Draft Recommendation Y.17ethps

Ethernet Protection Switching

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.

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 Draft Recommendation G.8010, *Generic functional architecture of transport networks*

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

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

[5] IEEE 802.1D, 1998, *Spanning tree protocol*

[6] IEEE 802.1w, 2001, *Rapid Spanning Tree Protocol (RSTP)*

[7] IEEE Draft 802.1s, *Multiple Spanning Tree Protocol (MST)*

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

EDITOR'S NOTE:

Contribution WD3_GVA_05 is addressed.

Spanning tree protocol is assumed not to be use with Ethernet protection switching protection and clarification of interlocking between Spanning tree protocol and Ethernet Protection Switching is for further study.

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.

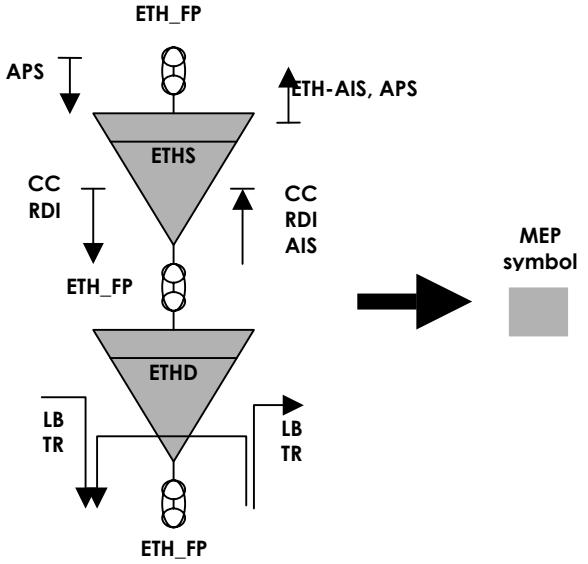


Figure 1/Y.ethps Maintenance entity End Point (MEP) symbol

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

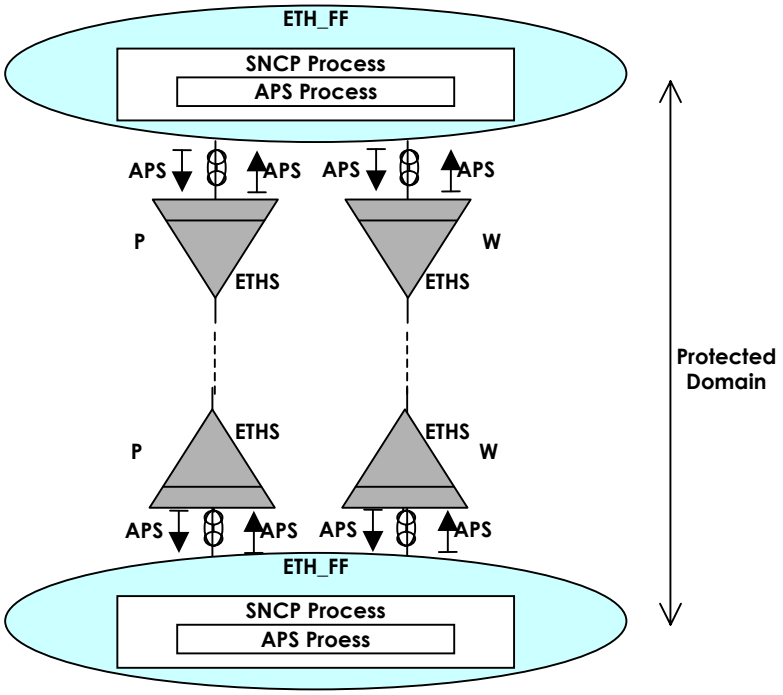


Figure 2/Y.ethps Relationship of ETH_FF and MEP

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.

