Technical Disclosure Commons

Defensive Publications Series

August 2021

LOW LATENCY LOW LOSS UNDER 1 MSEC PROTECTION IN 5G/ LTE-A PACKET FRONTHAUL

Prashant Anand

Dinuraj K

Guru P. P

Manoj Kumar

LOW LATENCY LOW LOSS UNDER 1 MSEC PROTECTION IN 5G/LTE-A PACKET FRONTHAUL

AUTHORS:
Prashant Anand
Dinuraj K
Guru P P
Manoj Kumar

ABSTRACT

Protection switching is important in a Third Generation Partnership Project (3GPP) Fifth Generation (5G) fronthaul network and for ultra-reliable and low latency communications (URLLC) types of applications. For example, protection switching requirements may necessitate an under one millisecond (msec) low loss and low latency protection switch over to, among other things, avoid a cell reset and support the emerging area of URLLC. To address those types of challenges, techniques are presented herein that support, among other things, a dedicated protection mechanism that is handled in a data plane where such protection switching is triggered in the data plane itself without any protocol interaction. Aspects of the techniques presented herein encompass, among other things, the dynamic configuration of a re-timer buffer depth, a custom extension header in a Radio over Ethernet (RoE) packet to support the conveyance of an indication of a path failure, little dependency on the transport network, etc.

DETAILED DESCRIPTION

In a Third Generation Partnership Project (3GPP) Fifth Generation (5G) or Long-Term Evolution (LTE) advanced (LTE-A) environment an intelligent converged access router may provide packet fronthaul or converged wireless/optical (often referred to as 'XHaul') transport capabilities for open radio access network (RAN) for RAN disaggregation. Usually, a fronthaul Centralized-RAN (C-RAN) use case is supported through an optical link with either coarse wavelength-division multiplexing (CWDM) (for passive use) or dense wavelength-division multiplexing (DWDM) (for active or passive

use). But, for a variety of reasons as 5G and LTE-A are being deployed RAN is moving towards packet fronthaul.

One of the prime applications for the techniques presented herein is to enable C-RAN by carrying radio in-phase (I) and quadrature (Q) samples over packets to a central location. Within that context one of the requirements is under one (1) millisecond (msec) low loss and low latency protection switch over to, for example, avoid a cell reset and support the emerging area of ultra-reliable and low latency communications (URLLC) applications.

Figure 1, below, depicts aspects of a 5G or LTE-A fronthaul or XHaul use case. In the environment that is depicted in Figure 1, below, radio facilities are at the service layer while an intelligent converged access router is at the ~~a~~ transport layer. Such a system is realized today with a field-programmable gate array (FPGA) and a switch router application-specific integrated circuit (ASIC). The FPGA's task is to perform radio processing.

