Transporting PTP messages (1588) over MPLS Networks
draft-ietf-tictoc-1588overmpls-02

Abstract

This document defines the method for transporting PTP messages (PDUs) over an MPLS network. The method allows for the easy identification of these PDUs at the port level to allow for port level processing of these PDUs in both LERs and LSRs.
The basic idea is to transport PTP messages inside dedicated MPLS LSPs. These LSPs only carry PTP messages and possibly Control and Management packets, but they do not carry customer traffic.
Two methods for transporting 1588 over MPLS are defined. The first method is to transport PTP messages directly over the dedicated MPLS LSP via UDP/IP encapsulation, which is suitable for IP/MPLS networks. The second method is to transport PTP messages inside a PW via Ethernet encapsulation, which is more suitable for MPLS-TP networks.

Status of this Memo

Copyright Notice

review these documents carefully, as they describe your rights and
restrictions with respect to this document. Code Components extracted
from this document must include Simplified BSD License text as
described in Section 4.e of the Trust Legal Provisions and are provided
without warranty as described in the Simplified BSD License.

Table of Contents

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119]. When used in lower case, these words convey their typical use in common language, and are not to be interpreted as described in RFC2119 [RFC2119].

1. Introduction

The objective of Precision Time Protocol (PTP) is to synchronize independent clocks running on separate nodes of a distributed system. [IEEE] defines PTP messages for clock and time synchronization. The PTP messages include PTP PDUs over UDP/IP (Annex D and E of [IEEE]) and PTP PDUs over Ethernet (Annex F of [IEEE]). This document defines mapping and transport of the PTP messages defined in [IEEE] over MPLS networks. PTP defines several clock types: ordinary clocks, boundary clocks, end-to-end transparent clocks, and peer-to-peer transparent clocks. One key attribute of all of these clocks is the recommendation for PTP messages processing to occur as close as possible to the actual transmission and reception at the physical port interface. This targets optimal time and/or frequency recovery by avoiding variable delay introduced by queues internal to the clocks. To facilitate the fast and efficient recognition of PTP messages at the port level when the PTP messages are carried over MPLS LSPs, this document defines the specific encapsulations that should be used. In addition, it can be expected that there will exist LSR/LERs where only a subset of the physical

ports will have the port based PTP message processing capabilities. In order to ensure that the PTP carrying LSPs always enter and exit ports with this capability, routing extensions are defined to advertise this capability on a port basis and to allow for the establishment of LSPs that only transit such ports. While this path establishment restriction may be applied only at the LER ingress/egress ports, it becomes more important when using Transparent Clock capable LSRs in the path.
The port based PTP message processing involves PTP event message recognition. Once the PTP event messages are recognized they can be modified based on the reception or transmission timestamp. An alternative technique to actual packet modification could include the enforcement of a fixed delay time across the LSR to remove variability in the transit delay. This latter would be applicable in a LSR which does not contain a PTP transparent Clock function.
This document provides two methods for transporting PTP messages over MPLS. One is principally focused on an IP/MPLS environment and the second is focused on the MPLS-TP environment.
While the techniques included herein allow for the establishment of paths optimized to include PTP Timestamping capable links, the performance of the Slave clocks is outside the scope of this document.

2. Terminology

1588: The timing and synchronization as defined by IEEE 1588
PTP: The timing and synchronization protocol used by 1588
Master Clock: The source of 1588 timing to a set of slave clocks.
Master Port: A port on a ordinary or boundary clock that is in Master state. This is the source of timing toward slave ports.
Slave Clock: A receiver of 1588 timing from a master clock
Slave Port: A port on a boundary clock or ordinary clock that is receiving timing from a master clock.
Ordinary Clock: A device with a single PTP port.
Transparent Clock. A device that measures the time taken for a PTP event message to transit the device and then updates the correctionField of the message with this transit time.
Boundary Clock: A device with more than one PTP port. Generally boundary clocks will have one port in slave state to receive timing and then other ports in master state to re-distribute the timing.
PTP LSP: An LSP dedicated to carry PTP messages
PTP PW: A PW within a PTP LSP that is dedicated to carry PTP messages.
CW: Pseudowire Control Word
LAG: Link Aggregation
ECMP: Equal Cost Multipath
CF: Correction Field, a field inside certain PTP messages (message type 0-3)that holds the accumulative transit time inside intermediate switches

