TICTOC Working Group	S. Davari	
Internet-Draft	A. Oren	
Intended status: Standards Track	Broadcom Corp.	
Expires: July 30, 2011	L. Martini	
	Cisco Systems	
	M. Bhatia	
	P. Roberts	
	Alcatel-Lucent	
	January 26, 2011	

TOC

Transporting PTP messages (1588) over MPLS Networks
draft-ietf-tictoc-1588overmpls-00

Abstract

This document defines the method for transporting PTP messages (PDUs) over an MPLS network to enable a proper handling of these packets (e.g. implementation of Transparent Clocks (TC)) in 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

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 http://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 July 30, 2011.

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

1. Introduction

TOC

The objective of Precision Time Protocol (PTP) is to synchronize independent clocks running on separate nodes of a distributed system. [IEEE] (IEEE 1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .) defines PTP messages for clock and time synchronization. The PTP messages include PTP PDUs over UDP/IP (Annex D & E of [IEEE] (IEEE 1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .)) and PTP PDUs over Ethernet (Annex F of [IEEE] (IEEE 1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .)). This document defines mapping

and transport of the PTP messages defined in [IEEE] (IEEE 1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .) over MPLS networks.
PTP defines intermediate clock functions (called transparent clocks) between the source of time (Master) and the Slave clocks. Boundary Clocks (BC) form Master-Slave hierarchy with the Master clock as root. The messages related to synchronization, establishing the Master-Slave hierarchy, and signaling, terminate in the protocol engine of a boundary clock and are not forwarded. Management messages however, are forwarded to other ports on the boundary clock.
Transparent clocks modify a "correction field" (CF) within the synchronization messages to compensate for residence and propagation delays. Transparent clocks do not terminate synchronization, Master-Slave hierarchy control messages or signaling messages.
There is a need to transport PTP messages over MPLS networks. The MPLS network could be a transit network between 1588 Masters and Slaves. The accuracy of the recovered clock improves and the Slave logic simplifies when intermediate nodes (e.g. LSRs) properly handle PTP messages (e.g. perform TC), otherwise the jitter at the 1588 Slave may be excessive and therefore the Slave may not be able to properly recover the clock and time of day.
This document defines a "1588-aware LSR" that is able to identify 1588 timing flows carried over MPLS.
Transparent Clock (TC) function requires a 1588-aware LSR in the middle of an LSP to identify the PTP messages and perform proper update of the CF, via a 1-step or 2-step process.
More generally this document requires that an LSR should be able to properly handle the PTP messages. For instance for those cases when the TC function is not viable (e.g. due to layer violation) as an alternative it should be possible to instead control the delay for these messages on both directions across the node.
In the above cases it is beneficial that PTP packets can be easily identified when carried over MPLS.
This document provides two methods for transporting PTP messages over MPLS. The main objectives are for LSRs to be able to deterministically detect and identify the PTP messages.

---

2. Terminology

TOC

1588: The timing and synchronization as defined by IEEE 1588
PTP: The timing and synchronization protocol used by 1588
Master: The Source of 1588 Timing and clock
Slave: The Destination of 1588 Timing and clock that tries to follow the Master clock
OC: Ordinary Clock

TC: Transparent Clock, a time stamping method applied by intermediate nodes between Master and Slave
BC: Boundary Clock, is a node that recovers the Master clock via a Slave function and uses that clock as the Master for other Slaves
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

TOC

When PTP messages are transported over MPLS networks, there is a need for intermediate LSRs to detect such messages and perform proper processing (e.g. Transparent Clock (TC)). Note the TC processing could be in the form of 1-Step or 2-Step time stamping.
PTP messages over Ethernet or IP can always be tunneled over MPLS. However the 1588 over MPLS mapping defined in this document is applicable whenever MPLS LSRs are 1588-aware and the intention is for those LSRs to perform proper processing on these packets.
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 (HW) to do deep packet inspection at line rate. Even if one assumes a deep packet inspection HW at line rate 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) and LSRs don't know what is a PW's payload (Ethernet, ATM, FR, CES, etc). Even if one assumes only Ethernet PWs are permitted in an LSP, 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.