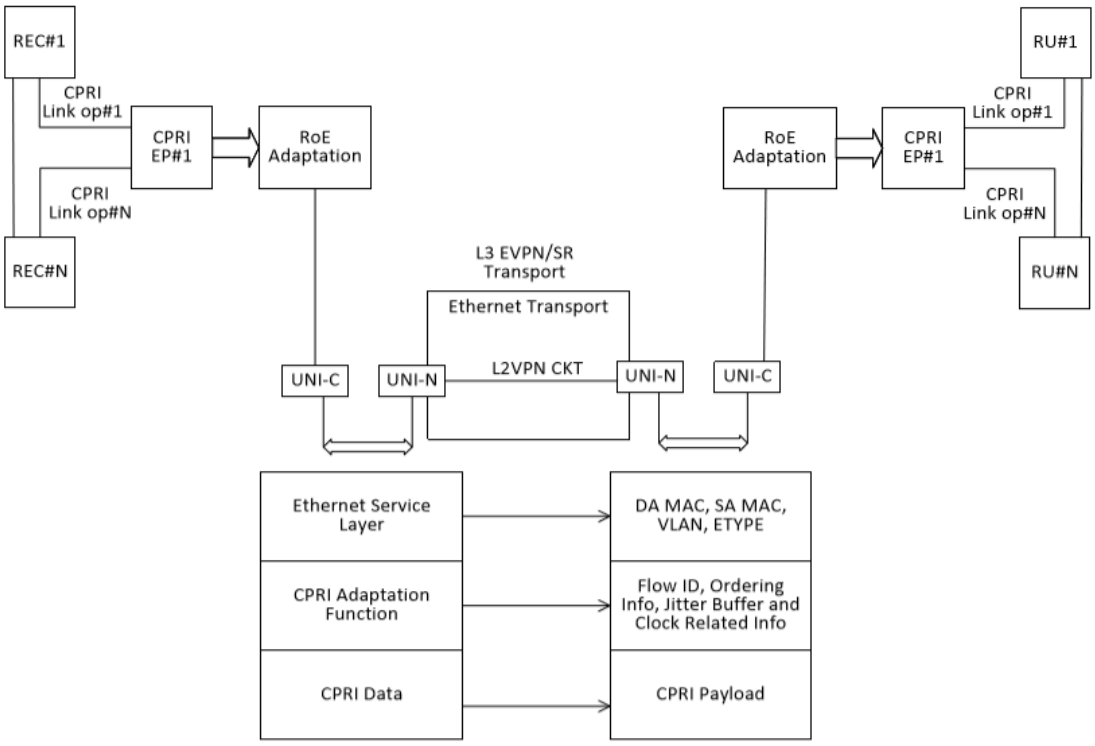

Figure 1: Illustrative Fronthaul Environment

To address the challenges that were described above, techniques are presented herein that support, among other things, a dedicated protection mechanism that is handled in the data plane where such protection switching is triggered in the data plane itself without any protocol interaction and provides under one msec low loss and low latency protection switch over to, among other things, avoid a cell reset and support the emerging area of URLLC.

A key performance indicator (KPI) of low latency low loss protection of under one msec will necessitate, possibly among other things, dedicated protection that needs to be handled in the data plane. Such protection switching is triggered in the data plane itself without any protocol interaction. Also, fronthaul traffic is very critical and comprises a heavy volume of traffic. Therefore, it needs to be source-to-destination protected rather than network protected.

At the same time, a fronthaul CPRI flow has very strict jitter requirements (e.g., plus or minus 8.138 nanoseconds (nsecs) of jitter in one direction). Such requirements cannot be met by a traditional scheduling method or even by Time-Sensitive Networking (TSN) frame preemption.

Aspects of the techniques presented herein leverage Layer 3 (L3), Ethernet virtual private network (EVPN), or segment routing for a fronthaul application. While L3 is very good for an any-to-any paradigm, programmability, resilience, scale, and Operations, Administration and Maintenance (OAM), deficiencies may arise in XHaul applications.

Such an approach presents a number of challenges. For example, one of the CPRI requirement is a one-way path delay jitter of plus or minus 8.138 nsecs and a two-way path delay jitter of plus or minus 16.276 nsecs. These requirements cannot be met with an Ethernet switch or router. Even by enabling IEEE 802.1Qbu frame preemption it cannot be met. Since such precise jitter numbers are involved, different kinds of jitter must be considered, including:

- Jitter of 114.4 nsecs over a 10 Gigabit Ethernet (10GE) interface even with IEEE 802.1Qbu.
- Jitter of 11.44 nsecs jitter on 100 Gigabit Ethernet (100GE) interface even with IEEE 802.1Qbu.

- Jitter introduced with self-inference due to other equal CPRI over Ethernet (CoE) flows.
- Jitter introduced due to a higher utilization in an XHaul application.
- Jitter introduced due to different arbiters in a packet processing pipeline.
- Jitter introduced due to clock domain transfer.
- Jitter introduced due to digital logic.

In the end, these jitter amounts can be additive or compensating across multiple hops from an ingress CoE or RoE mapper and an egress CPRI to an Ethernet to CoE or RoE demapper.

Within this context, some of the important points of interest in connection with the techniques presented herein include, for example:

- A Radio Equipment Controller (REC) or baseband unit (BBU) is the frequency and phase master for a remote radio head (RRH).
- At an RRH frequency is recovered from the bitstream as a physical clock and will be used to generate a carrier frequency on an air interface.
- There is no Precision Time Protocol (PTP) or PTP Time of Day (ToD) or ToD at an RRH. There is a concept of very strict phase alignment between a REC or BBU and an RRH. But this is not a clock edge or ToD alignment. This is frame counter alignment, where such a counter creates an event for an air interface transfer. This is referred to as a basic frame number (BFN) or Hyper Frame Number (HFN) counter. A REC as master initiates the session with an RRH and it sends the BFN or HFN and an RRH turns around the same number. That is how a REC and an RRH may be phase aligned.
- When a REC and an RRH are out of phase that will result in a delay for a frame or signal from a REC to reach an RRH. Such a delay may be mitigated with an accurate delay measurement between a REC and an RRH and sending the radio frame in advance (e.g., timing advance (TADV)) equal to delay between the REC and the RRH. So, by the time the radio frame reaches the RRH its phase is aligned because it was started ahead to mitigate the delay (i.e., the TADV).

