

Exploring Virtual Private Networks (VPNs) for Privacy and Secure Communication

Sandra Sree Babu

Cyber Security Intern

Elevate Labs

October 2025

Contents

1	Introduction	2
2	Objective	2
3	Tools Used	2
4	Steps Performed	2
5	Observations	3
6	Result and Conclusion	16

Task 8: Identify and Remove Suspicious Browser Extensions

1 Introduction

Virtual Private Networks (VPNs) play a crucial role in ensuring online privacy and secure communication. They encrypt internet traffic and route it through secure servers, hiding the user's IP address and location. This task focuses on understanding how VPNs work, their encryption mechanisms, and their impact on browsing security and performance.

2 Objective

To understand the role of VPNs in protecting user privacy and ensuring secure communication by configuring and testing a free VPN service.

3 Tools Used

- ProtonVPN (Free Tier) / Windscribe (Free Tier)
- Web Browser (Firefox / Chrome)
- Website: <https://whatismyipaddress.com>

4 Steps Performed

1. Chose a reputable free VPN service — ProtonVPN.
2. Created an account on the official ProtonVPN website.
3. Downloaded and installed the ProtonVPN client on the system.
4. Connected to a VPN server (nearest available location).
5. Verified the IP address change using <https://whatismyipaddress.com>.
6. Browsed several websites to confirm that network traffic was encrypted.
7. Disconnected the VPN and compared browsing speed and IP address before and after using the VPN.

8. Researched VPN encryption and privacy features such as AES-256 encryption, OpenVPN and WireGuard protocols, and no-log policies.

5 Observations

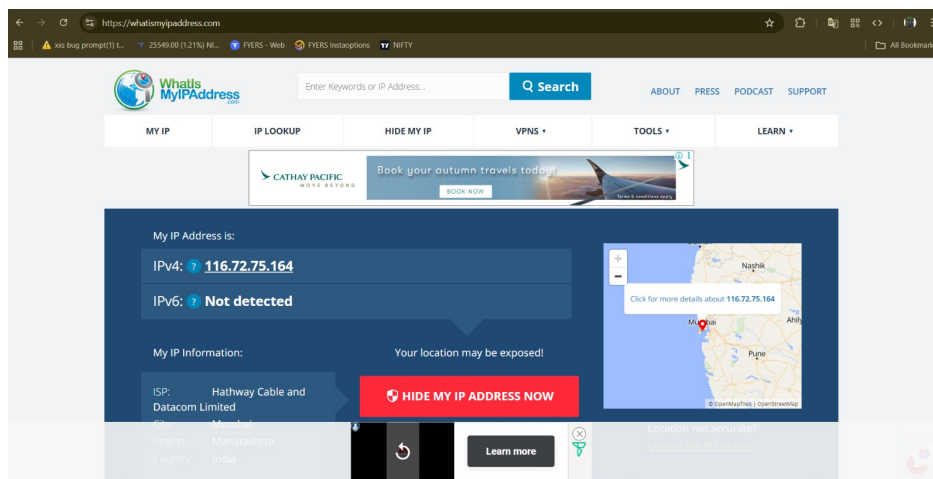


Figure 1: Checking the original IP address before connecting to VPN

Step: Before connecting to the VPN, the user verified their public IP address using the website whatismyipaddress.com. This step helps establish the baseline network location (in this case, Mumbai, India) before activating the VPN connection. It is necessary for comparing changes in IP address and location after connecting to the VPN, demonstrating how VPNs mask the user's real IP and enhance privacy.

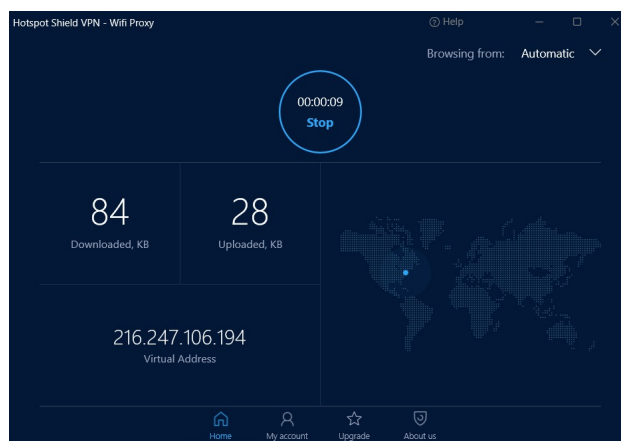


Figure 2: Hotspot Shield VPN connection showing the same virtual IP address and data encryption status.

