

Task 8: In-Depth VPN Setup and Analysis Report

Objective

The primary objective of this task was to gain practical, hands-on experience with VPN technology. The process involved installing and configuring a VPN client, verifying its functionality by masking the public IP address, researching the core technologies that make VPNs effective, and evaluating their overall benefits and limitations as a security tool.

Tool Used

- **VPN Service:** ProtonVPN (Free Tier)
- **Operating System:** Windows 11
- **Verification Tool:** whatismyipaddress.com

VPN Setup and IP Verification Process

A systematic approach was taken to test and verify the functionality of the VPN service.

1. Baseline IP Address Documentation (VPN Off)

Before installing or connecting to the VPN, I established a baseline by documenting my public-facing IP address. This was accomplished by visiting whatismyipaddress.com. The website revealed my real IP address, the associated Internet Service Provider (ISP), and my approximate geographic location.

For critical privacy and security reasons, all personally identifiable information in the following screenshot has been redacted.

[All IP Ranges](#) > [49.0.0.0/8](#) > [49.43.0.0/16](#) > [49.43.4.0/24](#) > 49.43.4.173





My IP address

   Star   mobile

Need more data or want to access it via API or data downloads? Sign up to get free access

Sign up for free >

Summary

ASN	 Reliance Jio Infocomm Limited
Hostname	No Hostname
Range	
Company	Reliance Jio Infocomm Limited
Hosted domains	0
Privacy	 False
Anycast	 False
ASN type	ISP
Abuse contact	ip.abuse@ril.com

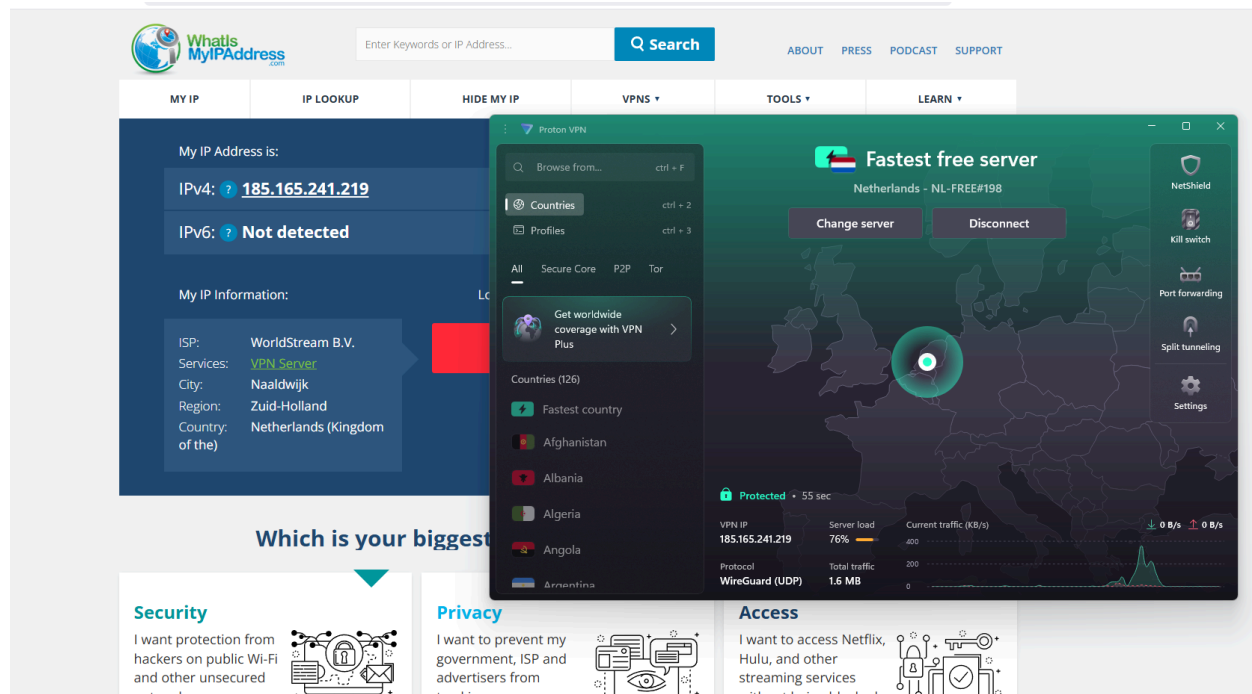
2. VPN Client Installation and Connection

The official ProtonVPN client for Windows was downloaded from the provider's website. After a standard installation, I logged into the application using my registered credentials. I then utilized the "Quick Connect" feature, which automatically selected the fastest available server in their free network and established a connection.

3. Post-Connection IP Address Verification (VPN On)

Once the ProtonVPN application confirmed a stable and active connection, I revisited whatismyipaddress.com. The website now reported a completely new public IP address and a different geographic location (in this case, one of ProtonVPN's servers). This successfully demonstrated the VPN's core capability of masking the user's true IP address and routing traffic through a remote server.

The original IP details have been redacted from this screenshot as well.



In-Depth Research: VPN Encryption and Privacy Features

A core part of this task was to research the technologies that make a VPN a powerful tool for security and privacy.

VPN Encryption: The Secure Tunnel

The primary security mechanism of a VPN is **encryption**. When a VPN is active, it creates a "tunnel" between the user's device and the VPN server. All data passing through this tunnel is scrambled using a complex algorithm, making it completely unreadable to outsiders. This includes the user's ISP, administrators on a local network, or attackers on a public Wi-Fi hotspot. The industry-standard for strong encryption is **AES-256 (Advanced Encryption Standard with a 256-bit key)**, a military-grade cipher that is computationally infeasible to break with current technology.

