MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 07, 2013

H. van Helvoort, Ed.
Huawei Technologies
J. Ryoo, Ed.
ETRI
H. Zhang
Huawei Technologies
F. Huang
Alcatel-Lucent Shanghai Bell
H. Li
China Mobile
A. D'Alessandro
Telecom Italia
May 06, 2013

Linear Protection Switching in MPLS-TP
draft-zulr-mpls-tp-linear-protection-switching-07.txt

Abstract

This document specifies a linear protection switching mechanism for MPLS-TP. This mechanism supports 1+1 unidirectional/bidirectional protection switching and 1:1 bidirectional protection switching. It is purely supported by MPLS-TP data plane, and can work without any control plane.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunications Union Telecommunications Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network as defined by the ITU-T.

Status of This Memo

This Internet-Draft will expire on November 07, 2013.

Copyright Notice

Table of Contents

1. Introduction

MPLS-TP is defined as transport profile of MPLS technology to fulfill the deployment in transport network. A typical feature of transport network is that it can provide fast protection switching for end-to-end or segments. The protection switching time is generally required to be less than 50ms according to the strictest requirement of services such as voice, private line, etc.

The goal of linear protection switching mechanism is to satisfy the requirement of fast protection switching for MPLS-TP network. Linear protection switching means that, for one or more working transport entities, there is one protection transport entity, which is disjoint from any of working transport entities, ready for taking over the service transmission when a working transport entity failed.

This document specifies 1+1 unidirectional protection switching mechanism for unidirectional transport entity (either point-to-point or point-to-multipoint) as well as bidirectional point-to-point transport entity, and 1+1/1:1 bidirectional protection switching mechanism for point-to-point bidirectional transport entity. Since bidirectional protection switching needs the coordination of the two endpoints of the transport entity, this document also specifies APS (Automatic Protection Switching) protocol details which is used for this purpose.

The linear protection mechanism described in this document is applicable to both LSPs and PWs.

The APS protocol specified in this document is based on the same principles and behavior of the APS protocol designed for SONET/SDH networks (i.e., it is mature and proven) and provides commonality with the established operation models utilized in other transport network technologies (e.g., SDH/SONET and OTN).

It is also worth noting that multi-vendor implementations of the APS protocol described in this document already exist.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunications Union Telecommunications Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network as defined by the ITU-T.

2. Linear protection switching overview

To guarantee the protection switching time, for a working transport entity, its protection transport entity is always pre-configured before the failure occurs. Normally, the normal traffic will be transmitted and received on the working transport entity. The switching to protection transport entity is usually triggered by link /node failure, external commands, etc. Note that external commands are often used in transport network by operators, and they are very useful in cases of service adjustment, path maintenance, etc.

2.1. Protection architecture types

2.1.1. 1+1 architecture

In the 1+1 architecture, a protection transport entity is associated with the working transport entity. The normal traffic is permanently bridged onto both the working transport entity and the protection transport entity at the source endpoint of the protected domain. The normal traffic on working and protection transport entities is transmitted simultaneously to the sink endpoint of the protected domain where a selection between the working and protection transport entity is made, based on predetermined criteria, such as signal fail and signal degrade indications.

2.1.2. 1:1 architecture

In the 1:1 architecture, a protection transport entity is associated with the working transport entity. When the working transport entity is determined to be impaired, the normal traffic must be transferred from the working to the protection transport entity at both the source and sink endpoints of the protected domain. The selection between the working and protection transport entities is made based on predetermined criteria, such as signal fail and signal degrade indications from the working or protection transport entity.

The bridge at source endpoint can be realized in two ways: it is either a selector bridge or a broadcast bridge. With a selector bridge the normal traffic is connected either to the working transport entity or the protection transport entity. With a broadcast bridge the normal traffic is permanently connected to the working transport entity, and in case a protection switch is active also to the protection transport entity. Broadcast bridge is recommended to be used in revertive mode only.

2.1.3. 1:n architecture

Details for the 1:n protection switching architecture will be provided in a future version of this draft.

It is worth noting that the APS protocol defined here is ready to support 1:n operations.

