Network Administration

1. WPA2/WPA3

(a) Forward Secrecy:
WPA3 leverages SAE (Simultaneous Authentication of Equals) handshake to offer forward secrecy, a security feature that prevents attackers from decrypting old captured traffic even if they ever learned the password of a network.

(b) 192-bit Encryption:
For critical Wi-Fi networks handling sensitive information (such as government and industrial organizations), WPA3 can protect their Wi-Fi connections with 192-bit encryption.

References

[1] WPA3 Standard Officially Launches With New Wi-Fi Security Features

[2] Forward Security

2. SSID/BSSID

An SSID is the name for a Wi-Fi network. On the other hand, BSSID can be roughly explained as the AP's mac address. It's possible for an access point to have multiple SSIDs, usually with the aid of VLAN tagging. Also, it's possible for an ap to have multiple BSSIDs if we set up Virtual APs. Multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the MAC protocol layer that includes a unique BSSID and SSID. To sum up, a single AP can have multiple SSIDs and BSSIDs.

References

[1] What is SSID, BSSID, ESSID, and HESSID?

[2] The concepts of WLAN

[3] Overview of Wireless Virtual Access Point (VAP)

3. Channel

Wifi has serveral frequency bands, like 2.4GHz and 5GHz. A frequency band can be divided into serveral channels. For instance, 2.4GHz is theoretically divided into 14 channels according to IEEE 802.11, inclusive of 2.412GHz, 2.417GHz and so on. However, there're only 11 channels of 2.4GHz Wifi in Taiwan.

Co-channel interference occurs when 2 or more AP's are using the same channel. It causes unnecessary contention as all AP's and clients will be forced to defer transmissions until the medium is clear.

Adjacent channel interference is more serious and it occurs when 2 or more AP's are on overlapping channels. It affects the quality of transmission, requiring data re-transmissions.

References

[1] 2.4 GHz Wifi Test

[2] What is Co and Adjacent Channel Interference

[3] Co-Channel Interference

[4] Adjacent-channel Interference

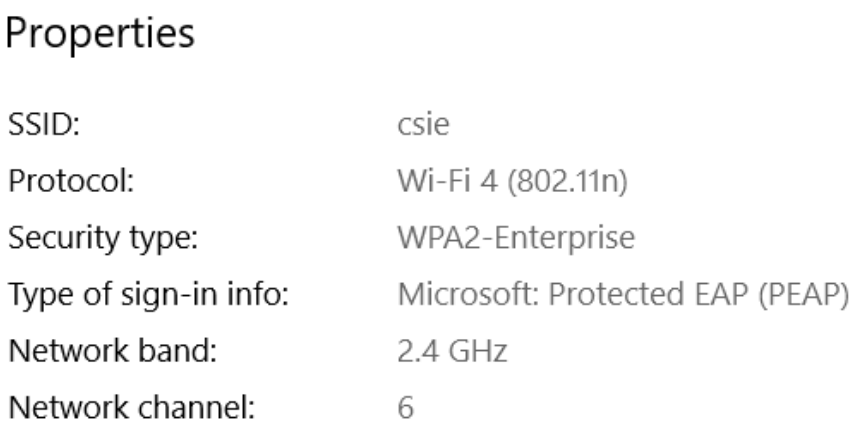
4. WPA2 Enterprise/Personal

WPA2-Personal provides a Pre-Shard Key (PSK) feature for those who are not able to afford the cost of an authentication server. All users are using the same password to access the Internet.

On the other hand, WPA2-Enterprise requires a RADIUS authentication server. There is no single public password, each user is authenticated with an unique set of account and password.

'csie' is a WPA2-Enterprise network because it requires different sets of account and password for each user.

Additionally, the information of wifi can be looked up within windows 10:



References

[1] Which encrypt method should we use for Wifi Router?

[2] enWiki-Wi-Fi Protected Access

5. PSK/EAP/PEAP

PSK has been roughly explained in Problem 4.

EAP is an authentication framework that provides some common functions and negotiations of authentication methods, in which it can be encapsulated. MD5, TLS, and PEAP are some examples of EAP methods.

PEAP authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS) session, over which the WLAN user, WLAN stations and the authentication server can authenticate themselves.

References

[1] The introduction of 802.1x

[2] The introduction of WPA/WPA2

[3] Protected Extensible Authentication Protocol

6. Wi-fi Certificate

The WIFI Certificate is used to provide users secure authentication against the trusted RADIUS server and prevent them from connecting to malicious RADIUS server. Having certificate installed, if someone decides to steal his/her AD credentials by installing a rogue RADIUS server, the device will pop up with a warning that RADIUS certificate is not trusted.

CA is short for Certificate authority, an entity that issues digital certificates. A CA acts as a trusted third party – trusted both by the owner of the certificate and by the party relying upon the certificate. One particularly common use for CA is to sign SSL certificates used in HTTPS.

References

[1] My school wifi asks to 'trust' a certificate on Iphone's, does it this allow them to view SSL traffic?

[2] enWiki-Certificate Authority

System Administration

1. I just messed up ...

(a) Commands:

```
$ sudo testdisk
> Create
> Proceed
> EFI GPT
> Advanced
> (Choose the second partition and change its type to 'EFI system'->'ext4')
> List
> (go into /home/nasa)
```

We can find the deleted files after the above steps. Follow the instruction to restore those files.

