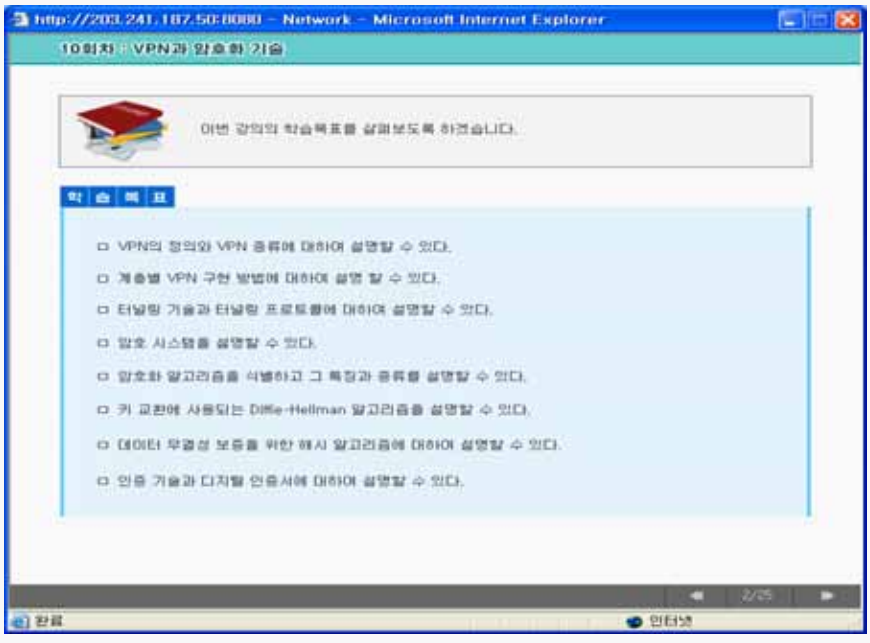
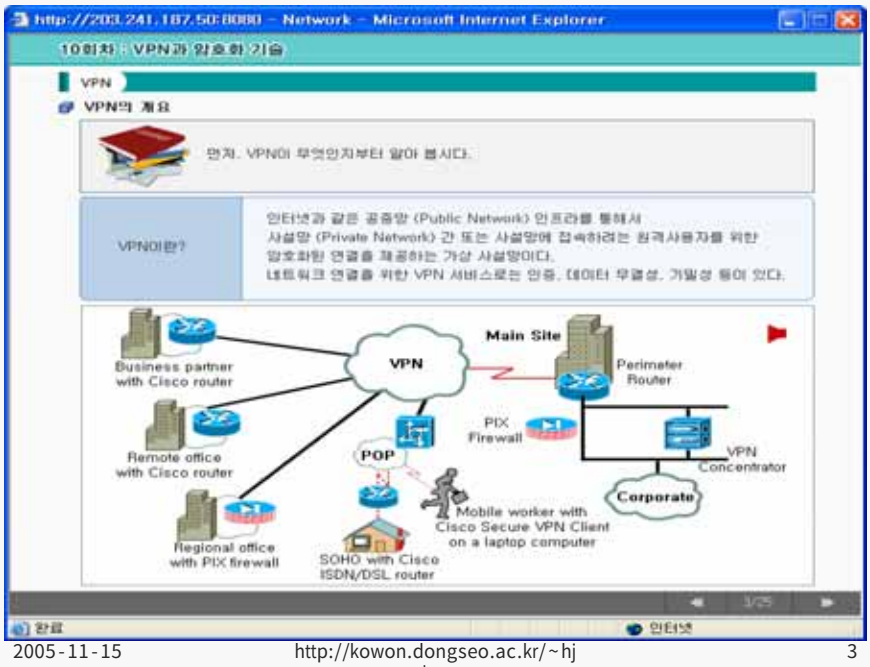
FNS

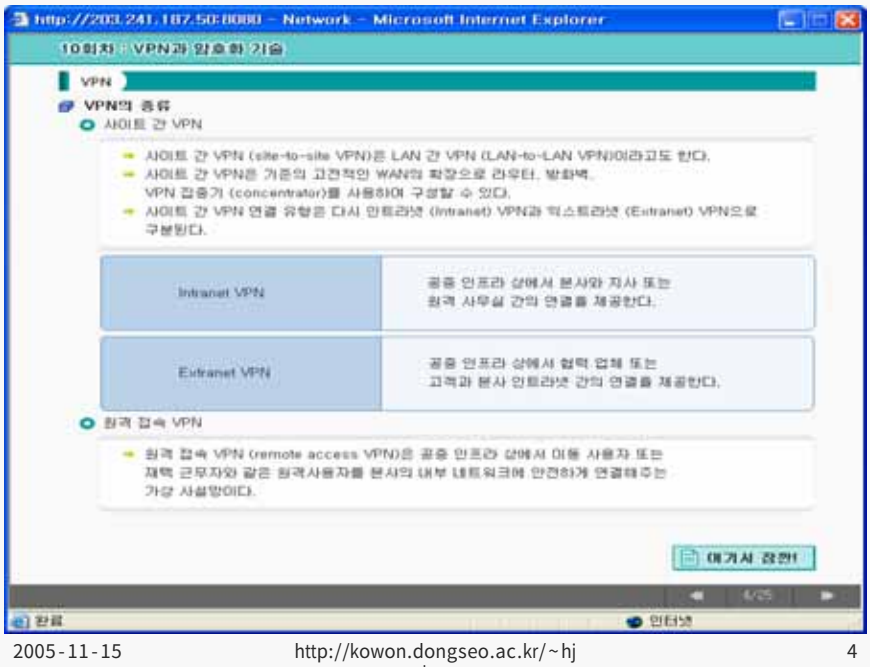
(Fundamental Network Security)

