Network Mapping

Intro to Cyber

Centre For Cybersecurity

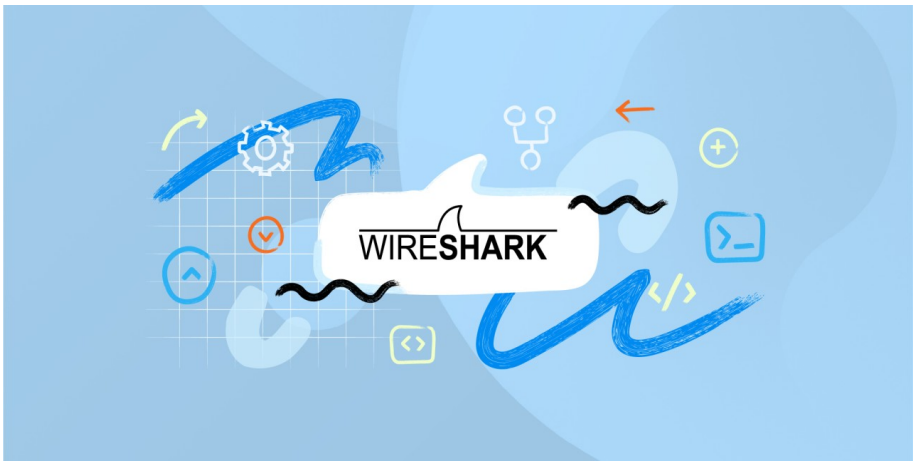
Edwin Lum
S8
CFC130124

TABLE OF CONTENTS

Introduction

The primary objective of this project was to create a detailed map of the home network, to show the web of connections between devices. Emphasising the networking aspect, this report will provide an overview of the network topology, the methodologies behind identifying the IP and MAC addresses, as well as the use of Wireshark to determine IP addresses of websites.

(Attacks from 4G/5G Core Networks: Risks of the Industrial IoT in Compromised Campus Networks, n.d.)



(Wireshark: an Open-Source Packet Capture Tool, n.d.)

Methodologies

Map the Network

The home network was mapped and it uses a star topology, with the router being the only connection for all the devices to the internet. There are a total of three devices regularly connected to the router.

The Main PC and the Home Entertainment System (Playstation 5) have a wired connection to the router while the Mobile Device is connected via Wi-Fi.