TOC

4. 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 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 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. Let's call these LSPs as the "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 and Slaves MAY be P2MP or P2P LSP while the PTP LSP between each Slave and Master SHOULD be P2P LSP. The PTP LSP between a Master and a Slave and the PTP LSP between the same Slave and Master 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.
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.
We should be selective about the kind of traffic that flows over PTP LSPs as these will be handled as a special case by the LSR. The only LSP user plane traffic MUST be PTP, but the LSP MAY also carry essential MPLS/MPLS-TP control plane traffic such as BFD and LSP-Ping.

---

5. 1588 over MPLS Encapsulation

TOC

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.

5.1. 1588 over LSP Encapsulation

TOC

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.

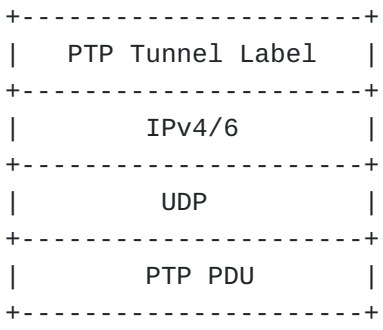

Figure 1 - 1588 over LSP Encapsulation

This encapsulation is very simple and is useful when the networks between 1588 Master and Slave 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] (IEEE 1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .).

5.2. 1588 over PW Encapsulation

TOC

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] (Martini, L., Rosen, E., El-Aawar, N., and G. Heron, “Encapsulation Methods for Transport of Ethernet over MPLS Networks,” April 2006.), 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.

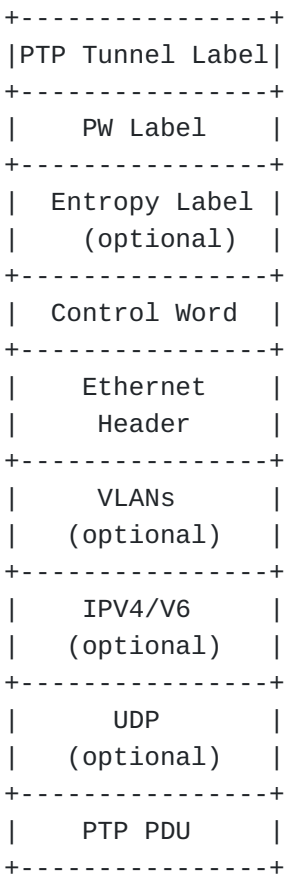

Figure 2 - 1588 over PW Encapsulation

The Control Word (CW) as specified in [RFC4448] (Martini, L., Rosen, E., El-Aawar, N., and G. Heron, “Encapsulation Methods for Transport of Ethernet over MPLS Networks,” April 2006.) 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.

An Entropy label [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 PSN,” October 2010.) MAY be present at the bottom of stack.

The Ethernet encapsulation of PTP MUST follow Annex F of [IEEE] (IEEE 1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .) and the UDP/IP encapsulation of PTP MUST follow Annex D and E of [IEEE] (IEEE

1588-2008, “IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” .).
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.

5.3. 1588 over pure MPLS mode

TOC

Editor Note: The encapsulation is general enough and can support transporting 1588 in a pure MPLS mode (i.e., without any IP/UDP or Ethernet headers). Should the WG pursue this?

---

6. 1588 Message Transport

TOC

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 TC 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 and Slave and MUST be transported over PTP LSPs. PDELAY_REQ and PDELAY_RESP are exchanged between adjacent routers and MAY be transported over single hop PTP LSPs. If Two Step Transparent clocks are present, then the FOLLOW_UP and DELAY_RESP 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 Transparent 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.

---

7. Protection and Redundancy

TOC

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 PTP LSP or PTP PW failure will trigger the slave to switch to the Redundant Master. 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 ensure the LSP/PW is ready for a future failure.
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 proper processing of PTP messages by LSRs in the backup path.

TOC

8. ECMP

To ensure the proper operation of 1588 Slaves, the physical path for PTP messages from Master to Slave 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.

