Intro to Cyber | Project: Net Crafts

Kenneth Wong

CFC190324

Trainer: Samson

Table of Contents

Introduction

In our current digital age where so many devices are interconnected. It is of utmost importance to understanding our network.

This project aims at network mapping, identifying all devices, their communication protocols, and strategic infrastructure points are crucial information to have for safeguarding it and making more informed decisions.

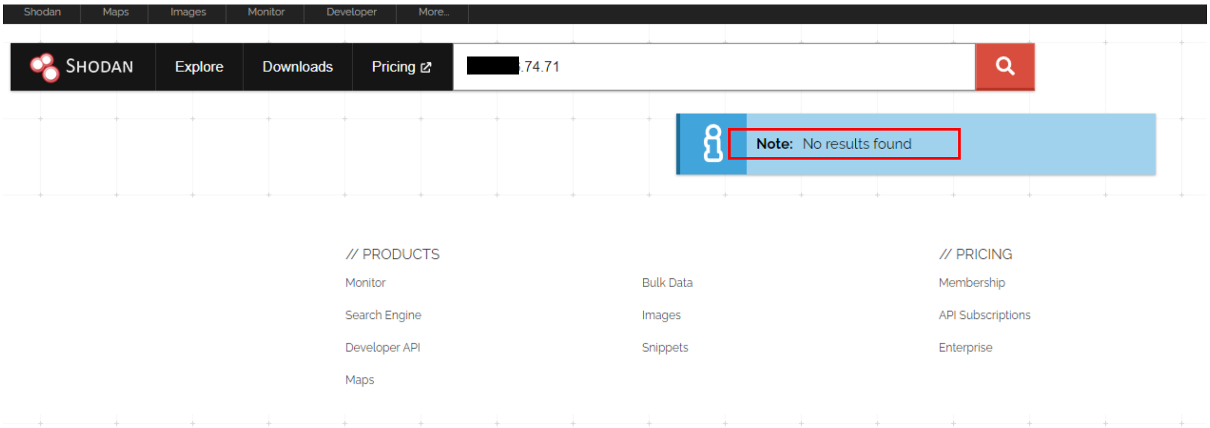
In a world where cybersecurity threats are prevalent, mapping our network and being able to conduct our OSINT (Open-sourced intelligence) research becomes indispensable.

By meticulously analyzing our network topology, we would then be able to understand its structure, vulnerabilities, and potential threats. This comprehensive understanding allows us to make informed decisions and strengthen our network.

The report aims to provide an overview of network mapping and cybersecurity practices in our interconnected digital environment with an emphasis on the significance of understanding our network infrastructure, identifying devices through the router's settings and utilizing tools like Shodan and WHOIS for IP address retrieval. Through conducting the following research, we have gained invaluable insights into my network's structure, vulnerabilities, and potential threats.

