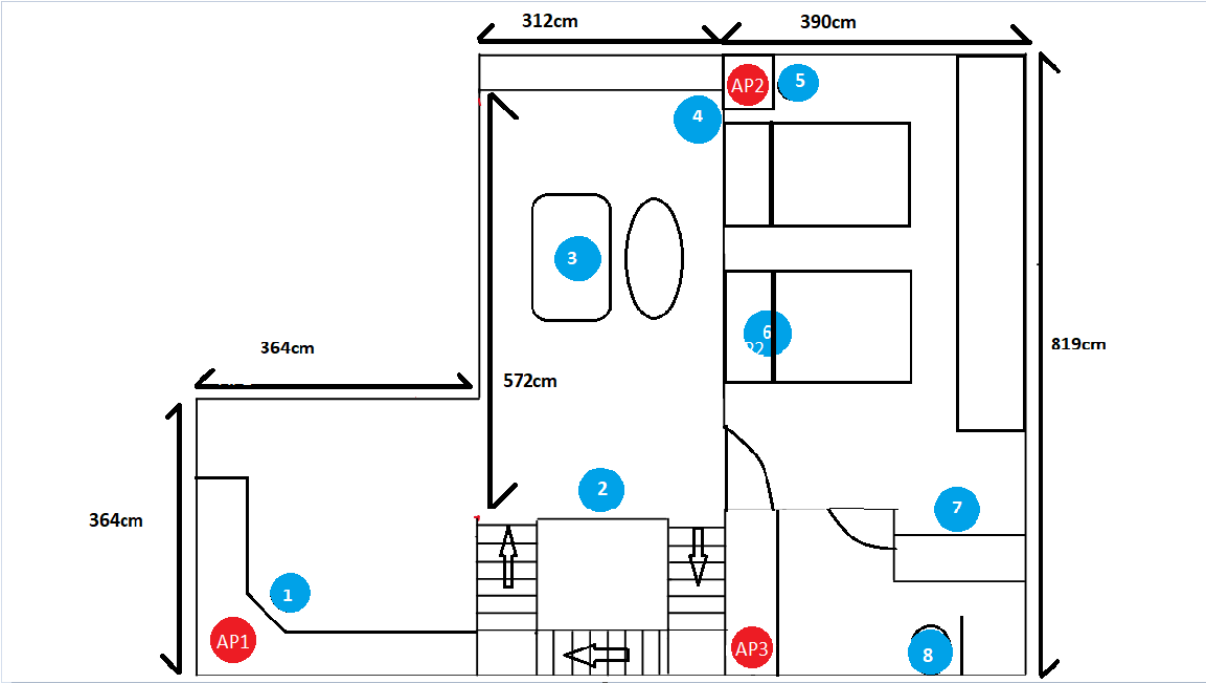
Assignment 2
FIT1047

KangHongBo
32684673

Part 1

1.1 Survey

The map below is the second floor of my house which has about 60 square meters



Location 1

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-37	-83	-91
	Percentage of current signal(%)	69	15	6
	Minimun value of signal (dBm)	-96	-85	-93
	Maximun value of signal (dBm)	-34	-22	-50
	Average value of signal (dBm)	-75	-52	-86
Upload Speed (Mbps)		56.76	2.13	Connection poor
Download Speed (Mbps)		103.89	1.23	Connection poor

Location 2

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-63	-66	-92
	Percentage of current signal(%)	38	35	5
	Minimun value of signal (dBm)	-96	-87	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-72	-60	-89
Upload Speed (Mbps)		55.05	2	0
Download Speed (Mbps)		104.3	5.6	3.48

Location 3

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-71	-75	-93
	Percentage of current signal(%)	29	24	3
	Minimun value of signal (dBm)	-96	-96	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-72	-63	-90
Upload Speed (Mbps)		56.61	4.22	Connection poor
Download Speed (Mbps)		102.78	13.39	Connection poor

Location 4

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-58	-69	-91
	Percentage of current signal(%)	44	31	6
	Minimun value of signal (dBm)	-96	-91	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-71	-64	-90
Upload Speed (Mbps)		54.09	2.33	Connection poor
Download Speed (Mbps)		106.17	14.81	Connection poor

Location 5

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-75	-33	-89
	Percentage of current signal(%)	24	73	8
	Minimun value of signal (dBm)	-96	-96	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-71	-64	-89
Upload Speed (Mbps)		54.64	1.93	0.17
Download Speed (Mbps)		105.3	19.74	3.55

Location 6

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-68	-67	-90
	Percentage of current signal(%)	33	34	7
	Minimun value of signal (dBm)	-96	-91	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-71	-64	-90
Upload Speed (Mbps)		56.62	1.45	0.35
Download Speed (Mbps)		102.23	19.33	2.94