---

9. OAM, Control and Management

TOC

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] (Katz, D. and D. Ward, “Bidirectional Forwarding Detection (BFD),” June 2010.), [RFC5884] (Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, “Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs),” June 2010.) and LSP-Ping [RFC4389] (Thaler, D., Talwar, M., and C. Patel, “Neighbor Discovery Proxies (ND Proxy),” April 2006.)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] (Nadeau, T. and C. Pignataro, “Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires,” December 2007.). In this case G-ACH, Router Alert Label (RAL), or PW label (TTL=1) are used to identify such management messages.

---

10. QoS Considerations

TOC

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.

TOC

11. FCS Recalculation

Ethernet FCS MUST be recalculated at every LSR that performs the TC processing and FCS retention described in [RFC4720] (Malis, A., Allan, D., and N. Del Regno, “Pseudowire Emulation Edge-to-Edge (PWE3) Frame Check Sequence Retention,” November 2006.) MUST not be used.

---

12. UDP Checksum Correction

TOC

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.

---

13. Routing extensions for 1588aware LSRs

TOC

MPLS-TE routing relies on extensions to OSPF [RFC2328] (Moy, J., “OSPF Version 2,” April 1998.) [RFC5340] (Coltun, R., Ferguson, D., Moy, J., and A. Lindem, “OSPF for IPv6,” July 2008.) and IS-IS [ISO] (ISO/IEC 10589:1992, “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),” .) [RFC1195] (Callon, R., “Use of OSI IS-IS for routing in TCP/IP and dual environments,” December 1990.) in order to advertise Traffic Engineering (TE) link information used for constraint-based routing. Indeed, it is useful to advertise data plane TE node 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 nodes that advertise themselves as 1588-aware, so that the PTP LSPs can be properly handled.
For this purpose, the following sections specify extensions to OSPF and IS-IS in order to advertise 1588 aware capabilities of a node.
Editor Note: There is an open issue on whether we must consider LSRs that may not want to support PTP on all ports. An example could be an LSR where a few blades have been upgraded to support PTP timestamping in silicon. In such cases, routers must explicitly indicate the ports that are 1588-aware. If the WG agrees about this then we will need to change the subsequent OSPF and IS-IS sections to advertise the 1588-aware capability on per port/interface basis, rather than per node as is current described.

13.1. 1588aware Node Capability for OSPF

TOC

This extension makes use of the Router Information (RI) Opaque LSA defined in [RFC4970] (Lindem, A., Shen, N., Vasseur, JP., Aggarwal, R., and S. Shaffer, "Extensions to OSPF for Advertising Optional Router Capabilities," July 2007.)for both OSPFv2 and OSPFv3, by defining a new OSPF Router Information (RI) TLV - The 1588-aware Capability TLV.
The 1588-aware Capability TLV is OPTIONAL and is defined as follows:

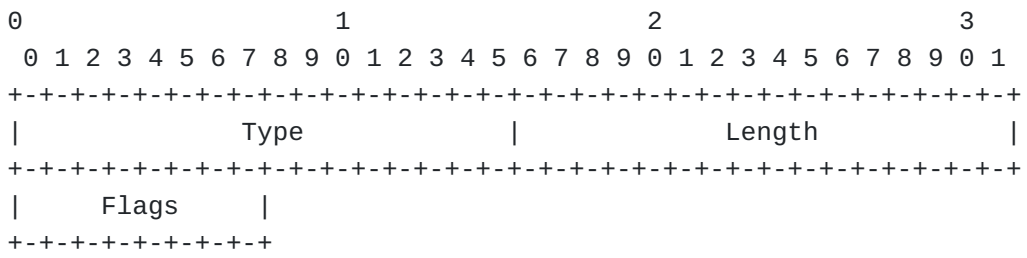

Figure 3: 1588-aware Capability TLV

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.