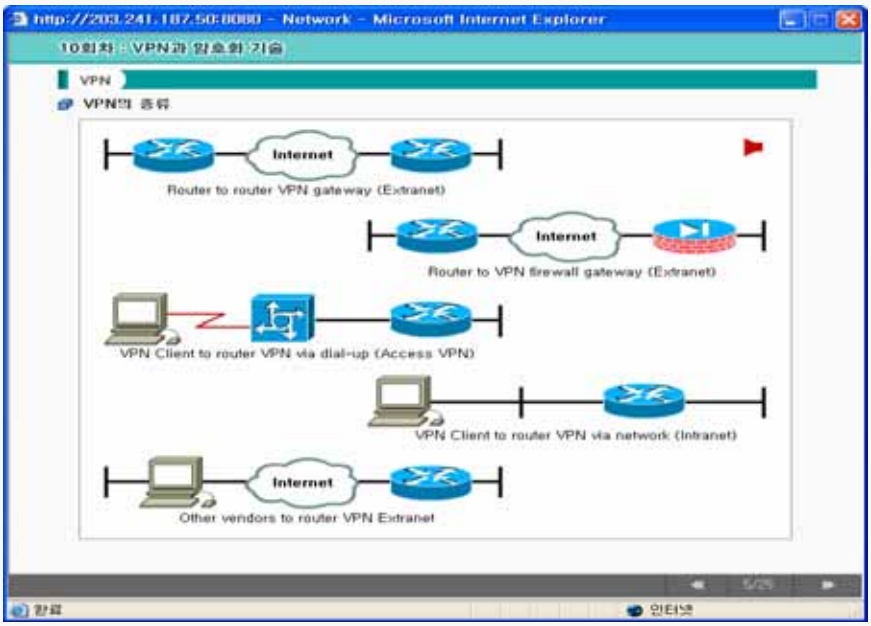
Ch10. VPN과 암호화 기술

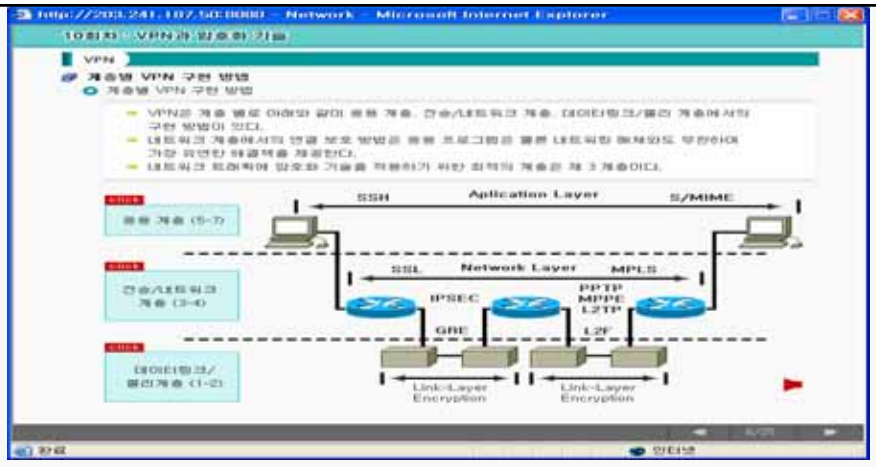
동서대학교/인터넷공학부
이 훈 재
hjlee@dongseo.ac.kr
http://kowon.dongseo.ac.kr/~hjlee
http://crypto.dongseo.ac.kr




http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
VPN
VPN의 개요
먼저, VPN이 무엇인지부터 알아 봅시다.
VPN이란?
인터넷과 같은 공중망 (Public Network) 인프라를 통해서
사설망 (Private Network) 간 또는 사설망에 접속하려는 원격사용자를 위한
암호화된 연결을 제공하는 가상 사설망이다.
네트워크 연결을 위한 VPN 서비스로는 인증, 데이터 무결성, 기밀성 등이 있다.
Business partner with Cisco router
VPN
Main Site
Perimeter Router
Remote office with Cisco router
PIX Firewall
POP
VPN Concentrator
Corporate
Mobile worker with Cisco Secure VPN Client on a laptop computer
Regional office with PIX firewall
SOHO with Cisco ISDN/DSL router
3/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
VPN
VPN의 종류
사이트 간 VPN
사이트 간 VPN (site-to-site VPN)은 LAN 간 VPN (LAN-to-LAN VPN)이라고도 한다.
사이트 간 VPN은 기존의 고전적인 WAN의 확장으로 라우터, 방화벽,
VPN 집중기 (concentrator)를 사용하여 구성할 수 있다.
사이트 간 VPN 연결 유형은 다시 인트라넷 (Intranet) VPN과 익스트라넷 (Extranet) VPN으로
구분된다.
Intranet VPN
공중 인프라 상에서 본사와 지사 또는
원격 사무실 간의 연결을 제공한다.
Extranet VPN
공중 인프라 상에서 협력 업체 또는
고객과 본사 인트라넷 간의 연결을 제공한다.
원격 접속 VPN
원격 접속 VPN (remote access VPN)은 공중 인프라 상에서 이동 사용자 또는
재택 근무자와 같은 원격사용자를 본사의 내부 네트워크에 안전하게 연결해주는
가상 사설망이다.
여기서 잠깐!
6/25
완료
인터넷





응용계층

- 과거에는 응용 계층에 프라이버시와 암호화 서비스를 제공하는 것이 일반적이었으며, 일부 환경에서는 아직도 많이 사용되고 있다.
- 그러나, 응용 계층 보안은 응용 프로그램에 의존적이어서 각각의 애플리케이션에 따라 별도로 구현되어야 할 필요가 있다.

