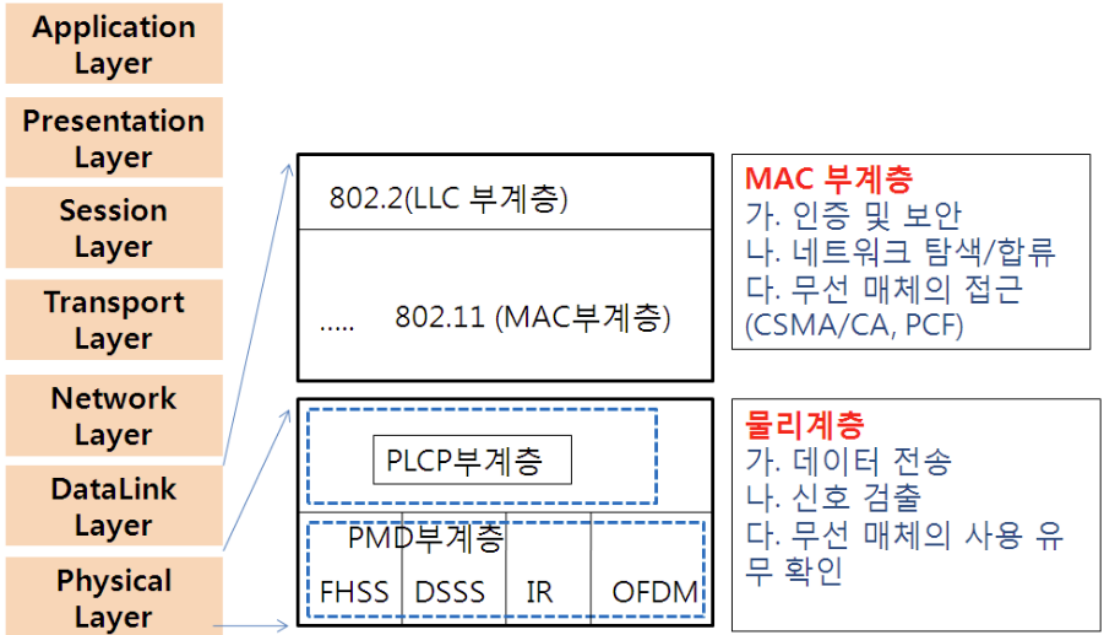
WiFi protocol(1)

