NASA Homework #7

Student Name: 林楷恩
Student ID: b07902075

Network Administration

1. WPA2/WPA3

1. **Simultaneous Authentication of Equals (SAE)**: Pre-shared Key (PSK) in WPA2-Personal is replaced with Simultaneous Authentication of Equals (SAE) in WPA3-personal, which makes it resistant to offline dictionary attack. This allows users to choose a easy-to-remember password without being posed under the risk.
2. **192-bit minimum-strength security protocols**: WPA3-Enterprise offers an optional 192-bit security mode, which provides stronger protecton for industrial, government, or other critical WiFi networks.

*** Reference**

- https://www.wi-fi.org/discover-wi-fi/security
- https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

2. SSID/BSSID

1. - **SSID**: SSID is the name of the network(WLAN), which may consist of multiple access points.
   - **BSSID**: BSSID is a unique identifier to distinguish different access points and their associated clients. By convention, BSSID is often the device's MAC address.
2. - **For SSID**: Yes, an access point can has multiple SSID. We can achieve this by the concept of VLAN, which help distinguish packets in different networks.
   - **For BSSID**: Yes, an access point can has multiple BSSID. For example, an access point with dual band(i.e. 2.4 GHz and 5 GHz) will have two different BSSID for a SSID, one is for 2.4 GHz, while the other is for 5 GHz.

*** References**

- www.juniper.net/documentation/en_US/junos-space-apps/network-director3.1/topics/concept/
- https://www.dummies.com/programming/networking/cisco/multiple-ssids-with-a-single-access-point/
- https://stackoverflow.com/questions/40139849/android-getting-different-bssid-for-the-same-

3. Channel

Channel is a smaller band within WiFi frequency band like 2.4 GHz or 5 GHz. For example, The IEEE standard divides the 2.4 GHz band into 14 separate channels. However, only channel 1, 6, 11 are non-overlapping channels(not interfere with each other), so typically only these three channels will be used.

Co-channel interference occurs when 2 or more AP's are using the same channel. It causes unnecessary latency since all devices should wait until the medium is clear. It reduces the performance of network, but the bandwidth is still managed. However, *Adjacent channel interference* is more serious and occurs when 2 or more AP's are on overlapping channels, for example channel 3 + 4 on the 2.4Ghz band. The network becomes a mess since the two channels cannot negotiate with each other properly, then the data is corrupted and frequent Layer 2 re-transmissions occur.

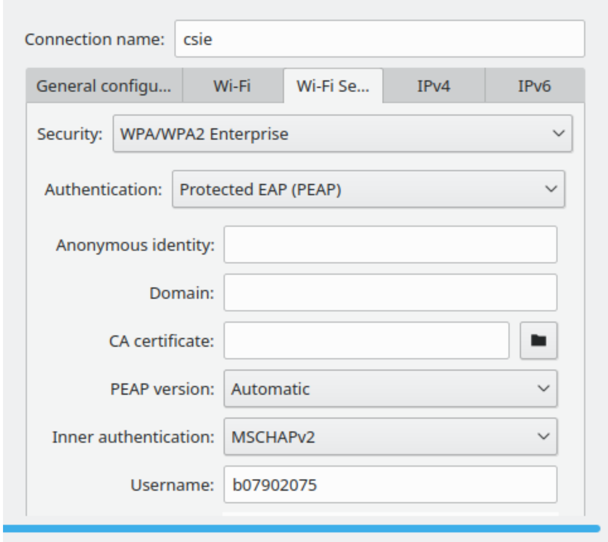
*** References**

- https://www.minim.co/blog/wifi-channels-explained
- https://www.metageek.com/training/resources/adjacent-channel-congestion.html

4. WPA2 Enterprise/Personal

The main difference between WPA2-Personal and WPA2-Enterprise is the authentication method. WPA2-Personal uses **Pre-Shared Keys(PSK)**, while WPA2-Enterprese uses a RADIUS server and a proper authentication method, like EAP.

