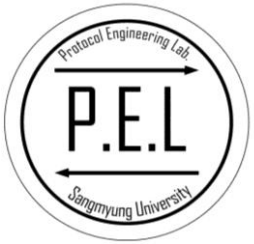


네트워크 보안 에센셜

6장 무선 네트워크 보안

Ji-Yeon Moon (jiyeon@pel.smuc.ac.kr)
Protocol **E**ngineering **L**ab., **Sangmyung** University

Content

- IEEE 802.11 무선 LAN
  - IEEE 802.11 개요
  - IEEE 802.11 프로토콜 구조
  - IEEE 802.11 네트워크 요소와 구조 모델
  - IEEE 802.11 서비스

- IEEE 802.11i 무선 LAN 보안
  - IEEE 802.11i 개요
  - IEEE 802.11i 서비스
  - IEEE 802.11i 동작 단계

IEEE 802.11 무선 LAN

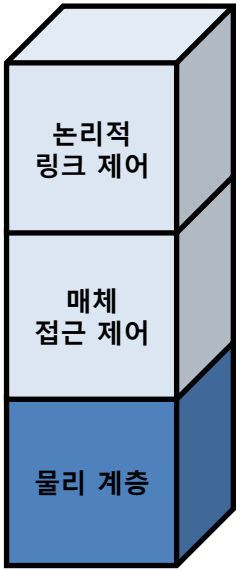
- IEEE 802.11 개요
  - IEEE 802
    - 근거리통신망(LAN)에 관한 표준안을 개발한 위원회
  - IEEE 802.11
    - 무선 LAN(WLAN: Wireless LAN)에 관한 프로토콜과 전송 규격 개발을 목표로 한 작업 그룹
    - 다양한 주파수와 데이터 전송속도를 갖춘 WLAN에 대한 요구가 증가함에 따라 확장된 표준안 발표

IEEE 802.11 무선 LAN

- IEEE 802.11 개요
  - Wi-Fi 연합
    - 산업계에서 수용한 IEEE 802.11b 표준은 동일한 기반의 제품이더라도 서로 다른 업체가 생산한 제품 간의 상호 호환 문제가 발생
    - 이런 문제 해결을 위해 1999년 산업체 연합인 WECA(Wireless Ethernet Compatibility Alliance) 설립
    - 나중에 Wi-Fi 연합(Wireless Fidelity Alliance)이라고 이름을 변경
    - 802.11b 규약을 준수하는 제품 간의 상호 동작을 인증해주는 시험 도구(Wi-Fi)를 만듦

IEEE 802.11 무선 LAN

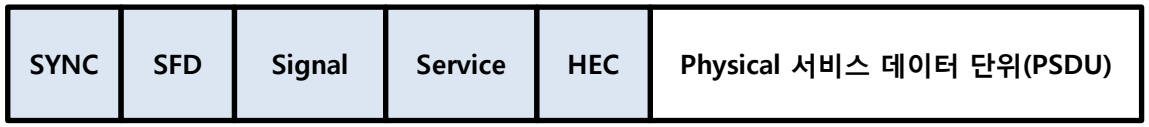
- IEEE 802.11 프로토콜 구조
  - 물리 계층(physical layer)
    - 신호의 인코딩/디코딩과 비트 송수신 기능을 담당
    - 주파수 범위와 안테나 특성 등 전송 매체에 대한 규격을 다룸
    - 상위 매체 접근 제어 계층의 데이터를 받아들이는데 이러한 데이터를 Physical 서비스 데이터 단위(PSDU: Physical Service Data Unit)라는 형태로 구성
    - 데이터 송신 시, 데이터는 Physical 프로토콜 데이터 단위(PPDU: Physical Protocol Data Unit)이라는 프레임으로 구성



IEEE 802.11 무선 LAN

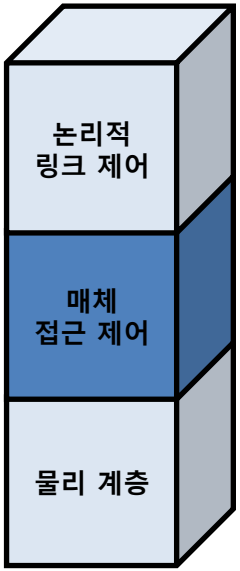
- IEEE 802.11 프로토콜 구조
  - 물리 계층(physical layer)

    PPDU(Physical Protocol Data Unit) 형식
    - SYNC(Synchronization): 동기화를 위한 비트 패턴
    - SFD(Start Frame Delimiter): 프레임의 시작을 알림
    - Signal: bit 단위로 데이터 속도를 나타냄
    - Service: bit 값에 따라 사용 용도가 다름
    - HEC(Header Error Control): 헤더에 대해서만 에러를 제어하는 필드 (ex CRC)



