Workgroup: RAW
Published: 4 March 2024
Intended Status: Informational
Expires: 5 September 2024
Authors: P. Thubert, Ed.

Reliable and Available Wireless Architecture

Abstract

Reliable and Available Wireless (RAW) provides for high reliability and availability for IP connectivity across any combination of wired and wireless network segments. The RAW Architecture extends the DetNet Architecture and other standard IETF concepts and mechanisms to adapt to the specific challenges of the wireless medium, in particular intermittently lossy connectivity. This document defines a network control loop that optimizes the use of constrained spectrum and energy while maintaining the expected connectivity properties, typically reliability and latency. The loop involves DetNet Operational Plane functions, with a new recovery Function and a new Point of Local Repair operation, that dynamically selects the DetNet path(s) for the future packets to route around local degradations and failures.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 September 2024.

Copyright Notice

Table of Contents

1. Introduction

Deterministic Networking aims to provide bounded latency and eliminate congestion loss, even when co-existing with best-effort traffic. It is getting traction in various industries including professional A/V, manufacturing, online gaming, and smartgrid automation, with both cost savings and complexity benefits (e.g., vs. loads of point-to-point (P2P) cables).

Bringing determinism in a packet network means minimizing the statistical effects of multiplexing that result in probabilistic jitter and loss. This can be approached with a tight control of the physical resources to maintain the amount of traffic within a budgeted volume of data per unit of time that fits the physical capabilities of the underlying network, and the use of time-shared resources (bandwidth and buffers) per circuit, and/or by shaping and/or scheduling the packets at every hop.

This innovation was initially introduced on wired networks, with IEEE 802.1 Time Sensitive networking (TSN) - for Ethernet LANs - and

IETF DetNet. But the wired and the wireless media are fundamentally different at the physical level and in the possible abstractions that can be built for IPv6 [IPv6], more in [IPoWIRELESS]. Nevertheless, deterministic capabilities are required in a number of wireless use cases as well [RAW-USE-CASES]. With scheduled radios such as Time Slotted Channel Hopping (TSCH) and Orthogonal Frequency Division Multiple Access (OFDMA) [RAW-TECHNOS] being developed to provide determinism over wireless links at the lower layers, providing DetNet capabilities is now becoming possible.

Wireless networks operate on a shared medium where uncontrolled interference, including the self-induced multipath fading cause random transmission losses. Fixed and mobile obstacles and reflectors may block or alter the signal, causing transient and unpredictable variations of the throughput and packet delivery ratio (PDR) of a wireless link. This adds new dimensions to the statistical effects that affect the quality and reliability of the link.

Reliable and Available Wireless (RAW) takes up the challenge of providing highly available and reliable end-to-end performances in a network with scheduled wireless segments. To achieve this, RAW can leverage multiple links and parallel transmissions, providing enough diversity and redundancy to ensure the timely packet delivery while preserving energy and optimizing the use of the shared spectrum.

Distance Vector (DV) protocols can enable more than one feasible successors along non-equal-cost multipath forwarding graphs. This provides redundancy and allows to dynamically adapt the forwarding operation to the state of the links. But this protection is limited since only a subset of the nodes along the path will have a feasible alternate successor.

RAW solves that problem by defining Protection Paths that can be fully non-congruent and can be activated dynamically upon failures. This requires additional control to take the routing decision early enough along the possible paths to route around the failure. RAW defines a end-to-end control loop that dynamically controls the activation and deactivation of the feasible Protection Paths.

In addition, RAW introduces the RAW API, which is an interface between the lower layer wireless technology and the DetNet layers. The RAW API is RAW technology [RAW-TECHNOS] dependent as it can vary what the different RAW technologies expose towards the DetNet layers. Furthermore, the different RAW technologies are equipped with different reliability features, e.g., short range broadcast, MUMIMO, PHY rate and other Modulation Coding Scheme (MCS) adaptation, (H)ARQ, constructive interference and overhearing. The RAW API enables interactions between the reliability functions

provided by the wireless technology and the reliability functions provided by DetNet. That is, the RAW API makes cross-layer optimization possible for the reliability functions of different layers depending on the actual exposure provided via the RAW API by the given RAW technology.

This document presents the RAW problem and associated terminology in Section 3.2, presents a conceptual model for RAW in Section 4, and, based on that model, elaborates on an in-network optimization control loop in Section 5.2.

2. Terminology

RAW reuses terminology defined for DetNet in the "Deterministic Networking Architecture" [RFC8655], e.g., PREOF for Packet Replication, Elimination and Ordering Functions. RAW inherits and augments the IETF art of Protection as seen in DetNet and Traffic Engineering.

RAW also reuses terminology defined for MPLS in [RFC4427] such as the term recovery as covering both Protection and Restoration, a number of recovery types. That document defines a number of concepts like recovery domain that are used in the RAW works, and creates the new term recovery graph. A recovery graph associates a topological graph with usage metadata that represent how the paths within the recovery graph are built.

RAW also reuses terminology defined for RSVP-TE in [RFC4090] such as the Point of Local Repair (PLR). The concept of backup path is generalized with protection path, which is the term mostly found in recent standards and used in this document.

RAW also reuses terminology defined for 6TiSCH in [6TiSCH-ARCHI] and equates the 6TiSCH concept of a Track with that of a recovery graph.

In an quantic analogy, a recovery graph is to a path what an atomic orbital is to a planetary orbit, in that the electron has a probability of presence within a known shape as opposed to a deterministic trajectory.

The concept of recovery graph is agnostic to the underlaying technology and applies but is not limited to any fully or partially wireless mesh. RAW specifies strict and loose recovery graphs depending on whether the path is fully controlled by RAW or traverses an opaque network where RAW cannot observe and control the individual hops.

RAW uses the following terminology and acronyms:

2.1. Acronyms

2.1.1. ARQ

Automatic Repeat Request, a well-known mechanism, enabling an acknowledged transmission with retries to mitigate errors and loss. ARQ may be implemented at various layers in a network. ARQ is typically implemented at Layer-2, per hop and not end-to-end in wireless networks. ARQ improves delivery on lossy wireless. Additionally, ARQ retransmission may be further limited by a bounded time to meet end-to-end packet latency constraints. Additional details and considerations for ARQ are detailed in [RFC3366].

2.1.2. FEC

Forward Error Correction, adding redundant data to protect against a partial loss without retries.

2.1.3. HARQ

Hybrid Automatic Repeat Request, combining FEC and ARQ.

2.1.4. MCS

Modulation and Coding Scheme. Controls the throughput of the Link to maintain reliable transmissions.

2.1.5. OAM

OAM stands for Operations, Administration, and Maintenance, and covers the processes, activities, tools, and standards involved with operating, administering, managing and maintaining any system. This document uses the terms Operations, Administration, and Maintenance, in conformance with the 'Guidelines for the Use of the "OAM" Acronym in the IETF' [RFC6291] and the system observed by the RAW OAM is the recovery graph.

2.1.6. OODA

Observe, Orient, Decide, Act. The OODA Loop is a conceptual cyclic model developed by USAF Colonel John Boyd, and that is applicable in multiple domains where agility can provide benefits against brute force.

2.2. Link and Direction

2.2.1. Flapping

In the context of RAW, a link flaps when the reliability of the wireless connectivity drops abruptly for a short period of time, typically of a subsecond to seconds duration.

2.2.2. Uplink

Connection from end-devices to a data communication equipment. In the context of wireless, uplink refers to the connection between a station (STA) and a controller (AP) or a User Equipment (UE) to a Base Station (BS) such as a 3GPP 5G gNodeB (gNb).

2.2.3. Downlink

The reverse direction from uplink.

2.2.4. Downstream

Following the direction of the flow data path along a recovery graph.

2.2.5. Upstream

Against the direction of the flow data path along a recovery graph.

2.3. Path and Recovery Graphs

2.3.1. Path

Quoting section 1.1.3 of [INT-ARCHI]:

> At a given moment, all the IP datagrams from a particular source host to a particular destination host will typically traverse the same sequence of gateways. We use the term "path" for this sequence. Note that a path is unidirectional; it is not unusual to have different paths in the two directions between a given host pair.

Section 2 of [I-D.irtf-panrg-path-properties] points to a longer, more modern definition of path, which begins as follows:

> A sequence of adjacent path elements over which a packet can be transmitted, starting and ending with a node. A path is unidirectional. Paths are time-dependent, i.e., the sequence of path elements over which packets are sent from one node to another may change. A path is defined between two nodes.

It follows that the general acceptance of a path is a linear sequence of links and nodes, as opposed to a multi-dimensional graph, defined by the experience of the packet that went from a node A to a node B. In the context of this document, a path is observed by following one copy or one fragment of a packet that conserves its uniqueness and integrity. For instance, if C replicates to E and F and D eliminates on the way from A to B, a packet from A to B can experience 2 paths, A->C->E->D->B and A->C->F->D->B. The terms lane is used to clarify when dealing with such path.

With DetNet and RAW, a packet may be duplicated, fragmented and network-coded, and the various byproducts may travel different paths that are not necessarily end-to-end between A and B; we refer to that complex experience as a DetNet path. As such, the DetNet path extends the above description of a path, but it still matches the experience of a packet that traverses the network.

With RAW, that experience is subject to change from a packet to the next, but all the possible experiences are all contained within a finite set. Therefore, we introduce below the term of a recovery graph that coalesces that set and covers the overall topology where the possible DetNet paths are all contained. As such, the recovery graph coalesces all the possible paths a flow may experience, each with its own statistical probability to be used.

2.3.2. Recovery Graph

A networking graph that can be followed to transport packets with equivalent treatment, associated with usage metadata; as opposed to the definition of a path above, a recovery graph represents not an actual but a potential, it is not necessarily a linear sequence like a simple path, and is not necessarily fully traversed (flooded) by all packets of a flow like a Detnet Path. Still, and as a simplification, the casual reader may consider that a recovery graph is very much like a DetNet path, aggregating multiple paths that may overlap, fork and rejoin, for instance to enable a protection service by the PREOF operations.

