Wifi-Protocol-1

20210638 최무송

Plan

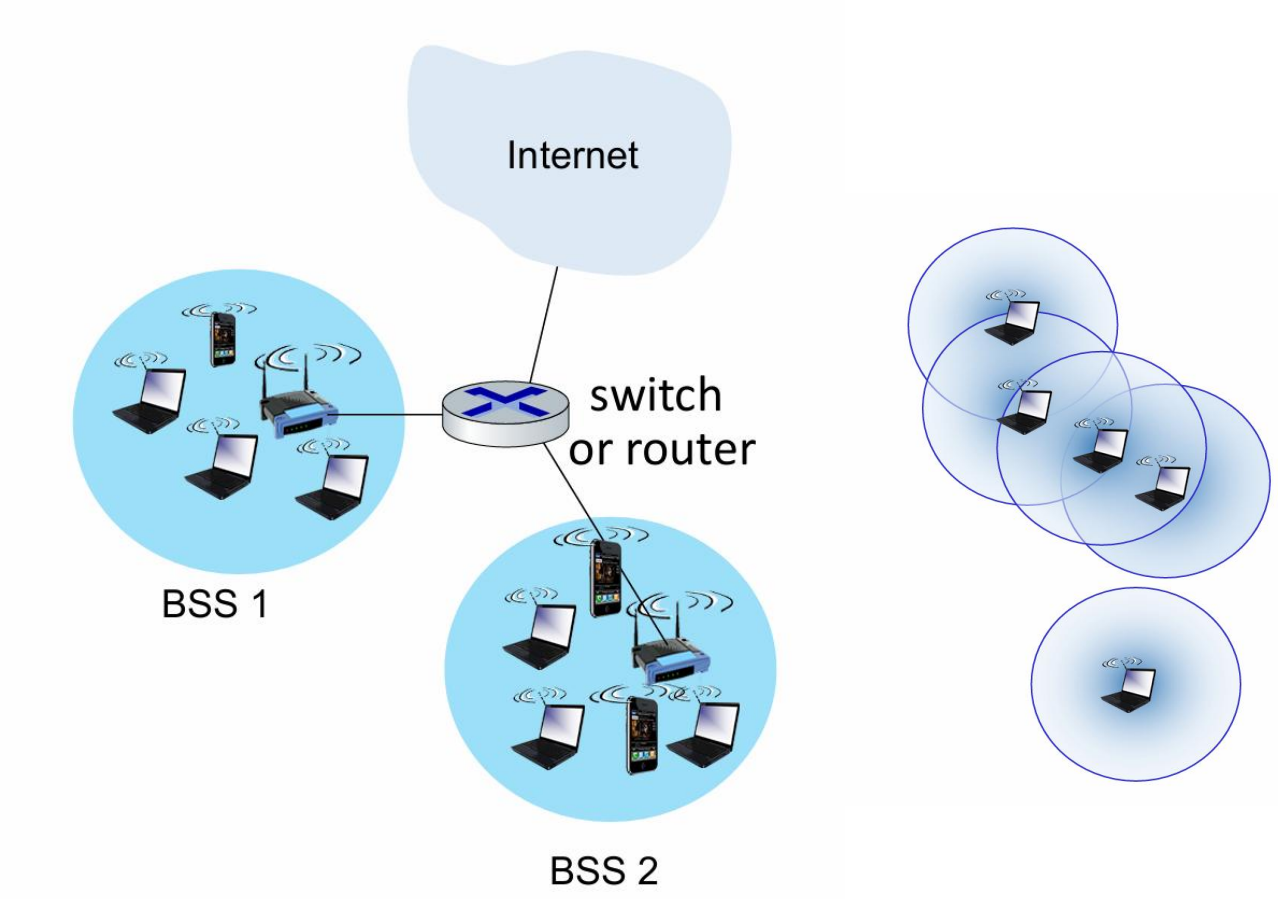
- Contents of Wifi-protocol (week 1)
- WireShark + Security Vulnerability of Wifi-protocol (week 2)
- Security Vulnerability Attack practice with online platform (week 3)

IEEE 802.11 Wireless LAN (Wi-Fi)