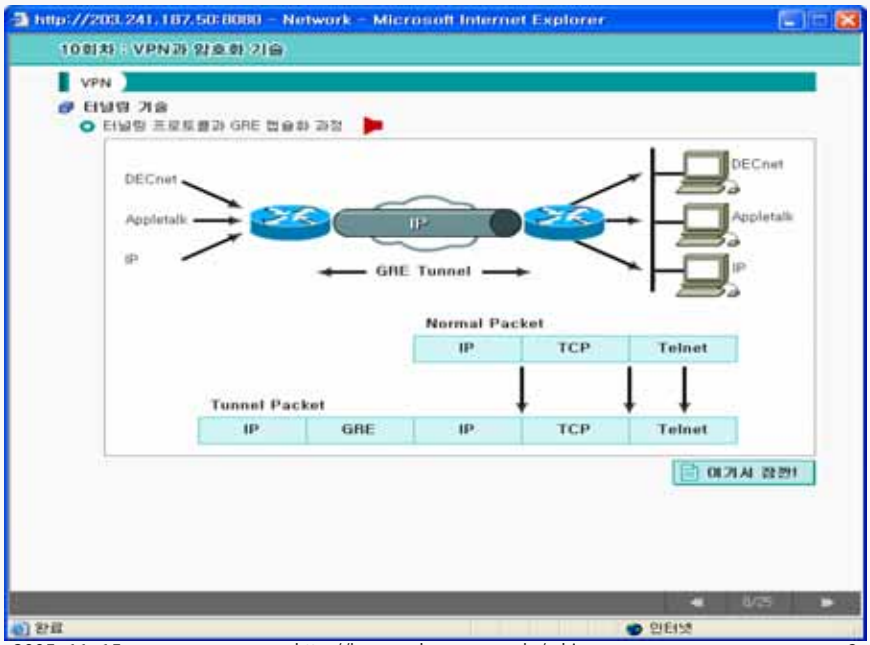
데이터링크/물리계층

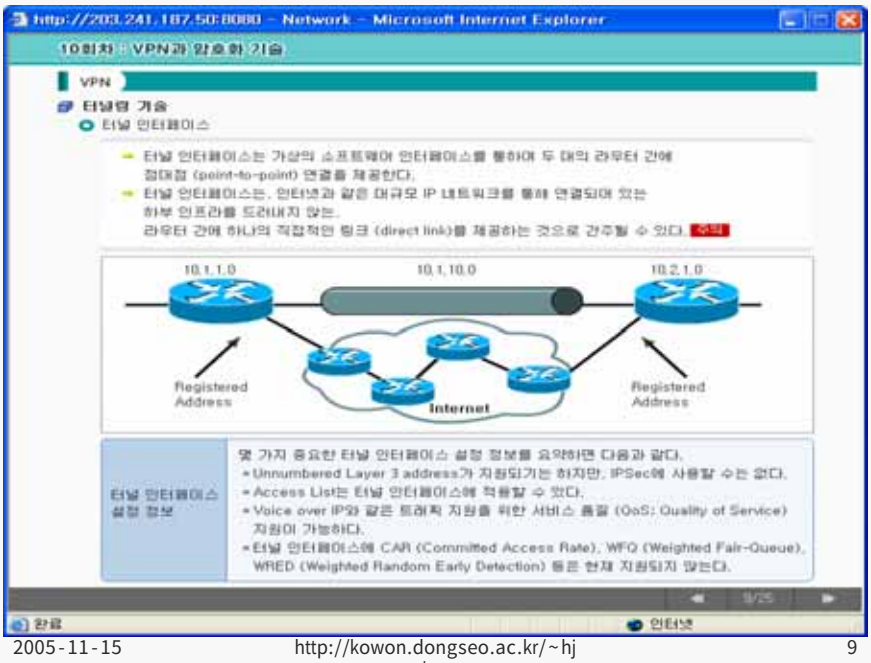
- 데이터링크 계층과 같은 하위 계층에서의 연결 보호 기능은 신뢰성 있는 통신이 문제시되는 특정 링크 상에서 상위 계층 프로토콜에 독립적인 통신 기능을 제공한다.
- 그러나, 데이터링크 계층 보호 방안은 모든 단일 링크를 개별적으로 보호해야 할 필요가 있기 때문에 대규모 네트워크에 적용하기에는 상당한 비용이 소요된다.

전송/네트워크계층

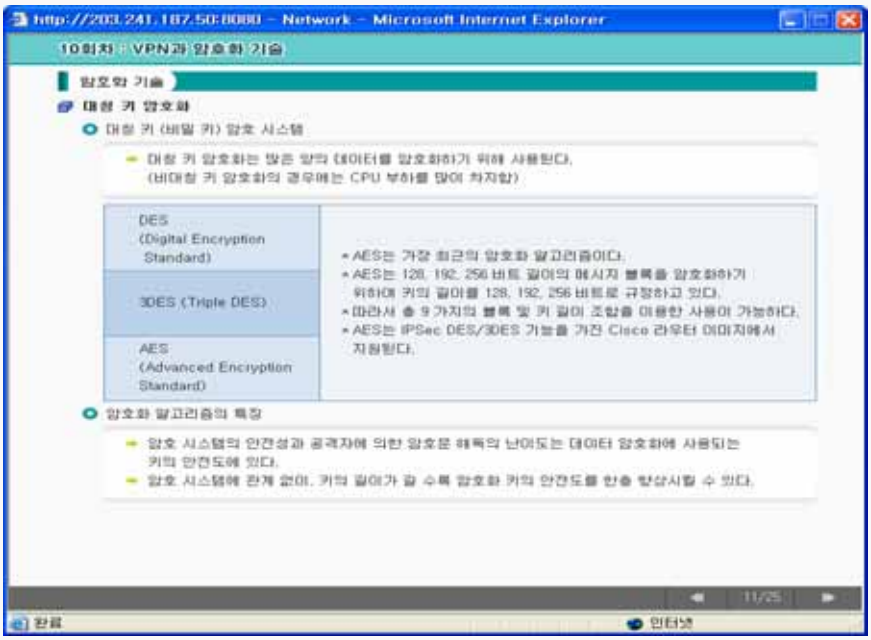
- TCP 기반의 애플리케이션에 프라이버시, 인증, 무결성을 제공하는 SSL (Secure Socket Layer)과 같은 프로토콜을 이용한 일부 제 4 계층 보안 표준은 성공적이었다.
- SSL은 오늘날 전자 상거래 사이트에 많이 사용되고 있으나, 유연성 (flexibility), 구현 상의 용이성, 애플리케이션에 독립적이어야 할 이슈들을 해결하지는 못한다.
- SSL의 이러한 여러 가지 한계점을 해결할 수 있는 최근의 기술로는 TLS (Transport Layer Security)가 있다.

