Network Security Essential

- 6장 무선 LAN 보안 -

명 세인(sein@pel.smuc.ac.kr)

상명대학교 프로토콜공학연구실

목 차

- IEEE 802.11 무선 LAN 개요
- IEEE 802.11i 무선 LAN 보안

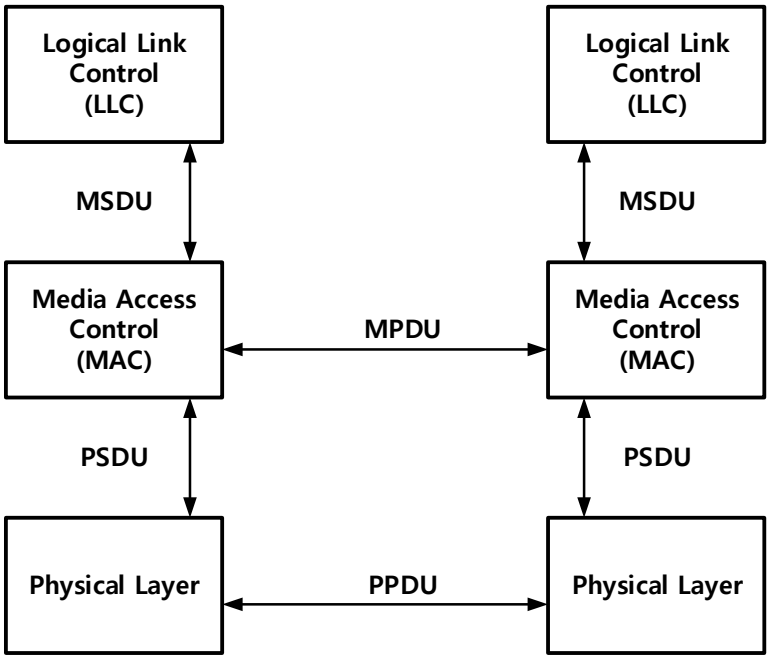
IEEE 802.11 무선 LAN 개요

- IEEE 802와 WI-FI
  - IEEE 802
    - 근거리 통신망과 도시권 통신망을 관할하는 전기 전자 기술자 협회의 표준 규칙들의 계열을 의미함
    - IEEE: Institute of Electrical and Electronics Engineers
  - IEEE 802.11
    - WLAN(Wireless Local Area Network)에 관한 프로토콜과 전송 규격 개발을 목표로 한 작업 그룹을 의미
    - 산업계에서 가장 먼저 수용한 표준은 IEEE 802.11b
      - 표준에 기반하더라도 서로 다른 업체가 만든 제품의 상호 호환을 위한 산업체 연합을 결성 시험 도구로 인증된 제품을 Wi-Fi(Wireless Fidelity Alliance)라고 칭함
      - 마지막 알파벳 글자로 표준의 종류를 구별함

IEEE 802.11 무선 LAN 개요

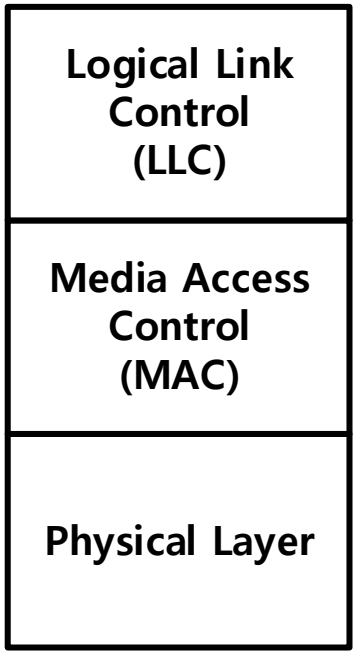
- IEEE 802 프로토콜 구조
  - 개요
    - 논리적 연결 제어 (LLC)
    - 매체 접근 제어 (MAC)
    - 물리 계층

    - MAC 서비스 데이터 유닛 (MSDU)
    - MAC 프로토콜 데이터 유닛 (MPDU)
    - 물리 계층 서비스 데이터 유닛(PSDU)
    - 물리 계층 프로토콜 데이터 유닛(PPDU)



IEEE 802.11 무선 LAN 개요

- IEEE 802 프로토콜 구조
  - 물리 계층 (Physical Layer)
    - 신호의 인/코딩과 비트의 송/수신 기능
    - 전송 매체에 대한 규격(주파수 범위, 안테나 특성 등)
    - 네트워크 모델과 같이 인/디캡슐화 기능
    - 상위 계층에서 받은 데이터는 PSDU, 전송되는 데이터를 PPDU라 함

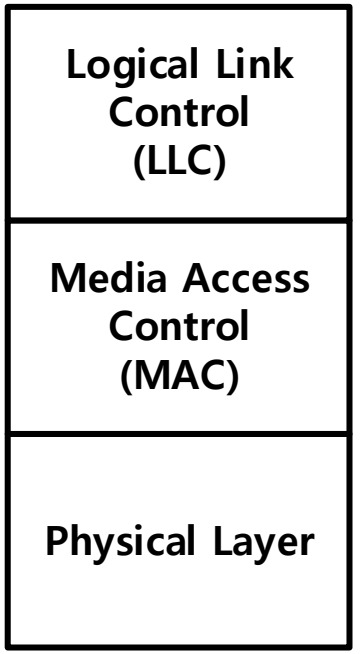


IEEE 802.11 무선 LAN 개요

- IEEE 802 프로토콜 구조
  - 물리 계층 프로토콜 데이터 유닛 포맷 (PPDU)

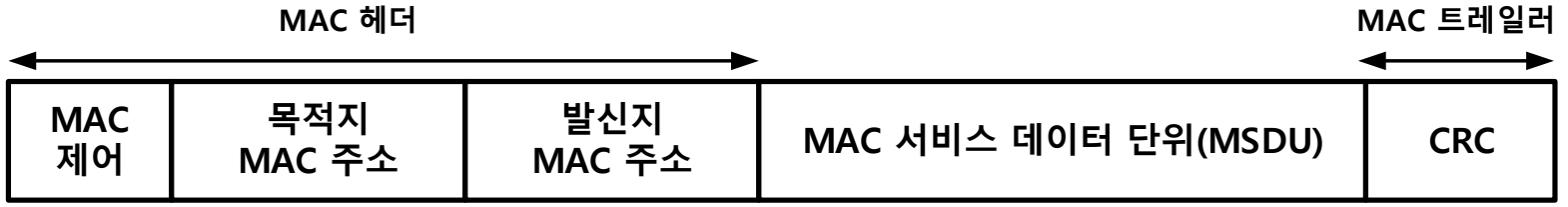
SYNC	SFD	PLW	PSF	HEC	MAC 프로토콜 데이터 유닛(MSDU)