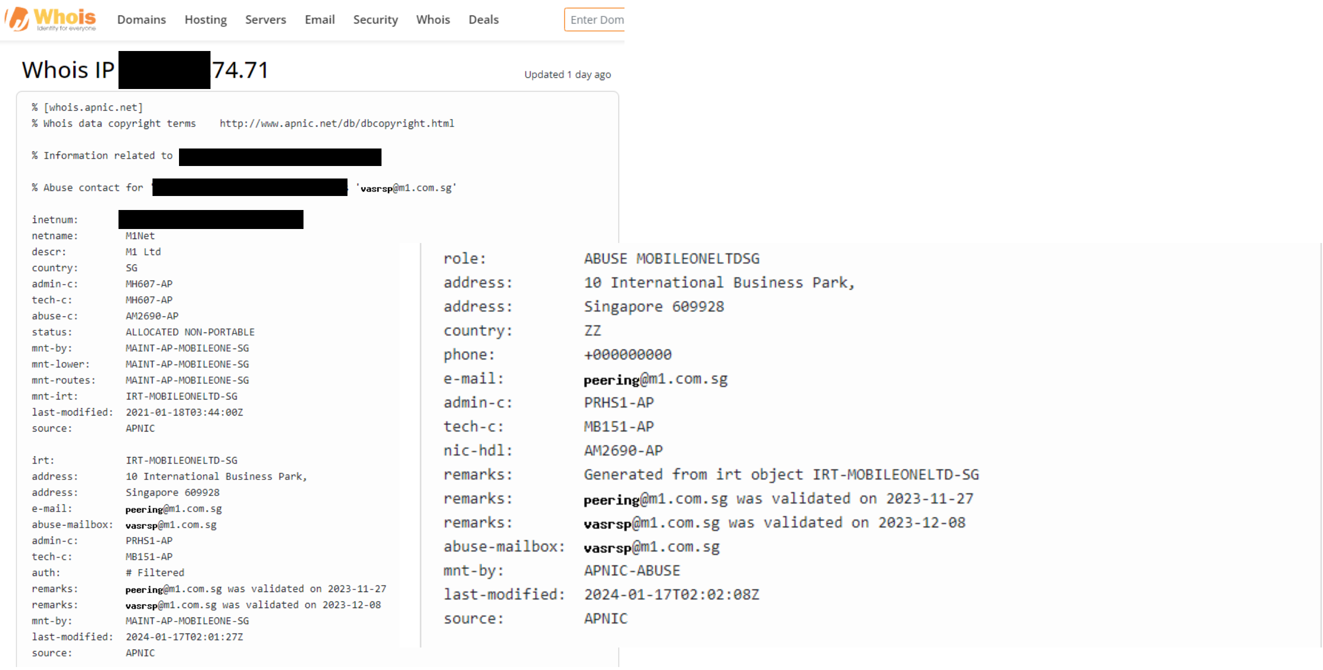
Methodologies

Shodan



When searching our IP on Shodan, there are no results displayed. Likely due to my external IP address which the ISP (Internet service provider) has provided being a dynamic one instead of static. Also, the norm for Singapore ISP is to provide customers with dynamic IP addresses. Shodan indexes IP addresses based on their availability at the time of scanning. If your IP address changes before or after a scan, it may not appear in Shodan's database.

Whois



Whois IP [redacted] 74.71

Updated 1 day ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to [redacted]

% Abuse contact for [redacted] 'vasrsp@m1.com.sg'

inetnum:        [redacted]
netname:        M1Net
descr:          M1 Ltd
country:        SG
admin-c:        MH607-AP
tech-c:         MH607-AP
abuse-c:        AM2690-AP
status:         ALLOCATED NON-PORTABLE
mnt-by:         MAINT-AP-MOBILEONE-SG
mnt-lower:      MAINT-AP-MOBILEONE-SG
mnt-routes:     MAINT-AP-MOBILEONE-SG
mnt-irt:        IRT-MOBILEONELTD-SG
last-modified:  2021-01-18T03:44:00Z
source:         APNIC

