GL.iNet Beryl AX (GL-MT3000) Re-Imaging & Recovery Field Guide

Tactical Operating Procedure for Deploying Personnel • Zero-Trust Hardware Sanitization • DPI Censorship Evasion

1.0 SITUATION & SUPPLY CHAIN REALITY

The GL.iNet Beryl AX (GL-MT3000) and Slate AX (GL-AXT1800) represent the hardware standard for deployed personnel due to high thermal efficiency, pocketability, and hardware-accelerated WireGuard throughput. However, because GL.iNet hardware is designed and assembled in Shenzhen and Hong Kong, procurement inside a NATO or Five Eyes operational context presents legitimate supply-chain questions.

The Clean Slate Protocol: Fortunately, GL.iNet hardware is 100% open-source compliant with unlocked U-Boot bootloaders and mainline Linux support. You do *not* have to trust or run factory vendor software out of the box. By re-imaging the router's NAND flash memory, you eliminate proprietary telemetries and replace the operating system with audited, sovereign code.

2.0 MISSION PARAMETERS & REQUIRED GEAR

PARAMETER	OPERATIONAL SPECIFICATION
Time Required	15 Minutes (Zero coding or Linux command-line skills required; 100% browser-based point-and-click).
Target Hardware	GL.iNet Beryl AX (GL-MT3000) or Slate AX (GL-AXT1800).
Power Source	Included 5V/3A Type-C wall brick, 20W+ USB-C PD power bank, or standard laptop charger (100–240V).
Uplink & Client Gear	1x Laptop (Windows / macOS / Linux), 1x RJ-45 Ethernet Patch Cable (included), 1x SIM ejector / paperclip.
Target Theatre	CAF OP REASSURANCE (Latvia / Baltics), OP IMPACT (Middle East), Maritime Fleet Deployments, Austere Forward Operating Bases.

3.0 DECISION MATRIX: CHOOSE YOUR FIRMWARE TRACK

Path 1: GL.iNet AmneziaWG Track

RECOMMENDED (90% OF TROOPS)

Best for: Combat arms (Infantry, Armoured, Artillery), Logistics, and non-cyber specialists who want high security without manual networking.

- Retains the user-friendly visual web GUI at `192.168.8.1`.
- 1-click hotel/FOB captive portal login and Wi-Fi repeater mode.
- Native **AmneziaWireGuard** support (v4.8+ / v4.11) that scrambles VPN packet headers to bypass Russian / state Deep Packet Inspection (DPI).
- Zero Linux terminal commands or package management required.

Path 2: Vanilla OpenWrt Scorched Earth

SIGNAL OPS / CYBER PURISTS

Best for: ACISS-IST cyber operators and OPSEC purists requiring 100% community-audited Linux sovereignty.

- Completely strips all proprietary GL.iNet vendor software.
- Replaced with official mainline OpenWrt and bare-metal **LuCI** GUI at `192.168.1.1`.
- Pure open-source transparency; zero cloud pings or analytics.
- *Trade-off:* Requires manual configuration of Wi-Fi repeating and routing packages in LuCI.

4.0 EXECUTION — PHASE 1: PAYLOAD ACQUISITION (PRE-FLIGHT CANADA)

Pre-Deployment Order of March: Never wait until you are sitting in a transit tent in Kuwait or Camp Ādaži with spotty cell reception to acquire software. Download firmware payloads while connected to Canadian home broadband:

1. **Acquire Target Payload:**
   • *For Path 1 (AmneziaWG GUI - Recommended):* Visit `https://dl.gl-inet.com/router/mt3000/` (or the Beta tab) and download the latest release (file ending in `.tar` or `.bin`).
   • *For Path 2 (Vanilla OpenWrt):* Visit `https://firmware-selector.openwrt.org/`, search `GL-MT3000`, and download the **Sysupgrade** image (file ending in `.bin`).
2. **DO NOT Unzip or Extract the File:** Operating systems (notably macOS Safari) may attempt to automatically decompress `.tar` or `.bin` files. Stop this immediately. The flash utility requires the raw, uncompressed archive.