2.2. Protection switching type

The linear protection switching types can be a unidirectional switching type or a bidirectional switching type.

o Unidirectional switching type: Only the affected direction of working transport entity is switched to protection transport entity; the selectors at each endpoint operate independently. This switching type is recommended to be used for 1+1 protection in this document.

o Bidirectional switching type: Both directions of working transport entity, including the affected direction and the unaffected direction, are switched to protection transport entity. For bidirectional switching, automatic protection switching (APS) protocol is required to coordinate the two endpoints so that both have the same bridge and selector settings, even for a unidirectional failure. This type is applicable for 1+1 and 1:1 protection.

2.3. Protection operation type

The linear protection operation types can be a non-revertive operation type or a revertive operation type.

o Non-revertive operation: The normal traffic will not be switched back to the working transport entity even after a protection switching cause has cleared. This is generally accomplished by replacing the previous switch request with a "Do not Revert (DNR)" request, which has a low priority.

o Revertive operation: The normal traffic is restored to the working transport entity after the condition(s) causing the protection switching has cleared. In the case of clearing a command (e.g., Forced Switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of a "Wait-to-Restore (WTR)" timer, which is used to avoid chattering of selectors in the case of intermittent defects.

3. Protection switching trigger conditions

3.1. Fault conditions

Fault conditions mean the requests generated by the local OAM function.

- Signal Failure (SF): If an endpoint detects a failure by OAM function or other mechanism, it will submit a local signal failure (local SF) to APS module to request a protection switching. The local SF could be on working transport entity or protection transport entity.

- Signal Degrade (SD): If an endpoint detects signal degrade by OAM function or other mechanism, it will submit a local signal failure (local SD) to APS module to request a protection switching. The local SD could be on working transport entity or protection transport entity.

3.2. External commands

The external command issues an appropriate external request on to the protection process.

3.2.1. End-to-end commands

These commands are applied to both local and remote nodes. When the APS protocol is present, these commands are signaled to the far end of the connection. In bidirectional switching, these commands affect the bridge and selector at both ends.

- Lockout of Protection (LO): This command is used to provide operator a tool for temporarily disabling access to the protection transport entity.

- Manual switch (MS): This command is used to provide operator a tool for temporarily switching normal traffic to working transport entity (MS-W) or protection transport entity (MS-P), unless a higher priority switch request (i.e., LP, FS, or SF) is in effect.

- Forced switch (FS): This command is used to provide operator a tool for temporarily switching normal traffic from working transport entity to protection transport entity, unless a higher priority switch request (i.e., LP) is in effect.

- Exercise (EXER): Exercise is a command to test if the APS communication is operating correctly. The EXER command will not affect the state of the protection selector and bridge.

o Clear: This command between management and local protection process is not a request sent by APS to other endpoints. It is used to clear the active near end external command or WTR state.

3.2.2. Local commands

These commands apply only to the near end (local node) of the protection group. Even when an APS protocol is supported, they are not signalled to the far end.

o Freeze: This command freezes the state of the protection group. Until the freeze is cleared, additional near end commands are rejected and condition changes and received APS information are ignored. When the Freeze command is cleared, the state of the protection group is recomputed based on the condition and received APS information.

   Because the freeze is local, if the freeze is issued at one end only, a failure of protocol can occur as the other end is open to accept any operator command or a fault condition.

o Clear Freeze: This command clears the local freeze.

4. Protection switching schemes

4.1. 1+1 unidirectional protection switching

```
      +-----------+                                       +-----------+
      |           |----------------------------------------|           |
      |          -+----------------------------------------+-          |
      |         / |----------------------------------------| \         |
      |        /  |        Working transport entity        |  \        |
   ---+------->   |                                        |   --------+->
      |        \  |                                        |           |
      |         \ |----------------------------------------|           |
      |          -+----------------------------------------|           |
      |  source   |----------------------------------------|    sink   |
      +-----------+        Protection transport entity    +-----------+
                              (normal condition)

      +-----------+                                       +-----------+
      |           |----------------------------------------|           |
      |          -+-------------------XX-------------------+           |
      |         / |----------------------------------------|           |
      |        /  |    Working transport entity (failure)  |           |
   ---|------->   |                                        |   --------+->
      |        \  |                                        |  /        |
      |         \ |----------------------------------------| /         |
```

```
      |          -+----------------------------------------+-          |
      |  source   |----------------------------------------|    sink   |
      +-----------+      Protection transport entity       +-----------+
                             (failure condition)
```

Figure 1: 1+1 unidirectional linear protection switching

1+1 unidirectional protection switching is the simplest protection switching mechanism. The normal traffic is permanently bridged on both the working and protection transport entities at the source endpoint of the protection domain. In normal condition, the sink endpoint receives traffic from working transport entity. If the sink endpoint detects a failure on working transport entity, it will switch to receive traffic from protection transport entity. 1+1 unidirectional protection switching is recommended to be used for unidirectional transport entity.

