PROJECT:
MY NETWORK

INTRO TO CYBER

TAN KE HAN KEITH
[S9]

NETWORK MAP

XX . XX . 184 . 72

welcome home, Keith Tan

Cisco AnyConnect VPN
(VPN Server)
New DNS IP Address: 10.8.28.5
New Default Gateway IP Addr: 10.119.176.1
New MAC Address: XX:XX:XX:3C:7A:00
New VPN IP Address: 10.119.181.86

THE INTERNET

VPN Router

Samsung Galaxy A34 5G
Operating System: Android 13
IP Address: 192.168.50.14
MAC Address: XX:XX:XX:DF:B8:F1

ISP: Starhub Cable Vision
External IP Address: XX.XX.184.72

Encrypted VPN Tunnel

iPhone 15 Pro Max
Operating System: iOS 17.0.3 (21A360)
IP Address: 192.168.50.90
MAC Address: XX:XX:XX:96:F6:77

Mesh Router:
Asus ZenWiFi AX6600
Internal IP Address: 192.168.50.1
DHCP IP Address: 192.168.50.1
DNS IP Address: 192.168.50.1
Default Gateway IP Address: 192.168.50.1
MAC Address: XX:XX:XX:1B:8C:D0

Mesh Node:
Asus ZenWiFi AX6600

Macbook Pro 14-inch, 2023
(Personal)
Operating System: macOS Sonoma 14.0
IP Address: 192.168.50.193
MAC Address: XX:XX:XX:C6:CD:7A

Ethernet

Dell XPS 13, 2020
(Personal)
Operating System: Microsoft Windows 11 Home
IP Address: 192.168.50.207
MAC Address: XX:XX:XX:5E:AD:F6

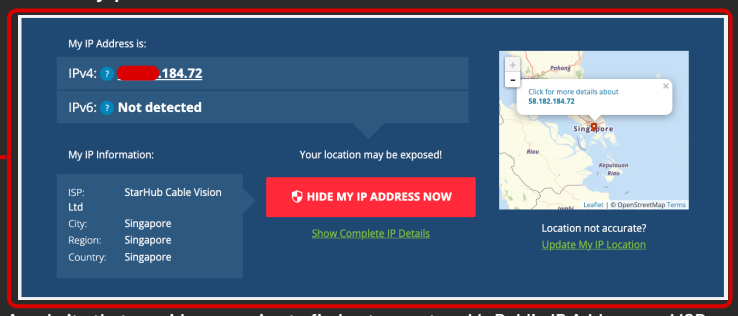
Lenovo ThinkPad T14 Gen 2
(Work)
Operating System: Microsoft Windows 10
IP Address: 192.168.50.37
MAC Address: XX:XX:XX:FB:68:D7

DOCUMENTATION

MESH ROUTER: ASUS ZENWIFI AX6600

ISP: Starhub Cable Vision
External IP Address: XX.XX.184.72

whatismyipaddress.com



A website that provides a service to find out my network's Public IP Address and ISP.

Mesh Router:
Asus ZenWiFi AX6600

Internal IP Address: 192.168.50.1
DHCP IP Address: 192.168.50.1
DNS IP Address: 192.168.50.1
Default Gateway IP Address: 192.168.50.1
MAC Address: XX:XX:XX:1B:8C:D0

Terminal > netstat -nr | grep default

```
keithtan@Keiths-MBP ~ % netstat -nr | grep default
default            192.168.50.1       UGScg                en0
default            link#24            UCSIg           bridge100      !
default            link#26            UCSIg           bridge101      !
default                                 fe80::%utun0                          UGcIg                utun0
default                                 fe80::%utun1                          UGcIg                utun1
default                                 fe80::%utun2                          UGcIg                utun2
default                                 fe80::%utun3                          UGcIg                utun3
default                                 fe80::%utun4                          UGcIg                utun4
default                                 fe80::%utun5                          UGcIg                utun5
default                                 fe80::%utun6                          UGcIg                utun6
keithtan@Keiths-MBP ~ %
```

Terminal command filters out the default gateway and internal IP Address of the Router.

