Two-Port MAC Relay Use Cases, Etc

David W. Martin
Nortel
v01

IEEE 802.1
September 19-22, 2005
Garden Grove, CA

Context

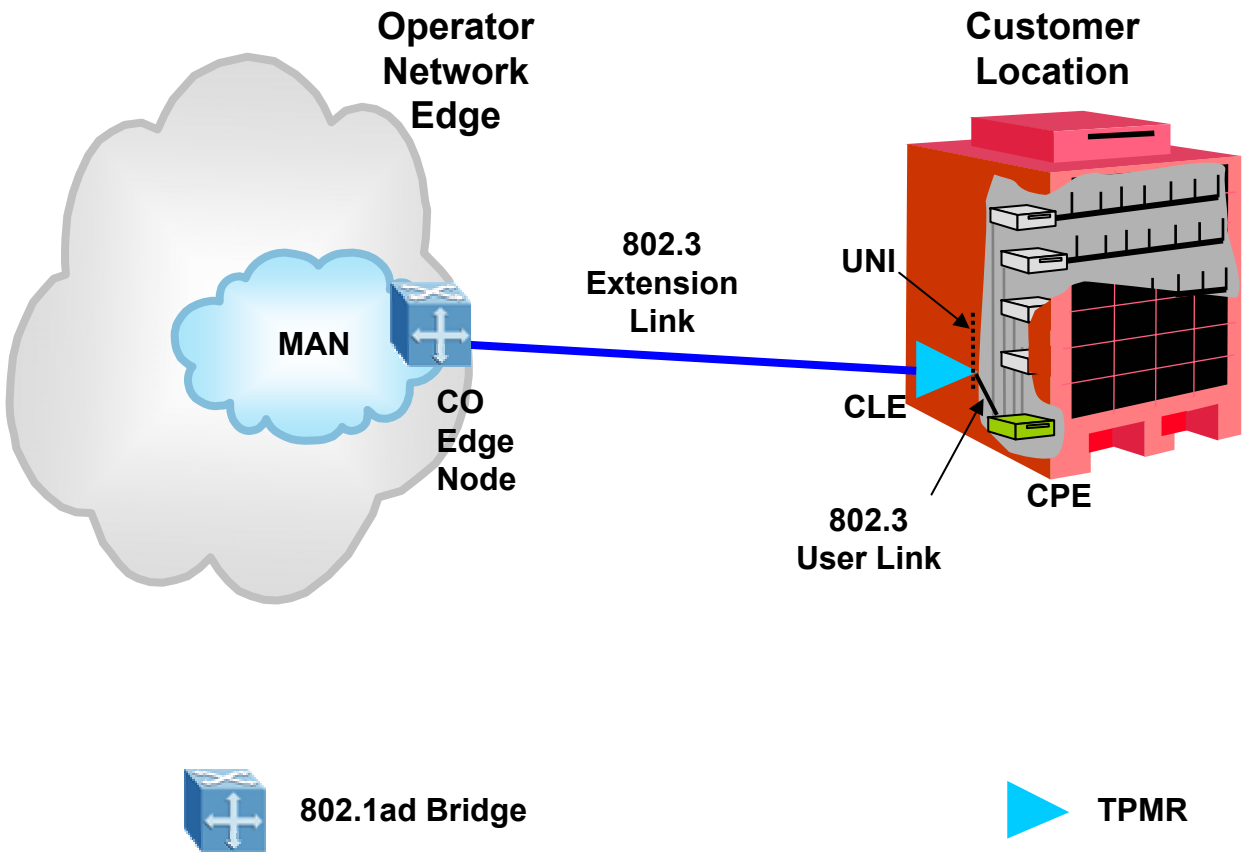
- There are several Editor's Notes in P802.1aj/D1.1 clause 22 requesting input on:
  - Use cases (c22.3.1.1)
  - Failure notification (c22.3.2)
  - Daisy chain impact (c22.3.2)
  - EFM OAM extensions (c22.5)

Agenda

- Uses Cases
- Failure Notification
- EFM OAM Extensions
- Summary

(some)
Use Cases

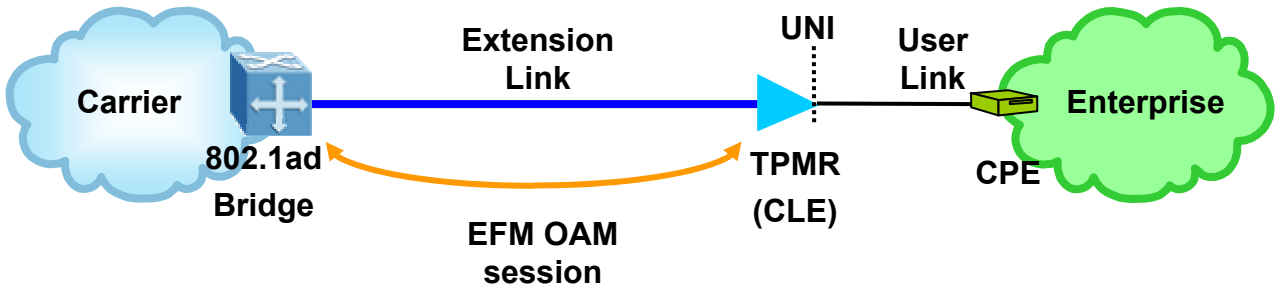
Use Case 1


Operator
Network
Edge
Customer
Location
MAN
802.3
Extension
Link
UNI
CLE
CO
Edge
Node
CPE
802.3
User Link
802.1ad Bridge
TPMR

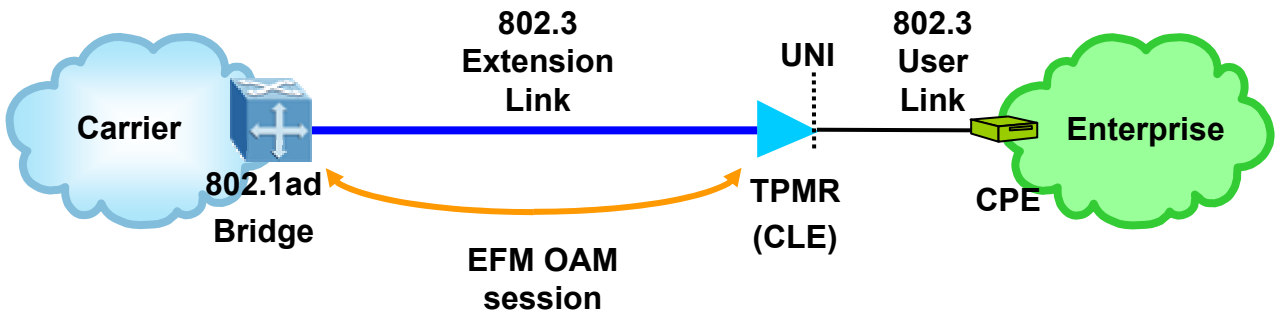
Use Case 1 (cont'd)