`csie` use WPA-Enterprise. I obtain this information from Kubuntu's network configuration window:



Connection name: csie

Security: WPA/WPA2 Enterprise

Authentication: Protected EAP (PEAP)

Anonymous identity:

Domain:

CA certificate:

PEAP version: Automatic

Inner authentication: MSCHAPv2

Username: b07902075

*** References**

- https://security.stackexchange.com/questions/35780/why-is-wpa-enterprise-more-secure-than-wpa2

5. PSK/EAP/PEAP

PSK means Pre-Shared Keys, which is a shared secret among certain parties of users. All users use the same password for authenticationi.

EAP(Extensible Authentication Protocol) is an authentication framework. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication. PEAP(Protected Extensible Authentication Protocol) is a version of EAP.

PEAP authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS) session.

With PSK, all users have the same password, while with EAP, there is a authentication server requiring users to give a special key to complete authentication. And in PEAP, this process is under the protectioin of TLS, which is more secure.

Since the security level of PSK is lower, it is more likely to be used in personal network.

*** References**

- https://kb.iu.edu/d/aodl
- https://searchsecurity.techtarget.com/definition/PEAP-Protected-Extensible-Authentication-Protocol

- https://searchsecurity.techtarget.com/definition/PEAP-Protected-Extensible-Authentication-Protocol

6. Wi-fi Certificate

A Wi-fi certificate certifies the ownership of a public key, providing cryptographically-backed assurance to the visitor that the device they're connecting to genuinely belongs to the organization they think they're connecting with.

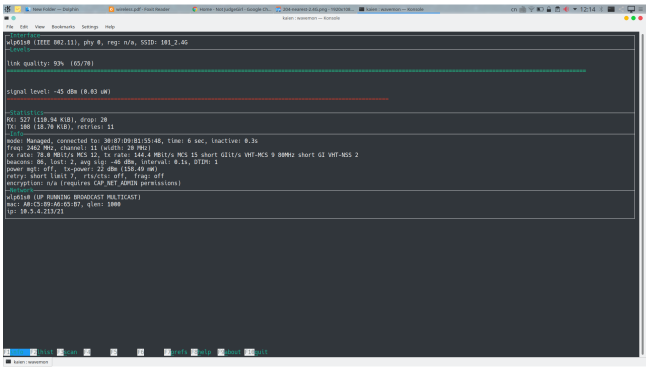
A Certificate Authority (CA) is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. This allows the relying parties to rely upon signatures or on assertions made about the private key that corresponds to the certified public key.

* Reference

- https://support.dnsimple.com/articles/what-is-certificate-authority/
- https://en.wikipedia.org/wiki/Certificate_authority

7. Lab

I use *Wavemon* to obtain the following information, and here are some of the screenshots:



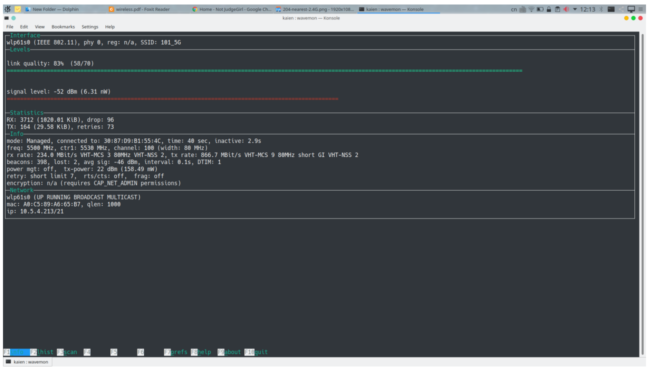
New Folder — Dolphin
wireless.pdf - Foxit Reader
Home - Not JudgeGirl - Google Ch...
204-nearest-2.4G.png - 1920x108...
kaien : wavemon — Konsole
File
Edit
View
Bookmarks
Settings
Help

```
─Interface─
wlp61s0 (IEEE 802.11), phy 0, reg: n/a, SSID: 101_2.4G
─Levels─

link quality: 93%  (65/70)


signal level: -45 dBm (0.03 uW)


─Statistics─
RX: 527 (110.94 KiB), drop: 20
TX: 108 (18.70 KiB), retries: 11
─Info─
mode: Managed, connected to: 30:87:D9:B1:55:48, time: 6 sec, inactive: 0.3s
freq: 2462 MHz, channel: 11 (width: 20 MHz)
rx rate: 78.0 MBit/s MCS 12, tx rate: 144.4 MBit/s MCS 15 short GIit/s VHT-MCS 9 80MHz short GI VHT-NSS 2
beacons: 86, lost: 2, avg sig: -46 dBm, interval: 0.1s, DTIM: 1
power mgt: off,  tx-power: 22 dBm (158.49 mW)
retry: short limit 7,  rts/cts: off,  frag: off
encryption: n/a (requires CAP_NET_ADMIN permissions)
─Network─
wlp61s0 (UP RUNNING BROADCAST MULTICAST)
mac: A0:C5:89:A6:65:B7, qlen: 1000
ip: 10.5.4.213/21
```



