Connectionless Technology Management

Table of Contents

Table of Figures

Table of Tables

1 Scope

This supporting document aims at specifying a framework for supporting connectionless technologies from the Interface. While seeking compliance with the generic modelling concepts recommended in ITU-T (G.809 [7], G.8010 [8]) this work is initially intended to address the management of Ethernet and related technologies as defined in ITU-T G.8011 [9] and MEF 10 [15]. The term “Ethernet” refers to the Ethernet MAC layer (ETH). This model is designed to complement and integrates seamlessly with the existing ITU-T G.805 [16] based MTNM release 3.0 interface aimed at connection oriented technologies. Similar modelling activities from ITU-T (Q.840.1 [33]) and MEF Phase 1 (MEF 7 [11]) have been considered for consistency.

The connectionless solution is primarily targeted at managing Ethernet over traditional or next generation transport network such as SONET/SDH, WDM, ATM or RPR. The Interface provides fully integrated support for SONET/SDH, WDM and ATM while only the access points (Connectionless Port Termination Points (CPTPs)) are supported in case of RPR transport.

Support for point-to-point services (Ethernet Private Line (EPL), Ethernet Virtual Private Line (EVPL)) are provided in compliance with MEF 10 [15] definitions. MEF Phase 2 however has not yet completed its work on multipoint services (Ethernet Private Local Area Network (EPLAN), Ethernet Virtual Private Local Area Network (EVPLAN)) at the time this TMF specification is published. Therefore, future alignment with MEF (Phase 2) will be required in a subsequent Interface release. With regard to the EPL, this release of the Interface provides an alternative to the previous Interface release support based on the connection oriented model and TP containment relationships. An target OS may support either or both EPL implementations (though not simultaneously on the same object instances) in order to meet the objectives of the requesting OS.

The following capabilities are supported:

- Point-to-point services (EPL, EVPL) in compliance with MEF Service Definition Phase 1
- Multipoint services (EPLAN, EVPLAN)
- Link Aggregation (LAG)
- Point-to-point Call (represent connectionless connectivity between NEs) provisioning (including Control Plane option)
- Diverse routes for point-to-point Calls
- Multipoint Topological Links (e.g., for representing RPR transport connectivity)
- CPTP provisioning
- Fixed MFD modelling (e.g., direct mapped EPL services)
- VLAN-unaware routing as per IEEE 802.1D
- C-VLAN based tagging as per IEEE 802.1Q
- S-VLAN based tagging as per 802.1ad
- Port (UNI/NNI), C-VLAN/EVC and/or CoS (802.1p) based classification
- Spanning Tree management
- Ingress traffic conditioning
- C-Tag/S-Tag translation
- Non routed layer 2 networks (using singleton Flow Domains)
- Integrated or separate transport (SONET/SDH, etc.) and Ethernet OSs

To support the abovementioned features the following new terms have been defined:

- Flow Domain (FD)
- Matrix Flow Domain (MFD)

- Connectionless Port Termination Point (CPTP)
- Flow Point (FP)
- Flow Domain Fragment (FDFr)
- TC Profile

The following functionalities have been deferred to future Interface releases:

- Enhancement of connectionless technologies from Ethernet to client layers (e.g., IP)
- Non layer 2 frame based technologies (e.g., RPR)
- Non S-VLAN based tagging (e.g., Pseudo-wire encapsulation)
- Egress and internal Traffic Conditioning
- Handling of mutual influence of bandwidth configurations within one port
- Splitting/merging of MFD and FD
- Multipoint Topological Link provisioning (e.g., RPR transport)
- Point-to-multipoint ELL provisioning (e.g., for WiMAX applications)
- RPR transport layer (beyond multipoint RPR layer Topological Link and RPR layer CPTP)
- Modelling of client side of a UNI (per MEF 10)

2 References

[1] IETF RFC 1493 (July 1993): Definitions of Managed Objects for Bridges.

[2] IETF RFC 2613 (June 1999): Remote Network Monitoring MIB Extensions for Switched Networks, Version 1.0.

[3] IETF RFC 2674 (August 1999): Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions.

[4] IETF RFC 3289: Management Information Base for the Differentiated Services Architecture.

[5] IEEE Std. 802.1D (2004): IEEE standard for local and metropolitan area networks: Media Access Control (MAC) Bridges. NOTE – 802.1D-2004 incorporates 802.1t and 802.1w.

[6] IEEE Std. 802.1Q (2003): IEEE standard for local and metropolitan area networks: Virtual Bridged Local Area Networks. NOTE – 802.1Q-2003 incorporates 802.1u, 802.1v, and 802.1s

[7] ITU-T G.809 (2003): Functional architecture of connectionless layer networks.

[8] ITU-T G.8010/Y.1306 (2004): Architecture of Ethernet Layer Networks.

[9] ITU-T G.8011/Y.1307 (2004): Ethernet Services Framework.

[10] MEF: Draft TS D00011_v5.7 (April 14, 2004) [MEF 6]: Ethernet Services Definitions – Phase I.

[11] MEF TS MEF 7 (October 2004): EMS-NMS Information Model.

[12] IEEE Std. 802.3 (2002): IEEE Standard for Information technology - Telecommunications and information exchange between systems - IEEE standard for local and metropolitan area networks - Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

[13] IEEE Std. 802.3ae (2002): IEEE Standard for Information technology - Telecommunications and information exchange between systems - IEEE standard for local and metropolitan area networks - Specific requirements – Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Amendment: Media Access Control (MAC) Parameters, Physical Layers, and Management Parameters for 10 Gb/s Operation

[14] IEEE Draft Std. P802.1ad/D6.0 (August 17, 2005): Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges.

[15] MEF TS MEF 10.2 (October 2009): Ethernet Services Attributes Phase II.

[16] .ITU-T G.805 (2000): Generic functional architecture of transport networks

[17] ITU-T Y.1730 (2004): Requirements for OAM functions in Ethernet based networks and Ethernet services.

[18] TMF 513 (April 2004): MTNM Business Agreement Version 3.0.

[19] ITU-T G.7041/Y.1303 (2003): Generic Framing Procedure (GFP).

[20] ITU-T G.7042/Y.1305 (2004): Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals.

[21] ITU-T G.808.1 (2003): Generic protection switching - Linear trail and subnetwork protection.

[22] ITU-T G.8012 (2004): Ethernet UNI and Ethernet NNI.

[23] ITU-T Q.838.1 (2004): Requirements and Analysis for the Management Interface of Ethernet Passive Optical Networks.

[24] ITU-T G.8011.1/Y.1307.1 (2004): Ethernet Private Line Service.

[25] MEF Draft TS 10033_000 (July 23, 2004): Requirements for Management of MetroEthernet Network Elements.

[26] MEF Draft TS D00021_001 (March 27, 2003): Ethernet Performance Monitoring.

[27] MEF Draft TS 10035_001 v1.2 (July 23, 2004): MEF Service OAM Requirements & Framework.

[28] ITU-T Draft Y.17ethoam: OAM Functions and Mechanisms for Ethernet based networks.

[29] IETF Internet Draft draft-ietf-bridge-bridgemib-smiv2-06 (April 2004): Definitions of Managed Objects for Bridges.

[30] IETF Internet Draft draft-ietf-bridge-ext-v2-02 (March 2004): Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions.

[31] IETF Internet Draft draft-ietf-bridge-rstpmib-04 (March 2004): Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol.

[32] MEF TS MEF 4 (May 2004): Metro Ethernet Network Architecture Framework - Part 1: Generic Framework

[33] ITU-T Draft Q.840.1 (02/2006): Requirements and Analysis for NMS-EMS Management Interface of Ethernet over Transport and Metro Ethernet Network

3 Acronyms and Definitions

Bridge	The 802.1D term used here to represent a matrix FD (i.e., the smallest possible Flow Domain)
CPTP	Connectionless Port Termination Point
ELL	Encapsulation Layer Link
EPL	Ethernet Private Line
EPLAN	Ethernet Private LAN
ETH	Ethernet MAC layer
Ethernet layer	a (non-)continuous of flow of ETH_CI traffic units as specified in G.8010
EVPL	Ethernet Virtual Private Line
EVPLAN	Ethernet Virtual Private LAN
FD	Flow Domain
FDEdgeTP	Flow Domain Edge Termination Point
FDFr	Flow Domain Fragment
FP	Flow Point
FPP	Flow Point Pool
LAG	Link Aggregation or Link Aggregation Group
LAN	Local Area Network
MAC	Media Access Control
MEF	Metro Ethernet Forum
MEN	Metro Ethernet Network
MFD	Matrix Flow Domain
MFDFr	Matrix Flow Domain Fragment (not modelled in version 3.5)
NNI	Network Node Interface
NVP	Name/Value Pair
RMON	Remote Network Monitoring
SMON	Switched Network Monitoring (RMON for switched networks)
SNI	Service Node Interface
STP	Spanning Tree Protocol
TPP	TPPool object as specified in MTNM v3.0
UNI	User Network Interface
VLAN	Virtual LAN

4 Connectionless technology modeling terms

4.1 Connectionless Port TP (CPTP)

A Connectionless Port TP is a logical entity which represents a port capability of an equipment. It can be any kind of port capable of supporting a connectionless client layer (e.g., external port, internal encapsulation port).

The term "Connectionless Port TP" is a general term used in this specification for defining the characteristics of a port at a connectionless matrix (note: the clients of a CPTP, i.e. Flow Points (FPs), are connected via the matrix). It is modelled as a Physical Termination Point (PTP) if the port does not support encapsulation or link aggregation. It is modelled as a Floating Termination Point (FTP) if the port does provide encapsulation or link aggregation. It is modelled as a Connection Termination Point (CTP) if the port does provide encapsulation but not link aggregation. A Boolean layered parameter for PTPs, FTPs and CTPs at connectionless layers (e.g. Ethernet) identifies the TP as a CPTP.

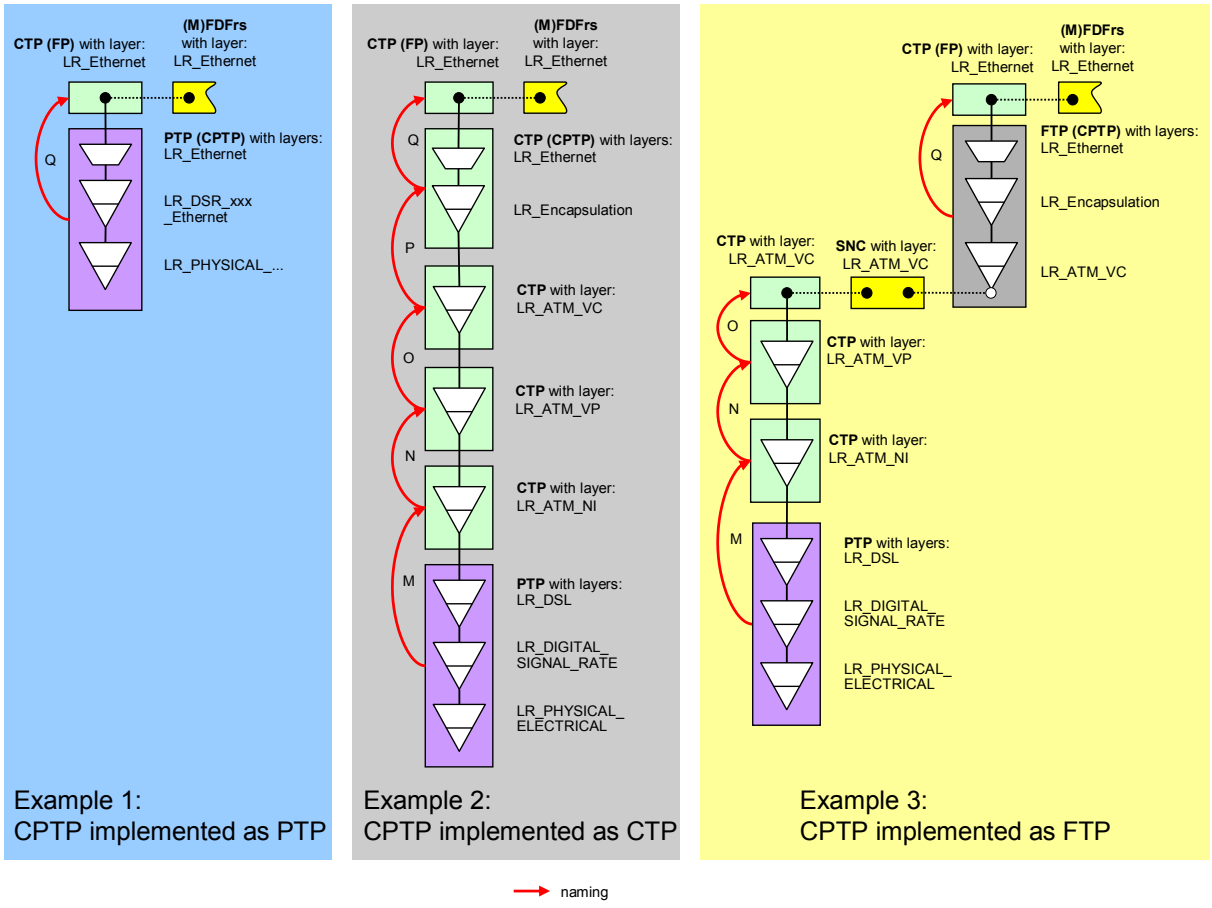


Figure 1: Implementations of CPTPs

In the context of a Flow Domain (FD), a CPTP can be an edge port or an internal port. The *fdEdge* port is identified by the value "fdEdge" in the layered parameter "PortTPRoleState" (see following definition) and the *fdInternal* port is a CPTP that is assigned to one of the Matrix Flow Domains (MFDs) which are associated to the FD but not acting as an edge (i.e. have the value "assigned" in the layered parameter "PortTPRoleState").

A CPTP can "play" several roles depending on its usage in the network:

- **unassigned** CPTP
  This is the usual initial role of a CPTP. CPTPs (if automatically created) will be created as "unassigned" CPTPs when the equipment (which supports the port) is plugged into the NE. In this role, the CPTP cannot carry any traffic.

  In case the NE allows traffic to flow automatically when the equipment is plugged in, the OS has to
  - create a default MFD,
  - create a default FD to which the MFD is associated to,
  - assign all relevant CPTPs to the MFD (either as fdEdge or assigned),
  - create all default Flow Domain Fragments (FDFrs) and corresponding FPs. An "unassigned" CPTP has a relationship to its supporting equipment and naming relationship to its containing NE.

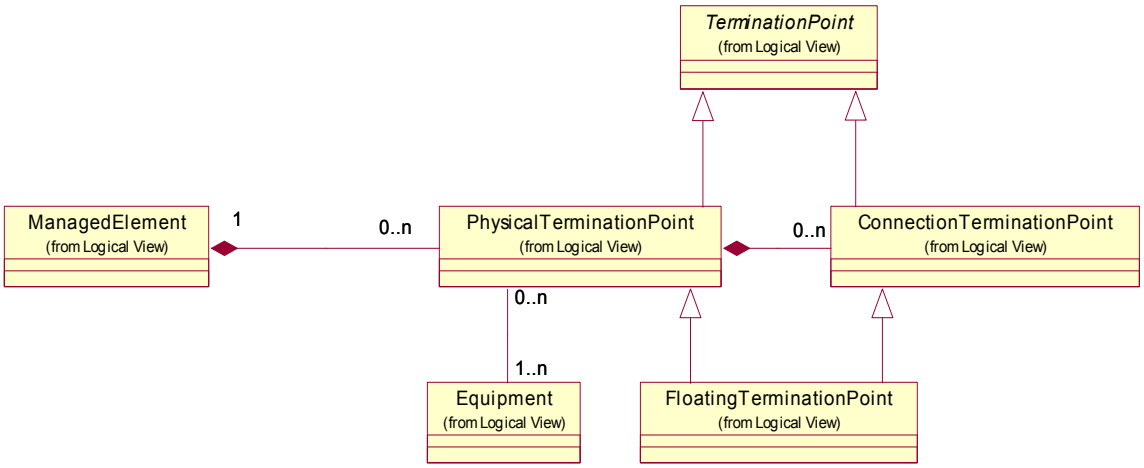


Figure 2: unassigned CPTP

Note: The naming relationship between ManagedElement and Equipment (via EquipmentHolder) is not shown in the UML diagram.

- **assigned** CPTP
  An "unassigned" CPTP becomes an "assigned" CPTP when it is associated to a Matrix Flow Domain (MFD) via a management operation.
  In this role, the CPTP cannot carry any traffic because the MFD is not associated to a Flow Domain (FD).
  An "assigned" CPTP has, in addition to the relationships of an "unassigned" CPTP, a relationship to its associated MFD.

