

Homework #10

Due Time: 2024/05/06 (Mon.) 21:59

Contact TAs: vegetable@csie.ntu.edu.tw

Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please submit your PDF to Gradescope of Homework 10.

Grading

- Total score: 103 points
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = Total score + Tidiness score.

Wireless

- 請盡可能寫出你所知道/查到的內容，我們會依照作答的完整程度及詳細程度評分
- 請務必附上資料來源；如果使用 chatGPT 等 LM 提供的資訊，請不要全部照抄，請用自己的話寫，並附上 LM 生成回覆的截圖或是連結

1. 課程內容：

請用至多兩句話 (和/或算式) 解釋並回答下面的幾個問題 (20 points in total, 4 points each)：

- 對於一個頻率為 5 GHz 的 Wi-Fi，其波長為何？(相對誤差 10% 以內即可)
- 呈上題，根據 Friis transmission equation，假設 $G_t = G_r = 1$ ，且兩端距離為 1(m)，求 P_r/P_t
- 僅根據 Friis transmission equation，2.4 GHz 和 5 GHz Wi-Fi 哪個訊號隨距離衰減的速率較快？(note: 例如距離同樣增加 x 倍，其功率衰減為 y 倍；請比較兩種頻段的 y 值差異)
- 僅根據 Friis transmission equation，在相同距離、相同發射功率以及相同接收/發射面積下，2.4 GHz 和 5 GHz Wi-Fi 哪個訊號強度較高？ Pr
- bandwidth 和 throughput 的差別為何？

2. 討論題：

Hint: 以下題目建議可以用表格方式作答

(a) Wi-Fi Security (10 points)

在 Lab 上課中，我們有稍微介紹過 IEEE 制定的 Wi-Fi 加密標準，包含 WEP、WPA、WPA2 及 WPA3。請比較這幾個加密方式的優缺點，或是從上一代的標準改進了哪些內容。比較的項目包含但不限於使用的訊息加密演算法、加密演算法的安全性、訊息內容完整性檢驗 (integrity check) 方式、密鑰管理方式、支援的認證方式及可能的攻擊方式或弱點等。

(b) Wi-Fi Generations (10 points)

Wi-Fi 在過去已經推出過許多的世代標準，目前最新的標準是今年推出的 Wi-Fi 7。目前主流的 Wi-Fi 世代主要有 Wi-Fi 5、Wi-Fi 6、Wi-Fi 6E 世代標準，請先寫出其所對應的 IEEE 802.11 標準名稱、支援的傳輸無線電波頻率及理論傳輸速率，接著簡單比較以上三個世代每個世代與前一個世代的差異、改進了哪些功能或是新增了哪些功能。

這個每個資料講的都不一樣？

(c) Wi-Fi Channels (10 points)

我們知道 Wi-Fi 的主流世代標準，主要支援了 2.4 GHz、5 GHz 及 6 GHz 的通訊頻道，而這幾個頻道各自有其優缺點，因此，請先比較這三種主流 Wi-Fi 通訊頻道的優缺點，比較的項目包含但不限於傳輸速率、頻道壅塞程度、訊號覆蓋範圍大小及訊號易被阻擋的程度等。接著，由於 6 GHz 的頻道是較新的 Wi-Fi 6E 標準才開始支援的，請根據你查到的資料，簡單說明為什麼 IEEE 會選擇為 Wi-Fi 加入新的頻道？

(d) AP Working Mode (10 points)

在 Lab 中，我們有介紹過我們系館使用的 Ruckus AP 支援 standalone mode 及 controller mode，而目前我們系館是採用 controller mode 搭配 AP controller 管理所有的 AP。雖然不同品牌所推出的 AP 可能會有各自支援的模式及可以使用的 AP controller，但大多數商業用途的 AP 至少都會包含 standalone mode 及 controller mode 兩種運作模式 (不同品牌的產品可能會有不同的模式名稱，不過基本上的概念相似)。因此，請簡單比較這兩種模式各自適合在什麼樣的環境及情境下使用 (請描述這兩種模式各自適用的環境，例如裝置數量、範圍等資訊，並說明為什麼會比較適合)。

3. 問答題：

(a) SSID (24 points) AP 的 MAC address

- (1) 請簡述 SSID 與 BSSID 分別是什麼？兩者之間是什麼關係？(6 points)
- (2) 同一個 AP 是否有可能同時有很多 SSID？不同 AP 是否有可能共用同一個 SSID？如果可以，請稍微描述一下可能的情境，如果不行，請解釋原因。(6 points)
- (3) Evil Twin 是一個與 SSID 相關的問題，請簡述其攻擊原理並提供一種防止此攻擊的方式。(6 points)
- (4) 如果同時偵測到多個使用同一個 SSID 的 AP(相同網路)，請問這時候裝置如何判斷要連到哪個 AP 嗎？(6 points)

(b) AP location (6 points)

近幾年有越來越多人來到系館修課，隨著人數的上升，對 Wi-Fi 的需求也越來越高，以下附圖 (Figure 1) 為 103 教室的俯視圖，藍色的位置是目前 103 教室兩台 AP 的位置。請問如果可以多擺放一台 AP，你會將 AP 擺在 103 教室的哪一個位置？為什麼？(6 points)

放在牆邊不會很浪費嗎？

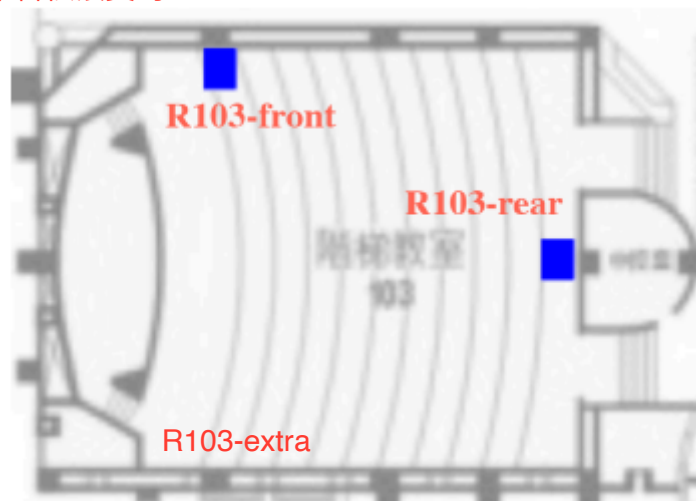


Figure 1: AP locations in R103

4. 實作題：

Enterprise: 要有 user

以下題目皆不限定作答的作業系統。

(a) Connect to WiFi with terminal (5 points)

請透過 terminal 以文字指令連接身邊附近的 Wi-Fi 網路，並說明你是怎麼做到的，並附上證明 (可以連上後去 ping 某個網站)。(提示：Windows 可以用 netsh)

(b) 無線加密方式 (5 points)

目前系館網路 (csie、csie-5g) 使用的是哪一種加密方式？請簡述你是如何判斷的？

WPA2 / AES