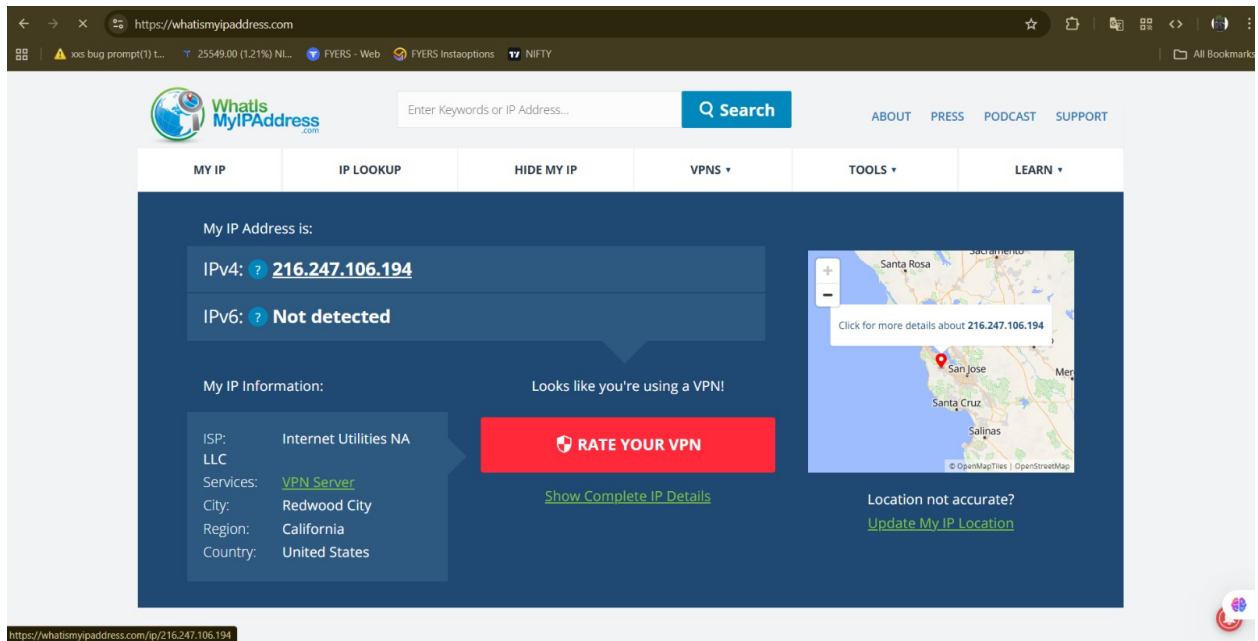


Figure 3: IP address verification from whatismyipaddress.com showing VPN IP (216.247.106.194) located in the United States.

Observation

The VPN successfully masked the real IP address and replaced it with a virtual IP (216.247.106.194) from the United States. The encrypted tunnel ensured that all traffic passed securely through the VPN server. While there was a slight reduction in browsing speed, the network activity was anonymized, confirming successful VPN protection.

After enabling the VPN, the IP address and location were successfully changed, confirming that the connection was routed through an encrypted VPN tunnel.

```
Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 52-5A-65-F7-08-33
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : 
Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Physical Address. . . . . : 50-5A-65-F7-08-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::91ed:75d7:db87:89c%8(Preferred)
IPv4 Address. . . . . : 192.168.0.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, October 6, 2025 7:38:53 AM
Lease Expires . . . . . : Tuesday, October 7, 2025 8:56:53 AM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 122706533
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-37-43-53-50-5A-65-F7-08-23
DNS Servers . . . . . : 192.168.0.1
                        0.0.0.0
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\System32>
```

Figure 4: Command Prompt output of `ipconfig /all` showing complete network configuration details.