Terminal > arp -a

```
keithtan@Keiths-MBP ~ % arp -a
zenwifi_xt8-8cd0 (192.168.50.1) at c8:7f:54:1b:8c:d0 on en0 ifscope [ethernet]
? (192.168.50.90) at de:df:c4:ae:66:57 on en0 ifscope [ethernet]
lgwebostv (192.168.50.167) at 30:a9:de:b3:ed:de on en0 ifscope [ethernet]
laptop-6mm9623c (192.168.50.242) at 58:96:1d:f7:b9:67 on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on bridge100 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on bridge101 ifscope permanent [ethernet]
keithtan@Keiths-MBP ~ %
```

Terminal command displays the ARP cache, listing IP Addresses with their associated MAC Addresses, for devices within my local network

Terminal > scutil --dns

```
keithtan@Keiths-MBP ~ % scutil --dns
DNS configuration

resolver #1
  nameserver[0] : 192.168.50.1
  if_index : 15 (en0)
  flags    : Request A records
  reach    : 0x00020002 (Reachable,Directly Reachable Address)
```

Terminal command displays the DNS configuration information and settings.

- In Unix OS, "resolver" handles translation of domain names into IP Addresses by working with DNS settings and configurations.
- "if_index" refers to unique identifier assigned to a network interface within the computer.
- "flags: Request A records" mean that the DNS query is seeking IPv4 address associated with a given domain name.

Terminal > ipconfig getpacket en0

```
keithtan@Keiths-MBP ~ % ipconfig getpacket en0
op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0xa3b43118
secs = 0
ciaddr = 192.168.50.193
yiaddr = 192.168.50.193
siaddr = 192.168.50.1
giaddr = 0.0.0.0
chaddr = 80:65:7c:c6:cd:7a
sname =
file =
options:
Options count is 10
dhcp_message_type (uint8): ACK 0x5
server_identifier (ip): 192.168.50.1
lease_time (uint32): 0x15180
renewal_t1_time_value (uint32): 0x9d63
rebinding_t2_time_value (uint32): 0x11bf3
subnet_mask (ip): 255.255.255.0
broadcast_address (ip): 192.168.50.255
domain_name_server (ip_mult): {192.168.50.1}
router (ip_mult): {192.168.50.1}
end (none):
keithtan@Keiths-MBP ~ %
```

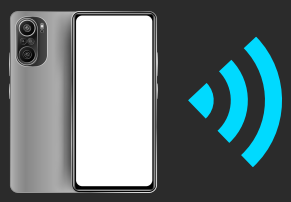
→ DHCP Server IP Address

Terminal command retrieves detailed network configuration for "en0" which represents the primary network interface.

- op = BOOTREPLY: Indicates this is a DHCP response packet (not request packet).
- htype: Hardware type, where "1" means Wi-Fi is used (not Ethernet).
- flags: Provides information/instructions on how the packet should be handled.
- hlen: Hardware address length.
- hops: Number of relay agents (routers) packet has passed through.
- xid: Transaction ID for the DHCP transaction.
- secs: Seconds passed where client has been trying to obtain an IP Address.
- ciaddr: Client IP Address, the current IP Address of DHCP client.
- yiaddr: Your IP Address, the IP Address assigned to client by DHCP server.
- siaddr: DHCP Server IP Address.
- giaddr: Gateway IP Address, the IP Address of DHCP relay agent/gateway.
- chaddr: Client Hardware Address, MAC Address of client's network interface

