BLUEDOT

COMMUNITY EDITION · 1.4.0 GA

BlueDot QuantumTouch IPoE

Features — The Operator Plane

The feature summary for QuantumTouch, the operator plane over the BlueDot Quantum IPoE BNG, and the companion to its Theory of Operations. Every capability under Operator Experience, Control & Protection, and Security & Platform ships and runs in this Community Edition GA release; planned additions are gathered under Coming Next.

Document Type	BlueDot Feature Summary
Component	QuantumTouch — Operator Plane
Edition	Community Edition — 1.4.0 GA
Audience	ISP Operators, NOC & Technical Evaluators
Companion To	QuantumTouch IPoE — Theory of Operations
Source Tree	`ipoe/quantumtouch-bng` @ `v1.4.0-14`
Classification	**BlueDot Proprietary**
Date	October 2026

© 2026 BlueDot · All rights reserved.

Every item below is implemented and running in this build. It is the operator plane above the forwarding stack — QuantumTouch never touches a packet. Designed-but-not-yet-shipping capabilities are listed only under Coming Next.

Operator Experience Features

Onboarding & Setup

- One-time bootstrap-token first admin (spent after first account)
- Guided, resumable setup wizard (welcome → … → review)
- Per-section apply with partial-success ✓ / ✕ grid
- Auto-saving draft (browser-refresh safe)
- DHCP punt-path self-heal on startup

Harvesting & Sampling

- Single five-second sampler heartbeat
- Three sources: controller, VPP-direct, BMC
- Reachability probes (RADIUS, uplink, portal, journal, hardware)
- Feature-aware probes (quiet when unconfigured)
- Reply-path stall detector (load-gated)
- Layered per-source caches (5 s – 60 s)
- Defensive ticks (zeros, never a crash)

Analytics & Observability

- Dual-resolution in-memory history (1 h @ 5 s / 30 d @ 5 min)
- Per-subscriber fast history (~4 h)
- Throughput charts (green/yellow/red, up + down, pps overlay)
- Live QoS-band proportion bar
- Sessions-over-time (CE ceiling reference line)
- Per-session traffic drawer
- Prometheus `/metrics` surface (~65 series, aggregate-only)
- Reset-aware counters (baseline-reset annotation)
- Disk-backed history (restart replays last hour)
- One-tick lag by design; honest gaps across outages
- Durable accounting drained from live subscriber traffic, independent of any open browser
- Grafana dashboard pack, installable as an add-on (five dashboards)
- IPMI chassis sensors exported to Prometheus, with shipped alerting rules

Dashboards & Health

- One shared health poll (single source of truth)
- Monotonic Healthy / Degraded / Fault verdict + reason sentence
- 15 s staleness grace (no single-miss flicker)
- KPI row + orphan-session reconciliation
- Pool-pressure bars (ok / warn / full)
- Radial gauges (CPU, mem, workers, disk, RX/TX) with thresholds
- Per-worker thread strip, hugepages, BMC hardware cards
- Live CPE → edge → BNG → core topology (stall-freeze tell)
- Session-capacity indicator against the licensed cap

Control & Protection Features

Configuration Surfaces

- Typed screens for every controller resource
- Identity-attached controller proxy (change logged to real operator)
- No-clobber drafts (background poll never overwrites edits)
- Live re-rate awareness (names sessions a save re-rates)
- Delete-refusal pre-warning (plans in live use)
- Wire units vs display units (kbps commit / Mbps display)
- Local pool-occupancy correction (works around controller bug)
- Writable pools, plans, captive portal, edge routers
- DSCP marking policy per direction (green AF11 / yellow AF12 by default; off by default)
- Local AAA as the authoritative subscriber store (not a view over the controller)
- Monthly data caps with an operator-chosen consequence, applied by the box
- Static IP assignment from the subscriber drawer, with conflict refusal
- Per-subscriber raw rate, expressed as a plan
- An account's live sessions on its own page, endable from there

Snapshots & Config Protection

- Point-in-time snapshots across five domains
- Content-hash identity (rename-stable, tamper-flagged on read)
- Structured + text diff (live-vs-snap and snap-vs-snap)
- Reboot-aware diffs
- Locked restore (safe order, explicit outcome)
- Dry-run restore (no lock, no change)
- Signed export/import (same-box / cross-box / legacy)
- Auto-prune with golden-tag protection