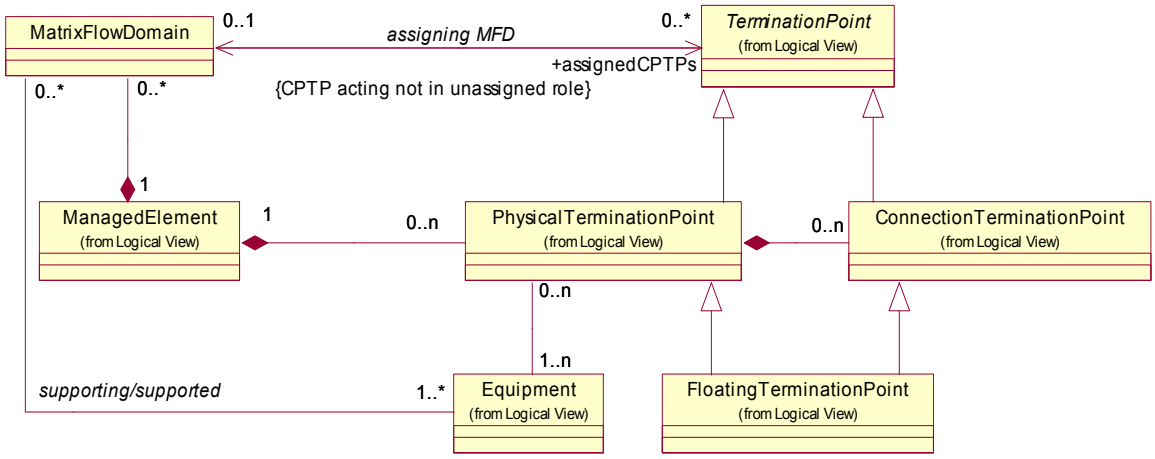


Figure 3: assigned CPTP

- **fdInternal** CPTP (FD Internal CPTP)
  An "assigned" CPTP becomes an "fdInternal" CPTP when its MFD is associated to a Flow Domain.
  An "unassigned" CPTP becomes an "fdInternal" CPTP when it is assigned to an MFD that is already associated to a Flow Domain.
  In the fdInternal role, the "potential" client Flow Points of the CPTP can be used as internal points of the route (in case auto-routing is not supported, e.g., in case of Ethernet automatic VLAN-ID registration is not supported) of a Flow Domain Fragment; i.e., can carry traffic.
  An "fdInternal" CPTP has, in addition to the relationships of an "assigned" CPTP, a relationship to its associated Flow Domain.

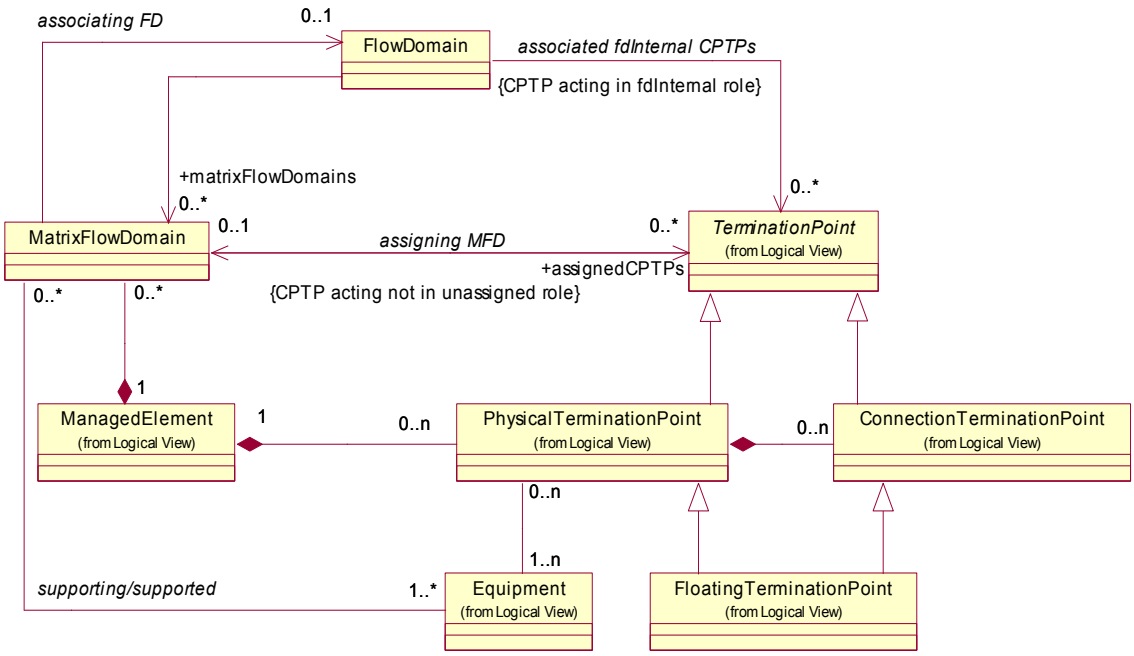


Figure 4: fdInternal CPTP

- **fdEdge** CPTP (FD Edge CPTP)
  An "assigned" CPTP becomes an "fdEdge" CPTP via a management operation (Note: Precondition is, that the MFD is already associated to the FD). In this role, the "potential" client

Flow Points of the CPTP can be used as edge points of a Flow Domain Fragment; i.e., can carry traffic.

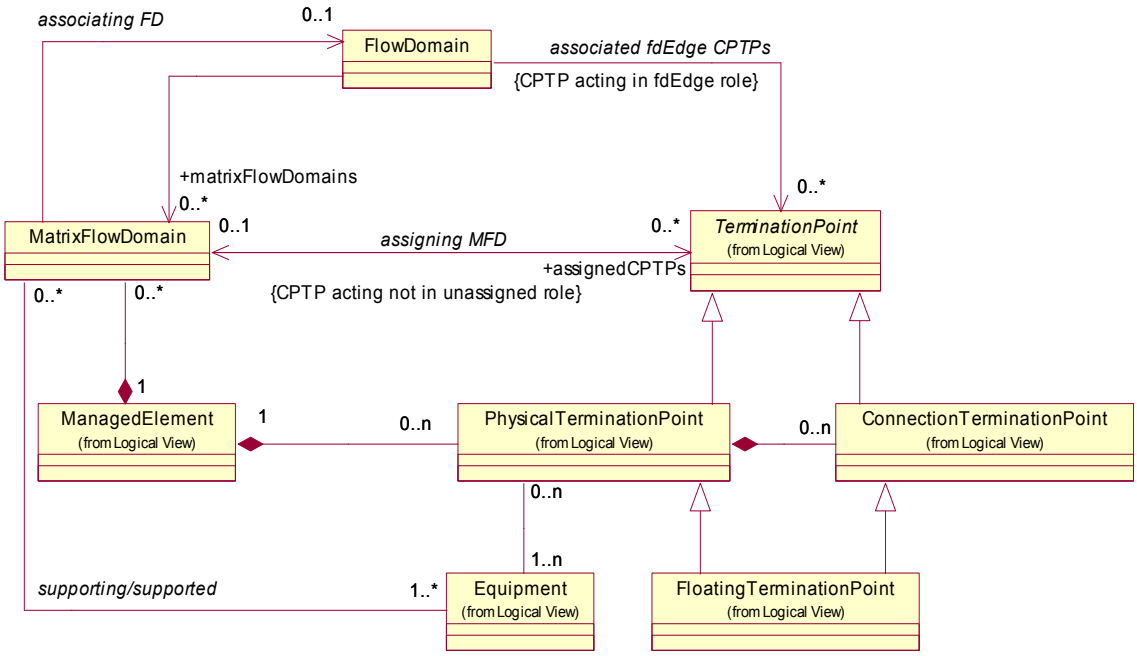


Figure 5: fdEdge CPTP

A CPTP can exist in four major states:

CPTP state examples	CPTP assigned to MFD	MFD associated to FD	CPTP configured to fdEdge	PortTPRoleState	CPTP can carry traffic?
1	no	not applicable	not possible	unassigned	no
2	yes	no	not possible	assigned	no
3	yes	yes	no	fdInternal	yes
4	yes	yes	yes	fdEdge	yes

Table 1: Major CPTP states

The kind of role that a CPTP is "playing" for its connectionless client layer is stored in a new layered parameter "port TP Role State" associated to the PTP/FTP/CTP object.

The retrieval of the CPTPs over the interface is possible with the following operations:

- The operations "ManagedElement:getAllPTP(Name)s" will return all (assuming layer rate filter is set properly) CPTPs (playing any role) within the NE.
- The operations "ManagedElement: getAllPTP(Name)sWithoutFTPs" will return all (assuming layer rate filter is set properly) "PTP" CPTPs (playing any role) not supporting encapsulation or link aggregation within the NE.
- The operations "ManagedElement: getAllFTP(Name)s" will return all (assuming layer rate filter is set properly) "FTP" CPTPs (playing any role) supporting encapsulation or link aggregation within the NE.

- The operations "MatrixFlowDomain:getAllAssignedCPTPs" will return all CPTPs assigned to this MFD (i.e., playing "assigned", "fdInternal" or "fdEdge" role).
- The operations "MatrixFlowDomain:getAllAssignableCPTPs" will return all CPTPs that are potentially able to be assigned to this MFD. Potentially means: The CPTPs are on the same Equipment or same Rack with backplane connectivity as the MFD. It is irrelevant whether the CPTPs are already assigned to an MFD or not.
- The operations "FlowDomain:getAllCPTPs" will return all CPTPs associated to this FD (i.e., playing "fdInternal" or "fdEdge" role). It is possible to filter the request to retrieve only fdEdge, only fdInternal or all CPTPs.

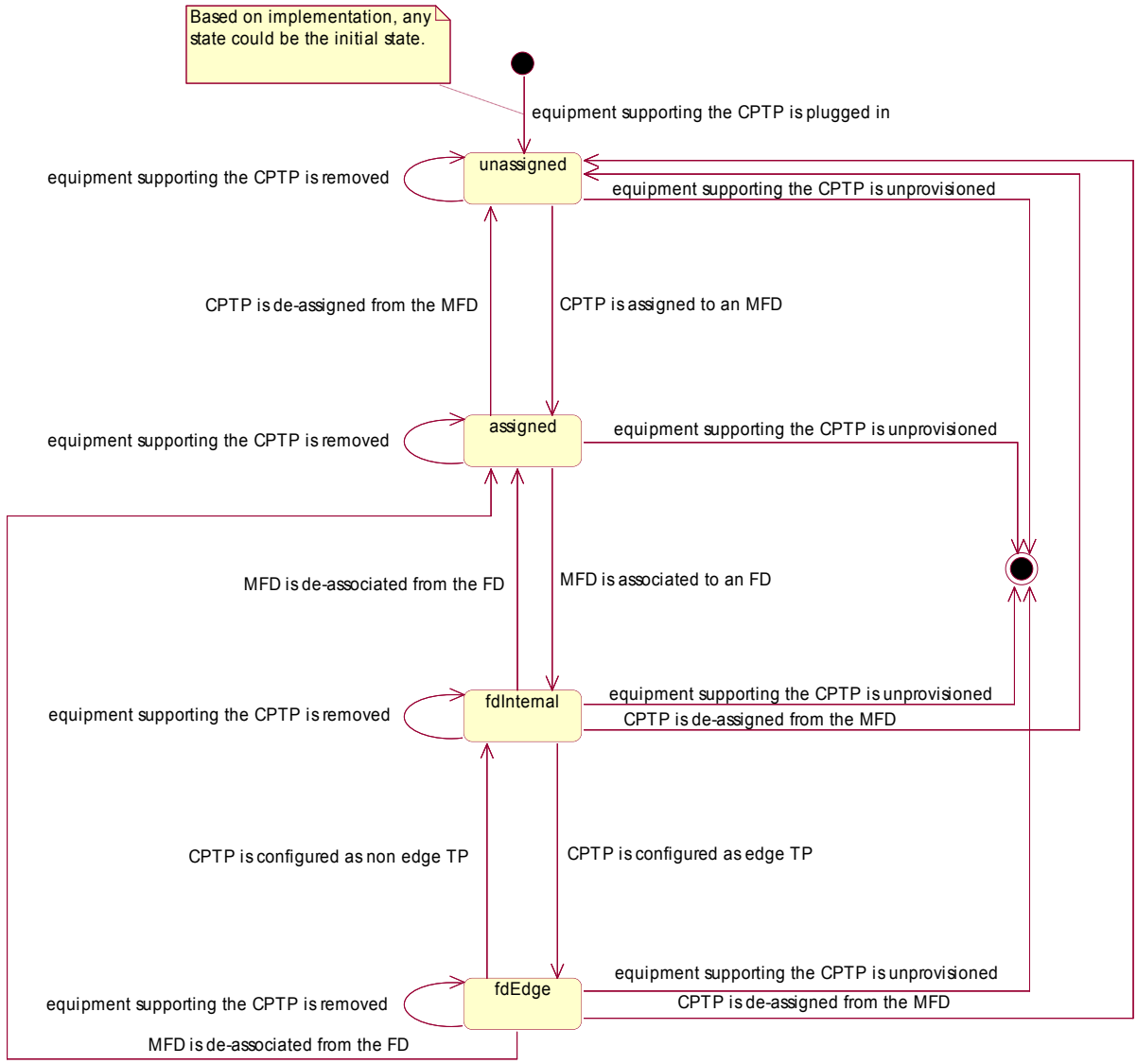


Figure 6: State diagram for Port TP Role State

4.2 Call

Refer to chapter 6

4.3 Flow Domain (FD)

G.809: "*A topological component used to effect forwarding of a specific characteristic information.*" This entity groups Matrix Flow Domains (MFDs) and obliquely the CPTPs (i.e., server layer TPs of Flow Points) assigned to the MFDs. Traffic cannot flow between points that are related solely by an FD. Traffic can only flow if there exist a Flow Domain Fragment (FDFr) within the FD. An FD is used to indicate the potential for flow of traffic between a set of points (and in this sense it is directly analogous with the connection oriented Subnetwork). The lowest level of decomposition of an FD is a single (non-decomposable) Matrix Flow Domain (e.g., a Bridge in case of Ethernet).

The Flow Domain represents an administrative partitioning of the connectionless network domain. Similarly with connection oriented Subnetworks, the Flow Domain primary role is to identify within each OS the portion of connectionless networks that participate in the same higher level Flow Domain known and managed by an OS (i.e., two-level hierarchy). Flow Domains differ from Subnetworks as they provide the requesting OS for defining them and requesting explicit implementation by the target OS across the management interface (Subnetworks can only be discovered). Unlike connection oriented Subnetworks which often constitute the widespread transport layer (DWDM, SONET/SDH) shared by many network applications, connectionless Subnetworks such as Metro Ethernet are likely to be deployed as smaller “islands” dedicated to a single network application (e.g., multiple sites of a corporate customer). Flow Domain provisioning capability allows a requesting OS to instantiate and to change a Flow Domain so it can meet the infrastructure requirement (CPTPs, MFDs) needed to fulfil requests (FDFrs set up, tear down and modify) received from a service order system.

An additional difference between FD and Subnetwork is that an ME can participate in more than one FD at the same layer rate but in only one subnetwork.

Note: Appendix I show some hypothetical Ethernet network examples.

4.4 Flow Domain Fragment (FDFr)

This entity represents a Virtual Private Network (VPN) for a single customer in the provider’s network and enables the flow of traffic between Flow Points (FPs). The server layer CPTPs of the FPs that are connected via an FDFr have to be assigned to the MFDs that are associated to the FD containing the FDFr. If traffic that is correctly structured (i.e., not damaged by previous transport) arrives at a point that is a member of an FDFr, it will (barring a fault or frame dropping) emerge at one or more of the other edge Flow Points that are members of the same FDFr (and in this sense it is directly analogous with the connection oriented subnetwork connection). An FDFr may relate two or more edge Flow Points activating traffic connectivity between those points. The FDFr within an FD that is not the MFD/Bridge will potentially have a route that would be described by internal FPs and smaller Matrix Flow Domain Fragments (MFDFrs). The edge Flow Points that act as endpoints of the FDFr may be associated with CPTPs connected to customer domains or they may be associated with CPTPs connected to other provider domains (of the same or different providers) or they may be a mixture of both.

An FDFr may be associated with a certain VLAN ID on one Flow Point, and with a different VLAN ID on another Flow Point when VLAN swapping is supported within the FDFr. When VLAN swapping is not supported, VLAN Ids of the FPs must equal the VLAN Id of the FDFr. The only VLAN ID seen by an FDFr is the VLAN ID of the outermost frame. An FDFr may also support untagged frames, or may be unaware of frame tags.

A Flow Domain Flow (as defined in G.809 [7]) is not modelled as it describes the instantaneous transfer of a single MAC frame and it is therefore transient and highly variable.
A Flow Domain Fragment may be considered as the aggregation of all potential Flow Domain Flow

(FDFs) within its containing Flow Domain and hence as the connectionless analogue of the connection-oriented Subnetwork Connection (SNC). Individual FDFs are generally not modelled at the NML-EML Interface.

Note: An FDFr is similar to an "EVC" defined in MEF.

4.5 Flow Point (FP)

A point in a connectionless layer (e.g., Ethernet layer) which represents an association between a CPTP and an FDFr. It is either an endpoint of an FDFr, where traffic enters or exits an FDFr or an internal point of an FDFr, used to define the route of an FDFr. It is modelled as a CTP. Operations on frames, which occur on entry to or exit from an FDFr, are defined on the CTP object.

Note: The Flow Point will not be used for the modelling of a single MAC frame (as defined in ITU-T).
Note: In the case of Ethernet, Flow Points are always bidirectional.

4.6 Flow Point Pool (FPP)

G.809 [7]: "*A group of co-located flow points that have a common routing.*" The ITU-T FPP will not be used in the model. The CPTP represents the grouping of Flow Points on the server layer.

4.7 Flow Point Pool Link (FPP Link)

G.809 [7]: "*A "topological component" which describes a fixed relationship between Flow Domains.*" The ITU-T FPP Link will not be used in the model. The Call represents an FPP Link on the server layer.

4.8 Link Flow

G.809 [7]: "*A "transport entity" that transfers information between "ports" across a Flow Point Pool Link.*" The ITU-T Link Flow will not be used in the model.