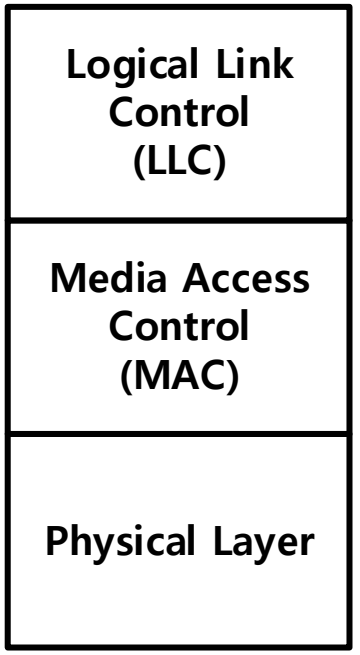
필드	기능
SYNC	동기화를 위한 비트패턴
SFD	프레임 시작
PLW	페이로드 전체 길이
PSF	페이로드 전송 속도
HEC	헤더 오류 제어



IEEE 802.11 무선 LAN 개요

- IEEE 802 프로토콜 구조
  - 매체 접근 제어 (MAC)
    - LAN 상의 네트워크 매체들을 질서 있고 효율적으로 사용할 수 있도록 하기 위한 접근 제어 기능 등을 수행
    - 상위 계층의 MSDU를 받아 MPDU를 생성하여 전송
      - MAC주소와 오류 감지 필드를 갖는 프레임으로 구성
  - MAC 프로토콜 데이터 유닛의 포맷 (MPDU)
    - MAC제어: MAC 프로토콜 동작에 필요한 모든 프로토콜 제어정보를 담는 필드
    - CRC: 순환 중복 검사 값을 통한 오류 감지



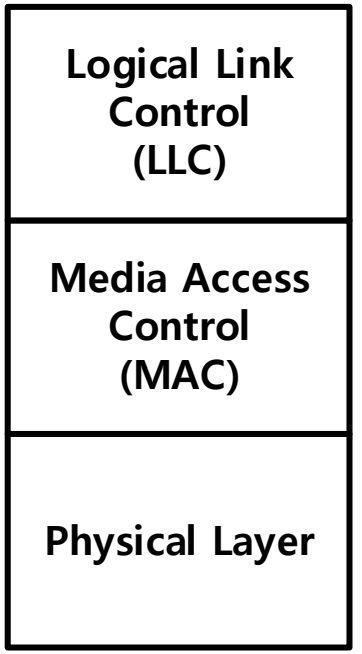


IEEE 802.11 무선 LAN 개요

- IEEE 802 프로토콜 구조
  - 논리적 연결 제어 (LLC)
    - CRC를 통해 오류 발견 시 오류 복구 기능
      - 프레임 추적과 재전송 기능을 가짐
    - MSDU를 생성하여 MAC 계층에 전달
  - MAC 서비스 데이터 유닛의 포맷 (MSDU)

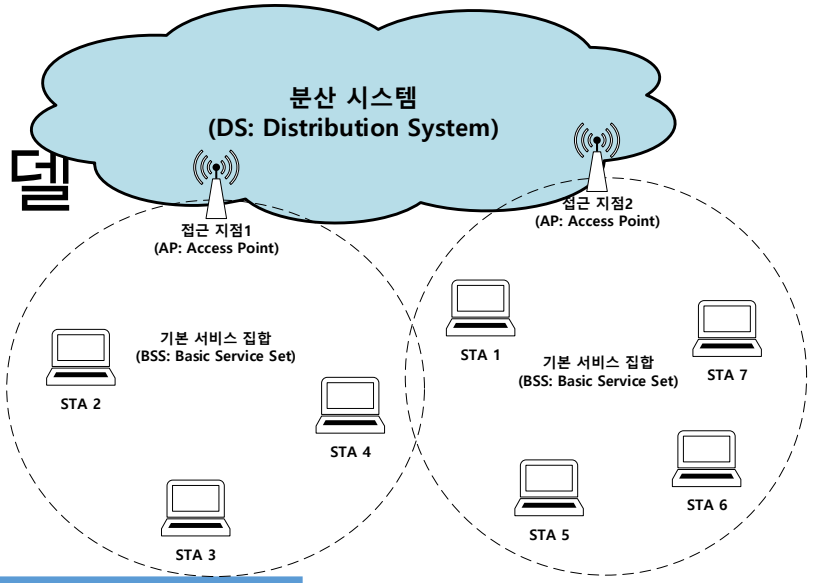
DSAP	SSAP	Control	Data

필드	기능
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 개요

- IEEE 802.11 구성 요소와 모델
  - IEEE 802.11 에 사용되는 용어와 모델



용어	의미
접근 지점 (AP)	지국 기능을 가지고 있으며 연관된 지국 무선 매체를 경유해서 분배 시스템에 대한 접근을 제공하는 개체
기본 서비스 집합 (BSS)	단일 조정 기능에 의해 제어되는 지국들의 집합
조정 함수 (Coordination Function)	BSS내에서 동작하는 지국이 PDU를 전송하거나 받아들이는 것을 언제 허가할 것인지를 결정하는 논리함수
확장 서비스 집합 (ESS)	BSS중 하나와 연관된 지국에 있는 LLC 계층에서 하나의 BSS로 보이는 집중화된 LAN 여러 개의 상호 연결된 BSS 집합
MAC 프로토콜 데이터 단위 (MPDU: MAC Protocol Data Unit)	물리 계층 서비스를 이용하여 통신하는 두 개의 대등한 MAC 개체 간의 데이터 교환 단위
MAC 서비스 데이터 단위 (MSDU: MAC Service Data Unit)	MAC 사용자간에 하나의 단위로 전달되는 정보
지국 (STA: Station)	IEEE 802.1에 호환되는 MAC과 물리계층을 지원하는 장비

