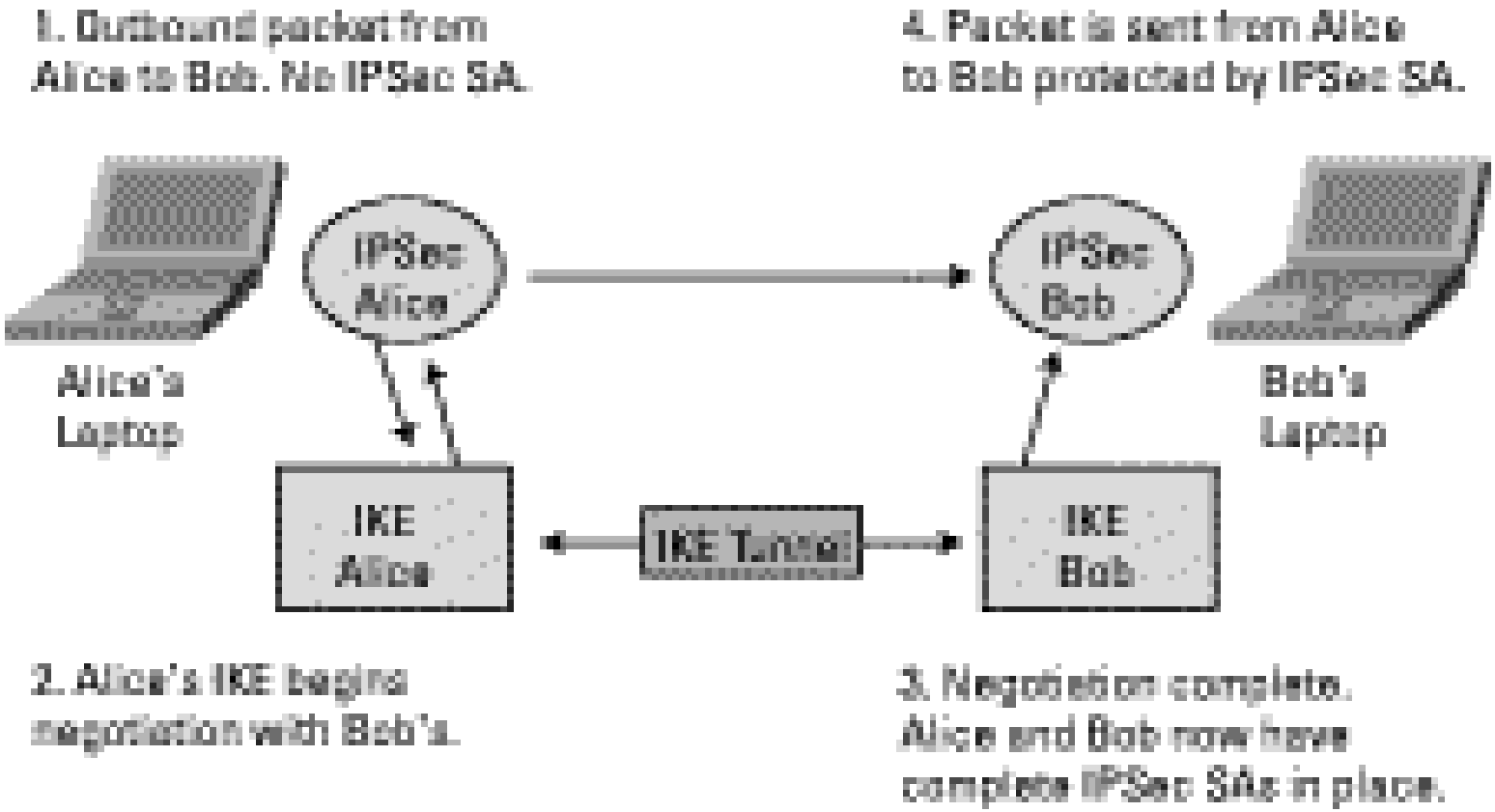
- SA의 적용 예
  - 협력 업체간의 VPN 구성시
- SA와 SPI
  - SA : 개념적
  - SPI : SA에서의 unique number(32bit),
    - 암호화에서 제외
    - AH /ESP header

IPSec : IKE

- Internet Key Exchange (IKE)
  - a powerful, flexible negotiation protocol that allows users to agree on authentication methods, encryption methods, the keys to use, how long to use the keys before changing them, and that allows smart, secure key exchange
  - key교환 방법 : Diffie-Helman 기준
  - Strong data encryption requires frequent key change
  - IKE phase
    - Phase I - 양 IKE peer간에 secure channel 형성
    - Phase II - 양 peer 간에 SA를 위한 negotiation
      - Dynamically exchanges keys for bulk data encryption