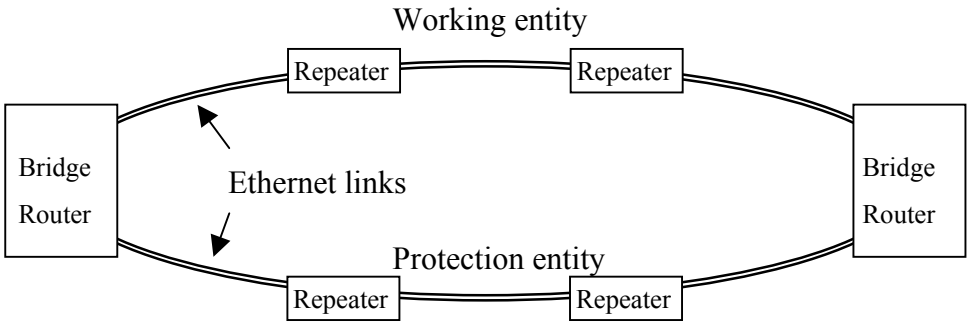


Figure 3/Y.ethps p-p Ethernet Trail protection

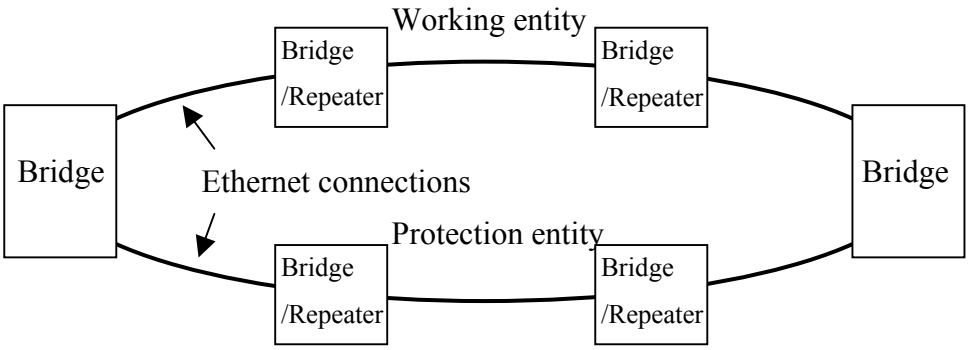


Figure 4/Y.ethps p-p Ethernet SNC protection

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.ethps. The OAM levels of working transport entity and protection entity can be set independently.

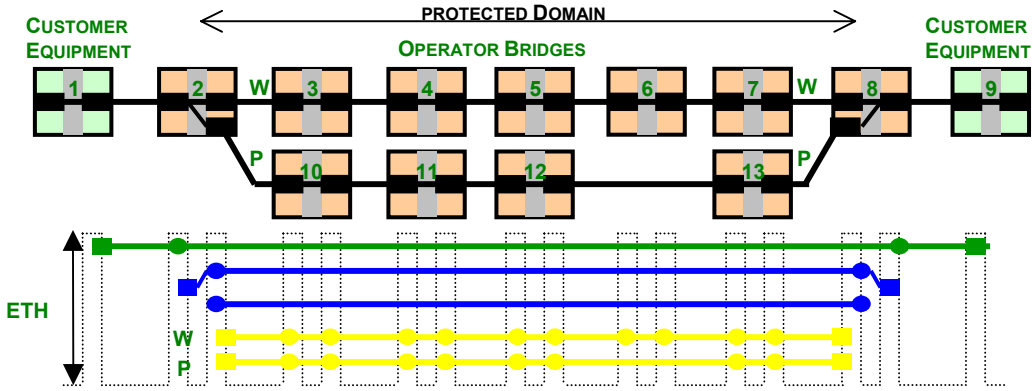


Figure 5/Y.ethps UNI-UNI ETH SNC/S Protection in single operator network

Figure 6/Y.ethps 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.

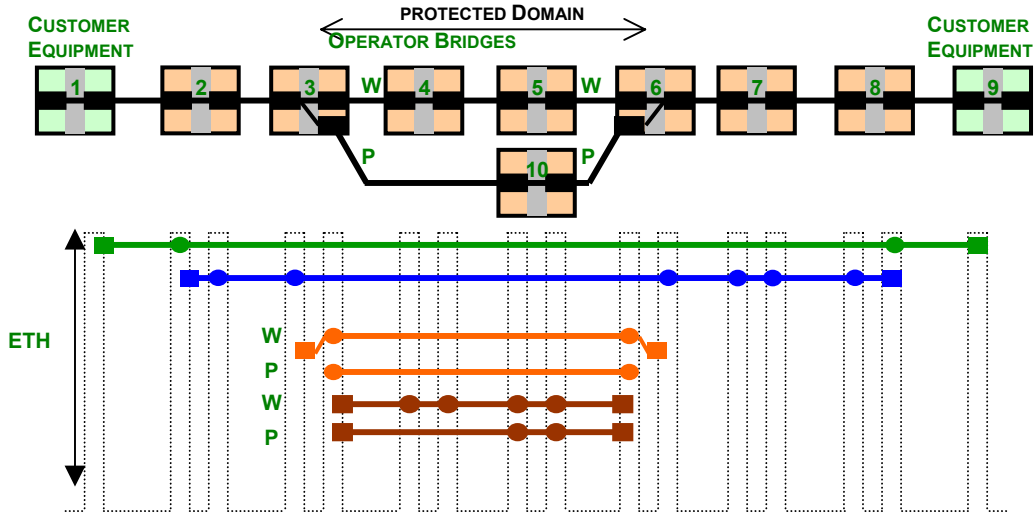


Figure 6/Y.ethps UNI-UNI ETH SNC/S Protection in single operator network

More details of the law for configuration of level need to be discussed. Figure 7/Y.ethps 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)