IEEE 802.11 무선 LAN 개요

- IEEE 802.11 서비스
  - 유선 LAN과 동일한 수준의 서비스를 무선 LAN에도 제공할 수 있도록 하는 서비스가 IEEE 802.11에 정의됨

서비스	제공자	기반 기능
인증	지국	LAN 접근과 보안
인증 제거	지국	LAN 접근과 보안
프라이버시	지국	LAN 접근과 보안
MSDU 전달	지국	MSDU 전달
연관	분배 시스템	MSDU 전달
연관 제거	분배 시스템	MSDU 전달
분배	분배 시스템	MSDU 전달
통합	분배 시스템	MSDU 전달
재 연관	분배 시스템	MSDU 전달

IEEE 802.11 무선 LAN 개요

- IEEE 802.11 서비스
  - DS 내부 메시지 분배
    - 분배(Distribution) 서비스
      - MSDU를 반드시 DS를 통해 하나의 BSS에 속한 지국에서 다른 BSS 에 속한 지국으로 전달할 때 사용하는 서비스
    - 통합(Integration) 서비스
      - IEEE 802.11 LAN에 속한 지국과 통합된(Integrated) IEEE 802.x LAN 에 속한 장비간의 통신 서비스
        - Integrated: 물리적으로 DS에 연결된 유선 LAN을 지칭

IEEE 802.11 무선 LAN 개요

- IEEE 802.11 서비스
  - 연관 관련 서비스
    - DS 내부에서 목적지 STA 까지 메시지를 전달하기 위해서는 전달 해야 할 AP의 ID를 알아야 함 (3개의 연관서비스)
    - 각 연관을 통해 각 지국의 정보(ID, 위치)를 관리
    - 무선 인터넷에서는 이동성 장비에 대해 전이(Transition) 개념을 정의
      - 전이 없음: 해당하는 BSS외부로의 이동이 없음
      - BSS 전이: 동일 ESS내부에서 서로 다른 BSS간의 지국 이동을 의미, 이동 후 데이터 전송을 위해 주소 지정 기능이 이동한 지국의 주소를 알 수 있어야 함
      - ESS 전이: ESS에 속한 BSS에서 관련이 없는 ESS로 이동하는 것을 의미, 이동할 가능성이 있는 경우만 지원하고, 서비스 보장 안됨

IEEE 802.11 무선 LAN 개요

- IEEE 802.11 서비스
  - 연관 관련 서비스
    - 3개의 연관 서비스
      - 연관(Association): 지국과 AP간의 초기 연관 수립(지국의 ID와 주소), 연관된 주소를 가진 프레임을 라우팅 가능
      - 재연관(Reassociation): 하나의 AP에서 확립된 연관을 다른 AP로 전달할 수 있는 기능, 이동 지국에 대한 전이를 처리
      - 연관 제거(Disassociation): 기존에 존재하는 연관이 종료됨을 통지, 지국이 ESS전이나 종료되기 전에 통지해야 함(MAC 관리 기능으로 통지 없이 사라지는 지국을 처리 가능)

목 차

- IEEE 802.11 무선 LAN 개요
- IEEE 802.11i 무선 LAN 보안

IEEE 802.11i 무선 LAN 보안

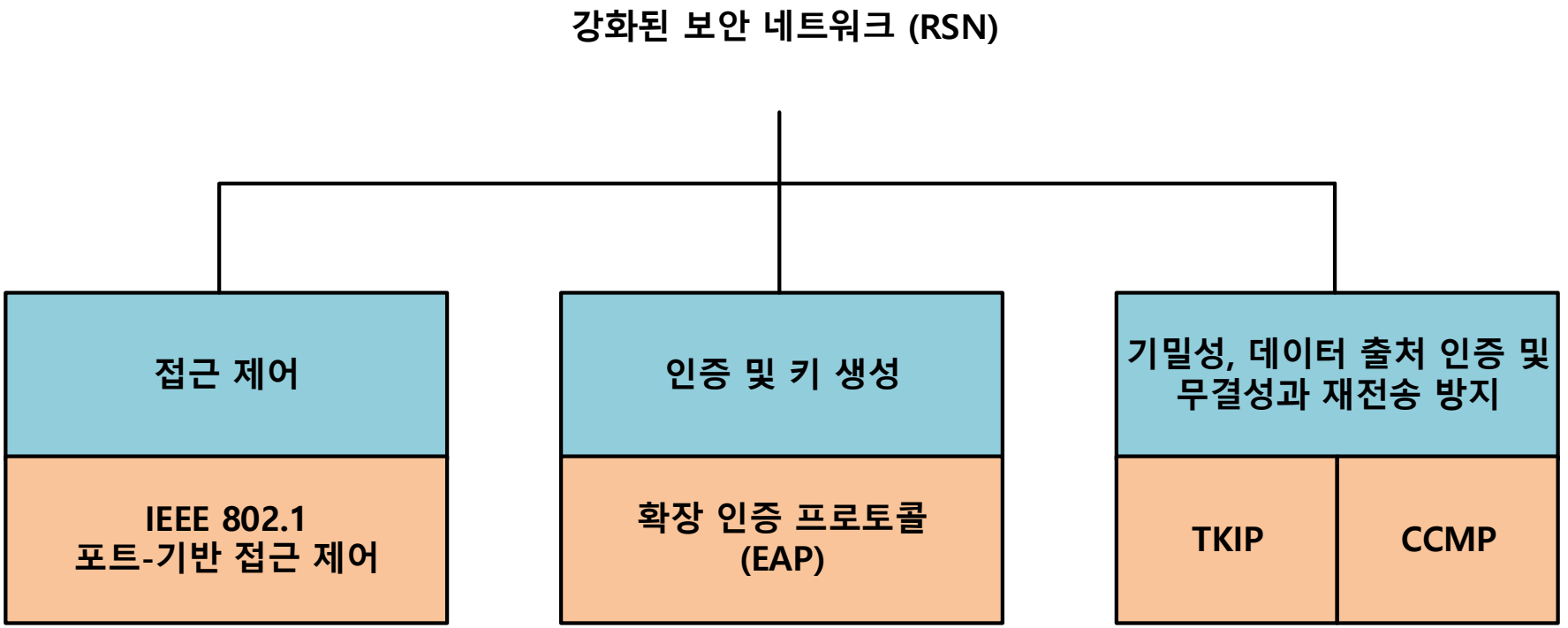
- 개요
  - 유선 LAN과 무선 LAN의 차이
    - 유선 LAN의 물리적 연결은 일부 인증 포함한다고 생각, 무선 LAN은 범위 안의 모든 장비가 인증 시도 가능
    - 유선 LAN은 통신시 물리적 연결이 필수, 프라이버시가 보장된다고 볼 수 있지만, 무선 LAN은 기본적으로 브로드캐스트 개념임
  - WPA(Wi-Fi Protected Access)
    - Wi-Fi연합에서 Wi-Fi 표준의 일부로서 공표, 802.11이 가졌던 대부분의 보안 문제를 802.11i 표준에 기반하여 해결
      - WPA2는 IEEE 802.11i WLAN 보안 표준의 모든 특성을 가짐
    - 최신 802.11i 표준 버전을 RSN(Robust Security Network)이라고 함