Note that 1+1 unidirectional protection switching does not need APS coordination protocol since it only perform protection switching based on the local request.

4.2. 1+1 bidirectional protection switching

```
      +-----------+                                        +-----------+
      |           |----------------------------------------|           |
      |          -+<---------------------------------------+-          |
      |         / +--------------------------------------->+ \         |
      | sink   / /|----------------------------------------|\ \   sink |
   <--+-------/ / |         working transport entity       | --\-------+->
   ---+--------->  |                                        |    <------+--
      | source  \ |                                        |   / Source|
      |          \|----------------------------------------|  /        |
      |           +--------------------------------------->| /         |
      |           |<---------------------------------------+-          |
      | APS <....................................................> APS |
      |           |----------------------------------------+           |
      +-----------+       Protection transport entity      +-----------+
                             (normal condition)

      +-----------+                                        +-----------+
      |           |----------------------------------------|           |
      |           +<-----------------XX--------------------+-          |
      |           +--------------------------------------->+ \         |
      |          /|----------------------------------------|  \        |
      | source  / |    working transport entity (failure)  |   \ source|
   ---+--------->  |                                        |    \<-----+--
   <--+-------  \ |                                        |  --/------+->
      | sink  \  \|----------------------------------------| / /  sink |
```

```
      |        \  +--------------------------------------->+- /        |
      |         --+<---------------------------------------+-/         |
      | APS <....................................................> APS |
      |           |----------------------------------------+           |
      +-----------+       Protection transport entity      +-----------+
                               (failure condition)
```

Figure 2: 1+1 bidirectional linear protection switching

In 1+1 bidirectional protection switching, for each direction, the normal traffic is permanently bridged on both the working and protection transport entities at the source endpoint of the protection domain. In normal condition, for each direction, the sink endpoint receives traffic from working transport entity.

If the sink endpoint detects a failure on the working transport entity, it will switch to receive traffic from protection transport entity. It will also send an APS message to inform the sink endpoint on another direction to switch to receive traffic from protection transport entity.

APS mechanism is necessary to coordinate the two endpoints of transport entity and implement 1+1 bidirectional protection switching even for a unidirectional failure.

4.3. 1:1 bidirectional protection switching

```
      +-----------+                                        +-----------+
      |           |----------------------------------------|           |
      |          -+<---------------------------------------+-          |
      |         / +--------------------------------------->+ \         |
      | sink   / /|----------------------------------------|\ \  source|
   <--+-------/ / |         working transport entity       | \ <-------+--
   ---+-------->  |                                        |  ---------+->
      | source    |                                        |      sink |
      |           |----------------------------------------|           |
      |           |                                        |           |
      |           |                                        |           |
      | APS <....................................................> APS |
      |           |----------------------------------------|           |
      +-----------+       Protection transport entity      +-----------+
                             (normal condition)

      +-----------+                                        +-----------+
      |           |----------------------------------------|           |
      |           |                  \/                    |           |
      |           |                  /\                    |           |
      |           |----------------------------------------|           |
```

```
      | source    |    working transport entity (failure)  |      sink |
   ---+------->   |                                        |   --------+->
   <--+------- \  |                                        |  / <------+--
      | sink  \ \ |----------------------------------------| / / source|
      |        \ -+--------------------------------------->+- /        |
      |         --+<----------------------------------------+--         |
      | APS <....................................................> APS |
      |           |-----------------------------------------+           |
      +-----------+       Protection transport entity      +-----------+
                              (failure condition)
```

Figure 3: 1:1 bidirectional linear protection switching

In 1:1 bidirectional protection switching, for each direction, the source endpoint sends traffic on either working transport entity or protection transport entity. The sink endpoint receives the traffic from the transport entity where the source endpoint sends on.

In normal condition, for each direction, the source endpoint and sink endpoint send and receive traffic from working transport entity.

