NovaLink

Latin America ISP & Home Internet Memorandum

Why running an Nx1/Hx1 Home Station is not “reselling your internet” — and every other ISP objection, answered one by one

Document ID: NL-LATAM-02
Version: 1.1
Status: Position memo
Issuing entity: Auralink Nova Technology L.L.C (Dubai, UAE, Reg. No. 1607764) — Technology Provider
Applies to: Node Operators and prospective Node Operators in Latin America assessing their home internet connection
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: 30 July 2026
Contact: support@novalink.tech

1. The concern this memorandum answers

“My internet provider will not allow this.” This is the most common concern we hear in Latin America, and it usually rests on one of a handful of specific fears — reselling, “commercial use”, servers, congestion, suspicious traffic, security, or licensing. This memorandum takes each of those, one by one, and explains specifically why it does not apply to hosting an Nx1/Hx1 Home Station. It also sets out what your ISP contract may genuinely say, what the net-neutrality laws of the region guarantee you, and what the Company does to stand behind you. It complements the general ISP Compatibility & Acceptable Use Note (NL-ISP-01).

2. What the machine actually does with your connection

The Nx1/Hx1 Home Station is a computer in your home that runs verified third-party workloads — scheduled computing tasks — and those tasks use a portion of the internet capacity you already pay for and are not otherwise using. In network terms it behaves exactly like any other

authorised application in your house: it opens outbound connections from one device, under your account, on your line. Nobody else connects to your Wi-Fi. Nobody receives internet access through you. No password is shared. Your neighbours cannot use your line. There is no hotspot. Its usage can be capped so it never interferes with your own use or your plan's data limit.

3. Objection 1 — “This is reselling internet”

“Reselling internet service” has a specific meaning in ISP contracts and telecommunications law across the region: taking the access service you bought and providing internet access to third parties — running a neighbourhood Wi-Fi service for money, wiring a building and charging tenants, or operating as an unlicensed mini-ISP. In every one of those cases, a third person receives internet access through your subscription.

The Nx1/Hx1 Home Station does none of that. No person receives internet access through your line. Your machine — one authorised device, owned and operated by you — performs computing tasks that generate its own traffic, in the same way that other everyday applications generate traffic you do not individually inspect:

- Windows Update Delivery Optimization, on hundreds of millions of home PCs, uploads update files from your connection to strangers' computers by default.
- Cloud backup (Google Photos, iCloud, OneDrive) uploads gigabytes from your line to remote data centres every week.
- Video calls, cloud gaming, smart-TV streaming and security cameras run continuous, sometimes symmetric, traffic around the clock.
- Peer-assisted delivery inside popular apps and smart TVs serves pieces of content to other users from your device.

Nobody describes any of these as “reselling internet”, and none of them turns the subscriber into a telecom operator — because using your own capacity through your own device for a lawful application is simply using the service you pay for. The Nx1/Hx1 Home Station belongs in that category: it is your device, running a lawful application, on capacity you already bought.

There is also a darker version of this, and it is worth naming because your ISP may have encountered it: for years, a hidden “residential proxy” industry has embedded software in smart TVs, set-top boxes, free applications and connected appliances that silently enrols the device in a commercial proxy network — the household's IP address is then sold to strangers, with no meaningful consent, no identification of who is behind the traffic, and no accountability when that traffic is abusive. That industry is precisely what this network was built to replace. Same idle capacity — opposite ethics: here the machine's owner opts in explicitly and knowingly, every participant is identified, every workload is verified and bound by a published Acceptable Use Policy, and a named company stands behind the traffic with attribution letters and an indemnity. If your ISP has ever seen suspicious traffic from residential lines, it may well have come from

that hidden industry — which is exactly why transparency with ISPs is at the centre of our model rather than something we avoid.

4. Objection 2 — “Earning rewards makes it commercial use of a residential plan”

Residential-plan classifications are about the premises and the usage profile of the connection — a home, with home-scale traffic — not about whether anything a household does has economic value. Households already earn through their home connections every day without anyone reclassifying their plan: people work remotely on a salary, sell on Mercado Libre, stream on YouTube or Twitch for ad revenue, take paid surveys, and upload photography they sell. An ISP does not require a business plan because your home activity happens to produce value; what matters to the plan is the traffic profile — and the Home Station's capped, home-scale profile fits a residential line. Where a specific plan defines “commercial use” unusually broadly, Section 10 gives you the simple written-confirmation or small-business-plan route; but as a category, earning participation rewards from your own device no more converts your internet plan into a commercial circuit than a remote-work salary does.