- Technical Standard for Wireless LAN
- Started from 1997, currently revising
  - ex) Wifi 6E (802.11ax)
- Layer
  - Data Link Layer
  - Physical Layer

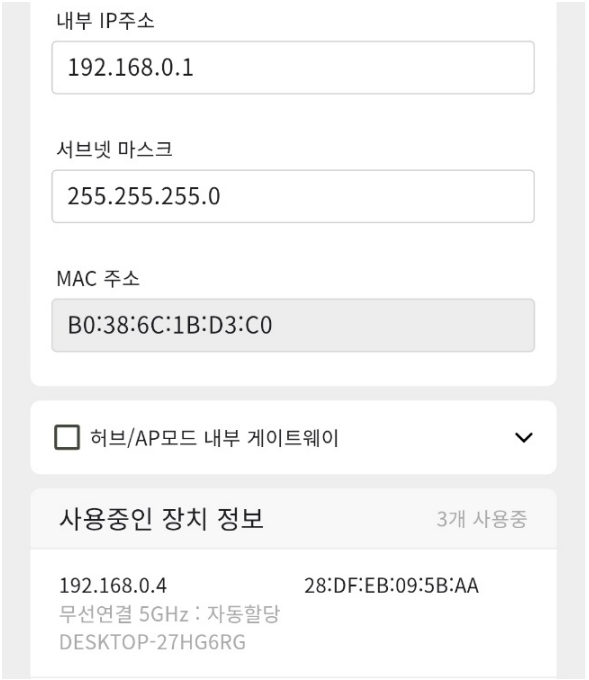
IEEE 802.11 Architecture

- Infrastructure mode
  - Access Point (Base station)
  - Basic Service Set (or cell)
    - cf. ESS
- Ad hoc mode