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스 (RSN 보안 규격)
  - 인증
    - 프로토콜을 통한 사용자와 AS간 상호인증 후, 무선 링크 상에서 클라이언트와 AP간에 사용할 임시 키 생성을 정의
  - 접근 제어
    - 인증 기능의 사용, 적절한 메시지 라우팅, 키 교환을 통해서 이루어지도록 함, 인증 프로토콜들로 기능 구현
  - 메시지 무결성을 통한 프라이버시
    - MAC 계층의 데이터(LLC PDU등)와 데이터 인증을 위한 MIC를 함께 암호화
      - MIC: Message Integrity Code

IEEE 802.11i 무선 LAN 보안

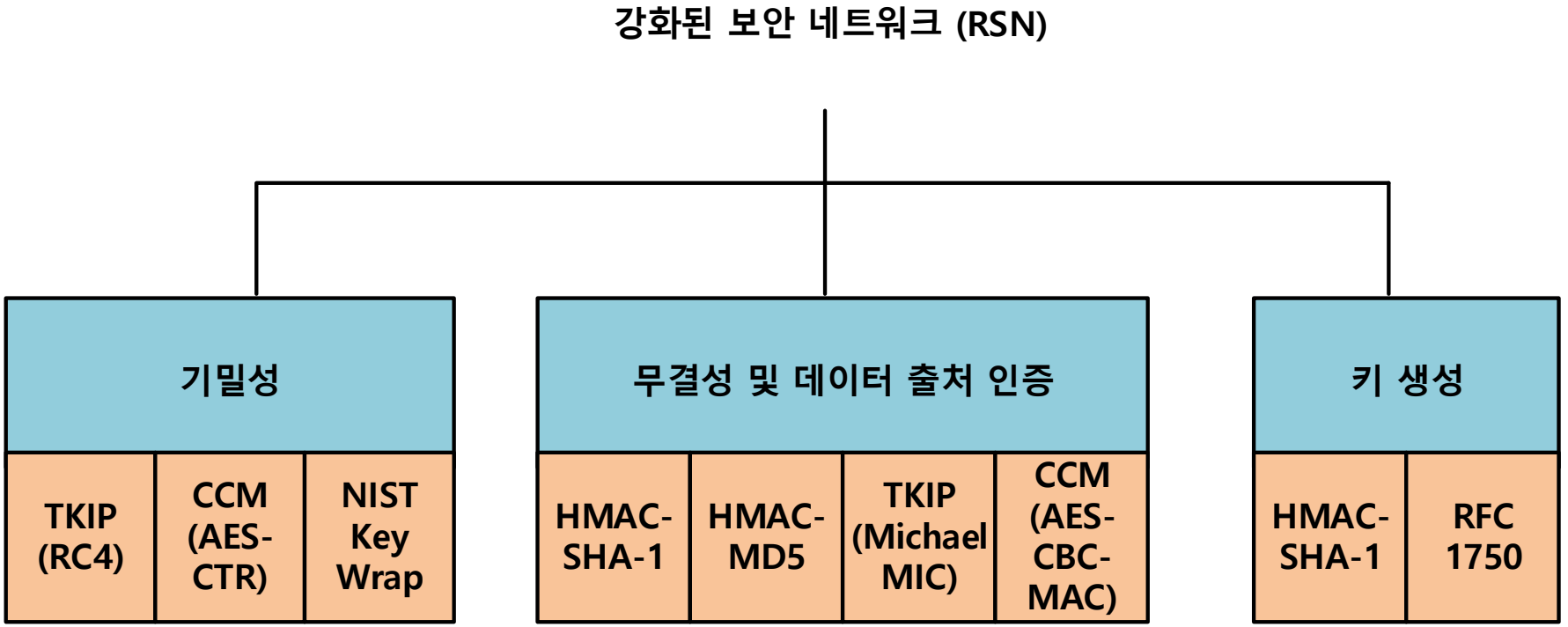
- IEEE 802.11i 서비스 (RSN 보안 규격)
  - RSN의 서비스와 프로토콜



TKIP: 임시 키 무결성 프로토콜
CCMP: 암호블록 체인 MAC 프로토콜을 갖는 카운터 모드

IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i 서비스 (RSN 보안 규격)
  - RSN의 서비스와 알고리즘