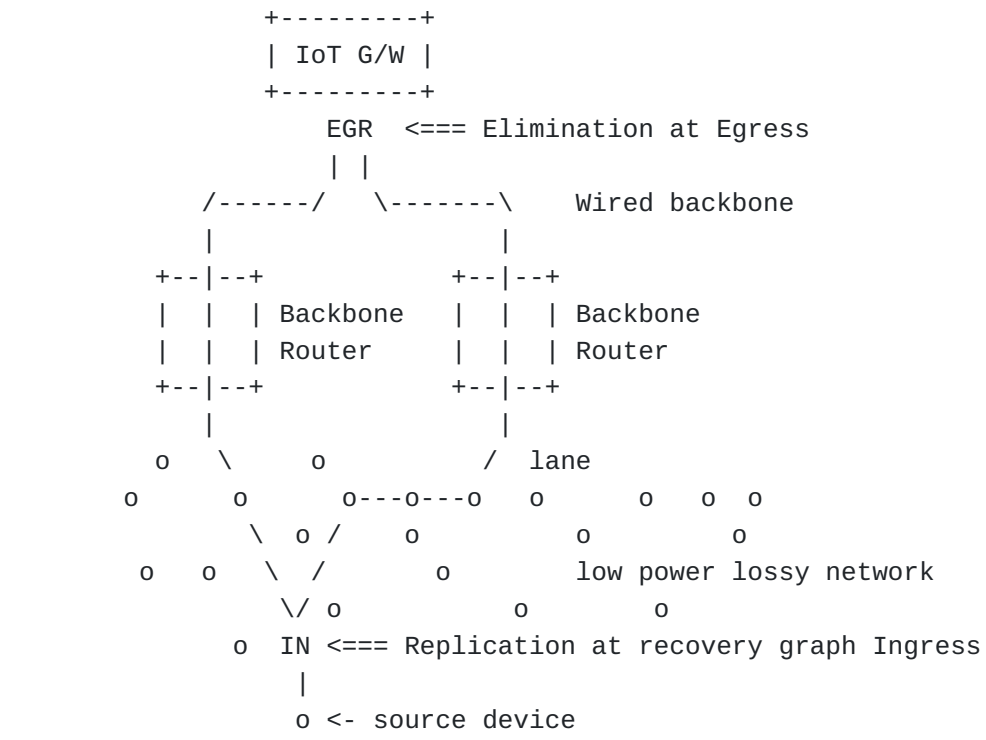

Figure 1: Example IoT Recovery Graph to an IoT Gateway with 1+1 Redundancy

Refining further, a recovery graph is defined as the coalescence of the collection of all the feasible DetNet Paths that a packet which flow is assigned to the recovery graph may be forwarded along. A packet that is assigned to the recovery graph will experience one of the feasible DetNet Paths based on the current selection by the PLR at the time the packet traverses the network.

Refining even further, the feasible DetNet Paths within the recovery graph may or may not be computed in advance, but decided upon the detection of a change from a clean slate. Furthermore, the PLR decision may be distributed, which yields a large combination of possible and dependant decisions, with no node in the network capable of reporting which is the current DetNet Path within the recovery graph.

In DetNet [RFC8655] terms, a recovery graph has the following properties:

*A recovery graph is a Layer-3 abstraction built upon P2P IP links between routers. A router may form multiple P2P IP links over a single radio interface.

*A recovery graph has one Ingress and one Egress nodes, which operate as DetNet Edge nodes.

*The graph of a recovery graph is reversible, meaning that packets can be routed against the flow of data packets, e.g., to carry OAM measurements or control messages back to the Ingress.

*The vertices of that graph are DetNet Relay nodes that operate at the DetNet Service sub-layer and provide the PREOF functions.

*The topological edges of the graph are strict sequences of DetNet Transit nodes that operate at the DetNet Forwarding sub-layer.

Figure 2 illustrates the generic concept of a recovery graph, between an Ingress Node and an Egress Node The recovery graph is composed of forward Lanes and forward or crossing Segments, see the definition for those terms in the next sections. A Protection Path contains at least 2 Lanes as a main path and a backup path.

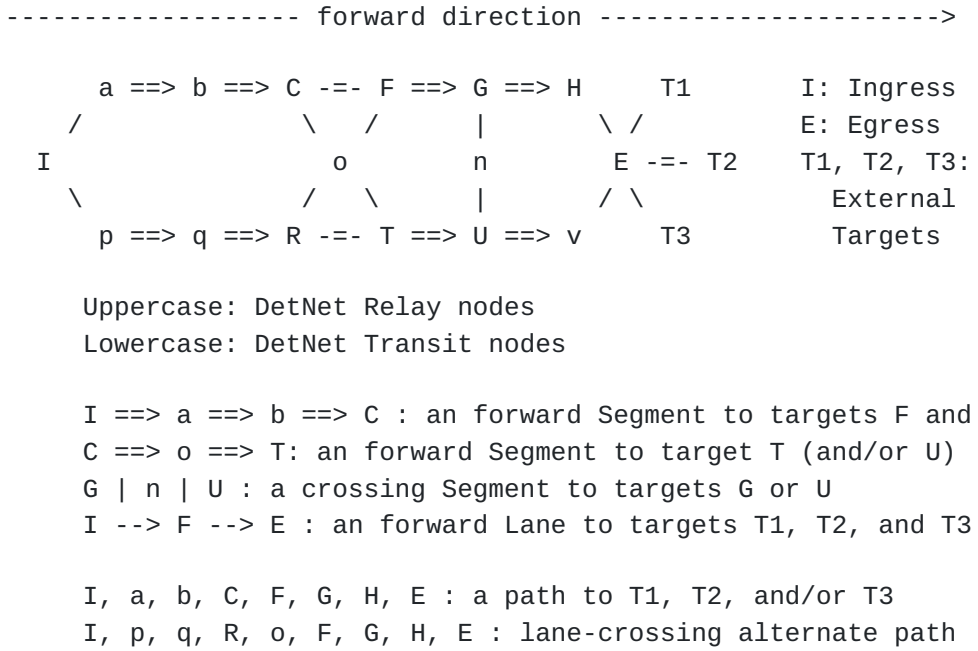

Figure 2: A Recovery Graph and its Components

2.3.3. Forward and Crossing

Forward refers to progress towards the recovery graph Egress. Forward links are directional, and packets that are forwarded along the recovery graph can only be transmitted along the link direction. Crossing links are bidirectional, meaning that they can be used in both directions, though a given packet may use the link in one direction only. A Segment can be forward, in which case it is composed of forward links only, or crossing, in which case it is

composed of crossing links only. A lane is always forward, meaning that is is composed of forward links and Segments.

2.3.4. Lane

An end-to-end forward lane between the Ingress and Egress Nodes of a recovery graph. A lane in a recovery graph is expressed as a strict sequence of DetNet Relay nodes or as a loose sequence of DetNet Relay nodes that are joined by recovery graph Segments.

2.3.5. Segment

A strict sequence of DetNet Transit nodes between 2 DetNet Relay nodes; a Segment of a recovery graph is composed topologically of two vertices of the recovery graph and one edge of the recovery graph between those vertices.

2.4. Deterministic Networking

This document reuses the terminology in section 2 of [RFC8557] and section 4.1.2 of [RFC8655] for deterministic networking and deterministic networks.

2.4.1. Flow

A collection of consecutive IP packets defined by the upper layers and signaled by the same 5 or 6-tuple, see section 5.1 of [RFC8939]. Packets of the same flow must be placed on the same recovery graph to receive an equivalent treatment from Ingress to Egress within the recovery graph. Multiple flows may be transported along the same recovery graph. The DetNet Path that is selected for the flow may change over time under the control of the PLR.

2.4.2. Deterministic Flow Identifier (L2)

A tuple identified by a stream_handle, and provided by a bridge, in accordance with IEEE 802.1CB. The tuple comprises at least destination MAC and VLAN ID. Continuous streams are characterized by bandwidth and max packet size; scheduled streams are characterized by a repeating pattern of timed transmissions.

2.4.3. Deterministic Flow Identifier (L3)

See section 3.3 of [DetNet-DP]. The classical IP 5-tuple that identifies a flow comprises the source IP, destination IP, source port, destination port, and the upper layer protocol (ULP). DetNet uses a 6-tuple where the extra field is the DSCP field in the packet. The IPv6 flow label is not used for that purpose.

2.4.4. TSN

TSN stands for Time Sensitive Networking and denotes the efforts at IEEE 802 for deterministic networking, originally for use on Ethernet. Wireless TSN (WTSN) denotes extensions of the TSN work on wireless media such as the selected RAW technologies [RAW-TECHNOS].

2.5. Reliability and Availability

In the context of the RAW work, Reliability and Availability are defined as follows:

2.5.1. Service Level Agreement

In the context of RAW, an SLA (service level agreement) is a contract between a provider (the network) and a client, the application flow, about measurable metrics such as latency boundaries, consecutive losses, and packet delivery ratio (PDR).

2.5.2. Service Level Objective

A service level objective (SLO) is one term in the SLA, for which specific network setting and operations are implemented. For instance, a dynamic tuning of the packet redundancy will address an SLO of consecutive losses in a row by augmenting the chances of delivery of a packet that follows a loss.

2.5.3. Service Level Indicator

A service level indicator (SLI) measures the compliance of an SLO to the terms of the contract. It can be for instance the statistics of individual losses and losses in a row as time series.).

2.5.4. Reliability

Reliability is a measure of the probability that an item will perform its intended function for a specified interval under stated conditions (SLA). RAW expresses reliability in terms of Mean Time Between Failure (MTBF) and Maximum Consecutive Failures (MCF). More in [NASA].).

2.5.5. Available

That is exempt of unscheduled outage or derivation from the terms of the SLA. A basic expectation for a RAW network is that the flow is maintained in the face of any single breakage or flapping.

2.5.6. Availability

Availability is a measure of the relative amount of time where a RAW Network operates in stated condition (SLA), expressed as (uptime)/(uptime+downtime).

2.6. OAM variations

2.6.1. Active OAM

See [RFC7799]. In the context of RAW, Active OAM is used to observe a particular recovery graph, DetNet Path, or Segment of a recovery graph regardless of whether it is used for traffic at that time.

2.6.2. In-Band OAM

An active OAM packet is considered in-band for the monitored recovery graph when it traverses the same set of links and interfaces and if the OAM packet receives the same QoS and service protection treatment as the packets of the data flows that are injected in the recovery graph.

2.6.3. Out-of-Band OAM

Out-of-band OAM is an active OAM whose path is not topologically congruent to the recovery graph, or its test packets receive a QoS and/or service protection treatment that is different from that of the packets of the data flows that are injected in the recovery graph, or both.