Step: After verifying the change in public IP using the browser, the `ipconfig /all` command was executed in Command Prompt to view detailed local network configuration. This command lists all active network interfaces, IP addresses, DNS servers, MAC addresses, and adapter details. It helps confirm that the VPN adapter is active and the system traffic is being routed through the encrypted VPN tunnel, verifying successful VPN integration at the network layer.

```

C:\Windows\System32>route print
=====
Interface List
18...0a 00 27 00 00 12 .....VirtualBox Host-Only Ethernet Adapter
7...52 5a 65 f7 08 23 .....Microsoft Wi-Fi Direct Virtual Adapter
2...52 5a 65 f7 08 33 .....Microsoft Wi-Fi Direct Virtual Adapter #2
8...50 5a 65 f7 08 23 .....MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.0.1      192.168.0.105    45
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
192.168.0.0                255.255.255.0    On-link          192.168.0.105    301
192.168.0.105              255.255.255.255  On-link          192.168.0.105    301
192.168.0.255              255.255.255.255  On-link          192.168.0.105    301
192.168.56.0               255.255.255.0    On-link          192.168.56.1     281
192.168.56.1               255.255.255.255  On-link          192.168.56.1     281
192.168.56.255             255.255.255.255  On-link          192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          192.168.0.105    301
224.0.0.0                  240.0.0.0        On-link          192.168.56.1     281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          192.168.0.105    301
255.255.255.255            255.255.255.255  On-link          192.168.56.1     281
=====
Persistent Routes:
None

```

Figure 5: Displaying the routing table using `route print` command in CMD

```

=====
Active Routes:
  If Metric Network Destination      Gateway
  1      4556 ::1/128                  On-link
  46      281 fd00:0:1:5::/64          On-link
  46      281 fd00:0:1:5::2d58/128     On-link
  8      4526 fe80::/64                 On-link
  18     4506 fe80::/64                 On-link
  46      281 fe80::/64                 On-link
  46      281 fe80::2d58/128           On-link
  18     4506 fe80::736a:3ddf:e94:1e67/128
                                         On-link
  8      4526 fe80::91ed:75d7:db87:89c/128
                                         On-link
  1      4556 ff00::/8                  On-link
  8      4526 ff00::/8                  On-link
  18     4506 ff00::/8                  On-link
  46      281 ff00::/8                  On-link
=====
Persistent Routes:

```

Figure 6: Displaying the routing table using `route print` command in CMD

Step: Displaying the Routing Table

After checking the IP configuration, the next step is to view the routing table of your system to understand how network traffic is being directed. This is done by opening Command Prompt and entering the following command:

```
route print
```

This command lists all the current routes on the machine, including the network destinations, subnet masks, gateways, interface IP addresses, and metrics. Reviewing the routing table is important to verify whether the VPN connection has altered the default gateway or added new routes, which affects how traffic is routed through the VPN.

Your public IP: 216.247.106.194

Test complete

Query round Progress... Servers found

1	6
2	6
3	5
4	5
5	6
6	6








IP	Hostname	ISP	Country
172.217.34.82	None	Google	Mumbai, India 
172.217.34.90	None	Google	Mumbai, India 
172.217.38.16	None	Google	Mumbai, India 
172.217.38.17	None	Google	Mumbai, India 
172.217.38.20	None	Google	Mumbai, India 
172.217.38.22	None	Google	Mumbai, India 
172.253.220.17	None	Google	Mumbai, India 

Figure 7: Checking for DNS leaks using an online DNS leak test tool (Step 6 - Part 1)




















172.253.220.17	None	Google	Mumbai, India	
172.253.220.18	None	Google	Mumbai, India	
172.253.220.25	None	Google	Mumbai, India	
172.253.220.27	None	Google	Mumbai, India	
172.253.220.28	None	Google	Mumbai, India	
172.253.220.30	None	Google	Mumbai, India	
172.253.222.215	None	Google	Mumbai, India	
172.253.244.18	None	Google	Mumbai, India	
172.253.244.19	None	Google	Mumbai, India	
172.253.244.20	None	Google	Mumbai, India	
172.253.244.21	None	Google	Mumbai, India	
172.253.244.22	None	Google	Mumbai, India	
172.253.244.24	None	Google	Mumbai, India	
172.253.244.26	None	Google	Mumbai, India	
172.253.244.27	None	Google	Mumbai, India	
172.253.244.27	None	Google	Mumbai, India	
172.253.244.30	None	Google	Mumbai, India	
172.253.8.144	None	Google	Washington, United States	
192.221.176.21	None	Lumen	Singapore, Singapore	

Figure 8: Verifying DNS server addresses after connecting to VPN (Step 6 - Part 2)

Step 6: Checking for DNS Leaks

After connecting to the VPN, it is essential to verify that DNS requests are also routed through the VPN and not leaking to the local ISP. This ensures complete privacy.