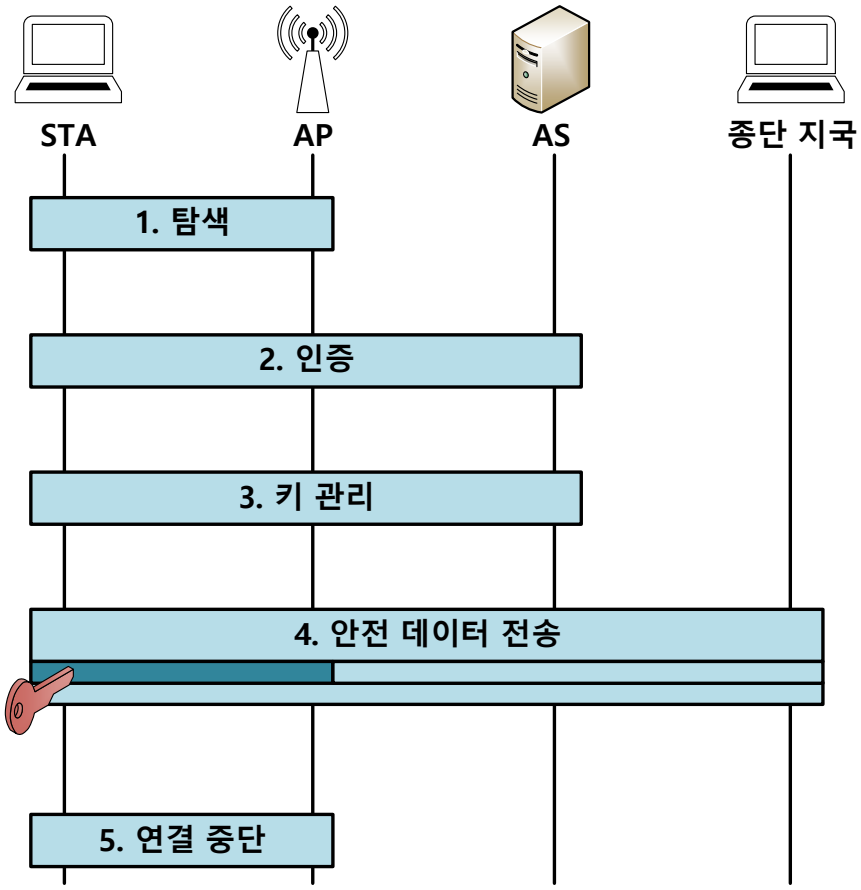


CBC-MAC: 암호블록 블록체인 메시지 인증 코드
CCM: 암호블록 체인 메시지 인증 코드를 갖는 카운터 모드

IEEE 802.11i 무선 LAN 보안

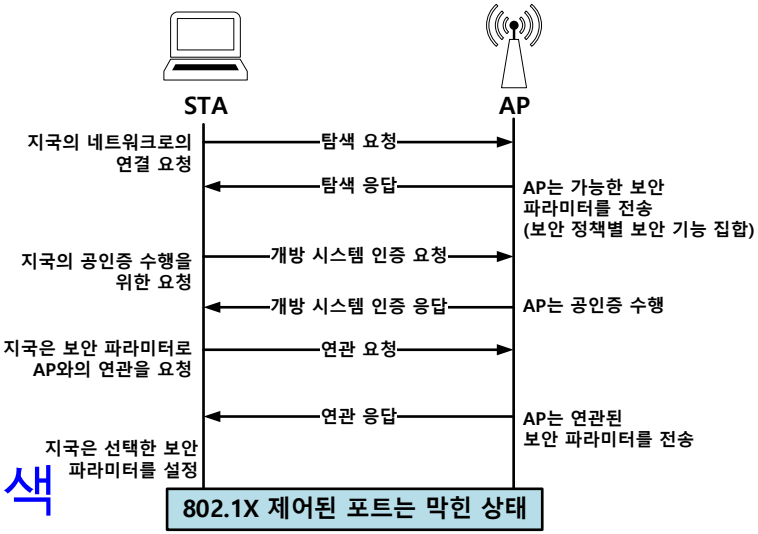
- IEEE 802.11i RSN 동작
  - 5단계로 분류하며 각 단계의 구체적인 특성은 통신 단말에 따라 달라짐

통신 단말에 따른 분류
BSS 내에서 AP를 통해 통신하는 두 지국
동일한 애드 혹(ad hoc) IBSS에서 직접 상호 통신하는 두 지국 IBSS: Independent Basic Service Set
서로 다른 BSS에 있으며 분산 시스템을 통해 각각의 AP를 경유하여 통신하는 두 지국
AP와 분산 시스템으로 연결 된, 유선 네트워크 상의 종단과 통신하는 무선 지국



IEEE 802.11i 무선 LAN 보안

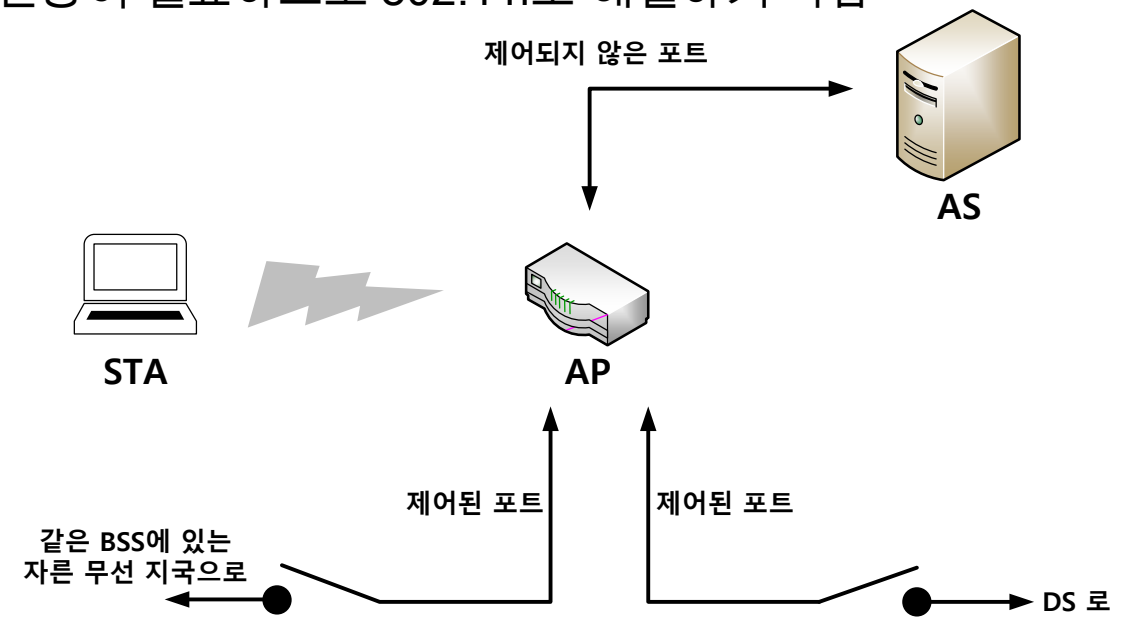
- IEEE 802.11i RSN 동작
  - 1단계: 탐색
    - 네트워크와 보안 기능 탐색
      - Beacon프레임 공지 또는 Probe Request/Response프레임을 통해 지국과 AP가 대응되는 보안 기능 탐색



