

SneakernetUSA: Project Baseline & Roadmap

System Architecture, Hardware Mitigation, and Non-Profit Launch Strategy

Domain:
SneakernetUSA.com

Founder: Senior Architect (60+ Yrs Exp)

Target Launch: Q4 2026

Target Status: 501(c)(3) / GWSNP

10
HARDWARE NODES

1 / 10
A12 SIDELOAD BREAKTHROUGH

192.168.12.x
SUBNET ISOLATED

100%
OFFLINE AIRGAP CAPABILITY

1. EXECUTIVE SUMMARY & FOUNDATIONAL VISION

SneakernetUSA is designed to deliver secure, decentralized edge content and software services using optimized low-cost Android set-top boxes. Led by an industry veteran with over 60 years of hands-on computing history—ranging from IBM 360 mainframes to modern Linux network stacks and CompTIA credentials—the project combines technical rigor with a social mission.

The initiative serves a dual purpose: launching an operational edge-delivery network and creating a specialized non-profit coding academy. The infrastructure is currently staged in safe mode, with plans to re-establish 501(c)(3) tax-exempt status and onboard into **Google Workspace for Nonprofits (GWSNP)** prior to public launch by the end of the year.

2. MASTER NETWORK TOPOLOGY MAP

Device ID	Role / System Description	IP Address	Configured App / Port Status	Operational Baseline
Admin Laptop	HP Workstation (Linux / Safe-Mode Mask)	192.168.12.99	ADB Daemon / Netcat Active	MASTER CONTROL
TV_01	Primary Target Node (Spoofed A14 / Real A12)	192.168.12.121	FlexTV (com.flextv.livestore)	ACTIVE / STAY-AWAKE = 3
TV_02	Secondary Test Node (Spoofed A14 / Real A12)	192.168.12.122	Prepped for ADB Sideload	STAGED FOR SIDELOAD
Workstation_01	Win/Linux Dual-Boot Staging Station	192.168.12.123	Peripheral Formatting / Direct Media	OPERATIONAL
Workstation_02	Win/Linux Dual-Boot Staging Station	192.168.12.124	APK Packaging & Testing	OPERATIONAL
Nodes 03–10	Remaining Set-Top Box Hardware Pool	192.168.12.125+	Pending ADB Script Rollout	BATCH STAGED

Current System Milestone: Primary Node Breakthrough

Node **192.168.12.121 (TV_01)** has successfully bypassed local software blockades via direct ADB sideloading and peripheral injection. Process `com.flextv.livestore` is active in memory (PID 2976), and global stay-awake policies (`stay_on_while_plugged_in = 3`) have been verified.

3. HARDWARE CONTINGENCY PLAN: COUNTERFEIT A14 ANALYSIS

Hardware Failure & Fraud Analysis

Ten set-top boxes purchased in good faith as high-performance **A14 architecture** failed stock network deployment testing. System interrogation via low-level Android ADB shell tools revealed fake firmware reporting: the hardware is built on lower-spec **A12 system-on-chip (SoC)** components with spoofed build properties.

Option A: Hardware Optimization & Remediation

Extract max efficiency from existing A12 nodes by stripping stock bloatware via ADB, locking background execution limits, and sideloading lightweight streaming targets (`com.flextv.livestore`). This turns a hardware defect into a proof-of-concept for minimal resource overhead.

Option B: Enterprise Replacement Strategy

If A12 chipsets encounter thermal throttling or memory saturation during multi-stream stress tests, pivot hardware procurement to standardized, verified reference units (e.g., authentic Rockchip or Amlogic SoC nodes) prior to public rollout.

4. MULTI-PHASE OPERATIONAL ROADMAP

Phase 1: Activation & Overnight Burn-In (Immediate Focus)

- Maintain lock on `TV_01` (`192.168.12.121`) using global stay-awake parameters to evaluate memory leaks or background OS termination overnight.
- Initiate direct contact with FlexTV support during operational hours to complete activation and bind incoming media stream sockets.

Phase 2: Automated Batch Deployment Across Network Pool

- Execute automated ADB shell connection scripts from Admin Laptop (`192.168.12.99`) targeting nodes `.122` through `.130` .
- Automate batch sideloading of primary packages (`com.flextv.livestore` , `in.snapcore.screen_alive`) and set global battery optimization overrides across all 10 units.

Phase 3: Institutional Onboarding & Curriculum Launch (Q4 2026)

- **Sanitization & Scrubbing:** Scrub all hardware media, staging databases, and the website domain (`SneakernetUSA.com`) to ensure zero operational data leakage.
- **501(c)(3) & GWSNP Registration:** Re-activate corporate non-profit status and complete Google Workspace for Nonprofits enrollment to lock in enterprise-grade data privacy and AI safety policies.
- **Educational Academy Rollout:** Launch a specialized coding academy leveraging real-world low-level systems architectures, ADB automation, and network topology engineering.

Data Control & Security Commitments

Prior to official launch, all staging environments and internal system IDs remain masked under safe-mode identity layers. Full Google Workspace for Nonprofits integration will ensure that all enterprise code, student records, and operational data are strictly excluded from external public AI training sets.