DOCUMENTATION

SAMSUNG GALAXY A34 5G



Samsung Galaxy A34 5G

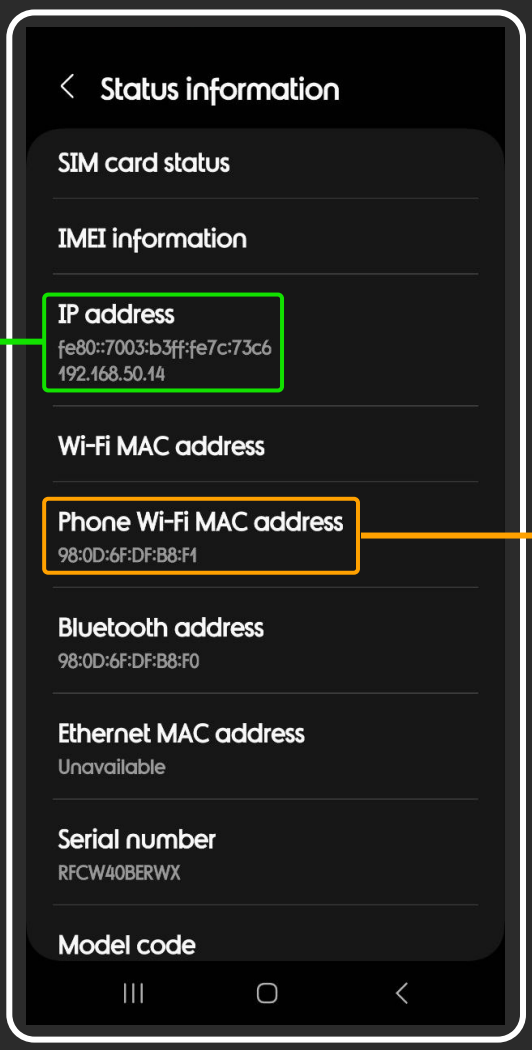
Operating System: Android 13

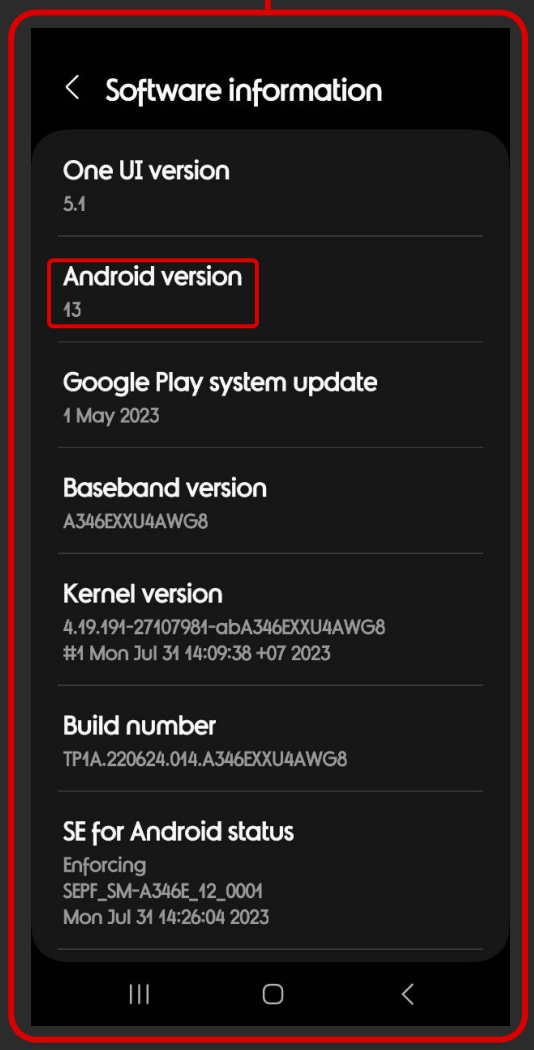
IP Address: 192.168.50.14

MAC Address: XX:XX:XX:DF:B8:F1

Settings > About Phone > Software Information

Settings > About Phone > Status Information





DOCUMENTATION

IPHONE 15 PRO MAX

iPhone 15 Pro Max

Operating System: iOS 17.0.3 (21A360)

