A Framework for Fast Network Notifications

draft-song-fann-framework-01

H. Song (Futurewei) · J. Dong (Huawei) · W. Cheng (China Mobile)
Y. Zhu (China Telecom) · R. Pang (China Unicom) · L. M. Contreras (Telefonica)
L. Guo (COSCO Shipping Technology)

IETF FANN Working Group

Purpose & Scope

- The FANN framework deliverable (Informational): architecture and integration with existing technologies
- Defines functional roles, an information model, and delivery & scoping models
- Not a wire protocol, encoding, or YANG model — those are separate documents
- Solution-agnostic: control-plane, forwarding-plane, and in-band mechanisms can all conform
- Forwarding plane (ideally hardware) is primary for latency; control/management consumption is secondary and must preserve routing stability
- Deployment: networks under a single administrative control; scoped notification domains
- “Fast” = sub-millisecond to a few milliseconds, shorter than the affected traffic’s RTT

Where It Fits: the Detection–Reaction Gap

- Hardware detects failures / degradation / congestion in microseconds to sub-millisecond
- Disseminating that state to remote nodes that can act is the bottleneck — this gap is the problem
- Companion WG documents this framework builds on:
  - Problem Statement — draft-ietf-rtgwg-net-notif-ps
  - Requirements — draft-geng-fantel-fantel-requirements
  - Gap Analysis — draft-geng-fantel-fantel-gap-analysis
- Supplies the architecture, information, delivery and integration models a solution instantiates

Document Structure

- 1. Introduction / Scope / Requirements Language
- 2. Terminology
- 3. Fast Network Notification Framework
  - Principles · Scenarios · Architecture · Information model · Delivery & scoping · Discovery/registration · Loop prevention & damping
- 4. Realization & Operational Considerations
  - Integration · Candidate approaches · Applications · Scaling · Operational
- 5. Security Considerations
- 6. IANA Considerations

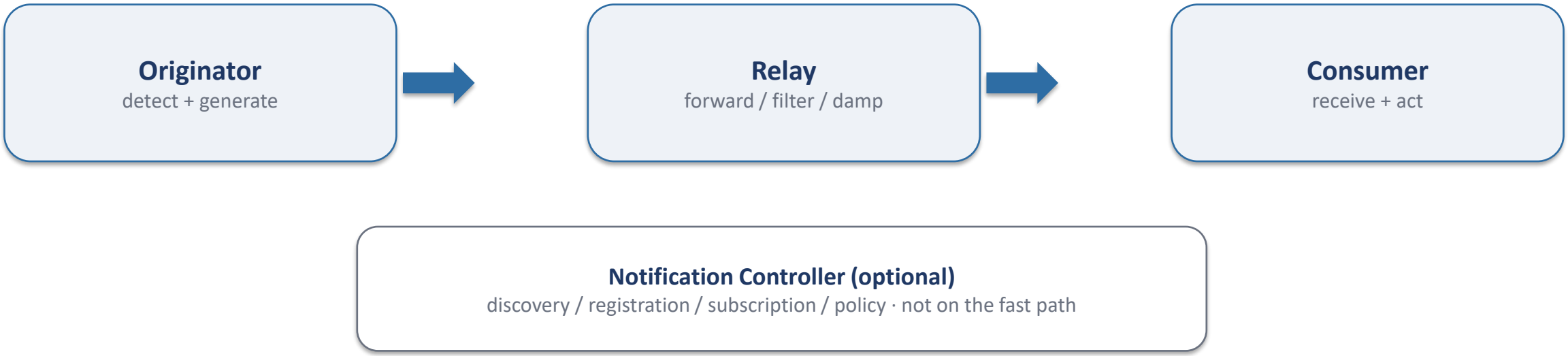
Design Principles

- Event-driven, not periodic
- Forwarding-plane optimized (ideally hardware); control/management consumption secondary
- Lightweight & bounded — must not worsen the event it reports
- Action-agnostic — conveys information; does not mandate a reaction
- Extensible — information model, event taxonomy, and on-the-wire encoding (forward-compatible must-ignore rule)
- Complementary to OAM, telemetry, and control-plane mechanisms
- Scoped & isolated to a notification domain
- Decoupled from routing convergence — carry fast-changing state outside the IGP