Figure 2, below, depicts aspects of the re-timing process that was described above. In the figure, a REC or BBU are an intelligent converged access router that are performing

mapping and demapping of CPRI signals to packets and an RRH or radio unit (RU) are tracing the same synchronous Ethernet frequency (according to, for example, the International Telecommunication Union (ITU) recommendation 8262.1) and PTP IEEE standard 1588v2 clock phase (with, for a Class C clock, a Constant Time Error (cTE) of eight nsecs).

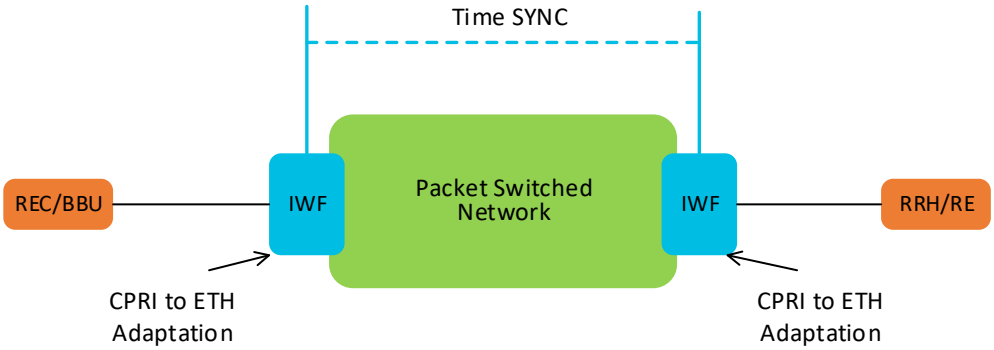

Figure 2: Exemplary Re-timing Process

In connection with Figure 2, above, re-timing a radio flow in a model synchronous network may encompass a number of considerations, including:

- Re-timing may be considered in connection with reducing jitter. For example:
  - A residual time stamp (e.g., `T1`) may be placed in a packet at the ingress node.
  - A packet arrives at the egress node at time stamp `T2`.
  - The packet may be buffered until time stamp `T3` (where `T3 >= T2`) at which point it may be sent.
  - The duration `T3 - T1` is a fixed value and should be long enough to cover, for example, all possible jitter, fiber propagation delay, processing delay, serialization delay, etc.
  - Additionally, the duration `T3 - T1` should be as low as possible.
- Time synchronization is required at the ingress and egress nodes.
- Such a model may be used for RoE time division (RoE-TD), RoE frequency division (RoE-FD), eCPRI, and CPRIoE.
- De-jittering may possibly be done in an REC or RE for RoE and eCPRI (helping in cleaning some noise).

- For CPRIoE such an approach is needed.

As noted previously, aspects of the techniques presented herein leverage L3, EVPN, or segment routing. It is well established that L3, EVPN, or segment routing may provide many benefits such as, for example, virtualizing the topology, scale, resilience and protection, OAM, programmability, and automation. However, there will be an asymmetrical delay between an uplink and a downlink path with jitter which will violate the CPRI KPI as described above.

Figure 3, below, depicts aspects of a data flow architecture that is possible under aspects of the techniques presented herein.