3. Problem Statement

When PTP messages are transported over MPLS networks, there is a need for PTP message processing at the physical port level. This requirement exists to minimum uncertainty in the transit delays. If PTP message processing occurs interior to the MPLS routers, then the variable delay introduced by queuing between the physical port and the PTP processing will add noise to the timing distribution. Port based processing applies at both the originating and terminating LERs and also at the intermediate LSRs if they support transparent clock functionality.
PTP messages over Ethernet or IP can always be tunneled over MPLS. However there is a requirement to limit the possible encapsulation options to simplify the PTP message processing required at the port level. This applies to all 1588 clock types implemented in MPLS routers. But this is particularly important in LSRs that provide transparent clock functionality.
When 1588-awareness is needed, PTP messages should not be transported over LSPs or PWs that are carrying customer traffic because LSRs perform Label switching based on the top label in the stack. To detect PTP messages inside such LSPs require special hardware to do deep packet inspection at line rate. Even if such hardware exists, the payload can't be deterministically identified by LSRs because the payload type is a context of the PW label and the PW label and its context are only known to the Edge routers (PEs); LSRs don't know what is a PW's payload (Ethernet, ATM, FR, CES, etc). Even if one restricts an LSP to only carry Etehrent PWs, the LSRs don't have the knowledge of whether PW Control Word (CW) is present or not and therefore can't deterministically identify the payload.
Therefore a generic method is defined in this document that does not require deep packet inspection at line rate, and can deterministically identify PTP messages. The defined method is applicable to both MPLS and MPLS-TP networks.

4. 1588 over MPLS Architecture

1588 communication flows map onto MPLS nodes as follows: 1588 messages are exchange between PTP ports on Ordinary and boundary clocks. Transparent clocks do not terminate the PTP messages but they do modify the contents of the PTP messages as they transit across the Transparent clock. SO Ordinary and boundary clocks would exist within LERs as they are the termination points for the PTP messages carried in MPLS. Transparent clocks would exist within LSRs as they do not terminate the PTP message exchange.
Perhaps a picture would be good here.

5. Dedicated LSPs for PTP messages

Many methods were considered for identifying the 1588 messages when they are encapsulated in MPLS such as by using GAL/ACH or a new

reserved label. These methods were not attractive since they either
required deep packet inspection and snooping at line rate or they
required use of a scarce new reserved label. Also one of the goals was
to reuse existing OAM and protection mechanisms.

The method defined in this document can be used by LER/LSRs to identify
PTP messages in MPLS tunnels by using dedicated LSPs to carry PTP
messages.

Compliant implementations MUST use dedicated LSPs to carry PTP messages
over MPLS. These LSPs are herein referred to as "PTP LSPs" and the
labels associated with these LSPs as "PTP labels". These LSPs could be
P2P or P2MP LSPs. The PTP LSP between Master Clocks and Slave Clocks
MAY be P2MP or P2P LSP while the PTP LSP between each Slave Clock and
Master Clock SHOULD be P2P LSP. The PTP LSP between a Master Clock and
a Slave Clock and the PTP LSP between the same Slave Clock and Master
Clock MUST be co-routed. Alternatively, a single bidirectional co-
routed LSP can be used. The PTP LSP MAY be MPLS LSP or MPLS-TP LSP.
This co-routing is required to limit differences in the delays in the
Master clock to Slave clock direction compared to the Slave clock to
Master clock direction.

The PTP LSPs could be configured or signaled via RSVP-TE/GMPLS. New
RSVP-TE/GMPLS TLVs and objects are defined in this document to indicate
that these LSPs are PTP LSPs.

The PTP LSPs MAY carry essential MPLS/MPLS-TP control plane traffic
such as BFD and LSP Ping but the LSP user plane traffic MUST be PTP
only.

6. 1588 over MPLS Encapsulation

This document defines two methods for carrying PTP messages over MPLS.
The first method is carrying IP encapsulated PTP messages over PTP LSPs
and the second method is to carry PTP messages over dedicated Ethernet
PWs (called PTP PWs) inside PTP LSPs.