Likely Extension Link types:
- **1000BASE-LX, LX10, 'ZX'**

Likely User Link types:
- **10/100BASE-T,**
- **1000BASE-CX, T**

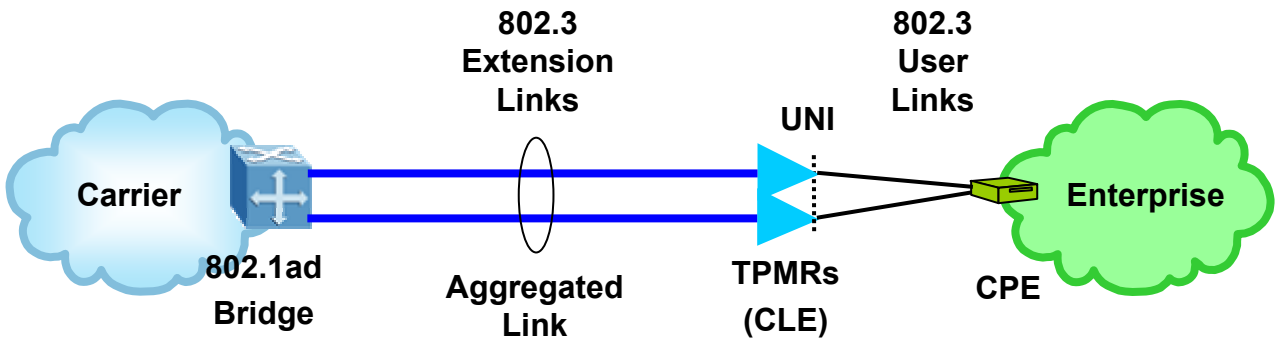


Use Case 1 (cont'd)



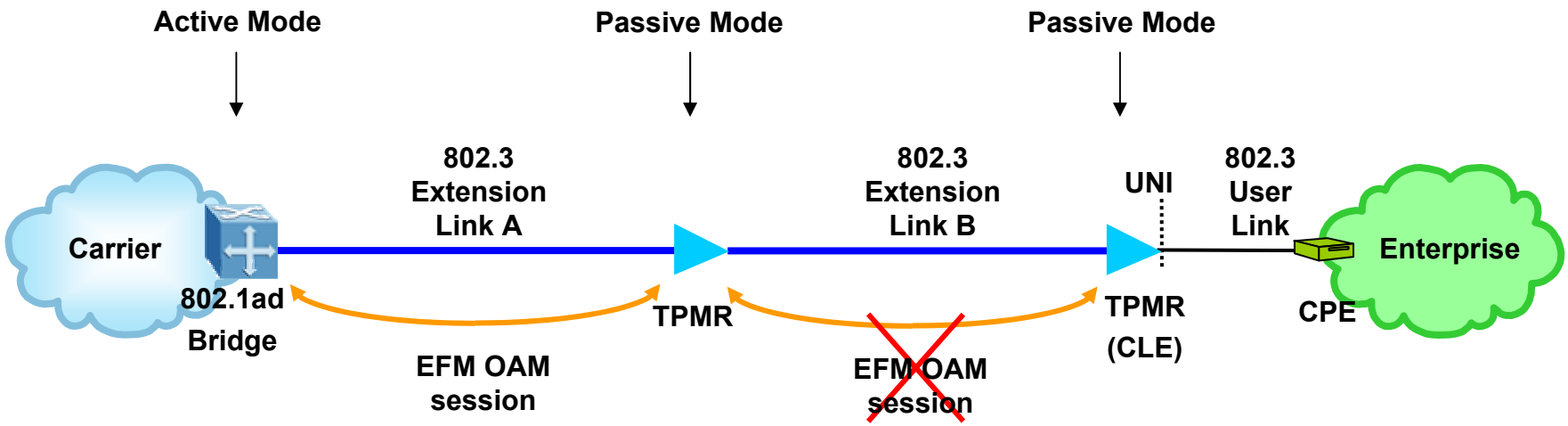
- EFM OAM provides the CO bridge the ability to:
  - Put the TPMR into an intrusive loopback for OOS testing (turn-up, troubleshooting)
  - Query the 802.3 MIB
  - Be notified of critical events (Link Fault, Dying Gasp, Critical Event), and vice versa
  - Be notified of link performance events (ESP, EFS, EFP, EFSS), and vice versa
- Allows extensions (Organization Specific OAMPDU, Info TLV, Event TLV) we can leverage to manage the port facing the User Link/CPE, and typical Bridge-related objects

Use Case 2



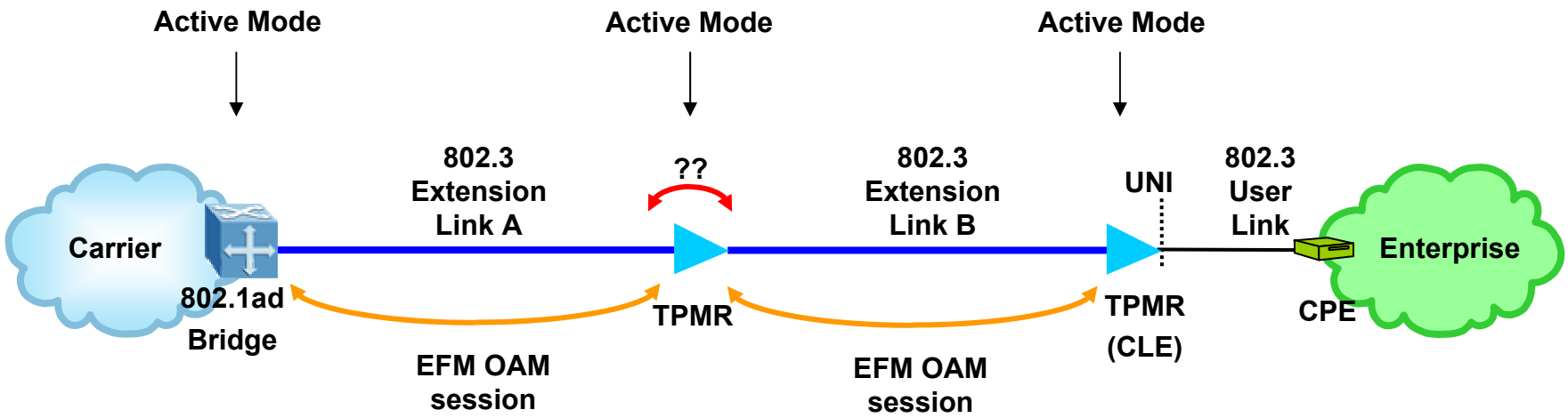
- The TPMRs are transparent to clause 43 Link Aggregation (802.3ad)
- Each is managed separately by the CO bridge (as in Case 1)

Use Case 3



- When used as a demarc device, commercial TPMRs power-up in EFM OAM Passive mode, waiting to hear from the Active mode CO master
- A Passive-to-Passive EFM OAM session will never activate – would never make it through the Discovery process