IEEE 802.11 protocol의 동작 원리

20210741 황정현

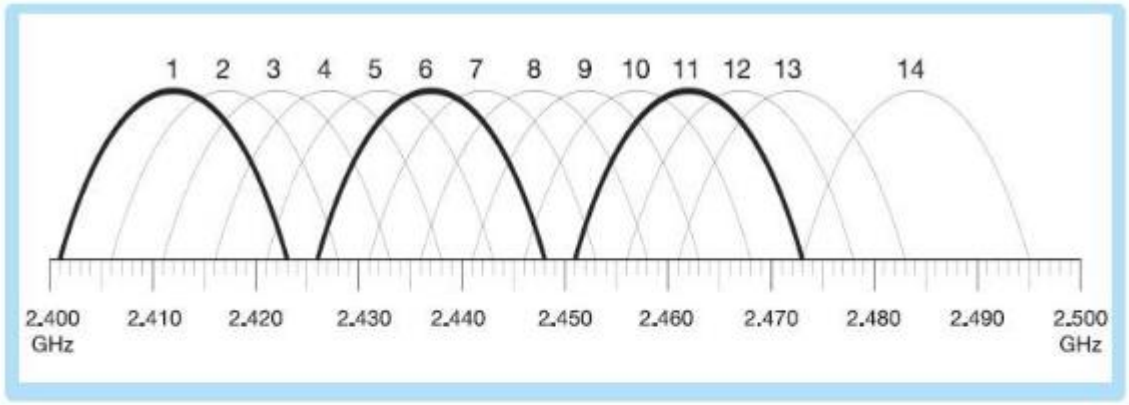
IEEE 802.11 계층 구조

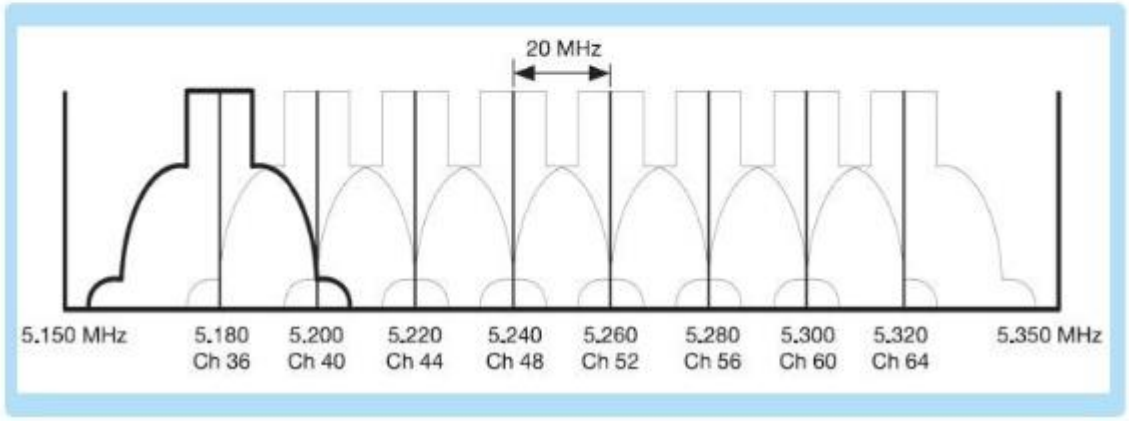


DataLink Layer – 데이터를 확인하고 검증하는 역할
Physical Layer – 데이터를 물리적으로 전송하는 역할

- 802.11은 OSI 7계층 중 하위 두 계층인 물리 계층과 데이터 링크 계층에 해당
- 데이터 링크 계층은 다시 LLC와 MAC으로 나뉨
- **LLC(Logical Link Control):** 네트워크 계층과의 인터페이스 제공
- **MAC(Media Access Control):** 무선 매체 접근 제어, 데이터 암호화, 오류 검출 등 **핵심 역할**
- 대부분의 보안 취약점이 **MAC 계층**에서 발생

