NASA hw10 繳交版

Author: B12705014陳泊華

1

(a) Consider the speed of light 3* 10^ 8(m/s) and the given frequency 5GHz = 5*10^6, putting them into the formula and solve c=fλ, we obtain an estimate of λ 0.06m.

(b) According to the formula mentioned in class, plugging in antenna gain Gt = Gr = 1 and λ = 0.06m from (a), we obtain Pr/Pt = (0.06/4pi)^2

$$P_r = \frac{P_t G_t A_e}{4\pi d^2} = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2}$$

(c) According to Friis formula and (b), we can observe that the signal attenuation rate (1-Pr/Pt, with r representing the receiver side, t representing the transmission side) is proportional to the distance d. Moreover, since the wavelength of 2.4GHz Wi-Fi is larger, and wavelength is inversely proportional to the signal attenuation rate, it has a lower signal attenuation rate compared to 5GHz Wi-Fi.

(d) Consider the Friis formula, we can observe that given the same distance, transmission power and area , the theoretic signal strength (Pr) would be proportionate to the power of wavelength. From c=fλ, we know that the wavelength of 2.4GHz is higher, and hence have higher signal strength.

*Pr應該跟wave^2成正比

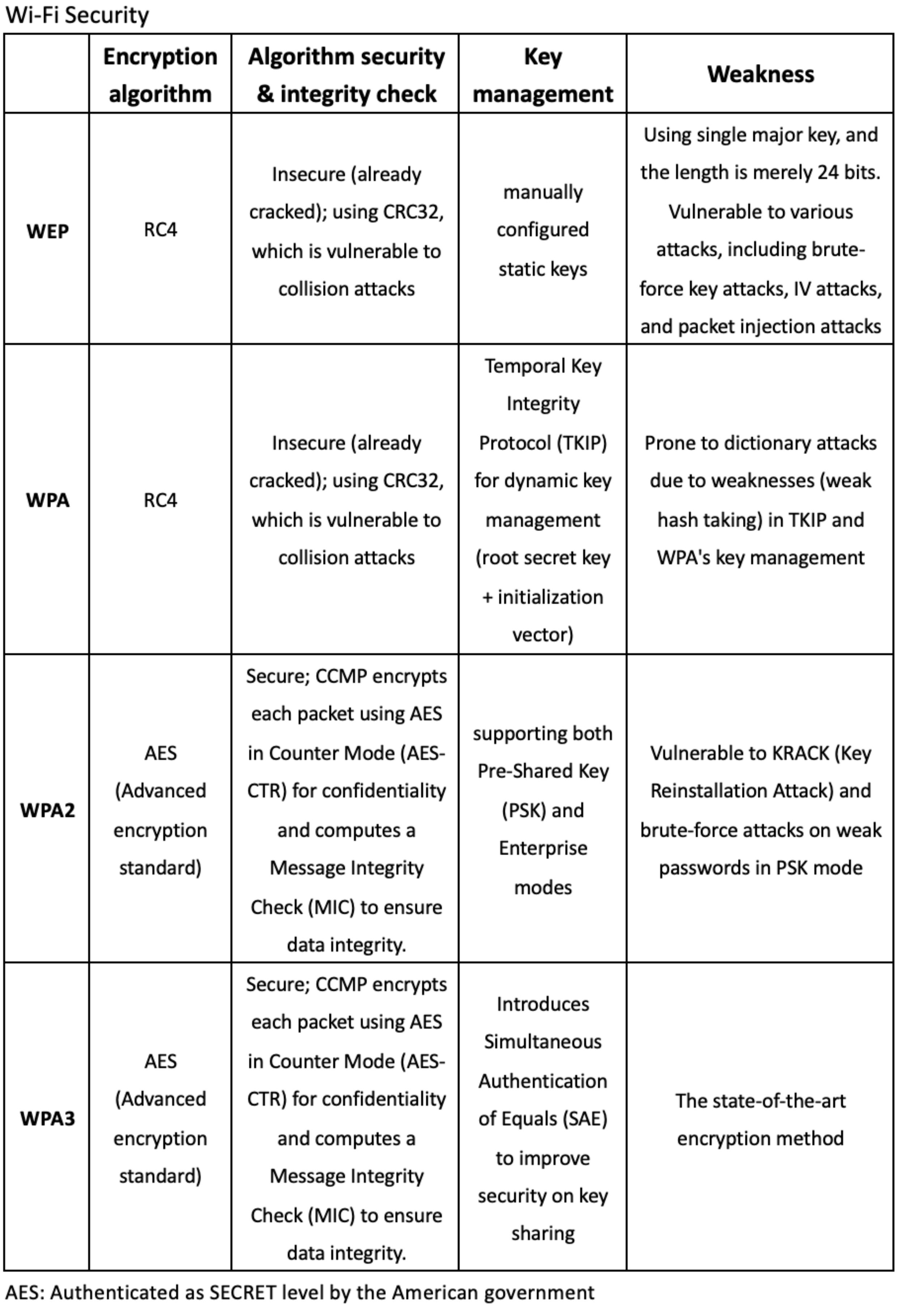
(e) Bandwidth generally determines how high of a network throughput rate the network can possibly handle. That is to say, bandwidth aims to describe capacity, while throughput is a practical criterion that measures actual packet delivery rate.