Essential Privacy Features of a Reputable VPN

Beyond encryption, trustworthy VPN services implement several critical features to protect user privacy:

- **Audited No-Logs Policy:** This is the most important privacy feature. A strict no-logs policy is a commitment from the VPN provider to not collect or store any data that could be used to identify a user or their online activities. This includes the user's original IP address, browsing history, and connection timestamps. The most reputable providers have their no-logs claims verified by independent, third-party security audits.
- **Kill Switch:** A kill switch is a fail-safe mechanism. If the VPN connection is unexpectedly

interrupted, the kill switch immediately blocks all internet traffic from the device until the secure VPN connection is re-established. This crucial feature prevents the user's real IP address and unencrypted data from being accidentally exposed.

- **DNS Leak Protection:** By default, a computer sends DNS queries (to translate domain names into IP addresses) to the ISP's servers. A "DNS leak" occurs when these queries are sent outside the VPN tunnel, allowing the ISP to see which websites are being accessed. A secure VPN forces all DNS queries through the encrypted tunnel to its own private DNS servers, plugging this privacy hole.
- **Secure Tunneling Protocols:** The strength and speed of a VPN tunnel are determined by the protocol it uses. Modern, secure VPNs utilize protocols like **OpenVPN** (highly secure and the industry standard) and **WireGuard** (newer, faster, and also highly secure). They avoid outdated and insecure protocols like PPTP.

Detailed Summary of VPN Benefits and Limitations

Benefits:

- **Privacy from Internet Service Providers (ISPs):** A VPN encrypts traffic, preventing ISPs from engaging in bandwidth throttling based on activity or collecting browsing data to sell to advertisers.
- **Security on Public Wi-Fi:** On unsecured networks (like in airports or cafes), attackers can easily intercept unencrypted data. A VPN creates a secure tunnel, making it safe to transmit sensitive information.
- **IP Address Masking:** By hiding the user's real IP address, a VPN helps prevent tracking by websites and advertisers and protects against targeted online attacks.
- **Accessing Geo-Restricted Content:** A VPN allows users to connect to servers in different countries, making it possible to access streaming services, news websites, or other content that might be blocked in their physical location.

Limitations:

- **Impact on Network Speed:** The process of encrypting and decrypting data, combined with the physical distance the data must travel to the VPN server, inevitably introduces latency and reduces connection speed.
- **The Element of Trust:** While a VPN hides your activity from your ISP, the VPN provider itself can see your traffic. It is crucial to choose a reputable provider with a strict, audited **no-logs policy**.
- **Does Not Guarantee Anonymity:** A VPN is a tool for privacy, not perfect anonymity. Activities within your browser (like logging into a Google account) can still be used to track you. It also does not protect against malware, viruses, or phishing attacks.
- **VPN Blocking:** Some websites, especially streaming services, actively detect and block traffic coming from known VPN servers.

Interview Questions & Answers

1. What is a VPN?

A VPN (Virtual Private Network) is a service that creates a secure, encrypted connection—often called a "tunnel"—between your device and the internet. All your internet traffic is routed through this tunnel to a remote server operated by the VPN provider, protecting your data from your local network and masking your true IP address.

2. How does a VPN protect privacy?

A VPN protects privacy in two primary ways:

1. **Encryption:** It encrypts your internet traffic, making it unreadable to your ISP, network administrators, or anyone snooping on the network (especially on public Wi-Fi).
2. **IP Masking:** It hides your real IP address and replaces it with the IP address of the VPN server, making it difficult for websites, advertisers, and trackers to identify your location and trace your online activity back to you.

3. Difference between VPN and proxy?

A **proxy** server acts as a simple intermediary for your web browser, hiding your IP address for that specific application. It does not typically encrypt your traffic. A **VPN** is more comprehensive; it operates at the operating system level and encrypts *all* network traffic from your entire device (not just the browser), providing a much higher level of security and privacy.

4. What is encryption in VPN?

Encryption in a VPN is the process of scrambling your data into a secure, unreadable code before it leaves your device. Only the VPN server has the key to unscramble it. This ensures that even if your traffic is intercepted, it cannot be read. Modern VPNs use strong encryption standards like AES-256.

5. Can VPN guarantee complete anonymity?

No, a VPN cannot guarantee complete anonymity. While it is a powerful privacy tool, you can still be tracked through browser cookies, device fingerprinting, or by logging into personal accounts (like Google or Facebook). Furthermore, the VPN provider could potentially log your activity, which is why choosing a provider with a strict no-logs policy is essential.

6. What protocols do VPNs use?

VPNs use various "tunneling" protocols to create the secure connection. Common

protocols include:

- **OpenVPN:** Very secure, open-source, and highly configurable. The industry standard.
- **WireGuard:** A newer, faster, and more modern protocol with strong security.
- **IKEv2/IPsec:** A fast and stable protocol, popular on mobile devices.

7. What are some VPN limitations?

Limitations include a potential reduction in internet speed, the fact that the VPN provider can see your traffic (requiring trust), and that some websites and services actively block VPN connections. A VPN also does not protect you from malware, viruses, or phishing attacks if you download a malicious file or visit a dangerous website.

8. How does a VPN affect network speed?

A VPN almost always reduces network speed to some degree. This is because of the "encryption overhead" (the processing power needed to encrypt and decrypt data) and the physical distance the data has to travel to the VPN server and then to its final destination. The speed reduction is usually minor with premium VPNs but can be significant with overloaded or distant free servers.