irt:            IRT-MOBILEONELTD-SG
address:        10 International Business Park,
address:        Singapore 609928
e-mail:         peering@m1.com.sg
abuse-mailbox:  vasrsp@m1.com.sg
admin-c:        PRHS1-AP
tech-c:         MB151-AP
auth:           # Filtered
remarks:        peering@m1.com.sg was validated on 2023-11-27
remarks:        vasrsp@m1.com.sg was validated on 2023-12-08
mnt-by:         MAINT-AP-MOBILEONE-SG
last-modified:  2024-01-17T02:01:27Z
source:         APNIC
```

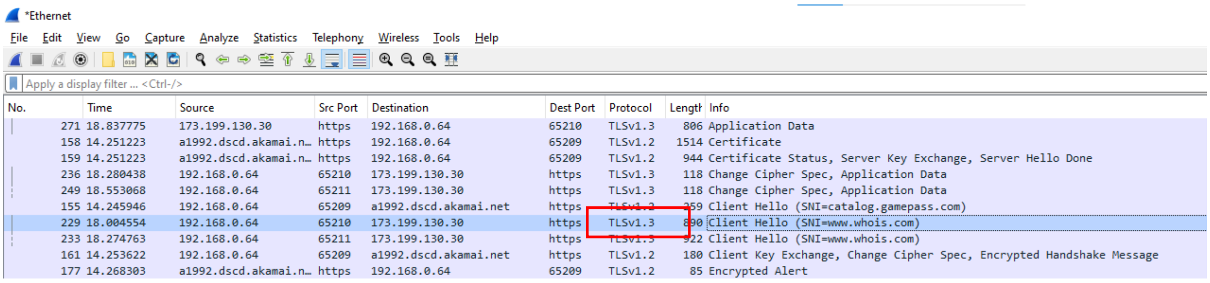
```
role:           ABUSE MOBILEONELTDSG
address:        10 International Business Park,
address:        Singapore 609928
country:        ZZ
phone:          +000000000
e-mail:         peering@m1.com.sg
admin-c:        PRHS1-AP
tech-c:         MB151-AP
nic-hdl:        AM2690-AP
remarks:        Generated from irt object IRT-MOBILEONELTD-SG
remarks:        peering@m1.com.sg was validated on 2023-11-27
remarks:        vasrsp@m1.com.sg was validated on 2023-12-08
abuse-mailbox:  vasrsp@m1.com.sg
mnt-by:         APNIC-ABUSE
last-modified:  2024-01-17T02:02:08Z
source:         APNIC
```

Upon using Whois, we find out that our IP address is registered under the ISP. What this could it mean is that the ISP; in this case M1, is the entity responsible for allocating and managing that IP address.

ISPs typically own a block of IP addresses which are then assigned to their subscribers which is also reflected in the above search result.

Wireshark

TLS 1.3 (Transport layer security)

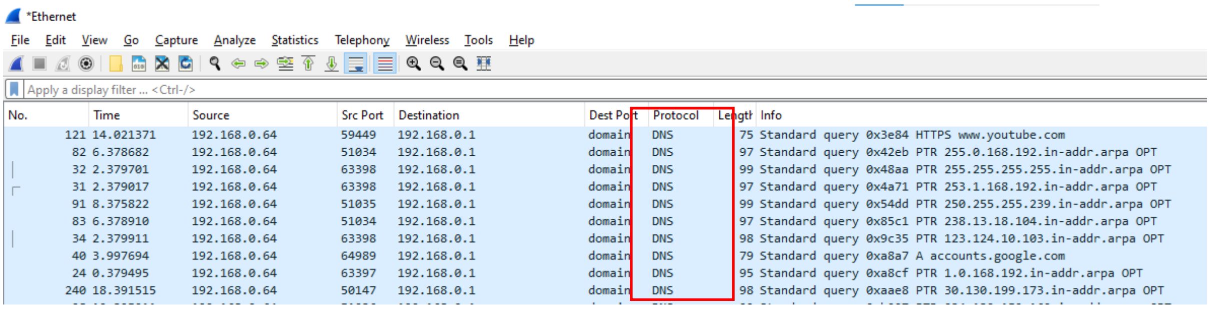

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
271	18.837775	173.199.130.30	https	192.168.0.64	65210	TLSv1.3	806	Application Data
158	14.251223	a1992.dscd.akamai.n…	https	192.168.0.64	65209	TLSv1.2	1514	Certificate
159	14.251223	a1992.dscd.akamai.n…	https	192.168.0.64	65209	TLSv1.2	944	Certificate Status, Server Key Exchange, Server Hello Done
236	18.280438	192.168.0.64	65210	173.199.130.30	https	TLSv1.3	118	Change Cipher Spec, Application Data
249	18.553068	192.168.0.64	65211	173.199.130.30	https	TLSv1.3	118	Change Cipher Spec, Application Data
155	14.245946	192.168.0.64	65209	a1992.dscd.akamai.net	https	TLSv1.2	259	Client Hello (SNI=catalog.gamepass.com)
229	18.004554	192.168.0.64	65210	173.199.130.30	https	TLSv1.3	890	Client Hello (SNI=www.whois.com)
233	18.274763	192.168.0.64	65211	173.199.130.30	https	TLSv1.3	922	Client Hello (SNI=www.whois.com)
161	14.253622	192.168.0.64	65209	a1992.dscd.akamai.net	https	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
177	14.268303	a1992.dscd.akamai.n…	https	192.168.0.64	65209	TLSv1.2	85	Encrypted Alert

TLS 1.3 is the latest version of the TLS protocol. TLS, which is used by HTTPS and other network protocols for encryption, is the modern version of SSL. TLS 1.3 dropped support for older, less secure cryptographic features, and it sped up TLS handshakes, among other improvements.

