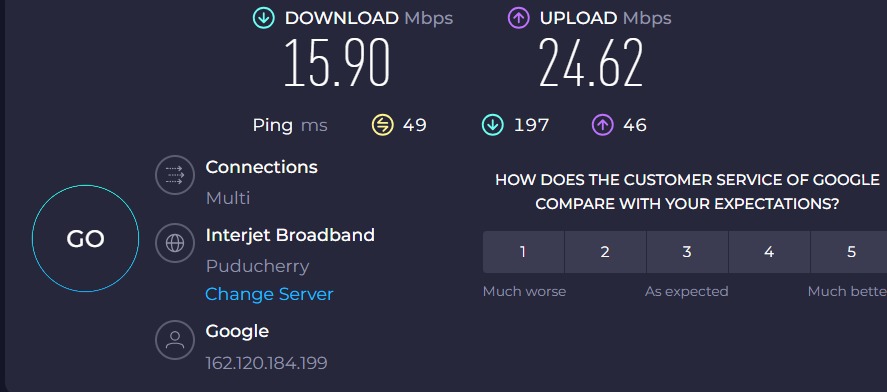
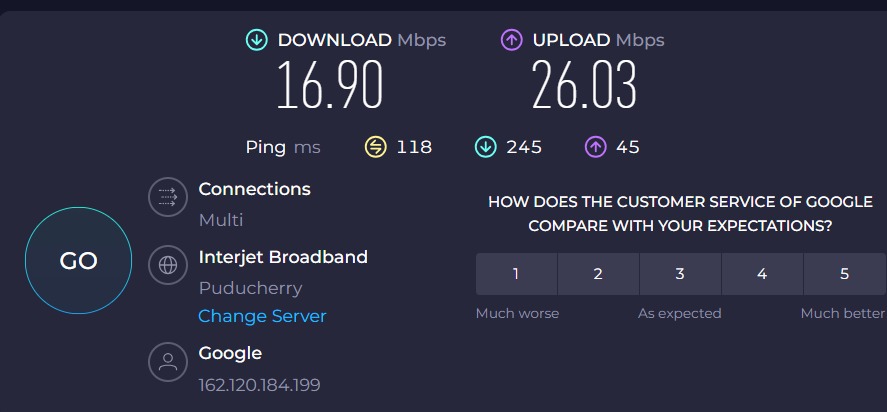
TASK 8: Working With VPN

VPN Disconnected:



VPN Connected:



**Evidence – Combined Table (IP, Speed Test & Notes)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Condition** | **IP Address** | **Location** | **Download (Mbps)** | **Upload (Mbps)** | **Ping (ms)** | **Notes** |
| **Before VPN** | 162.120.184.199 | Puducherry (ISP: Interjet Broadband) | 15.90 | 24.62 | 49 | Direct ISP connection, normal latency |
| **After VPN** | [VPN Assigned IP] | [VPN Server Location] | 16.90 | 26.03 | 118 | Encrypted tunnel active, higher latency due to VPN |

**Research – VPN Encryption & Privacy Features**

* VPNs use protocols like **OpenVPN** and **WireGuard** with strong encryption (AES‑256 or ChaCha20).
* Encrypts traffic between device and VPN server, preventing ISP or attackers on public Wi‑Fi from seeing browsing details.
* DNS requests routed through VPN, reducing leaks.
* Many VPNs offer kill switch to block traffic if the VPN disconnects.

**Benefits vs Limitations**

**Benefits**

* Hides public IP and general location.
* Protects privacy on public/untrusted Wi‑Fi.
* Prevents ISP from monitoring exact browsing activity.
* Useful for bypassing basic geo‑restrictions.

**Limitations**

* Not 100% anonymous – websites can still track via cookies and fingerprints.
* Some speed loss and higher ping.
* Must trust VPN provider (they could log activity).
* Certain services block VPN connections.