Network Administration HW6

B04705003 資工三 林子雋

1 Reference

1.1 Wi-Fi Authentication

1. https://www.tp-link.com/us/FAQ-500.html
2. https://www.wikiwand.com/en/Wi-Fi_Protected_Access

1.2 Wi-Fi Encryption

1. Find the Wireless Security Information (e.g., SSID, Network key, etc.) for Windows
2. https://www.wikiwand.com/en/Wired_Equivalent_Privacy#/Encryption_details
3. https://www.wikiwand.com/en/Wi-Fi_Protected_Access
4. https://www.wikiwand.com/en/RC4
5. https://www.wikiwand.com/en/IEEE_802.11i-2004#/Four-way_handshake

1.3 WPA3

1. https://www.digitaltrends.com/computing/what-is-wpa3/

1.4 Seeing is Believing

1. http://www.rhyshaden.com/8021x.htm
2. http://kezeodsnx.pixnet.net/blog/post/33952172-802.1x-%E4%BB%8B%E7%B4%B9
3. Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and
4. https://hpbn.co/transport-layer-security-tls/
5. what is the difference between Inner and outer authentication? Empirical Experience
6. https://sites.google.com/site/amitsciscozone/home/switching/peap---protected-eap-pr
7. https://hpbn.co/transport-layer-security-tls/

2 Problem

2.1 Wi-Fi Authentication

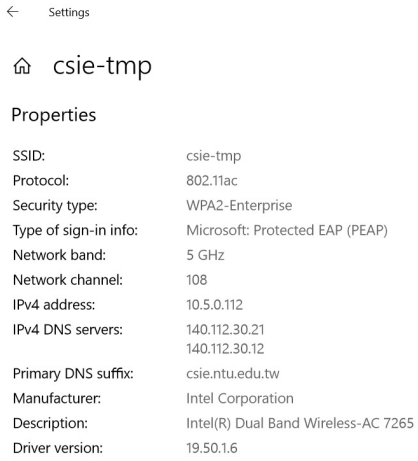
1. See Table 1.

Table 1: Difference between WPA-Personal and WPA-Enterprise

	WPA-Personal	WPA-Enterprise
Environment	Home networks	Business environment
Management	Wireless access should be individually managed	Wireless can be individualized or centralized controlled.
Authentication	One password applies to all users(using pre-shared key) and passwords are stored on the wireless clients	Supports 802.1x RADIUS authentication where a RADIUS server is deployed and passwords are stored in the RADIUS server

2. They both use WPA-Enterprise to authenticate users. See Figure 1 and 2.

Figure 1: csie authentication



2.2 Wi-Fi Encryption

1. See Table 2.

2. Both of them use AES cipher. See Figure 3 and 4

Figure 2: csie-5G authentication

Table 2: Encryption protocol

WEP	RC4 stream
WPA	RC4 stream
WPA2	AES block

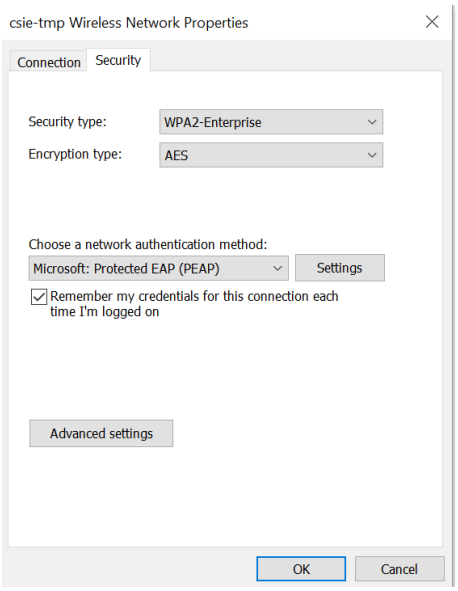


Figure 3: csie cipher

2.3 WPA3

1. **Individualized data encryption**: your individual connection to an open wireless network will be encrypted, even if the network is not protected by a password.

2. **192-bit security suite**: WPA3 uses CNSA(Commercial National Security Algo-

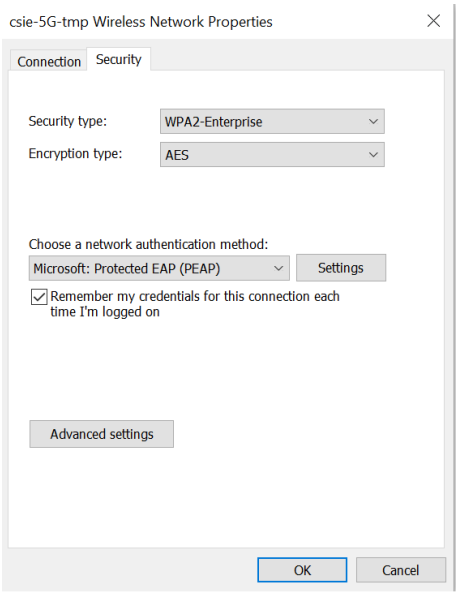


Figure 4: csie 5G cipher

rithms), which meets security requirements for institution such like government.