6.1. 1588 over LSP Encapsulation

The simplest method of transporting PTP messages over MPLS is to
encapsulate PTP PDUs in UDP/IP and then encapsulate them in PTP LSP.
The 1588 over LSP format is shown in Figure 1.

```
+----------------------+
|   PTP Tunnel Label   |
+----------------------+
|        IPv4/6        |
+----------------------+
|         UDP          |
+----------------------+
|        PTP PDU       |
+----------------------+
```
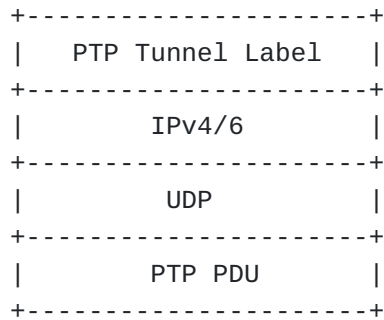
Figure 1 - 1588 over LSP Encapsulation

This encapsulation is very simple and is useful when the networks
between 1588 Master Clock and Slave Clock are IP/MPLS networks.
In order for an LSR to process PTP messages, the PTP Label must be the
top label of the label stack.
The UDP/IP encapsulation of PTP MUST follow Annex D and E of [IEEE].

6.2. 1588 over PW Encapsulation

Another method of transporting 1588 over MPLS networks is by
encapsulating PTP PDUs in Ethernet and then transporting them over
Ethernet PW (PTP PW) as defined in [RFC4448], which in turn is
transported over PTP LSPs. Alternatively PTP PDUs MAY be encapsulated
in UDP/IP/Ethernet and then transported over Ethernet PW.
Both Raw and Tagged modes for Ethernet PW are permitted. The 1588 over
PW format is shown in Figure 2.

```
                    +----------------+
                    |PTP Tunnel Label|
                    +----------------+
                    |    PW Label    |
                    +----------------+
                    |  Control Word  |
                    +----------------+
                    |    Ethernet    |
                    |     Header     |
                    +----------------+
                    |     VLANs      |
                    |   (optional)   |
                    +----------------+
                    |    IPV4/V6     |
                    |   (optional)   |
                    +----------------+
                    |      UDP       |
                    |   (optional)   |
                    +----------------+
                    |    PTP PDU     |
                    +----------------+
```

          Figure 2 - 1588 over PW Encapsulation

The Control Word (CW) as specified in [RFC4448] SHOULD be used to
ensure a more robust detection of PTP messages inside the MPLS packet.
If CW is used, the use of Sequence number is optional.
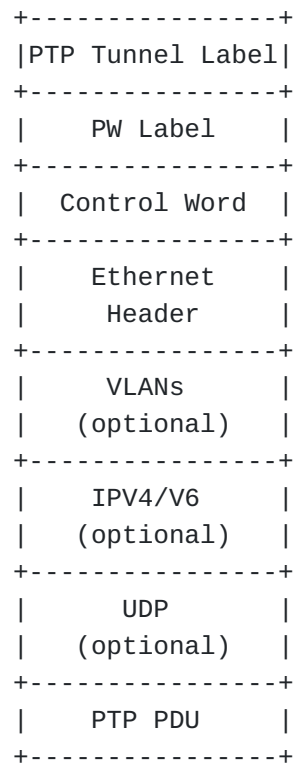The use of VLAN and UDP/IP are optional. Note that 1 or 2 VLANs MAY
exist in the PW payload.
In order for an LSR to process PTP messages, the top label of the label
stack (the Tunnel Label) MUST be from PTP label range. However in some
applications the PW label may be the top label in the stack, such as
cases where there is only one-hop between PEs or in case of PHP. In
such cases, the PW label SHOULD be chosen from the PTP Label range.
In order to ensure congruency between the two directions of PTP message
flow, ECMP should not be used for the PTP LSPs. Therefore, no Entropy
label [I-D.ietf-pwe3-fat-pw] is necessary and it SHOULD NOT be present
in the stack.
The Ethernet encapsulation of PTP MUST follow Annex F of [IEEE] and the
UDP/IP encapsulation of PTP MUST follow Annex D and E of [IEEE].
For 1588 over MPLS encapsulations that are PW based, there are some
cases in which the PTP LSP label may not be present:

     *When PHP is applied to the PTP LSP, and the packet is received
      without PTP LSP label at PW termination point .