If the sink endpoint detects a failure on the working transport entity, it will switch to send and receive traffic from protection transport entity. It will also send an APS message to inform the sink endpoint on another direction to switch to send and receive traffic from protection transport entity.

APS mechanism is necessary to coordinate the two endpoints of transport entity and implement 1:1 bidirectional protection switching even for a unidirectional failure.

5. APS protocol

5.1. APS PDU format

APS packets MUST be sent over a G-ACh as defined in [RFC5586].

The format of APS PDU is specified in Figure 4 below.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |0 0 0 1|0 0 0 0|0 0 0 0 0 0 0 0|   Y.1731 Channel Type (0xXX)  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | MEL | Version |    OpCode     |     Flags     |   TLV Offset  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                  APS Specific Information                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
   |    End TLV    |
   +-+-+-+-+-+-+-+-+
```

Figure 4: APS PDU format

The following values shall be used for APS PDU:

o The Y.1731 Channel Type is set as defined in [BHH_MPLS-TP_OAM]

o MEL: set as defined in [BHH_MPLS-TP_OAM];

o Version: 0x00

o OpCode: 0d39 (=0x27)

o Flags: 0x00

o TLV Offset: 4

o End TLV: 0x00

The format of the APS-specific information is defined in Figure 5

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |Request|Pr.Type|   Requested   |    Bridged    | |             |
   |   /   |-+-+-+-|               |               |T|  Reserved(0)|
   | State |A|B|D|R|    Signal     |     Signal    | |             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: APS specific information format

All bits defined as "Reserved" shall be transmitted as 0 and ignored on reception.

o Request/State:

   The 4 bits indicate the protection switching request type. See Figure 6 for the code of each request/state type.

   In case that there are multiple protection switching requests, only the protection switching request with the highest priority will be processed.

```
       +-------------------------------------+---------------+
       |             Request/State           | code/priority |
       +-------------------------------------+---------------+
```

Lockout of Protection (LO)	1111 (highest)
Signal Fail for Protection (SF-P)	1110
Forced Switch (FS)	1101
Signal Fail for Working (SF-W)	1011
Signal Degrade	1001
Manual Switch	0111
Wait to Restore (WTR)	0101
Exercise (EXER)	0100
Reverse Request (RR)	0010
Do Not Revert (DNR)	0001
No Request (NR)	0000 (lowest)

Figure 6: Protection switching request code/priority

- Protection type (Pr.Type):

  The 4 bits are used to specify the protection type.

  A: reserved (set by default to 1)
  B: 0 - 1+1 (permanent bridge)
     1 - 1:1 (no permanent bridge)
  D: 0 - Unidirectional switching
     1 - Bidirectional switching
  R: 0 - Non-revertive operation
     1 - Revertive operation

- Requested signal:

  This byte is used to indicate the traffic that the near end requests to be carried over the protection entity.

  value = 0 Null traffic
  value = 1 Normal traffic 1
  value = 2~255 Reserved

- Bridged signal:

This byte is used to indicate the traffic that is bridged onto the protection entity.

value = 0 Null traffic
value = 1 Normal traffic 1
value = 2~255 Reserved

o Bridge Type (T):

This bit is used to further specify the type of non-permanent bridge for 1:1 protection switching.

value = 0 Selector bridge
value = 1 Broadcast bridge

o Reserved:

This field should be set to zero.

5.2. APS transmission

The APS message should be transported on protection transport entity by encapsulated with the protection transport entity label. If an endpoint receives APS-specific information from the working entity, it should ignore this information, and should detect the Failure of Protocol defect (see Section 6).

A new APS packet must be transmitted immediately when a change in the transmitted status occurs. The first three APS packets should be transmitted as fast as possible only if the APS information to be transmitted has been changed so that fast protection switching is possible even if one or two APS packets are lost or corrupted. The interval of the first three APS packets should be 3.3ms. APS packets after the first three should be transmitted with the interval of 5 seconds.

If no valid APS-specific information is received, the last valid received information remains applicable.

5.3. Hold-off timer

In order to coordinate timing of protection switches at multiple layers, a hold-off timer may be required. The purpose is to allow a server layer protection switch to have a chance to fix the problem before switching at a client layer.

Each protection group should have a provisioned hold-off timer. The suggested range of the hold-off timer is 0 to 10 seconds in steps of 100 ms (accuracy of +/-5 ms).

When a new defect or more severe defect occurs (new SF/SD) on the transport entity that currently carries traffic, this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the hold-off timer expires, it will be checked whether a defect still exists on the transport entity that started the timer. If it does, that defect will be reported to protection switching. The defect need not be the same one that started the timer.

This hold-off timer mechanism shall be applied for both working and protection transport entities.

6. Protection switching logic