2.6.4. Limited OAM

An active OAM packet is a Limited OAM packet when it observes the RAW operation over a node, a segment, or a DetNet Path of the recovery graph, though not from Ingress to Egress. It is injected in the datapath and extracted from the datapath around the particular function or subnetwork (e.g., around a relay providing a Service sub-layer replication point) that is being tested.

2.6.5. Upstream OAM

An upstream OAM packet is an Out-of-Band OAM packet that traverses the recovery graph from egress to ingress on the reverse direction, to capture and report OAM measurements upstream. The collection may capture all information along the whole recovery graph, or it may only learn select data across all, or only a particular DetNet Path, or Segment of a recovery graph.

2.6.6. Residence Time

A residence time (RT) is defined as the time period between the reception of a packet starts and the transmission of the packet begins. In the context of RAW, RT is useful for a transit node, not ingress or egress.

2.6.7. Lower Layer information

The RAW Operational Plane elements (PLR and OAM Supervisor) may gather aggregated information from lower layers about e.g., link quality. This information may be obtained from inside the device using specialized API (e.g., L2 triggers) or via control protocols such as BFD [RFC5880] or DLEP [DLEP]. It may then be massaged and exported through oOAM messaging, and passed to the Controller Plane using the aCPF.

2.6.8. Additional References

[DetNet-OAM] provides additional terminology related to OAM in the context of DetNet and by extension of RAW, whereas [RFC7799] defines the Active, Passive, and Hybrid OAM methods.

3. Reliable and Available Wireless

3.1. Reliability and Availability

3.1.1. High Availability Engineering Principles

The reliability criteria of a critical system pervades through its elements, and if the system comprises a data network then the data network is also subject to the inherited reliability and availability criteria. It is only natural to consider the art of high availability engineering and apply it to wireless communications in the context of RAW.

There are three principles [pillars] of high availability engineering:

1. elimination of each single point of failure
2. reliable crossover
3. prompt detection of failures as they occur.

These principles are common to all high availability systems, not just ones with Internet technology at the center. Examples of both non-Internet and Internet are included.

3.1.1.1. Elimination of Single Points of Failure

Physical and logical components in a system happen to fail, either as the effect of wear and tear, when used beyond acceptable limits, or due to a software bug. It is necessary to decouple component failure from system failure to avoid the latter. This allows failed components to be restored while the rest of the system continues to function.

IP Routers leverage routing protocols to reroute to alternate routes in case of a failure. There is a rather open-ended issue over alternate routes -- for example, when links are cabled through the same conduit, they form a shared risk link group (SRLG), and will share the same fate if the bundle is cut. The same effect can happen with virtual links that end up in a same physical transport through the games of encapsulation. In a same fashion, an interferer or an obstacle may affect multiple wireless transmissions at the same time, even between different sets of peers.

Intermediate network Nodes such as routers, switches and APs, wire bundles and the air medium itself can become single points of failure. For High Availability, it is thus required to use physically link- and Node-disjoint paths; in the wireless space, it is also required to use the highest possible degree of diversity (time, space, code, frequency, channel width) in the transmissions over the air to combat the additional causes of transmission loss.

From an economics standpoint, executing this principle properly generally increases capitalization expense because of the redundant equipment. In a constrained network where the waste of energy and bandwidth should be minimized, an excessive use of redundant links must be avoided; for RAW this means that the extra bandwidth must be used wisely and with parsimony.

3.1.1.2. Reliable Crossover

Having a backup equipment has a limited value unless it can be reliably switched into use within the down-time parameters. IP Routers execute reliable crossover continuously because the routers will use any alternate routes that are available [RFC0791]. This is due to the stateless nature of IP datagrams and the dissociation of the datagrams from the forwarding routes they take. The "IP Fast Reroute Framework" [FRR] analyzes mechanisms for fast failure detection and path repair for IP Fast-Reroute, and discusses the case of multiple failures and SRLG. Examples of FRR techniques include Remote Loop-Free Alternate [RLFA-FRR] and backup label-switched path (LSP) tunnels for the local repair of LSP tunnels using RSVP-TE [RFC4090].

Deterministic flows, on the contrary, are attached to specific paths where dedicated resources are reserved for each flow. Therefore each DetNet path must inherently provide sufficient redundancy to provide the guaranteed SLA at all times. The DetNet PREOF typically leverages 1+1 redundancy whereby a packet is sent twice, over non-congruent paths. This avoids the gap during the fast reroute operation, but doubles the traffic in the network.

In the case of RAW, the expectation is that multiple transient faults may happen in overlapping time windows, in which case the 1+1 redundancy with delayed reestablishment of the second path will not provide the required guarantees. The Data Plane must be configured with a sufficient degree of redundancy to select an alternate redundant path immediately upon a fault, without the need for a slow intervention from the Controller Plane.

3.1.1.3. Prompt Notification of Failures

The execution of the two above principles is likely to render a system where the user will rarely see a failure. But someone needs to in order to direct maintenance.

There are many reasons for system monitoring (FCAPS for fault, configuration, accounting, performance, security is a handy mental checklist) but fault monitoring is sufficient reason.

"An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" [STD 62] describes how to use SNMP to observe and correct long-term faults.

"Overview and Principles of Internet Traffic Engineering" [TE] discusses the importance of measurement for network protection, and provides an abstract method for network survivability with the analysis of a traffic matrix as observed by SNMP, probing techniques, FTP, IGP link state advertisements, and more.

Those measurements are needed in the context of RAW to inform the controller and make the long term reactive decision to rebuild a recovery graph based on statistical and aggregated information. RAW itself operates in the DetNet Network Plane at a faster time scale with live information on speed, state, etc... This live information can be obtained directly from the lower layer, e.g., using L2 triggers, read from a protocol such as the Dynamic Link Exchange Protocol (DLEP) [DLEP], or transported over multiple hops using OAM and reverse OAM, as illustrated in Figure 11.

3.1.2. Applying Reliability Concepts to Networking

The terms Reliability and Availability are defined for use in RAW in Section 2 and the reader is invited to read [NASA] for more details

on the general definition of Reliability. Practically speaking a number of nines is often used to indicate the reliability of a data link, e.g., 5 nines indicate a Packet Delivery Ratio (PDR) of 99.999%.

This number is typical in a wired environment where the loss is due to a random event such as a solar particle that affects the transmission of a particular packet, but does not affect the previous or next packet, nor packets transmitted on other links. Note that the QoS requirements in RAW may include a bounded latency, and a packet that arrives too late is a fault and not considered as delivered.

For a periodic networking pattern such as an automation control loop, this number is proportional to the Mean Time Between Failures (MTBF). When a single fault can have dramatic consequences, the MTBF expresses the chances that the unwanted fault event occurs. In data networks, this is rarely the case. Packet loss cannot be fully avoided and the systems are built to resist to some loss, e.g., using redundancy with Retries (HARQ) or Packet Replication and Elimination (PRE), or, in a typical control loop, by linear interpolation from the previous measurements.

But the linear interpolation method cannot resist multiple consecutive losses, and a high MTBF is desired as a guarantee that this will not happen, IOW that the number of losses-in-a-row can be bounded. In that case, what is really desired is a Maximum Consecutive Failures (MCF). If the number of losses in a row passes the MCF, the control loop has to abort and the system, e.g., the production line, may need to enter an emergency stop condition.

Engineers that build automated processes may use the network reliability expressed in nines or as an MTBF as a proxy to indicate an MCF, e.g., as described in section 7.4 of the "Deterministic Networking Use Cases" [RFC8578].

3.1.3. Wireless Effects Affecting Reliability

In contrast with wired networks, errors in transmission are the predominant source of packet loss in wireless networks.

The root cause for the loss may be of multiple origins, calling for the use of different forms of diversity:

Multipath Fading: A destructive interference by a reflection of the original signal.

A radio signal may be received directly (line-of-sight) and/or as a reflection on a physical structure (echo). The reflections take a longer path and are delayed by the extra distance divided by

the speed of light in the medium. Depending on the frequency, the echo lands with a different phase which may add up to (constructive interference) or cancel the direct signal (destructive interference).

The affected frequencies depend on the relative position of the sender, the receiver, and all the reflecting objects in the environment. A given hop will suffer from multipath fading for multiple packets in a row till a physical movement changes the reflection patterns.

Co-channel Interference: Energy in the spectrum used for the transmission confuses the receiver.

The wireless medium itself is a Shared Risk Link Group (SRLG) for nearby users of the same spectrum, as an interference may affect multiple co-channel transmissions between different peers within the interference domain of the interferer, possibly even when they use different technologies.

Obstacle in Fresnel Zone: The optimal transmission happens when the Fresnel Zone between the sender and the receiver is free of obstacles.

As long as a physical object (e.g., a metallic trolley between peers) that affects the transmission is not removed, the quality of the link is affected.

In an environment that is rich of metallic structures and mobile objects, a single radio link will provide a fuzzy service, meaning that it cannot be trusted to transport the traffic reliably over a long period of time.

Transmission losses are typically not independent, and their nature and duration are unpredictable; as long as a physical object (e.g., a metallic trolley between peers) that affects the transmission is not removed, or as long as the interferer (e.g., a radar) keeps transmitting, a continuous stream of packets will be affected.

The key technique to combat those unpredictable losses is diversity. Different forms of diversity are necessary to combat different causes of loss and the use of diversity must be maximized to optimize the PDR.

A single packet may be sent at different times (time diversity) over diverse paths (spatial diversity) that rely on diverse radio channels (frequency diversity) and diverse PHY technologies, e.g., narrowband vs. spread spectrum, or diverse codes. Using time diversity will defeat short-term interferences; spatial diversity combats very local causes such as multipath fading; narrowband and

spread spectrum are relatively innocuous to one another and can be used for diversity in the presence of the other.

3.2. The RAW problem

While the generic "Deterministic Networking Problem Statement" [RFC8557] applies to both the wired and the wireless media, the methods to achieve RAW must extend those used to support time-sensitive networking over wires, as a RAW solution has to address less consistent transmissions, energy conservation and shared spectrum efficiency.

Operating at the Layer-3, RAW does not change the wireless technology at the lower layers. OTOH, it can further increase diversity in the spatial, time, code, and frequency domains by enabling multiple link-layer wired and wireless technologies in parallel or sequentially, for a higher resilience and a wider applicability. RAW can also provide homogeneous services to critical applications beyond the boundaries of a single subnetwork, e.g., using diverse radio access technologies to optimize the end-to-end application experience.