     *When the PW is established between two routers directly connected
      to each other and no PTP LSP is needed.

In such cases it is required for a router to identify these packets as PTP packets. This would require the PW label to also be a label that is distributed specifically for carrying PTP traffic (aka PTP PW label). Therefore there is a need to add extension to LDP/BGP PW label distribution protocol to indicate that a PW label is a PTP PW labels.

7. 1588 Message Transport

1588 protocol comprises of the following message types:

    *Announce

    *SYNC

    *FOLLOW UP

    *DELAY_REQ (Delay Request)

    *DELAY_RESP (Delay Response)

    *PDELAY_REQ (Peer Delay Request)

    *PDELAY_RESP (Peer Delay Response)

    *PDELAY_RESP_FOLLOW_UP (Peer Delay Response Follow up)

    *Management

    *Signaling

A subset of PTP message types that require timestamp processing are called Event messages:

    *SYNC

    *DELAY_REQ (Delay Request)

    *PDELAY_REQ (Peer Delay Request)

    *PDELAY_RESP (Peer Delay Response)

SYNC and DELAY_REQ are exchanged between Master Clock and Slave Clock and MUST be transported over PTP LSPs. PDELAY_REQ and PDELAY_RESP are exchanged between adjacent PTP clocks (i.e. Master, Slave, Boundary, or Transparent) and MAY be transported over single hop PTP LSPs. If Two Step PTP clocks are present, then the FOLLOW_UP, DELAY_RESP, and PDELAY_RESP_FOLLOW_UP messages must also be transported over the PTP LSPs.
For a given instance of 1588 protocol, SYNC and DELAY_REQ MUST be transported over two PTP LSPs that are in opposite directions. These

PTP LSPs, which are in opposite directions MUST be congruent and co-routed. Alternatively, a single bidirectional co-routed LSP can be used.
Except as indicated above for the two-step PTP clocks, Non-Event PTP message types don't need to be processed by intermediate routers. These message types MAY be carried in PTP Tunnel LSPs.

8. Protection and Redundancy

In order to ensure continuous uninterrupted operation of 1588 Slaves, usually as a general practice, Redundant Masters are tracked by each Slave. It is the responsibility of the network operator to ensure that physically disjoint PTP tunnels that don't share any link are used between the redundant Masters and a Slave.
When redundant Masters are tracked by a Slave, any prolonged PTP LSP or PTP PW outage will trigger the Slave Clock to switch to the Redundant Master Clock. However LSP/PW protection such as Linear Protection Switching (1:1,1+1), Ring protection switching or MPLS Fast Reroute (FRR) SHOULD still be used to provide resiliency to individual network segment failures..
Note that any protection or reroute mechanism that adds additional label to the label stack, such as Facility Backup Fast Reroute, MUST ensure that the pushed label is a PTP Label to ensure recognition of the MPLS frame as containing PTP messages as it transits the backup path..

9. ECMP

To ensure the optimal operation of 1588 Slave clocks and avoid errors introduced by forward and reverse path delay asymmetry, the physical path for PTP messages from Master Clock to Slave Clock and vice versa must be the same for all PTP messages listed in section 7 and must not change even in the presence of ECMP in the MPLS network.
To ensure the forward and reverse paths are the same PTP LSPs and PWs MUST NOT be subject to ECMP.

10. OAM, Control and Management

In order to manage PTP LSPs and PTP PWs, they MAY carry OAM, Control and Management messages. These control and management messages can be differentiated from PTP messages via already defined IETF methods.
In particular BFD [RFC5880], [RFC5884] and LSP-Ping [RFC4389]MAY run over PTP LSPs via UDP/IP encapsulation or via GAL/G-ACH. These Management protocols are easily identified by the UDP Destination Port number or by GAL/ACH respectively.
Also BFD, LSP-Ping and other Management messages MAY run over PTP PW via one of the defined VCCVs (Type 1, 2 or 3) [RFC5085]. In this case G-ACH, Router Alert Label (RAL), or PW label (TTL=1) are used to identify such management messages.