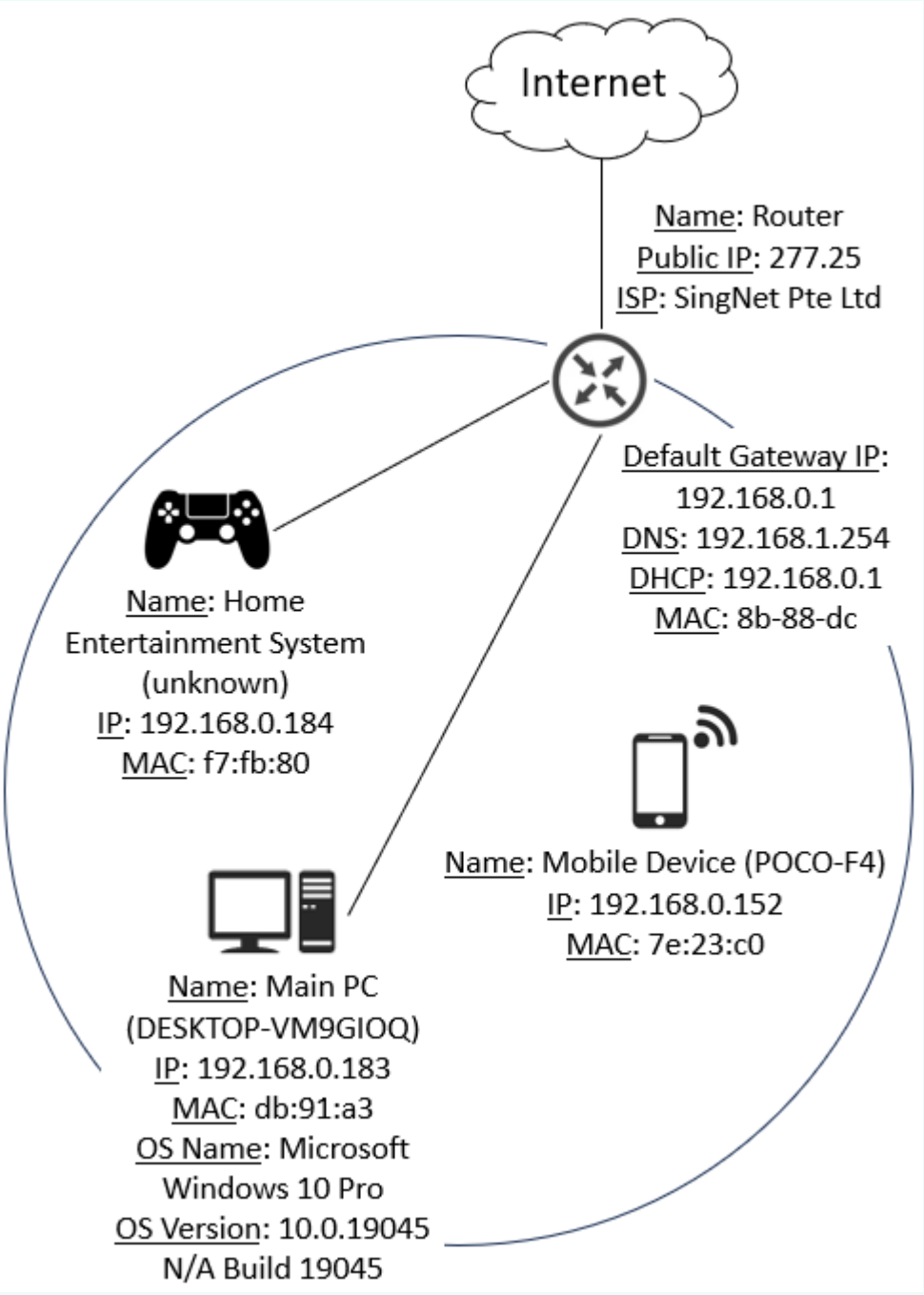


Figure 1: Home network map (Draw.io, n.d.)

Commands and Websites

Determining the Devices Connected to the Network

The router's web interface allows for easy access to the router's settings to configure and customize the network according to each organisation or individual's needs.

The network settings on the interface displayed the IP addresses and MAC addresses of all devices connected to the home network.

As the router is very old, it is unable to detect the Playstation 5 connected to the network and hence, displaying it as (unknown).

