Project Title: NetCraft Project
Student Code: S8
Trainer Name: Samson

Table of Contents

Introduction

In today's digitally reliant world, understanding the intricate dance of devices within our home network is no longer a luxury, but a necessity. This report delves into the heart of a typical home network, dissecting the role of each device. A visual representation created using Canva was made to help facilitate learning. I will be exploring the tools and functions available to locate critical network details like Internet Protocol (IP) and Media Access Control (MAC) addresses, along with identifying the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers. In addition, I will venture beyond the confines of my hostel network, utilising online tools like Shodan and ViewDNS to unveil information about my internet service provider (ISP) and public IP address. By the end of this report, I seek to attain greater knowledge of the networking system surrounding my hostel, along with a greater appreciation of it through a future cybersecurity practitioner's perspective.

Methodologies

In this chapter, we will be briefly describing the commands and tools used to obtain the relevant information of the home network.

Displaying the device's and router's internal IP address

In order to identify my device's internal IP address, the command *"ipconfig"* was used in the command prompt.

Displaying the device's MAC address, DNS and DHCP addresses in my network.

To display the device's MAC address, DNS and DHCP addresses, the command *"ipconfig /all*" was used in the command prompt. The addition of the *"/all*" switch command is more comprehensive as it provides details of all network adapters in my system with additional information like the MAC address, DHCP server and DNS server.

Displaying the device's name, operating system (OS) and version.

The command *"systeminfo*" was keyed into the command prompt. The command gives detailed information about the computer's software and hardware configuration.

Displaying the other devices' MAC address and internal IP address.

The command *"arp -a"* was used in the command prompt to obtain the MAC addresses and internal IP addresses of the devices connected to the same router.

Displaying the Vendor of the other devices' MAC address

The website *"www.macvendors.com"* was used to identify the manufacturer of a network device based on its MAC address.

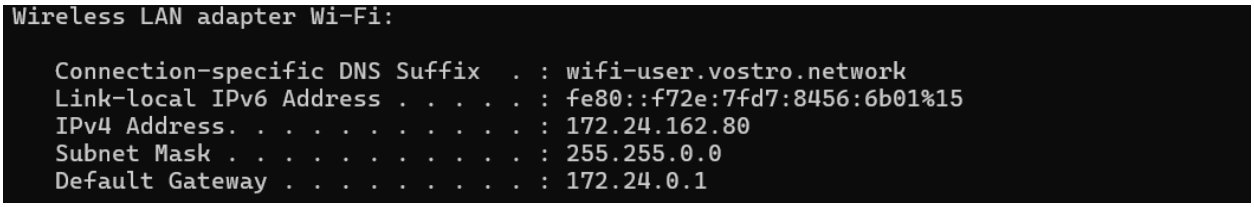
Finding my public IP address and ISP

The website "www.whatismyipaddress.com" was used to obtain the public IP address along with details about my ISP.

Discussion

Displaying the device's and router's internal IP address

Keying in "ipconfig" in the command prompt gave the following result.