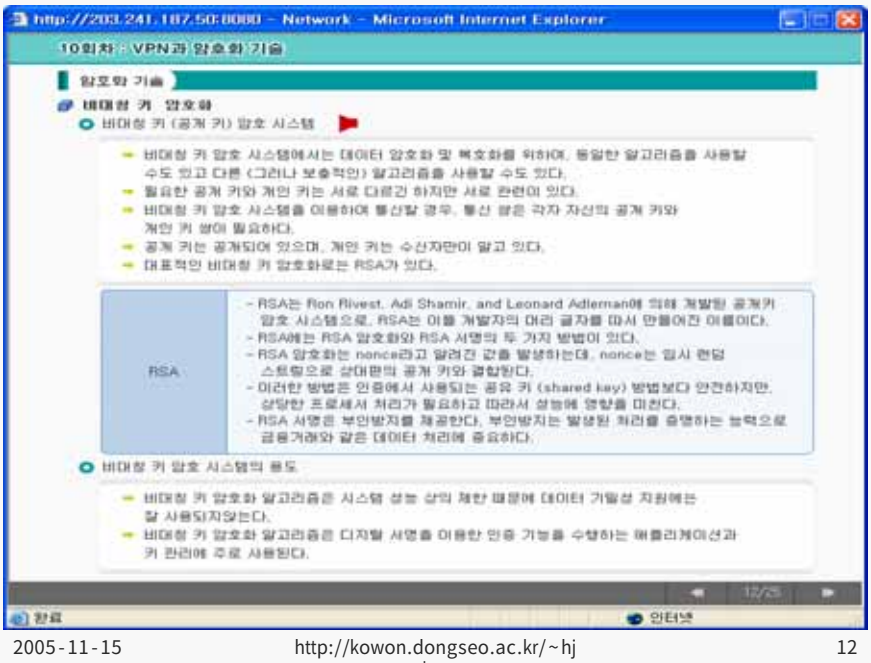

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
VPN
터널링 기술
터널링 프로토콜 종류
공중 네트워크 상에서 VPN을 생성하는 다양한 터널링 프로토콜이 있으며,
아래에 대표적인 몇 가지를 요약하였다.
Description
Standard
GRE
Generic Routing Encapsulation
RFC1701 and 2784
IPSec
Internet Protocol Security
RFC2401
L2F
Layer 2 Forwarding
Cisco
L2TP
Layer 2 Tunneling Protocol
RFC 2661
MPLS
Multiprotocol Label Switching
RFC 2547
PPTP
Point-To-Point Tunneling Protocol
Microsoft
GRE
IPSec
L2TP
MPLS
• IPSec은 VPN 보안성 지원을 위한 기술이며, IP 유니캐스트
트래픽 만을 지원한다.
• IP 유니캐스트 타입 이외의 터널링 패킷을 지원하기 위해서는
GRE나 L2TP를 사용해야 한다. 따라서 이러한 경우에는 IPSec은
암호화 기능 제공을 위하여 L2TP/IPSec과 GRE/IPSec과 같이
다른 프로토콜과 결합하여 사용할 수 있다.
3/25
완료
인터넷

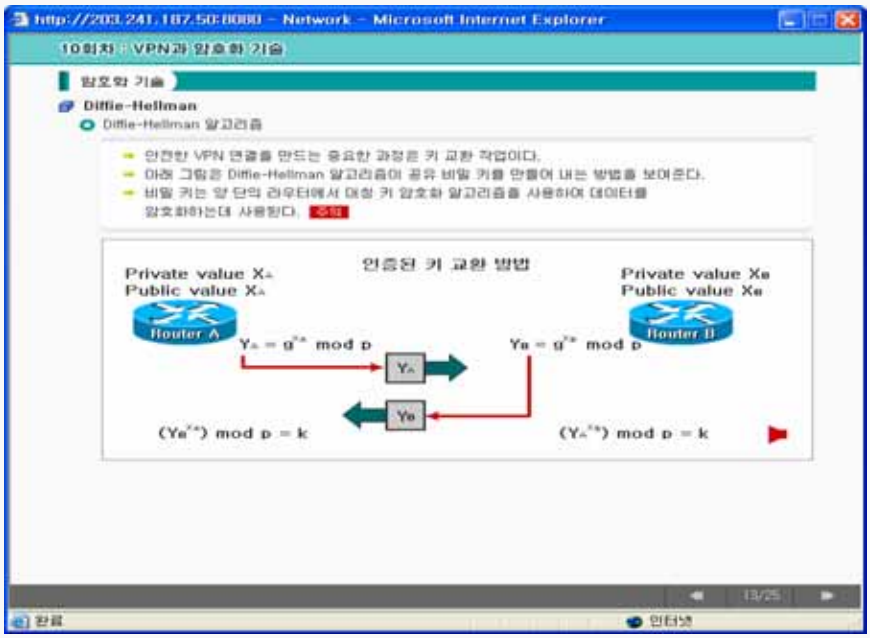

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
VPN
터널링 기술
터널링 프로토콜과 GRE 캡슐화 과정
DECnet
Appletalk
IP
IP
GRE Tunnel
DECnet
Appletalk
IP
Normal Packet
IP
TCP
Telnet
Tunnel Packet
IP
GRE
IP
TCP
Telnet
여기서 끝!!
8/25
완료
인터넷

