Technical Specification
MEF 43

Virtual NID (vNID) Functionality for E-Access Services

April, 2014

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and the Metro Ethernet Forum (MEF) is not responsible for any errors. The MEF does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by the MEF concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by the MEF as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. The MEF is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any MEF member company which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any MEF member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

c) any form of relationship between any MEF member companies and the recipient or user of this document.

Implementation or use of specific Metro Ethernet standards or recommendations and MEF specifications will be voluntary, and no company shall be obliged to implement them by virtue of participation in the Metro Ethernet Forum. The MEF is a non-profit international organization accelerating industry cooperation on Metro Ethernet technology. The MEF does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

List of Figures

List of Tables

1 List of Contributing Members

The following members of the MEF participated in the development of this document and have requested to be included in this list.

ADTRAN	Cyan, Inc.
Adva Optical Networking	Ericsson AB
Albis Technologies	EXFO
Alcatel-Lucent	Iometrix
Allstream	Nokia Siemens Networks
AT&T	Omnitron Systems Technology, Inc.
CENX	PLDT
Ciena Corporation	Pulse Communications (Pulsecom)
Cisco Systems	Tellabs
Colt	Transition Networks
Comcast	Verizon

2 Abstract

This document specifies the functionality offered by an Access Provider (AP) that, when combined with an Ethernet-Access (E-Access) Service, allows a Service Provider (SP) to monitor and configure selected objects associated with a given UNI and one or more OVC End Points at that UNI in the AP's network. The effect is that the AP provides functionality similar to what would otherwise require the SP to place a Network Interface Device (NID) at the customer's location. Hence, the AP is said to be providing "virtual NID (vNID)" functionality to the E-Access Service that the SP has purchased. This is accomplished via the SP communicating over a Remote Management Interface (RMI) Connection to the AP, using an RMI Protocol.

The content of this document can be divided into two types.

- **Requirements on the AP network:** There are behaviors required across UNI and ENNI interfaces. This is the focus of this document; to define a known, standard service that SPs can buy from APs that provide access service having vNID functionality.
- **Functionality of the SP network:** SP functions will be discussed as information to provide guidance for vendors and suppliers in an informational appendix (see Section Appendix B).

The above imply requirements for devices that provide the needed functionality. This document does not specify which device must implement which functions.

In addition, this document provides guidance, where necessary, on how the SP and AP should interact to configure and manage these capabilities. This framework is presented to explain the assumptions of what interactions between the SP and AP need to be supported via the RMI Protocol, and what interactions are assumed to be supported via the Service Order process.

3 Terminology and Acronyms

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other MEF or external documents.

Table 1: Acronyms and Definitions

Term	Definition	Source
AP	Access Provider	MEF 33 [64]
AP RMI End Point	The point at the intersection of the RMI Connection and the ENNI-N in the AP's network.	This document
AIS	Alarm Indication Signal	ITU-T G.8021 [44]
Bandwidth Profile	A characterization of Service Frame or ENNI Frame arrival times and lengths at a reference point.	MEF 10.2 [51]
BWP	Bandwidth Profile	MEF 12.1 [53]
CBS	Committed Burst Size	MEF 10.2 [51]
CCM	Continuity Check Message	ITU-T G.8021 [44]
CE	Customer Edge	MEF 10.2 [51]
CEN	Carrier Ethernet Network	MEF 12.1 [53]
CE-VLAN	Customer Edge VLAN	MEF 10.2 [51]
CF	Coupling Flag	MEF 10.2 [51]
CIR	Committed Information Rate	MEF 10.2 [51]
CM	Color Mode	MEF 10.2 [51]
CoS	Class of Service	MEF 23.1 [58]
DEI	Drop Eligible Indicator	MEF 23.1 [58]
DM	Delay Measurement	MEF 35 [65]
EBS	Excess Burst Size	MEF 10.2 [51]
EIR	Excess Information Rate	MEF 10.2 [51]
E-LAN	An Ethernet service type that is based on a Multipoint-to-Multipoint EVC.	MEF 6.1 [48]
EMS	Element Management System	MEF 7.2 [50]
E-Line	An Ethernet service type that is based on a Point-to-Point EVC	MEF 6.1 [48]
E-LMI	Ethernet Local Management Interface	MEF 16 [55]
ENNI	External Network Network Interface	MEF 26.1 [59]
EPL	Ethernet Private Line	MEF 6.1 [48]
EP-LAN	Ethernet Private LAN	MEF 6.1 [48]
Ethernet Virtual Connection	An association of two or more UNIs that limits the exchange of Service Frames to UNIs in the Ethernet Virtual Connection	MEF 10.2 [51]
E-Tree	An Ethernet service type that is based on a Rooted-Multipoint EVC.	MEF 6.1 [48]
EVC	Ethernet Virtual Connection	MEF 10.2 [51]

Term	Definition	Source
EVPL	Ethernet Virtual Private Line	MEF 6.1 [48]
EVP-LAN	Ethernet Virtual Private LAN	MEF 6.1 [48]
FM	Fault Management	MEF 30.1 [61]
L2CP	Layer 2 Control Protocol	MEF 10.2 [51]
LM	Loss Measurement	MEF 35 [65]
Maintenance association End Point	A Maintenance association End Point is equivalent to a MEG End Point.	IEEE Std 802.1Q™-2011 [1]
Maintenance Entity Group End Point	An actively managed SOAM entity associated with a specific service instance that can generate and receive SOAM PDUs and track any responses. It is an end point of a single MEG, and is an end point of a separate Maintenance Entity for each of the other MEPs in the same MEG. This term is equivalent to Maintenance association End Point in IEEE.	ITU-T Y.1731 [43]
Maintenance Entity	A point-to-point relationship between two MEPs within a single MEG. This term is equivalent to a Maintenance Entity, or ME, as defined by IEEE Std 802.1Q-2011.	IEEE Std 802.1Q-2011 [1], ITU-T Y.1731 [43]
Maintenance Entity Group	A set of MEs that exist in the same administrative boundary, with the same MEG Level and MEG ID. This term is equivalent to Maintenance Association (MA) in IEEE.	ITU-T Y.1731 [43]
Maintenance Entity Group Identifier	An identifier for a MEG, unique over the domain that SOAM is to protect against the accidental concatenation of service instances. This term is equivalent to Maintenance Association Identifier (MAID) in IEEE.	ITU-T Y.1731 [43]
Maintenance Entity Group Level	Maintenance Entity Group Level. A small integer in a field in a SOAM PDU that is used, along with the VID in the VLAN tag, to identify to which Maintenance Association among those associated with the SOAM frame's VID, and thus to which ME, a SOAM PDU belongs. The MEG Level determines the MPs a) that are interested in the contents of a SOAM PDU, and b) through which the frame carrying that SOAM PDU is al-lowed to pass. This term is equivalent to MD Level, which is used in [IEEE Std 802.1Q-2011].	ITU-T Y.1731 [43]
ME	Maintenance Entity	ITU-T Y.1731 [43] IEEE Std 802.1Q-2011 [1]

Term	Definition	Source
MEG	Maintenance Entity Group	ITU-T Y.1731 [43]
MEG End Point	Maintenance Entity Group End Point	ITU-T Y.1731 [43] or MEF 17 [56]
MEG ID	Maintenance Entity Group Identifier	ITU-T Y.1731 [43]
MEG Level	Maintenance Entity Group Level	ITU-T Y.1731 [43]
MEP	Maintenance association End Point, or equivalently, MEG End Point	IEEE Std 802.1Q-2011 [1]
MIP	Maintenance domain Intermediate Point (IEEE Std 802.1Q-2011), or equivalently a MEG Intermediate Point (ITU-T Y.1731 or MEF 17).	IEEE Std 802.1Q-2011 [1], ITU-T Y.1731 [43], MEF 17 [56]
MTU	Maximum Transmission Unit	MEF 10.2 [51]
NE	Network Element	MEF 4 [47]
NETCONF	NETwork CONFiguration protocol	RFC 6241 [41]
NETwork CONFiguration protocol	Network management protocol for managing device configuration.	RFC 6241 [41]
Network Interface Device	Network device that the Subscriber connects directly to.	This document
NID	Network Interface Device	This document
OAM	Operations, Administration, and Maintenance	MEF 17 [56]
OSS	Operations Support System	MEF 7.2 [50]
OVC	Operator Virtual Connection	MEF 26.1 [59]
PCP	Priority Code Point	IEEE Std 802.1Q [1]
Performance Monitoring	Performance Monitoring involves the collection of data concerning the performance of the network.	ITU-T M.3400 [45]
PM	Performance Monitoring	ITU-T M.3400 [45]
Remote Processing Entity	The entity that receives and processes messages from the SP over the RMI Connection, and transmits responses. It can also generate autonomous messages. There is a one to one relationship between the RMI and an RPE. One RPE can be associated with one AP UNI, or a set of UNIs.	This document
RMI	Remote Management Interface	This document
RMI Connection	Logical connection that supports messages between the SP and the appropriate RPE in the AP's network responsible for vNID functionality for a given set of UNIs.	This document

Term	Definition	Source
RMI Protocol	Protocol that is used on a given RMI Connection, using an associated data model that supports the vNID Service. Examples include SNMP v2c and NETCONF.	This document
RMI Protocol Message	An individual message sent via the RMI Protocol on an RMI Connection.	This document
RPE	Remote Processing Entity	This document
Service Provider	The organization providing Ethernet service(s) to the Subscriber.	MEF 10.2 [51]
Service Provider Processing Entity	The Management Entity in the SP network that communicates to the RPE using the RMI Protocol	This document
SLS	Service Level Specification	MEF 10.2 [51]
SOAM	Service Operations, Administration, and Maintenance	MEF 17 [56]
SP	Service Provider	MEF 10.2 [51]
SPPE	Service Provider Processing Entity	This document
S-VLAN ID	S-VLAN Identifier	MEF 26.1 [59]
S-VLAN Identifier	The 12 bit VLAN ID field in the S-Tag of an ENNI Frame	MEF 26.1 [59]
UDP	User Datagram Protocol	RFC 768 [4]
UNI	User Network Interface	MEF 10.2 [51]
UNI-N	Network side UNI functions	MEF 4 [47]
UNI Tunnel Access	The UNI Tunnel Access (UTA) associates a VUNI and remote UNI and is composed of VUNI and remote UNI Components and at least one supporting OVC	MEF 28 [60]
UTA	UNI Tunnel Access	MEF 28 [60]
VID	VLAN Identifier	IEEE Std 802.1Q [1]
Virtual UNI	Virtual UNI (VUNI) is the component consisting of a collection of service attributes in the VUNI Provider's CEN. The VUNI is paired with a remote UNI in an Access Provider's CEN. The main function of the VUNI is to map frames between a set of one or more OVCs present in the VUNI Provider domain and a single vNID Service OVC (e.g., supporting vNID Service Case B).	Updated from MEF 28 [60]
VLAN	Virtual Local Area Network	IEEE Std 802.1Q [1]
vNID	virtual Network Interface Device	This document
vNID Service	Shorthand for "E-Access Service with vNID Functionality"	This document
VUNI	Virtual UNI	MEF 28 [60]

Term	Definition	Source
VUNI End Point	An End Point at the VUNI Provider's side of a specific ENNI that associates the ENNI with a VUNI; e.g., in support of vNID Service Case B.	Updated from MEF 28 [60]
VUNI Provider	The Operator CEN providing the VUNI.	MEF 28 [60]

4 Key Concepts, Scope, and Objectives

Note that additional motivation and other background material is contained in Appendix A.

4.1 Motivation and Problem Definition

Because many Subscribers require national or even global connectivity, Service Providers (SPs) must be able to extend their Carrier Ethernet offerings beyond their normal footprint. This requires Service Providers to collaborate with Access Providers (APs).

The Service Provider may just order E-Access service as defined in MEF 33 [64], or it may have the option of ordering vNID functionality provided by the AP to purchase an enhanced version of E-Access service.

4.1.1 E-Access Service without vNID Functionality

Figure 1 shows an example where the SP's Subscriber has a UNI requiring connectivity through an AP, in addition to UNI W and UNI X that the SP supports directly. A straightforward approach to offering service is for the SP to deploy a device at the Subscriber's location to the left of UNI Z[1], as shown in the figure. Such a device is often in addition to a local device that the AP has deployed to the right of UNI Z. The SP's device provides a UNI to the Subscriber (UNI Y).

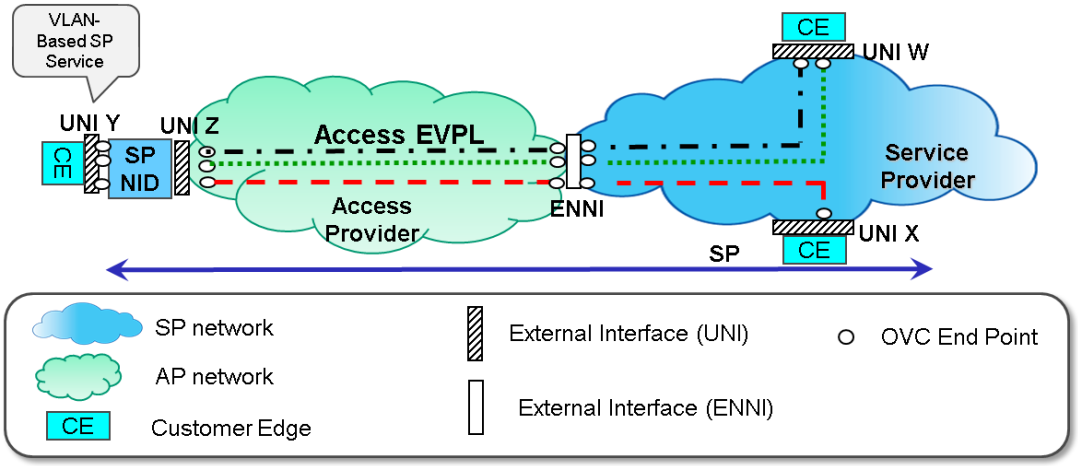

Figure 1: Network Topology with SP Placing its Own NID

[1] Note that what is called "UNI Z" is a UNI from the point of view of the Access Provider. Such an arrangement does not comply with the MEF assumptions of how Operators connect. In the interest of simplicity, the UNI terminology is abused here rather than introducing a new term.

This approach provides the SP with a direct interface to the Subscriber using the SP's device, and the ability to test, monitor the performance and instantiate key service attributes without coordinating with the AP in a manner similar to what it offers at in-network UNIs.

However, this approach has some constraints. First, the SP must place a device at the Subscriber's location, and this may be difficult for reasons ranging from lack of installation personnel to difficulties in getting approval to place equipment in another country (homologation). In addition, each device introduces another failure point and another possibility for mis-configuration or errored performance that complicates any troubleshooting effort. For the SP, servicing the remote device in a timely manner can be problematic.

An alternative approach is for the SP to *not* place a device at the Subscriber's UNI, but instead to rely on the AP to provide all required functions. This is shown in Figure 2. With this approach, the AP is responsible for deployment of the sole edge device, and with quickly resolving issues (using its local workforce). However, the challenge with this approach is that coordination between SP and AP is required for many functions (e.g., collecting data for troubleshooting), and the response would be much slower for the SP than querying its own device.

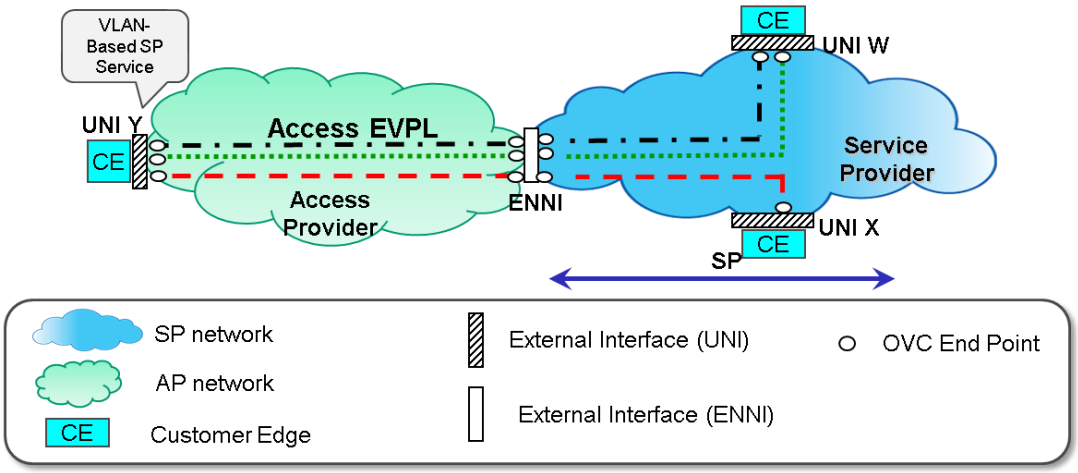

Figure 2: Network Topology with SP Relying on AP

Each of these approaches has strengths and weaknesses. The goal of specifying vNID functionality is to combine the strengths of each of the above approaches. Doing so requires a standard approach and model, which is the focus of this document.

4.1.2 E-Access Service with vNID Functionality

An example of the vNID approach is shown in Figure 3. In this example, the E-Access service is an enhanced version of the MEF 33 E-Access service, which differs in ways that will be discussed.

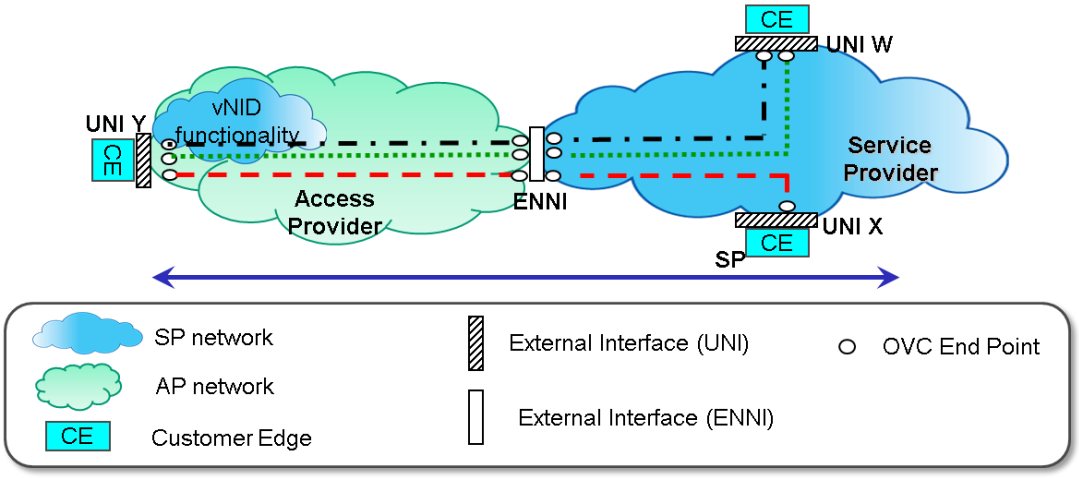

Figure 3: Network Topology with AP Offering vNID Functionality

With the vNID approach, the AP has equipment at Subscriber premises to support UNI functions. In the AP network, a set of managed objects supporting the service are identified that the SP is allowed to interact with, and the nature of the allowed interaction (e.g., "read", "write") are also specified for each object. The goal is for the AP to provide the SP with the key service management functionality that an SP's NID would have provided, but to do so through virtual NID (vNID) functionality. This allows the SP to interact with functions quickly and naturally based on existing element management protocols, without requiring interaction with AP administrative processes each time the SP wants information about the UNI.[2] It also relieves the SP of the burdens of deploying and maintaining a separate device.

