HAMR-FORGE

FORGE OS · PUBLIC TECHNICAL WHITEPAPER

Secure Overlay & Multi-WAN Transport

Authenticated MPTCP transport, dynamic routing, and bounded failover across heterogeneous WAN services

PUBLIC RELEASE

VALIDATED BASELINE V0.9.239 · SUPERSEDES V0.9.173 EDITION

PUBLISHED BY HAMR-FORGE, LLC · AUGUST 2026

Executive Abstract

This paper describes the FORGE OS v0.9.239 underlay-to-overlay model: outbound mutual-TLS enrollment, MPTCP subflow aggregation, routed tunnel interfaces, BGP or OSPF adjacency, path recovery, QoS policy, and fail-closed forwarding. It explains what the platform bonds, what it does not promise, and how operators can verify live path contribution.

Intended audience. Network architects, transport engineers, systems integrators, and technical evaluators.

> **Publication boundary: v0.9.239 capability is stated as current. Future work is labeled ROADMAP — NOT INCLUDED IN v0.9.239.**

1. Scope and Claim Boundary

This paper describes the publicly releasable behavior of FORGE OS v0.9.239, the current validated pre-release baseline. Validation evidence cited here comes from the project's automated release gates, virtual-appliance exercises, physical hardware testing, and a completed 72-hour firmware-lock endurance soak under continuous load. The term validated does not imply a third-party certification, government approval, product-level FIPS validation, or general-availability designation.

FORGE OS bonds reachable IP paths into an authenticated transport. It does not combine carrier radio spectrum, guarantee the arithmetic sum of advertised carrier rates, or eliminate congestion, latency, loss, NAT, or policy imposed by an upstream provider.

2. Underlay, Transport, and Overlay

The platform's central discipline is keeping three planes distinct: the physical or provider underlay, the authenticated MPTCP transport, and the routed overlay that carries protected traffic.

Plane	Examples	FORGE OS treatment
Underlay	Ethernet, fiber handoff, cellular router, satellite terminal, managed WAN	Each configured WAN provides source addressing, reachability, metric, and optional plan metadata
Transport	MPTCP over TCP 4500 with TLS 1.3 mutual authentication	One logical connection can use multiple subflows
Overlay	Point-to-point tunnel plus BGP or OSPF	Carries authorized routed prefixes independently of underlay addressing

FIGURE PLACEHOLDER

layered model — WAN underlays feeding one authenticated MPTCP session, routed overlay above

> **Reading the layers correctly:** multi-WAN availability (surviving a path loss), MPTCP subflow aggregation (multiple paths carrying one session), per-flow throughput, aggregate throughput, routing convergence, and application continuity are six different properties. Bonding is not a universal throughput multiplier: a single TCP flow, asymmetric carrier policy, receiver limits, loss, or latency can each cap what aggregation delivers.

3. Enrollment and Authentication

A SPOKE originates the connection to its configured HUB address and verifies the provisioned HUB CA fingerprint. The HUB accepts only the expected site identity and signs the approved SPOKE certificate. Subsequent sessions use certificate-based mutual authentication.

A certificate proves appliance identity; it does not by itself authorize arbitrary prefixes. Site registration, protocol configuration, explicit LAN advertisement, and the HUB's forwarding allowlist constrain the routed result.

- TLS 1.3 transport with server identity pinned to the configured HUB trust anchor
- ECDSA P-384 certificate identity in the validated baseline
- **AES-256-GCM-SHA384 is the required tunnel cipher suite**, selected for CNSA 1.0 alignment. The requirement is enforced at three layers: the SPOKE advertises only this suite, the HUB selects only this suite, and the data path re-verifies the negotiated suite at runtime. A peer unable to negotiate it fails the handshake — there is no downgrade path.
- Cryptographic operations in the data path execute within a FIPS 140-3 validated cryptographic module (CMVP certificate #5247). FORGE OS itself is not separately certified.

4. MPTCP Session Model

With identity established, transport begins on whichever WAN is reachable first. That first path creates the MPTCP-capable connection; additional eligible WAN addresses are signaled as endpoints and become subflows of the same logical session. A surviving subflow preserves the connection while another path is repaired or returns.

The dashboard and tunnel views report the aggregate session, the number of active WAN paths, and per-path contribution. TCP reset messages from unsuccessful parallel attempts can occur during subflow racing; they are diagnostic noise when a healthy authenticated session and expected subflow count remain present.

> **Aggregation is workload and path dependent. A single flow, asymmetric carrier policy, receiver limits, packet loss, or high latency can prevent linear throughput scaling.**

5. Path Health and Recovery

Path recovery is a cooperation among four mechanisms, each with a narrow job. The route guard — the platform's gate for tunnel-bearing routes — installs a narrowly scoped route to the HUB only after a WAN gateway is actually resolvable, so a cold boot with slow DHCP cannot strand a stale or premature route. The reconnect loop continues for as long as a HUB endpoint remains configured; there is no terminal give-up state that requires an operator to click reconnect. Endpoint rotation lets the session shed a missing WAN address and admit its replacement in place, while surviving subflows retain the session token — the tunnel does not tear down because one carrier re-addressed. Finally, routing reconvergence re-evaluates BGP or OSPF state over the recovered transport and withdraws overlay paths that are no longer usable.

