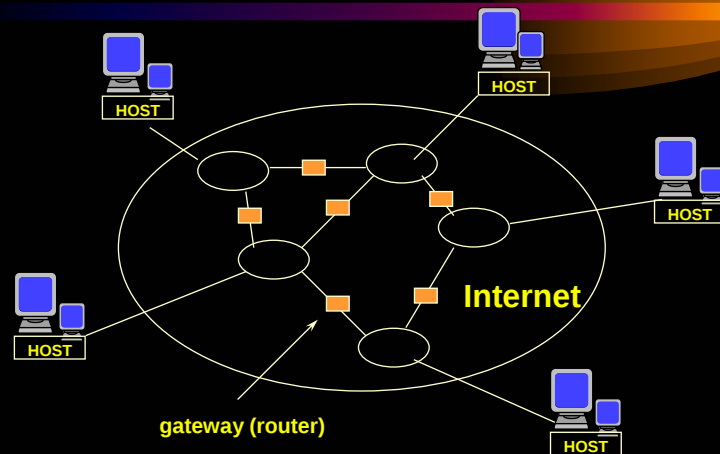


INTERNET SECURITY

□ Structure of TCP/IP Internet



INTERNET SECURITY

□ Internet Address

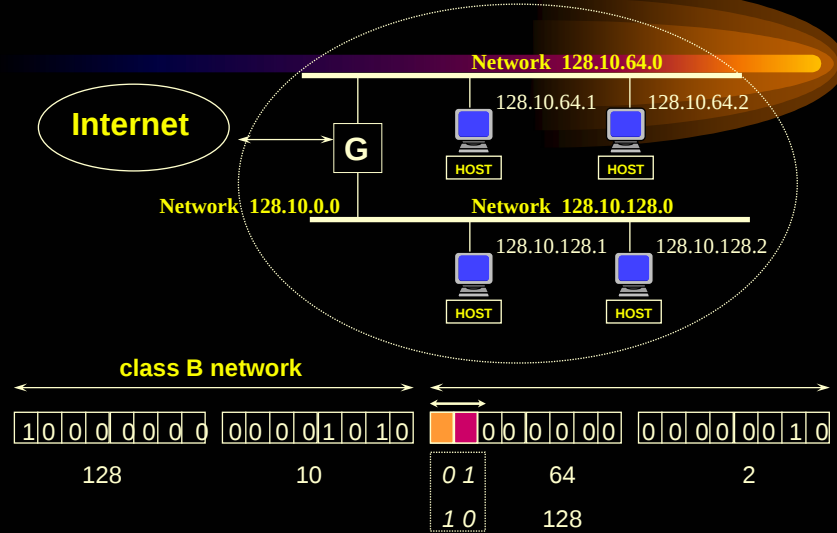
	0	8	31
Class A	0	netid	hostid
	0	16	31
Class B	1 0	netid	hostid
	0	24	31
Class C	1 1 0	netid	hostid

