MPLS-TP Linear Protection

draft-weingarten-mpls-tp-linear-protection-04.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 29, 2010.
Abstract

The MPLS Transport Profile (MPLS-TP) being specified jointly by IETF and ITU-T includes requirements documents and framework documents. The framework documents define the basic architecture that is needed in order to support various aspects of the required behavior. This document addresses the functionality described in the Survivability Framework document [11] and defines a protocol that may be used to fulfill the function of the Protection State Coordination for linear protection, as described in that document.
# Table of Contents

1. Introduction ................................................. 4  
   1.1. Contributing authors ................................ 5  
2. Conventions used in this document ............................. 5  
   2.1. Acronyms .............................................. 6  
   2.2. Definitions and Terminology ............................. 6  
3. Protection switching logic .................................... 6  
   3.1. Protection switching trigger mechanisms ................. 6  
   3.2. Protection switching control logical architecture ....... 7  
      3.2.1. PSC Status Module ................................. 8  
4. Protection state coordination (PSC) protocol .................. 8  
   4.1. Transmission and acceptance of PSC control packets ....... 9  
   4.2. Protocol format ....................................... 9  
      4.2.1. PSC Requests ..................................... 11  
      4.2.2. Path Fault Identifier ............................. 12  
      4.2.3. Active path indicator ............................. 12  
      4.2.4. Current Protection Type ........................... 12  
   4.3. Principles of Operation ................................ 13  
      4.3.1. PSC States ....................................... 13  
      4.3.2. Failure or Degraded condition (Working path) ..... 14  
      4.3.3. Lockout of Protection .............................. 15  
      4.3.4. Failure or Degraded condition (Recovery path) ..... 15  
      4.3.5. Operator Controlled Switching ..................... 16  
      4.3.6. Recovery from switching ............................ 17  
5. IANA Considerations .......................................... 18  
6. Security Considerations ...................................... 18  
7. Acknowledgements ........................................... 18  
8. References .................................................. 18  
   8.1. Normative References .................................. 18  
   8.2. Informative References ................................. 18  
Authors’ Addresses ............................................ 19
1. Introduction

As noted in the architecture for Multi-Protocol Label Switching Transport Profile (MPLS-TP) [7], the overall architecture framework for MPLS-TP is based on a profile of the MPLS and Pseudowire (PW) procedures as specified for the MPLS and (MS-)PW architectures defined in RFC 3031 [3], RFC 3985 [5] and [6]. One of the basic survivability functions, pointed out by the Survivability Framework document [11], is that of simple and rapid protection switching mechanisms for Label Switched Paths (LSP) and Pseudo-wires (PW).

Protection switching is a fully allocated survivability mechanism. It is fully allocated in the sense that the route and bandwidth of the recovery path is reserved for a selected working path. It provides a fast and simple survivability mechanism, that allows the network operator to easily grasp the active state of the network, compared to other survivability mechanisms.

As specified in the Survivability Framework document [11], protection switching is applied to a protection domain. For the purposes of this document, we define the protection domain of a P2P LSP as consisting of two Label Switching Relays (LSR) and the transport paths that connect them. For a P2MP LSP the protection domain includes the root (or source) LSR, the destination (or sink) LSRs, and the transport paths that connect them.

In 1+1 unidirectional architecture as presented in [11], a recovery transport path is dedicated to each working transport path. Normal traffic is bridged and fed to both the working and the recovery transport entities by a permanent bridge at the source of the protection domain. The sink of the protection domain selects which of the working or recovery entities to receive the traffic from, based on a predetermined criteria, e.g. server defect indication. When used for bidirectional switching the 1+1 protection architecture must also support a Protection State Coordination (PSC) protocol. This protocol is used to help synchronize the decisions of both ends of the protection domain in selecting the proper traffic flow.

In the 1:1 architecture, a recovery transport path is dedicated to the working transport path of a single service. However, the normal traffic is transmitted only once, on either the working or the recovery path, by using a selector bridge at the source of the protection domain. A selector at the sink of the protection domain then selects the path that carries the normal traffic. Since the source and sink need to be coordinated to ensure that the selector bridge at both ends select the same path, this architecture must support the PSC protocol.
The 1:n protection architecture extends this last architecture by sharing the recovery path amongst n services. Again, the recovery path is fully allocated and disjoint from any of the n working transport paths that it is being used to protect. The normal data traffic for each service is transmitted only once, either on the normal working path for that service or, in cases that trigger protection switching (as defined in [11]) may be sent on the recovery path. It should be noted that in cases where multiple working path services have triggered protection switching that some services, dependent upon their Service Level Agreement (SLA), may not be transmitted as a result of limited resources on the recovery path. In this architecture there is a need for coordination of the protection switching, and in addition there is need for resource allocation negotiation. Due to the added complexity of this architecture, the procedures for this will be delayed to a different document and further study.