    - 개방 시스템 인증
      - 보안 없이 지국와 AP간 단순 식별자(ID)를 교환
    - 연관
      - 지국은 연관 요청(Association Request)프레임을 전송하여, 이후 AP와 사용할 보안 기능에 대한 협상
      - 인증 및 키 관리도구, 암호도구 쌍, 그룹 키 암호 도구 등을 하나 선택하여 협상, 공통 암호 도구가 없거나, 보안 공격이 의심되면 연관 요청을 거부

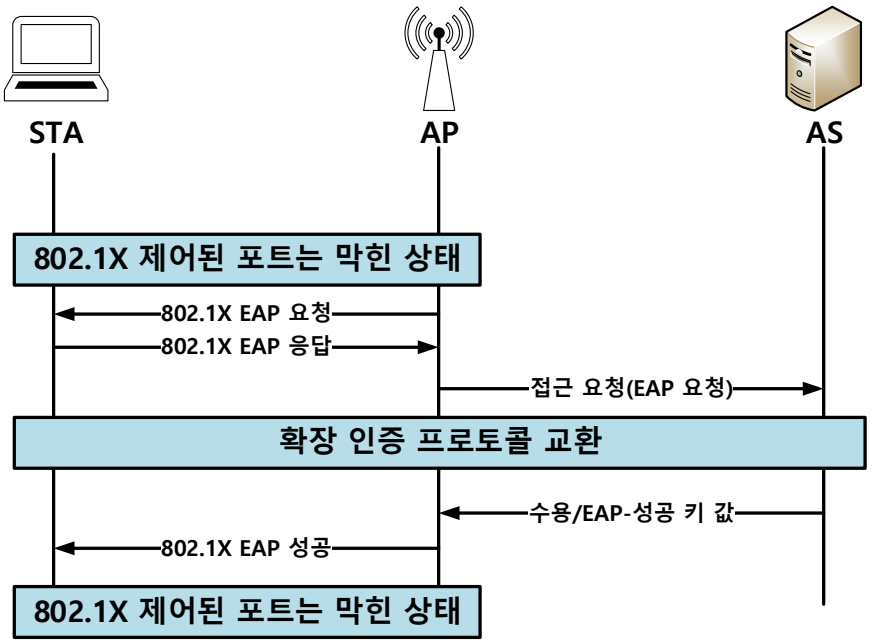
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i RSN 동작
  - 2단계: 인증
    - 접근 제어
      - IEEE 802.11i에서는 LAN용 접근제어 기능을 제공하기 위해 설계된 다른 표준을 사용 (IEEE 802.1X 표준으로 정의된 EAP는 포트기반 네트워크 접근제어 방식)
        - EAP: Extensible Authentication Protocol
        - IBSS에서는 지국간 쌍 별 인증이 필요하므로 802.11i로 해결하기 복잡



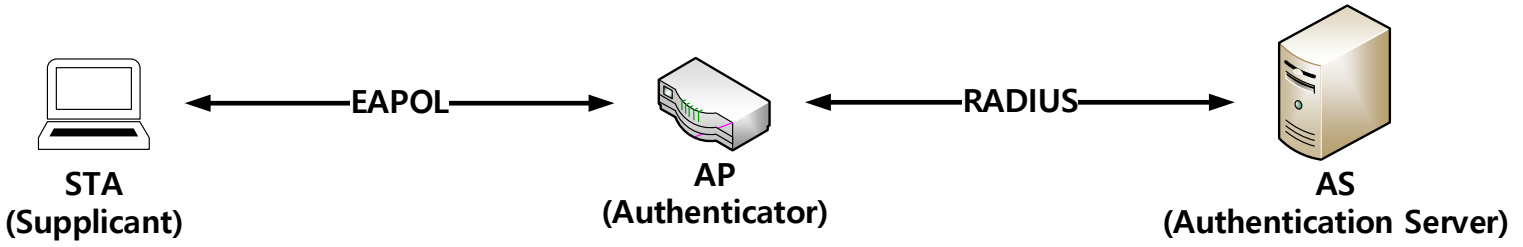
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i RSN 동작
  - 2단계: 인증 MPDU 교환
    - AS 연결
      - 지국은 해당하는 BSS의 AP를 통해 AS로 접근을 요청
    - EAP 교환
      - 지국 과 AS는 상호 인증을 위한 EAP 수행
    - 안전한 키 전달
      - AS는 마스터 세션 키(MSK)를 생성해 AP를 통해 지국으로 전달



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i RSN 동작
  - 2단계: 인증 EAP 수행
    - EAP 동작을 설명하기 위해 요청자(Supplicant), 인증자(Authenticator), 인증 서버(AS: Authentication Server) 용어를 사용
    - EAP와 결합되어 사용되는 프로토콜
      - 지국과 AP간의 메시지 전달은 EAPOL 프로토콜을 사용
        - EAPOL: EAP Over LAN
      - AP와 AS 간의 메시지 전달은 RADIUS프로토콜을 사용
        - RADIUS: Remote Authentication Dial In User Service



