NASA 2025 Wireless Lab

Week 12 5/5/2025

NA Wireless
謝政洋

Special Thanks: 歷屆助教

Outline

- Wireless Security Protocol
- Wireless Network Architecture of CSIE
- Lab

Outline

- Wireless Security Protocol
- Wireless Network Architecture of CSIE
- Lab

Protocols

- WEP(Wired Equivalent Privacy)
- WPA(Wi-Fi Protected Access)
- WPA2(Wi-Fi Protected Access version 2)
- WPA3(Wi-Fi Protected Access version 3)

WEP

- Wired Equivalent Privacy (WEP)
- Designed to provide the same level of security as wired networks
- Ratified as wi-fi security standard in 1999
- A few security flaws were discovered. WEP was abandoned by the Wi-Fi Alliance in 2004
    - Vulnerable stream encryption standard: RC4

RC4

How it Works:

1. Key Scheduling Algorithm (KSA):
    - Initializes a 256-byte state array (S) based on a secret key (40–2048 bits).
    - Adding IV, additional input to vary encryption each session.
2. Pseudo-Random Generation Algorithm (PRGA):
    - Continuously shuffles S and generates a pseudo-random byte stream.
3. Encryption/Decryption:
    - Plaintext XOR Keystream = Ciphertext
    - Ciphertext XOR Keystream = Plaintext

WPA

- Designed to replace WEP, adapted in 2003
- TKIP(Temporal Key Integrity Protocol)
- Via firmware upgrades, WPA could be implemented on existing WEP-enabled devices
- Flaw in WPA: still some weaknesses in WEP existed (RC4)

WPA2

- Mandatory for all new devices from 2006
- Includes CCMP(Counter Mode Cipher Block Chaining Message Authentication Code Protocol), a stronger encryption mode
- RC4 is replaced by AES
- Implements the mandatory elements of IEEE 802.11i
- Authentication: Personal (PSK) & Enterprise (802.1X)
- “Krack Attack” → But most vendors have patched their implementation.

WPA3

- Based on WPA2
- Compatible with WPA2 devices
- Improvement of security
  - Privacy on public wi-fi network
  - Protection against brute force attack

Outline

- Wireless Security Protocol
- Wireless Network Architecture of CSIE
- Lab

AP

- Access Points to Wi-Fi, what your devices connect to when using Wi-Fi
- Layer 2 device (Data link layer)
- AP to wireless network is like switch network port to wired network
- Commercial AP has more power and provide more wireless functionality than consumer product
    - But consumer product usually has more things integrated into single machine, such as router, AP, switch, firewall or etc.