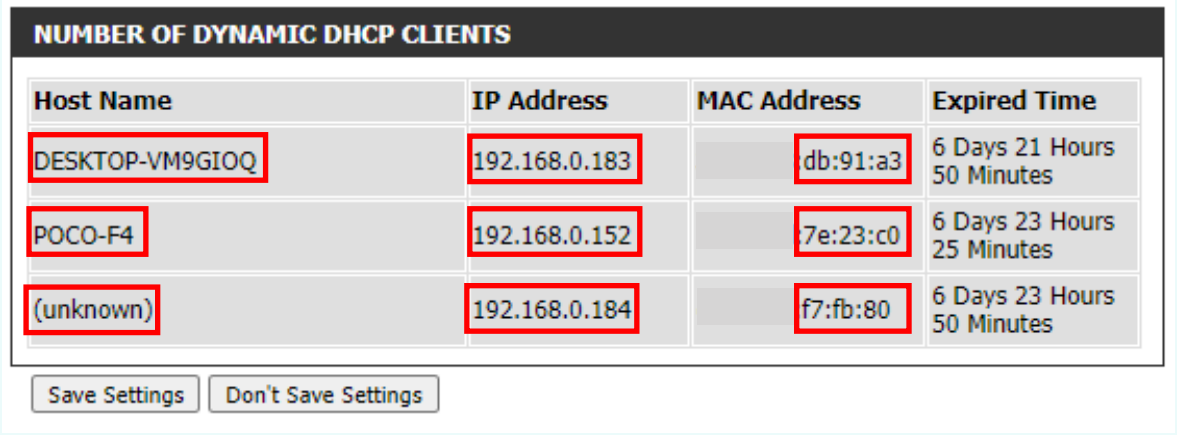


Figure 2: Router's web interface showing devices on the network

Identifying the External IP and Internet Service Provider (ISP) of the Router

WhatIsMyIPAddress.com displays the external IP address and ISP of the router used in the home network.

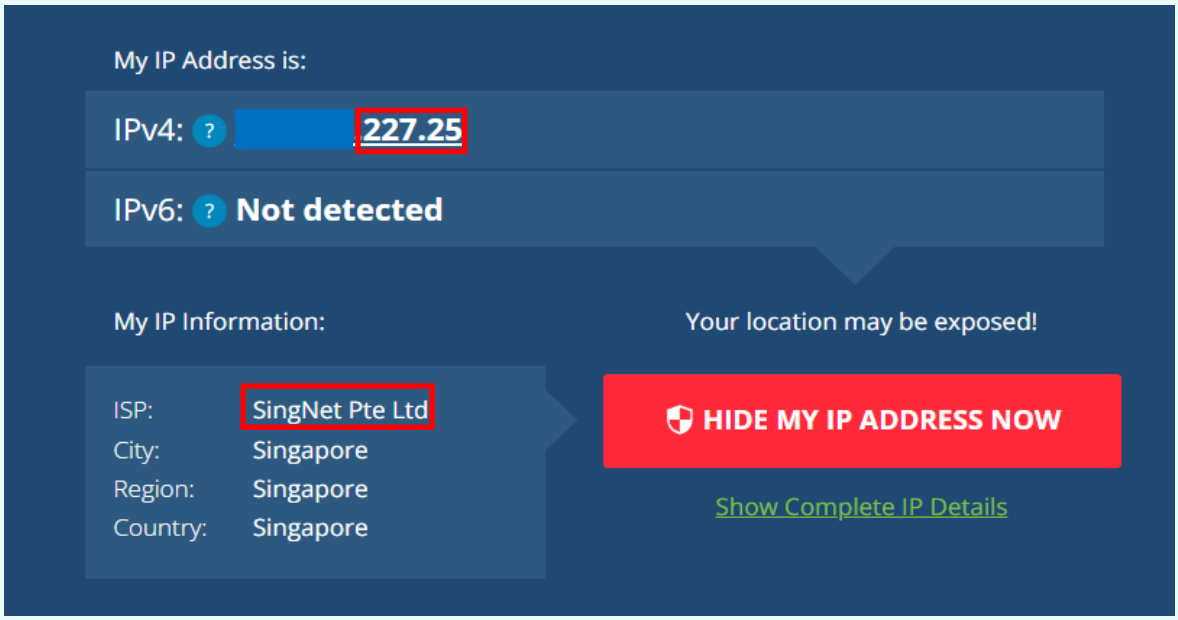


Figure 3: WhatIsMyIPAddress.com with external IP address and ISP information (WhatIsMyIPAddress.com, 2000)

Finding information on Router and Operating System (OS) of the Device

Command Prompt is a command line interpreter application that allows the user to enter commands to automate tasks and perform administrative functions.

The command, ipconfig /all, was used to display the full TCP/IP configuration for all adapters.

The /all flag displayed the detailed TCP/IP configuration for all adapters.