Network Address : (A) 1 ~ 127, (B) 128 ~ 191, (C) 192 ~ 223

10000000 00001010 00000010 00011110
128 . 10 . 2 . 30

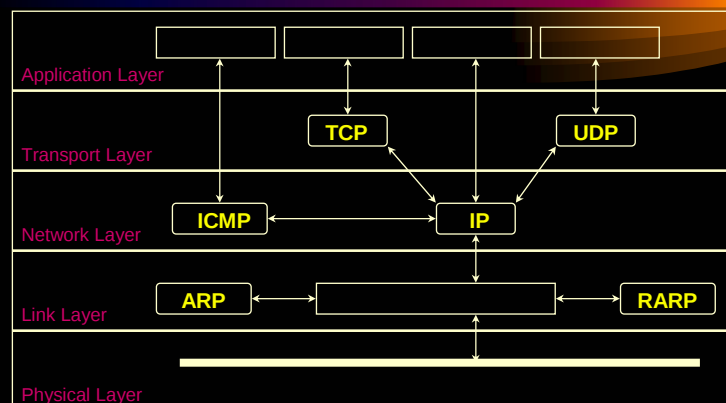
INTERNET SECURITY

Subnet Address



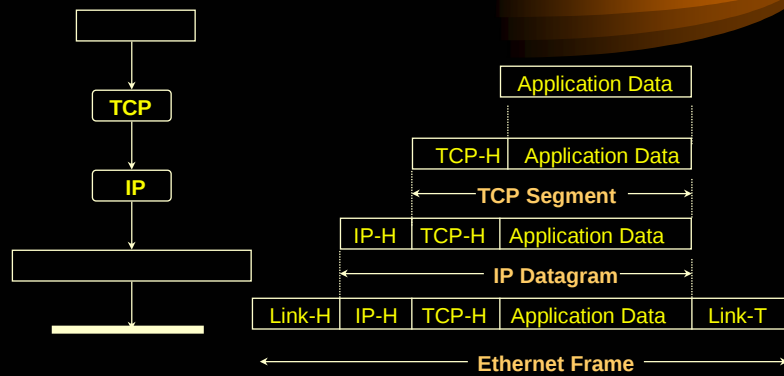
INTERNET SECURITY

TCP/IP Network Model



INTERNET SECURITY

❑ Encapsulation



INTERNET SECURITY

❑ IP (Internet Protocol)

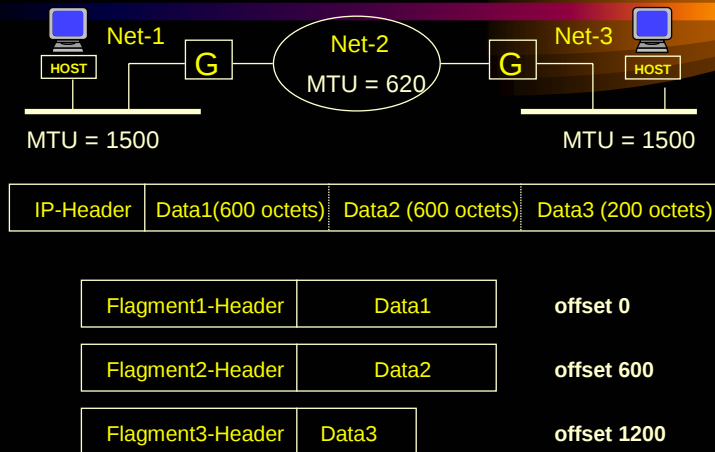
- Unreliable, connectionless delivery system
- Routing function
- IP Datagram = Header + Data

Ver	HLen	Service Type	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
IP Option (if any)				Padding
DATA				