The default port for TLSv1.3 is the same as other versions of TLS, which is typically port 443 for HTTPS connections. However, TLS can be used with other protocols as well, so the port number may vary depending on the specific application or service using TLSv1.3.

DNS (Domain name system)


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
121	14.021371	192.168.0.64	59449	192.168.0.1	domain	DNS	75	Standard query 0x3e84 HTTPS www.youtube.com
82	6.378682	192.168.0.64	51034	192.168.0.1	domain	DNS	97	Standard query 0x42eb PTR 255.0.168.192.in-addr.arpa OPT
32	2.379701	192.168.0.64	63398	192.168.0.1	domain	DNS	99	Standard query 0x48aa PTR 255.255.255.255.in-addr.arpa OPT
31	2.379017	192.168.0.64	63398	192.168.0.1	domain	DNS	97	Standard query 0x4a71 PTR 253.1.168.192.in-addr.arpa OPT
91	8.375822	192.168.0.64	51035	192.168.0.1	domain	DNS	99	Standard query 0x54dd PTR 250.255.255.239.in-addr.arpa OPT
83	6.378910	192.168.0.64	51034	192.168.0.1	domain	DNS	97	Standard query 0x85c1 PTR 238.13.18.104.in-addr.arpa OPT
34	2.379911	192.168.0.64	63398	192.168.0.1	domain	DNS	98	Standard query 0x9c35 PTR 123.124.10.103.in-addr.arpa OPT
40	3.997694	192.168.0.64	64989	192.168.0.1	domain	DNS	79	Standard query 0xa8a7 A accounts.google.com
24	0.379495	192.168.0.64	63397	192.168.0.1	domain	DNS	95	Standard query 0xa8cf PTR 1.0.168.192.in-addr.arpa OPT
240	18.391515	192.168.0.64	50147	192.168.0.1	domain	DNS	98	Standard query 0xaae8 PTR 30.130.199.173.in-addr.arpa OPT

The DNS protocol allows us to translate human-readable domain names to machine readable IP addresses. The DNS protocol is like a phonebook for the internet, which allows us to remember easy-to-remember domain names when we want to visit websites.

When you type a website into a browser, your computer will kickstart the process of finding the IP address for the website. The computer will then search for the IP address for the domain name in the local DNS cache or in the resolver's cache.

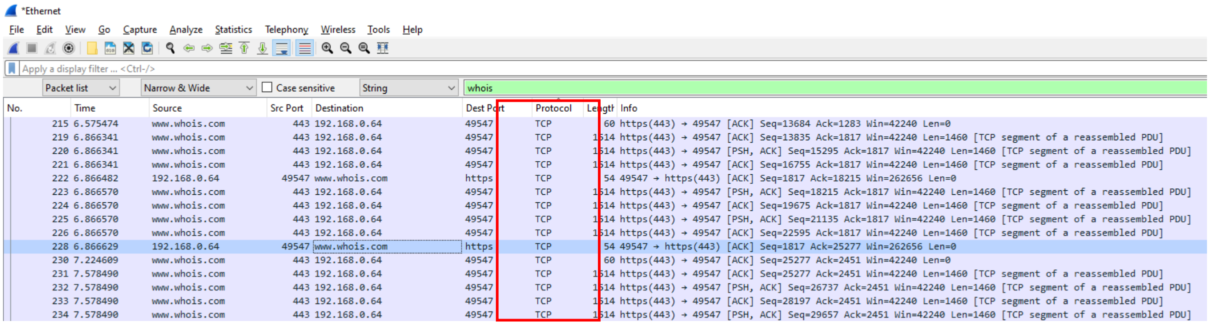
If the information is found, the website will begin to load quickly. Otherwise, the recursive DNS server or servers query elsewhere. The query will continue up the chain of authoritative DNS servers. The server continues its search until it finds a nameserver for the domain. These authoritative nameservers store these records for their respective domain names.

The queries go through a number of DNS servers until it reaches the authoritative DNS server with information on the domain name

The authoritative DNS server responds to the query by providing the IP address associated with the domain name. Once we get the IP address, we are then connected to the server and the IP address may then be cached by the computer or DNS resolver for future use.

The standard port for used for communication between a DNS client and serve r is port 53.

TCP


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Packet list
Narrow & Wide
□ Case sensitive
String
whois

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