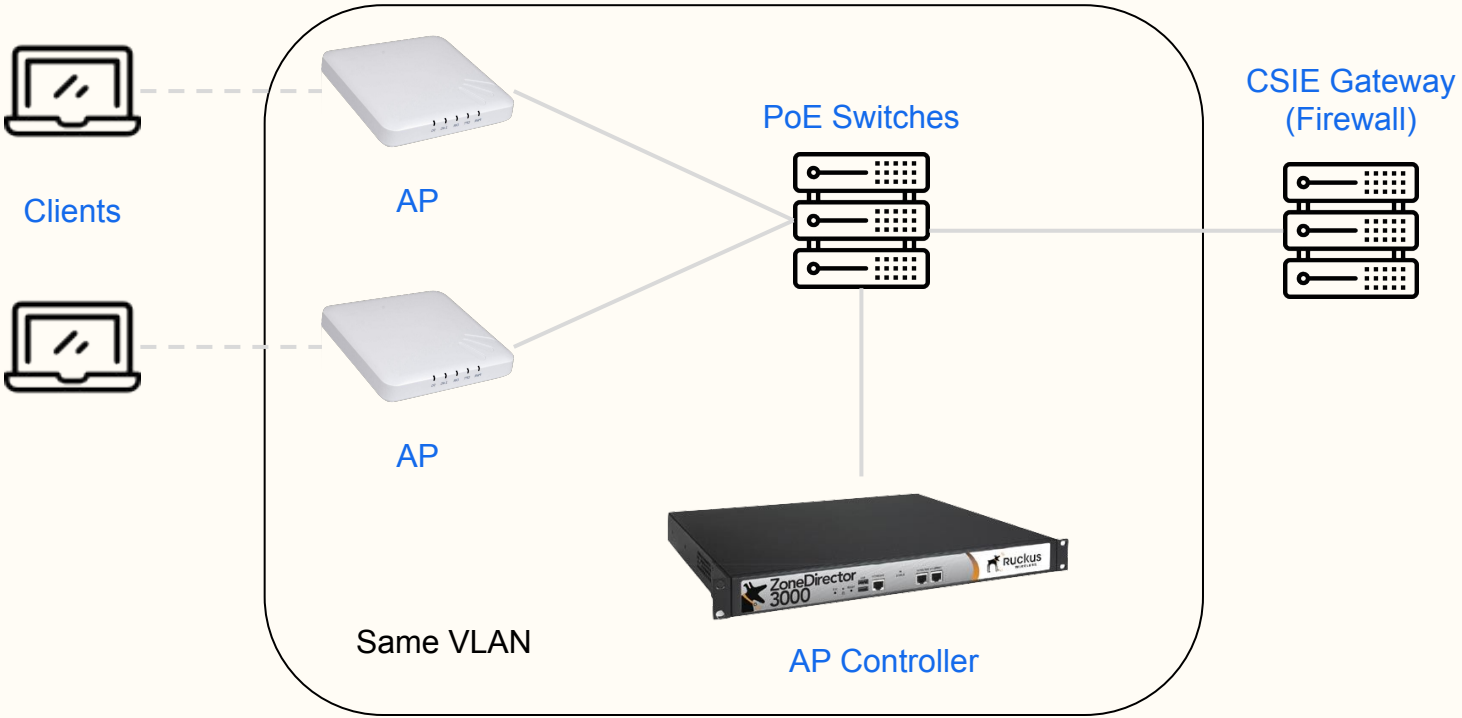
AP Controller

- In commercial environment, usually there are plenty of APs
  - Hard to manage
  - Use AP Controller to manage all AP from one interface
- AP controller allows administrators to do the following tasks easily
  - Apply changes Ex: add a new SSID, to some APs
  - Monitor APs
- Most commercial AP products can run in either standalone mode or controller mode
  - Standalone mode: All APs work on its own
  - Controller mode: Use an AP controller to manage all APs
  - Some brands even provide in-between mode, often called “controller-less mode”
    - No controller, but allow small amount of APs to be managed together

