**UAS to GCS Communication and Tailscale Tunneling**

The AETHER drone system requires a robust and secure method of communication between the ground station and the drone, especially for Beyond Visual Line of Sight (BVLOS) operations. This involves the transmission of high-bandwidth data including real-time telemetry, navigation parameters, and optical/video feeds. Since the drone uses a 4G LTE cellular connection to access the internet (via the Sixfab modem), it is assigned a dynamic, carrier-grade NAT IP address. The private NAT is not predictable or accessible from the private ground station, essentially cutting the option of port forwarding through the cell carrier like you would be able to over a static home network. This makes it virtually impossible to establish or maintain direct inbound connections from the ground station to the drone using traditional networking methods. The lack of a fixed IP and the limitations of LTE NAT traversal pose a major challenge for consistent and secure remote access.

Tailscale provides our solution by creating a secure, peer-to-peer virtual private network (VPN) using the WireGuard protocol and building a secure tunnel through the NAT, letting the ground control system (GCS) reach the drone no matter what private IP it is hiding behind. It assigns each connected device—including the Raspberry Pi 5 onboard the drone and the ground station—a stable, private virtual IP within the Tailscale network. This allows both systems to communicate as if they were on the same local network, regardless of their physical location or internet provider. Tailscale automatically handles NAT traversal and relays if necessary, meaning no port forwarding or router configuration is required. All communication is end-to-end encrypted using WireGuard, ensuring that telemetry, control signals, and video feeds remain secure and inaccessible to third parties. Even if the drone’s IP changes due to LTE handoff or network switching, the Tailscale connection persists, providing reliable remote access and real-time data transfer throughout the mission. This setup dramatically simplifies long-range communication infrastructure while ensuring both security and stability, making Tailscale an essential component of AETHER’s BVLOS operations.

At this point the reader may be wondering, what is WireGuard? In short, it is a modern and high performance VPN protocol that enables fast, ultra secure and lightweight encrypted communication between devices. Its efficiency is fantastic on low power applications like the UAS, where power density limitations are always a concern. WireGuard encryption works by scrambling data into a ciphertext. Public keys for both the GCS and UAS are established, a handshake occurs between the keys, generating a private key for encryption/decryption. WireGuard uses ChaCha20 for encryption, Curve25519 for public key exchange and Poly1305 for message authentication. After a tunnel is established all data is encrypted before it leaves the Pi and is only decrypted when it arrives at the ground station, and vice versa. Even if data is intercepted the packets are useless, and data is always verified.

**Code**

1. Install Tailscale on both the Pi and your Windows PC GCS

<https://tailscale.com/download>

1. Login using the same account
2. Get the Tailscale IP of the GCS

Install tailscale on the UAS computer by running the following:

| curl -fsSL https://tailscale.com/install.sh | sh |
| --- |

Start up Tailscale

| sudo tailscale up |
| --- |

You will see something like the following

| To authenticate, visit:<https://login.tailscale.com/xxxxx>  |
| --- |

Copy the URL, open in a browser of any device (not exclusive to the Pi if running a headless setup), login with your account or sign up for the free service

**Windows based GCS:**

Go to: <https://tailscale.com/download>

Download the Windows version

Log in with the **same account** used on the Pi

Your Windows PC will now also have a Tailscale IP (100.XX.XX.XXX)

**AETHER uses QGroundControl:**

Go to **Windows Firewall** → **Allow an app** → ensure **QGroundControl** is allowed on **Private networks and Public networks**

On the RPI run the single line argument:

| mavproxy.py --master=/dev/ttyAMA0 --baudrate 57600 --out=udpin:0.0.0.0:14551 --out=udp:<GCS\_Tailscale\_IP>:14550 |
| --- |

Broken down:

| mavproxy.py \ --master=/dev/ttyAMA0 \ # Connects Pi to Pixhawk via UART  --baudrate 57600 \ # Sets a Baud Rate --out=udpin:0.0.0.0:14551 \ # Helper port unlocks MP’s ability to use UDP by giving a local network connection through this door --out=udp:100.107.171.127:14550 # Tells MAVProxy to send outbound MAVLink messages to GCS. udp:<Tailscale IP>:<14550> |
| --- |

**High-Level summary**

The Pixhawk speaks to the Pi via a UART connection

The Pi runs MAVProxy

The Windows GCS runs QGroundControl and listens on UDP 14550

Tail Scale connects both devices across networks, including cellular