RAW extends the DetNet services by providing elements that are specialized for transporting IP flows over deterministic radio technologies such as listed in [RAW-TECHNOS]. Conceptually, RAW is agnostic to the radio layer underneath though the capability to schedule transmissions is assumed. How the PHY is programmed to do so, and whether the radio is single-hop or meshed, are unknown at the IP layer and not part of the RAW abstraction. Nevertheless, cross-layer optimizations may take place to ensure proper link awareness (think, link quality) and packet handling (think, scheduling).

The "Deterministic Networking Architecture" [RFC8655] is composed of three planes: the Application (User) Plane, the Controller Plane, and the Network Plane. The DetNet Network Plane is composed a Dataplane (packet forwarding) and an Operational Plane where OAM operations take place. In the Network Plane, the DetNet service sub-layer focuses on flow protection (e.g., using redundancy) and can be fully operated at Layer-3, while the DetNet forwarding sub-layer estapblishes the patsh, associates the flows to the paths, qnd ensures the availability of the necessary resources, leverages Layer-2 functionalities for timely delivery to the next DetNet system.

The RAW Architecture extends the DetNet Network Plane, to accommodate one or multiple hops of homogeneous or heterogeneous wired and wireless technologies. RAW adds reactivity to the DetNet service sub-layer to compensate the dynamics for the radio links in

terms of lossiness and bandwidth. This may apply for instance to mesh networks as illustrated in Figure 4, or diverse radio access networks as illustrated in Figure 10.

As opposed to wired links, the availability and performance of an individual wireless link cannot be trusted over the long term; it varies with transient service discontinuity, and any lane that includes wireless hops is bound to face short periods of high loss. On the other hand, being broadcast in nature, the wireless medium provides capabilities that are atypical on modern wired links and that the RAW Architecture can leverage opportunistically to improve the end-to-end reliability over a collection of paths.

Those capabilities include:

Promiscuous Overhearing: Because the medium is broadcast as opposed to physically point to point like a wire, more than one node in the forward direction of the packet may hear or overhear a transmission, and the reception by one may compensate the loss by another. The concept of path can be revisited in favor multipoint to multipoint progress in the forward direction and statistical chances of successful reception of any of the transmissions by any of the receivers.

L2-aware routing: As the quality and speed of a link variates over time, the concept of metric must also be revisited. Shortest path loses its absolute value, and hop count turns into a bad idea as the link budget drops with the distance. Routing over radio requires both 1) a new and more dynamic sense of the link, with new protocols such as DLEP and L2-trigger to maintain L3 up to date with the link quality and availability, and 2) a new approach to multipath routing, where non-equal cost multipath becomes the norm as shortest path loses its meaning with the instability of the metrics.

ARQ, FEC and codes: Though feasible on any technology, proactive (forward) and reactive (ARQ) error correction are typical to the wireless media. Bounded latency can still be obtained on a wireless link while operating those technologies, provided that the extra transmission happens within the budget allocated to that hop, or that the introduced delay is compensated along the path. In the case of coded fragments and retries, it makes sense to variate all the possible physical properties of the transmission to reduce the chances that the same effect causes the loss of both original and redundant transimissions.

Relay Coordination and constructive interference: Though it can be difficult to achieve at high speed, a fine time synchronization and a precise sense of phase allows the energy from multiple

coordinated senders to add up at the receiver and actually improve the signal quality, compensating for either distance or physical objects in the Fresnel zone that would reduce the link budget.

RAW and DetNet route application flows that require a special treatment along the paths that provide that treatment. This may be seen as a form of Path Aware Networking and may be subject to impediments documented in [RFC9049].

The establishment of a path is not in-scope for RAW. It may be, e.g., the product of a centralized Controller Plane Function (CPF) like a Path computation Element (PCE) [RFC4655], or may be computed in a distributed fashion ala Resource ReSerVation Protocol (RSVP) [RFC2205]. On the other hand, RAW leverages DetNet Network Plane enhancements to optimize the use of the paths and match the quality of the transmissions over time.

As opposed to wired networks, the action of installing a path over a set of wireless links may be very slow relative to the speed at which the radio conditions vary, and it makes sense in the wireless case to provide redundant forwarding solutions along a (see Section 2.3) and to leave it to the Network Plane to select which of those forwarding solutions are to be used for a given packet based on the current conditions.

RAW distinguishes the longer time scale at which routes are computed from the the shorter time scale where forwarding decisions are made for a limited time RAW Network Plane operations happen at a time scale that sits between the routing and the forwarding time scales, on one DetNet flow, to select a DetNet path within the resources delineated by a recovery graph (see Section 2.3.2). The recovery graph is preestablished and installed by means outside of the scope of RAW; it may be strict or loose depending on whether each or just a subset of the hops are observed and controlled by RAW.

The RAW Architecture is based on an abstract OODA Loop (Observe, Orient, Decide, Act). The generic concept involves:

1. Operational Plane measurement protocols for Operations, Administration and Maintenance (OAM) to Observe some or all hops along a recovery graph as well as the end-to-end packet delivery

2. The DetNet Controller Plane Function (CPF) is split with an optional asynchronous CPF (aCPF) that reports data and information such as link statistics to be used asynchronously by the routing CPF (rCPF) to compute, install, and maintain the recovery graphs, e.g., by generating knowledge and wisdom such

as a trained model for link quality prediction, which in turn can be used by the aCPF to Orient the Path selection by the PLR within the RAW OODA loop.

3. An Operational Plane PLR that hosts the Decision function of which DetNet Paths to use for the future packets that will be routed within the recovery graph

4. Service protection actions that operate at the DetNet Service sub-layer to increase the reliability of the end-to-end transmissions. The RAW architecture also covers in-situ signaling when the decision is Acted by a node that down the recovery graph from the PLR.

The overall OODA Loop optimizes the use of redundancy to achieve the required reliability and availability Service Level Agreement (SLA) while minimizing the use of constrained resources such as spectrum and battery.

4. The RAW Conceptual Model

RAW inherits the conceptual model described in section 4 of the DetNet Architecture [RFC8655] as illustrated in Figure 3, which also shows example reliability Functions in the different layers. RAW extends DetNet with Point of Local Repair (PLR, see Section 5.5) to provide additional agility against transmission loss. The PLR can act, e.g., based on indications from the wireless layer or based on OAM.

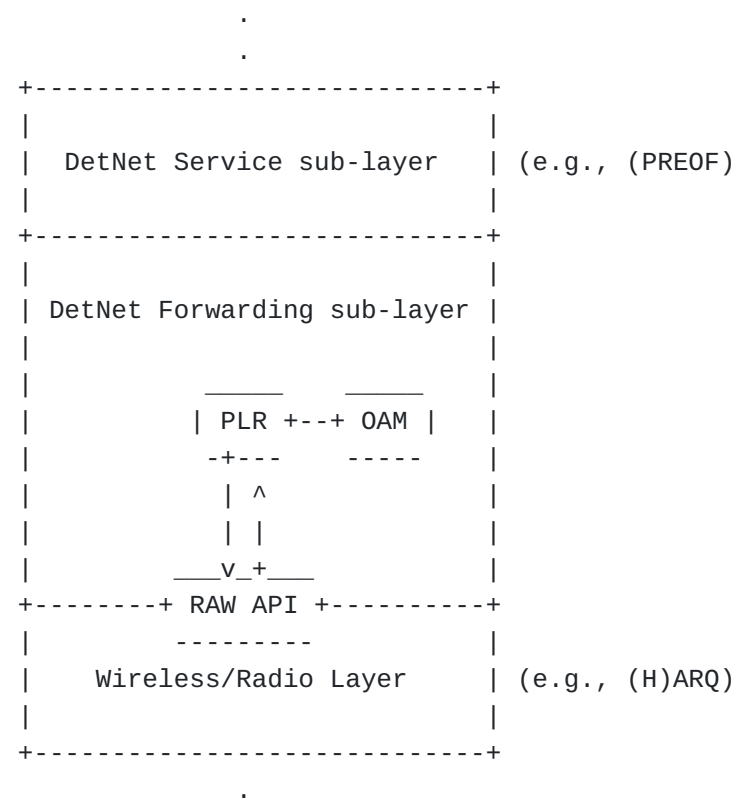

Figure 3: Wireless layer and DetNet sub-layers

The RAW API enables interactions between the reliability functions provided by the wireless technology and the reliability functions provided by DetNet. Thus, the RAW aPI enables cross-layer optimizations to improve reliability.

4.1. The RAW Planes

A RAW Network Plane may be strict (as illustrated in Figure 6 or loose (as illustrated in Figure 7, depending on whether RAW observes and takes actions on all hops or not. For instance, the packets between two wireless entities may be relayed over a wired infrastructure, in which case RAW observes and controls the transmission over the wireless first and last hops, as well as end-to-end metrics such as latency, jitter, and delivery ratio. This operation is loose since the structure and properties of the wired infrastructure are ignored, and may be either controlled by other means such as DetNet/TSN, or neglected in the face of the wireless hops.

The RAW Nodes are DetNet relays that operate in the RAW Network Plane and are capable of additional diversity mechanisms and measurement functions related to the radio interface. RAW leverages a CPF that operates inside the RAW Nodes (typically the Ingress Edge

Nodes) to dynamically adapt the path of the packets and optimizes the resource usage.

An RAW-enabled rCPF interacts with RAW Nodes over a Southbound API. It consumes data and information from the network and generates knowledge and wisdom to help steer the traffic optimally inside a recovery graph.