3. **Updated handshake**: The updated standard adds extra protection against password-crakers.

2.4 Seeing is Believing

1. **Filtered packages**: See Figure 5
2. **Identity showni**: See Figure 6
3. (a) Stage 1: The frame number is 1, 2
   (b) Stage 2: Negotiation phase: frame 4-14
   (c) Stage 3: Application data sent: frame 15-22
   (d) Stage 4: The frame number is 23
   (e) Stage 5: The frame number are 24-27.

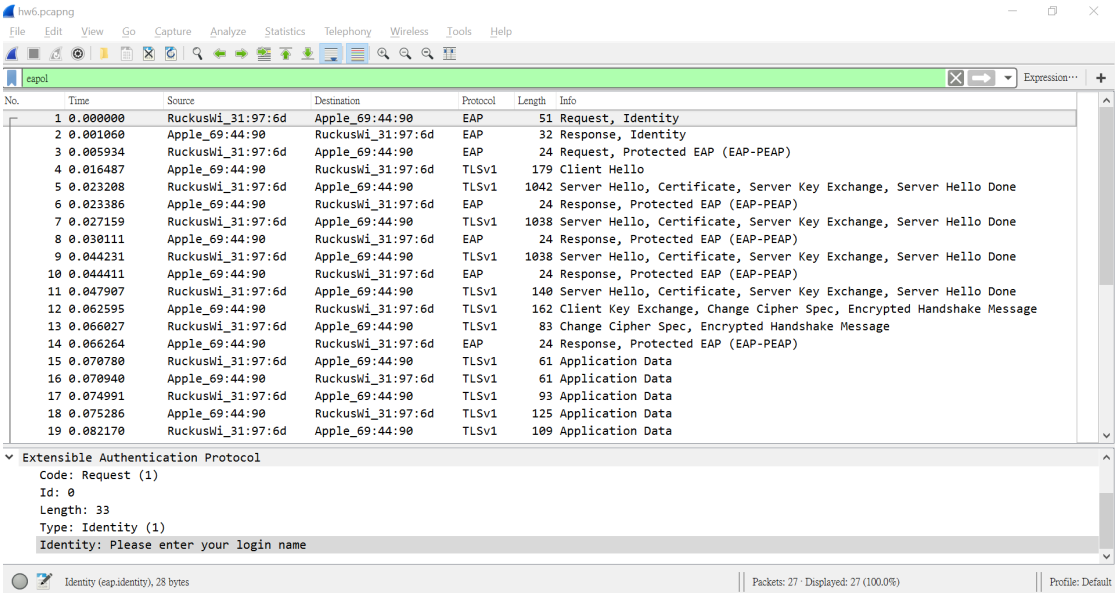


Figure 5: Screenshot 3.

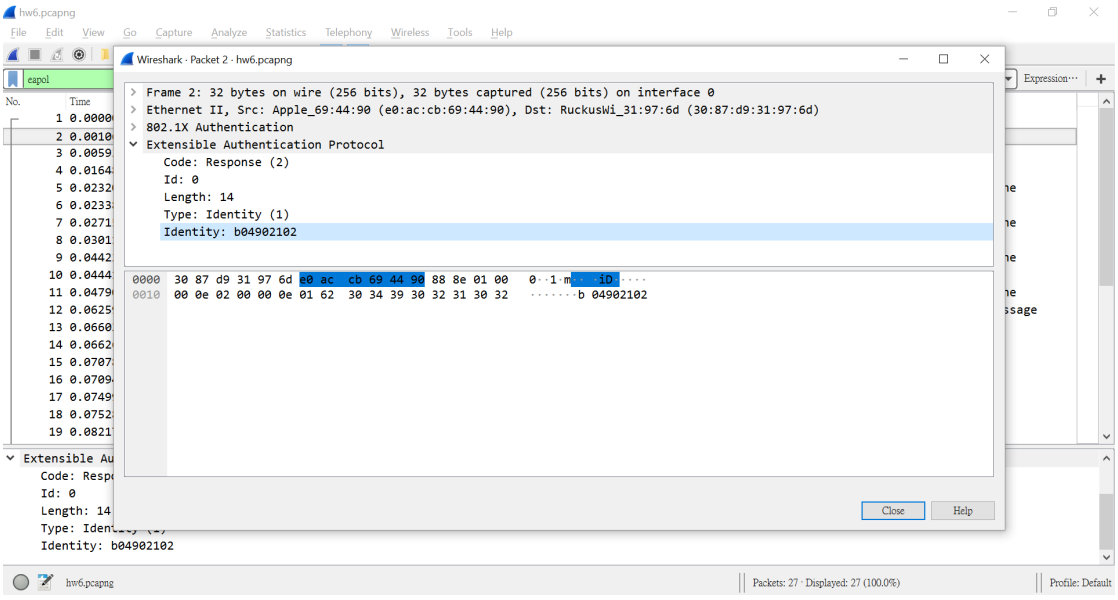


Figure 6: Screenshot 4.