IEEE 802.11 무선 LAN

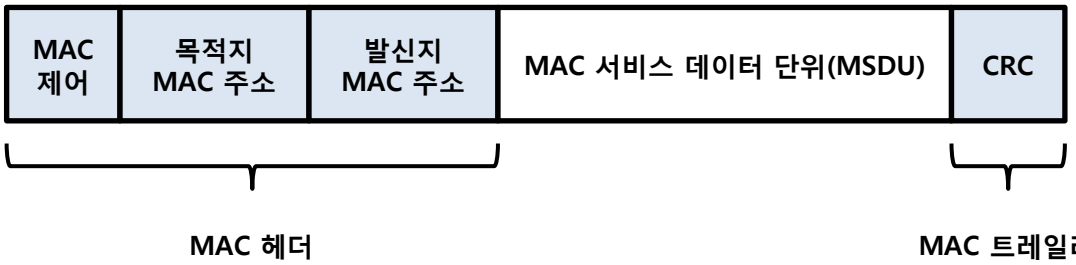
- IEEE 802.11 프로토콜 구조
  - 매체 접근 제어(MAC: Media Access Control) 계층
    - LAN 상의 네트워크 전송 능력을 질서 있고, 효율적으로 사용할 수 있도록 하는 접근 제어 방식을 제공
    - 상위 논리 링크 제어 계층의 데이터를 받아들이는데 이러한 데이터를 MAC 서비스 데이터 단위(MSDU: MAC Service Data Unit)라는 형태로 구성
    - 데이터 송신 시, 데이터는 MAC 프로토콜 데이터 단위(MPDU: MAC Protocol Data Unit)이라는 주소와 오류 감지 필드를 갖는 프레임으로 구성
    - 데이터 수신 시, 프레임을 분해하여 주소를 인식하고 오류를 감지



IEEE 802.11 무선 LAN

- IEEE 802.11 프로토콜 구조
  - 매체 접근 제어(MAC: Media Access Control) 계층

    MPDU(MAC Protocol Data Unit) 형식
    - **MAC 제어**: MAC 프로토콜 동작에 필요한 모든 프로토콜 제어 정보 (ex 우선순위 레벨)
    - **목적지 MAC 주소**: 해당 MPDU의 목적지 주소
    - **발신지 MAC 주소**: 해당 MPDU의 발신지 주소
    - **MAC 서비스 데이터 단위**: 상위 계층에서 제공된 데이터
    - **CRC**: 전체 MPDU에 대한 CRC를 계산

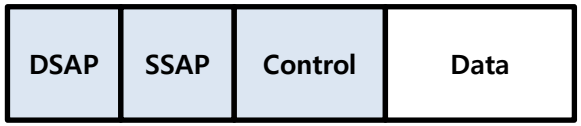


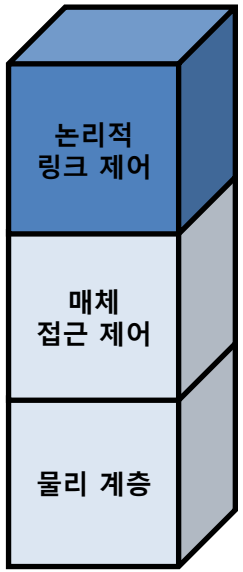
IEEE 802.11 무선 LAN

- IEEE 802.11 프로토콜 구조
  - 논리 링크 제어(LLC: Logical Link Control) 계층
    - CRC를 이용하여 어떤 프레임이 제대로 전송되었는지를 추적하고, 실패한 프레임을 재전송
    - 데이터 송신 시, 데이터는 MAC 서비스 데이터 단위(MSDU: MAC Service Data Unit)이라는 주소와 오류 감지 필드를 갖는 프레임으로 구성

MSDU(MAC Service Data Unit) 형식

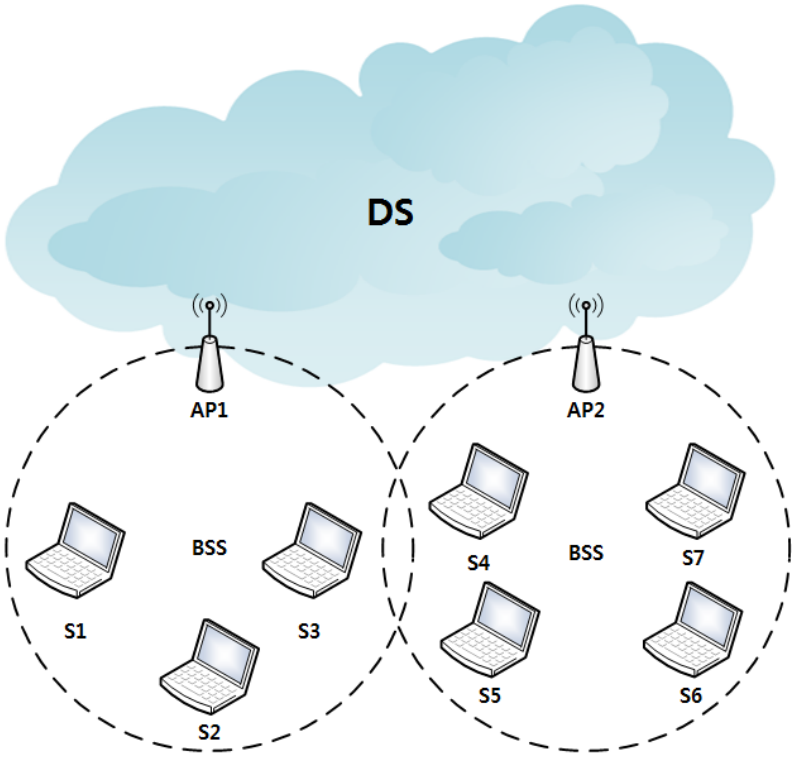
- DSAP(Destination Service Access Point): 목적지의 주소
- SSAP(Source Service Access Point): 발신지의 주소
- Control: 프레임 또는 ACK의 번호를 나타냄
- Data: 데이터 존재





IEEE 802.11 무선 LAN

- IEEE 802.11 네트워크 요소와 구조 모델



용어	설명
지국 (Station)	IEEE 802.11에 호환되는 MAC과 물리 계층을 가진 장치
기본 서비스 집합 (BSS: Basic Service Set)	분산 시스템에 접근 지점을 통해서 연결되는 지국의 집합
분산 시스템 (DS: Distribution System)	AP 사이에서 메시지를 전송하는 데 사용되는 네트워크
접근 지점 (AP: Access Point)	지국들에게 분산 시스템에 대한 접근을 제공
확장 서비스 집합 (ESS: Extended Service Set)	하나의 분산 시스템에 의해 연결된 두 개 이상의 기본 서비스 집합

IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - DS 내부 메시지 분배

    분배(Distribution) 서비스

    - 하나의 BSS에 속한 STA이 DS를 통해 다른 BSS에 속한 STA으로 MPDU를 전달할 때 사용
    - 통신을 수행하는 두 STA이 동일한 BSS 안에 있을 경우, BSS의 AP에서 수행

    통합(Integration) 서비스

    - IEEE 802.11 LAN에 속한 STA과 물리적으로 DS에 연결된 유선 LAN에 속한 장비 간 논리적 연결 및 통신을 제공

IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - **연관 관련 서비스**
    - DS가 하나의 STA으로 송수신을 하려면 해당 STA은 연관 설정이 필요
    - 따라서 DS가 작동하는데 필요한 ESS 내부에 존재하는 STA에 관한 정보를 제공

    표준 이동성과 관련된 3가지 전이(Transition)
    - **전이 없음:** STA이 물리적으로 이동하지 않거나, 이동하더라도 하나의 BSS 내부에서 통신이 가능한 범위 내에서만 이동
    - **BSS 전이:** 동일 ESS 내부에서 서로 다른 BSS 간의 STA 이동
    - **ESS 전이:** 하나의 ESS 내부의 한 BSS에 속한 STA이 다른 ESS에 속한 BSS의 영역으로 이동

IEEE 802.11 무선 LAN

- IEEE 802.11 서비스
  - 연관 관련 서비스
    - DS 내부에서 목적지 STA까지 메시지를 전달하려면 DS는 먼저 메시지를 전달해야 할 AP의 ID를 알아야 함
    - 따라서 각 STA은 현재 BSS 내의 AP와 연관을 유지해야 함

    관련 서비스
    - **연관(Association)**: 무선 LAN에서 STA이 메시지를 송/수신하려면 다른 STA의 ID와 주소를 알아야 하므로 STA과 AP 간의 초기 연관을 설립
    - **재연관(Reassociation)**: 하나의 AP에서 확립된 연관을 다른 AP로 전달할 수 있는 기능을 제공하여, 이동 STA이 하나의 BSS에서 다른 BSS로 이동 가능
    - **연관제거(Disassociation)**: STA 혹은 AP에서 보내는 통지로 기존에 존재하는 연관 종료

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 개요
  - 유선 LAN에는 존재하지만 무선 LAN에는 존재하지 않는 특징
    1. 유선 LAN은 물리적으로 장비와 연결되어 있어야 하므로 일부 인증 기능을 포함
    2. 유선 LAN은 물리적으로 연결된 장비만 수신할 수 있기 때문에 프라이버시 보장

  - Wi-Fi WPA(Wi-Fi Protected Access)
    - Wi-Fi 연합에서 개발한 IEEE 802.11 보안 표준 인증 과정
    - 가장 최근 버전인 WPA2는 IEEE 802.11i WLAN 보안 표준의 모든 특성을 가짐

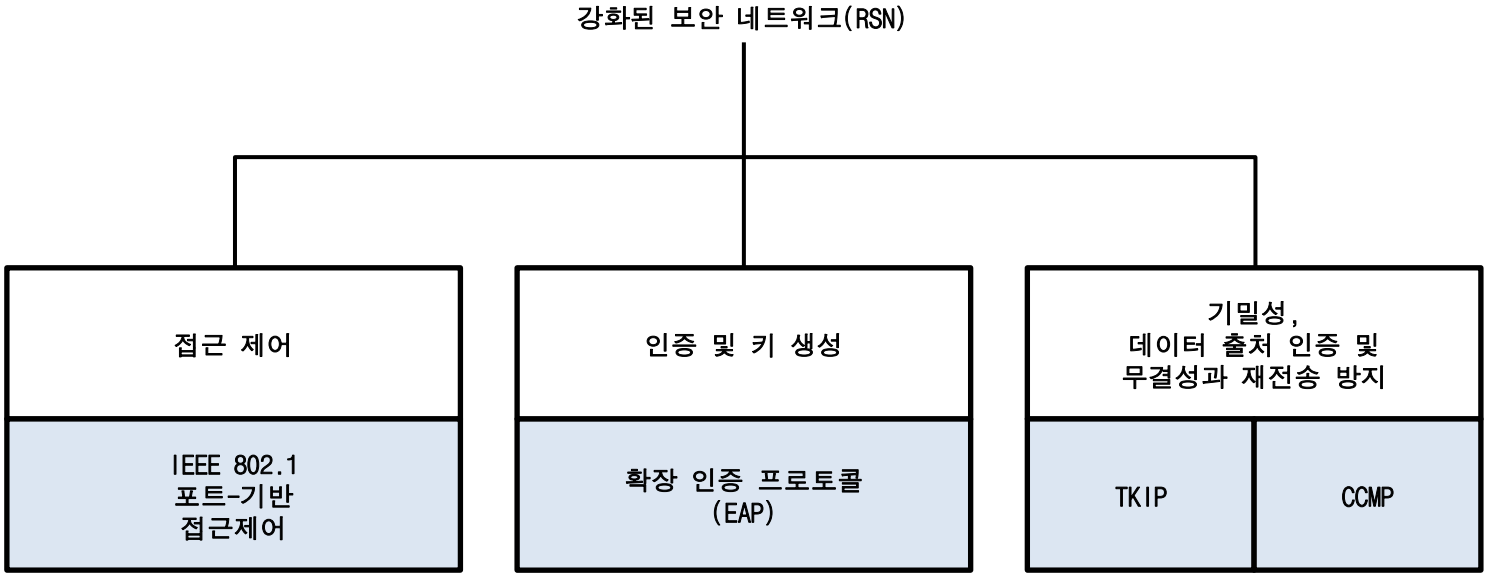
  - IEEE 802.11i
    - 표준 버전을 RSN(Robust Security Network)라고 함
    - Wi-Fi 연합에서 WPA2 프로그램으로 802.11i 규격을 준수하는 업체를 인증

