Enabling Secure Field Migration from OpenWRT to RDK-B

White paper for RDK Tech Summit 2026

iwedia.com R&D in Belgrade and Novi Sad, Serbia

Purpose

Define a practical, operator-controlled migration pattern for deployed OpenWRT gateways moving toward RDK-B capabilities without immediate hardware replacement.

This paper treats migration as a staged, evidence-driven process rather than a single firmware replacement.

Audience	RDK engineers, architects, operators, OEMs, SoC vendors, system integrators
Scope	Brownfield ISP gateways, A/B boot strategy, configuration preservation, validation, telemetry, containerized application handling and rollback
Author	Viktor Nejgebauer, iWedia - broadband software, embedded system integration, OTA, TR-069/TR-369 and remote fleet-management experience

iWedia

- iWedia has over 15 years of experience delivering embedded device software at operator scale.
- This includes tens of millions of STBs and hybrid devices shipped across Tier-1 operators in Europe, MENA, and APAC, including Orange, Bouygues Telecom, NTT DOCOMO, and Jio.
- We bring deep embedded software expertise in OS porting, driver tuning, and BSP development. Our team also has hands-on experience with the core RDK ecosystem through RDK integration projects with Sky and Comcast.
- iWedia has a proven track record of in-field device upgrades and lifecycle extension, delivering new capabilities to existing hardware without customer disruption.

1. Motivation and goal

Operators already have large, stable brownfield broadband fleets in customer homes. These devices are installed, provisioned, remotely managed and part of live networks. Replacing them only to adopt a new platform is costly and operationally risky. A secure field migration path can reduce that barrier by moving deployed OpenWRT gateways toward RDK-B capabilities while preserving the device state needed for service continuity.

The central design point is simple: the router must not lose the information that makes it manageable and usable on Day 0 after migration. Device identity, WAN and LAN configuration, Wi-Fi settings, firewall and NAT rules, DHCP and DNS behavior, ACS ownership, credentials, certificates, application state and rollback metadata all have to survive the transition.

1.1 Migration goals

- **Preserve field identity:** retain serial, provisioning data, certificates, keys and operator ownership.
- **Preserve service configuration:** carry forward router and application configuration instead of forcing manual re-provisioning.
- **Control risk:** separate download, verification, boot, health validation and final commit into distinct stages.
- **Keep the operator in control:** use ACS and USP/TR-369 telemetry so the fleet manager can observe, approve, stop, or roll back migration.
- **Enable RDK-B adoption:** make existing hardware useful for RDK-B evaluation and phased deployment when the platform and BSP support it.

1.2 What success looks like

A successful migration is not merely an RDK-B image booting once. It is an RDK-B boot that restores WAN, LAN, Wi-Fi, management connectivity, telemetry, required applications and health reporting. The operator must have enough evidence to decide whether the device should remain on the new bank or automatically return to the previous working image.