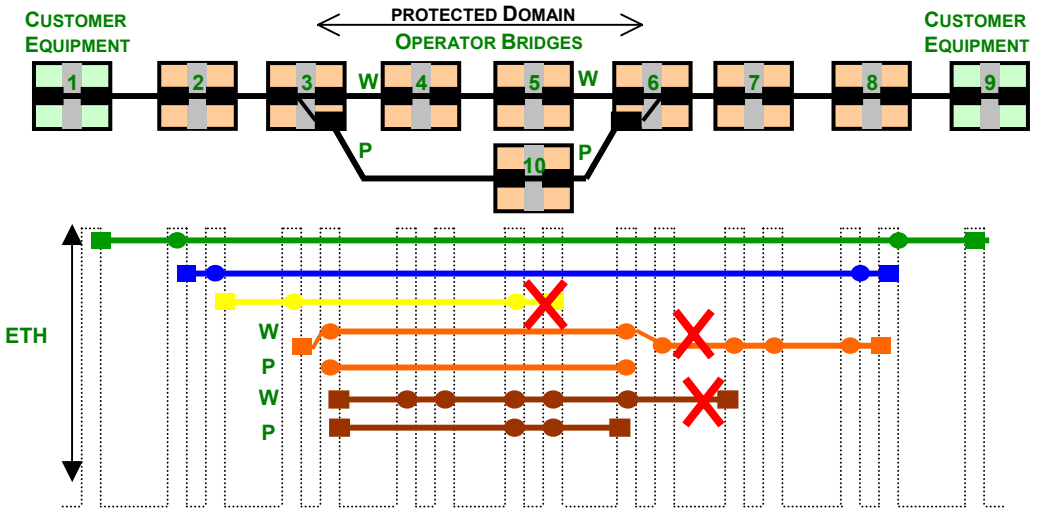


Figure 7/Y.ethps UNI-UNI ETH SNC/S Protection in single operator network

6.2.1.2 Multi Operator Case

6.2.1.2.1 Multi Operator Case with Single Protected Domain

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

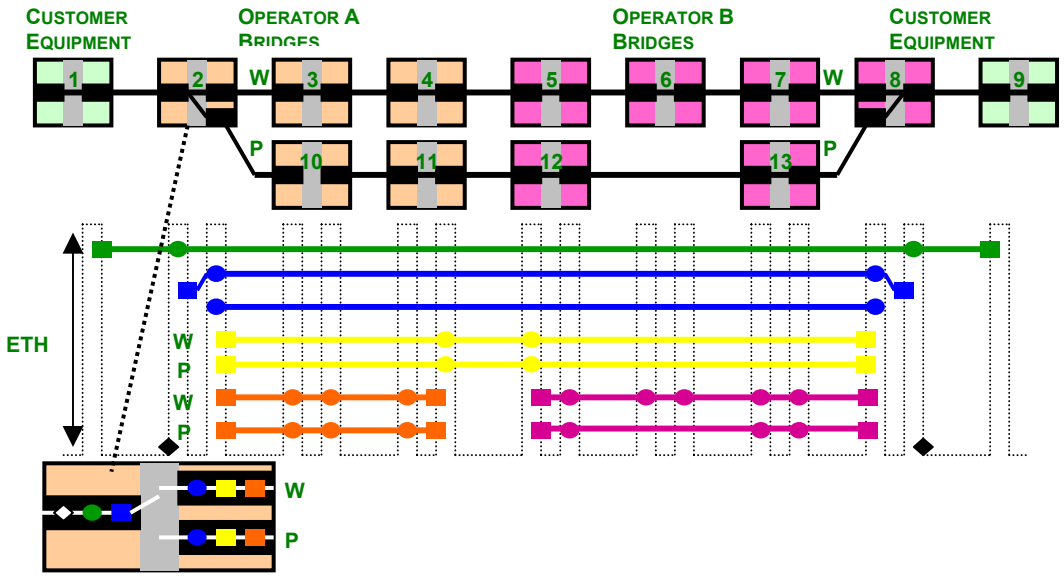


Figure 8/Y.ethps UNI-UNI ETH SNC/S Protection in multi operator network

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.ethps. Two operators independently preside each protected domain.