Location 7

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-71	-67	-91
	Percentage of current signal(%)	29	34	6
	Minimun value of signal (dBm)	-96	-96	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-71	-64	-89
Upload Speed (Mbps)		26.5	1.8	0.33
Download Speed (Mbps)		105.89	13.51	2.83

Location 8

Access Point (AP)		1	2	3
SSID		KangChinYeh-5GHz@unifi	ocop	Mi 10T
MAC Address		00:AD:24:51:AF:DA	4A:69:C2:11:96:59	32:6C:CE:E5:7B:05
Security		WPA2 Personal	WPA2 Personal	WPA2 Personal
802.11 version supported		802.11ac	802.11ac	802.11ax
Frequency Band (GHz)		5	2.4	5
Frequency Channel Used		149	11	56-1
Signal Strength	Signal (dBm)	-79	-78	-71
	Percentage of current signal(%)	20	21	29
	Minimun value of signal (dBm)	-96	-96	-93
	Maximun value of signal (dBm)	-33	-22	-50
	Average value of signal (dBm)	-71	-65	-88
Upload Speed (Mbps)		21.43	2.49	0.25
Download Speed (Mbps)		79.89	12.27	2.5

Part 1.2 Report

1. Channel Occupancy:

In these three access points, the channels are not competing on the same access point. Because the access point which I have taken are two 5GHz which are channel 149 and channel 56-1 and one 2.4Ghz which is channel 11 so there will not be any overlapping channels. And it is available for roaming in these three access points. For the roaming, my laptop will automatically connect to the access point which has the stronger wifi signal.

2. Interference:

The signal from other sources can impair WLAN transmission by frequency interference if the sources have a crossed path with our wifi signal on a similar bandwidth it will corrupt or overpower the signal. For example, microwaves, BlueTooth, neighboring wifi, and others will cause frequency interference. Location 8 in my map is in a toilet and it has a concrete wall with a mirror on it and location 7 is a table outside the toilet we can compare the download speed ad the signal(dBm) we can see that the concrete wall with the mirror has a high interference level which is the physical interference.

3. Attenuation:

The density of the materials will affect the signal strength. The signal need to pass through the materials which will definitely affect the signal strength. Location 4 and 5 in my map can observe that the distance between AP2 is similar but the signal strength is about 20db difference so we know that the concrete wall will affect the signal strength. Attenuation caused by our body is possible since our body has a density that will affect the signal to pass through our body. It is possible to measure

the result by taking one report which has a body between the sniffing tools and access point another which is a normal sniff. Then compare the reports for the result.

4. Coverage:

The access points are sufficiently cover the desired area because AP1 and AP2 have a very large coverage which and for AP3 it can be removed since AP1 and 2 can be connected in location 8 without the package losing. So instead of adding a new access point, I could remove one of the access points.

5. Signal to noise ratio:

In this signal-to-noise ratio, I will use three data to calculate. For AP1 I will use location 1, for AP2 I will use location 5 and for AP3 I will use location 8. All this data is the strongest signal strength for these three AP's.

For AP1 in location 1

- SNR(dB)=Ps(dBm)-Pn(dBm)
  =-37-(-96)
  = 59(dBm)

SNR(dB)=$10\log_{10}$SNR
59=$10\log_{10}$SNR
SNR=$10^{5.9}$

Shannon equation
C=$B\log_2(1+SNR)$
C=$20\log_2(1+10^{5.9})$
C=391.988..

For AP2 in location 5

- SNR(dB)=Ps(dBm)-Pn(dBm)
  =-33-(-96)
  = 63(dBm)

SNR(dB)=$10\log_{10}$SNR
63=$10\log_{10}$SNR
SNR=$10^{6.3}$

Shannon equation
C=$B\log_2(1+SNR)$
C=$20\log_2(1+10^{6.3})$
C=418.563..

For AP3 in location 8

- SNR(dB)=Ps(dBm)-Pn(dBm)
  =-71-(-96)
  = 25(dBm)

SNR(dB)=$10\log_{10}$SNR
25=$10\log_{10}$SNR
SNR=$10^{2.5}$

Shannon equation
C=$B\log_2(1+SNR)$
C=$20\log_2(1+10^{2.5})$
C=166.188..