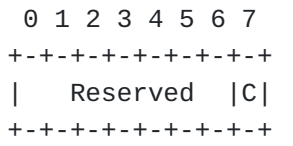

Figure 4: Flags Format

Correction (C) field Update field, 1 bit: Setting the C bit to 1 indicates that the node 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 node 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 TLV is applicable to both OSPFv2 and OSPFv3.
The 1588-aware Capability TLV MAY be advertised within an area-local or autonomous system (AS) scope Router Information (RI) LSA. But the 1588-

aware Capability TLV SHOULD NOT be advertised into an area in more than one RI LSA irrespective of the scope of the LSA.
The flooding scope is controlled by the Opaque LSA type in OSPFv2 and by the S1 and S2 bits in OSPFv3. For area scope, the 1588-aware Capability TLV MUST be carried within an OSPFv2 Type 10 RI LSA or an OSPFv3 RI LSA with the S1 bit set and S2 bit clear. If the flooding scope is the entire routing domain (AS scope), the 1588-aware Capability TLV MUST be carried within an OSPFv2 Type 11 RI LSA or OSPFv3 RI LSA with the S1 bit clear and the S2 bit set.

13.2. 1588aware Node Capability for IS-IS

TOC

Generic capability advertisement mechanisms for IS-IS are defined in [RFC4971] (Vasseur, JP., Shen, N., and R. Aggarwal, “Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information,” July 2007.). These allow a router to advertise its capabilities within an IS-IS area or an entire IS-IS routing domain. This document defines a new sub-TLV (named the 1588-aware Capability) to be carried within the IS-IS Router Capability TLV.
The IS-IS extensions defined in this document allow for discovering 1588-aware nodes within an IS-IS routing domain. Solutions for 1588-aware nodes discovery across AS boundaries are beyond the scope of this document, and are for further study.
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] (Smit, H. and T. Li, “Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE),” June 2004.). 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.

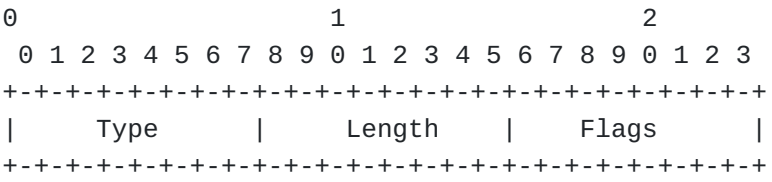

Figure 5: 1588-aware Capability sub-TLV

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.

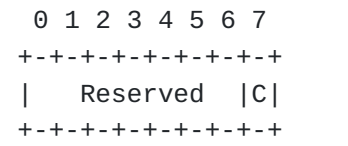

Figure 6: Flags Format

Correction (C) field Update field, 1 bit: Setting the C bit to 1 indicates that the node 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 node 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 sub-TLV is optional and is carried within an IS-IS Capability TLV [RFC4971] (Vasseur, JP., Shen, N., and R. Aggarwal, "Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information," July 2007.) to facilitate selection of 1588-aware nodes.
The flooding scope for 1588-aware node information advertised through IS-IS can be a single L1 area, an L1 area and the L2 sub-domain, or the entire IS-IS routing domain.

---

14. RSVP-TE Extensions for support of 1588

TOC

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 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:

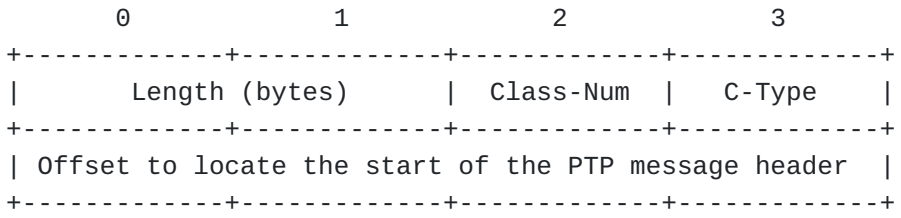

Figure 7: RSVP 1588_PTP_LSP object

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

15. Distributing PW labels

TOC

15.1. LDP extensions for distributing PW labels

TOC

TBD

15.2. BGP extensions for distributing PW labels

TOC

TBD

16. Behavior of LER/LSR

TOC

16.1. Behavior of 1588-aware LER

TOC

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

TOC

1588-aware LSRs are LSRs that understand the 1588_PTP_LSP RSVP object and can perform 1588 processing (e.g. TC 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 what type of processing (TC) if any 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

TOC

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 Slaves. 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. TC 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 TC processing. However as explained in QoS section the 1588 over MPLS packets MUST be still be treated with the highest priority.