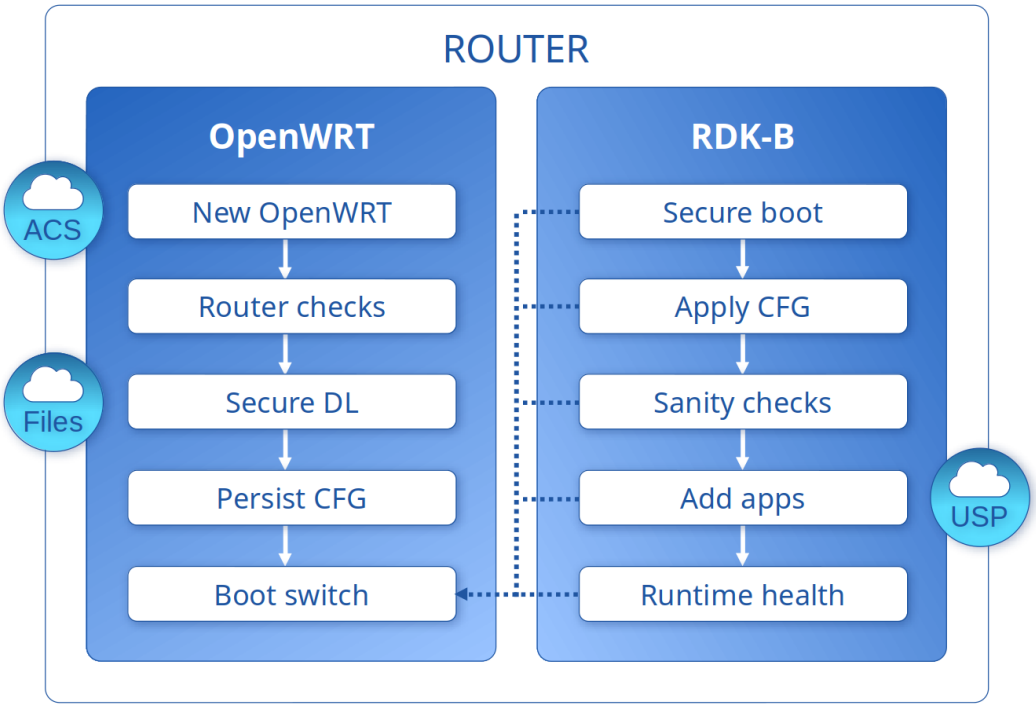
Core principle

Downloaded does not mean verified. Verified does not mean booted. Booted does not mean healthy. Healthy does not mean committed. Each transition needs explicit evidence.

2. Migration Strategy and Control Plane

The proposed strategy uses a staged flow. The first stage prepares the currently deployed OpenWRT environment with the checks and tooling required for a safe transition. The second stage downloads and verifies the target payload. The third stage persists the required state outside the replaceable root file system. The fourth stage switches boot to RDK-B. The final stages apply configuration, validate runtime health, start application containers and either commit or roll back.

The diagram shows three control-plane inputs. ACS coordinates migration initialization, authorization, rollout policy and rollback. The file server provides controlled payload delivery. USP/TR-369 reports event-driven migration state so the operator can see progress and failure reasons without waiting for periodic polling. It also deals with deployment of containerized applications.



2.1 New OpenWRT

Install or confirm a migration-capable OpenWRT image with the required tools, board adapters, ACS hooks, storage access and boot-control utilities. It must contain the necessary scripts that can start the migration, persist all necessary settings on a shared partition and switch boot partition to one containing the RDK-B image.

2.2 Pre-migration checks

Before accepting a migration, the device performs compatibility and readiness checks. These checks prevent unauthorized, undersized, or incomplete upgrades. They also provide the operator with early failure reasons before the router touches the boot chain.

- Compatible hardware specification and board capability match.
- Current router software and migration-tool version are supported.
- A/B partitioning, boot control and rollback metadata are present.
- Free space is sufficient for payloads, configuration snapshots and logs.
- Network reachability to ACS and file server is stable enough for staged download.

2.3 Secure download

Download signed image metadata and payload from the approved file server, preferably over authenticated TLS. Verify source authorization, manifest signature, image hash, size, version and anti-rollback constraints before writing the inactive bank.

2.4 Configuration Preservation and TR-181 Mapping

Configuration migration is the highest-risk part of the process. A generic RDK-B image cannot be preconfigured for every deployed router because each live unit has device-specific WAN credentials, VLAN or PPPoE parameters, Wi-Fi SSIDs and keys, LAN addressing, firewall behavior, remote-management identity, ACS credentials, certificates and application state. Losing any of these can turn a successful image boot into a field outage.

The OpenWRT side must collect state from UCI configuration, files, service databases, certificates, provisioning identifiers and application-specific storage. That state should be normalized into an explicit migration package with versioning, checksums, source metadata and target RDK-B mapping rules. The package must live in a partition that is not erased when the root file system changes.