IP Header

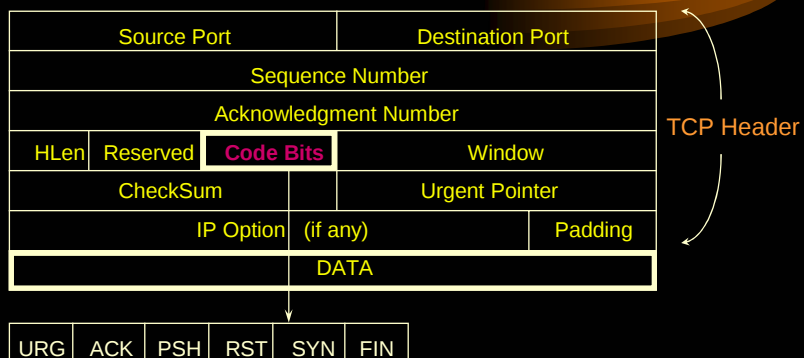
INTERNET SECURITY

❑ Fragmentation



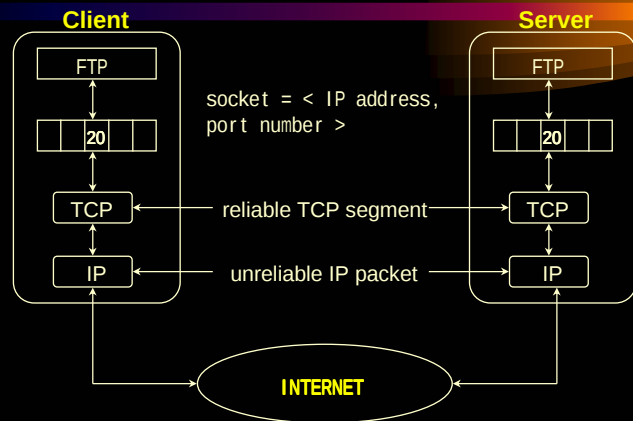
INTERNET SECURITY

❑ TCP Segment Format



INTERNET SECURITY

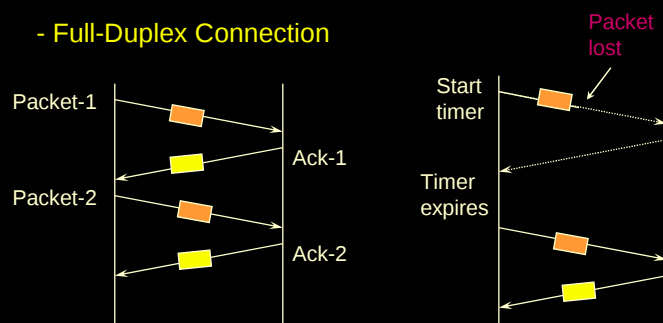
❑ TCP Connection



INTERNET SECURITY

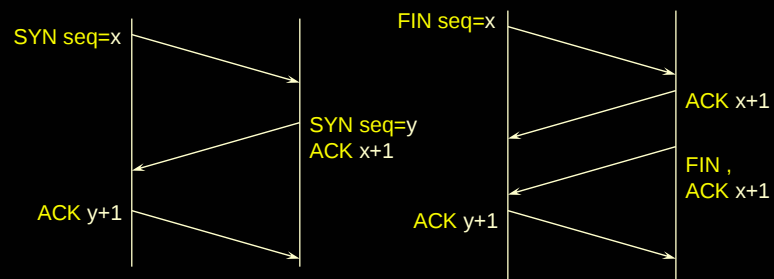
❑ TCP (Transport Control Protocol)

- Reliable Delivery Service
 - Acknowledgment with Retransmission
- Connection-Oriented Service
- Full-Duplex Connection



INTERNET SECURITY

❑ Open/Close TCP Connection

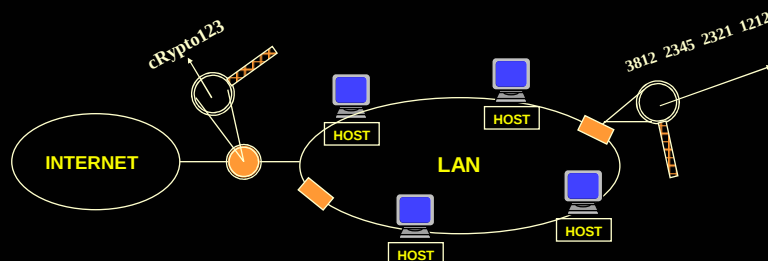


INTERNET SECURITY

❑ Sniffing

• LAN analyzer (sniffer)