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스
  - 인증
    - 프로토콜을 이용하여 사용자와 AS(Authentication Server) 간에 상호 인증하고, 무선 링크상에서 클라이언트와 AP 간에 사용할 임시키 생성
  - 접근 제어
    - 인증 기능 사용, 적절한 메시지 라우팅, 키 교환을 통해서만 이루어지도록 하며 다양한 인증 프로토콜을 이용하여 구현

IEEE 802.11i 무선 LAN 보안

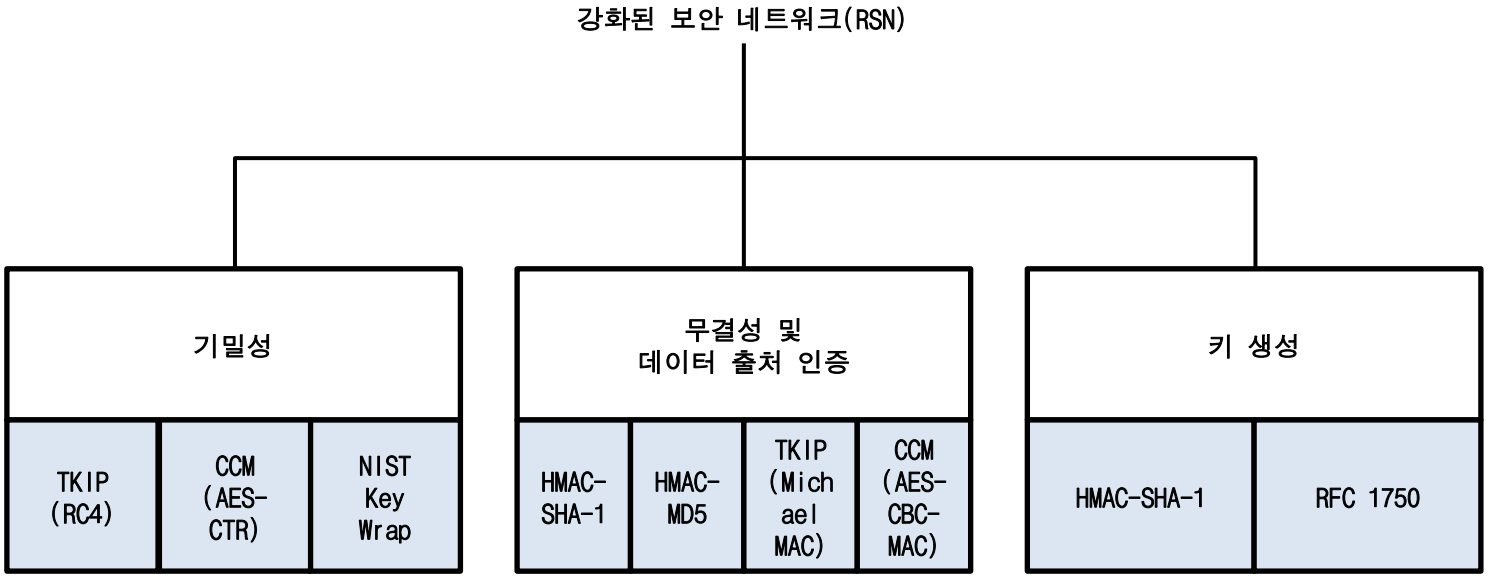
- IEEE 802.11i 서비스
  - 서비스와 프로토콜



✓ TKIP(Temporal Key Integrity Protocol) = 임시 키 무결성 프로토콜
✓ CCMP(Counter Mode-CBC MAC Protocol) = 카운터 모드-CBC MAC 프로토콜