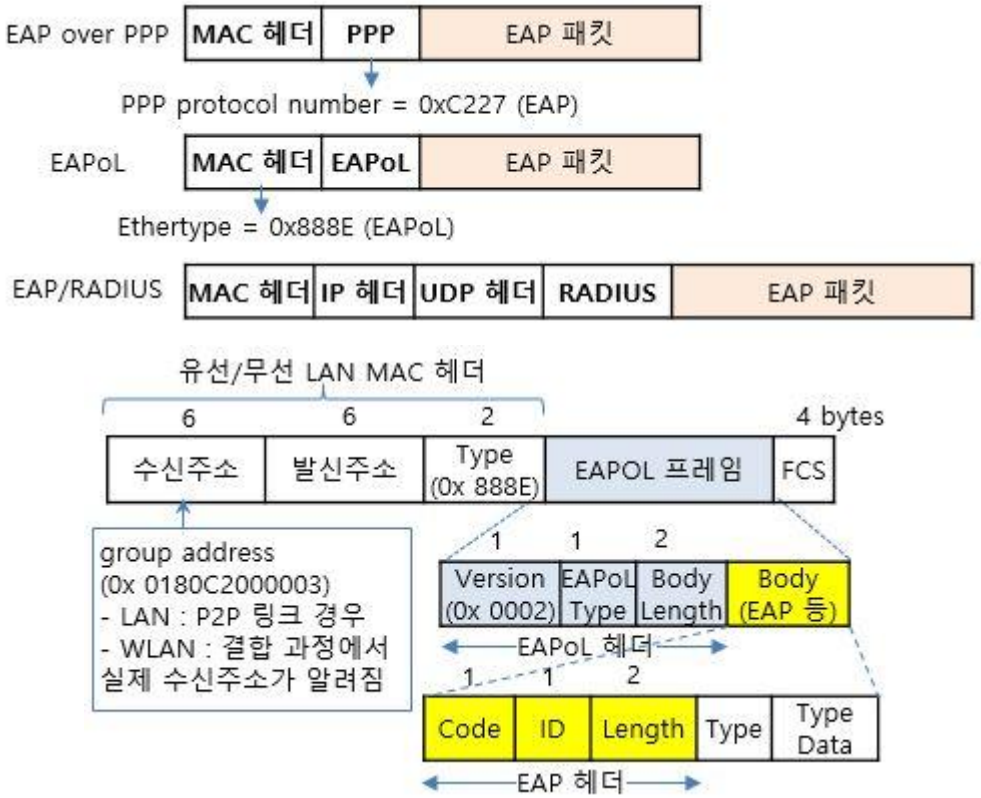
IEEE 802.11 Association

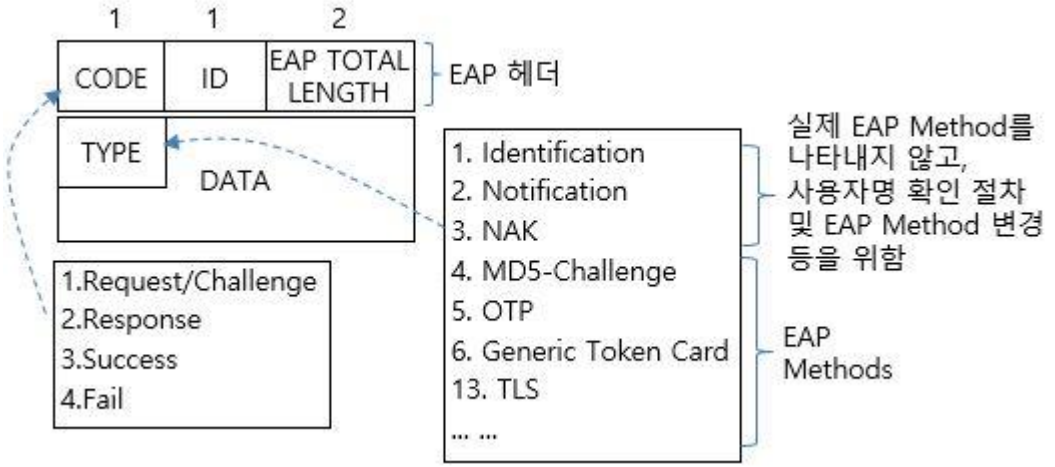
- Host scans channels & listening for Beacon Frames
  - Beacon frames: SSID(AP's name) + MAC address
- Select AP for authentication
  - EAPoL
- AP-Host association
- DHCP (host gets IP address)



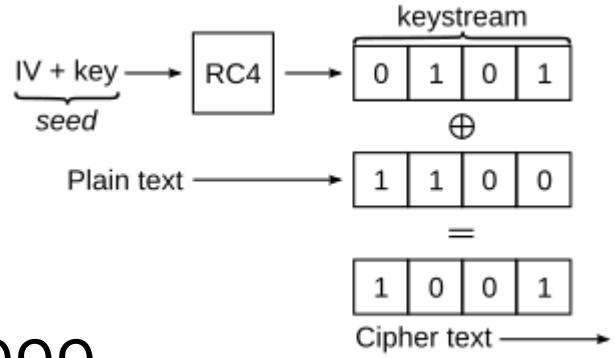
IEEE 802.11 EAPoL

- EAP(Extensible Authentication Protocol) Encapsulation over LAN
- Authentication Framework





Ciper Algorithm: WEP



- WEP: Wired Equivalent Privacy, Developed in 1999

- 4-step challenge and response
  - Client sends authentication request to AP
  - AP sends clear-text challenge to client
  - Client encrypts the text with WEP key and send it to AP
  - AP decrypts the response

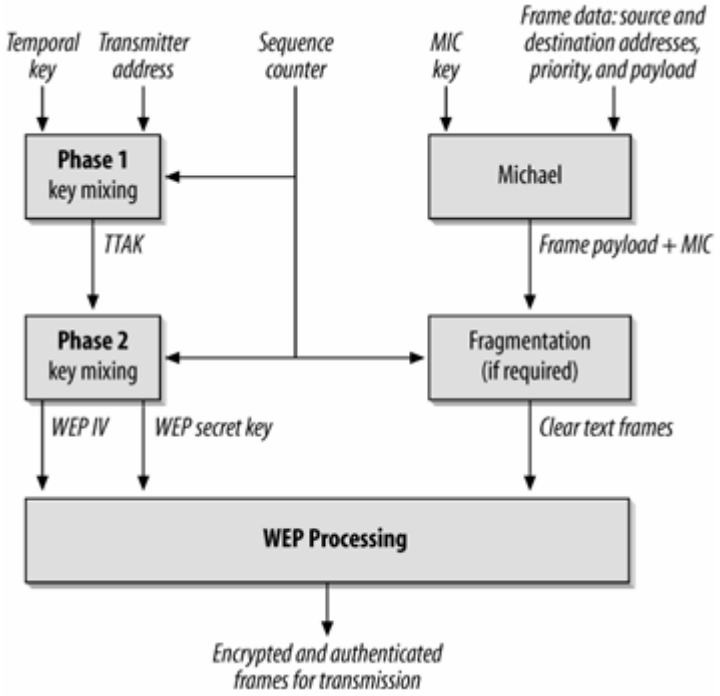
- Weak security: Stream-Cipher with static key

