

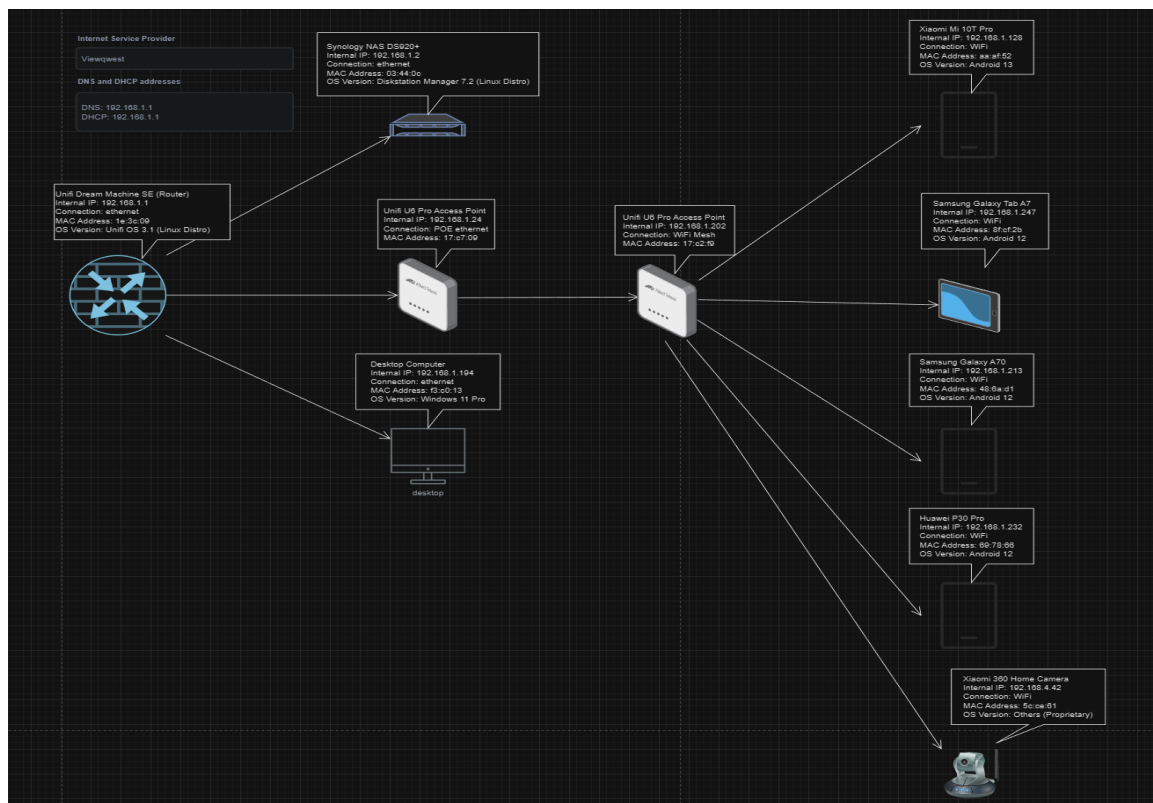
Unit : CFC020823

Name : Sean Teo Wei Chong

Student Code : S28

# Intro to Cyber

Image 1: Network map of my devices



Things to note:

- 1<sup>st</sup> access point are wired connect to my router and 2<sup>nd</sup> access point is connected to 1<sup>st</sup> access point via mesh connection.
- Xiaomi security camera is connected to a different network ID for security. In the event of being hacked, hackers are not able to access main network due to different network ID.

## Image 2: Getting DNS and DHCP server address using command prompt

2.1 Command used:

```
C:\Users\sean1>ipconfig /all
```

Router Server: 192.168.1.1

DHCP Server: 192.168.1.1

DNS Server: 192.168.1.1

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : localdomain
Description . . . . . : Realtek PCIe 2.5GbE Family Controller
Physical Address. . . . . : 04-D9-F5-F3-C0-13
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f58e:abcc:217:63fd%7(Preferred)
IPv4 Address. . . . . : 192.168.1.194(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, 17 August 2023 8:29:36 pm
Lease Expires . . . . . : Friday, 18 August 2023 8:29:35 pm
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 100981237
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-30-23-38-04-D9-F5-F3-C0-13
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