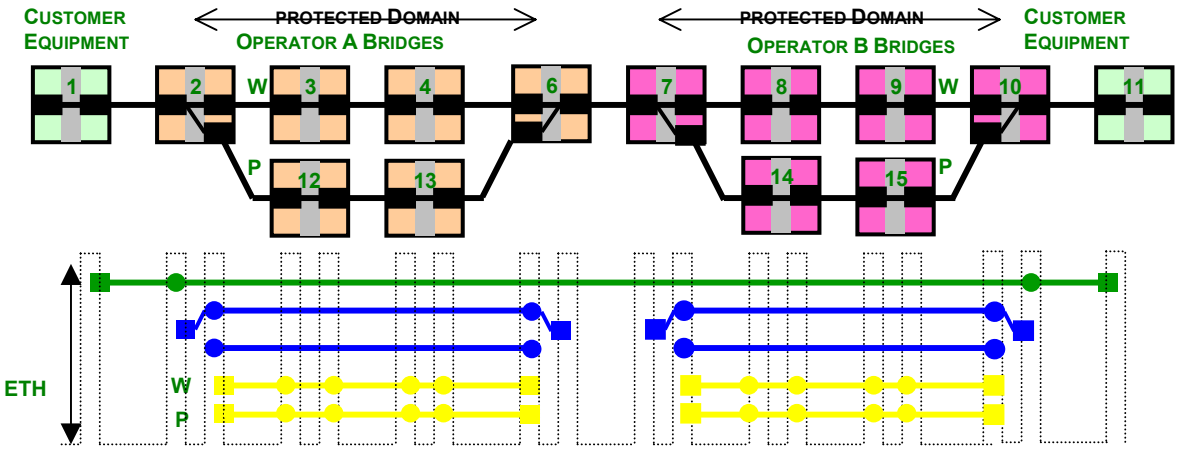


Figure 9/Y.ethps ETH cascaded SNC/S Protection in multi operator network

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.ethps 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.

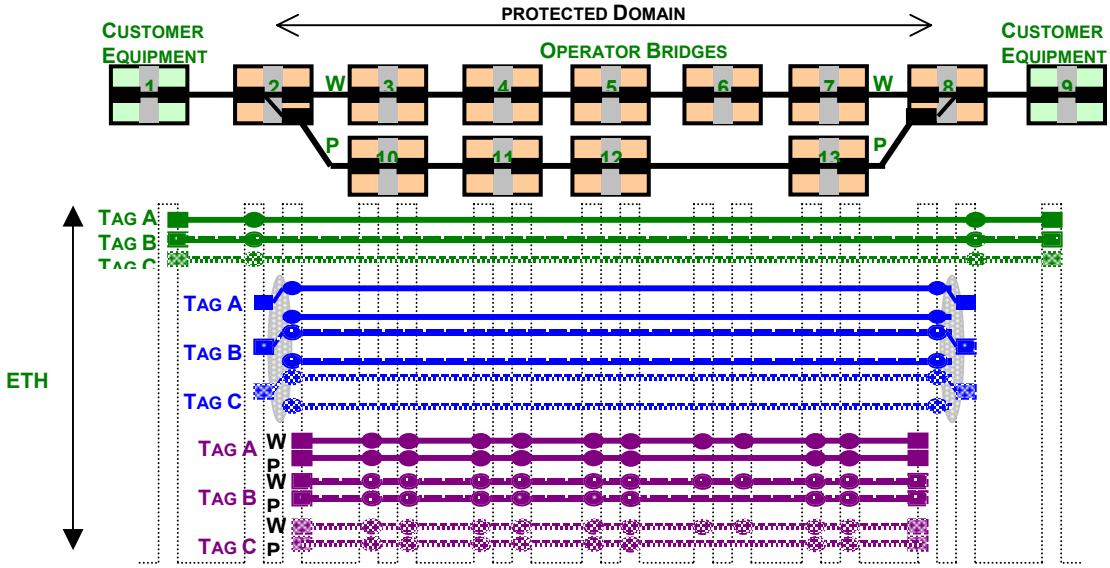


Figure 10/Y.ethps ETH SNC/S Group Protection in single operator network

Figure 11/Y.ethps 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.

