INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2005-2008

STUDY GROUP 15

TD 30 (WP 3/15)

English only

Original: English

Question(s): 22/15 (ex-3/13) Geneva, 29 November-3 December 2004

TEMPORARY DOCUMENT

(Ref. : COM 13 – C 43 – E)

Source: Editors Recommendation Y.17ethps

Title: Draft Recommendation Y.17ethps - Ethernet Protection Switching

This Contribution provides the text for draft Recommendation Y.17ethps, "Ethernet Protection Switching" in the ANNEX. This is originated in the interim meeting on Q.3/13 (Sophia Antipolis 20-24 Sept. 2004).

Contact:	Ken-ichi Kawarai Fujitsu Limited Japan	Tel: Fax: Email	+81 44 754 3877 +81 44 754 3524 kawarai@jp.fujitsu.com
Contact:	Ana Szpaizer Nortel Networks Canada	Tel: Fax: Email	+1 613 765 1674 +1 613 765 4371 janele@nortelnetworks.com

Annex

Draft Recommendation Y.17ethps

Ethernet Protection Switching

Summary

This Recommendation provides motivation and requirements for Ethernet survivability. It aims to enhance Ethernet reliability for carrier service. This Recommendation describes p-p Ethernet Trail protection and p-p SNC protection.

EDITOR’S NOTE: "Scope" should be modified so that this Recommendation aims at describing mechanisms also as well as motivation and requirements.

Keywords

TBD

TABLE OF CONTENTS

1. Scope

This Recommendation provides motivation and requirements for Ethernet survivability. It aims to enhance Ethernet reliability for carrier service. This Recommendation describes p-p Ethernet Trail protection and p-p SNC protection.

EDITOR’S NOTE: "Scope" should be modified so that this Recommendation aims at describing mechanisms also as well as motivation and requirements.

2. References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation G.805, Nov 1995, *Generic functional architecture of transport networks*

[2] ITU-T Recommendation G.8010, *Generic functional architecture of transport networks*

[3] ITU-T Recommendation G.808.1, *Generic protection switching – Liner trail and subnetwork protection*

[4] IEEE 802.3ad, Apl 2002, *Link Aggregation*

[5] IEEE 802.1D, 2004, *Media Access Control (MAC) Bridges*

[6] IEEE Draft 802.1s, 2002, Virtual Bridged Local Area Networks: Multiple Spanning Trees

3. Definitions

This Recommendation defines the following terms:

EDITOR'S NOTE:to be completed

4. Abbreviations

This Recommendation uses the following abbreviations:

ETH	Ethernet
ETH-AIS	Ethernet Alarm Indication Signal
ETH-APS	Ethernet Auto Protection Switch
ETH-CC	Ethernet Continuity Check
ETH-RDI	Ethernet Remote Defect Signal
ETH_FF	Ethernet Flow Function
FS	Forced switching
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point

SNC	Subnetwork Connection
SNCP	Subnetwork Connection Protection
SNC/S	SNCP with Sub-layer monitoring
SNC/T	SNCP with Test trail monitoring
DNI	Dual Node Interconnection

EDITOR'S NOTE:to be completed

5. Conventions

Maintenance Entity End Point (MEP) is a short name for an expanded ETH flow point that includes an ETH Segment flow termination function, introduced in Y.ethoam. MEP recieve/send the ETH-APS OAM from/to ETH_FP.

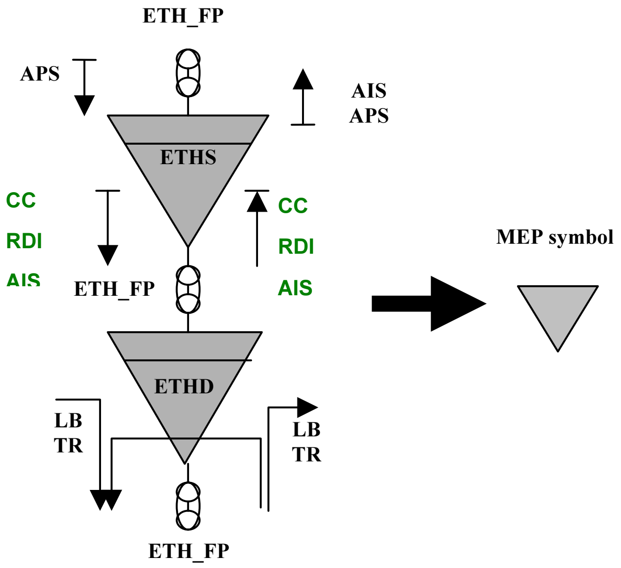


Figure 1/Y.17ethps Maintenance entity End Point (MEP) symbol

EDITOR'S NOTE: MEP sysmbol should be chaged to tragle in the entire document.

ETH-APS process inside SNCP process control the ETH-APS flow. Protected domain is designed between two of ETH-APS process.

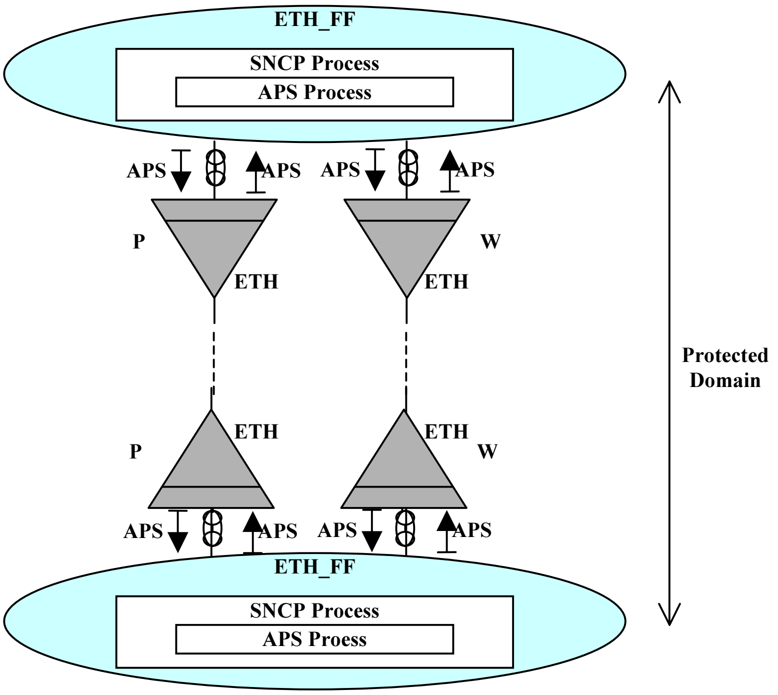


Figure 2/Y.17ethps Relationship of ETH_FF and MEP

6. Reference Model

Ethernet protection switching is shown in the following figures in case of p-p Ethernet trail protection and p-p Ethernet SNC protection. The detail models are described in the next subsection.

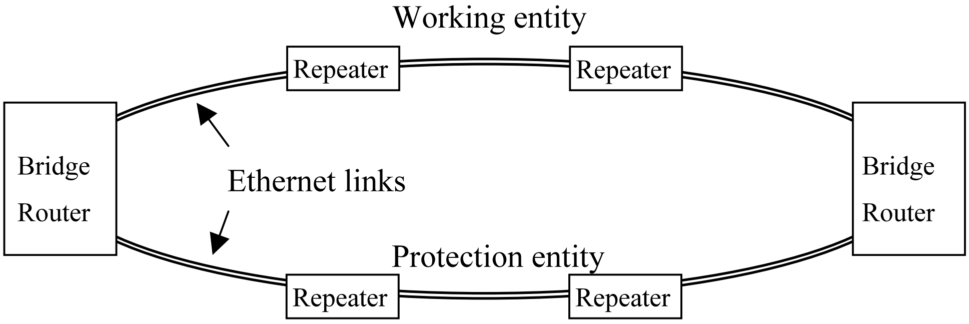


Figure 3/Y.17ethps p-p Ethernet Trail protection

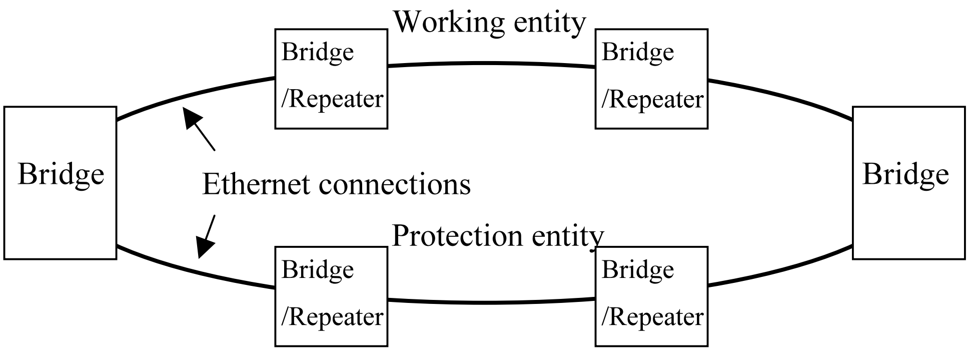


Figure 4/Y.17ethps p-p Ethernet SNC protection

6.1. Point to point Ethernet Trail Protection

TBD

6.2. Point to point Ethernet SNC Protection

6.2.1. Individual SNC Protection model

6.2.1.1. Single Operator Case

The most simple single operator case is shown in Figure 5/Y.17ethps. The OAM levels of working transport entity and protection entity can be set independently.

