



NET CRAFTS

COLLECTING INFORMATION

Author: Yvette K

CONTENTS

INTRODUCTION 03

METHODOLOGIES 04

DISCUSSION 05

CONCLUSION 08

REFERENCES 10

Introduction

The purpose of this report is to inspect the importance of a network map that shows all the devices in a home network and all the information these devices contain, investigate our public IP addresses and study protocols.

These are basic information that cybersecurity practitioners need to be familiar with and their importance in maintaining a safe cyber space will be studied.

Methodologies

Firstly, the Internet Service Provider's website was visited to view the router configuration page.

<https://whatismyipaddress.com/> was visited to find out what the external IP address was. Wireshark was then turned on to capture traffic.

The device's external IP address was searched on <https://www.shodan.io/> and <https://www.whois.com/>.

Lastly, the capture on Wireshark was studied to identify three different protocols and examine what interactions took place.

Discussion

Firstly, all the devices on the targeted network were mapped out by visiting its ISP's website to view the router configuration page and inspect the devices connected to the router.

The external IP address was obtained on <https://whatismyipaddress.com/>.

Wireshark was turned on to capture traffic while the external IP address was searched on <https://www.shodan.io/>, which is a search engine that allows users search for various types of servers connected to the internet, and received no results.

The external IP address was next searched on <https://www.whois.com/>, a widely used Internet record listing that identifies who owns a domain and how to get in contact with them, and found it registered to SingNet, along with some of their details, including address, email, phone and fax numbers.

Lastly, the capture on Wireshark was studied to identify three different protocols and examine what interactions took place.

ARP (Address Resolution Protocol)

The first protocol studied was ARP, which is responsible for finding the hardware (MAC) address of a host from a known IP address. It is one of the most important protocols of the Data Link (2) layer in the OSI model.

No.	Time	Source	Destination	Protocol	Length	Info
10	1.356469	fe80::1	fe80::4586:8c27:891...	ICMPv6	86	Neighbor Solicitation for fe80::4586:8c27:8914:3738 from 78:3e:a1:99:97:80
11	1.356659	fe80::4586:8c27:891...	fe80::1	ICMPv6	86	Neighbor Advertisement fe80::4586:8c27:8914:3738 (sol, ovr) is at d4:e9:8a:3d:f0:d1
12	1.361400	NokiaShangha_99:97:...	Intel_3d:f0:d1	ARP	60	Who has 192.168.1.17? Tell 192.168.1.254
13	1.361493	Intel_3d:f0:d1	NokiaShangha_99:97:...	ARP	42	192.168.1.17 is at ...:3d:f0:d1

> Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{7B13DD64-27-0000-8000-0000-000000000000}	0000	78 3e a1 99 97 80 d4 e9 8a 3d f0 d1 08 06 00 01	x>.....
> Ethernet II, Src: Intel_3d:f0:d1, Dst: NokiaShangha_99:97:80 (78:3e:a1:99:97:80)	0010	08 00 06 04 00 02 d4 e9 8a 3d f0 d1 c0 a8 01 11
> Address Resolution Protocol (reply)	0020	78 3e a1 99 97 80 c0 a8 01 fe	x>.....

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: Intel_3d:f0:d1
Sender IP address: 192.168.1.17
Target MAC address: NokiaShangha_99:97:80 (78:3e:a1:99:97:80)
Target IP address: 192.168.1.254

In the Wireshark capture above, we can see this exchange of information.

Unlike TCP or UDP, ARP does not use port numbers. Instead, ARP packets are identified by the EtherType value 0x0806 in Ethernet frames.

ARP is vulnerable to attacks such as ARP spoofing, where an attacker sends falsified ARP messages to associate their MAC address with the IP address of another device, potentially intercepting or disrupting network traffic.

DNS (Domain Name System)

DNS was the second protocol studied. It translates domain names to IP addresses, enabling web browsers to locate and interact with websites. It eliminates the need for humans to memorise numeric or alphanumeric IP addresses by converting a hostname, which is easier to remember, into a computer-friendly IP address.