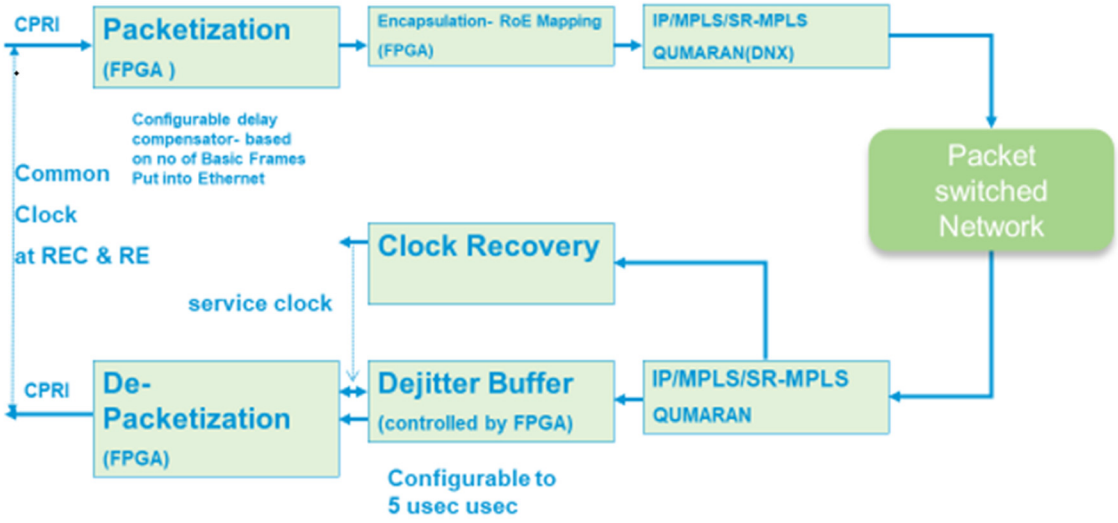

Figure 3: Exemplary Data Flow Architecture

Further, CPRI has an under one msec low loss low latency protection switch over requirement. Detection of failure in primary path, notification and switchover to backup path, dataflow resume in backup path and RRH detecting continuity in under one msec is the requirement.

With an under one msec low loss low latency protection switch over requirement, aspects of the techniques presented herein encompass a number of constraints, including:

- A solution needs to offer dedicated protection, meaning a backup path must be setup in advance.

- Protection switching needs to be triggered by a data plane.
- Since CPRI is 100% duty cycle traffic, which emits a basic frame every 260.4 nsecs, in the instant RoE or eCPRI case the Nx basic frame is packetized in an Ethernet frame and then the maximum one-way latency is 100 usecs. As a result, if non-availability of data is observed for, as an example, 5 x 100 usecs (or for any configured delay) then it can be assumed that some fault has occurred. This will indicate the fault in the transport section of a RoE or eCPRI network.
- A transport failure as described above may happen in one direction or in both directions. Both of these cases are addressed by the techniques that are presented herein.

For simplicity of exposition, the discussion and the figures that are presented in the narrative that follows will focus on one direction. However, it will be understood that the same steps, according to aspects of the techniques that are presented herein, are (as noted above) applicable to the other direction as well.

For purposes of illustration, aspects of the techniques presented herein may be described through a series of steps, including:

- NGFI IEEE 1914.3 RoE is 100% duty cycle traffic and hence once a data flow is started continuity in the data flow itself can be used as a keep-alive indicator. If there is discontinuity in the data flow then it indicates some failure in the data path and requires a path switchover.
- Considering an under one msec, or a few msecs, protection switch time implies dedicated protection, meaning two paths from a source to a destination are already established.
- One of the paths is marked as active and the other path is considered a hot-standby.
- At the same time, the path delay and the peak-to-peak (P2P) jitter for both paths are measured using conventional means.
- The maximum excursion (P2P jitter) and the path delay may be considered for the active and backup path in one direction and the re-timer buffer may be configured based on these parameters (e.g., in the REC to RRH direction one has following parameters -- `T_active_path_delay`, `T_active_p2p_jitter`,

`T_backup_path_delay`, and `T_backup_p2p_jitter`). The re-timer buffer depth may then be configured as:

```
T_retimer_buffer_size = MAX (T_active_path_delay,T_backup_path_delay)
T_retimer_p2p_jitter  = MAX (T_active_p2p_jitter,T_backup_p2p_jitter)
```

Note that this is described and illustrated in detail in the narrative below.

- The above process can be repeated for the active and the backup path for the reverse direction as well. As long as an active path is healthy, it can be used. If an active path fails, and at a receiver data is not received for a configured delay time, it can be assumed that the path is broken.
- This information is conveyed to the other end through a custom header in the return flows in the active path as well as in the backup or hot-standby path. This will ensure that even if the active reverse path is also broken, the transmitter receives the failure event notification and can act upon it. The hot-standby path might not be carrying normal RoE traffic at that point in time. But, a dummy packet with a path failure indication needs to be sent to inform the transmitter about the failure in the forward path.
- A sender protection switches to a backup path.
- The above process may be completed in each direction.

Figure 4, below, illustrates the format of a custom extension header in a RoE packet that is possible under aspects of the techniques presented herein. Such a packet format may be proposed as an addition to the IEEE 1914.3 standard.