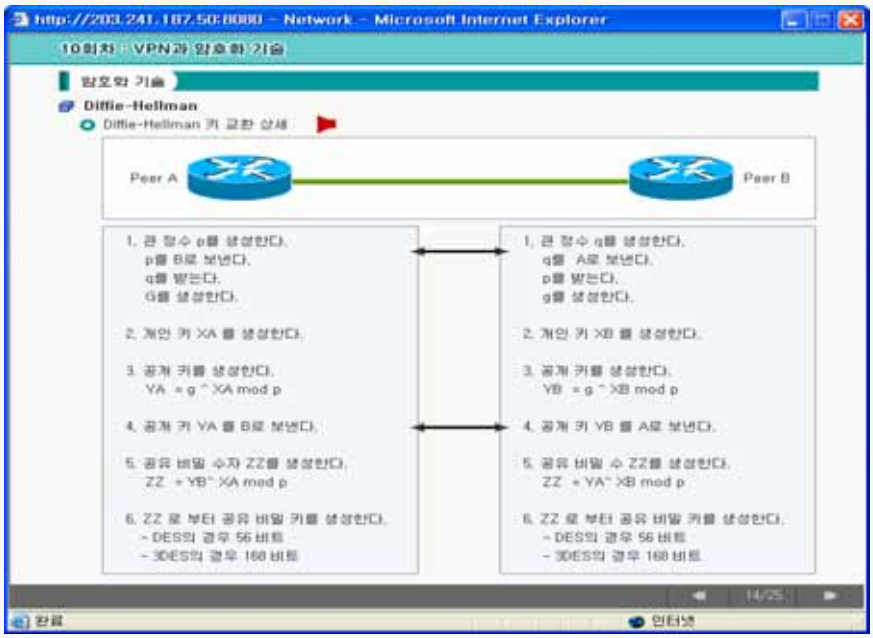

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
VPN
터널링 기술
터널 인터페이스
터널 인터페이스는 가상의 소프트웨어 인터페이스를 통하여 두 대의 라우터 간에 점대점 (point-to-point) 연결을 제공한다.
터널 인터페이스는, 인터넷과 같은 대규모 IP 네트워크를 통해 연결되어 있는 하부 인프라를 드러내지 않는,
라우터 간에 하나의 직접적인 링크 (direct link)를 제공하는 것으로 간주될 수 있다.
10.1.1.0
10.1.10.0
10.2.1.0
Registered Address
Internet
Registered Address
터널 인터페이스 설정 정보
몇 가지 중요한 터널 인터페이스 설정 정보를 요약하면 다음과 같다.
• Unnumbered Layer 3 address가 지원되기는 하지만, IPSec에 사용할 수는 없다.
• Access List는 터널 인터페이스에 적용할 수 있다.
• Voice over IP와 같은 트래픽 지원을 위한 서비스 품질 (QoS: Quality of Service) 지원이 가능하다.
• 터널 인터페이스에 CAR (Committed Access Rate), WFQ (Weighted Fair-Queue), WRED (Weighted Random Early Detection) 등은 현재 지원되지 않는다.
9/25
완료
인터넷

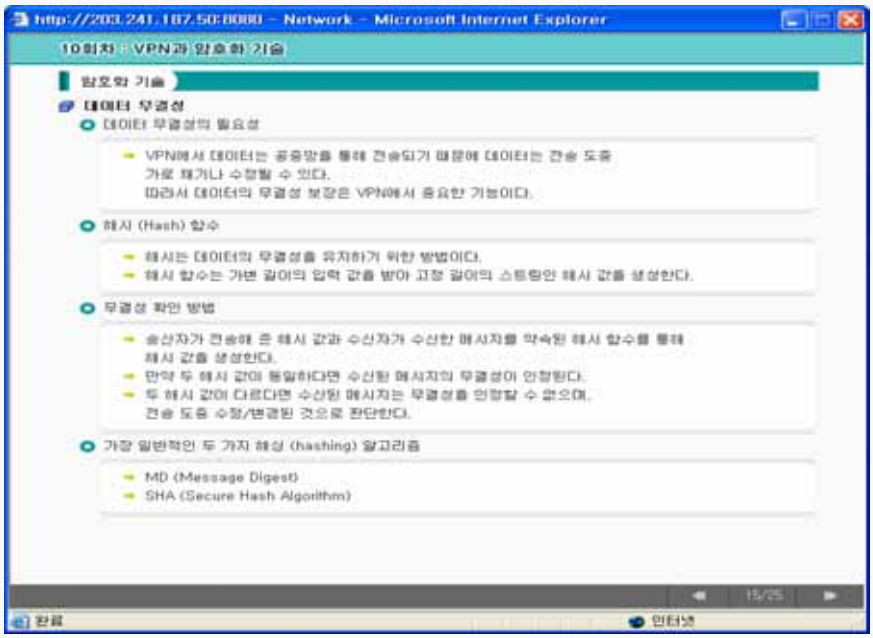

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
암호화 기술 개요
IOS 암호 시스템은 암호화 (encryption), 인증 (authentication), 키 관리 (key management)를 수행 할 수 있다.
암호화를 제공하는 두 가지 방법은 대칭 키와 비대칭 키 방법이다.
대칭 키 (비밀 키) 암호 시스템의 종류
- DES (Data Encryption Standard)
- 3DES (Triple Data Encryption Standard)
- AES (Advanced Encryption Standard)
비대칭 키 (공개 키) 암호 시스템의 종류
- RSA (Rivest, Shamir, Adleman) 알고리즘
- El Gamal 알고리즘
인증 기능을 제공하는 대표적인 기술의 종류는 아래와 같으며, MD5 (Message Digest 5)나 SHA (Secure Hash Algorithm)는 인증 작업을 도와주는 해시 함수에 속한다.
인증 기술의 종류
- MAC (Message Authentication Code)
- HMAC (Hashed Message Authentication Code)
- 디지털 서명 (digital signatures)
키 관리 방법에는 수동 작업 (manual operation), 비밀 키 교환 (secret key exchange), 공개 키 교환 (public key exchange)의 세 가지 방법이 있다.
이 중 비밀키 교환 방법인 Diffie-Hellman 방법이 가장 잘 알려져 있다.
Diffie-Hellman
Diffie-Hellman 방법은 실제의 키를 교환하지 않고 키 교환 기능을 구현한다.
Diffie-Hellman 방법은 데이터 암호화를 위한 세션 키 확립 알고리즘으로 널리 사용되고 있다.
10/25
완료
인터넷