IEEE 802.11i 무선 LAN 보안

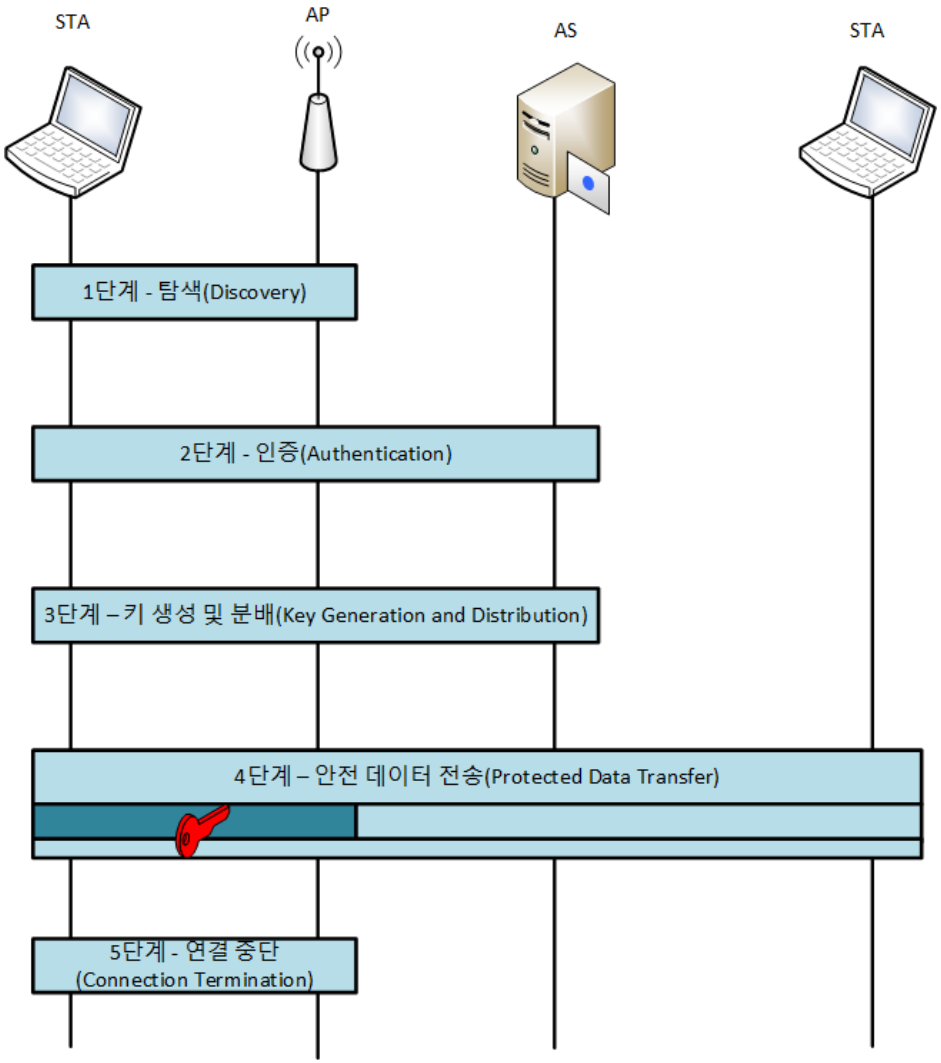
- IEEE 802.11i 서비스
  - 암호 알고리즘



✓ CBC-MAC = 암호 블록 블록 체인 메시지 인증 코드
✓ CCM = 암호 블록 체인 메시지 인증코드를 갖는 카운터 모드

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계



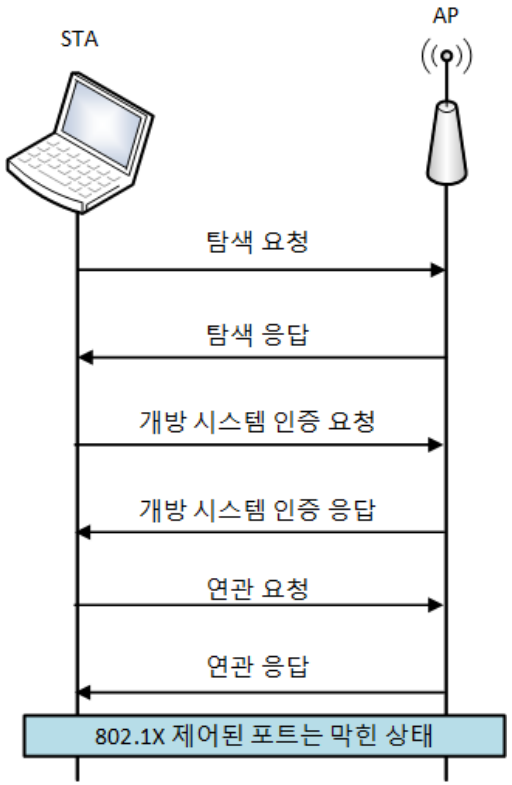
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

1단계 - 탐색

- STA와 AP가 연관을 통해 암호 도구와 인증 메커니즘을 선택

- **탐색:** Beacon, Probe Request/Response 프레임을 이용하여 STA는 AP와 대응되는 보안 기능 탐색
- **개방 시스템 인증:** STA와 AP는 ID 교환
- **연관:** STA는 Association Request 프레임을 이용하여 앞으로 AP와 사용할 보안 기능에 대한 합의

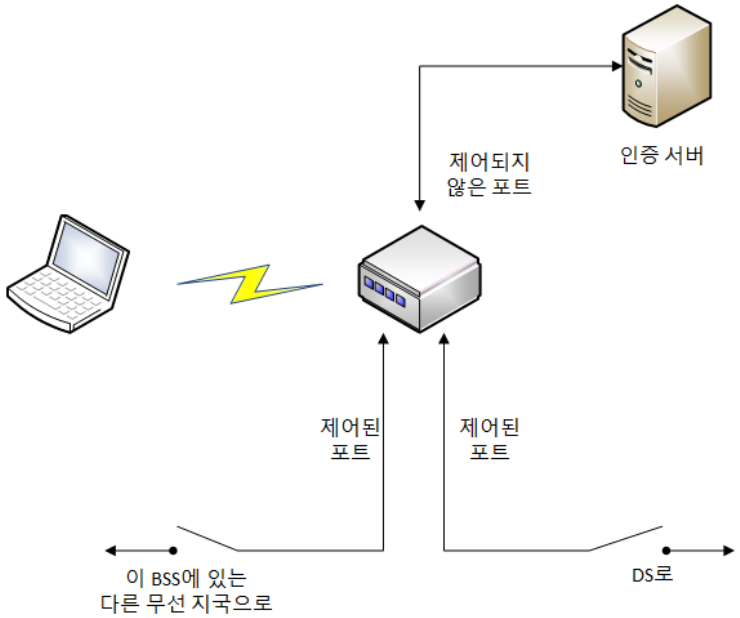


IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

2단계 - 인증

- 접근 제어
  - IEEE 802.11i에 접근 제어 기능을 제공하기 위해 포트 기반 네트워크 제어 방식인 IEEE 802.1X 표준을 사용
  - 구체적인 인증 프로토콜은 IEEE 802.1X 표준에 정의된 확장 인증 프로토콜(EAP: Extensible Authentication protocol)