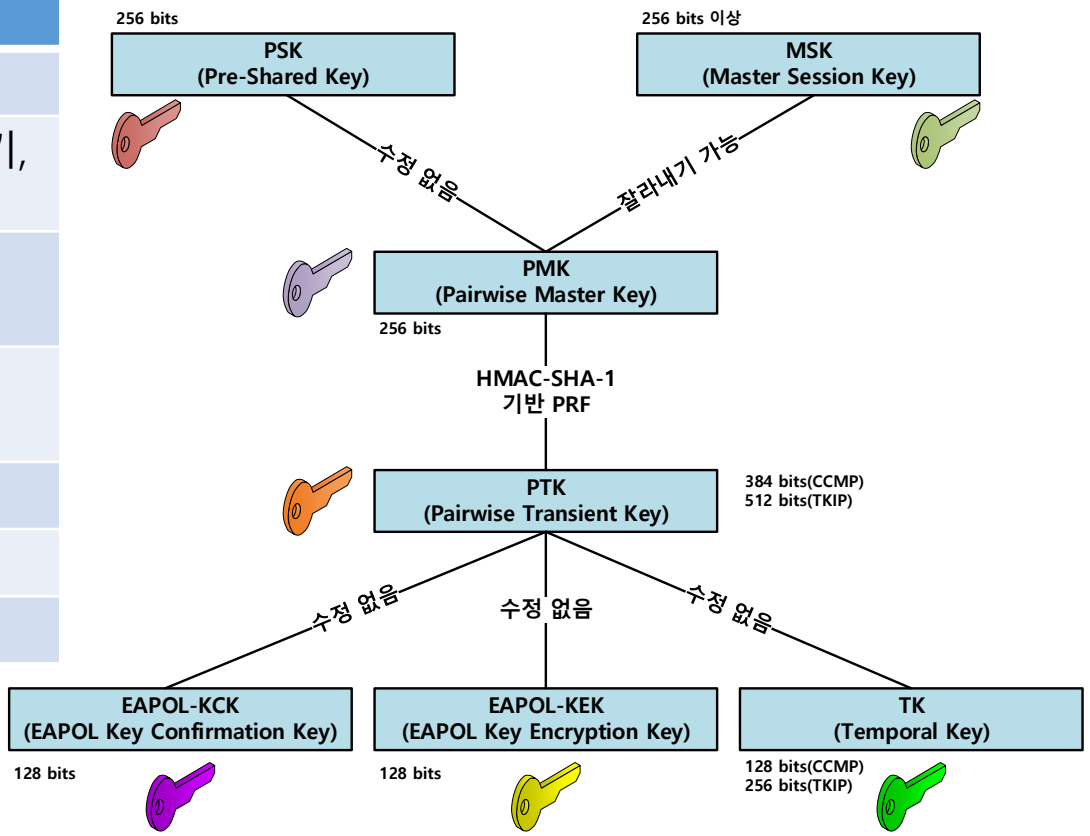
IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i RSN 동작
  - 2단계: 인증 EAP 수행
    - RADIUS
      - 인증자가 PPP프레임 등으로 ID와 암호를 받아 인증서버로 암호화(사전 공유 키)하여 전송(UDP 사용)
      - 인증 서버는 ID와 암호를 확인하고 허가 하거나 거절(거절 시 이유를 보냄)
    - DIAMETER Protocol
      - RADIUS보다 개선되어 대체되는 프로토콜
        - TCP사용, IPsec or TLS사용 등 RADIUS를 호환하며 개선된 프로토콜

IEEE 802.11i 무선 LAN 보안

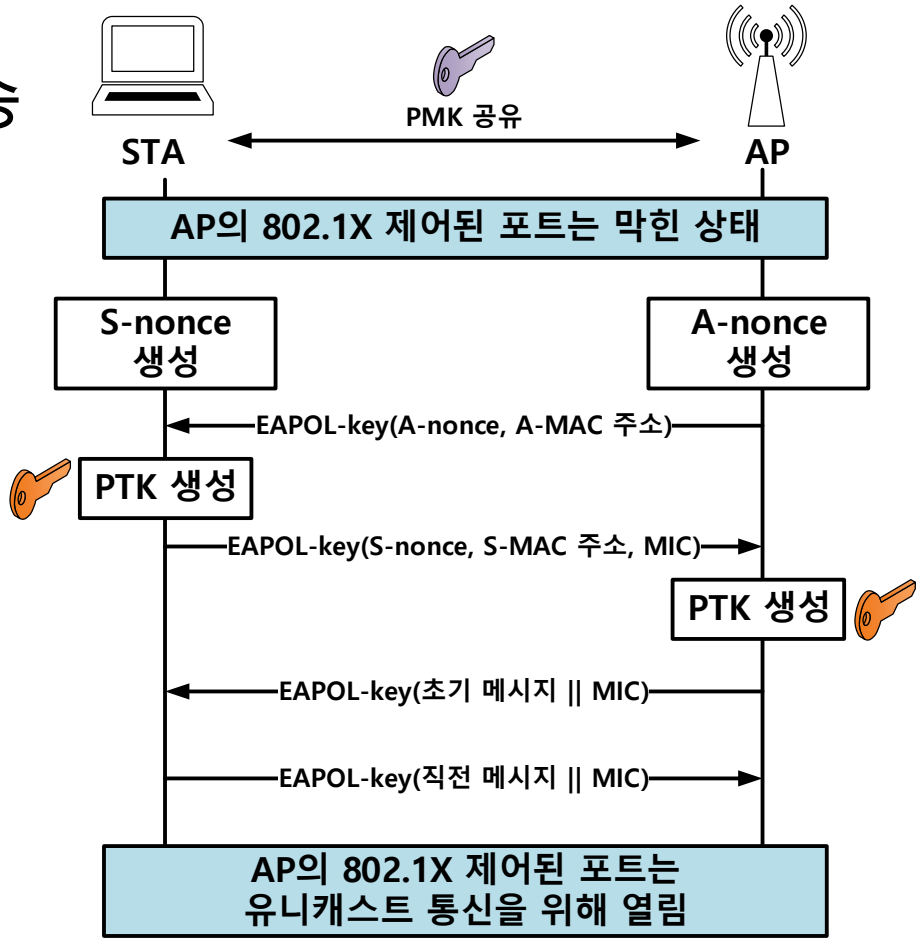
- IEEE 802.11i RSN 동작
  - 3단계: 각 연관 쌍 별 키 생성과 관리 설명 표와 구조

키	생성 및 관리
PSK	AP와 지국이 사전에 공유하는 비밀키
MSK	지국과 AP간의 상호 인증에서 생성된 세션 키, AS가 생성해 상호 공유
PMK	PSK로 PMK를 생성하거나, MSK의 일부를 잘라내어 PMK생성
PTK	PMK, 지국과 AP의 MAC주소, 비표를 PRF의 입력으로 생성한 해시값
KCK	메시지 인증을 위한 MIC 생성용
KEK	GTK 분배를 위한 키
TK	트래픽 보호용 키