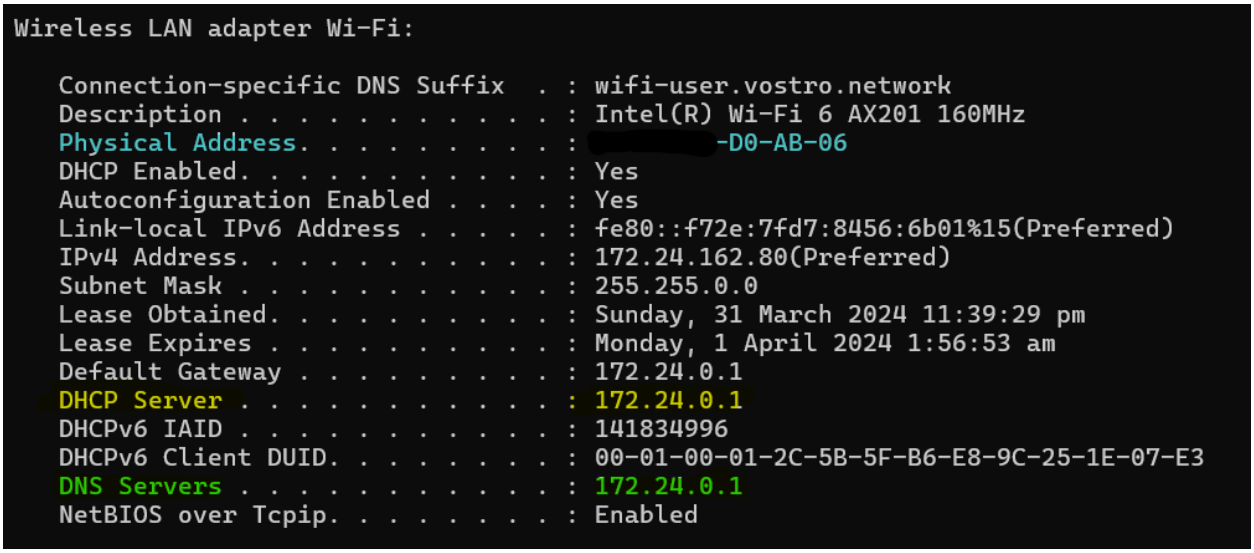
This command provides a summary of the current network configuration for the active adapter, either Wi-Fi or ethernet connection, displaying information like the internal IP address and the Default Gateway (router's internal IP address).

The device's internal IP address is reflected in the IPv4 Address row. The internal IP address is a unique numerical label assigned to devices within a private network, allowing easy identification and communication between devices in the same network.

The router's internal IP address is reflected in the Default Gateway row. In this case, the home router is the default gateway, acting as an access point between the local network and the internet (Higgins, M., 2020).

Displaying the device's MAC address, DNS and DHCP addresses in my network.

Keying in "ipconfig /all" in the command prompt gave the following result.



The device's MAC address is cyan, whereas the DHCP server and DNS server are highlighted in yellow and green respectively.

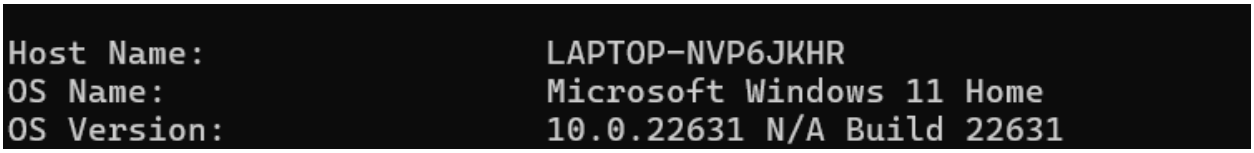
The "/all" addition gives detailed information about all adapters, including the IP address, subnet mask, default gateway, DHCP server, and DNS server

The device's MAC address is reflected in the Physical address row. The MAC address is a globally unique number assigned by the manufacturer during production, ensuring no two devices have the same address. This unique number allows it to be easily recognized by other devices on the network.

The DHCP server maintains and manages the pool of available internal IP addresses by assigning devices vacant internal IP addresses.
The DNS server allows us to communicate with our computer by translating human-readable domain names into machine-readable IP addresses that networks and computers use to connect to each other.

Displaying the device's name, operating system (OS) and version.

Keying in *"systeminfo*" into the command prompt gives the following result.



The System info command displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (systeminfo command, 2023).