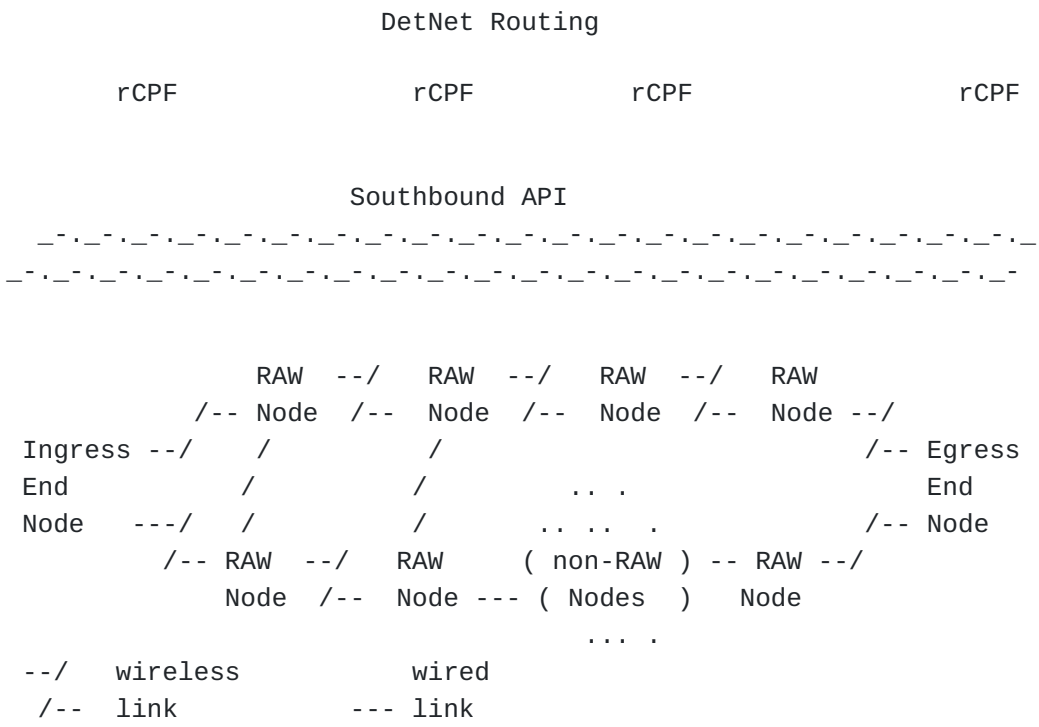

Figure 4: RAW Nodes

When a new flow is defined, the rCPF uses it current knowledge of the network to build a new recovery graph between an Ingress End System and an Egress End System for that flow; it indicates to the RAW Nodes where the PREOF and/or radio diversity and reliability operations may be actioned in the Network Plane.

- *The recovery graph may be strict, meaning that the DetNet forwarding sub-layer operations are enforced end-to-end

- *The recovery graph may be expressed loosely to enable traversing a non-RAW subnetwork as in Figure 7. In that case, RAW can not leverage end-to-end DetNet and cannot provide latency guarantees. The non-RAW subnetwork is neglected in the RAW computation, that is, considered jitterless, and infinitely reliable and/or available in comparison with the links between RAW nodes, so loss and jitter that is measured end-to-end is attributed to the RAW hops (typically an access link).

A local asynchronous CPF in the RAW node reports the Link-Layer metrics to the rCPF in a time-aggregated, e.g., statistical fashion. Example Link-Layer metrics include typical Link bandwidth (the medium speed depends dynamically on the PHY mode), number of flows (bandwidth that can be reserved for a flow depends on the number and size of flows sharing the spectrum) and average and mean squared deviation of availability and reliability figures such as Packet Delivery Ratio (PDR) over long periods of time.

Based on those metrics, the DetNet rCPF installs the recovery graph with enough redundant forwarding solutions to ensure that the Network Plane can reliably deliver the packets within a System Level Agreement (SLA) associated to the flows that it transports. The SLA defines end-to-end reliability and availability requirements, where reliability may be expressed as a successful delivery in order and within a bounded delay of at least one copy of a packet.

Depending on the use case and the SLA, the recovery graph may comprise non-RAW segments, either interleaved inside the recovery graph, or all the way to the Egress End Node (e.g., a server in the Internet). RAW observes the Lower-Layer Links between RAW nodes (typically, radio links) and the end-to-end Network Layer operation to decide at all times which of the diversity schemes is actioned by which RAW Nodes.

Once a recovery graph is established, per-segment and end-to-end reliability and availability statistics are periodically reported to the rCPF to assure that the SLA can be met or have it recompute the recovery graph if not.

4.2. RAW vs. Upper and Lower Layers

RAW improves the reliability of transmissions and the availability of the communication resources, but does not provide scheduling and shaping, so RAW itself does not provide guarantees such as latency for the application payload. Rather, it should be seen as a dynamic optimization of the use of redundancy to maintain it within certain boundaries. For instance, ARQ is operated by the lower layers and RAW will only abstract the concept and hint the lower layers on the desired outcome, as opposed to performing the retries at Layer-3.

Guarantees such as bounded latency depend on the upper layers (Transport or Application) to provide the payload in volumes and at times that match the contract with the DetNet sub-layers and the layers below. Excess of incoming traffic at the DetNet Ingress will cause either dropping, queueing, or reclassification of the packets, and entail loss, latency, or jitter, and moot the guarantees that are provided inside the DetNet Network.

When the traffic from upper layers matches the expectation of the lower layers, RAW still depends on the lower layers to provide the timing and physical resources guarantees that are needed to match the traffic SLA. When the availability of the physical resource varies, RAW will act on the distribution of the traffic to leverage alternates within a finite set of potential resources.

4.3. RAW and DetNet

RAW leverages the DetNet Forwarding sub-layer and requires the support of in-situ OAM in DetNet Transit Nodes (see fig 3 of [RFC8655] for the dynamic acquisition of link capacity and state to maintain a strict RAW service, end-to-end, over a DetNet Network. RAW extends DetNet to improve the protection against link errors such as transient flapping that are far more common in wireless links. Nevertheless, the RAW methods are for the most part applicable to wired links as well, e.g., when energy savings are desirable and the available path diversity exceeds 1+1 linear redundancy.

RAW adds sub-layer functions that operate in the DetNet Operational Plane. The RAW Operational sub-layer typically runs only in the DetNet Ingress Edge Node or End System, though it may also run in DetNet Relay Nodes when the RAW Control sub-layer is distributed along the recovery graph. The RAW Operational sub-layer functionality includes the PLR that decides the DetNet Path for the future packets of a flows along the DetNet Path through specific signaling, and the OAM Supervisor that triggers, and learns from, OAM observations, and feeds the PLR for its next decision.

RAW extends the DetNet Stack (see fig 4 of [RFC8655]) with additional functionality at the DetNet Service sub-layer for the actuation of the PLR decision. Layer-3 in general and DetNet in particular operates on abstractions of the lower layers and through APIs to control those abstractions. For instance, DetNet already leverages lower layers for time-sensitive operations such as time synchronization and traffic shapers. Because the performances of the radio layers are subject to rapid changes, so RAW needs more dynamic gauges and knobs. To that effect, the RAW API enables interactions between the reliability functions provided by the wireless technology and the reliability functions provided by DetNet. That is, the RAW API provides a radio abstraction to the DetNet layer. The RAW API can be used to push reliability and timing hints like suggest X retries (min, max) within a time window, or send unicast (one next hop) or multicast (for overhearing). The other way around RAW needs hints about the radio conditions like L2 triggers (RSSI, LQI, ETX…) over all the wireless hops. This information is useful to both the aCPF and the PLR.

The RAW Service sub-layer also adds the OAM Propagator that (re)generates the OAM information as it is formed and propagated In-Band or Out-of-Band. The RAW Service sub-layer may be present in DetNet Edge and Relay Nodes, though the PREOF Actuator has no operation in the Egress Edge Node.

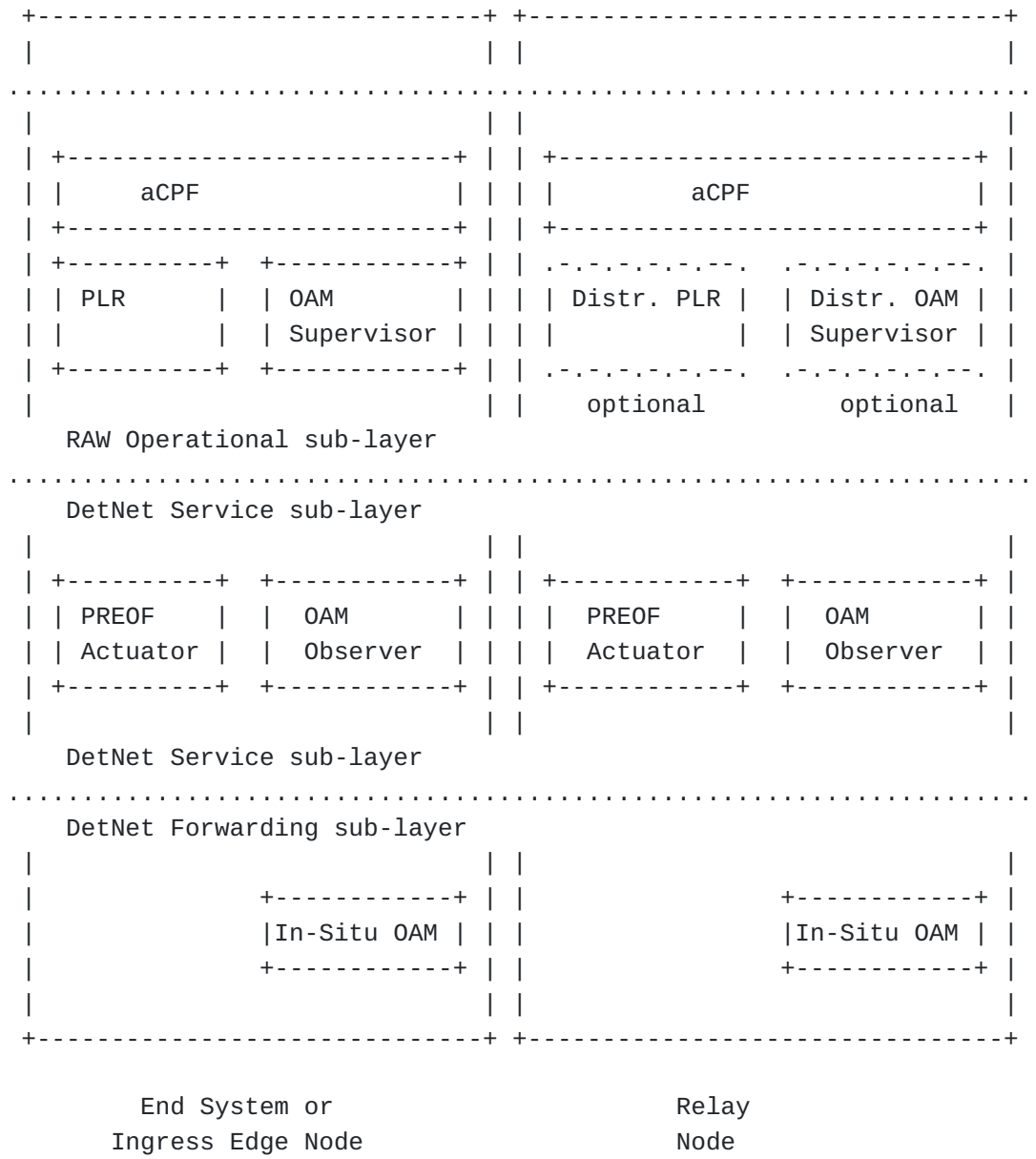

Figure 5: RAW functional posture within DetNet sub-layers

There are 2 main proposed models to deploy RAW and DetNet. In the first model (strict) illustrated in Figure 6, RAW operates over a continuous DetNet Service end-to-end between the Ingress and the Egress Edge Nodes or End Systems.