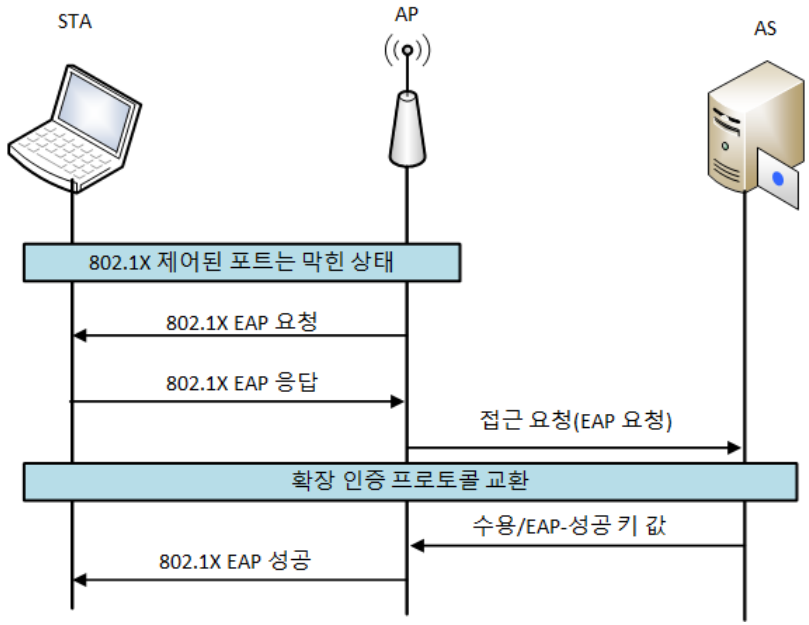
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

2단계 - 인증

- STA와 AS는 상호 인증하며 인증된 STA 만이 네트워크를 사용

- **AS 연결**: STA는 자신의 AP를 통해 AS로 접근을 요청
- **EAP 교환**: STA와 AS는 다양한 교환 방식으로 상호 인증
- **안전한 키 전달**: AS는 마스터 세션키(MSK: Master Session Key) 생성해 AP를 통해 STA로 전달

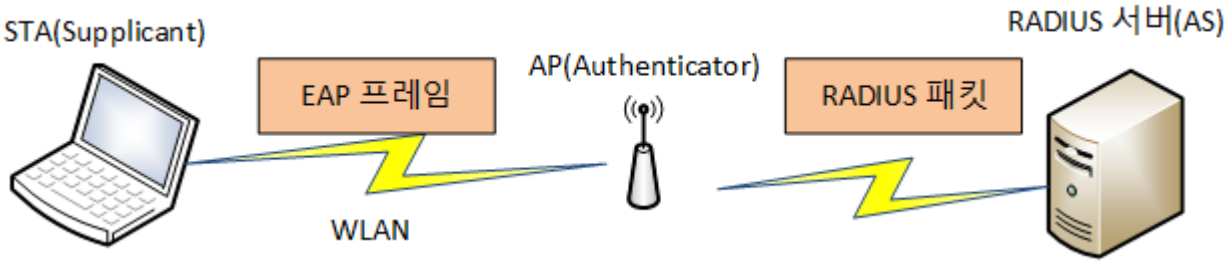


IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

  2단계 - 인증

  - EAP 교환
    - EAP는 특정한 인증 프로토콜은 아니지만 어떠한 인증 프로토콜과도 결합이 가능
    - STA와 AP 간의 메시지 전달은 LAN 상의 EAP(EAPOL: EAP over LAN) 프로토콜 사용
    - AP와 AS 간의 메시지 전달은 원격 인증 전화 접속 사용자 서비스(RADIUS: Remote Authentication Dial In User Service) 프로토콜 사용



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

2단계 - 인증

- EAP 교환

DIAMETER

- 기존의 RADIUS를 발전시킨 인증 프로토콜

	RADIUS	DIAMETER
프로토콜 구조	서버/클라이언트 (단방향)	Peer-to-Peer (양방향)
전송 계층	Connectionless (UDP)	Connect-oriented (TCP)
종단간 보안	제공 안함	End-to-End 보안
보안 기능	사전 공유키	End-to-End(TLS) 전송 계층(IPSec/TLS)