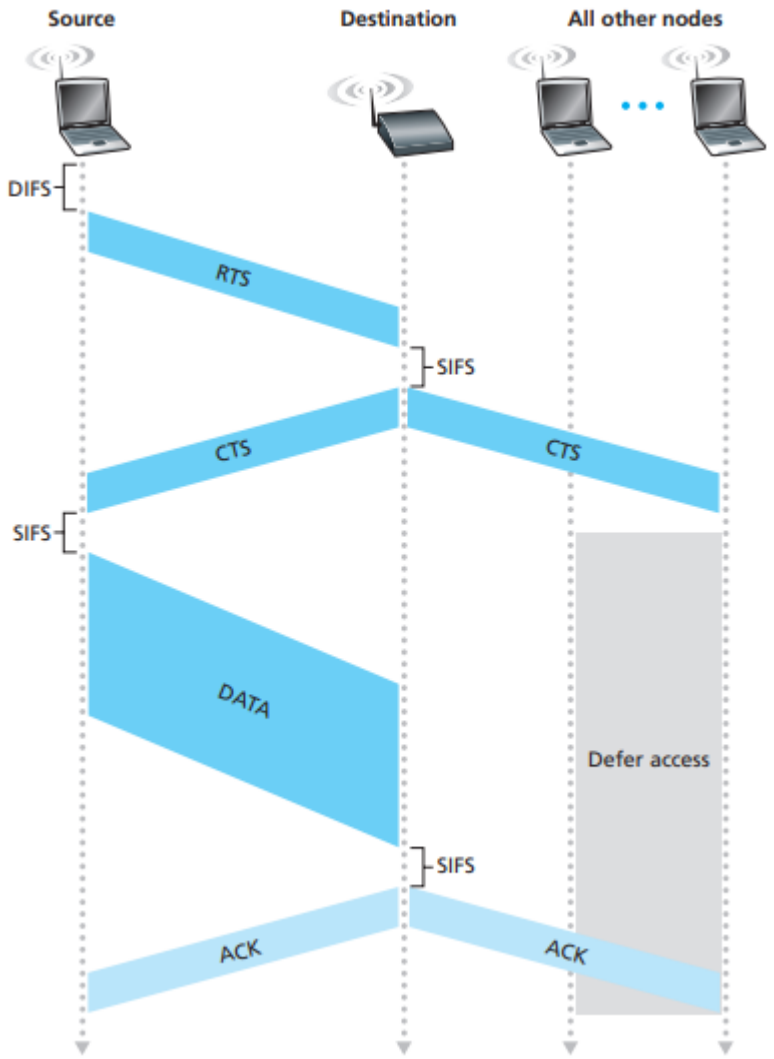
무선 주파수와 채널





- **주파수 대역:** WiFi는 주로 2.4GHz와 5GHz 대역을 사용함
- **채널(Channel):** 주파수 대역을 잘게 쪼갠 통신 도로
- **중첩(Overlapping):** 2.4GHz 대역은 채널 간 간섭이 심해, 서로 겹치지 않는 1, 6, 11번 채널을 주로 사용

CSMA/CA



- 무선 네트워크 특성 상(hidden terminal problem) 충돌을 미리 회피하는 **CSMA/CA(Collision Avoidance) 방식**을 사용
- 데이터를 보내기 전에 비어있는지(Idle) 확인하고, **랜덤한 시간(Backoff)**을 기다린 후 전송하여 충돌 확률을 낮춤.

- DIFS(Distributed Inter-frame Space): 채널이 빈 것을 확인 한 후 실제 프레임 전송까지 대기하는 시간
- SIFS(Short Inter-frame Spacing): 프레임 수신 이후 잠시 기다리는 시간
- RTS(Request to Send): 데이터를 보내도 될지 묻는 프레임
- CTS(Clear to Send): 특정 장치가 데이터를 보내고 있으니 모두 조용히 하라는 의미의 프레임
- ACK: 수신 성공을 알리는 프레임