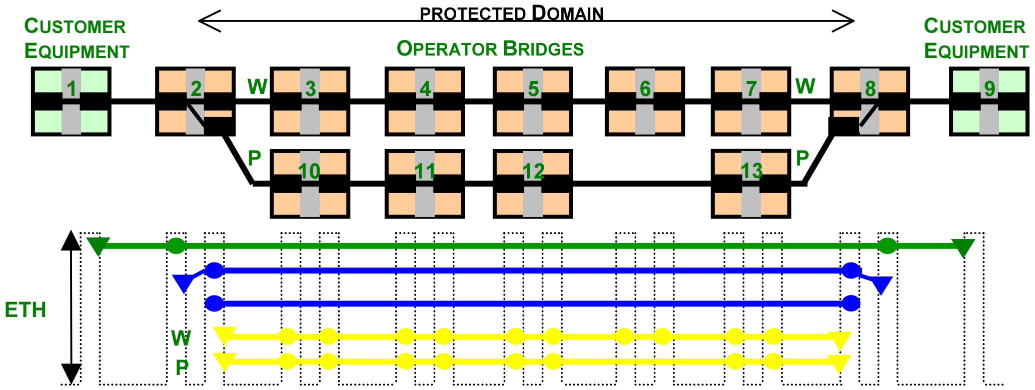


Figure 5/Y.17ethps UNI-UNI ETH SNC/S Protection in single operator network

Figure 6/Y.17ethps also shows the single operator case where the protected domain is set in between the operators intermediate bridge. It should be noted that the edge node of protected domain is always MEP of some level, so that ETH-APS packet is properly terminated within protected domain, and the ETH-APS packet belongs to that level.

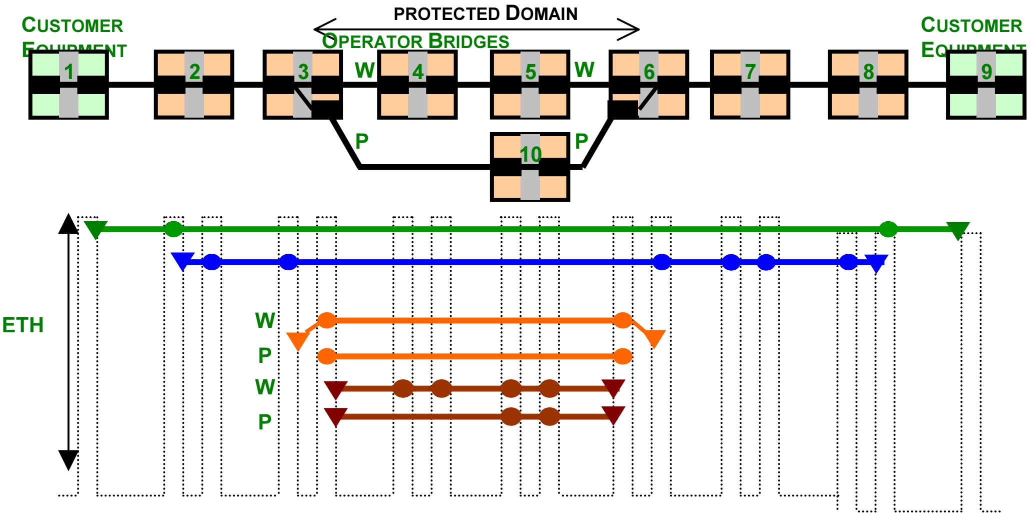


Figure 6/Y.17ethps UNI-UNI ETH SNC/S Protection in single operator network

More details of the law for configuration of level need to be discussed. Figure 7/Y.17ethps shows the prohibited example of level configuration. The points are following:

- The edge node of protected domain must be always MEP of some level preventing leaking of ETH-APS. (see brown level)
- The lower level below ETH-APS OAM level (see orange level) must be terminated within protected domain preventing nest of level that makes operators confused. (see brown level)
- The upper level over ETH-APS OAM level must fully covers the ETH-APS OAM level (see orange level) that also preventing nest of level that makes operators confused. (see yellow level)

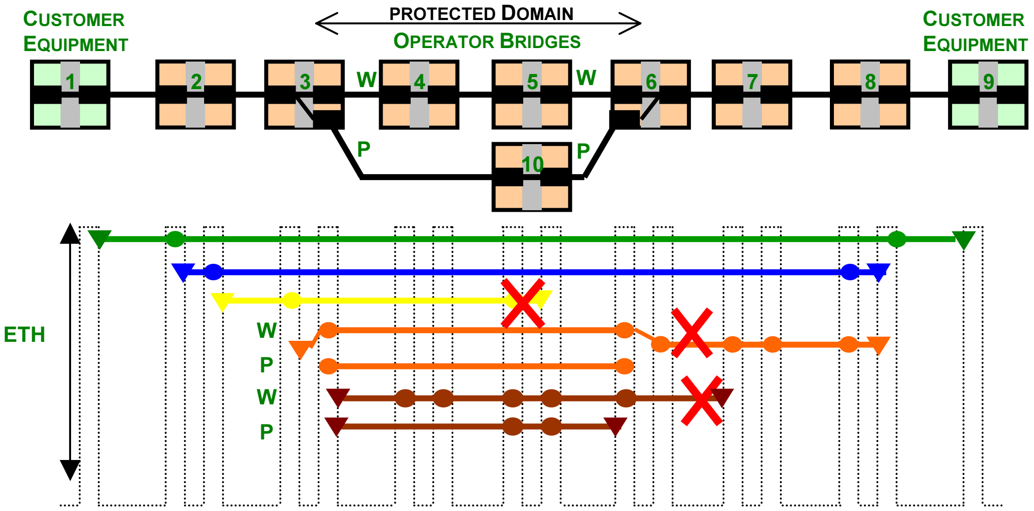


Figure 7/Y.17ethps UNI-UNI ETH SNC/S Protection in single operator network

6.2.1.2. Multi Operator Case

6.2.1.2.1. Multi Operator Case with Single Protected Domain

Figure 8/Y.17ethps shows the network model of SNC protection for multi operator case.

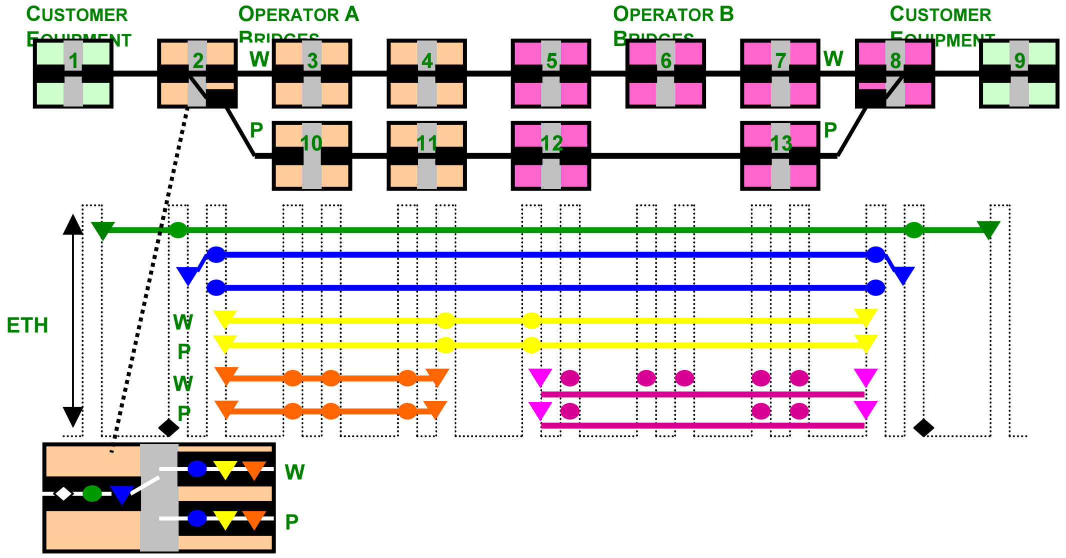


Figure 8/Y.17ethps UNI-UNI ETH SNC/S Protection in multi operator network

6.2.1.2.2. Multi Operator Case with Cascaded SNC/S Protected Domain

The cascaded protection for multi-operator case is shown in Figure 9/Y.17ethps. Two operators independently preside each protected domain.

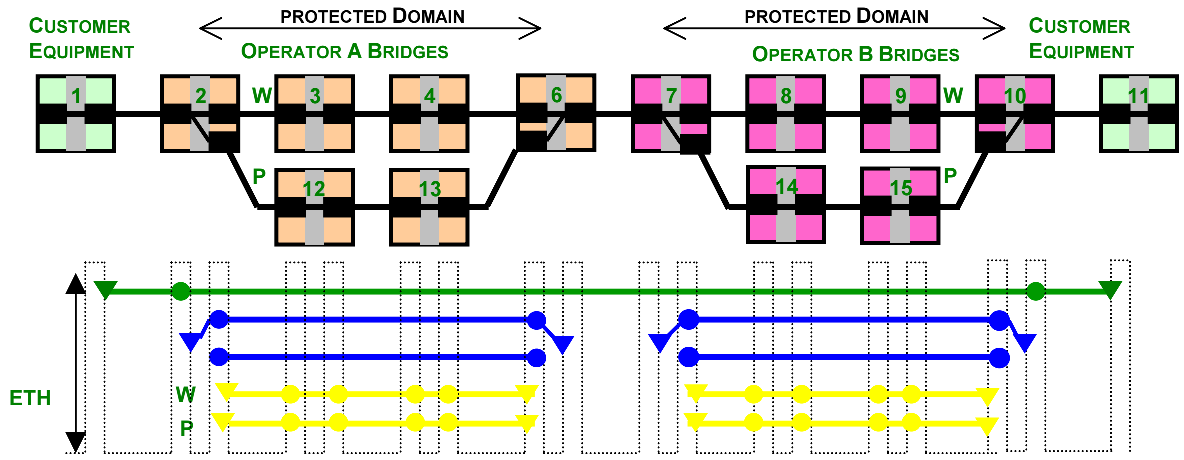


Figure 9/Y.17ethps ETH cascaded SNC/S Protection in multi operator network

6.2.1.2.3. Multi Operator Case with DNI(Dual Node Interconnection)

G.808.1 also illustrates another example of the fault tolerant subnetwork interconnects, but the mechanism of interconnecting point and its necessity is for further study.