The AP has full flexibility in meeting the requirements in this document, in that the functionality can be implemented in one or multiple devices, and there is no requirement that new devices must be deployed.

4.2 Specifying vNID Functionality: Fundamentals

In order to specify vNID functionality, it must be established what objects and functions the AP allows the SP to manage in the AP network. This document specifies this delineation. In addition, this document specifies the Remote Management Interface (RMI) Connection and the RMI Protocols which the SP can use to communicate with the AP about such objects.

As will be discussed in Section 6, two different vNID Service cases – Basic and Advanced – will be addressed in this version of this document, and there are differences in the specific models. However, they have the following common characteristics:

- All models specify what objects the SP can interact with in the AP network. In addition, the SP can have different types of interactions, depending on the object. Some AP objects will emit alarms that are sent to the SP upon the occurrence of a fault. Others can be read by the SP when desired; for example, performance counters. Other objects may allow the SP to modify their attributes, such as whether a SOAM MEP is active or not.

[2] Note that during maintenance intervals, there can be periods during which the RMI Connection or RPE might be inactive. During such periods, the AP would not respond to SP requests.

- All models have an RMI Connection through which the SP communicates with a Remote Processing Entity (RPE) in the AP's network. For a given set of UNIs, the RMI Connection supports the RMI Protocol[3] between the SP and the RPE responsible for the vNID functionality. This connection is assumed to be distinct and different from any management channel that the AP uses to manage its network elements; i.e. the expectation is that the AP will not allow the SP to have general access to its management network, and the RPE will terminate the RMI Protocol and would not allow packets from the SP to be routed beyond the RPE. The AP has freedom in locating the RPE implementation; it could be implemented in a device located at the UNI, in an Element Management System (EMS) of the AP, or at other locations.

The figure below illustrates how an SP uses a Service Provider Processing Entity (SPPE) to communicate via the RMI Connection to an RPE regarding a specific UNI in the AP's network. This ensures that both the SP and AP have a common understanding of the objects that are being managed.

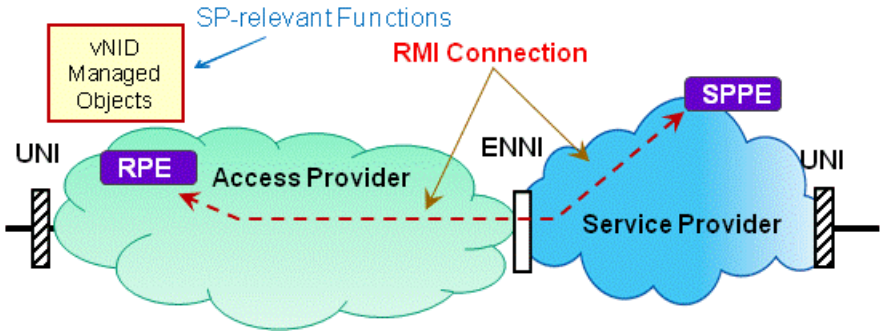

Figure 4: Overview of Communication between SP and AP via RMI Connection

The details of the implementation of the RMI connection shown in Figure 4 are beyond the scope of this document.

4.3 Scope

This section presents the assumptions made and the implications for the scope of this document.

- This document defines requirements for the AP's vNID functions. It does not define implementation methods to meet these requirements. This document does not define requirements on the SP except as implied by what is required at the ENNI.
- With vNID Service, the AP provides a point-to-point service. Just as with MEF 33 [64], the SP can use the vNID Service as a component of non point-to-point Subscriber services, non-MEF defined services, or even non-Ethernet services.

[3] "RMI Protocol" is the term that refers generically to the protocol (e.g. SNMP v2c, NETCONF) chosen to communicate with specific RPEs.

- Effort has been taken to align with the MEF 33 Access EPL and Access EVPL requirements where possible and prudent, but where changes were deemed to be needed, the differences are noted in this document.
- This document addresses the scenario where there is a single AP and a single SP.
  - It may be shown that it is possible to expand beyond the two-Operator case. However, defining an ENNI-ENNI intermediate service seems to be needed, and doing so is far outside the scope of this document. Future phases may address this case.
  - For this phase, we call the two Operators "Service Provider" and "Access Provider", to align with MEF 33.
- The UNI in the AP network is dedicated to services which are offered by the one SP. This implies that the AP cannot offer any EVCs associating the UNI directly with another UNI supported by that same AP without connecting to the SP.
- Each AP OVC between the ENNI and the UNI supports a single Class of Service (CoS) Name.
- There is some discussion about the levels and placement of SOAM MEPs and MIPs. This document draws upon SOAM FM, PM, and MEF Architecture work (in MEF30.1, MEF35, and MEF12.1), and does not duplicate previous work, but introduces some new requirements.
- vNID functionality requires protocol-specific data model(s) in order to implement the vNID managed objects specified in the Management Information Model. An SNMP vNID MIB Module is being defined in a separate document. A NETCONF YANG Model may be specified in the future.
- Section 7.3 of the protocol-independent Carrier Ethernet Management Information Model (MEF 7.2 [50]) provides guidance on the set of vNID managed objects of the SP and AP.

A number of items are part of a vNID Service, but are not specified in detail in this document:

- This document does not address UNI or ENNI protection schemes.
- Values for Service Level Specification (SLS) objectives are not addressed in this document.

Objectives: This document defines the following:

- Functionality that the SP can view or manage in the AP's network. This is accomplished via communication between the SP and AP via the RMI Protocol. Types of communication include information that the SP:
  - can receive from the AP, such as alarms and notifications.
  - can read in the APs network, such as performance information.
  - can write in the AP's network, such as configuring/activating EVCs, configuring MEPs, etc.

- The RMI Connection (with a focus on behavior at the ENNI). It includes items such as:
  - The specific RMI Protocol used (e.g., SNMP, NETCONF)
  - Relationship between an RPE and the number of UNIs it is associated with. The relationship can be 1:1, or alternatively one RPE may be associated with multiple UNIs.[4] Each RPE has its own IP address.
  - Security considerations for the RMI Protocol and Connection
- Administrative functions available to the SP, such as alarm configuration

In order to specify what objects in the AP network can be managed/viewed by the SP via the RMI Protocol, it is important to understand what interactions are assumed to take place via the Service Order[5] or are limited by the AP's Service Definition. This document does not specify requirements for those processes but does discuss what is assumed for them. This provides the context in which the RMI Protocol is assumed to operate.

Non-Objectives: As stated earlier, this work does not define requirements for a single device in which all vNID functions need to be performed. Functions could be implemented in one or multiple devices. Therefore, the interface between the AP's device at the UNI and the rest of the AP's network is not defined.

In addition, this document does not address the scenario where the SP places its own NID at the Subscriber location, and connects to the AP's network. Such a scenario does not involve vNID functions.

5 Compliance Levels

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in RFC 2119 [11]. All key words must be in upper case, bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

A paragraph preceded by **[CR*a*]<** specifies a conditional mandatory requirement that **MUST** be followed if the condition(s) following the "<" have been met. For example, "**[CR1]<[D38]**" indicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement 38 has been met. A paragraph preceded by **[CD*b*]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the "<" have been met. A

[4] As an example of 1:1, a NID with a single UNI could have its own RPE. Examples of many:1 include: a NID with multiple UNIs that has a single RPE (assuming all UNIs are managed by the same SP), an AP with one centralized RPE for each SP, or an AP with multiple RPEs for each SP (for scale/ redundancy).

[5] The Service Order is the method by which one carrier specifies the specific parameters and attributes associated with the service it orders from another carrier.

paragraph preceded by **[CO*c*]<** specifies an Conditional Optional Requirement that **MAY** be followed if the condition(s) following the "<" have been met.

5.1 Numerical Prefix Conventions

This document uses the prefix notation to indicate multiplier values as shown in Table 2.

Table 2: Numerical Prefix Conventions

Decimal		**Binary**	
Symbol	Value	Symbol	Value
k	**10^3**	**Ki**	**2^{10}**
M	**10^6**	**Mi**	**2^{20}**
G	**10^9**	**Gi**	**2^{30}**
T	**10^{12}**	**Ti**	**2^{40}**
P	**10^{15}**	**Pi**	**2^{50}**
E	**10^{18}**	**Ei**	**2^{60}**
Z	**10^{21}**	**Zi**	**2^{70}**
Y	**10^{24}**	**Yi**	**2^{80}**

6 Service Models

In order to leverage appropriate models and requirements in existing MEF work, it is necessary to specify the services offered by the SP and AP in several key scenarios, and discuss each in turn. This will allow a separate specification of the requirements relevant to each scenario.

In contrast to the scenario where the Service Provider offers service directly to Subscriber UNIs without an AP, the vNID approach requires the SP to additionally consider the service that the AP provides to the Service Provider.

Table 3 summarizes the service types defined in MEF 6.1. These are services that are offered to Subscribers. In this document we consider scenarios where the SP may offer any of the six E-Line, E-LAN and E-Tree services shown.

Table 3: Ethernet Service Types, from MEF6.1

Service Type	**Port-Based (All-to-One Bundling)**	**VLAN-Based (Service Multiplexed)**
E-Line (Point-to-Point EVC)	Ethernet Private Line (EPL)	Ethernet Virtual Private Line (EVPL)
E-LAN (multipoint-to-multipoint EVC)	Ethernet Private LAN (EP-LAN)	Ethernet Virtual Private LAN (EVP-LAN)
E-Tree (rooted multipoint EVC)	Ethernet Private Tree (EP-Tree)	Ethernet Virtual Private Tree (EVP-Tree)

MEF 33 defines two Access services that an AP can offer the SP as shown in Table 4. Note that only services based on point-to-point OVCs are supported, and others are not applicable. In the same way, the vNID Services only address point-to-point OVCs.

Table 4: E-Access Service Types Defined in MEF 33

OVC Type	Port-Based	VLAN-Based
Point-to-point	Access Ethernet Private Line (Access EPL)	Access Ethernet Virtual Private Line (Access EVPL)
Multipoint-to-multipoint	NA	NA
Rooted Multipoint	NA	NA

In this version of this document, we describe two levels of vNID Service functionality that the AP can offer to the SP, to enable the SP to have access to specific subsets of information and (in some selected areas) configuration control. Note that in all of these, the UNI in the AP is dedicated to one and only one SP:

- vNID Service – Basic Case ("Case B"): The AP provides a single OVC with vNID functionality for all traffic across the UNI. In particular, the AP does not need to configure attribute behavior as being CE-VLAN specific. Case B allows the SP to offer Port-based EVC services (EPL, EP-LAN, EP-Tree) across an AP. It requires functionality outside the AP for the SP to offer VLAN-based EVC services. This vNID Service is an enhancement of Access EPL.
- vNID Service – Advanced Case ("Case A"): The AP provides one or more OVCs with vNID functionality for the traffic across the UNI. The SP will be able to map at least one CE-VLAN ID to each OVC. Depending on the AP's capabilities, the SP might also be able to map to an OVC: multiple CE-VLAN IDs, or (if there is only one OVC) all CE-VLAN IDs to an OVC. Case A allows the SP to offer VLAN-based EVC service (EVPL, EVP-LAN, or EVP-Tree). Note also that if the AP allows the SP to specify that all CE-VLANs map to a single OVC, the SP could order a single OVC to a UNI and set values for the UNI to offer Port-based service to the Subscriber. In Case A, the AP is providing a service that can be configured by the SP to function as an enhancement of Access EPL service or an enhancement of Access EVPL. Differences from MEF 33's Access EPL and Access EVPL are listed in this document.

The Basic and Advanced vNID Service cases are briefly discussed in the following sub-sections. Detailed requirements are provided in later sections.

[R1] The AP **MUST** offer at least one case (Basic Case or Advanced Case) as a part of its vNID offering.

Any UNI that is supported by vNID functionality will be associated with one of the vNID Service cases. This is determined via the Service Order process. The SP will be able to read the value the AP assigns to a UNI, but will not be able to change it via the RMI Protocol.

[R2] The AP **MUST** be able to report, via the RMI Protocol, the case the AP has associated with a UNI that is supported by vNID functionality.

The vNID Service case is identified by a Case attribute, shown below.

Table 5: vNID Service Case ID Attribute

vNID Service	Case ID
Basic Case	1
Advanced Case	2

6.1 Common Aspects

For each vNID Service case listed previously there is an RMI Connection between the SP and AP that supports one or more UNIs in the AP's network. Details of the RMI Connection (such as the ID) will be discussed in Section 7.2.3. In all cases, the RMI Connection is identified at the ENNI via a unique S-VLAN ID value.

Parameters of interest to the vNID Service fall into the following groups:

- UNI Service Attributes,
- OVC per UNI Service Attributes[6],
- OVC Service Attributes,
- OVC End Point per ENNI attributes, and
- ENNI Service Attributes.

The AP and SP must agree through negotiation and/or the order entry process to many of the parameters that are configured. Service Order and negotiation involves the configuration of some parameters like OVC Bandwidth Profiles (BWPs) or Class of Service (CoS) identifiers, and these must be coordinated among the two operators.[7] The AP is responsible for managing these parameters and – although the SP may be able to read them – the SP cannot set their values via the RMI Protocol.

Other parameters within the list of service attributes can be set by the SP using the RMI Protocol. Depending on the case, this can involve parameters like OVC End Point Map at the UNI, SOAM configuration of EVC MEPs, and the CE-VLAN ID for untagged and priority tagged Service Frames at the UNI.

6.2 vNID Service – Basic Case (Case B)

In vNID Service Case B the AP sells the SP an enhancement of Access EPL service that is based on vNID functionality combined with a single OVC, where the OVC has the property that all CE-VLAN IDs are mapped to it at the UNI. In this case, the SP can provide either port-based

[6] Since an OVC can only associate one OVC End Point that is at a UNI (see MEF 26.1), these service attributes can be equivalently viewed as OVC End Point per UNI service attributes.

[7] Note that the BWP settings offered by the AP's service options may not exactly match the SP's service, and that the CoS markings could have different meanings in the SP and AP networks.

service or VLAN-based service to the Subscriber. If it is VLAN-based, it is assumed that VUNI functionality (see MEF 28) would be present in the SP network.

Figure 5 shows the single OVC that is provided by the AP in Case B.

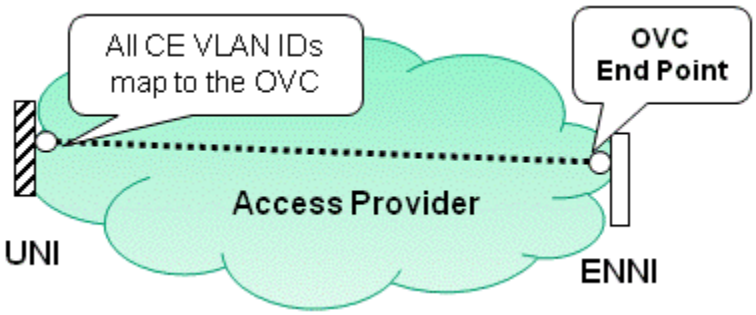

Figure 5: Configuration for vNID Service Case B

In this case, only one OVC is configured by the AP. There are some parameters that are agreed upon by the two parties through negotiation and/or the order entry process. There are also parameters that are specified by the SP via the RMI Protocol.

Case B supports only one OVC per UNI, and therefore only a single S-VLAN ID at the ENNI is used per UNI for Subscriber traffic.

6.3 vNID Service – Advanced Case (Case A)

In vNID Service case A the SP buys from the AP vNID functionality combined with one or more OVCs. One OVC may support more than one EVC (at least if mapping more than one CE-VLAN ID to an OVC is supported).

Figure 6 shows an example of Case A with three OVCs. Note that multiple OVCs per UNI can be configured between the UNI and one or more ENNIs to the same SP.

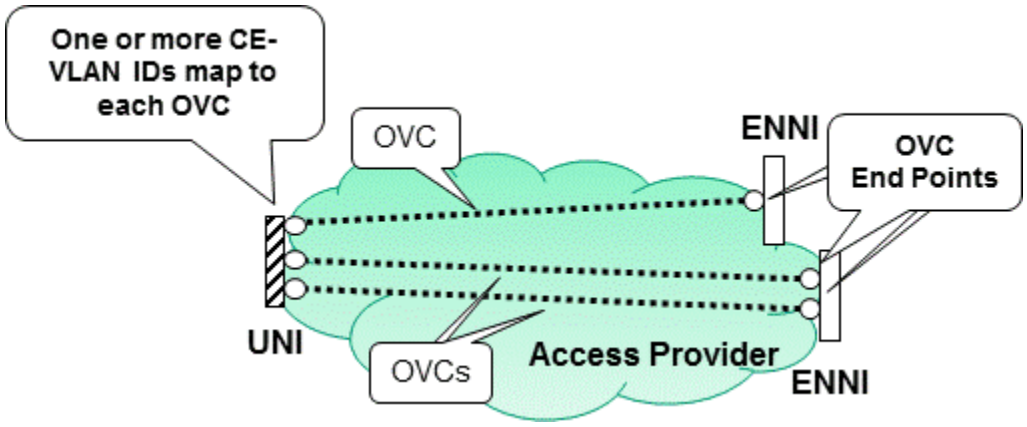

Figure 6: Example Configuration for vNID Service Case A, with Three OVCs

7 Virtual NID (vNID) Functionality: Requirements Common to all Cases

7.1 Overview of Requirements

As discussed previously there are two different vNID Service cases defined in this document. This section presents the requirements that are common across both use cases. The requirements are focused on four areas; requirements for the data plane, requirements for OAM, requirements for the RMI, and Administrative requirements. These requirements address all the service attributes and parameters from MEF 6.1, MEF 10.2, MEF 26.1 and MEF 33 that will be accessible to the SP via the RMI Protocol.

The requirements focus on the functions that the AP provides in support of vNID Service. They include aspects such as the UNI, the frame format at the ENNI, the placement of MEPs and specifics of the RMI Protocol.

"Support", vs. "able to support" in requirements: When a requirement includes a phrase like "the AP MUST be able to support" a capability, it means that the AP must offer that capability to the SP as an option. However, in specific case(s) where the SP has not chosen that option, the AP would not support the functionality.

When the AP must/should/may support something, it means that a service instance must/should/may have that specified thing.