IP Address: 192.168.50.90

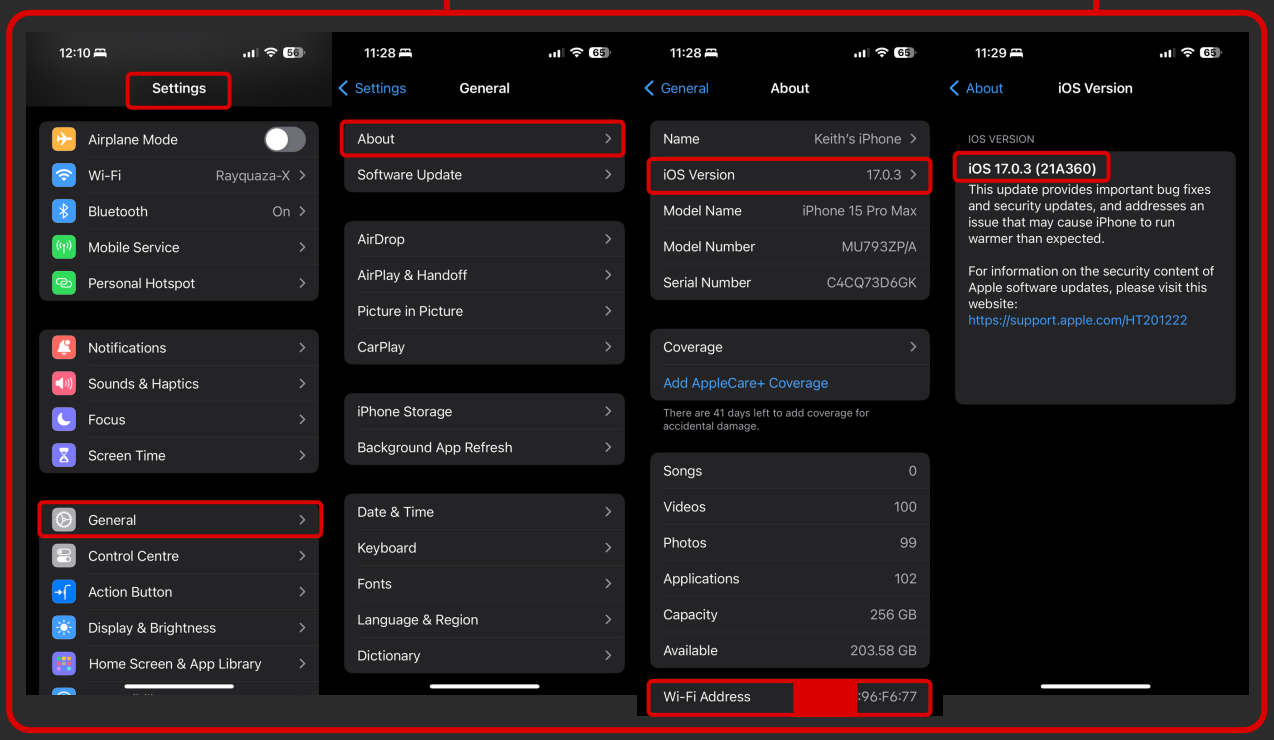
MAC Address: XX:XX:XX:96:F6:77

Settings > General > About > iOS Version:

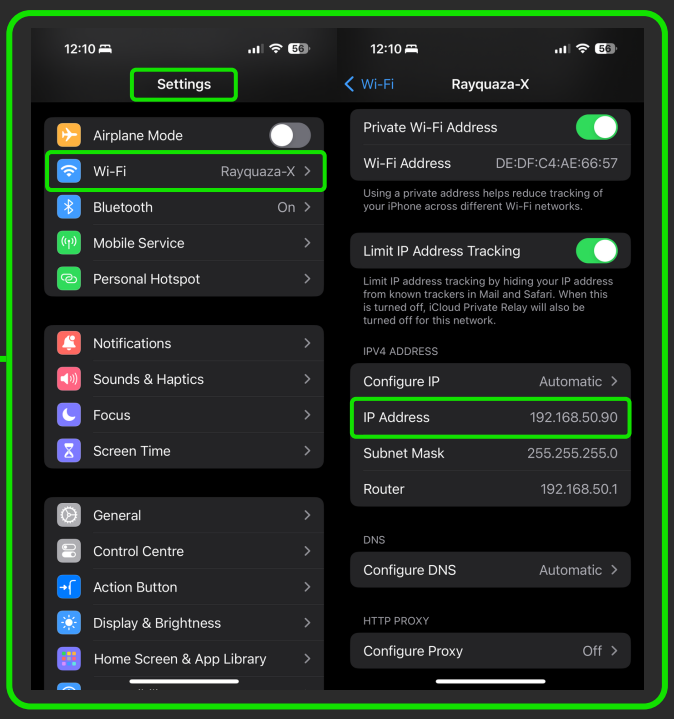
iOS 17.0.3 (21A360)