reference:
(i) Bandwidth vs. throughput
https://www.manageengine.com/products/netflow/network-throughput-vs-bandwidth.html (https://www.manageengine.com/products/netflow/network-throughput-vs-bandwidth.html)

(ii) Frequency hopping https://zh.wikipedia.org/zh-tw/跳频扩频 (https://zh.wikipedia.org/zh-tw/%E8%B7%B3%E9%A2%91%E6%89%A9%E9%A2%91)
(iii) Friis formula
https://uomustansiriyah.edu.iq/media/lectures/5/5_2018_03_08!11_25_59_PM.pdf (https://uomustansiriyah.edu.iq/media/lectures/5/5_2018_03_08!11_25_59_PM.pdf)

2

(a)

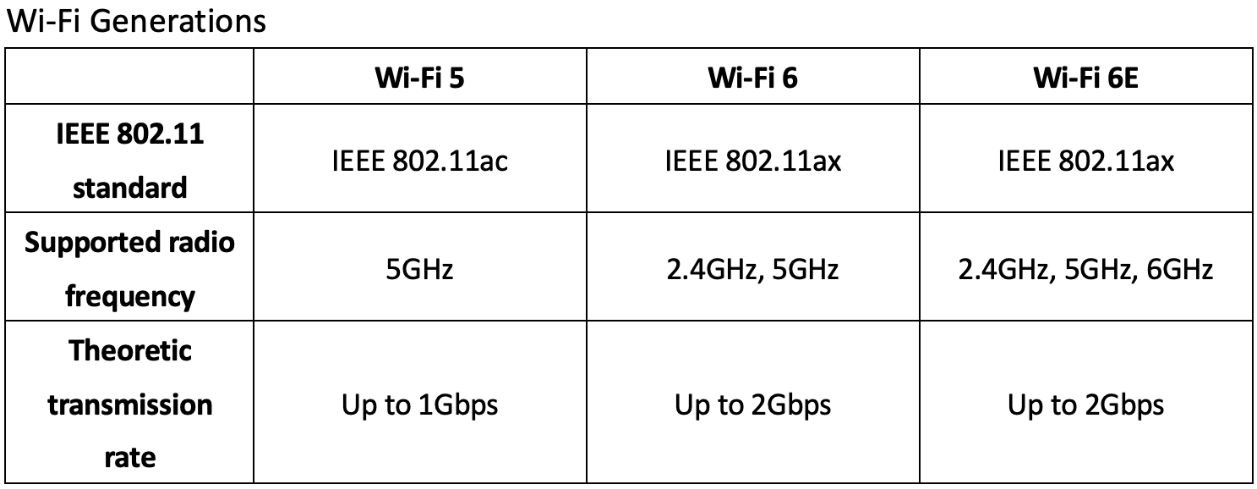


Wi-Fi Security

	Encryption algorithm	Algorithm security & integrity check	Key management	Weakness
WEP	RC4	Insecure (already cracked); using CRC32, which is vulnerable to collision attacks	manually configured static keys	Using single major key, and the length is merely 24 bits. Vulnerable to various attacks, including brute-force key attacks, IV attacks, and packet injection attacks
WPA	RC4	Insecure (already cracked); using CRC32, which is vulnerable to collision attacks	Temporal Key Integrity Protocol (TKIP) for dynamic key management (root secret key + initialization vector)	Prone to dictionary attacks due to weaknesses (weak hash taking) in TKIP and WPA's key management
