계층별 기능
물리 계층(physical layer): 물리적으로 데이터를 전송하는 역할-byte, bit stream
식별자: NIC(Network Interface Card)serial number

데이터 링크 계층(datalink layer): 데이터의 물리적 전송 오류를 해결, 오류검출, 흐름제어 – frame
식별자: mac(medium access control) address

네트워크 계층(network layer): 라우팅, 혼합제어, 패킷의 분할과 병합 – 패킷 식별자: IP address

전송 계층(transport layer): 흐름 제어, 오류 제어, 분할과 병합, 서비스 프리미티브 – 패킷
식별자: 포트(port)(예약번호 존재)

세션 계층: 대화 개념을 지원하는 상위의 논리적 연결을 지원

표현 계층: 데이터의 의미와 표현 방법을 처리, 데이터를 코딩하는 문제를 다룸

응용 계층(application layer): 최상위, 다양하게 존재하는 응용 환경에서 공통으로 필요한 기능을 다룸 – 메시지
식별자: socket number = process number

WAN(Wide Area Network): 광역통신, 먼거리의 통신

LAN(Local Area Network): 근거리 통신

MAN(Metropolitan Area Network): LAN보다 큰 지역을 지원하는 통신

HTTP(HyperText Transfer Protocol): 웹 서버와 사용자의 인터넷 브라우저 사이에 문서를 전송하기 위해 사용되는 통신 규약

FTP(File Transfer Protocol): 파일 전송 프로토콜

SMTP(Simple Mail Transfer Protocol): 인터넷 상에서 전자 메일을 전송할 때 쓰이는 표준적인 프로토콜

SNMP(Simple Network Management Protocol):네트워크 상의 장비로부터 정보를 읽거나 수정할 수 있는 프로토콜

IMAP(Internet Messaging Access Protocol): 메일을 읽기 위한 인터넷 표준 통신 규약

POP(Post Office Protocol): 메일 서버에 보관된 메일을 개인용 PC로 다운로드하는 프로토콜

전송계층
tcp 연결 해제는 양쪽 프로세스의 동의하에 해제(two-way)
tcp 연결 설정은 3단계 설정(Three-Way Handshake)방식으로 설정
1.송신 프로세스는 TCP 헤더의 SYN 플래그를 지정한 세그먼트를 전송함으로써 연결 설정을 요구
2.연결 설정 요구를 받은 수신 프로세스가 연결 수락->SYN과 ACK 플래그를 지정해 연결에 대한 긍정 응답 표시
3.세그먼트는 수신 프로세스가 전송한 연결 수락 세그먼트가 제대로 도착했음을 알림