```
            +-------------+ Persistent +----------+
SF,SD       | Hold-off    | fault      | Local    |
----------->| timer logic |----------->| request  |
            +-------------+            | logic    |
Other local requests ----------------->|          |
(LO, FS, MS, EXER, Clear)              +----------+
                                           |
                                           | Highest
                                           | local request
                                           |
Remote APS                                 V
Message       +-------+ Remote APS    +-----------------+
------------->|  APS  | request/state |  APS process    |
(received     | check |-------------->|  logic          |
from far end) +-------+               +-----------------+
                |   ^                   |            |
                |   |                   | Signaled   |
                |   |                   | APS        |
                |   | Txed              |            |
                |   | "Requested        V            |
                |   | signal"         +-----------+  |
                |   +-----------------| APS mess. |  |
                |                     | generator |  |
                |                     +-----------+  |
                |                       |            |
                V                       |            |
            Failure of                  V            |
            Protocol                  APS Message    |
```

```
                Detection                              V
                                                  Set local
                                                  bridge/selector
```

Figure 7: Protection Switching Logic

Figure 7 describes the protection switching logic.

One or more local protection switching requests may be active. The "local request logic" determines which of these requests is highest using the order of priority given in Figure 6. This highest local request information is passed on to the "APS process logic". Note that an accepted Clear command, clearance of SF(-P) or expiration of WTR timer shall not be processed by the local request logic, but shall be considered as the highest local request and submitted to the APS process logic for processing.

The remote APS message is received from the far end and is subjected to the validity check and mismatch detection in "APS check". Failure of Protocol situations are as follows:

- o The "B" field mismatch due to incompatible provisioning;
- o The reception of APS message from the working entity due to working/protection configuration mismatch;
- o No match in sent "Requested traffic" and received "requested signal" for more than 50 ms;
- o No APS message is received on the protection transport entity during at least 3.5 times the long APS interval (e.g. at least 17.5 seconds) and there is no defect on the protection transport entity.

Provided the "B" field matches:

- o If "D" bit mismatches, the bidirectional side will fall back to unidirectional switching.
- o If the "R" bit mismatches, one side will clear switches to "WTR" and the other will clear to "DNR". The two sides will interwork and the traffic is protected.
- o If the "T" bit mismatches, the side using a broadcast bridge will fall back to using a selector bridge.

The APS message with invalid information should be ignored, and the last valid received information remains applicable.

The linear protection switching algorithm commences immediately every time one of the input signals changes, i.e., when the status of any local request changes, or when a different APS specific information is received from the far end. The consequent actions of the algorithm are also initiated immediately, i.e., change the local bridge/selector position (if necessary), transmit a new APS specific information (if necessary), or detect the failure of protocol defect if the protection switching is not completed within 50 ms.

The state transition is calculated in the "APS process logic" based on the highest local request, the request of the last received "Request/State" information, and state transition tables defined in Section 7, as follows:

- If the highest local request is Clear, clearance of SF(-P) or of SD, or expiration of WTR, a state transition is calculated first based on the highest local request and state machine table for local requests to obtain an intermediate state. This intermediate state is the final state in case of clearance of SF-P otherwise, starting at this intermediate state, the last received far end request and the state machine table for far end requests are used to calculate the final state.

- If the highest local request is neither Clear, nor clearance of SF(-P) or of SD, nor expiration of WTR, the APS process logic compares the highest local request with the request of the last received "Request/State" information based on Figure 6.

    1. If the highest local request has higher or equal priority, it is used with the state transition table for local requests defined in Section 7 to determine the final state; otherwise

    2. The request of the last received "Request/State" information is used with the state transition table for far end requests defined in Annex A to determine the final state.

The "APS message generator" generates APS specific information with the signaled APS information for the final state from the state transition calculation (with coding as described in Figure 5).

7. Protection switching state transition table

In this section, state transition tables for the following protection switching configurations are described.

- 1:1 bidirectional (revertive mode, non-revertive mode);

- 1+1 bidirectional (revertive mode, non-revertive mode);

- 1+1 unidirectional (revertive mode, non-revertive mode).