7.1.1 Roles and Responsibilities

The roles and responsibilities of the AP and SP are included in this sub-section. The AP has specific roles and responsibilities, the SP has specific roles and responsibilities, and there are things that are jointly agreed upon by the two parties.

The AP must define the specifics of their vNID offering. The AP is responsible for providing vNID functionality, connecting the service to the Subscriber via a UNI and to the SP via an ENNI. The AP is then responsible for monitoring the device or devices that provide vNID functionality and for acting upon any problem reports generated by the SP. The AP will have the ability to read the value of all attributes, including those that are controlled by the SP. In other words, the vNID Service does not have any requirements that forbid the AP from reading values of attributes that the SP sets. This specification assumes the business relationship between the AP and SP can be relied upon to ensure that the AP does not use this information to damage or compete unfairly with the SP.

The SP is responsible for reviewing the AP's vNID offering and determining if it meets the SP's requirements. The SP then coordinates some variables with the AP during the ordering process. This process may be different for different APs and is outside the scope of this document.

7.1.2 SP Access to AP Objects

[R3] The AP **MUST** allow the SP access to all objects specified as readable ('R') or read/writeable ('R/W').

It is expected that the AP will *not* allow access to objects that are not 'R' or 'R/W', and will indicate an error if the SP attempts to access such objects.

[D1] The AP **SHOULD** prohibit access by the SP to all objects not specified as 'R' or 'R/W'.

However it is not forbidden for an AP to go beyond this specification and provide access to additional objects.

7.1.3 Structure of Requirement Tables

The Requirement Tables that follow have a structure described hereafter.

The first column identifies the attribute or function referenced in the row. The second column usually contains a requirement related to the attribute or function, but sometimes contains a definition or other pertinent information. Not all rows specify requirements. An example is shown below.

Table 6: The RMI, SO, and M-D Table Columns

Attribute or Function	Requirement	RMI	SO	M-D
Attribute 1	Requirement or description of Attribute 1goes here.	R, R/W, or blank	Yes, opt, or blank	Yes or blank
Attribute 2	Requirement 1 regarding Attribute 2	R, R/W, or blank	Yes, opt, or blank	Yes or blank
	Requirement 2 regarding Attribute 2			

A requirement might not apply to a variable that can be assigned a value, in which case the last three columns will be blank. However, when a requirement in a row applies to a variable that can take on values, the last three columns specify whether more than one value can be set, and if so, the roles of the Service Order and the RMI Protocol. Note that multiple requirements may apply to a variable, but the rightmost three columns apply to the variable, not to individual requirements. These three headings are:

- Single Value Mandated by this Document (M-D): This field is either 'yes' or blank. When only one value is allowed, this column entry is 'yes', and the AP will set that value.
- Service Order (SO): This field is either 'yes', 'opt' (optional), or blank.
  A 'yes' in this column indicates that the value (e.g., S-VLAN ID to use on an ENNI) is negotiated when the service is set up, and the value is not (re)writable via the RMI Protocol.
  'Opt' in the column indicates that a value can be communicated or set via the order process if desired.
  This field is blank when the SO is not appropriate; for example when M-D is yes (because there is no value to choose) or when a value refers to operational state.
- RMI: This field is either 'R', 'R/W', or blank.
  This column indicates whether the SP can access the variable via the RMI Protocol, and if so, whether the SP is limited to only reading the value or if it can also set (write) it to

another value. When the value is R/W we do not prohibit setting an initial value via the SO, so R/W has an associated SO value of "opt".

These definitions imply the following relationships among the three columns:

- If M-D is 'yes':
  - SO will be blank, because there is no need to specify a mandated value on a Service Order. There is no option to select.
  - RMI will be either 'R' or blank. The SP may be able to read the value via the RMI just to verify the value, but cannot change it. Thus, R/W is not an option.

If M-D is blank, the nine possible combinations of SO and RMI are summarized in Table 7, and discussed below.

Table 7: Relationship of RMI and SO in Requirement Tables

		RMI		
		blank	**R**	**R/W**
Service Order	**Yes**	A static value agreed to by the SP and AP is specified on the SO, but the SP cannot check value via the RMI	A static value agreed to by the SP and AP is specified on the SO, and the SP can check value via the RMI	NA Because there is one static value, it cannot be configured to a different value by the SP
	Opt	If AP unilaterally specifies a static value (e.g., its UNI ID), it may optionally communicate this via the SO if it wishes to.	If AP unilaterally specifies a static value, it may optionally communicate this via the SO if desired, and the SP can check it via the RMI	The SP can specify the value via the RMI. Optionally an initial value can be set via the SO.
	blank	There is no variable related to the requirement	The variable is not a configured entity (e.g., counter values), but the SP can read the value via the RMI	NA When a value can be configured, specification via the SO is never precluded.

- When SO is 'yes', the SP and AP agree to a fixed value for the variable:
  - RMI will be either blank or 'R'. A value of 'R' allows the SP to check the value that was ordered. A value of 'R/W' is not valid because the SP cannot change the single agreed-upon value.
- Else if SO is 'opt', it may be optional for different reasons.
  - The AP may unilaterally specify a static value that does not require consultation with the SP (e.g., the AP UNI ID). It may optionally communicate this value to the SP via the SO. If RMI is blank, the SP cannot verify the value via the RMI Protocol, but if RMI is 'R', the SP can verify the value.

  - When the SP and AP agree that the SP can change (write) the value via the RMI Protocol, it is not *necessary* to also specify the value on the Service Order; but an initial value could be specified.

  When SO is 'opt', the AP has the option to implement a Service Order entry for an attribute, but whether it decides to or not is out of scope of this document.

- Else if SO is blank, RMI can be blank or 'R'.
  - When there is no variable related to the requirement, then RMI is blank.
  - A variable might not be a configured entity (e.g. measurement counters). An RMI value of 'R' allows the SP to read such counters.
  - The combination of RMI as 'R/W' and SO as blank is not valid, because when a value can be configured (implied by 'R/W'), specification via the SO is never precluded.

The above points imply that the RMI entry can be 'R' regardless of the value of M-D and SO. It can be 'R/W' only if M-D is 'blank' and SO is 'opt'.

A summary of the combinations is below. The values in the red box below were covered in more detail in Table 7.

Table 8: Combinations of RMI, SO, and M-D

RMI	SO	M-D	Characteristics
blank	blank	Yes	Single mandated value that cannot be read by SP
R	blank	Yes	Single mandated value that can be read by SP
R/W	blank	Yes	Not valid
All values	Yes or Opt	Yes	Not valid
blank	Yes	blank	Value specified in SO, cannot be read by SP
R	Yes	blank	Value specified in SO, can be read by SP
R/W	Yes	blank	Not valid
blank	Opt	blank	Value may be specified in SO, cannot be read by SP
R	Opt	blank	Value may be specified in SO, can be read by SP
R/W	Opt	blank	Value may be specified in SO and can be written by SP
blank	blank	blank	No value, or value internal to AP that SP has no access to
R	blank	blank	Value not specified but can be read, e.g. counters, status
R/W	blank	blank	Not valid

Finally, note that the AP is not restricted from reading any of the variables' values, as was mentioned earlier.

Most attributes will be instantiated by the AP, but some will be created/deleted by the SP. Specific object requirements will be covered in other documents.

7.2 Common Requirements

The common requirements are requirements that are shared by vNID Service Cases A and B. These requirements must be met by an AP vNID offering that supports either of the two cases.

7.2.1 Data Plane Requirements

The common data plane requirements are detailed below and address UNI, OVC per UNI, OVC, OVC End Point per ENNI, and ENNI requirements.

Requirements related to the flow of data on the RMI Connection within the AP network are discussed separately in Section 7.2.3.1.

The requirements in this section are consistent with MEF 33, with exceptions noted.

7.2.1.1 Common UNI Service Requirements

In the table below, the following new attributes are defined, in addition to the usual UNI attributes:

- The **AP UNI Identifier** is controlled by the AP. It is the identifier communicated between the AP and SP.
- The **SP UNI Identifier** is controlled by the SP. It can be equal to the UNI Identifier seen by the Subscriber as is defined in MEF 10.2.
- **UNI MTU_{max}** is the maximum MTU that the AP is able to support on the UNI. This value is agreed to by the SP and AP among the options offered by the AP.

Table 9: Common UNI Service Requirements

UNI Service Attribute	Requirement on Service Attribute Parameters and Values		RMI	SO	M-D
AP UNI Identifier	**[R4]**	The AP **MUST** allow the SP to read, via the RMI Protocol, the value the AP has assigned to the AP UNI Identifier.	R	Opt	
	[R5]	The AP UNI Identifier field **MUST** be a non-null RFC 2579 DisplayString, not containing the characters 0x00 through 0x1F.			
	[R6]	The AP UNI Identifier field **MUST** contain no more than 45 characters.			
SP UNI Identifier	**[R7]**	The AP **MUST** allow the SP to set values for the SP UNI Identifier via the RMI Protocol.	R/W	Opt	
	[R8]	The SP UNI Identifier field **MUST** be a non-null RFC 2579 DisplayString, but not contain the characters 0x00 through 0x1F.			
	[R9]	The SP UNI Identifier field **MUST** contain no more than 45 characters.			

UNI Service Attribute	Requirement on Service Attribute Parameters and Values	RMI	SO	M-D
Physical Medium	**[R10]** The AP **MUST** allow the SP to read, via the RMI Protocol, the value of the PHY which was specified via the Service Order.	R	yes	
	[R11] The PHY **MUST** be one of the PHYs listed in IEEE Std 802.3™-2012 [2] (excluding 1000BASE-PX-D and 1000BASE-PX-U). Note that IEEE Std 802.3-2012 includes 40 Gb/s and 100Gb/s.			
Speed	No additional constraints from definition in MEF 26.1 [59]; see Section 7.4. **[R12]** The AP **MUST** allow the SP to read, via the RMI Protocol, the speed and duplex mode of the UNI.	R	yes	
	[R13] When Auto-Negotiation is "off" and the UNI PHY is capable of more than one speed, the AP **MUST** allow the SP to specify among the supported speeds of the interface and the duplex mode.	R/W	Opt	
Auto-Negotiation	**[R14]** The AP **MUST** support the ability for the SP to set Auto-Negotiation to “on” or “off”, except when the setting of Auto-Negotiation is mandated to comply with IEEE Std 802.3. If the PHY is 1000 BaseT(X) and 1000 Mbit/s is a valid speed, the IEEE Std 802.3 requires Auto-Negotiation to be ‘on’.	R/W	Opt	
Auto-negotiated Speed	**[R15]** When Auto-Negotiation is “on” for copper interfaces, the AP **MUST** support Auto-Negotiation speeds of 10/100.	R		
	[D2] When Auto-Negotiation is “on” for copper interfaces, the AP **SHOULD** support Auto-Negotiation speeds of 10/100/1000.			
	[R16] When Auto-Negotiation is “on” for optical interfaces, the AP **MUST** support Auto-Negotiation speed at the (single) optical rate.			
Mode	No additional constraints from definition in MEF 10.2 [51], where mode is always full duplex. Note that this applies as well for PHY rates of 40 Gb/s or 100 Gb/s.	R		yes

UNI Service Attribute	Requirement on Service Attribute Parameters and Values	RMI	SO	M-D
MAC Layer	No additional constraints from definition in MEF 10.2 [51].	R	yes	
UNI MTU_{max}	**[R17]** The UNI MTU_{max} **MUST** be ≥ 1522 bytes. **[D3]** The AP **SHOULD** be able to support UNI MTU_{max} values greater than 1522, including 1600 and 2000. See MEF 22.1 for an example of need for 1600 bytes. MEF 20 R73 includes a desirable requirement for 2000 bytes. Other frame sizes may be useful, such as 9600 to support applications desiring jumbo frames.	R	yes	
UNI MTU Size	**[R18]** The AP **MUST** allow the SP to set via the RMI any UNI MTU Size supported by the AP that is ≤ UNI MTU_{max}[8]. **[R19]** The AP **MUST** include UNI MTU_{max} in the values it offers to the SP.	R/W	Opt	
Ingress Bandwidth Profile Per UNI	**[R20]** The AP **MUST NOT** specify an Ingress Bandwidth Profile Per UNI[9]. **[R21]** The AP **MUST** allow the SP to verify via the RMI Protocol that an Ingress BWP is not specified on a UNI supporting vNID Service.	R		yes
Egress Bandwidth Profile Per UNI	**[R22]** The AP **MUST NOT** specify an Egress Bandwidth Profile Per UNI. **[R23]** The AP **MUST** allow the SP to verify via the RMI Protocol that an Egress BWP is not specified on a UNI supporting vNID Service.	R		yes
Layer 2 Control Protocol Processing	L2CP considerations other than Link OAM are for further study.			

The following differences in this table from MEF 33 are noted:

- SP UNI Identifier is new.
- 40 Gb/s and 100 Gb/s speeds are included.
- Auto Negotiation and Auto Negotiated Speed requirements have been added.

[8] Note that UNI MTU Size by definition must be ≤UNI MTU_{max} .
[9] Bandwidth profile is specified per OVC, not per UNI.

- UNI MTU_{max} requirements are new.

Like MEF 33, E-LMI requirements are not addressed in this version of this document.

7.2.1.2 Common OVC per UNI Service Requirements

The common OVC per UNI requirements are defined below. Since an OVC can only associate one OVC End Point that is at a UNI (see MEF 26.1), these service attributes can be equivalently viewed as OVC End Point per UNI service attributes.

Table 10: Common OVC per UNI Service Requirements

OVC per UNI Service Attributes	Requirement/ Possible Values	RMI	SO	M-D
UNI OVC Identifier	No additional constraints from definition in MEF 26.1 [59]. The UNI OVC Identifier is set by the AP.	R	Opt	
Class of Service Identifier for Service Frames	**[R24]** The CoS Identifier for Service Frames **MUST** be the OVC End Point to which the Service Frame is mapped.	R		yes
Class of Service Name for Service frames	The AP assigns a single CoS Name, agreed to by the SP and AP. This is single because there is one CoS ID based on the OVC End Point.	R	yes	
Class of Service Label for Service frames	**[D4]** The AP **SHOULD** be able to support at least one CoS Label, as specified in MEF 23.1 [57]. Via the Service Order, the SP will specify the CoS Label to be assigned to the OVC, from among the CoS Label(s) supported by the AP.	R	yes	
Ingress Bandwidth Profile Per OVC End Point at the UNI	**[R25]** The AP **MUST** allow the SP to read the values of <CIR, CBS, EIR, EBS, CM, CF> associated with the OVC End Point at the UNI.	R	yes	

OVC per UNI Service Attributes	Requirement/ Possible Values		RMI	SO	M-D
Ingress Bandwidth Profile Per OVC End Point at the UNI – CIR	**[R26]**	The AP **MUST** be able to support CIR values[10] in at least the following increments: 1 – 10 Mb/s, increments of 1 Mb/s 10 – 100 Mb/s, increments of 10 Mb/s 100 – 1000 Mb/s, increments of 100 Mb/s 1 – 10 Gb/s, increments of 1 Gb/s 10-100 Gb/s, increments of 10 Gb/s.	R	yes	
	[O1]	The AP **MAY** support other values of CIR.			
Ingress Bandwidth Profile Per OVC End Point at the UNI – EIR, EBS, CF, CM	**[R27]**	The AP **MUST** allow EIR = 0, EBS = 0, CF = 0, CM = "color blind"	R	yes	
	[O2]	The AP **MAY** support other values of EIR, EBS, CF, and CM.			
Ingress Bandwidth Profile Per OVC End Point at the UNI - CBS	As specified in MEF 10.2 [51], when CIR > 0, CBS **MUST** be greater than or equal to the largest Maximum Transmission Unit size among all of the EVCs that the Bandwidth Profile applies to.		R	yes	
Ingress Bandwidth Profile Per Class of Service Identifier at a UNI	This attribute is not used. The SP can verify this via the read capability that a single CoS Name or CoS Label is assigned to the OVC. (See requirements above for CoS Name and CoS Label.)				
Egress Bandwidth Profile Per OVC End Point at a UNI	**[R28]**	The AP **MUST NOT** specify an Egress Bandwidth Profile Per OVC End Point at a UNI.	R		yes
	[R29]	The AP **MUST** allow the SP to verify via the RMI Protocol that an Egress BWP per OVC End Point at a UNI is not specified on a UNI supporting vNID Service.			

[10] MEF Bandwidth Profile traffic parameters such as CIR count only Service Frame bits, not interframe gap or preamble bits.
Setting the value of the CIR parameter for each OVC End Point such that the sum of the values is greater than 76% of the physical layer speed of the External Interface where the OVC End Points are located can have negative consequences. See Appendix A of MEF 33.

OVC per UNI Service Attributes	Requirement/ Possible Values	RMI	SO	M-D
Egress Bandwidth Profile Per Class of Service Identifier at a UNI	**[R30]** The AP **MUST NOT** specify an Egress Bandwidth Profile Per Class of Service Identifier at a UNI.	R		yes
	[R31] The AP **MUST** allow the SP to verify via the RMI Protocol that an Egress BWP per CoS Identifier at a UNI is not specified on a UNI supporting vNID Service.			

The following differences in this table from MEF 33 are noted:

- The single CoS ID requirement in MEF 33 is expressed as two requirements here; one on the CoS ID and one on the CoS Name.
- CoS Label support has been added as an option.
- The CBS requirement of MEF 33 is relaxed and aligns with MEF 26.1.

7.2.1.3 Common OVC Service Requirements

The common OVC Service requirements are defined below.

Table 11: Common OVC Service Requirements

OVC Service Attribute	Possible Values	RMI	SO	M-D
OVC Identifier	No additional constraints from definition in MEF 26.1 [59].	R		
OVC Type	**[R32]** The AP **MUST** specify the OVC Type as Point-to-Point.	R		yes
OVC End Point List	**[R33]** The AP **MUST** specify one OVC End Point at the UNI, and one at the ENNI. The AP specifies the End Point Identifier values, which can be communicated to the SP via the SO process.		yes	
Maximum Number of UNI OVC End Points	**[R34]** The AP **MUST** specify the Maximum Number of UNI OVC End Points to be 1.	R		yes
Maximum number of ENNI OVC End Points	**[R35]** The AP **MUST** specify the Maximum number of ENNI OVC End Points to be 1.			yes

OVC Service Attribute	Possible Values	RMI	SO	M-D
OVC Maximum Transmission Unit Size	No additional constraints from definition in MEF 26.1 [59]. **[D5]** The AP **SHOULD** be able to support OVC MTUmax values greater than 1522, including 1600, and 2000. See MEF 22.1 for an example of need for 1600 bytes. MEF 20 R73 includes a desirable requirement for 2000 bytes. Other frame sizes may be useful, such as 9600 to support applications desiring jumbo frames.	R	yes	
CE-VLAN CoS ID Value Preservation	**[R36]** The AP **MUST** specify the CE-VLAN CoS Preservation to be Yes.	R		yes
S-VLAN ID Preservation	N/A as only one ENNI in the service.			
S-VLAN CoS Preservation	N/A as only one ENNI in the service.			
Color Forwarding	**[CR1]<** [O2] When EBR and/or EBS are non zero, the AP **MUST** configure Color Forwarding of the OVC to be Yes. The Color Identifier at the ENNI is specified in Table 12.	R		yes
Service Level Specification	**[D6]** The Service Level Specification provided by the AP **SHOULD** be based on CoS label H, M or L as specified in MEF 23.1 [53].	R	yes	
Unicast/Multicast/Broadcast Frame Delivery	**[R37]** The AP **MUST** specify the Unicast/Multicast/Broadcast Frame Delivery to be “Deliver Unconditionally”.	R		yes

The following differences in this table from MEF 33 are noted:

- There is more discussion on desirable values of OVC MTU
- MEF 33 specifies Color Forwarding as a Desirable Requirement (SHOULD). However, in this document we assume that the SP will require it because end to end performance can be negatively impacted by a service that promotes a yellow frame to green. See Section 7.2.15 of MEF 26.1.
- The Service Level Specification is specified differently.