- 17: Major Version Number - major updates/changes to O.S.
- 0: Minor Version Number - small updates/bug fixes
- 3: Patch Version Number - smaller updates/bug fixes
- (21A360): Build Number

Settings > General > About > Wi-Fi Address



Settings > Wi-Fi > IP Address



DOCUMENTATION

MACBOOK PRO 14-INCH, 2023

Macbook Pro 14-inch, 2023 (Personal)

Operating System: macOS Sonoma 14.0

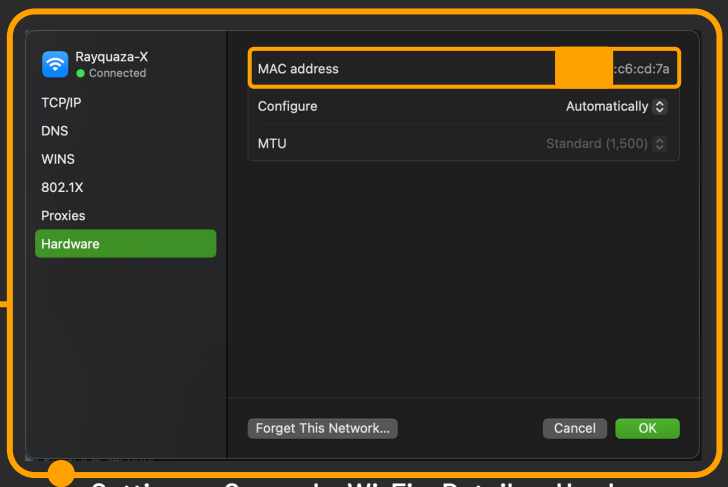
IP Address: 192.168.50.193

MAC Address: XX:XX:XX:C6:CD:7A

Settings > General > macOS

Terminal > "sw_vers"

```
keithtan@Keiths-MBP ~ % sw_vers
ProductName:        macOS
ProductVersion:     14.0
BuildVersion:       23A344
```



Settings > General > Wi-Fi > Details > Hardware

Terminal > "ipconfig getsummary en0"

Terminal command that provides a concise summary of network configuration settings for the primary network interface denoted by "en0"

OR:

Terminal > "ipconfig getsummary en0"

keithtan — -zsh — 145×63

```
keithtan@Keiths-MBP ~ % ipconfig getsummary en0
<dictionary> {
  Hashed-BSSID : cd:e6:fc:8a:05:9b
  IPv4 : <array> {
    0 : <dictionary> {
      Addresses : <array> {
        0 : 192.168.50.193
      }
      ChildServiceID : LINKLOCAL-en0
      ConfigMethod : DHCP
      DHCP : <dictionary> {
        LeaseExpirationTime : 10/13/2023 19:20:23
        LeaseStartTime : 10/12/2023 19:20:23
        Packet : op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0xa3b43114
secs = 0
ciaddr = 192.168.50.193
yiaddr = 192.168.50.193
siaddr = 192.168.50.1
giaddr = 0.0.0.0
chaddr =          :c6:cd:7a
```

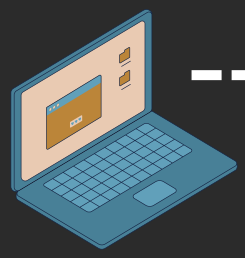
en0 is assigned to primary network interface

- htype → Type of hardware address used (1 = Ethernet/Wi-Fi)
- flags → Control and status info
- hlen → Length of MAC Address
- hops → # relay agents traversed by DHCP message
- xid → DHCP Transaction ID
- ciaddr → Client IP Address
- yiaddr → Your IP Address
- siaddr → DHCP Server IP Address
- giaddr → Gateway IP Address
- chaddr → MAC Address

DHCP Packet

DOCUMENTATION

DELL XPS 13, 2020



Ethernet

Dell XPS 13, 2020

(Personal)