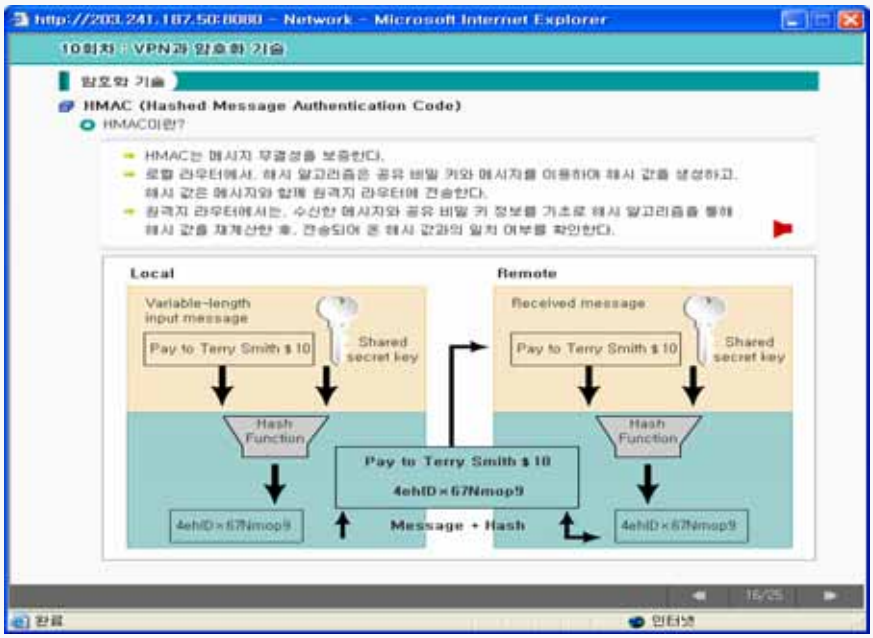

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
대칭 키 암호화
대칭 키 (비밀 키) 암호 시스템
대칭 키 암호화는 많은 양의 데이터를 암호화하기 위해 사용된다.
(비대칭 키 암호화의 경우에는 CPU 부하를 많이 차지함)
DES (Digital Encryption Standard)
3DES (Triple DES)
AES (Advanced Encryption Standard)
• AES는 가장 최근의 암호화 알고리즘이다.
• AES는 128, 192, 256 비트 길이의 메시지 블록을 암호화하기 위하여 키의 길이를 128, 192, 256 비트로 규정하고 있다.
• 따라서 총 9 가지의 블록 및 키 길이 조합을 이용한 사용이 가능하다.
• AES는 IPSec DES/3DES 기능을 가진 Cisco 라우터 이미지에서 지원된다.
암호화 알고리즘의 특징
암호 시스템의 안전성과 공격자에 의한 암호문 해독의 난이도는 데이터 암호화에 사용되는 키의 안전도에 있다.
암호 시스템에 관계 없이, 키의 길이가 길 수록 암호화 키의 안전도를 한층 향상시킬 수 있다.
11/25
완료
인터넷

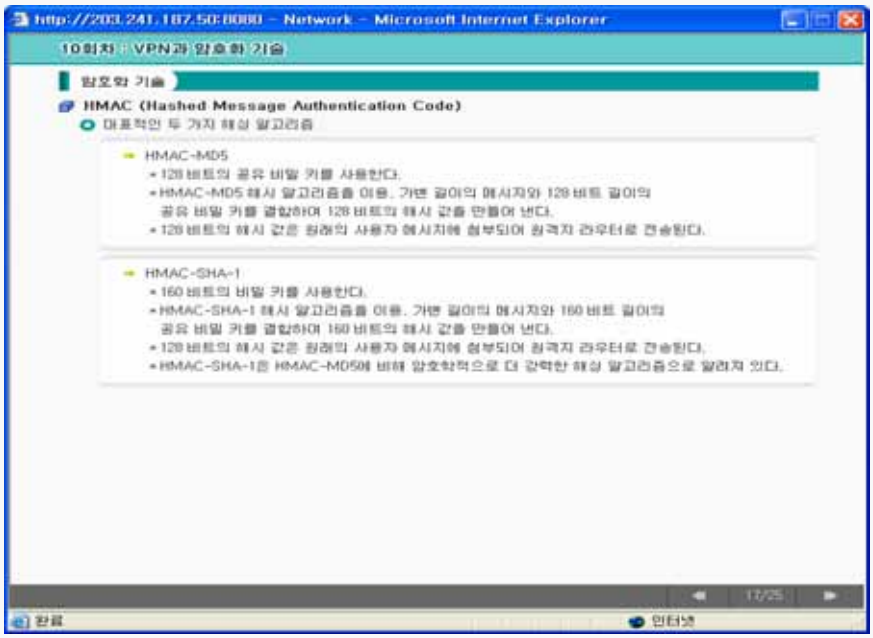

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
대칭 키 암호화
비대칭 키 (공개 키) 암호 시스템
비대칭 키 암호 시스템에서는 데이터 암호화 및 복호화를 위하여, 동일한 알고리즘을 사용할 수도 있고 다른 (그러나 보충적인) 알고리즘을 사용할 수도 있다.
필요한 공개 키와 개인 키는 서로 다르긴 하지만 서로 관련이 있다.
비대칭 키 암호 시스템을 이용하여 통신할 경우, 통신 참여 각자 자신의 공개 키와 개인 키 쌍이 필요하다.
공개 키는 공개되어 있으며, 개인 키는 수신자만이 알고 있다.
대표적인 비대칭 키 암호화로는 RSA가 있다.
RSA
- RSA는 Ron Rivest, Adi Shamir, and Leonard Adleman에 의해 개발된 공개키 암호 시스템으로, RSA는 이들 개발자의 머리 글자를 따서 만들어진 이름이다.
- RSA에는 RSA 암호화와 RSA 서명의 두 가지 방법이 있다.
- RSA 암호화는 nonce라고 알려진 값을 발생하는데, nonce는 임시 랜덤 스트링으로 상대편의 공개 키와 결합된다.
- 이러한 방법은 인증에서 사용되는 공유 키 (shared key) 방법보다 안전하지만, 상당한 프로세서 처리가 필요하고 따라서 성능에 영향을 미친다.
- RSA 서명은 부인방지를 제공한다. 부인방지는 발생된 처리를 증명하는 능력으로 금융거래와 같은 데이터 처리에 중요하다.
비대칭 키 암호 시스템의 용도
비대칭 키 암호화 알고리즘은 시스템 성능 상의 제한 때문에 데이터 기밀성 지원에는 잘 사용되지않는다.
비대칭 키 암호화 알고리즘은 디지털 서명을 이용한 인증 기능을 수행하는 애플리케이션과 키 관리에 주로 사용된다.
12/25
완료
인터넷