4.9 Matrix Flow Domain (MFD)

An MFD is a Flow Domain at the lowest level of decomposition that represents the actual minimum decomposition of the hardware. It is a logical entity that is contained within one single Managed Element (ME). One ME may contain many MFDs. An MFD is characterised by a set of (possible empty) MFD Ports (i.e. CPTPs).

The use of multiple MFDs in a single ME is an implementation decision. An example would be to provide the capability to separate Ethernet frames coming in from different customers. In this case, traffic coming in for Customer "A" on CPTP "x" would be assigned to MFD A, and traffic for Customer "B" on CPTP "y" would be assigned to MFD Y.

For the Ethernet technology, the Matrix Flow Domain corresponds to an IEEE (virtual) bridge.

Point to Point connectionless services without an explicitly created MFD are modelled with a "fixed" MFD.

4.10 MFD Port

An MFD Port is a Connectionless Port Termination Point (CPTP) which is associated to an MFD (i.e., is an assigned CPTP). It represents a port attached to an MFD at the server layer of the connectionless layer (e.g., Ethernet). An MFD Port can be associated as an FD Edge or an FD Internal CPTP to a Flow Domain. This is only possible when the MFD (to which the MFD Port is associated to) is associated to the FD.

For the Ethernet technology, the MFD Port is a Bridge Port whose uppermost layer can adapt to Ethernet (Ethernet server TP).

4.11 Topological Component

G.809 [7]: "*An architectural component, used to describe the transport network in terms of the topological relationships between sets of points within the same layer network.*"

4.12 Traffic Conditioning function

G.8010 [8]: "*A "transport processing function" which accepts the characteristic information of the layer network at its input, classifies the traffic units according to configured rules, meters each traffic unit to determine its eligibility, polices non-conformant traffic units and presents the remaining traffic units at its output as characteristic information of the layer network.*"

The Traffic Conditioning function is modelled by a Traffic Conditioning (TC) Profile that contains the (bandwidth) parameters (according to MEF 10.2 [15]) that policies the traffic at the ingress and or egress of a connectionless layer (e.g., Ethernet) network. The policies can be applied to

- a whole port (CPTP)
  (e.g., for Ethernet per VLAN-Id, Priority and CoS)
- a point of an FDFr (FP)
  (e.g., for Ethernet per VLAN-Id, Priority and CoS).

Both Ingress and Egress TC Profiles are associated to CPTPs and FPs via the "Traffic Mapping Table". Refer to chapter 9 for details of the "Traffic Mapping Table".

The association of a TC Profile to an FP or CPTP is defined in a "cascaded" manner; i.e., parameters associated to traffic units at a CPTP can be overwritten by parameters associated to the same traffic units at an FP.

4.13 Transport Entity

G.809 [7]: "*An architectural component which transfers information between its inputs and outputs within a layer network.*"

5 Different managers for connection-oriented and connection-less Technologies

In case the connectionless technology and the connection oriented technology are managed by two different OSes, the CPTPs (which are FTP objects) are known in both Managers and the attributes and operations might have restricted write access. The Call might be known to the SDH OS, or it might not.

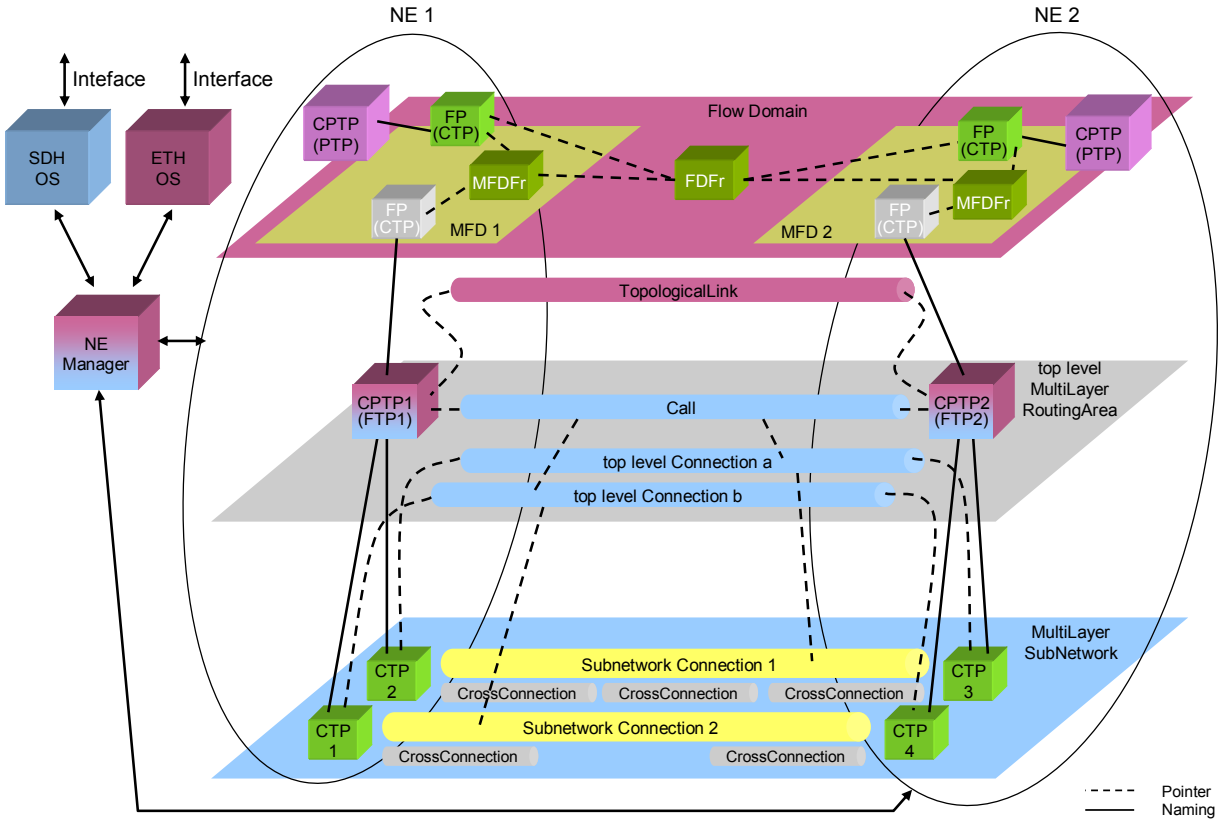


Figure 7: Example: Separate SDH-OS and Ethernet-OS

The following table identifies which objects in Figure 7 are represented by which OS:

OS	managed objects
SDH OS	MLSN top level MLRA CTPs in MLSN SNCs in MLSN FTP in NE 1, FTP in NE 2 Call top level Connections
ETH OS	FD, MFD and MFDFr in NE 1, MFD and MFDFr in NE 2 FPs in FD, PTPs in MFDs FDFr in FD FTP in NE 1, FTP in NE 2 (like ATM-NI the FTPs could also be represented as PTPs) TolplogicalLink

Table 2: Objects represented by SDH and ETH OS (simple example)

6 Call

6.1 Introduction

The Call is a link between two Matrix Flow Domains at the Encapsulation layer rate, i.e., it connects two CPTPs. The Call represents the bandwidth available to its client connectionless layer (e.g., Ethernet). It is used to "manage" the server layer (e.g., SDH VC12, SDH VC12-5v) capacity.

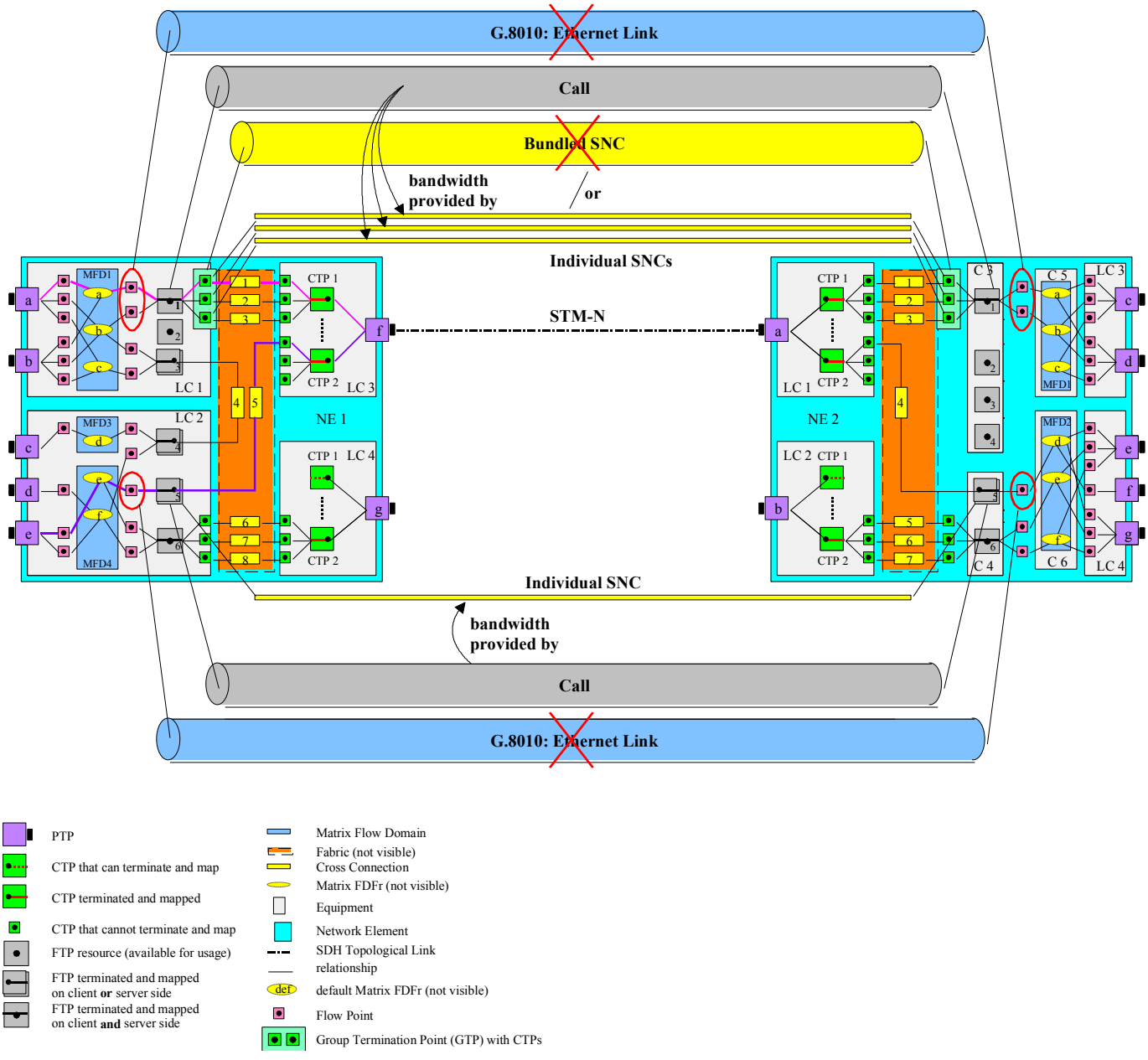


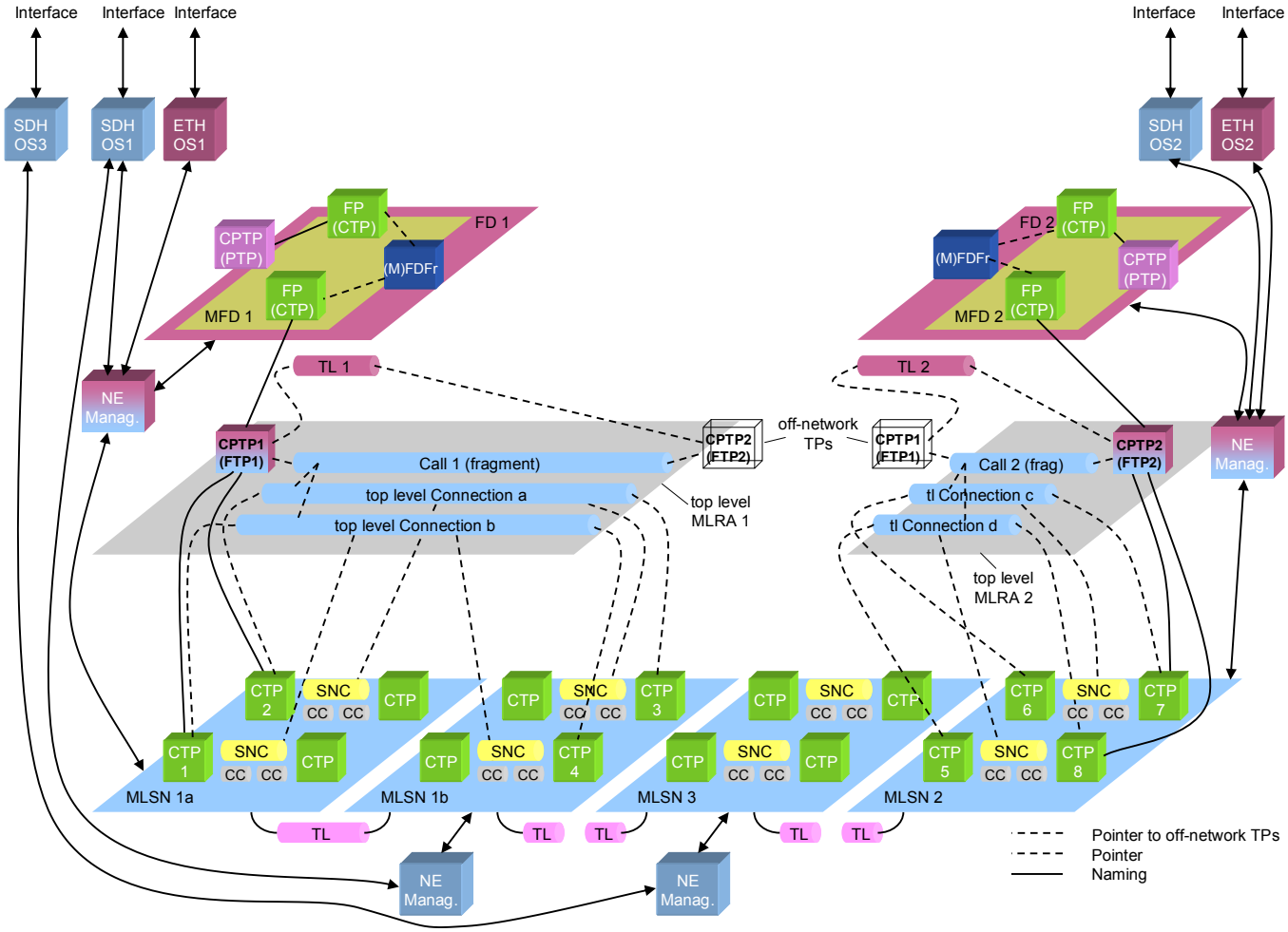
Figure 8: Encapsulation Layer Link usage

Note:
The bundledSNC can **not** be used (without modification) because it requires, that the ordering of the CTPs within the Group Termination Point (GTP) has to be preserved (which is not necessary when LCAS (Link Capacity Adjustment Scheme) is used) and because all "contained" SNC use the same

route (which is not necessary for VCAT (Virtual Concatenation) or LAG (Link Aggregation Group)). The Ethernet Link (G.8010) can **not** be used because it does not allow configuring the GFP (Generic Framing Procedure) and LCAS parameters.

In case the connectionless technology and the connection oriented technology are managed by two different OS, the Call object is known in the connection oriented technology OS and a corresponding Topological Link object is known in the connectionless technology OS.
Refer to Figure 7.

In the case where the OS only has visibility of one CPTP, the other CPTP (that is managed by another OS) is an off-network CPTP which will be referenced by a remote address. Refer to Figure 9.



Notes:
Resources are shown as they are represented at the mTOP interfaces.
Only one NE is shown in each MLSN. There may be many NEs within each MLSN.
FD1 and FD2 may contain many MFDs.

Figure 9: Example of Encapsulation Layer Link segments with off-network CPTPs

The following table identifies which objects in Figure 9 are represented by which OS:

OS	managed objects

OS	managed objects
SDH OS 1	MLSN 1a, MLSN 1b CTPs in MLSN 1a, CTPs in MLSN 1b SNCs in MLSN 1a, SNCs in MLSN 1b TL between MLSN 1a and MLSN 1b, TL segment in MLSN 1b FTP 1 Call 1 fragment, top level Connection a, top level Connection b
ETH OS 1	FD 1, MFD 1 CTPs in FD 1, PTP in MFD 1 FDFr in FD 1 FTP 1 TL 1
SDH OS 2	MLSN 2 CTPs in MLSN 2 SNCs in MLSN 2 TL segment in MLSN 2 FTP 2 Call 2 fragment, top level Connection c, top level Connection d
ETH OS 2	FD 2, MFD 2 CTPs in FD 2, PTP in MFD 2 FDFr in FD 2 FTP 2 TL 2
SDH OS 3	MLSN 3 CTPs in MLSN 3 SNCs in MLSN 3 two TL segments in MLSN 3

Table 3: Objects represented by SDH and ETH OS

Two types of Topological Links are modelled:

- Point to Point and
- Multipoint.

Point to Point connectivity is provided by the Topological Links described so far.
Multipoint (any-to-any) connectivity exists between MFDs in case the transport network consists of a broadcast medium such as a traditional physical Ethernet bus or a Resilient Packet Ring (RPR). The same amount of bandwidth has to be associated between each pair of nodes within an RPR.

