**Disconnect and Performance Comparison**

After verifying the VPN connection and testing encrypted browsing, the VPN was disconnected to observe differences in **speed, IP address, and browsing performance**. This phase focused on understanding the trade-offs between privacy and performance when using a VPN.

**1. Test Procedure**

1. Checked IP and network status **before** connecting to the VPN (baseline).
2. Connected to **ProtonVPN’s Singapore server** and ran browsing and speed tests.
3. Disconnected the VPN and repeated the same tests for comparison.
4. Recorded IP changes, connection stability, and latency differences.

**2. Performance Metrics**

| **Metric** | **Without VPN** | **With VPN (Singapore Server)** | **Observation** |
| --- | --- | --- | --- |
| **IP Address** | Original (India-based) | Changed to Singapore | IP successfully masked |
| **Download Speed** | ~52 Mbps | ~35 Mbps | Moderate decrease |
| **Upload Speed** | ~18 Mbps | ~12 Mbps | Slight reduction |
| **Latency (Ping)** | 23 ms | 87 ms | Noticeable delay |
| **Browsing Experience** | Fast and smooth | Slightly slower | Acceptable difference |

**3. Key Observations**

* **IP address** and **geolocation** changed immediately upon connecting to VPN.
* **Speed drop** observed (around 30–35%) due to encryption overhead and longer routing path.
* Despite slower speeds, the connection remained **stable and secure**.
* **Disconnection and reconnection** processes were seamless, showing good VPN client reliability.

**4. Interpretation**

The performance variation observed is typical for encrypted VPN tunnels.  
The added latency and reduced throughput are acceptable trade-offs for enhanced data security and IP masking.  
No abrupt disconnections or data leaks were detected during the transition between VPN ON/OFF states.

**5. Conclusion**

The VPN demonstrated **strong stability and reliable performance** under encrypted conditions.  
Although network speed reduced slightly, anonymity and encryption benefits outweighed performance loss.  
This confirms that VPNs are practical for secure browsing, provided users choose nearby servers to minimize lag.

**Research on VPN Encryption and Privacy Features**

After establishing and testing the VPN connection, research was conducted to understand the security mechanisms and privacy protections provided by modern VPN services. The analysis focused on **ProtonVPN** as the reference provider.

**1. Encryption Standards**

* **AES-256 Encryption:**  
  ProtonVPN uses Advanced Encryption Standard (AES) with 256-bit keys — the same level of encryption adopted by governments and militaries worldwide.  
  It ensures that intercepted data is unreadable to unauthorized parties.
* **Key Exchange & Authentication:**  
  Uses **4096-bit RSA** for key exchange and **HMAC with SHA-512** for data integrity verification.

**2. VPN Protocols Supported**

| **Protocol** | **Description** | **Security Level** | **Use Case** |
| --- | --- | --- | --- |
| **OpenVPN (UDP/TCP)** | Open-source tunneling protocol; balances speed and security. | High | Standard desktop VPN usage |
| **IKEv2/IPSec** | Fast reconnection and mobile stability. | High | Mobile and unstable networks |
| **WireGuard** | Lightweight, next-gen protocol with better efficiency. | High | Low-latency connections |

**3. Privacy and Security Features**

| **Feature** | **Description** |
| --- | --- |
| **No-Logs Policy** | ProtonVPN does not record browsing activity or connection logs. |
| **Kill Switch** | Automatically disconnects internet if VPN drops, preventing IP leaks. |
| **DNS Leak Protection** | Ensures DNS queries are encrypted and not exposed to ISPs. |
| **Secure Core** | Routes traffic through multiple VPN servers for extra anonymity. |
| **Perfect Forward Secrecy** | Generates new encryption keys for each session to prevent key reuse. |

**4. Interpretation**

The encryption and privacy research confirmed that ProtonVPN implements robust, transparent, and open-source technologies.  
The use of AES-256 encryption, strong key management, and multi-protocol support ensures high-level confidentiality.  
Privacy features like DNS leak protection and a strict no-logs policy further enhance user trust and anonymity.

**Summary of Findings and Performance Evaluation**

After completing all VPN connection tests and encryption verification steps, both privacy and performance metrics were analyzed to understand the overall impact of VPN usage.

**1. Observations**

| **Metric** | **Without VPN** | **With VPN (Singapore Server)** | **Impact** |
| --- | --- | --- | --- |
| **IP Address** | Original (India-based) | Masked (Singapore) | Location hidden successfully |
| **Download Speed** | ~52 Mbps | ~35 Mbps | ~32% drop due to encryption |
| **Latency (Ping)** | 23 ms | 87 ms | Increased due to distance |
| **Connection Stability** | High | High | Minimal interruptions |
| **Encryption Status** | Unencrypted | AES-256-bit Encrypted | Secure communication enabled |

**2. Security Findings**

* The VPN successfully hid the user’s real IP and location.
* Encrypted all outgoing and incoming traffic, preventing ISP-level tracking.
* HTTPS and VPN encryption combined ensured full confidentiality of transmitted data.
* No DNS or IP leaks detected during tests.

**3. Performance Findings**

* Slight reduction in speed due to encryption and server routing.
* Connection remained stable throughout the browsing session.
* Websites loaded slightly slower, but privacy protection outweighed this effect.

**4. Interpretation**

The performance analysis demonstrated a trade-off between **speed and privacy**.  
While connection speeds decreased slightly, the encryption layer and IP masking provided strong security advantages.  
The VPN effectively safeguarded user activity, making it suitable for secure browsing, especially on public or untrusted networks.

**5. Conclusion**

The VPN setup and testing proved that a reputable service like ProtonVPN can greatly enhance online privacy and security through advanced encryption, secure tunneling, and no-log policies.  
Although minor performance degradation occurs, the protection against tracking, eavesdropping, and data interception makes VPNs essential for secure internet usage.