New Folder — Dolphin
wireless.pdf - Foxit Reader
Home - Not JudgeGirl - Google Ch...
204-nearest-2.4G.png - 1920x108...
kaien : wavemon — Konsole
File
Edit
View
Bookmarks
Settings
Help

```
─Interface─
wlp61s0 (IEEE 802.11), phy 0, reg: n/a, SSID: 101_5G
─Levels─

link quality: 83%  (58/70)


signal level: -52 dBm (6.31 nW)


─Statistics─
RX: 3712 (1020.01 KiB), drop: 96
TX: 164 (29.58 KiB), retries: 73
─Info─
mode: Managed, connected to: 30:87:D9:B1:55:4C, time: 40 sec, inactive: 2.9s
freq: 5500 MHz, ctr1: 5530 MHz, channel: 100 (width: 80 MHz)
rx rate: 234.0 MBit/s VHT-MCS 3 80MHz VHT-NSS 2, tx rate: 866.7 MBit/s VHT-MCS 9 80MHz short GI VHT-NSS 2
beacons: 398, lost: 2, avg sig: -46 dBm, interval: 0.1s, DTIM: 1
power mgt: off,  tx-power: 22 dBm (158.49 mW)
retry: short limit 7,  rts/cts: off,  frag: off
encryption: n/a (requires CAP_NET_ADMIN permissions)
─Network─
wlp61s0 (UP RUNNING BROADCAST MULTICAST)
mac: A0:C5:89:A6:65:B7, qlen: 1000
ip: 10.5.4.213/21
```

1. SSID: 101_2.4G

Location	Signal Strength (dBm)	Transmission Rate (MBit/s)	Channel
farthest	-45	144.4	11
nearest	-24	144.4	11
behind wall	-50	144.4	11

2. SSID: 101_5G

Location	Signal Strength (dBm)	Transmission Rate (MBit/s)	Channel
farthest	-52	866.7	100
nearest	-32	866.7	100
behind wall	-54	234.0	100

3. SSID: 102_2.4G

Location	Signal Strength (dBm)	Transmission Rate (MBit/s)	Channel
farthest	-44	144.4	6
nearest	-27	144.4	6
behind wall	-32	144.4	6

4. SSID: 102_5G

Location	**Signal Strength (dBm)**	**Transmission Rate (MBit/s)**	**Channel**
farthest	-49	866.7	100
nearest	-28	866.7	100
behind wall	-52	866.7	100

5. SSID: 204_2.4G

Location	**Signal Strength (dBm)**	**Transmission Rate (MBit/s)**	**Channel**
farthest	-42	144.4	1
nearest	-23	144.4	1
behind wall	-41	144.4	1

6. SSID: 204_5G

Location	**Signal Strength (dBm)**	**Transmission Rate (MBit/s)**	**Channel**
farthest	-55	866.7	116
nearest	-32	866.7	116
behind wall	-54	866.7	116

System Administration

1. I just messed up ...

(a) (1) Extract `.vmdk` file from the provided `.ova` file: `$ tar -xvf nasa_2019_hw7.ova`

(2) Convert the `.vmdk` file to `.img` file:

```
$ qemu-img convert -f vmdk -O raw nasa_2019-disk1.vmdk hw7.img
```

(3) Execute *testdisk*: `$ testdisk hw7.img`

(4) In *testdisk*:

* select `"Disk hw7.img"->[EFI GPT]`

* select `[ Advanced ]`

* select `[ Type ]->"MS Data"->"ext4"`, Now I can see more options in menu.