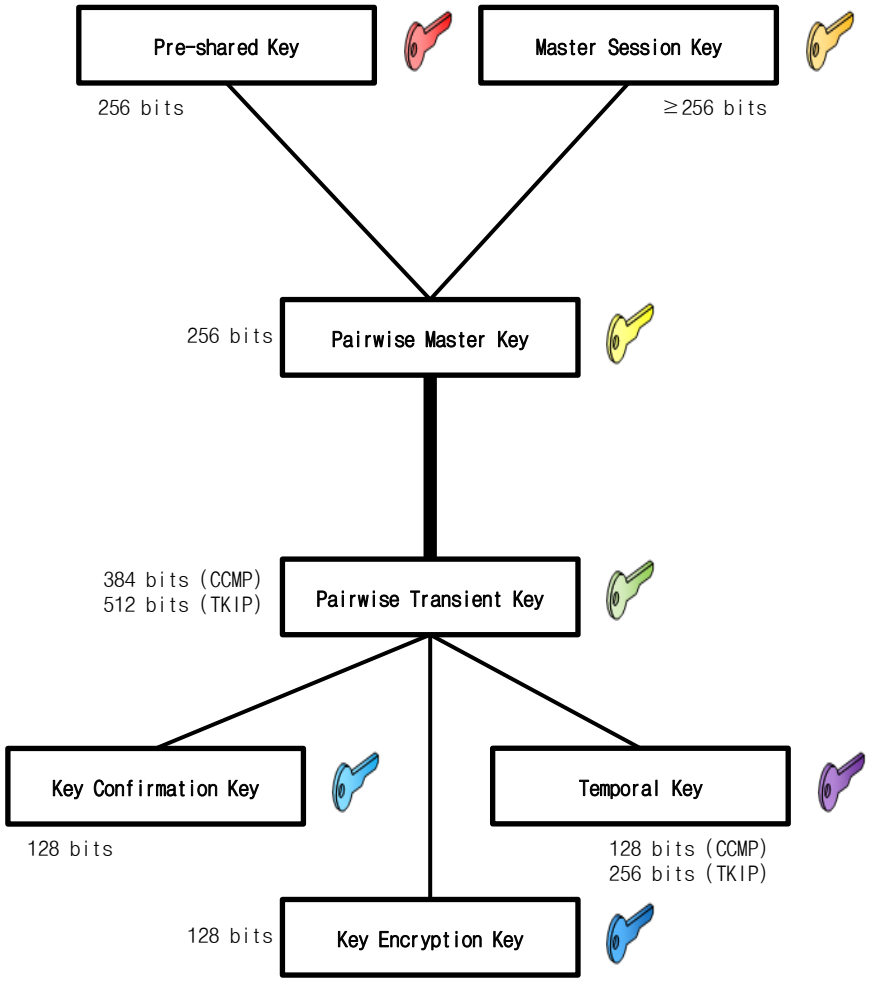
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

3단계 - 키 생성 및 분배

1. 하나의 STA와 하나의 AP 간에 사용되는 대칭키

- PSK(Pre-shared Key)
  - AP와 STA가 사전에 공유하는 비밀키
- MSK(Master Session Key)
  - STA와 AS 간의 상호 인증에서 생성된 세션 키로, AS가 생성해 AP와 STA가 상호 공유
- PMK(Pairwise Master Key)
  - PSK를 사용한다면, PSK를 PMK로 생성
  - MSK를 사용한다면, MSK의 일부를 잘라내어 PMK로 생성



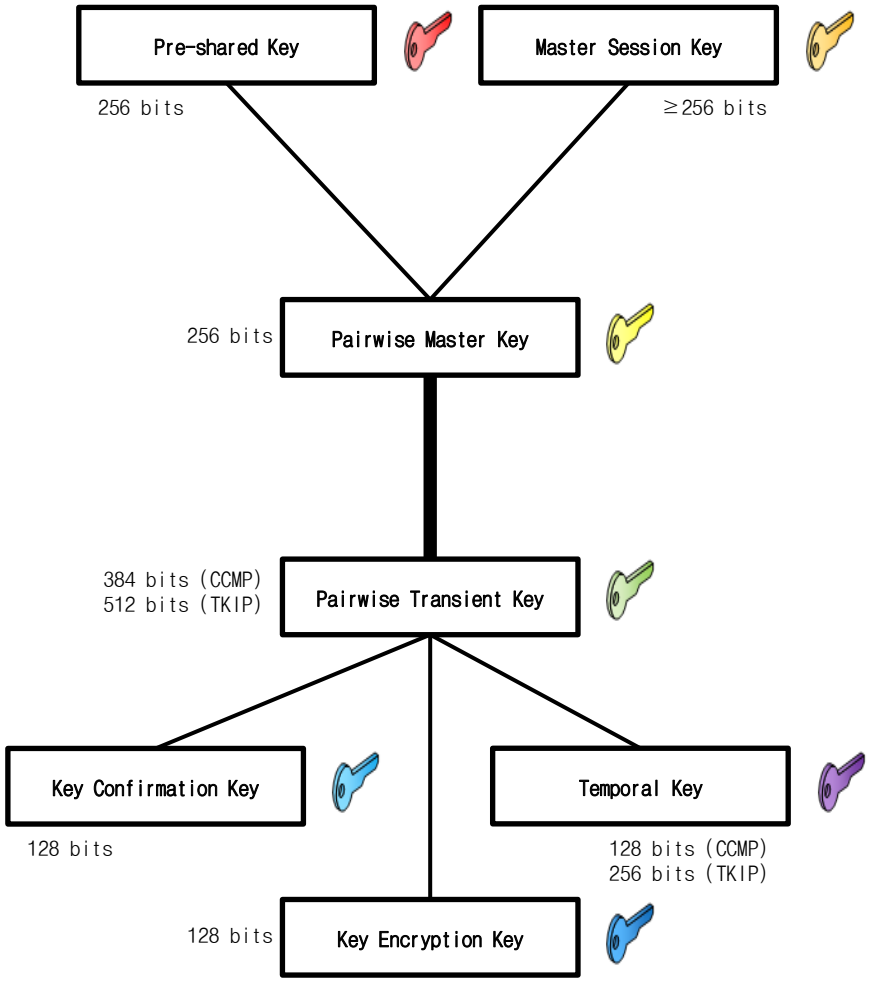
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

3단계 - 키 생성 및 분배

1. 하나의 STA와 하나의 AP 간에 사용되는 대칭키

- PTK(Pairwise Transient Key)
  - PMK, STA와 AP의 MAC 주소, Nonce를 HMAC-SHA-1 함수의 입력으로 사용하여 생성한 해시 값
- KCK(Key Confirmation Key)
  - 메시지 인증을 위한 MIC 생성에 사용되는 키
- KEK(Key Encryption Key)
  - GTK 분배를 위한 키
- TK(Temporal Key)
  - 안전한 데이터 전송을 위한 임시키