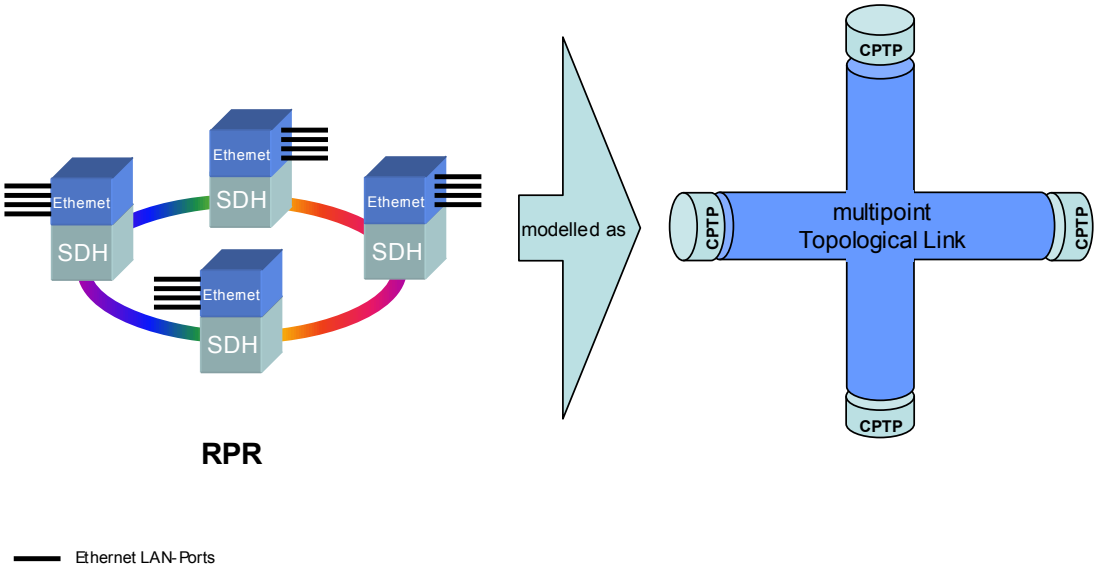


Figure 10: Example: Modelling of an RPR-Ring

A Call can be supported in its server layer by one of two varieties:

- with Inverse Multiplexing, using Virtual Concatenation (VCAT) or Link Aggregation (LAG)
- without Inverse Multiplexing, directly using SONET/SDH or other technologies

If VCAT is used, additional parameters are needed to indicate how many server layer SNCs should support the link and the single server layer rate (STS-1, VC-3, VC-4, etc.). Also, the requesting OS can direct the target OS to automatically create the server layer SNCs based on the target OS's routing method(s). LCAS and VCAT-related parameters are specified in the transmission parameters. The interface allows the requesting OS also to require diverse routed SNCs. This is described in the section below.

If LAG is used, additional parameters are needed to indicate how many server layer SNCs should support the link and the server layer rate (STS-1, VC-3, VC-4, Fragment, etc.). A Fragment server layer rate means that the LAG members are VCAT groups.

The operations will be:

- OS creates a Call
  VCAT or non-VCAT bandwidth at the server layer can also be created by this operation. The server layer SNC (in case of non-VCAT) or the server layer SNCs (in the case of VCAT or LAG), that are already created between the terminating CPTPs via other operations are automatically associated to the new Call. (Bandwidth using LAG cannot be created by this operation.)
- OS deletes a Call
  The Call (and all supporting server layer SNCs) is deleted.
- OS modifies a Call
  The attributes and the capacity of a Call are modified. Note that Routing constraints for each of the new server layer SNCs may be supplied by the requesting OS.

The typical life cycle for a non-VCAT supported Call would be to create the Call, modify the parameters as needed later, and then finally delete the Call.

The typical life cycle for a VCAT or LAG supported Call with automatic server layer SNC creation would be to create the Call (specify automatic server layer SNC creation, number of server layer SNCs and server layer rate); modify the Call later on, adding/removing automatically created server layer SNCs as needed; and then finally delete the Call.

The typical life cycle for a VCAT supported Call with manual server layer SNC creation would be to create the Call (specify manual server layer SNC creation and server layer rate); create explicitly the SNCs, routed as desired; modify the Call later on, creating/deleting the SNC's; and then finally delete the Call.

6.2 Call diversity

It is possible to increase the resilience of a Call by using diverse routed Connections.

7 LAG

7.1 Introduction

Ethernet Link Aggregation (LAG) is supported, both for the LAN side and the WAN side.

Ethernet Link Aggregation is specified in IEEE 802.3ad and will be covered also in ITU-T G.8010.

Supporting LAG is very similar to supporting VCAT. It is a particular variation of Inverse Multiplexing (see SD1-14). Inverse Multiplexing is also referred to as Fragmentation. The specific characteristics of LAG Fragmentation, which differentiate it from Fragmentation generally, are:

- its application specifically to Ethernet, and
- the fact that the signal in any member of the Link Aggregation Group is a valid Ethernet signal.

Link Aggregation is supported by a protocol, called LACP (Link Aggregation Control Protocol) whose task is to guarantee the compatibility of both sides of the aggregated link. This protocol, which is specified in IEEE 802.3ad, has many attributes and configuration parameters. However, these attributes and configuration parameters can be considered to be “low level”, in the sense that they can be handled at the target OS level. The current LAG support does not deal with these attributes and parameters at the requesting OS level.

Similarly, the criteria for distributing Ethernet frames among the LAG members can vary, and some implementations may allow configuring different LAGs with different criteria. It might be desirable to be able to do this from the requesting OS (implying support in the interface), but the specification would be too complex to work out and is therefore currently not included. Where needed, this configuration can be done at the target OS level, or below.

7.2 FTP with new Layer Rate

A LAG is represented by an FTP, whether on the LAN side or on the WAN side. A new layer rate is defined for this FTP, called LR_LAG_Fragment. It is similar to the LR_Fragment layer rate, but in addition to the layer attributes belonging to LR_Fragment, it also has Ethernet attributes, as explained below, and LAG attributes and notifications.

7.3 LAG creation

A LAG FTP may either be created by the target OS and discovered by the requesting OS (like most TPs), or it may be created by the requesting OS using the createFTP() operation.

Whether created by target OS or requesting OS, LAG FTPs act like other Fragment TPs, in that the maximum number of allowed members is in the read-only attribute “AllocationMaximum”, and the number of members desired by the requesting OS is configured using the “AllocatedNumber” attribute.

When created by the target OS, without possibility of creation by the requesting OS, the target OS creates all the potential LAG FTPs that it can handle, each with its “FragmentServerLayer” set to a layer rate for which LAG can be supported, and with “AllocationMaximum” set to the maximum number of members which can be supported for that layer rate. It is understood that populating a LAG FTP for some layer rate may block the possibility of populating other LAG FTPs at a different layer rate or even at the same layer rate. For example: If the bandwidth capacity is 16xVC4, and the possible layer rates are VC4 and VC4-4c, and a LAG can use all of the bandwidth, then the target OS will create 20 LAG FTPs. It will create 16 LAG FTPs with layer rate VC4 and AllocationMaximum=16, and it will create 4 LAG FTPs with layer rate VC4-4c and AllocationMaximum=4. If an operator populates a LAG FTP with 6 VC4s, then only 10 LAG FTPs with layer rate VC4, and 2 LAG FTPs with layer rate VC4-4c, remain as candidates for population. Even though the value of AllocationMaximum does not change, an

attempt to populate a LAG FTP with more members than there is remaining available bandwidth will be rejected.

7.4 Populating LAGs with VCATs

Since a LAG can also have members which are VCATs, where this is supported by the equipment, an target OS or requesting OS may create LAG FTPs which have FragmentServerLayer = LR_Fragment.

7.5 Associating LAG_Fragment CTPs with actual TPs

Once the AllocatedNumber attribute of a LAG FTP has been set to *n*, the requesting OS can assume, or it can discover by uploading the FTP, that there are *n* server side CTPs, numbered 1 through *n*. These CTPs will have layer rate LR_LAG_Fragment.

LAG_Fragment CTPs will have an attribute called LagMember which points to an actual TP, which is the actual member of the LAG. It is an error for the layer rate of the actual TP to be different from the layer rate specified in the FragmentServerLayer attribute of the LAG FTP.

Alternatively, there may be a cross-connect between the LAG_Fragment CTP and the actual TP to which it is associated. Here, too, it is an error for the layer rate of the actual TP to be different from the layer rate specified in the FragmentServerLayer attribute of the LAG FTP.

The value of a LagMember pointer is the DN (Distinguished Name) of the actual TP to which the LAG_Fragment CTP points.

When the LAG is aggregating VCATs, the LagMember pointer (or cross-connect) will point to an FTP which represents a VCAT. The target OS may reject an attempt to populate a LAG with VCATs which don't all have the same FragmentServerLayer and AllocatedNumber.

It is an error to have an actual TP being a member of more than one LAG.

On the LAN side, a LAG_Fragment CTP will point to an Ethernet PTP. All member PTPs of a LAG must be of the same Ethernet rate.

7.6 Naming of LAG TPs

LAG naming rules are the same as VCAT naming rules. A LAG FTP is identified in a similar way as a PTP, either with reference to the host equipment, with the specific FTP given some number by the target OS, or by some other identification scheme used by the target OS for PTPs. When the FTP is told to configure *n* member, they will become CTPs, under the FTP, with layer rate LR_LAG_Fragment, and numbered 1 to *n*.

For example, a LAG which aggregates 3 VC4s would look like this (in a "shorthand" version):

OS=xxx/NE=yyy/FTP=ftpIDi, layer= *the number for* LR_LAG_Fragment, FragmentServerLayer= *the number for* VC4, AllocatedNumber=3

CTP=/lag_fragment=1, LagMember=<DN of the real VC4 associated with 1st member CTP>

CTP=/lag_fragment=2, LagMember=<DN of the real VC4 associated with 2nd member CTP>

CTP=/lag_fragment=3, LagMember=<DN of the real VC4 associated with 3rd member CTP>

For another example, a LAG which aggregates 2 VCATs of VC4s might look like this:

OS=xxx/NE=yyy/FTP=ftpIDj, layer= the number for LR_LAG_Fragment, FragmentServerLayer= the number for LR_Fragment, AllocatedNumber=2

CTP=/lag_fragment=1, LagMember=<DN of the real VCAT FTP associated with 1st member CTP>

CTP=/lag_fragment=2, LagMember=<DN of the real VCAT FTP associated with 2nd member CTP>

7.7 Association by OS

In some implementations, setting the AllocatedNumber attribute of a LAG FTP causes the target OS to select the real TPs which will be associated with the LAG member CTPs. In this case, the target OS will set the LagMember pointers with the DNs of the selected TPs. In other implementations, setting the AllocatedNumber attribute of a LAG FTP causes the target OS to create the member CTPs, whose LagMember pointers remain empty until set by the requesting OS. An requesting OS can see if the target OS selected TPs for association by checking the value of LagMember pointer.

7.8 Manual LAG population vs Automatic LAG population by LACP

Some LACP implementations determine by themselves the number of members in a particular LAG and who those members are. In order to allow this, there will be a LAG attribute called AutoLAG, with values Enabled and Disabled. When Enabled, the target OS will set the AllocatedNumber attribute of the LAG FTP and LagMember attributes of the LAG_Fragment CTPs, according to the determination of the LACP. When the equipment does not support automatic LAG configuration, or if the target OS does not want to allow it, the target OS will reject an attempt to set AutoLAG to Enabled. If the requesting OS wants to impose LAG configuration, it will set AutoLAG to Disabled.

7.9 LAG members cannot be CPTPs

A LAN port, which usually can be an edge CPTP, cannot be an edge CPTP if it is a member of a LAG. The LAG FTP is the edge CPTP.

Similarly, an FTP on the WAN side, which usually can be a CPTP which is an endpoint of a Call, cannot be a Call endpoint if it is a member of a LAG. The LAG FTP is the Call endpoint.

7.10 LAG attributes and PM counters

The LAG FTP, in addition to being a Fragment, with Fragment attributes, and in addition to having the AutoLAG attribute which is special to the LAG FTP, also acts like an Ethernet port, with all of the attributes which Ethernet ports have.

Similarly, PM counters normally associated with an Ethernet port are also associated with a LAG FTP. LAN side counters will be maintained on LAN side LAG FTPs, and WAN side counters will be maintained on WAN side FTPs. This is in addition to the counters associated with each of the LAG members.

LAG FTPs will report TCAs, in addition to the TCAs which will be reported by the LAG members.

7.11 A LAG is a STP port

A LAG is an STP port, and therefore has all of the attributes needed for STP management. A port which is a member of a LAG cannot be a STP port. The target OS will reject an attempt to treat a LAG member like a STP port.

7.12 LAG Alarms

A LAG FTP will report the Ethernet alarms (and TCAs) and STP alarms (and TCAs) that can be reported by an Ethernet port. In addition, when all LAG members are down, a LinkDown alarm will be reported by the LAG FTP. When some members are functioning, but at least one member is down, a PartialLinkDown alarm will be reported. The individual LAG members will report their own alarms.

7.13 LAG use in Call creation must be explicit

The target OS will not create a LAG when a establishCall operation requests automatic creation of server SNCs. In order for a Call to use a LAG endpoint, the LAG must already exist and the Call created explicitly using that LAG.

7.14 Modeling aggregation of signals for Ethernet CPTPs

The following diagrams show that a CPTP on the Ethernet side (LAN side) of an MFD (the yellow connector on top) can either be a port (the purple PTP) or an aggregation of several ports (the striped FTP). On the transport side (WAN side), a CPTP is either a VCAT (striped FTP labeled VCAT), an aggregation of VCATs or VCx (striped FTP labeled LAG), or a single VCx. (VCx is used generically, and can also be a TUx or a SONET equivalent of these. VCx sometimes is used in the plural sense, to avoid writing VCxs.) A VCx can either be a floating one (see the striped FTP labeled VCx), which needs to be connected to a PTP, or it can be a CTP already belonging to a PTP. The first diagram (Figure 11) shows a floating VCx and the second diagram (Figure 12) shows a VCx belong to a PTP. The diagrams also show that a LAG on the WAN side can aggregate either VCATs or non-concatenated VCx.

A new layer rate LR_LAG_Fragment.has been introduced.

LAG Fragmentation differs from Fragmentation in that is doesn't change the nature of the signal, it just distributes it. Each LAG member carries a valid Ethernet signal. The regular Fragmentation is assumed to change the signal. VCAT Fragmentation, for example, takes Encapsulated Ethernet and distributes it among the VCx such that the VCx are not carrying valid Ethernet signals. In addition to this difference, a LAG Fragment FTP has specific characteristics of an Ethernet port, as opposed to the usual Fragment, which is a general TP. The LAG Fragment FTP has many more attributes than a Fragment TP.

Usually VCAT FTPs are created by the target OS (or below). The number of existing VCATs is the maximum number that the equipment can use at a given time. However, when the target OS allows CPTP creation, a CPTP can be created as a VCAT. Whether created by target OS or requesting OS, they are born unpopulated (without member CTPs). They become populated with member CTPs by configuration, when the requesting OS tells the target OS how many members are required. After that, the requesting OS associates the VCAT member CTPs with actual TPs.

LAG FTPs are very similar in this regard to VCAT FTPs. They can be created either by the target OS (or below) or by the requesting OS. LAG FTPs are populated in the same way as VCAT FTPs. A LAG member CTP is associated with an actual TP (port on the LAN side, VCAT or VCx on the WAN side) either by pointer or connection. Note that associating a VCAT FTP with a LAG member CTP means creating two levels of inverse multiplexing. A LAG FTP contains members which associate to FTPs which themselves contain members which associate to TPs.