A minimal Forwarding sub-layer service is provided at all DetNet Nodes to ensure that the OAM information flows. Relay Nodes may or may not support RAW services, and the Edge nodes do support RAW. DetNet guarantees such as latency are provided end-to-end, and RAW supports the DetNet Service to optimize the use of resources.

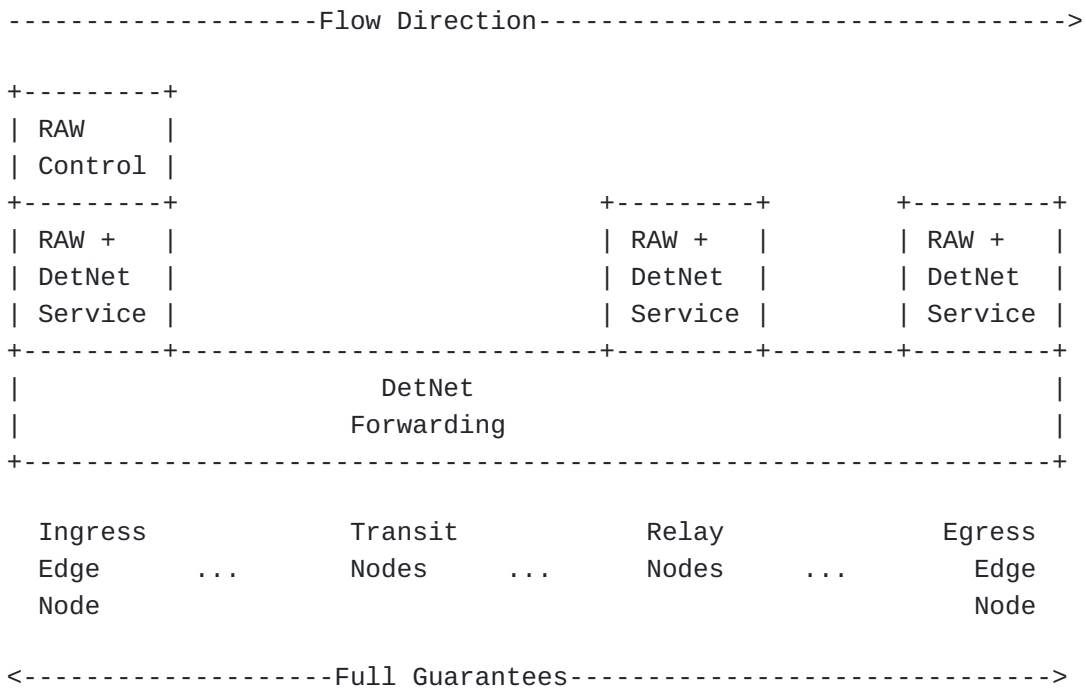

Figure 6: (Strict) RAW over DetNet

In the second model (loose), illustrated in Figure 7, RAW operates over a partial DetNet Service where typically only the Ingress and the Egress End Systems support RAW. The DetNet Domain may extend beyond the Ingress node, or there may be a DetNet domain starting at an Ingress Edge Node at the first hop after the End System.

In the loose model, RAW cannot observe the hops in network, and the path beyond the first hop is opaque; RAW can still observe the end-to-end behavior and use Layer-3 measurements to decide whether to replicate a packet and select the first hop interface(s).

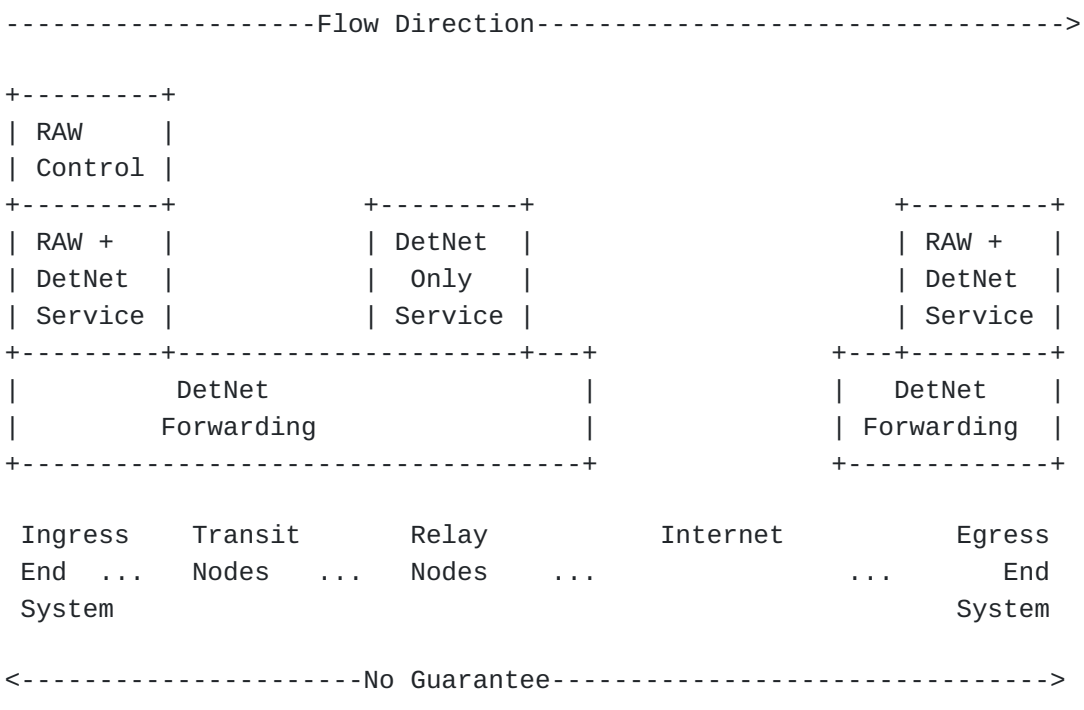

Figure 7: Loose RAW

5. The RAW Control Loop

5.1. Routing Time Scale vs. Forwarding Time Scale

With DetNet, the Controller Plane Function handles the routing computation and maintenance. With RAW, the routing part of the CPF (rCPF) is segregated from the RAW Control Loop, so it may reside outside of the RAW network. To achieve RAW capabilities, the rCPF is extended to generate the information required by the local aCPF, which acts as the orientation component in the loop. The rCPF may, e.g., propose DetNet Paths to be used as a reflex action in response to network events, or by provide aggregated history that the aCPF can use to make an oriented decision.

In a wireless mesh, the path to the DetNet CPF can be expensive and slow, possibly going across the whole mesh and back. Reaching to the CPF can also be slow in regards to the speed of events that affect the forwarding operation at the radio layer. Note that a distributed routing protocol may also take time and consume excessive wireless resources to reconverge to a new optimized state.

As a result, the DetNet CPF is not expected to be aware of and to react to very transient changes. The abstraction of a link at the routing level is expected to use statistical metrics that aggregate the behavior of a link over long periods of time, and represent its

properties as shades of gray as opposed to numerical values such as a link quality indicator, or a boolean value for either up or down.

The interaction with the (remote) RAW rCPF is handled by a (local) aCPF that builds reports to the rCPF and digests the control information back, to be used inside a forwarding control loop for traffic steering.

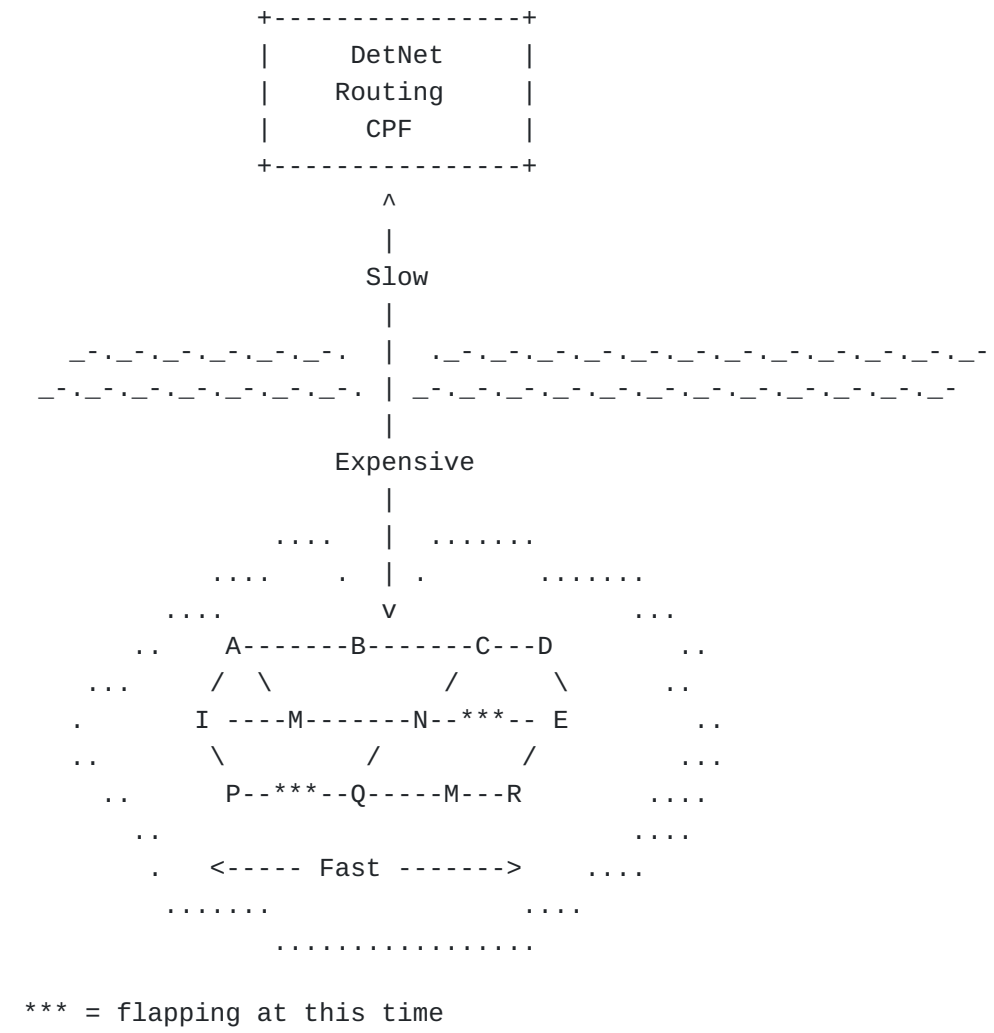

Figure 8: Time Scales

In the case of wireless, the changes that affect the forwarding decision can happen frequently and often for short durations, e.g., a mobile object moves between a transmitter and a receiver, and will cancel the line of sight transmission for a few seconds, or a radar measures the depth of a pool and interferes on a particular channel for a split second.