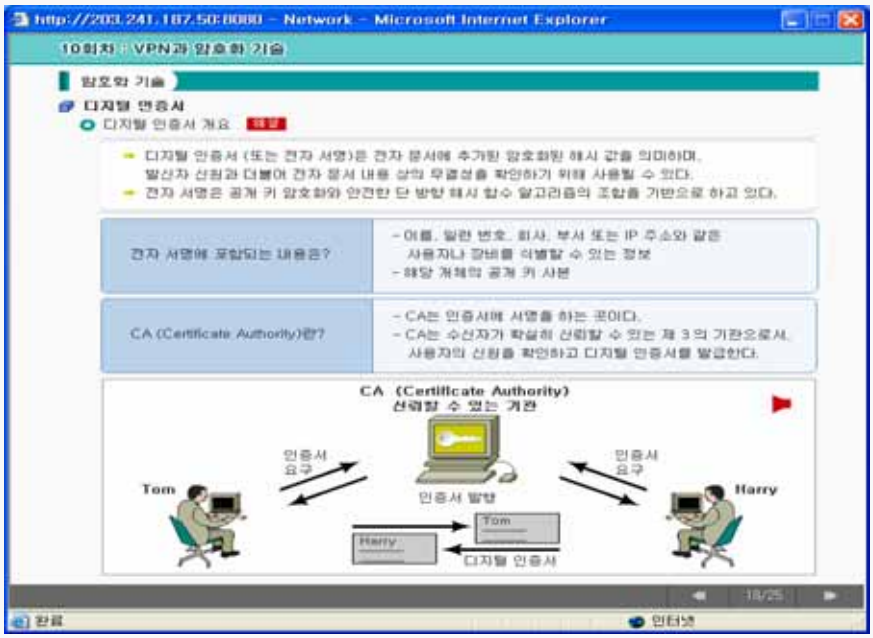

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
Diffie-Hellman
Diffie-Hellman 알고리즘
안전한 VPN 연결을 만드는 중요한 과정은 키 교환 작업이다.
아래 그림은 Diffie-Hellman 알고리즘이 공유 비밀 키를 만들어 내는 방법을 보여준다.
비밀 키는 양 단의 라우터에서 대칭 키 암호화 알고리즘을 사용하여 데이터를 암호화하는데 사용된다.
인증된 키 교환 방법
Private value XA
Public value XA
Private value XB
Public value XB
Router A
Router B
YA = g^XA mod p
YB = g^XB mod p
YA
YB
(YB^XA) mod p = k
(YA^XB) mod p = k
13/25
완료
인터넷