Use Case 3 (cont'd)



- Would require some EFM OAM relay mechanism on center TPMR to allow CO bridge to query the CLE TPMR and to be notified of Link B events detected by CLE TPMR
- Would require different EFM OAM handling of loopback on center TPMR to allow CO bridge to test Links A+B with CLE TPMR in loopback

Use Case 3 (cont'd)

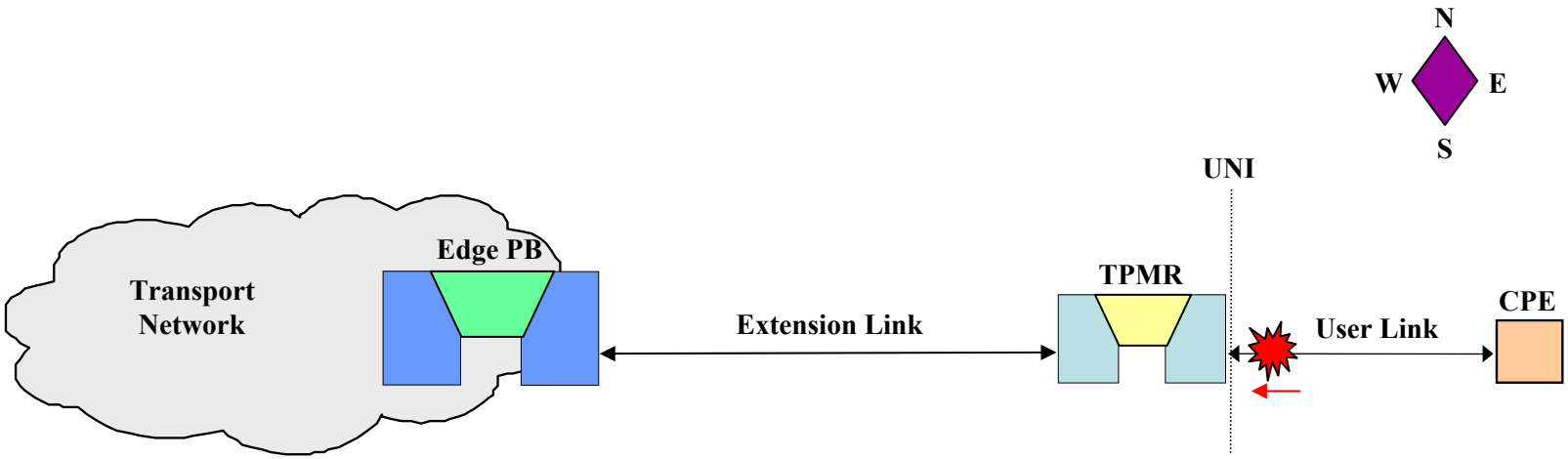
- What if more TPMRs were daisy chained?
- Do we preclude such scenarios?
- Or do we add optional support for SNMP to cover daisy chained cases?
- For non-802.3 media will need something other than EFM OAM
- Needs discussion…

Failure Notification

Guiding Assumptions

- Case 1 context: single TPMR, 802.3 media
- TPMR leverages EFM OAM
- TPMR does not support P802.1ag CFM…

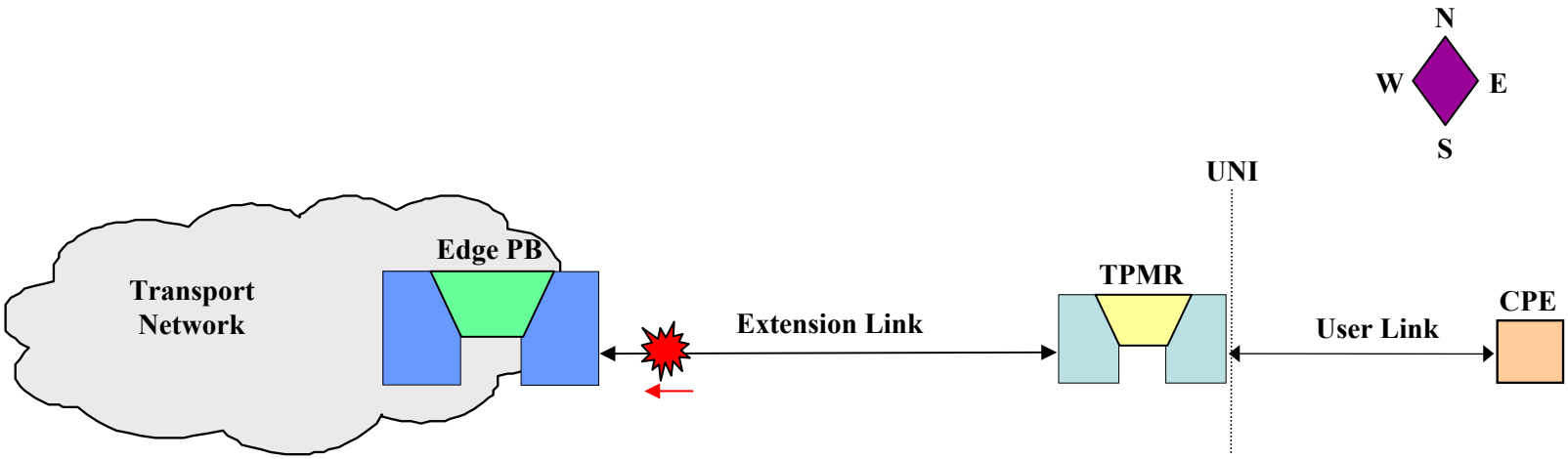
Westbound User Link Fail



P802.1aj Proposal

- **TPMR sends EFM Critical Event flag with Organization Specific Info TLV with indication of Remote Link Fail, shuts down TX to CPE, if Auto-Negotiation enabled sends Remote Fault to CPE.**
- **Edge PB sends ETH_AIS into network per P802.1ag.**