6.2.2. Group Protection model

Figure 10/Y.17ethps illustrates the case of group protection. The three parallel traffic signals with three types of tags in the group are protected jointly. ETH-APS information is transported over one of the protection entity of some tag shared with user signal. Or one dedicated transport entity can be configured to transport ETH-APS information, which will decrease the number of ASP packet suppressing bandwidth.

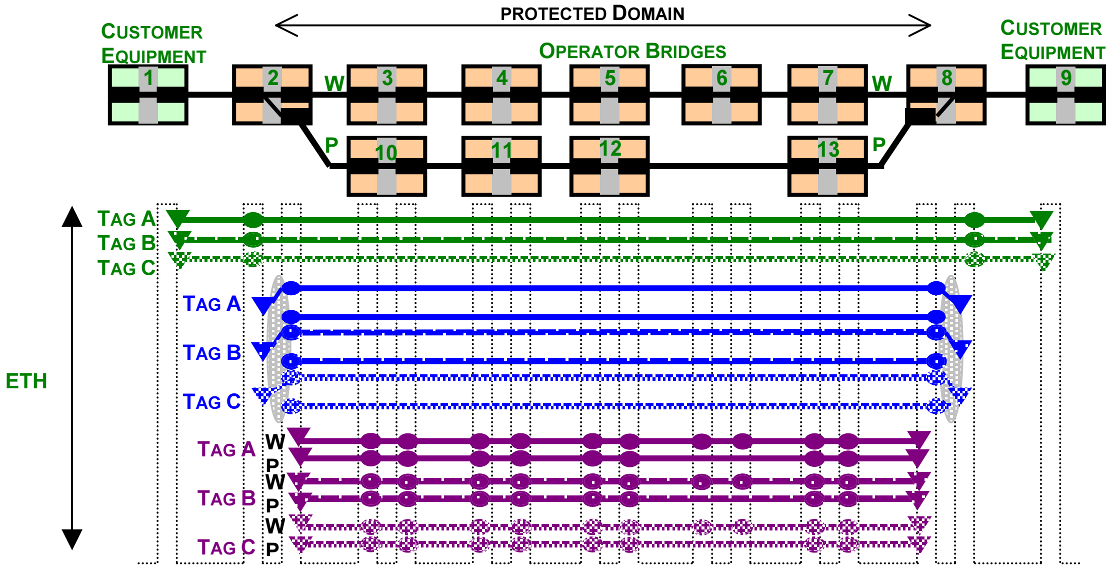


Figure 10/Y.17ethps ETH SNC/S Group Protection in single operator network

Figure 11/Y.17ethps illustrates SNC/T group protection model. One of the entity, described as Tag D, is a dedicated transportation entity for ETH-APS information, and also used for monitoring. The OAM packets with Tag D, e.g. ETH-CC or other monitoring function, are inserted and terminated at operator bridge 2 and 8. SNC/T model will decrease the number of ASP packet suppressing bandwidth.

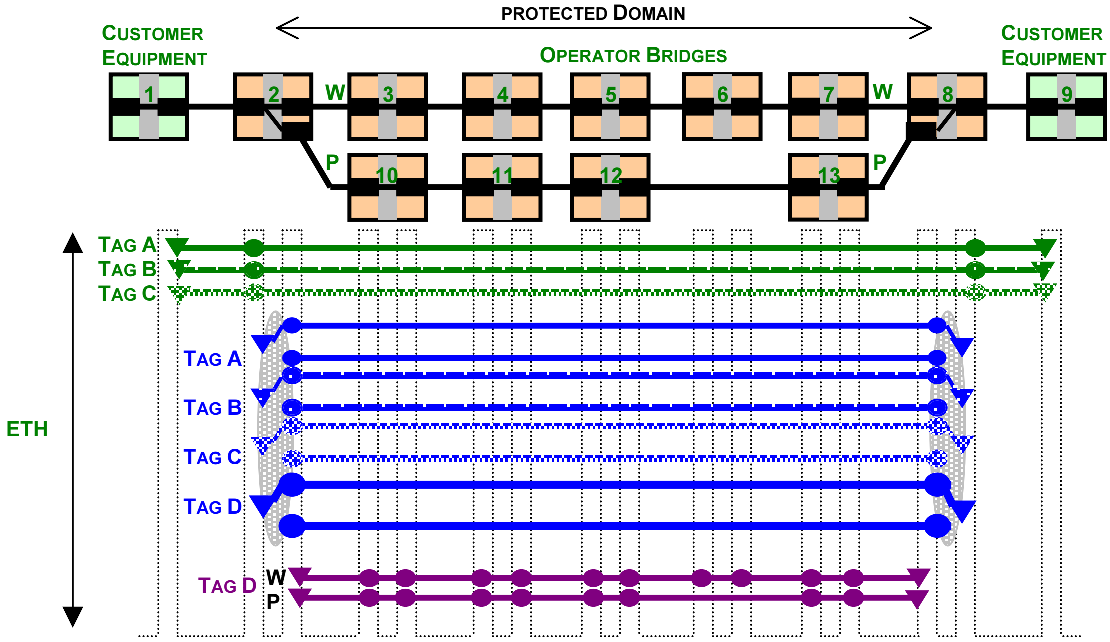


Figure 11/Y.17ethps ETH SNC/Ts Group Protection in single operator network

It is noted that S-tag encapsulation is also effective method for group protection. The protection encapsulated in S-tag is shown in the next section.

6.3. SNC Protection model for Dual Relay Model with Bundling

The Figure 12/Y.17ethps shows the case of protection model for dual relay model with bundling. It is noted that S-TAG and C-TAG belong to other independent sublayer, so OAM mechanism for protection is also independent.

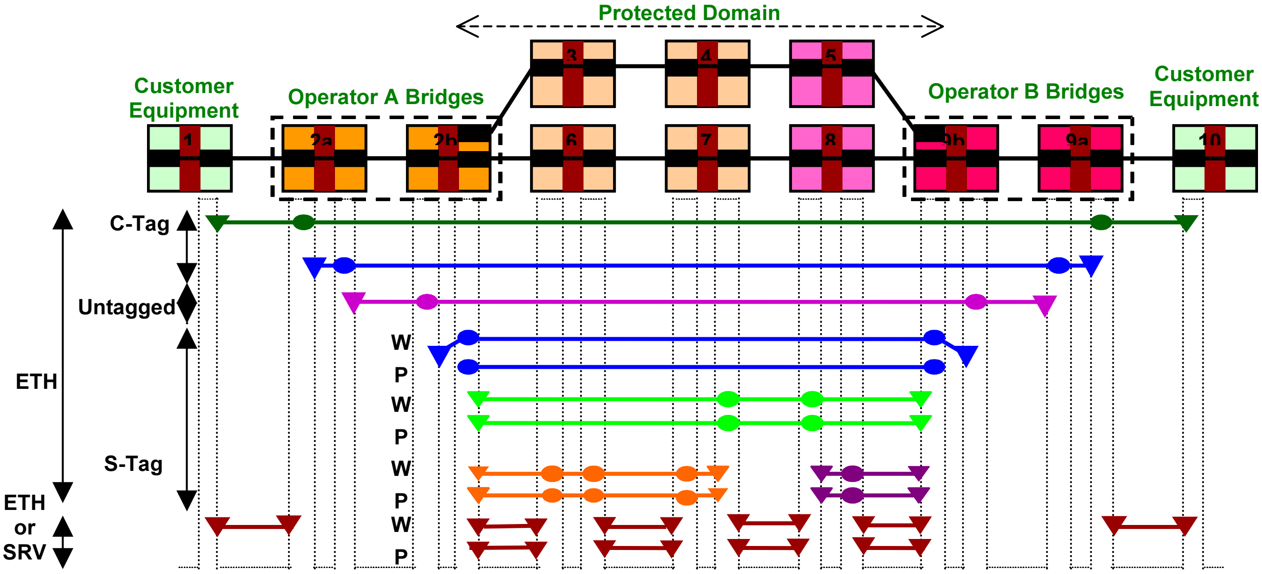


Figure 12/Y.17ethps Network model of ETH SNC/S Protection with Dual Relay Model with Bundling

6.4. Group Protection model for Dual Relay Model with Bundling

Figure 13/Y.17ethps illustrates SNC/T group protection model for Dual Relay Model with Bundling. One of the entity, described as Tag D, is a dedicated transportation entity of ETH-APS information, and also used for monitoring. The OAM packets with Tag D, e.g. ETH-CC or other monitoring function, are inserted and terminated at operator bridge 2 and 8. SNC/T model will decrease the number of ASP packet suppressing bandwidth.

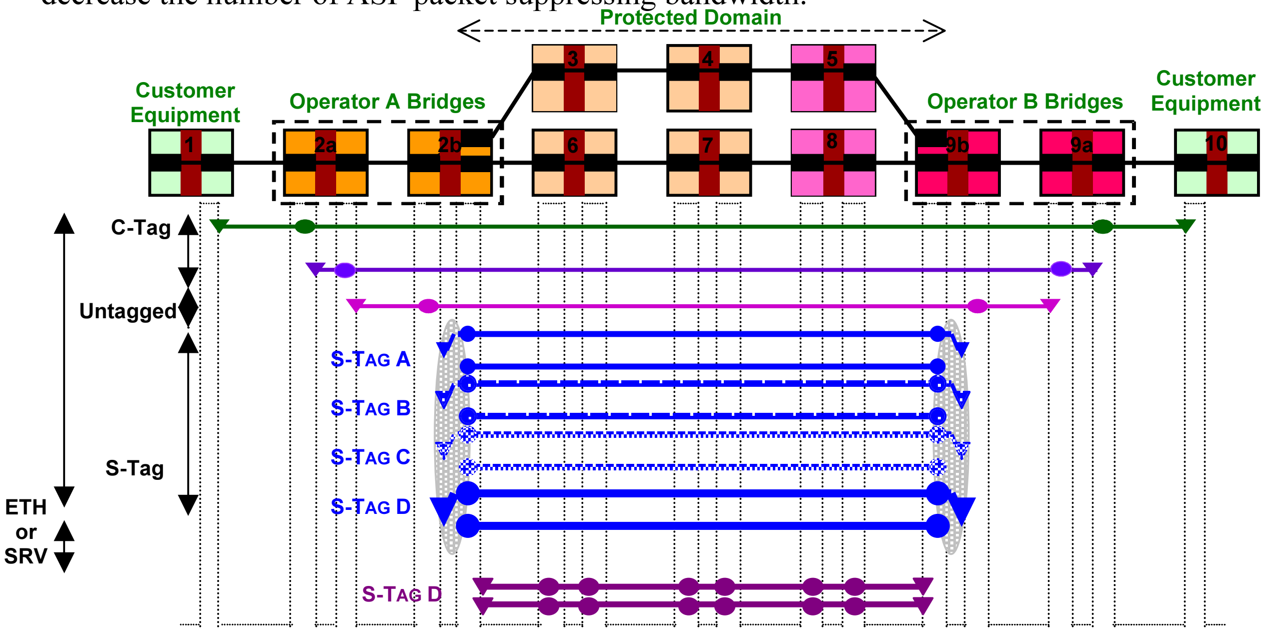


Figure 13/Y.17ethps Network model of ETH SNC/T Group Protection with Dual Relay Model with Bundling

Further encapsulation method by another Tag is for further study.