IPSec : IKE

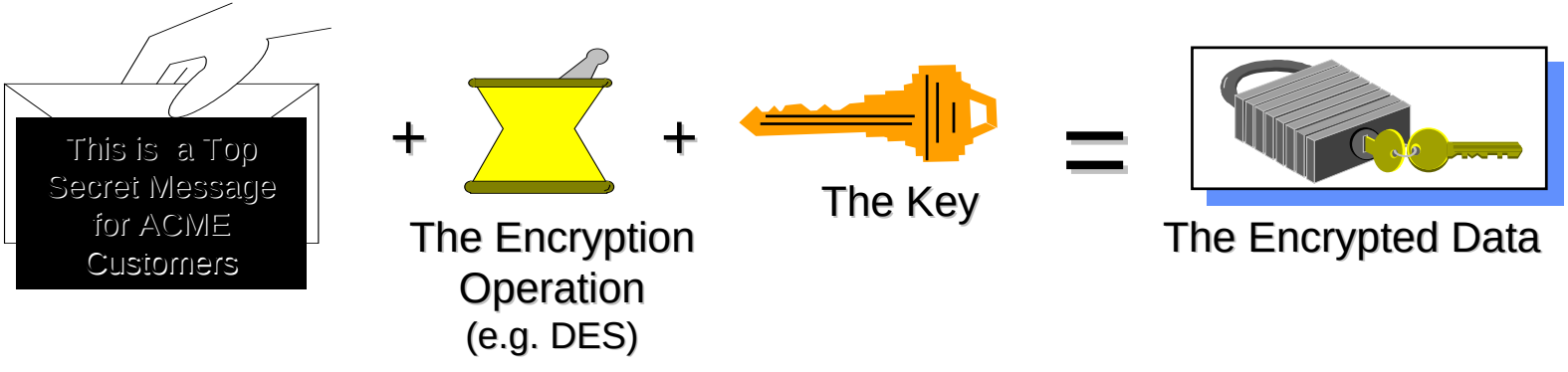
- Internet Key Exchange (IKE)



IPSec : IKE

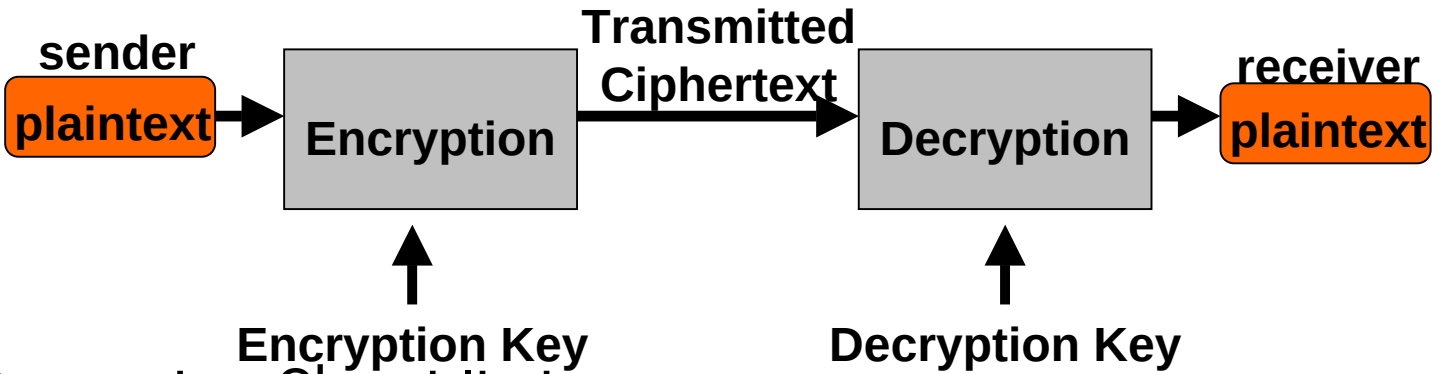
Internet Key Exchange (IKE)

- Coupled with IPSec's key management systems
- Employed to exchange information used to generate encryption key
- Agrees on encryption and data authentication algorithms
- Each participant has pair of keys; one private and one public.
- Digital signatures supplied by a Certificate Authority.



암호화(Cryptography)

⌘ Encrypted communication



⌘ Secret key와 public key

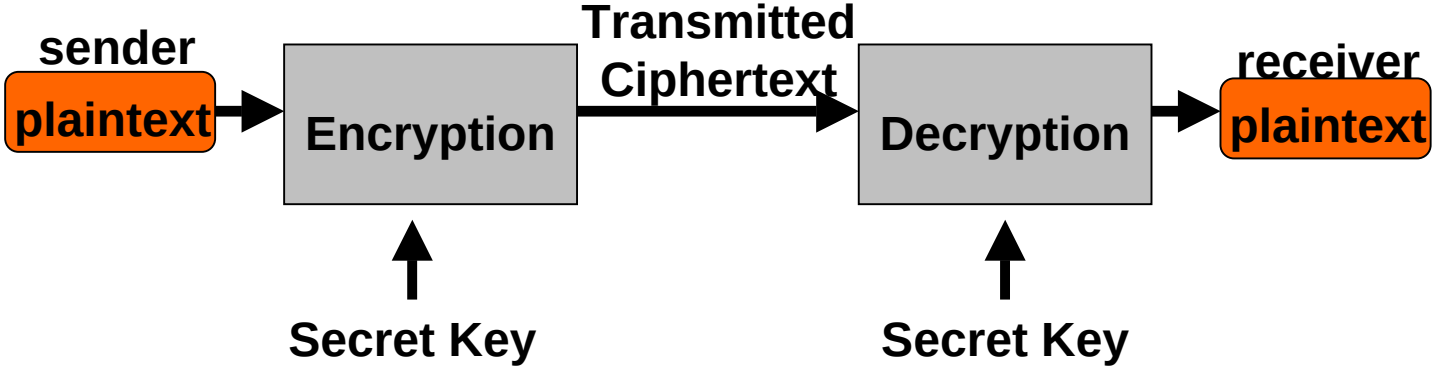
- secret key 암호화
  - single key, encryption key 와 decryption key 동일
  - symmetric key, N명과 교환시 N개의 key 소유
- public key 암호화
  - a pair of keys, public key 와 private key
  - asymmetric key