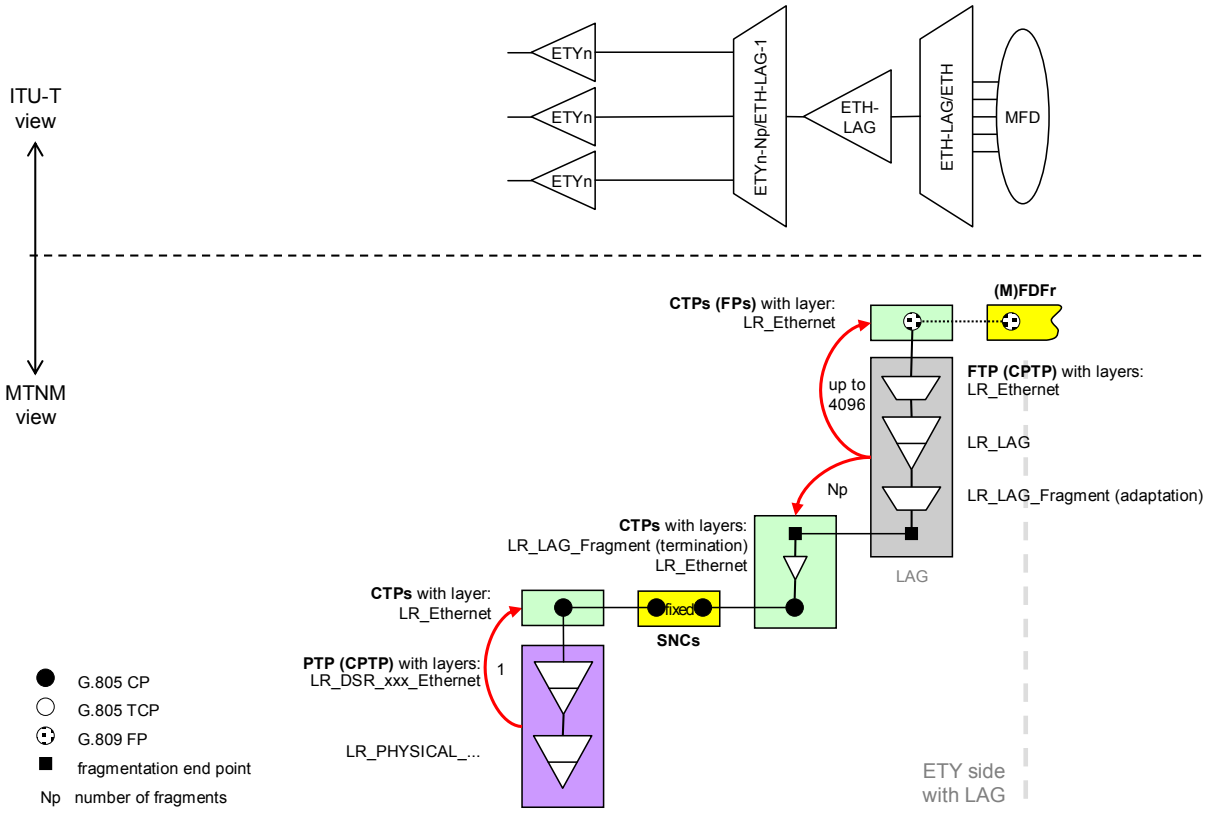


Figure 11: Example: Ethernet LAN port with LAG and VLAN

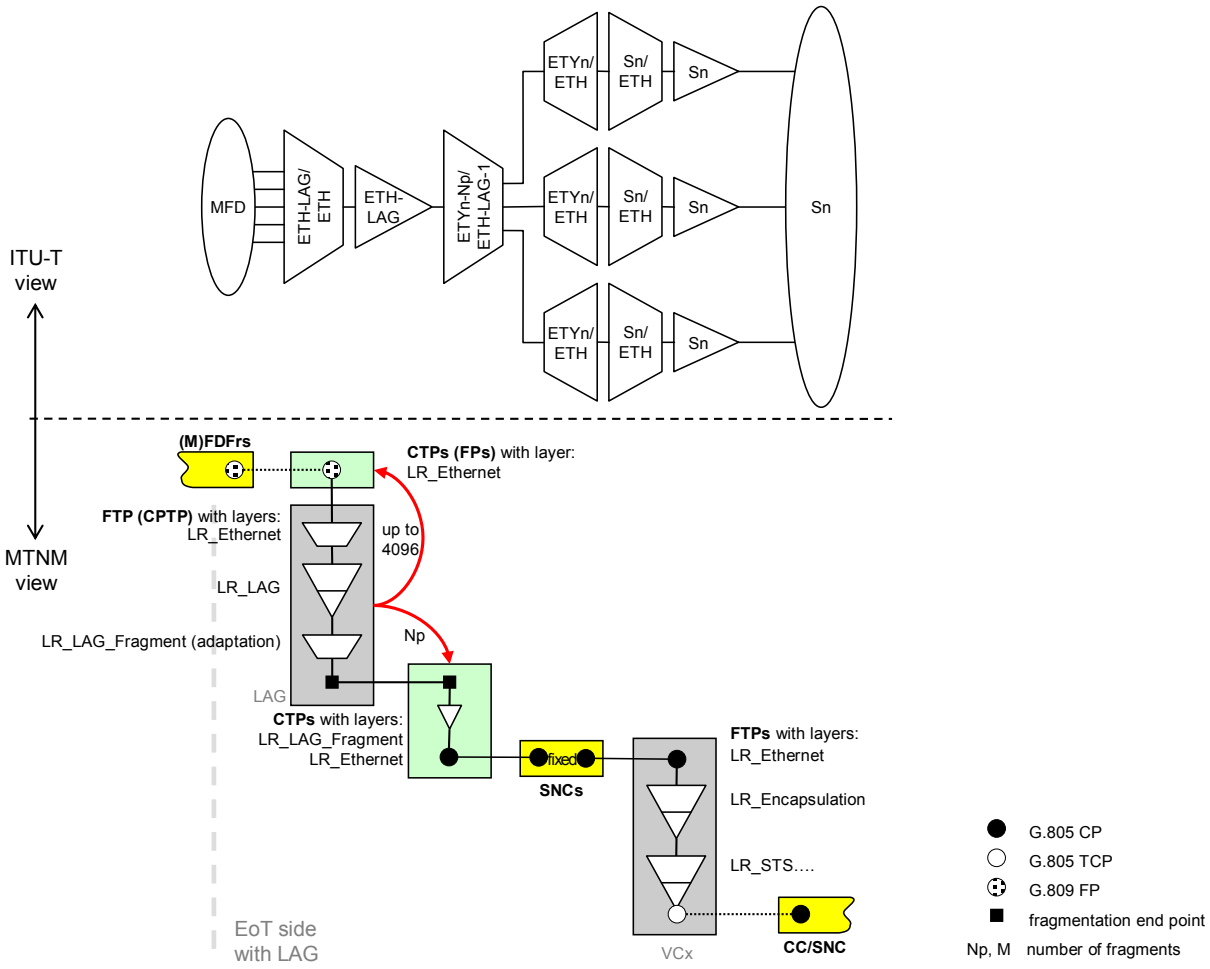


Figure 12: Example: Ethernet WAN port with LAG and VLAN

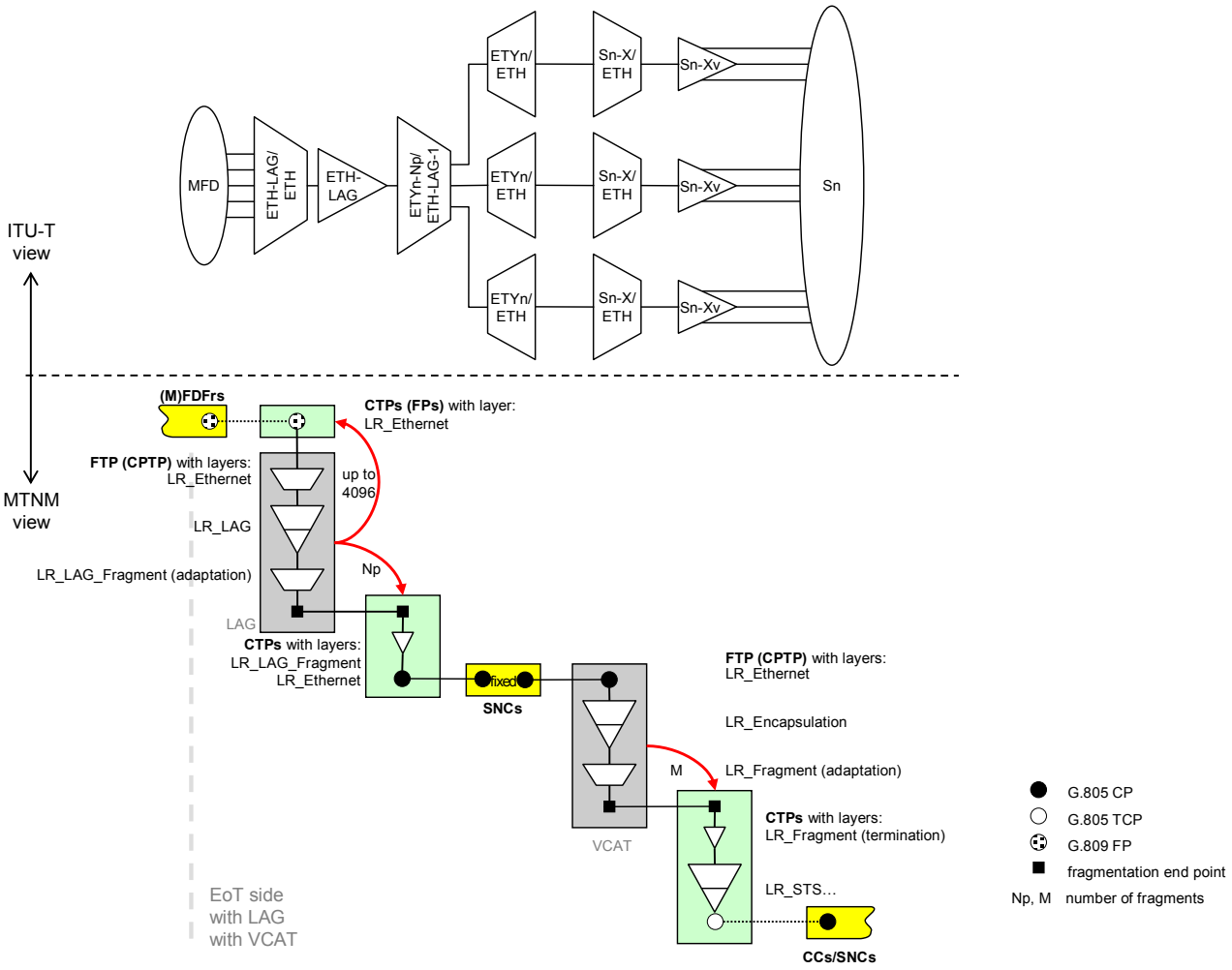


Figure 13: Example: Ethernet WAN port with LAG ,VLAN and VCAT

8 Tag Management

8.1 VLAN Tag

Per IEEE 802.1ad [14], a VLAN tag consists of the following parts:

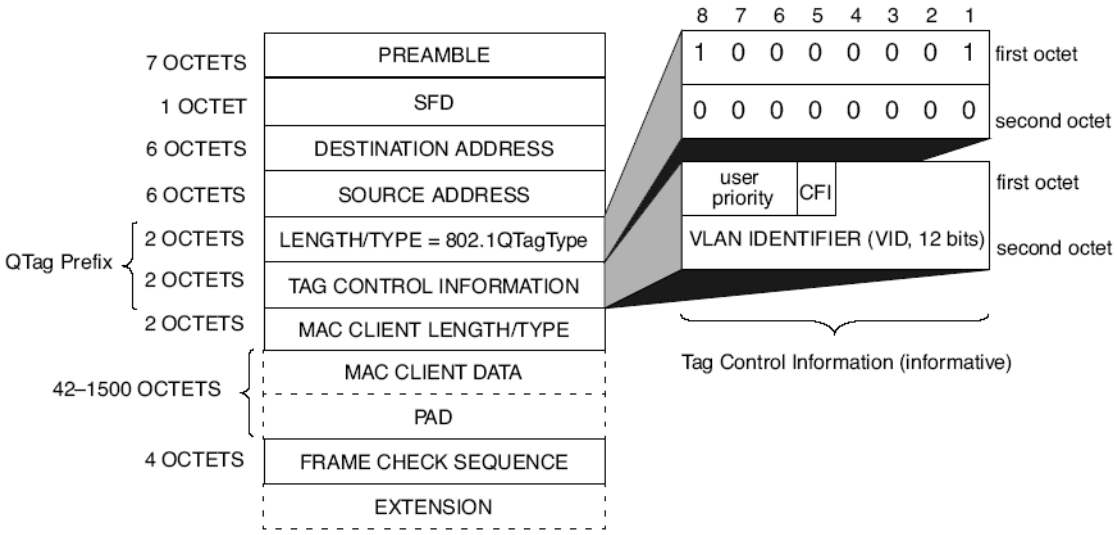


Figure 3–3—Tagged MAC frame format

Figure 14: Figure 3-3 / IEEE 802.3

- A Tag Protocol Identifier (TPID) – 16 bits. This will identify the tag as either being a "C-Tag" or an "S-Tag". The TPID of "81-00" is reserved for a "C-Tag", and the TPID of an "S-Tag" is "88-a8" (however, some vendors use "FF-FF" and some use "91-00").
- Tag Control Information (TCI):
    - If the Tag is a "C-Tag", the fields are:
        - Priority Code Point (PCP) – 3 bits
        - *Canonical Format Indicator* (CFI) – 1 bit
        - VLAN ID – 12 bits

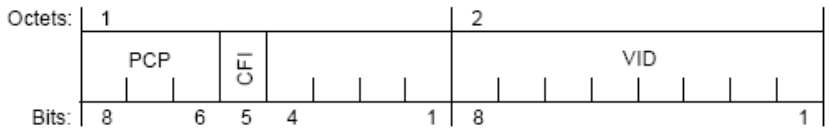


Figure 9-1— ~~VC~~-TAG TCI format

Figure 15: Figure 9-1 / IEEE 802.1ad

- If the Tag is an "S-Tag", the fields are:
    - Priority Code Point (PCP) – 3 bits
    - *Drop Eligibility Indicator* (DEI) – 1 bit
    - VLAN ID – 12 bits

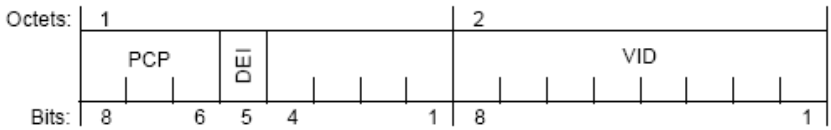


Figure 9-2— S-TAG TCI format

Figure 16: Figure 9-2 / IEEE 802.1ad

- Additional information, as needed by the tag type and Tag Control Information

8.2 General Tag Management

In order to enforce that incoming frames have a VLAN Tag (or not), the *PortAcceptableFrameTypes* parameter should be set accordingly. In addition, if *PortAcceptableFrameTypes* is “All” or “VlanTaggedOnly”, in order to enforce that those incoming frames have a VLAN Tag matching the provisioned VLANs on the port, the *EnableIngressFiltering* parameter should be set to “Enabled”.

To strip the outermost VLAN Tag from the frame on egress, the *VLANsForUntaggingOnEgress* would have the set of VLAN IDs that this should be performed on.

8.3 IEEE 802.1Q-compliant Tagging

As per IEEE 802.1Q, the incoming tag is a “C-Tag” and it is not translated.

The following parameters would be set on the CPTP:

- *PVID* = "0"
- *TPID* = “8100”

And the following parameters would be set on the Flow Point:

- *AddSTag* = “false”

If the port were to allow untagged frames and to tag them on ingress, the parameters would be set on the CPTP as follows instead:

- *PVID* = the C-Tag VLAN ID
- *PVIDFrameTypes* = “UntaggedOnly”
- *TPID* = “8100”
- *PortDefaultUserPriority* = default user priority for the added tag

The IEEE 802.1Q standard forbids tag translation, but if the hardware supported it anyway, the following parameters would be set on the CPTP:

- *CTagTranslationEnable* = “enabled”
- *CTagTranslation_Table_** = structure of pairs of external VLAN IDs and internal VLAN IDs.

  For example, a mapping of

  CTagTranslation_Table_Count = “3”

  CTagTranslation_Table_External = “1,2,3”

  CTagTranslation_Table_Internal = “2,3,1”

means on ingress, a VLAN ID of 1 will be re-mapped to 2 and on egress, a VLAN ID of 1 will be re-mapped to 3, etc.

In a color-aware network, it may be desired to encode the drop eligibility in the CFI bit (as is done for the DEI bit in the S-Tag).

8.4 IEEE 802.1ad-compliant Tagging

As per IEEE 802.1ad [14], the incoming tag is a “C-Tag” and it may be translated[1]. The Service Provider adds an additional tag, called an “S-Tag”.

The following parameters would be set on the CPTP:

- *PVID* = "0"
- *PVIDFrameTypes* = “AllFrames”
- *TPID* = any value from “0601 to FFFF”, except “8100”
- *PortDefaultUserPriority* = default user priority for the S-Tag

And the following parameters would be set on the Flow Point:

- *IVID* = VLAN ID for the FDFr
- *AddSTag* = “true”

If C-Tag (inner tag) translation were needed, the following parameters would be set on the CPTP:

- *CTagTranslationEnable* = “enabled”
- *CTagTranslation_Table_** = structure of pairs of external VLAN IDs and internal VLAN IDs.

  For example, a mapping of

  CTagTranslation_Table_Count = “3”

  CTagTranslation_Table_External = “1,2,3”

  CTagTranslation_Table_Internal = “2,3,1”

  means on ingress, a C-Tag VLAN ID of 1 will be re-mapped to 2 and on egress, a VLAN ID of 1 will be re-mapped to 3, etc. The S-Tag will remain the same.

If S-Tag (outer tag) translation were needed, the following parameters would be set on the CPTP:

- *STagTranslationEnable* = “enabled”
- *STagTranslation_Table_** = structure of pairs of external VLAN IDs and internal VLAN IDs.

  For example, a mapping of

  STagTranslation_Table_Count = “3”

  STagTranslation_Table_External = “1,2,3”

  STagTranslation_Table_Internal = “2,3,1”

  means on ingress, an S-Tag VLAN ID of 1 will be re-mapped to 2 and on egress, a VLAN ID of 1 will be re-mapped to 3, etc.

Both the C-Tag and S-Tag translation may be specified at the same time and will operate independently of each other.

[1] Note: C-Tag translation is not defined in IEEE 802.1ad (only S-Tag translation).

9 Traffic Mapping Table

9.1 Explanations

The Traffic Mapping Table is used to select frames coming into or going out of a CPTP, or an FP, and to specify some decisions about what to do with the selected frames. There is no limit, other than those imposed by practical processing considerations, to the number of selection criteria or to the number of resulting actions.