6.5. VLAN assignment for Working and Protection entity

This section is TBD. Current discussion and status is referred in Appendix III.

7. Requirement

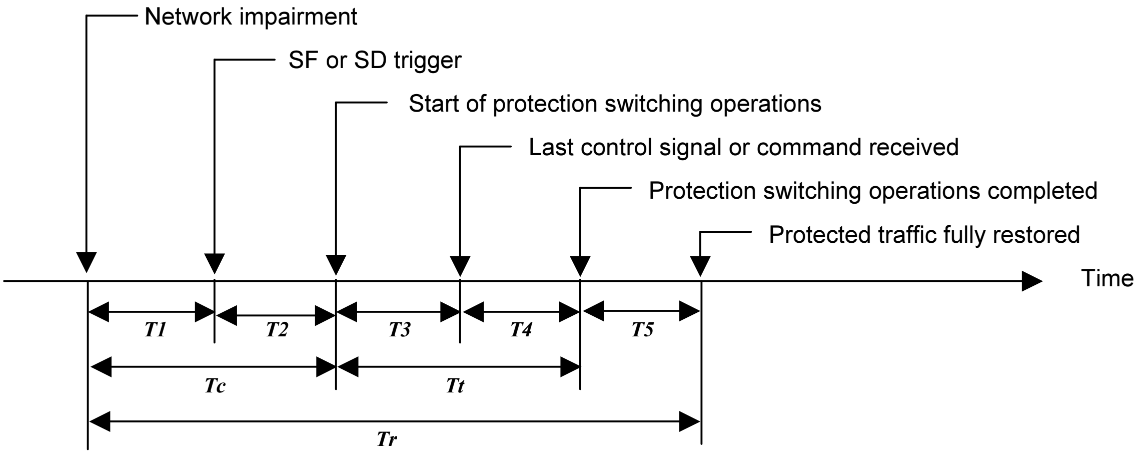
To enhance reliability performance of a Ethernet based network, rapid recovering capability form service interruption (e.g., due to defects) is important technique referred to as Ethernet Network survivability. Table 1 shows requirements for Ethernet Network Survivability.

Table 1/ Y.ethps - Requirements for Ethernet Network Survivability

Item	Requirements
Configuration	Protected entity should be configured by working entity and protection entity. All Ethernet flow in working entity should be switched to protection entity within the required interruption time when a service interruption is caused or FS(forced switching) is instructed by operator.
Bandwidth allocation	Allocate bandwidth to protection entity beforehand.
Protection switching performance	The total time of protection switching operation time and protection switching transfer time should be less than 50msec (see section 7.1)
Bandwidth efficiency	Not only bandwidth of working entity but also bandwidth of protection entity can be used completely.
Misordering	Frame sequence integrity should be maintained.
Latency	Additional latency that is introduced by the protection should be minimized.
Interoperability	Interoperability should be realized.

7.1. Protection Switching performance

Protection switching performance model is shown inFigure 14/Y.17ethps which is specified in ITU-T Recommendation G.808.1. The total time of protection switching operation time(T3) and protection switching transfer time(T4) should be less than 50msec.


Network impairment
SF or SD trigger
Start of protection switching operations
Last control signal or command received
Protection switching operations completed
Protected traffic fully restored
Time
T1
T2
T3
T4
T5
Tc
Tt
Tr

detection time, T1:

Time interval between the occurrence of a network impairment and the detection of a signal fail (SF) or signal degrade (SD) triggered by that network impairment.

hold-off time, T2:

Time interval after the detection of a SF or SD and its confirmation as a condition requiring the protection switching procedure.

NOTE: Recommendation M.495 identifies time T2 as the "***waiting time***"

protection switching operations time, T3:

Time interval between the confirmation of a SF or SD and completion of the processing and transmission of the control signals required to effect protection switching.

protection switching transfer time, T4:

Time interval between completion of the processing and transmission of the control signals required to effect protection switching and the completion of protection switching operations.

recovery time, T5:

Time interval between the completion of protection switching operations and the full restoration of protected traffic.

NOTE – This may include the verification of switching operations, re-synchronization of digital transmission, etc.

confirmation time, Tc:

The time from the occurrence of the network impairment to the instant when the triggered SF or SD is confirmed as requiring protection switching operations: Tc = T1 + T2.

***transfer time, Tt*:**

The time interval after the confirmation that a SF or SD requires protection switching operations to the completion of the protection switching operations: Tt = T3 + T4 （≦50msec） .

protected traffic restoration time, Tr:

The time from the occurrence of the network impairment to the restoration of protected traffic:

Tr = T1 + T2 + T3 + T4 + T5 = Tc + Tt + T5.

NOTE – An apparent network impairment might be detected by an equipment and not confirmed after confirmation operations. In this case, only times T_1 and T_2 are relevant.

Figure 14/Y.17ethps Protection Switching Temporal Model

8. Protection switching trigger

Protection switching should be performed when:

1) initiated by operator control (e.g. manual switch, forced switch, and lockout of protection);

2) Signal Fail (SF) is declared on the connected entity (i.e. working entity or protection entity) and is not declared on the other side of entities; or

3) In the bi-directional 1+1 and 1:1 architecture, Auto Protection Switch (ETH-APS) protocol co-ordinates switching between a pair of ETH trail and ETH flow points.

8.1. Manual control

Manual control of the protection switching function may be performed from the operation system.

8.2. Signal Fail declaration conditions

8.2.1. 1+1 architecture

For 1+1 architecture, Signal Fail (SF) is declared when the state of the sink point of the protection domain becomes the Near-End Defect State.

8.2.2. 1:1 architecture

For 1:1 architecture, Signal Fail (SF) is declared when:

- the state of the sink point of the protection domain becomes the Near-End Defect State, in case of bi-directional protection switching,
- the state of the source point of the protection domain becomes the Far-End Defect State by receiving ETH-RDI packets. Necessity of ETH-RDI is for further study.

8.2.3. Near End Defect State declaration

Near-End Defect State is declared when:

1) Physical layer failure (Los of Signal, Auto negotiation Error, Code violation) is detected

2) Loss of Continuity (condition that user packet or EHT-CC packet is missed for a certain period) is detected

3) EHT-AIS packets are received.

8.2.4. Far – End Defect State declaration

Far-End Defect State is declared when:

1) ETH-RDI packets are received. Necessity of EHH-RDI is for further study.

9. ETH-APS Flow

ETH-APS flows are shown according to the each switching trigger in next subsections. It is noted that the protocol type is regarded as 2-phase in the following figures. This protocol type is for further study.

9.1. ETH-APS flow triggered by ETH-AIS

9.1.1. ETH-APS flow triggered by ETH-AIS induced by server layer failure

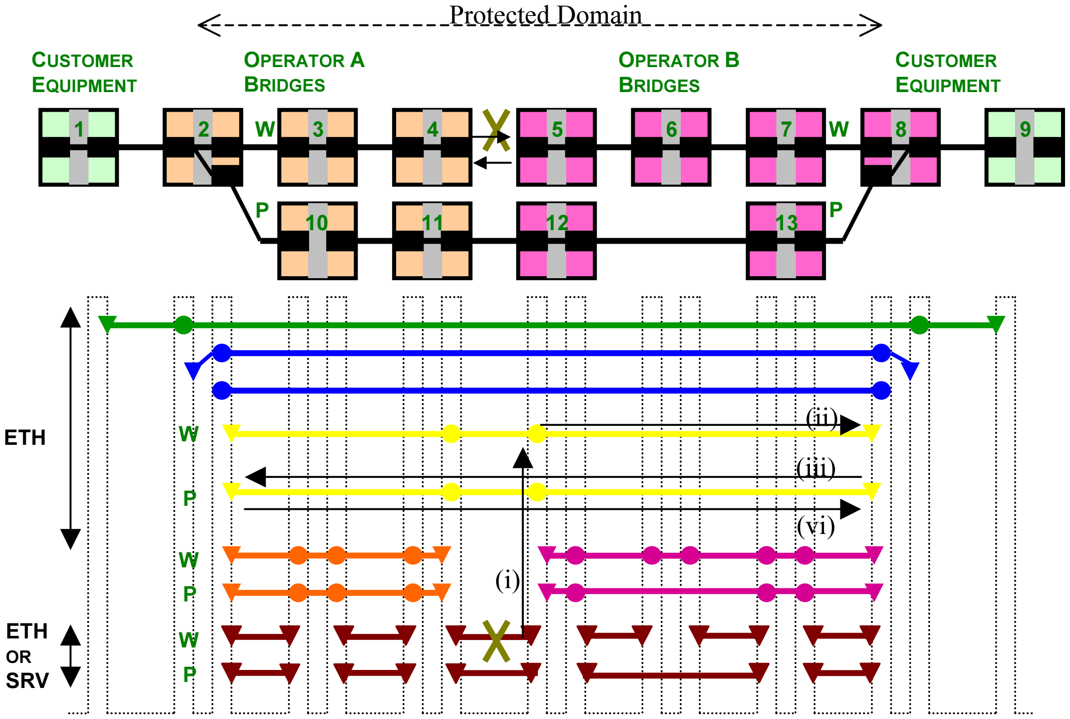
ETH-APS flows are trigged by ETH-AIS where a server layer failure is detected by MIP that has an ability to send ETH-AIS, shown in Figure 15/Y.17ethps. The switching mechanism is along these following procedure:

(i) ETH or SRV MEP of working entity detects failure then inserts ETH-AIS to MIP of the upper level at equipment 5.