## Image 3: Getting my external IP address

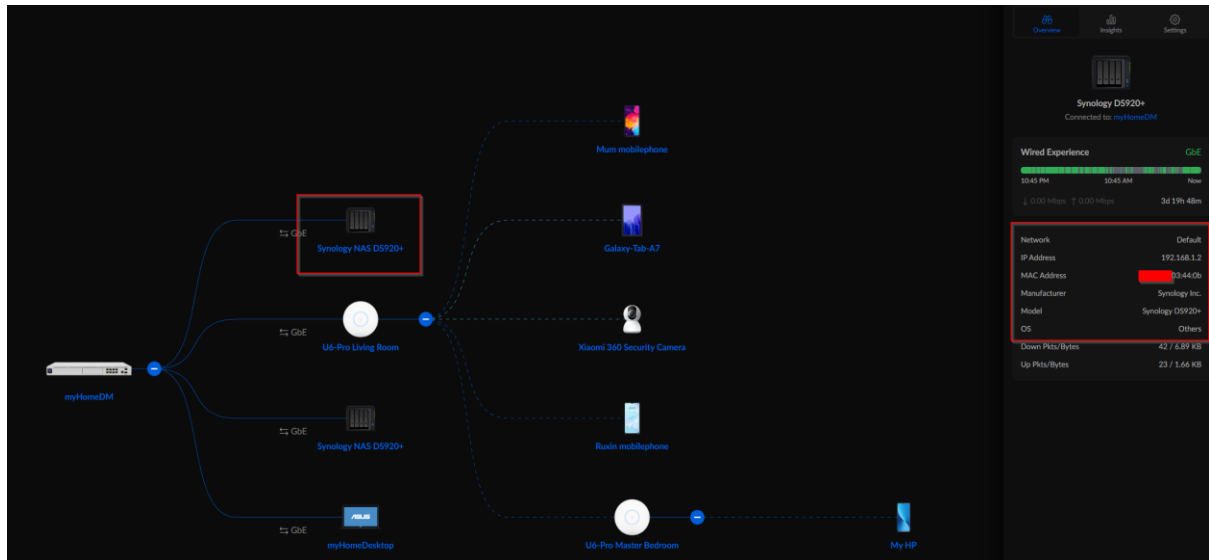
3.1 Go to <http://whatismyip.com> and you will be able to see external IP used and the **Internet Service Provider (ISP)**

The screenshot shows the homepage of WhatIsMyIP.com. The browser's address bar displays <https://www.whatismyip.com>. The website has a dark blue header with the logo and navigation links: Home, What Is My IP?, IP Address Lookup, IP WHOIS Lookup, DNS Lookup, and Internet Speed Test. Below the header, a large dark blue box contains the following information:

- What Is My IP?**
- My Public IPv4 is: **132.147.73.42**
- My Public IPv6 is: Not Detected
- My IP Location is: Singapore, - SG
- My ISP is: ViewQwest Fibernet

## Image 4: Obtaining devices information in network map

4.1 Login into my router settings page, select the device I want to know more and information will be available on the right side.



## Image 5: Wireshark capturing information of my device going to Facebook website

5.1 Open Wireshark program, select the NIC that my device is using and go to [www.facebook.com](https://www.facebook.com)

