MNA Interim 2023-10-19

MeetEcho meeting

MPLS Chairs:

Tarek Saad

Loa Andersson

Nic Leymann

Mach Chen (secr)

PALS Chairs:

Stewart Bryant

Andy Malis

David Sinicrope (secr)

DetNet Chairs:

Lou Berger

Janos Farkas

Ethan Grossman (secr)

This session is being recorded

Internet Engineering Task Force
© 2023 IETF Trust
Production by Meetecho

IETF

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Administrative

- **Blue Sheet**
  - Blue sheets will be automatically generated when you login into the Meetecho
- **MeetEcho URL:**
  - https://meetings.conf.meetecho.com/interim/?short=a7165148-295b-46ad-92fd-550945d8c3be
- **Minutes Taking:**
  - https://notes.ietf.org/notes-ietf-interim-2023-mpls-20-mpls
- **MPLS Session Agenda at:**
  - https://datatracker.ietf.org/doc/agenda-interim-2023-mpls-20-mpls-01/
- **Data tracker:**
  - http://datatracker.ietf.org/wg/mpls
- **MPLS WG Wiki:**
  - https://wiki.ietf.org/group/mpls
- **MPLS WG Github:**
  - https://github.com/ietf-wg-mpls/drafts

Agenda

1. **Agenda bashing**

2. **Review of Open Action Items - https://wiki.ietf.org/group/mpls/omc-ais**
3. **The MNA FWK security considerations - https://datatracker.ietf.org/doc/draft-ietf-mpls-mna-fwk/**
4. **Review of MNA usescases - https://datatracker.ietf.org/doc/draft-ietf-mpls-mna-usecases/**
5. **AOB**

Non-Juniper

Use Cases for MPLS Network Action Indicators and MPLS Ancillary Data

I-D.ietf-mpls-mna-usecases

Internet Engineering Task Force
© 2023 IETF Trust
Production by Meetecho

OVERVIEW

- The document was developed in the early process of MPLS MNA activities
- The document describes use cases that have a need for encoding network action indicators (and associated ancillary data) inside MPLS packets
- Is not an exhaustive set, but contains ones that are actively discussed by members of the IETF MPLS, PALS and DETNET working groups participating in the MPLS MNA activities

USE-CASE1: No Further Reroute (NFRR)
I-D.draft-kompella-mpls-nffrr

- Avoid subsequent fast reroute of packets that are already impacted by a 1st fast reroute event
- For example, in multi-homed PE usecase when multiple CE-PE links fail
- PE detecting failure can reroute protected traffic between them in a loop
- Packets may be marked with NFRR Action Indicator to avoid a subsequent fast reroute

Consider the following topology for multihoming an Ethernet VPN (EVPN [RFC7432]) Customer Edge (CE) device for protection against the failure of a Provider Edge (PE) device or a PE-CE link. To do so, there is a backup MPLS path between PE2 and PE3 (denoted by the starred line).

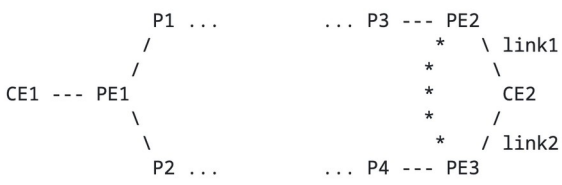

Figure 1: EVPN Multihoming

USE-CASE2: Insitu-OAM (passport method)
I-D.draft.gandhi-mpls-ioam-sr

- To record IOAM operational and telemetry information in data packets while they traverses an MPLS LSP path
- The IOAM packet data fields for OAM and PM are defined in [I-D.ietf-ippm-ioam-data]
- [I-D.ietf-ippm-ioam-data] defines following options: Pre-allocated Trace Option, Incremental Trace Option, Proof of Transit (POT) Option, and Edge-to-Edge Option
- For Hop-by-hop IOAM case:
  - Need for ***IOAM Action Indicator*** to alert transit and edge LSRs to process/update IOAM data
- Edge-to-edge case:
  - Need for ***IOAM Action Indicator*** to alert egress LER to process/dispose of IOAM data

USE-CASE3: Insitu-OAM Direct Export (postcard method)

I-D.ietf-ippm-ioam-direct-export

- IOAM Direct Export (DEX) option used as a trigger for IOAM data to be exported while data packets traverses an MPLS LSP path
- IOAM Direct Export (DEX) option formats are defined in draft-ietf-ippm-ioam-direct-export
- *Need for MPLS* ***IOAM-DEX Action Indicator*** for the hop-by-hop case to alert all LSRs to trigger IOAM data exporting, collection or aggregation
- Need for MPLS ***IOAM-DEX Action Indicator*** for the edge-to-edge case to alert ingress/egress LER to process/dispose of the IOAM data

USE-CASE4: Network Slicing

I-D.bestbar-teas-ns-packet and draft-ietf-teas-ietf-network-slices

- A Network Resource Partitions (NRP) is a subset of resources and associated policies on each of a connected set of links in the underlay network
- NRP may be built NRPs with dedicated topologies, or share topology with other NRPs
- The MPLS packets carried over Label Switched Paths may traverse a specific NRP that require enforcing specific scheduling and/or drop policy associated with the NRP
- Need for MPLS ***NRP Action Indicator*** in MPLS packets to associate NRP packets with the resources on specific LSRs

USE-CASE5: Generic Delivery Functions

I-D.bestbar-teas-ns-packet and draft-ietf-teas-ietf-network-slices

- Some functionalities (e.g., fragmentation/reassembly and Encapsulating Security Payload) are applicable to MPLS layer (and other layers like BIER or even Ethernet) independent of IP
- The proposal adapts:
  - The IPv6 Fragmentation header for use in non-IP contexts (e.g. MPLS) to achieve fragmentation/reassembly functions
  - The IP Encapsulating Security Payload (ESP) [RFC4303] can also be carried in MPLS packets to support ESP at MPLS layer
- The extended headers are carried as payload of MPLS packets
- Need for GDF Action Indicator to alert LSRs of presence of the specific functions

USE-CASE6: Delay Budgets for Time-Bounded Applications

I-D.stein-srtsn and I-D.draft-eckert-detnet-glbf

- Time sensitive traffic requires packets be delivered to their final destination by a strict deadline time
- An approach can be that packet headers carry the packet birth time and a delay budget
  - Routers use current time, birth time and delay budget to properly schedule packets
- Another approach is to carry precalculated individual "local" deadlines applicable to each traversed router to properly schedule a packet
  - The local deadlines can be carried in a "stack” like fashion similar to how Segment Routing carries forwarding instructions
  - For example, the number of deadline values encoded in the stack may be the number of routers the packet needs to traverse in the network, and each deadline value corresponds to a specific router

NEXT STEPS

- Some of the documented use-cases will need to be revalidated
- Some use cases reference other documents that have expired. Need to update references
- Welcome further input or updates to documented use-cases from the WG