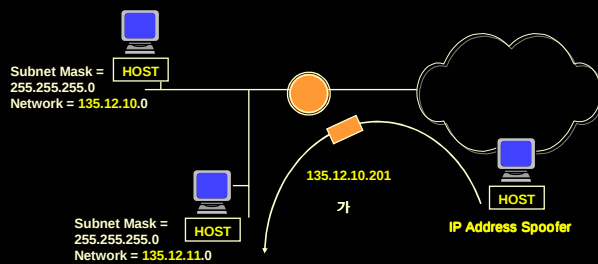
- password
- ()
- protocol



INTERNET SECURITY

❑ Spoofing

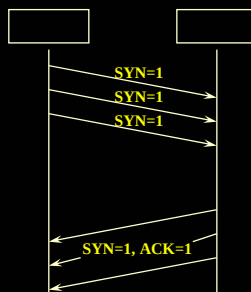
- IP spoofing



INTERNET SECURITY

❑ Spoofing

- Denial-of Service : TCP SYN flooding

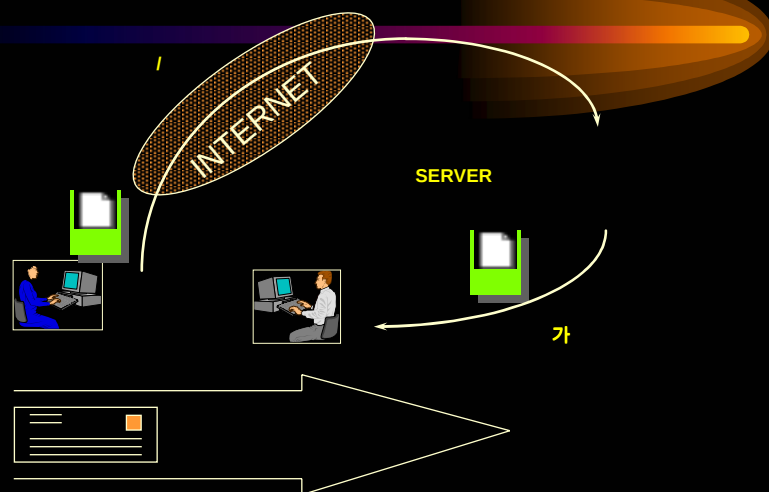


❑ Spoofing

- Plug-In (NetScape)
- ActiveX (MS Explorer)

- Plug-In (NetScape)

- **ActiveX** (MS Explorer)



- PGP

- 

- 

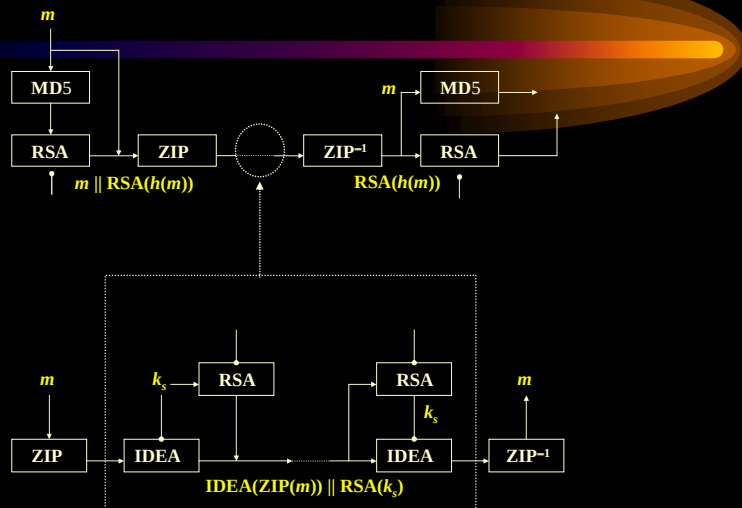
MD5

- 

9

INTERNET SECURITY

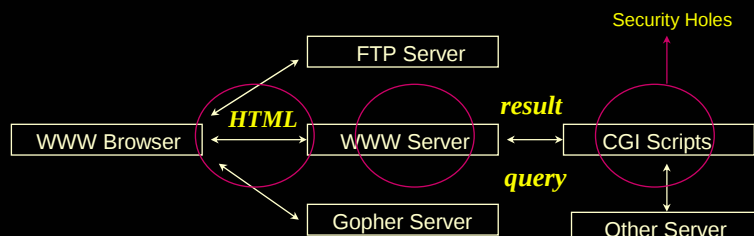
PGP



INTERNET SECURITY

WWW

- Browser (Mosaic, Netscape) Server (NCSA HTTP, httpd)
- URL (Uniform Resource Locator)
- HTML (HyperText Manipulation Language)
- CGI (Common Gateway Interface) - e.g. form processing