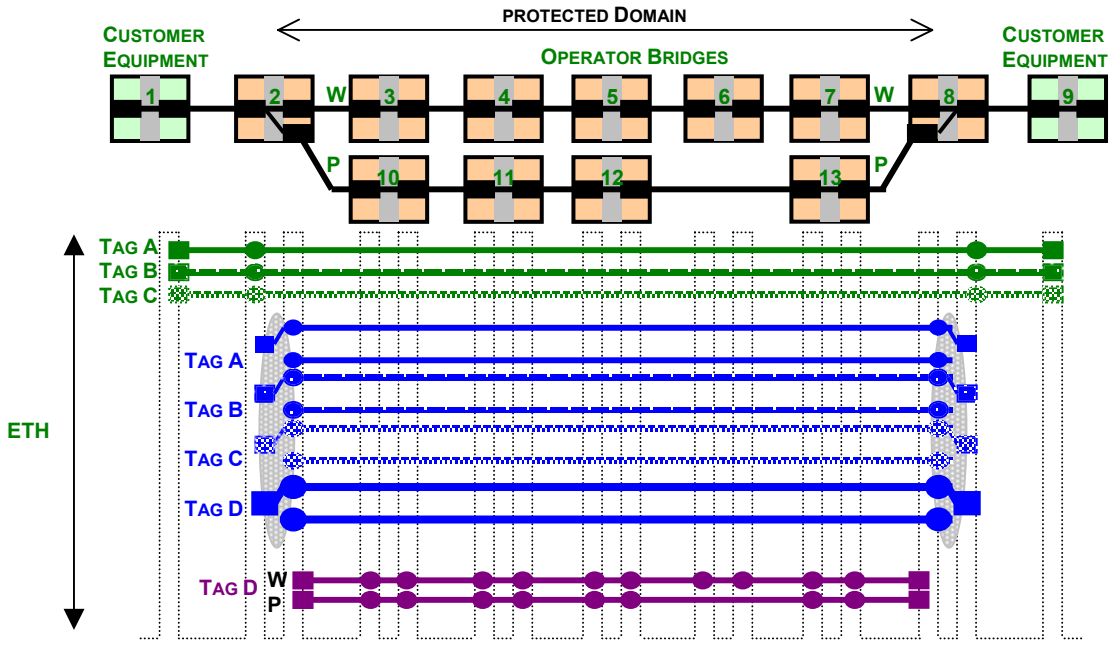


Figure 11/Y.ethps ETH SNC/Ts Group Protection in single operator network

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.ethps 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.

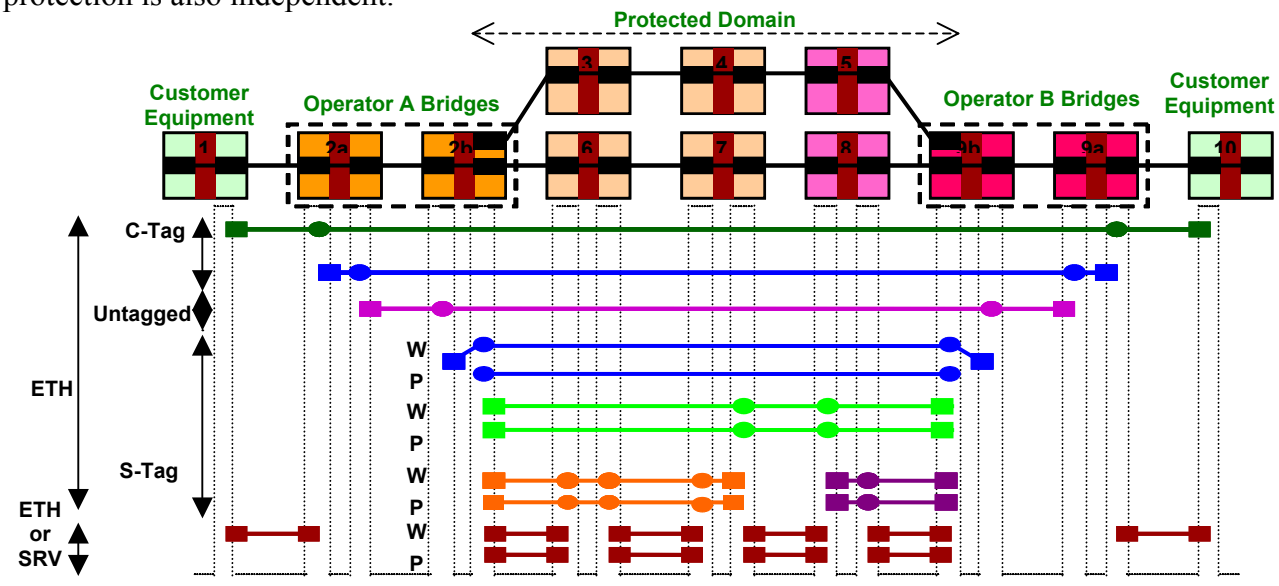


Figure 12/Y.ethps Network model of ETH SNC/S Protection with Dual Relay Model with Bundling

