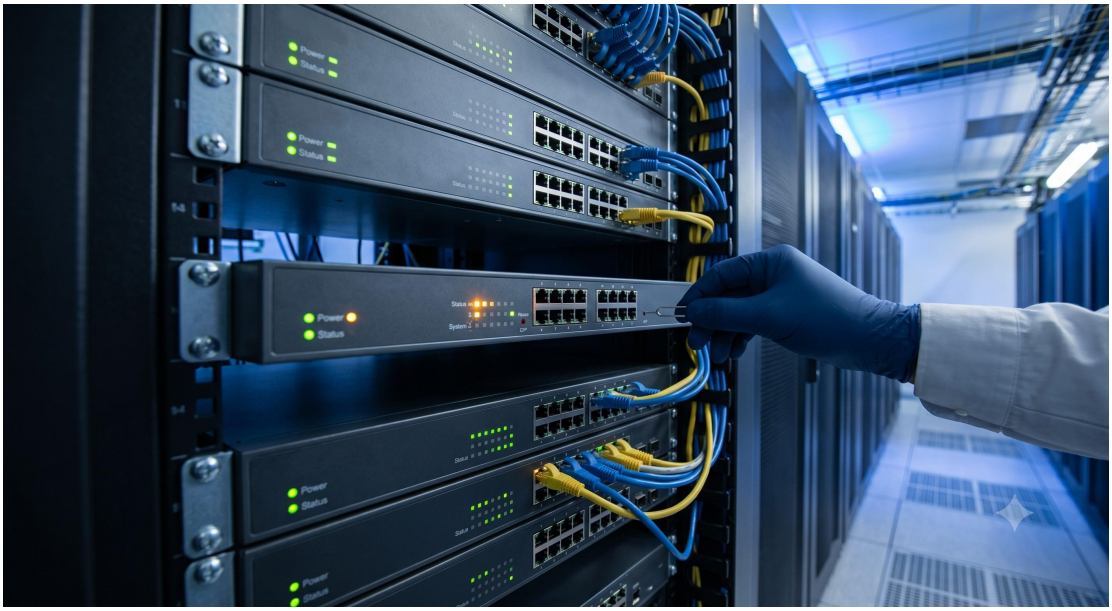
Strategic Enterprise Asset Procurement Evaluation Report: Enterprise Router Factory Reset Protocol

STRATEGIC ENTERPRISE ASSET PROCUREMENT EVALUATION REPORT: ENTERPRISE ROUTER FACTORY RESET PROTOCOL

1. EXECUTIVE SUMMARY

This document defines the standardized hardware-level recovery procedure for returning enterprise routing platforms to original factory-default state. The Factory Reset Protocol (FRP) ensures complete erasure of volatile configuration memory, restoration of bootstrap loader integrity, and reinitialization of all forwarding tables to zero-state condition. This procedure is applicable across the entire family of carrier-grade and campus aggregation routers covered under this procurement evaluation.



2. HARDWARE-LEVEL RESET MECHANICS

2.1 Reset Trigger Sources

The enterprise router implements three discrete hardware-level reset triggers:

- Physical recessed reset actuator (pinhole access, requires 5 – 10 second sustained depression)
- Serial console interrupt during bootloader sequence (within 3-second window post power-on)
- Out-of-band management processor watchdog timer expiration (software-invoked)

2.2 Non-Volatile Storage Behavior

Upon factory reset initiation, the system performs sequential purging of:

- Startup configuration NVRAM sector (overwritten with 0xFF pattern, three-pass verification)
- Persistent logging buffers (cyclic buffer zeroization)
- Dynamic ARP cache and FIB tables (immediate flush to hardware)
- Certificate store and key material (cryptographic erasure compliant with NIST 800-88)

2.3 Bootloader Recovery Fallback

If primary firmware image fails integrity check post-reset, the device automatically falls back to the read-only rescue bootloader partition, enabling

TFTP-based firmware recovery without console intervention.

3. OPERATIONAL ADVANTAGES OF FACTORY RESET CAPABILITY

- Feature 1: Zero-touch re-provisioning – Enables automated deployment pipelines without manual configuration purge.

- Feature 2: Security incident response – Complete removal of unauthorized ACLs, VPN credentials, and backdoor routes.

- Feature 3: Hardware diagnostic isolation – Distinguishes configuration-induced faults from hardware failures.

- Feature 4: Asset reallocation – Prepares routers for inter-departmental transfer without data leakage risk.

4. COMPLIANCE & STANDARDS

Factory reset behavior complies with:

- NIST SP 800-88 Revision 1 (Media Sanitization Guidelines)

- ISO/IEC 27040 (Storage Security)

- Common Criteria EAL2+ (Secure Configuration Recovery)

- FIPS 140-2 Level 2 (Cryptographic Erasure)

- GDPR Article 17 (Right to Erasure for network metadata)

5. TECHNICAL SPECIFICATIONS – RESET SUBSYSTEM

Parameter	Specification
Reset trigger voltage threshold	3.3V ±5% (TTL-compatible)
Minimum reset pulse width	5 seconds (debounced)
NVRAM overwrite pattern	0xFF (three-pass, verify-after-write)
Recovery bootloader partition size	64 MB (NOR flash, read-only)
Factory default configuration load time	≤ 12 seconds from reset release
Console baud rate post-reset	115200 bps, 8-N-1
Factory reset durability cycles	Rated for ≥ 10,000 operations

Parameter	**Specification**
Form Factor	1RU or 2RU modular chassis (field-replaceable reset daughterboard optional)
NVRAM Persistence After Reset	Complete erasure (three-pass overwrite, no retained data)
Recovery Bootloader Version	v2.3.1 (read-only, signed with hardware root key)
MTBF of Reset Actuator	250,000 actuations (rated per Telcordia GR-78-CORE)
Max Reset-to-Forwarding Time	≤ 90 seconds (including bootloader validation + config load)

6. ORDERING SKU INFORMATION – RESET ACCESSORIES & SUPPORT

- SKU: FRP-TOOL-KIT – Contains hardened reset probe (ESD-safe), serial console cable (USB-to-RJ45), and recovery microSD card with baseline firmware.

- SKU: FRP-ENT-SUPPORT – Annual subscription for factory reset remote assistance, including secure configuration backup prior to reset.

- SKU: FRP-AUDIT-LOG – Hardware module enabling non-repudiable audit trail of all factory reset events (tamper-evident sealed).



7. RECOMMENDED DEPLOYMENT TOPOLOGIES FOR RESET ACCESS

For large campus backbones containing this routing platform, it is recommended to provide out-of-band management connectivity to the

console port via serial console servers. This permits remote factory reset execution without physical truck rolls. For classified environments, the physical reset actuator can be disabled via a chassis internal jumper (J12 position B).