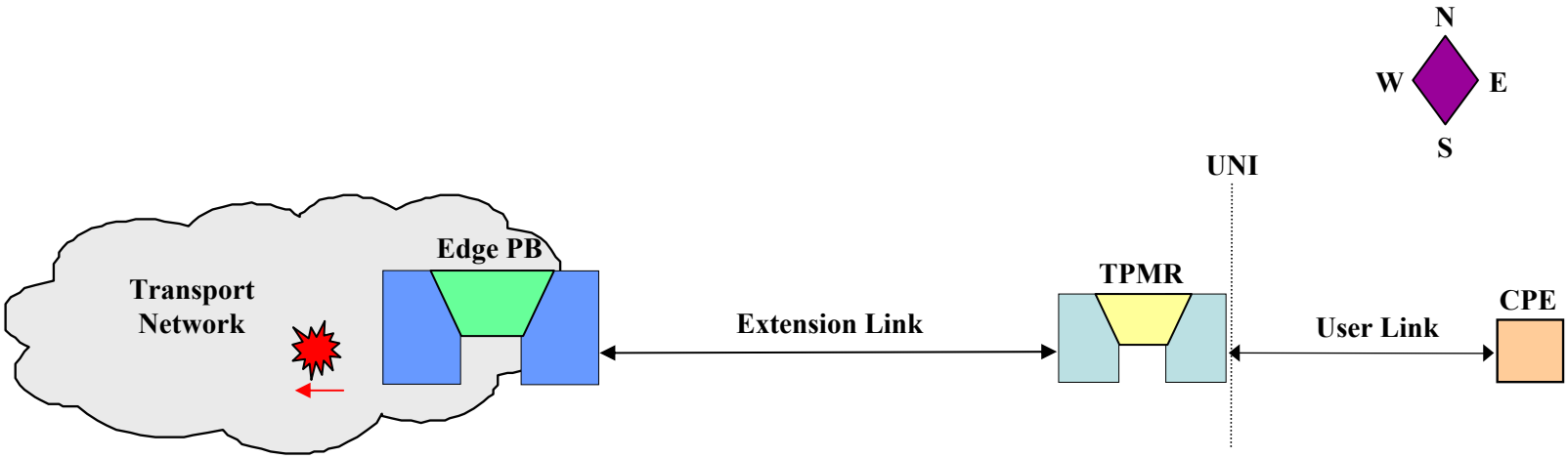
Westbound Extension Link Fail



P802.1aj Proposal

- **Edge PB sends EFM Link Fault flag towards TPMR. TPMR shuts down TX to CPE. TPMR ignores failures detected from CPE during TX shutdown.**
- **Edge PB sends ETH_AIS into network per P802.1ag.**

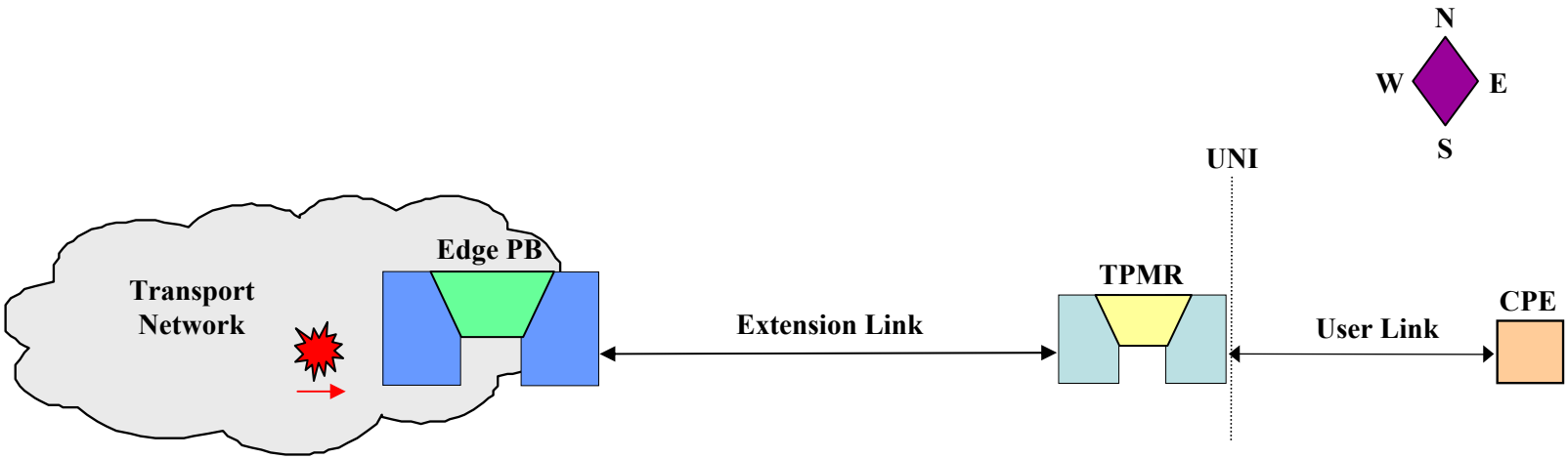
Westbound Network Connection Fail



P802.1aj Proposal

- **Edge PB may receive ETH_RDI (depending on P802.1ag evolution), if notified it sends EFM Critical Event flag with Organization Specific Info TLV with indication of Network Connection Fail towards TPMR (E-Line services).**
- **TPMR shuts down TX to CPE. TPMR ignores failures detected from CPE during TX shutdown.**

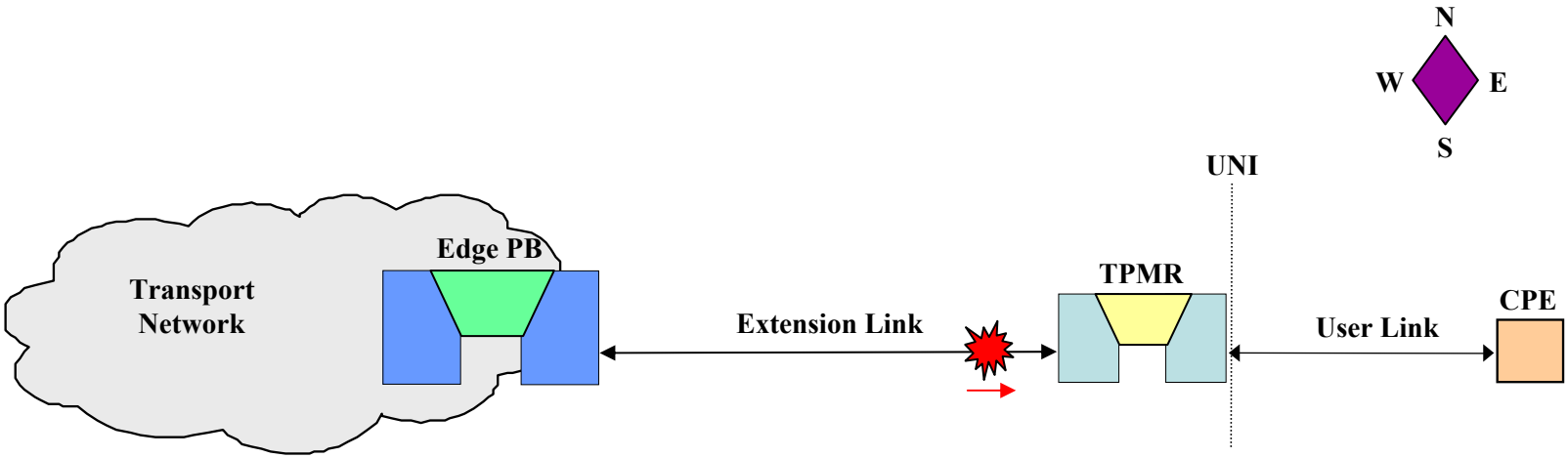
Eastbound Network Connection Fail



P802.1aj Proposal

- **Edge PB detects fault directly or ETH_AIS per P802.1ag (and possibly sends ETH_RDI back into network depending on P802.1ag evolution), sends EFM Critical Event flag with Organization Specific Info TLV with indication of Network Connection Fail towards TPMR (E-Line services).**
- **TPMR shuts down TX to CPE. TPMR ignores failures detected from CPE during TX shutdown.**

