International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.8011.4/Y.1307.4

(02/2010)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Packet over Transport aspects – Ethernet over Transport aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Transport

Ethernet virtual private rooted multipoint service

Recommendation ITU-T G.8011.4/Y.1307.4

ITU-T

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
Ethernet over Transport aspects	**G.8000–G.8099**
MPLS over Transport aspects	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
Service Management	G.8600–G.8699
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.8011.4/Y.1307.4

Ethernet virtual private rooted multipoint service

Summary

Recommendation ITU-T G.8011.4/Y.1307.4 defines the service attributes and parameters for carrying Ethernet characteristic information over shared bandwidth, rooted multipoint connections, provided by SDH, PDH, ATM, MPLS, OTH, ETY or ETH server layer networks. This type of service is referred to as Ethernet virtual private rooted multipoint service. This Recommendation is based on the Ethernet service framework as defined in Recommendation ITU-T G.8011/Y.1307.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.8011.4/Y.1307.4	2010-02-06	15

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T G.8011.4/Y.1307.4

Ethernet virtual private rooted multipoint service

1 Scope

This Recommendation defines the service attributes and parameters for carrying Ethernet characteristic information over shared-bandwidth, rooted multipoint connections, provided by SDH, ATM, MPLS, PDH, ETY, OTH or ETH server layer networks. This type of service is referred to as Ethernet virtual private rooted multipoint service (EVPRM). The initial focus of this Recommendation will be on uni-root and bi-root EVPRM. This Recommendation is based on the Ethernet service framework as defined in [ITU-T G.8011].

2 References

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

[ITU-T G.707] Recommendation ITU-T G.707/Y.1322 (2003), *Network node interface for the synchronous digital hierarchy (SDH)*.

[ITU-T G.709] Recommendation ITU-T G.709/Y.1331 (2001), *Interfaces for the Optical Transport Network (OTN)*.

[ITU-T G.7043] Recommendation ITU-T G.7043/Y.1343 (2004), *Virtual concatenation of plesiochronous digital hierarchy (PDH) signals*.

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[ITU-T G.809] Recommendation ITU-T G.809 (2003), *Functional architecture of connectionless layer networks*.

[ITU-T G.8001] Recommendation ITU-T G.8001/Y.1354 (2008), *Terms and definitions for Ethernet frames over Transport*.

[ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.

[ITU-T G.8011] Recommendation ITU-T G.8011/Y.1307 (2009), *Ethernet service characteristics*.

[ITU-T G.8011.1] Recommendation ITU-T G.8011.1/Y.1307.1 (2009), *Ethernet private line service*.

[ITU-T G.8011.2] Recommendation ITU-T G.8011.2/Y.1307.2 (2009), *Ethernet virtual private line service*.

[ITU-T G.8012] Recommendation ITU-T G.8012/Y.1308 (2004), *Ethernet UNI and Ethernet NNI*.

[ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2004), *Characteristics of Ethernet transport network equipment functional blocks*.

[ITU-T Y.1731] Recommendation ITU-T Y.1731 (2008), *OAM functions and mechanisms for Ethernet based networks*.

[IEEE 802.1AB] IEEE 802.1AB-2005, *IEEE Standard for Local and metropolitan area networks – Station and Media Access Control Connectivity Discovery*.

[IEEE 802.1ag] IEEE 802.1ag-2007, *IEEE Standard for Local and metropolitan area networks – Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management*.

[IEEE 802.1D] IEEE 802.1D-2004, *IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges*.

[IEEE 802.1Q] IEEE 802.1Q-2005, *IEEE standard for Local and metropolitan area networks – Virtual Bridged Local Area Networks*.

[IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control*.

[IEEE 802.3] IEEE 802.3-2008. *IEEE Standard for Information Technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*.

[IEEE 802.3ad] IEEE 802.3ad-2000, *Amendment to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications – Aggregation of Multiple Link Segments*.

[IEEE 802.3ah] IEEE 802.3ah-2004, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirement. Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*.

[MEF 6.1] The Metro Ethernet Forum MEF (2008), *Technical Specification MEF 6.1 – Ethernet Services Definitions-Phase 2*.

[MEF 10.1] The Metro Ethernet Forum MEF (2006), *Technical Specification MEF 10.1 – Ethernet Services Attributes-Phase 2*.

[MEF 16] The Metro Ethernet Forum MEF (2006), *Technical Specification MEF 16 – Ethernet Local Management Interface (E-LMI)*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined in [ITU-T G.8001]:

3.1.1 traffic conditioning function

This Recommendation uses the following terms defined in [ITU-T G.8010]:

3.1.2 ETH link

3.1.3 flow domain fragment (FDFr)

This Recommendation uses the following terms defined in [ITU-T G.8011] and [MEF 10.1]:

3.1.4 all-to-one bundling

3.1.5 bundling

3.1.6 CE-VLAN CoS

3.1.7 CE-VLAN ID

3.1.8 CE-VLAN ID preservation

3.1.9 CE-VLAN ID/EVC map

3.1.10 CE-VLAN tag

3.1.11 class of service (CoS)

3.1.12 class of service identifier

3.1.13 colour mode (CM)

3.1.14 committed burst size (CBS)

3.1.15 committed information rate (CIR)

3.1.16 coupling flag (CF)

3.1.17 customer edge (CE)

3.1.18 customer edge VLAN CoS

3.1.19 customer edge VLAN ID

3.1.20 customer edge VLAN tag

3.1.21 excess burst size (EBS)

3.1.22 egress bandwidth profile

3.1.23 excess information rate (EIR)

3.1.24 Ethernet virtual connection (EVC)

3.1.25 EVC maximum transmission unit size

3.1.26 ingress bandwidth profile

3.1.27 ingress service frame

3.1.28 Layer 2 control protocol service frame

3.1.29 Layer 2 control protocol tunnelling

3.1.30 maximum number of UNIs (MNU)

3.1.31 multipoint-to-multipoint EVC

3.1.32 point-to-point EVC

3.1.33 rooted-multipoint EVC

3.1.34 service multiplexing

3.1.35 service provider

3.1.36 subscriber

3.1.37 UNI maximum transmission unit (MTU) size

3.1.38 user network interface (UNI)

This Recommendation uses the following terms defined in [ITU-T G.809]:

3.1.39 flow domain

3.1.40 flow domain flow

3.1.41 flow point

3.1.42 flow termination

3.1.43 link flow

3.1.44 network flow

3.1.45 termination flow point

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Ethernet private rooted multipoint service: A rooted multipoint Ethernet virtual connection (EVC) for which several UNIs are attached over a dedicated server layer to a common UNI is defined as a private rooted multipoint service.

3.2.2 Ethernet virtual private rooted multipoint service: A rooted multipoint Ethernet virtual connection (EVC) for which several UNIs are attached (often with multiplexed access) over a dedicated or shared server layer (often over shared server layer) to a common UNI is defined as a virtual private rooted multipoint service.

3.2.3 EVPRM type 1: EVPRM type 1 is a rooted multipoint service over multiplexed access (root or leaf) and a dedicated server layer.

3.2.4 EVPRM type 2: EVPRM type 2 is a rooted multipoint service over a shared server layer.

3.2.5 EVPRM type 3: EVPRM type 3 is a rooted multipoint service over multiplexed access (root or leaf) and a shared server layer.

4 Acronyms and abbreviations

This Recommendation uses the following abbreviations:

APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
CBR	Constant Bit Rate
CBS	Committed Burst Size
CCM	Continuity Check Message
CE	Customer Edge
CF	Coupling Flag
CFM	Connectivity Fault Management
CI	Characteristic Information
CIR	Committed Information Rate
CM	Colour Mode
DA	Destination Address
DM	Delay Measurement
DMM	Delay Measurement Management

DMR	Delay Measurement Reply
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
EC	Ethernet Connection
EFM	Ethernet in the First Mile
EIR	Excess Information Rate
E-LMI	Ethernet Local Management Interface
ETH	Ethernet MAC layer network
ETH_C	Ethernet Connection (function)
ETH_CI	Ethernet MAC Characteristic Information
ETY	Ethernet PHY layer network
EVC	Ethernet Virtual Connection
EVPRM	Ethernet Virtual Private Rooted Multipoint Service
EVPT	Ethernet Virtual Private Tree
FCS	Frame Check Sequence
FD	Flow Domain
FDFr	Flow Domain Fragment
GFP	Generic Framing Procedure
LACP	Link Aggregation Control Protocol
LBM	Loopback Message
LCAS	Link Capacity Adjustment Scheme
LM	Less Measurement
LTM	Link Trace Message
MAC	Media Access Control
MEF	Metro Ethernet Forum
MEG	Maintenance Entity Group
MEN	Metro Ethernet Network
MEP	MEG End Point
MIP	MEG Intermediate Point
MPLS	Multi-Protocol Label Switching
MTU	Maximum Transmission Unit
NNI	Network-to-Network Interface
OAM	Operation, Administration, Maintenance
OTH	Optical Transport Hierarchy
OTN	Optical Transport Network
PA	(Ethernet) Preamble
PDH	Plesiochronous Digital Hierarchy

PHY	Physical device
SA	Source Address
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SFD	Start of Frame Delimiter
SNCP	Subnetwork Connection Protection
STP	Spanning Tree Protocol
TNE	Transport Network Equipment
UNI	User Network Interface
UNI-C	Customer side of UNI
UNI-N	Network side of UNI

5 Conventions

In this Recommendation, the term EC/EVC stands for "Ethernet Virtual Connection" in MEF and "Ethernet Connection" in ITU-T, with the same meaning.

EVPRM service is equivalent to EVP-Tree service defined in MEF.

6 Ethernet virtual private rooted multipoint (EVPRM) service

6.1 Description

A rooted-multipoint EVC is one for which each UNI is designated either as root or leaf. Ingress service frames at a root UNI can be delivered to one or more of any of the leaf UNIs in the EVC. Ingress service frames at a leaf UNI can only be delivered to one or more root UNIs in the EVC.

The EVPRM service achieves service multiplexing by using either a shared server layer or rooted multipoint EVCs. In the latter case service multiplexing MAY occur at none, one or more than one of the UNIs of the EVC.

The Ethernet virtual private rooted multipoint service with only one root (i.e., uni-root) is illustrated in Figure 6-1.

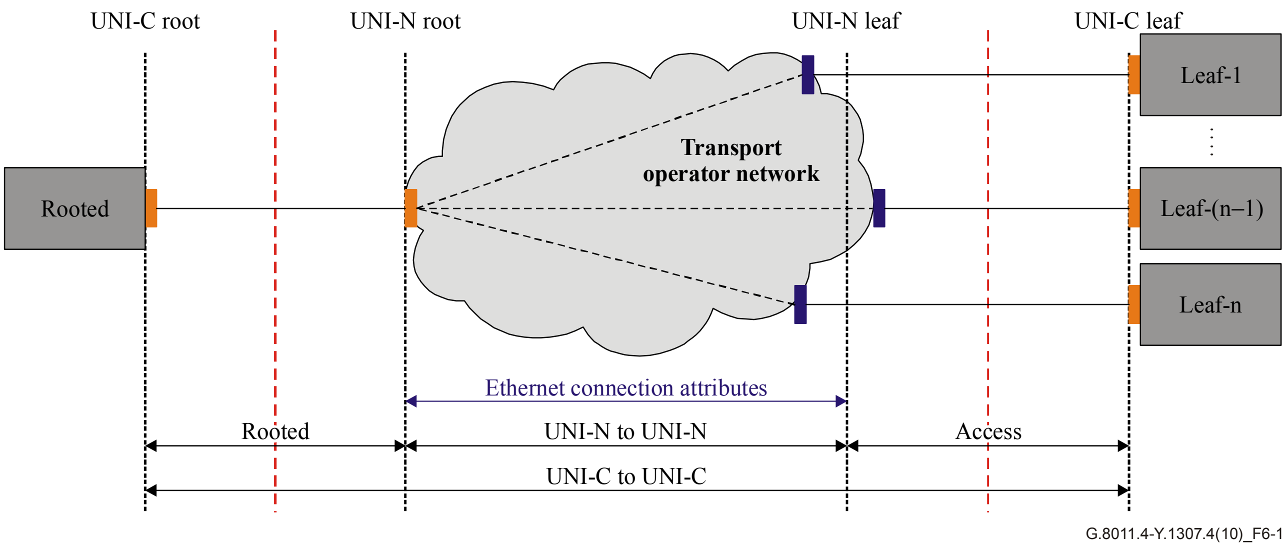

Figure 6-1 – Uni-root EVPRM service model

In its simplest form, an EVPRM service type can provide a single root for multileaf UNIs. Each leaf UNI can exchange data only with the root UNI. Service frames sent from one leaf UNI to the destination address of another leaf UNI in the same tree will be dropped by the network. Additionally, class of service (CoS) markings are usually available in the service.

In more sophisticated forms, an EVPRM service type may support two root (i.e, bi-root) UNIs. In this scenario, each leaf UNI can exchange data with one or more of the root UNIs. The roots can also communicate with each other. In such a service, redundant access to 'the root' can also be provided, effectively allowing for enhanced service reliability (i.e., protection) and load balancing. It should be noted that leaves would always behave as if there were a traditional unicast relationship from the leaf to the active root. There is no interaction among leaves, not even when they are redundantly attached to other roots; i.e., when they belong to multiple trees. This service is depicted in Figure 6-2.