No.	Time	Source	Destination	Protocol	Length	Info
214	2.526490	192.168.1.17	18.157.134.125	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
215	2.695125	192.168.1.17	192.168.1.254	DHIS	73	Standard Query 0x2694 A www.shodan.io
216	2.703635	18.157.134.125	192.168.1.17	TLSv1.2	344	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
217	2.709079	192.168.1.254	192.168.1.17	DHIS	105	Standard query response 0x2694 A www.shodan.io A 104.18.12.238 A 104.18.13.238
>	Frame 217: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface Device\NPF_{7B13D064-...}					0000 d4 e9 8a 3d f0 d1 78 3e a1 99 97 80 08 00 45 00 ...->x>.....E-
>	Ethernet II, Src: Nokiashangha_99:97:80 (78:3c:a1:99:97:80), Dst: Intel3d:f0:d1 (80:00:00:00:00:00)					0010 00 5b de 1c 40 00 40 11 d8 15 c0 a8 01 fe c0 a8 [...]@.@&.....
>	Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.17					0020 01 11 00 35 f5 22 00 47 41 7f 26 94 81 80 00 475"G A&.....
>	User Datagram Protocol, Src Port: 53, Dst Port: 62754					0030 00 02 00 00 00 00 03 77 77 77 06 73 81 80 64 61w ww-shoda
>	Domain Name System (response)					0040 6e 02 69 6f 00 00 01 00 c0 0c 00 01 00 01 00 n-io.....
						0050 00 01 27 00 04 68 12 0c ee c0 0c 01 00 01 00 ..'-h.....
						0060 00 01 27 00 04 68 12 0c ee ..'-h.....

It can be seen in the Wireshark capture above that www.shodan.io was translated to 104.18.12.238 and 104.18.13.238.

DNS's standard port number is 53. It operates primarily over UDP port 53 for standard queries and responses. For larger data transfers, such as zone transfers, DNS uses TCP port 53.

DNS can be targeted by attacks such as DNS spoofing or cache poisoning, where attackers manipulate DNS responses to redirect users to malicious sites.

TCP (Transmission Control Protocol)

The third protocol, TCP, is a connection-oriented communication protocol at the Transport Layer (Layer 4) of the OSI model that allows computing devices and application to send data via a network and verify its delivery. The task of this protocol is to carry packets across the Internet and one of its most critical features is the assurance of successful delivery on messages and data across networks. Before any data can be sent, the client and server must establish a connection.

Since TCP is connection based, it creates and maintains a connection between the receiver and sender while the data is being passed between them, thereby significantly reducing the likelihood of data corruption or loss during transmission.

TCP uses a three-way handshake to establish connections and verify data transmission. While this makes TCP highly reliable, it also introduces additional overhead, consuming more bandwidth compared to simpler protocols like UDP.

No.	Time	Source	Destination	Protocol	Length	Info
33	1.456140	192.168.1.17	142.251.10.106	UDP	133	49664 → 443 Len=91
34	1.473531	74.125.130.94	192.168.1.17	TCP	54	443 → 63618 [ACK] Seq=1 Ack=69 Win=301 Len=0
35	1.473531	74.125.130.94	192.168.1.17	TCP	54	443 → 63618 [ACK] Seq=1 Ack=108 Win=301 Len=0
36	1.473531	74.125.130.94	192.168.1.17	TLSv1.2	02	Application Data

> Frame 34: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{7B13DD64-27...} :3d:f0:d1
 > Ethernet II, Src: NokiaShangha_99:97:80 (78:3e:a1:99:97:80), Dst: Intel_3d:f0:d1
 > Internet Protocol Version 4, Src: 74.125.130.94, Dst: 192.168.1.17
 > Transmission Control Protocol, Src Port: 443, Dst Port: 63618, Seq: 1, Ack: 69, Len: 0

```

0000  d4 e9 8a 3d f0 d1 78 3e  a1 99 97 80 08 00 45 00  ...x> .....E
0010  00 28 0c 0b 00 00 75 06  ab 30 4a 7d 82 5e c0 a8  ..(...u:03)..^..
0020  01 11 01 bb f8 82 9b 57  a3 5d 7e a2 4f a8 50 10  ....W.]~O:P
0030  01 2d 18 d5 00 00
  
```

In the Wireshark capture above, we can see the acknowledgement received (third step of the three-way handshake), which is not required in UDP. In contrast, UDP (User Datagram Protocol) is a connectionless protocol that sends data via a network without verifying its delivery, which makes it faster and more efficient. This speed and efficiency however come at a cost of less error-checking mechanism that at times results in lost packets.

TCP is used by many application protocols, each of which has its own standard port number (e.g., HTTP uses TCP port 80, HTTPS uses TCP port 443).