11. QoS Considerations

In network deployments where not every LSR/LER is PTP-aware, then it is important to reduce the impact of the non-PTP-aware LSR/LERs on the timing recovery in the slave clock. The PTP messages are time critical and must be treated with the highest priority. Therefore 1588 over MPLS messages must be treated with the highest priority in the routers. This can be achieved by proper setup of PTP tunnels. It is recommended that the PTP LSPs are setup and marked properly to indicate EF-PHB for the CoS and Green for drop eligibility.
In network deployments where every LSR/LER supports PTP LSPs, then it MAY NOT be required to apply the same level of prioritization as specified above.

12. FCS Recalculation

Ethernet FCS of the outer encapsulation MUST be recalculated at every LSR that performs the Transparent Clock processing and FCS retention for the payload Ethernet described in [RFC4720] MUST NOT be used.

13. UDP Checksum Correction

For UDP/IP encapsulation mode of 1588 over MPLS, the UDP checksum is optional when used for IPv4 encapsulation and mandatory in case of IPv6. When IPv4/v6 UDP checksum is used each 1588-aware LSR must either incrementally update the UDP checksum after the CF update or should verify the UDP checksum on reception from upstream and recalculate the checksum completely on transmission after CF update to downstream node.

14. Routing extensions for 1588aware LSRs

MPLS-TE routing relies on extensions to OSPF [RFC2328] [RFC5340] and IS-IS [ISO] [RFC1195] in order to advertise Traffic Engineering (TE) link information used for constraint-based routing.
Indeed, it is useful to advertise data plane TE router link capabilities, such as the capability for a router to be 1588-aware. This capability MUST then be taken into account during path computation to prefer or even require links that advertise themselves as 1588-aware. In this way the path can ensure the entry and exit points into the LERs and, if desired, the links into the LSRs are able to perform port based timestamping thus minimizing their impact on the performance of the slave clock.
For this purpose, the following sections specify extensions to OSPF and IS-IS in order to advertise 1588 aware capabilities of a link.

14.1. 1588aware Link Capability for OSPF

OSPF uses the Link TLV (Type 2) that is itself carried within either the Traffic Engineering LSA specified in [RFC3630] or the OSPFv3 Intra-Area-TE LSA (function code 10) defined in [RFC5329] to advertise the TE

related information for the locally attached router links. For an LSA
Type 10, one LSA can contain one Link TLV information for a single
link. This extension defines a new 1588-aware capability sub-TLV that
can be carried as part of the Link TLV.

The 1588-aware capability sub-TLV is OPTIONAL and MUST NOT appear more
than once within the Link TLV. If a second instance of the 1588-aware
capability sub-TLV is present, the receiving system MUST only process
the first instance of the sub-TLV. It is defined as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Flags     |
+-+-+-+-+-+-+-+-+
```
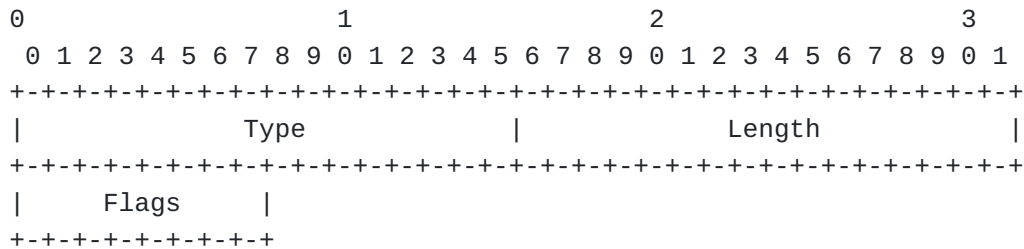
                Figure 3: 1588-aware Capability TLV

Where:

Type, 16 bits: 1588-aware Capability TLV where the value is TBD

Length, 16 bits: Gives the length of the flags field in octets, and is
currently set to 1

Flags, 8 bits: The bits are defined least-significant-bit (LSB) first,
so bit 7 is the least significant bit of the flags octet.