5. Objection 3 — “Residential plans don't allow running servers”

Some ISP acceptable-use policies restrict “operating servers” on residential lines. That clause is aimed at hosting public services — a website, game server or mail server that listens for inbound connections from the public internet, which changes the traffic profile the ISP engineered the plan for. The Nx1/Hx1 Home Station is not a public server in that sense: it operates as an outbound client. It initiates its own connections to the network's scheduling and delivery infrastructure — the same direction of traffic as a laptop, a streaming device or a backup agent — and it does not require port-forwarding, a public listening service, or any router changes that would expose a service to the public internet. Nothing listens on your line waiting for the public to connect to it.

6. Objection 4 — “It will congest the network / abuse an unlimited plan”

ISPs engineer residential networks for households that stream video for hours — a single HD stream runs continuously at several megabits per second, and families run several at once. The Home Station's consumption is of the same order and, unlike a movie night, it is configurable: its bandwidth can be capped, it yields to your own use, and on capped plans it can be set to stay comfortably inside the monthly limit (see Example B). It uses capacity that is otherwise idle — that is the design goal, not a marketing phrase. Fair-use policies exist for genuinely anomalous

consumption; a capped Home Station on a plan the household already uses for streaming does not approach them.

7. Objection 5 — “Strange traffic will get my IP flagged or blacklisted”

This fear is rational — it is what the hidden proxy industry described in Section 3 actually causes. Our model is engineered against it: every workload is verified and classified before it can run; the universally prohibited categories (set out in the Acceptable Use Policy, NL-AUP-01) are blocked at platform level; every workload session is attributable, so the Company can state in writing exactly what ran through your line and when; and if a complaint, flag or blocklist entry ever arises from a Company-scheduled workload, the Company investigates, issues a signed Attribution Letter, engages the complainant or your ISP directly, and — where it was not your fault — bears the costs under the Section 9 indemnity (NL-NOA-01, NL-INS-01). Compare that with the everyday alternative: a household whose smart TV was silently proxying traffic has nobody to call. A Node Operator has a named company, a published procedure and a deadline-bound claims process.

8. Objection 6 — “The box could be hacked and attack the ISP's network”

The Nx1/Hx1 Home Station is designed to a higher security standard than the average device already on a home line: a hardened, purpose-built operating system rather than a general-purpose PC; TPM-anchored identity and signed, verified updates; workloads executed in an isolated runtime that has no access to your LAN or your other devices (and the Node Operator Agreement, NL-NOA-01 Section 7, requires the machine to sit on a separate network segment); and no open inbound ports (Section 5). The Technical Security Whitepaper (NL-SEC-01) and Network Architecture & Workload Isolation (NL-ARCH-01) document this in full. The honest comparison: the typical home already contains routers with default passwords, old phones, and smart appliances that never receive an update. A sealed, centrally patched, isolated machine is a reduction in the attack surface of a typical home network, not an addition to it.

9. Objection 7 — “You need a telecom licence to do this”

Telecommunications licensing in Latin America applies to providing telecommunications services to the public — operating networks, selling access, using spectrum or numbering resources. A subscriber running a lawful application on their own connection is not providing a public telecommunications service, any more than hosting a video call or seeding a game update makes a household a carrier. The Home Station provides internet access to no one (Section 3), listens for no public traffic (Section 5), and offers no service to any third party; on our present analysis the participant needs no licence, registration or permit from the telecom regulator to run it — a position stated with the same honesty caveat as Section 14. (Whether any group

entity requires registrations in a given country is a separate corporate question, addressed for each market in the compliance documentation — it is never the participant's obligation.)

10. Your legal right to use lawful applications — net neutrality in Latin America

Latin America is, by law, one of the most protective regions in the world for a user's right to run the applications and devices of their choice. Chile was the first country in the world to enact a net-neutrality statute, and most major markets in the region followed:

Country	Law	What it gives you
Chile	Law 20.453 (2010) — world's first net-neutrality law	ISPs may not block, interfere with or discriminate against any lawful application, content or service
Brazil	Marco Civil da Internet, Law 12.965/2014	Guarantees net neutrality; ISPs must treat traffic equally regardless of content or application
Mexico	Federal Telecommunications and Broadcasting Law (2014)	Net-neutrality principles: free choice of applications and services
Argentina	Law 27.078 “Argentina Digital”, arts. 56–57	Express right to use, send, receive or offer any content, application, service or protocol, and to connect any device that does not harm the network
Peru	Law 29904 and OSIPTEL net-neutrality regulations	ISPs may not arbitrarily block, discriminate or restrict the use of any lawful application or protocol
Colombia	Law 1450/2011 art. 56 and CRC Resolution 3502	Free choice of applications and services; no arbitrary discrimination

Being precise about what this means: net-neutrality law protects your freedom to run lawful applications and devices on your connection — it is the reason your ISP cannot simply ban “applications it does not like”. It does not erase the contract you signed, so Section 11 addresses that contract honestly.