Note that any other global or local request which is not described in state transition tables does not trigger any state transition.

The states specified in the state transition tables can be described as follows:

- No request: No Request is the state entered by the local priority under all conditions where no local protection switching requests (including wait-to-restore and do-not-revert) are active. NR can also indicates that the highest local request is overridden by the far end request, whose priority is higher than the highest local request. Normal traffic signal is selected from the corresponding transport entity.

- Lockout, Signal Fail(P): The access by the normal traffic to the protection transport entity is NOT allowed, due to the SF detected on the protection entity or due to the lockout of protection command applied. The normal traffic is carried by the working transport entity, regardless of the fault/degrade condition possibly present (due to the highest priority of the switching triggers leading to this state).

- Forced Switch, Signal Fail(W), Signal Degrade(W), Signal Degrade(P), Manual Switch: A switching trigger, NOT resulting in the protection transport entity unavailability is present. The normal traffic is selected either from the corresponding working transport entity or from the protection transport entity, according to the behaviour of the specific switching trigger.

- Wait to Restore: In revertive operation, after the clearing of an SF or SD on working transport entity, maintains normal traffic as selected from the protection transport entity until a wait-to-restore timer expires or another request with higher priority, including a clear command, is received. This is used to prevent frequent operation of the selector in the case of intermittent failures.

- Do not revert: In non-revertive operation, this is used to maintain a normal traffic to be selected from the protection transport entity.

- Exercise: Exercise of the APS protocol.

- Reverse Request: The near end will enter and signal Reverse Request only in response to an EXER from the far end.

[State transition tables are shown at the end of the PDF form of this document.]

8. Security considerations

To be added in a future version of the document.

9. IANA considerations

To be added in a future version of the document.

10. Acknowledgements

The authors would like to thank Hao Long, Vincenzo Sestito, Italo Busi, Igor Umansky for their input to and review of the current document.

11. References

11.1. Normative References

[RFC5317] Bryant, S. and L. Andersson, "Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile", RFC 5317, Feburary 2009.

[RFC5586] Bocci, M., Vigoureux, M., and S. Bryant, "MPLS Generic Associated Channel", RFC 5586, June 2009.

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[BHH_MPLS-TP_OAM] Busi, I., van Helvoort, H., and J. He, "MPLS-TP OAM based on Y.1731", draft-bhh-mpls-tp-oam-y1731-07 , July 2011.

11.2. Informative References

[RFC6372] Sprecher, N. and A. Farrel, "MPLS-TP Survivability Framework", RFC 6372, Sept 2011.

Appendix A. Operation examples of APS protocol

The sequence diagrams shown in this section are only a few examples of the APS operations. The first APS message which differs from the previous APS message is shown. The operation of hold-off timer is omitted. The fields whose values are changed during APS packet exchange are shown in the APS packet exchange. They are Request/

State, requested traffic, and bridged traffic. For an example, SF(0,1) represents an APS packet with the following field values: Request/State = SF, requested signal = 0, and bridged signal = 1. The values of the other fields remain unchanged from the initial configuration. The signal numbers 0 and 1 refer to null signal and normal traffic signal, respectively. W(A->Z) and P(A->Z) indicate the working and protection paths in the direction of A to Z, respectively.

Example 1. 1:1 bidirectional protection switching (revertive mode) - Unidirectional SF case

```
                 A                  Z
                 |                  |
             (1) |---- NR(0,0)----->|
                 |<----- NR(0,0)----|
                 |                  |
                 |                  |
             (2) | (SF on W(Z->A))  |
                 |---- SF(1,1)----->| (3)
                 |<----- NR(1,1)----|
             (4) |                  |
                 |                  |
             (5) | (Recovery)       |
                 |---- WTR(1,1)---->|
                /|                  |
       WTR timer |                  |
                \|                  |
             (6) |---- NR(0,0)----->| (7)
             (8) |<----- NR(0,0)----|
                 |                  |
```

(1) The protection domain is operating without any defect, and the working entity is used for delivering the normal traffic.

(2) Signal Fail occurs on the working entity in the Z to A direction. Selector and bridge of node A select protection entity. Node A generates SF(r=1, b=1) message.

(3) Upon receiving SF(r=1, b=1), node Z sets selector and bridge to protection entity. As there is no local request in node Z, node Z generates NR(r=1, b=1) message.

(4) Node A confirms that the far end is also selecting protection entity.

(5) Node A detects clearing of SF condition, starts the WTR timer, and sends WTR(r=1, b=1) message.

(6) At expiration of the WTR timer, node A sets selector and bridge to working entity and sends NR(r=0, b=0) message.

(7) Node Z is notified that the far end request has been cleared, and sets selector and bridge to working entity.

(8) It is confirmed that the far end is also selecting working entity.

Example 2. 1:1 bidirectional protection switching (revertive mode) - Bidirectional SF case