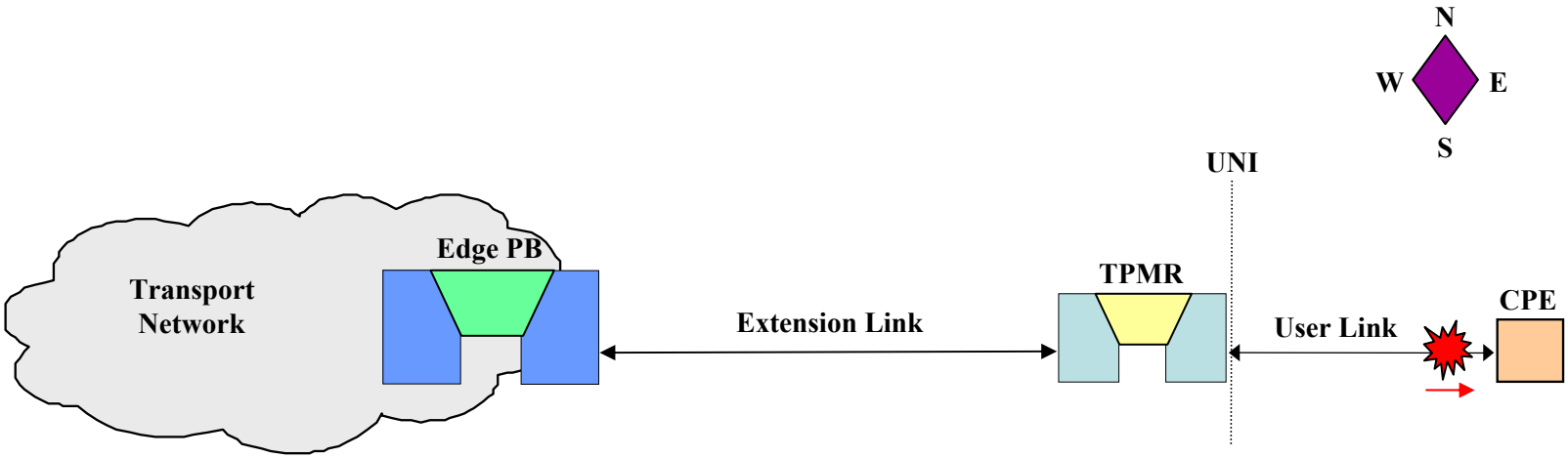
Eastbound Extension Link Fail



P802.1aj Proposal

- **TPMR shuts down TX to CPE and sends EFM Link Fault flag towards Edge PB. TPMR ignores failures detected from CPE during TX shutdown.**
- **Edge PB possibly sends ETH_RDI (depending on P802.1ag evolution) towards network.**

Eastbound User Link Fail



- If the CPE leaves its TX on, and if Auto-Negotiation is disabled, and assuming the CPE doesn't support EFM OAM Link Fault, then no failure is detectable by the TPMR.
- If Auto-Negotiation is enabled, then…

P802.1aj Proposal

- TPMR detects Remote Fault and sends EFM Critical Event flag with Organization Specific Info TLV with indication of Remote Link Fail towards PB.
- Edge PB sends ETH_AIS into network per P802.1ag.

Conditioning Rules Summary

TPMR ingress User Link port detects:
- **Input link failure,**

Consequent action is:
- **Sends EFM Critical Event flag with Organization Specific Info TLV with indication of Remote Link Fail towards the Edge PB, shuts down TX to CPE, or if Auto-Negotiation enabled sends Remote Fault (if sequence was initiated by AN then only does EFM piece).**

TPMR ingress Extension Link port detects:
- **Input link failure (sends EFM Link Fault flag towards Edge PB),**
- **EFM Link Fault flag,**
- **EFM Critical Event flag with Organization Specific Info TLV with indication of Network Connection Fail,**

Consequent action is:
- **Shuts down TX to CPE and ignores failures detected from CPE during TX shutdown.**

Conditioning Rules Summary (cont'd)

Edge PB ingress Extension Link port detects:
- **Input link failure (sends EFM Link Fault flag towards TPMR),**
- **EFM Critical Event flag with Organization Specific Info TLV with indication of Remote Link Fail,**

Consequent action is:
- **Send ETH_AIS per P802.1ag into the network.**

Edge PB ingress Extension Link port detects:
- **EFM Link Fault flag,**

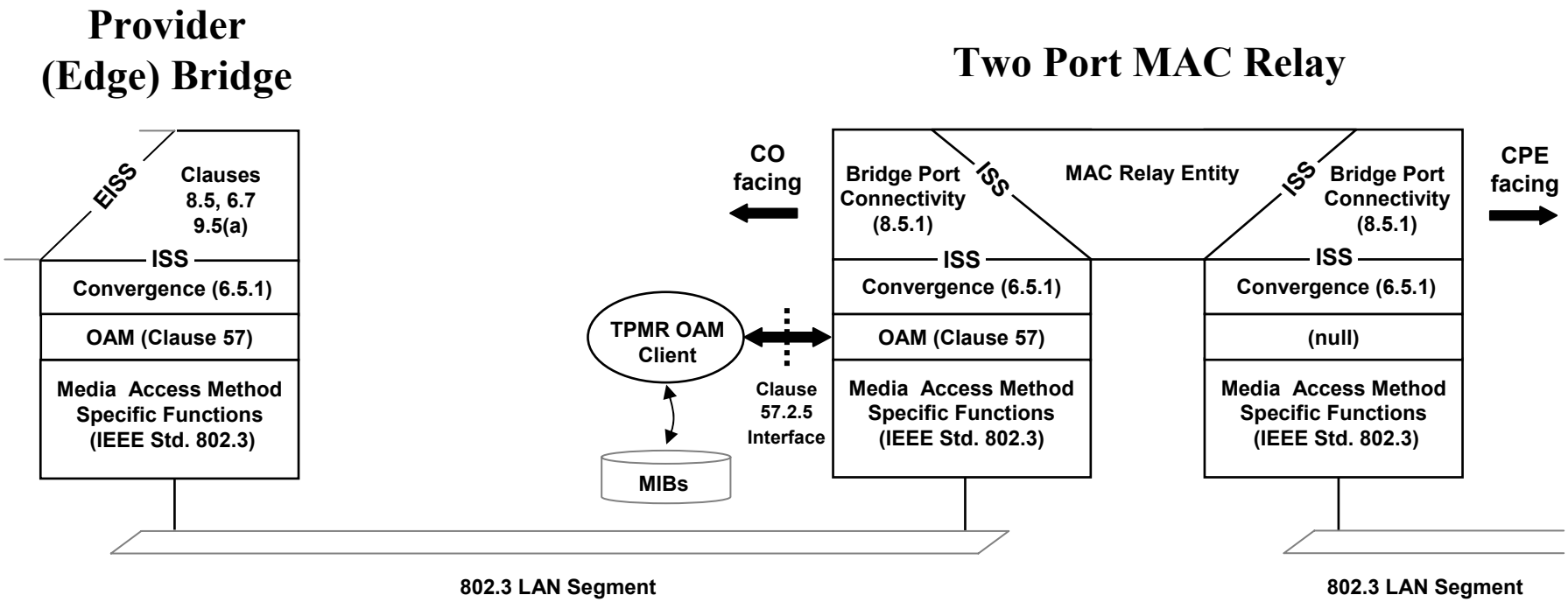
Consequent action is:
- **Send ETH_RDI per P802.1ag (if defined) into the network.**