In sequence: route guard admits the path, the reconnect loop re-establishes authenticated transport, endpoint rotation folds recovered or re-addressed WANs into the live session, and dynamic routing converges on the result. When diagnosing, read them together — MPTCP state, per-interface counters, routing state, and application tests each cover a different layer, and no single view proves health alone.

6. Dynamic Routing

FORGE OS supports BGP and OSPF over the tunnel. BGP is appropriate when a site has an independent autonomous-system identity. OSPF is appropriate when the deployment uses a shared link-state routing domain. The operator chooses the model when registering the site.

Neither is mandatory. A HUB fronted by a plain ISP router, or a deployment that carries everything as OSPF network extensions, may run no BGP at all — an unset autonomous-system number is a supported configuration rather than an incomplete one, and no platform function is gated on having one.

LAN and VLAN prefixes are advertised only when enabled. The UI exposes received and advertised route lists so a field operator can answer two practical questions: which networks is this site sending to the HUB, and which networks did it learn from the HUB?

State	Meaning
Tunnel connected	Authenticated overlay transport exists
BGP Established / OSPF Full	Routing control plane converged
Prefixes received	Remote networks accepted from the HUB

State	Meaning
Prefixes advertised	Local operator-selected networks announced upstream

7. QoS and Traffic Visibility

QoS policy is centrally distributed while shaping is applied where configured on SPOKEs. Ordered classes and DSCP markings express priority. The shaping engine pairs HTB (Hierarchical Token Bucket, a classful rate-reservation scheduler) with fq_codel (fair queuing with controlled-delay queue management) to enforce reservations under a measured or manual cap; the alternative CAKE engine (Common Applications Kept Enhanced, an integrated shaper) works from DiffServ tiers and ignores HTB reservation percentages.

Top-talkers and path-contribution views are operational safeguards, not decorative analytics. They help identify unexpected high-volume or multicast sources that could consume constrained WAN capacity.

- Multicast forwarding toward the HUB is disabled by default and explicitly enabled per SPOKE.
- Plan bandwidth fields scale visualizations; they are not proof of carrier performance.
- Use controlled speed testing and real traffic to establish a shaper value.

8. Failure Scenarios

Scenario	Expected behavior	Operator verification
One WAN lost	Session remains on surviving subflow; missing path retries	Active subflow count and per-path contribution
All WAN gateways absent at boot	HUB pinhole withheld; route guard waits for lease	WAN lease, gateway, route-guard logs
HUB restart	SPOKE retries; routing reconverges after listener returns	Tunnel connected plus BGP/OSPF state
Home HUB unreachable	Where a standby is assigned, SPOKE fails over to it automatically in approximately thirty seconds — a thirty-second all-WAN confirmation hold, then establishment. Break-then-make: traffic is interrupted, unlike a WAN path loss. Attachment is sticky until an operator schedules failback.	Serving-HUB indicator, tunnel state, and BGP Established / OSPF Full on the alternate

Scenario	Expected behavior	Operator verification
Carrier degraded but not down	Path may remain technically active	Latency/loss/application quality; use policy or physical remediation
Data-plane binary update	Controlled session rebuild	Installed/running hash match and convergence

FIGURE PLACEHOLDER

failover sequence — one WAN fails, the session survives on the remaining subflow, the path returns and reintegrates

9. Security and Isolation

WAN interfaces are not trusted merely because they are online. The SPOKE isolation controller blocks unauthorized egress and relaxes forwarding only around the authenticated overlay. Optional Internet breakout is explicit and visible.

> **FORGE OS cannot prevent an external modem, upstream router, hypervisor bridge, or physically bypassed LAN from creating a separate path outside the appliance.**

10. Roadmap — Not Included in v0.9.239

Roadmap items are architectural direction, not v0.9.239 capability. They are visually labeled and must not be used as procurement or deployment claims.

All four multi-HUB items carried in the v0.9.173 edition of this paper — multiple independently administered HUB destinations per SPOKE, per-SPOKE deterministic failover with NOC-visible current-HUB state, a replication and readiness model for secondary HUBs, and operator-controlled failback after primary recovery — have shipped. They are described in Sections 6 and 8.

Remaining roadmap work for the platform as a whole is tracked in the Platform Overview.

11. Acceptance Criteria

- Every intended WAN has a valid address and gateway.
- The live MPTCP session reports the expected subflow count.
- BGP is Established or OSPF is Full.
- Expected prefixes appear in received and advertised route views.

- A single-WAN removal preserves traffic within the deployment's accepted convergence window.
- Restoring the WAN re-adds path contribution without manual tunnel recreation.
- With all overlay paths removed, protected LAN traffic remains contained.

12. Conclusion

FORGE OS provides authenticated path aggregation and bounded resilience: multiple commodity WAN services carry one mutually authenticated session, dynamic routing scopes what the overlay may carry, and a fail-closed posture contains protected traffic when the overlay is absent. Performance and continuity remain dependent on underlay quality, routing convergence, application behavior, and customer configuration — the platform's role is to make each of those dependencies observable and verifiable rather than to promise them away. The acceptance criteria above convert this paper's claims into checks a deployment team can run on day one.

Document Control

Field	Value
Publisher	HAMR-FORGE, LLC
Platform	FORGE OS
Validated baseline	v0.9.239
Classification	Public release
Release date	22 August 2026
Supersedes	v0.9.173 edition (August 2026)
Claims boundary	No third-party certification or general-availability claim