6.4. Group Protection model for Dual Relay Model with Bundling

Figure 13/Y.ethps 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.

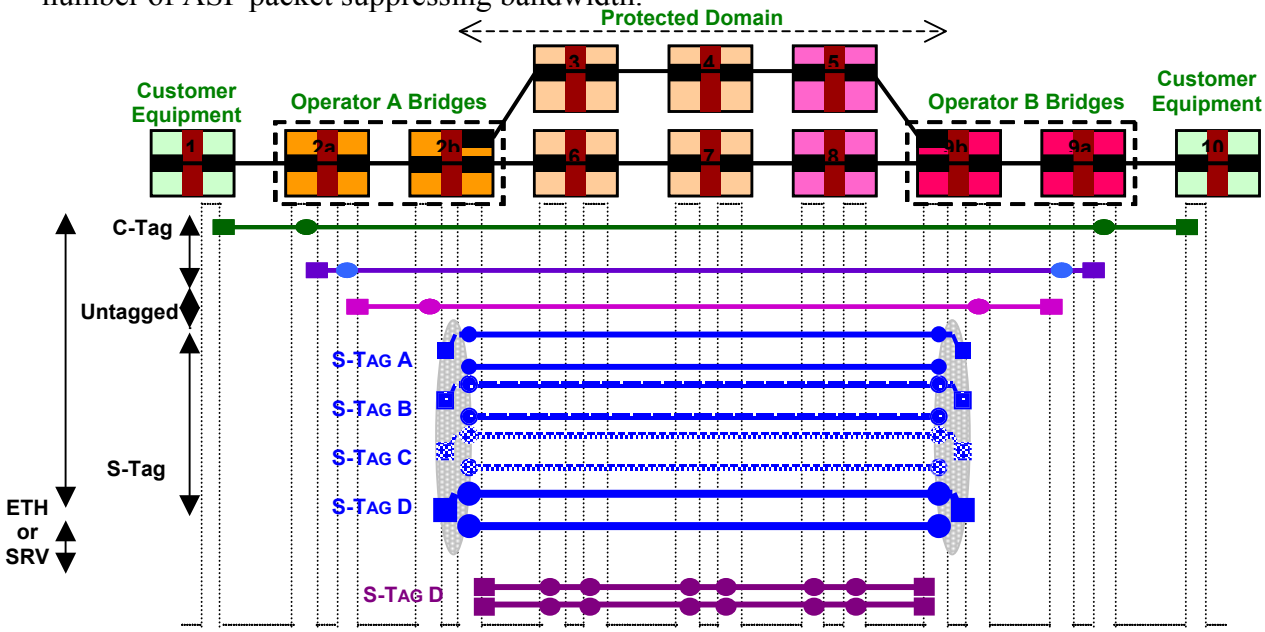


Figure 13/Y.ethps Network model of ETH SNC/T Group Protection with Dual Relay Model with Bundling

Further encapsulation method by another Tag is for further study.

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.
Interruption time	Fast recovery should be provided. 50ms is proposed for the objective for interruption.
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.

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 EHH-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

Two of ETH-APS flows are shown according to the switching trigger. 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

The first case is the trigger using ETH-AIS where a failure is detected by MIP that has an ability to send ETH-AIS, shown in Figure 14/Y.ethps. 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.

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 15/Y.ethps. 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.