As was pointed out in the Survivability Framework [11] and highlighted above, there is a need for coordination between the end-points of the protection domain when employing bidirectional protection schemes. This is especially true when there is a need to maintain traffic over a co-routed bidirectional LSP. This document presents a protocol and a set of procedures for activating this coordination within the protection domain.

1.1. Contributing authors

Hao Long (Huawei)

2. Conventions used in this document

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 RFC-2119 [1].
2.1. Acronyms

This draft uses the following acronyms:

+---------+----------------------------------------+
| DNR     | Do not revert                          |
| FS      | Forced Switch                          |
| GACH    | Generic Associated Channel Header      |
| LSR     | Label Switching relay                  |
| MPLS-TP | Transport Profile for MPLS             |
| MS      | Manual Switch                          |
| P2P     | Point-to-point                         |
| P2MP    | Point-to-multipoint                    |
| PDU     | Packet Data Unit                       |
| PSC     | Protection State Coordination Protocol |
| PST     | Path Segment Tunnel                    |
| SD      | Signal Degrade                         |
| SF      | Signal Fail                            |
| SLA     | Service Level Agreement                |
| WTR     | Wait-to-Restore                        |
+---------+----------------------------------------+

2.2. Definitions and Terminology

The terminology used in this document is based on the terminology defined in [10] and further adapted for MPLS-TP in [11]. In addition, we use the term LSR to refer to a MPLS-TP Network Element, whether it is a LSR, LER, T-PE, or S-PE.

3. Protection switching logic

3.1. Protection switching trigger mechanisms

The protection switching should be initiated in reaction to any of the following triggers:

- Server layer indication - if any of the lower layers (e.g. the physical layer) notifies the MPLS-TP layer that a failure has been detected.

- OAM signalling - if the OAM continuity and connectivity verification tools detect that there is a loss of continuity or mis-connectivity or the performance monitoring indicates a degradation of the utility of the working path for the current transport path. In cases of signal degradation, switching to the recovery path SHOULD only be activated if the recovery path can guarantee better conditions than the degraded working path.
Control plane - if there is a control plane active in the network (either signalling or routing), it MAY trigger protection switching based on conditions detected by the control plane. If the control-plane is based on GMPLS [13] then the recovery process should comply with the process described in [12].

Operator command - the network operator may issue commands that trigger protection switching. The commands that are supported include - Forced Switch, Manual Switch, Clear, Lockout of Protection, (see definitions in [10]).

3.2. Protection switching control logical architecture

Protection switching processes the triggers described above together with the inputs received from the far-end LSR. These inputs cause the LSR to take certain actions, e.g. switching the Selector Bridge to select the working or recovery path, and to transmit different protocol messages.

Figure 1: Protection switching control logic

Figure 1 describes the logical architecture of the protection
switching control. The Local Request logic unit accepts the triggers from the OAM, external operator commands, and from the local control plane (when present) and determines the highest priority request. This high-priority request is passed to both the PSC Message generator, that will generate the appropriate protocol message to be sent to the far-end LSR, and the Global Request logic, that will cross-check this local request with the information received from the far-LSR. The Global Request logic then processes these two PSC requests that determines the highest priority request that is passed to the PSC Process logic. The PSC Process logic uses this input to determine what actions need to be taken, e.g. switching the Selector Bridge, and the current status of the protection domain.

3.2.1. PSC Status Module

The PSC Control Logic must retain the status of the protection domain. The possible different states indicate the current status of the protection environment, and can be in one of three states:

- Normal (Idle) state - When both the recovery and the working paths are fully allocated and active, data traffic is being transmitted over the working path, and there are no events being reported within the domain.

- Protecting state - When either the working path has reported a signal failure or degradation of signal, or the operator has issued an operator command and the data traffic has been redirected to the recovery path.

- Unavailable state - When the recovery path is unavailable, either as a result of reporting a SF or SD condition, or as a result of an administrative Lockout command.

This state may affect the actions taken by the control logic, and therefore, the PSC Status Module transfers the current status to the Local Request Logic.

See section 4.3.1 for details on what actions are affected by the PSC state.