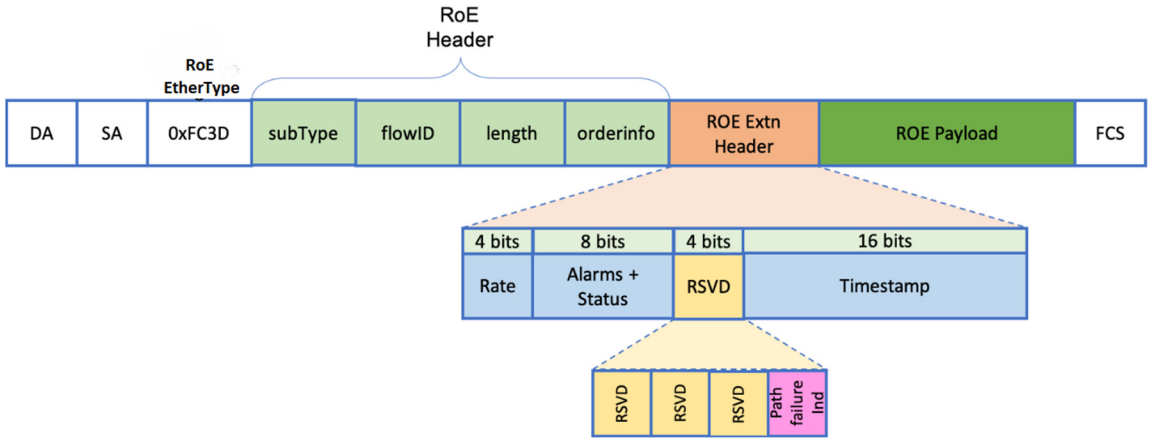

Figure 4: Exemplary Custom Extension Header

As depicted in Figure 4, above, one (1) bit in the reserved (RSVD) range may be employed to indicate a path failure to a transmitter. A headend may then use this indication to trigger a repair action.

Consider the illustrative example that is presented in Figure 5, below. With reference to the active path, if that path fails then there will be no traffic at IWF B for a configured amount of time (e.g., 500 usecs). Such an event is conveyed to IWF A with the return traffic through a custom header field in the return flows of both the active and backup paths. When IWF A receives notification of this event it immediately moves the traffic to the backup path. Note that in this example network the maximum one-way latency is 100 usecs.

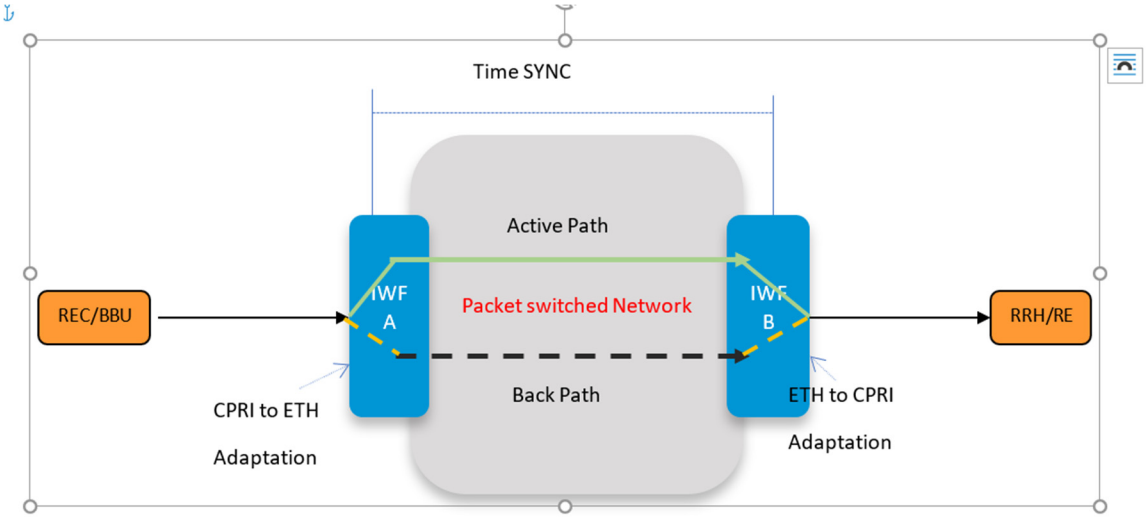

Figure 5: Illustrative Network Example

Continuing with the illustrative example that is presented in Figure 5, above, assume that the time interval is configured at 500 usecs (i.e., if there is no frame from IWF A to IWF B in that amount of time then it is decided that a path has failed).