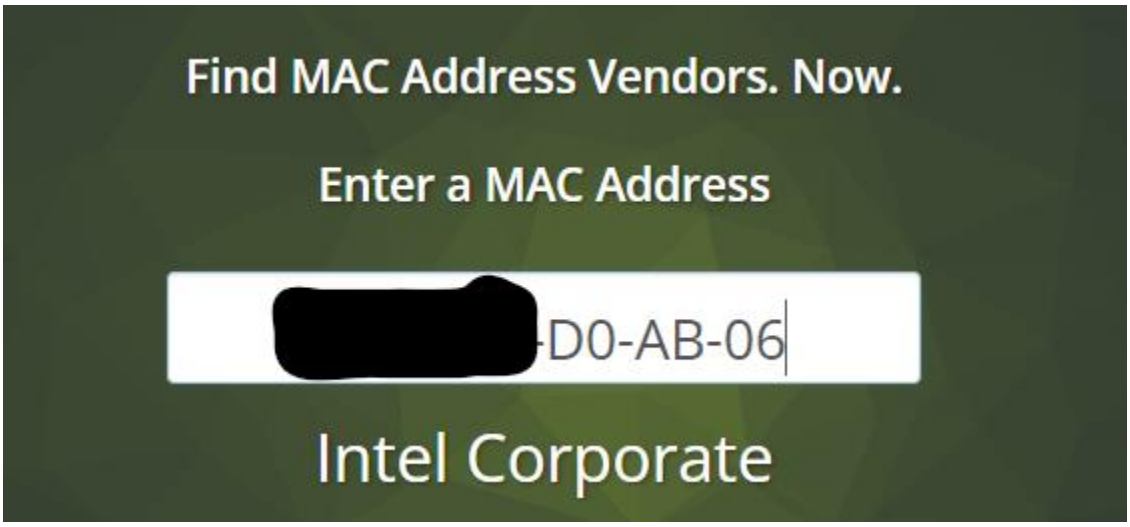
Displaying the other devices' MAC address and internal IP address.

The command *"arp -a"* was used in the command prompt to obtain the MAC addresses and internal IP addresses of the devices connected to the same router. The Address Resolution Protocol (ARP) is a networking protocol used to map network addresses such as a MAC address to an IP address. The *"arp -a"* command is used to display the ARP cache on a computer, which includes both static and dynamic entries (Kumar, 2023).

However as the network of this report is in a hostel, the MAC addresses of the connected devices were masked. Hence the MAC addresses and internal IP addresses were manually found by accessing the connected devices.

Displaying the Vendor of the other devices' MAC address

The mac addresses were keyed into "macvendor.com" to find out the MAC address vendor. The website "macvendors.com" provides a tool to lookup the manufacturer of a device based on its MAC address.
The following image gives an example of the process.



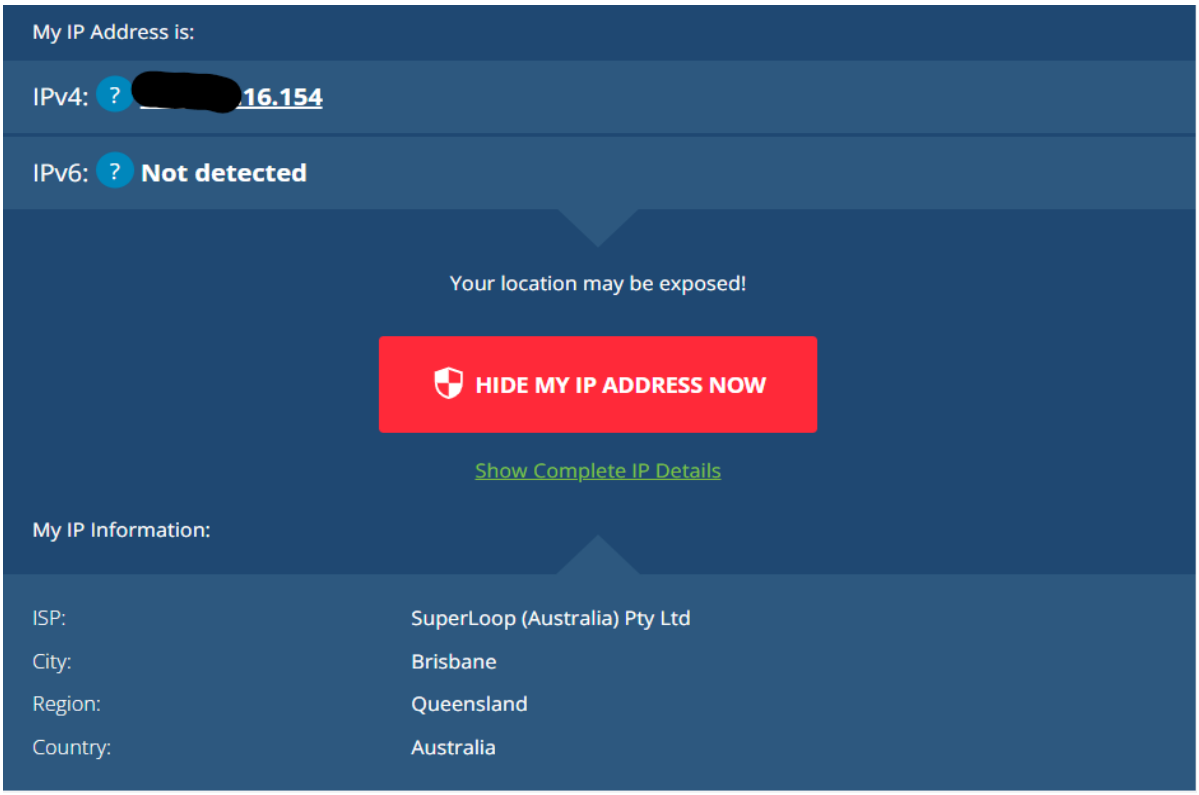
However, it was noted that two of the device's MAC addresses did not yield results in macvendor.com. Upon digging deeper, it was identified that the two devices had private MAC addresses as a form of data security feature in their phones.