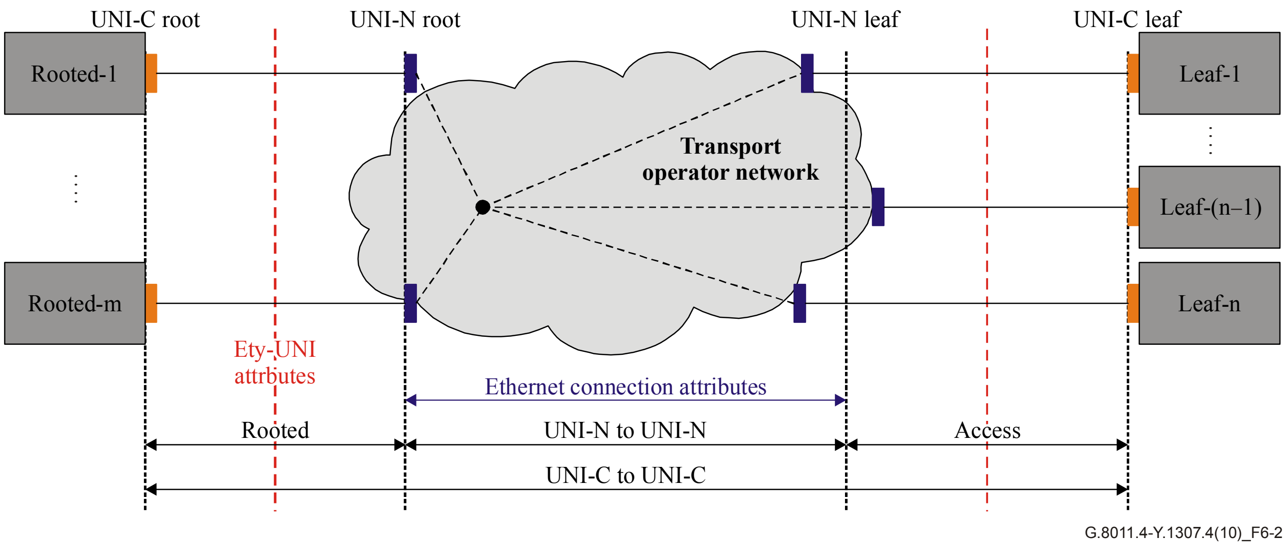

Figure 6-2 – Multi-root EVPRM service model

Load balancing and redundancy scenarios for multi-root EVPRM service, which is important, is for further study.

More sophisticated cases such as hierarchical or cascaded EVPRM service architectures are also for further study.

6.2 Ethernet virtual private rooted-multipoint service architecture

EVPRM service supports multiplexed access and uses either a dedicated or a shared server layer, which leads to the three types of EVPRM listed in Table 6-1:

Table 6-1 – EVPRM types

Type	Shared server layer	Multiplexed access
EVPRM Type 1	N	Y
EVPRM Type 2	Y	N
EVPRM Type 3	Y	Y

Appendix III describes use cases for each type.

6.2.1 EVPRM type 1

Figure 6-3 shows the basic architecture of the EVPRM type 1 service. The ETY layer is terminated at the rooted UNI-N and the multiplexed ETH frames are forwarded over single ETH_FPs to the dedicated server layer. The rooted UNI uses the VLAN tag for multiplexing at the demarcation point[1]. Multiplexed access (per clause 8.1.2 of [ITU-T G.8011]) is an Ethernet UNI attribute that indicates that multiple service instances exist across a single Ethernet UNI demarcation. Since this is the principal feature of the ingress of EVPRM type 1, it is also referred to as multiplexed access.

EVPRM type 1 can be further classified into the following three types, depending on whether multiplexing occurs at the root, the leaves or both:

– EVPRM type 1a: Dedicated server layer; multiplexed root access (see Figure 6-3a);

– EVPRM type 1b: Dedicated server layer; multiplexed leaf access (see Figure 6-3b);

– EVPRM type 1c: Dedicated server layer; multiplexed root and leaf access (see Figure 6-3c).

EVPRM type 1a is illustrated in Figure 6-3a below:

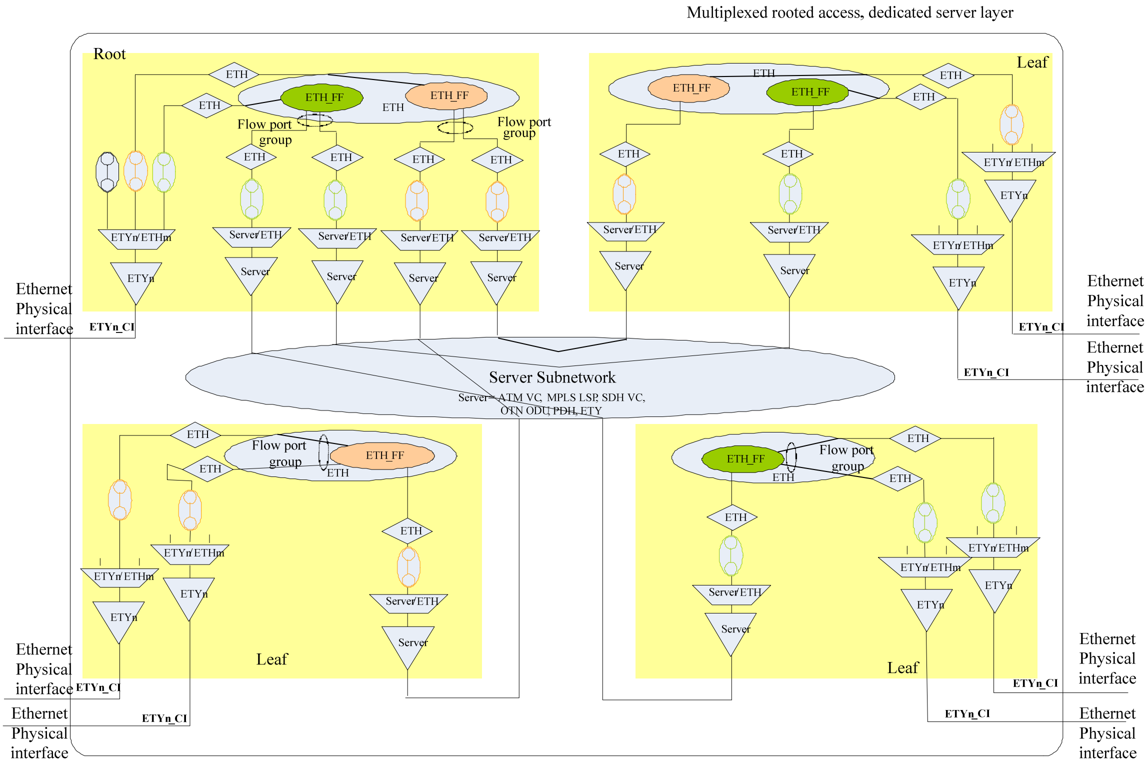

Figure 6-3a – EVPRM type 1a[2]

[1] Note that the choice of customer or provider VLAN tags depends on the agreement with the service provider.

[2] EVPRM can use asymmetric flow port grouping or VLANs. Only asymmetric flow port grouping is shown.

EVPRM type 1b is illustrated in Figure 6-3b below:

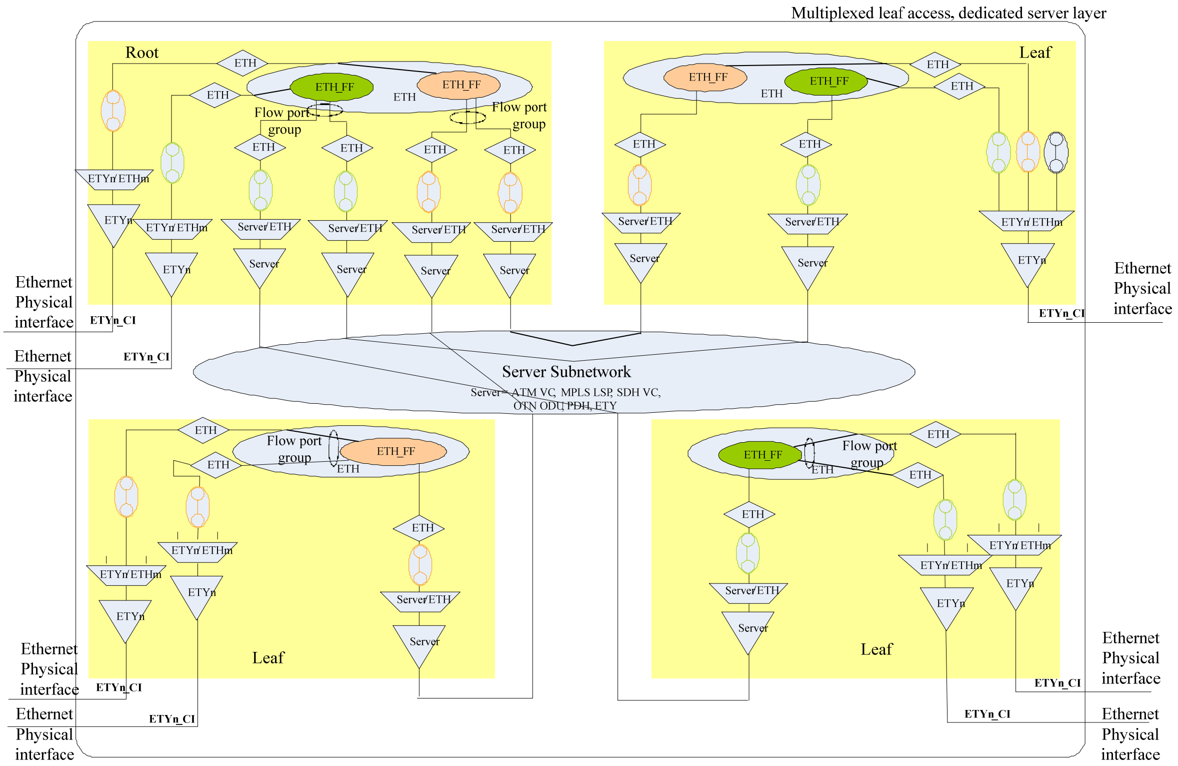

Figure 6-3b – EVPRM type 1b

EVPRM type 1c is illustrated in Figure 6-3c below:

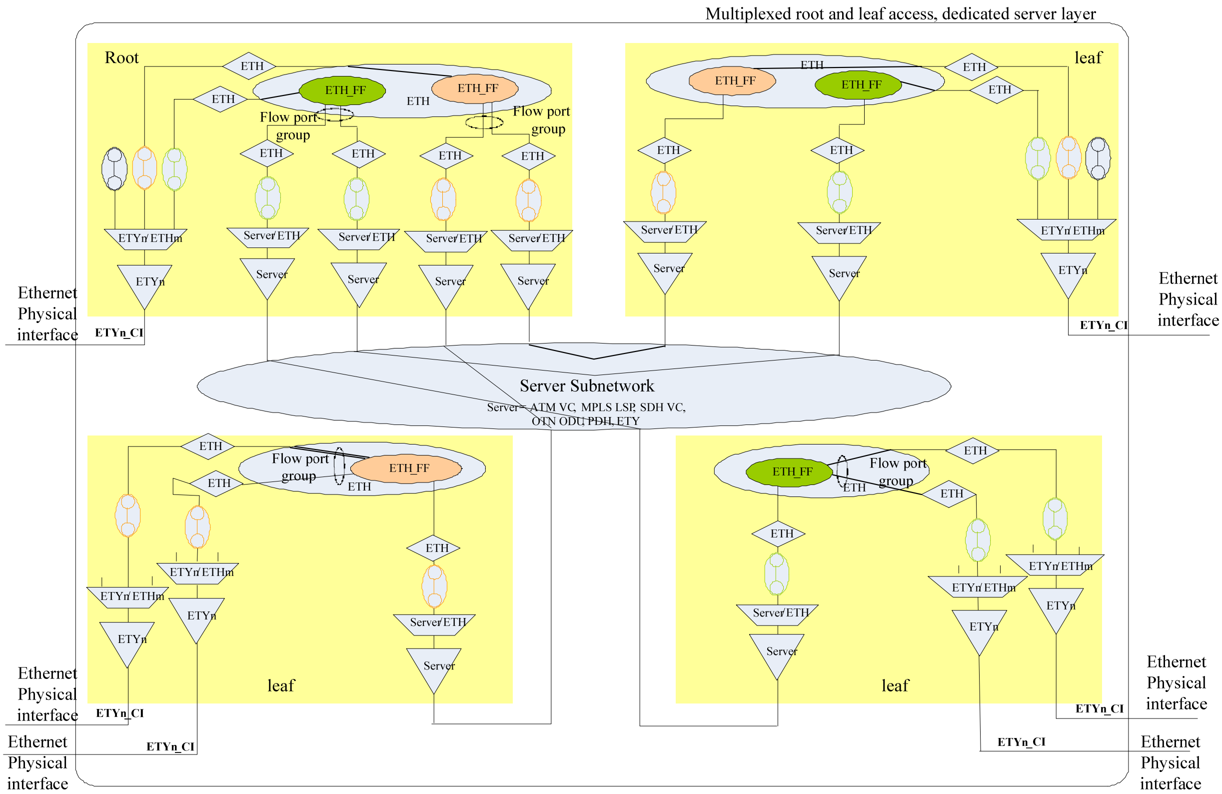

Figure 6-3c – EVPRM type 1c

6.2.2 EVPRM type 2

Figure 6-4 shows the basic architecture of the EVPRM type 2 service. Each service instance has dedicated access to the rooted UNI-N. The ETY layer is terminated at the rooted UNI-N and the ETH frames are forwarded over ETH_FPs to the shared server layer. A frame tag is associated with each frame in the server layer (i.e., logical separation) to perform the multiplexing. The tag is a service provider VLAN tag (S-VLAN).