(ii) ETH-AIS is transfered via MIP at equipment 5 at level yellow that is terminated at MEP of equipment 8.

(iii) MEP of equipment 8 send ETH-APS to protected side at level yellow that is terminated at MEP of equipment 2.

(vi) MEP of equipment 2 send back ack ETH-APS at level yellow that is terminated at MEP of equipment .2.



(i) ETH or SRV MEP of working entity detects failure then insertsETH-AIS to MIP of the upper level at equipment 5.
(ii) ETH-AIS is transfered via MIP at equipment 5 at level yellow that is terminated at MEP of equipment 8.
(iii) MEP of equipment 8 send APS to protected side at level yellow that is terminated at MEP of equipment 2..
(vi) MEP of equipment 2 send back ack APS at level yellow that is terminated at MEP of equipment .2..

Figure 15/Y.17ethps ETH-APS flow triggered by ETH-AIS applied at SNC protection

9.1.2. ETH-APS flow triggered by ETH-AIS induced by LOC

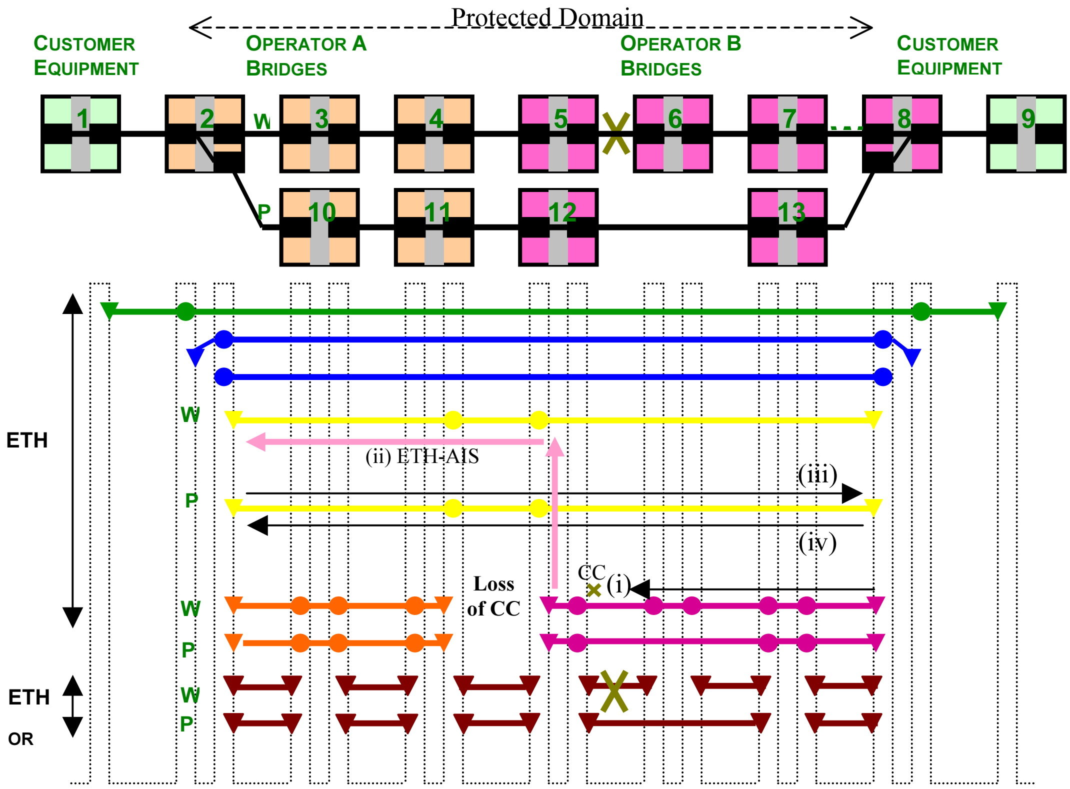
ETH-APS flows are trigged by ETH-AIS where Loss of Continuity is detected by MEP at lower ME level that has an ability to send ETH-AIS, shown in Figure 16/Y.17ethps. The switching mechanism is along these following procedure:

(i) ETH-CC packet of level pink does not arrive at MEP of equipment 5 for working entity, then detects Loss of CC (LOC).

(ii) MEP of equipment 5 of level pink injects ETH-AIS to level yellow.

(iii) MEP of equipment 2 receives ETH-AIS and sends APS to protected side at level yellow that is terminated at MEP of equipment 8.

(iv) MEP of equipment 8 sends back ack-APS at level yellow that is terminated at MEP of equipment 2.



(i) ETH-CC packet of level pink does not arrive at MEP of equipment 5 for working entity, then detects Loss of CC (LOC).
(ii) MEP of equipment 5 of level pink injects ETH-AIS to level yellow.
(iii) MEP of equipment 2 receives ETH-AIS and sends ETH-APS to protected side at level yellow that is terminated at MEP of equipment 8.
(iv) MEP of equipment 8 sends back ack-APS at level yellow that is terminated at MEP of equipment 2.

Figure 16/Y.17ethps ETH-APS flow triggered by Loss of ETH-CC and ETH-AIS and ETH-CCapplied to SNC protection.

9.2. ETH-APS flow triggered by Loss of ETH-CC

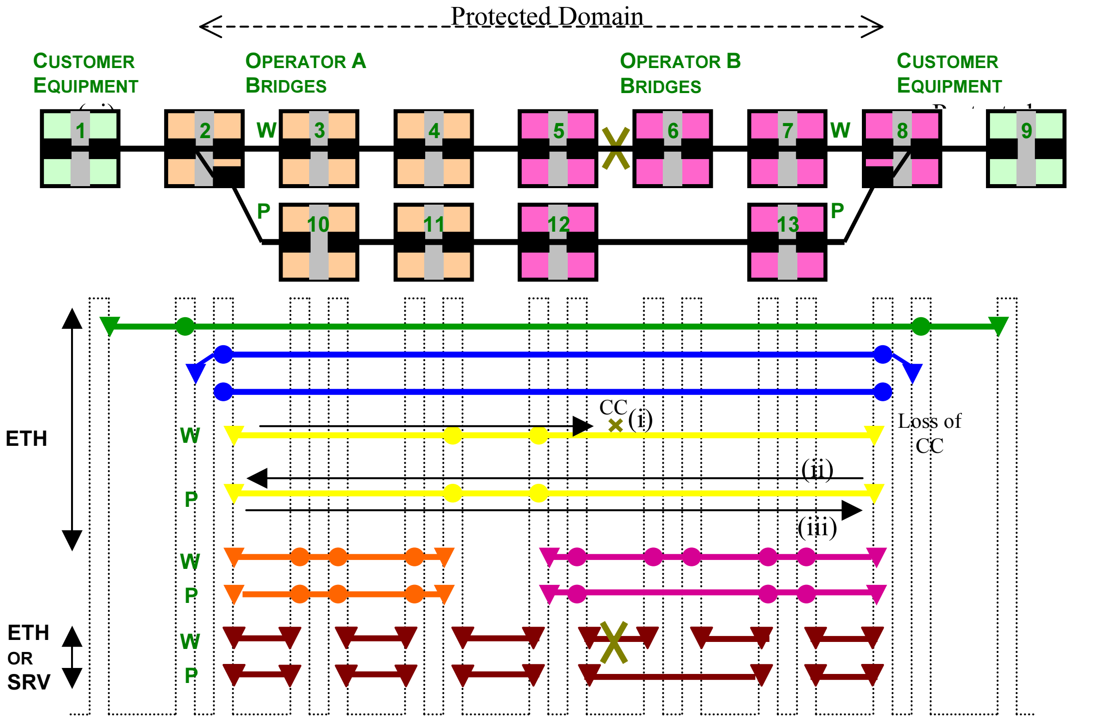
The second case is using ETH-CC where server layer does not send ETH-AIS OAM packet shown in Figure 17/Y.17ethps. The switching mechanism is along these following procedure:

(i) ETH-CC packet of level yellow does not arrive at MEP of equipment 8 for working entity, then detects Loss of CC (LOC).

(ii) MEP of equipment 8 send ETH-APS to protected side at level yellow that is terminated at MEP of equipment 2.

(iii) MEP of equipment 2 send back ack ETH-APS at level yellow that is terminated at MEP of equipment 8.

If ETH-CC is configured at both equipment 2 and 8, both sides will detect failure, therefore switching procedure from both sides will happen. The switching mechanism should go on even in this case.



(i) ETH-CC packet of level yellow does not arrive at MEP of equipment 8 for working entity, then detects Loss of CC (LOC).
(ii) MEP of equipment 8 send ETH-APS to protected side at level yellow that is terminated at MEP of equipment 2.
(iii) MEP of equipment 2 send back ack ETH-APS at level yellow that is terminated at MEP of equipment 8.