INTERNET SECURITY

□ WWW

□ Client / Server

-
-

□ WWW

-

- **SSL** (Secure Socket Layer)
- **PCT** (Privacy Communication Technology)

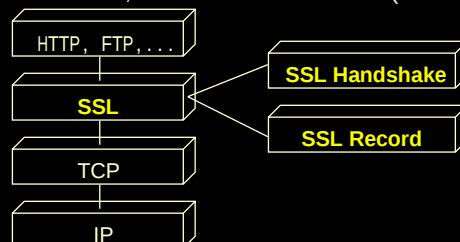
-

- **S-HTTP**

INTERNET SECURITY

□ **SSL (secure socket layer)**

- Netscape Communications
- Privacy, Data Integrity, Server [Client] Authentication,
- RSA, Diffie-Hellman, Fortezza for Key Exchange
- DES, 3DES, IDEA, RC2, RC4[stream cipher] for Data Encryption
- MD5, SHA for Hash Function (MAC)



Algorithm Negotiation,
Key Exchange,
Authentication

Data Encapsulation
for data protection

INTERNET SECURITY

❑ SSL Handshake Protocol



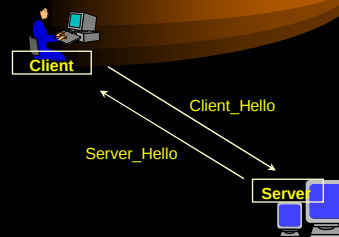
INTERNET SECURITY

❑ SSL Client Hello Phase

- ❑ client version
- ❑ 28-byte random number R
- ❑ session ID
- ❑ cipher_suites
- ❑ compression methods

❑ SSL Server Hello Phase

- ❑ client version
- ❑ 28-byte random number R'
- ❑ session ID -> If a new session, server's certificate
- ❑ cipher_suite { key exchange algorithm }
- ❑ compression method



INTERNET SECURITY

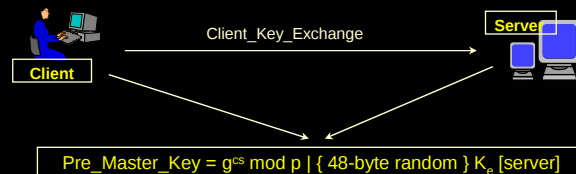
□ SSL Client Key Exchange

- Key Exchange Algorithm's Parameter in Certificate
- RSA : public exponent k_e , modulus n
- Diffie-Hellman : g , modulus p , $g^s \bmod p$
- From *Pre_Master_Key* To *Master-Key* [MD5, SHA, R, R']

$$\text{Master_Key} = \text{MD5}(\text{Pre_Master_Key} + \text{SHA}('A' + \text{Pre_Master_Key} + R + R')) +$$

$$\text{MD5}(\text{Pre_Master_Key} + \text{SHA}('BB' + \text{Pre_Master_Key} + R + R')) +$$

$$\text{MD5}(\text{Pre_Master_Key} + \text{SHA}('CCC' + \text{Pre_Master_Key} + R + R'))$$



INTERNET SECURITY

□ SSL Session Key Generation

- Keys for data encryption and data integrity

$$\text{Key_Block} = \text{MD5}(\text{Master_Key} + \text{SHA}('A' + \text{Master_Key} + R + R')) +$$

$$\text{MD5}(\text{Master_Key} + \text{SHA}('BB' + \text{Master_Key} + R + R')) +$$

$$\text{MD5}(\text{Master_Key} + \text{SHA}('CCC' + \text{Master_Key} + R + R')) + \dots$$

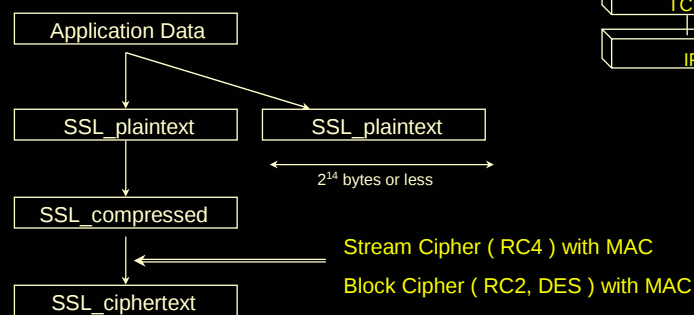
□ SSL Client-Server Finished

- Key Exchange, Authentication
- Negotiated Algorithm, Parameter
- All Handshaked Messages
- Sender's value { client[0x434C4E54], server[0x53525652] }