215	6.575474	www.whois.com	443	192.168.0.64	49547	TCP	60	https(443) → 49547 [ACK] Seq=13684 Ack=1283 Win=42240 Len=0
219	6.866341	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [ACK] Seq=13835 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
220	6.866341	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [PSH, ACK] Seq=15295 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
221	6.866341	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [ACK] Seq=16755 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
222	6.866482	192.168.0.64	49547	www.whois.com	https	TCP	54	49547 → https(443) [ACK] Seq=1817 Ack=18215 Win=262656 Len=0
223	6.866570	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [PSH, ACK] Seq=18215 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
224	6.866570	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [ACK] Seq=19675 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
225	6.866570	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [PSH, ACK] Seq=21135 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
226	6.866570	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [ACK] Seq=22595 Ack=1817 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
228	6.866629	192.168.0.64	49547	www.whois.com	https	TCP	54	49547 → https(443) [ACK] Seq=1817 Ack=25277 Win=262656 Len=0
230	7.224609	www.whois.com	443	192.168.0.64	49547	TCP	60	https(443) → 49547 [ACK] Seq=25277 Ack=2451 Win=42240 Len=0
231	7.578490	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [ACK] Seq=25277 Ack=2451 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
232	7.578490	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [PSH, ACK] Seq=26737 Ack=2451 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
233	7.578490	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [ACK] Seq=28197 Ack=2451 Win=42240 Len=1460 [TCP segment of a reassembled PDU]
234	7.578490	www.whois.com	443	192.168.0.64	49547	TCP	1514	https(443) → 49547 [PSH, ACK] Seq=29657 Ack=2451 Win=42240 Len=1460 [TCP segment of a reassembled PDU]

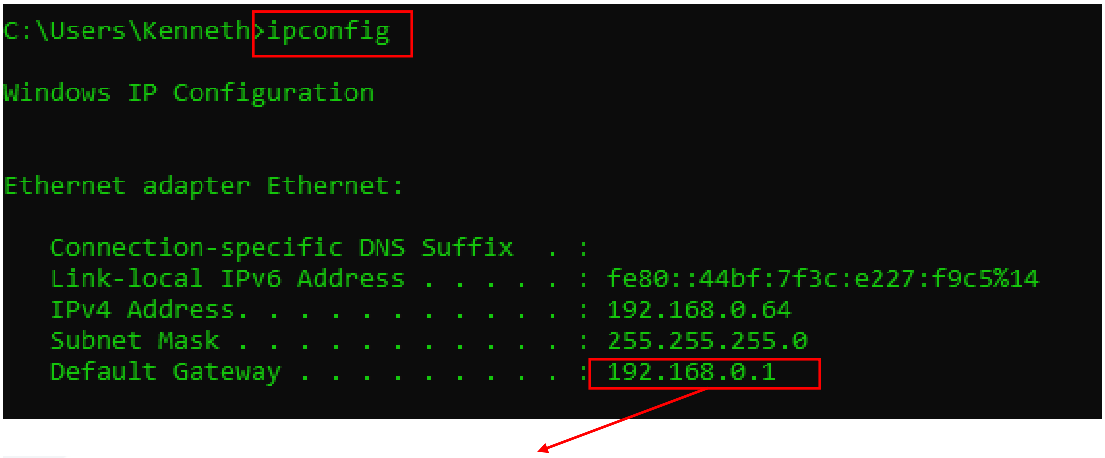
TCP is used at the transport layer to ensure reliable data delivery between the computer and the website. It establishes a connection between the device and the server to facilitate the transfer of Whois query and response data.

TCP does not have a fixed port number that it uses. Instead, TCP dynamically assigns source and destination ports as part of the TCP header in each TCP segment. This allows multiple network applications to communicate simultaneously over the same IP address.

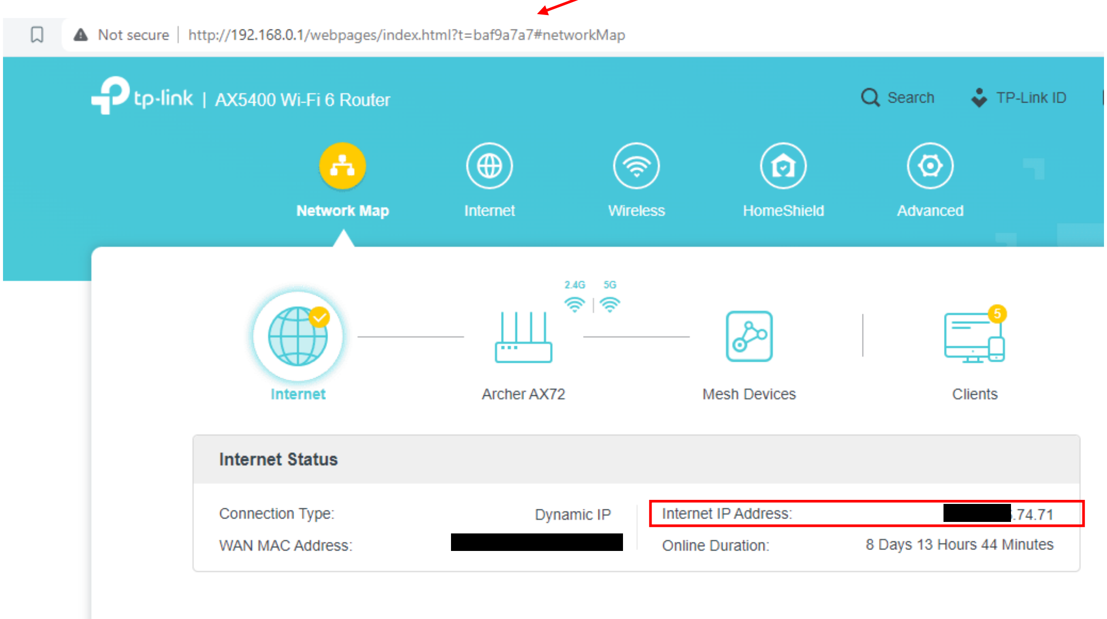
However, in this case, it uses port 443 which whois.com uses for encrypted browsing.

IP address of router / Public IP address

CMD – ipconfig – The *ipconfig* command is used to display information about your network configuration and refresh DHCP and DNS Settings. By default, the *ipconfig* command displays the IP Address, Subnet Mask, and default gateway.