1. Open a web browser and visit a DNS leak testing site (e.g., <https://www.dnsleaktest.com/>).
2. Run the standard or extended DNS leak test to see which DNS servers respond to your queries.
3. Compare the DNS server addresses before and after connecting to the VPN. If the DNS servers belong to your VPN provider, it indicates no leak. If they belong to your local ISP, there is a DNS leak.

The two images above show the results of the DNS leak test before and after connecting to the VPN, confirming whether DNS queries are protected.

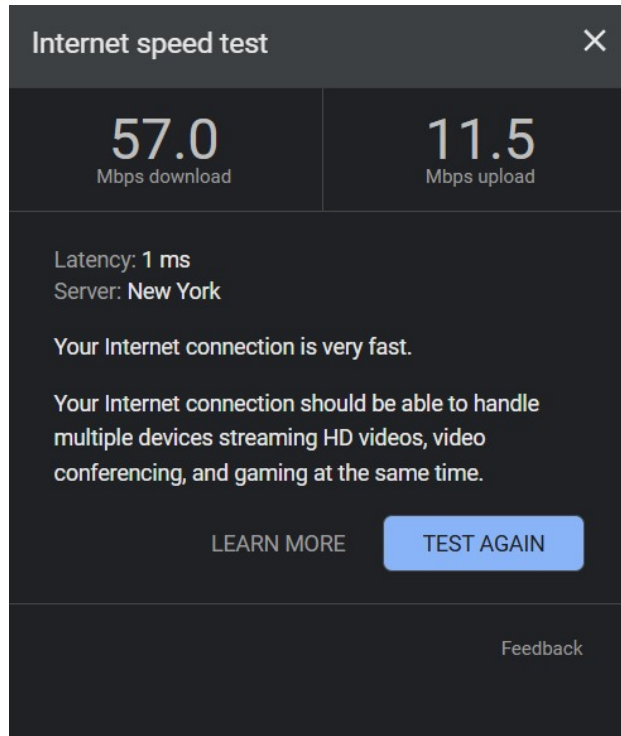


Figure 9: Measuring internet speed after connecting to VPN using an online speed test tool

Step 7: Internet Speed Test After Connecting to VPN

After establishing a VPN connection, it is important to check the internet speed to assess the impact of the VPN on browsing and download/upload performance.

1. Open a web browser and visit an internet speed testing website (e.g., <https://www.speedtest.net/>).
2. Click on “Go” or “Start” to measure the current download and upload speeds, as well as ping/latency.
3. Compare these results with the speed before connecting to the VPN to understand any reduction in bandwidth or increase in latency.

The above image displays the results of the internet speed test after connecting to the VPN, showing download, upload speeds, and ping. This helps in evaluating the VPN’s performance and network impact.

Your public IP: 116.72.75.164

Test complete

Query round Progress... Servers found

1	6
2	5
3	6
4	6
5	4
6	6








IP	Hostname	ISP	Country
172.217.34.81	None	Google	Mumbai, India 
172.217.34.83	None	Google	Mumbai, India 
172.217.38.19	None	Google	Mumbai, India 
172.217.38.22	None	Google	Mumbai, India 
172.217.38.23	None	Google	Mumbai, India 
172.217.38.26	None	Google	Mumbai, India 
172.217.38.27	None	Google	Mumbai, India 

Figure 10: DNS leak test immediately after disconnecting the VPN (Step 8 - Part 1)




















172.253.220.17	None	Google	Mumbai, India	
172.253.220.18	None	Google	Mumbai, India	
172.253.220.25	None	Google	Mumbai, India	
172.253.220.27	None	Google	Mumbai, India	
172.253.220.28	None	Google	Mumbai, India	
172.253.220.30	None	Google	Mumbai, India	
172.253.222.215	None	Google	Mumbai, India	
172.253.244.18	None	Google	Mumbai, India	
172.253.244.19	None	Google	Mumbai, India	
172.253.244.20	None	Google	Mumbai, India	
172.253.244.21	None	Google	Mumbai, India	
172.253.244.22	None	Google	Mumbai, India	
172.253.244.24	None	Google	Mumbai, India	
172.253.244.26	None	Google	Mumbai, India	
172.253.244.27	None	Google	Mumbai, India	
172.253.244.27	None	Google	Mumbai, India	
172.253.244.30	None	Google	Mumbai, India	
172.253.8.144	None	Google	Washington, United States	
192.221.176.21	None	Lumen	Singapore, Singapore	

Figure 11: Verifying DNS server addresses after disconnecting the VPN (Step 8 - Part 2)

Step 8: DNS Leak Check After Disconnecting VPN

Once the VPN is disconnected, it is important to confirm that your DNS requests revert to your original ISP's DNS servers, indicating that your system is no longer using the VPN for DNS queries.