```
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|   Reserved  |C|
+-+-+-+-+-+-+-+-+
```
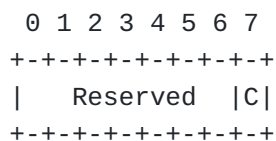
  Figure 4: Flags Format

Correction (C) field Update field, 1 bit: Setting the C bit to 1
indicates that the link is capable of recognizing the PTP event packets
and can compensate for residence time by updating the PTP packet
Correction Field. When this is set to 0, it means that this link cannot
perform the residence time correction but is capable of performing MPLS
frame forwarding of the frames with PTP labels using a method that
support the end to end delivery of accurate timing. The exact method is
not defined herein.

Reserved, 7 bits: Reserved for future use. The reserved bits must be
ignored by the receiver.

The 1588-aware Capability sub-TLV is applicable to both OSPFv2 and
OSPFv3.

14.2. 1588aware Link Capability for IS-IS

The IS-IS Traffic Engineering [RFC3784] defines the intra-area traffic
engineering enhancements and uses the Extended IS Reachability TLV
(Type 22) [RFC5305] to carry the per link TE-related information. This
extension defines a new 1588-aware capability sub-TLV that can be
carried as part of the Extended IS Reachability TLV.
The 1588-aware capability sub-TLV is OPTIONAL and MUST NOT appear more
than once within the Extended IS Reachability TLV or the Multi-Topology
(MT) Intermediate Systems TLV (type 222) specified in [RFC5120]. If a
second instance of the 1588-aware capability sub-TLV is present, the
receiving system MUST only process the first instance of the sub-TLV.
The format of the IS-IS 1588-aware sub-TLV is identical to the TLV
format used by the Traffic Engineering Extensions to IS-IS [RFC3784].
That is, the TLV is comprised of 1 octet for the type, 1 octet
specifying the TLV length, and a value field. The Length field defines
the length of the value portion in octets.

```
    0                   1                   2
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |     Length    |     Flags     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

          Figure 5: 1588-aware Capability sub-TLV

Where:
Type, 8 bits: 1588-aware Capability sub-TLV where the value is TBD
Length, 8 bits: Gives the length of the flags field in octets, and is
currently set to 1
Flags, 8 bits: The bits are defined least-significant-bit (LSB) first,
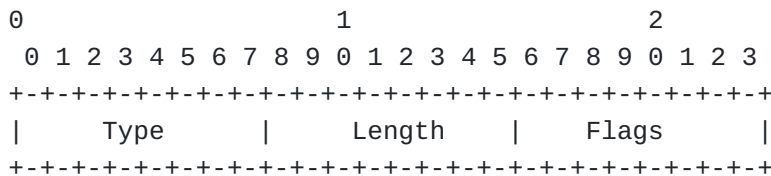so bit 7 is the least significant bit of the flags octet.


```
     0 1 2 3 4 5 6 7
    +-+-+-+-+-+-+-+-+
    |   Reserved  |C|
    +-+-+-+-+-+-+-+-+
```

  Figure 6: Flags Format

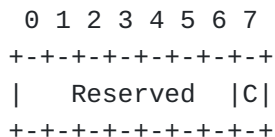Correction (C) field Update field, 1 bit: Setting the C bit to 1
indicates that the link is capable of recognizing the PTP event packets
and can compensate for residence time by updating the PTP packet
Correction Field. When this is set to 0, it means that this link cannot
perform the residence time correction but is capable of performing MPLS
frame forwarding of the frames with PTP labels using a method that

support the end to end delivery of accurate timing. The exact method is not defined herein.

Reserved, 7 bits: Reserved for future use. The reserved bits must be ignored by the receiver.