Figure 17/Y.17ethps ETH-APS flow triggered by Loss of ETH-CC applied at SNC protection

9.3. ETH-APS Flow for Dual Relay Model with Bundling

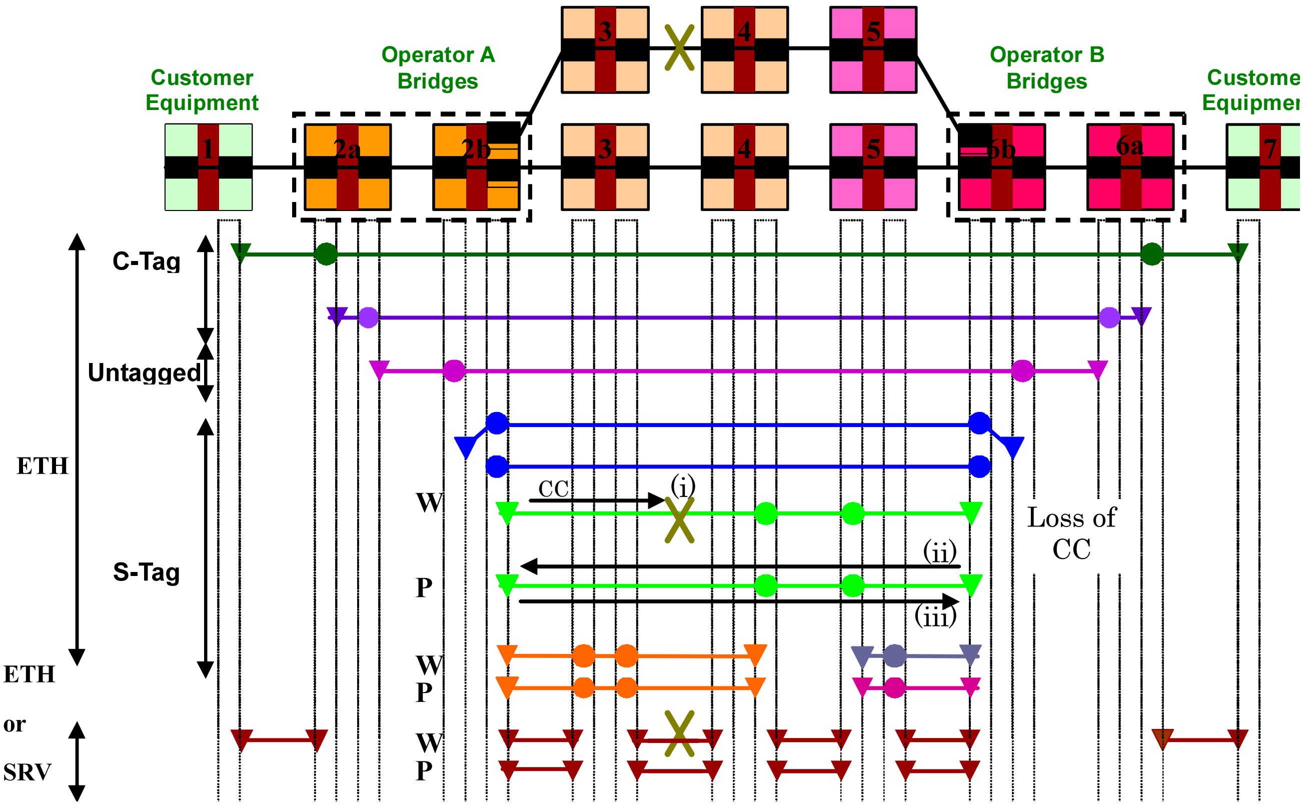
The ETH-APS flow encapsulated in S-TAG using ETH-CC is shown in Figure 18/Y.17ethps. The switching mechanism is along these following procedure:

(i) ETH-CC packet of S-Tag OAM for level yellow does not arrive at MEP of equipment 6b for working entity, then detects Loss of CC (LOC).

(ii) MEP of equipment 6b send ETH-APS to protected side at level yellow that is terminated at MEP of equipment 2b.

(iii) MEP of equipment 2b send back ack ETH-APS at level yellow that is terminated at MEP of equipment .6b.

If ETH-CC is configured at both equipment 2 and 8, both sides will detect failure, therefore switching procedure from both sides will happen. The switching mechanism should go on even in this case.



(i) ETH-CC packet of S-Tag OAM for level yellow does not arrive at MEP of equipment 6b for working entity, then detects Loss of CC (LOC).
(ii) MEP of equipment 6b send ETH-APS to protected side at level yellow that is terminated at MEP of equipment 2b.
(iii) MEP of equipment 2b send back ack ETH-APS at level yellow that is terminated at MEP of equipment .6b.

Figure 18/Y.17ethps Network model of ETH SNC/S Protection with Dual Relay Model with Bundling

10. Operation

10.1. Revertive (protection) operation

TBD

10.2. Non-revertive (protection) operation

TBD

11. Information Element

- Required Common Information Elements

  Refer to section 11 of Y.17ethoam
- Required ETH-APS Information Elements
  - K1
  - K2

EDITOR'S NOTE: Another alternative is proposed as following reffered to G.873.1. This is FFS.

- Request/state
- Protection type
- Requested Signal
- Bridged Signal

The topology of protection switching is assumed to be applied to point to point topology. Therefore Multicast DA is available for for ETH-AIS, ETH-CC and ETH-APS.

ANNEX A

Interaction between Ethernet Protection Switching (EPS) and STP

This section shows that in order to avoid interaction between STP and EPS, the EPS bridges must not participate in the STP. One way to ensure this is to not have any STP in the protection domain at all although the domains outside the protection domain could have STP. Another way to ensure this is if the protection and switching path belong to two separate STP domains. These two scenario are discussed in the remainder of this section.

Figure A- 1 shows the former way, EPS section and STP domains (#1 and #2) are segmented vertically and do not overlap. Bridge #A and #B of the boundary between EPS section and STP domains have both edge functions of EPS section and STP domains and interconnect the STP domains without looping problem which is shown in Appendix II. Another interaction way of EPS section and STP domains is shown in Figure A- 3. STP domains (#1 and #2) are segmented horizontally by EPS. Figure A- 4 shows one of derivation of Figure5. In this way Working entity and Protected entity for EPS are set separately in each VLAN and network resource within each STP domain would be used more effectively than the way of Figure A- 3.