Such a failure event is conveyed to the other end IWF A, which will take another 100 usecs. IWF A will then cut over to a protection path and hence IWF B will see the traffic arrive after 100 usecs. Consequently, the total protection switch time equals 500

usecs + 100 usecs + 100 usecs + 100 usecs (i.e., the other overhead amounts) for a total of 800 usecs, which is less than the 1 msec target (providing for a 200 usecs margin).

According to aspects of the techniques presented herein, configuration of the re-timer buffer may be accomplished through a series of steps, including:

- A residual time stamp (e.g., `T1`) may be placed in a packet at the mapping endpoint.
- A packet arrives at the demaping endpoint at time stamp `T2`.
- The propagation delay, or path_delay (`T_Delay`), is equal to `T2 - T1`.
- Assume a re-timing delay, `Tretimer_delay`, where `Tretimer_delay > T_Delay`.
- Here `Tretimer_delay` is intended to cover all different kinds of latency and latency variation or jitter.
- According to aspects of the techniques presented herein, based on the `active_path_delay`, `backup_path_delay`, `active_path_p2p_jitter`, and `backup_path_p2p_jitter` it is possible to derive:

```
Tretimer_delay = max (active_path_delay, backup_path_delay)
path_delay_P2P_jitter = (path_delay_max - path_delay_min)
Tretimer_p2p_jitter = max (active_path_p2p_jitter, backup_path_p2p_jitter)
```

These two values (i.e., `Tretimer_delay` and `Tretimer_p2p_jitter`) may then be used to configure the re-timer buffer, as depicted in Figure 6, below.

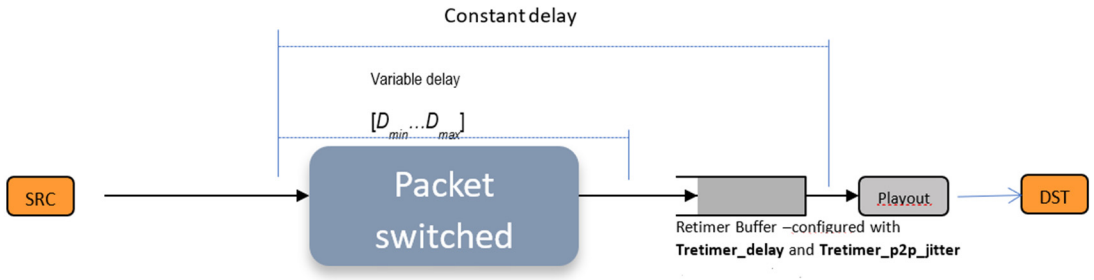

Figure 6: Exemplary Re-Timer Buffer Configuration

In connection with the techniques presented herein, it is important to consider a comparison between those techniques and transport protection mechanisms.

Transport networks provide resiliency features to recover from network failures. But there are problems using such schemes for low loss low latency flows like CPRI or RoE. Segment routing may have Topology-Independent Loop Free Alternate (TI-LFA) for resiliency. When a failure happens in the network, TI-LFA reroutes traffic over a pre-provisioned backup path and then, after a re-convergence, will reroute the traffic again on the post-convergence path (PCP). The first reroute may have up to 50 msecs of traffic loss and the second path can have a different transport latency compared to the failed active path. In the second reroute, even though it is lossless, the PCP can have a different latency compared to the pre-provisioned backup path. The 50 msecs traffic loss in the first reroute and the latency change in the second reroute can cause disruptions to the flow of a low latency low loss RoE stream. As a result, a TI-LFA kind of mechanism cannot be used to provide protections to such streams.

Aspects of the techniques presented herein employ application-level protection and there is little dependency on the transport network. The only requirement is to have the primary and backup streams routed through different paths in the packet switched network. This may be achieved through schemes like, for example, traffic engineering. The active and backup paths carry the same RoE streams with the same flow identifier (ID). But the outer encapsulations can change for primary and backup streams. If pseudowires (PWs) are used, then the PW labels would be different between the active and standby streams. If Layer 2 (L2) switching is used, then the virtual local area networks (VLANS) of the active and standby streams could be different.

In summary, techniques have been presented that support, among other things, a dedicated protection mechanism that is handled in a data plane where such protection switching is triggered in the data plane itself without any protocol interaction and provides an under one msec low loss and low latency protection switch over to, among other things, avoid a cell reset and support the emerging area of URLLC. Aspects of the techniques presented herein encompass, among other things, the dynamic configuration of a re-timer buffer depth, a custom extension header in a RoE packet to support the conveyance of an indication of a path failure, little dependency on the transport network, etc.