EVPRM type 2 is illustrated in Figure 6-4 below:

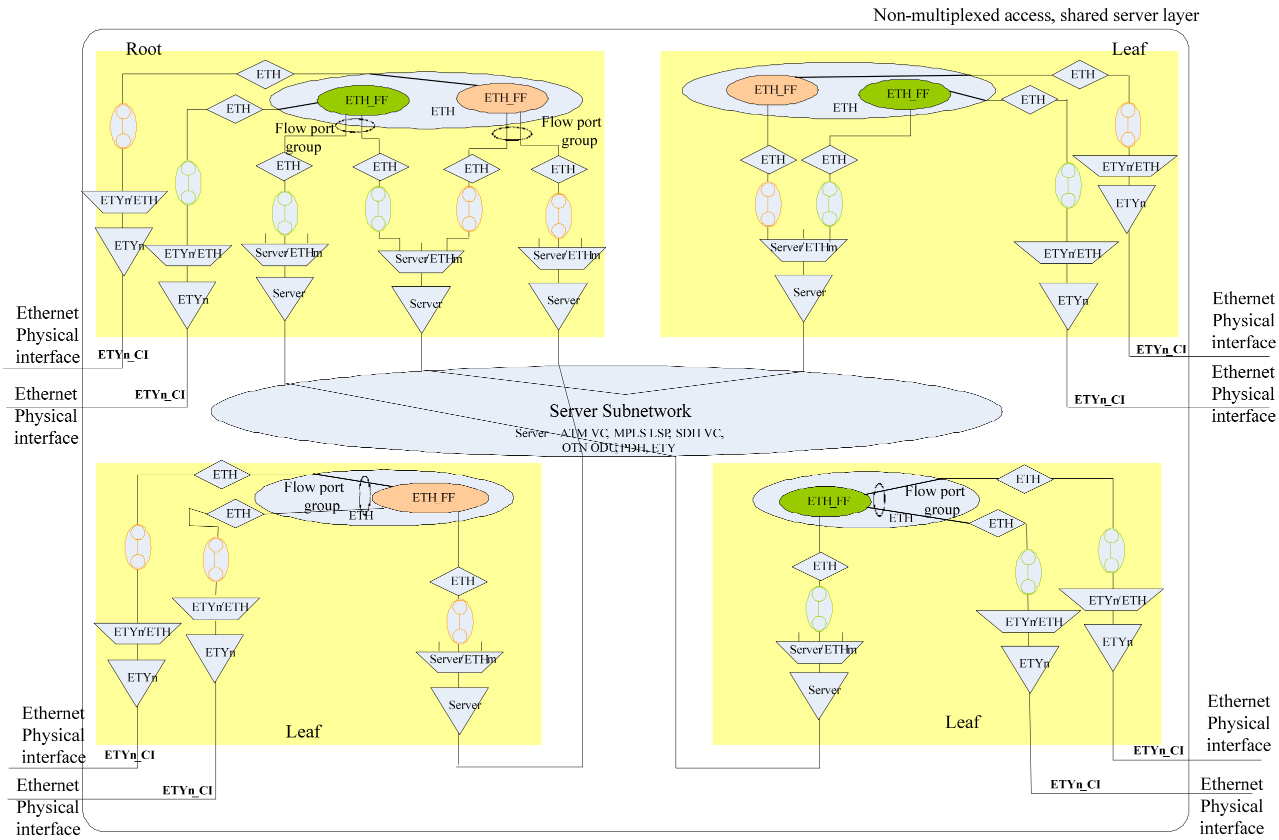

Figure 6-4 – EVPRM type 2

6.2.3 EVPRM type 3

Figure 6-5 shows the basic architecture of the EVPRM type 3 service. Each service instance is separated either logically or spatially at the rooted UNI-N (as shown in the figure). The ETY layer is terminated at the rooted UNI-N and the multiplexed ETH frames (i.e., logical separation) are forwarded over ETH_FPs to the shared server layer. In the combined multiplexing model, a frame tag is used for the multiplexing in the access network and in the server layer subnetwork. The access network may use VLAN tags and the server layer subnetwork may use VLAN tags (S-VLAN) or MPLS labels.

There are three types, depending on where multiplexation takes place.

EVPRM type 3a is illustrated in Figure 6-5a below:

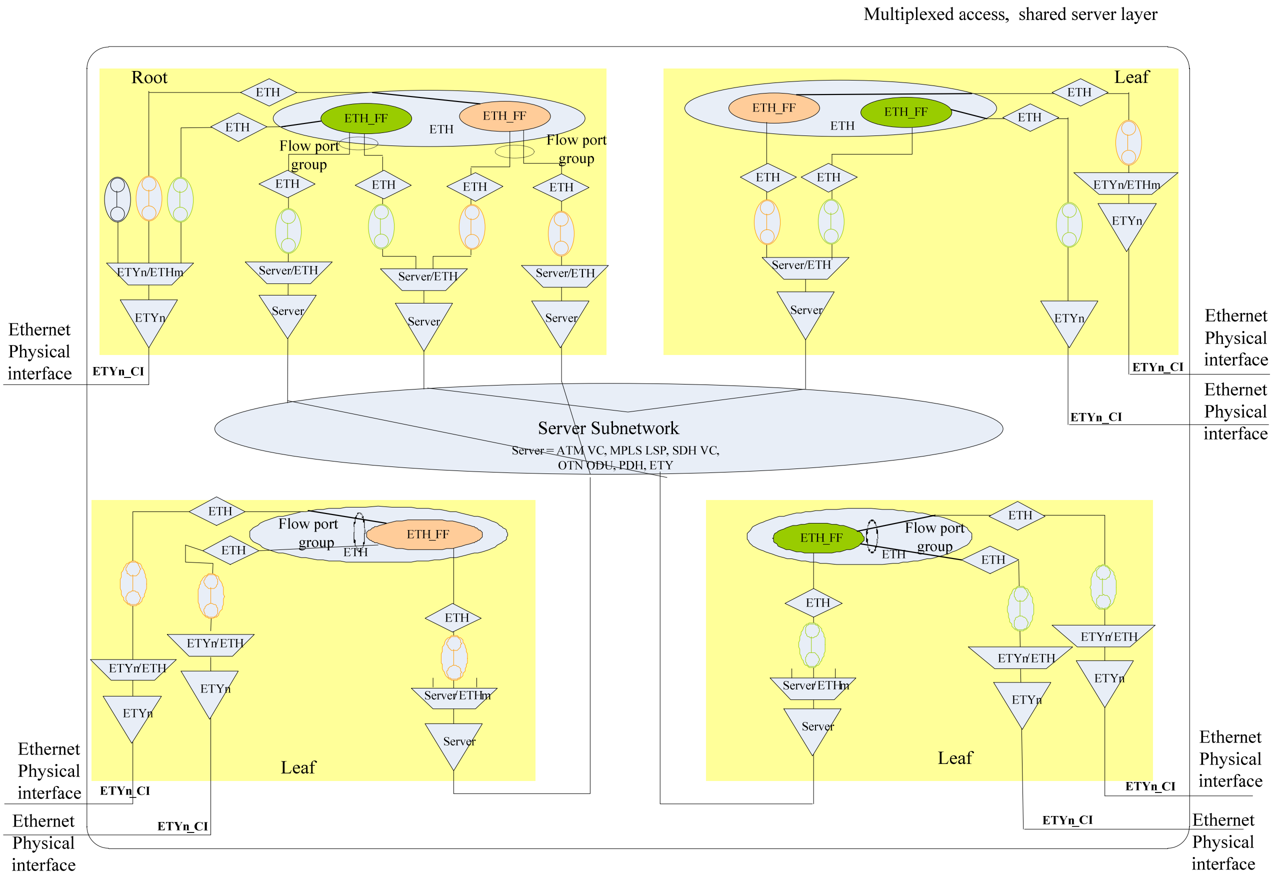

Figure 6-5a – EVPRM type 3a

EVPRM type 3b is illustrated in Figure 6-5b below:

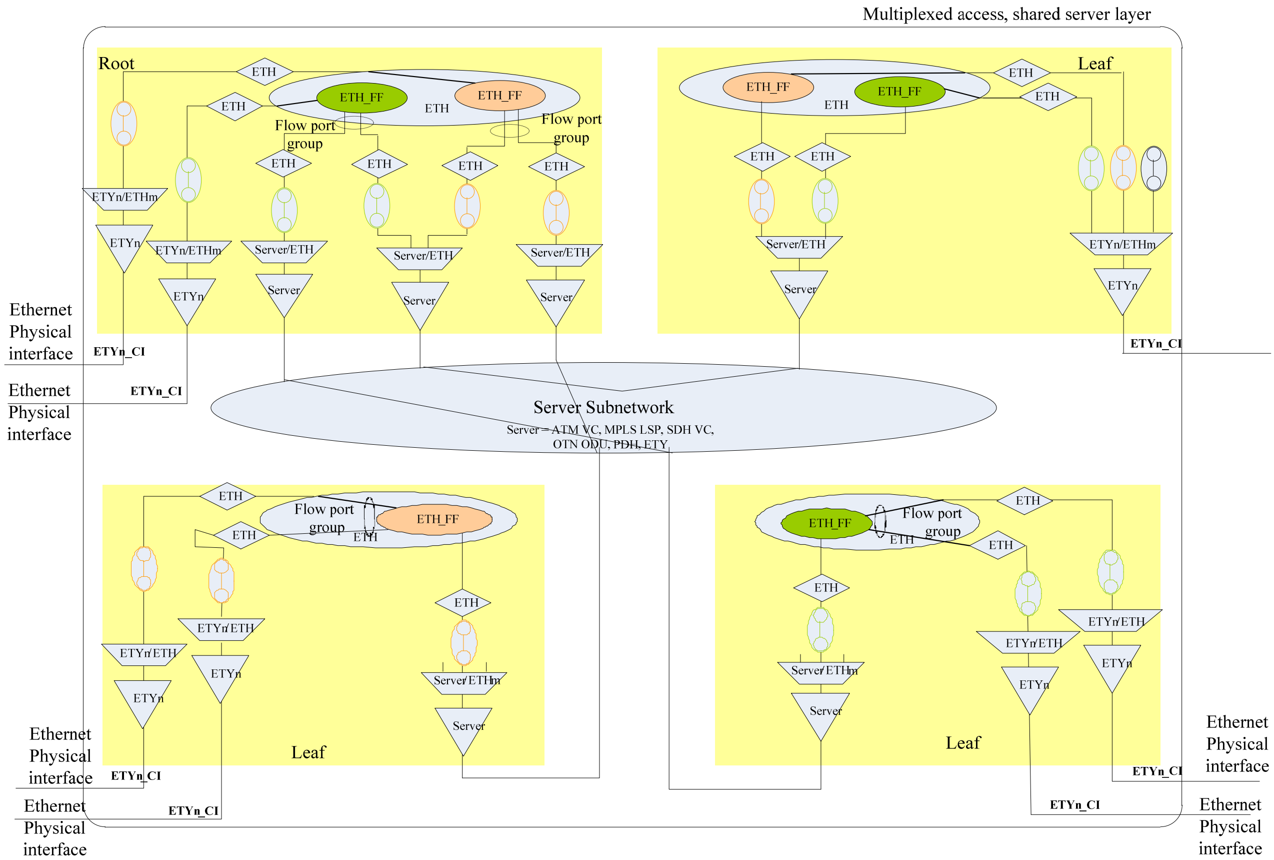

Figure 6-5b – EVPRM type 3b

EVPRM type 3c is illustrated in Figure 6-5c below:

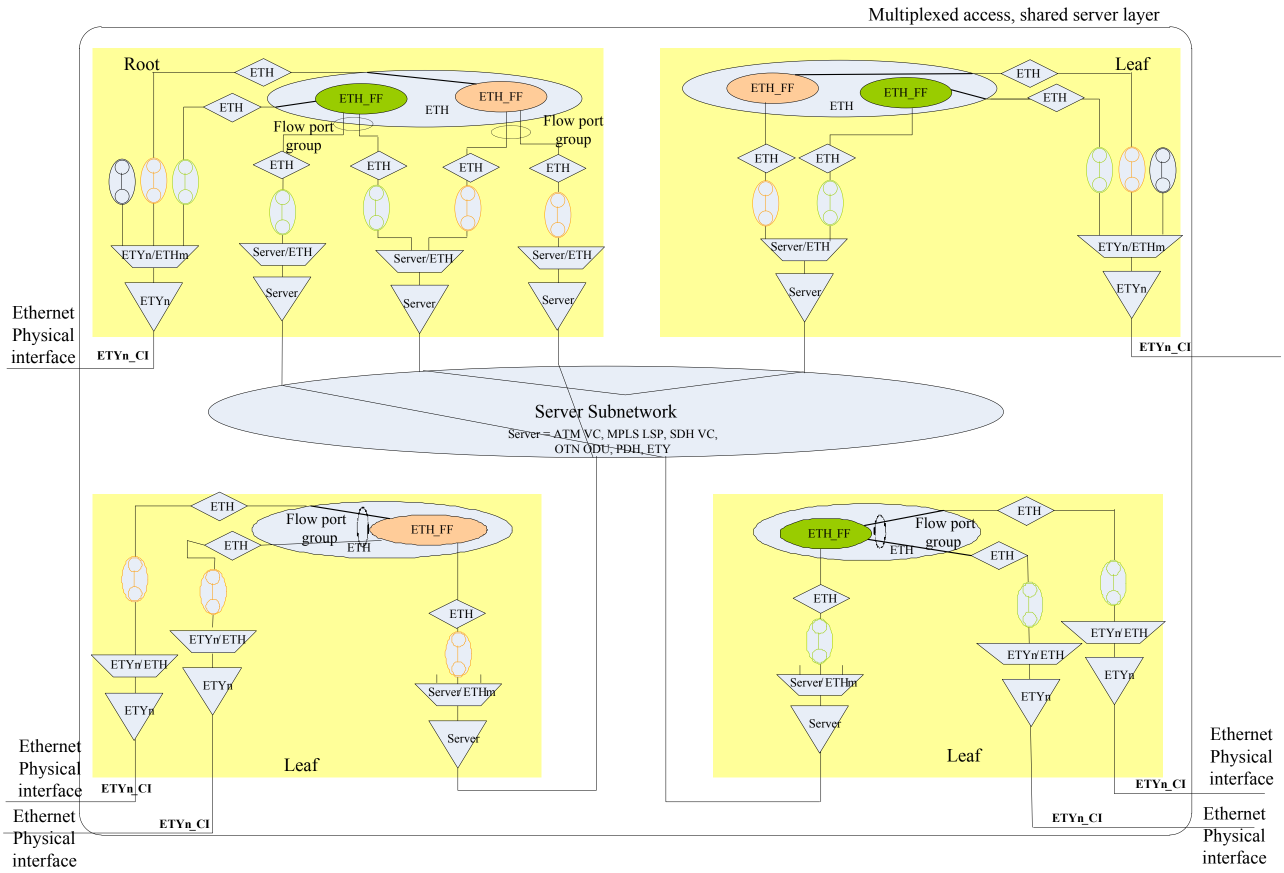

Figure 6-5c – EVPRM type 3c

7 Ethernet virtual connection (EVC) attributes for EVPRM

Table 7-1 provides the EVC service attributes, parameters, and values for the EVPRM service.