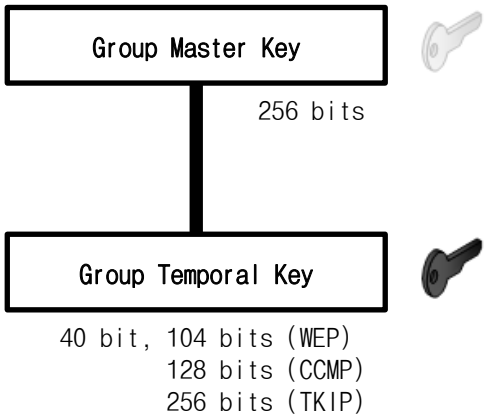
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

3단계 - 키 생성 및 분배

2. 멀티캐스팅 통신에 사용되는 그룹키

- GMK(Group Master Key)
  - AS가 생성하며 주기적 또는 침해시에 교체
- GTK(Group Temporal Key)
  - GMK와 정책에 따라 다른 입력을 사용하여 AP가 생성해 연관된 STA로 전달



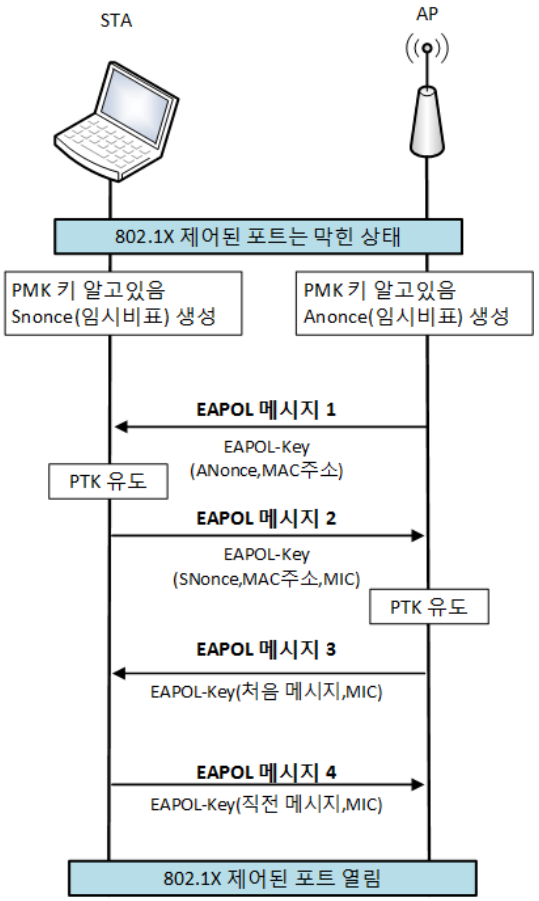
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

3단계 - 키 생성 및 분배

1. 대칭키 분배를 위한 4-way Handshake

- AP → STA
  - AP는 Anonce 생성
  - AP의 MAC 주소, Anonce가 포함된 메시지 전송
- STA → AP
  - STA는 Snonce 생성
  - STA는 S/Anonce, STA/AP MAC 주소, PMK를 이용하여 PTK 생성
  - STA의 MAC 주소, Snonce, 메시지 무결성 코드(MIC: Message Integrity Code)를 포함한 메시지 전송
- AP → STA
  - AP는 S/Anonce, STA/AP MAC 주소, PMK를 이용하여 PTK 생성
  - 처음 메시지, MIC를 포함한 메시지 전송
- STA → AP
  - 직전 메시지에 대한 단순 수신 응답으로 MIC를 포함한 메시지 전송

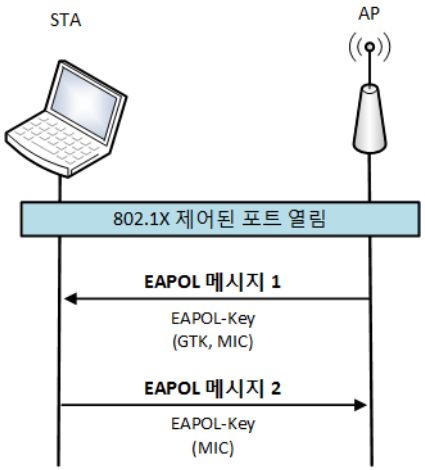


IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

3단계 - 키 생성 및 분배

2. 그룹키 분배를 위한 메시지 교환



- AP → STA
  - AP는 GTK 생성
  - GTK에 암호화키 KEK를 사용하여 RC4/AES로 암호화
  - GTK, MIC를 포함한 메시지 전송
- STA → AP
  - 수신 응답으로 MIC를 포함한 메시지 전송

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 동작 단계

4단계 - 안전 데이터 전송

- 데이터 전달을 위한 두 가지 시스템을 정의

- **임시 키 무결성 프로토콜(TKIP: Temporal Key Integrity Protocol)**
  - **메시지 무결성(Message Integrity):** 데이터 필드 뒤에 이어서 MIC를 붙여 무결성을 보장하며, MIC는 목적지 MAC 주소와 데이터 필드 그리고 키 값을 입력으로 하여 64비트 결과 값으로 생성
  - **데이터 기밀성:** 데이터와 MIC를 RC4로 암호화하여 데이터 기밀성을 제공

- **카운터 모드-CBC MAC 프로토콜(CCMP: Counter Mode-CBC MAC Protocol)**
  - **메시지 무결성:** 암호 블록 체인 인증 코드를 사용
  - **데이터 기밀성:** AES의 CTR 블록 암호 모드 사용

네트워크 보안 에센셜

끝!