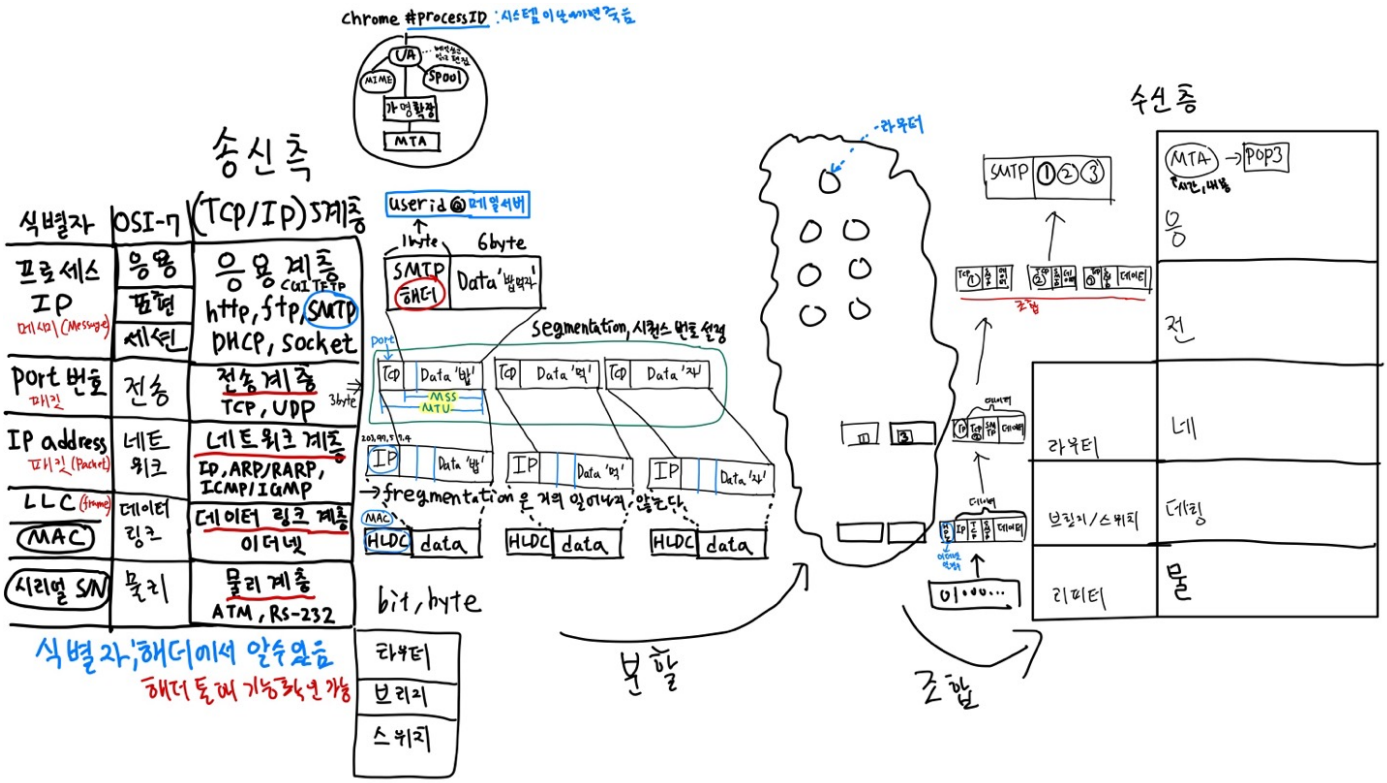
MTU(Maximum Transfer Unit): 전송할 수 있는 최대크기
MSS(Maximum Segmentation Size): TCP 헤더를 제외한 데이터크기
Segmentation: MTU 크기만큼 데이터를 나누는 것을 말합니다.

응용계층

MIME(Multipurpose Internet Mail Extensions): 인터넷의 전자 메일에서 사용되는 문자 데이터를 표현하기 위한 형식 표준(비 아스키코드->아스키코드)

Spool(동시처리 기술): 지연을 허용, 보조기억장치를 사용하여 그 데이터를 임시적으로 보관

UA(user, agent): 사용자 에이전트, MTA(Mail Transfer Agent): 메시지전달 에이전트, alias expansion: 가명 확장



TCP 포트 번호: TCP와 UDP가 상위 계층에 제공하는 주소 표현 방식

서비스	포트번호	서비스	포트번호
FTP(데이터 채널)	20	Telnet	23
FTP(제어 채널)	21	SMTP	25
DNS	53	HTTP	80
TFTP	69		

네트워크 보안

컴퓨터 보안: 컴퓨터 자체의 데이터 보호하는 것|

네트워크 보안: 컴퓨터 간에 데이터를 안전하게 전송하는 것

IP 스푸핑(IP Spoofing): IP 주소를 속이는 행위 => 외부 네트워크 공격자가 정보를 빼가는 행위 수법

차단방법: 액세스 제어(송신지 주소를 가진 외부 네트워크의 패킷을 모두 거부 -> IP 스푸핑을 공격 줄임), 필터링(송신지 주소를 보유하지 않는 패킷이 외부 차단), 암호화(패킷을 암호화하는 것)

IP 스니핑(IP Sniffing): 도청행위 => 비밀성과 무결성을 보장할 수 없으며 비밀성을 해치는 대표적인 공격 방법

방화벽(Firewall)
기본 구성요소: 네트워크 정책, 방화벽 사용자 인증 시스템, 패킷 필터링, 응용 계층 게이트웨이

종류
스크리닝 라우터: 필터링 속도가 빠르고, 비용이 적게 듦, 네트워크 계층과 전송 계층의 트래픽만 방어만 가능해서 응용 계층대한 데이터 공격에 방어할 수 없음
배스타 호스트: 게이트웨이 역할을 하며, 모든 시스템의 기록을 주기적으로 검사해서 응용 서비스 안전성이 높고 로그 정보의 생성과 관리가 용이하지만 베스타 호스트가 손상되면 내부 네트워크를 전혀 보호할 수 없고 각종 로그인 정보가 누출되면 방화벽 역할이 불가능함