WPA2	AES (Advanced encryption standard)	Secure; CCMP encrypts each packet using AES in Counter Mode (AES-CTR) for confidentiality and computes a Message Integrity Check (MIC) to ensure data integrity.	supporting both Pre-Shared Key (PSK) and Enterprise modes	Vulnerable to KRACK (Key Reinstallation Attack) and brute-force attacks on weak passwords in PSK mode
WPA3	AES (Advanced encryption standard)	Secure; CCMP encrypts each packet using AES in Counter Mode (AES-CTR) for confidentiality and computes a Message Integrity Check (MIC) to ensure data integrity.	Introduces Simultaneous Authentication of Equals (SAE) to improve security on key sharing	The state-of-the-art encryption method

AES: Authenticated as SECRET level by the American government

(b)

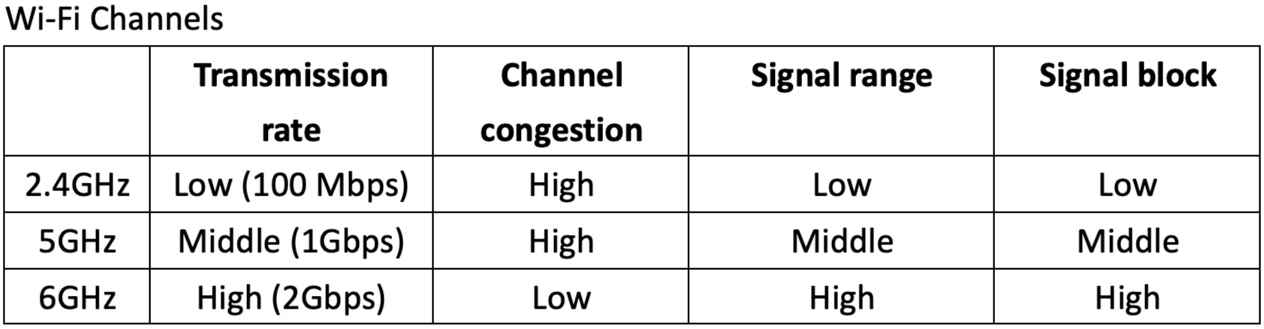


Wi-Fi Generations

	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E
IEEE 802.11 standard	IEEE 802.11ac	IEEE 802.11ax	IEEE 802.11ax
Supported radio frequency	5GHz	2.4GHz, 5GHz	2.4GHz, 5GHz, 6GHz
Theoretic transmission rate	Up to 1Gbps	Up to 2Gbps	Up to 2Gbps

Difference / improvements
Wi-Fi 6 introduces higher bandwidth, OFDM (Orthogonal Frequency Division Multiplexing), antenna and MIMO technology to achieve higher theoretic transmission rate, also adding more frequency spectrum support; Wi-Fi 6E further introduces wider bandwidth to decrease interference and channel congestion.

(c)



