

# Network Service

---



# Part 1.

---

## Network Service



# 01 전자 메일

## 전자 메일 기본

전자 메일 시스템은 MTA, MUA, MDA 로 구성된다

MTA(Mail Transfer Agent)

자신에 등록되어 있는 메일서버에 SMTP를 사용하여 메일 전달

MUA(Mail User Agent)

Outlook Express 등과 같이 메일을 작성하고 읽는 사용자 인터페이스

MDA(Mail Delivery Agent)

메일서버에서 수신된 메일을 분류하여 해당 수신자의 메일박스에 메일 전달

메일 클라이언트에서 송신은 SMTP, 수신은 POP3 또는 IMAP4를 이용한다

MIME(Multipurpose Internet Mail Extension)는 멀티미디어 전자우편을 위한 표준으로, 멀티미디어 데이터를 ASCII 형식으로 변환할 필요없이 인터넷 전자우편으로 송신하기 위한 SMTP의 확장 규격이다

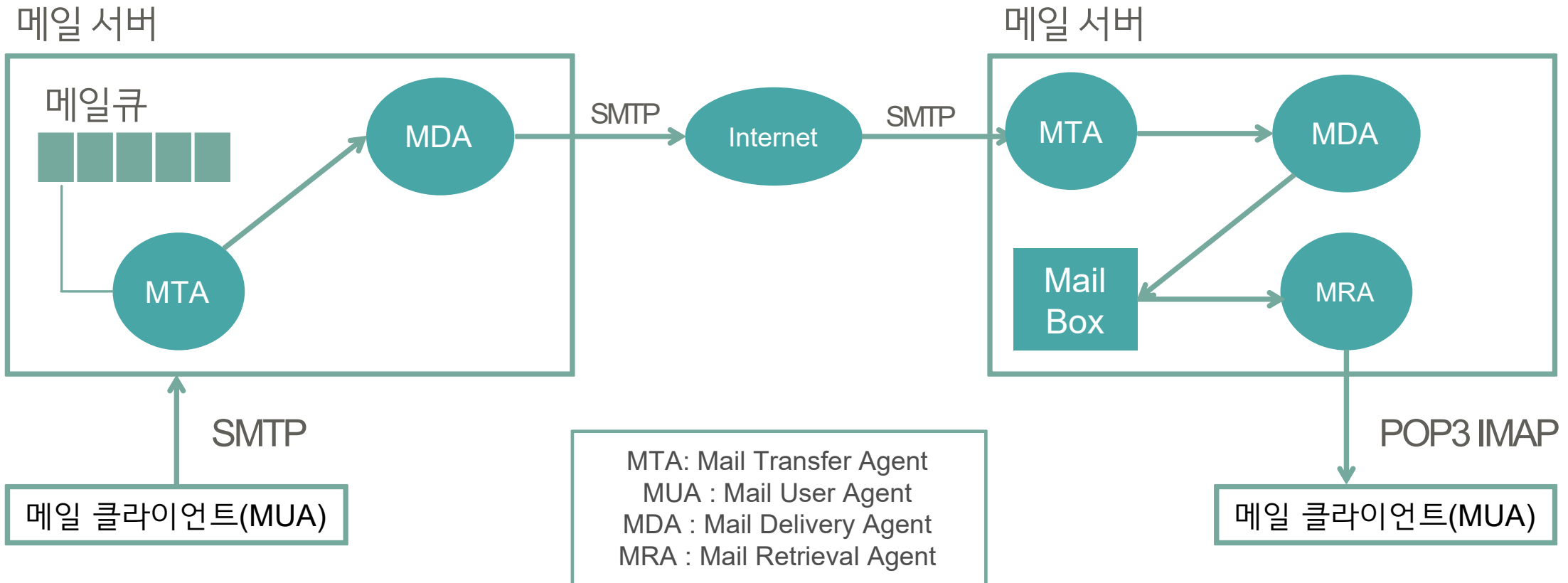
전자메일은 단순한 평문의 형태로 네트워크상의 여러 곳을 경유하여 수신자에게 전달되기 때문에 중간 노드에서 전자우편을 가로채거나 내용을 변조하여 다시 보낼 수도 있다

전자 우편의 보안상 취약점을 보완하기 위하여 기밀성, 무결성, 인증, 부인 방지 등의 보안 서비스를 지원하는 전자우편을 위한 보안 프로토콜이 개발되었다

전자메일을 안전하게 사용하기 위해 제공되는 보안 프로토콜은 PGP, PEM, S/MIME 등이 있다

# 01 전자 메일

## SMTP 메일 처리 방식



## 02 NTP

### NTP

인터넷을 통해 컴퓨터 시간을 최상위 동기 클럭원(Master Clock)에 동기시키는 프로토콜  
네트워크 상에 분산된 시간 서버들로부터 클라이언트(호스트, 라우터 등)의 동기화

### NTP 특징

시간 기준 및 정확도

- 시간 기준 : 협정세계시(UTC) 사용
- 시간 정확도 유지 : UTC에 비교하여, 수 밀리초 이하 정확도 유지 (1초 ~ 50 ms) 가능
  - . Straum 1 ~ 15 까지의 시간 서버들의 시간 오류 편차가 수 ms 이하

사용 포트 및 관련 IP 주소

- 사용 포트 : UDP 기반의 서비스
  - . 시간 서버 간에는 포트 123 (기본 포트)
  - . 일반 클라이언트 컴퓨터/장치는 포트 1023 이상을 사용
- 멀티캐스트 IP 주소 : 224.0.1.1