11. What your ISP contract may actually say — the honest part

Residential internet contracts in the region — with providers such as Claro, Movistar/Telefónica, Tigo, Telmex/Telcel, Vivo, TIM, Izzi, Totalplay, ETB, VTR, Entel and others — commonly contain two relevant kinds of clause: a prohibition on reselling or commercially redistributing the access service to third parties, and rules about “commercial use” of a residential plan. Wording differs between providers, countries and even plans, so read yours; that is also what we say in NL-ISP-01 for every region of the world.

Our position, stated plainly: hosting an Nx1/Hx1 Home Station does not provide internet access to any third party, and is therefore not resale of the service as that concept is used in these contracts. It is one authorised device generating application traffic under your own use of your own plan — like the everyday examples in Section 3. Where a plan contains unusually broad language, or where an operator prefers certainty, two simple options exist: ask your provider to confirm in writing that running a home server/computing device is permitted (it commonly is), or use a small-business plan, which typically removes any commercial-use ambiguity for a modest price difference. The Company never asks you to hide the machine or to breach a contract you have signed.

One boundary stated honestly, so nobody discovers it later: the Section 9 indemnity covers third-party claims arising from Company-scheduled workloads — it does not insure the commercial relationship between you and your ISP. If an ISP were ever to terminate or reprice a plan, that would fall outside the indemnity. This is precisely why the transparent routes above — written confirmation, or a small-business plan — exist, and why the Company offers to engage your ISP directly rather than asking you to run the machine quietly.

12. What the Company does to stand behind you

- Clean traffic only: every workload is verified, classified and bound by the Acceptable Use Policy (NL-AUP-01); prohibited categories are blocked at the platform level.
- Attribution letters: if anyone — including your ISP — questions traffic from your line, the Company will issue a signed letter identifying the disputed traffic as Company-scheduled workload traffic (see NL-INS-01).
- Direct ISP engagement: with your consent, the Company will correspond directly with your ISP to explain the machine, in Spanish or Portuguese where needed.
- Indemnity: under Section 9 of the Node Operator Agreement, where a claim arises from a Company-scheduled workload and is not your fault, Auralink Nova Technology L.L.C assumes the defence and bears the costs (NL-NOA-01, NL-INS-01).
- Bandwidth controls: the machine's usage can be capped so that it never interferes with your own use or any data cap on your plan.

13. Three worked examples

Example A — “My ISP says my plan is residential, not commercial.”

A Node Operator in Bogotá receives a call from her ISP asking about steady upstream traffic. She requests an attribution letter through support@novalink.tech; the Company provides it within days, in Spanish, explaining that the traffic is generated by a single authorised computing device she owns, that no third party receives internet access through her line, and offering technical contact. The ISP notes the account and takes no action. Had the ISP maintained an objection,

the practical resolution is a small-business plan — and if any claim had arisen from Company-scheduled workloads through no fault of hers, the Section 9 indemnity would have applied.

Example B — “My plan has a data cap.”

A Node Operator in Mexico City has a plan with a monthly data limit. He sets the machine's bandwidth cap so its monthly usage stays comfortably inside the plan. The machine contributes what his connection genuinely has idle — that is the design: idle capacity, not capacity you need.

Example C — “My IP address appeared on a blocklist.”

A Node Operator in São Paulo finds his IP listed on a public blocklist and worries his ISP will act. He contacts support@novalink.tech; the Company runs a workload-session attribution analysis for the period in question. If the listing traces to a Company-scheduled workload, the Company issues the Attribution Letter, contacts the blocklist operator and the ISP directly to obtain delisting, and handles costs under the indemnity where the operator was not at fault. If the analysis shows no workload ran at the relevant time — as is common, since home IPs are frequently recycled or flagged for unrelated reasons such as a previous subscriber or an infected phone — the Company documents that too, which itself gives the ISP the answer it needs.

14. Honest status of this memorandum

This memorandum is a position document, not legal advice and not a compliance certificate. Contract terms differ between providers and plans, telecommunications regulation differs between countries, and this memorandum has not yet been reviewed by qualified local counsel in each country. Nothing here encourages any operator to breach a contract; where your contract is genuinely restrictive, use the written-confirmation or business-plan route in Section 11. Country-by-country counsel review is on the compliance roadmap (NL-ROAD-01).

15. Contact

ISP questions, attribution letters, Spanish/Portuguese support: support@novalink.tech — subject “ISP — [your country]”.