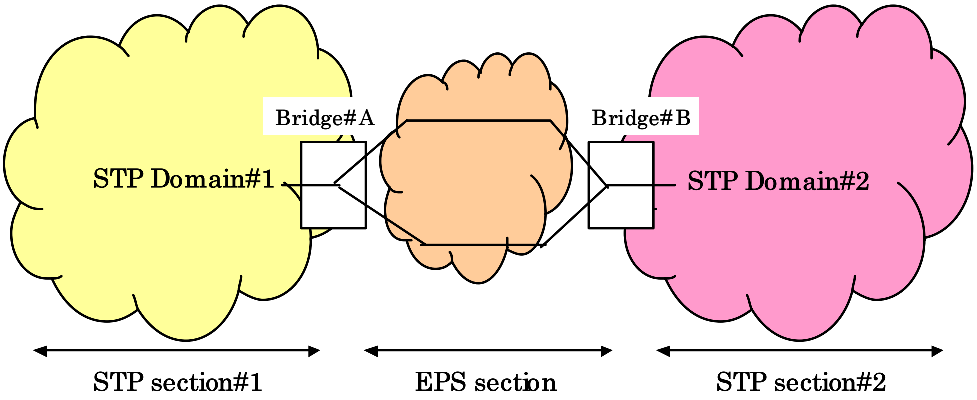


Figure A- 2 No overlapping interaction between EPS and STP

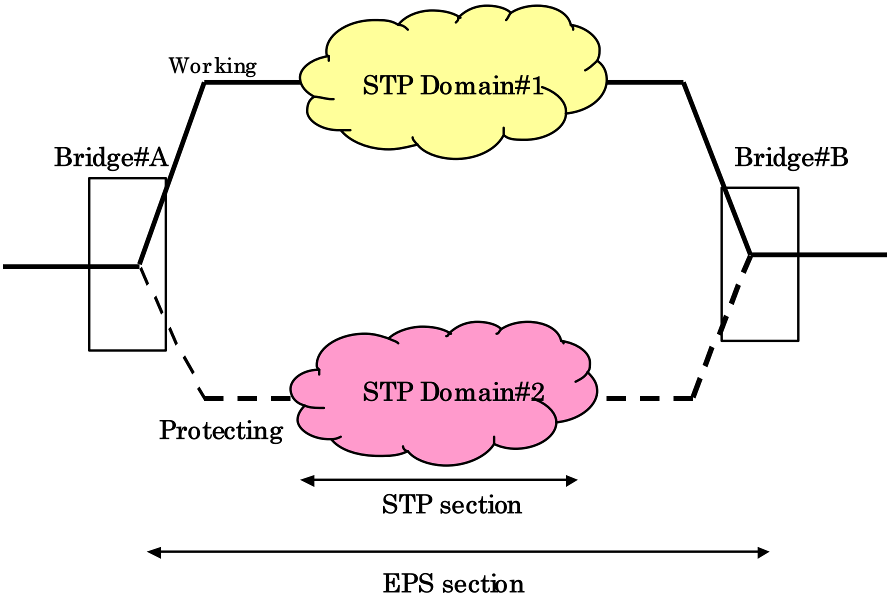


Figure A- 3 Overlapping interaction between EPS and STP

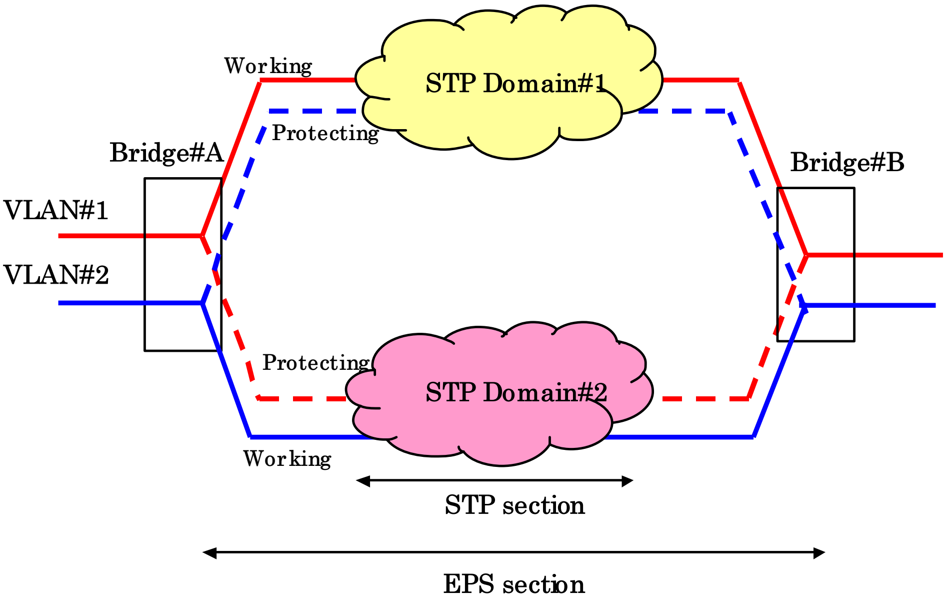


Figure A- 4 Overlapping interaction between EPS and STP per VLAN

APPENDIX I

Ethernet Protection Switching coexisting with Link Aggregation

In conventional ether network, Link Aggregation in IEEE802.3ad is widely used for the purpose of restoration in ETY level and virtual increase of link capacity. Since the scope of Link Aggregation is limited to ETY level, Ethernet Protection Switching (EPS) in Y.17ethps is applicable to support of requirement of ETH level protection. When EPS is introduced to conventional network that Link Aggregation is applied, application scenario coexisting with Link Aggregation and EPS should be considered.

Figure I- 1 shows an example of Link Aggregation and EPS coexisting network. LA is applied as ETY level function and EPS is ETH level function. In this scenario Ethernet Protection Section (between bridge #2 and #7) covers Link Aggregation (LA) section (between bridge #5 and #6, #11 and #12) and Ethernet Protection Section is superset of LA section. For example when i) link failure occurs between bridge #5 and #6 of working side, bridges on edge of Ethernet Protection switching (bridge #2 and #7) would detect of link failure in LA section by reception of ii) ETH-AIS from intermediate bridges (#5 and #6) or detection of LOC using ETH-CC between bridge #2 and #7. And finally iii) Ethernet protection switch is done between bridge #2 and #7F. As criteria for insertion of ETH-AIS the following case is considered.

Case 1) when one of aggregated links becomes failure

Case 2) when the predetermined number of aggregated links becomes failure

Case 3) when all of aggregated links become failure

Selection of these criteria depends on expected link capacity for protected entity. For example, if 100Mbps link capacity is expected for protected entity and three 100Mbps link is allocated in LA section, the criteria of case 3 will be selected because protected entity would not degrade until all aggregated links become failure. However, if 200Mbps or more link capacity is exptect for protected entity, the criteria of case 1 or 2 will be selected because protected would degrade before all aggregated links become failure.

In case of ETH-CC, ETH-CC passes through only one link of several aggregated links in LA section. Therefore ETH-CC would not detect a link failure in LA section because continuity of its ME level is still normal. As way to initiate protection switching for this case except ETH-AIS detection, ther are some possible scenario as follows.

1) To detect performance degradation by in-service test and/or performance monitoring.
2) Shutdown of all links in LA section by the criteria same as ETH-AIS insertion

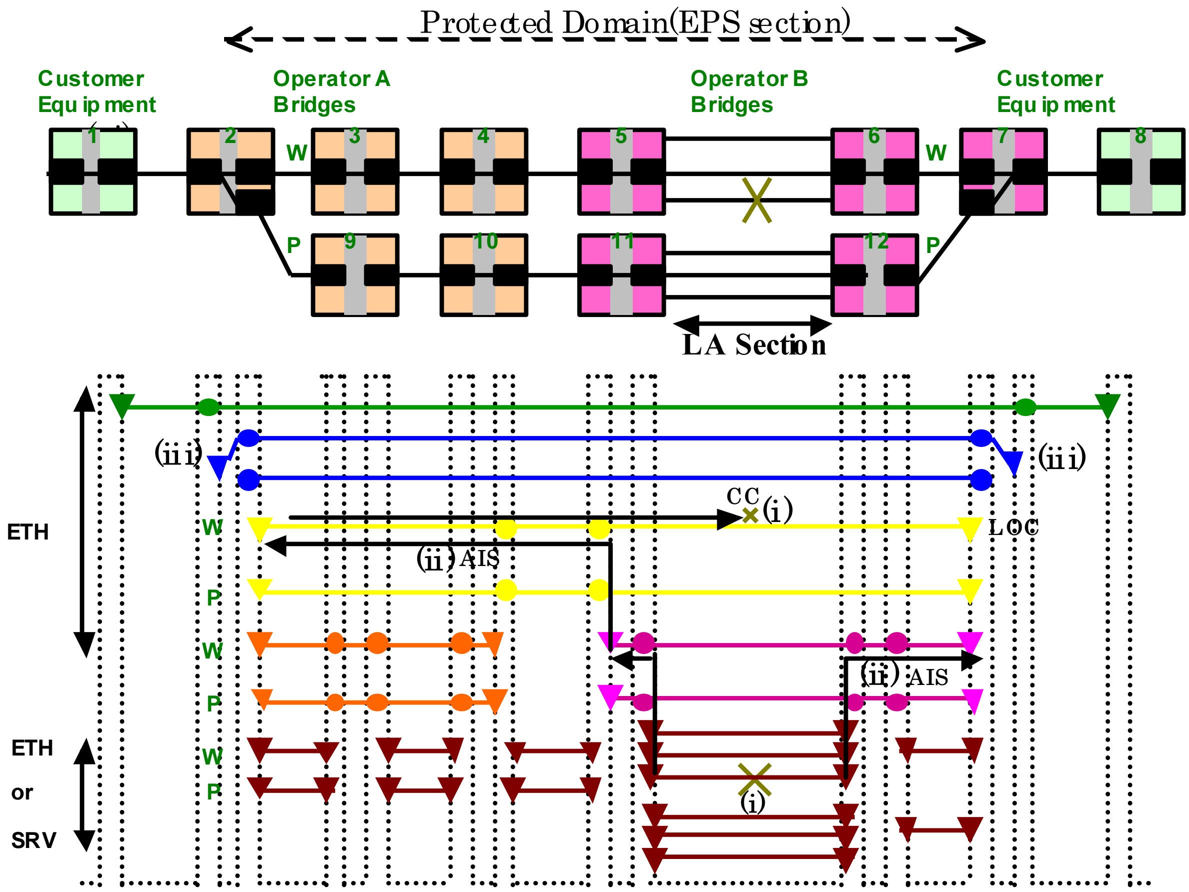


Figure I- 2 Example of LA and EPS coexisting in network

Figure I- 3 shows a specific case of Figure 1. In this scenario LA function and EPS function is applied in same adjacent bridges. This scenario could be applicable depending on implementation of bridge. This scenario is F.F.S because needs for this scenario is unclear. For example this scenario does not have any advantage compared with the case of Link Aggregation of six parallel links.

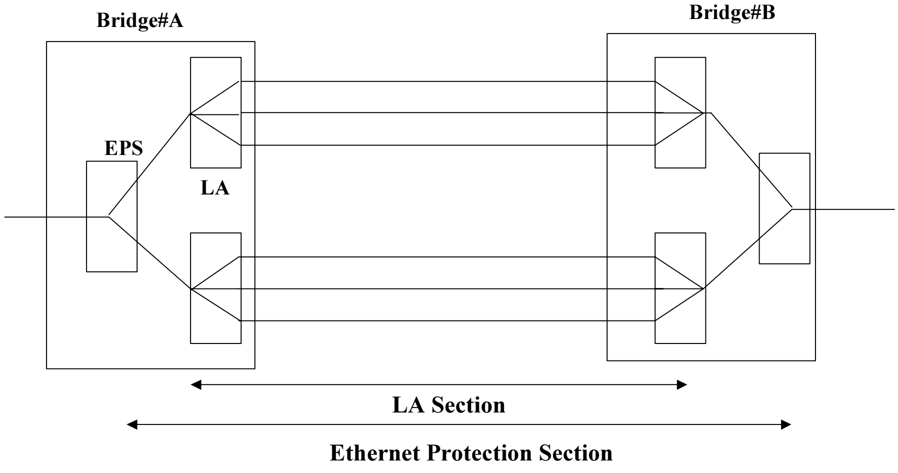


Figure I- 3 Example of LA and EPS coexisting in a bridge

APPENDIX II

Using Ethernet Protection switching to connect two STP domains

This section is an example of an application scenario in which we want to interconnect two STP domains. As will be shown in this section directly connected STP domain create looping problem. The solution could be to use protection switching domain between two STP domains.

In conventional ether network, STPs in IEEE802.1D and 1s is widely used for the purpose of restoration in EHY level as well as Ethernet Protection Switching. STPs support all network topology but the range of the trouble spread is wide. For example, one link failure would cause topology change of all networks within STP domain. Therefore segmentation of STP domain would be applied to minimise the range of the trouble spread and intersection of STP domain is required. Figure II- 1 shows case where intersection of STP domain becomes problem.