2.4.1 Mapping model

OpenWRT / field state	RDK-B target behavior
WAN, VLAN, PPPoE, DHCP client, DNS	TR-181 InternetGatewayDevice / Device IP, routing and WAN service parameters
Wi-Fi SSID, credentials, radio state, security mode	RDK-B Wi-Fi backend / OneWifi compatible parameters and ACS templates
LAN bridge, DHCP server, NAT and firewall	CCSP-managed LAN, firewall, NAT and routing configuration
ACS credentials, certificates, serials, IDs	Management connectivity and device identity after first RDK-B boot
Application config and databases	Mounted container configuration and application-specific health validation

Router adapters and ACS templates reduce per-device logic. The adapter knows how to interpret the source platform and hardware variant. The ACS template knows what RDK-B parameters must be applied for that operator profile. This separation lets the same migration framework support multiple board revisions, operators and RDK-B versions without turning the migration script into a monolithic custom image.

Operational rule

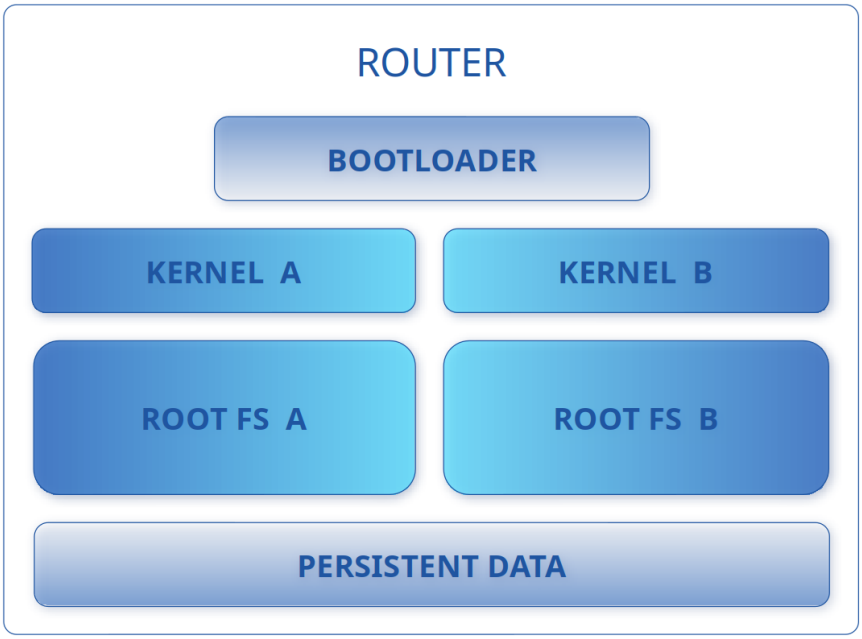
The first RDK-B boot must restore management access quickly. Once ACS and USP/TR-369 are healthy, the operator can reconcile the remaining configuration remotely.

2.5 Boot switch

Set the next boot target to the candidate RDK-B bank, retain the previous working bank, initialize retry counters and record rollback reason fields for post-mortem analysis.

2.6 Secure boot

The partition model should separate immutable boot components, replaceable operating-system banks and persistent data. A/B banks allow the device to try a new RDK-B image while retaining a known-good OpenWRT or previous image. Rollback can then be based on boot counters, validation results, ACS reachability and operator policy rather than on a single boot success.



2.6.1 Secure boot chain

Control	Migration requirement
FIT image verification	The bootloader verifies the signed FIT image for the selected bank. The FIT can bind kernel, device tree and related boot artifacts to a signed descriptor.
Keys and trust anchor	Verification keys must be controlled by the device vendor or operator trust model. The router must reject images signed with unknown or unauthorized keys.
DM-verity	The RDK-B root file system should be protected with dm-verity or an equivalent read-only integrity mechanism so runtime tampering is detected after boot.
Rollback safety	Boot counters, previous-bank metadata and validation outcome decide whether the router commits the new bank or returns to the previous working image.

2.7 Apply configurations

Configuration apply starts from the persisted package, not from assumptions baked into the image. The migration adapter reads OpenWRT UCI state, service files, application databases, certificates and provisioning identifiers, then maps them to target RDK-B parameters and service configuration. The minimum goal is to restore management access quickly; the complete goal is service continuity for WAN, LAN, Wi-Fi, firewall/NAT, DNS/DHCP, ACS ownership, USP identity and required applications.

2.8 Sanity Checks

Once RDK-B is running certain health or sanity checks are needed to confirm critical processes are running, no blocking failed units exist, ACS/USP are reachable and connectivity checks passed.