Table 7-1 – EVC service attributes and parameters for the EVPRM service

EVC service attribute	Service attribute parameters and values
EVC type	MUST be rooted-multipoint.
EVC ID	An arbitrary string, unique across the MEN, for the EVC supporting the service instance.
UNI list	MUST list the UNIs associated with the EVC. The UNI type for at least one UNI MUST be Root. The UNI type of Leaf MAY be used for any number of UNIs, it may be zero when leaf UNIs are being added or removed.
Maximum number of UNIs	MUST be ≥ 2 (An EVPRM service may have no leaves, for example, during times when leaf UNIs are being added or removed).
EVC maximum transmission unit size	Integer, MUST be ≤ 2000 and MUST be ≤ minimum of UNI MTU sizes.
CE-VLAN ID preservation	MUST be either Yes or No.
CE-VLAN CoS preservation	MUST be either Yes or No.
Unicast service frame delivery	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.

Table 7-1 – EVC service attributes and parameters for the EVPRM service

EVC service attribute	Service attribute parameters and values
Multicast service frame delivery	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Broadcast service frame delivery	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Layer 2 control protocols processing	For each protocol passed to the EC, MUST specify one of: Tunnel or Discard. MUST specify in accordance with clause 7.8.
EVC performance	MAY specify one or more CoS. For each CoS, MUST specify a CoS identifier and one or more sets of ordered UNI pairs. MAY specify a frame delay value, a frame delay variation value, a frame loss value, and an availability value for each set of ordered UNI pairs.
Ingress bandwidth profile per EVC	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other ingress bandwidth profile is applied at this UNI for this EVC.
Egress bandwidth profile per EVC	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other egress bandwidth profile is applied at this UNI for this EVC.
Link type	Dedicated, shared.
Traffic separation	Service instance: Spatial, logical. Customer: Spatial, logical.
Connectivity monitoring	Sub-layer monitoring: On demand and/or proactive. Inherent monitoring: Proactive.
Survivability	None, Ethernet protection or server specific.

7.1 EVC type

The connectivity of EVPRM is rooted multipoint.

7.2 EVC ID

An arbitrary string, unique across the domain, for EVCs supporting the service instance.

7.3 UNI list

The UNI list is an arbitrary string administered by the service provider, which is used to identify the UNIs connected to the EVC. It is intended for management and control purposes. There is at least one UNI for the root and any number of UNIs for leaves. The number of leaves may be zero. An EVPRM service may have no leaves, for example, when leaf UNIs are being added or removed.

7.4 Maximum number of UNIs

The number of UNIs should be more than two (but when the EVPRM service has no leaves, it should be one).

7.5 EVC maximum transmission unit size

The maximum MAC frame size supported at the UNI is at least 1522, as defined in clause 6.10 of [MEF 10.1], but not larger than 2000 (as specified in [IEEE 802.3]) and UNI MTU size.

7.6 Preservation (CE-VLAN ID/CoS preservation)

This attribute indicates the preservation of specific components of the ETH_CI provided by the ETH layer network that is used to transport the Ethernet service. Preservation means that the parameter value will be the same on ingress and egress to the EC. The two parameters are the ingress VLAN ID and class of service (priority) of the ETH_CI. Both can be preserved in EVPRM.

7.7 Service frame delivery

All Ethernet MAC data frames are transported regardless of their destination address, including unicast, multicast or broadcast.

For EVPRM types 1 and 3 with multiplexed access, the Ethernet MAC data frames may be conditionally transported based on their destination address and optionally based on the class of service (priority) of the ETH_CI.

7.8 Layer 2 control protocols

This attribute indicates which layer 2 control protocols will be tunnelled by the EVC and which will be discarded. The layer 2 control protocols are listed in Table 8-2. Only the tunnel and discard directives in the L2CP requirements are relevant for the EVC – irrespective of the UNI applicability.

7.9 Performance

This parameter indicates the overall performance such as frame delay performance, frame delay variation performance, frame loss ratio performance and availability performance; and associated class of service identifier(s) of the Ethernet virtual connection.

It MAY specify one or more CoS. For each CoS, MUST specify a CoS identifier and one or more sets of ordered UNI pairs. It MAY specify a frame delay value, a frame delay variation value, a frame loss value, and an availability value for each set of ordered UNI pairs.

7.10 Bandwidth profile

It is generally defined by the traffic parameters: CIR, CBS, EIR, EBS, CM and CF, per [MEF 6.1].

It is OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. It MUST NOT be allowed if any other egress bandwidth profile is applied at this UNI for this EVC.

An Ethernet flow that exceeds its committed rate will have its frames dropped or tagged with high drop precedence depending on the value of the EIR. Frames that exceed the flow EIR will be denied entry to the network and will be dropped at the access. Frames that exceed the flow CIR but are within its EIR will be marked with high drop precedence. Frames with high drop precedence will be dropped first when the network encounters congestion.

The function of the traffic conditioner includes frame metering and marking. The metering function is responsible for ensuring flow compliance to CIR and EIR. The marking function is responsible for marking the flow frames with the appropriate drop precedence based on frame compliance with CIR or EIR. A customer may implement shaping to avoid frame loss due to statistical variation in traffic.

Network engineering and a level of resource allocation is required in order to ensure that flow performance objectives, e.g., frame delay and frame loss, are satisfied. Performance measures are usually applicable only to frames that are compliant with the flow CIR.

7.11 Link type

The server link is referred to as dedicated for EVPRM type 1, as defined in clause 7.11.1 of [ITU-T G.8011]. The server link is referred to as shared for EVPRM types 2 and 3, as defined in clause 7.11.2 of [ITU-T G.8011].

7.12 Traffic separation

The EVPRM may use logical or spatial separation between customer traffic, as defined in clause 7.12.1 of [ITU-T G.8011]. EVPRM types 2 and 3 use logical or spatial separation, but EVPRM type 1 uses logical separation.

The EVPRM may use logical or spatial separation between service instances, as defined in clause 7.12.2 of [ITU-T G.8011] for EVPRM types 2 and 3. EVPRM type 1 uses logical separation.

7.13 Connectivity monitoring

While EVPT services must be supported by rooted-multipoint Ethernet (VLAN) connections that include ETH_C functions, server layer OAM (used in inherent monitoring) will be unable to determine the status of those multipoint Ethernet connections. Such status can only be determined by means of Ethernet OAM (proactive or on-demand).

Status monitoring of rooted-multipoint Ethernet connections requires the use of Ethernet OAM specified in [ITU-T Y.1731] and ETH MEP and ETH MIP functions specified in [ITU-T G.8010] and [ITU-T G.8021]. ETH MEP and ETH MIP functions and their ownership (customer, service provider, network operator) are shown in Figure 7-1.

Figure 7-1 provides the typical OAM configurations on UNI-N and intra domain NNI ports for EVPT services supported by a single network operator.

– ETH MIP functions on the UNI-N ports which are accessible from ETH MEP functions located in the customer network;
– ETH MEP functions on the UNI-N ports which are accessible by the service provider (which is the network operator); and
– ETH MIP functions on the intra domain NNI ports which are accessible from the service provider ETH MEP functions.

The service provider ETH MEP functions are responsible for UNI-N-to-UNI-N connectivity monitoring.

The ETH MIP functions on the UNI-N ports are used to help locating connectivity faults observed by the customer, which are not observed by the network. The ETH MIP functions on the intra domain NNI ports are used to help locating connectivity faults inside the network.

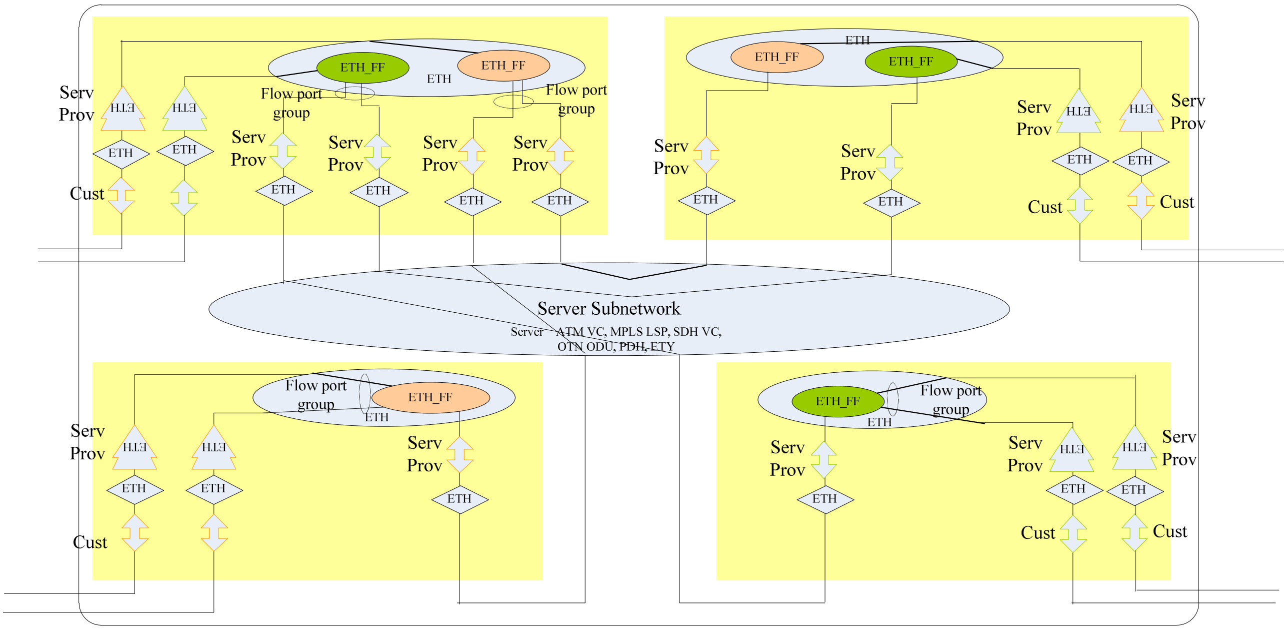

Figure 7-1 – Basic ETH MEP and MIP functions for all EVPRM types

Frame delay and frame delay variation monitoring within these rooted-multipoint Ethernet connections can be supported via on-demand Ethernet DMM/DMR OAM. Such DMM/DMR OAM is run between any two service provider ETH MEP functions.

Frame loss monitoring via the service provider ETH MEP functions is not possible with the Ethernet OAM frames currently specified in [ITU-T Y.1731]. In case frame loss is monitored between any two service provider ETH MEP functions, such measurement will count frames that are lost due to transmission errors (bit errors and congestion) on the ETH links and due to traffic conditioning at the ingress of the ETH link connections. The service provider and network operators are not accountable for the latter frame loss, which is due to customer traffic exceeding service level agreement for the link. Frames lost due to transmission errors or congestion on the ETH links can be detected when additional ETH MEP functions at the endpoints of the p2p ETH link connections are activated. Those ETH MEP functions are not illustrated in Figure 7-1.

7.14 Survivability

The transport network (service layer) can provide survivability for the EVPRM. The survivability alternatives for the ETH link are, for example:

– no protection;

– protection by means of SDH or OTH or ATM or MPLS protection schemes;

– restoration by means of SDH or OTH or ATM or MPLS restoration schemes.

The applicability of survivability by means of linear protection switching and ring protection based on APS can also be an option.

The applicability of survivability by means of LAG/STP/RSTP is for further study.

When the failure occurs, the entire tree can be switched to the backup root, or only the broken link between the leaf and root is switched to the backup link. An illustration of this is given in Appendix II.

8 UNI Attributes

8.1 ETH UNI attributes

A UNI can have a number of characteristics that will be important to the way that the CE sees a service. One of the key aspects of a service description will be the allowable mix of UNIs with different characteristics in an EVC. For example, a specific (simple) service might require all UNIs to have the same speed at the physical layer. A more sophisticated service may allow a wide variety of speeds.

Table 8-1 provides the UNI service attributes, parameters, and values for the EVPRM service.