Operating System: Microsoft Windows 11 Home

IP Address: 192.168.50.207

MAC Address: XX:XX:XX:5E:AD:F6

CMD > "systeminfo"

```
C:\Users\kehan>systeminfo

Host Name:                 DESKTOP-3FPC48L
OS Name:                   Microsoft Windows 11 Home
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          kehan95@outlook.com
Registered Organization:   N/A
Product ID:                00325-80000-00000-AAOEM
Original Install Date:     3/19/23, 9:52:28 PM
System Boot Time:          8/11/23, 12:25:29 AM
System Manufacturer:       Dell Inc.
System Model:              XPS 13 9300
System Type:               x64-based PC
```

Windows Command Prompt that provides a detailed summary of system information about the machine. Useful for system analysis and troubleshooting.

CMD > "ipconfig /all"
> Ethernet 8
> Physical Address

CMD > "ipconfig /all"
> Ethernet 8
> IPV4 Address

Command Prompt

```
Microsoft Windows [Version 10.0.22621.2134]
(c) Microsoft Corporation. All rights reserved.

C:\Users\kehan>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-3FPC48L
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter
   Physical Address. . . . . . . . . : [redacted]5E-AD-F6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::4cba:1095:b56f:5e58%51(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.207(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, October 13, 2023 6:54:39 PM
   Lease Expires . . . . . . . . . . : Saturday, October 14, 2023 6:54:39 PM
   Default Gateway . . . . . . . . . : 192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 855641798
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-D9-E9-7E-00-E0-4C-68-04-F5
   DNS Servers . . . . . . . . . . . : 192.168.50.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Windows Command Prompt that displays comprehensive details about the machine's network configuration.

DOCUMENTATION

LENOVO THINKPAD T14 GEN 2
+ CISCO ANYCONNECT VPN

Lenovo ThinkPad T14 Gen 2 (Work)

Operating System: Microsoft Windows 10 Enterprise

IP Address: 192.168.50.37

MAC Address: XX:XX:XX:FB:68:D7

```
C:\Users\lta_tankh13>systeminfo

Host Name:                 LTA-L101279
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
```

CMD > "systeminfo"

Cisco AnyConnect VPN

New DNS IP Address: 10.8.28.5

New Default Gateway IP Address: 10.119.176.1

New MAC Address: XX:XX:XX:3C:7A:00

New VPN IP Address: 10.119.181.86

CMD > "ifconfig /all"
> Cisco AnyConnect

CMD > "ifconfig /all"
> Wireless LAN adapter Wi-Fi

```
C:\Users\lta_tankh13>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : LTA-[redacted]
   Primary Dns Suffix  . . . . . . . : [redacted]
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : [redacted]

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . : [redacted]
   Description . . . . . . . . . . . : Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for Windows x64
   Physical Address. . . . . . . . . : [redacted]-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1030:e87b:4f47:819%8(Preferred)
   Link-local IPv6 Address . . . . . : fe80::2fd5:5bab:3e63:7729%8(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.119.181.86(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : ::
                                       10.119.176.1
   DHCPv6 IAID . . . . . . . . . . . : 117441946
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-DA-8B-26-38-F3-AB-B8-8F-5F
   DNS Servers . . . . . . . . . . . : 10.8.28.5
                                       10.122.1.103
   NetBIOS over Tcpip. . . . . . . . : Disabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX210 160MHz
   Physical Address. . . . . . . . . : [redacted]-FB-68-D7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::801d:5c63:70e7:1f1b%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.50.37(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, 11 October 2023 9:07:55 pm
   Lease Expires . . . . . . . . . . : Thursday, 12 October 2023 9:09:10 pm
   Default Gateway . . . . . . . . . : 192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.1
   DHCPv6 IAID . . . . . . . . . . . : 151279333
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-DA-8B-26-38-F3-AB-B8-8F-5F
   DNS Servers . . . . . . . . . . . : 192.168.50.1
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

With Cisco AnyConnect VPN used, the machine now has 2 distinct Internal IP Addresses:

- IP Address assigned by DHCP Server (Router often has this function)
- IP Address provided by VPN

This Cisco AnyConnect VPN Server also assigns new DNS IP Address, new Default Gateway IP Address, and new MAC Address, to enhance privacy and route traffic over the encrypted VPN tunnel.