INTERNET SECURITY

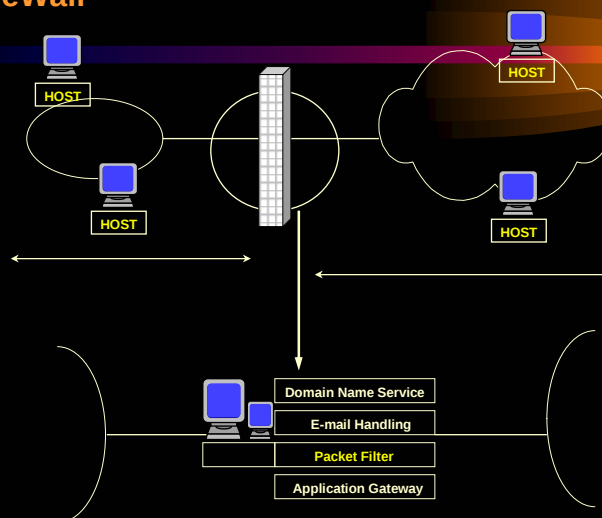
SSL Record Protocol

- Fragmentation
- Compression
- Protection



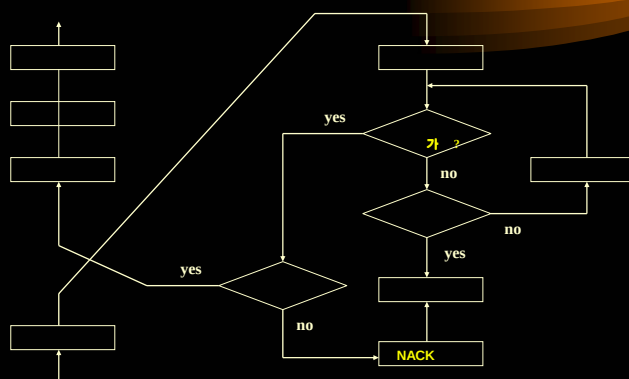
INTERNET SECURITY

FireWall



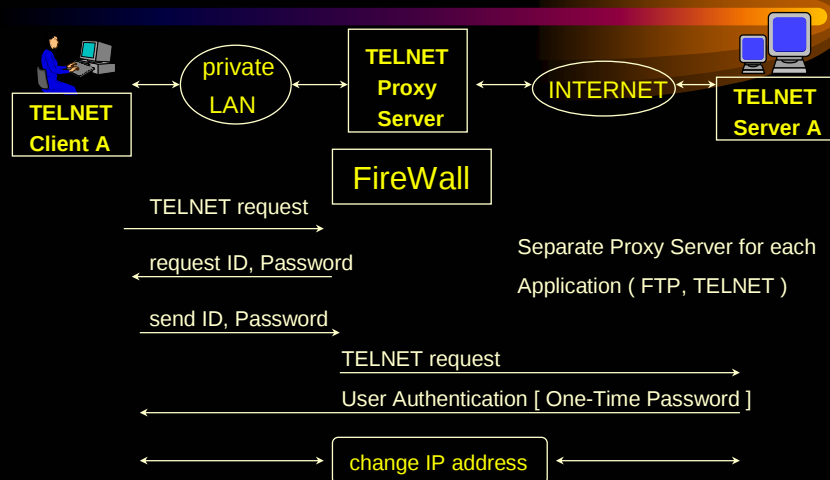
INTERNET SECURITY

❑ Packet Filter Operations



INTERNET SECURITY

❑ Proxy Server



INTERNET SECURITY

❑ Externalized FTP Server