Table 8-1 – UNI attributes and parameters for the EVPRM service

Layer	UNI service attribute	Service attribute parameters and values
ETH	UNI identifier	Arbitrary text string to identify the UNI.
	MAC layer	IEEE 802.3 – 2008.
	UNI maximum transmission unit size	2000 ≥ Integer ≥ 1522.
	Service multiplexing	SHOULD be supported at one or more UNIs. EVPRM type 1 and 3: SHOULD be supported. EVPRM type 2: MUST be No.
	UNI EVC ID	A string formed by the concatenation of the UNI ID and the EVC ID.
	CE-VLAN ID/EVC map	MUST specify mapping table of CE-VLAN IDs to the EVC ID.
	Bundling	Yes or No. If Yes, then CE-VLAN ID preservation MUST be Yes.
	All-to-one bundling	MUST be No.
	CE-VLAN ID for untagged and priority tagged service frames	MUST specify CE-VLAN ID for untagged and priority tagged service frames in the range of 1-4094.
	Maximum number of EVCs	MUST be ≥ 1.
	Ingress bandwidth profile per ingress UNI	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other ingress bandwidth profile is applied at this UNI.
	Ingress bandwidth profile per class of service identifier	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other ingress bandwidth profile is applied at this UNI.
	Egress bandwidth profile per egress UNI	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other egress bandwidth profile is applied at this UNI for this EVC.
	Egress bandwidth profile per class of service identifier	OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other egress bandwidth profile is applied at this UNI for this EVC.
	Layer 2 control protocols processing	A list of Layer 2 control protocols with each being labelled with one of Discard, Peer, Pass to EVC, Peer and Pass to EVC. MUST specify in accordance with clause 8.1.11.

Table 8-1 – UNI attributes and parameters for the EVPRM service

Layer	UNI service attribute	Service attribute parameters and values
	UNI type	Leaf or root.
	Connectivity monitoring	MEG levels, [ITU-T Y.1731] messages.
ETY	Physical medium	A standard Ethernet PHY.
	Speed	10 Mbit/s, 100 Mbit/s, 10/100 Mbit/s auto-negotiation, 1 Gbit/s, or 10 Gbit/s.
	Mode	Full duplex.

8.1.1 UNI ID

The UNI ID is an arbitrary string administered by the service provider, which is used to identify the UNI. It is intended for management and control purposes.

8.1.2 MAC layer

It supports all 802.3 MAC frames.

8.1.3 Maximum MTU size

The maximum MAC frame size supported at the UNI is at least 1522 bytes, as defined in clause 7.4 of [MEF 10.1], but not larger than 2000 (as specified in [IEEE 802.3]).

8.1.4 Service multiplexing

This attribute indicates whether the access to the Ethernet transport service is multiplexed (i.e., contains multiple service instances) or not. EVPRM type 2 does not use multiplexed access. However, EVPRM types 1 and 3 support multiplexed access.

8.1.5 UNI EVC ID

The UNI EVC ID is an arbitrary string administered by the service provider, which is used to identify an EVC at the UNI. It is intended for management and control purposes.

For CE-VLAN ID for untagged and priority tagged service frames, it MUST specify CE-VLAN ID for untagged and priority tagged service frames in the range of 1-4094.

8.1.6 CE-VLAN ID/EVC mapping

At the UNI there is a mapping of each customer VLAN ID to at most one EVC. For EVPRM, VLAN ID mapping is supported, it MUST specify a mapping table of CE-VLAN IDs to the EVC ID.

8.1.7 Bundling

When a UNI has the bundling attribute, it is configurable so that more than one VLAN ID can map to an EVC at the UNI. For EVPRM type 2, bundling is all-to-one and bundling is no. For EVPRM types 1 and 3, bundling is not supported.

8.1.8 All-to-one bundling

For EVPRM, all-to-one bundling is not supported.

8.1.9 Maximum number of EVCs

The maximum number of EVCs supported at the UNI is at least 1, per [MEF 6.1].

8.1.10 Bandwidth profile

The bandwidth profile at the ETH_UNI is specified in clause 7.10 of [MEF 10.1], it is OPTIONAL. If supported, MUST specify <CIR, CBS, EIR, EBS, CM, CF>. MUST NOT be allowed if any other ingress bandwidth profile is applied at this UNI.

8.1.11 Layer 2 control protocol processing

L2 control frames may be passed, processed, generated, or blocked as specified in Tables 8-2 and 8-3. [ITU-T G.8011] describes these actions.

For EVPRM, the choice of pass (tunnel), block (discard) or process (peer) on ingress, and whether to *generate* or have an action of *none* on egress is independent of the server layer (except as noted), but is customer service dependent.

Table 8-2 specifies the L2CP processing requirements for EVPRM service at UNI. The first column identifies the standard protocol, and the second column identifies the MAC DA used to carry that protocol data unit. The third column specifies the required action, and the fourth column specifies the applicability, i.e., whether the action taken must be the same at all UNIs in the EVC, or whether the action taken can be different on different UNIs in the EVC.

Table 8-2 – L2CP processing requirements for the EVPRM service at UNI

	MAC DA	L2CP Requirement (Ingress)	Applicability	L2CP Requirement (Egress)
STP/RSTP/MSTP (IEEE 802.1d/802.1w/802.1s）	01-80-C2-00-00-00	MUST Peer or Discard	All UNIs in the EVC	Generate or none
PAUSE [IEEE 802.3]	01-80-C2-00-00-01	MUST Discard	All UNIs in the EVC	None
LACP/LAMP [IEEE 802.3ad]	01-80-C2-00-00-02	MUST Peer or Discard	Per UNI	Generate or none
Link OAM [IEEE 802.3ah]	01-80-C2-00-00-02	MUST Peer or Discard	Per UNI	Generate or none
Port Authentication [IEEE 802.1X]	01-80-C2-00-00-03	MUST Peer or Discard	Per UNI	Generate or none
E-LMI [MEF 16]	01-80-C2-00-00-07	MUST Peer or Discard	Per UNI	Generate or none
LLDP [IEEE 802.1AB]	01-80-C2-00-00-0E	MUST Discard	All UNIs in the EVC	None
GARP/GMRP Block [IEEE 802.1D/802.1p]	01-80-C2-00-00-20 through 01-80-C2-00-00-2F	MUST Peer, Discard or Tunnel	Per UNI	Generate or none

8.1.12 UNI type

The possible attribute values are leaf or root.

8.1.13 Connectivity monitoring

For EVPRM, connectivity monitoring is achieved via Ethernet OAM mechanisms defined in [ITU-T Y.1731]/[IEEE 802.1ag] and is optional.

If specified, the MEG levels at the customer service layer are:

1) Tunnelled.
2) Tunnelled with UNI-N MIP.
3) Peered at UNI-N.
4) Blocked at UNI-N.

   Specifically, it will be blocked at the UNI-N if there is an up MEP at an equal or higher level, or a down MEP at a higher level.

For each level, any specific ITU-T Y.1731 messages (e.g., CCM, LT, LB, AIS) that can be supported (i.e., tunnelled, peered or blocked) are listed (the default, if nothing is listed, is that they are all supported).

In addition, there is a need to indicate at which level AIS/LCK is expected at. This may be indicated in the previous attribute: if it is not indicated, it is not expected.

Note that EFM OAM and E-LMI support at the UNI are already covered by listing it under clause 8.1.11. There are implications on network performance when these messages are tunnelled or blocked.

OAM requirements in this clause are based on protocols specified in [IEEE 802.1ag] and [ITU-T Y.1731].

Connectivity monitoring can either be proactive (layer monitoring, sub-layer monitoring, inherent monitoring) or on-demand, as specified in [ITU-T G.8010] and [ITU-T Y.1731]. In some network implementations, connectivity monitoring can rely on the server layer connectivity monitoring (inherent monitoring). It is an option to not perform proactive monitoring.

Table 8-3 – Connectivity monitoring

Attribute	Type	Function	ITU-T Y.1731 message
Proactive	Status	Continuity check and connectivity check	CCM.CC
	Performance	Interruption	CCM.CC, CCM.RDI
		Frame loss	CCM.LM
	Maintenance	Alarm suppression	AIS
		Locked indication	LCK
		Remote defect indication	CCM.RDI
		Client signal fail	–
On-demand	Status	Connectivity check	LBM/LBR
	Performance	Frame loss	LMM/LMR
		Frame delay	DMM/DMR, 1DM
		Frame delay variation	DMM/DMR, 1DM
		Throughput	LBM/LBR, TST
	Fault localization	Channel connectivity	LBM/LBR
		Flow connectivity	LTM/LTR
	Discovery	Flow connectivity	LTM/LTR

CFM (CC, LB, LT, LCK/AIS and TST, etc.) requirements are referred to in Table 8-4.

LM and DM are for further study.

Table 8-4 – CFM processing requirements for the EVPRM service at UNI

	MAC DA	L2CP Requirement (Ingress)	MEL level	Applicability	L2CP Requirement (Egress)
Service OAM, UNI ME, CC [IEEE 802.1ag]/[ITU-T Y.1731]	01-80-C2-00-00-3X or Unicast	MUST Peer or Discard or Tunnel	Specify	All UNIs in the EVC	Generate or none
Service OAM, UNI ME, LT [IEEE 802.1ag]/[ITU-T Y.1731]	01-80-C2-00-00-3Y	MUST Peer or Discard or Tunnel	Specify	All UNIs in the EVC	Generate or none
Service OAM, UNI ME, LB [IEEE 802.1ag]/[ITU-T Y.1731]	Unicast	MUST Peer or Discard or Tunnel	Specify	All UNIs in the EVC	Generate or none
Service OAM – Test ME [IEEE 802.1ag]/[ITU-T Y.1731]	Unicast	MUST Peer or Discard or Tunnel	Specify	All UNIs in the EVC	Generate or none
Service OAM – Subscriber MD [IEEE802.1ag]/[ITU-T Y.1731]	Unicast, multicast	MUST Peer or Discard or Tunnel	Specify	All UNIs in the EVC	Generate or none

8.2 ETY UNI attributes

The ETY_UNI is a PHY characterized by speed, mode and medium. These attributes are described in [ITU-T G.8011]. The attributes that apply to EVPRM are specified as follows:

8.2.1 Medium

This attribute indicates the medium of the Ethernet PHY layer that is used to transport the Ethernet service. The values are defined in clause 8 of [ITU-T G.8012]. It is a standard Ethernet PHY including 10BASE-T, 100BASE-T, 1000BASE-SX, 1000BASE-LX, 10GBASE-SR, 10GBASE-LR, 10GBASE-ER.

8.2.2 Speed

This attribute indicates the speed of Ethernet PHY layer that is used to transport the Ethernet service. There are four values defined by [ITU-T G.8012]: 10 Mbit/s, 100 Mbit/s, 10/100 Mbit/s auto-negotiation, 1 Gbit/s or 10 Gbit/s.

8.2.3 Mode

This attribute indicates the mode of Ethernet PHY layer that is used to transport the Ethernet service. EVPRM uses the full duplex mode.

9 NNI service attributes

9.1 ETH NNI attributes

Table 9-1 – NNI service attributes for the EVPRM service

Layer	NNI service attribute	Service attribute parameters and values
ETH	MAC service	IEEE 802.3-2008 frame format.
	NNI ID	Arbitrary text string to identify each NNI instance.
	NNI EVC ID	Arbitrary text string to identify each EVC instance.
	Multiplexed link	Yes, No.
	VLAN ID mapping	For further study.
	Bundling	For further study.
	Bandwidth profile	<CIR, CBS, EIR, EBS, CM, CF>.
	Layer 2 control protocol processing	Discard (Block), Peer (process), pass per protocol on ingress. Generate or none per protocol on egress.
	NNI type	Hub or spoke.
	Connectivity monitoring	FFS.
Server	Server layer	SDH, PDH, OTH, ETY, ATM, MPLS.

9.1.1 MAC service

The EVPRM NNI supports all 802.3 MAC frames. All ETH_CI is passed.

9.1.2 NNI ID

The NNI ID is an arbitrary string administered by the service provider, which is used to identify the NNI. It is intended for management and control purposes.

9.1.3 NNI EVC ID

It is an arbitrary text string to identify each EVC instance.

9.1.4 Multiplexed link

EVPRM type 1 does not support multiplexed NNI links. EVPRM types 2 and 3 can use or not use multiplexed NNI links.

9.1.5 VLAN mapping

At the multiplexed NNI, there is a mapping of service provider VLAN ID to at most one EVC.

For non-multiplexed NNI, VLAN ID mapping is not applicable.

It is for further study.

9.1.6 Bundling

For further study.

9.1.7 Bandwidth profile

For further study.

9.1.8 Layer 2 control protocol processing

L2 protocols are only visible at the NNI if it is an ETY. In this case, the L2 control protocols can be passed, processed, blocked, or none (per [ITU-T G.8011]). All 802 L2 protocols, as listed in Table 8-2 of [ITU-T G.8011] are passed. Note that the action taken at the NNI should be consistent with the action taken at the UNI.

9.1.9 NNI type

It should be hub or spoke.

9.1.10 Connectivity monitoring

For further study.

9.2 Server layer

The server layers for all EVPRM types described in clause 6 are specified in Table 9-2.