A Traffic Mapping Table at a CPTP applies to all frames entering into or going out of the CPTP. A Traffic Mapping Table at an FP selects the frames, from among the frames entering at the CPTP, which are to be directed to the FDFr for whom this FP is an endpoint. An attempt to create an FP, with a Traffic Mapping Table which would select some frames which are already selected by some other FP of the same CPTP, is rejected with INVALID_INPUT. Any frame coming into a CPTP, which is not selected by some FP of the CPTP, is dropped.

Some columns of the table represent selection criteria (these are called “From” columns), and the other columns represent resulting actions to be performed on selected frames (these are called “To” columns). A row of the table contains the values by which frames are selected. In each cell of a row, in the “From” columns of the table, there must be values which belong to the set of values which are compatible with the selection criteria which the column represents. Similarly, in each cell of a row, in the “To” columns of the table, there must be values which belong to the set of values which are compatible with the results actions which the column represents. The result actions specified in the “To” columns of a row of the table are applied to the frames which were selected by the “From” columns of the same row of the table. In order for a frame to be selected, it must fulfill the criteria in all of the “From” columns for some row. The actions specified in all of the “To” columns, in a particular row, will be applied to all of the frames selected by the “From” columns in the same row. It is not acceptable for a frame to be able to be selected by more than one row.

There is a layered parameter, "TrafficMappingTable_Count", which contains the number of rows in the table. There is a layered parameter for each column. The “From” columns are represented by layered parameters named "TrafficMappingFrom_Table_xxxx", where xxxx is the name of the selection criterion. See example. The “To” columns are represented by layered parameters named "TrafficMappingTo_Table_xxxx", where xxxx is the name of the action to be applied. Each parameter representing a column has a value which is a string of cell values separated by commas. The number of comma-separated values in each parameter must be equal to the value of "TrafficMappingTable_Count".

The names of certain parameters, representing selection criteria (“From” columns) and results actions (“To” columns), are to be recognized and understood by all complying systems (even if not used). These are listed in the Layered Parameters list. Other parameter names may be used as agreed by cooperating systems.

Example 1:

The following table specifies selection criteria VLAN ID and Priority field, and result actions Traffic Class assignment and Traffic Conditioning Profile assignment.
Note: in this example there is no Egress Traffic Conditioning Profile defined, as it is optional.

VLAN ID	Priority	Traffic Class	TC Profile ID
1-1000	0-1	0	52
1-1000	2-3	1	64
1-1000	4-5	2	17

VLAN ID	Priority	Traffic Class	TC Profile ID
1-1000	6-7	3	99
1001-2000	0-2	0	52
1001-2000	3-7	1	127
2001-3600	0	0	100
2001-3600	1-6	2	102
2001-3600	7	3	103
4000, 4010, 4020	all	1	101
allOthers	all	0	100

Table 4: Example Traffic Mapping Table

All frames whose VID (in the outermost header) has a value between 1 and 1000, and whose priority field (in the outermost header) is 0 or 1, will be assigned to Traffic Class 0 and will be assigned the TC Profile whose ID is 52. All frames whose VID (in the outermost header) has a value between 2001 and 3600, will be assigned Traffic Classes and Profiles according to their Priority Fields. All frames with VID 4000 or 4010 or 4020 will be assigned to Traffic Class 1 and will be assigned the TC Profile whose ID is 101. Etc. All frames which are not covered by the selection criteria specified in the first ten rows of the table (the row of titles is not counted) will be assigned to Traffic Class 0 and will be assigned the TC Profile whose ID is 100.

Example 2:

The following tables specifies a VLAN ID and Priority field selection criteria, and the resulting Traffic Class assignment, and both Ingress and Egress Traffic Conditioning profile assignment. This traffic mapping is designed to be applied to a flow point (FP) representing the UNI/EVC specification for an Ethernet Virtual Private Line. The Ingress and Egress TC Profiles are to be applied “per EVC”. For all ingress traffic with VLAN ID = 10-100, TC profile 100 will be applied; similarly, for egress traffic TC profile 102 is applied.

VLAN Id	Priority	Traffic Class	TC Profile	Egress TC Profile
10-100	All	1	100	102

Table 5: Example of Traffic Mapping for Ingress and Egress

9.2 Table Processing Rules

9.2.1 Selection Criteria strings, recognized by compliant systems

9.2.1.1 Outer VLAN ID

Layered parameter: "TrafficMappingFrom_Table_VID"

meaning: select according to VLAN ID of outermost frame header

values: single integer between 1 and 4094 (inclusive), or
parenthesized list of single integers (1-4094), separated by commas, or
range in the form a-b, where 1 ≤ a, b ≤ 4094 and a < b, or
“all”, or
“untagged”, or
“allOthers”

9.2.1.2 Inner VLAN ID

Layered parameter: "TrafficMappingFrom_Table_InnerVID"

meaning: select according to VLAN ID of inner frame header

values: single integer between 1 and 4094 (inclusive), or
parenthesized list of single integers (1-4094), separated by commas, or
range in the form a-b, where 1 ≤ a, b ≤ 4094 and a < b, or
“all”, or
“untagged”, or
“allOthers”

9.2.1.3 Priority field of header

Layered parameter: "TrafficMappingFrom_Table_Priority"

meaning: select according to the priority field of outermost frame header

values: 1-digit number in the range 0-7, or
parenthesized list of 1-digit numbers in the range 0-7, separated by commas, or
range in the form a-b, where a and b are 1-digit numbers (0-7) and a < b, or
“all”, or
“allOthers”

9.2.1.4 Inner Priority field of header

Layered parameter: "TrafficMappingFrom_Table_InnerPriority"

meaning: select according to the priority field of inner frame header

values: 1-digit number in the range 0-7, or
parenthesized list of 1-digit numbers in the range 0-7, separated by commas, or
range in the form a-b, where a and b are 1-digit numbers (0-7) and a < b, or
“all”, or
“allOthers”

9.2.2 Results Actions strings, recognized by compliant systems

9.2.2.1 Traffic Class

Layered parameter: "TrafficMappingTo_Table_TrafficClass"

meaning: assign selected frames to the specified traffic class

values: integer between 0 and 7 (inclusive), or “default” or empty (same as “default”)

9.2.2.2 Traffic Conditioning Profiles

Layered parameter:

"TrafficMappingTo_Table_TcProfile" and
“TrafficMappingTo_Table_EgressTcProfile”

meaning: assign specified traffic conditioning profile to the selected frames in either an ingress or egress direction

values: existing profile ID, or “default” or empty (same as “default”)

9.2.3 Order of selection columns

When only VID and Priority are used as selection criteria, the order of applying them should not make any difference in the selection results. If other selection criteria are used, by agreement, and if the order of applying the criteria is significant, the agreement should specify the ordering rules.

9.2.4 Order of selection rows

Since it is an error for a frame to be able to be selected by more than one row, the order of rows is not significant.

VLAN ID	Priority	Traffic Class	TC Profile ID
1-250	all	0	52
200-1000	2-3	1	64

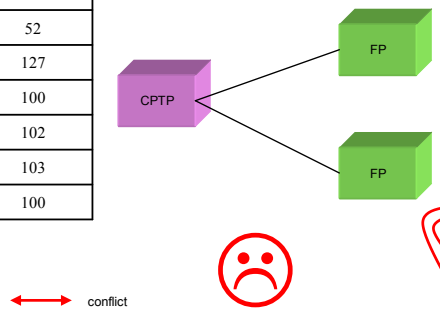
Note that “allOthers” can appear in a row which is before rows with specific values. It still means that the values used are the ones left after the specific values have been used. “allOthers” cannot appear in a column more than once, unless they are mutually exclusive due to other selection columns. “all” cannot appear with any other rows, unless they are mutually exclusive due to other selection columns.

VLAN ID	Priority	Traffic Class	TC Profile ID
1-1000	0-1	0	52
1-1000	allOthers	1	64
1-1000	4-5	2	17
1-1000	6-7	3	99
1001-2000	AllOthers	0	52
1001-2000	3-7	1	127

VLAN ID	Priority	Traffic Class	TC Profile ID
1-250	All	0	52
1-250	2-3	1	64

Furthermore, since a frame cannot be selected by more than one FP, “allOthers” cannot appear in a column more than once among all of the Traffic Mapping Tables of all the FPs of a CPTP, unless they are mutually exclusive due to other selection columns. Similarly, “all” cannot appear with any other rows among all of the Traffic Mapping Tables of all the FPs of a CPTP, unless they are mutually exclusive due to other selection columns.

VLAN ID	Priority	Traffic Class	TC Profile ID
1001-2000	0-2	0	52
1001-2000	3-7	1	127
2001-3600	0	0	100
2001-3600	1-6	2	102
2001-3600	7	3	103
AllOthers	all	0	100



VLAN ID	Priority	Traffic Class	TC Profile ID
1-250	all	0	52
allOthers	allOthers	1	64

VLAN ID	Priority	Traffic Class	TC Profile ID
200-250	2-3	0	52
all	default	1	64
1001-2000	0-2	2	100
1001-2000	allOthers	1	120
2001-3600	allOthers	0	100

“allOthers” can be used to select all remaining frames which are not selected by any other FP of the CPTP. Note that “allOthers” might not select any frames, if every frame is selected by some row from among all of the Traffic Mapping Tables of all the FPs of the CPTP. Therefore, it is legal for both “all” and “allOthers” to appear, in which case the “allOthers” will not select any frames.

9.2.5 Default and empty values

Where the value “default”, or an empty value (which means “default”), is acceptable, and is used, the result is that the target OS chooses the value which is to be used.

9.2.6 Unselected frames

The frames entering a CPTP which has no Traffic Mapping Table can still be selected by a Traffic Mapping Table at one of the FPs of the CPTP. When a CPTP has a Traffic Mapping Table, a frame which is not selected by any of the rows of the CPTP’s Traffic Mapping Table can still be selected by a Traffic Mapping Table at one of the FPs of the CPTP. A frame which is not selected by a Traffic Mapping Table, at one of the FPs of a CPTP, is dropped.

9.2.7 Invalid values

An invalid value in a column representing a recognized selection criterion or results action (i.e., that appears in the Layered Parameters list) is considered an error.

9.2.8 Wrong number of columns

It is an error (INVALID_INPUT) for any "TrafficMappingFrom_Table_xxxx" or "TrafficMappingTo_Table_xxxx" parameter to contain a number of members which is different from "TrafficMappingTable_Count". Empty members can be designated by consecutive commas or a comma with nothing after it (if the last member is empty).

9.2.9 Unrecognized selection criterion or results action

If a "TrafficMappingFrom_Table_xxxx" or "TrafficMappingTo_Table_xxxx" parameter is not in the Layered Parameters list or in an implementation agreement, the request which introduces the unrecognized parameter is rejected with exception EXCPT_NOT_IMPLEMENTED, with the name(s) of all unrecognized parameters (separated by commas) in the Error Reason field of the exception.

9.2.10 Selection using two frame headers

There are systems which need to select frames according to both the outermost header and the header directly “under” the outermost header. Typically they would be the S-Tag and the C-Tag. In order to accommodate this situation, two more columns would be used: InnerVID and InnerPriority. In order for a frame to be selected by a particular row, it would need to fulfill the criteria expressed by all four “From” columns: VID, Priority, IVID, and IPriority.

Example:

VLAN ID	Priority	Inner VLAN ID	Inner Priority	Traffic Class	TC Profile ID
1000	0-1	10	0-3	0	52
1000	0-1	10	allOthers	1	64
1000	allOthers	10	2-3	1	64
1000	0-1	20	0	2	17
1000	allOthers	20	allOthers	3	99
1000	all	allOthers	all	0	90
2000	(0,7)	all	all	2	30
2000	allOthers	all	all	3	33
2001-4000	all	all	all	0	52

Table 6: Example Traffic Mapping Table for 2-header selection

In order for a frame to be selected by the first row, the outer header must have VID =1000 and Priority either 0 or 1 AND the next inner header must have VID=10 and Priority in the 0 to 3 range.

9.3 Example layered parameters

The tables described in Table 4 could be represented as layered parameters, as follows:

"TrafficMappingTable_Count" = "11"

"TrafficMappingFrom_Table_VID” =

“1-1000,1-1000,1-1000,1-1000,1001-2000,1001-2000,2001-3600,2001-3600,2001-3600,(4000,4010,4020),allOthers”

"TrafficMappingFrom_Table_Priority” = “0-1,2-3,4-5,6-7,0-2,3-7,0,1-6,7,all,all”

"TrafficMappingTo_Table_TrafficClass” = “0,1,2,3,0,1,0,2,3,1,0”

"TrafficMappingTo_Table_TcProfile” = “52,64,17,99,52,127,100,102,103,101,100”

The table described in Table 6 would be represented as layered parameters, as follows:

"TrafficMappingTable_Count" = "9"

"TrafficMappingFrom_Table_VID" = “1000,1000,1000,1000,1000,1000,2000,2000,2001-4000”

"TrafficMappingFrom_Table_Priority” = “0-1,0-1,allOthers,0-1,allOthers,all,(0,7),allOthers,all”

"TrafficMappingFrom_Table_InnerVID” = “10,10,10,20,20,allOthers,all,all,all”

"TrafficMappingFrom_Table_InnerPriority” = “0-3,allOthers,2-3,0,allOthers,all,all,all,all”

"TrafficMappingTo_Table_TrafficClass” = “0,1,1,2,3,0,2,3,0”

"TrafficMappingTo_Table_TcProfile” = “52,64,64,17,99,90,30,33,52”

Appendix I Hypothetical Ethernet network examples

Figure 17and Figure 18 depict an Ethernet WAN application deployed over a single SONET/SDH transport ring. Some transport NEs participate in bridging and VLAN activities while some other NEs are only operated at the SONET/SDH layer. A requesting OS may manage this application by means of one or several target OS depending on the NE vendors involved (most likely only one in this particular example). Each target OS may itself support a different level of abstraction of the Ethernet network, for example:

Each individual matrix (a.k.a., bridge) within the ME is presented as a flow domain, hence providing the requesting OS for managing flow domain fragments (FDFr, a.k.a. VLANs) within the boundaries of a single matrix. SONET/SDH sub-network connections provisioned to interconnect flow domains/matrices (inter-FD) are top-level topological links (at Ethernet layer rate) similar to those interconnecting Multi Layer Subnetworks (MLSNs) in a connection-oriented network. This mode of operation is equivalent to the singleton MLSN view with the exception that the level of granularity is no longer the ME but its matrix sub-component. A vendor target OS may need to use this solution if it does not support a network view within its own management domain. In this case a flow domain does not usually reflect the resources involved for delivering Ethernet services to customers but rather an implementation constraint. Figure 17 illustrates this scenario.

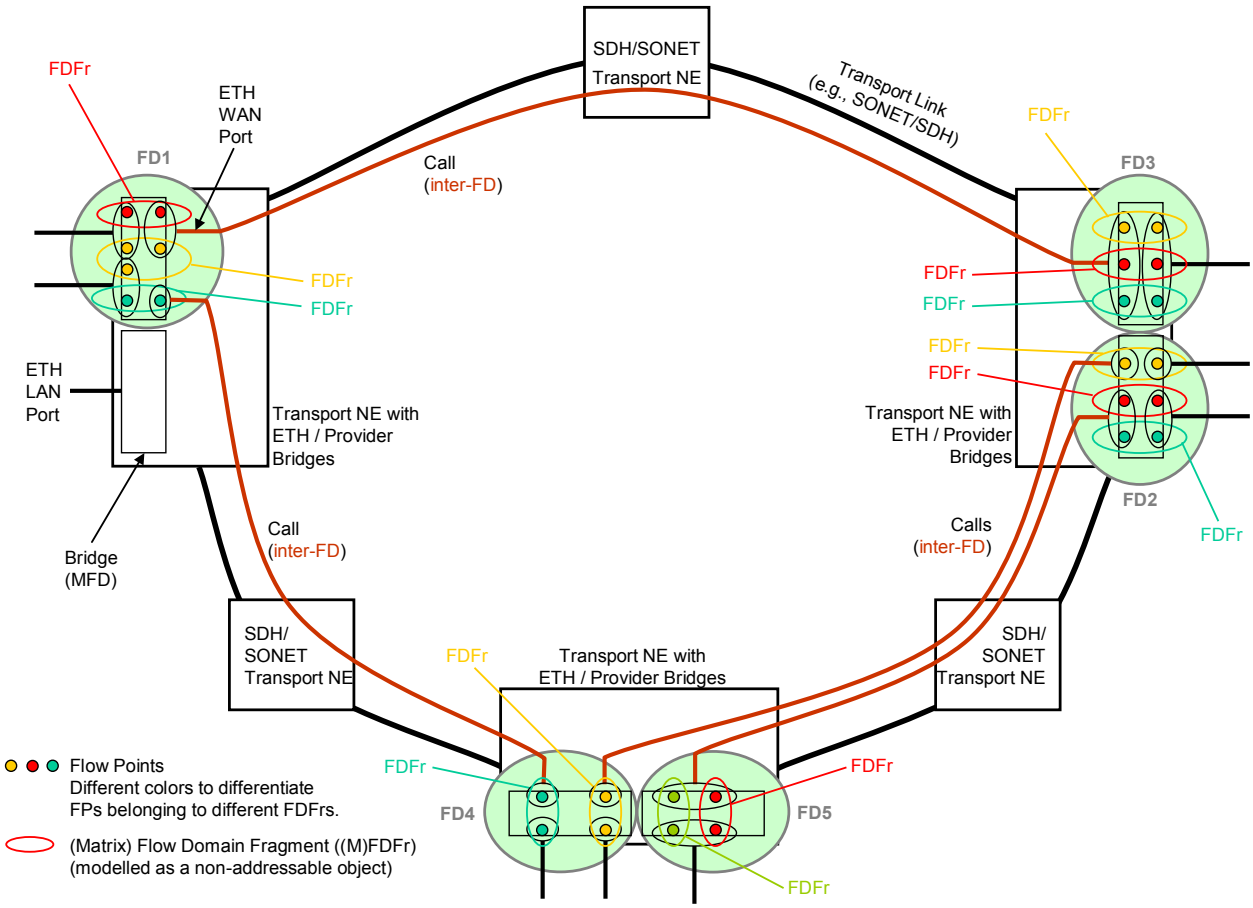


Figure 17: Hypothetical network example showing singleton FDs

Note: Not all entities shown are modelled as managed objects.