```
C:\Users\Kenneth>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::44bf:7f3c:e227:f9c5%14
   IPv4 Address. . . . . . . . . . . : 192.168.0.64
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1
```



Not secure | http://192.168.0.1/webpages/index.html?t=baf9a7a7#networkMap

Internet Status

Connection Type: Dynamic IP

WAN MAC Address: [redacted]

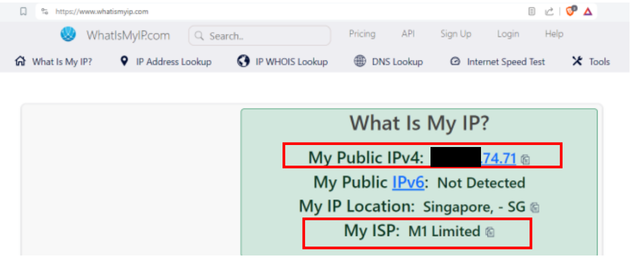
Internet IP Address: [redacted].74.71

Online Duration: 8 Days 13 Hours 44 Minutes

Access the router page which then shows the IP address.

Internet service provider / Public IP address

Access whatismymyip.com



What Is My IP?

My Public IPv4: [redacted].74.71

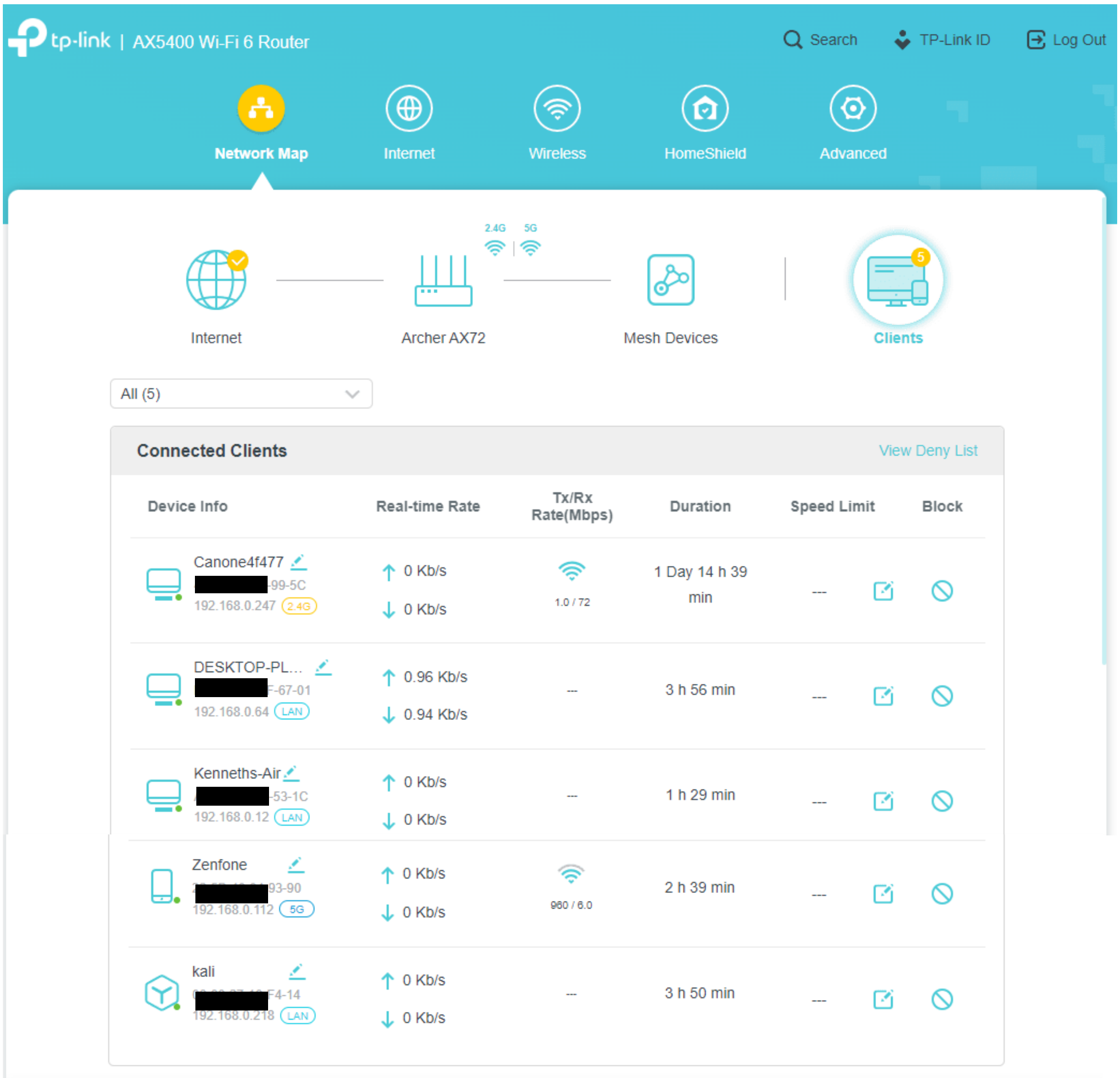
My Public IPv6: Not Detected

My IP Location: Singapore, - SG

My ISP: M1 Limited

Finding all connected devices / Device names / IP / MAC addresses

Network map > Clients



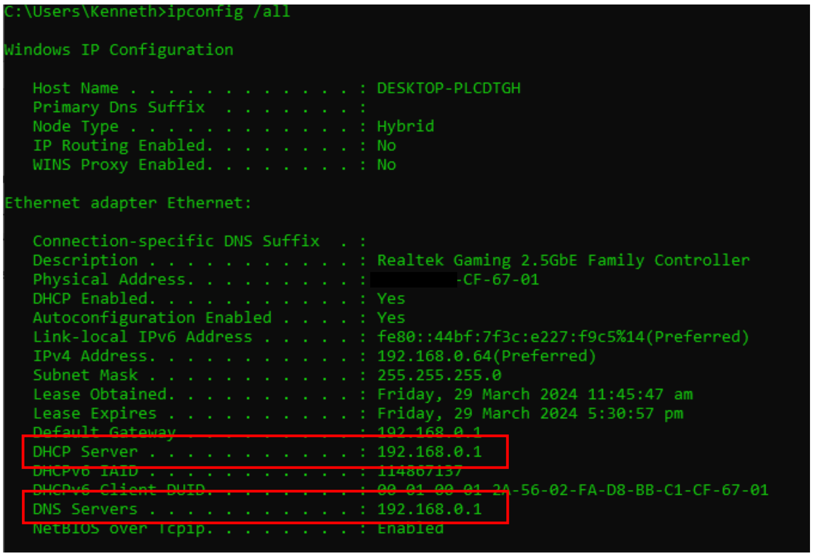
Connected Clients

View Deny List

Device Info	Real-time Rate	Tx/Rx Rate(Mbps)	Duration	Speed Limit	Block
Canone4f477 [redacted]-99-5C 192.168.0.247 2.4G	↑ 0 Kb/s ↓ 0 Kb/s	1.0 / 72	1 Day 14 h 39 min	---	⊘
DESKTOP-PL... [redacted]F-67-01 192.168.0.64 LAN	↑ 0.96 Kb/s ↓ 0.94 Kb/s	---	3 h 56 min	---	⊘
Kenneths-Air [redacted]-53-1C 192.168.0.12 LAN	↑ 0 Kb/s ↓ 0 Kb/s	---	1 h 29 min	---	⊘
Zenfone [redacted]93-90 192.168.0.112 5G	↑ 0 Kb/s ↓ 0 Kb/s	960 / 6.0	2 h 39 min	---	⊘
kali [redacted]F4-14 192.168.0.218 LAN	↑ 0 Kb/s ↓ 0 Kb/s	---	3 h 50 min	---	⊘

DNS and DHCP server

CMD – ipconfig / all



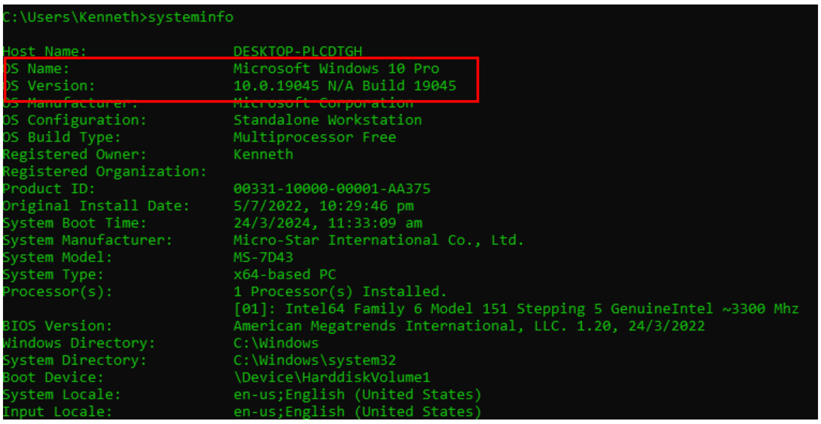
```
C:\Users\Kenneth>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-PLCDTGH
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek Gaming 2.5GbE Family Controller
   Physical Address. . . . . . . . . : [redacted]-CF-67-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::44bf:7f3c:e227:f9c5%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.64(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, 29 March 2024 11:45:47 am
   Lease Expires . . . . . . . . . . : Friday, 29 March 2024 5:30:57 pm
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 114867137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-56-02-FA-D8-BB-C1-CF-67-01
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