Table 9-2 – EVPRM server layers

Server layer technology
SDH
OTH
PDH
MPLS
ATM
ETY
ETH

Appendix I

Example of Ethernet virtual private rooted multipoint service

(This appendix does not form an integral part of this Recommendation)

This appendix presents some examples of EVPRM:

I.1 Single root

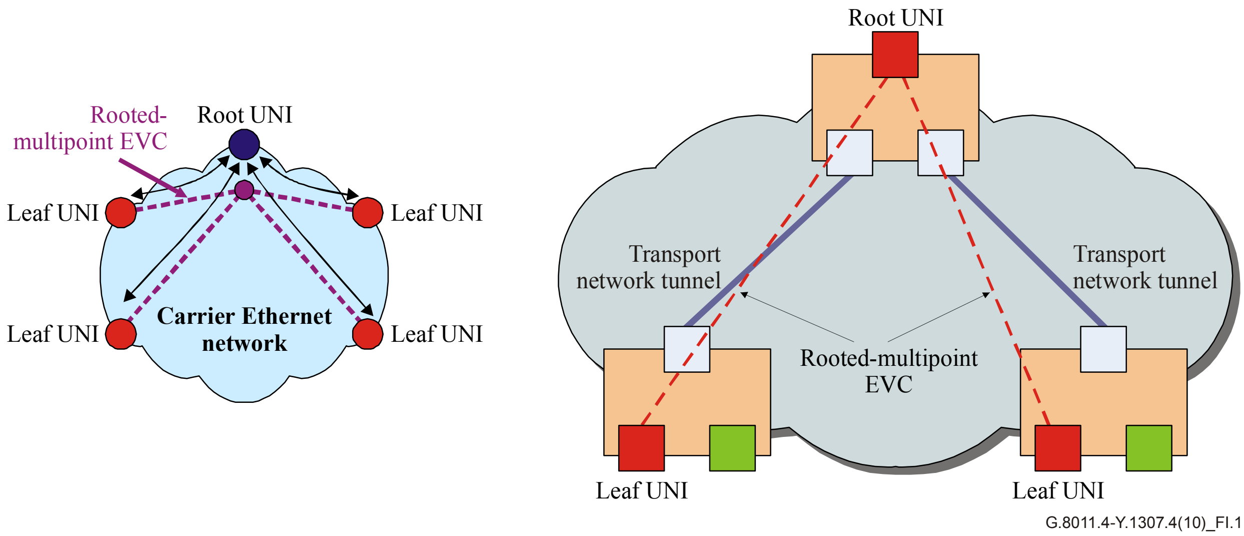

Figure I.1 – Single-root model

Single root is the simplest model. It is composed of one root and multiple leaves. The left part of Figure I.1 describes the abstract model of the single-root EVPRM, while the right part describes the concrete model.

This example is easy for deployment, but if the root fails, the whole EVPRM service will collapse.

I.2 Redundant roots

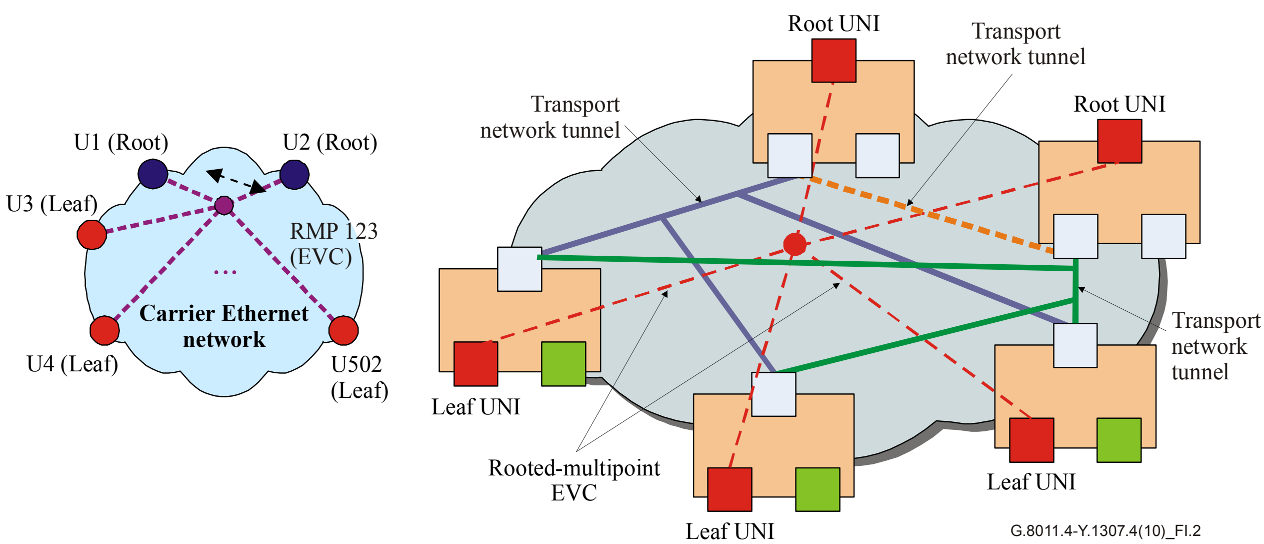

Figure I.2 – Redundant-root model

As Figure I.2 shows, the redundant root example has two roots and multiple leaves. Only one of the two roots should be in active status at a given moment, and the other which is redundant for the active one should be in standby status. To keep the right status, the two roots should exchange status messages and monitor the status of each other. When the active one does not work well, the standby root will take over the transmission task.

The configuration shown in this example provides reliable protection for the root node, which is very important for applications. This model is very much deployed in the network.

I.3 Load-balance root

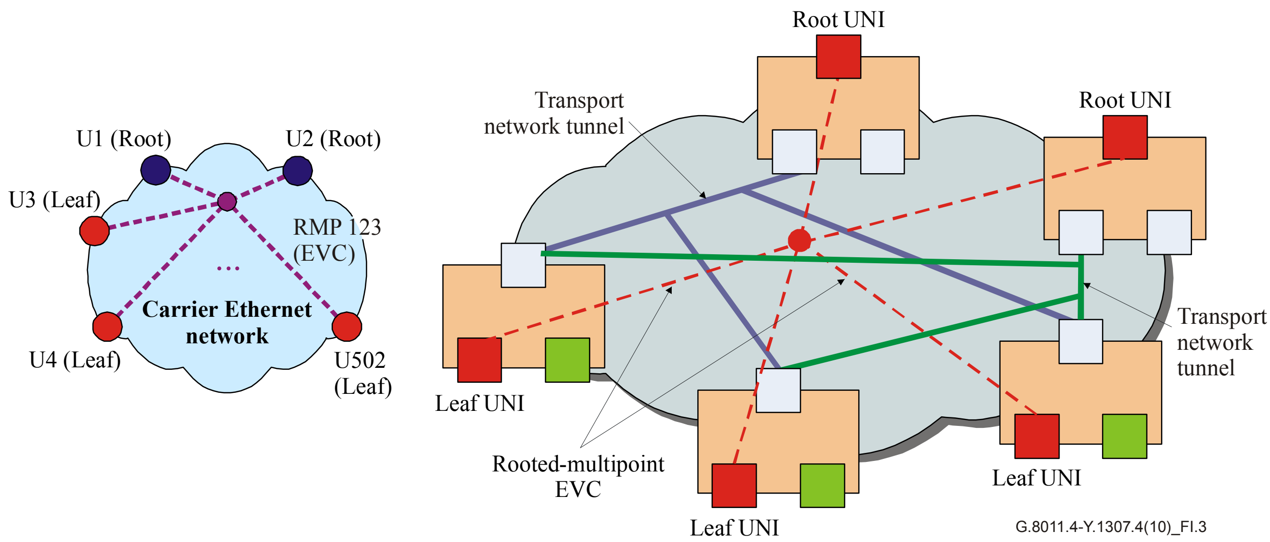

Figure I.3 – Load-balance root model

As Figure I.3 shows, the load-balance root example has multiple roots and multiple leaves. The multiple roots always work together for the same service, and the service traffic is distributed among the roots.

This example provides load balance ability for the root node. It is suitable for the case when all of the server access nodes are in heavy load and thus none can provide enough capacity to transport all of the service traffic. Actually, this model can also be viewed as the combination of multiple EVPRMs.

I.4 Hierarchical branch

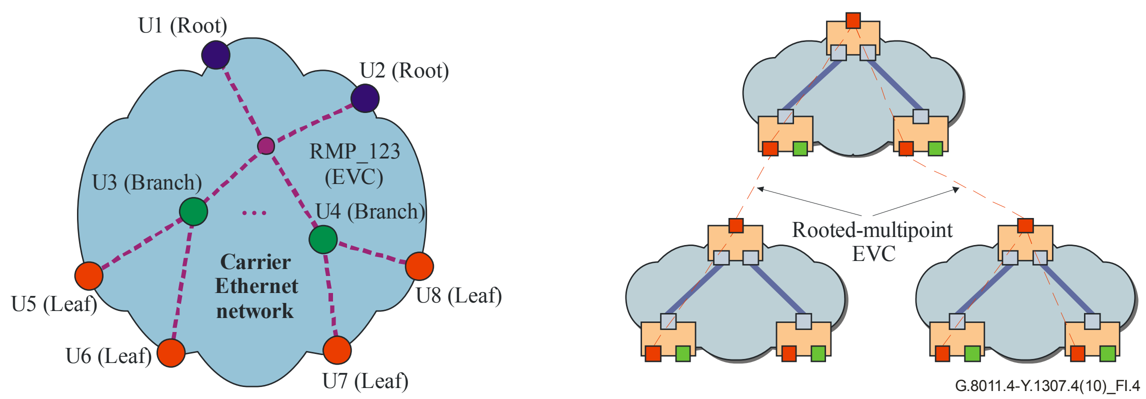

Figure I.4 – Hierarchical-branch model

Hierarchical branch has one or more branch NNIs. As Figure I.4 shows, it can be used to describe the case in which the Ethernet service spans multiple transport networks.

Appendix II

Protection of Ethernet virtual private rooted multipoint service

(This appendix does not form an integral part of this Recommendation)

This appendix describes EVPRM 1+1 and 1:1 protection switching.

II.1 1+1 protection switching architecture

The 1+1 multicast protection switching architecture is shown in Figure II.1. One protection tree is dedicated to one working tree. The working traffic is permanently bridged to the working and protection trees at the root node. The leaves receive traffic only by using the selective selector on the working tree.

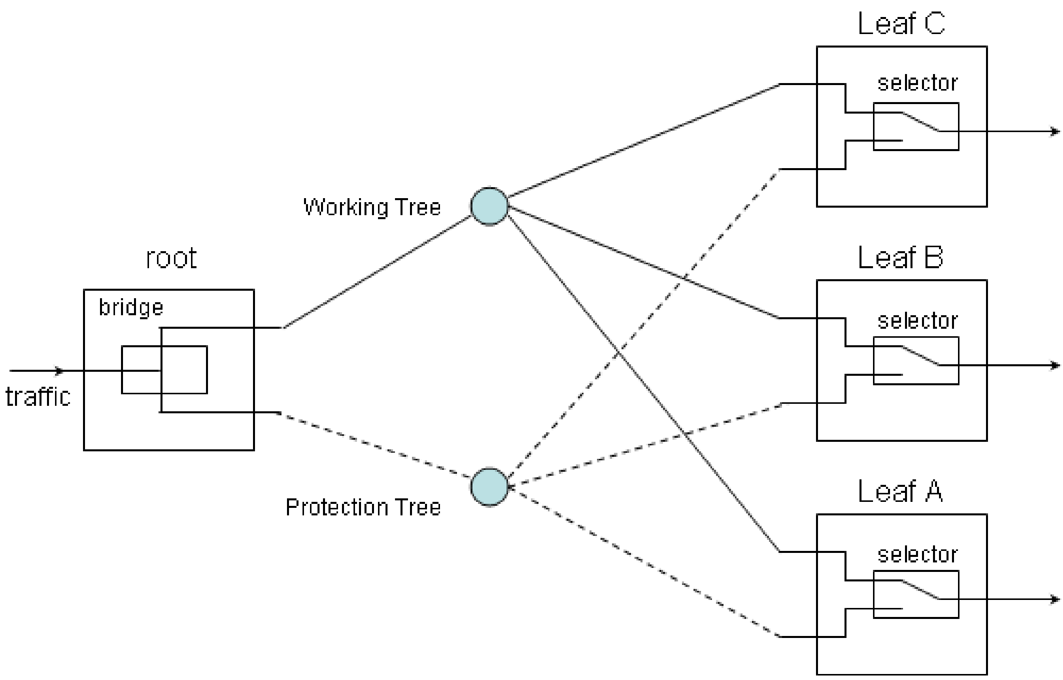

Figure II.1 – 1+1 protection switching architecture

If for example, a defect occurs in the working tree and the traffic to leaf node C is affected, as shown in Figure II.2, the defect will be detected at node C. All the leaves can be switched to the protection tree by using a 2-phase APS protocol. The protocol is as follows:

1) Node C detects the defect and switches the selector to the protection tree after validating the priority.
2) The APS protocol from node C to the root requests a protection switch.
3) The root node sends APS protocol to all leaves for a protection switch.
4) After all other leaves validate the priority of the protection request, the selectors of these leaves are switched to the protection tree.