동작 모드(1) – 표준 모드

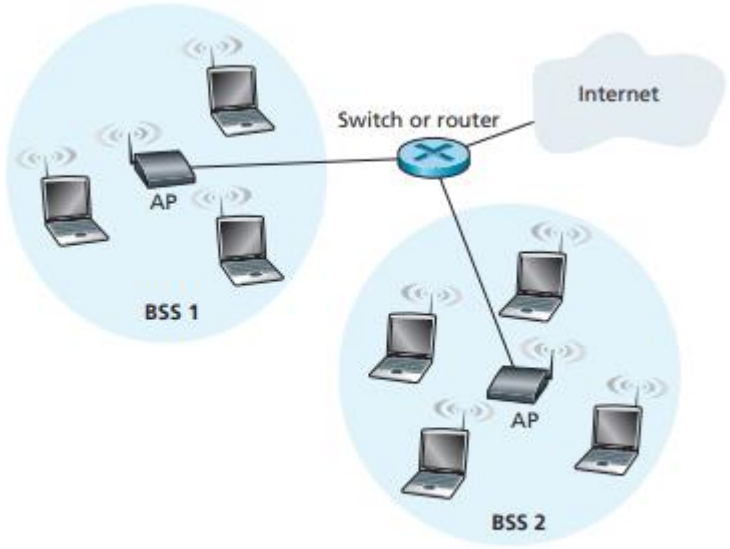


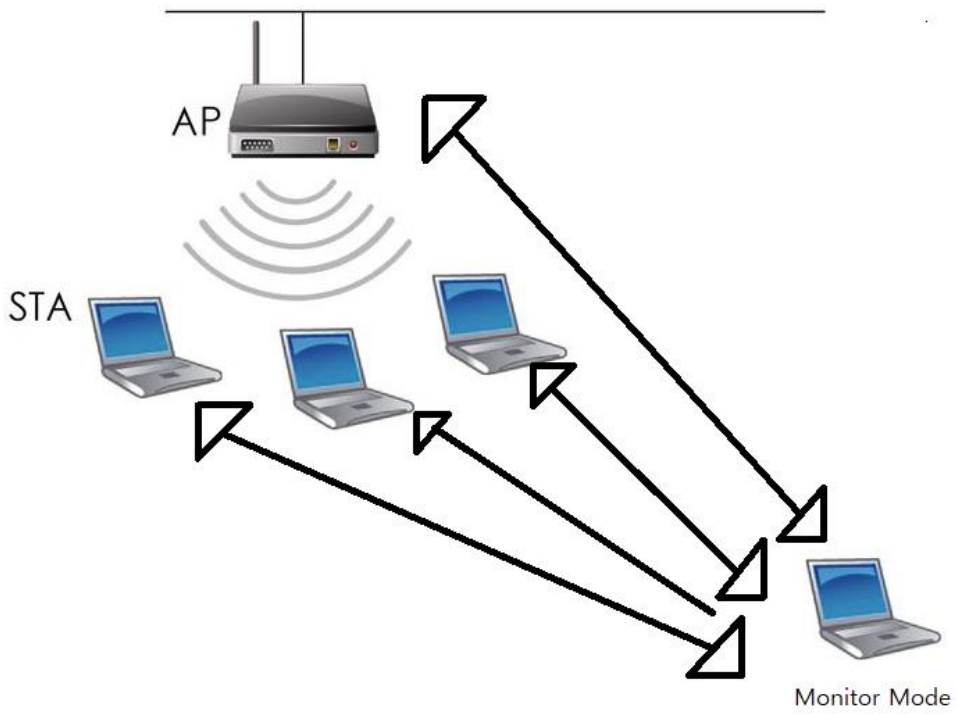
Figure 7.7 ♦ IEEE 802.11 LAN architecture

Figure 7.8 ♦ An IEEE 802.11 ad hoc network

- **Infrastructure Mode:** 가장 흔히 사용하는 방식. 모든 단말이 **AP(Access Point, 공유기)**를 거쳐서 통신함. AP가 포함된 네트워크 그룹을 **BSS(Basic Service Set)**이라 함.

- **Ad-hoc Mode:** AP 없이 단말기 끼리 직접 통신하는 방식.

동작 모드(2) – 모니터 모드



- 일반적인 모드에서는 자신에게 온 패킷만 처리하고 **나머지는 무시**함.
- **Monitor Mode:** 공중에 날아다니는 **모든 패킷(타인의 통신 포함)을 수집(Sniffing)**함.
- WiFi 취약점 공격들은 대부분 모니터 모드에서 수행됨.

802.11 프레임 구조

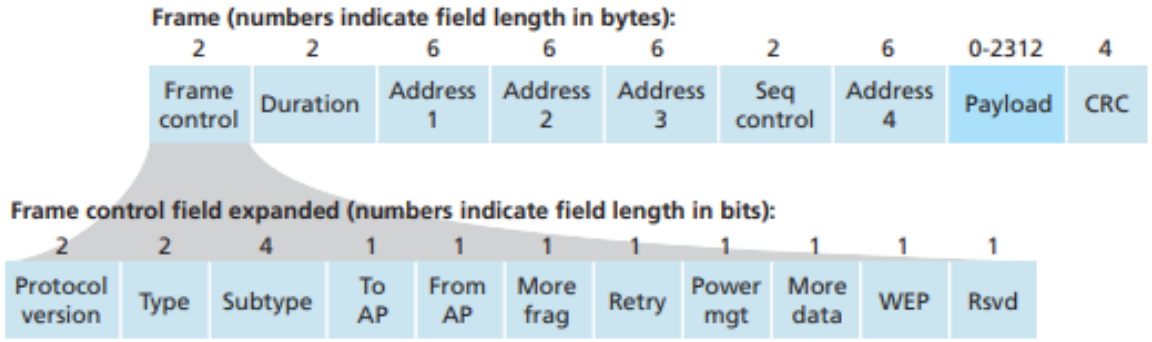


Figure 7.13 ♦ The 802.11 frame

Frame Control의 하위 필드
- Type & Subtype: 프레임의 종류를 구분함.
- To AP / From AP: 주소 필드의 의미를 정의.
- WEP: 보안 암호화 적용 여부를 나타냄.