If a device uses the same MAC addresses for different Wi-FI networks, network operators or network observers will be able to relate that MAC address to the network activity and location over time, which creates profiling. Hence, a private MAC address prevents that (Apple Support, 2023).

Finding my public IP address and ISP

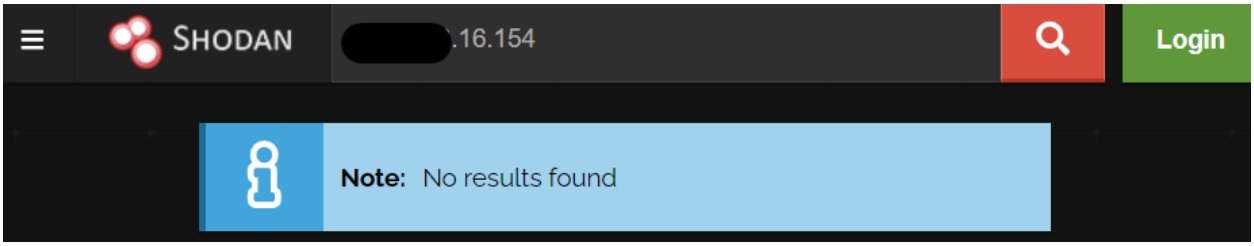
The website “whatismyipaddress.com” is a website that helps users identify their public IP address and ISP.

Entering whatismyipaddress.com yielded the following result.



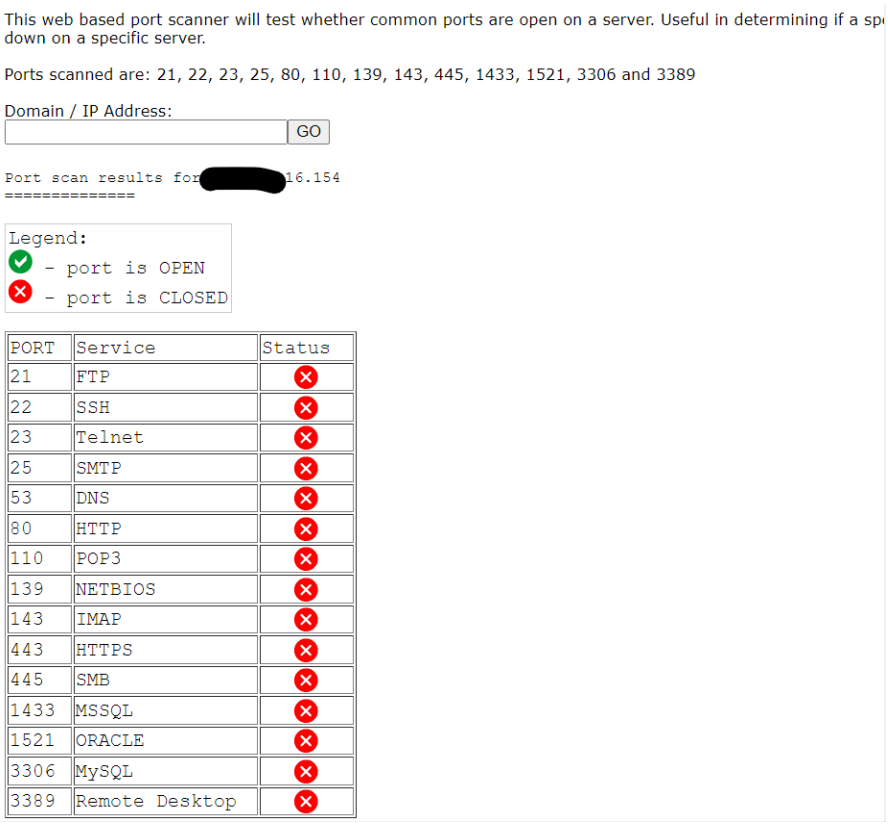
Entering my public IP address into Shodan