(b) I tried to use systemd to restart ssh and rsync and it worked all properly. Then I typed 'systemctl status' and found out the status is 'degraded'. Using that keyword, I found a post that explained the term means some of the services failed to start, and it demonstrated a command, 'systemctl –failed' to list the failed services.

I observed the failed service was apache2. Then, I typed 'service apache2 status' to find out which part went wrong. It turned out to be the '/etc/apache2/sites-enabled/000-default.conf' has a redundant ';'. Delete it and restart apache2, everything got back on track.

(c) The systemd service file can be divided into three necessary blocks: Unit, Service, and Install. The following is the explanation of my service file:

- Unit:
  After – The order in which units are started. Since the program requires apache2 to work, 'After' should includes apache2.service. Likewise, 'Wants' should includes apache2.service.
- Service:
  Due to the program limited on which directory it must be launched (or we will run into 'length_error'error), I set 'WorkingDirectory' as /home/nasa, and ExecStart as /home/nasa/web. 'Type' is trivial, so I set it as simple.
- Install:
  I set WantedBy as multi-user.target so that it will run in the multi-user shell.

After the file was set properly, I named it 'web_onboot.service' and moved it to /etc/systemd/system/; 'systemctl daemon-reload' and 'systemctl start web_onboot' or reboot. Accordingly, it should function normally.

References

[1] How to Recover deleted files in Ubuntu through TestDisk

[2] Tutorial of Systemd

[3] Usage of Systemd

[4] Executing chdir before starting systemd service

[5] Trying to change WorkingDirectory of Systemd Service Unit

2. Web terminology

(a) A proxy server is an intermediary server that forwards requests for content from multiple clients to different servers across the Internet. A reverse proxy server, on the contrary, is a type of proxy server that typically sits behind the firewall in a private network and directs client requests to the appropriate backend server. The reverse proxy server can help improve security by intercepting requests headed for backend servers, thereby protecting their identities and acting as an additional defense against security attacks.

(b)
- A Model is data or business logic used by a proram, like a database, file, or a simple object like an icon.
- A View is the means of displaying objects within an application so that the users can see.
- A controller accepts input and performs the corresponding update to the models and views.

References

[1] What Is a Reverse Proxy Server?

[2] MVC Definition

[3] MVC introduction

3. Try MySQL

(a)

```
> USE sahw7;
> SELECT name,since,origin FROM restaurants;
```

(b)

```
> UPDATE restaurants SET nickname="麥當當" WHERE id=1;
> UPDATE restaurants SET nickname="啃雞雞" WHERE id=2;
> UPDATE restaurants SET nickname="火烤就是美味" WHERE id=3;
```

(c)

```
> CREATE TABLE dishes (id INT AUTO_INCREMENT NOT NULL, \
> name VARCHAR(40), price INT, restaurant_id INT, PRIMARY KEY (id));
```

(d)

```
> INSERT INTO dishes (name, price, restaurant_id) \
> VALUES ("Fried Chicken",87,1);
```

(e)

```
> SELECT r.name, r.nickname, c.name, c.price from restaurants r, \
> (SELECT d.name, d.price, d.restaurant_id from dishes d) c \
> WHERE r.id = c.restaurant_id ORDER BY c.price DESC;
```

```
MariaDB [sahw7]> SELECT r.name, r.nickname, c.name, c.price from restaurants r,
(SELECT d.name, d.price, d.restaurant_id from dishes d) c WHERE r.id = c.restaur
ant_id ORDER BY c.price DESC;
+-------------+--------------------+---------------+-------+
| name        | nickname           | name          | price |
+-------------+--------------------+---------------+-------+
| Burger King | 火烤就是美味       | Fried Chicken |    99 |
| McDonald's  | 麥當當             | Fried Chicken |    87 |
| KFC         | 啃雞雞             | Fried Chicken |    79 |
| McDonald's  | 麥當當             | French fries  |    55 |
| Burger King | 火烤就是美味       | French fries  |    49 |
| KFC         | 啃雞雞             | French fries  |    45 |
+-------------+--------------------+---------------+-------+
6 rows in set (0.00 sec)
```

References

[1] Creating and Selecting a Database

[2] MySQL UPDATE

[3] MySQL CREATE TABLES

[4] MySQL INSERT

[5] MySQL ORDER BY

SPECIAL THANKS: Prof. Winston Hsu and amjltc295

4. More LAMP

a. Run a website:

1 Configure network

2 Install php7, httpd

3 Configure Firewall

4 Write a PHP code saving as 'index.php' in /var/www/html:

```
<?php echo "Welcome!"; ?>
```

b. GET parameters:

```
<?php echo "Welcome! ".$_GET['name']; ?>
```

c. Directive: Edit '/etc/httpd/conf/httpd.conf'. In <Directory "/var/www/html/">block I added two lines, 'Require all denied' and 'Require ip 192.168.50.209' (it's my host ip).

d. Apache Virtual Host: Virtual Host is the practice of running more than one website on a single machine. It can be 'IP-based', meaning that each website has a different IP address, or 'name-based', meaning that multiple names running on each IP address.

References

[1] How do I require an IP range instead of 1 IP?

[2] VirtualHost Examples