The relevant information on IP addresses for the Default Gateway, DNS Server and DHCP Server was then extracted.

```
C:\Users\User>ipconfig /all
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . :       DB-91-A3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::459e:8a3d:da2b:3991%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.183(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, 23 January 2024 6:31:02 PM
   Lease Expires . . . . . . . . . . : Tuesday, 30 January 2024 6:31:00 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 70294563
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-9A-36-B3-30-9C-23-DB-91-A3
   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 4: ipconfig /all command used to extract information on router

The command, systeminfo | findstr /B /C:"OS Name" /B /C:"OS Version", was used to display the detailed configuration information of the device.

findstr searches for specific text string appearing from the systeminfo. The /B flag matches the string if it appears at the beginning of the line while the /C:string flag searches for the specified string.

```
C:\Users\User>systeminfo | findstr /B /C:"OS Name" /B /C:"OS Version"
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
```

Figure 5: systeminfo command used to extract OS information from PC

Wireshark

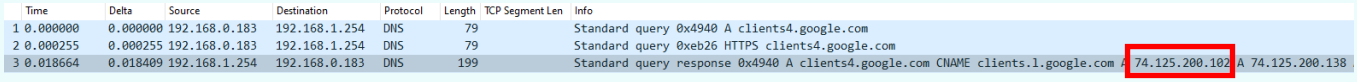
Wireshark is a free, open-source packet analyser that can be used for network troubleshooting, tracing connections and analysing network traffic to protect the network.

When the PC was used to access the website, 'https://www.google.com/', packets were captured using Wireshark.

The DNS filter was then used to display only the packets involving the DNS protocol, which translates domain names to IP addresses.

The packets were analysed and Figure 6 shows the query request from the PC to the DNS server. The DNS server then responds to the query with multiple IP addresses of Google. The highlighted portion shows the IP address of the website.

There are multiple servers setup with multiple IP addresses mapped to the same domain name of google.com for load balancing purposes, to handle a large number of users accessing the domain at the same time.



	Time	Delta	Source	Destination	Protocol	Length	TCP Segment Len	Info
1	0.000000	0.000000	192.168.0.183	192.168.1.254	DNS	79		Standard query 0x4940 A clients4.google.com
2	0.000255	0.000255	192.168.0.183	192.168.1.254	DNS	79		Standard query 0xeb26 HTTPS clients4.google.com
3	0.018664	0.018409	192.168.1.254	192.168.0.183	DNS	199		Standard query response 0x4940 A clients4.google.com CNAME clients.l.google.com A 74.125.200.102 A 74.125.200.138

Figure 6: Analysis of packets on Wireshark to find IP address of Google's website

One of the IP addresses of 'https://www.google.com/' is 74.125.200.102.

Conclusion

There are many easily accessible tools that can be used to aid in network mapping, like Command Prompt, web interface of the router and websites like WhatIsMyIPAddress.com. Wireshark is also a useful tool to capture network traffic.

Gathering information on a network can be done via a variety of methods. Exploring such methods are an opportunity for personal and professional growth, enhancing one's ability to think critically and strategically.

Gaining more experience with all of the tools and being adaptable to optimise the effectiveness of the many information gathering methods will help one become more proficient and tackle the evolving challenges within the cybersecurity field.

References

1. Attacks from 4G/5G Core Networks: Risks of the Industrial IoT in Compromised Campus Networks. (n.d.). Available at: https://www.iiot-world.com/ics-security/cybersecurity/attacks-from-4g-5g-core-networks-risks-of-the-industrial-iot-in-compromised-campus-networks/ [Accessed 24 Jan. 2024].

2. Wireshark: an Open-Source Packet Capture Tool. (n.d.). Available at: https://blog.invgate.com/wireshark [Accessed 24 Jan. 2024].

3. Draw.io (n.d.). Flowchart Maker & Online Diagram Software. [online] app.diagrams.net. Available at: https://app.diagrams.net/.

4. WhatIsMyIPAddress.com. (2000). What Is My IP Address? IP Address Tools and More. [online] Available at: https://whatismyipaddress.com/.