As we can see from these three data the maximum achievable data rate in bits/second AP2 has the highest value and AP3 has the least value so we can observe that AP3 is not a good Access point that does not have a capacity of 166.188

Part 2

2.1 Summary

In the article 'NFC Flaws in POS Devices and ATMs', there are some security researchers found that instead of hacking the ATMs using a thumb drive or drilling a hole to expose internal wiring they could use an NFC reader to hack ATMs. A researcher names Josep Rodriguez found out that there is a vulnerability in near-field-communications reader chips which are frequently used in the ATMs. He also built an application that allows his smartphone to mimic credit card radio communications and exploit flaws in the NFC system's firmware. He can exploit a variety of bugs to crash point-of-sale devices, hack them to collect and transmit credit card data, and so on. Then the other researchers IOActive hacker Barnaby Jack and the team at Red Balloon Security have been able to uncover those ATM vulnerabilities and even shown that hackers can remotely trigger ATM jackpotting remotely.

2.2 Identify

In this issue, the NFC reader is mainly affected since all the issues are connected with the near-field communications and the signal from the NFC products. To read the data transmission through the product and even control the data transmission along with the products.

2.3 Describe The Problem

The problem was discovered by Josep Rodriguez, he found out that the data transmission along the NFC system is vulnerable by using other devices to read the data transmission. He even used an application on his phone to access the data transmission. Besides that, other researchers like the IOActive hacker Barnaby Jack

and the team at Red Balloon Security have shown that hackers can remote ATM jackpotting.

2.4 Estimate the Seriousness

For these issues, it is a huge problem for the security of ATM users because nowadays lots of people use NFC products to pay or use ATMs. Hence, their credit card is actually saved in their smartphone for waving the NFC readers. So if the NFC system is vulnerable the users might encounter the problem of displaying an error message if the reader was hacked. So the ATM companies need to spend more time to produce a more secure NFC reader for their ATM vendors. Besides that, we should not rely on NFC products even though it is convenient to the users. We could use a credit card instead of NFC to pay or use an ATM. Otherwise, we could wait till the

The NFC system is mature and safe to use. For the policy level, the government needs to withdraw the NFC reader for the safety of the citizen. They should ensure that the product could give safety and privacy for all of the users before it is frequently used in the country to prevent data from being hacked. Moreover, the government could set the law to remove the NFC system if the systems have a bug or are being hacked in this case the security of the users can be ensured.

Reflective Journal 2

Week 6

This week I learned the OS system. It was quite interesting especially for the BIOS and the UEFI booting process. It is something that is normally seen in our life when we are booting up our computers. Besides that, for the lab, there is more explanation between BIOS and UEFI booting systems. In this lab, we also learned about the chipset of the motherboard. It is quite interesting because I am interested in setting up the motherboard but haven’t tried before so it gave me a clearer image of the whole motherboard for example the things inside northbridge and southbridge.

Week 7

This week for the pre-recorded video we are starting a new topic about the internet. It is a very new knowledge for me, in my knowledge network is something that is very unbelievable. I can't imagine how the network would actually work and return the website or something that used the internet. The lecture taught me that network systems have many layers and are all different for every layer. In the lab, we briefly talked about the operating systems and examined running processes. This lab is quite unique to learn about Linux operating system calls even though we just briefly talked about it.

Week 8

This week we go through the physical layer and data link layer. In the physical layer, until now I know that cable has different types for the connections between network devices which can be differentiated into UTP, STP, Optical Fiber, Coaxial. For their digital transmission is somehow hard to remember it has a lot of different transmissions which all represent the signal. For the lab, we are taught about basic knowledge of network layers and we learned about the Wireshark which can capture the packet from the internet.

Week 9

For this week in the pre-recorded video the network layer, but for the lecture is somehow rushing fast, and adding classes in this few weeks it is quite heavy to observe all the knowledge but still trying to catch up. For the video, we know that how routers work within each other and the transport layers we know that the addressing of an application is differentiated by the port. In this week I also started to do my assignment with the map plotting and trying to set the places which are needed. In this week's lab, we learned about the different email protocols and MIME in detail. We also try to capture the packet by using Wireshark with the guidance of the tutor.

Week 10

This week also has an extension class which I have almost forgotten but fortunately, I remembered it on the morning of that day. In the pre-recorded video this week we learned about security attacks which are likely interesting, it is somehow cool that to know all of the possible attacks can be made by others. Then the cryptography is a very awesome thing that is created to secure the data in the data link. For the lab this week the calculating of subnet address is quite blurred but still understandable and the routing system was taught in this lab too. For assignment 2 I started to collect the data this week and created the table.

Week 11

In this week we learned security protocol in the pre-recorded video and it is a huge topic but it is some common knowledge about security protocol. For assignment 2, I was starting to answer all the questions and read the article which is related to the security of NFC readers and the article is very good content for us since the NFC product become more popular nowadays. So overall for this unit is quite good for me till now although it is a massive subject that covered a lot of new knowledge and others. For the lab this week, we were having a ciphertext changing lab and it is great and fun for me cause it is just like morse code in our real life but it is in the computer.