- Matrices, usually (but not necessarily) located on separate MEs, are logically associated and presented by the target OS as the flow domains within which the requesting OS can establish

flow domain fragments. A flow domain is likely to represent the resources involved within the target OS domain for delivering Ethernet services to a group of customers. Some level of details internal to the flow domain may not need to be presented to the requesting OS which would then assume that proper instrumentation (matrices) and connectivity (intra-FD Ethernet links) are in place for Ethernet services (FDFr) to be managed. Those flow domains would usually have administrative significance (customer segregation), so the need for topological links between flow domains managed by the same target OS is less likely than for singleton case. Figure 18 illustrates this scenario.

Note that in order to manage flow domain fragments across the entire network the requesting OS needs to define the topological links established between flow domains managed by different target OS (in the same way that it needs to know the topological links existing between MLSNs in order to manage network connections made of multiple SNCs).

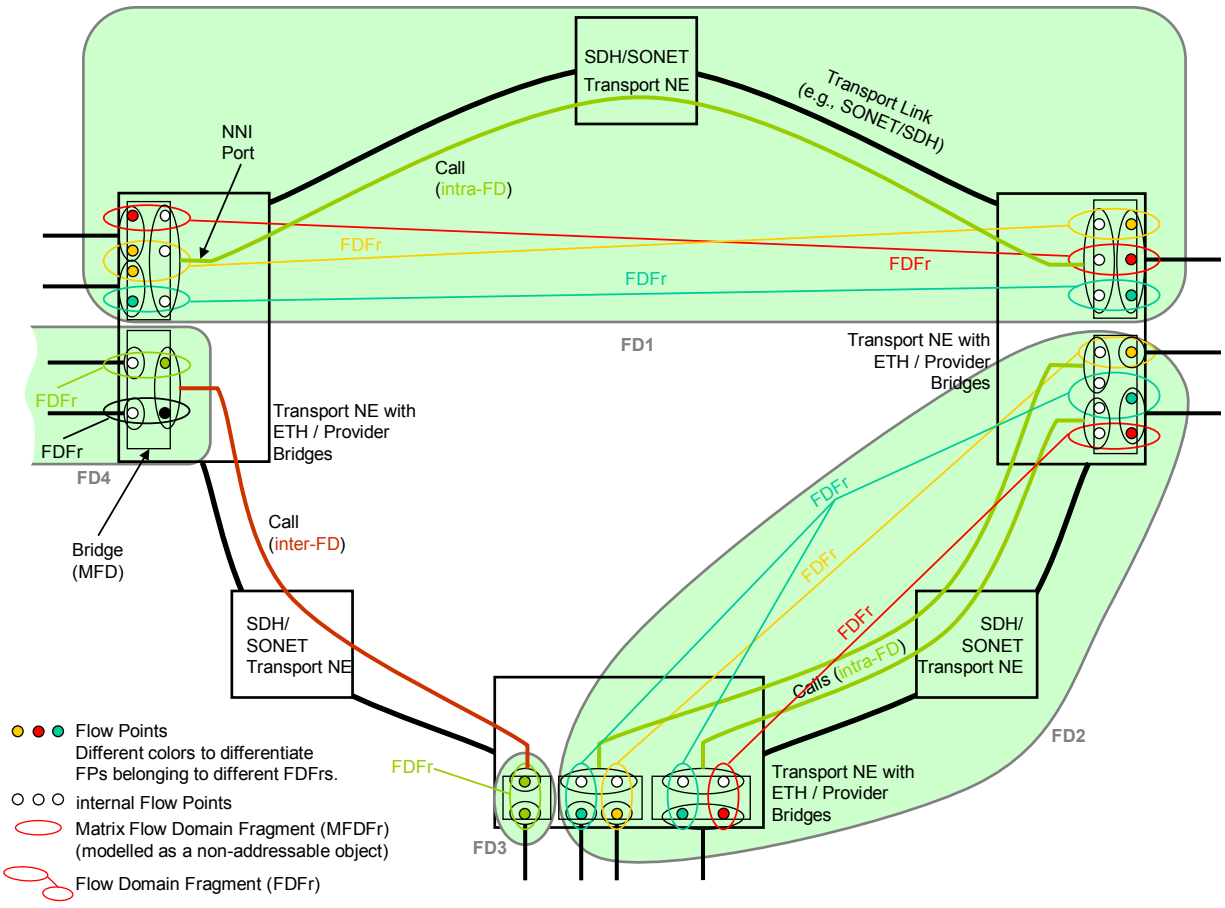


Figure 18: Hypothetical network example showing FDs that span several NEs

Note: Not all entities shown are modelled as managed objects.

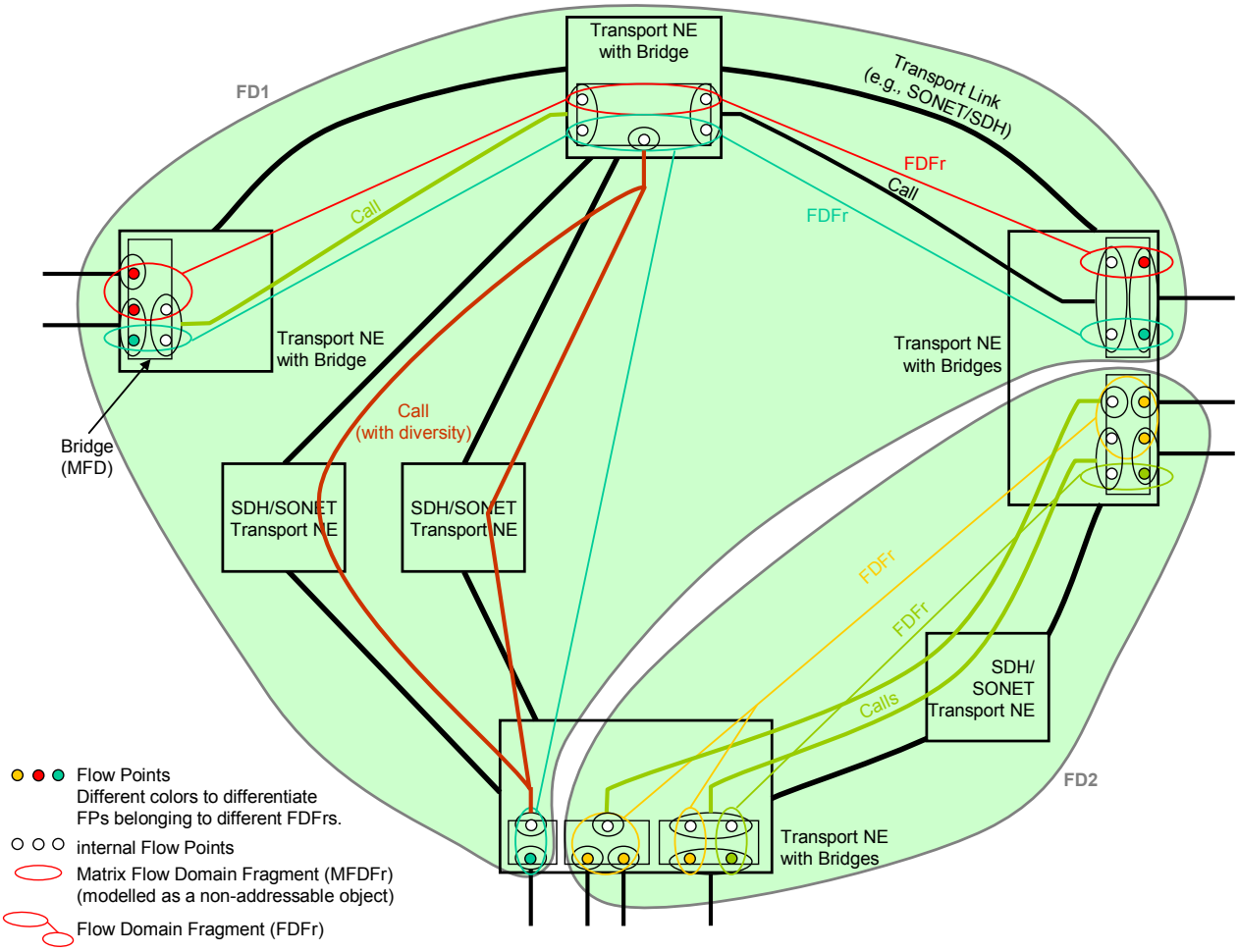


Figure 19: Hypothetical network example showing FDs that span several NEs and internal MFDs

Note: Not all entities shown are modelled as managed objects.

Mapping of G.8010 Entities

The intention of Figure 20 is to list the network entities within the Ethernet Layer Network Domain identified in G.8010 and to explain their mapping and relations to mTOP Interface objects.

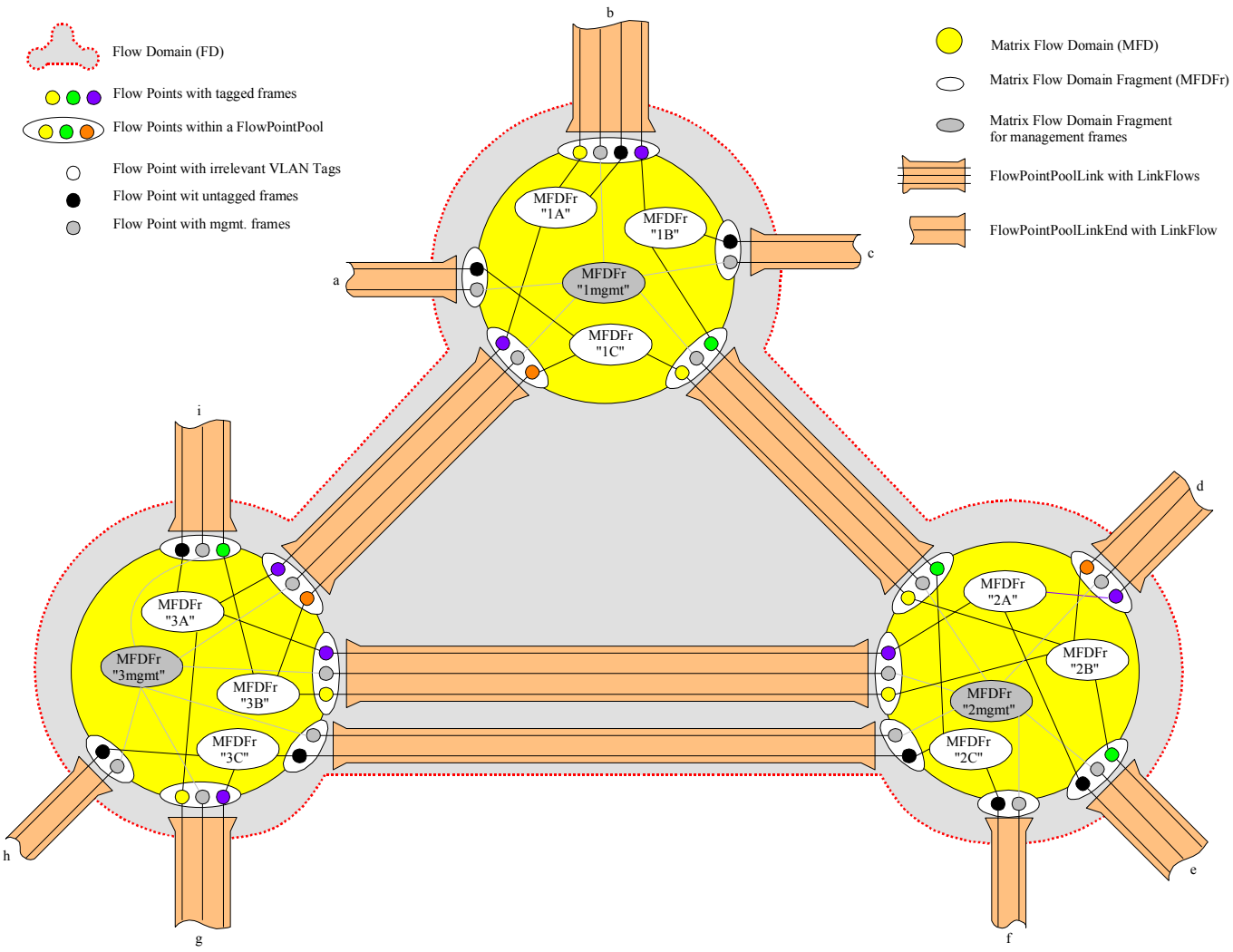


Figure 20: G.8010 resources of the Ethernet Layer Network Domain

Appendix II Modelling of Bridges

This appendix clarifies how the model works out in practice to represent the various types of Ethernet bridges that have been standardised by the IEEE (and that are also analysed in ITU-T G.8010): VLAN-unaware bridges (IEEE 802.1D), …. (.1Q), (.1ad).

II.1 Rationale

The existing mTOP/Ethernet document set explains in general how Ethernet bridges are modelled, using the terminology of ITU-T connectionless networks (e.g., flow domains). But it does not specify how exactly this representation applies to the various types of bridges described in IEEE standards. This appendix aims to clarify these questions.

II.2 Summary

Frame mapping and tag translation are represented by tables both in CPTP and FP.

Frame mapping consists in filtering input frames, and performing various operations on them according to their content.

The main inputs are:

- The contents of the incoming tag (if applicable): VLAN ID and priority.
- The port of entry (however, this does not appear as such in the model since the tables are themselves properties of CPTPs and FPs; objects themselves correspond to IEEE ports.).
- Other parameters may be used.

The main outputs are:

- the traffic class and TC profile.

Tag translation consists in replacing an existing tag VID by another one.

II.3 Representation of VLAN-Unaware bridge (IEEE 802.1D)

II.3.1 What happens in the Bridge

The bridge collaborates with other bridges in the network (via spanning tree protocol, or by other means such as fixed provisioning) to form a spanning tree, so that frames do not go round and round in loops. (This is implemented by “switching off” some of the ports in the bridges; Spanning Tree Protocol maintains the port states dynamically so as to preserve connectivity in spite of network evolution and faults).

No processing of VLAN tags is performed.

Routing of frames does not depend on their user priority. However, the bridge performs classification according to priority and may regenerate priority.

In IEEE 802.1D, section 7.7.1 describes the selection of transmission (egress) ports, i.e, routing. The following is an integral quote of the section; note that priority does not feature in the selection criteria:
Each Port is selected as a potential transmission Port if, and only if

a) The Port on which the frame was received was in a forwarding state (8.4), and
b) The Port considered for transmission is in a forwarding state, and
c) The Port considered for transmission is not the same as the Port on which the frame was received, and

d) The size of the mac-service-data-unit conveyed by the frame does not exceed the maximum size of mac-service-data-unit supported by the LAN to which the Port considered for transmission is attached.

II.3.2 For each Port not selected as a potential transmission Port, the frame shall be discarded.What happens in the model

- Tag translation: not applicable.
- Frame mapping: Yes. Priority is an input.
- Flow Point identification: by default. There is only 1 FP per CPTP for user traffic. An additional FP may be instantiated to represent management frames.
- Salient feature: port state (for Spanning Tree Protocol).

II.4 Representation of VLAN-aware bridge (IEEE 802.1Q and P802.1ad)

II.4.1 What happens in the Bridge

The idea of the Virtual LAN is to separate out the traffic flows belonging to different users, without the expense of maintaining multiple physical infrastructures. This is implemented by an additional field called the “VLAN tag” in the user frames (the bridge may add or remove tags, or it may merely make use of tags that are already present in the frames). Conceptually, the VLAN aware bridge is envisaged as a superposition of VLAN-unaware bridges, in which each separate “virtual” bridge has its own behaviour (e.g., its own instance of spanning tree protocol => its own port states).

There are two particular kinds of VLAN-aware bridges (described in IEEE P802.1ad [14]): Customer Bridge and Provider Bridge. See section II.5 and section II.6 respectively.

II.4.2 What happens in the model

This is the generic case – the bridge may be either C-TAG aware or S-TAG aware.

- Tag translation in CPTP: Optional
- Frame mapping in CPTP: no
- Tag translation in FP: no
    - See remarks for Provider Bridge
- Frame mapping in FP: yes
- Flow Point identification: The flow point is identified by the C-VID or S-VID value that it recognises (C-VID for a customer bridge, S-VID for a provider bridge). This value is also present in the Frame Mapping Table.

Comments:

- In the case of a singleton representation, or when there is no VID swapping in the Flow Domain, the VID can be used to identify both the FDFr itself and its connected FPs.