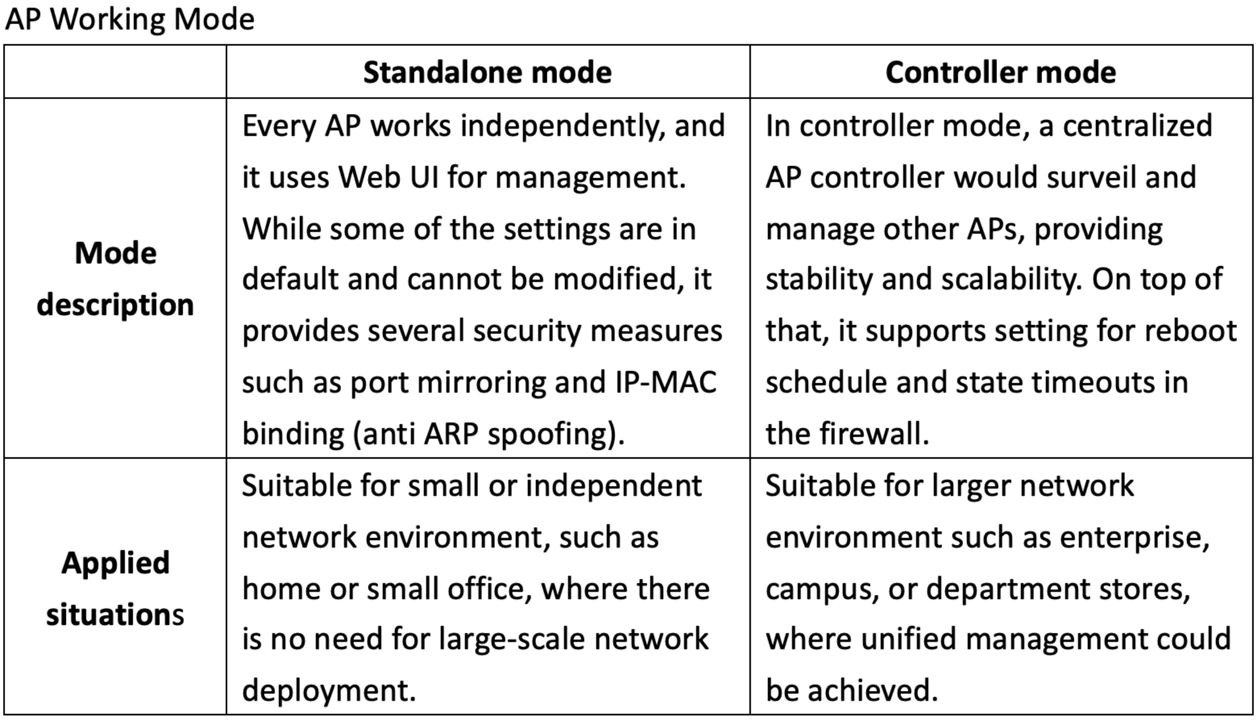
Wi-Fi Channels

	Transmission rate	Channel congestion	Signal range	Signal block
2.4GHz	Low (100 Mbps)	High	Low	Low
5GHz	Middle (1Gbps)	High	Middle	Middle
6GHz	High (2Gbps)	Low	High	High

signal range: the longer the wavelength, the bigger the signal range
signal block: the longer the wavelength, the lower the signal block

The reason why IEEE add 6GHz Wi-Fi channel in Wi-Fi 6E is because it provides a wider bandwidth (7 more 160MHz channel), providing additional spectrum and capabilities to meet the growing demands for high-performance wireless connectivity.

(d)



AP Working Mode

	Standalone mode	Controller mode
Mode description	Every AP works independently, and it uses Web UI for management. While some of the settings are in default and cannot be modified, it provides several security measures such as port mirroring and IP-MAC binding (anti ARP spoofing).	In controller mode, a centralized AP controller would surveil and manage other APs, providing stability and scalability. On top of that, it supports setting for reboot schedule and state timeouts in the firewall.
Applied situations	Suitable for small or independent network environment, such as home or small office, where there is no need for large-scale network deployment.	Suitable for larger network environment such as enterprise, campus, or department stores, where unified management could be achieved.

reference:
(i) network security (WEP, WPA, WPA2, WPA3)
https://www.trendmicro.com/zh_hk/what-is/network-security/network-security-basics.html (https://www.trendmicro.com/zh_hk/what-is/network-security/network-security-basics.html)
(ii) standalone vs. controller mode
https://www.tp-link.com/us/support/faq/3357/ (https://www.tp-link.com/us/support/faq/3357/)
(iii) port mirroring
https://www.tp-link.com/tw/support/faq/3924/ (https://www.tp-link.com/tw/support/faq/3924/)
(iv) Wi-Fi 6 vs. Wi-Fi 6E
https://www.tp-link.com/us/blog/86/ (https://www.tp-link.com/us/blog/86/)
(v) 2.4G vs. 5G vs. 6G
https://www.intel.com/content/www/us/en/products/docs/wireless/2-4-vs-5ghz.html (https://www.intel.com/content/www/us/en/products/docs/wireless/2-4-vs-5ghz.html)
(vi) Wi-Fi 6
https://zh.wikipedia.org/zh-tw/Wi-Fi_6 (https://zh.wikipedia.org/zh-tw/Wi-Fi_6)
(vii) Wi-Fi 7
https://www.tp-link.com/tw/wifi7/ (https://www.tp-link.com/tw/wifi7/)
(viii) AES encryption mechanism
https://zh.wikipedia.org/wiki/高级加密标准 (https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86)
(viiii) TKIP
https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol (https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol)
(X) KRACK https://zh.wikipedia.org/zh-tw/KRACK (https://zh.wikipedia.org/zh-tw/KRACK)
(Xi) MIMO https://zh.wikipedia.org/zh-tw/MIMO (https://zh.wikipedia.org/zh-tw/MIMO)
(Xii) RC4 mechanism