Audit, Events & Compliance

- Unified four-source timeline (QT, controller, journal, portal)
- Parallel fetch with graceful per-source degrade
- Deterministic row IDs (dashboard deep-link)
- Formula-injection-safe export (CSV / JSON, bulk to 1 year)
- Self-audited bulk export
- Off-box shipping: syslog (RFC 5424/6587 TLS), HTTP, S3
- At-least-once delivery, per-destination spool
- Drop-oldest back-pressure, destination isolation
- Encrypted destination secrets
- Sticky event feed (new → active → recovered → ack)
- Flap-safe incidents (re-fire, no event storm)
- RADIUS exchanges on the timeline — decoded and linted, off by default

Security, Platform & Roadmap

Security & Access

- HTTPS front door on `:8443` (single external surface)
- Session cookies, strong hashing, progressive lockout
- Optional TOTP MFA
- SAML SSO and LDAP/AD with group-to-role mapping
- Three roles (read-only / read-write / admin), server-enforced
- Reveal-once bearer keys (hashed; rotate, not recover)
- Per-key restrictions (IP allow-list, path scope, expiry)
- Secrets encrypted at rest (MFA seeds, LDAP bind, ship creds)
- Managed TLS (PEM import, cert history + rollback, policy)
- In-product ACME (HTTP-01)
- Signed security webhooks (failed-login burst, admin grant, …)
- Prometheus read proxy (default-deny allow-list) and a scoped metrics-only key preset

Platform & Capacities

- Single-node operator plane (one process owns state)
- One plugin per deployment
- Web UI `:8443`, controller `:3000` (proxied)
- Prometheus loopback `:9090`, demo portal `:8088`
- Durable operator state preserved across upgrades
- Linux / Python 3.12 / systemd / commodity x86
- Runs on the same host as the BNG (no separate box)
- Capacity-tier session licensing, activated from the console
- Add-on lifecycle: update checking, offline tarball install, catalogue URL, one-step rollback
- One-button diagnostic support bundle for a ticket

New in 1.4.0

- **Capacity-tier session licensing, operable from the console** — the alpha shipped the Licensing page but could not activate from it; activation was command-line only. It now reads status, shows the machine fingerprint, and activates a pasted or uploaded licence
- **Full accounting from live subscriber traffic** — usage records were a preview in the alpha, drained only while someone had a page open. A background drain now claims the controller's accounting spool and commits it to a durable local ledger, acknowledging upstream only after the commit lands
- **Local AAA as system of record** — the authoritative subscriber store, not a view over controller state
- **Data-cap enforcement** — a monthly cap and a consequence the operator chooses, applied by the box
- **Static IP assignment** from the subscriber drawer, with a conflicting address refused
- **Per-subscriber raw rate**, expressed as a plan and settable per subscriber
- **Subscriber sessions** — an account's live sessions listed on its own page, and endable from there
- **Support bundle** — one button produces a diagnostic bundle for a ticket
- **Add-on lifecycle** — update checking that stays quiet when it should, install from an uploaded tarball for an offline box, a catalogue URL an offline mirror can own, and one retained previous artifact so a failed update rolls back without a download
- **Six new Prometheus alert rules** and a metrics reference documenting all 36 exported series

Coming Next

- Prometheus-first analytics store (read-path cutover + source badge)
- Curated analytics query API (CSV / PromQL, RADIUS histograms)
- Port-role map populated (`bng_uplink_*` / `bng_access_*` live)
- Auth event counters (`auth_*_total`) incrementing
- RADIUS config-write from the UI
- In-product ACME DNS-01 automation
- Horizontal (multi-node) operator plane
- Platform lifecycle for the BNG itself: update checking, in-place upgrade, rollback (the add-on half shipped in 1.4.0)

Scope & Caveats

- Owns operator experience, never the forwarding path
- Single-node management plane (HA is roadmap)
- Poll, don't push (5 s model; no WebSocket)
- Aggregate-only metric cardinality
- Analytics store today is in-memory history, not Prometheus (yet)
- Two port families + auth counters report zero until wired
- RADIUS is not active in this release; local AAA is the AAA backend, and there is no RADIUS page in the console
- ACME issuance is partial (HTTP-01 ships; DNS-01 later)
- One plugin per deploy

Prepared from the QuantumTouch source tree (`ipoe/quantumtouch-bng` , tag `v1.4.0-14`) as the operator-plane companion to the QuantumTouch IPoE Theory of Operations. Field-level request/response shapes are authoritative in the generated OpenAPI spec and the source. *© 2026 BlueDot Insight LLC. BlueDot Proprietary.*