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

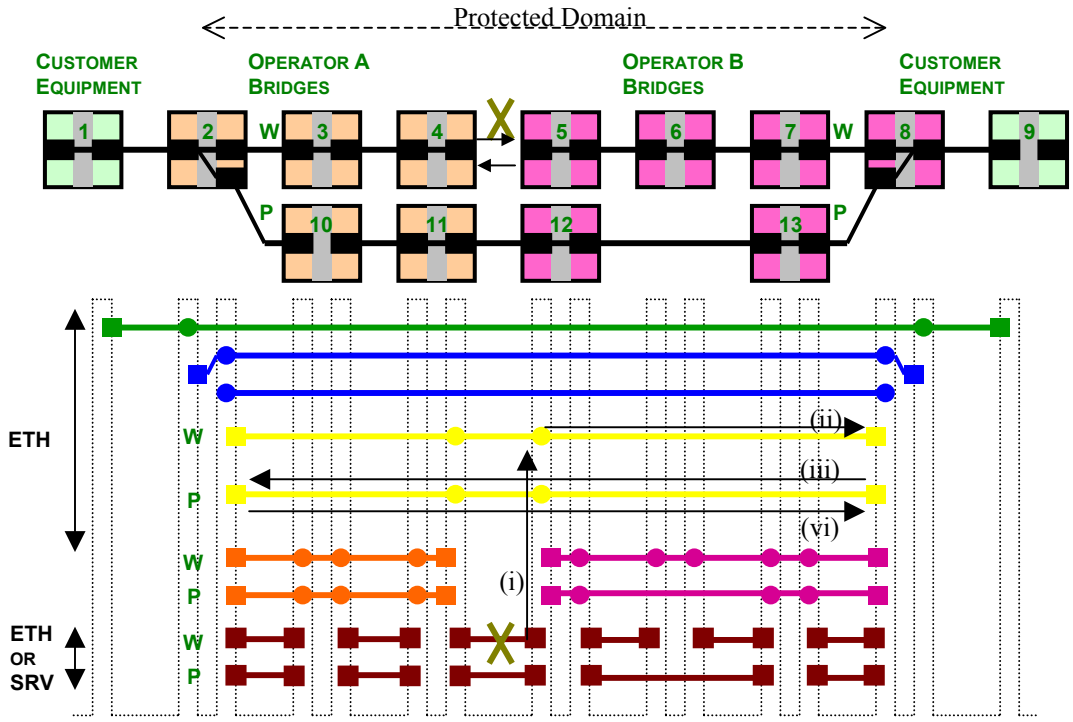
The ETH-APS flow encapsulated in S-TAG using ETH-CC is shown in Figure 16/Y.ethps. The switching mechanism is along these following procedure:

(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.

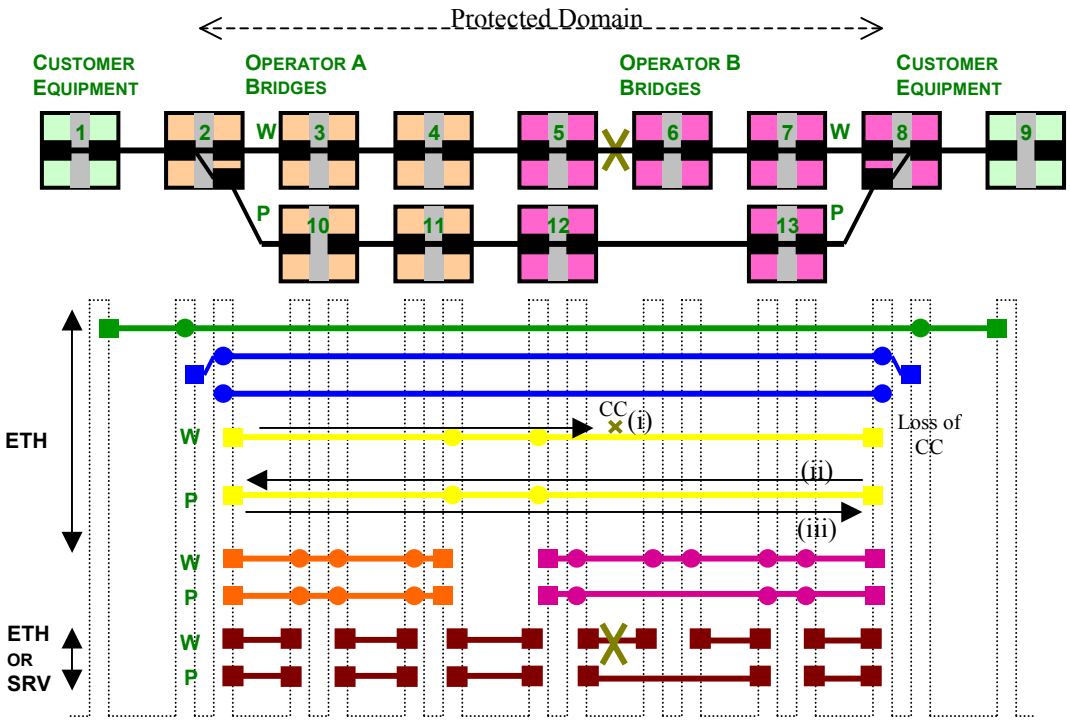
(iii) MEP of equipment 2b send back ack ETH-APS at level yellow that is terminated at MEP of equipment .6b.