## 02 NTP

### NTP 특징

시간 교정 : 정확한 현재 시간 획득이 아닌 타임서버에 대한 시간 오류 교정

- 네트워크 지연에 대한 시간 정보 오류 교정 방법 : 4개의 타임스탬프 사용
  - . reference timestamp
  - . originate timestamp
  - . receive timestamp
  - . transmit timestamp

NTP 동작 모드

- 개별 PC, 장비들은 다수의 NTP 서버와 Multicast 모드로 동작하며 시간 교정
- NTP 서버들은 상위계층 서버들과는 Client/Server 모드로 동작,  
동일계층 서버들과는 Symmetric 모드로 동작하며 시간 교정

모듈 구성

- intersection 모듈, clustering 모듈, combining 모듈

동작방식

- 최초 클럭 동기는 5~10분 동안 모두 6번의 시간 교환을 통해 이루어짐.
- 그 후 매 10분 마다 메시지 교환을 통해 클럭 수정

## 03 Syslog

### Syslog 프로토콜

통신 프로토콜 : syslog 프로토콜

- 네트워크를 통해 다른 컴퓨터와 로그를 송수신하는 프로토콜 (RFC 3164)

syslog 프로토콜

- 어떤 이벤트 발생시,
  - 이를 자신의 로그 파일로 저장하는 동시에 syslog 서버로 UDP 유니캐스트로 전송함
- syslog 서버
  - 로그 메시지들을 수집 관리하는 별도의 서버
- 사용 프로토콜 및 포트번호
  - UDP 및 포트번호 514 사용
- 메시지 형식 구성
  - facility(로그 메시지 유형), severity(로그 메시지 중요도), 메시지(로그 내용)

## 04 SNMP

### SNMP Protocol

네트워크 장비 요소 간에 네트워크 관리 및 전송을 위한 프로토콜

- UDP / IP 상에서 동작하는 비교적 단순한 형태의 메시지 교환형 네트워크 관리 프로토콜

### SNMP 특징

매우 단순하고 구현 용이

- 매우 간단(구조의 간단함, 구현의 용이함 등)하여 쉽게 관리 적용이 가능

정보 지향적 동작 구조

- 명령 지향적 보다는 정보 지향적
  - 특정 정보 변수에 대한 단순한 요청/응답 메카니즘 (Get / Set)

Manager/Agent(관리자/대리인) 형태로 동작

여러 프로토콜과의 협동

- 크게, '정보 운반' 및 '관리 정보' 프로토콜을 분리함



## 04 SNMP

### SNMP 프레임워크 및 프로토콜



### 정보 운반 프로토콜

수송용 프로토콜 : UDP (User Datagram Protocol)

포트 번호 : 161번, 162번  
· UDP 161번 : Get, Set 등 통상의 메시지  
· UDP 162번 : 트랩 메시지

3가지 주요 동작 패턴 : Get, Set, Trap

관련 메시지 종류  
GetRequest, GetNextRequest, SetRequest, GetReponse, Trap 등

## 04 SNMP

### ‘관리 정보’ 프로토콜

- 정보 구조 : SMI 및 MIB 라는 다른 2개의 정보 구조를 설명하는 프로토콜과 함께 사용
  - . SMI (Structure of Management Information) : 관리정보구조
    - .. SNMP 관리 정보의 표현 구문 문법 등을 규정
    - .. ‘변수 작명’, ‘변수 유형’, ‘객체 및 값들을 부호화’ 등의 규칙
    - .. 장비마다 다르게 표현될 수 있는 MIB 객체의 표현 동질성을 유지하는 표준
  - . MIB (Management Information Base) : 관리 대상을 규격화한 정보 모음
    - .. 관리 특성을 묘사하는 변수 객체들의 모음
- 정보 식별 (망관리 대상 객체 식별 체계)
  - . OID : 트리 형태의 계층구조 (Tree Hierarchy)
    - .. 식별된 관리 정보와 관련된 값을 계층화된 데이터베이스 MIB에서 저장/유지/관리

## 04 SNMP

### SNMP 장비 구분

- Manager (NMS, Network Management System)
  - 관리하는 시스템 (호스트 등)
    - . 관리시스템 안에 탑재, 관리용 메시지를 에이전트에 요청 및 모니터링
      - .. Manager S/W, Management S/W(각종 관리용 응용 S/W)
      - .. 例) MRTG, HP OpenView, TWSNMP 등
- Agent (Managed Device)
  - 관리되는 장비들 (허브, 라우터, 스위치, 브리지, 호스트 등)
    - . 관리되는 장치 안에 탑재되는 서버 형태의 모듈
      - .. Agent S/W, MIB(Agent 노드에 수집되는 정보)
    - . 장비 동작에 필요한 변수, 상태 정보 등을 데이터베이스화하여 유지함

## 04 SNMP

### SNMP 장비 구분

동작 이해

- Manager는 Agent에게 관리정보 요청을 하고,
  - . Agent가 생산하는 관리정보(MIB) 데이터를 통하여 관리 역할을 수행
- Manager와 Agent의 상호 데이터 교환
  - . MIB 내 변수에서 읽기,쓰기(Get, Set) 명령과 가져오기(GetNext) 명령에 의함



## 04 SNMP

### SNMP 장비 구분

- 3가지 주요 동작 패턴 : Get, Set, Trap
  - SNMP 관련 메시지 형태
    - . SNMP는 관리자와 에이전트 간에 주고받는 메시지 패킷의 형식을 정의함
  - 기본 명령어 종류
- SNMP 메시지 문법 체계
  - OSI가 표준화한 ASN.1/BER (Abstract Syntax Notation One/Basic Encoding Rule)  
라는 문법체계를 따름

# END

---

고생하셨습니다