4. Protection state coordination (PSC) protocol

Bidirectional protection switching, as well as unidirectional 1:1 protection, requires coordination between the two end-points in determining which of the two possible paths, the working or recovery path, is operational in any given situation. When protection switching is triggered as described in section 3.1, the end-points
must inform each other of the switch-over from one path to the other in a coordinated fashion.

There are different possibilities for the type of coordinating protocol. One possibility is a two-phased coordination in which the MEP that is initiating the protection switching sends a protocol message indicating the switch but the actual switch-over is performed only after receiving an ‘Ack’ from the far-end MEP. The other possibility is a single-phased coordination, in which the initiating MEP switches over to the alternate path and informs the far-end of the switch, and the far-end must complete the switch-over.

In the following sub-sections we describe the protocol messages that should be used between the two end-points of the protection domain.

For the sake of simplicity of the protocol, this protocol is based on the single-phase approach described above.

4.1. Transmission and acceptance of PSC control packets

The PSC control packets should be transmitted over the recovery path only. This allows the transmission of the messages without affecting the normal traffic in the most prevalent case, i.e. the idle state. In addition, limiting the transmission to a single path avoids possible conflicts and race conditions that could develop if the PSC messages were sent on both paths.

A new PSC control packets must be transmitted immediately when a change in the transmitted status occurs.

The first three PSC packets should be transmitted as fast as possible only if the PSC information to be transmitted has been changed so that fast protection switching is possible even if one or two PSC packets are lost or corrupted. For protection switching within 50ms, the interval of the first three PSC signals should be 3.3ms. PSC packets after the first three should be transmitted with an interval of 5 seconds.

If no valid PSC specific information is received, the last valid received information remains applicable. In the event a signal fail condition is detected on the protection transport entity, the received PSC specific information should be evaluated.