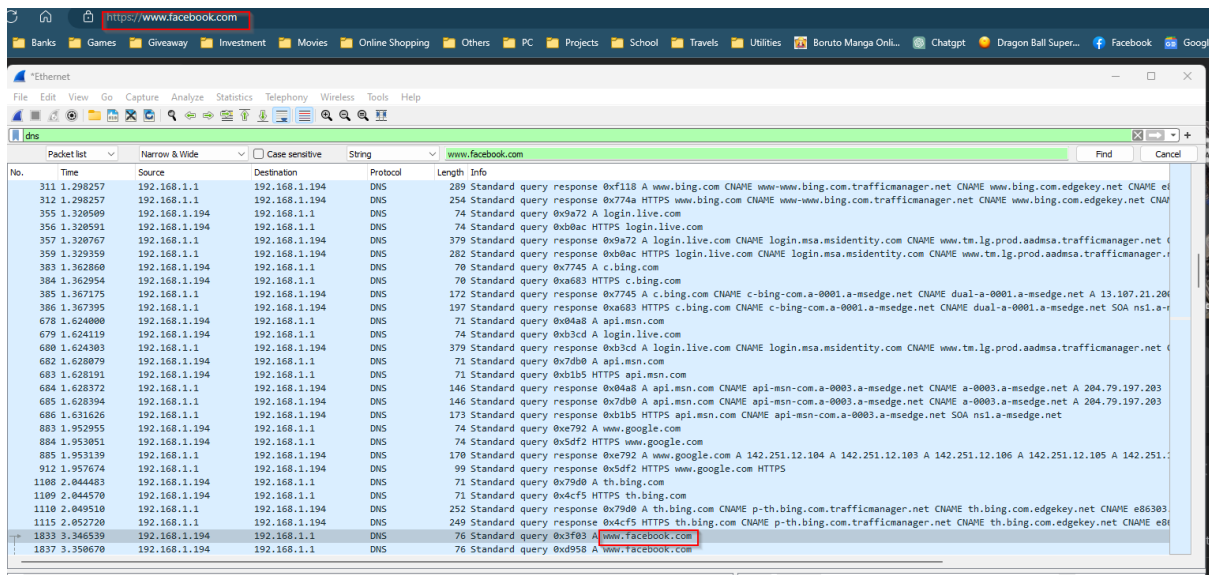


Image 6: Capturing www.facebook.com IP address

## 6.1 Applying "DNS" filter and searching for "www.facebook.com" string

dns						
Packet list		Narrow & Wide		Case sensitive		String
						www.facebook.com
no.	Time	Source	Destination	Protocol	Length	Info
383	1.362860	192.168.1.194	192.168.1.1	DNS	70	Standard query 0x7745 A c.bing.com
384	1.362954	192.168.1.194	192.168.1.1	DNS	70	Standard query 0xa683 HTTPS c.bing.com
385	1.367175	192.168.1.1	192.168.1.194	DNS	172	Standard query response 0x7745 A c.bing.com CNAME c-bing-com.a-0001.a-msedge.net CNAME dual-a-0001.a-msedge.net A 13.1
386	1.367395	192.168.1.1	192.168.1.194	DNS	197	Standard query response 0xa683 HTTPS c.bing.com CNAME c-bing-com.a-0001.a-msedge.net CNAME dual-a-0001.a-msedge.net SC
678	1.624000	192.168.1.194	192.168.1.1	DNS	71	Standard query 0x04a8 A api.msn.com
679	1.624119	192.168.1.194	192.168.1.1	DNS	74	Standard query 0xb3cd A login.live.com
680	1.624303	192.168.1.1	192.168.1.194	DNS	379	Standard query response 0xb3cd A login.live.com CNAME login.msa.msidentity.com CNAME www.tm.lg.prod.aadmsa.trafficman
682	1.628079	192.168.1.194	192.168.1.1	DNS	71	Standard query 0x7db0 A api.msn.com
683	1.628191	192.168.1.194	192.168.1.1	DNS	71	Standard query 0xb1b5 HTTPS api.msn.com
684	1.628372	192.168.1.1	192.168.1.194	DNS	146	Standard query response 0x04a8 A api.msn.com CNAME api-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.
685	1.628394	192.168.1.1	192.168.1.194	DNS	146	Standard query response 0x7db0 A api.msn.com CNAME api-msn-com.a-0003.a-msedge.net CNAME a-0003.a-msedge.net A 204.79.
686	1.631626	192.168.1.1	192.168.1.194	DNS	173	Standard query response 0xb1b5 HTTPS api.msn.com CNAME api-msn-com.a-0003.a-msedge.net SOA ns1.a-msedge.net
883	1.952955	192.168.1.194	192.168.1.1	DNS	74	Standard query 0xe792 A www.google.com
884	1.953051	192.168.1.194	192.168.1.1	DNS	74	Standard query 0x5df2 HTTPS www.google.com
885	1.953139	192.168.1.1	192.168.1.194	DNS	170	Standard query response 0xe792 A www.google.com A 142.251.12.104 A 142.251.12.103 A 142.251.12.106 A 142.251.12.105 A
912	1.957674	192.168.1.1	192.168.1.194	DNS	99	Standard query response 0x5df2 HTTPS www.google.com HTTPS
1108	2.044483	192.168.1.194	192.168.1.1	DNS	71	Standard query 0x79d0 A th.bing.com
1109	2.044570	192.168.1.194	192.168.1.1	DNS	71	Standard query 0x4cf5 HTTPS th.bing.com
1110	2.049510	192.168.1.1	192.168.1.194	DNS	252	Standard query response 0x79d0 A th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net CNA
1115	2.052720	192.168.1.1	192.168.1.194	DNS	249	Standard query response 0x4cf5 HTTPS th.bing.com CNAME p-th.bing.com.trafficmanager.net CNAME th.bing.com.edgekey.net
1833	3.346539	192.168.1.194	192.168.1.1	DNS	76	Standard query 0x3f83 A www.facebook.com
1837	3.350670	192.168.1.194	192.168.1.1	DNS	76	Standard query 0xd958 A www.facebook.com
1838	3.350742	192.168.1.194	192.168.1.1	DNS	76	Standard query 0x2f6a HTTPS www.facebook.com
1841	3.353081	192.168.1.1	192.168.1.194	DNS	121	Standard query response 0x3f83 A www.facebook.com CNAME star-mini.c10r.facebook.com A 157.240.15.35
1842	3.353105	192.168.1.1	192.168.1.194	DNS	121	Standard query response 0xd958 A www.facebook.com CNAME star-mini.c10r.facebook.com A 157.240.15.35
1843	3.354525	192.168.1.1	192.168.1.194	DNS	150	Standard query response 0x2f6a HTTPS www.facebook.com CNAME star-mini.c10r.facebook.com SOA a.ns.c10r.facebook.com
1913	3.769790	192.168.1.194	192.168.1.1	DNS	79	Standard query 0x597f A static.xx.fbcdn.net
1914	3.769867	192.168.1.194	192.168.1.1	DNS	79	Standard query 0x1304 HTTPS static.xx.fbcdn.net

6.2 Alternately we can also use Windows Command Prompt to find out the IP address of Facebook.com by using "Ping <URL/domain names>"

```
C:\Users\sean1>ping facebook.com

Pinging facebook.com [157.240.13.35] with 32 bytes of data:
Reply from 157.240.13.35: bytes=32 time=1ms TTL=57
Reply from 157.240.13.35: bytes=32 time=3ms TTL=57
Reply from 157.240.13.35: bytes=32 time=2ms TTL=57
Reply from 157.240.13.35: bytes=32 time=3ms TTL=57

Ping statistics for 157.240.13.35:
```