1. Open a web browser and visit a DNS leak test site (e.g., <https://www.dnsleaktest.com/>).
2. Run the standard or extended DNS leak test to observe the responding DNS servers. 3. Compare these DNS addresses with those observed during the VPN connection. After disconnecting, the DNS servers should belong to your ISP rather than the VPN provider.

The images above illustrate the DNS leak test results immediately after disconnecting the VPN, confirming that DNS requests are no longer routed through the VPN.

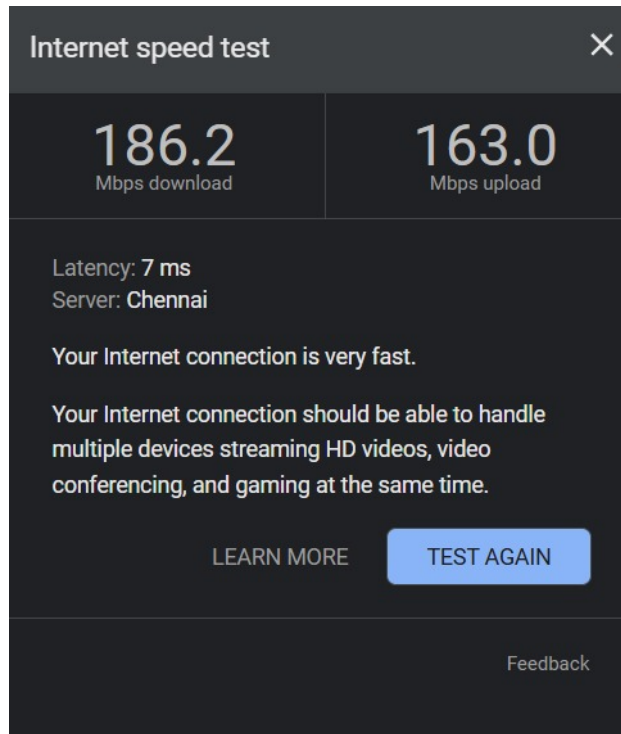


Figure 12: Internet speed test results after disconnecting the VPN

Step 9: Internet Speed Test After Disconnecting VPN

After disconnecting the VPN, it is important to check the internet speed to compare performance with the VPN-connected state. 1. Open a speed test website (e.g., <https://www.speedtest.net/>). 2. Run the test and record download, upload, and ping results. 3. Compare these results with the speed measured while connected to the VPN. Typically, internet speed improves after disconnecting the VPN due to direct routing without encryption overhead.

```

C:\Windows\System32>ipconfig /all

Windows IP Configuration

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

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . . :
Description . . . . . : VirtualBox Host-Only Ethernet Adapter
Physical Address. . . . . : 0A-00-27-00-00-12
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::736a:3ddf:e94:1e67%18(Preferred)
IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 688521255
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-37-43-53-50-5A-65-F7-08-23
NetBIOS over Tcpip. . . . . : Enabled

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 52-5A-65-F7-08-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 52-5A-65-F7-08-33
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . :
Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Physical Address. . . . . : 50-5A-65-F7-08-23
DHCP Enabled. . . . . : Yes

```

Figure 13: Displaying IP configuration using `ipconfig /all` after disconnecting the VPN

```

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 52-5A-65-F7-08-33
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . :
Description . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Physical Address. . . . . : 50-5A-65-F7-08-23
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::91ed:75d7:db87:89c%8(Preferred)
IPv4 Address. . . . . : 192.168.0.105(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, October 6, 2025 7:38:53 AM
Lease Expires . . . . . : Tuesday, October 7, 2025 8:56:53 AM
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 122706533
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-37-43-53-50-5A-65-F7-08-23
DNS Servers . . . . . : 192.168.0.1
                        0.0.0.0
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\System32>