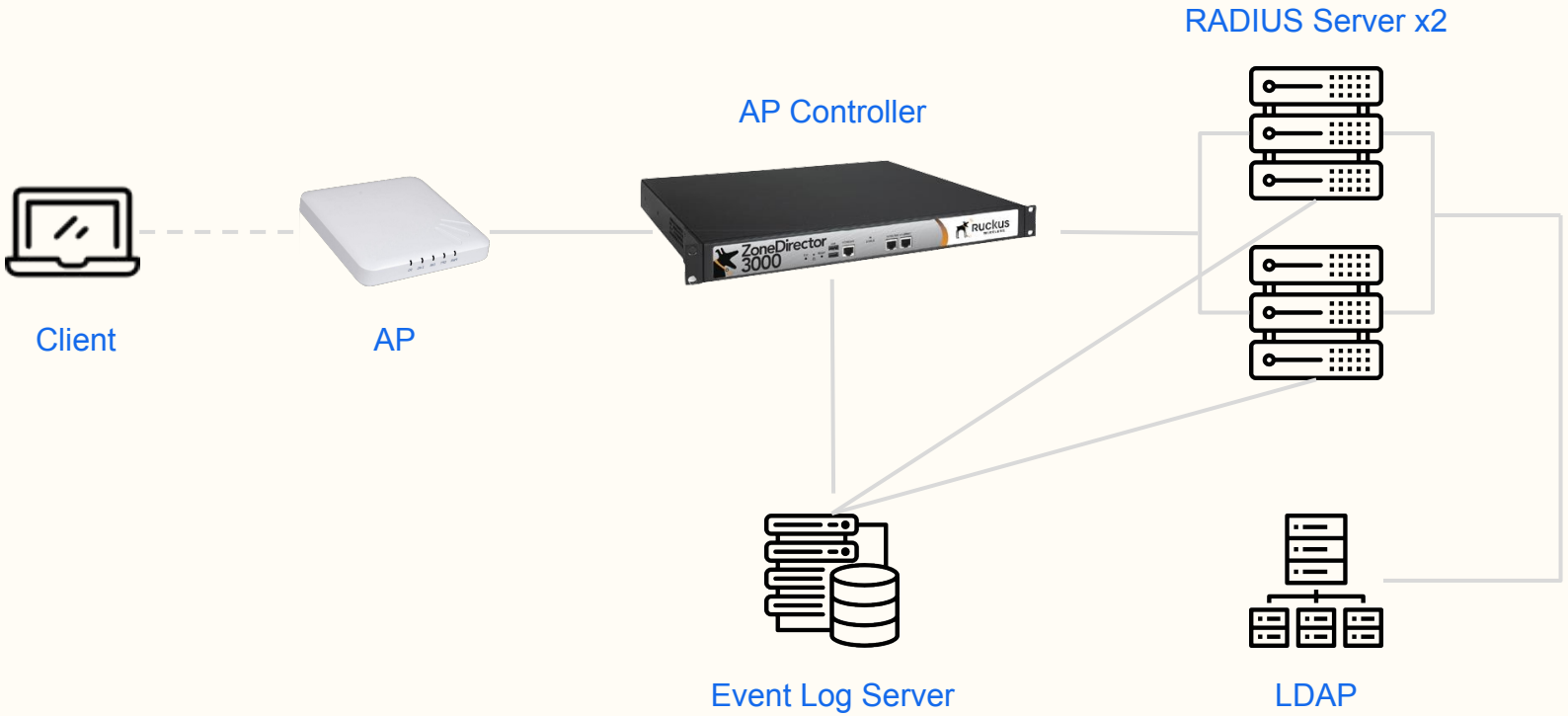
RADIUS Server

- RADIUS protocol - Remote Authentication Dial-In User Service
- AAA service
  - Authorization: Manage which user can use the network
  - Authentication: Check if the user credentials are correct
  - Accounting: Record the network usage by the users
- Often being used with 802.1X protocol together
  - Authentication & Authorization
  - 802.1 not 802.11
  - Also applicable to wired network
- Implementation software: FreeRADIUS (Open-source)

Our Infrastructure Overview - Network



Our Infrastructure Overview - Authorization



Questions?

Outline

- Wireless Security Protocol
- Wireless Network Architecture of CSIE
- Lab

前置作業-Linux

- Iwconfig
  - man iwconfig
- Wavemon
  - (Debian / Ubuntu) sudo apt-get install wavemon

前置作業-Windows

- 下載 Wi-Fi Scanner (link)
  - 個人使用免費

前置作業-MacOS

- 連上某個 SSID 之後，按住 Option 鍵再點擊 Menu Bar 上的 Wi-Fi 圖示，就可以看到各項數據了

1. 測量數據

[請附截圖並以表格呈現以下數據]

找一個有兩個 SSID的網路，分別是 2.4G 和 5G。請你在以下地點

- 離 AP 最遠(未隔牆)點
  - 盡量離至少5公尺，盡量在連的到的情況越遠越好
- 離 AP 最近點
- 和 AP 隔著牆壁

分別測量以下數據:

- Signal Strength
- SNR (MacOS / Linux) / Quality (Windows)
- Transmission rate

同時請說明以上數據各自代表的意義及單位 (若有的話)

2. 分析數據

請比較

- 距離對各項數據的影響
- 2.4G 和 5G 在隔牆時的訊號衰減

並解釋造成該差異的原因，以及你測量的結果是否符合預期

Submission

- 請將 lab 結果寫成 report 並以 pdf 格式上傳至 NTU Cool 作業區，report 內容須包含
  - 你所測量到的數據，請附截圖並以表格呈現各項數據
    - 測量的時候記得要製造流量！ (e.g. 瀏覽網頁等)
  - 根據第二步驟中的數據，分析並寫出你所觀察到的內容
  - 以上各項的詳細內容請參考前面幾頁投影片
- 檔案名稱格式：{student id}_lab11.pdf，e.g. *b13902999_lab11.pdf*
- Deadline: 2025/05/11 21:59
- 如果有遇到任何問題，請寄信到 vegetable@csie.ntu.edu.tw
  - 請在主旨前加上 [Lab11]

Reference & Resource

- Wavemon: https://github.com/uoaerg/wavemon
- Wi-Fi Scanner: https://lizardsystems.com/wi-fi-scanner/
- IEEE 802.11: https://www.ieee802.org/11/
- 去年 Lab 投影片: https://docs.google.com/presentation/d/1U6Ig4Oqgw1llAwnJMaGWxHvsajcHfcH-jbcnrQIv6LE/edit#slide=id.g26b9e2910e6_1_26