- OS release and platform profile match the expected migration target.
- Critical CCSP processes are running and systemd has no blocking failed units.
- WAN interface, default route, DNS and Internet connectivity are operational.
- LAN bridge, DHCP, firewall and NAT behavior are sane.
- TR-069 and TR-369/USP sessions can report state to the operator.
- CCSP logs exist and contain enough context for remote troubleshooting.
- Wi-Fi backend or OneWifi validation confirms configured radios and SSIDs.

2.9 Installing containerized applications

Applications should be migrated as managed units rather than copied blindly. The flow is: build an application list, securely download required artifacts, create the container execution unit, mount preserved configuration, run health checks and report application-specific telemetry.

Dobby provides a container-management layer for RDK environments. In this migration pattern it acts as the boundary between the base RDK-B platform and additional operator or product applications. The base system stays clean; application binaries, writable data and configuration can be mounted explicitly from controlled locations. Dobby also gives lifecycle control so an application can be started, stopped, restarted and diagnosed independently from the base boot process.

Application step	Reason
List	Determine which apps are required for this device, operator and customer state.
Download	Fetch signed or otherwise controlled application artifacts from approved file server.
Container execution unit	Start the app with a predictable runtime boundary and lifecycle control.
Mount configuration	Inject preserved app data without polluting the base root file system.
Health checks	Use app-specific probes, logs, ports and telemetry to decide success.

This model also supports app-specific validations. A VPN service, smart-home service, or telemetry agent can each expose different success criteria while still fitting into the same migration framework.

2.10 Runtime health

Once RDK-B is running certain health or sanity checks are needed to confirm critical processes are running, no blocking failed units exist, ACS/USP are reachable and connectivity checks passed.

Rollback must remain available until the router proves that it is usable and manageable. For fleets, ACS can also apply rollout policy based on aggregate success rates. For example, if a sample group shows too many failures, the operator can stop the rollout and roll back affected devices before continuing with a larger population.

3. Proof-of-Concept Environment

The summit work is presented as a proof of concept and migration pattern, not as a claim that every deployed router can be migrated without vendor participation. Production migration depends on BSP availability, signed images, bootloader behavior, board partitioning, Wi-Fi and switch drivers, operator policy and access to representative hardware.

If everything runs smoothly, the migration takes between 4 and 5 minutes.

Component	Version / role
Hardware	Banana Pi BPI-R4 Pro 8x lab target
Source platform	OpenWRT 24.10 plus project patches
Target platform	RDK-B on Kirkstone-based Yocto 6.1 plus project patches
ACS	Genie 1.2.13
USP / TR-369	Oktopus 1.24.6
File server	FastAPI 0.136.1 based service for controlled payload delivery

4. Lessons learned

- **TR-181 mapping is not universal:**
  it depends on RDK-B version, board capabilities and used ACS templates.
- **Telemetry must be robust:**
  the operator needs event-driven state, not just periodic polling, especially during failure handling.
- **Fleet policy matters:**
  ACS-side rollout thresholds can prevent a local issue from becoming a fleet incident.
- **Applications need their own validation:**
  each migrated app requires specific probes and rollback impact assessment.

5. Value for the RDK community

A reusable migration pattern can shorten RDK-B adoption cycles for brownfield fleets. The immediate value is a repeatable automated strategy, safer rollback and clearer validation. The longer-term value is shared guidance for operators, OEMs, SoC vendors and system integrators around secure boot, A/B partitioning, configuration mapping, telemetry and app migration.

Application specific telemetry and rollback that considers application health checks can be applied outside of migration - in updates between different RDK-B versions or during standard operation.

Proposed next step

Create an RDK community working group
focused on brownfield OpenWRT-to-RDK-B migration patterns:
secure boot, state persistence, TR-181 mapping, validation, telemetry and rollback.

The practical conclusion is that brownfield migration is feasible only when treated as a controlled lifecycle operation. The router must preserve identity, prove health, expose evidence and keep a safe path back. When those rules are followed, existing devices can become a bridge toward RDK-B adoption instead of a barrier to it.