Shodan is a search engine for internet-connected devices, allowing users to gather publicly-available information about all devices directly connected to the internet (What is shodan?, no date).
Entering my IP address into Shodan did not yield any results.



This could be due to either of the following reasons:

1. Shodan gets its information that it displays from banners (What is shodan, no date), which obtains information running on a system from its open ports. Internet Service Providers (ISPs) may intentionally close ports for security reasons. Searching my public IP address on the port scanner in viewdns.info revealed that there were no open ports. Hence, as there are no open ports, no information will be available for Shodan.



This web based port scanner will test whether common ports are open on a server. Useful in determining if a sp
down on a specific server.

Ports scanned are: 21, 22, 23, 25, 80, 110, 139, 143, 445, 1433, 1521, 3306 and 3389

Domain / IP Address:

GO

Port scan results for [redacted]16.154
==========

Legend:
- port is OPEN
- port is CLOSED

PORT	Service	Status
21	FTP	✗
22	SSH	✗
23	Telnet	✗
25	SMTP	✗
53	DNS	✗
80	HTTP	✗
110	POP3	✗
139	NETBIOS	✗
143	IMAP	✗
443	HTTPS	✗
445	SMB	✗
1433	MSSQL	✗
1521	ORACLE	✗
3306	MySQL	✗
3389	Remote Desktop	✗

2. ISPs assign dynamic IP addresses to their customers. The frequency of change may vary. However, the information from the free Shodan scan is based on information conducted by weekly scans (Shodan Help Centre, no date). Hence it is possible that Shodan's weekly scan took place before a change in IP address, leading to no results being shown even if an open port was present.

Using WHOIS to check is registered on my public address

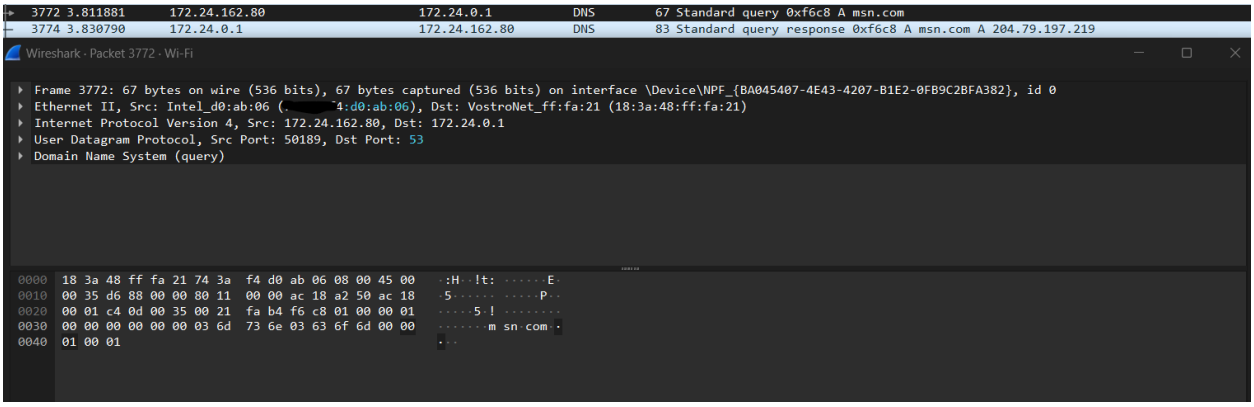
Searching my public IP address on WHOIS reveals my ISP as the associated organisation. WHOIS is a database that keeps track of who is assigned the IP addresses. Regional registries hand out the IP addresses to the various ISPs to be sold. Hence, the public IP is under my ISP.