IEEE 802.11i 무선 LAN 보안

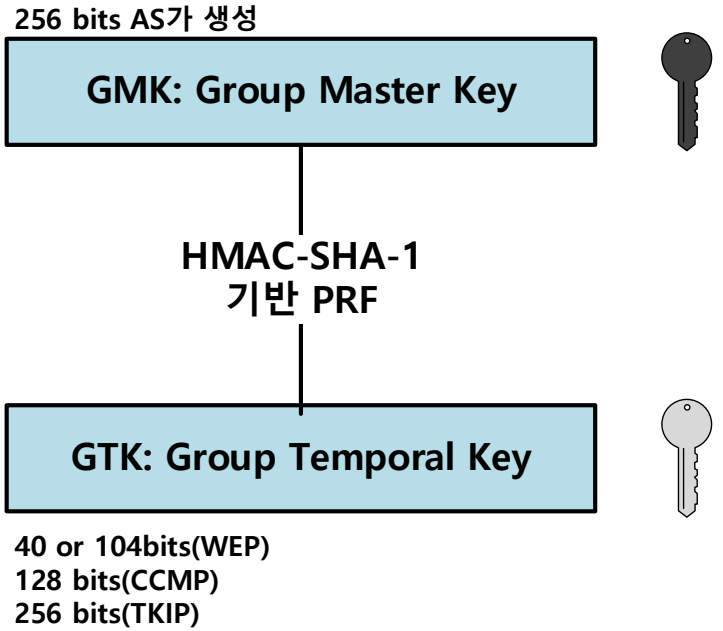
- IEEE 802.11i RSN 동작
  - 3단계: 4 way 협상을 통한 쌍 별 키 분배
    1. AP -> STA
       AP의 MAC 주소, Nonce값 전송
    2. STA -> AP
       STA의 MAC주소, Nonce값과 MIC전송
    3. AP -> STA
       첫 번째 메시지에 MIC을 추가한 전송
    4. STA -> AP
       직전 메시지에 대한 응답으로 MIC을 포함한 전송



IEEE 802.11i 무선 LAN 보안

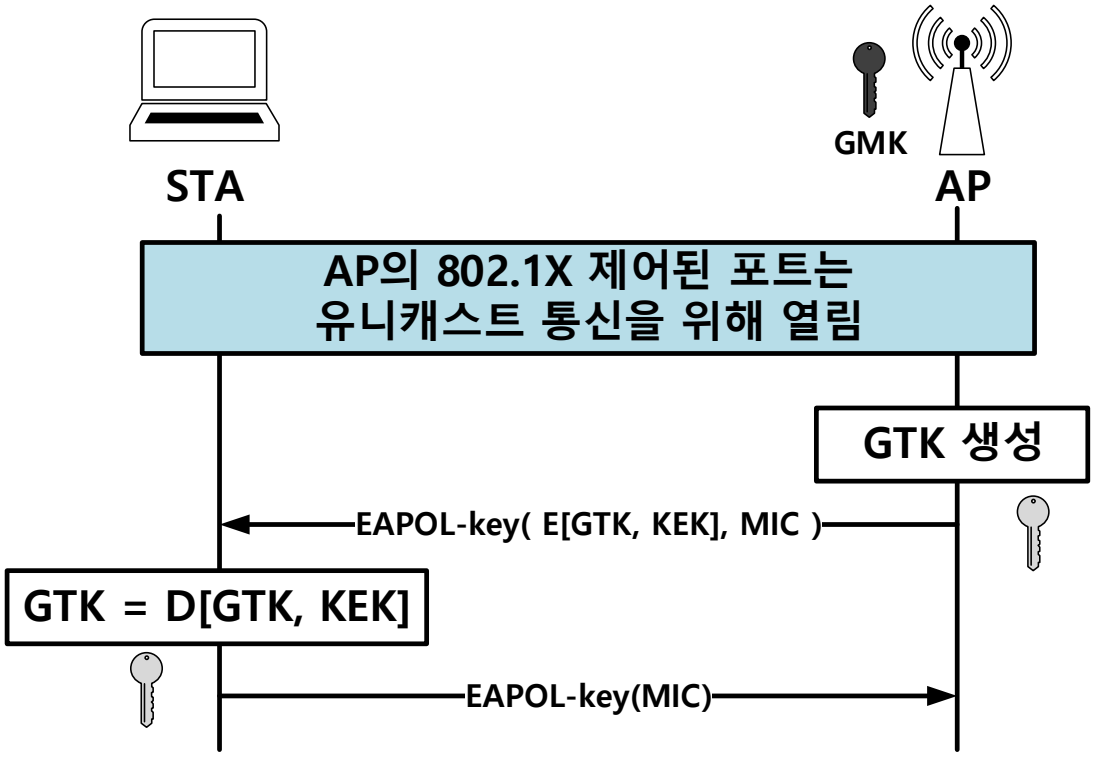
- IEEE 802.11i RSN 동작
  - 3단계: 멀티캐스트용 그룹 키 생성

키	생성 및 관리
GMK	AS가 생성, 주기적으로 교체하거나 침해 시 교체
GTK	GMK와 정책에 따라 다른 입력을 통해 생성, AP가 생성해 연관된 지국에게 전달



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i RSN 동작
  - 3단계: 멀티캐스트용 그룹 키 분배
    - AP가 GTK생성 후 KEK를 통해 암호화(RC4 or AES)
    - 암호문과 MIC을 포함한 메시지 전송
    - 수신 메시지 복호화 후 응답으로 MIC을 포함한 메시지 전송



IEEE 802.11i 무선 LAN 보안

- IEEE 802.11i RSN 동작
  - 4단계: 안전한 통신
    - TKIP (Temporal key Integrity Protocol) 제공 서비스
      - 메시지 무결성
        - MAC 프레임과 키를 입력으로 64bits MIC을 생성하고 함께 전송
      - 데이터 기밀성
        - 데이터와 MIC을 RC4로 암호화하여 데이터 기밀성 제공
    - CCMP (Counter CBC MAC Protocol) 제공 서비스
      - 메시지 무결성
        - 암호 블록 체인 인증 코드(CBC-MAC) 사용
      - 데이터 기밀성
        - AES-CTR을 사용한 암호화

감사합니다!