- In MEF 33, the treatment of Unicast, Multicast, and Broadcast Frame Delivery differs between Access EPL and Access EVPL. In this document, the requirement matches the Access EPL requirement, and the assumption is that if the SP desires conditional delivery, the SP will implement the conditional treatment in its own network.

7.2.1.4 Common OVC End Point per ENNI Requirements

The common OVC End Point per ENNI requirements are defined below.

Table 12: Common OVC End Point per ENNI Requirements

OVC End Point per ENNI Service Attributes	Requirement / Possible Values	RMI	SO	M-D
OVC End Point Identifier	No additional constraints from definition in MEF 26.1 [59]. The OVC End Point Identifier is set by the AP.		Opt	
Class of Service Identifier for ENNI frames	**[R38]** The CoS Identifier for ENNI Frames **MUST** be the OVC End Point to which the ENNI Frame is mapped.			yes
Class of Service Name for ENNI frames	**[R39]** The AP **MUST** support a single CoS Name which is associated with the entire set of S-Tag PCP values {0-7}.		yes	
Ingress Bandwidth Profile Per OVC End Point at the ENNI - CIR	**[R40]** The AP **MUST** be able to support CIR values in at least the following increments: 1 – 10 Mb/s, increments of 1 Mb/s 10 – 100 Mb/s, increments of 10 Mb/s 100 – 1000 Mb/s, increments of 100 Mb/s 1 – 10 Gb/s, increments of 1 Gb/s 10-100 Gb/s, increments of 10 Gb/s.		yes	
	[O3] The AP **MAY** support other values of CIR.			
Ingress Bandwidth Profile Per OVC End Point at the ENNI – EIR, EBS, CF, CM	**[R41]** The AP **MUST** be able to support values of EIR = 0, EBS = 0, CF = 0, CM = "Color Aware".		yes	
	[O4] The AP **MAY** support other values of EIR, EBS, and CF.			
Color ID Mechanism	The Color ID mechanism could be DEI or PCP. **[D7]** The AP **SHOULD** be able to support a Color ID mechanism using DEI.		yes	
Color ID Value	**[CR2]<** [D4] When a CoS Label is specified for an OVC, the AP **MUST** support Color ID values as specified in MEF 23.1.		yes	

OVC End Point per ENNI Service Attributes	Requirement / Possible Values	RMI	SO	M-D
Ingress Bandwidth Profile Per OVC End Point at the ENNI – CBS, EBS	As specified in MEF 26.1 [59], when the CIR > 0, CBS ≥ OVC MTU, and when the EIR > 0, EBS ≥ OVC MTU.		yes	
Ingress Bandwidth Profile Per Class of Service Identifier at an ENNI	**[R42]** The AP **MUST NOT** specify an Ingress Bandwidth Profile Per Class of Service Identifier at an ENNI.			yes
Egress Bandwidth Profile Per End Point at an ENNI	No additional constraints from definition in MEF 26.1 [59]. Note the CoS ID restrictions of [R38] .		yes	
Egress Bandwidth Profile Per ENNI Class of Service Identifier at an ENNI	No additional constraints from definition in MEF 26.1 [59]. Note the CoS ID restrictions of [R38] .		yes	
Trunk Identifiers	This attribute does not apply because the OVCs are always point-to-point.			

The following differences in this table from MEF 33 are noted:

- The single CoS Identifier attribute of MEF 33 is expressed here in two rows; one for CoS ID and one for CoS Name.
- This document mentions the Color ID mechanism, including a preference for DEI.
- A Color Mode value other than “Color Aware” is optional in MEF 33, but is not allowed in this document, because MEF 26.1 mandates Color Awareness.
- The CBS requirement of MEF 33 is relaxed and aligned with MEF 26.1.
- The Egress BWP per OVC End Point at an ENNI and Egress BWP per CoS ID at an ENNI are forbidden in MEF 33, but are not forbidden in this document.
- The Trunk Identifier attribute is explicitly mentioned in this document. However, because it does not apply, the result is the same in both documents.

7.2.1.5 Common ENNI Service Requirements

The common ENNI Service requirements are defined below.

Table 13: Common ENNI Service Requirements

ENNI Service Attributes	Requirement / Possible Values	RMI	SO	M-D
Operator ENNI Identifier	No additional constraints from definition in MEF 26.1 [59].		yes	
Physical Layer	No additional constraints from definition in MEF 26.1 [59].		yes	
Frame Format	No additional constraints from definition in MEF 26.1 [59].		yes	
Number of Links	No additional constraints from definition in MEF 26.1 [59].		yes	
Protection Mechanism	No additional constraints from definition in MEF 26.1 [59].		yes	
ENNI MTU Size	No additional constraints from definition in MEF 26.1 [59].		yes	
S-VLAN ID value in End Point Map	**[R43]** Exactly one S-VLAN ID at an ENNI **MUST** map to an OVC End Point that is associated with an OVC supporting an instance of vNID Service.		yes	
Maximum Number of OVCs	No additional constraints from definition in MEF 26.1 [59].		yes	
Maximum Number of OVC End Points per OVC	No additional constraints from definition in MEF 26.1 [59].		yes	

Note that an ENNI can support multiple E-Access service instances. Thus, when an SP orders E-Access service, the ENNI could have been ordered previously. The ENNI information in the above table is listed for completeness, but only the End Point Map entry must be specified for every vNID Service order.

7.2.2 OAM Requirements

The common OAM requirements are detailed below. These include common requirements for Link OAM, SOAM FM and SOAM PM.

7.2.2.1 Port-Level and OVC-Level Counters

Port-level counts are needed per UNI, which are specified in MEF 15.

[R44] The AP **MUST** provide the SP access to port-level octet and frame counts specified in Section 8.2 of MEF 15, Requirements Group 31 and 33, plus R32.1 and R32.3 of Requirements Group 32, on a per-UNI basis, via the RMI Protocol.

R32.2 is not included because it applies to the Egress Bandwidth Profile.

Note that some of the MEF 15 requirements can apply to congestible resources other than the UNI; in this document we are interested in per-OVC counts at the UNI.

[R45] The AP **MUST** provide the SP access to per-OVC octet and frame counts at the UNI specified as mandatory in Requirements Group 32 of MEF 15, via the RMI Protocol.

[O5] The AP **MAY** provide the SP access to per-OVC octet and frame counts at the UNI specified as optional in Requirements Group 32 of MEF 15, via the RMI Protocol.

7.2.2.2 Link OAM Requirements

The requirements detailed here apply to the UNI supported by vNID Service and not to the ENNI. Support for Link OAM is optional for UNI 2.1 so the requirements detailed in this sub-section apply only if the AP vNID offering supports Link OAM.

The behavior implied by requirements in the below table are summarized here. If Link OAM can be supported on a given UNI by an AP, it can be Enabled or Disabled. When Link OAM is Enabled, the AP side (i.e., UNI-N) is required by IEEE Std 802.3 to be set to the Active mode, and the Subscriber side can be set to either Active or Passive mode. Thus, Link OAM can be set to Enabled or Disabled via the RMI Protocol, but if Link OAM is enabled, the mode of the UNI-N must be set to Active.

Active mode for Link OAM indicates that a Link OAM connection is initiated by the Active mode device. It also means that Link OAM loopbacks are initiated by the Active mode device.

Table 14: Link OAM Requirements (Common)

Link OAM Function	Possible Value	RMI	SO	M-D
Link OAM Support	**[D8]** The AP **SHOULD** be able to support Link OAM functionality at the UNI-N. The SP will be able to read whether Link OAM is supported on a given UNI, via the RMI Protocol. If Link OAM is supported, no additional constraints from definition in MEF 20 [57] exist regarding the UNI-N.	R	Opt	

Pause frames	Note that Pause must be disabled when Link OAM is Enabled (see MEF 20 [57], R30). **[R46]** The AP **MUST** never let Service Frames containing the Pause protocol egress at the UNI. **[R47]** The AP **MUST** ignore and discard any ingress Service Frames at the UNI containing the Pause Protocol.			
Enable/ Disable Link OAM	**[CR3]**< [D8] If Link OAM is supported by the AP, the AP **MUST** allow the SP to set Link OAM to Enabled or Disabled via the RMI Protocol.	R/W	Opt	
Verification of Active mode when Link OAM is enabled	**[CR4]**< [D8] If Link OAM is supported by the AP, when enabled by the SP, the AP **MUST** allow the SP to verify that the mode is Active.	R	Opt	
Link OAM Loopback	**[CR5]**< [D8] If Link OAM is supported by the AP, the AP **MUST** allow the SP to set Link OAM Loopback to Enabled and Disabled via the RMI Protocol.	R/W	Opt	
Link OAM State	**[CR6]**< [D8] If Link OAM is supported by the AP, the AP **MUST** provide to the SP via the RMI Protocol the discovery state of the Link OAM, including notifications for OAM Events as defined in IEEE Std 802.3-2012 [2] 57.2.10.	R		

7.2.2.3 Common SOAM FM Requirements

The requirements in this sub-section apply to the UNI supported by vNID Service and any MEPs managed by the SP on that UNI. See Figure 7. The following guidelines apply:

- UNI 2.1 requires support for SOAM FM at the UNI ME.
- The AP needs to allow the SP to manage one MEP per OVC at the SP or EVC MEG Level. The SP may choose an SP ME MEP or an EVC ME MEP at its discretion. The SP can also request that a MIP be created at the ENNI for the chosen MEG Level.[11]

[11] This means that the AP and SP will agree what MEG Levels are used for the SP ME and the EVC ME (e.g., MEF 30.1 recommends values of 3 and 4 respectively), and the SP will specify which MEG Level it wants to use. The local behavior in the AP's network is the same regardless of whether the MEP is considered by the SP to be part of an SP ME or EVC ME.

- As explained in MEF 30.1, the Test ME is instantiated only when needed for testing. (Hence it is shown as a dashed line in the figure below.) When that ME is in effect, the SP will be able to monitor and manage the Test ME.
- The Subscriber MIP at the AP UNI could also be supported.

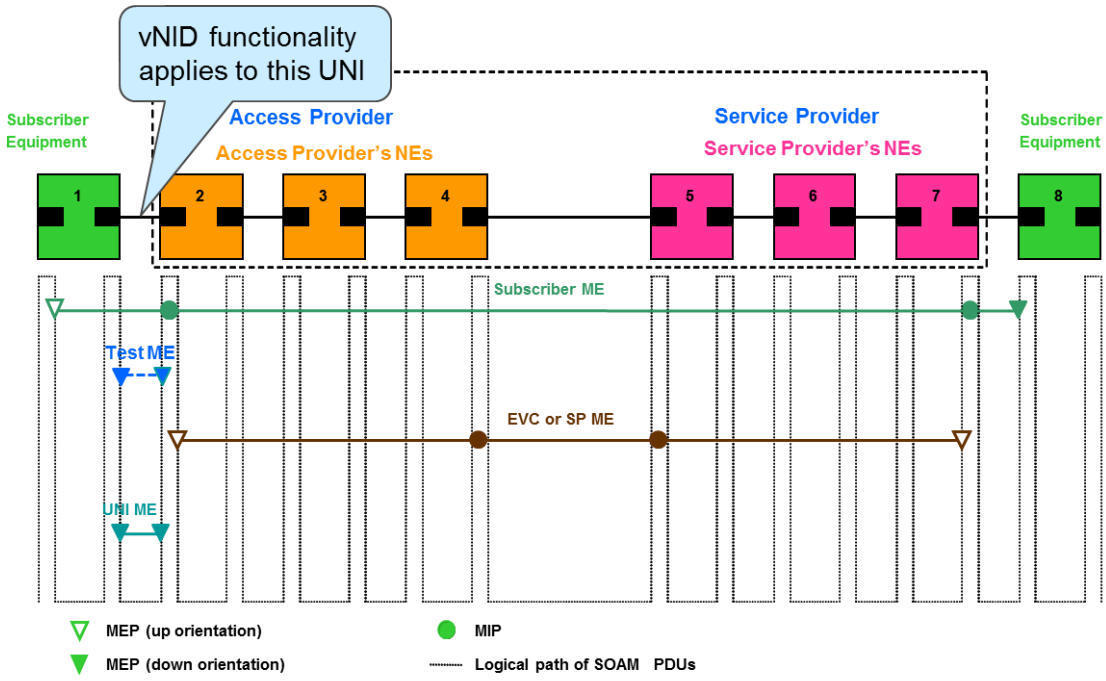

Figure 7: ME Levels to be Supported by vNID

Figure 7 shows an example where the SP / EVC ME is from UNI to UNI. Note that if an SP ME is selected, it does not necessarily terminate at the non-AP UNI.

Note that the AP's support of a ME does not imply that it always be active. Rather, it implies that the AP accepts requests from the SP to create and activate the specified MEP, and to read requested results.

[R48] The AP and SP **MUST** agree on the MEG Level to be used for each ME.

[D9] The AP and SP **SHOULD** use MEF 30.1 Default MEG Levels.

Test MEP: A Test MEP could be placed in one of many possible locations in theory. In the example shown in Figure 7, the Test MEG is at the UNI-N. As stated in MEF 30.1 there is incremental value in supporting the Test MEP at a UNI-N beyond the functionality provided by the UNI ME, because the Test MEG applies to an EVC and the UNI ME applies at the port level.

MEF 30.1 only requires that the SP support a Test MEP at a UNI-N in its network, and not at the AP's UNI-N. With the additional functionality offered to an SP by vNID Service, support at the AP's UNI-N is desirable.

Note that in Figure 7 if the Test ME is configured with one MEP in the customer's device #1 and the other in the SP's network (e.g., at device #7), then there are no Test MEPs or MIPs in the AP's network, and there are no requirements in scope of this document.

SOAM Configurations when the SP uses a VUNI: Figure 7 is only one of several SOAM arrangements in which the SP can provide Ethernet service.[12] Figure 8 shows an example where the SP implements a VUNI, and the overall configuration is very similar to UTA/VUNI description in MEF 28 [60]. Note that the EVC ME cannot extend into the AP's network in this example.

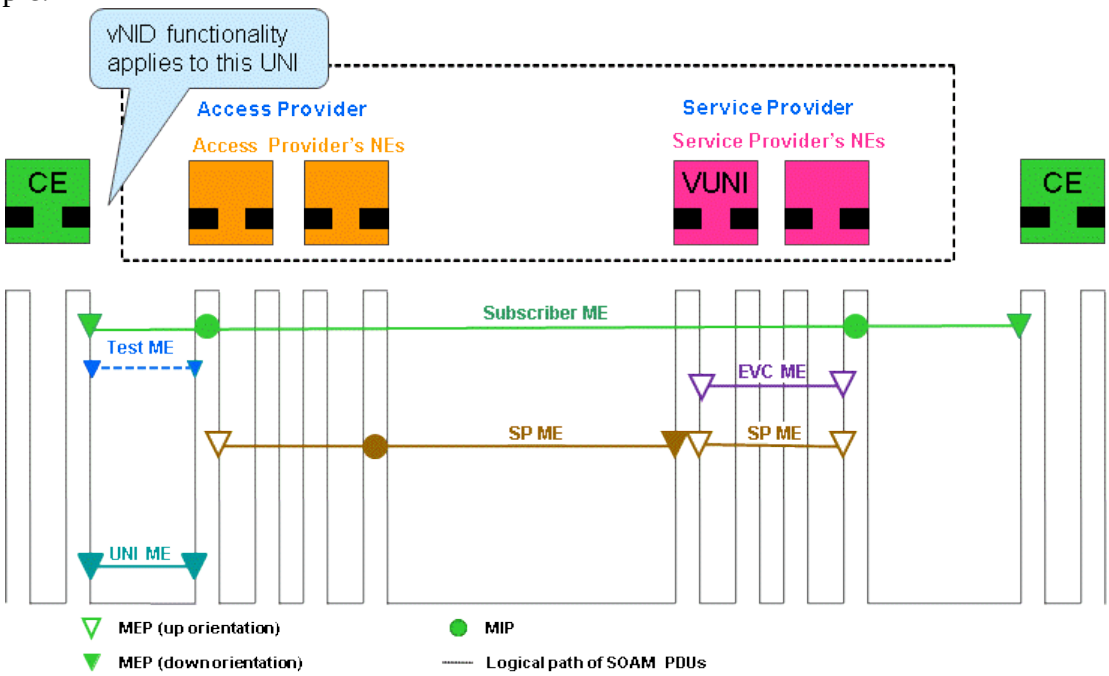

Figure 8: SOAM Example where the SP uses a VUNI

Common SOAM FM requirements are below.

[12] Recall that E-Access services specify functionality for the AP. The SP could choose to provide functionality that results in an end-to-end Ethernet service, but is not obligated to do so. For example, the E-Access service could just provide connectivity to a Layer 3 VPN service that the SP offers. However, these examples of SOAM assume that the SP is offering Ethernet service.