* select `[ List ]`, and navigate to `/home/nasa/`, find `NTU.jpg` and `'NTU GO.jpg'`.

* select the two files, press `'C'` to copy files, and paste them to a proper directory.

(5) Quit program and go to check the content of the file. I find that `NTU.jpg` is a file of size 55596, whose content is all zero, while the `'NTU GO.jpg'` is an empty file.

* **References**

- https://docs.openstack.org/image-guide/convert-images.html
- https://vitux.com/how-to-recover-deleted-files-in-ubuntu-through-testdisk

(b) (1) Find the broken service: `$ sudo systemctl list-units --state=failed`

⇒ I find that the broken service is `apache2.service`

(2) Check what happened: `$ sudo systemctl status apache2`

⇒ there is a invalid command `';'` in `/etc/apache2/sites-enabled/000-default.conf`

(3) Remove the `';'`, then restart the service: `$ sudo systemctl restart apache2`

⇒ then it run without error

* **References**

- https://unix.stackexchange.com/questions/341060/what-are-the-systemctl-options-to-list-all-failed-units

(c) (1) the content of my systemd service file:

```
[Unit]
Description=Nasa Hw7 Web

[Service]
Type=simple
WorkingDirectory=/home/nasa/
ExecStart=/home/nasa/web

[Install]
WantedBy=multi-user.target
```

(2) make it start on boot: `$ sudo systemctl enable web.service`

* **References**

- https://unix.stackexchange.com/questions/341060/what-are-the-systemctl-options-to-list-all-failed-units

2. Web terminology

1. *Reverse Proxy* is a mechanism acting on the server side. Basically, it intercepts all requests sent to a specific set of servers, and retrieves resources on behalf of the client from the servers ”standing behind the proxy”.

The difference between *reverse proxy* and *forward proxy* is: a *forward proxy* intercepts all traffic sent from a specific set of clients, and ensures that no origin server ever communicates directly with those clients, while a *reverse proxy* intercepts traffic on the server side, ensuring that no client ever communicates directly with the servers behind the proxy.

One of the advantages of *reverse proxy* is that it can be used to achieve **load balancing**, by distributing the incoming traffic properly to the pool of servers behind it.

* **References**

- https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/

2. - **Model**: holds, manages the data and logic, manipulated by **controller** and updating **view**

- **View**: the visualization of the data that **model** contains
- **Controller**: accepts input from the user and passes it to **model**

* **References**

- https://en.wikipedia.org/wiki/Model-view-controller
- https://www.tutorialspoint.com/design_pattern/mvc_pattern.htm

3. Try MySQL

a.

```
SELECT name, since, origin FROM restaurants;
```

b.

```
UPDATE restaurants SET nickname = ’MaiDangDang’ WHERE id = 1;
UPDATE restaurants SET nickname = ’KidsFatCenter’ WHERE id = 2;
UPDATE restaurants SET nickname = ’BargarKing’ WHERE id = 3;
```

c.