- **Frame Control:** 프레임의 종류(Type) 등을 정의
- **Duration**: 데이터 전송과 그에 따른 ACK 전송에 필요한 총 시간을 기록. 이 값을 기반으로 주변 장치들이 전송을 멈추어 충돌을 피함.
- **Sequence Control:** 패킷 순서를 맞추고 중복 제거에 사용.
- **Payload:** IP 데이터그램이나 ARP 패킷이 담김.
- **CRC:** 비트 오류 감지를 위한 32비트 체크섬

802.11 프레임 구조 – Address Field

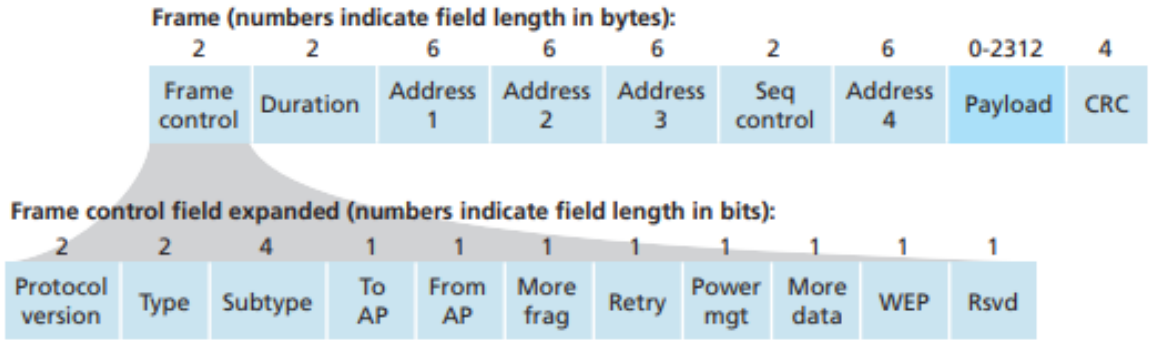
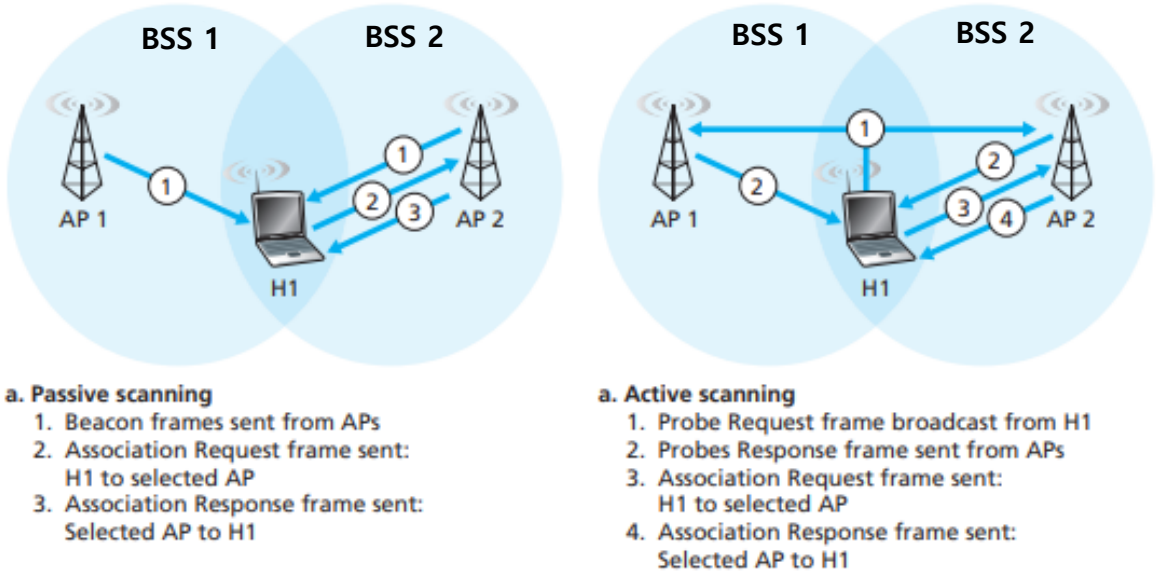


Figure 7.13 ♦ The 802.11 frame

- 802.11은 상황에 따라 주소 필드 (Address 1~4)의 의미가 바뀜.
- 이를 결정하는 것은 Frame Control 필드의 'To DS'와 'From DS' 비트