```
                 A                  Z
                 |                  |
             (1) |---- NR(0,0)----->| (1)
                 |<----- NR(0,0)----|
                 |                  |
                 |                  |
             (2) | (SF on W(Z<->A)) | (2)
                 |<---- SF(1,1)---->|
             (3) |                  | (3)
                 |                  |
             (4) |    (Recovery)    | (4)
                 |<---- NR(1,1)---->|
             (5) |<--- WTR(1,1)---->| (5)
                /|                  |\
       WTR timer |                  | WTR timer
                \|                  |/
             (6) |<---- NR(1,1)---->| (6)
             (7) |<----- NR(0,0)--->| (7)
             (8) |                  | (8)
```

(1) The protection domain is operating without any defect, and the working entity is used for delivering the normal traffic.

(2) Nodes A and Z detect local Signal Fail conditions on the working entity, set selector and bridge to protection entity, and generate SF(r=1, b=1) messages.

(3) Upon receiving SF(r=1, b=1), each node confirms that the far end is also selecting protection entity.

(4) Each node detects clearing of SF condition, and sends NR(r=1, b=1) message as the last received APS message was SF.

(5) Upon receiving NR(r=1, b=1), each node starts the WTR timer and sends WTR(r=1, b=1).

(6) At expiration of the WTR timer, each node sends NR(r=1, b=1) as the last received APS message was WTR.

(7) Upon receiving NR(r=1, b=1), each node sets selector and bridge to working entity and sends NR(r=0, b=0) message.

(8) It is confirmed that the far end is also selecting working entity.

Example 3. 1:1 bidirectional protection switching (revertive mode) - Bidirectional SF case - Inconsistent WTR timers

```
                 A                  Z
                 |                  |
             (1) |---- NR(0,0)----->| (1)
                 |<----- NR(0,0)----|
                 |                  |
                 |                  |
             (2) | (SF on W(Z<->A)) | (2)
                 |<---- SF(1,1)---->|
             (3) |                  | (3)
                 |                  |
             (4) |    (Recovery)    | (4)
                 |<---- NR(1,1)---->|
             (5) |<--- WTR(1,1)---->| (5)
                /|                  |\
       WTR timer |                  | |
                \|                  | WTR timer
             (6) |----- NR(1,1)---->| | (7)
                 |                  |/
             (9) |<----- NR(0,0)----| (8)
                 |---- NR(0,0)----->| (10)
```

(1) The protection domain is operating without any defect, and the working entity is used for delivering the normal traffic.

(2) Nodes A and Z detect local Signal Fail conditions on the working entity , set selector and bridge to protection entity, and generate SF(r=1, b=1) messages.

(3) Upon receiving SF(r=1, b=1), each node confirms that the far end is also selecting protection entity.

(4) Each node detects clearing of SF condition, and sends NR(r=1, b=1) message as the last received APS message was SF.

(5) Upon receiving NR(r=1, b=1), each node starts the WTR timer and sends WTR(r=1, b=1).

(6) At expiration of the WTR timer in node A, node A sends NR(r=1, b=1) as the last received APS message was WTR.

(7) At node Z, the received NR(r=1, b=1) is ignored as the local WTR has a higher priority.

(8) At expiration of the WTR timer in node Z, node Z node sets selector and bridge to working entity, and sends NR(r=0, b=0) message.

(9) Upon receiving NR(r=0, b=0), node A sets selector and bridge to working entity and sends NR(r=0, b=0) message.

(10) It is confirmed that the far end is also selecting working entity.

Example 4. 1:1 bidirectional protection switching (non-revertive mode) - Unidirectional SF on working followed by unidirectional SF on protection