Table 15: Common SOAM FM Requirements

SOAM FM Function	Requirement / Possible Value	RMI	SO	M-D
Configuration of UNI ME	**[R49]** The AP **MUST** be able to support the UNI ME as defined in MEF 30.1[61] and allow the SP, via the RMI Protocol, to set UNI ME parameters and variables as defined in MEF 30.1 [61]. Note that the SP can specify the UNI ME MEP ID and MEG ID via the RMI protocol.	R/W	Opt	
Configuration of SP and EVC ME	**[R50]** The AP **MUST** be able to support the SP ME and EVC ME for a given OVC End Point at the UNI, as defined in MEF 30.1 [61] and allow the SP, via the RMI Protocol, to be able to set ME parameters and variables as defined in MEF 30.1 [61]. Note that the SP will be able to create a MEP and specify the SP/EVC ME MEP ID and MEG ID via the RMI protocol.	R/W	Opt	
	For a given OVC, the AP needs to only be able to support one MEP on either the SP ME or the EVC ME. **[R51]** For a given OVC End Point at the UNI, the AP **MUST** be able to support one MEP on either the SP ME or the EVC ME.			
	[D10] The AP **SHOULD** support a MIP at the ENNI on an SP or EVC ME on an OVC, if requested by the SP via the Service Order process.			
Configuration of Test ME	**[R52]** The AP **MUST** be able to support the Test ME as defined in MEF 30.1 [61] and allow the SP, via the RMI Protocol, to be able to set Test ME parameters and variables as defined in MEF 30.1 [61]. Note that the SP can specify the Test ME MEP ID and MEG ID via the RMI protocol.	R/W	Opt	
Configuration of Test MEP	**[R53]** The AP **MUST** allow the SP to specify, via the RMI Protocol, a Down Test MEP at the UNI-N.	R/W	Opt	

SOAM FM Function	Requirement / Possible Value	RMI	SO	M-D
Configuration of Subscriber ME	**[D11]** The AP **SHOULD** support the Subscriber ME as defined in MEF 30.1 [61] and allow the SP, via the RMI Protocol, to be able to set Subscriber ME parameters and variables as defined in MEF 30.1 [61]. This allows the SP to create, via the RMI Protocol, a MIP at the Subscriber ME Level.	R/W	Opt	
Loopback Message Support	**[R54]** The AP **MUST** allow the SP, via the RMI Protocol, to initiate the generation of LBMs as defined in MEF 30.1 [61] for each UNI, SP, EVC, and Test ME supported. Note that MEPs will respond to received LBMs with Loopback Response Messages. MEF 30.1 does not support independently turning off Loopback responses by a MEP.	R/W	Opt	
Linktrace Message Support	**[R55]** The AP **MUST** allow the SP, via the RMI Protocol, to initiate the generation of LTMs as defined in MEF 30.1 [61] for each UNI, SP, EVC, and Test ME supported. Note that MEPs will respond to received LTMs with Linktrace Response Messages. MEF 30.1 does not support independently turning off Linktrace responses by a MEP.	R/W	Opt	
CCM	**[R56]** The AP **MUST** provide the SP the ability to configure and enable CCM via the RMI for each UNI, EVC, and SP ME supported.	R/W	Opt	
UNI ME CCM Transmission Period	**[R57]** The AP **MUST** be able to support the required CCM transmission periods of 1s and 10s defined in the CCM section of MEF 30.1 [61] for the UNI ME.	R/W	Opt	
EVC and SP ME CCM Transmission Period	**[R58]** The AP **MUST** be able to support the required CCM transmission periods of 1s and 10s defined in the CCM section of MEF 30.1 [61] for the EVC and SP ME supported.	R/W	Opt	

SOAM FM Function	Requirement / Possible Value	RMI	SO	M-D
Loopback, Link Trace, and Continuity Check Results Support	**[R59]** The AP **MUST** allow the SP, via the RMI Protocol, to read the MIB objects defined in MEF 31 [62] related to UNI, EVC, SP, and Test MEPs running Loopback, Linktrace, and Continuity Check processes, as defined in MEF 30.1 [61]. Note that this includes reading of the results of initiated tests.	R		
Configuration of AIS	**[D12]** The AP **SHOULD** allow the SP, via the RMI Protocol, to configure the AIS function at a MEP as defined in MEF 30.1 [61] for each UNI, SP, and EVC ME supported.	R/W	Opt	
AIS Status and Counters	**[D13]** The AP **SHOULD** allow the SP, via the RMI Protocol, to read the status and counters related to the AIS function at a MEP as defined in MEF 30.1 [61] for each UNI, SP, and EVC ME supported.	R	Opt	
Configuration of LCK	**[D14]** The AP **SHOULD** allow the SP, via the RMI Protocol, to configure the LCK function at a MEP as defined in MEF 30.1 [61] for each UNI, SP, and EVC ME supported.	R/W	Opt	
LCK Status and Counters	**[D15]** The AP **SHOULD** allow the SP, via the RMI Protocol, to read the status and counters related to the LCK function at a MEP as defined in MEF 30.1 [61] for each UNI, SP, and EVC ME supported.	R	Opt	

7.2.2.4 Common SOAM PM Requirements

Support of PM-1 is required, which in turn requires the AP to support common requirements (e.g. Performance Monitoring life cycle requirements) in Section 9 of MEF 35. Note that MEF 35 does not specify any values of Δt for availability.

Table 16: Common SOAM PM Requirements

SOAM PM Function	Requirement / Possible Value	RMI	SO	M-D
SOAM PM support	**[R60]** The AP **MUST** be able to support the SOAM PM mandatory requirements of Section 9 (Common Requirements) of MEF 35 [65], with the exception of R1, R47, R48, and R50.	R/W	Opt	
	[D16] The AP **SHOULD** support the SOAM PM common desirable requirements of Section 9 and [R49] of MEF 35 [65].			
	[R61] The AP **MUST** allow the SP to specify the AP-supported settable parameters of Section 9 of MEF 35 [65], via the RMI Protocol.			
Availability Δt	**[R62]** The AP **MUST** allow the SP to specify the value of Δt for Availability, via the RMI Protocol, to any of the values supported by the AP.	R/W	Opt	
	[R63] The AP **MUST** be able to support a value of Δt = 1 second for Availability.			
	[O6] The AP **MAY** support values of Δt other than 1 second for Availability.			
	The SP needs to set Δt and the SLM PDU period to values that are compatible. For example, Δt needs to be an integer multiple of the SLM PDU period. **[R64]** The AP **MUST NOT** allow the SP to set values of Δt that are not an integer multiple of the SLM PDU period. Note that the SP must set the SLM PDU period to a value that allows this requirement to be met.			
Configuration of PM-1 parameters	**[R65]** The AP **MUST** allow the SP to set the required parameters for PM-1 as defined in Section 10 of MEF 35 [65] via the RMI Protocol.	R/W	Opt	

SOAM PM Function	Requirement / Possible Value	RMI	SO	M-D
Reading PM-1 measurements	**[R66]** The AP **MUST** allow the SP to read the required data and counters for PM-1 as defined in Section 10 of MEF 35 [65] for monitored MEs via the RMI Protocol. These are specified by the tables associated with R66 (Table 6), R67 (Table 7), and R87 (Table 9) of MEF 35.	R		

7.2.3 RMI Overview

The RMI concept is defined in this document to refer to the capability provided by the AP to allow the SP to set and/or read values for some attributes and managed objects within the AP network, and to receive alarms and performance data from the AP network. The RMI concept is a central part of the AP's vNID offering for all vNID use cases. In the AP's network, the key components are the RMI Connection, the RMI Protocol and the Remote Processing Entity (RPE).

The RMI Connection is the connection between the Service Provider Processing Entity (SPPE) and the RPE. The RMI Protocol is the management protocol (e.g., SNMP, NETCONF) that is supported by the RPE. The RPE is an abstract function within the AP network that processes the RMI Protocol commands and requests received via the RMI Connection. All of these RMI concepts are defined within this document.

It is noted that a low loss of RMI Protocol frames by the AP and SP is important for the proper operation of interactions between the RPE and the SPPE.

The details of how the AP manages its network (e.g., how an RPE communicates with network equipment), based on the information the RPE receives from the SP, is out of scope of this document.

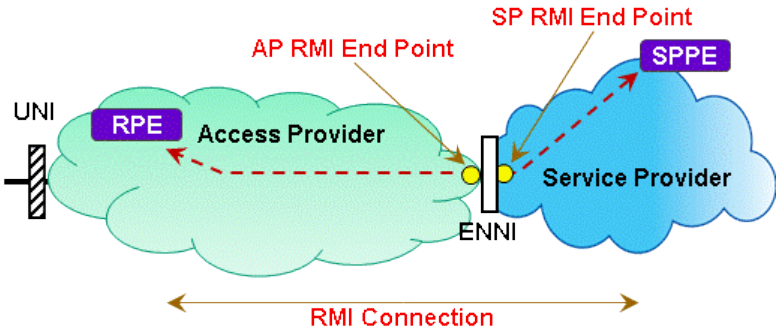

Figure 9: RMI Connection Overview

The RMI Protocol allows the SP to read and specify values for those parameters and variables that the SP is permitted to set, change or view as a part of the vNID offering. By using a standard RMI Protocol and associated information model, the Service Provider can interoperate with any Access Provider that supports vNID functionality.

The RMI Connection extends from the SP network across an ENNI to the RPE, as shown in Figure 9. The RPE terminates the RMI Connection within the AP network. While the RMI Connection is similar in some ways to EVCs and OVCs, it is not an EVC or an OVC because it terminates at internal interfaces.

An RMI Connection is always associated with a single SPPE at one end and a single RPE at the other end. An RMI Connection might exist for each UNI supported by vNID Service or there might be a small number (perhaps as low as one) of RMI Connections per SP-AP pairing[13]. Redundancy or protection methods may be used to ensure that a single failure does not keep an SP from accessing their vNID Services or receiving results or traps from the RPE. However, such methods are outside the scope of this document.

The AP might be required to configure an ingress and/or egress BWP on the AP RMI End Point (located at the ENNI), as shown in Figure 10. At the ENNI, the ingress BWP is set to ensure that the SP does not send more bandwidth than the AP RMI End Point has been configured to support. An egress BWP is configured at the ENNI-N of the AP to ensure that the RPE does not send more traffic than the SP has configured their network to support. The BWPs at the AP RMI End Point should be configured based on the needs of the RMI Connection, and would be ordered or negotiated as part of the Order process.[14] The PCP values in the S-Tag of RMI frames need to be set appropriately so that the SP and AP can handle the frames appropriately across their respective networks.

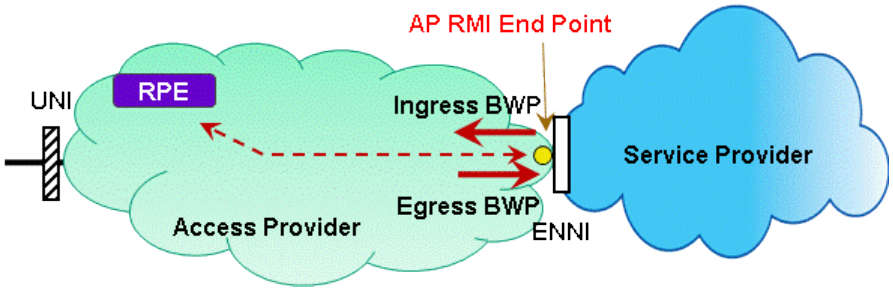

Figure 10: Ingress and Egress BWP at the AP RMI End Point

Each RPE has an IP address that is preferably specified by the SP and is configured for the SP by the AP. However, the AP may have constraints on the IP addresses it can support, so at a minimum the IP address is jointly agreed to by the SP and AP. The IP address, sub-network mask and gateway address are specified to the AP as part of the order process when IPv4 is used. The AP then configures the RPE with this information. In IPv4, the SP uses a standard ARP request to resolve the MAC address of the RPE, and then sends unicast frames containing the RMI Protocol to the RPE.

When IPv6 is used the SP and AP agree on an IPv6 prefix, and all other parameters should then be autodetected by the IPv6 protocol stacks.

[13] Currently every RMI connection uses an S-VLAN ID value at the ENNI. This should be considered when determining the preferred number of RMI connections.

[14] Note that the bandwidth needs might not be symmetric. For example, reports of statistical measurements will flow from the AP to the SP.

7.2.3.1 AP RMI End Point Requirements

The AP RMI End Point requirements are detailed below.

Table 17: AP RMI End Point Requirements

RMI Function	Requirement / Possible Value	RMI	SO	M-D
RMI Connection to RPE	**[R67]** An RPE **MUST** be associated with only one AP RMI End Point at any given moment.			yes
	[R68] A given AP RMI End Point **MUST** be associated with only one RPE.			yes
AP RMI End Point S-Tag VLAN ID	**[R69]** The AP and SP **MUST** agree to the value of the S-VLAN ID at the ENNI used to distinguish the RMI End Point from other services at the ENNI.		yes	
AP RMI End Point MTU Size	**[R70]** The AP **MUST** be able to support an MTU Size ≥ 1526 Bytes for the AP RMI End Point. This value aligns with MEF 26.1[59].		yes	
Ingress Bandwidth Profile at ENNI	**[O7]** The AP **MAY** instantiate an Ingress Bandwidth Profile at an AP RMI End Point.		yes	
	[CR7]< [O7] When an Ingress Bandwidth Profile per AP RMI End Point is in force, the algorithm and parameters described in Section 7.6.1 and 7.6.2 of MEF 26.1 [59] **MUST** be applied to all incoming ENNI Frames mapped to the RMI Connection.			
	[CR8]< [O7] When an Ingress Bandwidth Profile per AP RMI End Point is in force, the AP **MUST** be able to support values of EIR = 0, EBS = 0, CF = 0, CM = "Color Aware".			
	[CO1]< [O7] When an Ingress Bandwidth Profile per AP RMI End Point is in force, the AP **MAY** support other values of EIR, EBS, and CF.			
	[CR9]< [O7] When an Ingress Bandwidth Profile per AP RMI End Point is in force: When the CIR > 0, the CBS **MUST** be ≥ RMI End Point MTU Size, and When the EIR > 0, the EBS **MUST** be ≥ RMI End Point MTU Size.			

RMI Function	Requirement / Possible Value	RMI	SO	M-D
Egress Bandwidth Profile at ENNI	**[O8]** The AP **MAY** instantiate an Egress Bandwidth Profile at an AP RMI End Point.		yes	
	[CR10]< [O8] When an Egress Bandwidth Profile per AP RMI End Point is in force, the length and arrival times of the egress frames mapped to the AP RMI End Point **MUST** satisfy the Bandwidth Profile described in Section 7.6.1 and 7.6.3 of MEF 26.1 [59].			
	[CR11]< [O8] When an Egress Bandwidth Profile per AP RMI End Point is in force, the AP **MUST** be able to support values of EIR = 0, EBS = 0, CF = 0, CM = "Color Aware".			
	[CO2]< [O8] When an Egress Bandwidth Profile per AP RMI End Point is in force, the AP **MAY** support other values of EIR, EBS, and CF.			
	[CR12]< [O8] When an Egress Bandwidth Profile per AP RMI End Point is in force: When the CIR > 0, the CBS **MUST** be ≥ RMI End Point MTU Size, and When the EIR > 0, the EBS **MUST** be ≥ RMI End Point MTU Size.			

It is noted that SPPE-RPE communications could become inoperative for a while, or have intermittent poor performance. In this phase of this document, we are not addressing events such as inability to send change commands.

The RMI Connection is not required to support per-frame Class of Service. The S-Tag PCP markings carry no meaning unless otherwise agreed by the SP and AP, and thus are outside the scope of this document.

The AP and SP could agree to identify the RMI Protocol at the ENNI by a combination of the S-VLAN ID plus a C-tag value, but discussion of this point is out of scope at present.

7.2.3.2 RMI Protocol Message and RPE Requirements

The RMI Protocol Message format (plus the protocol-specific data model(s) defined outside of this document; e.g. SNMP MIB or NETCONF YANG) describes the format and types of RMI Protocol Messages that can be exchanged across an ENNI to set and/or read values for attributes of vNID functionality. This section specifies the mandatory and optional requirements for the RMI Protocol Message format as seen at an ENNI.

The RMI Protocol requirements mandate that the SNMPv2c format and procedures specified in RFCs 2578 [14], 2579 [15], and 2580 [16] be offered by the AP because it is simple, well-understood and ubiquitous. The RMI Protocol requirements allow the AP to additionally offer

the use of the NETCONF messaging format specified in RFCs 6241 [41] and 4742 [35] and/or the use of SNMPv3 or NETCONF over SSH.[15]

It is assumed that Service Providers will generate, receive and process RMI Protocol Messages in the Operations Support System (OSS) layer of their network. The OSS is typically an IP-based network where SNMP Messages (along with other protocols) are processed. Typically, a connectionless protocol such as UDP is used to transport SNMP datagrams between Managers residing in the OSS and Agents residing on Network Elements (NEs). Service Providers also require a dedicated S-VLAN to identify the RMI Protocol at the ENNI. Therefore, an RMI Protocol Message using SNMPv2c will take on the format described in Figure 11, which equates to SNMP over UDP over IP over IEEE Std802.1Q [1].

[R71] An RMI Protocol Message supporting SNMPv2c or SNMPv3 **MUST** have the format described in Figure 11 at the ENNI.

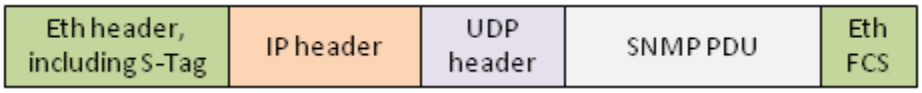

Figure 11: SNMP Message Format

As will be specified below, an AP can also choose to support SNMPv3.

The RMI can also use NETCONF as a supported protocol. An AP may decide that they want to support both SNMP and NETCONF.

[CR13]< [O10] When the AP supports NETCONF, an RMI Protocol Message supporting NETCONF **MUST** have the format described in Figure 12 at the ENNI.

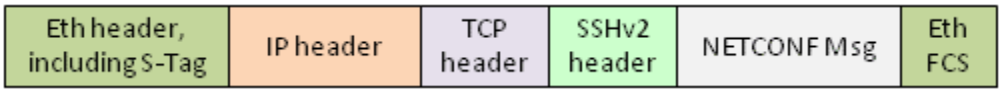

Figure 12: NETCONF Message Format

Support for IPv4 is required.

Vendors and/or carriers might not be ready to support IPv6 for initial implementations, so support for IPv6 is desirable but not required. If IPv6 is supported (as specified in requirement [D18] and its related requirements in Table 18) the addresses specified in RFC4291 [33], section 2.8, need to be supported.

For Unicast address assignment, the AP needs to:

- Support at least stateless address auto configuration according to RFC4862 [37] for the prefix
- Statically assign the suffix according to agreement between the AP and SP

The RPE requirements are detailed below. Recall that the phrase "able to support" a capability means that the AP must offer that capability to the SP as an option. However, in specific case(s) where the SP has not chosen that option, the AP would not support the functionality.

[15] To summarize, an AP must offer one or more RMI Protocols and the set of offered protocols is required to include SNMPv2c. The SP will select the RMI Protocol it desires from the AP's list.