To DS	From DS	설명	Address 1 (수신)	Address 2 (송신)	Address 3	Address 4
0	0	Ad-hoc (IBSS) 또는 관리 프레임	DA (목적지)	SA (출발지)	BSSID	N/A
0	**1**	**Infrastructure (AP-> Station)**	DA (Station)	BSSID (AP)	SA (Router/Server)	N/A
1	**0**	**Infrastructure (Station -> AP)**	BSSID (AP)	SA (Station)	DA (Router/Server)	N/A
1	1	WDS (Wireless Distribution System)	RA (수신 AP)	TA (송신 AP)	DA	SA

연결 수립 과정(1) – 스캐닝(Scanning)



a. Passive scanning
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1

a. Active scanning
1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: Selected AP to H1

Figure 7.9 ♦ Active and passive scanning for access points

- **Passive Scanning(수동)**: AP가 주기적으로 뿌리는 **Beacon 프레임**을 단말이 듣고 AP를 찾음.
  Beacon 프레임에는 AP의 SSID와 MAC 주소가 포함됨.

- **Active Scanning(능동)**: 단말이 먼저 **Probe Request**를 보내면, AP가 **Probe Response**로 응답.

연결 수립 과정(2) – 인증 및 결합

- 스캐닝 이후 실제 연결에 거치는 과정
- **Authentication(인증):** 단말과 AP가 서로 합법적인 기기인지 확인.
- **Association(결합):** 실제 데이터 전송을 위한 논리적 연결을 맺음. 결합 과정이 끝난 후 AP는 단말을 관리 테이블에 등록

프레임 타입

- **Management Frame(관리):** 연결을 맺거나 끊을 때 사용
  (ex: Beacon, Probe, Auth, Assoc)
  -> Beacon Flooding(가짜 AP), Deauth Attack(강제 연결 해제)

- **Control Frame(제어):** 데이터 전송을 도움. (ex: ACK, RTS, CTS)
  -> Virtual Jamming(RTS/CTS 지속시간 조작)