TCP is susceptible to attacks such as SYN flooding, where an attacker exploits the handshake process to overwhelm a server with connection requests, potentially causing denial of service.

Conclusion

Through this mapping exercise, there is increased awareness of which devices are connected to our networks and users are better equipped to detect any unknown devices connected to their network. In the process of identifying each device, it was also discovered that Apple masks their MAC addresses to provide their users higher security to prevent device tracking and MAC address spoofing, enhancing user privacy on public and private networks.

From the search results of Shodan and whois, it can be seen that no personal information is available online on the external IP address. In the wrong hands, external IP addresses can be utilised to cause significant damage.

On the less damaging end of the spectrum, advertisers can embed trackers to record our IP address and send us targeted ads based on our browsing. Although targeted advertising may offer convenience, it raises significant privacy concerns.

The city indication from an IP address also means that with some sleuthing online, one may be able to find exact physical address of a target. While home invasions and thefts are rare in Singapore, it can happen. Stalkers can also use this information for nefarious intents.

On the darker end of the spectrum, skilled hackers can steal valuable information for identity thieves or impersonate targets online and frame targets for crimes such as buying and selling drugs or creating national security threats.

In an era of increasingly sophisticated cyber threats, the ability to visualise and understand one's network is not just beneficial—it is essential for robust cybersecurity. Through network mapping, we gain a comprehensive overview of all devices and connections within our home environment, enabling us to detect unauthorised access, identify vulnerabilities, and respond swiftly to potential incidents. This proactive approach is fundamental for both preventing breaches and optimising the performance and resilience of our networks.

Moreover, familiarity with protocols such as ARP, DNS, and TCP deepens our understanding of how information flows and where security controls must be applied. By regularly monitoring our public IP address and network activity, we can better protect our personal data from misuse by advertisers, stalkers, or cybercriminals.

Ultimately, as cybersecurity practitioners, maintaining up-to-date network maps and staying vigilant about network behaviours are foundational practices. These measures not only safeguard our digital assets but also empower us to adapt to evolving threats and ensure a safer cyberspace for all users.

References

Andriekutė, Aurelija. “What is a MAC address and how can you hide it?” *NordVPN*, Jan 02, 2023, <https://nordvpn.com/blog/mac-address/#:~:text=A%20hacker%20could%20use%20your,to%20the%20same%20Wi%2DFi>

Vigderman, Aliza and Turner, Gabe. “What Can Someone Do With Your IP Address?” *Security.org*, 19 March 2024, <https://www.security.org/vpn/what-can-someone-do-with-your-ip/#:~:text=If%20someone%20has%20your%20IP,is%20change%20your%20IP%20address>

Danao, Monique. “What Can Someone Do With Your IP Address?” *Forbes Advisor*, 27 November 2023, <https://www.forbes.com/advisor/business/what-can-someone-do-with-ip-address/#:~:text=An%20IP%20address%20is%20not,and%20launch%20cyberattacks%20or%20scams>

“How Address Resolution Protocol (ARP) works?” *GeeksforGeeks*, 13 February 2024, <https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/>

“What is DNS? | How DNS works” *Cloudflare*, <https://www.cloudflare.com/learning/dns/what-is-dns/>

BasuMallick, Chiradeep. “TCP vs. UDP: Understanding 10 Key Differences” *Spiceworks*, 18 April 2022, https://www.spiceworks.com/tech/networking/articles/tcp-vs-udp/#_001

“Network Mapping: A Vital Tool for Cybersecurity Professionals” *Blue Goat Cyber*, <https://bluegoatcyber.com/blog/network-mapping-a-vital-tool-for-cybersecurity-professionals/>

Ashtari, Hossein. “What Is Network Mapping? Definition, Process, Importance, and Best Practices for 2022” *Spiceworks*, 8 March 2022, <https://www.spiceworks.com/tech/networking/articles/what-is-network-mapping/>

“What is Network mapping?” *Reason Labs*, <https://cyberpedia.reasonlabs.com/EN/network%20mapping.html>

Pismisoglu, Sinan. “Network Topology and Mapping: Cornerstones of Data Security – Part 1” *Bradley*, 1 December 2023, <https://www.bradley.com/insights/publications/2023/12/network-topology-and-mapping-cornerstones-of-data-security--part-1>

Perplexity, <https://www.perplexity.ai/>