Edge PB ingress Network port detects:
- **Input link failure (sends ETH_RDI per P802.1ag if defined into the network),**
- **ETH_AIS per P802.1ag (sends ETH_RDI per P802.1ag if defined into the network),**
- **ETH_RDI per P802.1ag (if defined),**

Consequent action is:
- **Send EFM Critical Event flag with Organization Specific Info TLV with indication of Network Connection Fail towards TPMR (E-Line services).**

EFM OAM Extensions

Example EFM / TPMR Link



Managed objects which need to be accessed by the TPMR OAM Client:

- **TPMR Management Entity: TPMR Configuration, Port Configuration**
- **Forwarding Process of the MAC Relay Entity: Port Counters**
- **MAC Entities** (oMACEntity, on CO and CPE sides)
- **PHY Entities** (oPHYEntity, on CO and CPE sides)
- **OAM Sublayer Entity** (oOAM, on CO side)

EFM OAM Extensions: Mgmt

- The following managed objects can be accessed by the currently defined EFM Variable Request / Response OAMPDUs (codes 02 / 03):
  - oMACEntity, on CO side
  - oPHYEntity, on CO side
  - oOAM, on CO side
- The remaining managed objects can be accessed by a new "802.1aj" Organization Specific OAMPDU (code FE), which will provide a similar Request / Response mechanism for indexed entities:
  - TPMR Management Entity
  - Forwarding Process of the MAC Relay Entity
  - oMACEntity, on CPE side
  - oPHYEntity, on CPE side
- To accommodate Set commands, a new "802.1aj" Set OAMPDU could be defined

EFM OAM Extensions: Mgmt (cont'd)

Octets	
6	Destination Address = 01-80-c2-00-00-02
6	Source Address
2	Length/Type = 88-09
1	Subtype = 0x03
2	Flags
1	Code = 0xFE
3	802.1 OUI
1	802.1aj Subtype
1	**TPMR Variable Request**
1	**Requested Entity**
x	**Variable Descriptors** (c57.6.1)
z	Pad
4	FCS

Octets	
6	Destination Address = 01-80-c2-00-00-02
6	Source Address
2	Length/Type = 88-09
1	Subtype = 0x03
2	Flags
1	Code = 0xFE
3	802.1 OUI
1	802.1aj Subtype
1	**TPMR Variable Response**
1	**Requested Entity**
y	**Variable Containers** (c57.6.2)
z	Pad
4	FCS

Requested Entity	
x0000	TPMR Management Entity
x0001	Forwarding Process of MAC Relay Entity
x0010	oMACEntity on CPE side
x0011	oPHYEntity on CPE side

EFM OAM Extensions: Mgmt (cont'd)

Octets	
6	Destination Address = 01-80-c2-00-00-02
6	Source Address
2	Length/Type = 88-09
1	Subtype = 0x03
2	Flags
1	Code = 0xFE
3	802.1 OUI
1	802.1aj Subtype
1	**TPMR Variable Set**
1	**Requested Entity**
x	**Variable Containers ***
z	Pad
4	FCS

* The Variable Container format for the Set OAMPDU is the same as c57.6.2 except the Variable Value field is the value to be Set, rather than returned.

EFM OAM Extensions: Faults

Octets	
6	Destination Address = 01-80-c2-00-00-02
6	Source Address
2	Length/Type = 88-09
1	Subtype = 0x03
2	Flags: **Critical Event**
1	Code = 0x00
1	Information TLV Type = 0xFE
1	Length
3	802.1 OUI
1	802.1aj Subtype
1	**Remote Link Fail**
35	Pad
4	FCS

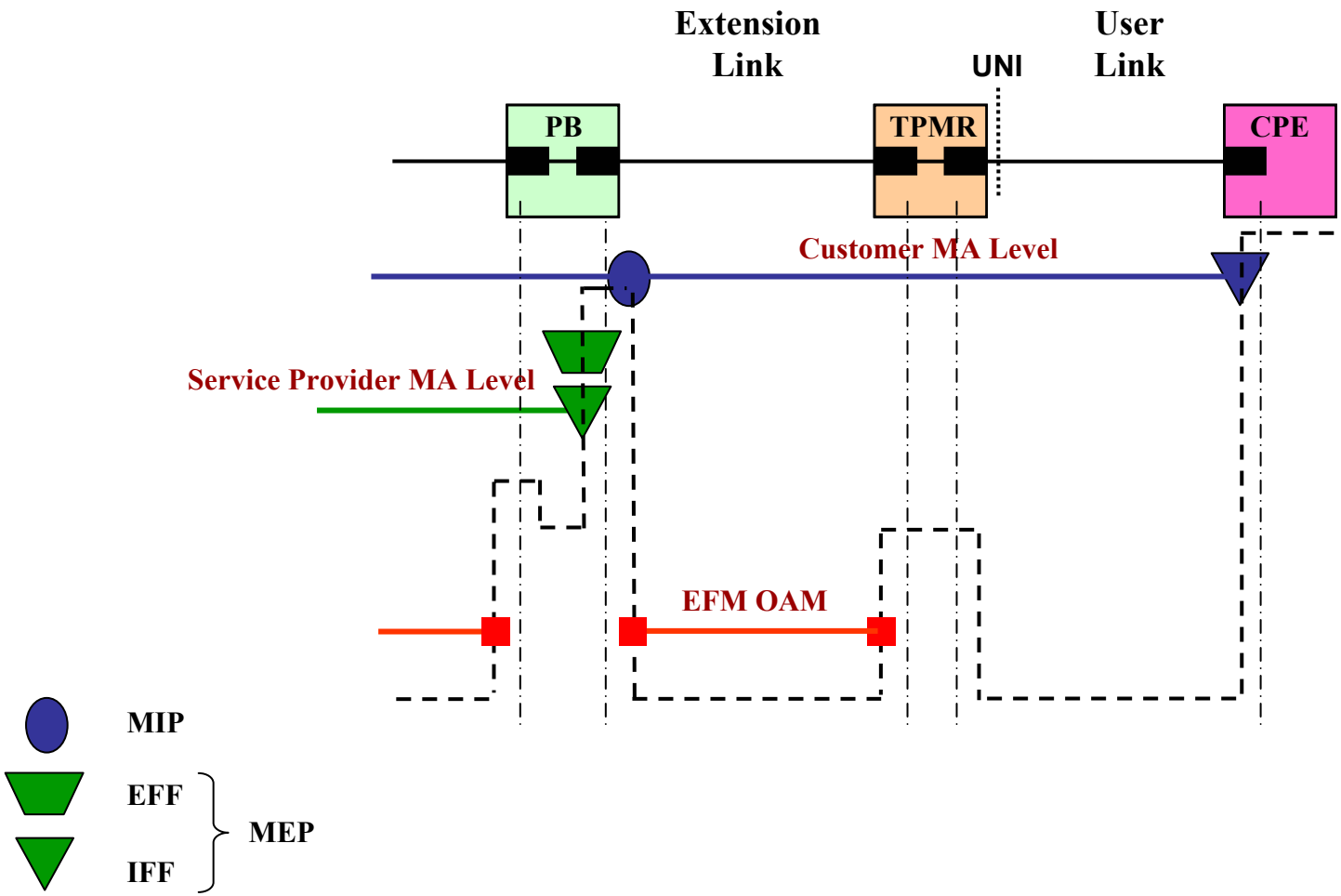
Octets	
6	Destination Address = 01-80-c2-00-00-02
6	Source Address
2	Length/Type = 88-09
1	Subtype = 0x03
2	Flags: **Critical Event**
1	Code = 0x00
1	Information TLV Type = 0xFE
1	Length
3	802.1 OUI
1	802.1aj Subtype
1	**Network Connection Fail**
35	Pad
4	FCS