- **Data Frame(데이터):** 실제 데이터를 전송함.
  -> 암호화의 대상

WiFi 보안 연결

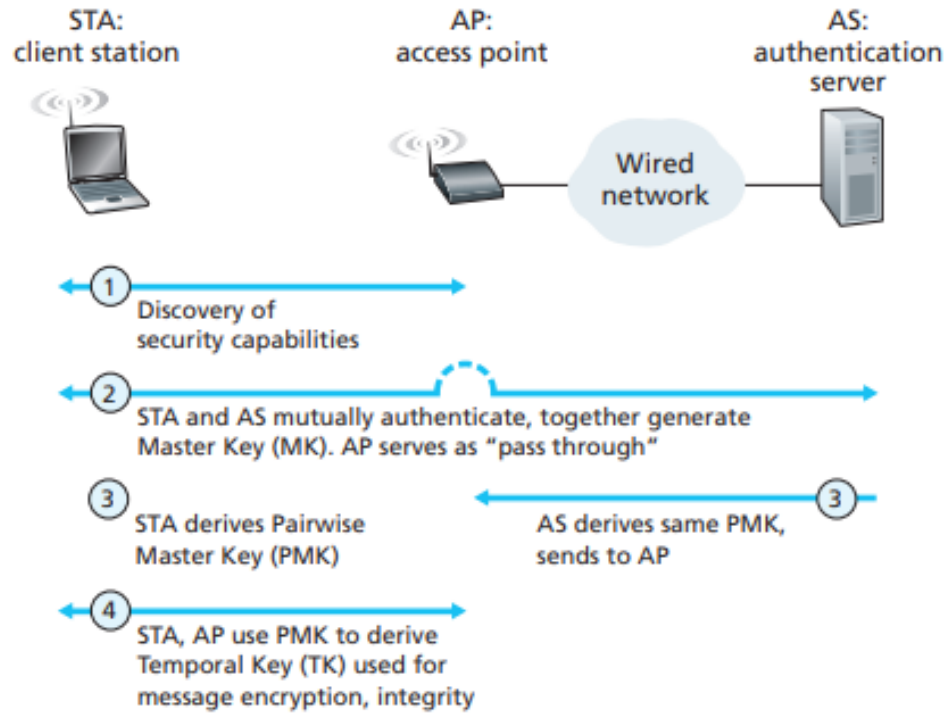
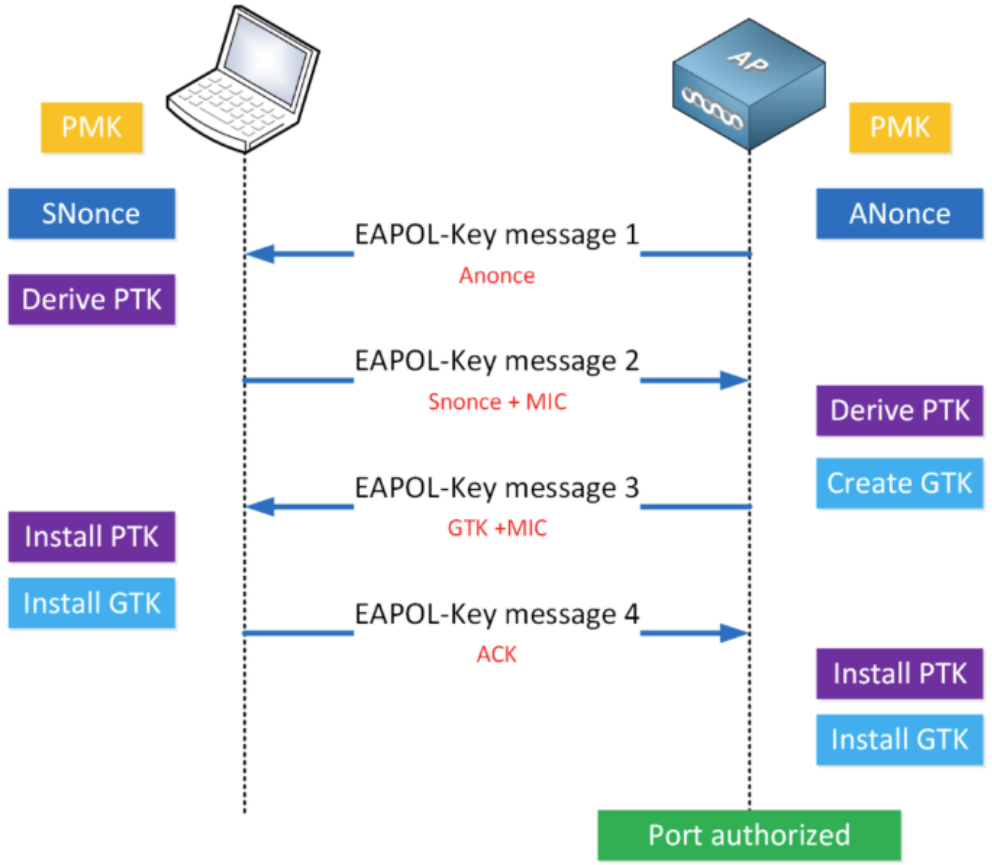


Figure 8.31 ♦ 802.11i: Four phases of operation

- WiFi 보안 연결의 4단계
  1. Discovery: 보안 방식 결정
  2. Authentication: MK 생성
  3. Key Generation: PMK 공유
  4. Secure Data Transfer: TK 생성 후 통신

- 환경별 차이점
  - Enterprise: 인증서버(AS)가 개별 사용자 인증 수행
  - Personal: 미리 설정된 PSK와 SSID로 PMK 역할을 대신함.

EAPoL과 4-way handshake



- **EAPoL**(Extensible Authentication Protocol over LAN): IP 주소 할당 전, LAN 구간에서 인증 데이터를 전달하는 프로토콜. 앞 슬라이드의 3~4단계.

- **4-way-handshake**
  목적: **공유된 PMK를 이용해** 실제 암호화에 쓸 임시 키 생성 및 검증
  특징: 비밀번호(PMK) 자체를 전송하지 않음 -> 해킹 방지
  취약점: 교환되는 Nonce와 무결성 값을 캡처하여 대입 공격 가능

감사합니다.

- 1주차 요약: 802.11의 MAC 계층 기술(CSMA/CA 등), 연결 과정
- 2주차 계획: 암호화 방식과 구체적인 해킹 방식 학습 예정

Reference

- Computer Networking – a top-down approach: Ch 7.3, 8.8
- 구글링