GOVERNMENT OF BIHAR // NATIONAL INFORMATICS CENTRE (NIC)

Synthetic Probe Execution Timings & Architecture

Duration, Frequency, Latency Milestones, and Network Overhead Blueprint

CURRENT ENGINE
`CNI-NOC-KERNEL:3001`

Timing Executive Summary: Each monitoring cycle operates on two precise time axes: **(1) Execution Duration:** Each individual synthetic transaction takes only **200ms to 450ms** to complete the full DNS, TCP, SSL, and HTTP validation. **(2) Polling Frequency:** Probes trigger every **60 seconds** (1,440 checks/portal/day). If an anomaly occurs, it retries after **60 seconds**, confirming real downtime within **120 seconds** without false alarms.

NODE.JS KERNEL (PORT 3001)
Single-Threaded Asynchronous libuv Event Loop Engine

1. Web & API Server

- **Serves Web UI:** Vue 3 SPA frontend delivered to NOC browsers.
- **Handles Logins:** Verifies BCrypt hashes & signs JWT session tokens.
- **WebSockets Push:** Broadcasts sub-second live telemetry via Socket.IO.
- **Status Page Gateway:** Streams live health to department dashboards.

2. Synthetic Engine

- **DNS Lookup:** Measures hostname resolution timing in milliseconds.
- **SSL Handshake:** Negotiates TLS and extracts x509 expiration date.
- **HTTP Status 200:** Checks status codes (200 OK, 401 Auth handshake).
- **Measures Millis:** Tracks exact end-to-end user experience latency.

3. Database Engine

- **Writes to SQLite (WAL):** Appends heartbeats with zero lock delays.
- **Calculates SLA %:** Computes rolling 24-hour, 30-day, and 1-year uptime.
- **Incident Logs:** Captures exact outage timestamp, error code & recovery.
- **Compaction Daemon:** Aggregates historical metrics to save disk space.

1. CORE TIMING METRICS (LIVE PRODUCTION PARAMETERS)

Production Timers

PROBE FREQUENCY
`60 sec`
Standard interval between scheduled synthetic health checks.

CHECK DURATION
`240-400 ms`
Time taken to execute each complete L7 synthetic transaction.

FAULT RETRY TIMER
`60 sec`
Re-probes once after 60s if the first attempt encounters an error.

DOWNTIME ALERT
`≤ 120 sec`
Total time to confirm true outage and dispatch emergency alerts.

2. ANATOMY OF A SINGLE PROBE: "HOW LONG DOES 1 PING TAKE?"

Sub-Second Breakdown

PHASE 1: DNS LOOKUP	PHASE 2: TCP HANDSHAKE	PHASE 3: TLS CRYPTOGRAPHY	PHASE 4: HTTP REQUEST	TOTAL COMPLETED
`10 - 35 ms`	`15 - 45 ms`	`70 - 140 ms`	`120 - 220 ms`	`240 - 440 ms`
Queries local NOC DNS cache to resolve portal domain name.	Establishes 3-way SYN-ACK handshake with remote web server.	Negotiates SSL cipher and inspects certificate expiration date.	Transmits GET request, receives HTTP 200/401, parses payload.	Complete end-to-end transaction written to SQLite database.

LIVE FLEET TELEMETRY BENCHMARKS

Production Portal Latency & Network Overhead Analysis

Measured Telemetry from STATE-NOC-NODE Across Departmental Endpoints

TELEMETRY SOURCE
LIVE KUMA.DB

3. LIVE TELEMETRY BENCHMARKS (RECORDED DIRECTLY ON STATE-NOC-NODE)

Actual Fleet Data

DEPARTMENT / PORTAL	PROTOCOL	CHECK FREQUENCY	MEASURED LATENCY	CHECKS / 24H	OPERATIONAL STATUS
VLTS Transport Portal (Transport Dept)	HTTPS (IIS Auth Handshake)	Every **60 seconds**	**241 ms – 334 ms**	1,440 checks	HEALTHY (100% SLA)
ISTP Bihar (Agriculture Dept)	HTTPS GET (200 OK)	Every **60 seconds**	**315 ms – 434 ms**	1,440 checks	HEALTHY (100% SLA)
Khanan Soft Bihar (Mines & Geology)	HTTPS GET (200 OK)	Every **60 seconds**	**347 ms – 396 ms**	1,440 checks	HEALTHY (100% SLA)
Bihar State NOC Dashboard (Internal Core)	HTTP GET (LAN Routing)	Every **60 seconds**	**2 ms – 8 ms**	1,440 checks	LOCAL LOOPBACK

4. NETWORK BANDWIDTH & SERVER OVERHEAD FOOTPRINT

Zero Strain Verification

NETWORK BANDWIDTH USAGE

- **Payload per probe:** ~2.5 Kilobytes (HTTP HEAD/GET request + headers).
- **Bandwidth per target per minute:** ~0.04 KB/second.
- **Total monthly bandwidth per portal:** ~108 Megabytes.
- **Executive Conclusion:** Negligible network overhead; uses less than **0.001%** of NOC link capacity.

SERVER HARDWARE RESOURCE IMPACT

- **CPU Consumption:** < 0.5% average CPU load on host `STATE-NOC-NODE`.
- **RAM Footprint:** Enforced 512 MB ceiling; actively runs at **~165 MB**.
- **Database Growth:** SQLite appends ~45 KB per day per target.
- **Executive Conclusion:** Zero contention with IIS Port 80 web traffic.

5. FLAPPING & OUTAGE ESCALATION LIFECYCLE

Timeline to Alert

ELAPSED TIME	INTERNAL STATE	SYSTEM ACTION	NOC STATUS
T = 0s	Target Fails Probe	Records socket timeout / HTTP 500. Sets state to `PENDING`.	PENDING (NO ALARM)
T = 60s	Retry Probe Triggered	Initiates second probe attempt to confirm failure.	RE-TESTING
T = 60.3s	Failure Confirmed	Failure verified twice. State transitions to `DOWN (0)`.	INCIDENT DECLARED
T = 61s	Incident Dispatched	Turns RED on NOC video wall; dispatches WhatsApp/Telegram alert.	NOC ALERT TRANSMITTED

Manager Summary Statement: *"Our probes run every 60 seconds and complete in roughly 300 milliseconds. If any portal experiences a disruption, our system double-checks it after 60 seconds and alerts the duty officer within 2 minutes total—eliminating false alarms while ensuring instant reaction to real outages."*