There is thus a desire to separate the long term computation of the route and the short term forwarding decision. In that model, the routing operation computes a recovery graph that enables multiple Non-Equal Cost Multi-Path (N-ECMP) forwarding solutions along so-called protection paths, and leaves it to the Network Plane to make the per-packet decision of which of these possibilities should be used.

In the context of Traffic Engineering (TE), an alternate path can be used upon the detection of a failure in the main path, e.g., using OAM in MPLS-TP or BFD over a collection of SD-WAN tunnels. RAW formalizes a forwarding time scale that is an order(s) of magnitude shorter than the controller plane routing time scale, and separates the protocols and metrics that are used at both scales. Routing can operate on long term statistics such as delivery ratio over minutes to hours, but as a first approximation can ignore flapping. On the other hand, the RAW forwarding decision is made at the scale of the packet rate, and uses information that must be pertinent at the present time for the current transmission(s).

5.2. A OODA Loop

OODA (Observe, Orient, Decide, Act) is a generic formalism to represent the operational steps in a Control Loop. The RAW Architecture applies that generic model to continuously optimize the spectrum and energy used to forward packets within a recovery graph, instantiating the OODA steps as follows:

Observe: Network Plane measurements, including protocols for Operations, Administration and Maintenance (OAM), to Observe the local state of the links and some or all hops along a recovery graph as well as the end-to-end packet delivery, more in Section 5.3;

Orient: An asynchronous CPF that reports data and information such as the link statistics, and leverages offline-computed wisdom and knowledge to Orient the PLR for its forwarding decision, more in Section 5.4;

Decide: A local PLR that decides which DetNet Path to use for the future packet(s) that are routed along the recovery graph, more in Section 5.5;

Act: PREOF Dataplane actions are controlled from the DetNet Service sub-layer to increase the reliability of the end-to-end transmission. The RAW architecture also covers in-situ signaling when the decision is Acted by a node that down the recovery graph from the PLR, more in Section 5.6.

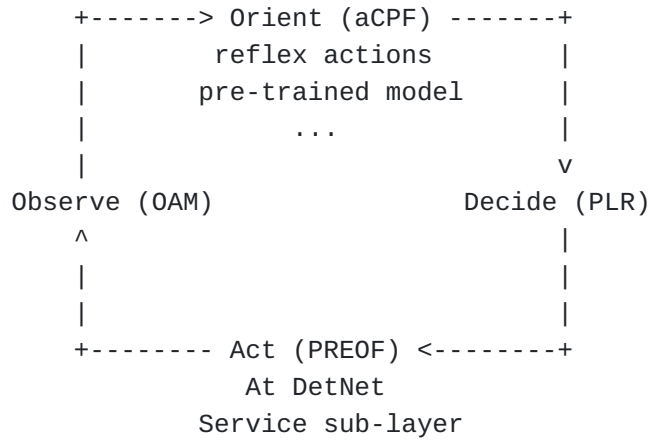

Figure 9: The RAW OODA Loop

The overall OODA Loop optimizes the use of redundancy to achieve the required reliability and availability Service Level Agreement (SLA) while minimizing the use of constrained resources such as spectrum and battery.

5.3. Observe: The RAW OAM

RAW In-situ OAM operation in the Network Plane may observe either a full recovery graph or the DetNet Path that is being used at this time. As packets may be load balanced, replicated, eliminated, and / or fragmented for Network Coding (NC) forward error correction (FEC), the RAW In-situ operation needs to be able to signal which operation occured to an individual packet.

Active RAW OAM may be needed to observe the unused segments and evaluate the desirability of a rerouting decision.

Finally, the RAW Service sub-layer Assurance may observe the individual PREOF operation of a relay node to ensure that it is conforming; this might require injecting an OAM packet at an upstream point inside the recovery graph and extracting that packet at another point downstream before it reaches the egress.

This observation feeds the RAW PLR that makes the decision on which path is used at which RAW Node, for one a small continuous series of packets.

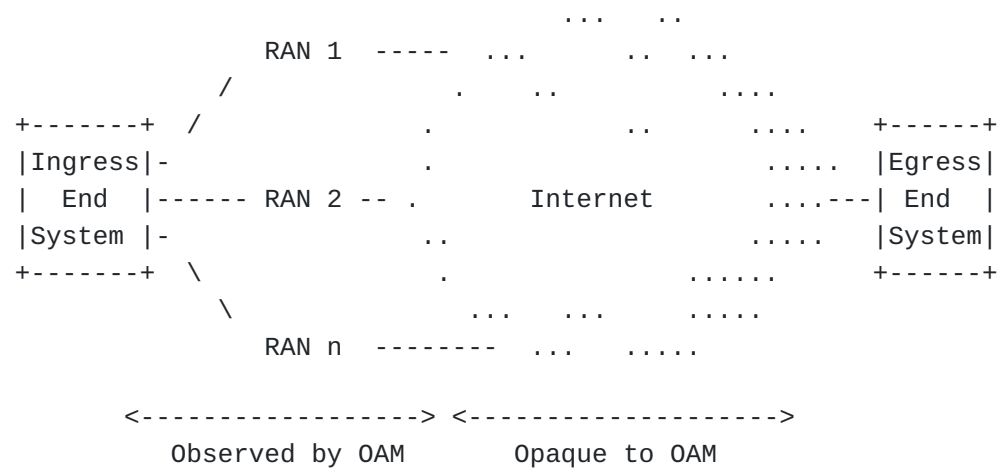

Figure 10: Observed Links in Radio Access Protection

In the case of a End-to-End Protection in a Wireless Mesh, the recovery graph is strict and congruent with the path so all links are observed.

Conversely, in the case of Radio Access Protection illustrated in Figure 10, the recovery graph is Loose and only the first hop is observed; the rest of the path is abstracted and considered infinitely reliable. The loss if a packet is attributed to the first hop Radio Access Network (RAN), even if a particular loss effectively happens farther down the path. In that case, RAW enables technology diversity (e.g. Wi-Fi and 5G) which in turn improves the diversity in spectrum usage.

The Links that are not observed by OAM are opaque to it, meaning that the OAM information is carried across and possibly echoed as data, but there is no information capture in intermediate nodes. In the example above, the Internet is opaque and not controlled by RAW; still the RAW OAM measures the end-to-end latency and delivery ratio for packets sent via each if RAN 1, RAN 2 and RAN 3, and determines whether a packet should be sent over either or a collection of those access links.

5.4. Orient: The RAW-extended DetNet Operational Plane

RAW separates the long time scale at which a recovery graph is elaborated and installed, from the short time scale at which the forwarding decision is taken for one or a few packets (see in Section 5.1) that will experience the same path until the network conditions evolve and another path is selected within the same recovery graph.

The recovery graph computation is out of scope, but RAW expects that the CPF that installs the recovery graph also provides related knowledge in the form of meta data about the links, segments and possible DetNet Paths. That meta data can be a pre-digested statistical model, and may include prediction of future flaps and packet loss, as well as recommended actions when that happens.

The meta data may include:

- A set of Pre-Determined DetNet Paths that are prepared to match expected link degradation profiles, so the DDCPEs can take reflex rerouting actions when facing a degradation that matches one such profile.

- Link Quality Statistics history and pre-trained models, e.g., to predict the short-term variation of quality of the links in a recovery graph

The recovery graph is installed with measurable objectives that are computed by the rCPF to achieve the RAW SLA. The objectives can be expressed as any of maximum number of packet lost in a row, bounded latency, maximal jitter, maximum number of interleaved out of order packets, average number of copies received at the elimination point, and maximal delay between the first and the last received copy of the same packet.

5.5. Decide: The Point of Local Repair

The RAW OODA Loop operates at the path selection time scale to provide agility vs. the brute force approach of flooding the whole recovery graph. The OODA Loop controls, within the redundant solutions that are proposed by the acynchronous CPF, which will be used for each packet to provide a Reliable and Available service while minimizing the waste of constrained resources.

To that effect, RAW defines the Point of Local Repair (PLR) as a synchronous CPF that performs rapid local adjustments of the forwarding tables within the diversity that the asynchronous CPF has in store for the recovery graph. The PLR enables to exploit the richer forwarding capabilities at a faster time scale over the smaller domain that is the recovery graph, in either a loose or a strict fashion.

The PLR operates on metrics that evolve faster, but that need to be advertised at a fast rate but only locally, within the recovery graph, and reacts on the metrics updates by changing the DetNet path in use for the affected flows.

The rapid changes in the forwarding decisions are made and contained within the scope of a recovery graph and the actions of the PLR are

not signaled outside the recovery graph. This is as opposed to the rCPF that must observe the whole network and optimize all the recovery graphs globally, which can only be done at a slow pace and using long-term statistical metrics, as presented in Table 1.

	rCPF	PLR (In Scope)
Operation	Typically Centralized	Source-Routed or Distributed
Communication	Slow, expensive	Fast, local
Time Scale	hours and above	seconds and below
Network Size	Large, many recovery graphs to optimize globally	Small, within one recovery graph
Considered Metrics	Averaged, Statistical, Shade of grey	Instant values / boolean condition

Table 1: CPF vs. PLR

The PLR sits in the DetNet Service sub-Layer of Edge and Relay Nodes. On the one hand, it operates on the packet flow, learning the recovery graph and path selection information from the packet, possibly making local decision and retagging the packet to indicate so. On the other hand, the PLR interacts with the lower layers (through triggers and DLEP) and with its peers (through iOAM and oOAM) to obtain up-to-date information about its links and the quality of the overall recovery graph, respectively, as illustrated in Figure 11.