/ all – The */all* flag will show all the information about your network adapter:

- **Physical Address**: This is the MAC address of your network adapter.
- **DHCP Enabled**: Indicates if the network connection is using DHCP or Static IP Address
- **IPv4 Address**: The IP Address of your computer
- **Default Gateway**: The router to which your computer is connected
- **DHCP Server**: Router/server that hands out IP Addresses in your network
- **DNS Servers**: Servers used to translate domain names to IP Addresses
- **Link-Local IPv6 Address**: IPv6 address of your computer (often not used)
- **Lease Obtained**: Date-time when your computer received the IP Address

OS and device version

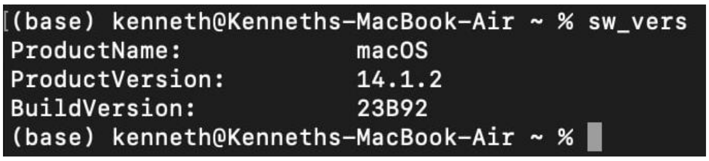
CMD – systeminfo – The *systeminfo* command displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards).



```
C:\Users\Kenneth>systeminfo

Host Name:                 DESKTOP-PLCDTGH
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Kenneth
Registered Organization:
Product ID:                00331-10000-00001-AA375
Original Install Date:     5/7/2022, 10:29:46 pm
System Boot Time:          24/3/2024, 11:33:09 am
System Manufacturer:       Micro-Star International Co., Ltd.
System Model:              MS-7D43
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 151 Stepping 5 GenuineIntel ~3300 Mhz
BIOS Version:              American Megatrends International, LLC. 1.20, 24/3/2022
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
```

Identifying the OS and device version on macOS

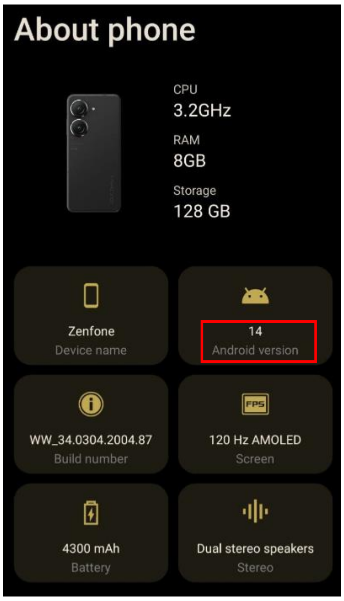
Terminal – sw_vers



```
(base) kenneth@Kenneths-MacBook-Air ~ % sw_vers
ProductName:            macOS
ProductVersion:         14.1.2
BuildVersion:           23B92
(base) kenneth@Kenneths-MacBook-Air ~ %
```

Identifying the OS and device version on android OS

Settings > System > About phone



About phone

CPU
3.2GHz

RAM
8GB

Storage
128 GB

Zenfone
Device name

14
Android version

WW_34.0304.2004.87
Build number

120 Hz AMOLED
Screen

4300 mAh
Battery

Dual stereo speakers
Stereo

Discussion

ipconfig /all

The ‘/all’ flag displays detailed information about all adapters, including the IP address, subnet mask, default gateway, DHCP server, and DNS servers.

We used ipconfig ‘/all’ to gather information about the computer’s network configuration. It serves multiple crucial purposes in the context of network administration and troubleshooting. As we are searching for the DNS server and DHCP server, it allows them to be properly configured and lets us diagnose any problems if they were to surface.