방화벽 시스템 방식->패킷 필터링 방식, 응용 프로그램 게이트웨이, 회로 레벨 게이트웨이, 혼용 방화벽

침입 탐지 시스템(IDS -> Intrusion Detection System): 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템

침입 방지 시스템(IPS -> Intrusion Prevention System): 비정상적인 트래픽을 능동적으로 처단하고 격리하는 등의 방어 조치를 취하는 보안 솔루션

대칭키 방식: 암호키 = 해독키, 비대칭키 방식: 암호키 ≠ 해독키

DES(Data Encryption Standard) 알고리즘: 대칭키의 비공개키, 암호키->56비트, 64비트 단위로 암호화, 16+2단계

RSA(Rivest Shamir Adleman) 알고리즘: 비대칭키의 공개키 알고리즘 => 공개키: 모든 사람이 암호화 과정 수행, 비공개키: 특정인만 해독 과정 수행

전자 서명: RSA 알고리즘과 반대 원리로 동작 =>공개키: 모든 사람이 해독 과정 수행, 비공개키: 특정인만 암호화 과정 수행

"비밀키 암호화 방식: 암호키와 복호키가 동일, 두 개체가 같은 키를 공유하면서 하나의 키를 사용하여 암호화하고 복호화

공개키 암호화 방식: 암호키가 공개되어 있어 누구나 원하는 내용을 암호화할 수 있지만, 해당 복호화키를 가진 사람만 그 암호문을 복호화할 수 있음 -> 암호키를 '공개키'라 하고, 복호키를 '개인키'

PGP(Pretty Good Privacy): 이메일을 암호화하거나 복호화하여 제3자가 알 수 업도록 만드는 보안 프로그램

PEM(Privacy Enhanced Mail): SMTP에는 메시지를 암호화하거나 메시지가 중간에 수정되는 것을 검증하는 보안 기능이 포함되지 않음, 암호화 -> 데이터 유출되면 내용 알아보기 힘듦, 인터넷 표준안, 군사용 및 은행 시스템용"

낮은 중요한 내용

전송계층

TCP(Transmission Control Protocol): IP 프로토콜 위에서 연결형 서비스를 지원하는 전송계층 프로토콜

UDP(User Datagram Protocol): 비연결형, 신뢰성이 떨어지지만 처리가 빠르고 실시간으로 보냄

응용계층
URL(Uniform Resource Locator): 웹 서버의 자원 명칭(프로토콜X)

APM(Apache, PHP, MySQL)

CGI(Common Gateway Interface): 서버와 응용프로그램 사이에 데이터를 주고받기 위한 표준화된 방법

TFTP(Trivial File Transfer Protocol): 임의의 시스템이 원격 시스템으로부터 부팅 코드를 다운로드하는 데 사용되는 프로토콜

DHCP(Dynamic Host Configuration Protocol): 종적의 IP 주소 사용(동적 IP 받음) => DHCP서버가 판별할 수 있도록 하고 서브 네트워크에 적절한 IP 주소를 할당함

인터네트워킹: 둘 이상의 서로 다른 네트워크를 연결하는 기능

리피터(repeater): 물리 계층의 기능을 지원, 신호를 증폭, 단순히 전달하는 역할

스위치(switcher): 데이터 링크 계층의 기능 지원, 통신 허용 장비

브리지(bridge): 데이터 링크 계층의 기능을 지원, MAC 계층 헤더를 다른 단의 MAC 계층 헤더로 변형해 전송

라우터(router): 네트워크 계층의 기능 지원, 라우팅 기능을 수행, 여러 포트를 사용해서 다수의 LAN을 연결 구조

게이트웨이(Gateway): 서로 다른 프로토콜끼리 네트워크 통신 가능한 연결 기기(응용계층, 전송계층)

가로채기(Interruption): 송신 측과 수신 측의 중요한 정보가 유출되는 심각 문제 발생

변조(Modification): 수신 측에서 송신 측에서 잘못된 데이터를 전송한 것으로 오인

네트워크 보안의 요구 사항: 비밀성, 무결성, 가용성

대체 암호화: 특정 문자 -> 문자
종류: 시저 암호화, 키워드 암호화

위치 암호화: 문자들의 배열 순서를 변경
종류: 칼럼 암호화, 키워드 암호화

인증: 사용자만 정보에 접근할 수 있도록 하는 것

전자 서명: 신원 확인을 위해 한 쌍의 키를 사용하여 자신을 증명하는 것