WIRESHARK

FIND THE IP ADDRESS OF CHEWY.COM

By running "ipconfig" on CMD, internal IPv4 Address of my Windows computer (on VMware) is known to be 172.16.156.128.

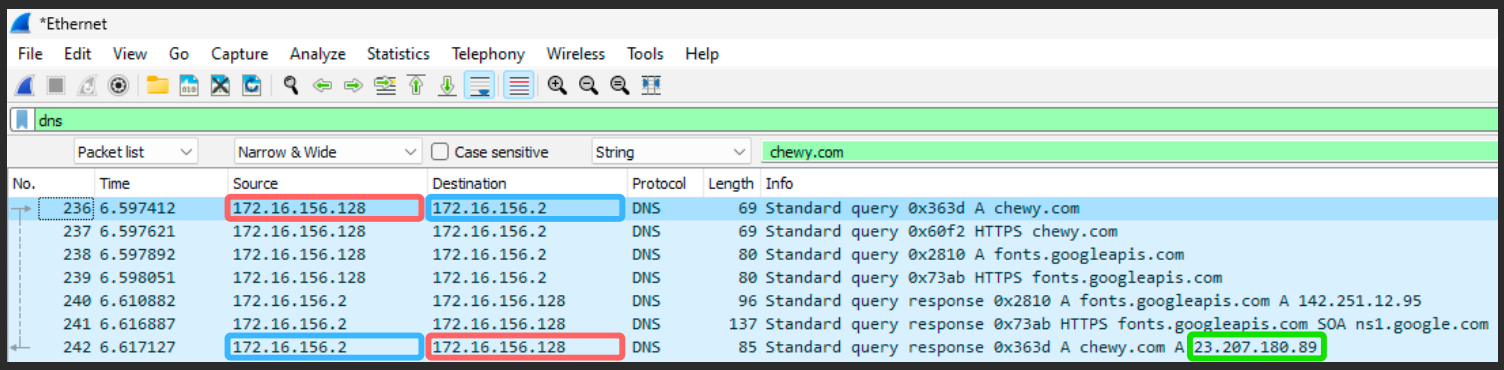
```
C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::d720:2a69:dc10:5e10%6
   IPv4 Address. . . . . . . . . . . : 172.16.156.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.156.2

C:\Users\user>
```

Subsequently, Wireshark is executed in the following sequence:

- Start Wireshark Capture
- Visit https://www.chewy.com
- Stop Wireshark Capture
- Filter "dns"
- Search string "chewy.com"

Filtered results (Packets 236 to 242) are shown below:

- Red: My Machine IP Address = 172.16.156.128
- Blue: DNS Server IP Address = 172.16.156.2
- Green: IP Address of chewy.com = 23.207.180.89



No.	Time	Source	Destination	Protocol	Length	Info
236	6.597412	172.16.156.128	172.16.156.2	DNS	69	Standard query 0x363d A chewy.com
237	6.597621	172.16.156.128	172.16.156.2	DNS	69	Standard query 0x60f2 HTTPS chewy.com
238	6.597892	172.16.156.128	172.16.156.2	DNS	80	Standard query 0x2810 A fonts.googleapis.com
239	6.598051	172.16.156.128	172.16.156.2	DNS	80	Standard query 0x73ab HTTPS fonts.googleapis.com
240	6.610882	172.16.156.2	172.16.156.128	DNS	96	Standard query response 0x2810 A fonts.googleapis.com A 142.251.12.95
241	6.616887	172.16.156.2	172.16.156.128	DNS	137	Standard query response 0x73ab HTTPS fonts.googleapis.com SOA ns1.google.com
242	6.617127	172.16.156.2	172.16.156.128	DNS	85	Standard query response 0x363d A chewy.com A 23.207.180.89

At Packet 236, my machine (Source) sends a query to the DNS Server (Destination), requesting for the IP Address of chewy.com.

At Packet 242, the DNS Server (Source) responds to my machine's (Destination)query, and provides the IP Address of chewy.com (which is 23.207.180.89).