4.2. Protocol format

The protocol messages SHALL be sent over the GACH as described in [8]. There is a single channel type for the set of PSC messages, each message will be identified by the first field of the ACH payload.
as described below. PSC messages SHOULD support addressing by use of the method described in [8]. The following figure shows the format for the full PSC message.

```
  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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 1|0 0 0 0|0 0 0 0 0 0 0 0|   MPLS-TP PSC Channel Code   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                         ACH TLV Header |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Addressing TLV                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   PSC Control Packet                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Format of PSC packet with a GACH header

Where:

- **MPLS-TP PSC Channel Code** is the GACH channel number assigned to the PSC = TBD
- **The ACH TLV Header** is described in [8]
- **The use of the Addressing TLV** are for further study
- **The following figure shows the format of the PSC Control message** that is the payload for the PSC packet.

Editor’s note: There is a suggestion that this format should be aligned with the format used by G.8031/G.8131/Y.1731 in ITU. The argument being that this would make it easier to pass review from ITU and allow easier transfer of technology.

The counter-argument is that the ITU format is based upon an attempt to find a common format for different functionality and therefore involves different fields that are not necessary for the protection switching. Defining a new dedicated format would make for a simpler and more intuitive protocol. End of editor’s note.
Where:

- **Ver**: is the version of the protocol, for this version the value SHOULD be 0.
- **Request**: this field indicates the specific PSC request that is being transmitted, the details are described in section 4.1.1.
- **Typ**: indicates the type of protection scheme currently supported, more details are given in section 4.1.4.
- **FPath**: used to indicate the path that is reporting a failure condition, the possible values are described in section 4.1.2.
- **Path**: used to indicate the currently active path, possible values are described in section 4.1.3.
- **Rsv, Reserved**: these fields are reserved for possible future use. These bits MUST be set to zero on transmission, and ignored upon reception.

### 4.2.1. PSC Requests

The Protection Switching Coordination (PSC) protocol SHALL support the following request types, in order of priority from highest to lowest:

- (1111) Clear
- (1110) Lockout protection
- (1101) Forced switch
- (0110) Signal fault
- (0101) Signal degrade
- (0100) Manual switch
(0011) Wait to restore
(0010) Do not revert (DNR)
(0000) No request

See section 6.3 for a description of the operation of the different requests.

4.2.2. Path Fault Identifier

The Fpath field of the PSC control SHALL be used only in a Signal fault (0101) or Signal degrade (0100) control packet. Its value indicates on which path the signal anomaly was detected. The following are the possible values:

- 0: indicates that the fault condition is on the Recovery path
- 1: indicates that the fault condition is on the Working path
- 2-255: for future extensions

4.2.3. Active path indicator

The Path field of the PSC control SHALL be used to indicate which path the source MEP is currently using for data transmission. The MEP should compare the value of this bit with the path that is locally selected for data transmission to verify that there is no inconsistency between the two end-points of the protected domain. If an inconsistency is detected then an alarm should be raised. The following are the possible values:

- 0: indicates that normal traffic is being transmitted on the Working path.
- 1: indicates the Recovery path is being used to transmit the normal traffic from the Working path.
- 2-255: for future extensions

4.2.4. Current Protection Type

The Typ field indicates the currently configured protection architecture type, this should be validated to be consistent for both ends of the protected domain. If an inconsistency is detected then an alarm should be raised. The following are the possible values:
4.3. Principles of Operation

In all of the following sub-sections, assume a protected domain between LSR-A and LSR-Z, using paths W (working) and R (recovery).

4.3.1. PSC States

4.3.1.1. Normal State

When the protected domain has no special condition in effect, the ingress LSR SHOULD forward the user data along the working path, and, in the case of 1+1 protection, the Permanent Bridge will bridge the data to the recovery path as well. The receiving LSR SHOULD read the data from the working path.

The ingress LSR MAY transmit a No Request PSC packet with the Path field set to 0 for the recovery path.

4.3.1.2. Protecting State

When the protection mechanism has been triggered and the protected domain has performed a protection switch, the domain is in the protecting state. In this state the normal traffic is transmitted and received on the recovery path.

If the protection domain is currently in a protecting state, then the LSRs SHOULD NOT accept a Manual Switch request.

If the protection domain is currently in a protecting state, and a Forced Switch is requested then the normal traffic SHALL continue to be transmitted on the recovery path even if the original protection trigger is cleared, and the Forced Switch condition will be signalled by the PSC messages.

4.3.1.3. Unavailable State

When the recovery path is unavailable — either as a result of a Lockout operator command (see section 4.3.3), or as a result of a SF or SD detected on the recovery path (see section 4.3.4) — then the protection domain is in the unavailable state. In this state, the
normal traffic is transmitted and received on the working path.

While in unavailable state any event that would trigger a protection switching SHOULD be ignored with the following exception - If a Signal Degrade request is received, then protection switching will be activated only if the recovery path can guarantee a better signal than the working path.

The protection domain will exit the unavailable state and revert to the normal state when, either the operator clears the Lockout command or the recovery path recovers from the signal fault or degraded situation. Both ends will resume sending the PCS packets over the recovery path, as a result of this recovery.

4.3.2. Failure or Degraded condition (Working path)

If one of the LSRs (for example, LSR-A) detects a failure condition or a serious degradation condition on the working path that warrants invoking protection switching, then it SHOULD take the following actions:

- Switch all traffic for LSR-Z to the recovery path only.
- Transmit a PCS control packet, using GACH, with the appropriate Request code (either Signal fault or Signal degrade), the Fpath set to 1, to indicate that the fault/degrade was detected on the working path, and the Path set to 0, indicating that normal traffic is now being transmitted on the recovery path.
- Verify that LSR-Z replies with a PCS control packet indicating that it has switched to the recovery path. If this is not received after xxx then send an alarm to the management system.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has switched, it SHOULD perform the following actions:

- Check priority of the request
- Switch all traffic addressed to LSR-A to the recovery path only.
- Begin transmission of a PCS control packet, using GACH, with the appropriate Request code (either Signal fault or Signal degrade), the Fpath set to 1, to indicate that the fault/degrade was detected on the working path, and the Path set to 1, indicating that traffic is now being transmitted on the recovery path.
4.3.3. Lockout of Protection

If one of the LSRs (for example, LSR-A) receives a management command indicating that the protection is disabled, then it SHOULD indicate this to the far-end LSR (for example, LSR-Z) that it is not possible to use the recovery path. The following actions MUST be taken:

- Transmit a PCS control packet, using GACH, with the Request code set to Lockout of protection (1110), the Fpath set to 0, and the Path set to 0.

- All normal traffic packets should be transmitted on the working path only.

- Verify that the far-end LSR (for example LSR-Z) is forwarding the data packets on the working path. Raise alarm in case of mismatch.

- The PSC control logic should go into Unavailable state.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has switched, it SHOULD perform the following actions:

- Check priority of request

- Switch all normal traffic addressed to LSR-A to the working path only.

- The PSC control logic should go into Unavailable status.

- Begin transmission of a PCS control packet, using GACH, with the appropriate Request code (Lockout of protection), the Fpath set to 0, and the Path set to 0, indicating that traffic is now being transmitted on the working path only.

4.3.4. Failure or Degraded condition (Recovery path)

If one of the LSRs (for example, LSR-A) detects a failure condition or a serious degradation condition on the recovery path, then it SHOULD take the following actions:

- Begin transmission of a PCS control packet with the appropriate Request code (either Signal fault or Signal degrade), the Fpath set to 0, to indicate that the fault/degrade was detected on the recovery path, and the Path set to 0, indicating that traffic is now being forwarded on the working path. Note that this will actually reach the far-end if this is a unidirectional fault or
A recovery path is possibly in a degraded situation.

- The PSC control logic should go into Unavailable state.
- All traffic MUST be transmitted on the working path for the duration of the SF/SD condition.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has become Unavailable, it SHOULD perform the following actions:

- Transmit all traffic on the working path for the duration of the SF/SD condition
- The PSC Control logic should go into Unavailable state.

### 4.3.5. Operator Controlled Switching

If the management system indicated to one of the LSRs (for example LSR-A) that a switch is necessary, e.g. either a Forced Switch or a Manual Switch, then the LSR SHOULD switch the traffic to the recovery path and perform the following actions:

- Switch all data traffic to the recovery path only.
- Transmit a PCS control packet, using GACH, with the appropriate Request code (either Manual switch or Forced switch), the Fpath set to 0, to indicate that the fault/degrade was detected on the working path, and the Path set to 1, indicating that traffic is now being forwarded on the recovery path.
- Verify that LSR-Z replies with a PCS control packet indicating that it has switched to the recovery path. If this is not received after xxx then send an alarm to the management system.

When the far-end LSR (in this example LSR-Z) receives the PCS packet informing it that other LSR (LSR-A) has switched, it SHOULD perform the following actions:

- Check priority of the request
- Switch all normal traffic addressed to LSR-A to the recovery path only.
- Begin transmission of a PCS control packet, using GACH, with the appropriate Request code (either Manual switch of Forced switch), the Fpath set to 1, to indicate that the fault/degrade was detected on the working path, and the Path set to 1, indicating
that traffic is now being forwarded on the recovery path.

4.3.5.1. Clearing operator commands

The operator may clear the switching condition by issuing a Clear request. This command will cause immediate recovery from the switch that was initiated by any of the previous operator commands, i.e. Forced Switch or Manual Switch. In addition, a Clear command after a Lockout Protection command should clear the Unavailable state and return the protection domain to the normal state.

If the Clear request is issued in the absence of a Manual Switch, Forced Switch, or Lockout protection, then it SHALL be ignored. In the presence of any of these commands, the Clear request SHALL clear the state affected by the operator command.

4.3.6. Recovery from switching

When the condition that triggered the protection switching clears, e.g. the cause of the failure condition has been corrected, or the operator clears a Manual Switch, then the protection domain SHOULD follow the following procedures:

- If the network is configured for non-revertive behaviour, then the two LSRs SHOULD transmit DNR (Request code 0010) messages.
- If the network is recovering from an operator switching command (in revertive mode), then both LSRs SHOULD return to using the working transport path and transmit No request (Request code 0000) messages.
- If the network is recovering from a failure or degraded condition (in revertive mode), then the LSR that detects this recovery SHALL activate a local Wait-to-restore (WTR) timer (see section 4.3.6.1) to verify that there is not an intermittent failure. After the WTR expires, the LSR SHOULD return to using the working transport path and transmit No request (Request code 0000) messages.

4.3.6.1. Wait-to-restore timer

In revertive mode, in order to prevent frequent activation of protection switching due to an intermittent defect, the working transport path must become stable and fault-free before reverting to the normal condition. In order to verify that this is the case a fixed period of time must elapse before the normal traffic uses the working transport path. This period, called the WTR period, should be configurable by the operator in 1-minute intervals within the range 1-12 minutes. The default value is 5 minutes.
During this period, if a failure condition is detected on the working transport path, then the WTR timer is cleared and the normal traffic SHALL continue to be transported over the recovery transport path. If the WTR timer expires without being pre-empted by a failure, then the traffic SHOULD be returned to use the working transport path (as above).

5. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Security Considerations

This document does not by itself raise any particular security considerations.

7. Acknowledgements

The authors would like to thank all members of the teams (the Joint Working Team, the MPLS Interoperability Design Team in IETF and the T-MPLS Ad Hoc Group in ITU-T) involved in the definition and specification of MPLS Transport Profile.

8. References

8.1. Normative References


8.2. Informative References


Authors’ Addresses

Stewart Bryant (editor)
Cisco
United Kingdom

Email: stbryant@cisco.com