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.



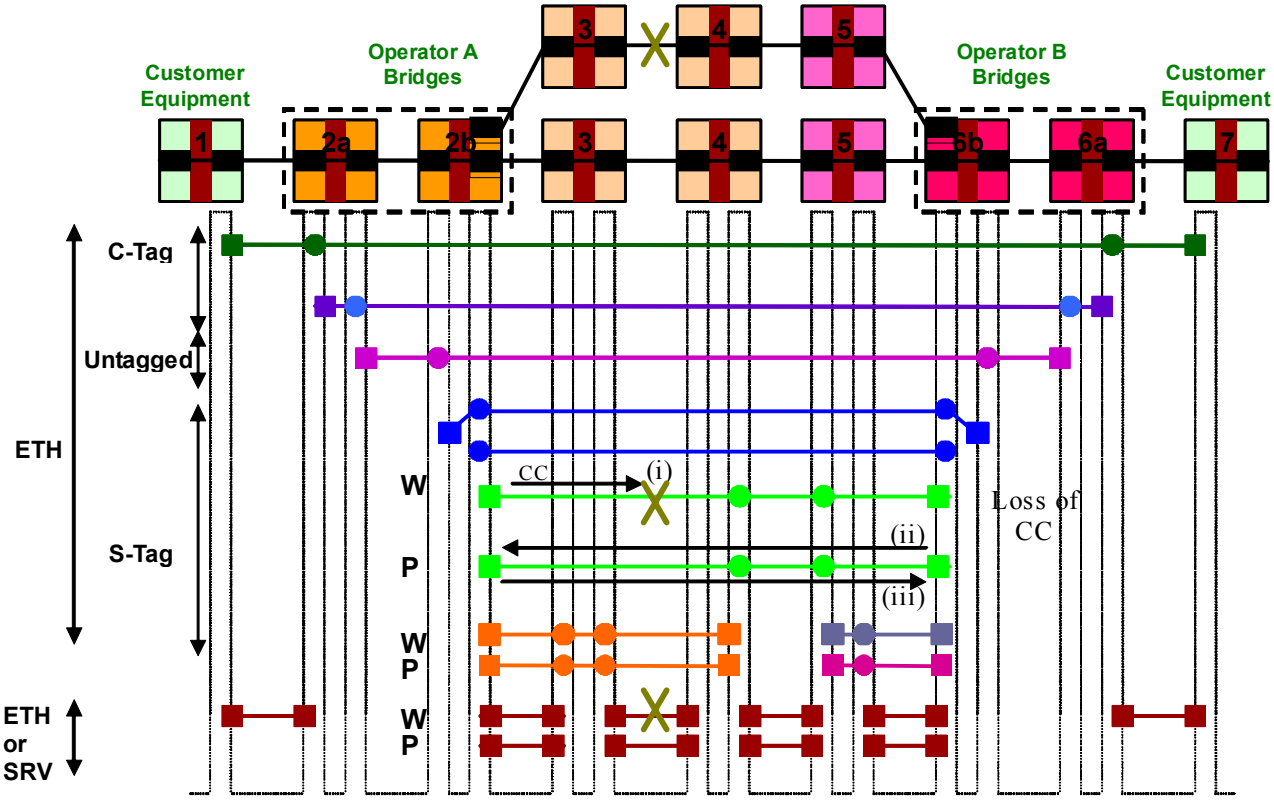
(i) ETH or SRV MEP of working entity detects failure then inserts FDI to MIP of the upper level at equipment 5.
(ii) FDI is transfered via MIP at equipment 5 at level yellow that is terminated at MEP of equipment 8.
(iii) MEP of equipment 8 send APS to protected side at level yellow that is terminated 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 14/Y.ethps ETH-APS flow triggered by ETH-AIS applied at SNC protection



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

Figure 15/Y.ethps ETH-APS flow triggered by Loss of ETH-CC applied at SNC protection



(i) 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 APS to protected side at level yellow that is terminated at MEP of equipment 2b.
(iii) MEP of equipment 2b send back ack APS at level yellow that is terminated at MEP of equipment .6b.

Figure 16/Y.ethps 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.

_____