Deployment Scenarios

Scenario	Character	Notification approach
Intra-DC fabric	Few hops; sub-ms budget; HW detect + consume	In-band / scoped flooding; volume is the challenge
Single-hop DCI / P2P WAN	Small, known recipient set; budget = link delay	Unicast / directed to upstream or ingress
Multi-hop managed DCI	Deterministic TE paths; slicing; AI collaborative computing	Per-slice / per-path scoping; hop-by-hop along path
Multi-hop / arbitrary WAN	Many hops & recipients; ms budget; storm risk	Subscription, relaying with filtering, bounded scope

Reference Architecture & Lifecycle



Lifecycle: Detect → Generate → Deliver → Consume → Act → Recover / withdraw

A single node MAY implement more than one role; a consumer may also relay.

Information Model

- Event type — failure / degradation / congestion; onset or recovery
- Location — link, node, interface, or queue identifier
- Fine-grained status — utilization, available bandwidth, capacity, queue, delay, jitter, loss → graduated, not binary, responses
- Path identification; flow / service identification (e.g., 5-tuple)
- Timing & validity; optional action hint
- Origin (may be the source IP) + optional sequence/epoch
- Per scenario, some elements mandatory, others optional

Delivery, Scoping & Control

- Delivery modes: unicast · multicast / P2MP · hop-by-hop · scoped flooding
- Transport MUST support prioritization (dedicated DSCP / EF PHB, low-latency queue) — not queued behind the congestion it reports
- Notification domain: identify membership and isolate; no cross-domain propagation without policy
- Discovery / registration / subscription — each consumer receives only relevant information
- Loop prevention, filtering & aggregation, and flap damping bound the load

Integration with Existing Technologies

- Layer 2 / link: FEC alarms as detection inputs; L2 protection as a response
- Layer 3 / routing: complements IGP/BGP & FRR; wider view than a local PLR; MUST preserve routing stability
- Layer 4 / transport: richer & faster than ECN; runs concurrently with E2E congestion control — stay net-positive, don’t suppress E2E signals
- Detection & OAM: BFD is a detection input; IOAM, Alternate-Marking, IPFIX are telemetry — not rapid alerts

Candidate Realization Approaches

- Neighbor link/path status advertisement, decoupled from the IGP — draft-zzhang-rtgwg-router-info
- IGP / BGP protocol extensions
- In-band / data-plane signaling — motivated by draft-clad-rtgwg-ipfrr-aiml; protocols draft-camarillo-rtgwg-lsn, draft-csaszar-rtgwg-ipfrr-fn (+ draft-lu-fn-transport)
- Tunnel / overlay delivery in the WAN — draft-hzh-fantel-wan-tunnel
- Telemetry-assisted collection toward the source — draft-song-rtgwg-falcon
- Path- & slice-scoped flow control / backpressure — draft-liu-rtgwg-srv6-cc, draft-han-rtgwg-fine-grained-backpressure

Illustrative Applications (actions out of scope)

- Upstream (remote) protection — activate a pre-computed backup upstream; avoids LFA/TI-LFA hairpinning (draft-clad-rtgwg-efficient-remote-protection)
- Fast protection in AI/ML fabrics — tens of microseconds, in the forwarding plane (draft-clad-rtgwg-ipfrr-aiml)
- Graduated load-sharing & flow control — rebalance path weights, or per-flow / per-tenant / per-slice backpressure, by severity
- Common need: convey more than a binary state, reach the acting node, beat the traffic's control loop

Scaling, Operational & Security

- Scaling: subscription, scoping & domain isolation, relay filtering / aggregation, damping, rate limiting
- Operational: configurable triggers, delivery modes/scopes, damping and priority; YANG management; observability
- Security: integrity protection, origin authentication, and rate control are MUST
- Single-administrative-control bounds the threat surface — defense-in-depth, not a substitute for in-domain controls

Next Steps & Discussion

- Seeking WG review and feedback on the architecture and models
- Kept solution-agnostic and aligned with the Problem Statement / Requirements
- Request: consider adoption as the WG framework document

Thank You!

Comments welcome on the list.