NovaLink

Published notice — status, accuracy and right to amend. This document is published by the Company in good faith for general information and transparency. It is current only as of its stated date and is provided “as is,” without warranty of completeness or accuracy; it may contain errors or omissions and does not constitute legal, financial, tax, or investment advice, an offer or solicitation, or any guarantee. The Company may revise, correct, update, supplement, or withdraw this document at any time without prior notice, and the version published on the NovaLink Transparency Portal is the controlling current version and supersedes any earlier copy. Where this document conflicts with a signed agreement between you and the Company, or with applicable law, that signed agreement or applicable law prevails. If you believe anything here is inaccurate or out of date, please contact support@novalink.tech so we can review it and, where appropriate, correct it. To the maximum extent permitted by law, the Company accepts no liability for any reliance placed on this document.

Network Architecture & Workload Isolation

Topology, isolation model, and built-in separation from the home network

---

Document ID: NL-ARCH-01

Version: 1.1 (revised 10 November 2026)

Status: Issued

Issuing entity: Auralink Nova Technology L.L.C (Dubai, UAE, Reg. No. 1607764) — Technology Provider

Applies to: the NovaLink product, network and Nx1/Hx1 Home Stations, regardless of which Community Platform a participant joined through

The NovaLink entities: Ntech Link Technologies Ltd, Co. No. 2195904 (Store Operator) · Auralink Nova Technology L.L.C, Dubai, Reg. No. 1607764 (Technology Provider) · NodeLink USA, Inc., Delaware, File No. 10606222 (US Distribution)

Effective date: 22 May 2026

Contact: support@novalink.tech

---

1. Purpose

This document complements the Technical Security Whitepaper (NL-SEC-01) with a more topology-oriented description of the Company Network and an operator-facing explanation of how the Nx1/Hx1 Home Station keeps its work separate from the home or small-business network it is plugged into.

2. The Company Network — high-level topology

The Company Network has four logical planes:

1. Nx1/Hx1 Home Station Plane. The set of all Nx1/Hx1 Home Station devices deployed in Node Operator homes. Each is identified by a TPM-anchored certificate, runs the Workload Runtime, and maintains a single outbound mTLS connection to the Coordination Plane.

2. Coordination Plane. The Company-operated control servers that authenticate Nx1/Hx1 Home Stations, schedule Workload Sessions, distribute signed Workload artefacts, and collect operational telemetry. Hosted in the Company-managed regions with active-active redundancy.
3. Workload Publisher Plane. The API surface through which approved Workload Publishers submit Workloads. Authenticated via API key + mTLS. Workload artefacts must be signed.
4. Settlement & Identity Plane. The ledger that tracks Workload Session metering, reward attribution, and (where applicable) on-chain settlement (USDN).

3. Data flows

3.1 Outbound from Nx1/Hx1 Home Station.

Standard outbound flows from an Nx1/Hx1 Home Station are: (a) mTLS heartbeat to Coordination Plane every 60 seconds, (b) telemetry batch upload every 5 minutes, (c) Workload Session traffic flows (rate-limited, per-class destination policies), (d) signed-update channel pulls.

3.2 Inbound to Nx1/Hx1 Home Station.

By default, no inbound public-internet traffic reaches the Nx1/Hx1 Home Station. Inbound listeners, needed only by rare Workload classes, are exposed through a Company-managed reverse proxy on the Coordination Plane and are disabled by default.

4. Workload isolation model — per Workload class

Class	Isolation	Network namespace	CPU/RAM limit	Filesystem
Privacy-preserving compute	Linux container	Dedicated; egress whitelist only	cgroups: 1 vCPU, 1 GB RAM	Ephemeral tmpfs; nothing persists
Storage shards	Linux container	Dedicated; coordinator endpoints only	cgroups: 0.5 vCPU, 512 MB RAM	Persistent encrypted volume, sealed to TPM
Bitcoin proof-of-work	Linux container	Dedicated; mining pool endpoint only	cgroups: 0.5 vCPU, 256 MB RAM	Ephemeral
Nx1/Hx1 Home Station-Owner VPN	Linux container	Dedicated; user-traffic only	cgroups: 1 vCPU, 256 MB RAM	Ephemeral
Enterprise edge compute	microVM (Firecracker-class)	Dedicated; egress whitelist only	Up to 2 vCPU, 4 GB RAM	Ephemeral
Consumer connectivity relay (not enabled until microVM isolation is independently reviewed)	microVM with strict egress policy	Dedicated; class-specific destination policy	Up to 2 vCPU, 4 GB RAM	Ephemeral

5. Built-in separation from the home network

The Nx1/Hx1 Home Station plugs into the Node Operator's router like any other home device. It is not placed between the Node Operator's devices and the internet, so their traffic never passes through it. Separation is built into the device and requires no router configuration:

- The LAN interface has its own network namespace; the only LAN-facing service is the local dashboard page, bound to RFC1918 / link-local addresses.
- No Workload network namespace has a route to the LAN interface.
- A default-deny host firewall and AppArmor profiles protect both interfaces, independent of the Workload sandboxes.
- No inbound ports are open; all Workload and control traffic is outbound.
- Every Workload runs in its own container or microVM with an egress allow-list (Section 4).

6. Inbound port policy — what to expect

- No inbound ports are required for default operation. The Node Operator does not need to set up port-forwarding.
- If the Node Operator switches on the Owner VPN, the VPN server runs on the Nx1/Hx1 Home Station, but inbound is initiated by the user's VPN client; no router port-forwarding is required (the Company handles NAT traversal through the Coordination Plane).
- Workload classes that need inbound listeners (rare) use the Coordination-Plane reverse proxy described in Section 3.2; these listeners are disabled by default.

7. Public IP behaviour

- The Nx1/Hx1 Home Station's public IP is the IP issued to the Node Operator by their ISP. The Company does not provide a separate static IP. Under Section 3 of the Node Operator Agreement, the Node Operator agrees to the Company using that IP to deliver Workload traffic, subject to the AUP.
- For Default-Allowed Workloads, the Nx1/Hx1 Home Station does not act as an exit point for third-party traffic; outbound goes to whitelisted the Company endpoints only.
- For connectivity-relay Workloads (once enabled, after independent review of microVM isolation), the Nx1/Hx1 Home Station's IP may appear to destination servers as the source of relay traffic. This is the highest-risk Workload class: the Workload Publisher must satisfy additional onboarding and screening, the class runs only inside a microVM with a strict egress policy and per-Workload rate limits, and every outbound packet is attributed to a Workload Session ID (NL-SEC-01 §5.4).

8. Decommissioning and zeroisation

The Nx1/Hx1 Home Station has a built-in "Zeroise" function, available from the dashboard when a device is decommissioned. It triggers cryptographic erasure of all per-device keys held in the TPM and a secure wipe of the persistent storage volumes. The Company also revokes the Nx1/Hx1 Home Station Device Identity certificate on the Coordination Plane.

9. Contact

Architecture and integration questions: support@novalink.tech | Questions about how the device is isolated: support@novalink.tech