Table 18: RPE Requirements

RPE Attribute/ Function	Requirement / Possible Value	RMI	SO	M-D
Support of RPE	**[R72]** The AP **MUST** provide an RPE that terminates the RMI Connection and supports the selected RMI Protocol for each RMI Connection to the SP.			
Identification of UNI to RPE	**[R73]** When an RPE supports more than one UNI, the RMI protocol (e.g., SNMP) **MUST** have a mechanism for identifying the UNI that each attribute in an RMI message applies to.		Opt	
RPE IP Address Assignment	**[R74]** The AP **MUST** support assigning a valid public or private IP address, jointly agreed to with the SP, to the RPE. Note that when IPv6 uses auto configuration, the specific address is selected via the auto configuration capability. **[D17]** The AP **SHOULD** support assigning any valid public or private IP address, specified by the SP, to the RPE.			
RPE IP Type	**[R75]** The AP **MUST** support an RPE IP Type field, which specifies whether the RPE is using IPv4 or IPv6.	R	yes	
Required support of IPv4	**[R76]** The AP **MUST** be able to support IPv4 on the RPE as defined in RFC 791 [5].			
Support of ARP	**[R77]** When the RPE IP Type is IPv4, the AP **MUST** support ARP on the RPE as defined in RFC 826 [8].			
ICMP Enablement for IPv4	**[R78]** The AP **MUST** be able to support ICMP on the RPE as defined in RFC 792 [6], and indicate via the RMI Protocol whether ICMP is currently enabled. ICMP is used to implement both Ping and Traceroute.	R	Opt	
IPv4 Address	**[R79]** When the RPE IP Type is IPv4, the AP **MUST** configure the RPE IPv4 Address supplied on the Service Order.	R	yes	
IPv4 Subnet Mask ("IPv4 Prefix Length")	**[R80]** When the RPE IP Type is IPv4, the AP **MUST** configure the RPE IPv4 Subnet Mask supplied on the Service Order.	R	yes	

RPE Attribute/ Function	Requirement / Possible Value	RMI	SO	M-D
IPv4 Gateway Address	**[R81]** When the RPE IP Type is IPv4, the AP **MUST** configure the RPE IPv4 Gateway Address supplied on the Service Order.	R	yes	
Support of IPv6	**[D18]** The AP **SHOULD** be able to support IPv6 according to RFC4291 [33], section 2.8[16] for an RPE.			
Indication of Ability to Support IPv6	**[R82]** The AP **MUST** indicate via the RMI Protocol whether the AP is able to support IPv6 as an option for this RPE.	R		
IPv6 Auto configuration Enablement	**[CR14]<** [D18] The AP **MUST** be able to support stateless address auto configuration (RFC4862 [37]) for the IPv6 Prefix for the Unicast address.	R	Yes	
	[CR15]< [D18] When an RPE's IP Type is specified as IPv6 and when auto configuration is specified as "enabled" on the Service Order, the AP **MUST** use stateless address auto configuration (RFC4862 [37]) to determine the IPv6 Prefix for the Unicast address.			
IPv6 Prefix Length	**[CR16]<** [D18] When an RPE's IP Type is specified as IPv6, the AP **MUST** be able to support a Prefix Length of 64 bits. Other Prefix Lengths are allowed.	R	Opt	
	[CR17]< [D18] When an RPE's IP Type is specified as IPv6, the AP **MUST** configure the IP Prefix Length value, agreed to by the AP and SP.			
IPv6 Address (when auto configuration is not used)	**[CR18]<** [D18] When an RPE's IP Type is specified as IPv6 and if auto configuration is NOT enabled, the AP **MUST** configure the IPv6 Address agreed to by the AP and SP.	R	Yes	
IPv6 Static Suffix (when auto configuration is used)	**[CR19]<** [D18] When an RPE's IP Type is specified as IPv6 and when auto configuration is enabled, the AP **MUST** provision a Static Suffix for stateless address auto configuration of a Unicast address.	R	Yes	

[16] Support of IPv6 in the future will be a critical feature. For initial implementations, IPv6 is considered a capability that vendors and/or carriers might or might not be ready to support.

RPE Attribute/ Function	Requirement / Possible Value	RMI	SO	M-D
IPv6 Gateway Address (when auto configuration is not used)	**[CR20]<** [R75] When the RPE IP Type is IPv6 and if auto configuration is NOT enabled, the AP **MUST** configure the IPv6 Gateway Address supplied on the Service Order by the SP.	R	Yes	
Support of Router Discovery	**[CR21]<** [D18] When the RPE IP Type is specified as IPv6 and if auto configuration is enabled, the AP **MUST** support routing based on router discovery from the Neighbor Discovery Protocol, as defined in RFC 4861 [36].			
ICMP Enablement for IPv6	**[CR22]<** [D18] When an RPE's IP Type is specified as IPv6, the RPE **MUST** be able to support ICMPv6 as defined in RFC 4443 [34], and indicate via the RMI Protocol whether ICMP is currently enabled. ICMPv6 is used to implement both Ping and Traceroute.	R	Opt	
List of RMI Management Protocols Supported	**[R83]** The AP **MUST** allow the SP to read the list of RMI Protocols (i.e. SNMPv2c, SNMPv3, or NETCONF) the AP supports.	R	Opt	
	[R84] The AP's list **MUST** include SNMPv2c, which requires support for the PDU format and procedures defined in RFCs 2578 [14], 2579 [15], and 2580 [16].			
	[O9] The AP's list of RMI Protocols **MAY** include SNMPv3, which requires support for the PDU format and procedures described in RFCs 3411 to 3418 ([18], [19], [20], [21], [22], [23], [24], and [25]).			
	[O10] The AP's list of RMI Protocols **MAY** include NETCONF as defined in RFC 6241 [41].			
Selected RMI Management Protocol	**[R85]** The AP **MUST** allow the SP to select for a given RPE any protocol in the AP's RMI Protocol list via the Service Order process.		Yes	
Support of SSHv2	**[CR23]<** [O10] If the AP supports an RMI Protocol using NETCONF, it **MUST** support the mandatory SSHv2 transport mapping specified in RFC 4742 [35].			

RPE Attribute/ Function	Requirement / Possible Value	RMI	SO	M-D
RPE Notification IP Address(es)	**[R86]** The AP **MUST** allow the SP to specify for each RPE up to three destination IP addresses that notifications defined in the administrative sub-section are sent to,. If an RPE's IP Type is specified as IPv4, these addresses are expected to be IPv4. If an RPE's IP Type is specified as IPv6, these addresses are expected to be IPv6.	R/W	Opt	

7.2.3.3 RMI Security Requirements

The RMI Connection connects between the AP and the SP with each party involved in the function of the RMI. Ensuring that the RMI provides a secure interface between the two parties is extremely important. Some of the security issues raised with the RMI are not unique to it. These same issues exist when a SP or AP installs a NID at the Subscriber premises. This document does not intend to resolve these existing security issues. Issues that are unique to the RMI are addressed within this document.

It should be noted that SNMPv2 does not, by itself, protect against unauthorized access to sniffing the packets to obtain the community strings and user information, which could be used to gain unauthorized access into the managed system. SNMPv3 provides a security framework with enhancements supporting encryption, message integrity, and robust authentication. As stated earlier, NETCONF is implemented over SSHv2, which provides encryption to prevent unauthorized access to management information including user account access credentials.

Protecting the AP network from being adversely affected by the SP is a key requirement for an AP offering vNID functionality. The SP must not be able to reach beyond the vNID functionality into the AP's network or back office systems. There are several methods that are used to limit vulnerabilities to the AP network. These are shown below:

- Ensure that SP cannot use AP management network to reach other devices, parties or databases
  - ACLs based on source/destination IP address used in AP management network
  - No connectivity between AP and SP management VLANs
  - No routing allowed between SP and AP management IP subnets
- Ensure that the Subscriber cannot access RPE functionality via the UNI of the AP
  - The use of a separate S-VLAN ID at the ENNI for RMI Protocol Messages provides separation of Subscriber and RMI traffic
  - RMI Protocol Messages are not allowed to egress at the UNI
- Ensure that SP communicates only with the desired RPE.
  - RMI Connection limits access to single RPE

- RMI is limited by the data model to a subset of functionalities.

The SP is also concerned with ensuring that their network is not vulnerable to unauthorized access. Similar methods can be used to protect the SP network. These methods are beyond the scope of this document but possible examples are shown below:

- Ensure that AP cannot use SP management network to reach other devices, parties or databases
  - ACLs based on source/destination IP address used in SP management network
  - No connectivity between AP and SP management VLANs
  - No routing allowed between SP and AP management IP subnets
- Ensure that Subscriber cannot access SP management network
  - Rely on business relationship between AP and SP to ensure security of SP's configuration

The following table details the RMI security requirements.

Table 19: RMI Security Requirements

Security Attribute	Requirement / Solution	RMI	SO	M-D
Access to AP devices, parties or databases by SP	**[D19]** The AP **SHOULD** implement methods to ensure that the SP cannot access anything beyond the RPE, such as ACLs based on IP addressing, separate management VLAN IDs, and/or no routing between AP and SP sub-nets.			
Access to AP devices, parties or databases by Subscriber	**[R87]** The AP **MUST** ensure that RMI Protocol messages that ingress at the UNI do not reach the RPE.			
	[R88] RMI Protocol Messages **MUST NOT** be allowed to egress at the UNI.			
SP unable to modify AP controlled objects	**[R89]** The AP implementation of the RMI data model **MUST** limit write access to only those objects the SP can modify.			
AP unable to modify SP controlled objects within the vNID	Relies on business relationship between AP and SP.			

The intent is for the vNID Service to provide security comparable to today's single or two-NID configurations, but not to require the vNID Service to be significantly more secure than those alternatives. Thus, preventing illicit activities such as sniffing the RMI at the ENNI, spoofing the

SP or AP via the RMI or other methods of determining the RMI S-Tag VID, IP address, are outside the scope of this document.

7.2.4 Administrative Requirements

The administrative requirements cover items such as alarms, reporting SOAM information and performing backup and restoral of SP configuration.

7.2.4.1 Timing Needs

The vNID Service does not provide the tools for one way delay measurements and thus the need for Time of Day precision is quite relaxed. On the other hand, the vNID Service connects management domains from the Service Provider and from the Access Provider. Therefore it is important that both parties have a common timing reference. Only a common timing reference allows the Service Provider to reference received messages by a timestamp the Access Provider could look up as well. The rules set by RFC3339 [17] apply.

In case SNMP is used for the RMI, RFC1907 [10] defines for notifications the system up time (sysUpTime) value to be used, which is defined as:

```
sysUpTime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time (in hundredths of a second) since the network
            management portion of the system was last re-initialized."
```

The reference point for a trap is the re-initialization of a device and thus a relative time. For getting absolute values, the network management system of the Service Provider needs to query the vNID Service for time information instead of relying on local time information.

[R90] If SNMP is used, the AP **MUST** maintain timing information according to SNMPv2-TC, RFC2570 [12].

[R91] If NETCONF is used, the AP **MUST** maintain timing information as described in RFC5277 [39] and RFC3339 [17].

[R92] The AP **MUST** maintain a timezone value.

[R93] If SNMP is used, the vNID Service **MUST** provide actual local time information through a MIB object that defines Date and Time and the Offset from UTC for use by the vNID Service.

The Date and Time object is expected to be defined in the SNMP MIB for vNID Service.

[R94] If SNMP is used, the AP **MUST** allow SP to read the system up time via the RMI Protocol.

[R95] If SNMP is used, the AP **MUST** allow SP to read the Date and Time object via the RMI Protocol.

The SP could acquire correct time information with read access on the two MIB elements (system up time, Date and Time) in one run. This provides a read on the relative system up time counter and absolute time this refers to. With this information, notification timestamps can be translated into absolute time, as system up time will be restarted upon next reboot.

In case NETCONF is to be used for the RMI, the above outlined procedure could be skipped, as RFC5277 [39] mandates use of fully qualified absolute timestamps in notifications.

[R96] Accuracy of the time provided by the AP **MUST** be within +/- 1 second of Coordinated Universal Time (UTC) + local timezone offset.

In case UTC is used for time, the local timezone offset will be 0.

7.2.4.2 Administration State

[R97] The AP **MUST** allow the SP to set the administrative state of a UNI as up or down via the RMI Protocol.

[R98] The AP **MUST** allow the SP to set the administrative state of an OVC End Point at the UNI as up or down via the RMI Protocol.

It is assumed that the AP will be able to determine the status of a UNI or OVC End Point. However, this is beyond the scope of this document.

7.2.4.3 Notification Requirements

[R99] The AP **MUST** support using the RMI Protocol to deliver alarms/notifications to the SP.

[R100] The notifications presented in Table 20 **MUST** be delivered to the SP via the RMI Protocol.

Depending on which RMI Protocol is chosen (as discussed in Section 7.2.3), the notification requirements will be implemented with the appropriate data model specification (e.g., SNMP or NETCONF).

[R101] SOAM related notifications **MUST** apply to the UNI, SP and EVC MEs.

Notifications of SOAM FM and SOAM PM will indicate the MEG ID and MEP ID.

Table 20: Notifications (Mandatory Requirements)

Notification Name	Description	MIB Examples
UNI Link down	Link down condition on the UNI.	linkDown (IF-MIB)
UNI Link up	Link up condition on the UNI.	linkUp (IF-MIB)
SOAM Config Error Assert	A SOAM Config Error Assert notification is sent when a configuration error occurs during the setup for an SOAM FM entity, and provides a list of Interfaces and VLAN IDs that are incorrectly configured.	mefSoamConfigErrorAssertAlarm in SNMP (see MEF 31 [62])

Notification Name	Description	MIB Examples
SOAM Config Error Clear	A SOAM Config Error Clear notification is sent when a configuration error has been resolved during the setup for a SOAM FM entity, and provides a list of Interfaces and VLAN-IDs that are correctly configured.	mefSoamConfigErrorClearAlarm in SNMP (see MEF 31 [62])
SOAM MEP Operational Status	A SOAM MEP Operational Status notification is sent when the Operational State of a MEP changes. It indicates an operational state change in the MEP.	mefSoamMepOperStatusAlarm in SNMP (see MEF 31 [62])
SOAM MEP Administrative Status	A SOAM MEP Operational Status notification is sent when the Administrative State of a MEP changes.	mefSoamMepOperStatusAlarm in SNMP (see MEF 31 [62])
SOAM MEP Defect	A SOAM MEP Defect notification is sent when a MEP enters or exits the Defect state. (Note that this includes the Continuity Check Defect and RDI Defect.)	mefSoamMepDefectAlarm in SNMP (see MEF 31 [62])
SOAM Availability Change	A SOAM Availability Change notification is sent when the state of the availability of the indicated service changes.	mefSoamAvailabilityChangeAlarm in SNMP (see MEF 36 [66])
SOAM LM Session State Change	A SOAM LM Session State Change notification is sent when the state of the LM session changes; i.e., when it either starts or stops.	mefSoamLmSessionStartStopAlarm in SNMP (see MEF 36 [66])
SOAM DM Session State Change	A SOAM DM Session State Change notification is sent when the state of the DM session changes; i.e., it either starts or stops.	mefSoamDmSessionStartStopAlarm in SNMP (see MEF 36 [66])

[D20] The EVC and/or SP ME notifications presented in Table 21 **SHOULD** be delivered to the SP via the RMI Protocol.

Table 21: Notifications (Desired Requirements)

Notification Name	Description	Comments
SOAM LCK	An SOAM LCK notification is sent when reception of a LCK PDU causes the MEP to enter Lock State, or when the Lock State is exited. This notification is sent whenever the operational lock status of the MEP changes.	mefSoamLckAlarm in SNMP (see MEF 31 [62])
SOAM AIS	An SOAM AIS notification is sent when either AIS frames are starting to be sent by the MEP or when the MEP stops sending AIS frames, or when AIS PDUs are starting to be received or when AIS PDUs stop being received.	mefSoamAisAlarm in SNMP (see MEF 31 [62])

[R102] The following notifications from Link OAM **MUST** be delivered to the SP via the RMI Protocol if Link OAM is supported at the UNI.

Table 22: Link OAM Notifications (Mandatory Requirements)

Notification Name	Description	Comments
Link OAM Critical Link Event Rx	Link OAM Critical Event Received	See IEEE Std 802.3.1-2011 [3][2]
Link OAM Dying Gasp Rx	Link OAM Dying Gasp Received	See IEEE Std 802.3.1-2011 [3]
Link OAM Link Fault Rx	Link OAM Link Fault Received	See IEEE Std 802.3.1-2011 [3]
Link OAM Critical Link Event Tx	Link OAM Critical Event Transmitted	See IEEE Std 802.3.1-2011 [3]
Link OAM Link Fault Tx	Link OAM Link Fault Transmitted	See IEEE Std 802.3.1-2011 [3]

Note: The 802.3 Link OAM MIB supersedes the RFC 4878 [38] MIB and so is specified here.

Depending on which RMI Management Protocol is chosen (as discussed in Section 7.2.3), the notification requirements will be implemented with the appropriate MIB or model (e.g., SNMP or NETCONF).

7.2.4.4 Configuration Backup Requirements

Configuration backup concerns the ability of the SP to request from the AP a backup of the vNID configuration. The backup and restore capability can be offered by the AP, but it is not a requirement of the vNID Service.

If the AP offers a backup capability, the AP and the SP could agree to aspects such as frequency of scheduled backups, how to initiate unscheduled backups, and how to initiate restorals; the details of which are outside the scope of this document.

8 vNID Service Basic Case (Case B) Requirements

The requirements in this Section are specific to vNID Service Case B as defined in Section 6.2. They are broken down into two areas; data plane and OAM requirements. There are no Case B specific RMI or Administrative requirements.

8.1 Case B Data Plane Requirements

The Data Plane requirements for Case B include UNI Service Attributes, OVC per UNI Service Attributes, OVC End Point per ENNI Service Attributes, OVC Service Attributes and ENNI Service Attributes. These requirements are defined in the following sub-Sections, and are in addition to the requirements listed in the Common Requirements section.

The requirements in this section are consistent with MEF 33, with exceptions noted.

8.1.1 Case B UNI Service Requirements

The mapping of all Service Frames, tagged, untagged or priority tagged, into the OVC is required for Case B, as specified in this section.

Table 23: Case B UNI Service Requirements

UNI Service Attribute	Requirement / Service Attribute Parameters and Values	RMI	SO	M-D
Maximum number of OVCs per UNI	**[R103]** For UNIs supporting Case B, the AP **MUST** support a maximum number of OVCs per UNI = 1.	R		yes

8.1.2 Case B OVC per UNI Service Requirements

Table 24: Case B OVC per UNI Service Requirement

OVC per UNI Service Attribute	Requirement / Possible Value	RMI	SO	M-D
OVC End Point Map	**[R104]** For UNIs supporting Case B, the AP **MUST** configure the OVC End Point Map to contain all CE-VLAN ID values.	R		yes

8.1.3 Case B OVC Service Requirements

Table 25: Case B OVC Service Requirement

OVC Service Attribute	Possible Values	RMI	SO	M-D
CE-VLAN ID Preservation	**[R105]** For UNIs supporting Case B, the AP **MUST** specify the CE-VLAN ID Preservation to be Yes.	R		yes

8.1.4 Case B OVC End Point Per ENNI Requirements

See common requirements in Section 7.2.1.4.

8.1.5 Case B ENNI Service Attribute Requirements

See common requirements in Section 7.2.1.5.

8.2 Case B OAM Requirements

The Case B OAM requirements for SOAM FM and SOAM PM are detailed below. The requirements in this section allow the SP to configure SOAM at the EVC and Subscriber ME levels, and can be useful when the SP offers a single EVC. In instances where the SP has other configurations, an EVC MEG in the AP's network might not be reasonable or useful. For example, if the SP is employing a VUNI, a single EVC MEP could not be associated with EVC MEPs at UNI(s) in the SP's network.