15. RSVP-TE Extensions for support of 1588

RSVP-TE signaling MAY be used to setup the PTP LSPs. A new RSVP object is defined to signal that this is a PTP LSP. The OFFSET to the start of the PTP message header MAY also be signaled. Implementations can trivially locate the correctionField (CF) location given this information. The OFFSET points to the start of the PTP header as a node may want to check the PTP messageType before it touches the correctionField (CF). The OFFSET is counted from TBD
The LSRs that receive and process the RSVP-TE/GMPLS messages MAY use the OFFSET to locate the start of the PTP message header.
Note that the new object/TLV Must be ignored by LSRs that are not compliant to this specification.
The new RSVP 1588_PTP_LSP object should be included in signaling PTP LSPs and is defined as follows:

```
        0             1             2             3
    +-------------+-------------+-------------+-------------+
    |      Length (bytes)       | Class-Num   |  C-Type     |
    +-------------+-------------+-------------+-------------+
    | Offset to locate the start of the PTP message header  |
    +-------------+-------------+-------------+-------------+
```
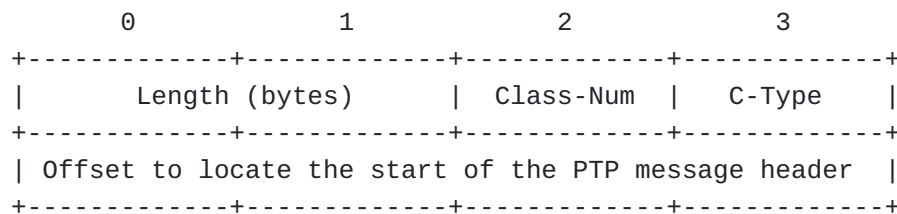
Figure 7: RSVP 1588_PTP_LSP object

The ingress LSR MUST include this object in the RSVP PATH Message. It is just a normal RSVP path that is exclusively set up for PTP messages

16. Behavior of LER/LSR

16.1. Behavior of 1588-aware LER

A 1588-aware LER advertises it's 1588-awareness via the OSPF procedure explained in earlier section of this specification. The 1588-aware LER then signals PTP LSPs by including the 1588_PTP_LSP object in the RSVP-TE signaling.
When a 1588 message is received from a non-MPLS interface, the LER MUST redirect them to a previously established PTP LSP. When a 1588 over MPLS message is received from an MPLS interface, the processing is similar to 1588-aware LSR processing.

16.2. Behavior of 1588-aware LSR

1588-aware LSRs are LSRs that understand the 1588_PTP_LSP RSVP object
and can perform 1588 processing (e.g. Transparent Clock processing).
A 1588-aware LSR advertises it's 1588-awareness via the OSPF procedure
explained in earlier section of this specification.
When a 1588-aware LSR distributes a label for PTP LSP, it maintains
this information. When the 1588-aware LSR receives an MPLS packet, it
performs a label lookup and if the label lookup indicates it is a PTP
label then further parsing must be done to positively identify that the
payload is 1588 and not OAM, BFD or control and management. Ruling out
non-1588 messages can easily be done when parsing indicates the
presence of GAL, ACH or VCCV (Type 1, 2, 3) or when the UDP port number
does not match one of the 1588 UDP port numbers.
After a 1588 message is positively identified in a PTP LSP, the PTP
message type indicates whether any timestamp processing is required.
After 1588 processing the packet is forwarded as a normal MPLS packet
to downstream node.

16.3. Behavior of non-1588-aware LSR

It is most beneficial that all LSRs in the path of a PTP LSP be 1588-
aware LSRs. This would ensure the highest quality time and clock
synchronization by 1588 Slave Clocks. However, this specification does
not mandate that all LSRs in path of a PTP LSP be 1588-aware.
Non-1588-aware LSRs are LSRs that either don't have the capability to
process 1588 packets (e.g. perform Transparent Clock processing) or
don't understand the 1588_PTP_LSP RSVP object.
Non-1588-aware LSRs ignore the RSVP 1588_PTP_LSP object and just switch
the MPLS packets carrying 1588 messages as data packets and don't
perform any timestamp related processing. However as explained in QoS
section the 1588 over MPLS packets MUST be still be treated with the
highest priority.

17. Other considerations

The use of Explicit Null (Label= 0 or 2) is acceptable as long as
either the Explicit Null label is the bottom of stack label (applicable
only to UDP/IP encapsulation) or the label below the Explicit Null
label is a PTP label.
The use of Penultimate Hop Pop (PHP) is acceptable as long as either
the PHP label is the bottom of stack label (applicable only to UDP/IP
encapsulation) or the label below the PHP label is a PTP label.

18. Security Considerations

MPLS PW security considerations in general are discussed in [RFC3985]
and [RFC4447],and those considerations also apply to this document.

An experimental security protocol is defined in [IEEE]. The PTP security extension and protocol provides group source authentication, message integrity, and replay attack protection for PTP messages.