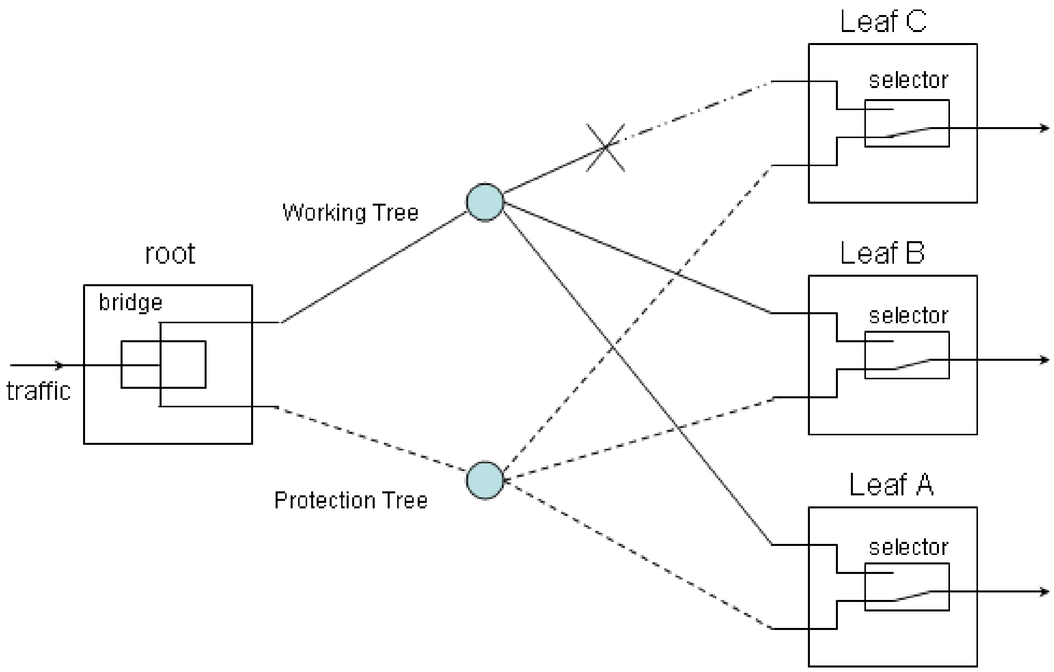

**Figure II.2 – 1+1 protection switching architecture –
All leaves switch to protection**

In the case in which only the affected leaf (e.g., only node C) is switched to the protection tree after protection switching, the other leaves will still work on the working tree. The APS protocol is not necessary. When node C detects the defect, it switches the selector to the protection tree directly after validating the priority. The scenario is shown in Figure II.3.

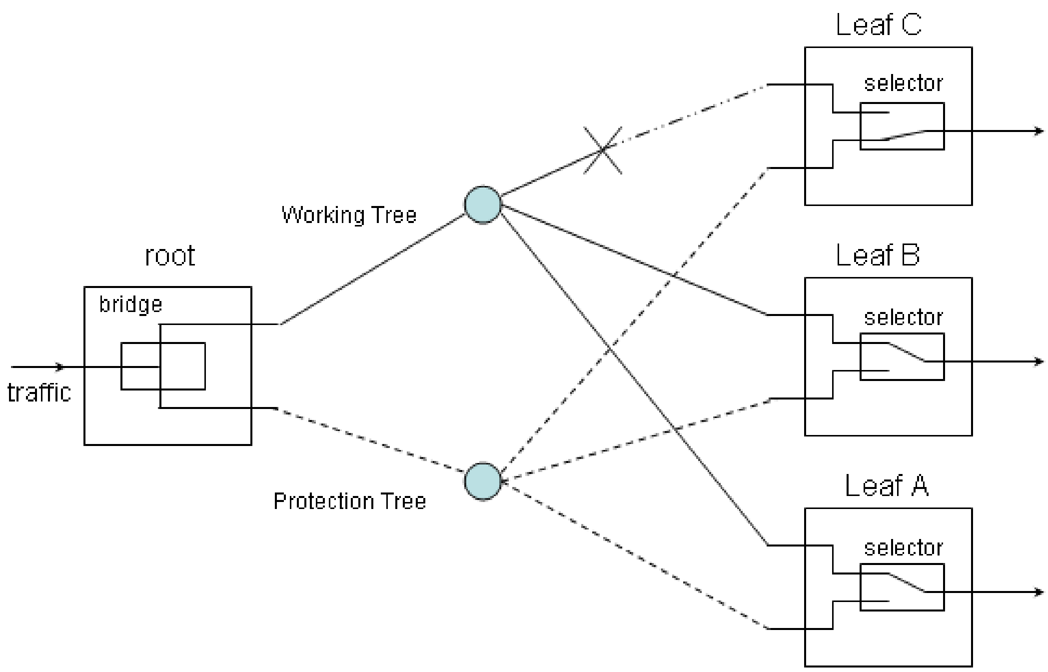

**Figure II.3 – 1+1 protection switching architecture –
Only the affected leaf switches to protection**

II.2 1:1 protection switching architecture

The 1:1 multicast protection switching architecture is shown in Figure II.4. One protection tree is dedicated to one working tree. The working traffic is normally only transmitted on the working tree. The leaves receive traffic only by using the selective selector on the working tree.

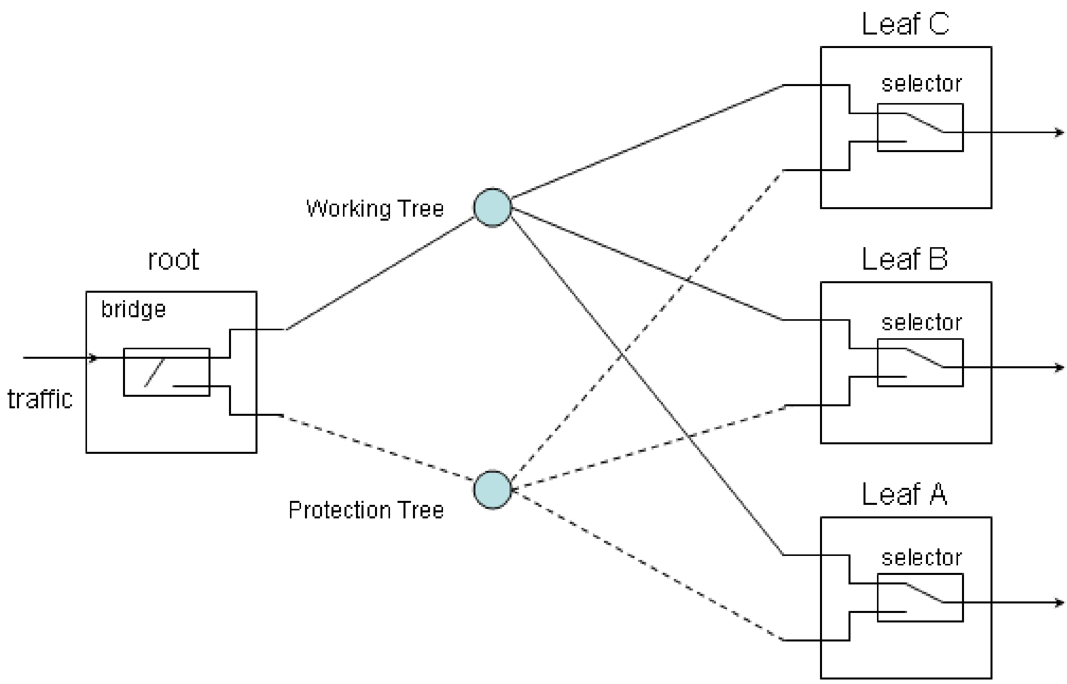

Figure II.4 – 1:1 protection switching architecture

If for example, a defect occurs on the working tree and the traffic to node C is affected, as shown in Figure II.5, the defect will be detected at node C. All the leaves can be switched to the protection tree by using a 2-phase APS protocol. The protocol is as follows:

1) Node C detects the defect and switches the selector to the protection tree after validating the priority.
2) The APS protocol from node C to root requests a protection switch.
3) After the root node validates the priority of the protection request, it operates the bridge to the protection tree (NOTE – The working traffic will be bridged to both the working tree and the protection tree after the root operates the broadcast bridge).
4) The root sends APS protocol to all leaves for a protection switch.
5) After all other leaves validate the priority of the protection request, the selectors of these leaves are switched to the protection tree.

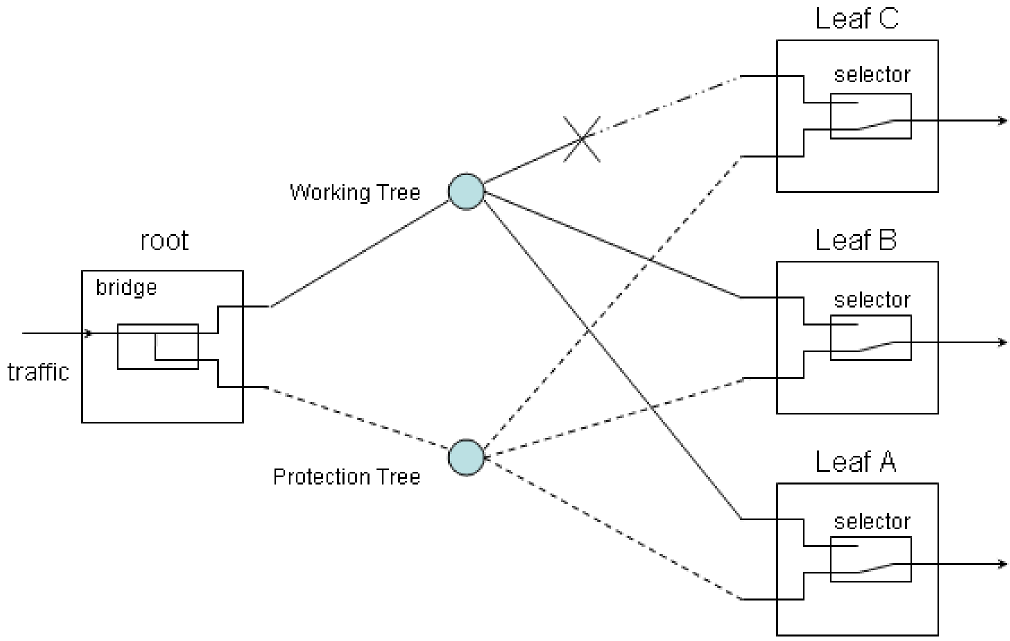

Figure II.5 – 1:1 protection switching architecture –
All leaves switch to protection

In the case in which only the affected leaf (e.g., only node C) is switched to the protection tree after protection switching, the other leaves will still work on the working tree. A 1-phase APS protocol is used. The process of the APS protocol is similar to the one mentioned above, but steps 4 and 5 are not necessary. After the protection switching, the affected leaf receives the working traffic on the protection tree, and the other leaves receive the traffic on the working tree. The scenario is shown in Figure II.6.

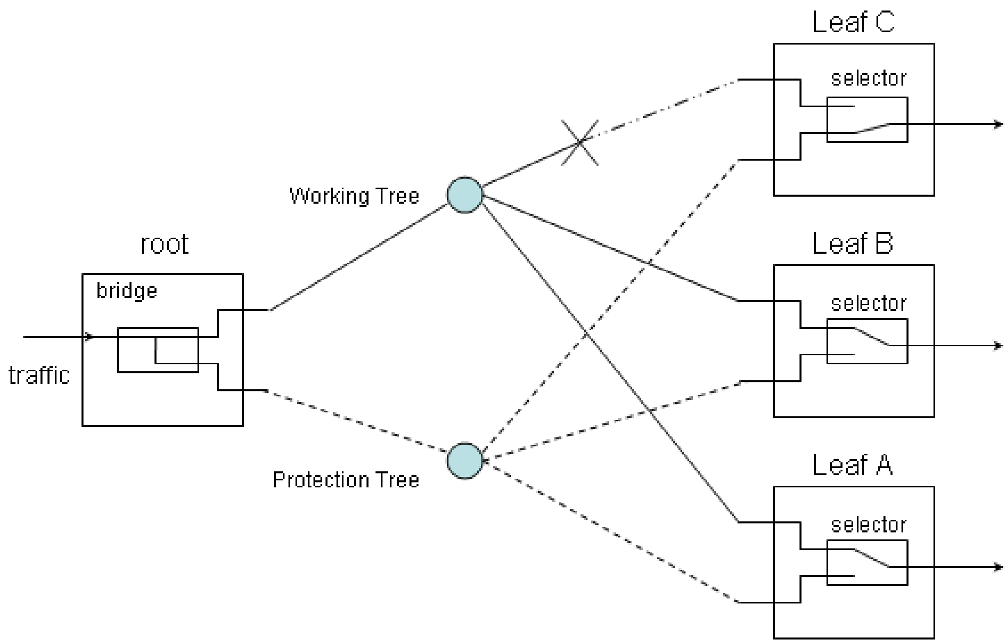

Figure II.6 – 1:1 protection switching architecture –
Only the affected leaf switches to protection

In the 1:1 protection switching architecture shown in Figure II.7, the root sends the working traffic only on the working tree or on the protection tree, and all leaves are permanently set to receive from both trees.

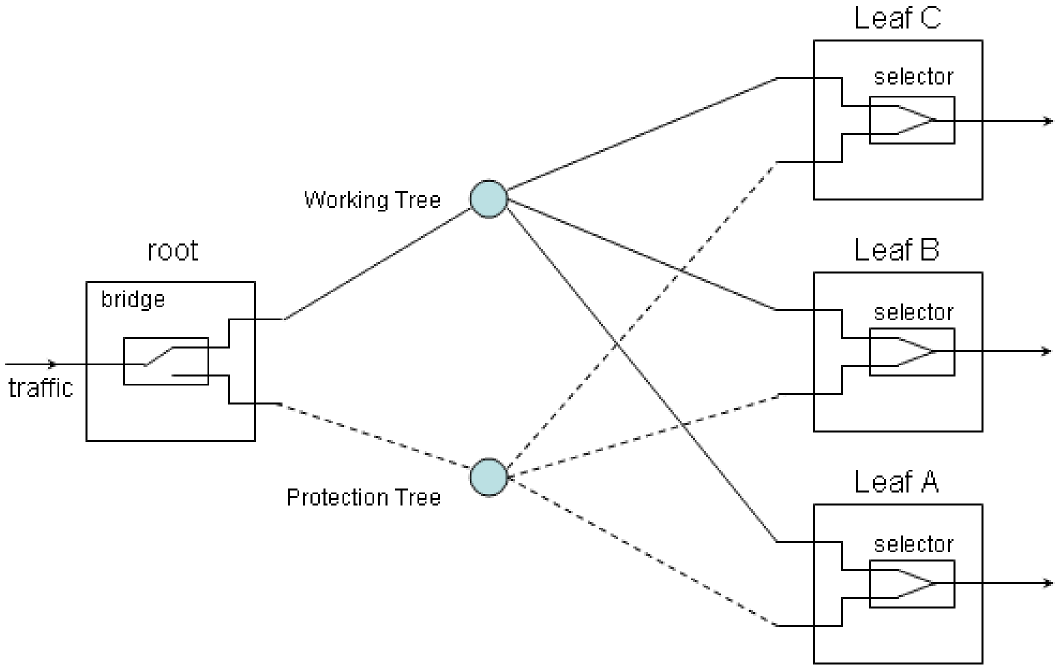

Figure II.7 – 1:1 protection switching architecture

If for example, a defect occurs on the working tree and the traffic to node C is affected, as shown in Figure II.8, the defect will be detected at node C. When the root is switched to the protection tree after protection switching, all leaves will receive the working traffic on the protection tree. A 1-phase APS protocol is used. The protocol is follows:

1) Node C detects the defect, then the APS protocol from node C to root requests a protection switch.