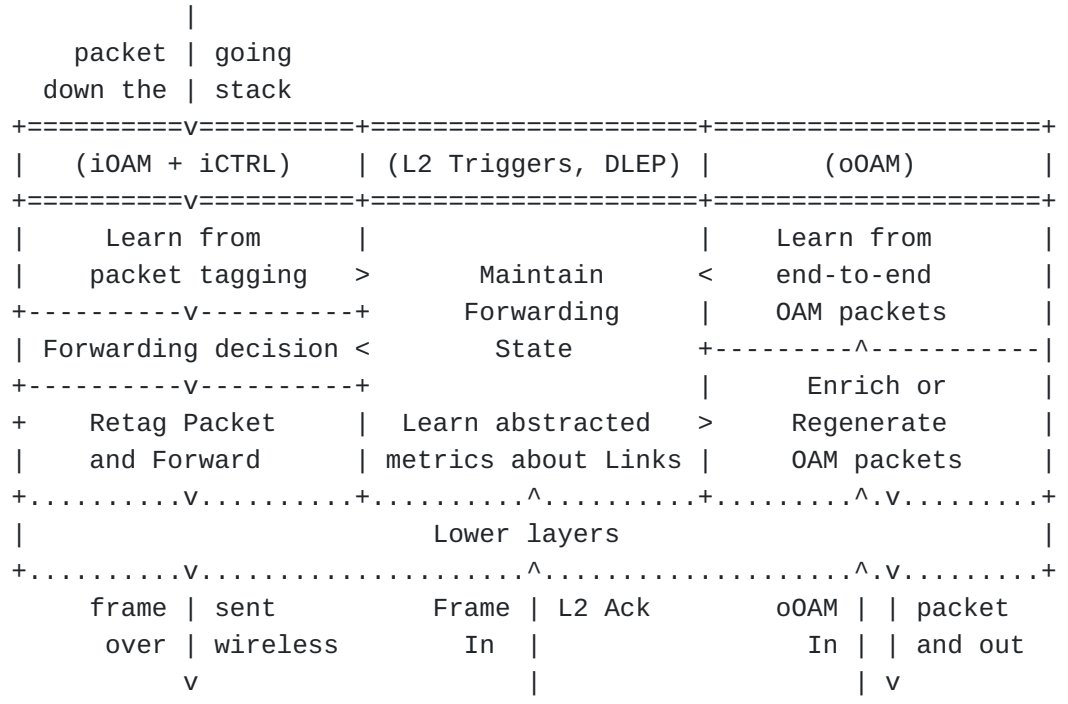

Figure 11: PLR Interfaces

5.6. Act: DetNet Path Selection and reliability functions

The main action by the PLR is the swapping of the DetNet Path within the recovery graph for the future packets. The candidate DetNet Paths represent different energy and spectrum profiles, and provide protection against different failures.

The RAW API enriches the DetNet protection services (PREOF) with potential possiblity to interact with lower layer one-hop reliability functions that are more typical to wireless than wires, including Automatic Repeat reQuest (ARQ), Forward Error Correction (FEC), Hybrid ARQ (HARQ) that includes both, and other techniques such as overhearing and constructive interferences. Because RAW may be leveraged on wired links, e.g., to save power, it is not expected that all lower layers support all those capabilities.

RAW provides hints to the lower layer services on the desired outcome, and the lower layer acts on those hints to provide the best approximation of that outcome, e.g., a level of reliability for one-hop transmission within a bounded budget of time and/or energy. Thus, the RAW API makes possible cross-layer optimization for reliability depending on the actual abstraction provided. That is, some reliability functions are controlled from Layer-3 using an abstract interface, while they are really operated at the lower layers.

The RAW Path Selection can be implemented in both centralized and distributed scheduling approaches. In the centralized approach, the PLR may obtain a set of pre-computed DetNet paths matching a set of expected failures, and apply the appropriate DetNet paths for the current state of the wireless links. In the distributed approach, the signaling in the packet may be more abstract than an explicit Path, and the PLR decision might be revised along the select DetNet Path based on a better knowledge of the rest of the way.

The dynamic DetNet Path selection in RAW avoids the waste of critical resources such as spectrum and energy while providing for the guaranteed SLA, e.g., by rerouting and/or adding redundancy only when a spike of loss is observed.

6. Security Considerations

RAW uses all forms of diversity including radio technology and physical path to increase the reliability and availability in the face of unpredictable conditions. While this is not done specifically to defeat an attacker, the amount of diversity used in RAW makes an attack harder to achieve.

6.1. Layer-2 encryption

Radio networks typically encrypt at the MAC layer to protect the transmission. If the encryption is per pair of peers, then certain RAW operations like promiscuous overhearing become impossible.

6.2. Forced Access

A RAW policy may typically select the cheapest collection of links that matches the requested SLA, e.g., use free Wi-Fi vs. paid 3GPP access. By defeating the cheap connectivity (e.g., PHY-layer interference) the attacker can force an End System to use the paid access and increase the cost of the transmission for the user.

7. IANA Considerations

This document has no IANA actions.

8. Contributors

The editor wishes to thank the document co-authors:

Lou Berger: Lab N

Xavi Vilajosana: Wireless Networks Research Lab, Universitat Oberta de Catalunya

Geogios Papadopolous: IMT Atlantique

Remous-Aris Koutsiamanis: IMT Atlantique

Rex Buddenberg: Individual contributor

Greg Mirsky: Ericsson

for their contributions to the text and ideas exposed in this document.

9. Acknowledgments

This architecture could never have been completed without the support and recommendations from the DetNet Chairs Janos Farkas and Lou Berger, and Dave Black, the DetNet Tech Advisor. Many thanks to all of you.

The authors wish to thank Balazs Varga, Dave Cavalcanti, Don Fedyk, Nicolas Montavont, and Fabrice Theoleyre for their in-depth reviews during the development of this document.

10. References

10.1. Normative References

[6TiSCH-ARCHI] Thubert, P., Ed., "An Architecture for IPv6 over the Time-Slotted Channel Hopping Mode of IEEE 802.15.4 (6TiSCH)", RFC 9030, DOI 10.17487/RFC9030, May 2021, <https://www.rfc-editor.org/info/rfc9030>.

[INT-ARCHI] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <https://www.rfc-editor.org/info/rfc1122>.

[RFC4427] Mannie, E., Ed. and D. Papadimitriou, Ed., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, DOI 10.17487/RFC4427, March 2006, <https://www.rfc-editor.org/info/rfc4427>.

[RAW-TECHNOS] Thubert, P., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-ietf-raw-technologies-08, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-raw-technologies-08>.

[RAW-USE-CASES] Bernardos, C. J., Papadopoulos, G. Z., Thubert, P., and F. Theoleyre, "RAW Use-Cases", Work in Progress, Internet-Draft, draft-ietf-raw-use-cases-11, 17 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-raw-use-cases-11>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, DOI 10.17487/RFC6291, June 2011, <https://www.rfc-editor.org/info/rfc6291>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/

RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8557] Finn, N. and P. Thubert, "Deterministic Networking Problem Statement", RFC 8557, DOI 10.17487/RFC8557, May 2019, <https://www.rfc-editor.org/info/rfc8557>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[RFC8939] Varga, B., Ed., Farkas, J., Berger, L., Fedyk, D., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP", RFC 8939, DOI 10.17487/RFC8939, November 2020, <https://www.rfc-editor.org/info/rfc8939>.

[RFC9049] Dawkins, S., Ed., "Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)", RFC 9049, DOI 10.17487/RFC9049, June 2021, <https://www.rfc-editor.org/info/rfc9049>.

10.2. Informative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997, <https://www.rfc-editor.org/info/rfc2205>.

[TE] Awduche, D., Chiu, A., Elwalid, A., Widjaja, I., and X. Xiao, "Overview and Principles of Internet Traffic Engineering", RFC 3272, DOI 10.17487/RFC3272, May 2002, <https://www.rfc-editor.org/info/rfc3272>.

[RFC3366] Fairhurst, G. and L. Wood, "Advice to link designers on link Automatic Repeat reQuest (ARQ)", BCP 62, RFC 3366,

DOI 10.17487/RFC3366, August 2002, <https://www.rfc-editor.org/info/rfc3366>.

[STD 62] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002, <https://www.rfc-editor.org/info/rfc3411>.

[RFC4090] Pan, P., Ed., Swallow, G., Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, DOI 10.17487/RFC4090, May 2005, <https://www.rfc-editor.org/info/rfc4090>.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[FRR] Shand, M. and S. Bryant, "IP Fast Reroute Framework", RFC 5714, DOI 10.17487/RFC5714, January 2010, <https://www.rfc-editor.org/info/rfc5714>.

[RLFA-FRR] Bryant, S., Filsfils, C., Previdi, S., Shand, M., and N. So, "Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)", RFC 7490, DOI 10.17487/RFC7490, April 2015, <https://www.rfc-editor.org/info/rfc7490>.

[DetNet-DP] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane Framework", RFC 8938, DOI 10.17487/RFC8938, November 2020, <https://www.rfc-editor.org/info/rfc8938>.

[DLEP] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <https://www.rfc-editor.org/info/rfc8175>.

[I-D.irtf-panrg-path-properties] Enghardt, R. and C. Krähenbühl, "A Vocabulary of Path Properties", Work in Progress, Internet-Draft, draft-irtf-panrg-path-properties-08, 6 March 2023, <https://datatracker.ietf.org/doc/html/draft-irtf-panrg-path-properties-08>.

[IPoWIRELESS] Thubert, P. and M. Richardson, "Architecture and Framework for IPv6 over Non-Broadcast Access", Work in Progress, Internet-Draft, draft-thubert-6man-ipv6-over-

wireless-15, 8 March 2023, <https://datatracker.ietf.org/doc/html/draft-thubert-6man-ipv6-over-wireless-15>.

[DetNet-OAM] Mirsky, G., Theoleyre, F., Papadopoulos, G. Z., Bernardos, C. J., Varga, B., and J. Farkas, "Framework of Operations, Administration and Maintenance (OAM) for Deterministic Networking (DetNet)", Work in Progress, Internet-Draft, draft-ietf-detnet-oam-framework-11, 8 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-detnet-oam-framework-11>.

[NASA] Adams, T., "RELIABILITY: Definition & Quantitative Illustration", <https://kscddms.ksc.nasa.gov/Reliability/Documents/150814-3bWhatIsReliability.pdf>.

Author's Address

Pascal Thubert (editor)
06330 Roquefort-les-Pins
France

Email: pascal.thubert@gmail.com