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
(https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf)
TKIP encryption algorithm

3

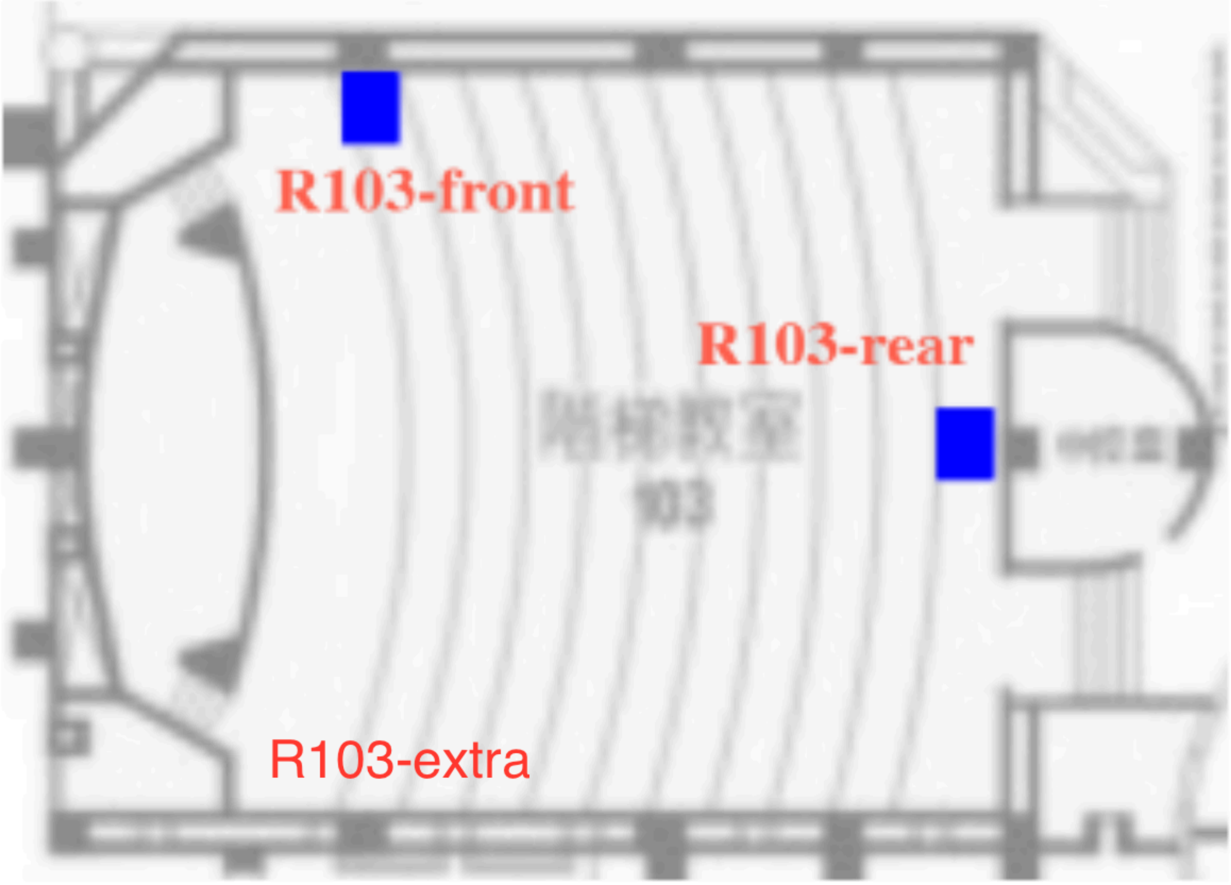
(a)
(1) SSID refers to "service set identifier". It is manually distributed where user can identify and connect to the specific wireless network. BSSID, on the other hand, stands for "basic service set identifier", which is a automatically generated identifier to identify access points (usually the MAC address of the AP).

(2) Yes. A single AP may simultaneously broadcast multiple SSID to provide different network services and access permission. On the other hand, different AP can share the same AP, where it allows bigger coverage (roaming) or higher stability.

(3) Evil twin is a kind of network security attack, where attackers create a fake access point using the same SSID as a normal access point to let the victim connect to the fake one and steal their private information. There are several ways to prevent this attack, including disabling auto connection, using HTTPs instead of HTTP, applying VPN, establishing good user habit (e.g. prevent logging in financial accounts with public Wi-Fi), etc.