2) After the root node validates the priority of the protection request, it operates the selective bridge to the protection tree.

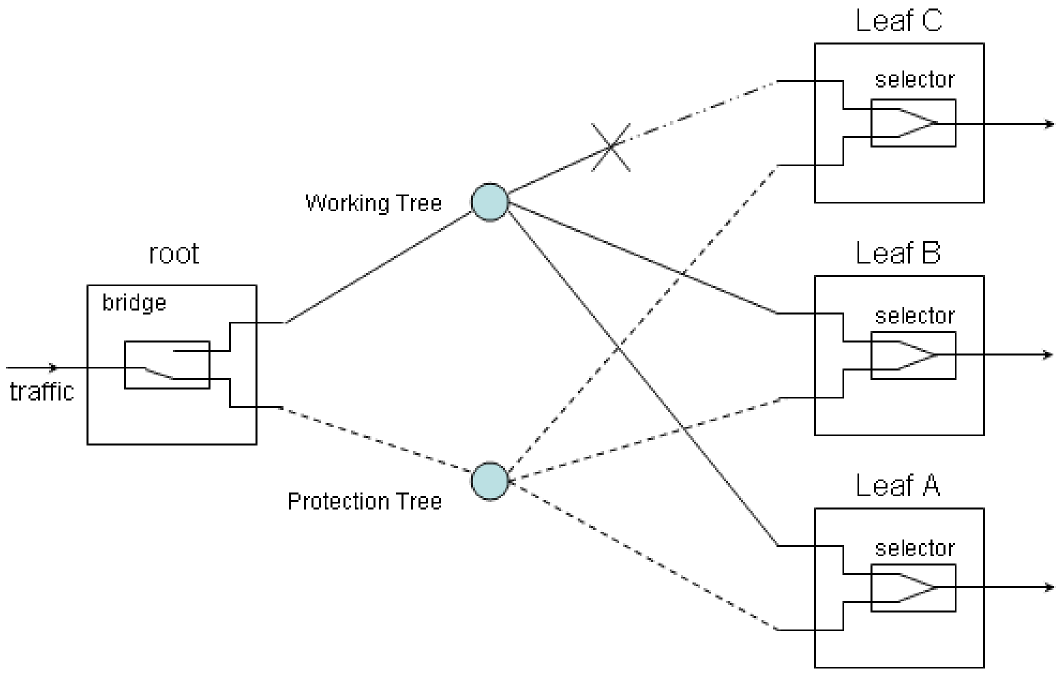

Figure II.8 – 1:1 protection switching architecture – All traffic is switched to the protection tree

Appendix III

Use cases of the Ethernet virtual private rooted multipoint service

(This appendix does not form an integral part of this Recommendation)

III.1 Introduction

Table III.1 elaborates on the meaning of the EVPRM types and indicates an example application for which the specific EVPRM type is suitable.

Table III.1 – EVPRM types and use case examples

Type	Shared server layer	Multiplexed access	Connectivity description	Use case example
EVPRM Type 1	N	Y	Multiplexed[3] access with EPL	IPTV transport over dedicated AN/TN with multiplexed AN
EVPRM Type 2	Y	N	Shared transport layer with dedicated access	RNC←→Node B Mobile Backhaul
EVPRM Type 3	Y	Y	Shared transport layer with multiplexed access	Centralized delivery node multiple business application services

III.2 Use cases in detail

III.2.1 Use Case 1 – IPTV transport

The following points present the set of assumptions that provide the basis for the IPTV transport use case:

– Two independent (owner or administered) IPTV service providers utilize a Type 1 EVPRM connectivity service from an Ethernet network operator to connect their video head end nodes (VHEs) (i.e., their root nodes) with their access nodes (DSLAM) (i.e., leaf nodes) equipment.

– The Type 1 EVPRM connections are built using dedicated ingress access and dedicated transport server links.

– Egress access is multiplexed (i.e., shared) to take advantage of the pre-existing access infrastructure footprint.

– Dedicated transport containers (e.g., VCGs or ODUs, etc.) are used to support two independent EVC client trees.

– All-to-one bundling is leveraged at the UNI-N to ensure CE-VLAN ID preservation.

– Since transport resources at the egress TNE is shared, PE-VLAN ID tagging is performed there to separate the individual traffic directed at specific AN equipment.

– Different classes of service (CoS) are supported; they are differentiated through either IEEE 802.1ad priority code points (PCP) or IETF RFC 2474 DSCP markings.

[3] In this use case example the multiplexed access is done at the sink termination rather than at the source termination.

Based on the previous set of assumptions, the example depicted in Figure III.1 illustrates the establishment of a Type 1 EVPRM connectivity service in which the root nodes are connected to the EVPRM over dedicated access and transport links but share the egress access transport connection to their individual network termination ports.

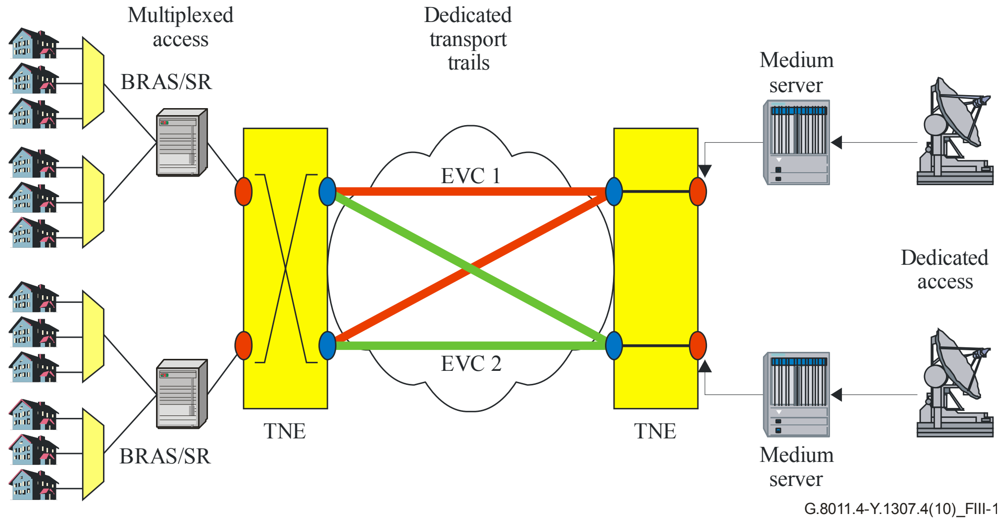

Figure III.1 – Use case 1 – IPTV transport

III.2.2 Use case: 2 – Mobile backhaul

The following points present the set of assumptions that provide the basis for this particular mobile backhaul use case:

– Two independent (owner or administered) mobile operators utilize Type 2 EVPRM connectivity services from an Ethernet network operator to connect their RNCs (root nodes) with their Node B (leaf nodes) equipment.

– Groups of k_i[4] RAN Node Bs are uniquely identified by a CE-VLAN ID[5]: associating several RAN Node Bs to the same CE-VLAN ID avoids any issues relating to VLAN ID address space limitations.

– The CE-VLAN ID is used for tagging the traffic of the associated group of RAN Node Bs.

– Tagging is performed at the individual RAN RNC UNI-C.

– PE-VLAN ID tagging is performed at the transport network equipment (TNE) to separate the individual traffic of the mobile operators over the shared transport resources.

– Different classes of service (CoS) are supported; they are differentiated through either IEEE 802.1ad priority code points (PCP) or IETF RFC 2474 DSCP markings.

– Shared aspects of EVPRM connectivity contain 2 EVCs i.e., EVC1 <Node B1, Node B2, RNC 1> and EVC2 <Node B3, Node B4, RNC 2>.

Based on the previous set of assumptions, the example depicted in Figure III.2 illustrates the establishment of a Type 2 EVPRM connectivity service with the root nodes connected to the EVPRM over dedicated access links but sharing the transport connection to their individual network termination ports. It is easy to observe in this example, the association of CE-VLAN ID to a

4 k_i indicates the number of RAN Node Bs belonging to the i-th group. This scenario can be extended to the case of a single group including all the RAN Node Bs connected to the RAN RNC.

5 Inside each group, each RAN Node B is uniquely identified by its own MAC address.

specific set of Node Bs. In addition, this EVPRM example easily accommodates CoS requirements based on <EVC+PCP> or <EVC+DSCP>.

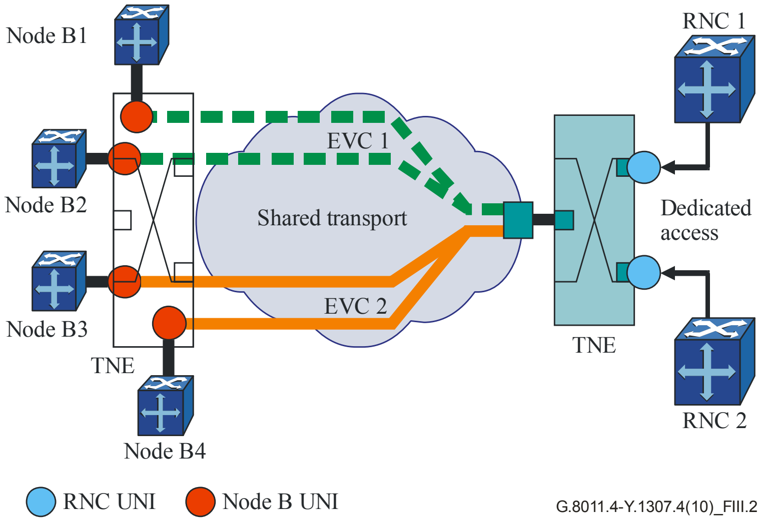

Figure III.2 – Use case 2 – EVPRM mobile backhaul

III.2.3 Use case 3 – Centralized delivery multiple business applications

The following points detail the set of assumptions that provide the basis for this particular centralized business application delivery use case:

– Centralized subscriber site utilizes a Type 3 EVPRM connectivity service from an Ethernet network operator to deliver two business application services (one being an IP-based video service).

– All subscriber business locations are connected with two EVCs, each supporting one of the business applications.

– A common UNI is employed for both services and therefore service multiplexing will be necessary at each UNI.

– Separate bandwidth profiles will also be necessary to ensure non-intrusive operation effects of one service on the other.

– CE-VLAN IDs are used to uniquely identify a specific traffic class/type. All local site customer equipment (CE) supporting the services will be required to handle the associated CE-VLAN ID processing[6].

– Traffic types running between the central site and local sites that are the same or identical will be tagged and identified with the same CE-VLAN ID value.

– Tagging is performed at the TNE UNI-C.

– Tagging is performed at the local site CE UNI-C.

– Traffic types and classes can be differentiated through their CE-VLAN IDs; in the event a traffic type requires a different level of prioritization (i.e., IP video stream) either IEEE 802.1ad PCP or IETF RFC 2474 DSCP values can be used.

6 Local site CEs are uniquely identified by their own MAC address.

In this example, each subscriber local site is being served by two different EVPRM trees, each delivering a different business application service. At each subscriber local site, the UNI-C tag forwards and terminates tagged frames (with different CE-VLAN IDs) to/from the UNI-N at the RNC.

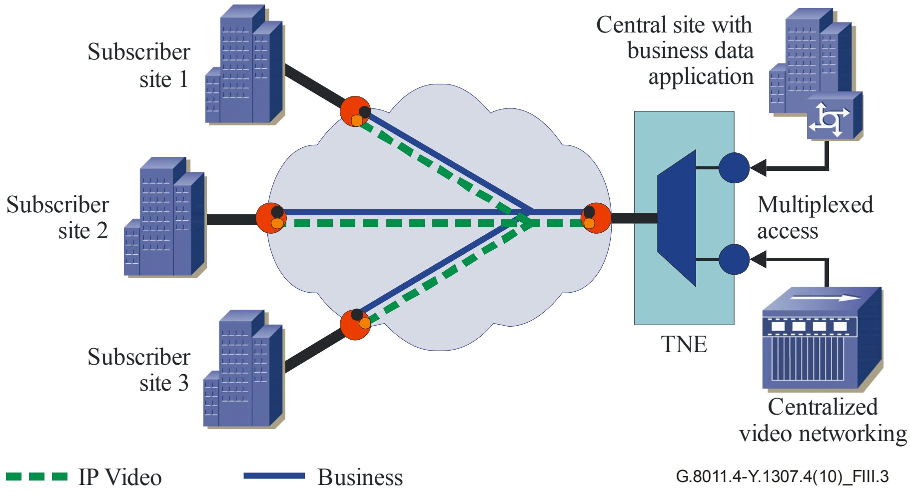

Figure III.3 – Use case 3 – EVPRM centralized delivery multiple business applications[7]

[7] Egress TNE is not shown.

Bibliography

[b-IEEE 802.1ad] IEEE 802.1ad-2005, *Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks, Amendment 4: Provider Bridges.*

[b-IETF RFC 2474] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.*

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010