Summary

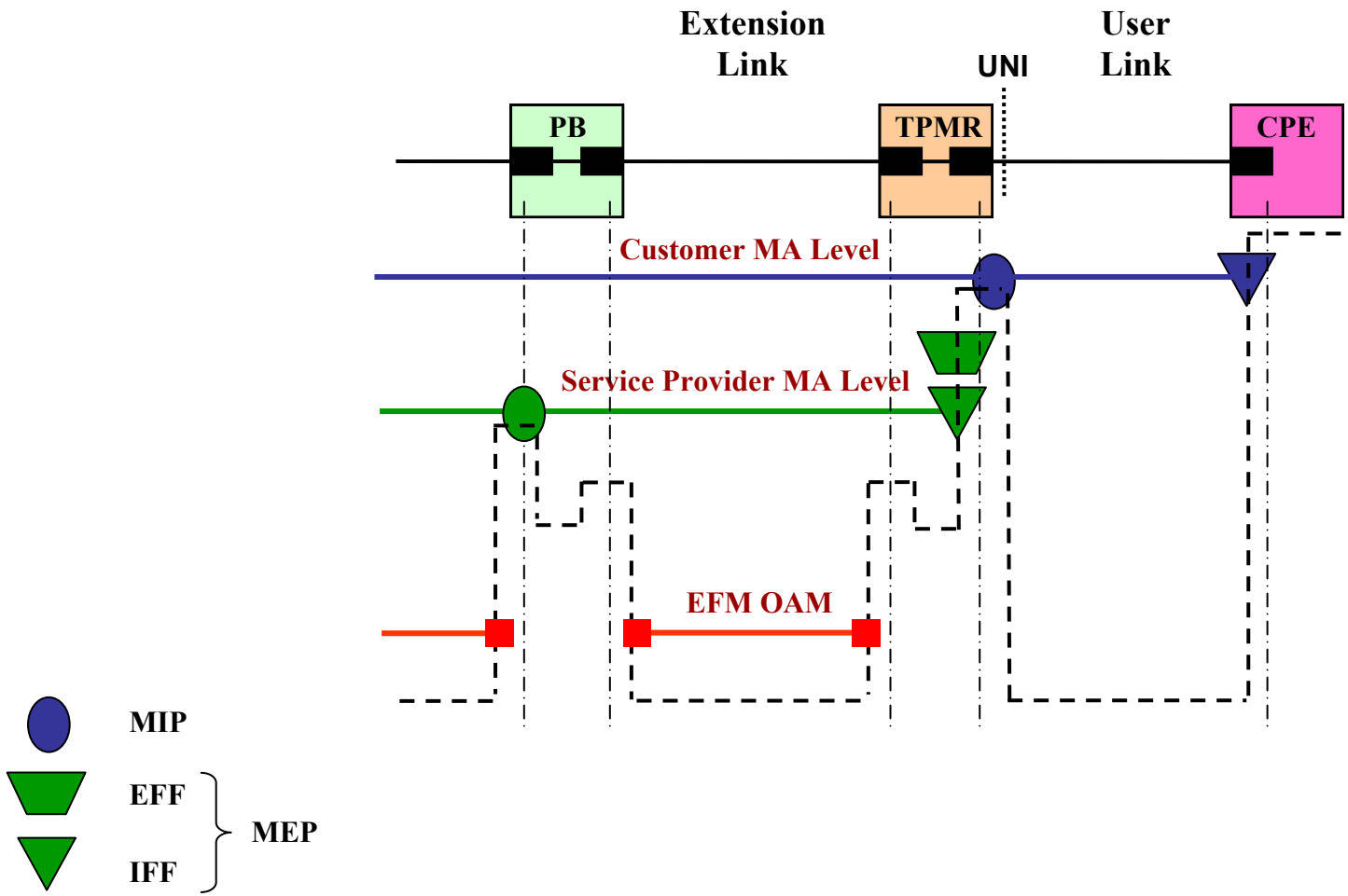
- For a single 802.3 link, EFM OAM with simple extensions can manage a TPMR
- Daisy chained TPMRs or non-802.3 media will require another management approach