---

17. Other considerations

TOC

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

TOC

MPLS PW security considerations in general are discussed in [RFC3985] (Bryant, S. and P. Pate, “Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture,” March 2005.) and [RFC4447] (Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, “Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP),” April 2006.),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. IANA Considerations

TOC

19.1. IANA Considerations for OSPF

TOC

IANA has defined a registry for TLVs carried in the Router Information LSA defined in [RFC4970] (Lindem, A., Shen, N., Vasseur, JP., Aggarwal, R., and S. Shaffer, “Extensions to OSPF for Advertising Optional Router Capabilities,” July 2007.). IANA is requested to assign a new TLV code-point for the PCED TLV carried within the Router Information LSA.

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

19.2. IANA Considerations for IS-IS

TOC

IANA has defined a registry for the sub-TLVs carried in the IS-IS Router Capability sub-TLVs defined in [RFC4971] (Vasseur, JP., Shen, N., and R. Aggarwal, “Intermediate System to Intermediate System (IS-

IS) Extensions for Advertising Router Information," July 2007.). IANA is requested to assign a new sub-TLV code-point for the 1588aware node sub-TLV carried within the Router Capability sub-TLV.

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

19.3. IANA Considerations for RSVP

TOC

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)

20. References

TOC

20.1. Normative References

TOC

[IEEE]	IEEE 1588-2008, "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 (TXT, HTML, XML).
[RFC3985]	Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture," RFC 3985, March 2005 (TXT).
[RFC4389]	Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)," RFC 4389, April 2006 (TXT).
[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 (TXT).
[RFC4448]	Martini, L., Rosen, E., El-Aawar, N., and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks," RFC 4448, April 2006 (TXT).
[RFC4720]	

	Malis, A., Allan, D., and N. Del Regno, “Pseudowire Emulation Edge-to-Edge (PWE3) Frame Check Sequence Retention,” RFC 4720, November 2006 (TXT).
[RFC5085]	Nadeau, T. and C. Pignataro, “Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires,” RFC 5085, December 2007 (TXT).
[RFC5880]	Katz, D. and D. Ward, “Bidirectional Forwarding Detection (BFD),” RFC 5880, June 2010 (TXT).
[RFC5884]	Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, “Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs),” RFC 5884, June 2010 (TXT).

20.2. Informative References

TOC

[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 PSN,” draft-ietf-pwe3-fat-pw-05 (work in progress), October 2010 (TXT).
[ISO]	ISO/IEC 10589:1992, “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).”
[RFC1195]	Callon, R., “Use of OSI IS-IS for routing in TCP/IP and dual environments,” RFC 1195, December 1990 (TXT, PS).
[RFC2328]	Moy, J., “OSPF Version 2,” STD 54, RFC 2328, April 1998 (TXT, HTML, XML).
[RFC3784]	Smit, H. and T. Li, “Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE),” RFC 3784, June 2004 (TXT).
[RFC4970]	Lindem, A., Shen, N., Vasseur, JP., Aggarwal, R., and S. Shaffer, “Extensions to OSPF for Advertising Optional Router Capabilities,” RFC 4970, July 2007 (TXT).
[RFC4971]	Vasseur, JP., Shen, N., and R. Aggarwal, “Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information,” RFC 4971, July 2007 (TXT).
[RFC5340]	Coltun, R., Ferguson, D., Moy, J., and A. Lindem, “OSPF for IPv6,” RFC 5340, July 2008 (TXT).

Authors' Addresses

TOC

	Shahram Davari
	Broadcom Corp.

	San Jose, CA 95134
	USA
Email:	davari@broadcom.com
	Amit Oren
	Broadcom Corp.
	San Jose, CA 95134
	USA
Email:	amito@broadcom.com
	Luca Martini
	Cisco Systems
	San Jose CA
	USA
Email:	lmartini@cisco.com
	Manav Bhatia
	Alcatel-Lucent
	Bangalore,
	India
Email:	manav.bhatia@alcatel-lucent.com
	Peter Roberts
	Alcatel-Lucent
	Kanata,
	Canada
Email:	peter.roberts@alcatel-lucent.com