19. Acknowledgements

The authors would like to thank Luca Martini, Ron Cohen, Yaakov Stein, Tal Mizrahi and other members of the TICTOC WG for reviewing and providing feedback on this draft.

20. IANA Considerations

20.1. IANA Considerations for OSPF

IANA has defined a sub-registry for the sub-TLVs carried in an OSPF TE Link TLV (type 2). IANA is requested to assign a new sub-TLV codepoint for the 1588aware capability sub-TLV carried within the Router Link TLV.

```
   Value            Sub-TLV                   References
   -----      ----------------------         ----------
    TBD       1588aware node sub-TLV     (this document)
```

20.2. IANA Considerations for IS-IS

IANA has defined a sub-registry for the sub-TLVs carried in the IS-IS Extended IS Reacability TLV. IANA is requested to assign a new sub-TLV code-point for the 1588aware capability sub-TLV carried within the Extended IS Reacability TLV.

```
   Value            Sub-TLV                   References
   -----      ----------------------         ----------
    TBD       1588aware node sub-TLV     (this document)
```

20.3. IANA Considerations for RSVP

IANA is requested to assign a new Class Number for 1588 PTP LSP object that is used to signal PTP LSPs.
1588 PTP LSP Object
Class-Num of type 11bbbbbb
Suggested value TBD
Defined CType: 1 (1588 PTP LSP)

21. References

21.1. Normative References

[IEEE]	, , "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", .
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC4720]	Malis, A., Allan, D. and N. Del Regno, "Pseudowire Emulation Edge-to-Edge (PWE3) Frame Check Sequence Retention", RFC 4720, November 2006.
[RFC5884]	Aggarwal, R., Kompella, K., Nadeau, T. and G. Swallow, "Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)", RFC 5884, June 2010.
[RFC4448]	Martini, L., Rosen, E., El-Aawar, N. and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, April 2006.
[RFC4389]	Thaler, D., Talwar, M. and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, April 2006.
[RFC5085]	Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, December 2007.
[RFC5880]	Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, June 2010.
[RFC3985]	Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.
[RFC4447]	Martini, L., Rosen, E., El-Aawar, N., Smith, T. and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

21.2. Informative References

[I-D.ietf-pwe3-fat-pw]	Bryant, S, Filsfils, C, Drafz, U, Kompella, V, Regan, J and S Amante, "Flow Aware Transport of Pseudowires over an MPLS Packet Switched Network", Internet-Draft draft-ietf-pwe3-fat-pw-07, July 2011.
[RFC1195]	Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.
[RFC2328]	Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.
[RFC3784]	Smit, H. and T. Li, "Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)", RFC 3784, June 2004.
[RFC4970]	Lindem, A., Shen, N., Vasseur, JP., Aggarwal, R. and S. Shaffer, "Extensions to OSPF for Advertising Optional Router Capabilities", RFC 4970, July 2007.

[RFC4971]	Vasseur, JP., Shen, N. and R. Aggarwal, "Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information", RFC 4971, July 2007.
[RFC5340]	Coltun, R., Ferguson, D., Moy, J. and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.
[RFC3630]	Katz, D., Kompella, K. and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, September 2003.
[RFC5329]	Ishiguro, K., Manral, V., Davey, A. and A. Lindem, "Traffic Engineering Extensions to OSPF Version 3", RFC 5329, September 2008.
[RFC5305]	Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, October 2008.
[RFC5120]	Przygienda, T., Shen, N. and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, February 2008.
[ISO]	, , "Intermediate system to Intermediate system routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)", .

Authors' Addresses

Shahram Davari Davari Broadcom Corp. San Jose, CA, 95134 USA EMail: davari@broadcom.com

Amit Oren Oren Broadcom Corp. San Jose, CA, 95134 USA EMail: amito@broadcom.com

Manav Bhatia Bhatia Alcatel-Lucent Bangalore, India EMail: manav.bhatia@alcatel-lucent.com

Peter Roberts Roberts Alcatel-Lucent Kanata, Canada EMail: peter.roberts@alcatel-lucent.com

Laurent Montini Montini Cisco Systems San Jose CA, USA EMail: lmontini@cisco.com