REFERENCE

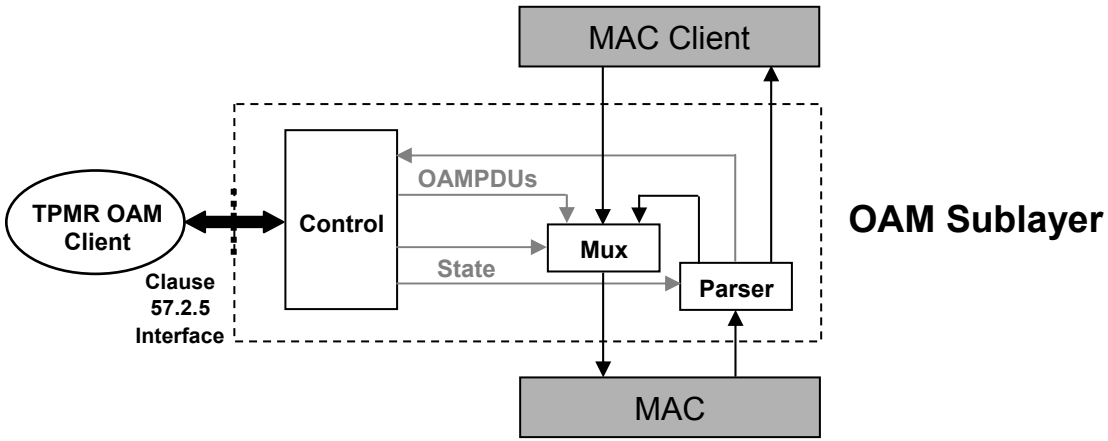
TPMR w/ EFM OAM only



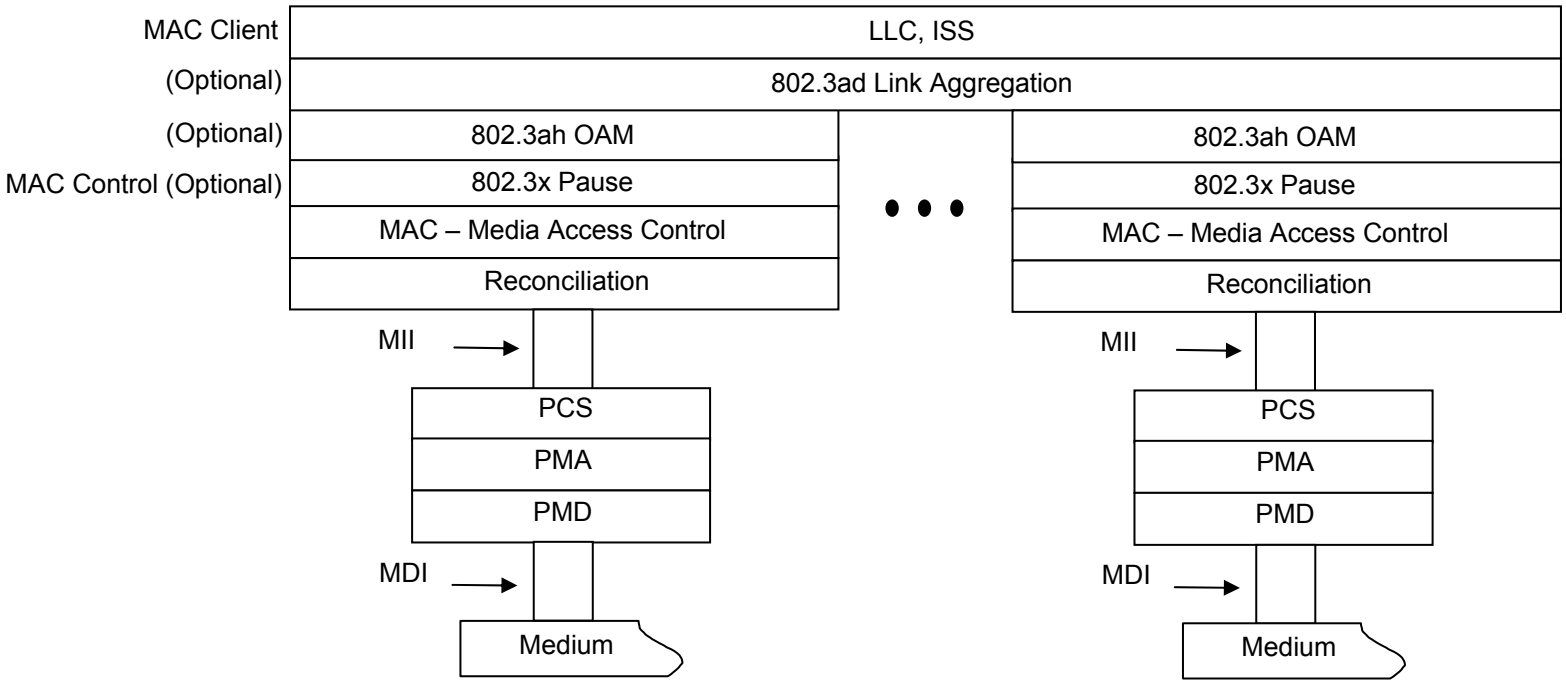
TPMR w/ EFM OAM and CFM



EFM OAM Sublayer Blocks



802.3 Link Aggregation Layering



TPMR 802.1 / .3 Protocols Handling

TPMR 802.1 Protocols Handling		
MAC Address	**Protocol**	**TPMR Handling**
01-80-C2-00-00-00	STP, MSTP, RSTP	pass
01-80-C2-00-00-03	802.1X Port Authentication	
01-80-C2-00-00-04…0D, 0F	reserved addresses	
01-80-C2-00-00-0E	LLDP	
01-80-C2-00-00-10	Bridge management	
01-80-C2-00-00-20	GARP – GMRP address	
01-80-C2-00-00-21	GARP – GVRP address	
01-80-C2-00-00-22…2F	GARP – reserved addresses	

TPMR 802.3 Protocols Handling[1]				
MAC Address	**Ethertype**	**Subtype**	**Protocol**	**TPMR Handling**
01-80-C2-00-00-01 or unicast	88-08	0x0001	MAC Control (PAUSE)	source to CPE or CO respond to a CO request ignore a CPE request
01-80-C2-00-00-02	88-09	0x01, 0x02	LACP, LAMP	pass
01-80-C2-00-00-02	88-09	0x03	EFM OAM	source / process on CO side don't source / ignore on CPE side

[1]For case when links are 802.3 media

P802.1aj PAR Extract

13. Scope of Proposed Project:

This standard specifies the function of a MAC Relay with two MACs, and the protocols and procedures to support its operation. A MAC Relay is transparent to all frame-based media independent protocols except those explicitly addressed to this device. It is remotely manageable through at least one of its external MACs, and signals a failure of either MAC's LAN through the other MAC.

Is the completion of this document contingent upon the completion of another document? Yes

This standard is designed to support Provider Bridges (IEEE P802.1ad).

14. Purpose of Proposed Project:

The wide and growing deployment of Ethernet Provider Services has created a demand for simple two-port demarcation devices that connect two 802 media or 802 media emulations. The lack of standards for such devices, and particularly for link-loss signalling and remote diagnosis, is impeding the growth of this industry. This standard will greatly improve this situation.

14a. Reason for the standardization project:

Public networks represent a new and very broad application space for IEEE 802 technologies and specifically for Provider Bridges (P802.1ad) and Ethernet in the First Mile (802.3ah). Numerous vendors and potential users (the Service Providers) have expressed the need to integrate Ethernet link technologies with their existing infrastructure at a low cost, while providing the manageability and remote diagnostic capabilities traditionally offered by circuit switched technologies.

(Extracted from the P802.1aj PAR Form approval letter from the IEEE-SA Standards Board December 10, 2004)