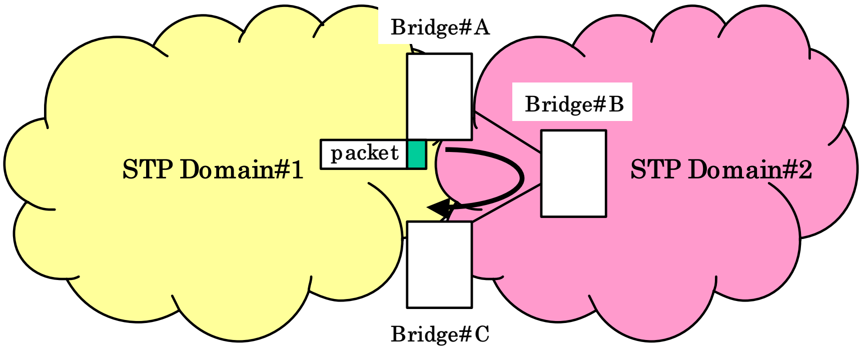


Figure II- 2 Case where intersection of STP domain becomes problem

Each STP domain is independent and the range of the trouble spread is restricted within each STP domain. One STP domain would form loop for the other STP domain. For example a packet which outputs from STP domain #1 to #2 would loop back via bridge #A, #B, and #C. To avoid this problem, each STP domain should connect within one bridge (Figure II- 3) or with one bridge (Figure II- 4). But these configurations have some limitation for reliability and distance of connected bridge because Link Aggregation is only applied to ETY link connection.

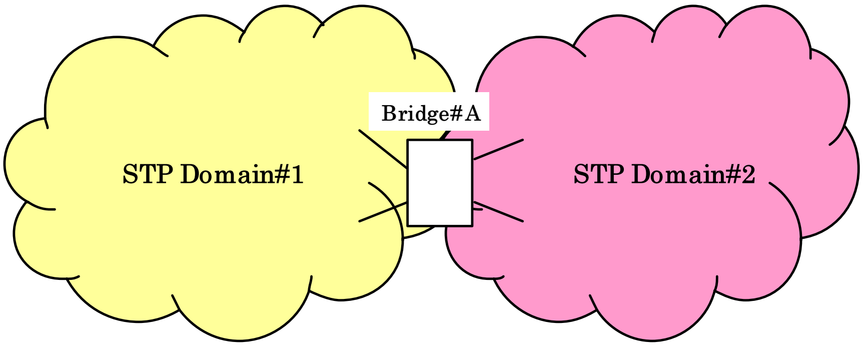


Figure II- 5 Case when STP domains connected within one bridge

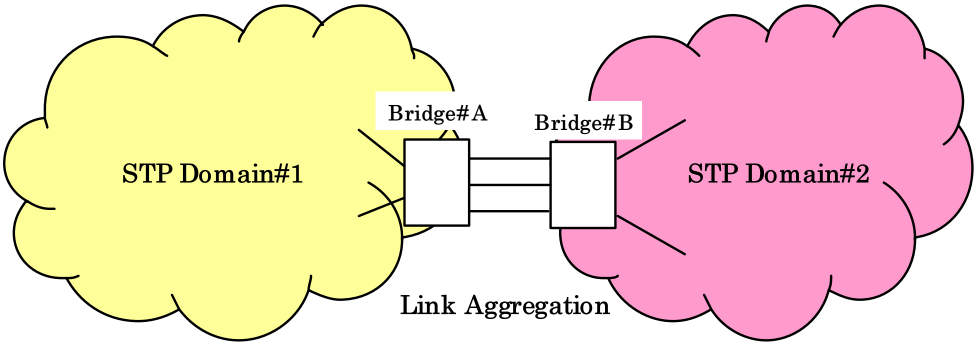


Figure II- 6 Case where STP domains connected with one bridge via single link or trunk

To solve the above-mentioned problem and eliminate the limitation, combination scenario of STP and Ethernet Protection Switching (EPS) is effective. Figure II- 7 shows case where STP domains connected with EPS section. In this case, there is no limitation for connection type between connected bridges (#A and #B). In addition to direct ETY link, connation via media converter and pseudo wire over SDH, ATM, and MPLS etc. are possible for connection type of between connected bridges.

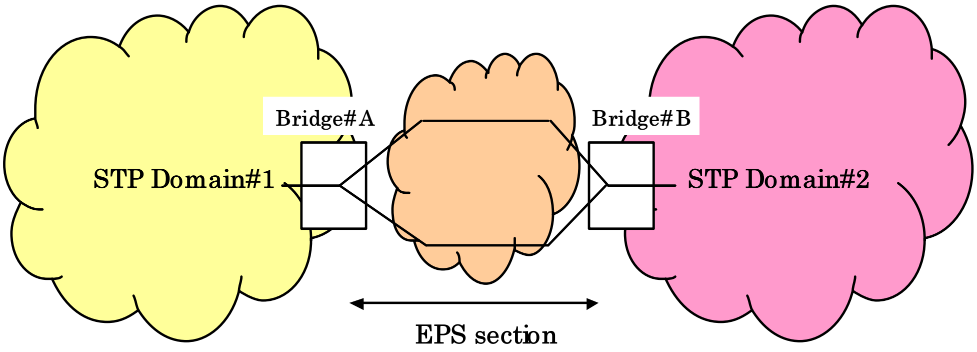


Figure II- 7 Case where STP domains connected with EPS section

APPENDIX III

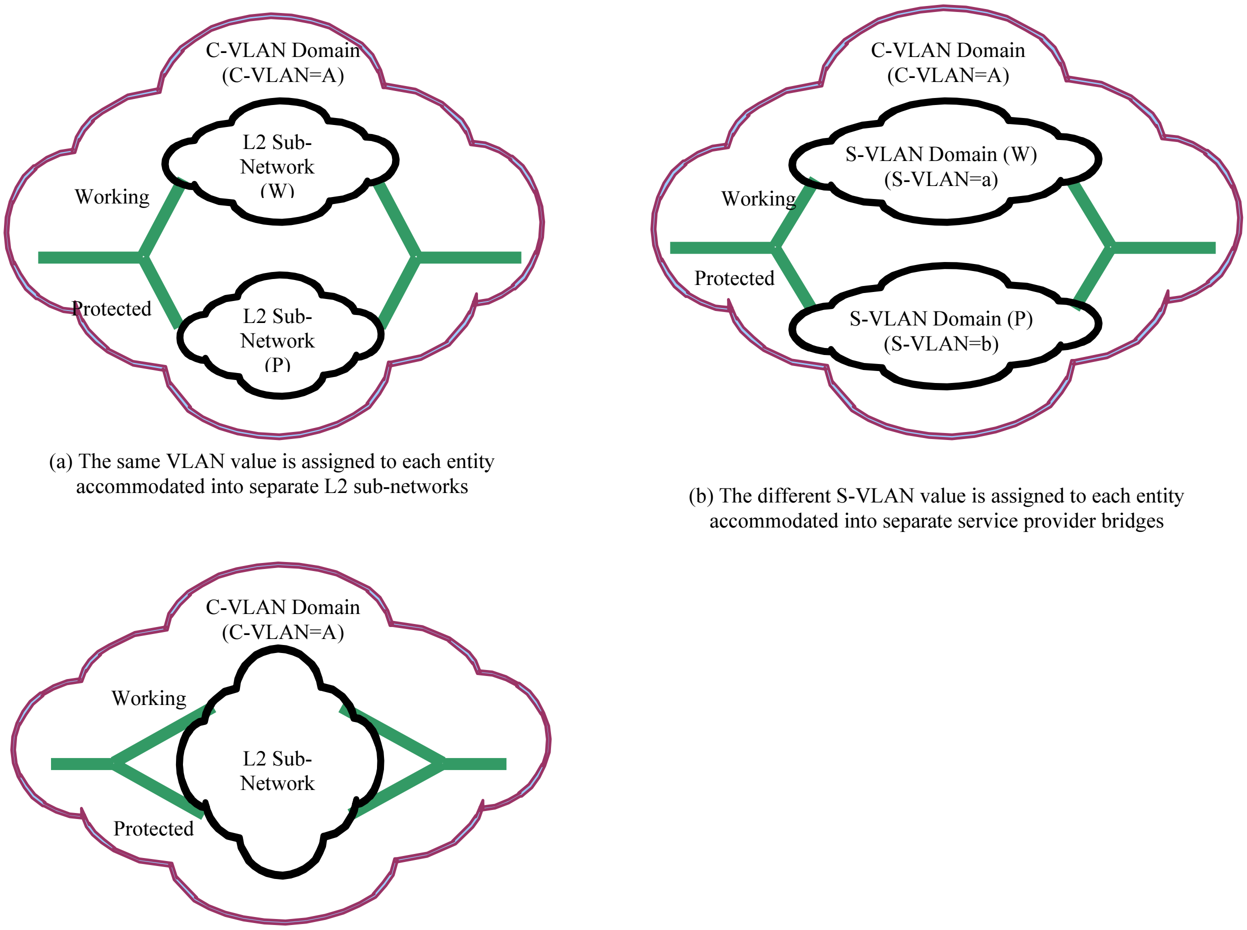
The Assignment of VLAN ID to Each Entity

This Appendix shows a guidance of allocation of VLAN ID to working and protected entity. Some variations can be considered. Some of them are practically applicable, but others are not. The applicable cases and inapplicable cases are shown in Fig. 1 where three patterns are shown:

(a) The same VLAN value is assigned to each entity, and the each entity is accommodated into separate L2 sub-networks. The L2 frames with the same VID will not be mixed up because their network is physically separated. Therefore this is an applicable case.

(b) The different S-VLAN value is assigned to each entity, and they are accommodated into separate service provider bridges. This case will most probably occur when the S-tag encapsulates customer frames. Each entity is encapsulated by separate S-tag; in this example S-tag is 'a' and 'b' respectively. The L2 frames with the different S-Tag will not be mixed up because S-tag handler will properly distinguish them. Therefore this is also an applicable case.

(c) The same VLAN value is assigned to each entity, and they are accommodated into the same L2 sub-networks. The L2 frames with the same VID will be confused because their network is not physically separated, and the intermediate nodes are possible to confuse. Therefore this is an inapplicable case.



(a) The same VLAN value is assigned to each entity accommodated into separate L2 sub-networks

(b) The different S-VLAN value is assigned to each entity accommodated into separate service provider bridges

(c) The same VLAN value is
assigned to each entity accommodated into the same L2

Figure III- 1 VLAN Value of Working and Protected entities