Sniff Your Network and identify three used protocols

1) DNS Protocol

The DNS protocol helps translate human readable domain names like “msn.com” to numerical IP addresses that are used by computers like (204.79.197.219). DNS is a query/response protocol whereby the client queries requests for information in a single User Datagram Protocol (UDP), and receives a single UDP reply from the DNS server. The DNS uses UDP port 53 to connect to the server, but Transmission Control Protocol (TCP) may be used for larger data sizes (Notermans, 2017).

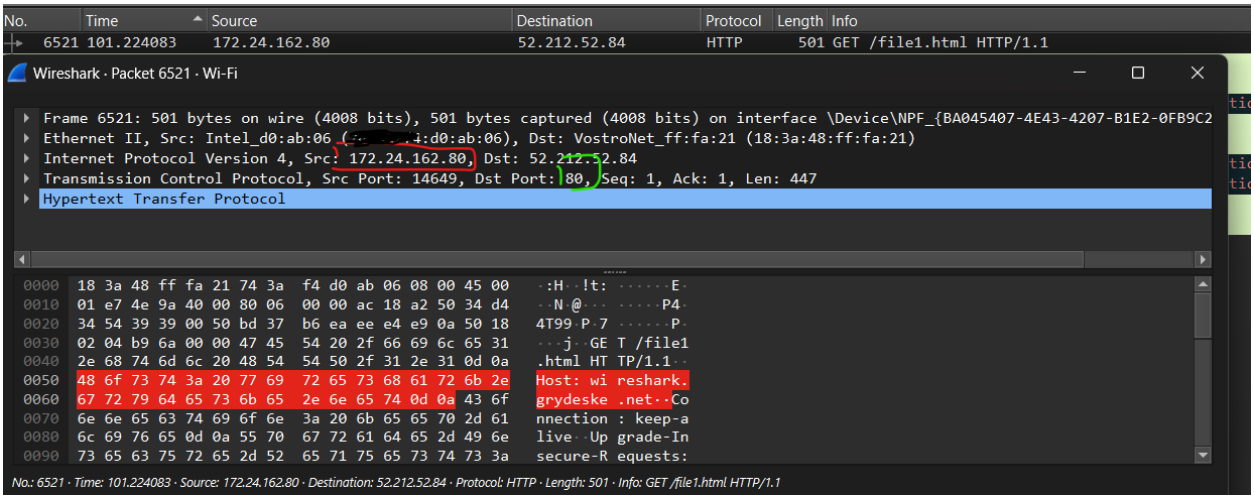
The attached image is a screen capture displaying the standard query for “msn.com” (from the computer with internal IP address 172.24.162.80) and the subsequent reply with the respective IP address from the DNS server (172.24.0.1). It also highlights the port number.



2) Hyper Text Transfer Protocol (HTTP)

The HTTP is designed to transfer information between networked devices, running on top of other layers of the network protocol stack. A typical process of HTTP involves a machine making a request to the server, which returns a response message (Cloudflare, no date). One of the most common HTTP methods is the ‘GET’ request, where the machine expects information back in return. This is commonly used for websites.

The following image is a HTTP protocol whereby the client (172.24.162.80) initiates a ‘GET’ request from IP address 52.212.52.84. From the screengrab, it also shows that port 80 is used.



3) DHCP

DHCP is a client/server protocol which automatically gives an IP host an IP address and other configuration information such as the subnet mask and default gateway. All devices on TCP/IP-based networks need to have a distinct IP address allocated to them in order to access the network and its resources. Without DHCP, IP addresses that move from one subnet to another must be configured manually (JasonGerend, 2021).

According to Droms (1997), the DHCP consists of 4 main phases: server discovery, IP lease offer, IP lease request and IP lease acknowledgement.