8.2.1 Case B SOAM FM Requirements

The requirements specified in Table 15 in the common section allow the SP to configure SOAM at different ME levels. In some use cases, the SP uses the Case B OVC to offer a port-based EVC to the subscriber (see Figure 7), and the SP will be able to create an EVC MEP and a Subscriber MIP.

However, a Case B OVC could also be combined with an SP VUNI to support VLAN-based service. See Figure 8. In this use case, it is valuable for the AP to support the SP ME, but support for the EVC or Subscriber MEs would not be appropriate.

In sum, the AP needs to provide the SP with the option of supporting the SOAM capabilities for either scenario.

8.2.2 Case B SOAM PM Requirements

The common requirements specified in Table 16 apply to the ME specified by the SP (either SP ME or EVC ME) for the OVC.

9 vNID Service Advanced Case (Case A) Requirements

The requirements in this Section are specific to vNID Service Case A as defined in Section 6.3. They are broken down into two areas; data plane, and OAM requirements. There are no RMI or Administrative requirements unique to Case A.

9.1 Case A Data Plane Requirements

The Data Plane requirements for Case A include UNI Service Attributes, OVC per UNI Service Attributes, OVC End Point per ENNI Service Attributes, OVC Service Attributes and ENNI Service Attributes. These requirements for Case A are defined in the following sub-Sections, and are in addition to the requirements listed in the Common Requirements section.

The requirements in this section are consistent with MEF 33, with exceptions noted.

9.1.1 Case A UNI Service Requirements

Table 26: Case A UNI Service Requirements

UNI Service Attribute	Requirement / Service Attribute Parameters and Values		RMI	SO	M-D
Untagged and priority tagged frames	**[R106]**	For UNIs supporting Case A, the AP **MUST** allow the SP to specify, via the RMI, the CE-VLAN ID for untagged/priority tagged frames.	R/W	Opt	
Maximum number of OVCs per UNI	**[R107]**	For UNIs supporting Case A, the AP **MUST** support a maximum number of OVCs per UNI ≥ 1.	R	yes	
Maximum number of CE-VLAN IDs per OVC	**[R108]**	For UNIs supporting Case A, the AP **MUST** allow the SP to specify, via the Service Order, a Maximum Number of CE-VLAN IDs per OVC that is = 1.	R	yes	
	[D21]	For UNIs supporting Case A, the AP **SHOULD** allow the SP to specify, via the Service Order, a Maximum Number of CE-VLAN IDs per OVC that is > 1.	R	yes	

9.1.2 Case A OVC per UNI Service Requirements

In the End Point Map specification below, the AP is always required to support mapping at least one CE-VLAN to one OVC end point. Support for mapping more than one CE-VLAN to the same OVC end point is desirable.

It is optional for the AP to support mapping of all CE-VLAN IDs (including untagged and priority tagged frames) to a single OVC end point. With such a configuration, the mapping of service frames will have the same behavior as in Case B (hence the functionality of Case B can be considered a subset of functionality offered by Case A).

Table 27: Case A OVC per UNI Service Requirements

OVC per UNI Service Attribute	Requirement / Possible Value		RMI	SO	M-D
OVC End Point Map	**[R109]**	For UNIs supporting Case A, the AP **MUST** allow the SP to set values for the OVC End Point Map via the RMI.	R/W	Opt	
	[R110]	For UNIs supporting Case A, the AP **MUST** support all valid CE-VLAN ID values.			
	[R111]	For UNIs supporting Case A, the AP **MUST** allow the SP to map at least one CE-VLAN ID to a given OVC end point at the UNI.			
	[D22]	For UNIs supporting Case A, the AP **SHOULD** allow the SP to map more than one CE-VLAN ID to a given OVC end point at the UNI.			
	[O11]	For UNIs supporting Case A, the AP **MAY** allow the SP to map all CE-VLAN IDs to a given OVC end point at the UNI.			

The following differences in this table from MEF 33 are noted:

- Allowing the mapping of all CE-VLAN IDs to a given OVC end point at the UNI is a difference from MEF 33.

9.1.3 Case A OVC Service Requirements

For Case A it should be possible to disable CE-VLAN ID Preservation when the vNID Service supports an EVP-Line/LAN/Tree EVC with CE-VLAN ID Preservation disabled. Otherwise an attribute would be needed at the SP side of the ENNI to specify what CE-VLAN ID value to put in frames going from the SP to the AP.

Table 28: Case A OVC Service Requirement

OVC Service Attribute	Possible Values		RMI	SO	M-D
CE-VLAN ID Preservation	**[R112]**	For UNIs supporting Case A, the AP **MUST** allow the SP to specify CE-VLAN ID Preservation value to either Yes or No.	R/W	Opt	

The following difference in this table from MEF 33 is noted:

- MEF 33 requires CE-VLAN ID Preservation to be Yes.

9.1.4 Case A OVC End Point Per ENNI Requirements

See common requirements in Section 7.2.1.4.

9.1.5 Case A ENNI Service Attribute Requirements

See common requirements in Section 7.2.1.5.

9.2 Case A SOAM Requirements

The Case A OAM requirements are detailed below. These include requirements for SOAM FM and SOAM PM.

9.2.1 Case A SOAM FM Requirements

The common requirements of Table 15 allow the SP to configure SOAM at different ME levels in Case A. This can be useful, for example, when the SP uses the OVC to offer one or more EVCs to the subscriber. In instances where the SP has other configurations, an SP ME in the AP's network might not be reasonable or useful. However, the AP should provide the SP with the *option* of using this SOAM capability.

The ability to support one ME (either SP ME or EVC ME) per Case A OVC is required.

9.2.2 Case A SOAM PM Requirements

The common requirements specified in Table 16 apply to the ME specified by the SP (either SP ME or EVC ME) for each OVC.

10 References

[1] IEEE Std 802.1Q-2011, "Virtual Bridged Local Area Networks", 2011

[2] IEEE Std 802.3-2012, IEEE Standard for Ethernet, 28 December 2012.

[3] IEEE Std 802.3.1-2011, IEEE Standard for Management Information Base (MIB) Module Definitions for Ethernet, 5 July 2011

[4] IETF RFC 768, User Datagram Protocol, August 1980.

[5] IETF RFC 791, Internet Protocol, September 1981.

[6] IETF RFC 792, Internet Control Message Protocol, September 1981

[7] IETF RFC 793, Transmission Control Protocol, September 1981

[8] IETF RFC 826, Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48-bit Ethernet Address for Transmission on Ethernet Hardware, November 1982

[9] IETF RFC 959, File Transfer Protocol, October 1985

[10] IETF RFC 1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996

[11] IETF RFC 2119, Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997. (Normative)

[12] IETF RFC 2570, Introduction to Version 3 of the Internet-standard Network Management Framework, April 1999

[13] IETF RFC 2576, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, March 2000

[14] IETF RFC 2578, Structure of Management Information Version 2 (SMIv2), April 1999

[15] IETF RFC 2579, Textual Conventions for SMIv2, April 1999

[16] IETF RFC 2580, Conformance Statements for SMIv2, April 1999

[17] IETF RFC 3339, Date and Time on the Internet: Timestamps, July 2002

[18] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002

[19] IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), December 2002

[20] IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications, December 2002

[21] IETF RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002

[22] IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002

[23] IETF RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), December 2002

[24] IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), December 2002

[25] IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002

[26] IETF RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers, January 2006

[27] IETF RFC 4251, The Secure Shell (SSH) Protocol Architecture, January 2006

[28] IETF RFC 4252, The Secure Shell (SSH) Authentication Protocol, January 2006

[29] IETF RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, January 2006

[30] IETF RFC 4254, The Secure Shell (SSH) Connection Protocol, January 2006

[31] IETF RFC 4255, Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, January 2006

[32] IETF RFC 4256, Generic Message Exchange Authentication for the Secure Shell Protocol (SSH), January 2006

[33] IETF RFC 4291, R. Hinden, S. Deering, IP Version 6 Addressing Architecture, February 2006

[34] IETF RFC 4443, A. Contra, et. al., Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, March, 2006.

[35] IETF RFC 4742, T. Wasserman and T. Goddard, Using the NETCONF Configuration Protocol over Secure Shell (SSH), December 2006.

[36] IETF RFC 4861, T. Narten, et. al., Neighbor Discovery for IP version 6 (IPv6), September 2007.

[37] IETF RFC 4862, IPv6 Stateless Address Autoconfiguration, September 2007

[38] IETF RFC 4878, M. Squire, Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces, June 2007

[39] IETF RFC 5277, NETCONF Event Notifications, July 2008

[40] IETF RFC 6020, M. Bjorklund, Ed., YANG - A data modeling language for the Network Configuration Protocol (NETCONF), October 2010.

[41] IETF RFC 6241, R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, Network Configuration Protocol (NETCONF), June 2011.

[42] IETF STD 62, Simple Network Management Protocol Version 3 (SNMPv3), D. Harrington, R. Presuhn, B. Wijnen, J. Case, D. Levi, P. Meyer, B. Stewart, U. Blumenthal, K. McCloghrie, December 2002
(Note, this includes the package of RFCs 3411-3418)

[43] ITU-T Recommendation G.8013/Y.1731, Edition 3 (07/2001), "OAM functions and mechanisms for Ethernet based Networks".

[44] ITU-T Recommendation G.8021/Y.1341 (05/2012), Characteristics of Ethernet Transport Network Equipment Functional Blocks

[45] ITU-T Recommendation M.3100 (04/2005), Generic network information model.

[46] ITU-T Recommendation Q.840.1 (2007), Requirements and Analysis for NMS-EMS Management Interface of Ethernet over Transport and Metro Ethernet Network.

[47] MEF Technical Specification MEF 4, "Metro Ethernet Network Architecture Framework - Part 1: Generic Framework", May 2004.

[48] MEF Technical Specification MEF 6.1, "Ethernet Services Definitions - Phase 2", April 2008.

[49] MEF Technical Specification MEF 6.1.1, " Layer 2 Control Protocol Handling Amendment to MEF 6.1", January 2012.

[50] MEF Technical Specification MEF 7.2, "Carrier Ethernet Management Information Model", April 2013.

[51] MEF Technical Specification MEF 10.2, "Ethernet Services Attributes Phase 2", October 2009.

[52] MEF Technical Specification MEF 10.2.1, "Performance Attributes Amendment to MEF 10.2", January 2011.

[53] MEF Technical Specification MEF 12.1, "Carrier Ethernet Network Architecture Framework, Part 2: Ethernet Services Layer – Base Elements", April 2010.

[54] MEF Technical Specification MEF 15, "Requirements for Management of Metro Ethernet Phase 1 Network Elements", November 2005.

[55] MEF Technical Specification MEF 16, "Ethernet Local Management Interface (E-LMI), January 2006.

[56] MEF Technical Specification MEF 17, "Service OAM Requirements & Framework - Phase 1", April 2007.

[57] MEF Technical Specification MEF 20, "User Network Interface (UNI) Type 2 Implementation Agreement", July 2008.

[58] MEF Technical Specification MEF 23.1, "Carrier Ethernet Class of Service – Phase 2", January 2012.

[59] MEF Technical Specification MEF 26.1, "External Network Network Interface (ENNI) - Phase 2", January 2012.

[60] MEF Technical Specification MEF 28, "External Network Network Interface (ENNI) Support for UNI Tunnel Access and Virtual UNI", October 2010.

[61] MEF Technical Specification MEF 30.1, "Service OAM Fault Management Implementation Agreement: Phase 2", April 2013.

[62] MEF Technical Specification MEF 31, "Service OAM Fault Management Definition of Managed Objects", January 2011.

[63] MEF Technical Specification MEF 31.0.1, "Amendment to Service OAM SNMP MIB for Fault Management", January 2012.

[64] MEF Technical Specification MEF 33, "Ethernet Access Services Definition ", January 2012.

[65] MEF Technical Specification MEF 35, "Service OAM Performance Monitoring Implementation Agreement", April 2012.

[66] MEF Technical Specification MEF 36, "Service OAM SNMP MIB for Performance Monitoring", January 2012.

[67] MEF Technical Specification MEF 39, "Service OAM Performance Monitoring YANG Module", April 2012.

[68] MEF Technical Specification MEF 40, "UNI and EVC Definition of Managed Objects", April 2013.

[69] MEF Technical Specification MEF 42, "ENNI and OVC Definition of Managed Objects", October 2013.

[70] MEF Technical Specification MEF 44, "vNID Definition of Managed Objects", April 2014.

Appendix A Additional Motivation and Overview of the vNID Approach (Informative)

This appendix provides additional background on the motivation for defined vNID functionality.

Many Ethernet Subscribers are requiring national or even global connectivity. In order to meet Subscriber needs, Service Providers must be able to extend their Carrier Ethernet offerings beyond their normal footprint. This requires Service Providers to collaborate with Access Providers (APs) supporting UNIs at locations the SP needs to reach.

However, collaborations between Service Provider and APs present some unique challenges. Both the Service Provider and AP have interests at the Subscriber premises. The Service Provider owns the Subscriber relationship and is ultimately responsible for the end-to-end Carrier Ethernet service. The Access Provider owns the access network and has physical access to the Subscriber premises. The vNID functionality defined in this specification addresses these challenges. It defines a structure for how services can be configured by Service and Access Providers. This structure allows each provider to effectively manage their respective part of the Carrier Ethernet service.

The model in this specification includes functionality and constructs necessary for delivering Carrier Ethernet services.

A.1 Service Provider and Access Provider Roles

The Service Provider, by definition, is the single point of contact for the Subscriber. The Service Provider handles all technical support and billing functions to the Subscriber. In addition, the Service Provider wants to give a Subscriber a definable service offering at each location the Subscriber is requesting. This relationship between the Subscriber and the Service Provider is for defined services that are at the Subscriber's demarcation points; i.e., the UNI. How those services are actually implemented or enabled is the contractual responsibility of the Service Provider. In essence the Subscriber sees only defined services, but not how they are implemented.

If the Service Provider owns all the facilities between the Subscriber's UNIs, then the Service Provider's methods and procedures are largely internal, and are not defined by the MEF. A single Service Provider network topology example is depicted in Figure 13 below.

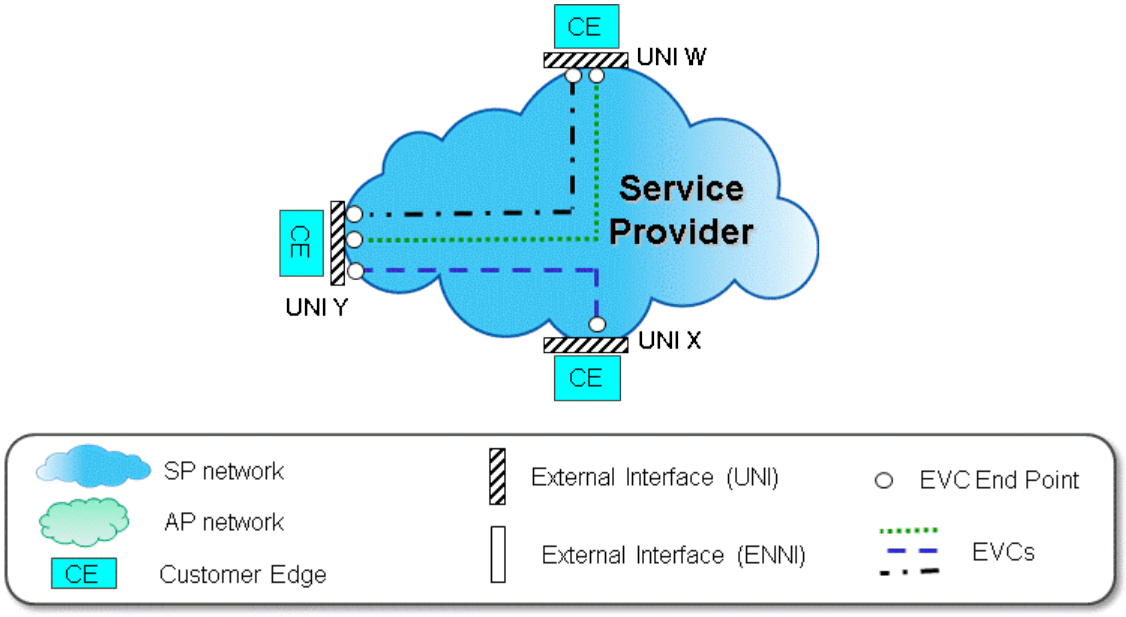

Figure 13: Single Service Provider Network Topology

When the Service Provider does not have direct access to a Subscriber demarcation point and has to go through a third party network (i.e., an Access Provider) to provide service, the desire of the Service Provider is to not affect the Subscriber. The Subscriber still wants the same service offerings, with the Service Provider as a single point of contact, and the AP in the middle is considered to be transparent to the Subscriber UNIs. This scenario changes several main components of the internal structure of the overall network that transports the Subscriber's traffic. What were once internal methods and procedures now involve multiple networks, as the interconnection needs to be defined between the Service Provider network and the AP network. An example of such a network topology is shown in Figure 14.

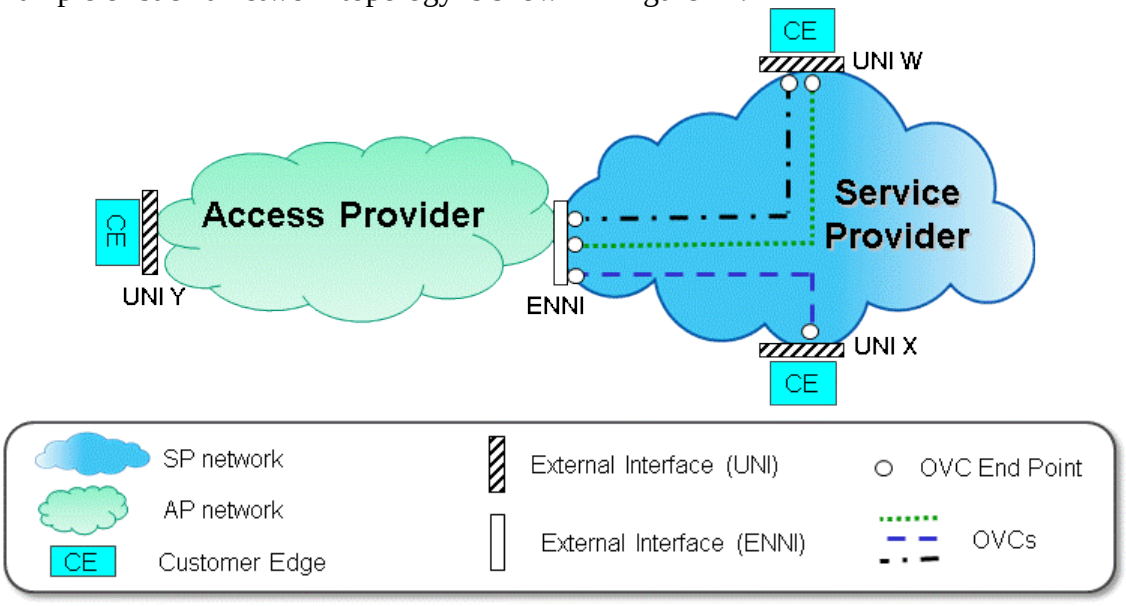

Figure 14: Network Topology with Two Networks

The MEF has addressed the interface between two networks with the ENNI specification (MEF 26.1), which includes the definition of the Operator Virtual Connection concept. The ENNI definition incorporates several aspects of defining how Subscriber traffic will flow across the networks to maintain the service offering that the Subscriber has negotiated with the Service Provider. The ENNI specification defines a set of behaviors on the interfaces, which allows the Service Provider and the AP to provision their interfaces with a known set of values for deterministic behavior.