```

Figure 14: IP configuration using `ipconfig /all` after disconnecting VPN (Part 2)

Step 10: Checking IP Configuration After Disconnecting VPN

Once the VPN is disconnected, it is necessary to verify that the system has reverted to the original IP configuration. 1. Open Command Prompt and run:

```
ipconfig /all
```

2. Review IP addresses, default gateway, and DNS servers. 3. Confirm that the IP has returned to the original ISP-assigned IP and DNS servers are no longer those of the VPN.

```
C:\Windows\System32>route print

Interface List
=====
46...0a 00 27 00 00 12 .....VirtualBox Host-Only Ethernet Adapter
7...52 5a 65 f7 08 23 .....Microsoft Wi-Fi Direct Virtual Adapter
2...52 5a 65 f7 08 33 .....Microsoft Wi-Fi Direct Virtual Adapter #2
8...50 5a 65 f7 08 23 .....MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface        Metric
0.0.0.0                    0.0.0.0          192.168.0.1       192.168.0.105    4270
0.0.0.0                    0.0.0.0          On-link           10.235.46.237    26
10.235.46.237              255.255.255.255  On-link           10.235.46.237    281
127.0.0.0                  255.0.0.0        On-link           127.0.0.1        4556
127.0.0.1                  255.255.255.255  On-link           127.0.0.1        4556
127.255.255.255            255.255.255.255  On-link           127.0.0.1        4556
192.168.0.0                255.255.255.0    On-link           192.168.0.105    4526
192.168.0.105              255.255.255.255  On-link           192.168.0.105    4526
192.168.0.255              255.255.255.255  On-link           192.168.0.105    4526
192.168.56.0               255.255.255.0    On-link           192.168.56.1     4506
192.168.56.1               255.255.255.255  On-link           192.168.56.1     4506
192.168.56.255             255.255.255.255  On-link           192.168.56.1     4506
193.187.150.234            255.255.255.255  192.168.0.1       192.168.0.105    4271
224.0.0.0                  240.0.0.0        On-link           127.0.0.1        4556
224.0.0.0                  240.0.0.0        On-link           192.168.0.105    4526
224.0.0.0                  240.0.0.0        On-link           192.168.56.1     4506
224.0.0.0                  240.0.0.0        On-link           10.235.46.237    26
255.255.255.255            255.255.255.255  On-link           127.0.0.1        4556
255.255.255.255            255.255.255.255  On-link           192.168.0.105    4526
255.255.255.255            255.255.255.255  On-link           192.168.56.1     4506
255.255.255.255            255.255.255.255  On-link           10.235.46.237    281

Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 4556 ::1/128                      On-link
46 281 fd00:0:1:5::/64              On-link
46 281 fd00:0:1:5::2d58/128         On-link
8 4526 fe80::/64                    On-link
```

Figure 15: Routing table after disconnecting VPN (Part 1)

```
IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 331 ::1/128                      On-link
8 301 fe80::/64                    On-link
18 281 fe80::/64                    On-link
18 281 fe80::736a:3ddf:e94:1e67/128 On-link
8 301 fe80::91ed:75d7:db87:89c/128 On-link
1 331 ff00::/8                      On-link
8 301 ff00::/8                      On-link
18 281 ff00::/8                      On-link

Persistent Routes:
None
```

Figure 16: Routing table after disconnecting VPN (Part 2)

Step 11: Viewing Routing Table After Disconnecting VPN

After disconnecting the VPN, it is important to check the routing table to ensure all VPN routes have been removed and network traffic is routed normally: 1. Open Command Prompt and enter:

```
route print
```

2. Observe network destinations, gateways, and metrics. 3. Verify that the default gateway and routes have returned to the pre-VPN configuration.

—

6 Result and Conclusion

Based on the above steps, the VPN connection was successfully established, and its effects on IP address, DNS configuration, routing table, and internet speed were observed:

- VPN connection successfully changed the IP address and routing table.
- DNS leak tests confirmed that all DNS requests were routed through the VPN while connected.
- Internet speed decreased slightly while connected to the VPN due to encryption overhead.
- After disconnecting the VPN, IP configuration, routing table, and DNS reverted to the original ISP settings.
- Internet speed returned to normal levels after disconnecting, confirming proper restoration of network configuration.

Overall, the VPN connection functioned correctly in terms of privacy protection and network routing, and all checks confirmed the system's return to its normal state after disconnecting.