Execution Phases 2–4 & Hardware U-Boot Failsafe Debricking

4.1 PHASE 2: PHYSICAL BREACH & STAGING

1. **Power On:** Connect the USB-C power adapter. Wait 60 seconds for the front LED indicator to stabilize solid.
2. **Port Identification (Critical):** Inspect the two Ethernet ports on the rear of the router:
   • **Blue Port (2.5G WAN):** Upstream internet uplink. **Leave this completely unplugged during flash.**
   • **Black Port (1G LAN):** Local client port. **Plug your Ethernet cable here and connect to your laptop.**
   (Wi-Fi alternative: Connect to the default SSID printed on the bottom label, but hardwired Ethernet is always safer).
3. **Access Admin Panel:** Open your browser and navigate to `http://192.168.8.1`. Select English and set a temporary admin password (e.g., `SoldierTest123!`).

4.2 PHASE 3: THE FLASH (THE SCORCHED-EARTH WIPE)

1. In the left-hand navigation sidebar, click on **System**, then select **Upgrade**. Click the **Local Upgrade** tab.
2. Drag and drop the `.bin` or `.tar` firmware file you downloaded in Phase 1 into the upload zone.
3. 🚨 **THE MOST CRITICAL STEP — UNCHECK "KEEP SETTINGS":**
   A checkbox will appear labeled **"Keep Settings"**. **YOU MUST UNCHECK THIS BOX.**
   If left checked, conflicting legacy configuration files will corrupt the new operating system, causing a boot loop ("soft brick"). Start with a completely sterile slate.
4. Click **Install / Update**.
5. 🛑 **STAND DOWN & DO NOT TOUCH THE ROUTER (3–5 MIN REBOOT):**
   The router will write to NAND flash and reboot. The front LED will blink rapidly and change colour/patterns. **Under no circumstances should you pull the power cable, unplug Ethernet, or shut your laptop lid.** Wait until the LED stabilizes.

4.3 PHASE 4: FIRST BOOT & OPERATIONAL VERIFICATION

If You Flashed Path 1 (AmneziaWG GUI):

- Laptop re-acquires DHCP automatically.
- Browse to `http://192.168.8.1`. Set permanent admin password & private Wi-Fi SSID/WPA3 key.
- Navigate to **VPN > WireGuard Client** to import native AmneziaWG obfuscated profiles.

If You Flashed Path 2 (Vanilla OpenWrt):

- **Notice IP Address Shift:** Gateway is now `http://192.168.1.1` (NOT `.8.1`).
- Connect via Ethernet or open Wi-Fi SSID `OpenWrt`.
- Browse to `http://192.168.1.1` into LuCI. Immediate Action: Go to **System > Administration** and set a strong root password. Secure Wi-Fi under **Network > Wireless**.

5.0 THE "OH CRAP" PROTOCOL: HARDWARE U-BOOT DEBRICKING FAILSAFE

Why You Cannot Brick This Hardware: GL.iNet embeds a read-only, hardware-isolated bootloader called **U-Boot** in protected ROM. It is physically separated from the NAND flash operating system. Even if power cuts out mid-flash or you upload an incompatible file, you can restore factory operation in under 5 minutes using a simple paperclip:

STEP	ACTION & OPERATIONAL PARAMETER
1. Prep Payload	Store an emergency copy of the official GL.iNet factory recovery firmware (`.bin`) locally on your laptop.
2. Power Off	Unplug the USB-C power cable from the router. Disconnect all cables except Ethernet.
3. Hardwire LAN	Connect an Ethernet patch cable directly between your laptop and the **Black LAN port** of the router.
4. Static IP	Configure your laptop's Ethernet adapter manually (DHCP is offline in failsafe mode): • IP Address: `192.168.8.2` | Subnet Mask: `255.255.255.0` | Default Gateway: `192.168.8.1`
5. Paperclip Pin	Using a paperclip or SIM ejector pin, press and **HOLD DOWN the recessed Reset button** on the router's side.
6. Power On	While holding Reset firmly down, plug the USB-C power cable back into the router.
7. Count 5 Blinks	Watch the front LED. It flashes once per second. **Count exactly 5 blinks (5 seconds), then release immediately.** The LED will blink rapidly, confirming U-Boot Web Failsafe server is active.
8. Access Failsafe	Open your browser and navigate to `http://192.168.8.1`. The bare-metal U-Boot Web Recovery screen will load.
9. Restore Firmware	Click **Choose File**, select your factory `.bin`, and click **Update firmware**. Wait 3 minutes for write & reboot.
10. Revert DHCP	Revert your laptop's Ethernet settings back to **"Obtain an IP address automatically (DHCP)"**. Device fully recovered.