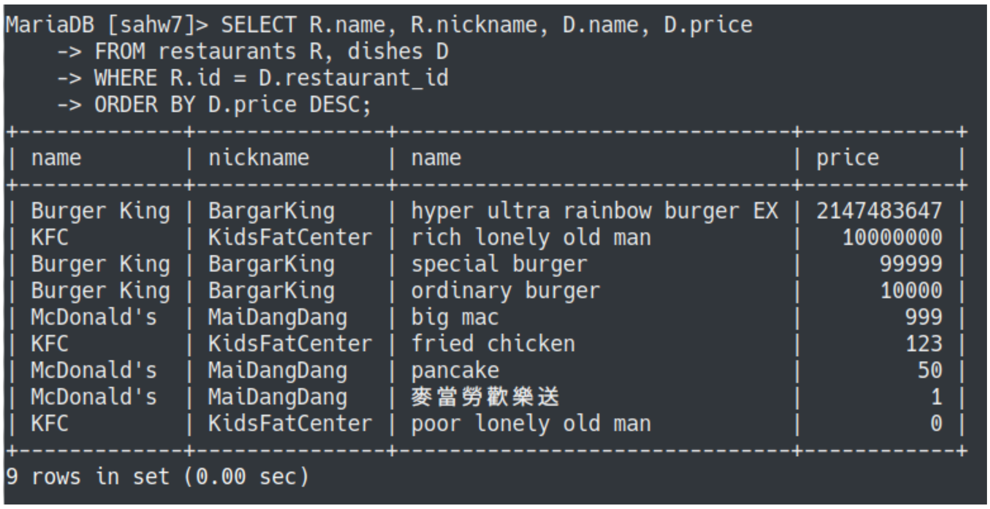
```
CREATE TABLE dishes (
    -> id int PRIMARY KEY NOT NULL AUTO_INCREMENT,
    -> name varchar(255),
    -> price int,
    -> restaurant_id int);
```

d. I insert 9 identities into this table in total, but I just list one of them to show the format of the SQL commands I use.

```
> INSERT INTO dishes (name, price, restaurant_id) VALUES (’big mac’, 999, 1);
```

e.

```
SELECT R.name, R.nickname, D.name, D.price
    -> FROM restaurants R, dishes D
    -> WHERE R.id = D.restaurant_id
    -> ORDER BY D.price DESC;
```



```
MariaDB [sahw7]> SELECT R.name, R.nickname, D.name, D.price
    -> FROM restaurants R, dishes D
    -> WHERE R.id = D.restaurant_id
    -> ORDER BY D.price DESC;
+-------------+---------------+------------------------------+------------+
| name        | nickname      | name                         | price      |
+-------------+---------------+------------------------------+------------+
| Burger King | BargarKing    | hyper ultra rainbow burger EX | 2147483647 |
| KFC         | KidsFatCenter | rich lonely old man          |   10000000 |
| Burger King | BargarKing    | special burger               |      99999 |
| Burger King | BargarKing    | ordinary burger              |      10000 |
| McDonald's  | MaiDangDang   | big mac                      |        999 |
| KFC         | KidsFatCenter | fried chicken                |        123 |
| McDonald's  | MaiDangDang   | pancake                      |         50 |
| McDonald's  | MaiDangDang   | 麥當勞歡樂送                 |          1 |
| KFC         | KidsFatCenter | poor lonely old man          |          0 |
+-------------+---------------+------------------------------+------------+
9 rows in set (0.00 sec)
```

4. More LAMP

a. (1) the content of `/var/www/html/index.php`:

```
<!DOCTYPE html>
<html>
<head>
        <title>PHP TEST</title>
</head>
<body>
<?php
    echo "Welcome!";
?>
</body>
</html>
```

(2) the `php7_module` module is loaded by `httpd` when I install `php`, so I don't need to do further configuration. The above file will run properly.

b. Below is the content of `/var/www/html/your-name.php`

```
<!DOCTYPE html>
<html>
<head>
    <title>君の名は。</title>
</head>
<body>
<?php
    echo "Welcome!␣" . $_GET["name"];
?>
</body>
</html>
```

c. In `/etc/httpd/conf/httpd.conf`, in the sectioin of `<Directory "/var/www/html">`, add:

```
    Require all denied
    Require ip 10.0.2.2 (My host's IP is 10.0.2.2)
```

d. *Apache Virtual Host* is used to run more than one web site(domain) in a single server. Different sites will be shown depending on the user's requested URL or IP address.

* References

- https://www.w3schools.com/php7/php7_syntax.asp

- https://www.php.net/manual/en/reserved.variables.get.php
- https://httpd.apache.org/docs/2.4/howto/access.html
- https://dasunhegoda.com/what-how-to-apache-virtual-host/444/