NovaLink

Network Architecture & Workload Isolation

Topology, isolation model, and Node Operator network setup recipes

---

Document ID: NL-ARCH-01

Version: 1.0

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 guide to safely placing an Nx1/Hx1 Home Station on a home or small-business network.

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. The Node Operator may, from the dashboard, opt into a the Company-managed reverse-proxy that exposes a Workload listener; this is required only for certain Opt-In Workload classes and is 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; 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 (opt-in, target Q4 2026)	microVM with strict egress policy	Dedicated; class-specific destination policy	Up to 2 vCPU, 4 GB RAM	Ephemeral

5. Recommended Node Operator network configurations

5.1 Default (no segmentation).

Acceptable, but only if the Node Operator has no sensitive devices on the LAN (no NAS, no IoT cameras, no work computers). In this case the Nx1/Hx1 Home Station simply sits on the home network.

5.2 Recommended — separate VLAN or guest network.

For most Node Operators, the Company recommends placing the Nx1/Hx1 Home Station on:

- A dedicated VLAN with no inter-VLAN routing to the main LAN.
- A "guest" Wi-Fi or LAN network on the router, with "client isolation" enabled.

5.3 High-assurance — separate physical link or business ISP.

For Node Operators running multiple Nx1/Hx1 Home Stations, or operating in a business context: a second ISP connection (or business plan with static IP) carrying only Nx1/Hx1 Home Station traffic. The Node Operator's primary LAN remains untouched.

5.4 Configuration recipes (high level).

Router family	Recipe (high level)
UniFi (Ubiquiti)	New Network → Corporate → assign VLAN ID (e.g., 20) → Firewall: deny LAN_IN to LAN, allow internet
ASUS / Asuswrt-Merlin	Guest Network → Enable Intranet Access: OFF → assign Nx1/Hx1 Home Station to guest SSID; for LAN port use VLAN tagging via merlin scripts
Netgear Orbi / Eero	Enable Guest Wi-Fi → assign Nx1/Hx1 Home Station → ensure "Allow guests to access local network" is OFF
MikroTik RouterOS	Bridge with VLAN filtering → assign untagged port → filter rules to drop forward from VLAN→LAN
OPNsense / pfSense	New interface (LAN2 or VLAN) → DHCP scope → Firewall rules: block from LAN2 net to LAN net
ISP-provided gateway with no VLAN support	Use a second downstream router behind the ISP gateway; place Nx1/Hx1 Home Station behind it; double-NAT is acceptable for the Nx1/Hx1 Home Station's use case

Detailed step-by-step recipes with screenshots are published on the Company documentation site (NL-DOC-NETWORK) and updated as router firmware changes.

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 opts into the Nx1/Hx1 Home Station-Owner VPN feature, 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).
- Opt-In Workload classes that need inbound listeners (rare) use the Coordination-Plane reverse-proxy described in Section 3.2; the Node Operator is asked to confirm during opt-in.

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.

- 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 Opt-In connectivity-relay Workloads (when enabled in Q4 2026), 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 and requires both the Node Operator and the Workload Publisher to satisfy additional onboarding and screening. The Node Operator may opt out of this class at any time from the dashboard, with immediate effect.

8. Decommissioning and zeroisation

When an Nx1/Hx1 Home Station is returned, sold to another Node Operator, or otherwise removed from the network, the Node Operator may from the dashboard initiate a "Zeroise" command. This 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 | Network setup help: support@novalink.tech