(4) Usually, a device would choose AP with same SSID based on signal strength, which generally indicates better connectivity. If signal strength is similar, devices may consider other factors such as network congestion or past connecting records.

(b) I would put the extra AP in the following position assuming that users in the building are evenly distributed. Considerations include lessening connection distance and reducing signal and power attenuation, to create better user experience.



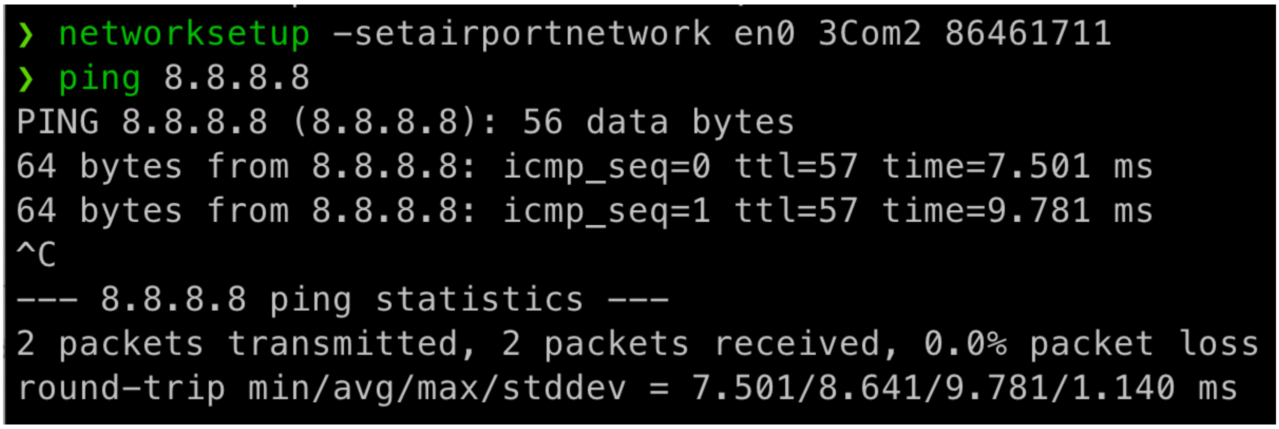
references:
(i) SSID vs. AP
https://community.zyxel.com/en/discussion/19706/understanding-the-difference-between-ap-and-ssid (https://community.zyxel.com/en/discussion/19706/understanding-the-difference-between-ap-and-ssid)
(ii) evil twin attack
https://www.kaspersky.com.tw/resource-center/preemptive-safety/evil-twin-attacks (https://www.kaspersky.com.tw/resource-center/preemptive-safety/evil-twin-attacks)
(iii) how do devices choose AP
https://www.quora.com/How-does-a-computer-decide-which-wireless-access-point-to-connect-to-assuming-all-are-on-the-same-network (https://www.quora.com/How-does-a-computer-decide-which-wireless-access-point-to-connect-to-assuming-all-are-on-the-same-network)

4

(a)