While the router administration page is a common method to access DNS and DHCP server information, using the command on a Windows system offers a more direct approach.

systeminfo

Systeminfo command serves as an efficient way to gather comprehensive information about the operating system (OS) and its version in Windows environments. With that, we are able to access a wealth of data including OS version, service pack level, system architecture, installation date, etc. This command provides crucial insights for system administration, troubleshooting, and software compatibility checks.

Alternatively, we could can navigate through the graphical user interface (GUI) to access basic system information. Tools like the System Properties window offers quick access to OS version and system type details. While GUI-based methods are user-friendly, they may lack the depth of information provided by systeminfo.

We have used the equivalent of command for my connected MacBook Air which is “sw_vers” and doublechecked the result by navigating through the settings using the GUI.

Conclusion

Working on this project opened our eyes with regards to the point of entries susceptible to attacks in which attackers has for our devices.

We are now able to recognize devices in my network which allows us to identify any rogue ones which are connected to our network in the future. Additionally, this project has equipped us with tools such as command prompt and the confidence in tinkering with the router settings to identify connectivity issues which we have normally been averse to.

We had to start off this project by resetting my router as the password had been changed and forgotten which led to a slew of problems for my home security cameras. We was not able to reconnect them to our network as we did not know how. Hence, they have been excluded from this project.

Wi-Fi devices present a security concern as they have full access to the internet. Attackers can be in the same general area as our Wi-Fi devices, allowing them to monitor the traffic being sent to and from your mobile and Wi-Fi devices which could be an opportunity for attackers to sit in between conversations using an on-path attack. If they are in the area, they can cause interference over the Wi-Fi creating a DoS (Denial of service attack) – mainly applicable in a workplace.

Continuously monitoring our connected devices allows us to detect any unusual behaviour or suspicious network traffic patterns which signals potential malicious activity. By comparing ongoing observations with established norms, we would be able to swiftly respond to threats and mitigate security breaches.

At the workplace, in the event of a security incident, having a clear view of network-connected devices streamlines our response efforts. This enables us to promptly assess the incident's impact, isolate affected devices, and take remedial actions to contain and eliminate threats.

In conclusion, comprehending and keeping an eye on the devices linked to our network are vital steps in safeguarding out interests. With the insights gained from device discovery and monitoring, we would then be able to take proactive measures to safeguarding our network assets.

Recommendation

Most wireless routers come pre-set with a default password which is easy to guess by malicious actors as long as they have information on the router manufacturer. It is important to select a secure password with an increased amount of entropy as it would prevent attackers from using password spraying or brute force attack. You may wish to use something which is not single-worded or obvious with a mix of upper- and lower-case letters, numbers, and special characters with at least 8 characters.

It is also advisable to use different passwords for each account; which would lead to the issue of remembering all of them to be a hassle. What we can do is to use a password manager to store all of them in a single database for easy access.

In our router configurations, we can also enable WPA2 or WPA3 encryption protocols which are used to secure our Wi-Fi network.

Additionally, we can ensure that all connected devices are properly updated. This will increase the odds that malicious will not be able to access our devices on our network as these updates often contain fixes for security vulnerabilities.

We could also use firewalls also provide protection against attackers by protecting your computer or network from malicious or unwanted network traffic.

Last but not least, it is crucial educate family members about cybersecurity best practices as they are all sharing the same network. By adopting safe browsing and email habits, family members contribute to the overall safety of the home Wi-Fi network.

References

1. LazyAdmin. "Home Network Diagram." https://lazyadmin.nl/home-network/home-network-diagram/.

2. Javatpoint. "How to Check Kali Linux Version." https://www.javatpoint.com/how-to-check-kali-linux-version.

3. Microsoft. "Systeminfo Command." https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo.

4. NordLayer. "How to Find the macOS Version Number Through Terminal." https://help.nordlayer.com/docs/macos-version-number#:~=To%20find%20the%20macOS%20version,to%20Apple%20%3E%20About%20This%20Mac.

5. Cisco. "What is Device Security?" https://www.cisco.com/c/en/us/products/security/what-is-device-security.html#~edge-devices.

6. Norton. "Keep Your Home Wi-Fi Safe." https://us.norton.com/blog/iot/keep-your-home-wifi-safe.

7. Chapple, Mike. *CompTIA Security+ Study Guide (SY0-701): Comprehensive Preparation for CompTIA Security+ Certification Exam.*

8. Cloudflare. "Why Use TLS 1.3?" https://www.cloudflare.com/learning/ssl/why-use-tls-1.3/#:~=TLS%201.3%20is%20the%20latest,TLS%20handshakes%2C%20among%20other%20improvements.

9. Encryption Consulting. "What is a TLS/SSL Port?" https://www.encryptionconsulting.com/what-is-a-tls-ssl-port/#:~=So%2C%20what%20port%20does%20TLS,protocol%20port%20(port%2080).

10. LiquidWeb. "How to Demystify the DNS Process." https://www.liquidweb.com/kb/how-to-demystify-the-dns-process/.

11. Fortinet. "What is ARP?" https://www.fortinet.com/resources/cyberglossary/what-is-arp.