Ciper Algorithm: WPA

- WPA: Wi-Fi Protected Access, also based on RC4

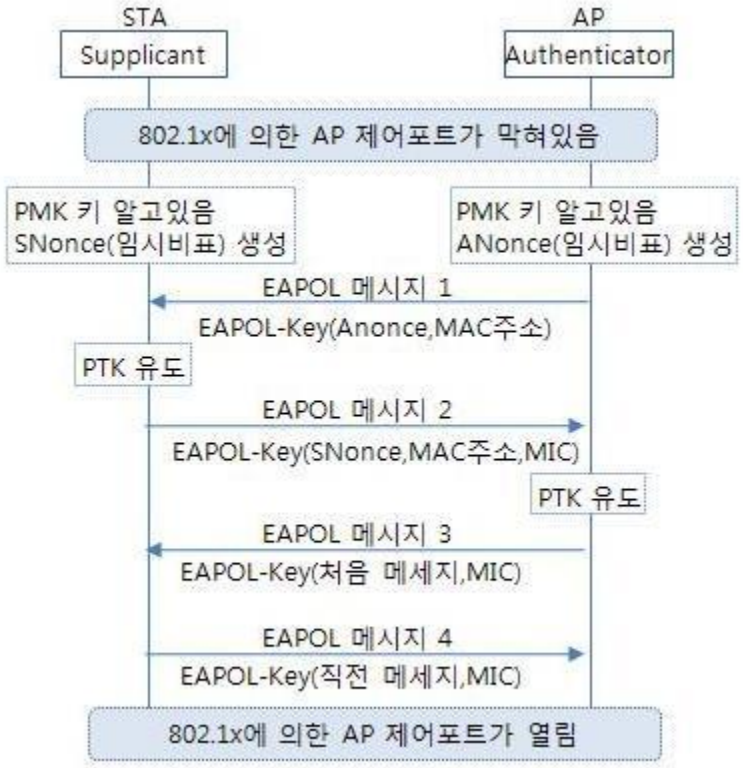
- WPA implements TKIP(Temporal Key Integrity Protocol)
  - key mixing function
  - Sequence counter
  - Message Integrity Check (replaces CRC)

- Weak security: Stream Cipher, MIC



PSK (Pre-Shared Key)

- Used in WPA/WPA2
- Authentication + PTK generation
- 4-way Handshake
  - AP sends a random number (ANonce) to client
  - Client responds with its random number (SNonce)
  - AP calculates PTK and sends an encrypted message to client.
  - Client decrypts the message with PTK



Ciper Algorithm: WPA2

- WPA2 is enhanced version of WPA
- AES based Counter mode with CBC-MAC
- Weak security: MIC (4-way handshake)
- KRACK(Key Reinstallation Attack) (M3), PMKID offline dictionary attack(M1)

Ciper Algorithm: WPA3

- 192-bit encryption in WPA3-Enterprise mode
- SAE(Simultaneous Authentication of Equals) instead of PSK (Pre-Shared Key) exchange
- Safe and personalized encryption
- Fragattack (WEP~WPA3)

SAE (Simultaneous Authentication of Equals)

- Password-authenticated key exchange (PAKE)
- Dragonfly handshake
- Forward secrecy guaranteed
- Dragonblood attack(Downgrade attack, Timing/Cache-based side-channel attack, DoS attack)