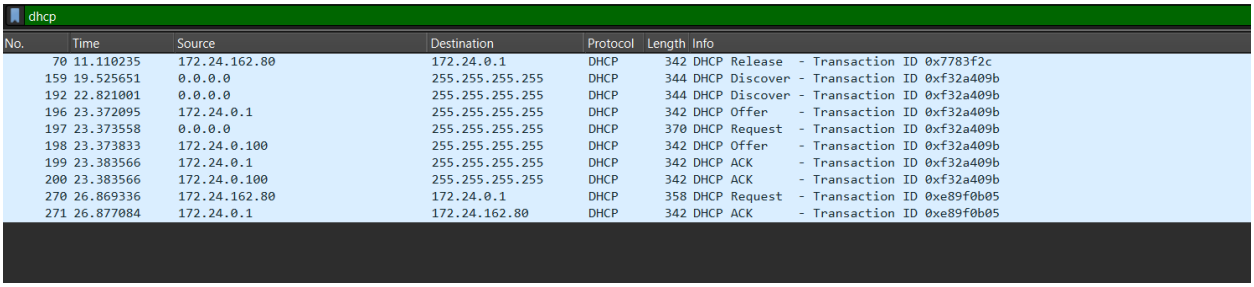
In server discovery, the device broadcasts a DHCPDISCOVER message on the network, which includes the client's MAC address.

Next, in the IP lease offer, DHCP servers that are listening on the network receive the DHCPDISCOVER message and willing servers respond with a DHCPOFFER message.

The device then chooses an offer, which then broadcasts a DHCPREQUEST message indicating its selection of the offered IP address.

Finally, the chosen server acknowledges the selection by sending a DHCPACK message, confirming the assignment of the offered IP address and other configuration settings to the client.

The following image gives an example of the mentioned process captured using wireshark.



Conclusion

By drafting out the network and researching my public IP address, I am able to find vulnerabilities in my network using websites like shodan.io. Despite discovering that my public IP address had no visible information available on shodan, I would not assume that my network is immune to cybersecurity vulnerabilities.

Mapping out the network also gave me insights into information not taught within the syllabus. For instance, the discovery of private MAC addresses and their benefits have been highlighted to me both as a consumer and as a future cybersecurity practitioner.

References

Apple Support (2023) *Use private wi-fi addresses on iPhone, iPad, iPod Touch and Apple Watch – Apple Support (AU)*, *Apple Support*. Available at: https://support.apple.com/en-au/102509 (Accessed: 01 April 2024).

Cloudfare (no date) *What is HTTP?* | *cloudflare*, *What is HTTP?* Available at: https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/ (Accessed: 01 April 2024).

Droms, R. (1997) *Dynamic Host Configuration Protocol*, *IETF Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc2131 (Accessed: 01 April 2024).

Higgins, Malcom (2020) *What is a default gateway?*, *NordVPN*. Available at: https://nordvpn.com/blog/what-is-a-default-gateway/#:~:text=The%20default%20gateway%20is%20the,make%20their%20devices%20more%20secure (Accessed: 01 April 2024).

JasonGerend (2021) *Dynamic Host Configuration Protocol (DHCP)*, *Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top (Accessed: 01 April 2024).

Kumar, S. (2023) *Arp commands*, *Tutorialspoint*. Available at: https://www.tutorialspoint.com/arp-commands (Accessed: 01 April 2024).

Notermans, T. (2017) *DNS query types and how to use DNS in performance troubleshooting*, *Accedian*. Available at: https://accedian.com/blog/dns-query-main-types/ (Accessed: 01 April 2024).

Shodan Help Centre (no date) *On-demand scanning - shodan help center*, *Shodan*. Available at: https://help.shodan.io/the-basics/on-demand-scanning#:~:text=Shodan%20crawls%20the%20entire%20Internet,scanning%20capabilities%20of%20the%20API. (Accessed: 01 April 2024).

Systeminfo command (2023) *Computer Hope*. Available at: https://www.computerhope.com/systemin.htm (Accessed: 01 April 2024).

What is shodan? - shodan help center (no date) *Shodan*. Available at: https://help.shodan.io/the-basics/what-is-shodan (Accessed: 01 April 2024).