A current deployment practice is to deploy two devices close to the Subscriber UNI; one owned by the Service Provider and one owned by the Access Provider. A key advantage of this model is that it provides Service Provider control near the Subscriber location, while providing strict separation of the AP and SP administrative responsibilities. However, it also has several undesirable characteristics. First, the SP must place a device at the Subscriber's location, and this may be difficult for reasons ranging from lack of installation personnel to difficulties in getting approval to place equipment in another country (homologation). In addition, each device introduces another failure point, and another possibility for mis-configuration or errored performance that complicates any troubleshooting effort. For the SP, servicing the remote device in a timely manner can be problematic.

A.2 vNID Functionality

To address these and other issues, this document specifies vNID functionality. To the Subscriber traffic plane, the resulting functionality should be identical, or almost identical, to the two-device model. The separation of the administrative domains is maintained. The vNID functionality specifications allow functionality to be defined for each administrative domain, but do not dictate where the functionality must be performed, only that it needs to be performed inside the domain. In other words, the vNID functionality does not specify an element, but rather of a model of behaviors for the AP to provide to the SP.

Where vNID functionality is to be deployed, there are a few assumptions that need to be specified. The first is that the AP owns all the network equipment at the Subscriber premises. As a result, it is also assumed that all general network element-level maintenance (e.g., repair) and network element-level administrative functions (e.g., software update) are the responsibility of the AP, since it owns the element(s).

However, other selected administrative functions are given to the SP to manage. Therefore, the AP's network element(s) must be capable of supporting functions of the Service Provider's administrative domain for services to the Subscriber and for interfacing to the AP.

A.2.1 Advantages of the vNID Approach

The main advantage of the vNID approach is the elimination of the need for the SP to deploy an additional element. Of course, the SP has the choice of placing its own NID at the Subscriber location (on the Subscriber side of the AP's network). This could be implemented via an ENNI interface between the SP's NID and the AP. Alternatively, the SP could choose to not place any equipment and rely on the AP to provide support of the interface to the Subscriber. However, relying on the AP to provide timely information, troubleshooting, and other information about all aspects of the Subscriber's service is expected to be risky. The SP will often desire more

information, more timely access to information, and control of some service aspects. The vNID approach is designed to meet this need.

A single edge element is intrinsically more reliable and easier to troubleshoot. The vNID approach does not remove any Subscriber service offerings. The AP maintains the administrative domain control over the interface into the AP network from the Subscriber premises element.

Appendix B Characteristics of VUNI in Support of vNID Service (Informative)

Most of the requirements to support vNID functionality apply to the AP only, and these have been defined in earlier sections. However, in order for the SP and AP to interoperate, the SP must clearly support compatible functions. For example, in order for the AP to respond to a standard SNMP or NETCONF command, the SP must initiate the command in a prescribed way. This appendix explains how the functionality of a VUNI[17] in a Service Provider's network can provide capabilities to complement and complete the functionality provided by vNID Service in support of VLAN-based services. This appendix provides guidance to Service Providers regarding the VUNI functionality they will need in their network to support various vNID scenarios, and in turn can form a basis for what capabilities a Service Provider may ask their vendors to support. This implies that an SP's equipment must meet certain requirements in order to be able to make use of certain vNID Services.

B.1 Background

vNID Service provides a means for the Service Frames of EVCs associated with a remote subscriber's UNI to be tunneled through an Access Provider's Carrier Ethernet Network (CEN) to an ENNI connecting that Access Provider's CEN with the Service Provider's CEN. With this arrangement, the Access Provider supports the vNID Service OVC (tunnel OVC) for transfer of Service Frames between the remote UNI and the ENNI. In addition, the service attributes related to the Subscriber service are distributed between the remote UNI (and associated vNID functionality) and the Virtual UNI (VUNI). Figure 15 shows an example of a VUNI for vNID Service when multiple CE-VLAN IDs map to the OVC at the UNI. This example could use Case A or Case B vNID Service.

[17] One example of VUNI is defined in MEF 28.

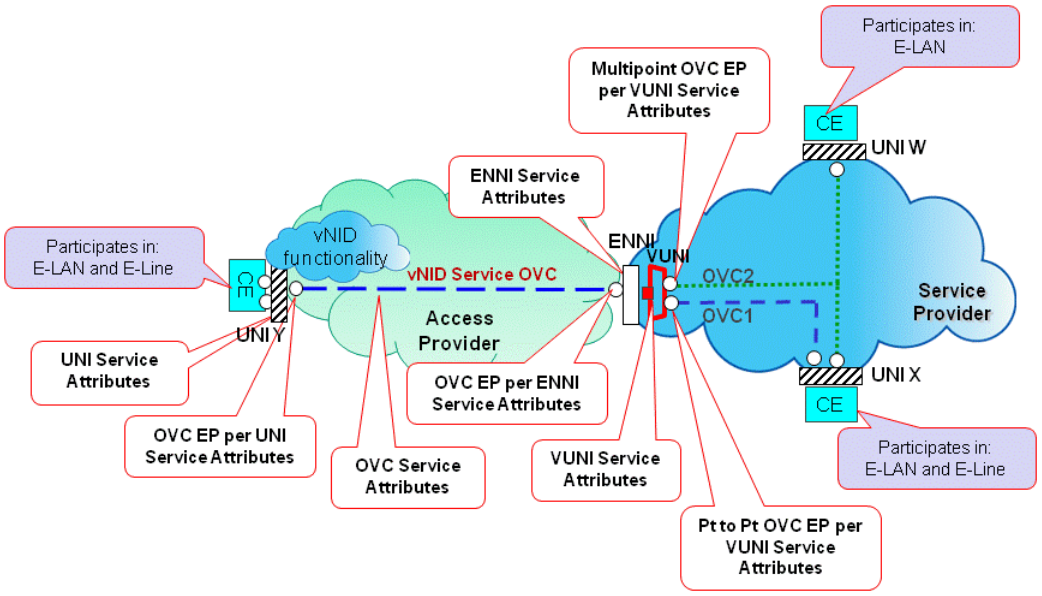

Figure 15: VUNI Example for vNID Service when >1 CE-VLAN IDs Map to the OVC

The VUNI in the Service Provider's CEN has service attributes similar to those of a UNI, and is paired with a remote UNI in the Access Provider's CEN. The VUNI is associated with a VUNI End Point at the Service Provider's side of an ENNI. Its main function is to specify the processing rules applicable to ENNI frames present in the Service Provider domain and associate them with a given service instance.

In Figure 15, two EVCs (an E-LAN EVC and an E-Line EVC) are available to the Subscriber at the remote UNI. The Access Provider is responsible for management of the vNID Service OVC between its side of the ENNI and the remote UNI. For vNID Services, the remote UNI and associated vNID functionality may support VLAN-based services, but the AP network is not aware of these aspects of the Subscriber EVCs.

Figure 15 shows an example where the CE at UNI Y participates in both the E-LAN EVC and E-Line EVC. At the remote UNI, Service Frames may be C-tagged, priority tagged, or untagged. The remote UNI is instantiated by the Access Provider as a UNI where the Access Provider maps multiple CE-VLAN IDs to the single OVC End Point supporting the vNID Service OVC. Traffic conditioning is applied at this remote UNI, and frames traverse the vNID Service OVC between the remote UNI and the ENNI. At the vNID Service OVC End Point at the Access Provider's side of the ENNI, an S-VLAN ID is used to map ENNI Frames to the OVC End Point supporting the vNID Service.

In the Service Provider's network, the relationship between the Access Provider's vNID Service OVC and the VUNI is realized by the S-VLAN ID present at the ENNI, whose value is negotiated between the Service Provider and the Access Provider. At the ENNI, when receiving an ENNI Frame, the Service Provider maps (using the End Point Map Service Attribute) a single S-VLAN ID to a VUNI End Point associated with a VUNI. The VUNI then maps each frame based on its CE-VLAN ID to the appropriate OVC End Point for OVC 1 or OVC 2. In the reverse direction, the VUNI multiplexes frames from OVC 1 and OVC 2 into the OVC denoted

by a unique S-VLAN ID, which is associated with the Access Provider's vNID Service OVC. Note that OVC 1 and OVC 2 must have non-overlapping CE-VLAN IDs at the VUNI.

Note that as per [MEF 28], a given ENNI can support more than one VUNI.

B.2 Behavior of the VUNI for vNID

This Section details the behavior of the Service Provider's VUNI that is associated with the ENNI related to the Access Provider's vNID Service OVC ("VUNI" in Figure 15). The VUNI attributes include mapping of the VUNI to the End Point associated with the Access Provider's vNID Service OVC, and mapping of ENNI Frames to one or more Service Provider OVC End Points in support of Subscriber services.

The characteristics of the VUNI for vNID are described by applying the following sets of attributes defined in [MEF 28]:

- VUNI Service Attributes.
- ENNI Service Attributes for the ENNI supporting the VUNI.
- Service Attributes for OVC End Points associated by the VUNI.

B.2.1 VUNI Service Attributes

The VUNI Service Attributes are described in [MEF 28]. This section describes how these VUNI service attributes focus on support of the vNID Service.

In order to describe the VUNI attributes, the concept of an ENNI CE-VLAN ID is defined in [MEF 28] for an ENNI Frame that is mapped to a VUNI End Point as follows:

- If an ENNI Frame is mapped to a VUNI End Point (depicted in Figure 15 as the red square on the right side of the ENNI) and the ENNI Frame has a C-Tag whose VLAN ID value is not zero, then the ENNI CE-VLAN ID for the ENNI Frame is the value of VLAN ID in the C-Tag.
- If an ENNI Frame is mapped to a VUNI End Point and the ENNI Frame either has no C-Tag or has a C-Tag whose VLAN ID value is zero, then the ENNI CE-VLAN ID is a value in the range 1, 2, …, 4094 that is agreed upon by both the Subscriber and the Service Provider supporting the VUNI.[18]

When a VUNI of MEF 28 is used to complement the vNID Service Case B, the VUNI service attributes and values need to be assigned according to Table 29.

Note, in Table 29, the Ingress Bandwidth Profile is applied at the VUNI to traffic that flows from the Subscriber at the remote UNI to the Service Provider CEN, and the Egress Bandwidth Profile is applied to traffic that flows from the Service Provider CEN to the Subscriber at the remote UNI.

A Service Provider may wish to consider applying a per VUNI bandwidth profile in the egress direction (from the Service Provider towards the Access Provider) in order to help ensure that the

[18] The value also needs to be agreed upon between the Service Provider and the Subscriber.

traffic is properly shaped to match up with the expected traffic conditioning function upon ingress to the Access Provider network at the OVC End Point for the vNID Service OVC.

Table 29: VUNI Service Attribute Constraints when Complementing vNID Service

VUNI Service Attribute (MEF 28)	Additional Constraints beyond MEF 28 Table 6 when VUNI is applied to vNID Service Case B
VUNI Identifier	*No Additional Constraints*
ENNI CE-VLAN ID value for ENNI Frames with no C-Tag or a C-Tag whose VLAN ID value is 0	*No Additional Constraints*
Maximum number of related OVC End Points in the VUNI Provider CEN	*No Additional Constraints*
Ingress Bandwidth Profile Per VUNI	Recommend to not specify
Egress Bandwidth Profile Per VUNI	*No Additional Constraints*

B.2.2 SP ENNI Service Attributes Supporting the VUNI

From the point of view of the vNID Service, the ENNI is the point of demarcation between the Service Provider CEN and the Access Provider CEN[19]. This section addresses the ENNI attribute constraints for vNID Case B associated with the Service Provider.

When VUNI attributes are enabled in support of the vNID Service, the ENNI Attributes as defined in Section 7.1 of MEF 26.1 [59] are applied to describe the behavior of the ENNI. However a specific attribute has been extended as described in the requirement below to allow for mapping of an S-VLAN ID at the ENNI to a specific VUNI End Point.

When VUNI of MEF 28 is used to complement the vNID Service Case B, at the ENNI in the Service Provider CEN, the End Point Type within an End Point Map for ENNI frames mapped to a VUNI needs to take the value of "VUNI"[20]

As per requirement [R16] of MEF 26.1 [59] and [R11] of MEF 28 [60], the End Point Map at the ENNI uses the S-VLAN-ID of a given S-Tagged ENNI Frame to determine the VUNI End Point to which an ENNI Frame is mapped.

B.2.3 SP Service Attributes for an OVC End Point associated by the VUNI

There are attributes for each instance of an OVC End Point associated with a specific VUNI.[21] These service attributes are described in Section 7.5 of MEF 26.1 and Section 7.3 of MEF 28.

For vNID Case B, traffic conditioning occurs for subscriber traffic at the VUNI for traffic entering the Service Provider network at the ENNI, for color declaration and to provide protection for the Service Provider network.

[19] These service attributes would remain the same in the case where an intermediate operator provides connectivity to the Access Provider supporting the remote UNI, as may be described in a Multi-CEN model.
[20] MEF 28 extends the End Point Type as defined in [R18] of MEF 26.1.
[21] Note that the OVC(s) discussed in this section are in the VUNI Provider CEN, as opposed to the vNID Service OVC that is in the Access Provider MEN.

When VUNI of MEF 28 is used to complement the vNID Service Case B, the OVC End Point's service attributes for an OVC End Point that is associated by a VUNI need to be configured with values according to Table 30.

Table 30: Service Attributes for OVC End Points Associated by the VUNI

Service Attributes for an OVC End Point associated by the VUNI (MEF 28)	Additional Constraints beyond MEF 28 Table 8 when VUNI is applied to vNID Service Case B (no change from MEF 28)
VUNI OVC Identifier	*No Additional Constraints*
OVC End Point Map	*No Additional Constraints*
Class of Service Identifiers	*No Additional Constraints*
Ingress Bandwidth Profile Per OVC End Point associated by a VUNI	May specify for point to point OVCs May specify for multipoint OVCs
Ingress Bandwidth Profile Per Class of Service Identifier associated by a VUNI	May specify for point to point OVCs May specify for multipoint OVCs
Egress Bandwidth Profile Per OVC End Point associated by a VUNI	May specify for point to point OVCs May specify for multipoint OVCs
Egress Bandwidth Profile Per Class of Service Identifier associated by a VUNI	May specify for point to point OVCs May specify for multipoint OVCs

B.2.4 VUNI Class of Service Identifiers

When VUNI of MEF 28 is used to complement the vNID Service Case B, there needs to be three mutually exclusive ways to determine the Class of Service Identifier from the content of a given ENNI Frame mapped to a VUNI as described in Section 7.3.1 of MEF 28 [60].

Appendix C Related MEF Source Documents

This section provides a brief summary of existing MEF specifications relating directly or indirectly to vNID functionality. This discussion is not intended to be complete or exhaustive. For additional information, refer to the corresponding MEF specification.

- **MEF 6.1** [48] defines Ethernet Service types and specifies their associated service attributes and parameters used to create Point-to-Point, Multipoint-to-Multipoint, and Rooted-Multipoint Ethernet services. **MEF 6.1.1** [49] augments MEF 6.1 to discuss L2CP handling.
- **MEF 7.2** [50] describes the overall Carrier Ethernet Management Information Model which identifies and defines the set of management information necessary to manage the Carrier Ethernet services as defined by the Metro Ethernet Forum, including support for the management aspects of vNID functionality.

- **MEF 10.2** [51], augmented with **10.2.1** [52], defines the attributes for Ethernet services, including Bandwidth Profiles (BWPs) and Performance Metrics. MEF 10.2 and MEF 10.2.1 have been superseded by MEF 10.3. However this vNID document aligns with MEF 10.2 and MEF 10.2.1.
- **MEF 12.1** [53] describes functional network models in support of MEF defined services, including vNID Services.
- **MEF 20** [57] defines requirements for UNI Type II interfaces or NEs with UNI Type II interfaces.
- **MEF 23.1** [58] defines a common CoS model for all EVC types, and defines performance objectives across different performance tiers (PTs) for the 3 CoS model.
- **MEF 26.1** [59] defines the requirements for the External Network Network Interface (ENNI). The document specifies a reference point that is the interface between two Carrier Ethernet Networks. Operator Virtual Connections (OVCs) are defined in this document. MEF 26.1 includes Service Level Specification Performance Metric definitions and related requirements.
- **MEF 28** [60] specifies requirements for UNI Tunnel Access (UTA) in an AP, relevant service attributes, Virtual UNI (VUNI) in an SP, and how they connect.
- **MEF 30.1** [61] specifies an Implementation Agreement for Service Operations, Administration, and Maintenance (SOAM) that builds upon the Fault Management (FM) framework and requirements specified in IEEE Std 802.1Q-2001 [1] and ITU-T Y.1731 [43]. It also defines the default configuration for different MEGs.
- **MEF 31** [62] defines SOAM FM Managed Objects.
- **MEF 33** [64] defines Ethernet Access Services, which are OVC-based Ethernet services in contrast to the EVC-based services which are defined in MEF 6.1. MEF 33 uses the UNI service attributes and parameters options defined in MEF 10.2 and ENNI and OVC service attributes defined in MEF 26.1, and applies them to create new Ethernet access services between a UNI and an ENNI. These new carrier-to-carrier Ethernet access services enable Ethernet Service Providers to reach customer locations through an Ethernet Access Provider's network, and deliver E-Line and E-LAN service types end to end to Subscribers.

  This vNID document draws heavily on the work of MEF 33, and is consistent and compatible with it except where noted.
- **MEF 35** [65]specifies an Implementation Agreement for Service Operations, Administration, and Maintenance (SOAM) for Performance Management (PM) requirements specified in ITU-T Y.1731. It uses the same SOAM foundation specified in MEF 30.1, but also addresses Performance Monitoring functionality.
- **MEF 36** [66] defines the SNMP MIB for SOAM PM Managed Objects.
- **MEF 39** [67] defines the NETCONF YANG Module for SOAM PM Managed Objects

- **MEF 44** [70] specifies the SNMP MIB aspects specific to supporting vNID functionality. It in turn draws upon the UNI-EVC MIB (MEF 40) and the ENNI-OVC MIB (MEF42).