```
                 A                  Z
                 |                  |
             (1) |---- NR(0,0)----->| (1)
                 |<----- NR(0,0)----|
                 |                  |
                 |                  |
             (2) | (SF on W(Z->A))  |
                 |----- SF(1,1)---->| (3)
             (4) |<----- NR(1,1)----|
                 |                  |
                 |                  |
             (5) |    (Recovery)    |
                 |----- DNR(1,1)--->| (6)
                 |<--- DNR(1,1)---->|
                 |                  |
                 |                  |
                 | (SF on P(A->Z))  | (7)
             (8) |<--- SF-P(0,0)----|
                 |---- NR(0,0)----->|
                 |                  |
                 |                  |
                 |     (Recovery)   | (9)
```

```
                  |<----- NR(0,0)----|
                  |                  |
```

(1) The protection domain is operating without any defect, and the working entity is used for delivering the normal traffic.

(2) Signal Fail occurs on the working entity in the Z to A direction. Selector and bridge of node A select the protection entity. Node A generates SF(r=1, b=1) message.

(3) Upon receiving SF(r=1, b=1), node Z sets selector and bridge to protection entity. As there is no local request in node Z, node Z generates NR(r=1, b=1) message.

(4) Node A confirms that the far end is also selecting protection entity.

(5) Node A detects clearing of SF condition, and sends DNR(r=1, b=1) message.

(6) Upon receiving DNR(r=1, b=1), node Z also generates DNR(r=1, b=1) message.

(7) Signal Fail occurs on the protection entity in the A to Z direction. Selector and bridge of node Z select the working entity. Node Z generates SF-P(r=0, b=0) message.

(8) Upon receiving SF-P(r=0, b=0), node A sets selector and bridge to working entity, and generates NR(r=0, b=0) message.

(9) Node Z detects clearing of SF condition, and sends NR(r=0, b=0) message.

Exmaple 5. 1:1 bidirectional protection switching (non-revertive mode) - Bidirectional SF on working followed by bidirectional SF on protection

```
                  A                  Z
                  |                  |
              (1) |---- NR(0,0)----->| (1)
                  |<----- NR(0,0)----|
                  |                  |
                  |                  |
              (2) | (SF on W(A<->Z)) | (2)
              (3) |<---- SF(1,1)---->| (3)
                  |                  |
                  |                  |
```

```
                (4) |    (Recovery)    | (4)
                (5) |<---- NR(1,1)---->| (5)
                    |<--- DNR(1,1)---->|
                    |                  |
                    |                  |
                (6) | (SF on P(A<->Z)) | (6)
                (7) |<--- SF-P(0,0)--->| (7)
                    |                  |
                    |                  |
                (8) |     (Recovery)   | (8)
                    |<---- NR(0,0)---->|
                    |                  |
```

(1) The protection domain is operating without any defect, and the working entity is used for delivering the normal traffic.

(2) Nodes A and Z detect local Signal Fail conditions on the working entity, set selector and bridge to protection entity, and generate SF(r=1, b=1) messages.

(3) Upon receiving SF(r=1, b=1), each node confirms that the far end is also selecting protection entity.

(4) Each node detects clearing of SF condition, and sends NR(r=1, b=1) message as the last received APS message was SF.

(5) Upon receiving NR(r=1, b=1), each node sends DNR(r=1, b=1).

(6) Signal Fail occurs on the protection entity in both directions. Selector and bridge of each node selects the working entity. Each node generates SF-P(r=0, b=0) message.

(7) Upon receiving SF-P(r=0, b=0), each node confirms that the far end is also selecting working entity

(8) Each node detects clearing of SF condition, and sends NR(r=0, b=0) message.

Authors' Addresses

Huub van Helvoort (editor)
Huawei Technologies

Email: huub.van.helvoort@huawei.com

Jeong-dong Ryoo (editor)
ETRI

Email: ryoo@etri.re.kr

Haiyan Zhang
Huawei Technologies

Email: zhanghaiyan@huawei.com

Feng Huang
Alcatel-Lucent Shanghai Bell

Email: feng.f.huang@alcatel-sbell.com.cn

Han Li
China Mobile

Email: lihan@chinamobile.com

Alessandro D'Alessandro
Telecom Italia

Email: alessandro.dalessandro@telecomitalia.it