II.5 Representation of Customer Bridge (IEEE P802.1ad)

II.5.1 What happens in the Bridge

Customer bridges are characterised by the following properties:

- They recognise only C-TAG format, not S-TAG format (the two differ by their Ethertype; that is the value of the TPID field in the tag.)
- They do not perform tag translation (on the VID part of the tag).

II.5.2 What happens in the model

- Tag translation in CPTP: No (by definition)
- Frame mapping in CPTP: no
- Tag translation in FP: No (by definition)
- Frame mapping in FP: yes
- Note: Customer bridges can route according to C-TAG, and we model this by tables at the FP

II.6 Representation of Provider bridge

II.6.1 What happens in the Bridge

Provider bridges are characterised by the following properties:

- They recognise only S-TAG format, not C-TAG (see above Customer Bridge)
- They can perform tag translation (on the VID part of the tag) through a VLAN translation table on each port.

II.6.2 What happens in the model

The following combinations of tables are used:

Case 1: Translation followed by mapping:

- Tag translation in CPTP: yes
- Frame mapping in CPTP: no
- Tag translation in FP:no
- Frame mapping in FP: yes

Case 2: No translation, just mapping:

- Tag translation in CPTP: no
- Frame mapping in CPTP: no
- Tag translation in FP: no
- Frame mapping in FP: yes
- Note: The frame mapping table may be trivial (same treatment for all frames).

II.7 Representation of “double VLAN-aware” bridge

II.7.1 Usage

This case may arise either because there is a bridge that behaves in exactly this way (which is not described in IEEE 802.1Q or P802.1ad), or because for practical reasons the target OS provider chooses to concatenate the representation of several bridges into a single bridge[2].

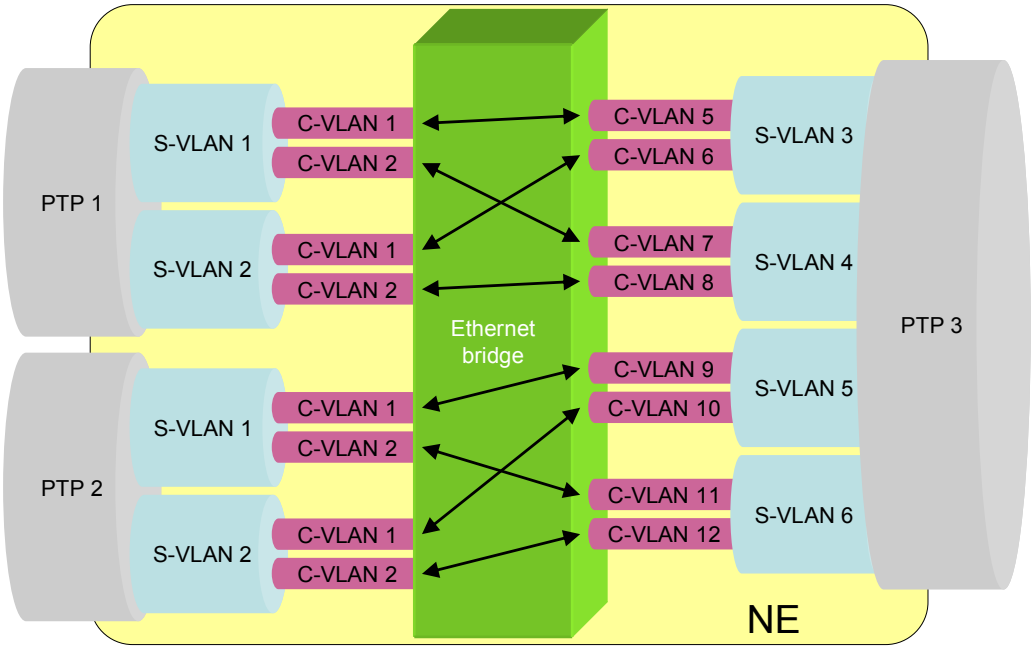


Figure 21: "double VLAN-aware" bridge

II.7.2 What happens in the Bridge

Whereas bridges conformant to IEEE 802.1Q or P802.1ad process only a single VLAN tag – either the C-VLAN or the S-VLAN tag – this new kind of bridge processes BOTH tags simultaneously.

This is modelled in the Frame Mapping Table by including input parameters from both kinds of VLAN tag:

- C-VID
- S-VID
- Priority

Note: The Traffic Mapping Table may be some 4000 times larger!

Note: It is theoretically possible for the bridge to discriminate between the priority field in the C-VLAN tag, and the same field in the S-VLAN tag. However, this does not seem to be required in practice.

II.7.3 What happens in the model

- Tag translation in CPTP: Optional
- Frame mapping in CPTP: no

[2] Typically, this will be done so as to have only one bridge per managed element, just as in MTNM release 3.0 there is only one connection-oriented "fabric" or connection matrix per managed element (which is not represented in the model by a separate object).

- Tag translation in FP: no
  - See remarks for Provider Bridge
- Frame mapping in FP: yes
  - The mapping table uses multiple VLAN Ids (see above).
- Flow Point identification: The flow point is identified by the combination of S-VID and C-VID.

Comments:

- This is the same model as the previous VLAN aware bridges: the only difference is in the greater complexity of the Traffic Mapping Table and the difference in flow point naming.

Appendix III MEF Mapping

The table in this appendix provides a mapping between the information model presented in MEF 7 [11], the Metro Ethernet Forum's EMS-NMS Information Model, and the mTOP Interface Connectionless Network Model.

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
ETH_Flow_Domain			**FlowDomain**		
ETH_Flow_Domain	attribute	userLabel	FlowDomain	userLabel	
ETH_Flow_Domain	operation	setupPtToPtETH_FDFr_EVCWithFPPs	FlowDomain	createFDFr	
ETH_Flow_Domain	operation	setupMultiToMultiETH_FDFr_EVCwithFPPs	FlowDomain	createFDFr	
ETH_Flow_Domain	operation	releaseETH_FDFr_EVC	FlowDomain	deleteFDFr	
ETH_FPP			**CPTP, PTP, FTP**		
ETH_FPP	attribute	fPP_FPPType	CPTP (TP) PTP, FTP	InterfaceType	
ETH_FPP	attribute	availableCapacity	CPTP (TP)	Layered Parameters: AvailableCapacity	
ETH_FPP	attribute	userLabel	CPTP (TP)	userLabel	
ETH_FPP	attribute	physAddress	CPTP (TP)	Layered Parameters: PhysAddress	
ETH_FPP	attribute	operState	CPTP (TP)	Layered Parameters: ServiceState	
ETH_FPP	attribute	availabilityStatus	CPTP (TP)	additionalInfo: "X.721::AvailabilityStatus"	
ETH_FPP	attribute	adminState	CPTP (TP)	Layered Parameters: ServiceState	
ETH_FPP	attribute	ingressMaxAssignableBW	CPTP (TP)	Layered Parameters: IngressMaxAssignableBW	

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
ETH_FPP	attribute	egressMaxAssignableBW	CPTP (TP)	Layered Parameters: EgressMaxAssignableBW	
ETH_FPP	attribute	maxNumEVCs	CPTP	Layered Parameters: MaxNumFDFrs	
ETH_FPP	attribute	numConfiguredEVCs		Layered Parameters: NumConfiguredFDFrs	
ETH_FPP_UNI			**CPTP**		
ETH_FPP_UNI	attribute	uniIdentifier	CPTP (TP)	CPTP Name	
ETH_FPP_UNI	attribute	layer2ControlProtocolProcessingList	CPTP (TP)	Layered Parameters: Layer2ControlProtocolProcessingList	
ETH_FPP_UNI	attribute	serviceMuxingIndicator	CPTP (TP)	Layered Parameters: ServiceMuxingIndicator	
ETH_FPP_UNI	attribute	bundlingIndicator	CPTP (TP)	Layered Parameters: BundlingIndicator	
ETH_FPP_UNI	attribute	allToOneIndicator	CPTP (TP)	Layered Parameters: AllToOneIndicator	
ETH_FPP_UNI	attribute	untaggedVLANAssignment	CPTP (TP)	Layered Parameters: PVID	
ETH_FPP_UNI	attribute	unassignedCeVlanIDList	CPTP (TP)		This optional attribute is not mapped
ETH_Link			**EncapsulationLayerLink**		
ETH_Link	attribute	availableCapacity	CPTP	Layered Parameters: AvailableCapacity	Reflected on FPP (CPTP)

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
ETH_Link	attribute	userLabel	EncapsulationLayerLink	userLabel	
ETH_Link	attribute	usageCost	CPTP	Layered Parameters: LinkUsageCost	Reflected on FPP (CPTP)
ETH_FDFr_EVC			**FlowDomainFragment**		
ETH_FDFr_EVC	attribute	adminState	FlowDomainFragment	Layered Parameters: ServiceState	
ETH_FDFr_EVC	attribute	operState	FlowDomainFragment	Layered Parameters: ServiceState	
ETH_FDFr_EVC	attribute	availabilityStatus	FlowDomainFragment	additionalInfo: "X.721::AvailabilityStatus	
ETH_FDFr_EVC	attribute	eVCProtected	FlowDomainFragment	staticProtectionLevel	
ETH_FDFr_EVC	attribute	userLabel	FlowDomainFragment	userLabel	
ETH_FDFr_EVC	attribute	eVCType	FlowDomainFragment	fDFrType	New attribute (e.g., Point-to-Point; E-Tree; Multi-Point)
ETH_FDFr_EVC	attribute	ethEVCID	FlowDomainFragment	userLabel	EVC ID may be included in the userLabel

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
ETH_FDFr_EVC	attribute	uniCeVlanIdPreservation	FlowDomainFragment	Layered Parameters: VLANIdPreservation	
ETH_FDFr_EVC	attribute	uniCeVlanCosPreservation	FlowDomainFragment	Layered Parameters: VLANPriorityPreservation	
ETH_FDFr_EVC	operation	performEVCTrace			Perform EVC Trace operation not mapped
ETH_FDFr_EVC	operation	addTPsToMultiETH_FDFr_EVCwithFPPs	FlowDomain	addFPsToFDFr	
ETH_FDFr_EVC	operation	removeTPsFromMultiETH_FDFr_EVC	FlowDomain	removeFPsFromFDFr	
ETH_Flow_Point			**FP / CTP**		
ETH_Flow_Point	attribute	operState	CTP (TP)	Layered Parameters: ServiceState	
ETH_Flow_Point	attribute	alarmStatus	CTP (TP)	additionalInfo: "M.3100::AlarmStatus"	
ETH_Flow_Point	attribute	currentProblemList	CTP (TP)	Get Active Alarms	OPEN ISSUE
ETH_Flow_Point	attribute	ethCeVlanIDList	CTP (TP)	Layered Parameters: TrafficMappingFrom_Table_VID	The Traffic Mapping Table maps CE VLAN IDs to FDFrs.
ETH_Flow_Point	attribute	ethUNIEVCID	CTP (TP)	userLabel	
ETH_Flow_Point	attribute	layer2ControlProtocolDispositionList	CTP (TP)	Layered Parameters: Layer2ControlProtocolDispositionList	

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
ETH_Flow_Point	attribute	unicastServiceFrameDelivery	CTP (TP)	Layered Parameters: UnicastServiceFrameDelivery	
ETH_Flow_Point	attribute	multicastServiceFrameDelivery	CTP (TP)	Layered Parameters: MulticastServiceFrameDelivery	
ETH_Flow_Point	attribute	broadcastServiceFrameDelivery	CTP (TP)	Layered Parameters: BroadcastServiceFrameDelivery	
ETH_Flow_Point	attribute	trailTerminating	CTP (TP)	tpMappingMode	
ETH_Flow_Point	attribute	adminState	CTP (TP)	Layered Parameters: ServiceState	
ETHBandwidthProfile (TrafficConditioner)			**TC Profile**		
ETHBandwidthProfile	attribute	bwCategoryIdentifier	CPTP FP	userLabel	
ETHBandwidthProfile	attribute	cir	CPTP FP	Layered Parameters: IngressCIR	May be per COS
ETHBandwidthProfile	attribute	cbs	CPTP FP	Layered Parameters: IngressCBS	May be per COS
ETHBandwidthProfile	attribute	eir	CPTP FP	Layered Parameters: IngressEIR	May be per COS
ETHBandwidthProfile	attribute	ebs	CPTP FP	Layered Parameters: IngressEBS	May be per COS
ETHBandwidthProfile	attribute	colorMode	CPTP FP	Layered Parameters: IngressColorMode	May be per COS
ETHBandwidthProfile	attribute	couplingFlag	CPTP FP	Layered Parameters: IngressCouplingFlag	May be per COS
ETHCosProfile			**CPTP FP**	**ingressCoSMapping**	

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
ETHCosProfile	attribute	cosIdentifier			Indicated on the individual parameters
ETHCosProfile	attribute	cosDelay	CPTP FP	Layered Parameters: Delay	Per COS
ETHCosProfile	attribute	cosJitter	CPTP FP	Layered Parameters: Jitter	Per COS
ETHCosProfile	attribute	cosLoss	CPTP FP	Layered Parameters: Loss	Per COS
TransportPort			**PhysicalTerminationPoint**		
TransportPort	attribute	characteristicInformationType	TP	Layer Rate	
TransportPort	attribute	operState	PTP	Layered Parameters: ServiceState	
TransportPort	attribute	alarmStatus	PTP	additionalInfo: "M.3100::AlarmStatus"	
TransportPort	attribute	currentProblemList	PTP	Get Active Alarms	OPEN ISSUE
TransportPort	attribute	portID	PTP	Layered Parameters: Location	
TransportPort	attribute	potentialCapacity	PTP	Layered Parameters: PotentialCapacity	
MAUTransportPTP					
MAUTransportPTP	attribute-INH	characteristicInformationType	TP	Layer Rate	
MAUTransportPTP	attribute-INH	operState	PTP	Layered Parameters: ServiceState	
MAUTransportPTP	attribute-INH	alarmStatus	PTP	additionalInfo: "M.3100::AlarmStatus"	

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
MAUTransportPTP	attribute-INH	currentProblemList	PTP	Get Active Alarms	OPEN ISSUE
MAUTransportPTP	attribute-INH	portID	PTP	Location	
MAUTransportPTP	attribute-INH	potentialCapacity	PTP	Layered Parameters: PotentialCapacity	
MAUTransportPTP	attribute	mauType	PTP	Layered Parameters: MauType	
MAUTransportPTP	attribute	mauStatus	PTP	Layered Parameters: MauStatus	
MAUTransportPTP	attribute	mauMediaAvailable	PTP	Layered Parameters: MauMediaAvailable	
MAUTransportPTP	attribute	mauJabberState	PTP	Layered Parameters: MauJabberState	
MAUTransportPTP	attribute	mauDefaultType	PTP	Layered Parameters: MauDefaultType	
MAUTransportPTP	attribute	mode	PTP	Layered Parameters: DuplexMode	
MAUTransportPTP	attribute	mauAutoNegSupported	PTP	Layered Parameters: AutoNegotiation	
MAUTransportPTP	attribute	mauTypeList	PTP	Layered Parameters: MauTypeList	
MAUTransportPTP	attribute	mauJackTypeList	PTP	Layered Parameters: MauJackTypeList	
MAUTransportPTP	attribute	mauAutoNegAdminState	PTP	Layered Parameters: MauAutoNegAdminState	
MAUTransportPTP	attribute	mauAutoNegRemoteSignaling	PTP	Layered Parameters: MauAutoNegRemoteSignaling	
MAUTransportPTP	attribute	mauAutoNegConfig	PTP	Layered Parameters: MauAutoNegConfig	

MEF 7 Object	Type	MEF 7 Item	mTOP Interface Object	mTOP Interface Item	Note
MAUTransportPTP	attribute	mauAutoNegCapability	PTP	Layered Parameters: MauAutoNegCapability	
MAUTransportPTP	attribute	mauAutoNegCapAdvertised	PTP	Layered Parameters: MauAutoNegCapAdvertised	
MAUTransportPTP	attribute	mauAutoNegCapReceived	PTP	Layered Parameters: MauAutoNegCapReceived	
MAUTransportPTP	attribute	mauAutoNegRemoteFaultAdvertised	PTP	Layered Parameters: MauAutoNegRemoteFaultAdvertised	
MAUTransportPTP	attribute	mauAutoNegRemoteFaultReceived	PTP	Layered Parameters: MauAutoNegRemoteFaultReceived	
MAUTransportPTP	operation	mauAutoNegRestart			MAU Auto Negotiation Restart operation not mapped

Color Key

Not Mapped (gap)

Table 7: MEF – mTOP Interace Ethernet Mapping

10 Administrative Appendix

10.1 Document History

Version	Date Modified	Description of changes
1.0	October 2007	This is the first version of the document and as such, there are no changes to report.
1.1	November 2007	Editorial updates to make applicable to MTNM and MTOSI products. Added note in Call section to indicate that support is not provided in MTOSI release 2.0.
1.2	March 2013	• Editorial change due to the addition of Egress TC Profile • Added a second example in section 9.1 with Egress TC Profile • Added a comment in section 4.9

10.2 Acknowledgments

First Name	Last Name	Company

10.3 How to comment on this document

Comments and requests for information must be in written form and addressed to the contact identified below:

Keith Dorking Ciena

Phone: +1 678 867 5007

Fax: +1 678 867 5010

e-mail: kdorking@ciena.com

Please be specific, since your comments will be dealt with by the team evaluating numerous inputs and trying to produce a single text. Thus we appreciate significant specific input. We are looking for more

input than wordsmith" items, however editing and structural help are greatly appreciated where better clarity is the result.