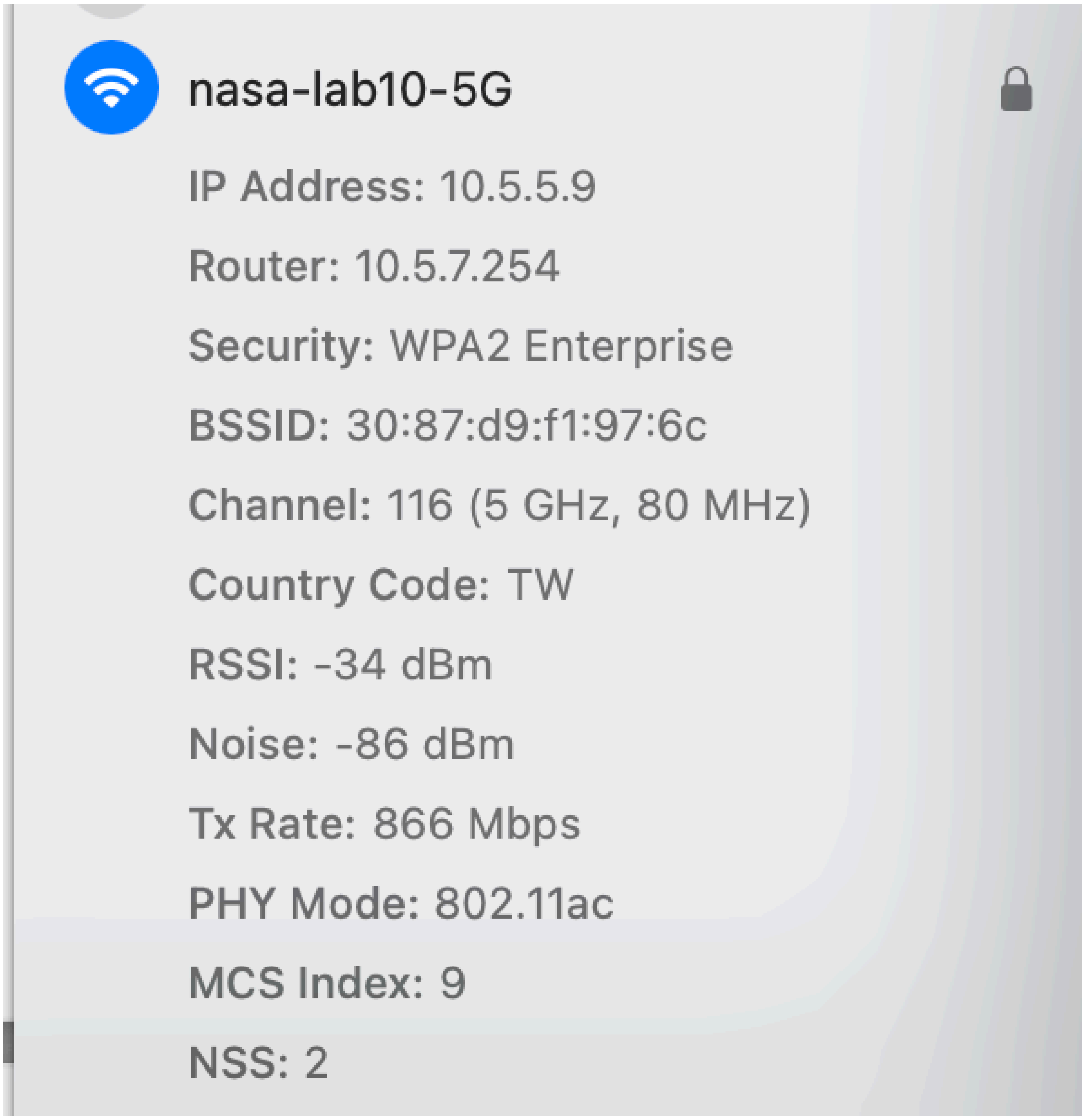
```
$ sudo networksetup -setairportnetwork en0 3Com2 86461711
```

First, forget the target network; then use the networksetup command in MAC PC and connect to Wi-Fi.



```
❯ networksetup -setairportnetwork en0 3Com2 86461711
❯ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=57 time=7.501 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=9.781 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.501/8.641/9.781/1.140 ms
```

(b) Deduce that the WPA2 Enterprise as its encryption method by referring to the screenshot for nasa-lab10-5G(since I wasn't able to make it to the building when doing this question, sorry...)



nasa-lab10-5G

IP Address: 10.5.5.9

Router: 10.5.7.254

Security: WPA2 Enterprise

BSSID: 30:87:d9:f1:97:6c

Channel: 116 (5 GHz, 80 MHz)

Country Code: TW

RSSI: -34 dBm

Noise: -86 dBm

Tx Rate: 866 Mbps

PHY Mode: 802.11ac

MCS Index: 9

NSS: 2

reference:
(i) SNR https://ithelp.ithome.com.tw/articles/10227252?sc=rss.iron (https://ithelp.ithome.com.tw/articles/10227252?sc=rss.iron)
(ii) nmcli

https://www.liquidweb.com/kb/how-to-install-and-configure-nmcli/ (https://www.liquidweb.com/kb/how-to-install-and-configure-nmcli/)

(iii) network setup

https://www.hexnode.com/blogs/connecting-the-dots-guide-to-manage-network-settings-on-macos/ (https://www.hexnode.com/blogs/connecting-the-dots-guide-to-manage-network-settings-on-macos/)

https://gist.github.com/jjnilton/add1eeeb3a9616f53e4c (https://gist.github.com/jjnilton/add1eeeb3a9616f53e4c)

(iv) TA slides