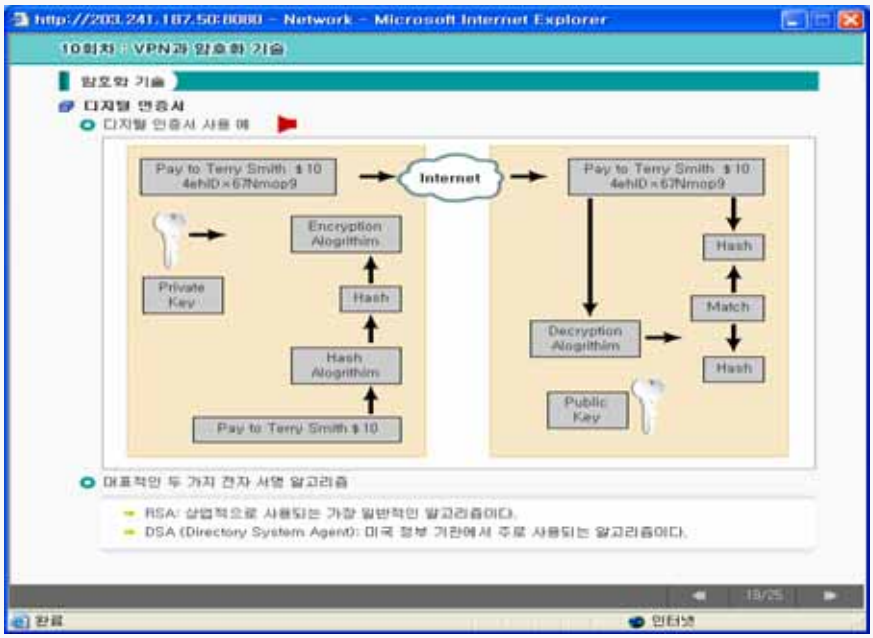

http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
Diffie-Hellman
Diffie-Hellman 키 교환 상세
Peer A
Peer B
1. 큰 정수 q를 생성한다.
p를 B로 보낸다.
q를 받는다.
g를 생성한다.
2. 개인 키 XA 를 생성한다.
3. 공개 키를 생성한다.
YA = g ^ XA mod p
4. 공개 키 YA 를 B로 보낸다.
5. 공유 비밀 수자 ZZ를 생성한다.
ZZ = YB^ XA mod p
6. ZZ 로 부터 공유 비밀 키를 생성한다.
- DES의 경우 56 비트
- 3DES의 경우 168 비트
1. 큰 정수 q를 생성한다.
q를 A로 보낸다.
p를 받는다.
g를 생성한다.
2. 개인 키 XB 를 생성한다.
3. 공개 키를 생성한다.
YB = g ^ XB mod p
4. 공개 키 YB 를 A로 보낸다.
5. 공유 비밀 수 ZZ를 생성한다.
ZZ = YA^ XB mod p
6. ZZ 로 부터 공유 비밀 키를 생성한다.
- DES의 경우 56 비트
- 3DES의 경우 168 비트
14/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
데이터 무결성
데이터 무결성의 필요성
VPN에서 데이터는 공중망을 통해 전송되기 때문에 데이터는 전송 도중
가로 채거나 수정될 수 있다.
따라서 데이터의 무결성 보장은 VPN에서 중요한 기능이다.
해시 (Hash) 함수
해시는 데이터의 무결성을 유지하기 위한 방법이다.
해시 함수는 가변 길이의 입력 값을 받아 고정 길이의 스트링인 해시 값을 생성한다.
무결성 확인 방법
송신자가 전송해 온 해시 값과 수신자가 수신한 메시지를 약속된 해시 함수를 통해
해시 값을 생성한다.
만약 두 해시 값이 동일하다면 수신된 메시지의 무결성이 인정된다.
두 해시 값이 다르다면 수신된 메시지는 무결성을 인정할 수 없으며,
전송 도중 수정/변경된 것으로 판단한다.
가장 일반적인 두 가지 해싱 (hashing) 알고리즘
MD (Message Digest)
SHA (Secure Hash Algorithm)
15/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
HMAC (Hashed Message Authentication Code)
HMAC이란?
HMAC는 메시지 무결성을 보증한다.
로컬 라우터에서, 해시 알고리즘은 공유 비밀 키와 메시지를 이용하여 해시 값을 생성하고,
해시 값은 메시지와 함께 원격지 라우터에 전송한다.
원격지 라우터에서는, 수신한 메시지와 공유 비밀 키 정보를 기초로 해시 알고리즘을 통해
해시 값을 재계산한 후, 전송되어 온 해시 값과의 일치 여부를 확인한다.
Local
Remote
Variable-length input message
Pay to Terry Smith $ 10
Shared secret key
Received message
Hash Function
Pay to Terry Smith $ 10
4ehID×67Nmop9
Message + Hash
16/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
HMAC (Hashed Message Authentication Code)
대표적인 두 가지 해싱 알고리즘
HMAC-MD5
128 비트의 공유 비밀 키를 사용한다.
HMAC-MD5 해시 알고리즘을 이용, 가변 길이의 메시지와 128 비트 길이의 공유 비밀 키를 결합하여 128 비트의 해시 값을 만들어 낸다.
128 비트의 해시 값은 원래의 사용자 메시지에 첨부되어 원격지 라우터로 전송된다.
HMAC-SHA-1
160 비트의 비밀 키를 사용한다.
HMAC-SHA-1 해시 알고리즘을 이용, 가변 길이의 메시지와 160 비트 길이의 공유 비밀 키를 결합하여 160 비트의 해시 값을 만들어 낸다.
128 비트의 해시 값은 원래의 사용자 메시지에 첨부되어 원격지 라우터로 전송된다.
HMAC-SHA-1은 HMAC-MD5에 비해 암호학적으로 더 강력한 해싱 알고리즘으로 알려져 있다.
17/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
디지털 인증서
디지털 인증서 개요
디지털 인증서 (또는 전자 서명)은 전자 문서에 추가된 암호화된 해시 값을 의미하며, 발신자 신원과 더불어 전자 문서 내용 상의 무결성을 확인하기 위해 사용될 수 있다.
전자 서명은 공개 키 암호화와 안전한 단 방향 해시 함수 알고리즘의 조합을 기반으로 하고 있다.
전자 서명에 포함되는 내용은?
- 이름, 일련 번호, 회사, 부서 또는 IP 주소와 같은 사용자나 장비를 식별할 수 있는 정보
- 해당 개체의 공개 키 사본
CA (Certificate Authority)란?
- CA는 인증서에 서명을 하는 곳이다.
- CA는 수신자가 확실히 신뢰할 수 있는 제 3 의 기관으로서, 사용자의 신원을 확인하고 디지털 인증서를 발급한다.
CA (Certificate Authority)
신뢰할 수 있는 기관
인증서 요구
인증서 요구
Tom
Harry
인증서 발행
Tom
Harry
디지털 인증서
18/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
암호화 기술
디지털 인증서
디지털 인증서 사용 예
Pay to Terry Smith $10
4ehID×67Nmop9
Internet
Pay to Terry Smith $10
4ehID×67Nmop9
Encryption Alogrithm
Private Key
Hash
Hash Alogrithm
Pay to Terry Smith $10
Hash
Match
Hash
Decryption Alogrithm
Public Key
대표적인 두 가지 전자 서명 알고리즘
RSA: 상업적으로 사용되는 가장 일반적인 알고리즘이다.
DSA (Directory System Agent): 미국 정부 기관에서 주로 사용되는 알고리즘이다.
19/25
완료
인터넷


http://203.241.187.50:8080 - Network - Microsoft Internet Explorer
10회차 : VPN과 암호화 기술
지금까지 공부한 내용을 요약하여 다시 한번 정리를 하도록 하겠습니다.
부족한 부분은 다시 한번 확인 하시기 바랍니다.
VPN
VPN은 공중망 상에서 가상의 사설망을 사용하는 것과 같은 효과를 주는 기술이다.
VPN의 종류로는 사이트 간 VPN과 원격 접속 VPN이 있다.
VPN을 구현하기 위해서는 터널링 기술이 필요하며, 터널링 프로토콜의 종류로는 GRE, IPSec, L2TP 등이 있다.
암호화 기술
IOS 암호 시스템은 암호화, 인증, 키 관리를 할 수 있다.
암호화를 제공하는 2가지 방법은 대칭 키와 비대칭 키 이다.
대칭 키 암호화는 암호화와 복호화에 사용하는 키가 동일한 것이고 비대칭 키 암호화는 암호화와 복호화에 사용하는 키가 다른 것이다.
인증 기술의 종류로는 MAC, HMAC이 있다.
키 관리 방법에는 수동 작업, 비밀 키 교환, 공개 키 교환 등이 있다.
키 교환과 데이터 무결성
암호화 통신을 위해서는 통신 당사자 간에 키를 교환해야 한다.
일반적으로 키 교환을 위해 Diffie-Hellman 알고리즘을 주로 사용한다.
데이터 무결성을 위해서는 해시 알고리즘을 주로 사용한다.
20/25
완료
인터넷

End of Lecture