암호화(Cryptography)

- Secret key 암호화 알고리즘-> Private Enterprise Network
  - DES(Data Encryption Standard)
  - Triple-DES
  - IDEA, Blowfish, CAST-128……
- DES
  - block cipher : 64bit plaintext ==> 64bit ciphertext
  - key length = 56 bits
  - 16회의 치환 과 대입 수행
  - 매회 다른 permutation(교환) of secret key를 가지고 실행
  - 일반화된 알고리즘
- Triple-DES
  - DES를 3번 적용
  - key length = 56bit * 3회 = 168 bits

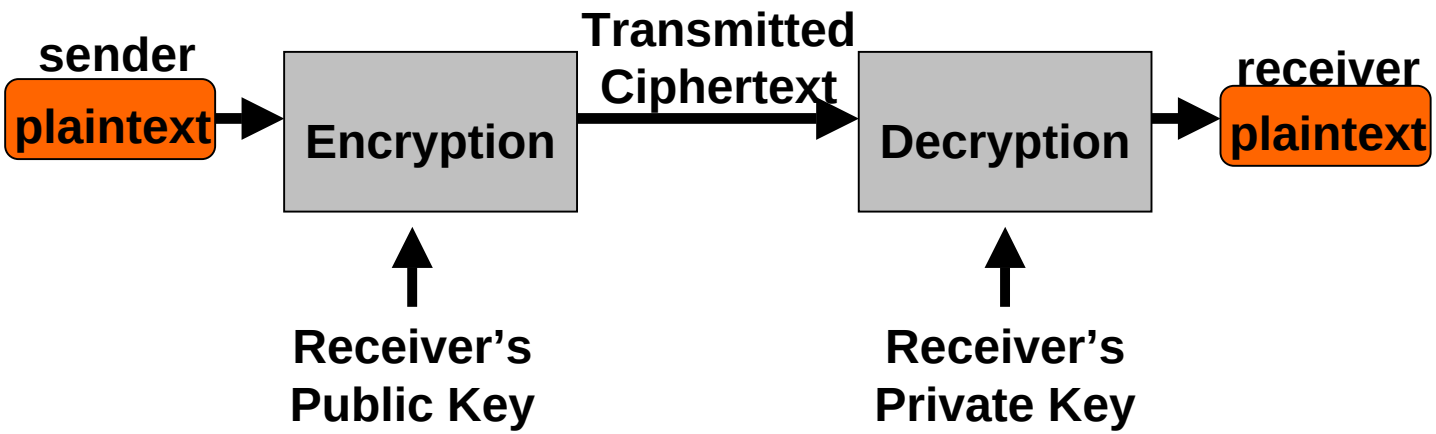
암호화(Cryptography)

- DES와 3-DES의 장점
  - 충분히 검증된 알고리즘
  - DES : brute-force attack 가능, plaintext에 대한 정보와 resource 필요
  - 3-DES : brute-force attack는 현재의 computer system으로 불가



암호화(Cryptography)

- Public key 알고리즘
  - RSA(Rivest-Shamir-Adleman)
  - system당 2개의 key 필요 (Public key, Private key)
    - Public key : 공개됨, 암호화에 사용
    - Private key : receiver 만 알고 있음, 복호화에 사용
  - 복잡한 수학연산이 필요, 속도가 느림



암호화(Cryptography)

- Public key 암호화-> 전자상거래
  - CPU load가 secret key에 비해 상대적으로 큼
  - 암호화 key 관리나 digital signature application에 사용
  - 단순 암호화에는 사용치 않음
  - encryption :
    - sender : receiver의 public key로 암호화
    - receiver: receiver의 private key로 복호화
  - authentication :
    - sender : sender의 private key로 암호화
    - everyone : sender의 public key로 복호화

PKI : Public Key Infrastructure

- PKI 개요
  - 공개 키 기반 구조 :
    - 전자상거래 시스템과 같은 정보 시스템에 안전성을 부여하며, 통신 시스템의 신뢰성을 높이기 위한 기반 구조로, 네트워크 상에 연결된 각 사용자 및 메시지에 대한 인증 기능을 부여하기 위하여, 공개키 방식을 이용한 인증용 기반 구조
  - PKI 구성요소
    - 암호 서비스
    - 인증서 관리 서비스
    - 부가 서비스